THE DIOPHANTINE EQUATION

$$ax^3 + by^3 + cz^3 = 0.$$

By

ERNST S. SELMER
of Oslo.

Contents.

Index of Theorems.

Introduction.

In this paper, we shall be mainly concerned with the integer solutions of the homogenous Diophantine equation

$$ax^3 + by^3 + cz^3 = 0, \tag{1}$$

where a, b and c are rational integers, which we may suppose cubefree and coprime in pairs. — In the Introduction, I give a brief survey of the paper.

Chapter I treats more general topics such as:

The *Weierstrass* normal form for the curve (1), and the connection between this curve and the more special form (Theorem I, § 2)

$$X^3 + Y^3 = AZ^3, \qquad abc = A. \tag{2}$$

An extended field of rationality for the coefficients and unknowns of (1), in particular $K(\varrho)$, $\varrho = e^{\frac{2\pi i}{3}}$.

The exceptional points of the curves (1) and (2).

The finding of new solutions from other, known points on the curve (1).

The method of CASSELS [1][1] for proving the insolubility of (2). I have found some cases where his necessary conditions for solubility turn out to be *insufficient.*

Chapter II deals with the elementary solubility-conditions for the congruence corresponding to (1):

$$ax^3 + by^3 + cz^3 \equiv 0 \pmod{p^\delta}, \tag{3}$$

and also the more general case

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 \equiv Ez^3 \pmod{p^\delta}, \tag{4}$$

for different primes p and all exponents δ. For $p = 3$ or any prime dividing the coefficients — and in the second case also the discriminant of the left hand side — it is clear that we can form simple necessary criteria for solubility of the corresponding equations. The more difficult part of the problem is to show that the congruences are always soluble for all *other* primes p.

I also mention the more general congruence

$$\sum_{i=1}^{n} a_i x_i^3 \equiv 0 \pmod{p^\delta},$$

which is always soluble if $n \geqq 7$. The corresponding *equation* can be proved soluble for $n \geqq 9$.

---

[1] Numbers in square brackets denote references, see end of the paper. Cassels' results were published quite recently, but I was fortunate to have access to his paper in manuscript. — I must also express my gratitude to Dr. Cassels for correcting the English of the present paper, and for valuable help and suggestions during my work on it. I further owe my warm thanks to Prof. *Skolem* and Prof. *Mordell,* whose lectures on Diophantine analysis incited my investigations in this field.

If we multiply the equation (1) by a^2 and replace ax by $-x$, we get an equation

$$x^3 - my^3 = nz^3 \tag{5}$$

(where no longer necessarily $(m, n) = 1$). Chapter III deals with the corresponding ideal-equation in the purely cubic field $K(\sqrt[3]{m}) = K(\vartheta)$:

$$[x - y\vartheta] = \mathfrak{n}\mathfrak{a}^3,$$

where $\mathfrak{n}$ is an ideal from a finite set. This equation can sometimes be proved impossible by class-number considerations, the simplest case occurring when the class-number $h = 3$ and $\mathfrak{n}$ is not a principal ideal. If such an exclusion is not possible, we are led to a finite number of equations between integers of $K(\vartheta)$:

$$x - y\vartheta = \mu\alpha^3 = (e + f\vartheta + g\vartheta^2)(u + v\vartheta + w\vartheta^2)^3.$$

Equating the coefficient of ϑ^2 to zero, we get "the resulting cubic equation" in u, v and w; this is considered in Chapter IV. The insolubility of this equation can again be proved by congruence considerations, which now become rather complicated. To facilitate these considerations, an extensive theory of *cubic residues in the cubic field* $K(\vartheta)$ is developed in Chapters V and VI. By means of this theory, I can add new necessary conditions for solubility of (1) to the elementary congruence conditions drawn from (3) (Theorems II—VI. The conditions are also *sufficient for solubility of the congruence* corresponding to the resulting cubic equation.)

This is one of the main results of the paper. It is well known that the congruence conditions — together with solubility in real numbers — are *sufficient* for solubility of a homogenous quadratic equation (in any number of variables). It is further easily shown by elementary means that they are *not* sufficient in the quartic case, cf. my report [1]. But as far as I am aware, it has never been shown before that *the elementary congruence conditions are not sufficient for solubility of a homogenous cubic equation.* (SKOLEM [1] has proved a similar result for *inhomogenous* equations, cf. my report [1].)

The equations that can be excluded by my new methods are quite frequent, in average about 30 % of those of the examined equations which are possible for all moduli. The simplest example is

$$3x^3 + 4y^3 + 5z^3 = 0.$$

The results of my extensive calculations are given in Chapter VII, and in Tables 2^{a-c} and 4^b. I have treated systematically all equations (5) with

$2 \leqq m < n \leqq 50$, m and n cubefree, and also the form (1) with $abc \leqq 500$. I can *not* prove the sufficiency of my new conditions (in the case of $n = 1$ in (5), it is even possible to show their *insufficiency* for most m), but I have found solutions of nearly all equations which I cannot exclude. Some methods of numerical solution are indicated.

Two striking empirical facts emerge from the calculations:

1. In the case (5), with $2 \leqq m < n \leqq 50$, all excluded equations have been proved insoluble *in both fields* $K(\sqrt[3]{m})$ *and* $K(\sqrt[3]{n})$. — A single exception would have shown the insufficiency of my conditions in one field $K(\sqrt[3]{m})$ alone.

2. For a given cubefree integer A, we form all possible equations (if any) of the type (8). Then *the excluded equations seem to occur in groups of four*, with the same value of A. This is more precisely expressed in the *conjectures* of Ch. VII, § 4.

My methods also apply to the more general cubic equation corresponding to (4). As an example, Chapter VIII deals with *Sylvester's* equations

$$u^3 - 3u^2v + v^3 = 3pw^3 \tag{6}$$

$$u^3 - 3u^2v + v^3 = pw^3, \tag{7}$$

where p is a prime $\equiv \pm 1 \pmod 9$, or a product of such primes. These equations can be proved insoluble for several primes $p \equiv +1$ (Table 3), the smallest one in the two cases being $p = 73$ and $p = 271$ respectively, although the corresponding congruences are soluble for all moduli. — Under certain conditions (Theorem VII, § 5), the equations (6) and (7) cannot be *simultaneously* soluble.

The concluding Chapter IX deals with the equation $X^3 + Y^3 = AZ^3$. This has been studied by Sylvester [1], Pépin [1]—[3] and others, and many interesting results about insolubility are known. (The trivial solution with $Z = 0$ is not considered.) Most of the earlier proofs work with the theory of *quadratic forms*, which makes it necessary to treat the cases AZ odd or even differently; further every residue of A mod 9 must be considered separately. Hurwitz [1], Nagell [1] and Faddeev [1] have indicated how the first distinction can be avoided when working in the field $K(\varrho)$, $\varrho = e^{\frac{2\pi i}{3}}$. I carry this through systematically, and have found that all residues of A mod 9 can also be included in *one* formula. By means of this simplification and *the cubic law of reciprocity*,

I can give short proofs of all earlier results and add many of my own. As an application, I have treated all cubefree $A \leqq 500$ systematically (Table 4).

The method is one of "infinite descent", which takes 3 different forms:

1. If A is not of the forms 2. or 3. below, solubility of $X^3 + Y^3 = AZ^3$ implies solubility of at least one of the equations (Th. IX, § 4):

$$(8) \quad ax^3 + by^3 + cz^3 = 0, \; abc = A, \; 1 \leqq a < b < c, \; (a, b) = (a, c) = (b, c) = 1.$$

The original equation $X^3 + Y^3 = AZ^3$ is insoluble — I call it shortly "A is insoluble" — if all equations (8) are. This can in some cases be shown by congruence considerations (if an equation (8) exists at all); this leads to Theorem VIII, § 2 (*Sylvester*, *Pépin*), see Table 4[a]. But I can exclude several more equations (8) by my methods; these give 22 new insoluble values of $A \leqq 500$ (Table 4[b]).

2. If $A = p$ is a prime $\equiv \pm 1 \pmod 9$, a product of such primes or 9 times such a product, there is also another form of descent which leads to the equations (6) or (7) (Theorem X, § 5). Even if these can be proved insoluble for several primes $p \equiv +1 \pmod 9$, this does not necessarily imply the insolubility of A, since there are still other ways of descent in this case. (But see 3. below.)

3. If A contains one or more primes $\equiv +1 \pmod 3$, there are further possibilities depending on the fact that such rational primes are no longer primes in $K(\varrho)$. The superiority of working in $K(\varrho)$ instead of with quadratic forms is now clearly demonstrated. All earlier results in this case turn out to be particular cases of my two general Theorems XI (§ 8) and XII (§ 10), but I also give other, more special criteria for insolubility.

This descent leads to equations of the form (9.6.3):

$$(9) \qquad bu^3 + 3(a-b)u^2v - 3auv^2 + bv^3 = \frac{s}{3t} A_1 w^3,$$

where $\frac{s}{3t} = 3$ or $\frac{1}{9}$ and $A = A_1 \cdot (a^2 - ab + b^2)$. (The equations (6) and (7) correspond to $a = 0$, $b = 1$, $A = A_1$.) The excluded values of $A \leqq 500$ in Tables 4[c–d] (Th. XI—XII) and 4[e] are cases where (9) can be proved insoluble by congruence considerations. But these fail in the cases mentioned at the end of 2. above. For complete exclusion, I then have to extend the methods of Chapter VIII to the non-purely cubic fields defined by the left hand side of (9) (Table 4[f]).

A complete list of the excluded values of A in Tables 4^{a-f} is reproduced in Table 4^g; these are *all the cubefree values of* $A \leqq 500$ *which have been proved insoluble in the present paper* (indeed so far as I know all which have been proved insoluble at all).

Table 5 contains the equations (9) with $A \leqq 500$ which I cannot exclude one way or other; a solution is found in nearly all cases. — As in Tables 2^{a-c} and 3, *I believe that my solutions are the simplest possible, and that the unsolved equations are all soluble.*

The concluding §§ 15—18 deal with *the number g of generators (basic solutions) for an equation* $X^3 + Y^3 = A Z^3$. This has been studied by FADDEEV [1], both in the field $K(\sqrt[3]{A})$ and in the field $K(\varrho)$, but in the latter case only when A is a prime or the square of a prime. His methods in $K(\varrho)$ can be immediately extended to all cases where there are no soluble equations (8) (Th. XIII, § 15). By an improvement of his methods, I can also include this possibility of descent (Th. XIV, § 16). It turns out that *the number of generators can be found simply from the number of soluble descents* 1.—3. *above.* (The descents 2. and 3. must then be counted together.)

By means of Tables 2^b, 3 and 5, I have calculated *the basic solutions in Table 6*, which contains all cubefree $A \leqq 500$ not proved insoluble (Table 4^g). The only cases where no solution is found are given by (cf. 7.4.2 and 9.11.1):

$$A = 283,\ 337,\ 346,\ 382,\ 409,\ 445,\ 473,\ 499. \tag{10}$$

SYLVESTER ([1] pp. 313 and 316) stated that he knew whether or not any number $A \leqq 100$ is a sum of two cubes, cf. my historical remarks to 9.4.5 and 9.17.1.

The basic solutions of Table 6 for $A \leqq 50$ are also given by FADDEEV (but I choose the solutions for $A = 19$ and 37 differently). Some of the remaining solutions in Table 6 were given by LENHART (see DICKSON [1], Ch. XXI, ref. 186), but most of them have been found by me.

It turns out that *there are at most two generators for all* $A \leqq 500$. The smallest value of A with $g > 2$ is $A = 657$, where $g = 3$ (cf. 9.17.2—3).

CHAPTER I. General Remarks.

§ 1. The main object of the present paper is to examine the rational points on the cubic curve

1.1.1 $$ax^3 + by^3 + c = 0, \quad abc \neq 0, \quad a, b \text{ and } c \text{ rational},$$

or, what is the same, the integer solutions x, y and z (not all zero) of the homogenous indeterminate equation

1.1.2 $$ax^3 + by^3 + cz^3 = 0.$$

We may clearly suppose a, b and c to be *positive, cubefree* integers (since any cubed factor can be absorbed in the unknowns), and *coprime in pairs*:

1.1.3 $$(a, b) = (a, c) = (b, c) = 1,$$

if we exclude equations of the type (p any prime)

1.1.4 $$a_1 x^3 + p b_1 y^3 + p^2 c_1 z^3 = 0, \quad p \nmid a_1 b_1 c_1,$$

which are clearly insoluble. (We conclude in turn that p divides x, y and z. — The insolubility of this type of equation had been noted by EULER, see DICKSON [1], Ch. XXI, ref. 144.) If 1.1.2 is not of the type 1.1.4, and

$$a = p^i a_1, \quad b = p^i b_1, \quad p \nmid a_1 b_1 c, \quad i = 1 \text{ or } 2,$$

then $p \mid z$, $z = p z_1$, and

$$a_1 x^3 + b_1 y^3 + p^{3-i} c z_1^3 = 0,$$

where no longer two of the coefficients have the common divisor p.

When a, b and c are cubefree, we may also suppose that the unknowns are coprime in pairs:

1.1.5 $$(x, y) = (x, z) = (y, z) = 1.$$

§ 2. There is a close connection between 1.1.2 and the equations

1.2.1 $$X^3 + Y^3 = abc Z^3 \quad \text{(homogenous form)}$$

1.2.2 $$\eta^2 = 4\xi^3 - 27 a^2 b^2 c^2 \quad \text{(inhomogenous form)}.$$

The *invariants* g_2 and g_3 of both 1.1.2 and 1.2.1 are (cf. NAGELL [2], § 1)

$$g_2 = -\frac{27}{4} S = 0, \quad g_3 = \frac{27}{64} T = \frac{1}{2^6} \cdot 27 a^2 b^2 c^2$$

(the "equianharmonic" case, with $g_2 = 0$). Since rational 6^{th} powers can be removed from g_3, both equations can be transformed birationally into the *Weierstrass* normal form 1.2.2. The transformation of the general equation 1.1.2 is carried through by NAGELL [3], pp. 30—33. The coefficients can be made *rational* only if a rational point on the original curve is known. This is always the case for 1.2.1, with $(X, Y, Z) = (1, -1, 0)$, and the corresponding transformation into 1.2.2 is given by (cf. Ch. IX, § 15):

1.2.3
$$\frac{\xi}{3Z} = \frac{\eta}{9(X-Y)} = \frac{abc}{X+Y}.$$

The verification is immediate if we write 1.2.1 as

$$(X+Y)^3 + 3(X-Y)^2(X+Y) = 4abcZ^3,$$

or

$$1 + 3\left(\frac{X-Y}{X+Y}\right)^2 = 4abc\left(\frac{Z}{X+Y}\right)^3.$$

As an important consequence of the above relations, we see that 1.1.2 and 1.2.1 can be transformed into each other birationally with rational coefficients if one rational solution of 1.1.2 is known. In particular, we have the important

Theorem I. *A rational solution of the equation*

$$ax^3 + by^3 + cz^3 = 0, \qquad abc \neq 0,$$

with $xyz \neq 0$, *leads to a rational solution of*

$$X^3 + Y^3 = abcZ^3$$

with $Z \neq 0$ (i.e. $X + Y \neq 0$. The *converse* of this theorem is false, cf. the concluding remark of Ch. VII, § 4.) The actual formulae are given by

1.2.4
$$\begin{cases} X + Y = -9abcx^3y^3z^3 & (\neq 0) \\ X - Y = (ax^3 - by^3)(by^3 - cz^3)(cz^3 - ax^3) \\ Z = 3(abx^3y^3 + bcy^3z^3 + caz^3x^3)xyz. \end{cases}$$

These were first (in slightly different form) given by EULER, see DICKSON [1], Ch. XXI, ref. 183. We shall find the same result later (Ch. IX, § 4), when applying *infinite descent* to the equation 1.2.1.

A *permutation* of the terms ax^3, by^3 and cz^3 leaves the same solution 1.2.4 (possibly with an interchange of X and Y); this follows at once from the symmetrical form. — It is also easily verified that the conditions 1.1.3 and 1.1.5 imply

$$(X, Y) = (X, Z) = (Y, Z) = 1 \text{ or } 9.$$

There is an interesting birational connection between 1.2.2 and the equation

1.2.5 $$\eta_1^2 = 4\xi_1^3 + a^2b^2c^2,$$

cf. BILLING [1], Ch. V. The transformation 1.2.4 can be obtained rather simply by writing 1.2.5 as

$$(\eta_1 + abc)(\eta_1 - abc) = 4\xi_1^3$$

and drawing some immediate conclusions about the factors of the left hand side.

§ 3. Throughout this paper, we shall suppose the coefficients a, b and c in 1.1.2 to be *rational* integers, and the same for x, y and z. From some points of view, it may seem more natural to extend the domain of the unknowns to the field

$$K(\sqrt{-3}) = K(\varrho), \qquad \varrho = e^{\frac{2\pi i}{3}} = \frac{-1 + i\sqrt{3}}{2}.$$

There are two main reasons for this:

1. When examining the congruence conditions for solubility of 1.1.2, we must use cubic residues, and the cubic law of reciprocity takes the simplest form in $K(\varrho)$.

2. We shall work systematically in the purely cubic field $K(\sqrt[3]{m})$, where m is a rational integer. This is not a *Galois* field, but becomes one by adjunction of ϱ. (The resulting field is considered in Ch. IV, § 4.)

The question of *solubility* of 1.1.2 is, however, not affected by adjunction of ϱ to the field of the unknowns. Such problems have been studied by several writers; for references, see BILLING [1], Ch. I, and NAGELL [4], § 10. — If (x, y, z) is a solution of 1.1.2 in $K(\varrho)$, then a *chord* through this point and the *conjugate* point $(\bar{x}, \bar{y}, \bar{z})$ will cut the curve in a third rational point, provided the coefficients are rational (cf. 1.5.3).

§ 4. The question of *exceptional points* of the curve 1.1.2 is easily dealt with. It was shown by HURWITZ [1] that the curve

1.4.1 $$ax^3 + by^3 + cz^3 + dxyz = 0,$$

where a, b and c are *squarefree* rational integers, and coprime in pairs, has the following exceptional points:

1. *None, if at least two of the numerical values* $|a|$, $|b|$ *and* $|c|$ *are* > 1.

2. The one exceptional point $(x, y, z) = (1, -1, 0)$ if $a = b = 1$, $|c| > 1$, except in the cases $c + d \pm 2 = 0$ and $4c + d \pm 1 = 0$, when there are two such points.

The method is as follows. We define the weight of a solution (x, y, z), where x, y and z are coprime integers, to be $|xyz|$. We then show that the *tangential* of (x, y, z) (i.e. the point at which the tangent at (x, y, z) cuts the curve again) has a greater weight than (x, y, z).

The condition of squarefree coefficients is only necessary to make certain that x, y and z are coprime in pairs. In the case $d = 0$, i.e. the equation 1.1.2, we have seen that this condition is automatically satisfied if a, b and c are *cubefree*, and *Hurwitz' result holds in general for this equation.*

If $d = 0$, then 2. above shows that *the equation* $X^3 + Y^3 = A Z^3$ *has the only exceptional point* $(1, -1, 0)$ *when* $|A| > 2$ (and cubefree). For $A = 2$, the equation

1.4.2 $$X^3 + Y^3 = 2 Z^3$$

has the additional exceptional point $(1, 1, 1)$, and for $A = 1$ it is well known that the equation

1.4.3 $$X^3 + Y^3 = Z^3$$

has the three exceptional points with $XYZ = 0$. These are *all* the rational points in the last two cases.

1. above still holds after adjunction of ϱ to the field of the *unknowns.* This follows from NAGELL [3], Théorème 22 (p. 3), but can also be proved directly for the field $K(\varrho)$ by a simple generalization of *Hurwitz'* proof, and this time when both unknowns and *coefficients* are integers of $K(\varrho)$ (if now $|\ |$ means modulus). The generalization also shows that the only exceptional points in $K(\varrho)$ occur in the following cases:

The equation $X^3 + Y^3 = A Z^3$, where $A \in K(\varrho)$, A cubefree and $\neq \pm 1$ and ± 2: Three points with $X^3 = 1$, $Y = -1$, $Z = 0$.

The equation 1.4.2: The same three points, and in addition the nine points with $X^3 = Y^3 = 1$, $Z = 1$.

The equation 1.4.3: Nine points with $XYZ = 0$.

Finally the equation

1.4.4 $$x^3 + \varrho y^3 + \varrho^2 z^3 = 0$$

with the nine exceptional points with $x^3 = y^3 = 1$, $z = 1$. These are *all* the rational points in $K(\varrho)$ in this case, since it is easily seen that any other solution of 1.4.3 would lead to a solution of 1.4.3 in $K(\varrho)$ with $XYZ \neq 0$, by 1.2.4.

§ 5. The homogenous ternary cubic equations, both the general form and the more special forms 1.1.2 and 1.2.1, have been studied by many earlier writers. Apart from some results about the equation $X^3 + Y^3 = AZ^3$, to which we shall return in Ch. IX, most of the papers deal with the finding of new solutions from other, known points on the curve (tangentials, third intersection of the chord etc.). Full references are given in DICKSON [1], Ch. XXI, under the following headings:

1.5.1
- Two equal sums of two cubes.
- Three » » » » »
- Binary cubic form made a cube.
- Numbers the sum of two rational cubes: $x^3 + y^3 = Az^3$.
- Homogenous cubic equation $F(x, y, z) = 0$.

For completeness, I quote the following results for the curve 1.1.2 (DESBOVES [1], p. 552 and p. 565): The *tangential* to a point (x_1, y_1, z_1) is given by

1.5.2 $$x_2 = x_1(by_1^3 - cz_1^3), \quad y_2 = y_1(cz_1^3 - ax_1^3), \quad z_2 = z_1(ax_1^3 - by_1^3),$$

and *the third intersection of the chord* through the points (x_1, y_1, z_1) and (x_1', y_1', z_1') (cf. Ch. IX, § 16, Lemma 5):

1.5.3 $$\begin{cases} x_2 = x_1^2 y_1' z_1' - x_1'^2 y_1 z_1, \quad y_2 = y_1^2 z_1' x_1' - y_1'^2 z_1 x_1, \\ z_2 = z_1^2 x_1' y_1' - z_1'^2 x_1 y_1. \end{cases}$$

Both formulae 1.5.2—3 are valid also for the more general cubic curve 1.4.1.

In close connection with these questions stands the problem of a *basis* for the rational solutions (in the *Mordell-Weil* sense), in particular *the number of generators*. If the curve 1.1.2 has one rational point, we have seen in § 2 that it can be transformed birationally with rational coefficients into any of the two curves 1.2.1—2, and consequently has *the same number of generators of infinite order* as any of these.

The number of generators for $X^3 + Y^3 = AZ^3$ has been studied by FADDEEV [1], who gives a complete list of basic points in all soluble cases with $A \leqq 50$, reproduced as the first part of my Table 6. — I return to his methods in Ch. VII, § 6 and Ch. IX, § 15.

The finding of a basis for the equation 1.2.2, or rather the general equianharmonic case

1.5.4 $$\eta^2 = \xi^3 \pm D,$$

is treated by BILLING [1], who gives a table for all $D \leqq 25$. In a recent paper, CASSELS [1] has given some far-reaching theorems about the number of generators for the same curve, together with a table for all $D \leqq 50$. (Cf. § 6 below.)

Independently PODSYPANIN [1] has given a table of generators for $D \leqq 89$, making an interesting use of the connection between the equations

$$\eta^2 = 4\xi^3 - D \quad \text{and} \quad \eta^2 = 4\xi^3 + 27D.$$

(But see corrigenda in CASSELS [2].)

Among earlier writers, there has been a tendency to distinguish between positive and negative solutions, especially of the equation $X^3 + Y^3 = AZ^3$. We may clearly suppose A and Z positive, and there is the question of expressing the number A as the sum of or the difference between two positive rational cubes. It is well known that these two problems are *equivalent*, see the first two references in 1.5.1. I will just point out the connection between this problem and a result of HURWITZ [1], who has shown that if a cubic curve has an infinity of rational points, then *the infinite branch is densely covered* by these. (See also NAGELL [5].) And the curve $x^3 + y^3 = A$ (like the more general curve 1.1.1) consists only of an infinite branch.

In what follows, I do not distinguish between positive and negative solutions.

§ 6. The insolubility of an equation $X^3 + Y^3 = AZ^3$, and thereby (Th. I) of all equations $ax^3 + by^3 + cz^3 = 0$, with $abc = A$, can also be proved by the methods of CASSELS [1]. 1.2.2 and 1.2.5 show that we may consider instead the equation

$$\eta_1^2 = 4\xi_1^3 + A^2, \quad \text{or} \quad y^2 = x^3 + 2^4 A^2 = x^3 - D,$$

i.e. $D = -2^4 A^2$ in Cassels' notation. He works in the purely cubic field

$$K(\sqrt[3]{D}) = K(\sqrt[3]{2^4 A^2}) = K(\sqrt[3]{2\,A^2}) = K(\sqrt[3]{4\,A}).$$

This means a simplification if A is even, $A = 2A_1$, $K(\sqrt[3]{D}) = K(\sqrt[3]{A_1})$. Since the factor 2^6 can be removed from D, we get ($\|$ means "*exactly divides*"):

1.6.1 $$2 \| A \to 2 \nmid D, \quad 2^2 \| A \to 2^2 \| D, \quad 2 \nmid A \to 2^4 \| D.$$

The first two cases are covered by Cassels' Theorems VIII and XI respectively. When $D \not\equiv \pm 1 \pmod 9$ and not a perfect cube, his methods can never lead to a proof of insolubility if one of the possible μ's (different from 1) is a quadratic residue of 4. The generalization of his Lemma 6 shows that this is always so *if the class-number h is even.*

I have verified several insoluble values of A by Cassels' methods, and have also found cases with an even class-number, i.e. *cases where his conditions are not sufficient.* (As Cassels mentions at the end of his paper, the conditions turn out to be sufficient for all[1] $|D| \leqq 50$.) The simplest cases, representing the first two possibilities 1.6.1, are given by

$$A = 122 = 2.61, \quad A_1 = 61, \quad h_{61} = 6, \quad \varepsilon_{61} = 1 - 16\vartheta + 4\vartheta^2$$
$$A = 116 = 2^2.29, \quad A_1 = 58, \quad h_{58} = 6, \quad \varepsilon_{58} = 1 - 8\vartheta + 2\vartheta^2.$$

The insolubility of $A = 122$ and $A = 116$ follows from my Theorems XI (Table 4^c) and VIII (Table 4^a) respectively. The fundamental units ε_{58} and ε_{61} are given by NAGELL [6]. Since $\varepsilon_{61} \equiv 1 \pmod 4$ is a quadratic residue of 4, it follows from Cassels' Lemma 6 that h_{61} must be even. — The class-numbers have been calculated by me and checked by Cassels.

CHAPTER II. Congruence Considerations.

§ 1. The impossibility of an equation 1.1.2 can often be decided immediately by simple congruence considerations mod 9 or mod p, where p is a prime dividing one of the coefficients a, b or c. — We exclude once and for all the equations of the type 1.1.4, which are insoluble mod p^3.

First a trivial remark: Let $p \neq 3$ be a prime. If the congruence

2.1.1 $$F(x, y, z) = ax^3 + by^3 + cz^3 \equiv 0 \pmod p$$

is soluble, then it is soluble mod p^δ for all positive integer exponents δ. Because

[1] He conjectured in [1] that his conditions were sufficient for all D, but retracted this in an addendum [2], after I had shown him my counter-examples.

of the conditions 1.1.3 and 1.1.5, p can divide at most one of the terms of $F(x, y, z)$. If for instance $(p, ax) = 1$, then $\frac{\partial F}{\partial x} = 3ax^2$ is prime to p, and we can come from the modulus p to p^δ for any $\delta > 1$ by varying x only.

This does not hold when $p = 3$, because of the factor 3 in $\frac{\partial F}{\partial x}$. But it is easily seen that *solubility mod* 9 is sufficient for solubility mod 3^δ, $\delta > 2$. (Cf. SKOLEM [1], p. 8.)

If $(a, b) = (a, c) = (b, c) = 1$, *the insoluble equations mod* 9 are typified by (arbitrary signs):

2.1.2 $\quad a \equiv \pm 1, \quad b \equiv \pm 2, \quad c \equiv \pm 4$

2.1.3 $\quad a \equiv 0, \quad b \not\equiv \pm c$

$\Big\}$ (mod 9).

This is a consequence of 0 and ± 1 being the only cubic residues mod 9. In particular, *the equation is always possible mod* 9 *if one of the coefficients is exactly divisible by* 3.

For all other primes, we have to distinguish between the two types

2.1.4 $$q \equiv -1, \quad r \equiv +1 \pmod 3.$$

Throughout this paper, q and r denote only such primes, while p is any prime.

All rational integers are cubic residues of q, and *the congruence* 2.1.1 *is clearly soluble for all $p = q$*, since we can choose for instance y and z arbitrarily and determine x uniquely mod q from the resulting congruence, provided $(a, q) = 1$.

A complete system of residues mod r (0 excluded):

$$\pm 1, \pm 2, \ldots \pm \frac{r-1}{2},$$

consists of *three classes*, each with $\frac{r-1}{3}$ elements: One class K of cubic residues and two classes K' and K'' of non-residues. The elements of each class occur in pairs with opposite sign. The rules of multiplication are given by the table

2.1.5

	K	K'	K''
K	K	K'	K''
K'	K'	K''	K
K''	K''	K	K'

In particular, a and ax^3 belong to the same class mod r if $(r, ax) = 1$, and a congruence

2.1.6 $$ax^3 + by^3 \equiv 0 \pmod{r}, \quad r \nmid ab,$$

is soluble if and only if a and b belong to the same class, i.e. if they are what I shall call "*equivalent mod r*", and denote by

2.1.7 $$a \sim b \pmod{r}.$$

This implies that $ab^{-1} \sim ab^2$ is a cubic residue of r, which will be denoted by

2.1.8 $$ab^2 (R) r.$$

Cubic non-residuacity is similarly denoted by (N). I reserve symbols like $(\ )_3$ or $[\ ]$ for the field $K(\varrho)$ (Ch. IX); such symbols for rational primes have no simple rules of multiplication, and can only cause confusion.

If $p = r$ divides for instance c in 2.1.1, we get the congruence 2.1.6 and hence *the necessary and sufficient condition* 2.1.7 *or* 2.1.8 *for solubility mod r in this case.* — Similarly for all other primes r dividing one of the coefficients.

As mentioned in the Introduction, we shall treat the equation 1.1.2 in the form (5):

2.1.9 $$x^3 - my^3 = nz^3.$$

The above conditions for solubility then take the form:

2.1.10
$$\begin{cases} \text{Mod } 9: \begin{cases} m \not\equiv \pm 2 \text{ if } n \equiv \pm 4;\ m \not\equiv \pm 4 \text{ if } n \equiv \pm 2 \pmod 9 \\ m \equiv 0 \text{ or } \pm 1 \text{ if } n \equiv 0;\ n \equiv 0 \text{ or } \pm 1 \text{ if } m \equiv 0 \pmod 9 \\ m_1 \equiv \pm n_1 \pmod 9 \text{ if } m = 3m_1,\ n = 3n_1,\ 3 \nmid m_1 n_1. \end{cases} \\ \text{Mod } r: \begin{cases} m(R)r & \text{if } r \mid n,\ r \nmid m \\ n(R)r & \text{if } r \mid m,\ r \nmid n \\ m_1 n_1^2 (R) r & \text{if } m = r^i m_1,\quad n = r^i n_1,\ i = 1 \text{ or } 2,\quad r \nmid m_1 n_1. \end{cases} \end{cases}$$

I have treated systematically all equations 2.1.9 with $2 \leqq m < n \leqq 50$, m and n cubefree. The equations which can be shown insoluble by elementary congruence considerations (including the type 1.1.4) are indicated by horizontal lines in *Table 2a*.

We note that *the elementary congruence conditions cannot prove the insolubility of an equation*

$$X^3 + Y^3 = AZ^3$$

for any value of A. (Cf. my report [1].)

§ 2. In order to show that the conditions of the last paragraph are also *sufficient for solubility for all moduli*, we must prove that the congruence

2.2.1 $$ax^3 + by^3 + cz^3 \equiv 0 \pmod{r}, \quad r \nmid abc,$$

is always soluble. SKOLEM [1] has shown (pp. 6—7) that this is always possible for $r > 7$, and even with

2.2.2 $$xyz \not\equiv 0 \pmod{r}.$$

With this restriction, 2.2.1 is insoluble when $r = 7$, and for instance

2.2.3 $$b \equiv \pm a, \quad c \equiv \pm 3a \pmod{7}.$$

But in this case the congruence is clearly soluble with $z \equiv 0 \pmod{7}$, which suffices for our purpose. (This remark is often very useful in the *numerical solution* of such an equation, cf. 6.7.2.)

Skolem's proof is based on a result of HURWITZ [2] about the number of incongruent solutions of 2.2.1. If we abandon the condition 2.2.2, it is possible to prove the solubility of 2.2.1 very simply, using the first step of an (unpublished) argument of Prof. *Marshall Hall*, Jr.[1]:

If two of the coefficients, for instance a and b, belong to the same class mod r, we can put $z \equiv 0$ and get the soluble congruence 2.1.6. The difficulty arises when a, b and c belong to the three different classes K, K' and K''. Since ax^3 can take all values in the class to which a belongs, it suffices to show that we can find elements k, k' and k'' from the three classes, such that for instance

2.2.4 $$k + k' \equiv k'' \pmod{r}.$$

In order to prove this, we form a table

	K	K'	K''
K	α	β	γ
K'	α'	β'	γ'
K''	α''	β''	γ''

[1] (Added later.) Dr. *Cassels* has pointed out to me that similar arguments were used by GAUSS [1] (Art. 358, pp. 445—9).

in the following way: To each element of the class K (left column) we add the number 1, and group the sums in the classes K, K' and K'' (heading), in numbers α, β and γ respectively. Similarly we add 1 to the elements of K' and K''. Then

2.2.5 $$\alpha' + \beta' + \gamma' = \alpha'' + \beta'' + \gamma'' = \frac{r-1}{3}$$

(the number of elements in each class). But

2.2.6 $$\alpha + \beta + \gamma = \frac{r-1}{3} - 1,$$

since -1 belongs to K, so that we lose the sum $-1 + 1 = 0$.

β is the number of elements k' of the form $k' = 1 + k$. Since a change of sign leaves the class unaltered, this can also be written as $k = 1 + k'$, and consequently $\beta = \alpha'$. Multiplication with $(k')^{-1} \in K''$ gives still another equation $k'' = 1 + k''$, i.e. $\underline{\beta = \alpha' = \gamma''}$. Similarly we find $\underline{\gamma = \beta' = \alpha''}$, and a comparison with 2.2.5—6 shows that $\underline{\gamma' = \beta'' = \alpha + 1 \geqq 1}$. Consequently $k'' = 1 + k'$, i.e. 2.2.4, is possible in at least one way.

In the next paragraph, I show the solubility of 2.2.1 (without the restriction 2.2.2) by still another simple method. The advantage of Marshall Hall's proof is, however, that *it holds equally well in any algebraic number-field* Ω, for any prime-ideal modulus $\mathfrak{p}$ (prime to 3 and to the coefficients, which together with the unknowns are then supposed to be integers of Ω). The number of residue-classes in Ω mod $\mathfrak{p}$ and prime to $\mathfrak{p}$ is given by $N(\mathfrak{p}) - 1$, and *Fermat's* theorem holds:

$$\xi^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}} \quad \text{if} \quad \mathfrak{p} \nmid \xi, \quad \xi \in \Omega.$$

As in elementary algebra, we can find a *primitive root* of $\mathfrak{p}$ and establish a system of *indices* (logarithms), from which we deduce the theory of cubic residues mod $\mathfrak{p}$. If $N(\mathfrak{p}) - 1 \not\equiv 0 \pmod 3$, then all integers of Ω are cubic residues mod $\mathfrak{p}$, and the congruence

2.2.7 $$\alpha\xi^3 + \beta\eta^3 + \gamma\zeta^3 \equiv 0 \pmod{\mathfrak{p}}, \quad \mathfrak{p} \nmid 3\alpha\beta\gamma$$

is of course always soluble. If however $N(\mathfrak{p}) - 1 \equiv 0 \pmod 3$, the numbers of Ω (prime to $\mathfrak{p}$) are divided in the same classes K, K' and K'' as above, with the rules of multiplication given by 2.1.5. Marshall Hall's argument still shows that 2.2.7 is then always soluble. — We shall make use of this remark in Ch. IV, § 4.

§ 3. For applications in Ch. VIII and IX, we shall also consider the more general cubic congruence

2.3.1 $$F(x, y) = Ax^3 + Bx^2y + Cxy^2 + Dy^3 \equiv Ez^3 \pmod{p^\delta}.$$

We denote by Δ the *discriminant* of the left hand side.

The prime $p = 3$ must be treated separately in each special case. For all other primes, solubility mod p is usually sufficient for solubility mod p^δ, $\delta > 1$. If $p \nmid Ez$, this can be obtained by varying z only. If $p \nmid \Delta$, at least one of $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ must be $\not\equiv 0 \pmod{p}$ (since elimination of $\frac{x}{y}$ between $\frac{\partial F}{\partial x} \equiv 0$ and $\frac{\partial F}{\partial y} \equiv 0$ leaves $\Delta \equiv 0$), and in this case variation of x or y gives the same result. Common divisors of E and Δ cause extra difficulties; all other divisors of E and Δ will obviously lead to simple conditions, which are easily dealt with in each given case. (A more special form of the congruence 2.3.1 will be treated in detail in Ch. IX, § 7.)

The problem is again all *other* primes p, such that $p \nmid 3E\Delta$. If $p = q \equiv -1 \pmod 3$, the term Ez^3 makes the congruence always soluble if $q \nmid E$. If $p = r \equiv +1 \pmod 3$, we can use a result of VON STERNECK [1]: If $r \nmid A(B^2 - 3AC)$, the cubic polynomial

2.3.2 $$f(x) = Ax^3 + Bx^2 + Cx + D$$

(the left hand side of 2.3.1 for $y = 1$) *takes* $\frac{2r+1}{3}$ *different values mod* r. Since the right hand side Ez^3 takes $\frac{r-1}{3} + 1$ values (included zero), and

$$\frac{2r+1}{3} + \frac{r-1}{3} + 1 = r + 1 > r,$$

the two sides of the congruence will have at least one value mod r in common, i.e. a solution.

If $r \mid A(B^2 - 3AC)$ but $r \nmid D(C^2 - 3BD)$, we can argue similarly with $x = 1$. Any common divisor of $B^2 - 3AC$ and $C^2 - 3BD$ divides Δ, and must be treated separately in any case.[1] But we may also have to consider the primes r dividing A or D.

The result is therefore that we only have to examine the congruence 2.3.1 for the following primes:

[1] A common divisor r of B and C, such that $r \nmid ADE$, leads to a soluble congruence of the type 2.2.1.

2.3.3 $$p = 3; \quad p = q \text{ if } q \mid E; \quad p = r \text{ if } r \mid ADE\Delta,$$

and for $\delta > 1$ only when $p = 3$ or $p \mid (E, \Delta)$. The last point can be facilitated by the results of KANTOR [1], who discusses the values of the polynomial 2.3.2 mod p^δ for all p and δ.

The above considerations lead to a very simple proof for the solubility of 2.2.1. Here r cannot divide both $a + b$ and $a - b$, and after a change of sign for b and y if necessary, we may suppose $a + b \not\equiv 0 \pmod r$. The substitution $y \equiv x + y_1$ gives

$$(a + b)x^3 + 3bx^2y_1 + 3bxy_1^2 + by_1^3 \equiv -cz^3 \pmod r,$$

which is of the form 2.3.1, with

$$A(B^2 - 3AC)E = 9(a + b)abc \not\equiv 0 \pmod r,$$

and consequently soluble.

Just before I found the reference to *von Sterneck's* paper, I wrote to Prof. *Marshall Hall* asking about the congruence 2.3.1 in the cases where $p = r \nmid ADE\Delta$. It turned out that he had found the same result about 2.3.2 independently (and his proof is in some respects simpler than von Sterneck's). Prof. Marshall Hall also communicated to me an additional argument, using the ideas of § 2 above, by which he can prove that the function $f(x)$ of 2.3.2 will *represent all three cubic classes mod r, i.e. the congruence* 2.3.1 *mod r is soluble with* $z \not\equiv 0$, provided $f(x)$ cannot be transformed linearly mod r into the form $A'x'^3 + C'x'$.

§ 4. I have also examined the congruence conditions for the more general cubic equation

2.4.1 $$\sum_{i=1}^{n} a_i x_i^3 = 0,$$

with all a_i *cubefree and* $\not\equiv 0$. It turns out that the corresponding congruence mod p^δ is soluble for all p and δ when

2.4.2 $$n \geqq 5 \text{ if } p = 3; \quad n \geqq 4 \text{ if } p = q; \quad n \geqq 7 \text{ if } p = r.$$

If $p = q \equiv -1 \pmod 3$, and $n = 4$, then at least two of the coefficients, e.g. a_1 and a_2, are exactly divisible by the same power q^i, $i = 0, 1$ or 2. Putting $a_1 = q^i a_1'$, $a_2 = q^i a_2'$, $x_3 \equiv x_4 \equiv 0 \pmod{q^\delta}$, we get the soluble congruence

$$a_1'x_1^3 + a_2'x_2^3 \equiv 0 \pmod{q^{\delta - i}}, \quad q \nmid a_1'a_2'.$$

If $p = r \equiv +1 \pmod 3$, and $n = 7$, at least three of the coefficients are exactly divisible by the same power r^i. Arguing as above, we get the soluble congruence

$$a_1' x_1^3 + a_2' x_2^3 + a_3' x_3^3 \equiv 0 \pmod{r^{\vartheta - i}}, \qquad r \nmid a_1' a_2' a_3'.$$

Similar arguments, a little more complicated, hold for $p = 3$, $n = 5$. — The numbers n in 2.4.2 are *minimal*, as seen from the following insoluble congruences:

$$\begin{aligned} x_1^3 + 2x_2^3 + 4x_3^3 + 9x_4^3 &\equiv 0 \pmod{3^3} \\ x_1^3 + 2x_2^3 + 2^2 x_3^3 &\equiv 0 \pmod{2^3} \\ x_1^3 + 2x_2^3 + 7(x_3^3 + 2x_4^3) + 7^2(x_5^3 + 2x_6^3) &\equiv 0 \pmod{7^3}. \end{aligned}$$

All congruence conditions are therefore automatically satisfied for 2.4.1 when $n \geqq 7$. — A slight modification of the *Hardy-Littlewood* approach to *Waring's problem* (Landau [1], part 6) shows that the equation 2.4.1 has always *an infinity of solutions when* $n = 9$, and the x_i can all be taken *positive* if the a_i are not all of the same sign. — I owe this remark to Dr. *Cassels*, who says that the fact had previously been noted by Prof. *Davenport*.

It may seem surprising that $n = 7$ is the minimum number of variables for the congruence corresponding to 2.4.1. Mordell [1] has given examples of insoluble cubic congruences in 9 variables, but these contain *product terms*.

The congruences in §§ 1—3 represent only particular cases of ternary cubic forms. The general homogenous cubic congruence

$$f_3(x, y, z) \equiv 0 \pmod p \tag{2.4.3}$$

has been treated by Mordell [2], who shows that the number N of solutions (in the *inhomogenous* form, with $z = 1$), is in general given by

$$N = p + O(p^{2/3}). \tag{2.4.4}$$

Consequently 2.4.3 is soluble for all sufficiently large p. The constant of the O-symbol is absolute, but the formula 2.4.4 only holds if $f_3(x, y, z)$ is *absolutely irreducible mod p*. If the invariant S of 2.4.3 (cf. Nagell [2], § 1) is $\equiv 0 \pmod p$, 2.4.4 is replaced by the stronger form

$$N = p + O(p^{\frac{1}{2}}). \tag{2.4.5}$$

The determination of the constant involved seems to become difficult. For the simpler *Weierstrass normal form:*

2.4.6 $$y^2 \equiv 4x^3 - g_2 x - g_3 \pmod{p},$$

the constant has been determined by HASSE [1], who finds

2.4.7 $$|N - p| \leqq 2\sqrt{p},$$

provided the right hand side of 2.4.6 has no multiple root mod p.

A particular case of the general cubic congruence 2.4.3, containing all possible terms (10 in all), will be dealt with in Ch. IV—VI.

CHAPTER III. The Equation in the Cubic Field.

§ 1. As already mentioned, we transform the cubic equation $ax^3 + by^3 + cz^3 = 0$ into the form

3.1.1 $$x^3 - my^3 = nz^3,$$

where no longer necessarily $(m, n) = 1$. We suppose *that the congruence conditions* 2.1.10 *are satisfied*, and shall treat the corresponding equation in *the purely cubic field* $K(\sqrt[3]{m})$. Most of the necessary information about this field, including references, is given by CASSELS [1]. In particular, I make use of his table of *class-numbers and units* for $m \leqq 50$.

I shall use the notation $\sqrt[3]{m} = \vartheta$, $K(\sqrt[3]{m}) = K(\vartheta)$, where we may suppose ϑ to be the *real* cube-root. The integers of $K(\vartheta)$ are given by $\alpha = u + v\vartheta + w\vartheta^2$, where usually u, v and w are rational integers. If m is not squarefree,

3.1.2 $$m = m_1 m_2^2, \quad (m_1, m_2) = 1, \ m_1 \text{ and } m_2 \text{ squarefree},$$

then w has a denominator m_2. In this case I sometimes use the notation

3.1.3 $$\sqrt[3]{m} = \sqrt[3]{m_1 m_2^2} = \vartheta_1, \quad \sqrt[3]{m_1^2 m_2} = \vartheta_2 = \frac{\vartheta_1^2}{m_2}.$$

The fields $K(\vartheta_1)$ and $K(\vartheta_2)$ are identical.

If $m \equiv \pm 1 \pmod 9$, a denominator 3 can occur in the coefficients u, v and w. This case will be treated in more detail in §§ 3—4.

I denote prime ideals of the 1st and 2nd degree by $\mathfrak{p}$ and $\mathfrak{q}$ respectively. Conjugate ideals are indicated by dashes. When giving the basic elements, ideals are denoted by square brackets. More precisely, we have (with the notations 2.1.4, 2.1.8 and 3.1.3):

3.1.4
$$\begin{cases} p \mid m_1 : [p] = [p, \vartheta_1]^3 = \mathfrak{p}_p^3 \\ p \mid m_2 : [p] = [p, \vartheta_2]^3 = \mathfrak{p}_p^3 \end{cases} p \text{ any prime.}$$
$$p = 3 \nmid m,\ m \not\equiv \pm 1 \pmod 9 \colon [3] = [3, \vartheta - m]^3 = \mathfrak{p}_3^3.$$
$$p = q \nmid m,\ d^3 \equiv m \pmod q \colon$$
$$[q] = [q, \vartheta - d]\,[q, \vartheta^2 + d\vartheta + d^2] = \mathfrak{p}_q \mathfrak{q}_q.$$
$$p = r \nmid m,\ m(R)r,\ d^3 \equiv d'^3 \equiv d''^3 \equiv m \pmod r \colon$$
$$[r] = [r, \vartheta - d]\,[r, \vartheta - d']\,[r, \vartheta - d''] = \mathfrak{p}_r \mathfrak{p}_r' \mathfrak{p}_r''.$$
$$p = r \nmid m,\ m(N)r : [r] \text{ a prime ideal.}$$

§ 2. In the field $K(\vartheta)$, the left hand side of 3.1.1 factorizes

3.2.1
$$[x^3 - my^3] = [x - y\vartheta]\,[x^2 + xy\vartheta + y^2\vartheta^2].$$

A common factor of the ideals on the right hand side must divide

$$x^2 + xy\vartheta + y^2\vartheta^2 - (x - y\vartheta)^2 = 3xy\vartheta, \text{ i.e. } 3\vartheta,$$

since $(x, y) = 1$. The factors of 3ϑ are all ideals of the first degree; let any of these be $\mathfrak{p}_p$, corresponding to the rational prime p. Then

$$\mathfrak{p}_p \mid \vartheta \,\&\, (x - y\vartheta) \to \mathfrak{p}_p \mid x \,\&\, m \to p \mid x \,\&\, m \to \underline{p \mid n};$$
$$\mathfrak{p}_p = \mathfrak{p}_3 \mid 3 \text{ but } 3 \nmid n \to \mathfrak{p}_3 \mid z^3 \to 3 \mid z \to 3 \nmid x \,\&\, y \to x^3 \,\&\, y^3 \equiv$$
$$\equiv \pm 1 \pmod 9 \to \underline{m \equiv \pm 1 \pmod 9},$$

a case which will be treated in the next paragraphs. In all other cases, it follows that we must have

3.2.2
$$[x - y\vartheta] = \mathfrak{p}_n \mathfrak{a}^3,$$

where $\mathfrak{a}$ is some ideal, and $\mathfrak{p}_n$ is a product of prime ideal divisors of n. Since

3.2.3
$$\mathfrak{q}_q \mid x - y\vartheta \to q \mid x \,\&\, y,$$

3.2.4
$$\mathfrak{p}_r \,\&\, \mathfrak{p}_r' \mid x - y\vartheta \to r \mid (x - yd) \,\&\, (x - yd') \to r \mid x \,\&\, y,$$

and since a comparison between 3.1.1 and 3.2.2 shows that the *norm* $N(\mathfrak{p}_n) = n$, the ideal $\mathfrak{p}_n$ has the following factors ($\parallel$ means "exactly divides"):

$$\mathfrak{p}_3^i \parallel \mathfrak{p}_n \quad \text{if} \quad 3^i \parallel n, \quad i = 1 \text{ or } 2$$

(in the case $i = 2$ we must have $3^2 \parallel m$, since $m \equiv \pm 1 \pmod 9$ is excluded in this paragraph),

$$\mathfrak{p}_q^i \| \mathfrak{p}_n \quad \text{if} \quad q^i \| n, \quad i = 1 \text{ or } 2,$$

and similarly if $r \mid n$. In this case either $r \mid m$ or $m(R)r$ (if the congruence conditions 2.1.10 shall be satisfied), and consequently $[r]$ is always the product of three ideals of degree 1. If $r \nmid m$, these ideals are all different, and only one of them can divide $x - y\vartheta$ at the time by 3.2.4; we thus get *three different equations* 3.2.2 corresponding to each such prime r.

§ 3. We now come to the case $m \equiv \pm 1 \pmod 9$. Throughout this chapter, I will suppose that

3.3.1 $$m \equiv +1 \pmod 9,$$

in order to simplify the formulae. The results for $m \equiv -1 \pmod 9$ can always be obtained by changing the sign of ϑ.

The integers of $K(\vartheta)$ are now given by

3.3.2 $$\alpha = \frac{u + v\vartheta + w\vartheta^2}{3}, \quad u \equiv v \equiv w \pmod 3,$$

where u, v and w are rational integers if m is squarefree, and w has a denominator m_2 in the case 3.1.2.

The ideal $[3]$ is no longer a perfect cube, but

3.3.3 $$[3] = \left[3, \vartheta - 1, \frac{\vartheta^2 + \vartheta + 1}{3}\right]^2 \cdot \left[3, \vartheta - 1, \frac{\vartheta^2 + \vartheta - 2}{3}\right] = \mathfrak{r}^2\mathfrak{s}.$$

In particular, we have

3.3.4 $$\mathfrak{r}\mathfrak{s} = [3, \vartheta - 1].$$

According to their form and divisibility by $\mathfrak{r}$ or $\mathfrak{s}$, MARKOFF [1] divides the integers 3.3.2 into 6 *classes*, with the following properties:

Class 1, $3 \mid \alpha$:

$\alpha = u + v\vartheta + w\vartheta^2$, $u \equiv v \equiv w \pmod 3$.

Class 2, $\mathfrak{r}\mathfrak{s} \mid \alpha$, $3 \nmid \alpha$:

$\alpha = u + v\vartheta + w\vartheta^2$, $u \not\equiv v \not\equiv w \not\equiv u \pmod 3$.

Class 3, $\mathfrak{r} \mid \alpha$, $\mathfrak{s} \nmid \alpha$:

$\alpha = \frac{u + v\vartheta + w\vartheta^2}{3}$, $u \equiv v \equiv w \not\equiv 0 \pmod 3$, $v + w - 2u \equiv 0 \pmod 9$.

Class 4, $\mathfrak{s} \mid \alpha$, $\mathfrak{r} \nmid \alpha$:

$$\alpha = \frac{u + v\vartheta + w\vartheta^2}{3},\ u \equiv v \equiv w \not\equiv 0 \pmod 3,\quad u + v + w \equiv 0 \pmod 9.$$

Class 5, $(\mathfrak{r}\mathfrak{s}, \alpha) = 1$, no denominator 3:

$\alpha = u + v\vartheta + w\vartheta^2$, with two and only two of the coefficients congruent mod 3.

Class 6, $(\mathfrak{r}\mathfrak{s}, \alpha) = 1$, denominator 3:

$$\alpha = \frac{u + v\vartheta + w\vartheta^2}{3},\ u \equiv v \equiv w \not\equiv 0 \pmod 3,$$

but with none of the other conditions under the classes 3 and 4 satisfied.

Markoff also shows the following relations: If α_t is any integer from the class t, then

3.3.5 $$\alpha_5 \cdot \alpha_6 = \alpha_6',\quad \alpha_6 \cdot \alpha_6' = \alpha_5.$$

(I avoid the term *group* for Markoff's classes, since they are not "groups" in the strict sense of this word. There can be no confusion with the *ideal-classes* of the field $K(\vartheta)$.)

The above class-conditions have a much simpler form than those originally given by Markoff. We must bear in mind that u and v are always integers, but w has a denominator $m_2 \not\equiv 0 \pmod 3$ in the case 3.1.2. — A similar classification also holds for the *ideals* in $K(\vartheta)$ (but we cannot then distinguish between the classes 5 and 6. When these classes are mentioned separately in the next paragraph, it is in order to get complete analogy with the corresponding equations between *integers* of $K(\vartheta)$.)

§ 4. We shall now consider the equation 3.1.1 when $m \equiv +1 \pmod 9$, and the corresponding ideal-equation 3.2.2. We can argue as in § 2 for the ideal divisors $\mathfrak{p}_q$ and $\mathfrak{p}_r$ of n, and *their product will be denoted by* $\mathfrak{p}_n$. But the factors of 3 need a special treatment. We must consider the different residues of n mod 9 separately:

1. $n \equiv \pm 4 \pmod 9$, i.e. $3 \mid z$, $x \equiv y \not\equiv 0 \pmod 3$, $\mathfrak{r}\mathfrak{s} = [3, \vartheta - 1] \mid x - y\vartheta$. Since $\mathfrak{r}^2\mathfrak{s} = [3] \mid x - y\vartheta \to 3 \mid x \,\&\, y$, and $3^3 \mid N(x - y\vartheta) = x^3 - my^3$, we must have $\mathfrak{r}\mathfrak{s}^2 \mid x - y\vartheta$. If $3^{i+1} \parallel z$, $i > 0$, the additional power $\mathfrak{s}^{3i}$ can be absorbed in $\mathfrak{a}^3$, and consequently we have

3.4.1 $$[x - y\vartheta] = \mathfrak{r}\mathfrak{s}^2\mathfrak{p}_n\mathfrak{a}^3,\ \mathfrak{a} \in \text{class } 4, 5, \text{ or } 6;\ N(\mathfrak{r}\mathfrak{s}^2\mathfrak{p}_n) = 3^3 n.$$

2. $n \equiv \pm 3 \pmod 9$: The same argument as under 1., but an additional $\mathfrak{s}$ from n, and the resulting $\mathfrak{s}^3$ can be absorbed in $\mathfrak{a}^3$:

3.4.2 $$[x - y\vartheta] = \mathfrak{r}\mathfrak{p}_n\mathfrak{a}^3, \quad \mathfrak{a} \in \text{class } 4; \quad N(\mathfrak{r}\mathfrak{p}_n) = n.$$

3. $n \equiv \pm 2 \pmod 9$: One possibility as under 1., but also the possibility $x \equiv -y \not\equiv 0$, $z \not\equiv 0 \pmod 3$, and so

3.4.3 $$[x - y\vartheta] = \mathfrak{p}_n\mathfrak{a}^3, \quad \mathfrak{a} \in \text{class } 5 \text{ or } 6; \quad N(\mathfrak{p}_n) = n.$$

4. $n \equiv \pm 1 \pmod 9$: The same two possibilities as under 3., but the second case when $xy \equiv 0$, $z \not\equiv 0 \pmod 3$.

5. $n \equiv 0 \pmod 9$: Arguing as under 1., we get the only possibility

3.4.4 $$[x - y\vartheta] = \mathfrak{r}\mathfrak{s}\mathfrak{p}_n\mathfrak{a}^3, \quad \mathfrak{a} \in \text{class } 4, 5 \text{ or } 6; \quad N(\mathfrak{r}\mathfrak{s}\mathfrak{p}_n) = n.$$

§ 5. We have seen that the equation 3.1.1 leads to a finite number of equations

3.5.1 $$[x - y\vartheta] = \mathfrak{n}\mathfrak{a}^3$$

in the field $K(\vartheta)$. *If in particular n contains no prime divisors $r \equiv +1 \pmod 3$ such that $r \nmid m$, and if $n \equiv 0, \pm 3$ or ± 4 when $m \equiv \pm 1 \pmod 9$, there is only one possible ideal* $\mathfrak{n}$.

By an unpublished argument used by *Mordell* and (independently) by *Marshall Hall* in similar cases, we can often show that 3.5.1 is impossible by *class-number considerations*. The simplest example is that of the class-number $h_m = 3$, in which case $\mathfrak{a}^3$ is always a principal ideal. *The equation* 3.5.1 *is then impossible if* $\mathfrak{n}$ *is not a principal ideal.*

But a similar argument can also be used when $h_m = 3k$, $k > 1$. Let us for simplicity suppose that the group of ideal-classes is *cyclic* (this is always the case for $m \leqq 50$), and let all classes be powers of a class I. Then the equation 3.5.1 is impossible if $\mathfrak{n}$ does not belong to any of the classes I^{3i}, $i = 0, 1, 2, \ldots k-1$.

As already mentioned, I have treated systematically all equations 3.1.1 with m and n cubefree, $\geqq 2$ and $\leqq 50$, and the result is given in *Table* 2^a, where crosses stand for equations which are possible for all moduli but which have been excluded one way or other in the cubic field. The cubefree $m \leqq 50$ with $3 \mid h_m$ are

3.5.2 $m = 7, 13, 14, 19, 20, 21, 22, 26, 28, 30, 31, 34, 35, 37, 38, 39, 42, 43, 49, 50$

(of which only $h_{39} = 6$ and $h_{43} = 12$ are > 3). *Nearly all* excluded equations in these cases have been proved insoluble by class-number considerations.[1]

§ 6. We shall now construct the equations between *integers* of $K(\vartheta)$ corresponding to 3.5.1, when this cannot be excluded by class-number considerations. — Let first $h_m = 1$; we then immediately get

3.6.1 $$x - y\vartheta = \eta \nu \alpha^3,$$

where η, ν and α are integers of $K(\vartheta)$, η a unit and ν any number such that $\mathfrak{n}$ is the principal ideal $[\nu]$, i.e. $N(\mathfrak{n}) = N(\nu) = n$ or $3^3 n$ (where $3^3 n$ occurs only in the cases 3.4.1).

If ε_m is the fundamental unit of $K(\vartheta)$, then

$$\eta = \pm \varepsilon_m^{\pm t}, \quad t = 0, 1, 2, 3, \ldots.$$

The sign can be absorbed in α^3, and the same holds for any multiple of 3 in t. We therefore have to consider only the three possibilities $\eta = 1$, ε_m and ε_m^2:

3.6.2 $$x - y\vartheta = \varepsilon_m^i \nu \alpha^3, \quad i = 0, 1, 2$$

(or with ε_m^{-1} instead of ε_m^2). It will obviously suffice that ε_m *is not the cube of another unit.* Some of the units given by *Cassels* have not been shown to be fundamental; for his purpose he has checked that they are not squares, and I have checked that they are not cubes of other units. This check can be performed quickly by the theory of *cubic residues* which is developed in Ch. V and VI; ε_m cannot be a cube if it is a cubic non-residue to an appropriate modulus.

Already here I will insert a remark which is very useful in many numerical examples. It often happens that the number ν in 3.6.1 can be very complicated and difficult to find, but that we can obtain easily an expression for the product of ν and some cube in $K(\vartheta)$. A striking example is the equation

$$x^3 - 33y^3 = 2z^3,$$

with the one corresponding ideal-equation in $K(\sqrt[3]{33}) = K(\vartheta)$:

3.6.3 $$[x - y\vartheta] = \mathfrak{p}_2 \mathfrak{a}^3.$$

[1] Dr. *Cassels* kindly lent me his calculations in connection with the determination of the class-numbers h_m for $m \leqq 50$. His notes were of very great use to me during my own calculations in the cubic fields.

The class-number $h_{33} = 1$, but the fundamental unit ε_{33} has very big coefficients, and it seems to be the same for the basic number ν_2 of $\mathfrak{p}_2$. But we see at once that

$$N(\vartheta - 1) = 33 - 1 = 2^5, \text{ i.e. } 1 - 2\vartheta + \vartheta^2 = \nu_2(\nu_2^3)^3\eta,$$

where η is a unit. If we replace 3.6.3 by

$$3.6.4 \qquad x - y\vartheta = \varepsilon_{33}^i(1 - 2\vartheta + \vartheta^2)\alpha^3,$$

then α is no longer necessarily an integer in $K(\vartheta)$, but has in its denominator *only powers of* ν_2.

The principle for exclusion of the equations 3.6.2 *is to show them impossible for certain moduli*, by a theory of cubic residues in $K(\vartheta)$. The modified equation 3.6.4 can still be treated by the same means, if we now use *moduli which are prime to* $\mathfrak{p}_2$. And we shall see in Ch. VI that a *first degree* ideal divisor of a prime $q \equiv -1 \pmod 3$ is never used as modulus for exclusions.

Similar arguments, usually not so simple, have been a great help to me in my extensive numerical calculations. There is no special rule for the use of such "*auxiliary cubes*". They must be prime to at least one of the moduli which can be used for exclusion, but to find them quickly is a matter of experience.

§ 7. We now come to the cases where $h_m > 1$, and let first $3 \nmid h_m$. The principles to be used can be illustrated by $h_m = 2$ (which ist he only actual case when $m \leqq 50$, namely for $m = 11$, 15 and 47). Let the two classes be Π and Γ where Π is the principal class and $\Gamma^2 = \Pi$.

If in 3.5.1 $\mathfrak{n} \in \Pi$, then also $\mathfrak{a} \in \Pi$, and we are led to an equation 3.6.2 as before. If however $\mathfrak{n}$ and consequently $\mathfrak{a}$ are not principal ideals, $\mathfrak{n}\,\&\,\mathfrak{a} \in \Gamma$, we must use the argument of "*auxiliary cubes*": Let $\mathfrak{b} \in \Gamma$, where $\mathfrak{b}$ is an integer ideal prime to the moduli which can be used by the exclusions. (It is well known that every class contains ideals prime to any given ideal.) The equation 3.5.1 can be written as

$$3.7.1 \qquad [x - y\vartheta] = \mathfrak{n}\mathfrak{b}^3(\mathfrak{a}\mathfrak{b}^{-1})^3,$$

where now both $\mathfrak{n}\mathfrak{b}^3$ and $\mathfrak{a}\mathfrak{b}^{-1}$ are principal ideals, the latter fractional. We are again led to an equation 3.6.2, where the possible denominator of α is prime to the moduli to be used.

A quick determination of the ideal $\mathfrak{b}$ is again a matter of experience. As a simple example, we can consider the equation

$$x^3 - 11y^3 = 15z^3,$$

or in the field $K(\sqrt[3]{11}) = K(\vartheta)$:

$$[x - y\vartheta] = \mathfrak{p}_3\mathfrak{p}_5\mathfrak{a}^3 = \mathfrak{n}\mathfrak{a}^3.$$

Here $h_{11} = 2$, $\mathfrak{p}_3 = [-2 + \vartheta] \in \Pi$, but $\mathfrak{p}_5 \in \Gamma$, and so $\mathfrak{n} \in \Gamma$. We can use $\mathfrak{b} = \mathfrak{p}_2 \in \Gamma$, and since

$$N(-1 + \vartheta^2) = -1 + 11^2 = 120 = 2^3 \cdot 15,$$

we can deal with the equation

3.7.2 $$x - y\vartheta = \varepsilon_{11}^i(-1 + \vartheta^2)\alpha^3,$$

if we use moduli which are prime to $\mathfrak{p}_2$.

The above remarks can also be useful in the search for a *numerical solution* of an equation $x^3 - my^3 = nz^3$ which cannot be excluded. We know that $\mathfrak{p}_z$, the product of first degree prime divisors of z, must belong to the same class as $\mathfrak{n}$ (either Π or Γ), and this *limits the possible choice for* z.

§ 8. Let finally $3 \mid h_m$, and suppose that 3.5.1 cannot be excluded by class-number considerations. Let $\mathfrak{n}^{-1} \in \Gamma$, and $\mathfrak{b}$ a particular ideal such that $\mathfrak{b}^3 \in \Gamma$. Using again the form 3.7.1, we must examine the classes to which $\mathfrak{a}\mathfrak{b}^{-1}$ can belong in order that $(\mathfrak{a}\mathfrak{b}^{-1})^3$ is a principal ideal. Let $\Gamma_0 = \Pi$ (principal class), $\Gamma_1, \Gamma_2, \ldots \Gamma_{k-1}$ be all such classes, i.e. $\Gamma_j^3 = \Pi$, $j = 0, 1, 2, \ldots k-1$, and let $\mathfrak{b}_0 = [1], \mathfrak{b}_1, \mathfrak{b}_2, \ldots \mathfrak{b}_{k-1}$ be one representative ideal from each such class. Then

$$\mathfrak{a}\mathfrak{b}^{-1} \in \Gamma_j, \text{ i.e. } \mathfrak{a} = \mathfrak{b}\mathfrak{b}_j\mathfrak{c}, \quad j = 0, 1, 2, \ldots k-1,$$

where $\mathfrak{c}$ is a (fractional) principal ideal. The equation 3.7.1 then takes the form

$$[x - y\vartheta] = \mathfrak{n}\mathfrak{b}^3 \cdot \mathfrak{b}_j^3 \cdot \mathfrak{c}^3,$$

where $\mathfrak{n}\mathfrak{b}^3$, $\mathfrak{b}_j^3$ and $\mathfrak{c}$ are all principal ideals, i.e.

3.8.1 $$\mathfrak{n}\mathfrak{b}^3 = [\nu], \quad \mathfrak{b}_j^3 = [\gamma_j], \quad \mathfrak{c} = [\alpha].$$

We are thus again led to an equation in *numbers* of $K(\vartheta)$, similar to 3.6.2:

3.8.2 $$x - y\vartheta = \varepsilon_m^i \gamma_j \nu \alpha^3; \; i = 0, 1, 2; \; j = 0, 1, 2, \ldots k-1; \; \gamma_0 = 1,$$

where α contains in its denominator only factors of $\mathfrak{b}$ and the $\mathfrak{b}_j$'s.

In the most frequent case $h_m = 3$ (cf. 3.5.2), these arguments can however be simplified considerably. Then $\mathfrak{n}$ must be a principal ideal, and we can choose $\mathfrak{b} = [1]$. Let the classes be Γ, Γ^2 and $\Gamma^3 = \Pi$, and let $\mathfrak{b}_1 \in \Gamma$, $\mathfrak{b}_1^3 = [\gamma]$. As the representatives $\mathfrak{b}_j$ we can then choose

$$\mathfrak{b}_1^0 = [1] \in \Pi, \ \mathfrak{b}_1 \in \Gamma \quad \text{and} \quad \mathfrak{b}_1^2 \in \Gamma^2.$$

The equation 3.8.2 consequently takes the form

3.8.3 $$x - y\vartheta = \varepsilon_m^i \gamma^j \nu \alpha^3, \quad i \text{ and } j = 0, 1, 2,$$

where $[\gamma]$ *is the cube of any ideal which is not a principal ideal.* And the equation can be treated for *any modulus prime to* γ.

In most cases we can even find γ *as a rational integer*, e.g. if $m \not\equiv \pm 1 \pmod 9$ and $\mathfrak{p}_3$ is not a principal ideal:

$$\mathfrak{p}_3^3 = [3] = [\gamma].$$

Another case is when for instance $m = qr$, where $q \nmid (N) r$. Then $\mathfrak{p}_q$ is not a principal ideal, and we can choose

$$\mathfrak{p}_q^3 = [q] = [\gamma].$$

But there are also other possibilities for rational γ, as seen from the example

$$x^3 - 30y^3 = 19z^3.$$

Here $h_{30} = 3$, and *of the three conjugate ideal divisors of* 19, *only one belongs to the principal class*, namely

$$\mathfrak{p}_{19} = [19, \vartheta + 3] = [19 - 3\vartheta - \vartheta^2].$$

Since neither $\mathfrak{p}_2$ nor $\mathfrak{p}_5$ are principal ideals in $K(\sqrt[3]{30})$, we can take $\gamma = 2$ or 5. With $\gamma = 2$ the equation 3.8.3 becomes

3.8.4 $$x - y\vartheta = \varepsilon_{30}^i 2^j (19 - 3\vartheta - \vartheta^2) \alpha^3, \quad i \text{ and } j = 0, 1, 2,$$

which can be treated to any modulus prime to 2, and *the three values of* j *need not be considered separately.*

A similar simplification for the γ's can also be obtained when $3 \mid h_m$, $h_m > 3$, and the group of ideal-classes is *cyclic.* As an example, we can consider

3.8.5 $$x^3 - 39y^3 = 44z^3,$$

where $h_{39} = 6$; let the classes be I^k, $k = 0, 1, 2, \ldots 5$. Here $\mathfrak{p}_2 \in I$ (with an appropriate choice of I), $\mathfrak{p}_{11} \in I$, and so $\mathfrak{n} = \mathfrak{p}_2^2 \mathfrak{p}_{11} \in I^3$. As the $\mathfrak{b}$ of 3.7.1 we can choose $\mathfrak{b} = \mathfrak{p}_5 \in I^3$, and as the $\mathfrak{b}_j$'s of 3.8.1: [1], $\mathfrak{p}_3 \in I^4$ and $\mathfrak{p}_3^2 \in I^2$. The resulting equation is

3.8.6 $$x - y\vartheta = \varepsilon_{39}^i 3^j (22 + 3\vartheta + \vartheta^2)\mathfrak{a}^3, \quad i \text{ and } j = 0, 1, 2,$$

since $N(22 + 3\vartheta + \vartheta^2) = 5^3 \cdot 44 = N(\mathfrak{n}\mathfrak{b}^3)$. This equation can be treated for any modulus prime to 3 and $\mathfrak{p}_5$, and the three values of j need not be considered separately.

§ 9. In the last paragraph, we have seen how different equations 3.8.3 can be treated as one by means of rational γ's. There is still another important case where a similar reduction in the number of equations is possible, namely when

3.9.1 $$m \equiv \pm 1, \; n \equiv \pm 1 \text{ or } \pm 2 \pmod 9.$$

For the same $\mathfrak{p}_n$ we then have to treat both possibilities 3.4.1 and 3.4.3. But the former can be written as

$$[x - y\vartheta] = [9] \cdot \mathfrak{p}_n (\mathfrak{a}\mathfrak{r}^{-1})^3,$$

since $[3] = \mathfrak{r}^2\mathfrak{s}$. The rational factor 9 and the denominator $\mathfrak{r}$ in the cube do not influence an argument to *a modulus prime to* 3, in which case the two equations can be *treated simultaneously in the simplest form* 3.4.3.

A simple example of 3.9.1 is

3.9.2 $$x^3 - 10y^3 = 47z^3,$$

with the corresponding equation 3.4.3 in $K(\sqrt[3]{10})$:

3.9.3 $$[x - y\vartheta] = \mathfrak{p}_{47}\mathfrak{a}^3, \text{ or } x - y\vartheta = \varepsilon_{10}^i (3 + \vartheta + \vartheta^2)\mathfrak{a}^3,$$

since $h_{10} = 1$. — If this can be excluded to a modulus prime to 3, the same also holds for the more complicated equation corresponding to the other possibility 3.4.1:

3.9.4 $$[x - y\vartheta] = \mathfrak{r}\mathfrak{s}^2 \mathfrak{p}_{47}\mathfrak{a}^3, \text{ or } x - y\vartheta = \varepsilon_{10}^i (9 - 4\vartheta + \vartheta^2)\mathfrak{a}^3.$$

But the same argument can be used when

3.9.5 $$m \equiv \pm 1, \; n \equiv \pm 4 \pmod 9,$$

in which case 3.4.1 is the only possibility. With the same limitation for the modulus, we can treat this case in the simpler form 3.4.3. — This remark is equally useful in numerical calculations, since 3.9.5 occurs frequently in excluded equations.

CHAPTER IV. **The Resulting Cubic Equation.**

§ 1. We have seen in the last chapter that the equation

4.1.1 $$x^3 - my^3 = nz^3$$

leads to a finite number of equations

4.1.2 $$x - y\vartheta = \mu\alpha^3$$

in the field $K(\sqrt[3]{m}) = K(\vartheta)$; here

4.1.3 $$N(\mu) = n \text{ or } 3^3 \cdot n, \quad z = N(\alpha) \text{ or } 3 \cdot N(\alpha),$$

where the last alternative occurs only in the cases 3.4.1. If we put

$$\mu = e + f\vartheta + g\vartheta^2 \text{ or } \frac{e + f\vartheta + g\vartheta^2}{3},$$

$$\alpha = u + v\vartheta + w\vartheta^2 \text{ or } \frac{u + v\vartheta + w\vartheta^2}{3},$$

and equate the coefficient of ϑ^2 in 4.1.2 to zero, we get for every combination of μ and α:

4.1.4 $$\begin{cases} F(u, v, w) = g(u^3 + mv^3 + m^2w^3 + 6muvw) \\ \qquad + 3f(u^2v + muw^2 + mv^2w) \\ \qquad + 3e(u^2w + uv^2 + mvw^2) = 0, \end{cases}$$

where

4.1.5 $$N(e + f\vartheta + g\vartheta^2) = e^3 + mf^3 + m^2g^3 - 3mefg = n$$

or 3^3n in some cases when $m \equiv \pm 1 \pmod 9$ (but never 3^6, since μ has no denominator 3 in the cases 3.4.1). — "Auxiliary cubes" in μ give corresponding cubed factors in 4.1.5, but it is clear that *a solution* $(u, v, w) \neq (0, 0, 0)$ *of* 4.1.4 *will under all circumstances lead to a solution of* 4.1.2 *and consequently of the given equation* 4.1.1.

The coefficients g and w are integers only if m is squarefree. If $m = m_1 m_2^2$, we obtain integer coefficients in the expressions

$$e + f\vartheta_1 + g\vartheta_2 \quad \text{and} \quad u + v\vartheta_1 + w\vartheta_2$$

(cf. 3.1.2—3), and the modified equation 4.1.4 for the coefficient of ϑ_2 then takes the form

$$4.1.6 \qquad \begin{cases} F_1(u,v,w) = g(u^3 + m_1 m_2^2 v^3 + m_1^2 m_2 w^3 + 6 m_1 m_2 u v w) \\ \qquad + 3 m_2 f(u^2 v + m_1 u w^2 + m_1 m_2 v^2 w) \\ \qquad + 3 e(u^2 w + m_2 u v^2 + m_1 m_2 v w^2) = 0 \end{cases}$$

(cf. 5.1.3—4), where now

$$4.1.7 \qquad N(e + f\vartheta_1 + g\vartheta_2) = e^3 + m_1 m_2^2 f^3 + m_1^2 m_2 g^3 - 3 m_1 m_2 efg = n,$$

possibly with the same cubed factors. We shall however use the notation n for the norms in 4.1.5 or 4.1.7 in any case, to simplify the formulae.

§ 2. We have seen that solubility of 4.1.4 implies solubility of 4.1.1, and *x, y and z are obviously expressed as rational cubic forms in u, v and w.* But we can prove that in this case *u, v and w can also be expressed rationally by x, y and z.* Since the curves 4.1.4 and (thereby) 4.1.1 are supposed to have rational points, they can both be transformed birationally with rational coefficients into a *Weierstrass* normal form, and it suffices to show that *these forms for the two curves coincide.*

The normal form for 4.1.1 is by 1.2.2

$$4.2.1 \qquad \eta^2 = 4\xi^3 - 27 m^2 n^2.$$

The *invariants* of 4.1.4 (cf. NAGELL [2], § 1, with references) are

$$4.2.2 \qquad g_2 = -\frac{27}{4} S = 0, \quad g_3 = \frac{27}{64} T = -\frac{3^6}{2^6} m^2 n^2.$$

We have the "equianharmonic" case, and can remove rational 6th powers from g_3. As the normal form of 4.1.4 we can therefore use

$$\eta_1^2 = 4\xi_1^3 + m^2 n^2.$$

But it is well known (cf. 1.2.5) that this can be transformed birationally with rational coefficients into 4.2.1, q.e.d.

I have carried through the direct calculation of the invariants S and T from the coefficients of $F(u, v, w)$. This becomes very tedious, and can be facilitated by the following linear transformation (with *irrational* coefficients, but this does not influence the invariants):

The *Hessian* of 4.1.4 is

$$H = \begin{vmatrix} \frac{1}{6}\frac{\partial^2 F}{\partial u^2} & \frac{1}{6}\frac{\partial^2 F}{\partial u \partial v} & \frac{1}{6}\frac{\partial^2 F}{\partial u \partial w} \\ \frac{1}{6}\frac{\partial^2 F}{\partial v \partial u} & \frac{1}{6}\frac{\partial^2 F}{\partial v^2} & \frac{1}{6}\frac{\partial^2 F}{\partial v \partial w} \\ \frac{1}{6}\frac{\partial^2 F}{\partial w \partial u} & \frac{1}{6}\frac{\partial^2 F}{\partial w \partial v} & \frac{1}{6}\frac{\partial^2 F}{\partial w^2} \end{vmatrix} = -(e^3 + mf^3 + m^2 g^3 - 3mefg)\cdot(u^3 + mv^3 + m^2 w^3 - 3muvw) = -n \cdot N(u + v\vartheta + w\vartheta^2).$$

The *inflexions* of the curve $F = 0$ are determined by $H = 0$, and are consequently not rational. They lie on the three irrational lines $\left(\varrho = e^{\frac{2\pi i}{3}}\right)$:

$$u + v\vartheta + w\vartheta^2 = 0, \quad u + v\varrho\vartheta + w\varrho^2\vartheta^2 = 0, \quad u + v\varrho^2\vartheta + w\varrho\vartheta^2 = 0,$$

which we choose as new axis by the transformation

4.2.3
$$\begin{cases} U = u + v\vartheta + w\vartheta^2 \\ V = u + v\varrho\vartheta + w\varrho^2\vartheta^2 \\ W = u + v\varrho^2\vartheta + w\varrho\vartheta^2 \end{cases}, \qquad D = \begin{vmatrix} 1 & \vartheta & \vartheta^2 \\ 1 & \varrho\vartheta & \varrho^2\vartheta^2 \\ 1 & \varrho^2\vartheta & \varrho\vartheta^2 \end{vmatrix} = -3m\sqrt{-3} \neq 0.$$

If we denote by one or two dashes the replacement of ϑ by $\varrho\vartheta$ or $\varrho^2\vartheta$ respectively, we have $V = U'$, $W = U''$. — We shall also use the notation

4.2.4
$$\begin{cases} E = e + f\vartheta + g\vartheta^2, & E' = e + f\varrho\vartheta + g\varrho^2\vartheta^2, \\ & E'' = e + f\varrho^2\vartheta + g\varrho\vartheta^2. \end{cases}$$

Apart from a possible denominator 3, U and E are nothing but α and μ of § 1. The construction of $F = F(u, v, w)$ of 4.1.4 as the coefficient of ϑ^2 shows that we have

$$EU^3 = G + H\vartheta + F\vartheta^2, \quad E'V^3 = G + H\varrho\vartheta + F\varrho^2\vartheta^2, \quad E''W^3 = G + H\varrho^2\vartheta + F\varrho\vartheta^2.$$

Elimination of G and H gives

4.2.5
$$F = F(u, v, w) = \frac{1}{3\vartheta^2}(EU^3 + \varrho E'V^3 + \varrho^2 E''W^3) =$$

$= AU^3 + BV^3 + CW^3$ (say). The invariants of this form (NAGELL, loc. cit.) are

$$S' = 0, \quad T' = A^2 B^2 C^2 = \frac{n^2}{3^6 m^4},$$

since

4.2.6 $$EE'E'' = N(e + f\vartheta + g\vartheta^2) = n.$$

The invariants of the original form $F(u, v, w)$ are consequently by 4.2.3:

$$S = D^4 S' = 0, \quad T = D^6 T' = -3^3 m^2 n^2,$$

which are the values given in 4.2.2. — We note that a cubed factor for n in 4.1.5 does not disturb the above argument, since it only leads to an extra rational 6th power in the expression for g_3.

§ 3. I call 4.1.4 (or the modified form 4.1.6) the "*resulting cubic equation*" in u, v and w. This equation can often be excluded by *congruence considerations*, even if the original equation 4.1.1 is possible for all moduli. A closer study of such exclusions is the object of this and the next two chapters.

First we can show that 4.1.6 *is always possible mod* p^δ *for all* δ, *when* $p \neq 3$ *is a prime divisor of* m (and the given equation 4.1.1 is not of the type 1.1.4). — We consider the congruence mod p:

4.3.1 $$F_1(u, v, w) \equiv 0 \pmod{p},$$

and form the three derivatives

4.3.2
$$\begin{cases} \frac{1}{3}\frac{\partial F_1}{\partial u} = e(m_2 v^2 + 2uw) + m_2 f(m_1 w^2 + 2uv) + g(u^2 + 2m_1 m_2 vw) \\ \frac{1}{3}\frac{\partial F_1}{\partial v} = m_1 m_2 g(\ \ " \ \ ) + m_2 e(\ \ " \ \ ) + m_2 f(\ \ " \ \ ) \\ \frac{1}{3}\frac{\partial F_1}{\partial w} = m_1 m_2 f(\ \ " \ \ ) + m_1 m_2 g(\ \ " \ \ ) + e(\ \ " \ \ ). \end{cases}$$

The only condition for u, v and w is $p \nmid u$, since $p \mid u \,\&\, m$ implies $p \mid z = N(u + v\vartheta + w\vartheta^2)$. — We must consider several cases:

1. $p \mid m_1$, $p \nmid n$, hence $p \nmid e$. With $v \equiv 0 \pmod{p}$, the congruence 4.3.1 takes the form

4.3.3 $$u^2(gu + 3ew) \equiv 0 \pmod{p},$$

which is always soluble with $u \not\equiv 0$ (whether $g \equiv 0$ or not). Since $\frac{\partial F_1}{\partial w} \equiv 3eu^2 \not\equiv 0$, we can come from a solution mod p to a solution mod p^δ for any $\delta > 1$ by varying w only.

2. $p \mid m_2$, $p \nmid n$, hence $p \nmid e$, and 4.3.1 takes the form 4.3.3 in any case, i.e. the same argument can be used.

3. $p \mid m_1$, $p \mid n$, hence $p \nmid m_2$, $p \| n$, $p \mid e$, $p \nmid f$, and 4.3.1 takes the form

$$u^2(gu + 3m_2fv) \equiv 0 \pmod{p}, \tag{4.3.4}$$

which is soluble with $u \not\equiv 0$, $\frac{\partial F_1}{\partial v} \equiv 3m_2fu^2 \not\equiv 0$.

4. $p \mid m_2$, $p \mid n$, hence $p^2 \| n$, $p \mid e$, $p \mid g$, $p \nmid f$. All coefficients of $F_1(u, v, w)$ in 4.1.6 are divisible by p. If we remove this factor beforehand and put $w \equiv 0 \pmod{p}$, the congruence takes a form similar to 4.3.4:

$$u^2(g_1u + 3m_2'fv) \equiv 0 \pmod{p} \tag{4.3.5}$$

(where $g = pg_1$, $m_2 = pm_2'$, $p \nmid m_2'$), and the same argument applies. — This concludes the proof.

It is clear that solubility mod 3^δ must be treated separately, whether or not $3 \mid m$. This will be dealt with in Ch. V, where I give *necessary and sufficient* conditions for solubility mod 3^δ in all cases that can arise.

For any prime p such that $p \nmid 3m$, let us examine under which conditions all three derivatives in 4.3.2 can be $\equiv 0 \pmod{p}$ *simultaneously*. There are two possibilities:

1. $m_2v^2 \equiv -2uw$, $m_1w^2 \equiv -2uv$, $u^2 \equiv -2m_1m_2vw$, or multiplying together:

$$m_1m_2u^2v^2w^2 \equiv -8m_1m_2u^2v^2w^2, \text{ hence } uvw \equiv 0.$$

But one of the variables u, v or $w \equiv 0$ implies all three $\equiv 0$, which is excluded *a priori*.

2. $D \equiv 0 \pmod{p}$, where

$$D = \begin{vmatrix} e & m_2f & g \\ m_1m_2g & m_2e & m_2f \\ m_1m_2f & m_1m_2g & e \end{vmatrix} = m_2(e^3 + m_1m_2^2f^3 + m_1^2m_2g^3 - 3m_1m_2efg) = m_2n$$

(cf. 4.1.7). We can therefore expect congruence conditions for all primes p such that

4.3.6 $$p \mid n, \quad p \nmid 3m.$$

These conditions — *necessary and sufficient* for solubility mod p^δ — are developed in Ch. VI.

§ 4. The difficulty is again all *other* primes p, such that $p \nmid 3mn$. The results of the last paragraph show that it suffices to consider the congruences mod p. Since $(p, m) = 1$, it will also suffice to use the simpler form $F(u, v, w)$ of 4.1.4 (the last remark holds for the primes 4.3.6 as well). We thus have to study the congruence

4.4.1 $$F(u, v, w) \equiv 0 \pmod{p}, \quad p \nmid 3mn.$$

In this case $F(u, v, w)$ is *absolutely irreducible* mod p, and we can apply the results mentioned at the end of Ch. II. *Mordell*'s result 2.4.5 implies that 4.4.1 is soluble for all sufficiently large primes p. If the constant of the O-symbol was the same as in *Hasse*'s formula 2.4.7, we would be able to conclude about solubility immediately, since

$$N \geqq p - 2\sqrt{p} > 0 \quad \text{for } p \geqq 5.$$

And the solubility for $p = 2$ is easily verified, since $e + f\vartheta + g\vartheta^2 \equiv 1$, ϑ or $\vartheta^3 \pmod 2$ when m and n are both odd.

But we can prove the solubility of 4.4.1 independently of such considerations. We begin with the case *when m is a cubic residue of p*, i.e. for all $p = q \equiv -1 \pmod 3$ and for those $p = r \equiv +1 \pmod 3$ such that $m(R)r$. We can then find (at least) one rational integer d such that

4.4.2 $$d^3 \equiv m \pmod{p},$$

i.e. the prime p *factorizes* in $K(\sqrt[3]{m}) = K(\vartheta)$.

We first note that it suffices to find *a solution of* 4.4.1 *in* $K(\varrho)$, since a chord through this point and the conjugate solution (with respect to $K(\varrho)$) will cut the curve $F \equiv 0$ in a third rational point mod p. If $p = r = \pi_r \bar{\pi}_r$ (the factorization in $K(\varrho)$), it will also suffice to treat the coprime moduli π_r and $\bar{\pi}_r$ separately. We denote any prime π_r, $\bar{\pi}_r$ or q in $K(\varrho)$ by π.

Because of the analogy between 4.4.2 and $\vartheta^3 = m$, the equations 4.2.3—5 show that the substitution mod π:

$$4.4.3 \quad \begin{cases} U \equiv u + v\,d + w\,d^2 \\ V \equiv u + v\,\varrho\,d + w\,\varrho^2 d^2, \\ W \equiv u + v\,\varrho^2 d + w\,\varrho\,d^2 \end{cases} \qquad D = \begin{vmatrix} 1 & d & d^2 \\ 1 & \varrho\,d & \varrho^2 d^2 \\ 1 & \varrho^2 d & \varrho\,d^2 \end{vmatrix} \equiv -3\,m\sqrt{-3} \not\equiv 0,$$

after multiplication with $3\,d^2 \not\equiv 0$ will transform $F(u, v, w) \equiv 0 \pmod{\pi}$ into

$$4.4.4 \quad (e + f\,d + g\,d^2)\,U^3 + \varrho\,(e + f\,\varrho\,d + g\,\varrho^2 d^2)\,V^3 + \\ + \varrho^2 (e + f\,\varrho^2 d + g\,\varrho\,d^2)\,W^3 \equiv 0 \pmod{\pi}.$$

The product of the coefficients is $\equiv n \not\equiv 0 \pmod{\pi}$ by 4.2.6. The argument of *Marshall Hall* (Ch. II, § 2, in particular the final remarks) then shows that this congruence is always soluble for U, V and W in $K(\varrho)$, which again leads to a solution for u, v and w by 4.4.3, since $D \not\equiv 0 \pmod{\pi}$.

The resulting cubic equation $F(u, v, w) = 0$ in the form 4.2.5:

$$4.4.5 \quad F(u, v, w) = \frac{1}{3\,\vartheta^2}(E\,U^3 + \varrho\,E'\,V^3 + \varrho^2 E''\,W^3) = 0,$$

is really an equation in the field $K(\sqrt[3]{m}, \varrho) = K(\vartheta, \varrho)$. This will be the field in which we have to work if the given equation $x^3 - my^3 = nz^3$ is to be solved in $K(\varrho)$, cf. Ch. I, § 3. The *coefficients* are then also supposed to be integers of $K(\varrho)$.

I have found it convenient to define this field in a slightly different way, as *a field $\Omega(\vartheta)$ over $K(\varrho)$ as the basic field of rationality.* Since $K(\varrho)$ is *Euclidean*, all usual results about algebraic number-fields still apply, if we make an appropriate use of norm symbols from $K(\varrho)$ in all formulae relating to *the norm of an ideal* (cf. 4.4.7).

The primes π of the basic field $K(\varrho)$ are the q, π_r and π_r mentioned above, and also $\lambda = 1 - \varrho$ (where $\lambda^2 = -3\,\varrho$). The factorization of these primes in $\Omega(\vartheta)$ is similar to that given in 3.1.4. There is complete analogy for the primes dividing m; all other primes $\pi \neq \lambda$ such that $\pi \nmid m$ will behave like the r's of 3.1.4, but d' and d'' can be replaced by $\varrho^2 d$ and $\varrho\,d$:

$$4.4.6 \quad \begin{cases} [\pi] = [\pi, \vartheta - d]\,[\pi, \vartheta - \varrho^2 d]\,[\pi, \vartheta - \varrho\,d] = [\pi, d - \vartheta]\,[\pi, d - \varrho\,\vartheta]\,[\pi, d - \varrho^2 \vartheta] = \\ \quad = \mathfrak{p}_\pi\,\mathfrak{p}'_\pi\,\mathfrak{p}''_\pi, \quad \text{if} \quad \left[\frac{m}{\pi}\right] = 1, \; d^3 \equiv m \pmod{\pi} \end{cases}$$

(where I use the notation of Ch. IX, § 1 for cubic residuacity). The *norm* of a first degree prime ideal $\mathfrak{p}_\pi$, i.e. the number of residue-classes mod $\mathfrak{p}_\pi$, must be

defined as the ordinary norm in $K(\varrho)$ of the basic prime π:

4.4.7 $$N(\mathfrak{p}_\pi) = N_\varrho(\pi),$$

i.e. the number of different residue-classes mod π in $K(\varrho)$.

The factorization of the prime $\lambda = 1 - \varrho$ if $\lambda \nmid m$ is much more complicated, and shall not be treated here. I can only mention that there are *four* different possibilities of factorization, corresponding to $\delta = 1, 2, 3$ or $\geqq 4$ in the expression $\lambda^\delta \| m - 1$ (if we suppose that $m \equiv +1 \pmod{\lambda}$, if necessary after a change of sign for m). There is also a close connection between the value of δ and the form of a *basis* for $\Omega(\vartheta)$.

The proof for solubility of 4.4.4 is really *a proof in the field* $\Omega(\vartheta)$, *making use of the fact that* $[\pi]$ *factorizes.* If however

4.4.8 $$\pi \nmid \lambda m n, \quad \left[\frac{m}{\pi}\right] \neq 1,$$

a similar simplification is not possible. We then have to use the full expression for $F(u, v, w)$ in 4.4.5. Treating this as a congruence mod π, and using Marshall Hall's argument again, we conclude as above that the congruence mod π has *a solution for* u, v *and* w *in* $\Omega(\vartheta)$. But I cannot see how to come from this solution to a solution in $K(\varrho)$.

Returning to rational primes, this means that the congruence 4.4.1 in the case $m(N)p = r$ must be proved soluble by other methods. I shall give a proof which is also valid in $\Omega(\vartheta)$ for the primes π of 4.4.8, if the r of 4.4.10 is replaced by $N_\varrho(\pi)$ in accordance with 4.4.7. With the necessary modifications, the method can in fact also be used for the primes $\pi \nmid \lambda m n$ which factorize in $\Omega(\vartheta)$, leading again to the substitution 4.4.3.

We note that it is equivalent to solve the congruence corresponding to 4.1.2:

4.4.9 $$x - y\vartheta \equiv \mu \alpha^3 \pmod{[r]},$$

i.e. to show that we can find an integer α of $K(\vartheta)$ such that the coefficient of ϑ^2 in $\mu\alpha^3$ vanishes mod r. Since $m(N)r$, the natural prime r remains a prime in $K(\vartheta)$ by 3.1.4. The residues mod $[r]$ and prime to $[r]$ are given by

4.4.10 $$\alpha = u + v\vartheta + w\vartheta^2, \quad u, v \text{ and } w = 0, 1, 2, \ldots r-1, \quad (u, v, w) \neq (0, 0, 0),$$

in number $r^3 - 1 \equiv 0 \pmod{3}$. The arguments used in connection with 2.2.7 show that we can divide the integers α in *three classes,* one of cubic residues

and two of non-residues mod $[r]$. There is a one-one correspondence with the division of the *rational norms* $N(\alpha)$ in classes mod r. First

$$\alpha_1 \sim \alpha_2 \pmod{[r]} \to \alpha_1 \equiv \xi^3 \alpha_2 \pmod{[r]} \to N(\alpha_1) \equiv N(\xi)^3 N(\alpha_2) \sim N(\alpha_2) \pmod{r}$$

(with the symbol of equivalence introduced in 2.1.7). Next $N(\alpha)(R)r \to \alpha(R)[r]$ (cubic residuacity in $K(1)$ and $K(\vartheta)$ respectively), since $\alpha(N)[r]$ would imply $\vartheta \sim \alpha^i \pmod{[r]}$, $i = 0, 1$ or 2, and hence $N(\vartheta) = m(R)r$. Finally, as a simple consequence, $N(\alpha_1) \sim N(\alpha_2) \pmod{r} \to \alpha_1 \sim \alpha_2 \pmod{[r]}$.

We notice in particular that a congruence $\mu\alpha^3 \equiv \nu$, $\mu\nu \not\equiv 0 \pmod{[r]}$ is soluble if and only if $\mu \sim \nu \pmod{[r]}$.

The given equation $x^3 - my^3 = nz^3$ has at least one solution (x_1, y_1, z_1) considered as congruence mod r:

4.4.11 $$x_1^3 - my_1^3 \equiv nz_1^3 \sim n \pmod{r}$$

($z_1 \equiv 0$ is excluded by $m(N)r$). But $x_1^3 - my_1^3 = N(x_1 - y_1\vartheta)$ and $n = N(\mu)$ (possibly with *cubed* factors), and the equivalence 4.4.11 implies that

$$x_1 - y_1\vartheta \sim \mu \pmod{[r]}.$$

Hence 4.4.9 is soluble with $x \equiv x_1$, $y \equiv y_1$.

This concludes the proof for solubility of the congruence 4.4.1. As a consequence, we can say that *the conditions developed in the next two chapters will be the necessary and sufficient conditions for solubility of the congruence (to any modulus) corresponding to the resulting cubic equation.*

CHAPTER V. **Conditions mod 3^δ.**

§ 1. A direct study of the congruence conditions for the equation 4.1.4 becomes very complicated. It is much simpler to consider the corresponding equation 4.1.2:

5.1.1 $$x - y\vartheta = \mu\alpha^3,$$

and examine the form of α^3. This method has led me to a study of *the cubic residues in the purely cubic field* $K(\vartheta)$. (The principle has already been used for proving 4.4.9.)

In this chapter we shall deal with the conditions mod 3^δ, and start with the case

5.1.2 $$\underline{m \not\equiv \pm 1 \pmod 9}, \text{ i.e. } [3] = \mathfrak{p}_3^3,\ (\mathfrak{p}_3, \alpha) = 1,$$

since $3 \nmid \varepsilon$. If we take the general case 3.1.2—3, the equation 5.1.1 can be written as

5.1.3 $$x - y\vartheta_1 = (e + f\vartheta_1 + g\vartheta_2)(u + v\vartheta_1 + w\vartheta_2)^3,$$

where $\vartheta = \vartheta_1$. — We first apply an argument due to HOLZER [1]: The expression

5.1.4 $$\begin{cases} \alpha^3 = (u + v\vartheta_1 + w\vartheta_2)^3 = u^3 + m_1 m_2^2 v^3 + m_1^2 m_2 w^3 + 6 m_1 m_2 u v w \\ \quad + 3(u^2 v + m_1 u w^2 + m_1 m_2 v^2 w)\vartheta_1 + 3(u^2 w + m_2 u v^2 + m_1 m_2 v w^2)\vartheta_2, \end{cases}$$

together with $(\mathfrak{p}_3, \alpha) = 1$, shows that

5.1.5 $$\alpha^3 = (u + v\vartheta_1 + w\vartheta_2)^3 \equiv \pm 1 \pmod 3.$$

Since the product of and ratio between two numbers $\equiv \pm 1 \pmod 3$ in $K(\vartheta)$ is always of the same form, we conclude that 5.1.3 is *only possible mod* 3 *if*

5.1.6 $$\underline{g \equiv 0 \pmod 3}.$$

It is also clear that the use of an "*auxiliary cube*" prime to 3 leaves this condition unaltered.

Holzer only uses 5.1.6 for the special equation $x^3 - m y^3 = z^3$; an (improved) account of his results is given in Ch. VII, § 5.

For our purpose, we must examine the residues mod 3 of g in the three different equations 3.6.2:

5.1.7 $$x - y\vartheta_1 = \varepsilon_m^i \nu \alpha^3 = \mu \alpha^3, \quad i = 0, 1, 2.$$

The simplest possibility is the case

5.1.8 $$\varepsilon_m \equiv 1 \pmod 3$$

($\varepsilon_m \equiv -1$ is excluded by $N(\varepsilon_m) = +1$). This gives the important

Theorem II. *The three equations* 5.1.7 *are all impossible if* $m \not\equiv \pm 1 \pmod 9$, $\varepsilon_m \equiv 1 \pmod 3$ *and the coefficient* g *of* ϑ_2 *in* ν *is* $\not\equiv 0 \pmod 3$. — ϑ_2 can be replaced by ϑ^2 whenever $m \not\equiv 0 \pmod 9$.

The condition 5.1.8 is satisfied for the following cubefree values of $m \leqq 50$ and $\not\equiv \pm 1 \pmod 9$ (cf. 6.10.4):

5.1.9 $$m = 6, 12, 15, 18, 30, 33, 34, 36, 42, 45$$

(of which only $m = 30$, 34 and 42 have a class-number h_m divisible by 3). *Nearly all* excluded equations (crosses in Table 2[a]) for the values 5.1.9 — and not already excluded by class-number considerations — have been proved insoluble by Theorem II. In particular, the equations 3.6.4 and 3.8.4 are both impossible mod 3, illustrating the cases with $3 \nmid h_m$ and $3 \mid h_m$ respectively. The auxiliary cube $\mathfrak{p}_2^9$ of 3.6.4 and the $[\gamma] = [2] = \mathfrak{p}_2^3$ of 3.8.4 are both *prime to the modulus* 3.

§ 2. If 5.1.8 is not satisfied,

5.2.1 $$\varepsilon_m \not\equiv 1 \pmod 3,$$

we can show that *the condition* 5.1.6 *is always satisfied for at least one value of* i *in* 5.1.7, *and usually for one value only.* In order to get a systematic treatment of the possible cases that arise, I have constructed the *Table* 1[a]. This shows the residues mod 9 of the norm

5.2.2 $$N(\alpha) = N(u + v\vartheta + w\vartheta^2) = u^3 + mv^3 + m^2w^3 - 3muvw$$

when α runs through a complete system of residues mod 3 (or rather half such a system, since it is unnecessary to consider a change of sign for α). It is clear that $N(\alpha_1) \equiv N(\alpha_2) \pmod 9$ when $\alpha_1 \equiv \alpha_2 \pmod 3$. The values $m \equiv 1, 2, 3$ and 4 (mod 9) must be considered separately; from these we come to $m \equiv -1, -2, -3$ and -4 only by changing the sign of ϑ. A squared factor in m, $m = m_1 m_2^2$, does not influence the argument if $m_2 \not\equiv 0 \pmod 3$. If $m = 9m_1$, $3 \nmid m_1$, we can avoid the difficulties which arise by operating in the field $K(\sqrt[3]{3m_1^2})$, cf. § 3 below.

When in the equation $x^3 - my^3 = nz^3$ the numbers m and n are given mod 9, Table 1[a] shows the possible forms mod 3 of ν and ε_m in 5.1.7, since we know the norms $N(\nu) = n$ and $N(\varepsilon_m) = 1$. An "auxiliary cube" does not influence this argument, because of 5.1.5. *(We can operate mod* 3 *only if the auxiliary cube is prime to* 3.*)*

We must combine all $m \not\equiv \pm 1 \pmod 9$ with all n such that $x^3 - my^3 = nz^3$ is possible mod 9, cf. the conditions 2.1.10. This becomes a tedious enumeration of cases, and I shall only give a typical example:

$m \equiv 4$, $n \equiv \pm 3 \pmod 9$: The congruence $x^3 - 4y^3 \equiv \pm 3z^3 \pmod 9$ shows that we must have $x \equiv y \not\equiv 0 \pmod 3$, i.e.

$$x - y\vartheta \equiv \pm(-1 + \vartheta) \pmod 3.$$

Table 1[a] gives the following possible residues for ν and ε_m:

$$\left.\begin{array}{l} \pm\nu \equiv -1+\vartheta,\ 1-\vartheta^2 \text{ or } -\vartheta+\vartheta^2 \\ \varepsilon_m \equiv 1,\ -1-\vartheta^2 \text{ or } 1+\vartheta-\vartheta^2 \end{array}\right\} \pmod 3.$$

Finally 5.1.7 gives the congruence

$$-1+\vartheta \equiv \pm \varepsilon_m^i \nu \pmod 3.$$

If $\varepsilon_m \equiv 1 \pmod 3$, the only possible residue of ν is $\pm\nu \equiv -1+\vartheta$; this is nothing but Th. II. If $\varepsilon_m \not\equiv 1 \pmod 3$, we note that

$$(-1-\vartheta^2)^2 \equiv 1+\vartheta-\vartheta^2,\ (1+\vartheta-\vartheta^2)^2 \equiv -1-\vartheta^2 \pmod 3,$$

so that *the three possible residues of* ε_m *will represent* $\varepsilon_m^0 = 1$, ε_m *and* ε_m^2 *in some order*, and this holds for all combinations of m and n when $\varepsilon_m \not\equiv 1 \pmod 3$. — We form a table of multiplication for the residues of $\varepsilon_m \cdot \nu \bmod 3$:

$\pm\nu$ \ ε_m	1	$-1-\vartheta^2$	$1+\vartheta-\vartheta^2$
$-1+\vartheta$	$-1+\vartheta$	$-\vartheta+\vartheta^2$	$1-\vartheta^2$
$1-\vartheta^2$	$1-\vartheta^2$	$-1+\vartheta$	$-\vartheta+\vartheta^2$
$-\vartheta+\vartheta^2$	$-\vartheta+\vartheta^2$	$1-\vartheta^2$	$-1+\vartheta$

Since $N(\varepsilon_m \nu) = N(\nu) = n$, the products must have the same residues as ν itself. But the table also shows that the only values of $\eta = \varepsilon_m^i$ which satisfy the condition 5.1.6 are

5.2.3
$$\left\{\begin{array}{ll} \pm\nu \equiv -1+\vartheta & : \eta \equiv 1 \\ \pm\nu \equiv 1-\vartheta^2 & : \eta \equiv -1-\vartheta^2 \\ \pm\nu \equiv -\vartheta+\vartheta^2 & : \eta \equiv 1+\vartheta-\vartheta^2 \end{array}\right. \pmod 3.$$

This is expressed in condensed form in *Table 1*[b], where the entries under $m \equiv 4$, $n \equiv 3 \pmod 9$ show the possible residues mod 3 of ν and ε_m, and the crosses give the possible combinations. The crosses for $\eta \equiv 1$ show *the residues mod* 3 *of* $x - y\vartheta$ (without the double sign).

The rest of Table 1[b] is constructed similarly; there is usually one and only one possible η for given ν. But in the cases

5.2.4 $\qquad m \equiv 2,\ n \equiv \pm 1$, and $m \equiv 4,\ n \equiv \pm 4 \pmod 9$

(we are not yet concerned with $m \equiv 1$) there are *two* possible values of η, i.e. only one value of i in 5.1.7 can be excluded for each ν if $\varepsilon_m \not\equiv 1 \pmod 3$. The reason for this, e.g. in the first case 5.2.4, is that the congruence $x^3 - 2y^3 \equiv \pm z^3 \pmod 9$ leaves the two possibilities $y \equiv 0$ or $x \equiv y \not\equiv 0 \pmod 3$, i.e. $x - y\vartheta \equiv \pm 1$ or $\pm(-1 + \vartheta) \pmod 3$.

In all occurring cases, the combinations 5.2.4 have been excluded either by class-number considerations or by the methods of the next chapter. — As examples of equations where only *one* value of i in 5.1.7 is possible mod 3, I can mention:

1. $x^3 - 5y^3 = 12z^3$, $m \equiv -4$, $n \equiv 3 \pmod 9$, where we can use 5.2.3 with a change of sign for ϑ. The class-number $h_5 = 1$, and the corresponding equation in $K(\sqrt[3]{5}) = K(\vartheta)$ becomes

5.2.5 $$x - y\vartheta = \varepsilon_5^i(-2 + 3\vartheta - \vartheta^2)\alpha^3,\ \varepsilon_5 = 1 - 4\vartheta + 2\vartheta^2, \text{ where}$$
$$\nu \equiv 1 - \vartheta^2,\ \varepsilon_5 \equiv 1 - \vartheta - \vartheta^2,\ \varepsilon_5^2 \equiv -1 - \vartheta^2 \pmod 3.$$

Consequently 5.2.3 shows that we must use $i = 2$, or

5.2.6 $$x - y\vartheta = (398 - 361\vartheta + 75\vartheta^2)\alpha^3.$$

We could also have used $i = -1$ *instead of* $i = 2$. Since $\varepsilon_5^{-1} = 41 + 24\vartheta + 14\vartheta^2$, we now get the much simpler equation

5.2.7 $$x - y\vartheta = (8 + 5\vartheta + 3\vartheta^2)\alpha^3.$$

2. $x^3 - 3y^3 = 22z^3$, $m \equiv 3$, $n \equiv 4 \pmod 9$. The class-number $h_3 = 1$, and we find

5.2.8 $$x - y\vartheta = \varepsilon_3^i(7 + \vartheta - 4\vartheta^2)\alpha^3,\ \varepsilon_3 = -2 + \vartheta^2, \text{ where}$$
$$\nu \equiv 1 + \vartheta - \vartheta^2,\ \varepsilon_3 \equiv 1 + \vartheta^2,\ \varepsilon_3^2 \equiv 1 - \vartheta^2 \pmod 3.$$

Table 1[b] shows that we must use $i = 1$, or

5.2.9 $$x - y\vartheta = (-11 - 14\vartheta + 15\vartheta^2)\alpha^3.$$

§ 3. Table 1[b] does not contain $m \equiv 0 \pmod 9$, $m = 9m_1$ (with $3 \nmid m_1$, since m is cubefree), in which case we must have $n \equiv 0$ or $\pm 1 \pmod 9$ by 2.1.10. A special treatment of this possibility can be avoided if we multiply the equation $x^3 - 9m_1y^3 = nz^3$ by $3m_1^2$:

5.3.1 $$(3m_1y)^3 - 3m_1^2x^3 = -3m_1^2nz^3,$$

and work in the field $K(\sqrt[3]{3m_1^2}) = K(\vartheta)$ (identical with $K(\sqrt[3]{m})$). There are two cases to consider:

1. $n \equiv 0 \pmod 9$, $n = 9n_1$, $3 \nmid n_1$. Then we must have $3 \mid x$, $x = 3x_1$, and a factor 3^3 can be removed in 5.3.1:

$$(m_1 y)^3 - 3m_1^2 x_1^3 = -m_1^2 n_1 z^3, \tag{5.3.2}$$

which comes under one of the cases in Table 1[b] with $m \equiv 3 \pmod 9$; we get the ordinary conditions mod 3. If we had worked with the given equation in the original form $x^3 - my^3 = nz^3$, and the corresponding

$$x - y\vartheta_1 = \mu\alpha^3, \tag{5.3.3}$$

it turns out that we have to treat this *mod* 9 to compensate for the removal of 3^3 in 5.3.1; this will be shown in § 5.

2. $n \equiv \pm 1 \pmod 9$. *In this case the equation* 5.3.3 *can never be excluded mod* 3, *since the coefficient of* ϑ_2 *in* μ *is always* $\equiv 0 \pmod 3$. To show this, we use the notation 3.1.3:

$$\vartheta_1 = \sqrt[3]{9m_1}, \quad \vartheta_2 = \sqrt[3]{3m_1^2}. \tag{5.3.4}$$

A squared factor $\not\equiv 0 \pmod 3$ in m_1 does not influence the argument. For the same reason, we can replace ϑ_2 and ϑ_1 by ϑ and ϑ^2 respectively and find the possible residues mod 3 of μ from Table 1[b], with $m \equiv 3$, $n \equiv \pm 1 \pmod 9$:

$$\pm\mu \equiv 1, \quad 1 + \vartheta^2 \text{ or } 1 - \vartheta^2 \pmod 3.$$

And neither of these contains $\vartheta = \vartheta_2$.

The transformed equation 5.3.1 shows that there is a close connection between the last case and the case

$$m \equiv \pm 3, \quad n \equiv \pm 3 \pmod 9, \tag{5.3.5}$$

where $m \equiv \pm n \pmod{27}$, cf. 2.1.10. As above, *the equation* 5.3.3 *can never be excluded mod* 3 *in this case.*

Table 1[a] gives the *a priori* possible residues of ν (if $m \equiv +3 \pmod 9$):

$$\pm\nu \equiv \vartheta, \ \vartheta + \vartheta^2 \text{ or } \vartheta - \vartheta^2 \pmod 3,$$

and we have to show that the last two cases do not occur under the condition $m \equiv \pm n \pmod{27}$. Since $3 \mid m$, the norm 5.2.2 has a unique value mod 27 if $3 \mid u$:

$$n = N(\nu) \equiv \pm N(\vartheta \pm \vartheta^2) = \pm(m \pm m^2) = \pm m(1 \pm m) \equiv \pm 2m \text{ or } \pm 4m \pmod{27},$$

a contradiction. — The case 5.3.5 is therefore *not included* in Table 1[b]. On the other hand, the table also contains $m \equiv 1 \pmod 9$, for use in §§ 7 and 10.

§ 4. If $m \not\equiv 0 \pmod 3$, we can sometimes obtain further conditions when operating *mod* 9. Let us suppose $m \equiv +1 \pmod 3$; the case $m \equiv -1$ will only imply a change of sign for ϑ. Since $3 \nmid m$, a squared factor in m does not influence the argument.

In order to construct a complete system of cubic residues mod 9 and prime to 3, we have to form $\alpha^3 = (u + v\vartheta + w\vartheta^2)^3$, where α runs through a complete system of residues mod 3 and prime to $\mathfrak{p}_3 = [3, \vartheta - 1]$. Apart from a change of sign, such a system for α is given by nine residues, contained in three classes:

5.4.1 $\quad 1 \quad , \vartheta \quad , \vartheta^2$

5.4.2 $\quad 1 + \vartheta \quad , \vartheta + \vartheta^2 \quad , 1 + \vartheta^2$

5.4.3 $\quad 1 + \vartheta - \vartheta^2, \; -1 + \vartheta + \vartheta^2, \; 1 - \vartheta + \vartheta^2.$

In each class, the different elements can be transformed into each other by multiplication with ϑ or ϑ^2 and the reduction $\vartheta^3 = m \equiv 1 \pmod 3$. But from $\vartheta^3 = m$ it also follows that the influence on the resulting cubic residues of such a multiplication is only a rational factor prime to 3. All elements of one class give *the same effective cubic residue mod* 9, if we define two residues to be *effectively equivalent if they differ only by a rational factor prime to the modulus.*

There are consequently *only three effective cubic residues mod* 9 when $m \equiv 1 \pmod 3$, and it is easily seen that these are the same for the three alternatives mod 9 for m:

5.4.4 $$k\alpha^3 \equiv 1, \; 1 - 3\vartheta - 3\vartheta^2 \text{ or } 1 + 3\vartheta + 3\vartheta^2 \pmod 9,$$

corresponding to the classes 5.4.1—3 respectively. Here $(k, 3) = 1$, k a rational integer.

Let now the condition 5.1.6, $g \equiv 0 \pmod 3$, be satisfied for an equation $x - y\vartheta = \mu\alpha^3$, i.e. $\mu \equiv e + f\vartheta \pmod 3$. The possible forms for μ (apart from the sign) for the different combinations of m and n are given by the crosses in the line for $\eta \equiv 1$ in Table 1[b]. Mod 9 we may have

$$\mu \equiv e + 3e_1 + (f + 3f_1)\vartheta + 3g_1\vartheta^2 \pmod 9,$$

where e_1 f_1 and g_1 have some unspecified values. Multiplication with the three possible residues 5.4.4 for $k\alpha^3$ gives the coefficient mod 9 for ϑ^2 in $\mu\alpha^3$:

5.4.5 $$\frac{3g_1}{k},\ \frac{3g_1-3(e+f)}{k} \text{ or } \frac{3g_1+3(e+f)}{k}.$$

A necessary condition for solubility is that the coefficient can be made $\equiv 0 \pmod 9$, and this is always the case for one and only one of the expressions 5.4.5 if $e+f \not\equiv 0 \pmod 3$. — This remark is useful in the *numerical solution* of an equation 4.1.4, since it shows to which one of the classes 5.4.1—3 the residue of a possible solution $u + v\vartheta + w\vartheta^2$ must belong.

If however

5.4.6 $$e+f \equiv 0 \pmod 3,$$

all expressions 5.4.5 are $\equiv \frac{3g_1}{k} \pmod 9$, and we get the necessary condition $3g_1 \equiv 0 \pmod 9$, where $3g_1$ is the coefficient of ϑ^2 in μ. Now 5.4.6 (which takes the form $e-f \equiv 0 \pmod 3$ if $m \equiv -1 \pmod 3$) is satisfied for the following combinations in Table 1[b] with $3 \nmid m$, $m \not\equiv \pm 1 \pmod 9$:

5.4.7 $$m \equiv \pm 2 \text{ or } \pm 4,\ n \equiv \pm 3 \pmod 9,$$

and we can enunciate the following

Theorem III. *If m and n are given by one of the combinations* 5.4.7, *and*

$$x - y\vartheta = (e + f\vartheta + g\vartheta^2)\alpha^3 = \mu\alpha^3,$$

then $g \equiv 0 \pmod 9$.

(**Remark.** The use of an "*auxiliary cube*" prime to 3 does not influence Th. III. If a possible denominator α_1^3 of α^3 is removed, the resulting left hand side $(x - y\vartheta)\alpha_1^3$ will still have a coefficient $\equiv 0 \pmod 9$ for ϑ^2, since the condition 5.4.6 is satisfied for $x - y\vartheta \equiv \pm(e + f\vartheta) \pmod 3$.)

Theorem III shows a close analogy with the results of Ch. VI, where we get solubility-conditions in $K(\sqrt[3]{m})$ for each prime $p \not\equiv 3$ such that

5.4.8 $$p \mid n,\ p \nmid m.$$

When $p = 3$, we always get the condition $g \equiv 0 \pmod 3$, but additional conditions only when 5.4.8 is satisfied.

By means of Th. III, I have excluded many equations, among them 5.2.6 (or the equivalent 5.2.7), since here 5.4.7 is satisfied. But this is *not* the case for the equation 5.2.9, even if $g \not\equiv 0 \pmod 9$.

Th. III can sometimes be used for exclusion when all conditions 5.1.6, 5.1.8 and 5.4.7 are satisfied, so that *all three equations* 5.1.7 *are possible mod* 3. If we put

5.4.9 $$\varepsilon_m = 3A + 1 + 3B\vartheta + 3C\vartheta^2$$

and form $\mu = \varepsilon_m^i \nu = \varepsilon_m^i (e + f\vartheta + g\vartheta^2)$, where $g \equiv 0 \pmod 3$, it is easily seen that the coefficient of ϑ^2 in μ is $\equiv g \pmod 9$ for $i = 0$, 1 and 2 when the unit 5.4.9 satisfies the condition (corresponding signs):

5.4.10 $$3B \equiv \pm 3C \pmod 9 \text{ if } m \equiv \pm 1 \pmod 3,$$

in which case *all three values of* i *are excluded if* $g \not\equiv 0 \pmod 9$; one and only one value of i is possible mod 9 if 5.4.10 is not satisfied. — The case $g \not\equiv 0 \pmod 3$ is of course covered by Th. II. The combination for m and n must be one from 5.4.7; the only such $m \leqq 50$ is $\underline{m = 34}$ (cf. 5.1.9), and $\varepsilon_{34} = 613 - 24\vartheta - 51\vartheta^2$ satisfies the condition 5.4.10, $-24 \equiv -51 \pmod 9$.

A comparison with 5.4.4 shows that 5.4.10 is nothing but *the necessary and sufficient condition for* ε_m *to be an effective cubic residue mod* 9 (cf. Ch. VI, § 10).

§ 5. When $3 \mid m$, the argument that led to 5.4.4 does not hold. It is in fact easy to verify that the *effective* cubic residues mod 9 and prime to 3 are given by

5.5.1 $$1,\ 1 \pm 3\vartheta_1,\ 1 \pm 3\vartheta_2,\ 1 \pm 3\vartheta_1 \pm 3\vartheta_2$$

(where ϑ_1 and ϑ_2 can be replaced by ϑ and ϑ^2 whenever $m \not\equiv 0 \pmod 9$), i.e. *all possible effective residues mod* 9, which are at the same time $\equiv 1 \pmod 3$. This shows that *we cannot expect to obtain more mod* 9 *than mod* 3 in this case. — The same argument, but with much more calculations involved, shows that we cannot obtain more mod 27 than mod 9 when $3 \nmid m$. If we calculate a complete system of effective cubic residues mod 27, we find that it can be deduced from that mod 9 (i.e. 5.4.4, if we suppose $m \equiv +1 \pmod 3$) by varying it in all possible ways with ± 9, $\pm 9\vartheta$, $\pm 9\vartheta^2$ or combinations of these.

There is, however, one case where $3 \mid m$ and where we can yet operate mod 9, namely when $m \equiv n \equiv 0 \pmod 9$. With the notation 5.3.3—4, we get $\mu = e + f\vartheta_1 + g\vartheta_2 \equiv \pm \vartheta_1 \pmod 3$, since $9 \parallel n = N(\mu) = e^3 + 9m_1 f^3 + 3m_1^2 g^3 - 9m_1 efg$. If now

$$\mu = 3e_1 + (3f_1 \pm 1)\vartheta_1 + 3g_1\vartheta_2$$

is multiplied by the cubic residues 5.5.1, the resulting coefficient of ϑ_2 is always

$\equiv 3 g_1 \pmod 9$ (since $\vartheta_1^2 = 3\vartheta_2$ and $\vartheta_1 \vartheta_2 = 3 m_1$). Consequently *Theorem III holds also when* $m \equiv n \equiv 0 \pmod 9$, if ϑ^2 is replaced by ϑ_2. But as already remarked in § 3, this case can also be treated in the form 5.3.2.

§ 6. We can now show that *the necessary conditions given by* 5.1.6, *Theorem III and the concluding remark of the last paragraph are also sufficient in the case* $m \not\equiv \pm 1 \pmod 9$ *for solubility of the congruence*

5.6.1 $$F_1(u, v, w) \equiv 0 \pmod{3^\delta}$$

for all δ; F_1 is the function of 4.1.6. The coefficients of F_1 are all divisible by 3 when the condition $g \equiv 0 \pmod 3$ is satisfied; we remove this common factor, and put $g = 3 g_1$. It will then suffice to find a solution of the congruence

5.6.2 $$\frac{1}{3} F_1(u, v, w) \equiv 0 \pmod 3,$$

such that at least one of the expressions 4.3.2 for $\frac{1}{3}\frac{\partial F_1}{\partial u}$, $\frac{1}{3}\frac{\partial F_1}{\partial v}$ and $\frac{1}{3}\frac{\partial F_1}{\partial w}$ is $\not\equiv 0 \pmod 3$.

The sufficiency in the cases when $3 \mid m$ is now proved in exactly the same way as in Ch. IV, § 3, if we replace p by 3, g by $3 g_1$ and divide the left hand side of the congruences 4.3.3—5 by 3 beforehand. In the last case we have $3 \mid g_1$ by the final remark of the last paragraph; the factor $\frac{1}{3}$ in 5.6.2 must then be replaced by $\frac{1}{9}$.

We then turn to the case $3 \nmid m$. The condition of Th. III, $9 \mid g$, is then always sufficient for solubility of 5.6.2. We can take $u \not\equiv 0$, $v \equiv w \equiv 0$, and at least one of $\frac{1}{3}\frac{\partial F_1}{\partial v} \equiv m_2 f u^2$ or $\frac{1}{3}\frac{\partial F_1}{\partial w} \equiv e u^2$ is then $\not\equiv 0 \pmod 3$. — It remains to show that the condition $3 \parallel g$ is sufficient in the cases where 5.4.6 is not satisfied, i.e. $e + f \not\equiv 0 \pmod 3$ if we suppose $m \equiv +1 \pmod 3$. Since m is prime to 3, we can replace $F_1(u, v, w)$ in 5.6.1—2 by the simpler form $F(u, v, w)$ of 4.1.4, i.e. $m_1 = m$, $m_2 = 1$ in 4.3.2. A solution of the congruence 5.6.2 can then always be found by comparing 5.4.5 with the possible residues 5.4.1—3 for $\alpha = u + v\vartheta + w\vartheta^2$.

The case $3 g_1 \equiv 0 \pmod 9$ has already been treated. If $3 g_1 - 3(e + f) \equiv 0 \pmod 9$, we must choose α from 5.4.2, e.g. $u \equiv v \equiv 1$, $w \equiv 0 \pmod 3$,

$\frac{1}{3}\frac{\partial F}{\partial w} \equiv e + f \not\equiv 0 \pmod 3$. — If $3g_1 + 3(e+f) \equiv 0 \pmod 9$, we must choose α from 5.4.3, e.g. $u \equiv v \equiv 1$, $w \equiv -1$, $\frac{1}{3}\frac{\partial F}{\partial w} \equiv -(e+f) \not\equiv 0 \pmod 3$. — This concludes the proof of the necessary and sufficient conditions mod 3^ϑ when $m \not\equiv \pm 1 \pmod 9$.

§ 7. We now turn to the case

5.7.1 $$m \equiv +1 \pmod 9.$$

We will suppose this sign + throughout, since we can always obtain the corresponding formulae for $m \equiv -1$ by only changing the sign of ϑ. — The preparatory remarks are already made in Ch. III, §§ 3—4. As before, we are led to one or more equations

5.7.2 $$x - y\vartheta = \mu\alpha^3 = \varepsilon_m^i \nu \alpha^3, \quad i = 0, 1, 2,$$

possibly with a γ as in 3.8.2, if $3 \mid h_m$. Auxiliary cubes may occur in ν if $h_m > 1$, cf. 3.7.1. The principles to be used are however clearly demonstrated if we suppose $h_m = 1$, to simplify the notation. We can then put (η a unit):

5.7.3 $$\begin{cases} \mathfrak{r} = [\tau], \ \mathfrak{s} = [\sigma], \ \tau^2\sigma = 3\eta; \\ \nu_n = \text{the product of the first degree factors } \textit{prime to } 3 \text{ of } [n] \end{cases}$$

(i.e. $N(\nu_n) = n$, $\frac{1}{3}n$ or $\frac{1}{9}n$ in the cases $3 \nmid n$, $3 \parallel n$ or $9 \parallel n$ respectively). With the class-notation of Ch. III, § 3, the equations 3.4.1—4 give the following possibilities for ν and α in 5.7.2:

5.7.4 $n \equiv \pm 4 \pmod 9$: $\nu = \tau\sigma^2\nu_n \in$ class 2, $\alpha \in$ class 4, 5 or 6.

5.7.5 $n \equiv \pm 3 \pmod 9$: $\nu = \tau\nu_n \in$ " 3, $\alpha \in$ " 4.

5.7.6 $n \equiv \pm 1$ or $\pm 2 \pmod 9$: The possibility under 5.7.4,

5.7.7 and also $\nu = \nu_n \in$ class 5 or 6, $\alpha \in$ class 5 or 6.

5.7.8 $n \equiv 0 \pmod 9$: $\nu = \tau\sigma\nu_n \in$ " 2, $\alpha \in$ " 4, 5 or 6.

Since the integers of class 5 have no denominator 3, the cases where

$$\alpha \in \text{class } 5$$

can be treated by the same means as in §§ 1—6 of this chapter. Two possibilities must be considered separately:

1. The cases when $\nu \in$ class 2, i.e. 5.7.4, 5.7.6 and 5.7.8, to which we can add the following variation of 5.7.5:

5.7.9 $\quad n \equiv \pm 3 \pmod 9$: $\nu = \tau\sigma^3\nu_n \in$ class 2, $\alpha \in$ class 4, 5 or 6.

(This is of course unpractical if it is a question of complete exclusion, but can be used effectively to *simplify a search for numerical solutions.* If we can exclude for instance the possibilities $\alpha \in$ class 5 and 6, but not $\alpha \in$ class 4, we know that $9 \mid z$ for a possible solution. Similar remarks can also be useful in the other cases 5.7.4—8.)

With ν also $\varepsilon_m^i \nu \in$ class 2, but the earlier results can only be applied if ε_m has no denominator 3, $\varepsilon_m \in$ class 5. But *we can avoid a denominator* 3 *in any case if we replace* ε_m *by* η_m, *where*

5.7.10 $\quad \eta_m = \varepsilon_m$ if $\varepsilon_m \in$ class 5; $\eta_m = \varepsilon_m^2$ if $\varepsilon_m \in$ class 6,

cf. 3.3.5 and the remarks to 3.6.2. — The units ε_m (as given by *Cassels*) for cubefree $m \leqq 50$ and $\equiv \pm 1 \pmod 9$ are distributed as follows:

5.7.11
$$\begin{cases} m = 17, 26, 37, 46 & : \varepsilon_m \in \text{class } 5 \\ m = 10, 19, 28, 35, 44 & : \varepsilon_m \in \text{ " } 6 \\ m = 10, 19, 37, 44, 46 & : \eta_m \equiv 1 \pmod 3 \\ m = 10, 44, 46 & : \eta_m \text{ satisfies 5.4.10 (cf. 6.10.4).} \end{cases}$$

We can now apply the condition 5.1.6, in particular *Theorem II*, and further the methods of § 4, combined with Table 1[b] for $m \equiv 1$, $n \equiv 0 \pmod 9$ (since $N(\nu) \equiv 0 \pmod 9$ when $\nu \in$ class 2). The possible residues mod 3 of ν are given by the cross of the first line:

$$e + f\vartheta + g\vartheta^2 \equiv \pm(1 - \vartheta) \pmod 3.$$

Since $e + f \equiv 0 \pmod 3$, the condition 5.4.6 is satisfied, and hence *Theorem III holds when* $m \equiv \pm 1 \pmod 9$, $\mu \in$ *class 2 and* $\alpha \in$ *class 5.*

If $\varepsilon_m \in$ class 6 (cf. 5.7.11), we can also reach the case

$$\alpha \in \text{class } 6$$

by the same means, since any such α can be written as

5.7.12 $\quad \alpha = \varepsilon_m \alpha', \quad \alpha' \in$ class 5.

Substituting this in 5.7.2 (with ε_m replaced by η_m), we get

$$x - y\vartheta = \eta_m^i \varepsilon_m^3 \nu \alpha'^3, \quad i = 0, 1, 2.$$

But $\varepsilon_m^2 = \eta_m$, and it is equivalent to consider the equation

5.7.13 $$x - y\vartheta = \eta_m^i \varepsilon_m \nu \alpha'^3, \quad i = 0, 1, 2, \quad \alpha' \in \text{class } 5,$$

which can be treated by the modified Theorems II and III.

As an application of the above principles, we can consider the example 3.9.4:

5.7.14 $x - y\vartheta = \eta_{10}^i \tau \sigma^2 \nu_{47} \alpha^3 = \eta_{10}^i (9 - 4\vartheta + \vartheta^2)\alpha^3 = \eta_{10}^i \nu \alpha^3$, where

5.7.15 $$\varepsilon_{10} = \frac{23 + 11\vartheta + 5\vartheta^2}{3} \in \text{class } 6, \quad \eta_{10} = \varepsilon_{10}^2 = 181 + 84\vartheta + 39\vartheta^2 \equiv 1 \pmod 3.$$

The modified Th. II shows at once that $\alpha \in$ class 5 is here impossible. Since it is easily seen that $\varepsilon_{10}\nu \equiv \vartheta - \vartheta^2 \pmod 3$, the equation 5.7.13 shows that $\alpha \in$ class 6 is also impossible mod 3.

2. The case 5.7.7 must be considered separately. It follows from 3.3.5 that μ and α of 5.7.2 must *both belong to either class* 5 *or class* 6, since $\mu\alpha^3 \in$ class 5. If ε_m is replaced by the η_m of 5.7.10, we have the same relation between ν and α, and can consequently use the results from §§ 1—6 when $\nu \in$ *class* 5. The case 5.7.7 can then in some cases be *completely excluded mod* 3 *by a modified form of Theorem II.* But Theorem III does not hold, as seen from $m \equiv 1$, $n \equiv \pm 1$ or $\pm 2 \pmod 9$ in Table 1[b]. None of the possible residues

$$e + f\vartheta + g\vartheta^2 \equiv \pm 1, \ \pm\vartheta \ \text{ or } \ \pm(1 + \vartheta) \pmod 3$$

satisfy the condition 5.4.6, $e + f \equiv 0 \pmod 3$.

The condition $\nu \in$ class 5 can always be satisfied if $\varepsilon_m \in$ *class* 6 (cf. 5.7.11). If we first find a $\nu \in$ class 6, we can replace it by

5.7.16 $$\nu' = \varepsilon_m \nu \in \text{class } 5$$

before we examine if the conditions of the modified Th. II are satisfied.

As an application, we can treat the equation 3.9.3 (cf. the last example):

5.7.17 $$x - y\vartheta = \eta_{10}^i \nu_{47} \alpha^3 = \eta_{10}^i (3 + \vartheta + \vartheta^2)\alpha^3, \ \eta_{10} \equiv 1 \pmod 3,$$

where already $\nu \in$ class 5. We get complete exclusion mod 3.

The necessary conditions developed in this paragraph were shown in § 6 to be *sufficient* for solubility of the congruence 5.6.1.

§ 8. We must here insert an important remark about the use of "*auxiliary cubes*" when $m \equiv \pm 1 \pmod 9$. If we operate mod 3 or 9, such cubes must be prime to 3, i.e. chosen from the classes 5 or 6, and it is a question of how the denominator 3 in class 6 will influence the arguments. (This problem does not arise if we only use moduli prime to 3 for the exclusion.)

If $\alpha = \frac{\alpha'}{\alpha_1}$ is *fractional* in the equation $x - y\vartheta = \mu\alpha^3$, removal of the denominator α_1 (prime to 3) gives

5.8.1 $$(x - y\vartheta)\alpha_1^3 = \mu\alpha'^3.$$

If here $\alpha_1 \in$ class 6, the coefficient of ϑ^2 on the left hand side is no longer necessarily divisible by 9 or even 3, since α_1 has a denominator 3. But *we can always suppose that* $\alpha_1 \in$ *class* 5, if necessary after multiplication of numerator and denominator in $\alpha = \frac{\alpha'}{\alpha_1}$ by some integer from class 6 (since a common factor prime to 3 for both sides of 5.8.1 does not influence our arguments mod 3^δ). And α' will then belong to *the same class* 4, 5 *or* 6 as is given for α in 5.7.4—9.

If $\alpha_1 \in$ class 5 (no denominator 3), the arguments that led to Th. III, and in particular the remark to this theorem, show that the coefficient of ϑ^2 in $(x - y\vartheta)\alpha_1^3$ is

5.8.2 $$\begin{cases} \equiv 0 \pmod 9 \text{ in the cases } 5.7.4\text{—}6 \text{ and } 5.7.8\text{—}9 \\ \equiv 0 \pmod 3 \text{ in the case } 5.7.7. \end{cases}$$

None of the conditions found so far for $m \equiv \pm 1 \pmod 9$ are therefore influenced by the use of auxiliary cubes, and we shall see that the same holds for the conditions obtained later in this chapter (§ 10). *Auxiliary cubes can be chosen from any of the classes* 5 *and* 6 *when we operate mod* 3^δ. — The same remark holds for the use of γ's in 3.8.2—3.

We have seen in 5.7.12 and 5.7.16 that *the case* $\alpha \in$ *class* 6 *can be completely dealt with by the methods of the last paragraph, provided* $\varepsilon_m \in$ *class* 6. If $\varepsilon_m \in$ class 5, we can obtain the same by *an auxiliary cube from class* 6. We only have to replace an $\alpha \in$ class 6 by $\alpha_1\alpha'$, i.e. μ by $\mu\alpha_1^3$, where $\alpha_1 \in$ class 6 is some fixed integer of $K(\vartheta)$. The number α' will then belong to class 5, and the arguments of § 7 apply.

We shall see in a moment that the form of α_1^3, i.e. of the cubic residues in class 6, is very restricted. Instead of performing the multiplication $\mu\alpha_1^3$ in each separate case, it is simpler to use the theory developed in the next paragraphs, in particular Table 1[c].

(The above argument does not apply at all when $\alpha \in$ class 4. If we substitute $\alpha = \alpha_1\alpha'$, where α_1 is a fixed integer from class 4, the number α' may still belong to this class.)

§ 9. We have to examine the forms of the cubic residues in the classes 4 and 6, and shall first *define congruences when the numbers involved contain denominators* 3: The congruence

$$\frac{u + v\vartheta + w\vartheta^2}{3} \equiv \frac{u_1 + v_1\vartheta + w_1\vartheta^2}{3} \pmod{3^\delta}$$

is to be equivalent to

$$u \equiv u_1, \quad v \equiv v_1, \quad w \equiv w_1 \pmod{3^{\delta+1}}.$$

Note that we define for instance

$$1 + \vartheta + \vartheta^2 \not\equiv 0 \pmod 3,$$

even if $\frac{1 + \vartheta + \vartheta^2}{3}$ is an integer in $K(\vartheta)$ (from class 3) when $m \equiv +1 \pmod 9$. *Congruences are to refer to the coefficients only.*

According to this definition, we say that an expression $\frac{u + v\vartheta + w\vartheta^2}{3}$ is reduced mod 1, 3 or 9 if the numerator is reduced mod 3, 9 or 27 respectively. And we can prove the important

Theorem IV. *There is only one effective cubic residue mod 9 in each of the classes 4 and 6. There are further only three effective cubic residues mod 27 in the class 4; if one of these is* $\frac{1}{3}(r + s\vartheta + t\vartheta^2)$, *the other two are given by*

5.9.1 $$\frac{1}{3}(r + 27 + (s - 27)\vartheta + t\vartheta^2), \quad \frac{1}{3}(r - 27 + (s + 27)\vartheta + t\vartheta^2).$$

The form of the cubic residues can be obtained by cubing one particular integer from each class. Putting $m = 9m_1 + 1$, we find for instance for

5.9.2 Class 4: $$\left(\frac{-2 + \vartheta + \vartheta^2}{3}\right)^3 = \frac{9m_1^2 - 9m_1 - 2 - (3m_1 - 1)\vartheta + (3m_1 + 1)\vartheta^2}{3}$$

5.9.3 Class 6: $$\left(\frac{4 + \vartheta + \vartheta^2}{3}\right)^3 = \frac{9m_1^2 + 10 - (12m_1 - 7)\vartheta + (3m_1 + 7)\vartheta^2}{3} \pmod 9.$$

We begin by proving Th. IV for class 6, since this is the simplest case. Let an arbitrary integer of this class be denoted by

$$\alpha = \frac{u + v\vartheta + w\vartheta^2}{3},$$

where we can suppose u, v and w to be rational *integers* (all prime to 3), since a possible denominator $m_2 \not\equiv 0 \pmod 3$ in w does not influence the argument.

We now vary the coefficients u, v and w of α with multiples of 9, and examine the influence on α^3. The variation can be expressed by

5.9.4 $$\frac{u + v\vartheta + w\vartheta^2}{3} + 3(u_1 + v_1\vartheta + w_1\vartheta^2) = \alpha + 3\Delta,$$

where u_1, v_1 and w_1 are rational integers. Cubing this, we get

5.9.5 $$(\alpha + 3\Delta)^3 = \alpha^3 + 9\alpha^2\cdot\Delta + 27\alpha\cdot\Delta^2 + 27\Delta^3,$$

where α and $\alpha^3 \in$ class 6 (denominator 3) and $\alpha^2 \in$ class 5 (*no denominator*, cf. 3.3.5). Consequently

5.9.6 $$(\alpha + 3\Delta)^3 \equiv \alpha^3 \pmod 9,$$

and we get a complete system of cubic residues mod 9 (i.e. mod 27 in the numerator) *by cubing a complete system of residues mod* 3 *for* α.

The congruence conditions defining the different classes in Ch. III, § 3 are all homogenous in u, v and w, and it is clear that the *effective* cubic residues of α to any modulus 3^δ can be obtained by keeping one of these coefficients fixed, for instance $w = 1$. (Cf. the definition of effective residues in § 4 above.) — With the limitation $w = 1$, a complete system of residues mod 3 in class 6 can be represented by

5.9.7 $$\alpha = \frac{4 + \vartheta + \vartheta^2}{3},\quad \alpha' = \frac{1 + 4\vartheta + \vartheta^2}{3},\quad \alpha'' = \frac{-2 - 2\vartheta + \vartheta^2}{3}.$$

But α' and α'' can be obtained from α by multiplication with ϑ and $-2\vartheta^2$ respectively and reduction mod 9 of the numerator. This corresponds to multiplying the resulting *cubes* with $\vartheta^3 = m$ or $(-2\vartheta^2)^3 = -8m^2$, i.e. with rational integers prime to 3. The only *effective* cubic residue mod 9 in class 6 is therefore the one given by 5.9.3.

The proof becomes more complicated when $\alpha \in$ class 4. The complete system of residues mod 3, corresponding to 5.9.7 and with the same limitation $w = 1$,

is here given by

$$5.9.8 \qquad \alpha = \frac{-2 + \vartheta + \vartheta^2}{3}, \quad \alpha' = \frac{1 - 2\vartheta + \vartheta^2}{3}, \quad \alpha'' = \frac{4 + 4\vartheta + \vartheta^2}{3},$$

where again α' and α'' can be obtained from α by multiplication with ϑ and $4\vartheta^2$ respectively. But the congruence 5.9.6 now only holds mod 3 (mod 9 in the numerator), since $\alpha^2 \in$ class 4 of 5.9.5 has a denominator 3. A slight extension of the argument shows that the basic system to be cubed is now obtained from the α of 5.9.8 by varying the first two coefficients with multiples of 9 (still keeping $w = 1$). Such a variation can be performed by successive use of 5.9.4, with $\Delta = \pm 1$ or $\pm\vartheta$, and 5.9.5 shows that

$$(\alpha + 3\Delta)^3 \equiv \alpha^3 + 9\alpha^2 \cdot \Delta \pmod 9.$$

But $\alpha^2 \in$ class 4, and so $\alpha^2 \equiv \pm \frac{1 + \vartheta + \vartheta^2}{3} \pmod 1$, which is unaltered by multiplication with ϑ. If therefore

$$\alpha^3 = \left(\frac{u + v\vartheta + w\vartheta^2}{3}\right)^3 \equiv \frac{U + V\vartheta + W\vartheta^2}{3} \pmod 9,$$

then

$$(\alpha + 3\Delta)^3 \equiv \frac{U \pm 9 + (V \pm 9)\vartheta + (W \pm 9)\vartheta^2}{3} \pmod 9$$

(corresponding signs). But these two expressions represent the same effective cubic residue:

$$\frac{U \pm 9}{U} \equiv \frac{V \pm 9}{V} \equiv \frac{W \pm 9}{W} \pmod{27},$$

since for instance

$$V(U \pm 9) - U(V \pm 9) = \pm 9(V - U) \equiv 0 \pmod{27}.$$

This concludes the proof of 5.9.2. — It is clear that a similar result holds for the cubic residues in *class* 3, but we do not need these here.

We now turn to the second half of Theorem IV. If one of the effective cubic residues mod 27 in class 4 or 6 is given by $\frac{1}{3}(r + s\vartheta + t\vartheta^2)$, all *a priori* possibilities for these residues are

$$\frac{r + 27\delta_1 + (s + 27\delta_2)\vartheta + t\vartheta^2}{3}, \quad \delta_1 \text{ and } \delta_2 = -1, 0, 1$$

(9 combinations). A closer examination shows that all these residues are represented in class 6, and we can consequently not obtain more information mod 27 than mod 9 in this case. But we only get *three* of the nine *a priori* possible combinations in class 4, and the relation between these three is the one given by 5.9.1. — I have found no short proof of this; my method has been one of "enumeration of cases", which I leave out here. ($m \equiv 1$, 10 and 19 (mod 27) must be treated separately.)

The effective cubic residues mod 9 in the classes 4 and 6 for $m \leqq 50$ are given in *Table 1c*; the residue in class 4 is chosen as *one* of the cubic residues mod 27. (Note that the expressions in 5.9.1 are replaced by

$$\frac{r + 27 + (s + 27)\vartheta + t\vartheta^2}{3}, \quad \frac{r - 27 + (s - 27)\vartheta + t\vartheta^2}{3},$$

when $m \equiv -1 \pmod 9$. As we shall see later, we do not need the explicit form of all three cubic residues mod 27.)

The residues in Table 1c are reduced to what I thought were the simplest possible forms, by multiplication with properly chosen integers prime to 3. The residues in the classes 4 and 6 for the same m contain *the same terms with* ϑ *and* ϑ^2; this is possible because (cf. 5.9.2—3):

$$\frac{12 m_1 - 7}{3 m_1 - 1} \equiv \frac{3 m_1 + 7}{3 m_1 + 1} \pmod{27}.$$

§ 10. We now turn to the usual equation

5.10.1 $$x - y\vartheta = \eta_m^i (e + f\vartheta + g\vartheta^2)\alpha^3 = \eta_m^i \nu \alpha^3,$$

or

5.10.2 $$x - y\vartheta = \eta_m^i \cdot \frac{e + f\vartheta + g\vartheta^2}{3} \alpha^3 = \eta_m^i \nu \alpha^3,$$

where ε_m is replaced by the η_m of 5.7.10, and shall examine the conditions arising when $\alpha \in$ class 4 or 6. Here $\nu \in$ class 2 in 5.10.1 and $\nu \in$ class 3 or 6 in 5.10.2. — Three cases must be considered separately:

1. The equation 5.10.1, with $\nu \in$ class 2, i.e. the cases 5.7.4, 5.7.6 and 5.7.8—9. Let $\frac{1}{3}(r + s\vartheta + t\vartheta^2)$ be the one effective cubic residue mod 9 in class 4 or 6, i.e.

5.10.3 $$\alpha^3 \equiv k \cdot \frac{r + s\vartheta + t\vartheta^2}{3} \pmod 9, \quad (k, 3) = 1,$$

where k is an unspecified rational integer. Since r, s and t are uniquely determined mod 27, substitution in 5.10.1 gives

5.10.4 $$x - y\vartheta \equiv k \cdot \eta_m^i (e_1 + f_1\vartheta + g_1\vartheta^2) \pmod 9.$$

The denominator 3 vanishes, since all coefficients of the expression

5.10.5 $$\begin{cases} (e + f\vartheta + g\vartheta^2)(r + s\vartheta + t\vartheta^2) = er + mgs + mft + \\ \quad + (fr + es + mgt)\vartheta + (gr + fs + et)\vartheta^2 \end{cases}$$

are divisible by 3. ($\nu\alpha^3$ still belongs to class 2.)

We can now apply all earlier results from §§ 1—6 above. In particular, 5.10.4 is insoluble if $g_1 \not\equiv 0 \pmod 3$ and $\eta_m \equiv 1 \pmod 3$ (Theorem II). If $\eta_m \not\equiv 1 \pmod 3$, one and only one value of the exponent i will give a coefficient $\equiv 0 \pmod 3$ for ϑ^2, and 5.10.4 is impossible if this coefficient is $\not\equiv 0 \pmod 9$ (Theorem III). If $3 \parallel g_1$ and $\eta_m \equiv 1 \pmod 3$, the equation is impossible if η_m satisfies 5.4.10 (cf. 5.7.11).

2. The equation 5.10.2, with $\nu \in$ class 3, $\alpha \in$ class 4, i.e. the case 5.7.5. We must use the three different cubic residues mod 27 to get resulting congruences of the type 5.10.4 mod 9 (the denominator 9 vanishes, since $\nu\alpha^3 \in$ class 2). *The three congruences are however all identical mod* 9, since a replacement of $\frac{1}{3}(r + s\vartheta + t\vartheta^2)$ by the other possibilities 5.9.1 will alter the coefficients e_1, f_1 and g_1 (deduced from those of 5.10.5 by division by 9) with

$$\pm 3(e - mg), \ \pm 3(f - e) \text{ and } \pm 3(g - f),$$

which are all $\equiv 0 \pmod 9$ by the class-condition $e \equiv f \equiv g \pmod 3$ for class 3.

The one resulting congruence 5.10.4 mod 9 can now be dealt with exactly as under 1.

3. The equation 5.10.2, with $\nu \in$ class 6, $\alpha \in$ class 6, i.e. the case 5.7.7. Substitution of the only cubic residue mod 9 in class 6 now gives a congruence mod 3:

5.10.6 $$x - y\vartheta \equiv k \cdot \eta_m^i (e_1 + f_1\vartheta + g_1\vartheta^2) \pmod 3$$

(the denominator 9 vanishes, since $\nu\alpha^3 \in$ class 5 by 3.3.5). This congruence is impossible if $g_1 \not\equiv 0 \pmod 3$ and $\eta_m \equiv 1 \pmod 3$ (Theorem II). If $\eta_m \not\equiv 1 \pmod 3$, the coefficient of ϑ^2 will be $\equiv 0 \pmod 3$ for one or two values of the exponent i, in the cases $n \equiv \pm 2$ or $\pm 1 \pmod 9$ respectively (cf. Table 1[b]). Nothing more can be excluded mod higher powers of 3.

The arguments of § 8, and in particular 5.8.2, show that the above conditions still hold if we use an "*auxiliary cube*" from class 5 or 6. The coefficient of ϑ^2 on the left hand side of 5.10.4 or 5.10.6 is still $\equiv 0$ mod 9 or mod 3 respectively.

It is now simple to prove that the conditions of the cases 1.—3. above are also *sufficient congruence-conditions* mod 3^δ for the resulting cubic equation 4.1.4. We only have to substitute

$$u + v\vartheta + w\vartheta^2 = \alpha_1(u' + v'\vartheta + w'\vartheta^2),$$

where α_1 is a fixed integer from class 4 or 6. If $\alpha_1^3 = \frac{1}{3}(r + s\vartheta + t\vartheta^2)$, 4.1.4 is transformed into a similar equation in u', v' and w', but with the coefficients e, f and g replaced by those of 5.10.5, divided by 3 in the case 1. and by 9 in the cases 2.—3. The conditions attached to 5.10.4 (a coefficient $\equiv 0$ (mod 9) for ϑ^2) and 5.10.6 (coefficient $\equiv 0$ (mod 3)) represent congruence conditions mod 3^δ for the resulting equation in u', v' and w', and were shown to be sufficient at the end of § 6 above.

As an example of case 1., let us consider the equation 3.9.4. It was shown in 5.7.14—15 that this is impossible if $\alpha \in$ class 5 or 6. To treat $\alpha \in$ class 4, we note that the effective cubic residue mod 9 in this class is (Table 1[c]):

$$\frac{r + s\vartheta + t\vartheta^2}{3} \equiv \frac{1 + \vartheta - 2\vartheta^2}{3}.$$

With the notation of 5.10.4, we get

$$e_1 + f_1\vartheta + g_1\vartheta^2 = (9 - 4\vartheta + \vartheta^2)\cdot\frac{1 + \vartheta - 2\vartheta^2}{3} = 33 - 5\vartheta - 7\vartheta^2.$$

Since $\eta_{10} \equiv 1$ (mod 3), $\alpha \in$ class 4 is also impossible.

In the same way we could have excluded $\alpha \in$ class 6:

$$e_1 + f_1\vartheta + g_1\vartheta^2 = (9 - 4\vartheta + \vartheta^2)\cdot\frac{7 + \vartheta - 2\vartheta^2}{3} = 51 - 13\vartheta - 5\vartheta^2.$$

This means that the equation 3.9.2 has been completely excluded mod 3^δ (cf. 5.7.17).

As an example of the case 2. above, we can consider the equation

$$x^3 - 17y^3 = 30z^3,$$

or

$$x - y\vartheta = \eta_{17}^i \tau \nu_2 \nu_5 \alpha^3 = \eta_{17}^i \cdot \frac{-5 + 2\vartheta + \vartheta^2}{3} \alpha^3,$$

where

$$h_{17} = 1, \ \eta_{17} = \varepsilon_{17} = 18 - 7\vartheta \equiv 2\vartheta \pmod 9 \not\equiv 1 \pmod 3.$$

Multiplication with the effective cubic residue mod 27 in class 4 (Table 1[c]) gives

$$\frac{-5 + 2\vartheta + \vartheta^2}{3} \alpha^3 \equiv k \cdot \frac{-5 + 2\vartheta + \vartheta^2}{3} \cdot \frac{32 + 4\vartheta - \vartheta^2}{3} \equiv k(4 + 3\vartheta - 4\vartheta^2) \pmod 9.$$

The only possibility mod 3 is $i = 1$, but

$$(4 + 3\vartheta - 4\vartheta^2)(18 - 7\vartheta) \equiv -1 - \vartheta - 3\vartheta^2 \pmod 9$$

is impossible mod 9. The given equation is consequently insoluble.

CHAPTER VI. Conditions mod q and r.

§ 1. For any prime $q \equiv -1 \pmod 3$ such that

6.1.1 $$q \mid nz, \quad q \nmid m,$$

the equation $x^3 - my^3 = nz^3 \equiv 0 \pmod q$ leads to one single possibility for the ratio $x : y \bmod q$:

$$x \equiv dy, \quad \text{where } d^3 \equiv m \pmod q.$$

For the corresponding equation in $K(\sqrt[3]{m}) = K(\vartheta)$:

6.1.2 $$x - y\vartheta = \varepsilon_m^i \nu \alpha^3 = \mu \alpha^3,$$

this means that

6.1.3 $$x - y\vartheta \equiv y(d - \vartheta), \quad y \not\equiv 0 \pmod q,$$

is divisible by $\mathfrak{p}_q = [q, \vartheta - d]$, which is of course obvious. We shall make use of this when treating the equation 6.1.2 mod q, by examining the form of α^3, i.e. the *cubic residues* mod q.

We first note that

$$[q] = \mathfrak{p}_q \mathfrak{q}_q = [q, \vartheta - d][q, \vartheta^2 + d\vartheta + d^2]$$

by 3.1.4, where a complete system of residues mod $\mathfrak{p}_q$:

6.1.4 $$0, 1, 2, \ldots q - 1,$$

is only *reproduced* when forming the cubes. It will therefore suffice to examine *the cubic residues mod* $\mathfrak{q}_q$ *in the field* $K(\vartheta)$. Since the exponent 3 is prime to $\mathfrak{q}_q$, every cubic residue of $\mathfrak{q}_q$ is also a cubic residue of $\mathfrak{q}_q^\delta$ for all $\delta > 1$, and it suffices to treat the simplest case $\delta = 1$.

If $q \mid m$, we have seen in Ch. IV, § 3, that the resulting cubic equation is always soluble mod q, whether or not $q \mid n$. The reason for this, expressed in terms of cubic residues, is that now

$$[q] = \mathfrak{p}_q^3 = [q, \vartheta]^3,$$

where a complete system of residues — and also *cubic* residues — mod $\mathfrak{p}_q$ is again given by 6.1.4.

A little more care is required to show that no conditions are obtained by cubic residues when a prime $r \mid m$. I omit the proof, since the result is in any case covered by § 3 of Ch. IV.

§ 2. There is a one-one correspondence between the cubic residues mod $\mathfrak{q}_q$ *in* $K(\vartheta)$ *and the cubic residues mod* q *in* $K(\varrho)$, $\varrho = e^{\frac{2\pi i}{3}}$, expressed by the following equivalence:

$$6.2.1 \qquad \left(\frac{t\,d + s\,\vartheta}{\mathfrak{q}_q}\right)_3 = 1 \rightleftarrows \left[\frac{t + s\,\varrho}{q}\right] = 1,$$

where I use the notation $(\ )_3$ and $[\ ]$ for cubic residuacity in $K(\vartheta)$ and $K(\varrho)$ respectively (cf. Ch. IX, § 1). The equivalence is immediately seen when cubing the expressions

$$6.2.2 \qquad \begin{cases} (v\,d + u\,\vartheta)^3 \equiv d^2\{(u^3 - 3\,u^2 v + v^3)\,d - 3\,u\,v\,(u - v)\,\vartheta\} \pmod{\mathfrak{q}_q} \\ (v + u\,\varrho)^3 = u^3 - 3\,u^2 v + v^3 - 3\,u\,v\,(u - v)\,\varrho, \end{cases}$$

where d^2 (as a rational integer) is always a cubic residue of $\mathfrak{q}_q$.

It is well known that a complete system of residues mod q and prime to q in $K(\varrho)$ is given by (cf. Bachmann [1], pp. 185—99):

$$a + b\,\varrho, \quad a \text{ and } b = 0, 1, 2, \ldots q - 1, \quad (a, b) \not\equiv (0, 0),$$

giving in all $q^2 - 1$ residues, of which only *one third* form the group of cubic residues mod q. Since all rational integers prime to q are contained in this group, we can divide out by a coefficient $b \not\equiv 0$, thus getting a system of *effective cubic residues mod* q (cf. Ch. V, § 4):

$$1 \text{ and } t_i + \varrho, \quad i = 1, 2, 3, \ldots \frac{q - 2}{3}.$$

A list of all such t for $q < 50$ is given in *Table 1d*, which consequently also gives the effective cubic residues $td + \vartheta \bmod \mathfrak{q}_q$ in $K(\vartheta)$. To facilitate the calculation with these residues, the table also contains a list of the reciprocals mod q and the values of d for different m.

The table is constructed by means of 6.2.2. The necessary values of the forms

$$u^3 - 3u^2v + v^3 \quad \text{and} \quad 3uv(u - v)$$

were already calculated by me for use in Ch. IX, cf. 9.11.2.

§ 3. We return to 6.1.2, which by means of 6.1.3 can be written as

6.3.1 $$y(d - \vartheta) \equiv \mu\alpha^3 \pmod{q}.$$

We multiply by $3d\vartheta$ and note that

$$(-d + \vartheta)^3 = -d^3 + m + 3d^2\vartheta - 3d\vartheta^2 \equiv 3d\vartheta(d - \vartheta) \pmod{q},$$

hence

6.3.2 $$y(-d + \vartheta)^3 \equiv 3d \cdot \vartheta\mu \cdot \alpha^3 \pmod{[q] = \mathfrak{p}_q\mathfrak{q}_q}.$$

Since $-d + \vartheta$ and α are both prime to $\mathfrak{q}_q$ (cf. 3.2.3), and the rational integers y and $3d$ are cubic residues, we conclude that the given equation is only possible if

6.3.3 $$\left(\frac{\vartheta\mu}{\mathfrak{q}_q}\right)_3 = 1,$$

which can be used for *exclusions mod q*.

If $q \mid n$, we shall find a simpler form of 6.3.3, but we note that the same condition must be satisfied if $q \nmid n$, $q \mid z$. This is *of great importance by numerical solution,* since we can exclude *a priori* certain prime divisors of z.

If $q \equiv -1 \pmod 9$, we know (by 9.1.3) that

$$\left[\frac{\varrho}{q}\right] = 1, \text{ i.e. } \left(\frac{\vartheta}{\mathfrak{q}_q}\right)_3 = 1,$$

in which case the factor ϑ can be omitted in 6.3.3.

The condition 6.3.3 will only be *necessary* for solubility if $q \mid n$, in which case it can be simplified. Let

6.3.4 $$\mu = e + f\vartheta + g\vartheta^2 \quad \text{or} \quad \frac{e + f\vartheta + g\vartheta^2}{3}.$$

A denominator 3 will not influence the arguments of this chapter, and we leave it out in the intermediate formulae. From $\mathfrak{p}_q = [q, \vartheta - d] \mid \mu$, we conclude that

$$e + f d + g d^2 \equiv 0 \pmod{q}, \text{ i.e. } \mu = e + f\vartheta + g\vartheta^2 \equiv (\vartheta - d)(f + g d + g\vartheta) \pmod{q},$$

which we substitute in 6.3.1. The common factor $\vartheta - d$ is divisible by $\mathfrak{p}_q$, but prime to $\mathfrak{q}_q$. Dividing out this factor, we thus get

$$6.3.5 \qquad -y \equiv (f + g d + g\vartheta)\alpha^3 \pmod{\mathfrak{q}_q}.$$

We finally multiply this by $f - g\vartheta \not\equiv 0 \pmod{\mathfrak{q}_q}$ (since $f \equiv g \equiv 0 \to e \equiv 0 \pmod{q}$), and get

$$6.3.6 \qquad -y(f - g\vartheta) \equiv (f^2 + f g d + g^2 d^2)\alpha^3 \pmod{\mathfrak{q}_q},$$

where all factors are prime to $\mathfrak{q}_q$, and the first factor on each side is a rational integer. We therefore have

Theorem V. *If $q \nmid m$, $q \mid n$, and $x - y\vartheta = \mu\alpha^3$, where μ is given by 6.3.4, then $f - g\vartheta$ is a cubic residue of $\mathfrak{q}_q$:*

$$6.3.7 \qquad \left(\frac{f - g\vartheta}{\mathfrak{q}_q}\right)_3 = 1.$$

It is clear that the use of "auxiliary cubes" prime to q leaves 6.3.3 and 6.3.7 unaltered; the same remark holds for the corresponding conditions mod r of § 5.

By means of Table 1[d], it is easily verified whether $f - g\vartheta$ is a cubic residue of $\mathfrak{q}_q$. Then

$$f - g\vartheta \equiv -g(td + \vartheta), \text{ i.e. } -fg^{-1}d^{-1} \equiv t \pmod{q}.$$

The auxiliary tables for d and m^{-1} give a quick determination of $-fg^{-1}d^{-1}$, which must be one of the values t for the prime q in question. If this is not the case, the corresponding equation $x - y\vartheta = \mu\alpha^3$ is impossible.

It follows from 6.2.1 that the condition of Th. V can be replaced by

$$6.3.8 \qquad \left[\frac{f - g d \varrho}{q}\right] = 1,$$

which enables us to *examine primes $q > 50$ without the Table 1[d]*. The calculations involved are then not so simple; $f - g d \varrho$ must be factorized in $K(\varrho)$, and the cubic character of each prime factor determined by the cubic law of reciprocity and a small table for cubic residuacity.

§ 4. We must examine the influence of the *unit* ε_m in 6.1.2, where $\mu = \varepsilon_m^i \nu$, $i = 0, 1, 2$. It follows from 6.3.3 that *one and only one value of* i *is possible mod* q *if* ε_m *is a cubic non-residue of* $\mathfrak{q}_q$. If however ε_m is a cubic residue, it suffices to replace μ by ν in the conditions 6.3.3 or 6.3.7. In this case all the values of the exponent i are *simultaneously possible or impossible* mod q, and the calculations are much simplified. — Similar remarks apply to a non-rational γ in 3.8.3.

It is therefore of great importance to examine the cubic character of ε_m mod $\mathfrak{q}_q$, for different combinations of m and q. I shall here only give a systematic account in the two simplest and most frequently occurring cases $q = 2$ and 5. (We return to the subject in § 10 below.)

$q = 2$: This is not included in Table 1[d], because solubility mod 2 can be decided immediately. Since $q = 2 \nmid m$, we have $d = 1$, and

$$[2] = \mathfrak{p}_2 \mathfrak{q}_2 = [2, 1 + \vartheta][2, 1 + \vartheta + \vartheta^2].$$

A complete system of residues mod $\mathfrak{q}_2$ and prime to $\mathfrak{q}_2$ is given by 1, ϑ and $1 + \vartheta$, and *the only cubic residue is* 1. The condition 6.3.7 implies that *the coefficient* g *of* ϑ^2 *must be even if* m *is odd and* n *is even* (since then $\mathfrak{p}_2 | \mu$ shows that e and f are odd).

Further ε_m *is a cubic residue of* $\mathfrak{q}_2$ *if and only if* $\varepsilon_m \equiv 1 \pmod 2$. For $\varepsilon_m \equiv 1 \pmod{\mathfrak{q}_2}$ implies

$$\varepsilon_m \equiv 1 \quad \text{or} \quad 1 + (1 + \vartheta + \vartheta^2) \equiv \vartheta + \vartheta^2 \pmod 2.$$

But the latter expression is divisible by $\mathfrak{p}_2$, which is impossible since ε_m is a unit. — The odd cubefree values of $m < 50$ for which $\varepsilon_m \equiv 1 \pmod 2$ are (cf. 6.10.3—4):

6.4.1 $$m = 5, 11, 15, 21, 23, 25, 29, 31, 33, 39, 41, 43, 45, 47.$$

By means of this, we can exclude some of the previous examples (partly excluded already mod 3 or 9). The simplest cases are the equations 3.6.4, 3.8.6 and 5.2.5, which all satisfy the conditions m odd, n even, $\varepsilon_m \equiv 1 \pmod 2$, g odd. (The equation 3.8.6 can also be completely excluded mod 11, since ε_{39} is a cubic residue and $f - g\vartheta = 3 - \vartheta$ a non-residue of $\mathfrak{q}_{11}$. — Note in particular that the auxiliary cube $\mathfrak{p}_2^9$ in 3.6.4 is *prime to* $\mathfrak{q}_2$.)

For the equation 5.2.8, $\varepsilon_3 \not\equiv 1 \pmod 2$, and consequently one value of the exponent i is possible mod 2. The form of ν shows that this is $i = 0$, which has again been proved impossible to the modulus 3 (for which $i = 1$, i.e. the equa-

tion 5.2.9, is the only possibility). The given equation is therefore *excluded by a combination of two different moduli*, a case which frequently occurs.

$q = 5$: A closer examination shows that ε_m is a cubic residue of $\mathfrak{q}_5$ for the following cubefree values of $m \not\equiv 0 \pmod 5$ and < 50 (cf. 6.10.3—4):

6.4.2 $m = 2, 4, 6, 11, 12, 13, 14, 18, 22, 23, 29, 33, 34, 36, 38, 41, 42, 44, 46, 47.$

The equation 3.7.2 can be completely excluded mod 5, since ε_{11} is a cubic residue and $f - g\vartheta = -\vartheta$ a non-residue of $\mathfrak{q}_5$. (ϑ is a residue only when $q \equiv -1 \pmod 9$.)

As an example of $q > 5$, we can finally consider 3.9.2, where $q = n = 47$. This gives rise to the two different equations 3.9.3—4, which were excluded step by step mod 3 and 9 in Ch. V, §§ 7 and 10. But we have seen in Ch. III that they can both be excluded *simultaneously* in the simplest form 3.9.3, to any modulus prime to 3. And here ε_{10} is a cubic residue, but $f - g\vartheta = 1 - \vartheta$ a non-residue of $\mathfrak{q}_{47}$, i.e. complete exclusion. (If $1 - \vartheta$ should be a cubic residue, we would have (Table 1[d]):

$$-1 + \vartheta \equiv td + \vartheta, \text{ i.e. } t \equiv -d^{-1} \equiv -20^{-1} \equiv 7 \pmod{47},$$

but this is not one of the values of t for $q = 47$.)

§ 5. We now turn to the primes $p = r \equiv 1 \pmod 3$, such that $r \nmid m$, $r \mid n$. We can use the earlier formulae developed for $p = q$, with the necessary modifications.

We suppose that the original congruence conditions 2.1.10 are satisfied, i.e. $m(R)r$, and hence by 3.1.4:

$$[r] = \mathfrak{p}_r \mathfrak{p}_r' \mathfrak{p}_r'' = [r, \vartheta - d][r, \vartheta - d'][r, \vartheta - d''],$$

where

$$d^3 \equiv d'^3 \equiv d''^3 \equiv m, \; d \not\equiv d' \not\equiv d'' \not\equiv d \pmod r.$$

Consequently 6.1.3 is replaced by

6.5.1 $$x - y\vartheta \equiv y(d - \vartheta), \; y(d' - \vartheta) \text{ or } y(d'' - \vartheta) \pmod r,$$

corresponding to the *three different equations* 6.1.2, which must be treated *separately*. We will suppose $\mathfrak{p}_r = [r, \vartheta - d] \mid \mu$, i.e. $x \equiv dy \pmod r$. The modulus $\mathfrak{q}_q$ must then be replaced by the product $\mathfrak{p}_r' \mathfrak{p}_r''$. The argument that led to 6.3.2 still holds:

6.5.2 $$y(-d + \vartheta)^3 \equiv 3d \cdot \vartheta\mu \cdot \alpha^3 \pmod{\mathfrak{p}_r' \mathfrak{p}_r''}.$$

But we can no longer conclude that the rational integers y or $3d$ are cubic residues, and the treatment becomes different.

Replacing 6.5.2 by two separate congruences mod $\mathfrak{p}'_r$ and $\mathfrak{p}''_r$, and writing $\mu = \mu(\vartheta)$, $\alpha = \alpha(\vartheta)$, we get the relations

$$6.5.3 \qquad \begin{cases} y(-d+d')^3 \equiv 3d\cdot d'\,\mu(d')\cdot\{\alpha(d')\}^3 \\ y(-d+d'')^3 \equiv 3d\cdot d''\,\mu(d'')\cdot\{\alpha(d'')\}^3 \end{cases} \pmod r$$

between *rational* integers. Dividing the two congruences, we find the necessary condition corresponding to 6.3.3:

$$6.5.4 \qquad d'\,\mu(d') \sim d''\,\mu(d'') \pmod r, \quad \text{or} \quad \frac{d'\,\mu(d')}{d''\,\mu(d'')}(R)\,r$$

(with the symbol of equivalence introduced in 2.1.7). This condition must be satisfied when $r \mid nz$ such that $\mathfrak{p}_r \mid \mu\alpha$, whether or not $r \mid n$. Similar conditions are of course obtained when $\mathfrak{p}'_r$ or $\mathfrak{p}''_r \mid \mu\alpha$.

If $r \mid n$, $\mathfrak{p}_r \mid \mu$, we are again led to the congruence 6.3.5, with the modulus $\mathfrak{p}'_r\mathfrak{p}''_r$. Treating this as in 6.5.3, we get

$$6.5.5 \qquad \begin{cases} -y \equiv (f+gd+gd')\cdot\{\alpha(d')\}^3 \equiv (f-gd'')\cdot\{\alpha(d')\}^3 \\ -y \equiv (f+gd+gd'')\cdot\{\alpha(d'')\}^3 \equiv (f-gd')\cdot\{\alpha(d'')\}^3 \end{cases} \pmod r,$$

since $d + d' + d'' \equiv 0$ by 6.6.3. Dividing these expressions, we get

Theorem VI. *If* $r \nmid m$, $r \mid n$, $x - y\vartheta = \mu\alpha^3$, $\mathfrak{p}_r = [r, \vartheta - d] \mid \mu$, *where* μ *is given by* 6.3.4, *then*

$$6.5.6 \qquad \frac{f-gd'}{f-gd''}(R)\,r.$$

(It is clear that both $f - gd'$ and $f - gd''$ must be prime to r. If we suppose for instance $f - gd' \equiv 0 \pmod r$, and combine this with $\mathfrak{p}_r \mid e + f\vartheta + g\vartheta^2$, i.e. $e + fd + gd^2 \equiv 0 \pmod r$, we find $e + fd'' + gd''^2 \equiv gd''(d + d' + d'') \equiv 0 \pmod r$, and so $\mathfrak{p}''_r \mid e + f\vartheta + g\vartheta^2$, which is impossible.)

It is not difficult to show (cf. 6.9.6) that the condition 6.5.6 is equivalent to

$$6.5.7 \qquad \left[\frac{f-gd\varrho}{r}\right] = 1,$$

in complete analogy with 6.3.8. Here [ ] means the *Jacobian* symbol, i.e. the product of the cubic characters

$$\left[\frac{f-g\,d\,\varrho}{\pi_r}\right] \text{ and } \left[\frac{f-g\,d\,\varrho}{\bar{\pi}_r}\right],$$

where $r = \pi_r \bar{\pi}_r$ is the factorization of r in $K(\varrho)$. But we never need the form 6.5.7, since the simpler original condition 6.5.6 can always be dealt with by the existing tables of cubic residues.

§ 6. We must also here examine the influence of the unit ε_m^i. Replacing $\mu(\vartheta)$ by $\{\varepsilon_m(\vartheta)\}^i \cdot \nu(\vartheta)$ in 6.5.4, we see that one and only one value of the exponent i is possible if $\varepsilon_m(d') \not\equiv \varepsilon_m(d'') \pmod r$ ("inequivalent"), and all three values of i are simultaneously possible or impossible if

6.6.1 $$\varepsilon_m(d') \sim \varepsilon_m(d''), \quad \text{or} \quad \frac{\varepsilon_m(d')}{\varepsilon_m(d'')} (R)\, r,$$

in which case we can get complete exclusion mod r by considering $\nu(\vartheta)$ only.

In the two other possible cases $\mathfrak{p}_r'$ or $\mathfrak{p}_r'' \mid \mu$, we similarly have to study the ratios

$$\frac{\varepsilon_m(d)}{\varepsilon_m(d'')} \text{ and } \frac{\varepsilon_m(d)}{\varepsilon_m(d')},$$

and all calculations become particularly simple if

6.6.2 $$\varepsilon_m(d) \sim \varepsilon_m(d') \sim \varepsilon_m(d'') \pmod r.$$

We can however show that 6.6.1 *automatically implies* 6.6.2. — Let

$$\varepsilon_m(\vartheta) = e_1 + e_2\vartheta + e_3\vartheta^2$$

(where possible denominators of the coefficients are prime to r). If we note that d, d' and d'' are solutions of the congruence $x^3 - m \equiv 0 \pmod r$, and so

6.6.3 $$d + d' + d'' \equiv 0, \quad d\,d' + d\,d'' + d'\,d'' \equiv 0, \quad d\,d'\,d'' \equiv m \pmod r,$$

it is easily verified that

6.6.4 $$\begin{cases} \varepsilon_m(d)\cdot\varepsilon_m(d')\cdot\varepsilon_m(d'') \equiv (e_1^3 + m\,e_2^3 + m^2 e_3^3 - 3\,m\,e_1\,e_2\,e_3) & \pmod r \\ \qquad = N(e_1 + e_2\vartheta + e_3\vartheta^2) = N(\varepsilon_m) = 1. \end{cases}$$

The product is therefore a cubic residue of r, and this is only possible if either $\varepsilon_m(d)$, $\varepsilon_m(d')$ and $\varepsilon_m(d'')$ all belong to the same class mod r, i.e. the case 6.6.2; or they must all belong to different classes:

6.6.5 $$\varepsilon_m(d) \not\equiv \varepsilon_m(d') \not\equiv \varepsilon_m(d'') \not\equiv \varepsilon_m(d) \pmod r.$$

In this case *all* the ratios

$$\frac{\varepsilon_m(d')}{\varepsilon_m(d'')}, \quad \frac{\varepsilon_m(d)}{\varepsilon_m(d'')} \quad \text{and} \quad \frac{\varepsilon_m(d)}{\varepsilon_m(d')}$$

are cubic non-residues of r.

It is easy to show that *the condition* 6.6.2 *is satisfied if and only if* ε_m *is an effective cubic residue of* r, i.e. if there is a rational integer t and an integer ξ in $K(\vartheta)$ such that

6.6.6 $$\varepsilon_m \equiv t \cdot \xi^3 \pmod{r}.$$

(Note that ε_m is not an *ordinary* cubic residue of r if $t(N)r$.) This is in complete analogy with the results of § 4. (Cf. § 10 below.)

If we have to use a non-ratiqnal γ in 3.8.3, the calculations are similarly simplified if

$$\gamma(d) \sim \gamma(d') \sim \gamma(d'') \pmod{r}.$$

Since $N(\gamma)$ is a rational cube, there is also here only the one other possibility corresponding to 6.6.5.

As an application of Theorem VI, we can consider the equation 3.8.5 with m and n interchanged:

6.6.7 $$x^3 - 44y^3 = 39z^3,$$

where $r = 13$. The class-number $h_{44} = 1$, and

$$\varepsilon_{44} = \frac{1}{3}(113 - 2\vartheta - \frac{17}{2}\vartheta^2) \equiv 3 - 5\vartheta - 5\vartheta^2 \pmod{13}.$$

The congruence $x^3 \equiv 44 \pmod{13}$ gives $d = -2$, $d' = -5$, $d'' = -6$, and

$$\varepsilon_{44}(d) \equiv 6, \quad \varepsilon_{44}(d') \equiv -6, \quad \varepsilon_{44}(d'') \equiv -4 \sim 6 \pmod{13},$$

satisfying the condition 6.6.2. We have the case 5.7.5, where here

$$\tau = \frac{1}{3}(-17 - 4\vartheta + \frac{5}{2}\vartheta^2), \quad \nu_{13} = \frac{1}{3}(-1 + 4\vartheta - \vartheta^2),$$

$$\nu'_{13} = \frac{1}{3}(-1 + \vartheta + \frac{1}{2}\vartheta^2), \qquad \nu''_{13} = 7 + 2\vartheta + \frac{1}{2}\vartheta^2.$$

We get three possibilities for ν, each of which must be examined by the condition 6.5.6:

$$\left.\begin{aligned} \tau\cdot\nu_{13} &= \tfrac{1}{3}(211 - 58\,\vartheta - \tfrac{1}{2}\vartheta^2), & \frac{f-gd'}{f-gd''} &= \frac{-58+\frac{1}{2}(-5)}{-58+\frac{1}{2}(-6)} \equiv 6+1 \\ \tau\cdot\nu'_{13} &= \tfrac{1}{3}(13 + 14\,\vartheta - 5\,\vartheta^2), & \frac{f-gd}{f-gd''} &= \frac{14+5\cdot(-2)}{14+5\cdot(-6)} \equiv 3+1 \\ \tau\cdot\nu''_{13} &= \tfrac{1}{3}(13 - 7\,\vartheta + \vartheta^2), & \frac{f-gd}{f-gd'} &= \frac{-7-1\cdot(-2)}{-7-1\cdot(-5)} \equiv -4+1 \end{aligned}\right\} \pmod{13}.$$

All cases are impossible mod 13, and the equation 6.6.7 is consequently insoluble.

Exclusions mod r do not occur frequently. One reason for this is that the congruence conditions 2.1.10 are more "strict" in this case, and most equations with a factor r in the coefficients are excluded already at this stage. But even then the percentage of excluded equations is very small. There are about a hundred equations in Table 2^a with a prime r dividing at least one of the coefficients, and possible for all moduli. Of these only six have been excluded by the new methods of this paper, against an average of 30 % excluded equations (possible for all moduli) in Table 2^a. — This must be explained by the three different possibilities for the factor $\mathfrak{p}_r$, which make complete exclusion less probable in this case.

§ 7. In analogy with the remark to 6.3.3, we can also use the condition 6.5.4 to *facilitate a search for numerical solutions* when $r \nmid n$; the criterion shows at once whether $\mathfrak{p}_r$, $\mathfrak{p}'_r$ or $\mathfrak{p}''_r$ can divide α. (It is obviously necessary to have $m(R)\,r$, so that r factorizes in $K(\vartheta)$.)

There is however an important additional remark in this case. Let

$$\mu(\vartheta) = e + f\vartheta + g\vartheta^2,\ N(\mu) = e^3 + mf^3 + m^2g^3 - 3\,mefg = n \not\equiv 0 \pmod{r}$$

(possibly with *cubed* factors for n). The argument that led to 6.6.4 now shows that

$$6.7.1 \qquad d\,\mu(d)\cdot d'\,\mu(d')\cdot d''\,\mu(d'') \equiv mn \sim n \pmod{r},$$

since $m(R)\,r$. We must distinguish between two cases:

$\underline{n(R)\,r}$: For the three factors on the left hand side of 6.7.1, there are then the two possibilities corresponding to 6.6.2 or 6.6.5, which means that all factors $\mathfrak{p}_r$, $\mathfrak{p}'_r$ or $\mathfrak{p}''_r \mid \alpha$ are *simultaneously possible or impossible* mod r. In the latter case, $r \mid \varepsilon$ is consequently excluded.

$n(N)r$: Of the factors on the left hand side of 6.7.1, two and only two will then be equivalent mod r, which means that one and only one of $\mathfrak{p}_r$, $\mathfrak{p}'_r$ and $\mathfrak{p}''_r$ is possible mod r as factor of α. *In this case we can never exclude $r \mid z$ by our methods.*

The last remark is also of theoretical importance. We have seen in 2.2.3 that in the case

6.7.2 $$m \equiv \pm 1, \quad n \equiv \pm 3 \pmod 7,$$

we *must* have $7 \mid z$. Since $3(N)7$, such equations can never be excluded by auxiliary considerations mod 7. — But we can find the one possible $\mathfrak{p}_7 \mid \alpha$, which gives us *a unique value of the ratio $x : y$ mod $7^3 = 343$*. This is of course a great help in a search for solutions.

There is still another additional remark in the case when $r \mid n$, and the condition 6.5.6 is satisfied. From 6.5.5 we conclude that

6.7.3 $$y \sim f - g d' \sim f - g d'' \pmod r.$$

This *restricts the choice of y* to one third of the residues mod r, and hence means another simplification of a search for solutions.

§ 8. We can now prove that the conditions of Theorems V and VI are also *sufficient congruence conditions* mod p^δ ($p = q$ or r, $p \mid n$, $p \nmid m$) for the resulting cubic equation 4.1.4. We can even put $w = 0$ (or only $\equiv 0 \pmod p$), in which case the congruence $F(u, v, w) \equiv 0$ takes the form

6.8.1 $$F(u, v, w) \equiv g u^3 + 3 f u^2 v + 3 e u v^2 + m g v^3 \equiv 0 \pmod p.$$

Using the formula 4.1.5, the discriminant of the left hand side can be written as

6.8.2 $$\begin{cases} \Delta = 3^3 (3 e^2 f^2 + 6 m e f g^2 - 4 e^3 g - 4 m f^3 g - m^2 g^4) = \\ \quad = 3^3 \{3 (m g^2 - e f)^2 - 4 g n\} \equiv 3^4 (m g^2 - e f)^2 \pmod p, \end{cases}$$

since $p \mid n$. — Let $\mathfrak{p}_q = [q, \vartheta - d]$ or $\mathfrak{p}_r = [r, \vartheta - d] \mid \mu = e + f\vartheta + g\vartheta^2$, i.e. $d^3 \equiv m$, $e + f d + g d^2 \equiv 0 \pmod p$, and consequently

6.8.3 $$m g^2 - e f \equiv d (f^2 + f g d + g^2 d^2) \not\equiv 0 \pmod p.$$

The last incongruence follows for $p = q$ from $f^2 + f g d + g^2 d^2 = N_\varrho (f - g d \varrho)$ (the norm in $K(\varrho)$), which can have no prime factor q unless $q \mid f$ & $g d$. For $p = r$, we have $f^2 + f g d + g^2 d^2 \equiv (f - g d')(f - g d'') \not\equiv 0 \pmod r$ by 6.6.3 and the remark to 6.5.6.

It is clear that a solution of 6.8.1 in the case $g \equiv 0 \pmod{p}$ is given by

$$u \not\equiv 0,\ v \equiv 0,\ \frac{\partial F}{\partial v} \equiv 3fu^2 \not\equiv 0 \pmod{p},$$

and we only have to consider the case $g \not\equiv 0$. From 6.8.2—3 we see that $\Delta \not\equiv 0 \pmod{p}$, and solubility of 6.8.1 will therefore imply solubility of the corresponding congruence mod p^δ for all $\delta > 1$ (cf. the beginning of § 3, Ch. II). Since Δ is a quadratic residue of p, it follows from a well-known result (cf. SKOLEM [2]) that the congruence 6.8.1 has *three* solutions mod p if it has one. And the solubility is now easily shown.

Let first $p = q$, and the condition 6.3.7 be satisfied. This implies that we can find two rational integers u_1 and v_1, not both $\equiv 0 \pmod{q}$, such that

6.8.4 $$f - g\vartheta \equiv (u_1 + v_1\vartheta)^3 \equiv u_1^3 - 3d^2u_1v_1^2 + mv_1^3 + 3(u_1^2v_1 - du_1v_1^2)\vartheta \pmod{\mathfrak{q}_q},$$ i.e.

$$f \equiv u_1^3 - 3d^2u_1v_1^2 + mv_1^3,\quad g \equiv 3(du_1v_1^2 - u_1^2v_1) \pmod{q}.$$

But $e \equiv -fd - gd^2 \pmod{q}$, so 6.8.1 can be written as

$$g(u^3 - 3d^2uv^2 + mv^3) \equiv 3f(duv^2 - u^2v) \pmod{q},$$

and we see at once that $u \equiv u_1,\ v \equiv v_1$ is a solution.

Let next $p = r$, and the condition 6.5.6 be satisfied. This implies that we can find three rational integers t, x_1 and x_2, all prime to r, such that

6.8.5 $$f - gd' \equiv tx_1^3,\quad f - gd'' \equiv tx_2^3 \pmod{r}.$$

We next define two other rational integers by

$$u_1 + v_1d' \equiv x_1,\quad u_1 + v_1d'' \equiv x_2 \pmod{r},$$

which is possible since $\begin{vmatrix} 1 & d' \\ 1 & d'' \end{vmatrix} = d'' - d' \not\equiv 0$. But then 6.8.5 is equivalent to

$$f - g\vartheta \equiv t(u_1 + v_1\vartheta)^3 \pmod{\mathfrak{p}_r'\mathfrak{p}_r'' = [r, \vartheta^2 + d\vartheta + d^2]},$$

in complete analogy with 6.8.4, and as above we see that 6.8.1 is soluble mod r.

This concludes the proof for the sufficiency of the conditions mod q and r. — In this connection, it may be worth while noting the almost obvious result that *the class-number conditions of Ch. III and the conditions of Ch. V and VI mod 3^δ, q and r contain the original congruence conditions* 2.1.10.

There are no elementary conditions mod any prime q, or mod 9 if $m \equiv \pm 1 \pmod 9$. If $m \not\equiv \pm 1 \pmod 9$, the condition $5.1.6 : g \equiv 0 \pmod 3$, i.e.

$$n = N(e + f\vartheta_1 + g\vartheta_2) \equiv e^3 + mf^3 \pmod 9,$$

shows that $x^3 - my^3 \equiv nz^3 \pmod 9$ is soluble. The case $3 \| m$, $3 \| n$ implies $3 | e$, $3 \nmid f$, and so $f^3 \equiv \pm 1 \pmod 9$, $m \equiv \pm n \pmod{27}$.

If $r | n$, $r \nmid m$, the prime r does not factorize in $K(\vartheta)$ unless $m(R)r$. And if $r | m$, $r \nmid n$, we have $n = N(e + f\vartheta + g\vartheta^2) \equiv e^3 \not\equiv 0 \pmod r$, so $n(R)r$. In this case the class-number h_m is always divisible by 3, and $n(N)r$ would have been excluded at the stage of *class-number considerations* in Ch. III. — If finally $m = r^i m_1$, $n = r^i n_1$, $i = 1$ or 2, $r \nmid m_1 n_1$, we must have $r | e$, $r \nmid f$, and in the case $i = 2$ also $r | g$. The norm-expression for n shows that

$$n_1 \equiv m_1 f^3 \pmod r, \quad \text{i.e. } m_1 \sim n_1, \quad m_1 n_1^2 (R) r.$$

If this condition is not satisfied, the equation in $K(\vartheta)$ would again be excluded by class-number considerations.

The insoluble case 1.1.4 is not dealt with in Ch. IV—VI. If for instance $p \| m$, $p^2 \| n$, we must have $p | e$, $p | f$, $p \nmid g$, and so

$$x - y\vartheta \equiv g\vartheta^2 \alpha^3 \pmod{[p] = \mathfrak{p}_p^3 = [p, \vartheta]^3}.$$

As under 1.1.4, we conclude in turn that

$$\mathfrak{p}_p | x,\ p | x; \quad \mathfrak{p}_p | y,\ p | y; \quad \mathfrak{p}_p | \alpha,\ p | z.$$

We could also have concluded in turn that $p | u$, v & w in the resulting cubic equation 4.1.4.

§ 9. I shall finally show how the necessary and sufficient congruence conditions of this chapter can be deduced directly from the resulting cubic equation, by means of the field $\Omega(\vartheta)$ introduced in Ch. IV, § 4. We suppose that π is a prime in $K(\varrho)$ such that

6.9.1 $$\pi | n, \quad \pi \nmid \lambda m, \quad \left[\frac{m}{\pi}\right] = 1,$$

and so π factorizes in $\Omega(\vartheta)$ by 4.4.6:

$$[\pi] = \mathfrak{p}_\pi \mathfrak{p}'_\pi \mathfrak{p}''_\pi = [\pi, d - \vartheta][\pi, d - \varrho\vartheta][\pi, d - \varrho^2\vartheta].$$

Then 4.4.5 shows that we must solve the congruence

6.9.2 $$EU^3 + \varrho E' V^3 + \varrho^2 E'' W^3 \equiv 0$$

to the three (coprime) moduli $\mathfrak{p}_\pi$, $\mathfrak{p}'_\pi$ and $\mathfrak{p}''_\pi$. If now for instance (cf. 4.2.4):

6.9.3 $\mathfrak{p}_\pi = [\pi, d-\vartheta] \,|\, E = e + f\vartheta + g\vartheta^2$, i.e. $e + fd + gd^2 \equiv 0 \pmod{\pi}$,

then $\mathfrak{p}'_\pi \,|\, E'$, $\mathfrak{p}''_\pi \,|\, E''$, and the necessary and sufficient conditions for solubility of 6.9.2 to the three moduli are respectively

6.9.4
$$\varrho E' \sim \varrho^2 E'' \pmod{\mathfrak{p}_\pi},$$
$$\varrho^2 E'' \sim E \pmod{\mathfrak{p}'_\pi} \quad \text{and} \quad E \sim \varrho E' \pmod{\mathfrak{p}''_\pi}.$$

It is only necessary to consider the first one, since the two others can be deduced from this simply by taking conjugates. Substituting in 6.9.4 the expressions 4.2.4 for E' and E'', and further (from 6.9.3) $e \equiv -fd - gd^2 \pmod{\pi}$, we get

$$\varrho(-fd - gd^2 + f\varrho\vartheta + g\varrho^2\vartheta^2) \sim \varrho^2(-fd - gd^2 + f\varrho^2\vartheta + g\varrho\vartheta^2) \pmod{\mathfrak{p}_\pi = [\pi, d-\vartheta]},$$

which gives a condition mod π if ϑ is replaced by d. Dividing out by $d\varrho(1-\varrho) \not\equiv 0 \pmod{\pi}$, we find this condition:

6.9.5
$$f - gd\varrho^2 \sim f - gd\varrho \pmod{\pi}, \quad \text{or} \quad \left[\frac{f-gd\varrho}{\pi}\right] = \left[\frac{f-gd\varrho^2}{\pi}\right] = 1.$$

This will be the only type of condition in the case 6.9.1 *if the given equation* $x^3 - my^3 = nz^3$ *is treated in the field* $\Omega(\vartheta)$, *leading to an equation* $x - y\vartheta = \mu\alpha^3$ *with* $\mathfrak{p}_\pi = [\pi, d-\vartheta] \,|\, \mu$.

The earlier conditions of this chapter are now easily deduced from 6.9.5, when m, f, g and d are all *absolutely rational*. If $\pi = q$, the characters

$$\left[\frac{f-gd\varrho}{q}\right] \text{ and } \left[\frac{f-gd\varrho^2}{q}\right]$$

have *conjugate* values in $K(\varrho)$ by 9.1.5, and their quotient is 1 only if both characters $= 1$, i.e. the condition 6.3.8. — For a prime $r = \pi_r\bar{\pi}_r$, we must use both factors as π in 6.9.5. But with an appropriate choice of the earlier d' and d'', we have

6.9.6
$$\begin{cases} d\varrho \equiv d', \; d\varrho^2 \equiv d'' \pmod{\pi_r}; \; d\varrho^2 \equiv d', \; d\varrho \equiv d'' \pmod{\bar{\pi}_r}, \text{ and so} \\ \dfrac{f-gd\varrho}{f-gd\varrho^2} \equiv \dfrac{f-gd'}{f-gd''} \pmod{\pi_r}, \; \equiv \dfrac{f-gd''}{f-gd'} \pmod{\bar{\pi}_r}, \end{cases}$$

and $\pi = \pi_r$ or $\bar{\pi}_r$ in 6.9.5 both lead to the condition 6.5.6.

I suppose that the conditions mod 3^δ of Ch. V can also be deduced in $\Omega(\vartheta)$ from the form 4.4.5 of the resulting cubic equation, by operating mod suitable powers of $\lambda = 1 - \varrho$. But such considerations seem to become very complicated, and I have not tried to carry them through.

§ 10. We conclude this chapter with some remarks about the cubic character of the units ε_m. We have seen repeatedly how important it is to study this character mod 3^δ, mod $\mathfrak{q}_q$ and mod r for different primes q and r. It will now turn out that *cubic residuacity can in most cases be determined without even knowing the unit.*

Let us consider the field $K(\vartheta) = K(\sqrt[3]{2})$, with the class-number $h_2 = 1$. It follows from 3.1.4 that

$$\mathfrak{p}_3^3 = [3].$$

But $\mathfrak{p}_3$ is a principal ideal, $\mathfrak{p}_3 = [\nu_3]$ (in this case we may choose $\nu_3 = 1 + \vartheta$), and we conclude that there exists a unit $\eta = \varepsilon_2^i$ such that

6.10.1 $$\nu_3^3 = 3\eta = 3\varepsilon_2^i, \quad 3 \nmid i.$$

Since the rational integer 3 is a cubic residue of all $\mathfrak{q}_q$ ($q = m = 2$ is of course excluded *a priori*), it follows that the same property holds for the basic unit ε_2, which is also (by 6.6.6) an effective cubic residue of all primes r. We shall say that ε_2 is of Type 1, i.e.: *A fundamental unit ε_m is of Type 1 when it is a cubic residue of all $\mathfrak{q}_q$ and an effective cubic residue of all r* (q and $r \nmid m$).

It is clear that ε_m is of Type 1 whenever $m = q$ or q^2, $q \not\equiv -1 \pmod 9$, $h_m \not\equiv 0 \pmod 3$. This covers the following cubefree values of $m \leqq 50$:

$$m = 2, 4, 5, 11, 23, 25, 29, 41, 47.$$

We cannot draw the same conclusion when $m = r$ or r^2, since then always $h_m \equiv 0 \pmod 3$, i.e. $\mathfrak{p}_3$ is not necessarily a principal ideal. When $m \equiv \pm 1 \pmod 9$, $[3] = \mathfrak{r}^2\mathfrak{s}$ is no longer the cube of an ideal.

We next consider the field $K(\vartheta) = K(\sqrt[3]{6})$, $h_6 = 1$. Here 6.10.1 still holds, together with a similar relation deduced from $[2] = \mathfrak{p}_2^3$:

6.10.2 $$\nu_2^3 = 2\eta = 2\varepsilon_6^i, \quad 3 \nmid i.$$

The factor 3 has disappeared on the right hand side. As a consequence, the basic unit ε_6 will not only have the properties of Type 1, but will also be an (effective)

cubic residue mod 3^δ for all exponents δ. (Since here $3 \mid m$, this only implies $\varepsilon_6 \equiv 1 \pmod 3$. For a value of $m \not\equiv 0 \pmod 3$, the additional condition 5.4.10 will also be satisfied. — If $m \equiv \pm 1 \pmod 9$, ε_m must be replaced by the η_m of 5.7.10.)

The last argument fails in the first case $m = 2$, since then $\nu_2 = \vartheta$, and we can deduce nothing from the trivial relation $\vartheta^3 = m$.

We say that *a fundamental unit ε_m is of Type 2 when it is of Type 1 and is in addition an (effective) cubic residue mod 3^δ for all δ.* It is clear that ε_m is of Type 2 whenever m is composite ($m = p^2$ excluded) and $h_m \not\equiv 0 \pmod 3$. This covers the following cubefree values of $m \leqq 50$:

$$m = 6, 10, 12, 15, 18, 33, 36, 44, 45, 46.$$

Let next $m = 14$, where $h_{14} = 3$. All the ideals $\mathfrak{p}_2$, $\mathfrak{p}_3$ and $\mathfrak{p}_7$ are non-principal, but

$$\mathfrak{p}_2 \mathfrak{p}_3 = [-2 + \vartheta]$$

shows that ε_{14} is of *Type 1*. The same principle ($3 \mid h_m$, $m \equiv \pm 2$ or $\pm 4 \pmod 9$ and composite) shows that the values

$$m = 14, 20, 22, 38, 50$$

are all of Type 1.

But we can also get the stronger *Type 2* in some cases when $3 \mid h_m$, e.g. when $3 \| h_m$ and m has at least three different prime factors ($m = 30$ and 42), or in the cases when m is composite and has a prime factor $p \neq 3$ such that $\mathfrak{p}_p$ is a principal ideal ($m = 34$).

To sum up, the following cubefree $m \leqq 50$ are of Type 1, and it is easily verified that there are no others:

6.10.3 Type 1 only: $m = 2, 4, 5, 11, 14, 20, 22, 23, 25, 29, 38, 41, 47, 50$

6.10.4 Type 2: $m = 6, 10, 12, 15, 18, 30, 33, 34, 36, 42, 44, 45, 46$.

We do not get all m for which ε_m is a cubic residue of different moduli. A comparison between 6.4.1 and the odd values of 6.10.3—4 shows that $m = 21$, 31, 39 and 43 are missing among the latter ones. Similarly $m = 13$ of 6.4.2 is missing. But 6.10.4 coincides with the combined values of 5.1.9 and the last line of 5.7.11.

CHAPTER VII. Results of the Calculations.

§ 1. As an application of my methods, I have treated systematically all equations

7.1.1 $$x^3 + my^3 + nz^3 = 0, \quad 2 \leqq m < n \leqq 50,$$

with *cubefree* m and n, and the result is given in *Table* 2^a. The case $n = 1$ will be dealt with later in this chapter (§ 5), and in Ch. IX. Note that x *has changed sign* from the equation in the earlier form, $x^3 - my^3 = nz^3$. — The upper limit 50 is the same as in CASSELS' [1] tables for class-numbers and units in $K(\sqrt[3]{m})$.

It is clear that several of the equations 7.1.1 will be *equivalent*, i.e. they can be reduced to the same equation

7.1.2 $$ax^3 + by^3 + cz^3 = 0, \ 1 \leqq a < b < c, \ (a, b) = (a, c) = (b, c) = 1$$

(which is not itself included in Table 2^a if $a > 1$ or if $c > 50$). For instance, there is equivalence between the three equations

7.1.3 $$x^3 + 4y^3 + 12z^3 = 0, \quad x^3 + 9y^3 + 18z^3 = 0, \quad x^3 + 2y^3 + 3z^3 = 0,$$

of which the last one has the form 7.1.2.

When constructing Table 2^a, I worked in the following steps:

1. I excluded all equations 7.1.1 which do not satisfy the elementary congruence conditions 1.1.4 or 2.1.10 (horizontal lines in Table 2^a); this was readily done.

2. I examined the remaining equations for the existence of simple solutions. In most cases this is quickly done; to facilitate the search, I constructed an auxiliary table of the products mx^3 for $m \leqq 50$, $x \leqq 16$.

3. For the equations with no simple solutions, I used the class-number considerations of Ch. III and the conditions of Ch. V—VI to see which of them could be proved impossible (crosses in Table 2^a). I examined all equations in both fields $K(\sqrt[3]{m})$ and $K(\sqrt[3]{n})$, and it was a striking experience that *every excluded equation could be proved impossible in both these fields.* (Equivalent equations of the type 7.1.3 were treated as *different.*) A single exception would have shown the insufficiency of my conditions in one field $K(\sqrt[3]{m})$ alone.

4. For the remaining equations, I tried to find solutions by the methods of the two next paragraphs. There are still a few equations of which I have no solution (blank spaces in Table 2[a]), namely the following combinations (m, n):

7.1.4 $$(11, 43), (17, 41), (29, 47), (41, 46).$$

None of these can be excluded in either field $K(\sqrt[3]{m})$ or $K(\sqrt[3]{n})$, and I believe that they are all soluble.

§ 2. In order to solve numerically an equation which cannot be excluded by some means, and where a simple solution is not found, I have used two different methods of "trial and error".

The first principle is simply to examine the given equation

7.2.1 $$x^3 - my^3 = nz^3,$$

draw the possible information about the unknowns x, y and z, substitute suitable values of x and y and examine if the left hand side divided by n becomes a perfect cube. This sounds an enormous task, but does in fact lead to a quick solution in many cases, because the choice of x and y is usually very restricted.

For any prime q dividing n, the ratio $x : y \equiv d \pmod q$ is uniquely determined. For a prime $r \mid n$, there are three corresponding ratios d, d' and d'', but one or two of these may be proved impossible by the criterion 6.5.6. If $m \not\equiv \pm 1 \pmod 9$, the ratio $x : y$ or $y : x$ will also be uniquely determined mod 3, except in the cases 5.2.4. If $m \equiv \pm 1 \pmod 9$, we can sometimes (if $n \equiv \pm 3$ or ± 4) conclude that $3 \mid z$, and by the remark to 5.7.9 even $9 \mid z$, which will give the ratio $x : y$ mod a higher power of 3. — In the case 6.7.2, we have also seen that the ratio $x : y$ is uniquely determined mod 7^3. Further 2.2.3 shows that $7 \mid x$ if $m \equiv \pm n \equiv \pm 2 \pmod 7$.

The result of these simultaneous congruences for $x : y$ is a usually unique value d such that

7.2.2 $$x \equiv dy \pmod{3^i 7^j n}, \quad i \geqq 0, \ j = 0, 1 \text{ or } 3.$$

We next examine the possible prime divisors of x and y. In the case of x, we can sometimes conclude mod 9 that $3 \mid x$ or $3 \nmid x$, and further x must be prime to m and n if $(m, n) = 1$ and divisible by an $(m, n) > 1$; these conditions will already be partly contained in 7.2.2. Apart from this, the only prime factors of x which can be shown impossible from 7.2.1 are the primes $r \equiv 1 \pmod 3$ such that $r \nmid mn$, $m + n \pmod r$.

For the prime divisors of y, we can sometimes conclude mod 9 that $3 \mid y$ or $3 \nmid y$, and 2.2.3 shows that $7 \mid y$ if $m \equiv \pm 3$, $n \equiv \pm 1 \pmod 7$. Further y must be prime to n (even if $(m, n) > 1$, since then $(m, n) \mid x$, and $(x, y) = 1$). The possible prime factors $r \mid y$ must be such that $n(R)r$; if $r \mid n$, the remark 6.7.3 is also useful. But we can usually obtain more information about y if we write 7.2.1 as

7.2.3 $$x^3 - nz^3 = my^3$$

and *operate in the field* $K(\sqrt[3]{n})$.

We can never exclude common factors of y and m, since then 7.2.3 would be completely excluded in $K(\sqrt[3]{n})$. For the primes $q \equiv -1 \pmod 3$ such that $q \nmid mn$, the criterion 6.3.3 gives several q for which $q \mid y$ is impossible. The most useful case is $q = 2$, i.e. m and n odd. It is of course a great help to know that y must be odd. If we can also exclude $2 \mid z$ (from the original form 7.2.1, in $K(\sqrt[3]{m})$), we know that x *must be even*. (A similar conclusion is not possible if $q > 2$.) — For the prime divisors $r \mid y$, $r \nmid mn$, we have already noted that we must have $n(R)r$. It follows from § 7 of Ch. VI that we can then exclude $r \mid y$ in $K(\sqrt[3]{n})$ only if also $m(R)r$.

If $n \equiv \pm 1 \pmod 9$, the methods of Ch. V (cf. the remark to 5.7.9) will sometimes give us only one of the three possibilities $3 \nmid y$, $3 \parallel y$ or $9 \mid y$. In the first case we may also be able to restrict α to one of the classes 5 or 6, which will further limit the choice of y if $\varepsilon_n \in$ class 5 (no denominator 3).

We can finally get a limitation for y by class-number considerations when $h_n > 1$, cf. the concluding remark of Ch. III, § 7, for the case when $3 \nmid h_n$. A similar limitation can be obtained when $h_n = 3k > 3$.

§ 3. My other method is to examine *the resulting cubic equation* 4.1.4 (or 4.1.6) for solutions. It is much more difficult to systematize this search, and it can only be a question of finding comparatively small solutions in u, v and w. (But even then the corresponding solution in x, y and z may be rather big.)

The earlier results about x, y and z do not help us very much. If we can show by some means for the equation 7.2.1 that for instance $q \nmid z$, then all we can say is that

7.3.1 $\mathfrak{p}_q = [q, \vartheta - d] \nmid \alpha = u + v\vartheta + w\vartheta^2$, and so $u + vd + wd^2 \not\equiv 0 \pmod q$,

in addition to the obvious condition

7.3.2 $\mathfrak{q}_q = [q, \vartheta^2 + d\vartheta + d^2] \nmid \alpha$, and so $u \equiv v\,d \equiv w\,d^2 \pmod{q}$ not satisfied.

If q is big, such conditions do not give much information, and it becomes rather complicated to combine the conditions for several primes. But 7.3.1—2 are of course very useful if $q = 2$.

We can also obtain information mod 3 or 9. If $m \equiv \pm 1 \pmod 9$, the methods of Ch. V will often restrict the choice of α to one of the classes 4, 5 or 6, in which case we can use the class-conditions of Ch. III, § 3. If $3 \mid m$, the obvious condition $3 \nmid z$ implies $3 \nmid u$. And if $m \equiv \pm 2$ or ± 4, $n \not\equiv \pm 3 \pmod 9$, i.e. 5.4.6—7 not satisfied, the condition that the coefficient 5.4.5 of ϑ^2 must be $\equiv 0 \pmod 9$ gives us one and only one of the classes 5.4.1—3 to which the residue of α mod 3 can belong.

The most important congruence condition for the resulting equation, and the one that has led me to all the big solutions in Tables 2^{a-b}, is, however, obtained from the relations 6.3.6 or 6.5.5. — Let first $r \equiv 1 \pmod 3$ be a prime such that $r \nmid m$, $r \mid n$. The conditions 6.5.5 must then be satisfied. Dividing the two expressions, we get Th. VI as before, but also the relation

$$\left\{\frac{\alpha(d')}{\alpha(d'')}\right\}^3 \equiv \frac{f - g\,d'}{f - g\,d''} \pmod r.$$

If we determine three rational integers t_i such that

$$t_i^3 \equiv \frac{f - g\,d'}{f - g\,d''} \pmod r, \quad i = 1, 2, 3$$

(which is possible by 6.5.6), and substitute $\alpha = u + v\vartheta + w\vartheta^2$, we get *three linear homogenous congruence conditions for the unknowns* u, v *and* w*:*

7.3.3 $$u + v\,d' + w\,d'^2 \equiv t_i\,(u + v\,d'' + w\,d''^2) \pmod r, \quad i = 1, 2, 3.$$

One of these conditions must be satisfied for any solution of the resulting equation.

Let similarly $q \equiv -1 \pmod 3$ be a prime such that $q \nmid m$, $q \mid n$; the condition 6.3.6 must then be satisfied. The only cubes of $K(\vartheta)$ which are congruent mod $\mathfrak{q}_q$ to a *rational* integer are congruent mod q to one of the forms x^3, $(y\vartheta)^3$ or $(z\vartheta^2)^3$, x, y and z rational. If therefore $\alpha = \alpha_1$ is determined such that

7.3.4 $$\alpha_1^3 = (u_1 + v_1\vartheta + w_1\vartheta^2)^3 \equiv \{u_1 - w_1 d^2 + (v_1 - w_1 d)\vartheta\}^3 \equiv t\,(f - g\vartheta) \pmod{\mathfrak{q}_q}$$

(t rational), the possible forms of α mod $\mathfrak{q}_q$ can differ from α_1 only by a factor of the type x, $y\vartheta$ or $z\vartheta^2$. We thus get *three linear homogenous congruence conditions*, one of the form

$$\frac{u - w d^2}{u_1 - w_1 d^2} \equiv \frac{v - w d}{v_1 - w_1 d} \pmod{q},$$

and two similar conditions when $\alpha_1 = u_1 + v_1\vartheta + w_1\vartheta^2$ is multiplied by ϑ or ϑ^2. (In the numerical applications, I have found it convenient to determine the α_1 of 7.3.4 in the field $K(\varrho)$ instead of $K(\vartheta)$, using the correspondence 6.2.1.)

§ 4. I have also systematized the treatment of the more general equation 7.1.2:

7.4.1 $$ax^3 + by^3 + cz^3 = 0, \quad 1 \leqq a < b < c, \quad (a, b) = (a, c) = (b, c) = 1,$$

with *cubefree* coefficients, and the result is given in *Table* 2^b. This contains all equations 7.4.1 with $\underline{abc = A \leqq 500}$, which cannot be excluded by the elementary congruence conditions 2.1.10, or by the methods of Ch. III, V and VI. This means that several soluble equations from Table 2^a will be repeated. Note that the equations $x^3 + y^3 + Az^3 = 0$ are *not included* in the list, because of the condition $a < b < c$.

To exclude an equation 7.4.1 with $a > 1$, it must be transformed into the type $x_1^3 - my_1^3 = nz_1^3$, $m < n$, by multiplication by a^2, b^2 or c^2. In the cases where this is not covered by Table 2^a, i.e. when $n > 50$, I have completed the exclusion *only in the one field* $K(\sqrt[3]{m})$ (but even then I sometimes had to work in a field with $m > 50$).

Blank spaces in Table 2^b in the column for x, y and z mean that I have not been able to find a solution. These unsolved equations all have $\underline{a = 1}$ in the form 7.4.1; the corresponding combinations (b, c) are:

7.4.2 $$(2, 173), (2, 191), (5, 89), (11, 43).$$

Of these only the last one is common with 7.1.4. All the other equations have a small $b = m$ (with $h_m = 1$), and $c = n > 50$ is a prime $q \equiv -1 \pmod 3$. I have checked in all cases that the methods of Ch. V and VI do *not* lead to exclusion in $K(\sqrt[3]{m})$; mod $q = n$ this was done by the criterion 6.3.8. I have also checked the conditions in all the fields $K(\sqrt[3]{n})$ when $n > 50$. I believe that the equations

7.4.2 are all soluble, in particular because of the *first conjecture* later in this paragraph.

Before I give the results about the *excluded* equations 7.4.1, we must study the number of such equations for given $abc = A$ which are possible for all moduli — I shall say simply *possible*. We call this number N_A (the equation $x^3 + y^3 + Az^3 = 0$ is possible for all moduli, but is *not counted* in N_A); it is clear that N_A will depend on *the number* n_A *of different prime factors in* A. In all cases I have treated, we have $n_A \leqq 4$.

The number A is supposed cubefree. To avoid a distinction between the primes and their squares, I shall use the following notation:

$$7.4.3 \qquad \begin{cases} P = p \text{ or } p^2, \ p \text{ any prime} \\ Q = q \text{ or } q^2, \ q \equiv -1 \pmod 3 \text{ a prime} \\ R = r \text{ or } r^2, \ r \equiv 1 \pmod 3 \text{ a prime.} \end{cases}$$

Different primes of the same type will be denoted by indices. I shall further use the abbreviated notation

$$7.4.4 \qquad \{a, b, c\}$$

for an equation $ax^3 + by^3 + cz^3 = 0$.

The cases $n_A = 1, 2, 3$ and 4 must be treated separately:

$n_A = 1$, $A = P$: Obviously $N_A = 0$.

$n_A = 2$, $A = P_1 P_2$: There is one *a priori* combination

$$7.4.5 \qquad \{1, P_1, P_2\},$$

which may or may not be possible (for all moduli), and so $N_A = 0$ *or* 1.

$n_A = 3$, $A = P_1 P_2 P_3$: There are four *a priori* combinations

$$7.4.6 \qquad \{1, P_1, P_2 P_3\}, \ \{1, P_2, P_1 P_3\}, \ \{1, P_3, P_1 P_2\}, \ \{P_1, P_2, P_3\}.$$

We have seen in Ch. II, § 1, that there are no congruence conditions mod any q, and none mod 9 if $3 \| A$. If therefore $P_1 = 3$, the combinations 7.4.6 are all possible mod 9, and similarly if $P_1 = 9$, $P_2 \equiv \pm P_3 \equiv \pm 1 \pmod 9$. If however $P_1 = 9$, but the last condition not satisfied, it is easily verified that one and only one of the combinations 7.4.6 is possible mod 9. (Cf. 2.1.3 and 9.10.2—5.) — If finally $3 \nmid A$, all four combinations are possible mod 9 if either (arbitrary signs) $P_1 \equiv \pm P_2 \equiv \pm P_3 \equiv \pm 1 \pmod 9$, or (for instance) $P_1 \equiv \pm P_2 \not\equiv$

$\not\equiv \pm P_3 \pmod 9$; in all other cases only one combination is possible mod 9. (Cf. 2.1.2 and 9.10.6—8.)

If only one combination is possible mod 9, this may or may not be possible mod some r such that $r \mid A$. If however all combinations are possible mod 9, and for instance $P_3 = R$, the solubility mod r (cf. 2.1.8) will depend on the cubic character of

$$P_1,\ P_2,\ P_1 P_2 \text{ and } P_1^2 P_2,$$

of which always only one or all four are cubic residues mod r. It is therefore clear that $N_A = 0,\ 1$ or 4 if $n_A = 3$.

$n_A = 4,\ A = P_1 P_2 P_3 P_4$: There are 13 *a priori* combinations, 12 of which can be obtained from the combinations 7.4.6 by inserting the factor P_4 in all possible places, and the additional combination $\{1, P_4, P_1 P_2 P_3\}$. — This principle can be used for general induction, leading to the number of *a priori* combinations for arbitrary n_A:

7.4.7 $$\frac{1}{2}(3^{n_A - 1} - 1).$$

In particular, all 13 combinations for $n_A = 4$ are possible (for all moduli) if

7.4.8 $$A = 3\, Q_1 Q_2 Q_3.$$

A tedious investigation of all other cases that can arise shows that we still get $N_A = 0, 1, 4$ or 13. — It would be an interesting combinatorial problem to examine whether the result can be generalized to

7.4.9 $$N_A = \frac{1}{2}(3^{n-1} - 1), \quad 1 \leqq n \leqq n_A,$$

cf. 7.4.7. We have seen that *this holds for* $n_A \leqq 4$; I have not examined further cases.[1]

It follows from my Theorem XIV (Ch. IX, § 16) that the number of *soluble* equations 7.4.1 is always of the form 7.4.9. Without exception, however, my numerical calculations have led me to the following stronger

Conjectures.

1. *When* $N_A = 1$, *the one possible equation* 7.4.1 *is always soluble.* — A *weaker* form, and one very probably easier to prove, would be to say "*can not be excluded*

[1] (Added later). The formula 7.4.9 can be *proved by group-considerations,* using the ideas of Ch. IX, § 16.

by the methods of the present paper". (All equations 7.4.2, and all but the last one of 7.1.4, are of this type. The weaker form of the conjecture holds for all equations I have examined.)

2. *When* $N_A = 4$, *all four possible equations* 7.4.1 *are simultaneously soluble or insoluble.* — This holds for all $abc = A \leqq 500$. The values of A with four possible but insoluble equations 7.4.1 are given in *Table* 4^b. (22 such values below 500. — The last equation of 7.1.4 has $N_A = 4$.)

3. *When* $N_A = 13$, *one and only one of the* 13 *possible equations is soluble.* — This holds for $A \leqq 1000$; the corresponding values of A, together with the one soluble equation, are given in *Table* 2^c. (5 such values below 1000, all of the type 7.4.8. The one soluble equation for $A = 330$ is also included in Table 2^b.)

The values A of Table 4^b all have $n_A = 3$, i.e. $N_A = 4$ is *maximal.* None of the A's are divisible by 9 or any prime $r \equiv 1 \pmod 3$. The smallest value of A with $r \mid A$, $N_A = 4$, and giving rise to excluded equations, is

7.4.10 $$A = 570 = 2 \cdot 3 \cdot 5 \cdot 19,$$

with the four possible but insoluble combinations

$$\{1, 19, 30\},\ \{2, 3, 95\},\ \{2, 5, 57\},\ \{3, 5, 38\}.$$

The first value of A where correspondingly $9 \mid A$, is

7.4.11 $$A = 990 = 2 \cdot 5 \cdot 9 \cdot 11,$$

with the four excluded equations

$$\{1, 10, 99\},\ \{1, 18, 55\},\ \{2, 11, 45\},\ \{5, 9, 22\}.$$

All excluded equations (crosses) in Table 2^a correspond to $N_A = 4$ or 13. In the cases with $A > 500$ and $N_A = 4$, I have verified that at least one of the other possible equations can also be excluded by my methods.

The equations with $N_A = 13$ (3rd conjecture and Table 2^c) demonstrate the important fact that *the converse of Theorem I (Ch. I, § 2) is false*, even if we suppose the equation $ax^3 + by^3 + cz^3 = 0$ possible for all moduli.

§ 5. When an equation $x^3 - my^3 = nz^3$ cannot be excluded by some means, I know of *no finite method* to decide whether or not the equation is soluble. We have seen that the elementary congruence conditions 2.1.10 are *not* sufficient

for solubility. My new conditions are of course stronger, but they also represent congruence conditions for a homogeneous cubic equation (the "resulting equation" of Ch. IV), and there is no *a priori* reason why they should be sufficient. We shall now even *prove their insufficiency in most cases when* $n = 1$, i.e. for the equation

7.5.1 $$x^3 - my^3 = z^3.$$

It was mentioned in connection with the elementary congruence conditions 2.1.10 that these can never exclude an equation 7.5.1. On the other hand, we can obtain rather strong conditions for solubility in the field $K(\varrho)$; this is shown in detail in Ch. IX. From Table 4^g we find the following cubefree values $2 < m \leqq 50$ for which 7.5.1 is insoluble:

7.5.2 $m = 3, 4, 5, 10, 11, 14, 18, 21, 23, 25, 29, 36, 38, 39, 41, 44, 45, 46, 47.$

The trivial solution $x = z$, $y = 0$ is not considered. All the corresponding equations were already proved insoluble by Sylvester [1] and Pépin [1]—[3].

We shall treat 7.5.1 in the ordinary way in $K(\sqrt[3]{m}) = K(\vartheta)$. — It is at once clear that class-number considerations will never lead to exclusion when $n = 1$; there are further *no primes* q *or* r dividing n, thus giving rise to the conditions of Ch. VI. The only possibility is to work mod a power of 3.

As already mentioned in Ch. V, § 1, this method was first used by Holzer [1]. But his treatment is incomplete, since he only considers the cases $m \equiv \pm 2, \pm 3$ or $\pm 4 \pmod 9$, m squarefree or a complete square, and the class-number $h_m \not\equiv 0 \pmod 3$.

When $m \not\equiv \pm 1 \pmod 9$, and $3 \nmid h_m$, the ordinary equation $x - y\vartheta = \mu\alpha^3$ now takes the form

7.5.3 $$x - y\vartheta = \varepsilon_m^i \alpha^3 = \varepsilon_m^i (u + v\vartheta_1 + w\vartheta_2)^3, \quad i = 0, 1, 2.$$

The case $i = 0$ is here *completely different* from the two other possibilities $i = 1$ or 2, and leads to the simple resulting equation 4.1.6:

7.5.4 $$u^2 w + m_2 uv^2 + m_1 m_2 vw^2 = 0.$$

This can never be excluded by congruence considerations, but by *infinite descent.* It had been noted by Krafft (cf. Dickson [1], Ch. XXI, ref. 145) that a solution of 7.5.4 (at least with m squarefree, i.e. $m_2 = 1$) will lead to a *smaller* solution (x_1, y_1, z_1) of 7.5.1 than the one which originally gave rise to 7.5.4. The

general case $m = m_1 m_2^2$ is treated by FADDEEV [1], who shows that a solution (x, y, z) which gives rise to an equation 7.5.3 with $i = 0$, will be the "*triplication*" of another solution (x_1, y_1, z_1) (cf. Ch. IX, § 15). In particular:

$$y = 3 x_1 y_1 z_1 (x_1^6 - x_1^3 z_1^3 + z_1^6), \text{ and so } 0 < |y_1| < |y|.$$

We can suppose that we start off with the solution of 7.5.1 for which $|y| > 0$ is minimal; the possibility $i = 0$ is then excluded. (Holzer's principle of descent is for the exponent δ of $3^\delta \| y$.)

We therefore have to examine the equation 7.5.3 with $i = 1$ or 2. It is clear that this cannot give the trivial solution $x = z = 1$, $y = 0$, since then $z = N(\alpha) = 1$ shows that α is a unit, $\alpha = \varepsilon_m^t$, and we get the impossible equation $\varepsilon_m^{3t+i} = 1$.

If $m \equiv 0 \pmod 9$, we have seen in Ch. V, § 3, 2. that this case can *never be excluded* mod 3. — If $m \equiv \pm 2$, ± 3 or $\pm 4 \pmod 9$, the only possibility for excluding 7.5.3 is that neither ε_m nor ε_m^2 have a coefficient divisible by 3 for ϑ^2. (We cannot operate mod 9, since the condition 5.4.7 is not satisfied.) Table 1[b] (the residues for η) shows that this condition is satisfied when

7.5.5 $$m \equiv \pm 3 \text{ or } \pm 4 \pmod 9, \quad \varepsilon_m \not\equiv 1 \pmod 3,$$

but *never when* $m \equiv \pm 2 \pmod 9$, since then at least one of ε_m and ε_m^2 has a coefficient $\equiv 0 \pmod 3$ for ϑ^2. (What Holzer calls "condition B'''" is consequently never satisfied when $m \equiv \pm 2 \pmod 9$.)

If $m \equiv \pm 1 \pmod 9$, there are the two possibilities $3 | z$ and $3 \nmid z$. In the latter case, we can replace ε_m in 7.5.3 by the η_m of 5.7.10; α must then be chosen from class 5 (no denominator 3). Complete exclusion is again *impossible*, since Table 1[b] shows that at least one of η_m or η_m^2 has a coefficient $\equiv 0 \pmod 3$ for ϑ^2. — The case $3 | z$, i.e. 5.7.6, implies an additional factor $\tau \sigma^2$ on the right hand side of 7.5.3, and can often be proved impossible by the methods of Ch. V, §§ 7—10. This might be helpful in a search for numerical solutions.

A class-number $h_m \equiv 0 \pmod 3$ was not treated by Holzer, but we shall see that the equation 7.5.1 can *never be excluded* by his methods in this case. We must introduce at least one γ in 7.5.3:

7.5.6 $$x - y\vartheta = \varepsilon_m^i \gamma^j (u + v\vartheta_1 + w\vartheta_2)^3, \quad i \text{ and } j = 0, 1, 2,$$

cf. 3.8.3. This will represent *all* possibilities when $h_m = 3$; there may also be

other values of γ if $h_m = 3k > 3$, but the factor γ^j $(j = 0, 1, 2)$ can in any case be made to represent three of the possible γ_j of 3.8.2.

It is clear from the case $j = 0$ that we can only hope to get complete exclusion in the cases 7.5.5. The norm $N(\gamma)$ is a rational cube, and so $\equiv \pm 1 \pmod 9$, and the possibilities for γ mod 3 are the same as for ε_m:

$$\gamma \equiv \pm 1, \ \pm \varepsilon_m \ \text{ or } \ \pm \varepsilon_m^2 \pmod 3.$$

We can therefore suppose $\gamma \equiv \pm 1 \pmod 3$, if necessary after multiplication by a properly chosen power of ε_m (which is $\not\equiv 1 \pmod 3$ by 7.5.5). The only possibility mod 3 in 7.5.6 is then $i = 0$:

$$x - y\vartheta = \gamma^j \alpha^3 = \gamma^j (u + v\vartheta_1 + w\vartheta_2)^3, \quad j = 0, 1, 2,$$

but here *only* $j = 0$ *can be excluded* (by infinite descent). This holds even when we can find a *rational* γ. The resulting cubic equation then gets the same simple form 7.5.4 for all values of j, but *the conditions for infinite descent are no longer satisfied for* $j > 0$, since then α can be *fractional.* (If this was not so, we could for instance exclude the case

$$m = 22 \equiv 4 \pmod 9, \quad h_{22} = 3, \quad \varepsilon_{22} = 23 + 3\vartheta - 4\vartheta^2 \not\equiv 1 \pmod 3, \quad \gamma = 2.$$

But the equation $x^3 - 22y^3 = z^3$ is soluble, cf. Table 6.)

The improvement of Holzer's method is therefore mainly *negative.* Apart from extending the principle of descent to non-squarefree m, I have shown systematically that *the method of exclusion only applies when the class-number* $h_m \not\equiv 0 \pmod 3$, *and the conditions* 7.5.5 *are satisfied* (i.e. under the conditions which were considered by Holzer).

But the results of Ch. VI, § 10 lead to still another limitation of the excluded values. If $h_m \not\equiv 0 \pmod 3$ and m has at least two different prime factors, then the unit ε_m will be of *Type 2*, i.e. in particular $\varepsilon_m \equiv 1 \pmod 3$. m *must consequently be a prime or the square of a prime.* Since $m = r$ or r^2 implies $3 \mid h_m$, the only excluded values of m are therefore given by

$$7.5.7 \qquad \begin{cases} m = 3; \ m = q \equiv 5 \pmod 9 \ \text{ or } \ m = q^2, \ q \equiv 2 \pmod 9 \\ \qquad \text{where } h_q \not\equiv 0 \pmod 3 \ \text{ and } \ \varepsilon_q \not\equiv 1 \pmod 3, \end{cases}$$

which are all *particular cases of Theorem VIII.* — For the values 7.5.2, this means that we can exclude only

7.5.8 $$m = 3, 4, 5, 23, 41$$

(which all have $h_m = 1$).

The negative results of this paragraph show that we can find *an infinity of resulting cubic equations which are possible for all moduli but insoluble in integers.* These equations will usually contain *all possible terms* (10 in all) in u, v and w, and they cannot be deduced trivially (e.g. by linear substitutions) from insoluble equations $x^3 - my^3 = nz^3$ or the more general type $Ax^3 + Bx^2y + Cxy^2 + Dy^3 = Ez^3$ (to which my above methods of exclusion also apply, cf. Ch. VIII and Ch. IX, §§ 12—14).

§ 6. The equation $x^3 - my^3 = z^3$ has also been treated by FADDEEV [1], both in the field $K(\sqrt[3]{m}) = K(\vartheta)$ and in the field $K(\varrho)$. I return to his methods in Ch. IX, § 15, and shall here only indicate his results in the field $K(\vartheta)$. Instead of my equation 3.8.2 for $n = 1$:

7.6.1 $$x - y\vartheta = \varepsilon_m^i \gamma_j \alpha^3 = \mu\alpha^3; \quad i = 0, 1, 2; \; j = 0, 1, 2, \ldots k-1; \quad \gamma_0 = 1$$

(also combined with the additional factor $\tau\sigma^2$ of 5.7.6 when $m \equiv \pm 1 \pmod 9$), Faddeev considers the equation

7.6.2 $$9(x-z)^2(x-y\vartheta) = \varepsilon_m^i \gamma_j \beta^3 = \lambda\beta^3, \; 3\lambda\beta^3 \text{ or } 9\lambda\beta^3$$

(the two last possibilities only when $m \equiv \pm 1 \pmod 9$). The left hand side is the cube of an integer of $K(\vartheta)$ if and only if (x, y, z) is the *triplication* of another solution (cf. Ch. IX, § 15). The number k of 7.6.1, and consequently also the number of *a priori* possible equations, is always a power of 3. The same holds for 7.6.2, but in this form Faddeev can prove (by group-considerations) that the number G of *soluble* equations is also of the same type:

7.6.3 $$G = 3^g.$$

Here g is the number of generators (basic solutions) of the corresponding equation $x^3 - my^3 = z^3$ (in the *Mordell-Weil* sense). — In order to prove the insolubility of such an equation, it will therefore suffice to prove that $G < 3$. I will show that this principle can also be applied to 7.6.1 in some cases where there is *a one-one-correspondence between the equations* 7.6.1 *and* 7.6.2.

Such a correspondence will obviously depend on the factor $(x-z)^2$. — If we substitute $x = X$, $y = Z$, $z = -Y$, $m = A$, the equation $x^3 - my^3 = z^3$ is

transformed into

7.6.4 $$X^3 + Y^3 = AZ^3,$$

which is considered in Ch. IX (this is also the notation used by Faddeev). It follows from 9.3.3 and 9.6.1 that we can put

7.6.5 $$x - z = X + Y = sA_1 w^3, \quad A_1 \mid A,$$

where s is given by 9.3.4. In particular, A_1 *contains all prime factors* $q \equiv -1 \pmod 3$ *of* A.

The detailed study in Ch. IX further restricts the choice of s and A_1, but we shall here only use the simplest results (obtained by treating 7.6.4 as a congruence mod 9):

7.6.6
$$\begin{cases} \text{If } A = m \text{ contains no prime factor } r \equiv +1 \pmod 3, \text{ then} \\ m \equiv \pm 3 \text{ or } \pm 4 \pmod 9 \to s = 9, \ A_1 = A = m, \ y = Z \equiv 0 \pmod 3 \\ \qquad\qquad \text{("case I" of 9.3.4);} \\ m \equiv \pm 2 \pmod 9 \to \text{either case I, or } s = 1, \ A_1 = A = m, \\ \qquad X \equiv Y \equiv \pm Z \not\equiv 0 \pmod 3 \text{ ("case II").} \end{cases}$$

If $m \equiv \pm 3$ or ± 4, then 7.6.5 takes the form

$$x - z = 9mw^3 = 9\vartheta^3 w^3,$$

showing that there is a one-one-correspondence between 7.6.1—2, expressed by

7.6.7 $$\underline{\lambda = \mu}, \quad \beta = 9\vartheta^2 w^2 \alpha.$$

In this case we can therefore conclude the insolubility of $x^3 - my^3 = z^3$ if the number of non-excluded equations[1] 7.6.1 is less than 3. It is however easily seen that this principle will cover all the values m of 7.5.7, but no others, and no new information is obtained in this way.

The other case of 7.6.6, $m \equiv \pm 2 \pmod 9$, will not only lead as above to the correspondence 7.6.7, but also to $x - z = mw^3 = \vartheta^3 w^3$, which leaves an extra factor 9 when comparing 7.6.1—2. Now $[9] = \mathfrak{p}_3^6$, which will introduce a unit $\eta \not\equiv 1$ if $\mathfrak{p}_3$ is a principal ideal $[\nu_3]$, i.e. $9 = \eta \nu_3^6$:

7.6.8 $$\underline{\lambda = \eta \mu}, \quad \beta = \nu_3^2 \vartheta^2 w^2 \alpha.$$

A γ is introduced if $\mathfrak{p}_3$ is non-principal.

[1] The case $\mu = 1$ is now counted as *not excluded*.

The result for $m \equiv \pm 2 \pmod 9$ demonstrates that one soluble equation 7.6.1 may lead to *several* soluble equations 7.6.2. In the case just treated, an additional consideration can however show a one-one-correspondence all the same under certain circumstances:

Let as before $m \equiv \pm 2 \pmod 9$, and further $h_m \not\equiv 0 \pmod 3$, $\varepsilon_m \not\equiv 1 \pmod 3$ and so $m = q$ or q^2 by the same argument that led to 7.5.7. The μ of 7.6.1 is then $\mu = \varepsilon_m^i$, $i = 0, 1, 2$. From Table 1[b] (the entry for $m \equiv 2$, $n \equiv 1 \pmod 9$) it follows that one and only one value of $\mu \neq 1$ is possible mod 3, and for this value:

$$x - y\vartheta = \mu\alpha^3 \equiv \pm\mu \equiv \pm(-1 + \vartheta), \quad \text{i.e. } \underline{y \not\equiv 0 \pmod 3}.$$

This excludes the first possibility 7.6.6 (the correspondence 7.6.7), and leaves the one-one-correspondence 7.6.8 between the equations 7.6.1—2. Since the number of non-excluded equations 7.6.1 is less than 3, we conclude that the given equation is insoluble under the above conditions.

Combining this result with 7.5.7, we see that *the equation* $X^3 + Y^3 = mZ^3$ *has only the trivial solution with* $Z = 0$ *when*

$$7.6.9 \qquad \begin{cases} m = 3; \ m = q \text{ or } q^2, \ q \not\equiv -1 \pmod 9, \text{ where } h_q \not\equiv 0 \pmod 3 \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{and } \varepsilon_q \not\equiv 1 \pmod 3). \end{cases}$$

Like 7.5.7, this result is still *a particular case of Theorem VIII.* — For the values 7.5.2, this means that we can now exclude

$$7.6.10 \qquad m = 3, 4, 5, 11, 23, 25, 29, 41, 47$$

(the values 7.5.8 are repeated).

The remaining m of 7.5.2 all give rise to at least 3 non-excluded equations 7.6.1, and can consequently not be proved insoluble by similar auxiliary considerations.

For completeness, I shall finally quote Faddeev's formulae for the exponent g of 7.6.3. The number k of γ's in 7.6.1—2 is a power of 3:

$$k = 3^s,$$

representing the number of different ideal-classes Γ of $K(\vartheta)$ such that Γ^3 is the principal class. It follows that the number of *a priori* possible equations 7.6.2 equals 3^{s+1} when $m \not\equiv \pm 1$ and 3^{s+2} when $m \equiv \pm 1 \pmod 9$. Faddeev does however state that not all these equations can be soluble when $m \not\equiv 0 \pmod 3$, and so for cubefree m:

7.6.11
$$\begin{cases} g \leqq s+1 & \text{when } m \equiv 0, \pm 1 \text{ or } \pm 3 \pmod 9 \\ g \leqq s & \text{when } m \equiv \pm 2 \text{ or } \pm 4 \pmod 9. \end{cases}$$

For $m \leqq 50$, this implies insolubility ($g = 0$) only in the cases 7.6.10, $m = 3$ excluded. We further get too great a maximum number of generators ($g \leqq 2$ instead of $g = 1$) for

$$m = 26, 28, 35, 42.$$

CHAPTER VIII. The Equation $u^3 - 3u^2v + v^3 = aw^3$.

§ 1. When applying infinite descent to the equation $X^3 + Y^3 = AZ^3$ of the next chapter, one of the possible equations to which we are led is

8.1.1
$$u^3 - 3u^2v + v^3 = 3pw^3,$$

if $A = p$ is a prime $\equiv \pm 1 \pmod 9$, or a product of such primes (Theorem X, § 5). If $A = 9p$ (with the same meaning of p), the right hand side is replaced by pw^3, cf. § 4 below. The equation 8.1.1 was already studied by SYLVESTER [1]; the corresponding inhomogenous equation (with $w = 1$) has been treated by LJUNGGREN [1].

As an application of my methods to an equation which is *not purely cubic*, I will treat 8.1.1 a little more in detail. I prefer to deal with the equivalent form

8.1.2
$$x^3 - 3xy^2 + y^3 = 3pz^3.$$

The corresponding congruence is soluble for all moduli. — We have the case 2.3.1, with the discriminant $\Delta = 3^4$, and therefore (by 2.3.3) only have to examine the solubility of the congruence mod 3^δ and mod p. It is known (cf. PÉPIN [4]) that the congruence

8.1.3
$$x^3 - 3x + 1 \equiv 0 \pmod p$$

is soluble when p is a prime $\equiv \pm 1 \pmod 9$. Substitution of $x = -y + 3x_1$ in 8.1.2 and division by 3 gives the new equation

$$9x_1^3 - 9x_1^2y + y^3 = pz^3,$$

which is possible mod 3^δ for all δ, since the corresponding congruence mod 9 is soluble with y and $z \not\equiv 0 \pmod 3$.

We shall treat 8.1.2 in the well-known field $K(\theta)$ defined by

8.1.4 $$\theta^3 - 3\theta + 1 = 0.$$

This is a *Galois field* (the discriminant $\Delta = 3^4$ is a perfect square), and the connection between the three (real) roots θ, θ' and θ'' is given by (cf. 8.1.11):

8.1.5 $$\theta' = -\frac{1}{\theta - 1} = -\theta^2 - \theta + 2, \quad \theta'' = \frac{\theta - 1}{\theta} = \theta^2 - 2.$$

The class-number $h = 1$, and a basis for the integers of $K(\theta)$ is given by $(1, \theta, \theta^2)$. Since $\Delta > 0$, there are *two fundamental units*; we may choose these as θ and θ', or as

8.1.6 $$\varepsilon_1 = \theta, \quad \varepsilon_2 = \theta - 1$$

(the first of these has a norm -1, but this does not influence our arguments).

The natural primes $\equiv \pm 2$ or $\pm 4 \pmod 9$ remain primes in $K(\theta)$. The factorization of 3 is

8.1.7 $$3 = (-1-\theta)^3 \cdot \underbrace{(-1-\theta+\theta^2)}_{\text{unit}}, \quad \text{i.e. } \mathfrak{p}_3 = [1+\theta].$$

The primes $p \equiv \pm 1 \pmod 9$ factorize into *three different, conjugate ideals:*

8.1.8 $$[p] = [p, \theta - d][p, \theta - d'][p, \theta - d''] = \mathfrak{p}_p \mathfrak{p}'_p \mathfrak{p}''_p,$$

where d, d' and d'' are the three solutions of the congruence 8.1.3. In particular:

8.1.9 $$d + d' + d'' \equiv 0, \quad dd' + dd'' + d'd'' \equiv -3, \quad dd'd'' \equiv -1 \pmod p;$$

8.1.10 $$d' \equiv \frac{d-1}{d} \equiv d^2 - 2, \quad d'' \equiv -\frac{1}{d-1} \equiv -d^2 - d + 2 \pmod p.$$

The last formulae are analogous to 8.1.5. The values of d' and d'' are apparently given in the wrong order, but the conjugates of an ideal $\mathfrak{p}_p = [p, \theta - d]$ are really determined by

$$\mathfrak{p}'_p = [p, \theta' - d] = \left[p, -\frac{1}{\theta - 1} - d\right] = [p, d\theta - d + 1] = \left[p, \theta - \frac{d-1}{d}\right] = [p, \theta - d'],$$

$$\mathfrak{p}''_p = [p, \theta'' - d] = \left[p, \frac{\theta - 1}{\theta} - d\right] = [p, (d-1)\theta + 1] = \left[p, \theta + \frac{1}{d-1}\right] = [p, \theta - d''].$$

The relations 8.1.5 follow at once from the *automorphisms* of the binary cubic form $x^3 - 3xy^2 + y^3$:

8.1.11 $$x' = -y,\ y' = x - y;\ x'' = -x + y,\ y'' = -x.$$

The *norm* of an integer in $K(\theta)$ is expressed by

8.1.12 $$\begin{cases} N(\alpha) = N(u + v\theta + w\theta^2) = u^3 - v^3 + w^3 + 6u^2w - 3uv^2 \\ \qquad\qquad + 9uw^2 + 3vw^2 + 3uvw, \end{cases}$$

and the cube of an integer:

8.1.13 $$\begin{cases} \alpha^3 = (u + v\theta + w\theta^2)^3 = U + V\theta + W\theta^2 = \\ \quad = u^3 - v^3 + w^3 - 9vw^2 - 6uvw \\ \quad + 3(v^3 - 2w^3 + u^2v - uw^2 - v^2w + 9vw^2 + 6uvw)\theta \\ \quad + 3(3w^3 + u^2w + uv^2 + 3uw^2 + 3v^2w - vw^2)\theta^2. \end{cases}$$

§ 2. To simplify the calculations, I will suppose that the factor p of 8.1.2 is a *prime* $\equiv \pm 1 \pmod 9$, or the *square* of such a prime. (Any cubed factor can be absorbed in ε^3). The equation 8.1.2 will then in the ordinary way lead to three different ideal-equations in $K(\theta)$:

8.2.1 $$[x - y\theta] = \mathfrak{p}_3 \mathfrak{p}_p \mathfrak{a}^3 = \mathfrak{n}\mathfrak{a}^3,$$

where $\mathfrak{p}_p$ is one of the three factors of 8.1.8 (squared if p is a square. The product of two *different* ideals $\mathfrak{p}_p$, $\mathfrak{p}'_p$ and $\mathfrak{p}''_p$ cannot divide $x - y\theta$.)

The automorphisms 8.1.11 show that the three equations 8.2.1 are *simultaneously soluble or insoluble*; in order to prove an equation 8.1.2 impossible, it will therefore suffice to *exclude only one* of the equations 8.2.1. (If p contains several different prime factors, and one of them is p_1, it will similarly suffice to exclude all those combinations for $\mathfrak{n}$ in 8.2.1 which contain only the one factor $\mathfrak{p}_{p_1}$ of $[p_1]$.)

The equation in integers of $K(\theta)$ corresponding to 8.2.1 is in analogy with 3.6.2:

8.2.2 $$\begin{cases} x - y\theta = \varepsilon_1^i \varepsilon_2^j \nu \alpha^3 = \varepsilon_1^i \varepsilon_2^j (e_1 + f_1\theta + g_1\theta^2)\alpha^3 = \\ \qquad = \mu\alpha^3 = (e + f\theta + g\theta^2)(u + v\theta + w\theta^2)^3, \quad i \text{ and } j = 0, 1, 2, \end{cases}$$

where $N(\mu) = N(\nu) = 3p$, and where the units are given by 8.1.6. We thus have to consider *nine* different equations, but we shall see that *it suffices for complete exclusion to prove one of them only insoluble.*

As in Ch. IV, we are led to a "resulting cubic equation" by equating the coefficient of θ^2 to zero in 8.2.2:

8.2.3 $$g\,U + f\,V + (e + 3\,g)\,W = 0,$$

cf. 8.1.13. By operating in the field $K(\theta)$, we shall (as in Ch. V and VI) obtain solubility conditions for the equation 8.2.2. It can be shown that these represent congruence conditions for the resulting cubic equation 8.2.3, but I will not go into details with this.

We first deduce the condition 5.1.6 again:

8.2.4 $$g \equiv 0 \pmod 3.$$

For $\alpha = u + v\theta + w\theta^2 \not\equiv 0 \pmod{\mathfrak{p}_3}$ (since $\mathfrak{p}_3 \mid \alpha \to 3 \mid z \to 3 \mid x \,\&\, y$), and 8.1.13 shows that then $\alpha^3 \equiv \pm 1 \pmod 3$.

If we cube a complete system of residues mod 3 and prime to 3, we find that all possible *effective* cubic residues mod 9 are represented:

$$1,\quad 1 \pm 3\theta,\quad 1 \pm 3\theta^2,\quad 1 \pm 3\theta \pm 3\theta^2$$

(cf. 5.5.1), which shows that we cannot expect to obtain stronger conditions mod 9 than mod 3. It is also easily verified directly that 8.2.4 is the *sufficient* congruence condition mod 3^δ, $\delta \geqq 1$, for the resulting equation 8.2.3.

Since $\mathfrak{p}_3 = [3,\ 1 + \theta] \mid e_1 + f_1\theta + g_1\theta^2$, i.e. $e_1 - f_1 + g_1 \equiv 0 \pmod 3$, there are only three possibilities:

$$\pm (e_1 + f_1\theta + g_1\theta^2) \equiv 1 + \theta,\quad 1 - \theta^2 \quad \text{or} \quad \theta + \theta^2 \pmod 3$$

(the fourth possibility $1 - \theta + \theta^2 \equiv 1 + 2\theta + \theta^2 = (1 + \theta)^2$ is divisible by $\mathfrak{p}_3^2$), and these can all be transformed into each other mod 3 by multiplication by suitable powers of the unit $\varepsilon_1 = \theta$. Doing this *beforehand*, we may assume that we have the first possibility, i.e. $g_1 \equiv 0 \pmod 3$ in 8.2.2. We can then only use those combinations $\eta = \varepsilon_1^i \varepsilon_2^j$ which leave this condition satisfied, and these are

$$\eta = 1,\quad = \varepsilon_1\varepsilon_2 = \theta(\theta - 1) \quad \text{or} \quad = \varepsilon_1^2\varepsilon_2^2 = \theta^2(\theta - 1)^2.$$

This limits the number of possibilities in 8.2.2 to three, given by

8.2.5 $$x - y\theta = \{\theta(\theta - 1)\}^i (e_1 + f_1\theta + g_1\theta^2)\,\alpha^3 = \eta^i \nu\, \alpha^3 = \mu\,\alpha^3,\quad i = 0,\ 1,\ 2,$$

provided $g_1 \equiv 0 \pmod 3$.

§ 3. We now come to the conditions mod p, corresponding to those of Ch. VI. From $\mathfrak{p}_p = [p, \theta - d] \mid x - y\theta$, we conclude that $x \equiv dy$, $x - y\theta \equiv y(d - \theta)$ (mod p), and we are led to a congruence

8.3.1 $$y(d - \theta) \equiv \mu\alpha^3 = \mu(\theta) \cdot \{\alpha(\theta)\}^3 \pmod{\mathfrak{p}'_p \mathfrak{p}''_p}.$$

The two separate congruences mod $\mathfrak{p}'_p$ and $\mathfrak{p}''_p$ give

$$y(d - d') \equiv \mu(d') \cdot \{\alpha(d')\}^3, \quad y(d - d'') \equiv \mu(d'') \cdot \{\alpha(d'')\}^3 \pmod{p},$$

which combined give the condition

8.3.2 $$\frac{d - d'}{d - d''} \sim \frac{\mu(d')}{\mu(d'')} \pmod{p}.$$

In particular, we must examine the influence on this condition of $\eta = o(\theta - 1) = \eta(\theta)$ in 8.2.5. Using the formulae 8.1.10, we find that

$$\frac{\eta(d')}{\eta(d'')} = \frac{d'(d' - 1)}{d''(d'' - 1)} \equiv \left(\frac{1 - d}{d}\right)^3 \pmod{p},$$

i.e. a *perfect cube.* It will therefore *suffice for exclusion mod p to consider only* $i = o$ in 8.2.5, and μ of 8.3.1—2 can be replaced by $\nu = e_1 + f_1\theta + g_1\theta^2$, $g_1 \equiv o \pmod 3$. In particular, 8.3.2 takes the form

8.3.3 $$\frac{d - d'}{d - d''} \sim \frac{\nu(d')}{\nu(d'')} \pmod{p}.$$

If this is not satisfied, the given equation is insoluble. Since all rational numbers are cubic residues when $p = q \equiv -1 \pmod 9$, *the method will only lead to effective conditions when* $p = r \equiv +1 \pmod 9$.

Replacing p by some other prime $p_1 \equiv \pm 1 \pmod 9$, 8.3.3 will represent a necessary condition for $p_1 \mid z$. If however p is the prime of the given equation, we have $\mathfrak{p}_p = [p, \theta - d] \mid \nu = e_1 + f_1\theta + g_1\theta^2$. The argument that led to 6.5.5 still holds (cf. 8.1.9), and 8.3.1 — with μ replaced by ν — leads to exactly the same condition as 6.5.6:

8.3.4 $$\frac{f_1 - g_1 d'}{f_1 - g_1 d''}(R)p, \quad g_1 \equiv o \pmod 3,$$

which will be *a necessary condition for solubility of the given equations* 8.1.1—2, *when p is a prime or the square of a prime.* — We shall see in the next paragraph that the condition $g_1 \equiv o \pmod 3$ can be *omitted* when $3 \mid (R)p$.

As an example, let us consider the smallest value of p that can be excluded, $p = 73$:

8.3.5 $$x^3 - 3xy^2 + y^3 = 3 \cdot 73 z^3.$$

The solutions of the congruence $x^3 - 3x + 1 \equiv 0 \pmod{73}$ are $d = 39$, $d' = 48$, $d'' = 59$, corresponding to the prime factors of 73:

$$\mathfrak{p}_{73} = [73, \theta - 39] = [5 - 2\theta], \quad \mathfrak{p}'_{73} = [73, \theta - 48] = [2 + 3\theta],$$
$$\mathfrak{p}''_{73} = [73, \theta - 59] = [3 - 5\theta].$$

We choose the first factor $\mathfrak{p}_{73}$, and multiply by $\mathfrak{p}_3 = [1 + \theta]$:

$$(1 + \theta)(5 - 2\theta) = 5 + 3\theta - 2\theta^2.$$

To get $g_1 \equiv 0 \pmod 3$, we must multiply by θ (the next paragraph will show that this is not really necessary, since $3 (R) 73$):

$$\theta(5 + 3\theta - 2\theta^2) = 2 - \theta + 3\theta^2 = e_1 + f_1\theta + g_1\theta^2, \quad \text{where}$$

$$\frac{f_1 - g_1 d'}{f_1 - g_1 d''} = \frac{-1 - 3 \cdot 48}{-1 - 3 \cdot 59} = \frac{145}{178} \equiv -\frac{1}{32} \sim 2 \pmod{73},$$

which is not a cubic residue; the equation 8.3.5 is consequently insoluble. (Cf. the end of § 5 below.)

The results of my calculations are given in *Table 3*, where I treat all equations 8.1.1 (in this form, with u, v and w) for which $p < 500$. Apart from primes, the list contains the squares 17^2 and 19^2 and the product $17 \cdot 19$. Crosses stand for equations which have been proved insoluble by the criterion 8.3.4. In all other cases a solution is found. It is rather striking that all non-excluded equations with $p \equiv +1 \pmod 9$ have a solution with $w = 1$. (I found these solutions, the bigger ones by the continued fraction for θ, before I excluded the remaining equations. To decide the cubic character of the fractions 8.3.4, I used the table of indices in KRAITCHIK [1]. — The solutions with $w > 1$ were found from the resulting equation 8.2.3.)

Because of the automorphisms 8.1.11, the solutions will always occur *in groups of three*, with the same value of w. Table 3 only gives the one solution in each group for which u, v and w are all positive.

§ 4. For use in the next chapter (Th. X, § 5), Table 3 also contains the equation

8.4.1 $$u^3 - 3u^2v + v^3 = pw^3$$

for $9p < 500$ (with the same meaning of p as above). Simple solutions are found in all cases. I shall sketch briefly how the earlier considerations must be modified for this equation, which I will treat in the form corresponding to 8.1.2:

8.4.2 $$x^3 - 3xy^2 + y^3 = pz^3.$$

This is *possible for all moduli.* The ideal-equation 8.2.1 now takes the form $[x - y\theta] = \mathfrak{p}_p \mathfrak{a}^3$. We suppose that p is a prime or the square of a prime; it will then suffice to exclude *one* of the three corresponding equations.

8.2.2 can be used as it stands, if $N(\mu) = N(\nu) = p$. Since $\mathfrak{p}_3 \nmid \nu$, there are now *nine* different possibilities mod 3:

$$\left.\begin{array}{lll} \pm(e_1 + f_1\theta + g_1\theta^2) \equiv 1, & \theta, & \theta^2 \\ 1-\theta, & \theta-\theta^2, & 1+\theta^2 \\ 1+\theta+\theta^2, & 1-\theta-\theta^2, & 1+\theta-\theta^2 \end{array}\right\} \pmod 3,$$

which can all be transformed into each other mod 3 by multiplication with suitable powers of the units $\varepsilon_1 = \theta$ and $\varepsilon_2 = \theta - 1$. Doing this beforehand, we may again suppose that we have the first possibility, i.e. $f_1 \equiv g_1 \equiv 0 \pmod 3$ in 8.2.2. The condition 8.2.4 is still necessary, and the only values of $\eta = \varepsilon_1^i \varepsilon_2^j$ which leave this condition satisfied are

8.4.3 $$\eta = 1, \quad \eta_1 = \theta, \quad \eta_2 = \theta - 1.$$

The condition 8.3.2 remains the same, and is only *effective* if $p = r \equiv +1 \pmod 9$. We then have to examine the influence of the factors (cf. 8.1.10):

8.4.4 $$\left\{\begin{array}{l} t_1 = \dfrac{\eta_1(d')}{\eta_1(d'')} = \dfrac{d'}{d''} \equiv -\dfrac{(d-1)^3}{d(d-1)} \sim \dfrac{1}{d(d-1)} \\ t_2 = \dfrac{\eta_2(d')}{\eta_2(d'')} = \dfrac{d'-1}{d''-1} \equiv \dfrac{d(d-1)}{d^3} \sim d(d-1) \end{array}\right. \pmod p.$$

The exclusion will therefore depend on the cubic character mod p of $d(d-1)$. The congruence

$$(d^2-1)^3 \equiv 3d(d-1) \pmod p$$

shows that 3 and $d(d-1)$ are simultaneously cubic residues or non-residues. *If therefore* $3(N)p$, *one and only one of the three units* 8.4.3 *is always possible mod* p, since then 1, t_1 and t_2 all belong to different classes mod p. If however

8.4.5 $$3(R)p, \quad \text{i.e. } d(d-1)(R)p,$$

all three units are *simultaneously possible or impossible.* From 8.1.9 we conclude that

$$d\,d'\,d'' \equiv -1\,(R)p, \quad (d-1)(d'-1)(d''-1) \equiv 1\,(R)p,$$

and 8.4.4 shows that the condition 8.4.5 is equivalent to

8.4.6 $$d \sim d' \sim d'', \quad d-1 \sim d'-1 \sim d''-1 \pmod{p}.$$

But then the condition 8.3.2 is independent of the use of any unit $\varepsilon_1^i \varepsilon_2^j = \theta^i(\theta-1)^j$. *The given equations* 8.4.1—2 *are therefore insoluble if* p *is a prime* $\equiv +1 \pmod 9$ *for which* $3(R)p$ *(or the square of such a prime), and if the condition* 8.3.4 *is not satisfied for an arbitrary* $\nu = e_1 + f_1\theta + g_1\theta^2$. — The only equations 8.4.1—2 with $p < 500$ which can be excluded correspond to

$$p = 271,$$

cf. the end of the next paragraph.

It is clear that when $3(R)p$, the criterion 8.3.4 is independent of the use of units also for the equation 8.1.2, and the additional condition $g_1 \equiv 0 \pmod 3$ can then be omitted.

§ 5. There is an interesting connection between the two equations

8.5.1 $$x^3 - 3xy^2 + y^3 = pz^3$$

8.5.2 $$x^3 - 3xy^2 + y^3 = 3pz^3,$$

expressed by the following

Theorem VII. *If* $p \equiv +1 \pmod 9$ *is a prime which has* 3 *as a cubic residue (or the square of such a prime), then at most one of the equations* 8.5.1—2 *is soluble if* d *is a cubic non-residue of* p.

We note that the choice of d among the roots of the congruence 8.1.3 is irrelevant, because of 8.4.6. — Let $\mathfrak{p}_p = [\nu(\theta)]$, so that the equations 8.2.2 corresponding to 8.5.1—2 take the form

$$x - y\theta = \eta \cdot \nu(\theta) \cdot \alpha^3 \quad \text{and} \quad x - y\theta = \eta \cdot (1+\theta) \cdot \nu(\theta) \cdot \alpha^3$$

respectively. We use the criterion 8.3.2, which is now independent of the unit η (since $3 \mid (R)p$), and we have to compare $\frac{d - d'}{d - d''}$ with

$$\frac{\nu(d')}{\nu(d'')} \quad \text{and} \quad \frac{1 + d'}{1 + d''} \cdot \frac{\nu(d')}{\nu(d'')}.$$

But these expressions *belong to different classes mod p*, since

$$\frac{1 + d'}{1 + d''} \equiv \frac{3\,d'}{(1 + d'')^3} \sim 3\,d' \sim 3\,d \pmod{p},$$

which is a cubic non-residue by the conditions of the theorem. This concludes the proof.

The primes $p \equiv +1 \pmod 9$ and < 500 for which $3 \mid (R)p$, with the corresponding values of d, are

$$p = 73,\ d = 39;\ p = 271,\ d = 83;\ p = 307,\ d = -86.$$

In all cases, d is a cubic non-residue of p. Since the following equations are soluble:

$$x^3 - 3xy^2 + y^3 = 73z^3 \quad : x = 5,\ y = 2,\ z = 1$$
$$x^3 - 3xy^2 + y^3 = 307z^3 \quad : x = 12,\ y = 7,\ z = 1$$
$$x^3 - 3xy^2 + y^3 = 3 \cdot 271 z^3 : x = 17,\ y = 10,\ z = 1,$$

it follows from Th. VII that 8.5.1 is insoluble for $p = 271$ and 8.5.2 for $p = 73$ and 307 (cf. Table 3 and the example 8.3.5). But Th. VII will of course *not cover all* insoluble equations 8.5.1—2.

CHAPTER IX. The Equation $X^3 + Y^3 = AZ^3$.

§ 1. We have seen in Ch. VII, §§ 5—6, that a treatment of the equation $X^3 + Y^3 = AZ^3$ in the field $K(\sqrt[3]{A})$ led to *incomplete* results about the solubility of such an equation. The object of the present chapter is to improve the results by a treatment in the field $K(\varrho)$, $\varrho = e^{\frac{2\pi i}{3}}$, as already indicated by Hurwitz [1], Nagell [1] and Faddeev [1]. *(See the Introduction.)*

I shall make use of the *cubic law of reciprocity*, and quote the following results from Bachmann [1], pp. 185—99 and 220—24:

As already mentioned in Ch. IV, § 4, the primes of $K(\varrho)$ are $\lambda = 1 - \varrho$ (where $\lambda^2 = -3\varrho$), the rational primes $q \equiv -1 \pmod 3$ and the conjugate factors of the rational primes $r \equiv +1 \pmod 3$, $r = \pi_r \bar{\pi}_r$. I denote by $\pi = a + b\varrho$ any prime q, π_r or $\bar{\pi}_r$. By multiplication by a properly chosen unit ε from $K(\varrho)$ ($\varepsilon = \pm 1$, $\pm\varrho$ or $\pm\varrho^2$), we can always put π in the *primary form:*

9.1.1 $$a \equiv -1, \quad b \equiv 0 \pmod 3.$$

For any integer ν of $K(\varrho)$, we have

$$\nu^{\frac{N(\pi)-1}{3}} \equiv 1, \varrho \text{ or } \varrho^2 \pmod \pi, \text{ if } (\nu, \pi) = 1,$$

where N means the norm in $K(\varrho)$; and we define the *cubic character* of ν mod π by

$$\left[\frac{\nu}{\pi}\right] = 1, \varrho \text{ or } \varrho^2$$

respectively; the first alternative corresponds to the cubic residues mod π. The symbol is *multiplicative:*

$$\left[\frac{\nu_1 \nu_2}{\pi}\right] = \left[\frac{\nu_1}{\pi}\right] \cdot \left[\frac{\nu_2}{\pi}\right].$$

The cubic law of reciprocity states that

9.1.2 $$\left[\frac{\pi}{\pi'}\right] = \left[\frac{\pi'}{\pi}\right],$$

when π and π' are two different primes in *primary form.* — We also need some supplementary results:

9.1.3 $$\left[\frac{\varrho}{\pi}\right] = \varrho^{\frac{N(\pi)-1}{3}},$$

which shows that ϱ is a cubic residue of π only if $\pi = q \equiv -1 \pmod 9$, or if $\pi = \pi_r$, where $r = \pi_r \bar{\pi}_r \equiv +1 \pmod 9$.

9.1.4 $$\left[\frac{3}{\pi}\right] = \left[\frac{3}{a + b\varrho}\right] = \varrho^{\frac{2b}{3}},$$

i.e. 3 is a cubic residue if and only if $b \equiv 0 \pmod 9$. — Further

9.1.5 $$\left[\frac{\bar{\nu}}{\bar{\pi}}\right] = \overline{\left[\frac{\nu}{\pi}\right]} = \left[\frac{\nu}{\pi}\right]^2.$$

The value of the cubic character [ ] is replaced by its *conjugate* (i.e. ϱ replaced by ϱ^2) if both "numerator" and "denominator" are replaced simultaneously by their conjugates. — Finally two conjugate primes are always cubic residues of each other:

9.1.6 $$\left[\frac{\pi}{\bar{\pi}}\right] = \left[\frac{\bar{\pi}}{\pi}\right] = 1.$$

The main formula 9.1.2 still holds if the definition 9.1.1 of the primary form is replaced by the *weaker* definition

9.1.7 $$b \equiv 0 \pmod 3.$$

This is *not* the case for 9.1.4, but the equivalence $9 \mid b \rightleftarrows 3\,(R)\,r$ is of course still valid. — If nothing else is said, "primary form" will throughout this chapter only refer to the weaker definition 9.1.7.

§ 2. As already mentioned in the Introduction, the equation

9.2.1 $$X^3 + Y^3 = A\,Z^3$$

was proved insoluble in many cases by SYLVESTER [1], PÉPIN [1]—[3] and others; for complete references, see the fourth heading 1.5.1. The most important result is

Theorem VIII *(Sylvester, Pépin). The equation* $X^3 + Y^3 = A\,Z^3$ *has only the trivial solution with* $Z = 0$ *if* A *has one of the following forms:*

9.2.2 $$\begin{cases} 3,\ q_1\,(>2),\ q_2,\ q_1^2,\ q_2^2,\ 9\,q_1,\ 9\,q_2,\ 9\,q_1^2,\ 9\,q_2^2, \\ q_1\,q_2,\ q_1^2\,q_2^2,\ q_1\,q_1'^2,\ q_2\,q_2'^2, \end{cases}$$

where $q_1 \equiv q_1' \equiv 2$ *and* $q_2 \equiv q_2' \equiv 5 \pmod 9$ *are primes.*

The cubefree $A \leqq 500$ covered by this theorem are given in *Table 4a*. — The insolubility of $A = 3$ and 4 had been proved earlier by LEGENDRE [1], who also stated that $A = 5$ and (erroneously) $A = 6$ are insoluble. The well-known simplest cases $A = 1$ and 2 are mentioned in 1.4.2—3.

The values 9.2.2 are *all* those with no prime factors $r \equiv 1 \pmod 3$ which were proved insoluble during the 19th century. (Cf. the comments to 9.4.5.) There are also some earlier results about insolubility when A contains *one* prime factor r; the most important of these results are

SYLVESTER [1], PÉPIN [3]:

9.2.3 $$A = 3\,r \text{ or } 3\,r^2, \text{ where } 3\,(N)\,r.$$

9.2.4 $$A = 2\,r,\ 4\,r,\ 2\,r^2 \text{ or } 4\,r^2, \text{ where } A \not\equiv \pm 1 \pmod 9,\ 2\,(N)\,r.$$

PÉPIN [3] (DICKSON [1], Ch. XXI, ref. 207):

$$9.2.5 \qquad \begin{cases} A = 18 \cdot (r_1, r_3, r_4, r_1^2, r_2^2, r_4^2)^1 \\ A = 36 \cdot (r_1, r_2, r_4, r_1^2, r_3^2, r_4^2), \end{cases}$$

where $r_1, \ldots r_4$ are primes which can be expressed in the forms

$$r_1 = (9m + 4)^2 + 3(9n \pm 4)^2, \quad r_2 = (9m + 1)^2 + 3(9n \pm 1)^2,$$
$$r_3 = (9m + 2)^2 + 3(9n \pm 2)^2, \quad r_4 = m^2 + 27(3n \pm 1)^2.$$

We shall need later the residues mod 9:

$$9.2.6 \qquad r_1 \equiv 1, \quad r_2 \equiv 4 \quad \text{and} \quad r_3 \equiv 7 \pmod 9,$$

and the cubic characters of 2 and 3:

$$9.2.7 \qquad \begin{cases} 2(N)r_1, \quad 2(N)r_2, \quad 2(N)r_3, \quad 2(R)r_4, \\ 3(R)r_1, \quad 3(R)r_2, \quad 3(R)r_3, \quad 3(N)r_4. \end{cases}$$

This follows from some well-known equivalences (cf. SYLVESTER [1], p. 346): Let $r = f^2 + 3g^2$ be a prime; then

$$3 \mid g \rightleftarrows 2(R)r, \quad 9 \mid g \quad \text{or} \quad 9 \mid f \pm g \rightleftarrows 3(R)r.$$

The values A of 9.2.5 all have the prime factors 2 and 3, and the varying factor r. PÉPIN [3] also gives some results of insolubility when the factor r is fixed and the other factors vary. I shall quote his results for the smallest value $r = 7$. (There is not full accordance between Pépin's introduction and his later proofs, and there are several errors. The formulae below are the correct ones.)

We group the primes $q \equiv -1 \pmod 3$ by their residues mod $126 = 2 \cdot 7 \cdot 9$ in the following way:

$$9.2.8 \qquad \begin{cases} q_1 = 126h + 29, 83 & q_2 = 126h + 41, 113 \\ q_3 = 126h + 47, 65 & q_3' = 126h + 11, 101 \\ q_4 = 126h + 5, 23 & q_4' = 126h + 59, 95 \\ q_5 = 126h + 17, 53, 89, 107. \end{cases}$$

---

[1] There is a misprint in Pépin (copied in Dickson): $\psi^2 = r_3^2$ should be replaced by $\varrho^2 = r_1^2$. — There are several misprints and inaccuracies in Pépin's paper.

Then the following values are proved insoluble by Pépin:

9.2.9 $$7\cdot(q_3,\ q_3',\ q_4^2,\ q_4'^2,\ q_5,\ q_5^2),\quad 7^2\cdot(q_3^2,\ q_3'^2,\ q_4,\ q_4',\ q_5,\ q_5^2),$$

9.2.10 $$2\cdot 7\cdot(q_1,\ q_2^2),\quad 2^2\cdot 7\cdot(q_5,\ q_5^2),\quad 2\cdot 7^2\cdot(q_5,\ q_5^2),\quad 2^2\cdot 7^2\cdot(q_1^2,\ q_2).$$

To these I can add

9.2.11 $$2\cdot 7\cdot(q_3',\ q_4^2),\quad 2^2\cdot 7^2\cdot(q_3'^2,\ q_4),$$

9.2.12 $$\begin{cases} 9\cdot 7\cdot(q_1,\ q_1^2,\ q_2,\ q_2^2,\ q_3^2,\ q_3',\ q_3'^2,\ q_4,\ q_4^2,\ q_4',\ q_5,\ q_5^2),\\ 9\cdot 7^2\cdot(q_1,\ q_1^2,\ q_2,\ q_2^2,\ q_3,\ q_3^2,\ q_3',\ q_4^2,\ q_4',\ q_4'^2,\ q_5,\ q_5^2).\end{cases}$$

We shall need later the residues mod 9 of the primes 9.2.8, and their cubic character mod 7:

9.2.13 $$\begin{cases} q_1 \equiv q_3 \equiv q_3' \equiv 2,\ \ q_2 \equiv q_4 \equiv q_4' \equiv 5,\ \ q_5 \equiv 8 \pmod 9;\\ q_1 \text{ and } q_2\ (R)7;\ \ q_3,\ q_3',\ q_4,\ q_4' \text{ and } q_5\ (N)7;\\ q_3 \sim q_4 \sim 2,\ \ q_3' \sim q_4' \sim 3 \div 2 \pmod 7.\end{cases}$$

Pépin also gives similar (incomplete) results for

$$r = 13,\ 19,\ 31 \text{ and } 37.$$

I omit them here, as they are all *covered by my general Theorems* XI (§ 8) and XII (§ 10).

§ 3. In the field $K(\varrho)$, the left hand side of 9.2.1 factorizes as

9.3.1 $$X^3 + Y^3 = (X + Y)(X + Y\varrho)(X + Y\varrho^2) = AZ^3$$

(where of course X and Y are supposed to be *rational integers*). We must have $(X, Y) = 1$, since we only consider *cubefree* values of A. Any common divisor of the three factors of 9.3.1 must divide the differences

$$Y(1-\varrho),\quad Y(1-\varrho^2) \text{ and } Y(\varrho-\varrho^2),$$

and the only possible common factor is therefore

9.3.2 $$\lambda = 1-\varrho,\ \text{ if }\ X + Y \equiv 0 \pmod 3,\ \text{ i.e. } 3 \mid AZ.$$

It is further clear that $X + Y\varrho$ or $X + Y\varrho^2$ cannot be divisible by a *rational* integer > 1, i.e. in particular not by $\lambda^2 = -3\varrho$.

Treating $X^3 + Y^3 = AZ^3$ as a congruence mod 9, we see that we *must* have $3 \mid Z$, i.e. the case 9.3.2, if $A \equiv \pm 3$ or $\pm 4 \pmod 9$. When $A \equiv \pm 2 \pmod 9$, there is also the alternative possibility $X \equiv Y \equiv \pm Z \not\equiv 0 \pmod 3$, and if $A \equiv \pm 1 \pmod 9$ the possibility $XY \equiv 0 \pmod 3$.

We will first suppose that A *contains no prime factors* $r \equiv 1 \pmod 3$. As all primes $q \equiv -1$ remain primes in $K(\varrho)$, and hence cannot divide $(X + Y\varrho)(X + Y\varrho^2)$, 9.3.1—2 give us the following possibilities:

Case I: $3 \mid Z$ (the only possibility when $A \equiv \pm 3$ or $\pm 4 \pmod 9$):

$$X + Y = 9Aw^3, \quad X + Y\varrho = \varepsilon\lambda(u + v\varrho)^3, \quad Z = 3w \cdot N(u + v\varrho).$$

Case II: $3 \nmid Z$, $A \equiv \pm 1$ or $\pm 2 \pmod 9$:

$$X + Y = Aw^3, \quad X + Y\varrho = \varepsilon(u + v\varrho)^3, \quad Z = w \cdot N(u + v\varrho).$$

Case III: $3 \nmid Z$, $A \equiv 0 \pmod 9$:

$$X + Y = \frac{1}{3}Aw^3, \quad X + Y\varrho = \varepsilon\lambda(u + v\varrho)^3, \quad Z = w \cdot N(u + v\varrho).$$

Here ε stands for some unit 1, ϱ or ϱ^2 of $K(\varrho)$ (a negative sign can be absorbed in $u + v\varrho$). The expression for $X + Y\varrho^2$ is always the conjugate of $X + Y\varrho$. u and v are rational integers, and the norm $N(u + v\varrho) = u^2 - uv + v^2$. In all cases we must have $\lambda \nmid u + v\varrho$, or $u + v \not\equiv 0 \pmod 3$. The condition $(X, Y) = 1$ implies $(u, v) = 1$.

The cases above will be referred to throughout as I, II and III, without further reference. In order to avoid a separate treatment of each case, we note that $\varepsilon(u + v\varrho)^3$ of case II can be replaced by $\frac{1}{9}\varepsilon_1\lambda(u_1 + v_1\varrho)^3$, where still $(u_1, v_1) = 1$, but now $u_1 + v_1 \equiv 0 \pmod 3$, i.e. $\lambda \| u_1 + v_1\varrho$, $9 = \varrho\lambda^4 \| \lambda(u_1 + v_1\varrho)^3$, and where ε_1 is some properly chosen unit. This device may seem artificial, but it means a great simplification of the calculations. The equations in the cases I—III can now all be *included in the one formula:*

9.3.3 $$X + Y = sAw^3, \quad X + Y\varrho = t\varepsilon\lambda(u + v\varrho)^3, \quad Z = \sqrt[3]{3st^2} \cdot (u^2 - uv + v^2) \cdot w,$$

where

9.3.4
$$\begin{cases} \textit{Case} \quad I: \ s = 9, \ t = 1, \ u + v \not\equiv 0 \pmod 3. \\ \textit{Case} \quad II: \ s = 1, \ t = \frac{1}{9}, \ u + v \equiv 0, \ w \not\equiv 0 \pmod 3. \\ \textit{Case III:} \ s = \frac{1}{3}, \ t = 1, \ u + v \not\equiv 0, \ w \not\equiv 0 \pmod 3. \end{cases}$$

§ 4. We can draw some immediate conclusions from 9.3.3, by substituting $\lambda = 1 - \varrho$, and comparing real and complex parts for the three possibilities $\varepsilon = 1$, ϱ and ϱ^2:

$$\underline{\varepsilon = 1}: \quad X = t(u^3 + 3u^2v - 6uv^2 + v^3)$$
$$Y = -t(u^3 - 6u^2v + 3uv^2 + v^3) \text{ and so}$$
$$X + Y = 9tuv(u - v) = sAw^3.$$

This is *impossible in case III*, since then $3 \| sAw^3$. In both cases I and II, we have $s = 9t$, and

$$uv(u - v) = Aw^3.$$

The factors of the left hand side are coprime in pairs (since $(u, v) = 1$), and we conclude that there must exist a factorization of $A = abc$, and three rational integers x, y and z, so that (the negative sign for u is convenient):

9.4.1 $$u = -ax^3, \quad v = by^3, \quad u - v = cz^3; \quad w = -xyz,$$

or by addition of the three first equations:

$$ax^3 + by^3 + cz^3 = 0, \quad abc = A, \quad (a, b) = (a, c) = (b, c) = 1.$$

If this is soluble, so is the given equation $X^3 + Y^3 = AZ^3$. Going through the calculations, we find that X, Y *and* Z *are expressed in terms of* x, y *and* z *by the formulae* 1.2.4 *of Theorem I.*

One possibility of factorization is of course:

9.4.2 $$a = b = 1, \quad c = A,$$

i.e. the same equation 9.2.1, but *with a smaller numerical value of* Z (cf. § 15, Lemma 1). For

$$Z = \sqrt[3]{3st^2} \cdot (u^2 - uv + v^2) \cdot w = -\sqrt[3]{3st^2} \cdot N(u + v\varrho) \cdot xyz.$$

We will suppose $A > 1$, i.e. $xy \neq 0$, and further $A \neq 2$, i.e. $xy \neq 1$, $|xy| > 1$. In case I we have $\sqrt[3]{3st^2} = 3$, $N(u + v\varrho) \geqq 1$, and in case II $\sqrt[3]{3st^2} = \frac{1}{3}$, $N(u + v\varrho) \geqq 3$ (since $\lambda | u + v\varrho$). In both cases we find

9.4.3 $$|z| < |Z|.$$

We can consequently use the argument of "*infinite descent*": If the original solution (X, Y, Z) is the one for which $|Z| > 0$ has the minimal value, then the possibility 9.4.2 is excluded.

We shall see in a moment (§ 5) that the other possibilities $\varepsilon = \varrho$ or ϱ^2 are excluded if A is not a product of primes $\equiv \pm 1 \pmod 9$, or 9 times such a product, and we can therefore enunciate the following

Theorem IX. *If $A > 2$ is cubefree and contains no prime factor $r \equiv +1 \pmod 3$, and if in the cases $A \equiv 0$ or $\pm 1 \pmod 9$ A contains at least one prime $q \not\equiv -1 \pmod 9$, then solubility of $X^3 + Y^3 = AZ^3$ implies solubility of at least one of the equations*

$$9.4.4 \quad ax^3 + by^3 + cz^3 = 0, \quad abc = A, \quad 1 \leqq a < b < c, \quad (a, b) = (a, c) = (b, c) = 1$$

(not necessarily all of these, cf. the 3rd conjecture of Ch. VII, § 4). If all such equations can be proved insoluble (in particular, if no such equation exists, i.e. when A is a prime $q \not\equiv -1 \pmod 9$ or the square of such a prime), then $X^3 + Y^3 = AZ^3$ has only the trivial solution with $Z = 0$.

The values of A for which the equations 9.4.4 (if existing) can be proved impossible by elementary congruence considerations are given by *Theorem VIII* (§ 2); they all correspond to $n_A = 1$ or 2 in Ch. VII, § 4. In the latter case, the equation 7.4.5 can be proved impossible mod 9 by 2.1.2—3.

We have seen in Ch. VII that all equations 9.4.4 can sometimes be excluded by my new methods when $N_A = 4$. The corresponding values of $A \leqq 500$ (22 in all) are given in *Table 4*^{b}; they satisfy the conditions of Th. IX, and consequently represent *insoluble equations* $X^3 + Y^3 = AZ^3$.

The smallest value of A in Table 4^b is

$$9.4.5 \qquad A = 60,$$

which was stated by *Pépin* to be insoluble (in a communication to *Lucas*, cf. SYLVESTER [1] p. 316). Sylvester could not verify this by his methods, and I doubt if Pépin possessed a valid proof. There are two direct errors in the same communication, namely the insolubility of $A = 31$ and 67, which are both soluble by Table 6. (But the insolubility of these was "verified" by Sylvester!)

The argument that led to 9.4.3 is easily extended to the cases $A = 1$ and 2, giving the well-known results mentioned in connection with 1.4.2—3.

We noticed that $\varepsilon = 1$ was impossible in case III. An interesting corollary is that if $A \equiv 0 \pmod 9$, and the conditions of Th. IX are satisfied, then all solutions of $X^3 + Y^3 = AZ^3$ must have $Z \equiv 0 \pmod 3$.

We can further note that $\varepsilon = 1$ for $A = abc \equiv \pm 1 \pmod 9$ is possible *only in case I*, since it is easily seen that we must then have $w = -xyz \equiv 0 \pmod 3$. If therefore $A \equiv \pm 1 \pmod 9$, and the conditions of Th. IX are satisfied, then all solutions of $X^3 + Y^3 = AZ^3$ must have $Z \equiv 0 \pmod 9$.

§ 5. If we put $\varepsilon = \varrho$ in 9.3.3 and compare the real and complex parts, we find (Z is included to avoid repetition in Th. X):

9.5.1
$$\begin{cases} X = t(u^3 - 6u^2v + 3uv^2 + v^3) \\ Y = t(2u^3 - 3u^2v - 3uv^2 + 2v^3) \\ Z = \sqrt[3]{3st^2}\cdot(u^2 - uv + v^2)\cdot w, \quad \text{and} \end{cases}$$

9.5.2
$$X + Y = 3t(u^3 - 3u^2v + v^3) = sAw^3.$$

The form $f(u, v) = u^3 - 3u^2v + v^3$ was treated in Ch. VIII. We have seen that it cannot be divisible by 9 if $(u, v) = 1$; and obviously $3 \| f(u, v)$ if and only if $u + v \equiv 0 \pmod 3$. This shows that 9.5.2 is *impossible in case I*, since then $\frac{s}{3t} = 3$ and $u + v \not\equiv 0 \pmod 3$. Further $f(u, v)$ can only contain prime factors $\neq 3$ which are all $\equiv \pm 1 \pmod 9$; the same holds for A if 9.5.2 shall be possible. Inserting the right values of s and t, we get

Theorem X *(Sylvester). Let the cubefree integer $A > 1$ be a product of primes $\equiv \pm 1 \pmod 9$. A solution of the equation*

9.5.3
$$u^3 - 3u^2v + v^3 = 3Aw^3$$

will lead to the solution 9.5.1, *with* $s = 1$, $t = \frac{1}{9}$, *of* $X^3 + Y^3 = AZ^3$; *and a solution of*

9.5.4
$$u^3 - 3u^2v + v^3 = Aw^3$$

will lead to the same solution, with $s = \frac{1}{3}$, $t = 1$, *of* $X^3 + Y^3 = 9AZ^3$.

Since we have the cases II and III only, we notice that all solutions given by 9.5.1 will have $Z \not\equiv 0 \pmod 3$.

The case $\underline{\varepsilon = \varrho^2}$ need not be treated separately. Instead of the equation 9.3.3, $X + Y\varrho = t\varrho^2\lambda(u + v\varrho)^3$, we can consider the (equivalent) conjugate one:

9.5.5 $$X + Y\varrho^2 = t\varrho\bar{\lambda}(u + v\varrho^2)^3,$$

where $\bar{\lambda} = 1 - \varrho^2 = -\varrho^2(1 - \varrho) = -\varrho^2\lambda$, $(u + v\varrho^2)^3 = (v + u\varrho)^3$, and multiplication by ϱ in 9.5.5 gives

9.5.6 $$Y + X\varrho = t\varrho\lambda(-v - u\varrho)^3.$$

This corresponds to the case $\underline{\varepsilon = \varrho}$, if we interchange X and Y and replace u by $-v$, v by $-u$.

The conditions under which $\varepsilon \neq 1$ is possible can also be deduced *independently of the properties of the form* $f(u, v) = u^3 - 3u^2v + v^3$. Subtraction of the two first equations 9.3.3 gives

9.5.7 $$Y\lambda = sAw^3 - t\varepsilon\lambda(u + v\varrho)^3.$$

In case I we have $s = 9 = \varrho\lambda^4$, $t = 1$, $\lambda \nmid u + v\varrho$, hence $(u + v\varrho)^3 \equiv \pm 1 \pmod{\lambda^4}$, and

$$Y \equiv \pm\varepsilon \pmod{\lambda^2}, \text{ i.e. mod } 3),$$

which is clearly impossible if $\varepsilon = \varrho$ or ϱ^2.

Let next $p \neq 3$ be a prime divisor of A, so $p \nmid Y$. It follows from 9.5.7 that

$$Y \equiv -t\varepsilon(u + v\varrho)^3, \text{ so } Y \equiv -t\bar{\varepsilon}(u + v\varrho^2)^3 \pmod{p}$$

by taking conjugates. Dividing these expressions, we see that

$$\frac{\bar{\varepsilon}}{\varepsilon}(R)p,$$

which is only possible with $\varepsilon \neq 1$, $\frac{\bar{\varepsilon}}{\varepsilon} = \varrho$ or ϱ^2, if $p \equiv \pm 1 \pmod 9$ (cf. 9.1.3).

A list of solutions for the equations 9.5.3—4 is given in *Table 3*, cf. Ch. VIII. Several equations 9.5.3 have been proved insoluble when A is a prime $r \equiv +1 \pmod 9$, or the square of such a prime. This does not necessarily imply insolubility of the corresponding equation $X^3 + Y^3 = AZ^3$, since there are also other possibilities of descent (§ 6) in this case. (But see §§ 12—14 below.)

If $A = Q = q$ or q^2 (in the notation 7.4.3), $q \equiv -1 \pmod 9$, the equation

9.5.3 represents *the only possibility of descent.* And the methods of exclusion in Ch. VIII *do not apply*, since the condition 8.3.4 is only effective for a prime $p = r \equiv +1 \pmod 9$.

The last remark also holds if $A = 9Q$ or $A = Q_1 Q_2$, where $q \equiv q_1 \equiv q_2 \equiv -1 \pmod 9$. But then the one equation 7.4.5 is also possible for all moduli, and cannot be excluded by the methods of this paper, if *the weaker form of the first conjecture* in Ch. VII, § 4 is true. This remark holds for *any* combination $A = Q_1 Q_2$ which is not covered by Th. VIII (§ 2), and we can consequently enunciate the following *negative* result:

Let A (cubefree) contain at most two different prime factors, and no prime $r \equiv +1 \pmod 3$. If the weaker form of the first conjecture in Ch. VII, § 4 is true, then Theorem VIII will give all such values of A, for which the equation $X^3 + Y^3 = AZ^3$ can be proved insoluble by the methods of the present paper.

§ 6. If A contains one or more prime factors $r \equiv +1 \pmod 3$, the above possibilities of descent *still exist*, giving rise to the Theorems I and X. But there is also another possible descent in this case, depending on the fact that the primes $r = \pi_r \bar{\pi}_r$ *factorize in* $K(\varrho)$. In addition to 9.3.3, we now get one or more systems

$$9.6.1 \quad \begin{cases} X + Y = sA_1 w^3, \quad X + Y\varrho = t\lambda(a + b\varrho)(u + v\varrho)^3, \\ \qquad\qquad\qquad\qquad\qquad\qquad a + b\varrho \neq \pm 1, \quad \pm\varrho, \quad \pm\varrho^2; \\ Z = \sqrt[3]{3st^2} \cdot (u^2 - uv + v^2) \cdot w, \text{ where } A = A_1 \cdot N(a + b\varrho), \end{cases}$$

with the values of s and t given by 9.3.4. — Here $a + b\varrho$ is a product of primes π_r such that $r \mid A$. *The unit ε is absorbed in $a + b\varrho$*, for which there are consequently three *a priori* possibilities for each choice of the factors π_r. The conditions $(X, Y) = 1$ and $\lambda \nmid a + b\varrho$ imply $(a, b) = 1$ and $a + b \not\equiv 0 \pmod 3$.

If A contains several primes r, the number of possible combinations $a + b\varrho$ may become considerable (some of these factors r can of course divide A_1, which *must* contain all prime factors q of A). But there are some important simplifications in this connection:

1. $a + b\varrho$ can never be divisible by two conjugate primes π_r and $\bar{\pi}_r$, i.e. by r.

2. The equations 9.6.1 for two *conjugate values $a + b\varrho$ and $a + b\varrho^2$ are equivalent*, and it suffices to treat one of these possibilities. For instead of the equation

$$X + Y\varrho = t\lambda(a + b\varrho^2)(u + v\varrho)^3,$$

we can consider the conjugate one:

$$X + Y\varrho^2 = t\bar{\lambda}(a + b\varrho)(u + v\varrho^2)^3.$$

The argument that led to 9.5.6 shows that this can be written as

$$Y + X\varrho = t\lambda(a + b\varrho)(-v - u\varrho)^3,$$

which is equivalent to 9.6.1.

3. If A (cubefree) is divisible by a square r^2, then $\pi_r \mid a + b\varrho \to \pi_r^2 \| a + b\varrho$, since the possibility $\pi_r \| a + b\varrho$, $r \| A_1$ implies the common factor π_r of $X + Y\varrho$ and $X + Y$.

As an important corollary of the above results, we see that *apart from the choice of unit, there is only one possible system* 9.6.1 *if A contains just one prime* $r \equiv 1 \pmod 3$ (to the first or second power).

Comparing the real and complex parts in 9.6.1, we find (Z is included for convenience):

$$9.6.2 \qquad \begin{cases} \dfrac{X}{t} = a(u^3 + 3u^2v - 6uv^2 + v^3) + b(u^3 - 6u^2v + 3uv^2 + v^3) \\ \dfrac{Y}{t} = -a(u^3 - 6u^2v + 3uv^2 + v^3) + b(2u^3 - 3u^2v - 3uv^2 + 2v^3) \\ Z = \sqrt[3]{3st^2}\cdot(u^2 - uv + v^2)\cdot w, \quad \text{and} \end{cases}$$

$$9.6.3 \qquad 3auv(u - v) + b(u^3 - 3u^2v + v^3) = \frac{s}{3t}\cdot A_1 w^3 = A_2 w^3 \quad \left(= \frac{X + Y}{3t}\right).$$

A solution of this equation will consequently lead to the solution 9.6.2 *of* $X^3 + Y^3 = AZ^3$, *where* $A = A_1\cdot(a^2 - ab + b^2)$. The values of s and t are given in 9.3.4. We note in particular that we get *the same equation* 9.6.3 in the two (most important) cases I and II, since then $\underline{\dfrac{s}{3t} = 3.}$

§ 7. The necessary and sufficient conditions for solubility of the congruence corresponding to 9.6.3:

$$9.7.1 \qquad 3auv(u - v) + b(u^3 - 3u^2v + v^3) \equiv \frac{s}{3t}\cdot A_1 w^3 = A_2 w^3 \pmod{p^\delta},$$

for all primes p and all exponents δ, are given by:

$$9.7.2 \qquad q \mid A, \text{ i.e. } q \mid A_2\colon \left[\frac{a + b\varrho}{q}\right] = 1.$$

9.7.3 $$r = \pi_r \bar{\pi}_r \mid A_2\colon \left[\frac{a + b\varrho}{\frac{a + b\varrho^2}{\pi_r}}\right] = 1, \text{ or } \frac{a + b\varrho}{a + b\varrho^2}(R) r.$$

9.7.4 $\pi_r \mid a + b\varrho$, i.e. $r \mid N(a + b\varrho)$: $b^2 A_2(R) r$, or $b \sim A_2 \pmod r$.

The above conditions are the same in all cases I—III. To obtain the conditions mod 3^δ, these cases must be treated separately:

9.7.5 Case I, if $3 \nmid A$: $b \equiv 0 \pmod 3$.

9.7.6 " ", if $3 \mid A$: $b \equiv 0 \pmod 9$.

9.7.7 Case II, $3 \nmid A_1$: $b - 2a \equiv \pm A_1 \pmod 9$.

9.7.8 Case III, $9 \parallel A_1$, $3 \nmid A_2$: $b \equiv \pm A_2 \pmod 9$.

To prove the conditions 9.7.2—8, we need the results of Ch. II, § 3, in particular 2.3.3. We note that the *discriminant* of the left hand side of 9.7.1 is

9.7.9 $$\Delta = 3^4 \cdot N(a + b\varrho)^2 = 3^4 \cdot (a^2 - ab + b^2)^2,$$

which has *no prime factor* $\neq 3$ *in common with* A_2 (by 3. of the last paragraph). For all $p \neq 3$, it will therefore suffice to treat 9.7.1 with $\delta = 1$.

With the notation of 2.3.1, we find for 9.7.1 that $A = b$, $B = 3(a - b)$, $C = -3a$, $D = b$, $E = A_2$, and the primes $p \neq 3$ which must be considered are by 2.3.3 and 9.7.9:

$$p = q \text{ if } q \mid A_2; \quad p = r \text{ if } r \mid b A_2 (a^2 - ab + b^2),$$

i.e. the primes of 9.7.2—4, and in addition the primes r such that $r \mid b$. But it is clear that in the latter case, the congruence 9.7.1 for $\delta = 1$ is always soluble with $u \equiv v \not\equiv 0$, $w \equiv 0 \pmod r$. And since $r \nmid a$, i.e. $r \nmid \Delta$, we can find solutions for any $\delta > 1$ by varying u or v only.

Let next $p \neq 3$ be a prime factor of A_2, so $p \nmid Y$. Subtraction of the two first equations 9.6.1 and division by $\lambda = 1 - \varrho$ shows that

$$-Y \equiv t(a + b\varrho)(u + v\varrho)^3, \text{ so } -Y \equiv t(a + b\varrho^2)(u + v\varrho^2)^3 \pmod p$$

by taking conjugates. If $p = q \equiv -1 \pmod 3$, Y and t (rational) are both cubic residues of q, and we get the necessary condition 9.7.2. If $p = r \equiv +1 \pmod 3$, division of the two expressions for Y similarly gives the condition 9.7.3. To show the *sufficiency* of these conditions, we note that they both imply the

existence of three rational integers u_1, v_1 (not both $\equiv 0 \pmod p$) and $k \not\equiv 0 \pmod p$ such that

$$a + b\varrho \equiv k(v_1 + u_1\varrho)^3 \pmod p, \quad \text{or}$$
$$a \equiv k(u_1^3 - 3u_1^2 v_1 + v_1^3), \quad b \equiv -k \cdot 3u_1 v_1(u_1 - v_1) \pmod p.$$

Since $p \mid A_2$, we have a solution $u \equiv u_1$, $v \equiv v_1$ of 9.7.1 (with $\delta = 1$, which suffices since $p \nmid \Delta$).

Let finally $r \mid A$ be one of the primes which have been used for forming $a + b\varrho$, i.e. $\pi_r \mid a + b\varrho$, $r \mid N(a + b\varrho) = a^2 - ab + b^2$, $r \nmid b$, $r \nmid A_2 w^3$. After multiplication with b^2, the congruence 9.7.1 (with $\delta = 1$, which suffices since $r \nmid A_2$) can be written as

$$(bv - au)^3 + [(a + b)u^3 - 3bu^2 v] \cdot (a^2 - ab + b^2) \equiv b^2 A_2 w^3 \pmod r,$$
$$\text{hence} \quad (bv - au)^3 \equiv b^2 A_2 w^3 \pmod r.$$

The necessity and sufficiency of 9.7.4 is an immediate consequence.

We now turn to the conditions mod 3^δ, and treat the simplest cases 9.7.7—8 first. In case II we have $3 \nmid A_1$ and $\frac{s}{3t} = 3$. Since $u + v \equiv 0 \pmod 3$, we substitute $v = -u + 3v_1$ in 9.7.1, and find after division by 3:

$$(b - 2a)u^3 + 9au^2 v_1 - 9(a + b)uv_1^2 + 9bv_1^3 \equiv A_1 w^3 \pmod{3^{\delta-1}},$$

for which clearly 9.7.7 is the necessary and sufficient condition for solubility for all δ.

In case III we have $9 \parallel A_1$ and $\frac{s}{3t} = \frac{1}{9}$, so $3 \nmid A_2$. From $u + v \not\equiv 0 \pmod 3$ we conclude that

9.7.10 $$uv(u - v) \equiv 0 \pmod 3, \quad u^3 - 3u^2 v + v^3 \equiv \pm 1 \pmod 9,$$

which proves 9.7.8.

In case I we have $\frac{s}{3t} = 3$ and $u + v \not\equiv 0 \pmod 3$. Since A and A_1 are exactly divisible by the same power of 3, the *necessity* of the conditions 9.7.5—6 is clear from 9.7.10. I omit the verification of their sufficiency here; the proof is an elementary, but tedious enumeration of cases.

§ 8. The conditions 9.7.5—8 show at once that we must have $b \equiv 0 \pmod 3$ *in case I*, $b \not\equiv 0 \pmod 3$ *in case III*. But we can also deduce similar properties in case II, namely: *For* $A \equiv \pm 1$ *or* $\pm 2 \pmod 9$ *in case II, we must have* $b \not\equiv 0$ *or* $b \equiv 0 \pmod 3$ *respectively.*

We notice that $\lambda \nmid a + b\varrho$ implies $a + b \equiv b - 2a \not\equiv 0 \pmod 3$, which leaves the following possibilities for $a + b\varrho$ (in all cases):

9.8.1 $$b \equiv 0, \quad a \equiv 0 \text{ or } a - b \equiv 0 \pmod 3.$$

These can all be obtained from one by multiplication with properly chosen units 1, ϱ or ϱ^2.

We suppose that we have case II, and let first $b \not\equiv 0 \pmod 3$, then

$$a^2 - ab + b^2 = (b - 2a)^2 - 3a(a - b) \equiv (b - 2a)^2 \pmod 9.$$

But then $A = A_1(a^2 - ab + b^2) \equiv A_1(b - 2a)^2$, and

$$A(b - 2a) \equiv A_1(b - 2a)^3 \equiv \pm A_1 \pmod 9,$$

which coincides with 9.7.7 if and only if $A \equiv \pm 1 \pmod 9$.

Let next $b \equiv 0 \pmod 3$, then

$$a^2 - ab + b^2 = -2(b - 2a)^2 + 9a^2 - 9ab + 3b^2 \equiv -2(b - 2a)^2 \pmod 9,$$

and we conclude similarly that

$$A(b - 2a) \equiv \pm 2A_1, \text{ or } A \equiv \pm 2 \pmod 9.$$

Consequently we must have $b \equiv 0 \pmod 3$ *for all* $A \not\equiv 0$ *or* $\pm 1 \pmod 9$. If in particular $a + b\varrho$ is *a prime* π_r, or the square π_r^2, this means that π_r must have the *primary form* 9.1.7. For a prime q such that $q \mid A$, we can use the *cubic law of reciprocity* 9.1.2 on the condition 9.7.2:

$$\left[\frac{a + b\varrho}{q}\right] = \left[\frac{\pi_r}{q}\right] = \left[\frac{q}{\pi_r}\right] = 1.$$

The same holds for *any* A if $q \equiv -1 \pmod 9$, i.e. $\left[\frac{\varrho}{q}\right] = 1$ by 9.1.3. We thus get the important condition:[1]

9.8.2 $$q \mid A, \quad A \not\equiv 0 \text{ or } \pm 1 \text{ if } q \not\equiv -1 \pmod 9, \quad a + b\varrho = \pi_r \text{ or } \pi_r^2 \to \underline{q(R)r}.$$

If $q(N)r$, the equation 9.6.3 is then impossible. If A contains only one prime factor r, there are no other possible equations of the same type. If

[1] A similar condition is easily deduced from 9.7.3:

$$r_1 \neq r, \quad r_1 \mid A_1, \quad A \not\equiv 0 \text{ or } \pm 1 \text{ if } r_1 \not\equiv +1 \pmod 9, \quad a + b\varrho = \pi_r \text{ or } \pi_r^2 \to r_1(R)r.$$

further A contains only one prime q, and $3 \nmid A$, i.e. $A = QR$ in the notation 7.4.3, then the only *a priori* possible equation 9.4.4:

$$x^3 + Qy^3 + Rz^3 = 0 \tag{9.8.3}$$

is excluded mod r if $q(N)r$. If we suppose $A \not\equiv \pm 1 \pmod 9$, then at least one of the primes q and r is $\not\equiv \pm 1 \pmod 9$, and the descent of § 5 is also excluded. The corresponding equation $X^3 + Y^3 = AZ^3$ is consequently insoluble.

Before we formulate this as a theorem, we shall find a similar result in the case $A = 3R$, $R = r$ or r^2, where $3(N)r$. From 9.1.4 we conclude that the condition 9.7.6 is not satisfied. (Note that

$$9 \mid b \rightleftarrows 9 \mid b_1 \quad \text{if} \quad a + b\varrho = \pi_r^2 = (a_1 + b_1\varrho)^2. \tag{9.8.4}$$

The equation $x^3 + 3y^3 + Rz^3 = 0$ is also insoluble, and the descent of § 5 excluded. — We can therefore state the following

Theorem XI. *The equation $X^3 + Y^3 = AZ^3$ has only the trivial solution with $Z = 0$ if A has one of the following forms:*

$$A = 3r \text{ or } 3r^2,\ 3(N)r; \tag{9.8.5}$$

$$A = qr,\ qr^2,\ q^2r \text{ or } q^2r^2,\ A \not\equiv \pm 1 \pmod 9,\ q(N)r, \tag{9.8.6}$$

where $q \equiv -1$ and $r \equiv +1 \pmod 3$ are primes, and (N) denotes cubic non-residuacity.

The case 9.8.5 is nothing but *Sylvester*'s result 9.2.3, and is included in the theorem for convenience. The general result 9.8.6 does, however, seem to be new. Sylvester's values 9.2.4 represent the special case $q = 2$, and Pépin's values 9.2.9 give all possibilities with $r = 7$ (this is easily verified by 9.2.13). As already mentioned, Pépin also proves similar (incomplete) results for $r = 13$, 19, 31 and 37, but not the general theorem.

The cubefree values of $A \leqq 500$ which can be proved insoluble by Th. XI are given in *Table 4*[c].

We can combine the above results with Th. IX (§ 4) to the following generalization of Th. XI: *Let A be cubefree and $\not\equiv 0$ or $\pm 1 \pmod 9$. If A contains exactly one prime factor $r \equiv +1 \pmod 3$, and at least one other prime p such that $p(N)r$, then solubility of $X^3 + Y^3 = AZ^3$ implies solubility of at least one of the equations* 9.4.4.

This does not lead to any new insoluble values of $A \leqq 500$. The smallest excluded A which is not covered by Th. XI is $\underline{A = 570} = 2 \cdot 3 \cdot 5 \cdot 19$ (cf. 7.4.10), where 2, 3 and 5 are all cubic non-residues of 19.

The equation 9.6.3 is also impossible for the values A of 9.8.6 under the modified condition

9.8.7 $$A = QR, \quad q \equiv -1, \quad r \equiv +1 \pmod 9, \quad q(N)r.$$

This follows at once from 9.8.2. — The equation 9.8.3 is excluded mod r in this case, but *the descent of § 5* is *a priori* possible.

§ 9. We shall show the following *negative* result about the strength of the conditions 9.7.2—8 (cf. the corresponding enunciation at the end of § 5 above):

Let A (cubefree) contain at most two different prime factors, of which at least one is a prime $r \equiv +1 \pmod 3$. *The possibility* 9.6.3 *of descent can then be completely excluded by congruence considerations only in the cases* 9.8.5—7, *and in the additional case*

9.9.1 $$A = 9r \text{ or } 9r^2, \quad r \equiv +1 \pmod 9, \quad 3(N)r.$$

(But then of course the descent of § 5 is possible, and the methods of exclusion in Ch. VIII do not apply, since 8.4.5 is not satisfied.)

We begin by proving the following lemma:

9.9.2 $$a + b\varrho = \pi_r \text{ or } \pi_r^2, \quad b \equiv 0 \pmod 3 \to 9\,b(R)r, \text{ i.e. } 3\,b^2(R)r.$$

This is a consequence of 9.1.6:

$$1 = \left[\frac{a + b\varrho}{a + b\varrho^2}\right] = \left[\frac{b(\varrho - \varrho^2)}{a + b\varrho^2}\right] = \left[\frac{b\varrho\lambda}{a + b\varrho^2}\right] = \left[\frac{b\varrho\lambda \cdot \lambda^3}{a + b\varrho^2}\right] = \left[\frac{9b}{a + b\varrho^2}\right]$$

(*Jacobian* symbols if $a + b\varrho = \pi_r^2$). Nagell ([7] pp. 16—17) has proved the more general result that *every prime factor* of $\frac{b}{3}$ (and also of $b - 2a$) is a cubic residue mod r.

The condition $b \equiv 0 \pmod 3$ *in* 9.9.2 *can be omitted if* $r \equiv +1 \pmod 9$, since then ϱ is a cubic residue of π_r and $\bar{\pi}_r$ by 9.1.3. — Let $a + b\varrho$ be one possible form; the other forms (irrespective of the sign) are then

9.9.3 $$\varrho(a + b\varrho) = -b + (a - b)\varrho = a_1 + b_1\varrho, \quad \varrho^2(a + b\varrho) = b - a - a\varrho = a_2 + b_2\varrho, \text{ where}$$

$$9.9.4 \qquad \begin{cases} \left[\frac{b_1}{a+b\varrho}\right] = \left[\frac{a-b}{a+b\varrho}\right] = \left[\frac{-b-b\varrho}{a+b\varrho}\right] = \left[\frac{b\varrho^2}{a+b\varrho}\right], \\ \left[\frac{b_2}{a+b\varrho}\right] = \left[\frac{-a}{a+b\varrho}\right] = \left[\frac{b\varrho}{a+b\varrho}\right]. \end{cases}$$

This shows that the three possibilities for b are all equivalent mod r if $r \equiv 1 \pmod 9$, and all inequivalent if $r \not\equiv 1 \pmod 9$.

The lemma 9.9.2 also holds in the more general case $\underline{a + b\varrho = \pi_{r_1}\pi_{r_2}}$ (possibly with squared factors), provided

$$9.9.5 \qquad \left[\frac{\bar\pi_{r_1}}{\pi_{r_2}}\right] = 1, \text{ i.e. } \left[\frac{\bar\pi_{r_1}}{\pi_{r_2}}\right] = \left[\frac{\pi_{r_2}}{\bar\pi_{r_1}}\right] = \left[\frac{\pi_{r_1}}{\bar\pi_{r_2}}\right] = \left[\frac{\bar\pi_{r_2}}{\pi_{r_1}}\right] = 1.$$

We still get $3\,b^2(R)r_1$ & r_2 if $b \equiv 0 \pmod 3$. The proof is similar, since now for instance

$$\left[\frac{a+b\varrho}{\bar\pi_{r_1}}\right] = \left[\frac{\pi_{r_1}}{\bar\pi_{r_1}}\right]\cdot\left[\frac{\pi_{r_2}}{\bar\pi_{r_1}}\right] = 1.$$

We now consider the different forms of A with at most two prime factors, which are not covered by 9.8.5—7:

1. $\underline{A = R = r \text{ or } r^2}$: If $r \equiv 4$ or 7, and so $R \not\equiv \pm 1 \pmod 9$, we have seen that the conditions 9.7.5 or 9.7.7 are satisfied if and only if $b \equiv 0 \pmod 3$. In both cases I and II we have $\frac{s}{3t} = 3$, $A_1 = 1$, $A_2 = 3$ in 9.6.3, and the only additional condition 9.7.4 is automatically satisfied by 9.9.2. The same holds if $r \equiv 1 \pmod 9$, even if we must then have $b \not\equiv 0 \pmod 3$ in case II (but still of course $b \equiv 0$ in case I, i.e. when $3 \mid Z$).

We note that there is no equation 9.4.4 if $A = R$. The descent of § 5 is *a priori* possible only if $r \equiv 1 \pmod 9$.

2. $\underline{A = 3R, \text{ where } 3(R)r}$ (the complement of 9.8.5): We have case I, with $A_1 = 3$, $A_2 = 9$, and the condition 9.7.6 is satisfied if $a + b\varrho$ is in primary form (cf. 9.1.4). Further $b^2 A_2 = 9\,b^2 \sim 3\,b^2(R)r$, so 9.7.4 also holds. — We note that in this case the one equation $x^3 + 3y^3 + Rz^3 = 0$ is possible for all moduli. The descent of § 5 is excluded.

3. $\underline{A = 9R}$: As in 2., we conclude that case I is possible if and only if $3(R)r$. In case III we have $A_2 = 1$, and the conditions 9.7.4 and 9.7.8 take the form

$$9.9.6 \qquad b^2(R)r, \quad b \equiv \pm 1 \pmod 9.$$

Let first $r \equiv 1 \pmod 9$, hence $3\, b^2(R)r$ for all forms of $a + b\varrho$. This contradicts the first condition 9.9.6 if $3(N)r$, i.e. the excluded case 9.9.1. If however $3(R)r$, i.e. $9 \mid b$ in the primary form, it follows from $R = N(a + b\varrho) = a^2 - ab + b^2 \equiv 1$ that $a \equiv \pm 1 \pmod 9$, i.e. b_1 and $b_2 \equiv \pm 1 \pmod 9$ in the two non-primary forms 9.9.3, which are consequently both possible for all moduli.

Let next $r \equiv 4$ or $7 \pmod 9$, in which case we have seen from 9.9.4 that the three possibilities for b all belong to different classes mod r; hence only one of them satisfies the first condition 9.9.6. If this is the primary form, i.e. if and only if $3(R)r$, the conditions 9.9.6 give a contradiction; but then case I is possible for all moduli. — It remains to show that both conditions 9.9.6 are satisfied *simultaneously* if $3(N)r$.

We suppose that $\underline{R = r}$, and let $\pi_r = a_1 + b_1\varrho$ be the primary form in the strict sense 9.1.1. We must use one of the non-primary forms $a + b\varrho$ defined by $a_1 + b_1\varrho = \varrho^i(a + b\varrho)$, $i = 1$ or 2. It follows from 9.9.4 that

$$9.9.7 \qquad \left[\frac{b}{a_1 + b_1\varrho}\right] = \left[\frac{\varrho^i b_1}{a_1 + b_1\varrho}\right] = \left[\frac{b_1}{a_1 + b_1\varrho}\right] \cdot \varrho^{i \cdot \frac{r-1}{3}},$$

cf. 9.1.3. On the other hand, it follows from 9.9.2 and 9.1.4 that

$$\left[\frac{3\, b_1^2}{a_1 + b_1\varrho}\right] = 1, \text{ i.e. } \left[\frac{b_1}{a_1 + b_1\varrho}\right] = \left[\frac{3}{a_1 + b_1\varrho}\right] = \varrho^{\frac{2b_1}{3}}, \quad \left[\frac{b}{a_1 + b_1\varrho}\right] = \varrho^{\frac{i(r-1)+2b_1}{3}},$$

where i must be chosen so that this expression equals 1 (since $b(R)r$ by the first condition 9.9.6), hence

$$i(r - 1) + 2\, b_1 \equiv 0 \pmod 9.$$

We have supposed $r \equiv 4$ or $7 \pmod 9$, $b_1 \equiv 0 \pmod 3$ but $\not\equiv 0 \pmod 9$ (since $3(N)r$), and get the four possible combinations (all congruences are taken mod 9):

$$r \equiv 4,\ b_1 \equiv 3,\ i = 1,\ a_1 \equiv -1; \quad r \equiv 4,\ b_1 \equiv -3,\ i = 2,\ a_1 \equiv -4;$$

$$r \equiv 7,\ b_1 \equiv 3,\ i = 2,\ a_1 \equiv 2 \quad ; \quad r \equiv 7,\ b_1 \equiv -3,\ i = 1,\ a_1 \equiv -1.$$

I have added the corresponding residues of a_1, which are uniquely determined from $r = N(a_1 + b_1\varrho) = a_1^2 - a_1 b_1 + b_1^2 \equiv a_1^2 - a_1 b_1 \pmod 9$ and $a_1 \equiv -1 \pmod 3$ (by 9.1.1). It follows from 9.9.3 that $b = -a_1$ if $i = 1$ and $b = a_1 - b_1$ if $i = 2$, hence in all cases $b \equiv \pm 1 \pmod 9$, which is the second condition 9.9.6.

I omit the case $R = r^2$; only a slight modification of the above proof is necessary.

We finally note that when $A = 9R$, the descent of § 5 is *a priori* possible if $r \equiv 1 \pmod 9$, and the one equation $x^3 + 9y^3 + Rz^3 = 0$ is possible for all moduli if also the additional condition $3 \mid (R)r$ is satisfied.

4. We now turn to the complement of 9.8.6, where $A = QR$. Let first $A \not\equiv \pm 1 \pmod 9$, $q \mid (R)r$. We must have the primary form $b \equiv 0 \pmod 3$, and

$$q \mid (R)r \to \left[\frac{a + b\varrho}{q}\right] = \left[\frac{q}{a + b\varrho}\right] = 1,$$

so 9.7.2 is satisfied. Further $A_1 = Q$, $A_2 = 3Q$ (case I or II), and 9.7.4 takes the form $3b^2 \mid Q(R)r$, which is also satisfied by 9.9.2 and $q \mid (R)r$. — We note that the equation 9.8.3 is possible for all moduli (the combination 2.1.2 implies $A \equiv \pm 1 \pmod 9$), but the descent of § 5 is excluded.

Let next $A \equiv \pm 1$, $q \equiv -1$, $r \equiv +1 \pmod 9$. The case $q \mid (N)r$ is already dealt with in 9.8.7. If $q \mid (R)r$, we conclude as above that case I ($3 \mid b$) and case II ($3 \nmid b$) both satisfy the conditions 9.7.2 and 9.7.4; in case II this follows from $\left[\frac{\varrho}{q}\right] = 1$ and 9.9.4. Further the descent of § 5 is *a priori* possible; the equation 9.8.3 is possible for all moduli if $q \mid (R)r$.

Let finally $A \equiv \pm 1$, q and $r \not\equiv \pm 1 \pmod 9$. The one equation 9.6.3 then represents *the only possible descent* (since 9.8.3 has the form 2.1.2). We notice that 9.9.2 is satisfied only if $3 \mid b$, and that $\left[\frac{\varrho}{q}\right] \neq 1$, hence only one form of $a + b\varrho$ is possible in 9.7.2. This is the primary form (case I only) if $q \mid (R)r$, and the condition 9.7.4, $3b^2 \mid Q(R)r$, is then also satisfied.

If however $q \mid (N)r$, the only possible form of $a + b\varrho$ is non-primary (case II only), $3b^2 \mid (N)r$, and the difficulty lies in showing that the condition 9.7.2 implies 9.7.4 also in this case:

9.9.8 $$\left[\frac{a + b\varrho}{q}\right] = 1 \to 3b^2 \mid Q(R)r.$$

As under 3. above, we introduce the primary form $a_1 + b_1\varrho = \varrho^i(a + b\varrho)$, $i = 1$ or 2; further $Q = q^j$, $j = 1$ or 2, and let first $R = r$, $\pi_r = a_1 + b_1\varrho$. We suppose that i is chosen so that the first condition 9.9.8 is satisfied, and shall deduce the second one:

$$\left[\frac{3b^2Q}{a_1+b_1\varrho}\right] = \left[\frac{3}{a_1+b_1\varrho}\right]\cdot\left[\frac{b}{a_1+b_1\varrho}\right]^2\cdot\left[\frac{q}{a_1+b_1\varrho}\right]^j, \text{ where}$$

$$\left[\frac{q}{a_1+b_1\varrho}\right] = \left[\frac{a_1+b_1\varrho}{q}\right] = \left[\frac{a+b\varrho}{q}\right]\cdot\left[\frac{\varrho}{q}\right]^i = 1\cdot\varrho^{i\cdot\frac{q^2-1}{3}} \text{ (by 9.1.3)},$$

$$\left[\frac{b}{a_1+b_1\varrho}\right] = \left[\frac{b_1}{a_1+b_1\varrho}\right]\cdot\varrho^{i\cdot\frac{r-1}{3}} \text{ (by 9.9.7), and so}$$

$$\left[\frac{3b^2Q}{a_1+b_1\varrho}\right] = \left[\frac{3b_1^2}{a_1+b_1\varrho}\right]\cdot\varrho^{ij\cdot\frac{q^2-1}{3}+2i\cdot\frac{r-1}{3}} = 1\cdot\varrho^{i\cdot\frac{j(q^2-1)+2(r-1)}{3}}$$

by 9.9.2, since $3\,|\,b_1$. But for all possible combinations of j, q and r such that $A = q^j r \equiv \pm 1 \pmod 9$:

$$q \equiv 2,\ r \equiv 4,\ j = 1; \quad q \equiv 2,\ r \equiv 7,\ j = 2;$$
$$q \equiv 5,\ r \equiv 4,\ j = 2; \quad q \equiv 5,\ r \equiv 7,\ j = 1,$$

it is seen that

$$j(q^2-1) + 2(r-1) \equiv 0 \pmod 9, \text{ i.e. } \left[\frac{3b^2Q}{a_1+b_1\varrho}\right] = 1,\ 3b^2Q(R)r,$$

q.e.d. — In the case $R = r^2$, it is easily verified that the numerator of the exponent is replaced by $j(q^2-1) + (r-1)$, which is $\equiv 0 \pmod 9$ for the combinations of q, r and j which now occur.

For later use, I shall also quote another result which is proved in exactly the same way: If $R = N(a+b\varrho) \equiv \pm Q \pmod 9$, then

9.9.9 $$\left[\frac{a+b\varrho}{q}\right] = 1 \to 3b^2Q^2(R)r.$$

As above, this result is an immediate consequence of 9.9.2 only if $q(R)r$.

5. The last case is $\underline{A = R_1R_2}$, $R_1 = r_1$ or r_1^2, $R_2 = r_2$ or r_2^2. There are then *four a priori* possible values for $a + b\varrho$:

9.9.10 $$\pi_{r_1},\ \pi_{r_2},\ \pi_{r_1}\pi_{r_2} \text{ and } \pi_{r_1}\bar{\pi}_{r_2},$$

possibly with *squared* factors. (The conjugate values need not be treated separately by 2. of § 6.) There are many possibilities to consider, and I shall only indicate that *the primary form can never be completely excluded.* The condition 9.7.5, $b \equiv 0 \pmod 3$, is satisfied for the combinations 9.9.10 if π_{r_1} and π_{r_2} are in primary form, and we must show that the conditions 9.7.3—4 can then always be *simultaneously* satisfied.

It follows from 9.1.2 and 9.1.5 that the relations between π_{r_1}, π_{r_2}, $\bar{\pi}_{r_1}$ and $\bar{\pi}_{r_2}$ can be characterized by

9.9.11
$$\begin{cases} \left[\frac{\pi_{r_1}}{\pi_{r_2}}\right] = \left[\frac{\pi_{r_2}}{\pi_{r_1}}\right] = \varrho^{\alpha}, \quad \left[\frac{\pi_{r_1}}{\bar{\pi}_{r_2}}\right] = \left[\frac{\bar{\pi}_{r_2}}{\pi_{r_1}}\right] = \varrho^{\beta}, \\ \left[\frac{\bar{\pi}_{r_1}}{\pi_{r_2}}\right] = \left[\frac{\pi_{r_2}}{\bar{\pi}_{r_1}}\right] = \varrho^{-\beta}, \quad \left[\frac{\bar{\pi}_{r_1}}{\bar{\pi}_{r_2}}\right] = \left[\frac{\bar{\pi}_{r_2}}{\bar{\pi}_{r_1}}\right] = \varrho^{-\alpha}, \text{ i.e.} \end{cases}$$

$$\left[\frac{r_1}{\pi_{r_2}}\right] = \varrho^{\alpha-\beta}, \quad \left[\frac{r_1}{\bar{\pi}_{r_2}}\right] = \varrho^{\beta-\alpha}, \quad \left[\frac{r_2}{\pi_{r_1}}\right] = \varrho^{\alpha+\beta}, \quad \left[\frac{r_2}{\bar{\pi}_{r_1}}\right] = \varrho^{-(\alpha+\beta)}.$$

Three typical cases must be considered separately:

$\alpha \equiv \beta \not\equiv 0 \pmod 3$, so $r_1(R)r_2$, $r_2(N)r_1$. We can then use $a + b\varrho = \pi_{r_2}$, $A_2 = 3r_1$, since $b^2 A_2 = 3b^2 r_1 \sim 3b^2(R)r_2$ by 9.9.2, and $\frac{a+b\varrho}{a+b\varrho^2} = \frac{\pi_{r_2}}{\bar{\pi}_{r_2}}(R)r_1$ by 9.9.11.

$\alpha \not\equiv 0$, $\beta \equiv 0 \pmod 3$, so $r_1(N)r_2$, $r_2(N)r_1$. We can use $a + b\varrho = \pi_{r_1}\pi_{r_2}$, $A_2 = 3$, since $b^2 A_2 = 3b^2(R)r_1$ & r_2 by 9.9.5, and there is no condition 9.7.3 in this case.

$\alpha \equiv \beta \equiv 0 \pmod 3$, so $r_1(R_2)r_2$, $r_2(R)r_1$. Combining the arguments of the other cases, we see that all combinations 9.9.10 are possible. — This is the only case where the equation $x^3 + R_1 y^3 + R_2 z^3 = 0$ is possible for all moduli (if not of the type 2.1.2). The descent of § 5 is *a priori* possible only if $r_1 \equiv r_2 \equiv 1 \pmod 9$.

This concludes the proof of the enunciation at the beginning of this paragraph.

§ 10. We now turn to the cases where A contains *three different prime factors*. For simplicity, we will suppose that only one of these is an $r \equiv +1 \pmod 3$. We shall further consider systematically only those cases *where all four equations* 7.4.6 *can be proved impossible by elementary congruence considerations mod* 9 *and mod* r. (Otherwise we cannot formulate any general result about insolubility of $X^3 + Y^3 = AZ^3$.) We shall make use of the results for $n_A = 3$ in Ch. VII, § 4, without further reference.

If all four equations 7.4.6 are possible mod 9, then at least one of them will be possible mod r. In particular, this is the case if $3 \| A$. We therefore consider only the cases $9 \| A$ and $3 \nmid A$, and find those combinations for which only one equation 7.4.6 is possible mod 9.

1. $A = 9QR$, $Q = q$ or q^2, $R = r$ or r^2. Of the four equations

9.10.1
$$\{1, 9, QR\}, \quad \{1, Q, 9R\}, \quad \{1, R, 9Q\}, \quad \{9, Q, R\},$$

only one is possible mod 9 in the following cases:

9.10.2	$Q \equiv \pm 1,\ R \not\equiv \pm 1$	(mod 9) : $\{1,\ Q,\ 9R\}$;	$q(N)r$
9.10.3	$Q \not\equiv \pm 1,\ R \equiv +1$	(" ") : $\{1,\ R,\ 9Q\}$;	$9Q(N)r$
9.10.4	$QR \equiv \pm 1,\ Q\ \&\ R \not\equiv \pm 1$	(" ") : $\{1,\ 9,\ QR\}$;	$3(N)r$
9.10.5	$Q \equiv \pm R \not\equiv \pm 1$	(" ") : $\{9,\ Q,\ R\ \}$;	$3Q(N)r$.

The possible combination mod 9 is given in each case, and also the condition under which this is impossible mod r. — We shall see that the one *a priori* possible equation 9.6.3 is insoluble in all cases 9.10.2—5. Since this also holds for the equations 9.10.1, and since the descent of § 5 is clearly impossible in all cases, we conclude that *the corresponding values of* $A = 9QR$ *represent insoluble equations* $X^3 + Y^3 = AZ^3$.

The insolubility of 9.6.3 for the first form 9.10.2 follows at once from 9.8.2, since $q \equiv -1 \pmod 9$ and $q(N)r$. — For the other forms 9.10.3—5, we have the *a priori* cases I and III (since $9 \mid A$), and begin by showing that case I is impossible. Then $9 \mid b$, $3(R)r$ by 9.7.6, and as in the proof of 9.8.2 we also conclude that $q(R)r$. But these simultaneous conditions are not satisfied for any of the forms 9.10.3—5.

In case III we have $\frac{s}{3t} = \frac{1}{9}$, $A_1 = 9Q$, $A_2 = Q$, and the condition 9.7.4 becomes

$$b^2 Q(R)r.$$

The form 9.10.3 has $r \equiv 1 \pmod 9$, i.e. $3b^2(R)r$ for all forms of $a + b\varrho$ by 9.9.4. From this and $9Q(N)r$ we conclude that $3^3 b^2 Q \sim b^2 Q(N)r$, which is impossible.

For the form 9.10.4, the conditions of 9.9.8 hold. But from $3b^2 Q(R)r$ and $3(N)r$ we get the same impossibility $b^2 Q(N)r$. For 9.10.5, the formula 9.9.9 together with $3Q(N)r$ leads to the same result.

This concludes the proof, which implies the insolubility of the values A in 9.2.5 and 9.2.12 as special cases; the impossibility of the four equations 9.10.1 for these A is easily verified by 9.2.6—7 and 9.2.13. The values 9.2.5 have $q = 2$, with r varying (but not all possible primes r). The values 9.2.12 give *all* combinations with $r = 7$ and varying q.

2. $\underline{A = Q_1 Q_2 R}$: Of the four equations 7.4.6, one and only one is possible mod 9 in the following cases:

9.10.6 $Q_1 \equiv \pm 1,\ Q_2 R \equiv \pm 1,\ Q_2 \,\&\, R \not\equiv \pm 1 \pmod 9 : \{1,\ Q_1,\ Q_2 R\};\quad q_1(N)r$

9.10.7 $R \equiv +1,\ Q_1 Q_2 \equiv \pm 1,\ Q_1 \,\&\, Q_2 \not\equiv \pm 1$ (" ") : $\{1,\ R,\ Q_1 Q_2\};\ Q_1 Q_2(N)r$

9.10.8 $Q_1 \equiv \pm Q_2 \equiv \pm R \not\equiv \pm 1$ (" ") : $\{Q_1,\ Q_2,\ R\};\quad Q_1^2 Q_2(N)r,$

where as above the condition for insolubility mod r is added. We shall see that also here the corresponding equations 9.6.3, and thereby *the given equations* $X^3 + Y^3 = A Z^3$, *are insoluble.*

We note that 9.10.6—8 all have $A \equiv \pm 1 \pmod 9$, and the one equation 9.6.3 must be treated in the cases I and II, which both give $\frac{s}{3t} = 3$, $A_2 = 3 Q_1 Q_2$, and the condition 9.7.4:

$$3 b^2 Q_1 Q_2(R)r.$$

The impossibility of 9.10.6 follows at once from 9.8.2, since $q_1 \equiv -1 \pmod 9$ and $q_1(N)r$. — For 9.10.7 we conclude from 9.9.4 and $r \equiv 1 \pmod 9$ that $3 b^2(R)r$ for all forms of $a + b\varrho$, which together with $Q_1 Q_2(N)r$ gives the impossibility $3 b^2 Q_1 Q_2(N)r$. Finally 9.9.9 shows that for 9.10.8 we have $3 b^2 Q_1^2(R)r$, which together with $Q_1^2 Q_2(N)r$ gives the same impossibility.

This concludes the proof, which implies the insolubility of the values A in 9.2.10—11, giving *all* cases with $q_1 = 2$, $r = 7$ and varying q_2. The impossibility of the corresponding four equations 7.4.6 is easily verified by 9.2.13.

As already mentioned, the case $3 \parallel A$, $A = 3 Q R$, will lead to at least one equation 7.4.6 which is possible for all moduli. We can therefore express the above results in the simple and general

Theorem XII. *Let A (cubefree) contain three different prime factors, one and only one of which is an $r \equiv +1 \pmod 3$. The equation $X^3 + Y^3 = A Z^3$ has then only the trivial solution with $Z = 0$ if the four possible equations*

9.10.9 $a x^3 + b y^3 + c z^3 = 0,\quad a b c = A,\quad 1 \leqq a < b < c,\quad (a, b) = (a, c) = (b, c) = 1,$

can all be excluded by elementary congruence considerations mod 9 and mod r.

The insoluble cubefree values of $A \leqq 500$ covered by this theorem are given in *Table 4[d]*.

§ 11. If A has three different prime factors, of which at least two are primes $r \equiv +1 \pmod 3$, Th. XII does no longer hold. Simple counter-examples of different types are

$$A = 9 \cdot 7 \cdot 37 = 2331 = 10^3 + 11^3$$
$$A = 2 \cdot 13 \cdot 19 = 494 = \left(\frac{59}{7}\right)^3 - \left(\frac{33}{7}\right)^3$$
$$A = 7 \cdot 13 \cdot 19 = 1729 = 1^3 + 12^3,$$

for which it is easily verified that all four equations 7.4.6 can be excluded by elementary congruence considerations in each case; the descent of § 5 is equally impossible.

One can prove some general results also when A has two prime factors r. I omit this here, and will just indicate the methods by treating those $A \leqq 500$ which can be proved impossible. In each case the four equations 7.4.6 and the descent of § 5 are easily excluded. We must consider the four *a priori* possible combinations 9.9.10 for $a + b\varrho$ in the equation 9.6.3.

1. $A = 266 = 2 \cdot 7 \cdot 19$: Since $A \equiv -4 \pmod 9$, we must use case I, with the *primary* form of $a + b\varrho$. From $2\,(N)\,7$, $2\,(N)\,19$ we see that $a + b\varrho = \pi_7$ or π_{19} is excluded by 9.8.2. Since

$$\left[\frac{\pi_7}{2}\right] = \left[\frac{1 + 3\varrho}{2}\right] = \left[\frac{1 + \varrho}{2}\right] = \left[\frac{\varrho^2}{2}\right] = \varrho^2, \quad \left[\frac{\pi_{19}}{2}\right] = \left[\frac{2 - 3\varrho}{2}\right] = \left[\frac{\varrho}{2}\right] = \varrho,$$

the only combination 9.9.10 which satisfies 9.7.2 is

$$a + b\varrho = \pi_7 \cdot \pi_{19} = (1 + 3\varrho)(2 - 3\varrho) = 11 + 12\varrho.$$

But $A_1 = 2$, $A_2 = 3 \cdot 2$, and $b^2 A_2 = 2^5 \cdot 3^3 \sim 2^2$ is a cubic non-residue of both 7 and 19; the condition 9.7.4 is consequently not satisfied.

In exactly the same way we can exclude $A = 364 = 2^2 \cdot 7 \cdot 13$, where $2\,(N)\,7$ and $2\,(N)\,13$.

2. $A = 434 = 2 \cdot 7 \cdot 31 \equiv 2 \pmod 9$, so we must use the primary form of $a + b\varrho$. Again $2\,(N)\,7$, but $2\,(R)\,31$, which shows that the only possibility satisfying 9.7.2 is

$$a + b\varrho = \pi_{31} = 1 + 6\varrho.$$

Here $A_1 = 2 \cdot 7$, $A_2 = 3 \cdot 2 \cdot 7$, $b^2 A_2 = 6^3 \cdot 7 \sim 7\,(N)\,31$, contrary to 9.7.4. — The impossibility of $a + b\varrho = 1 + 6\varrho$ could also have been shown by the condition 9.7.3:

$$\frac{a + b\varrho}{a + b\varrho^2} = \frac{1 + 6\varrho}{1 + 6\varrho^2} \equiv \frac{1 - \varrho}{1 - \varrho^2} = \frac{1}{1 + \varrho} = -\varrho \pmod 7,$$

i.e. a cubic non-residue of 7.

The insolubility of $A = 455 = 5 \cdot 7 \cdot 13$, where $5\,(N)\,7$, $5\,(R)\,13$, is proved in the same way. — The four values of A found in this paragraph are listed in *Table 4e*. They are all particular cases of the following general result: $A = Q R_1 R_2 \not\equiv \pm 1 \pmod 9$ *is insoluble if the four possible equations* 9.10.9 *can all be excluded by elementary congruence conditions mod* r_1 *and* r_2. (The conditions mod 9 are always satisfied when $A \not\equiv 0$ and $\pm 1 \pmod 9$.)

The Tables 4^{c-e} contain the values of $A \leqq 500$ for which the equation 9.6.3 can be proved insoluble by congruence considerations only. By extending the methods of Ch. VIII to this equation (§§ 12—14 below), we can prove the insolubility of a few more values of A, given in Table 4^f. Finally a complete list of the excluded values of A in Tables 4^{a-f} is reproduced in *Table 4g*; these are *all the cubefree values of* $A \leqq 500$ *which have been proved insoluble in the present paper* (indeed so far as I know all which have been proved insoluble at all).

The non-excluded equations 9.6.3 for $A \leqq 500$, corresponding to all possible descents 9.6.1, are listed in *Table 5*. It follows from § 6, 2. that conjugate values $a + b\varrho$ and $a + b\varrho^2$ need not be considered separately. The case $a + b\varrho = \varrho$ (§ 5) is covered by Table 3, and consequently not repeated.

A solution is found in nearly all cases of Table 5. The only unsolved equations represent the following values of A:

9.11.1 $\qquad 283,\ 337,\ 409,\ 499$ (all primes); $473 = 11 \cdot 43$.

The corresponding equations 9.6.3 (all of *case I*) are possible for all moduli, and cannot be excluded by the methods of §§ 12—14 below. I believe that they are all soluble.

In order to find the solutions of Table 5, I have computed the cubic forms

9.11.2 $$uv(u - v) \quad \text{and} \quad u^3 - 3u^2v + v^3$$

for several pairs of values u, v. It suffices to use the pairs such that for instance

$$0 \leqq v \leqq u, \quad (u, v) = 1,$$

since a change of sign for u and v does not influence the calculations, and the *automorphisms* of both forms 9.11.2 are (cf. 8.1.11):

9.11.3 $$u' = -v,\ v' = u - v; \quad u'' = v - u,\ v'' = -u.$$

This follows at once from 9.6.1, which is unaltered if we replace $u + v\varrho$ by

$$\varrho(u + v\varrho) = -v + (u - v)\varrho \quad \text{or} \quad \varrho^2(u + v\varrho) = v - u - u\varrho.$$

Because of the automorphisms, it is also possible to choose a solution with u, v and w *all positive* (or zero. The condition $v \leqq u$ must then be abandoned.) This is done in Table 5, cf. the concluding remark of Ch. VIII, § 3. — By an appropriate choice between the two conjugate values of $a + b\varrho$, we can also get a and b both positive in all cases.

The choice of u and v in an equation 9.6.3 can always be limited also by simple *congruence considerations*, which greatly facilitate the search for solutions.

§ 12. When A is a prime $r \equiv +1 \pmod 9$, or the square of such a prime, it follows from § 9, 1. that there are *three* different equations 9.6.3 which are possible for all moduli (*four* if we include 9.5.3, corresponding to $a + b\varrho = \varrho$. As usual, conjugate values $a + b\varrho$ and $a + b\varrho^2$ are not considered separately.) These equations for the *excluded* values (crosses) of Table 3 are given by (— before ϱ and ϱ^2 is included for convenience):

9.12.1
$$\begin{cases}
A = 73 : a+b\varrho = 1+9\varrho, & -\varrho(1+9\varrho) = 9+8\varrho \text{ and } -\varrho^2(1+9\varrho) = -8+ \\
A = 109 : a+b\varrho = 5+12\varrho, & -\varrho(5+12\varrho) = 12+7\varrho \text{ " } -\varrho^2(5+12\varrho) = -7+ \\
A = 181 : a+b\varrho = 4+15\varrho, & -\varrho(4+15\varrho) = 15+11\varrho \text{ " } -\varrho^2(4+15\varrho) = -11+ \\
A = 199 : a+b\varrho = 2+15\varrho, & -\varrho(2+15\varrho) = 15+13\varrho \text{ " } -\varrho^2(2+15\varrho) = -13+ \\
A = 307 : a+b\varrho = 1+18\varrho, & -\varrho(1+18\varrho) = 18+17\varrho \text{ " } -\varrho^2(1+18\varrho) = -17+ \\
A = 487 : a+b\varrho = -2+21\varrho, & -\varrho(-2+21\varrho) = 21+23\varrho \text{ " } \varrho^2(-2+21\varrho) = 23+ \\
A = 19^2 : a+b\varrho = 5+21\varrho, & -\varrho(5+21\varrho) = 21+16\varrho \text{ " } -\varrho^2(5+21\varrho) = -16+
\end{cases}$$

In all cases $A_1 = 1$, i.e. $A_2 = 3$. The first value of $a + b\varrho$ for each A corresponds to case I (primary form), the last two to case II (non-primary form).

None of these equations have simple solutions, and we shall see that *they can all be proved insoluble by an extension of the methods of Ch. VIII.* This implies that the corresponding values of A are also insoluble (*Table 4*).

We must distinguish between primary and non-primary forms. In the primary case we put $b = 3b_1$, and can remove a common factor 3 in the equation 9.6.3 $\left(\frac{s}{3t} = 3 \text{ in case I and II}\right)$. Multiplication by b_1^2 and the substitution $\underline{b_1 u = u_1}$ will transform this equation into

9.12.2
$$u_1^3 + (a - 3b_1)u_1^2 v - a b_1 u_1 v^2 + b_1^3 v^3 = b_1^2 A_1 w^3$$

(we consider the general case, with $A_1 \geqq 1$).

We shall treat this equation in the corresponding *non-purely* cubic field $K(\xi)$ defined by

9.12.3 $$\xi^3 + (a - 3b_1)\xi^2 - ab_1\xi + b_1^3 = 0.$$

The discriminant of this equation,

$$d(\xi) = \{b_1 \cdot N(a + 3b_1\varrho)\}^2,$$

is a perfect square (cf. 9.7.9), and $K(\xi)$ is consequently a *Galois field*; this also follows from the *automorphisms* 9.11.3.

We can obtain a *basis* for the integers of the field $K(\xi)$ by the method of Woronoj; an account of this is given in Sommer [1], pp. 257—62. An application to 9.12.3 shows that the basis is given by

9.12.4 $$\left(1, \xi, \omega = \frac{a\xi + \xi^2}{b_1}\right),$$

provided $N(a + 3b_1\varrho)$ is *squarefree* and $(a, b_1) = 1$. If $r^2 \| N(a + 3b_1\varrho)$, the prime r will occur in the denominator of ω, and the determination of the numerator becomes more complicated. I leave it out here; the only actual case of 9.12.1 is $A = -19^2$.

If $N(a + 3b_1\varrho)$ is squarefree, the discriminant of the *field* $K(\xi)$ is given by

9.12.5 $$\Delta = N(a + 3b_1\varrho)^2.$$

The *conjugates* of an integer $\alpha = x + y\xi + z\omega$ are

9.12.6 $$\begin{cases} \alpha' = x + 2b_1 y + (a + 5b_1)z + (2y + 7z)\xi - (y + 3z)\omega \\ \alpha'' = x + (b_1 - a)y + (-2a + 4b_1)z - (3y + 7z)\xi + (y + 2z)\omega. \end{cases}$$

The rules of multiplication take the form

9.12.7 $$\begin{cases} \xi^2 = -a\xi + b_1\omega, \quad \xi\omega = -b_1^2 - 2a\xi + 3b_1\omega, \\ \omega^2 = -ab_1 - 3b_1^2 - (6a + b_1)\xi + (a + 9b_1)\omega, \end{cases}$$

and lead to the important formulae

9.12.8 $$\begin{cases} \alpha\alpha'\alpha'' = N(\alpha) = N(x + y\xi + z\omega) = x^3 + (-a + 3b_1)x^2y - ab_1xy^2 - \\ - b_1^3y^3 + (-a + 9b_1)x^2z + (-2a^2 + ab_1 + 6b_1^2)xz^2 + \\ + (-2a^2b_1 + b_1^3)z^3 - (2ab_1^2 + 3b_1^3)y^2z - (a^2b_1 + 5ab_1^2)yz^2 - \\ - (a^2 + 3ab_1 - 3b_1^2)xyz, \end{cases}$$

9.12.9
$$\begin{cases} a^3 = (x + y\xi + z\omega)^3 = x^3 - b_1^3 y^3 - 3(a b_1 + 3 b_1^2) x z^2 - 9 b_1^3 y^2 z - \\ - 3(a b_1^2 + 9 b_1^3) y z^2 - (a^2 b_1 + 6 a b_1^2 + 26 b_1^3) z^3 - 6 b_1^2 x y z + \\ + \{3 x^2 y - 3 a x y^2 + (a^2 - 2 a b_1) y^3 - 3(6 a + b_1) x z^2 + \\ + 3(2 a^2 - 6 a b_1 - b_1^2) y^2 z + 3(4 a^2 - 18 a b_1 - 3 b_1^2) y z^2 + \\ + (6 a^2 - 53 a b_1 - 9 b_1^2) z^3 - 12 a x y z\} \cdot \xi + \{3 b_1 x y^2 + \\ + (- a b_1 + 3 b_1^2) y^3 + 3 x^2 z + 3(a + 9 b_1) x z^2 + 3(- 2 a b_1 + 9 b_1^2) y^2 z + \\ + 3(- 3 a b_1 + 26 b_1^2) y z^2 + (a^2 - a b_1 + 75 b_1^2) z^3 + 18 b_1 x y z\} \cdot \omega. \end{cases}$$

The natural primes r such that $r \mid \Delta$ are cubes of ideals in $K(\xi)$:

9.12.10
$$[r] = \left[r,\ \xi + \frac{a - 3 b_1}{3},\ \omega + \frac{a - 9 b_1}{3}\right]^3 = \mathfrak{p}_r^3.$$

All other primes either remain primes or factorize into *three different, conjugate ideals*:

9.12.11
$$[p] = [p,\ \xi - d] \cdot [p,\ \xi - d'] \cdot [p,\ \xi - d''] = \mathfrak{p}_p \mathfrak{p}_p' \mathfrak{p}_p'',$$

where d, d' and d'' are the solutions of the congruence mod p corresponding to 9.12.3, and where

$$d' \equiv - \frac{b_1 (b_1 - d)}{d}, \quad d'' \equiv \frac{b_1^2}{b_1 - d} \pmod{p}.$$

If in particular $p \mid b_1$, we get the factors

9.12.12
$$\begin{cases} \mathfrak{p}_p = [p, \xi, \omega], \quad \mathfrak{p}_p' = [p, \xi + a, \omega + 2a], \quad \mathfrak{p}_p'' = [p, \xi, \omega - a], \\ \text{where} \quad \mathfrak{p}_p \mathfrak{p}_p'' = [p, \xi]. \end{cases}$$

This also holds for $p = 3$, which remains a prime if $3 \nmid b_1$.

Only slight modifications are necessary if we consider a *non-primary* form of $a + b\varrho$, i.e. $3 \nmid b$. No common factor 3 can then be removed in the equation 9.6.3, which after multiplication by b^2 and the substitution $bu = u_1$ now takes the form

9.12.13
$$u_1^3 + 3(a - b) u_1^2 v - 3 a b u_1 v^2 + b^3 v^3 = 3 b^2 A_1 w^3$$

$\left(\text{or } = \frac{1}{9} b^2 A_1 w^3 \text{ in case III}\right)$, leading to a field $K(\xi)$ defined by

9.12.14
$$\xi^3 + 3(a - b)\xi^2 - 3 a b \xi + b^3 = 0.$$

Most of the earlier conclusions and formulae are still valid *if a is replaced by $3a$ and b_1 by b throughout.* The discriminant of 9.12.5 should now be written as

9.12.15 $$\Delta = 3^4 \cdot N(a + b\varrho)^2,$$

and the natural prime 3 *is now a perfect cube:*

9.12.16 $$[3] = [3, \xi + b, \omega - b]^3 = \mathfrak{p}_3^3, \quad \text{where} \quad \mathfrak{p}_3^2 = [3, \xi - \omega - b].$$

Since the discriminant $\Delta > 0$, the fields $K(\xi)$ have *two fundamental units* ε_1 *and* ε_2, which can be chosen as *conjugates.*

§ 13. We now form the *ideal-equation* corresponding to 9.12.2 or 9.12.13:

9.13.1 $$[u_1 - v\xi] = \mathfrak{n}\mathfrak{a}^3,$$

where $\mathfrak{n}$ is an ideal from a finite set, such that Norm $\mathfrak{n} = b_1^2 A_1$ (primary form), $= 3b^2 A_1$ (non-primary form in case II) or $= \frac{1}{9} b^2 A_1$ (non-primary form in case III). The prime factors of A_1 are easily dealt with in the usual way. It is further clear that $\mathfrak{p}_3 \| \mathfrak{n}$ for the non-primary form in case II, since 9.12.16 shows that $\mathfrak{p}_3^2$ cannot divide $[u_1 - v\xi]$ if $3 \nmid u_1$ and v. But the prime factors of b (if any) need a special treatment. This is the same for the primary and the non-primary form, and I give the formulae in the former case only.

It is quite possible that a solution (u, v) of the original equation 9.6.3 has a common factor of v and b_1. All such solutions occur in triplets of conjugates (by 9.11.3), and we can always choose one solution of each triplet such that $(v, b_1) = 1$, at least *provided b_1 has at most two different prime factors* (this holds in all cases 9.12.1). With this limitation, and because of the substitution $u_1 = b_1 u$, we may therefore suppose that

9.13.2 $$u_1 - v\xi \equiv -v\xi \pmod{b_1}, \quad (v, b_1) = 1.$$

Let p be any prime such that $p \mid b_1$. From 9.12.12, 9.13.2 and $p \nmid a$ we conclude that

$$\mathfrak{p}_p \mathfrak{p}_p'' \mid [u_1 - v\xi], \quad \text{but} \quad \mathfrak{p}_p' \nmid [u_1 - v\xi].$$

Further, if $p \| b_1$:

$$\mathfrak{p}_p^2 \mathfrak{p}_p''^2 = [p^2, \xi^2 = -a\xi + b_1\omega] \nmid [u_1 - v\xi],$$

from which we conclude that $\mathfrak{p}_p$ and $\mathfrak{p}_p'' \| \mathfrak{n}$, since additional powers of $\mathfrak{p}_p$ *or* $\mathfrak{p}_p''$ must occur with such exponents that they can be absorbed in $\mathfrak{a}^3$.

If $p^2 \| b_1$, it follows that

$$\mathfrak{p}_p^2 \mathfrak{p}_p''^2 = [p^2, \xi] \,|\, [u_1 - v\xi], \quad \text{but} \quad \mathfrak{p}_p^3 \mathfrak{p}_p''^3 = [p^3, -a\xi + b_1\omega] \nmid [u_1 - v\xi],$$

and so $\mathfrak{p}_p^2$ and $\mathfrak{p}_p''^2 \| \mathfrak{n}$. So far the choice of ideal factors from b_1 is unique.

If however $p^3 \| b_1$, i.e.

$$\mathfrak{p}_p^3 \mathfrak{p}_p''^3 = [p^3, \xi] \,|\, [u_1 - v\xi], \quad \text{but} \quad \mathfrak{p}_p^4 \mathfrak{p}_p''^4 = [p^4, -a\xi + b_1\omega] \nmid [u_1 - v\xi],$$

there are *three* possibilities for the choice of corresponding factors in $\mathfrak{n}$:

1. $\mathfrak{p}_p^3$ and $\mathfrak{p}_p''^3 \| \mathfrak{n}$ (as before)
2. $\mathfrak{p}_p^6 \| \mathfrak{n}$, $\mathfrak{p}_p'' \nmid \mathfrak{n}$, $\mathfrak{p}_p'' \| \mathfrak{a}$
3. $\mathfrak{p}_p''^6 \| \mathfrak{n}$, $\mathfrak{p}_p \nmid \mathfrak{n}$, $\mathfrak{p}_p \| \mathfrak{a}$.

The factors of $\mathfrak{n}$ are all *cubed*, and can consequently be absorbed in $\mathfrak{a}^3$. But to get analogy with the earlier formulae, we may suppose that we have case 1. This differs from 2. and 3. only by cubes of ideals, and will also cover these cases by the principle of "*auxiliary cubes*".

A similar argument applies also when b_1 contains a prime p to still higher powers. $\mathfrak{n}$ will contain the product $\mathfrak{p}_{b_1} \mathfrak{p}_{b_1}''$, if we define

$$\mathfrak{p}_{b_1} = \prod_{p^i \| b_1} \mathfrak{p}_p^i.$$

The ideal $\mathfrak{n}$ *of* 9.13.1 *is therefore uniquely determined if* A_1 *has at most one prime factor* (cf. the remarks to 8.2.1). In particular, $A_1 = 1$ in 9.12.1, and consequently

9.13.3 $\quad \mathfrak{n} = \mathfrak{p}_{b_1} \mathfrak{p}_{b_1}''$ (primary form) or $= \mathfrak{p}_3 \mathfrak{p}_b \mathfrak{p}_b''$ (non-primary form)

(where b_1 is replaced by b for the latter form).

As in Ch. III, § 5, it is also here possible to exclude some of the equations 9.12.1 by *class-number considerations*, namely the non-primary cases for $A = 73$ and 307 (the only primes where $3 \,(R)\, A$, i.e. $3 \,|\, b_1$ in the primary form). In both cases for $A = 73$ and in the first non-primary case for $A = 307$, we find *a class-number* $h = 9$, *with a non-cyclic group of classes*. Hence $\mathfrak{a}^3$ of 9.13.1 is a principal ideal, and the same turns out to be the case for $\mathfrak{p}_b$ and $\mathfrak{p}_b''$. But $\mathfrak{p}_3$ is non-principal, and the equations are consequently insoluble. The exclusion is similar in the last case for $A = 307$ ($b = 1$ **and** $\mathfrak{p}_3$ non-principal), but the class-number

is $h = 63$, the group of ideal-classes having two generators of order 3 and one of order 7.

When the equation 9.13.1 cannot be excluded by class-number considerations, we are as usual led to several equations between *integers* of $K(\xi)$. — In all *primary* forms of 9.12.1 we find $h = 1$, and get at once:

$$9.13.4 \qquad u_1 - v\xi = \varepsilon_1^i \varepsilon_2^j \nu \alpha^3 = \mu \alpha^3, \quad i \text{ and } j = 0, 1, 2,$$

where ε_1 and ε_2 are two fundamental units, and $\mathfrak{n} = \mathfrak{p}_{b_1} \mathfrak{p}_{b_1}'' = [\nu]$. — In all *non-primary* forms, except for $A = 73$ and 307, we find $h = 3$. We must consequently introduce a γ as in 3.8.3:

$$9.13.5 \qquad u_1 - v\xi = \varepsilon_1^i \varepsilon_2^j \gamma^k \nu \alpha^3 = \mu \alpha^3, \quad i, j \text{ and } k = 0, 1, 2,$$

where $\mathfrak{n} = \mathfrak{p}_3 \mathfrak{p}_b \mathfrak{p}_b'' = [\nu]$, and $[\gamma]$ is the cube of any ideal which is not a principal ideal. Such an equation can be treated to any modulus prime to γ.

When $h = 3$, three conjugate ideals (e.g. $\mathfrak{p}_b$, $\mathfrak{p}_b'$ and $\mathfrak{p}_b''$) will always be equivalent. Consequently $\mathfrak{n} = \mathfrak{p}_3 \mathfrak{p}_b \mathfrak{p}_b''$ is principal if and only if $\mathfrak{p}_3$ and $\mathfrak{p}_b$ belong to the same class, which is *non-principal* in all the non-primary cases mentioned above ($A \neq 73$ and 307). This leads to *a quick and general determination of* γ, since it is easily verified that

$$\mathfrak{p}_b^2 \mathfrak{p}_b'' = [-\xi], \quad \mathfrak{p}_b \mathfrak{p}_b''^2 = [-b + \xi], \quad \text{i.e. } (\mathfrak{p}_b \mathfrak{p}_b'')^3 = [\xi(b - \xi)],$$

and we can choose

$$9.13.6 \qquad \gamma = \xi(b - \xi) = (3a + b)\xi - b\omega.$$

We conclude this paragraph with an important remark about the fundamental units ε_1 and ε_2, where we can suppose $\varepsilon_1 = \varepsilon$, $\varepsilon_2 = \varepsilon'$, and where $\varepsilon'' = (\varepsilon \varepsilon')^{-1}$ (since $N(\varepsilon) = \varepsilon \varepsilon' \varepsilon'' = 1$). Under what conditions can two other units

$$\eta = \varepsilon^m \varepsilon'^n \quad \text{and} \quad \eta' = \varepsilon'^m \varepsilon''^n = \varepsilon^{-n} \varepsilon'^{m-n}$$

be used as fundamental units? This implies that $\eta^x \eta'^y = \varepsilon^i \varepsilon'^j$, or

$$9.13.7 \qquad mx - ny = i, \quad nx + (m - n)y = j,$$

must be soluble in integers x and y for all integer pairs (i, j), i.e. that the determinant

$$9.13.8 \qquad \begin{vmatrix} m & -n \\ n & m - n \end{vmatrix} = m^2 - mn + n^2 = N(m + n\varrho) = 1.$$

This gives $m + n\varrho = \pm 1$, $\pm\varrho$ or $\pm\varrho^2 = \mp(1 + \varrho)$, and so

$$\eta = \varepsilon^{\pm 1}, \quad (\varepsilon')^{\pm 1} \quad \text{or} \quad (\varepsilon\,\varepsilon')^{\mp 1} = (\varepsilon'')^{\pm 1},$$

i.e. only trivial cases.

When however ε_1 and ε_2 are to be used in equations such as 9.13.4—5, it will clearly suffice to replace the equations 9.13.7–8 by *congruences mod* 3 (cf. the remarks to 3.6.2). And $N(m + n\varrho) \equiv 1 \rightleftarrows m + n \not\equiv 0 \pmod 3$. If we form the ratio

$$\frac{\eta}{\eta'} = \varepsilon^{m+n} \cdot \varepsilon'^{2n-m},$$

this will be the cube of another unit if and only if $m + n \equiv 0 \pmod 3$. *Any unit* η *such that* $\frac{\eta}{\eta'}$ *is a cubic non-residue to an appropriate modulus will therefore suffice for our purpose.*

§ 14. We must study the possibilities of excluding equations of the type 9.13.4—5. It is not difficult to see that no prime factor $\neq 3$ of the discriminant 9.12.5 (or 9.12.15) can be used for exclusion; the same can be shown for the factors of b. — A prime q or r dividing A_1 will lead to conditions similar to 8.3.4 (which are only *effective* for primes r). But $A_1 = 1$ in our equations, and the only remaining possibility is to work mod a power of 3.

We first consider the *primary* cases, i.e. the equations 9.13.4. It is easily verified that α^3 of 9.12.9 runs through a complete system of residues mod 3 with α; no exclusions can therefore be obtained mod 3. But *the cubic residues mod* 9 are comparatively much more limited in number, since we only have to cube a complete system of residues mod 3 and prime to 3 for α. Apart from a change of sign, there are 13 such residues: four triplets of conjugates and in addition $\alpha = 1$. The corresponding (effective) cubic residues mod 9 must be calculated in each case (which is a rather tedious job).

In all primary cases 9.12.1, it turns out that ε_1 *and* ε_2 *are effective cubic residues mod* 9, which means that it suffices to consider $\underline{\mu = \nu}$ in 9.13.4. Each ν must be multiplied in turn by all the corresponding cubic residues mod 9. In the cases where $3 \nmid b_1$ (i.e. when $A \neq 73$ and 307), *all resulting coefficients of* ω *are* $\not\equiv 0 \pmod 9$, and we conclude as usual that the equations are insoluble.

If however $3 \mid b_1$, it suffices for exclusion that the coefficients of ω are all $\underline{\not\equiv 0 \pmod{27}}$ (even if we still operate with the cubic residues mod 9). Since

now ν is divisible by $\mathfrak{p}_3\mathfrak{p}_3'' = [3, \xi]$, it must have the form

$$\nu = 3A + B\xi + 3C\omega, \quad 3 \nmid B.$$

If $b_1 = 3b_2$, and $\alpha^3 \equiv X + Y\xi + Z\omega$ is a cubic residue mod 9, the coefficient of ω in $\nu\alpha^3$ is

$$\equiv 3\{CX + b_2BY + (A + 3b_2B + aC)Z\} \pmod{27},$$

which is *unaltered mod 27* if X, Y and Z are varied with multiples of 9. — In this way the primary forms for $A = 73$ and 307 are excluded.

We then turn to the *non-primary* cases which have not already been excluded by class-number considerations (the equation 9.13.5). From $\mathfrak{p}_3 \nmid \alpha$ and 9.12.9 it follows that in this case

9.14.1 $$\alpha^3 \equiv \pm 1 \pmod{3},$$

and we can apply the principles of Theorem II. But we get a considerable improvement of the method by the following additional argument:

Since $\mathfrak{p}_3 \| \nu$, the possible residues of ν mod 3 are given by

9.14.2 $$\pm\nu \equiv b + \xi, \quad \xi + \omega \quad \text{or} \quad b - \omega \pmod{3}.$$

If $\mu = \nu$, the equation 9.13.5 is only possible mod 3 if ν has the first one of these forms (with a coefficient $\equiv 0 \pmod 3$ for ω).

Among the residues mod 3 and prime to 3, the following ones are *unaltered when taking conjugates:*

9.14.3 $$\pm 1, \quad \pm(\xi - \omega), \quad \pm(b + \xi - \omega).$$

The product of two such residues is another residue from the same group (the rules of multiplication are the same as for the group ± 1, $\pm\varrho$, $\pm\varrho^2$). And the residues 9.14.2 are, apart from a possible change of sign, *unaltered mod* 3 when multiplied by a residue from 9.14.3 (which contains *all* residues with this property).

It follows immediately that *the equation* 9.13.5 *is insoluble if* ν *is not of the first form* 9.14.2, *and if both* $\varepsilon_1 = \varepsilon$ *and* γ *are of the type* 9.14.3. But the γ of 9.13.6 satisfies this condition, and it suffices to examine the forms of ν and ε. — In this way the non-primary cases of 9.12.1, $A = 73$ and 307 excluded, have been proved insoluble.

If we include $a + b\varrho = \varrho$ (§ 5), the values of A in 9.12.1 (Table 4[f]) all have *four* possible but insoluble descents 9.6.1. And the soluble values of the com-

bined Tables 3 and 5 all have one or four such descents. The result is in striking analogy with *the 1st and 2nd conjecture* of Ch. VII, § 4. (See also Th. XIV, § 16.)

§ 15. The concluding paragraphs deal with *the number of generators (basic solutions) of infinite order for the equation* $X^3 + Y^3 = AZ^3$, and are based on the ideas of FADDEEV [1]. I have already (Ch. VII, § 6) mentioned briefly his methods in the field $K(\sqrt[3]{A}) = K(\vartheta)$. In this paragraph, I shall give a more detailed account of his methods in $K(\varrho)$ (partly modified to fit in with my notation and earlier results).

It follows from 1.2.2, with $abc = A$, that the *Weierstrass* elliptic $\wp$-function corresponding to $x^3 + y^3 = A$ is given by

$$\wp = \wp(\zeta;\ 0,\ 27A^2)$$

(the "equianharmonic" case, with $g_2 = 0$. To avoid confusion with my earlier notation, I use ζ instead of the ordinary u to denote the elliptic argument). Further from 1.2.3:

$$\frac{X}{Z} = x = x(\zeta) = \frac{9A + \wp'(\zeta)}{6\wp(\zeta)}, \quad \frac{Y}{Z} = y = y(\zeta) = \frac{9A - \wp'(\zeta)}{6\wp(\zeta)}.$$

Let the periods of $\wp(\zeta)$ be ω (real) and $\omega\varrho$; we then get all the real points on the curve $x^3 + y^3 = A$ if $0 \leqq \zeta < \omega$. In particular, $\zeta = 0$ corresponds to the point at infinity ($Z = 0$); $\zeta = \frac{1}{3}\omega$ and $\frac{2}{3}\omega$ give the inflexions $(\sqrt[3]{A}, 0)$ and $(0, \sqrt[3]{A})$; and $\zeta = \frac{1}{2}\omega$ gives the point $\left(\sqrt[3]{\frac{A}{2}}, \sqrt[3]{\frac{A}{2}}\right)$. If A is cubefree and $\neq 1$ and 2 (and always supposed positive), it follows from Ch. I, § 4 that all rational points with $Z \neq 0$ have a ζ incommensurable with ω *(no exceptional points).*

Changing the sign of ζ *corresponds to interchanging* X *and* Y (keeping Z fixed). — When nothing else is said, an elliptic argument ζ_i will correspond to the point (X_i, Y_i, Z_i).

The *tangential* (argument $-2\zeta_1$) to a point (X_1, Y_1, Z_1) is given by 1.5.2, which can be written as

9.15.1 $$X_2 = -X_1(X_1^3 + 2Y_1^3), \quad Y_2 = Y_1(2X_1^3 + Y_1^3), \quad Z_2 = Z_1(Y_1^3 - X_1^3).$$

By direct calculation, we find *the third intersection of the chord* (argument $-\zeta_1-\zeta_2$) through the points $(X_1,\ Y_1,\ Z_1)$ and $(X_2,\ Y_2,\ Z_2)$:

$$9.15.2 \qquad \begin{cases} X = A Z_1 Z_2 (X_2 Z_1 - X_1 Z_2) + Y_1 Y_2 (X_1 Y_2 - X_2 Y_1) \\ Y = A Z_1 Z_2 (Y_2 Z_1 - Y_1 Z_2) + X_1 X_2 (X_2 Y_1 - X_1 Y_2) \\ Z = X_1 X_2 (X_2 Z_1 - X_1 Z_2) + Y_1 Y_2 (Y_2 Z_1 - Y_1 Z_2). \end{cases}$$

Desboves' formulae 1.5.3 are usually more convenient for numerical computations. — Combining his formulae with 9.15.1, we find the *triplication* (argument $3\zeta_1$) of a point $(X_1,\ Y_1,\ Z_1)$:

$$9.15.3 \qquad \begin{cases} X_3 = X_1^9 + 6 X_1^6 Y_1^3 + 3 X_1^3 Y_1^6 - Y_1^9 \\ Y_3 = -X_1^9 + 3 X_1^6 Y_1^3 + 6 X_1^3 Y_1^6 + Y_1^9 \\ Z_3 = 3 X_1 Y_1 Z_1 (X_1^6 + X_1^3 Y_1^3 + Y_1^6). \end{cases}$$

For use in the field $K(\varrho)$, Faddeev gives the following, easily verified relations:

$$9.15.4 \qquad \begin{cases} X_2 + Y_2 = (X_1 + Y_1)(Y_1 - X_1)^3 \\ X_2 + Y_2\varrho = (X_1 + Y_1\varrho)(Y_1\varrho - X_1)^3, \end{cases}$$

$$9.15.5 \qquad \begin{cases} 3(X_1 + Y_1)(X_2 + Y_2)(X + Y) = A[Z_2(X_1 + Y_1) - Z_1(X_2 + Y_2)]^3 \\ 3(X_1 + Y_1\varrho)(X_2 + Y_2\varrho)(X + Y\varrho) = A[Z_2(X_1 + Y_1\varrho) - Z_1(X_2 + Y_2\varrho)]^3, \end{cases}$$

$$9.15.6 \qquad \begin{cases} X_3 + Y_3 = 9A X_1^3 Y_1^3 Z_1^3 \\ X_3 + Y_3\varrho = \lambda(X_1^3\varrho - Y_1^3)^3 \quad (\lambda = 1 - \varrho). \end{cases}$$

If $(X_1,\ Y_1,\ Z_1)$ are coprime in pairs, so also are usually $(X_2,\ Y_2,\ Z_2)$ and $(X_3,\ Y_3,\ Z_3)$. But if $X_1 \equiv Y_1 \not\equiv 0 \pmod 3$, i.e. in case II when $A \equiv \pm 2 \pmod 9$, then $(X_2,\ Y_2,\ Z_2)$ have a common factor 3 and $(X_3,\ Y_3,\ Z_3)$ a factor 9. — There is usually a rather great common factor in the formulae 9.15.2, cf. 9.18.7.

Lemma 1. *A solution* $(X,\ Y,\ Z)$ *is the triplication of another solution* $(x,\ y,\ z)$ *if and only if the ordinary descent in* $K(\varrho)$, *applied to* $(X,\ Y,\ Z)$, *leads to the same equation* $x^3 + y^3 = Az^3$. — We have seen that this descent then must take the form 9.3.3, with $\varepsilon = 1$:

$$9.15.7 \qquad X + Y = sA w^3, \quad X + Y\varrho = t\lambda(u + v\varrho)^3,$$

and further the condition 9.4.2 must be satisfied:

$$9.15.8 \qquad a = b = 1, \quad c = A.$$

Substituting this in the formulae 1.2.4 of Th. I, we find that they take the form 9.15.3. — On the other hand, it follows from 9.15.6 that a triplication will lead to the descent mentioned.

For a given solution (X, Y, Z), we now introduce the corresponding "*Faddeev-constant*" φ defined by

$$9.15.9 \qquad (X + Y)^2(X + Y\varrho) = \varphi \cdot \varrho^2 A^2 \alpha^3, \qquad \alpha \in K(\varrho).$$

We shall say that two solutions (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are F(addeev)-equivalent if and only if the ratio between their constants φ_1 and φ_2 is a (possibly fractional) cube in $K(\varrho)$, and we express this by

$$9.15.10 \qquad \varphi_1 \approx \varphi_2.$$

The sign of equivalence thus denotes *equality when cubes of* $K(\varrho)$ *are ignored.*

We can now prove

Lemma 2. *A solution* (X, Y, Z) *will lead to a descent* 9.15.7 *if and only if*

$$9.15.11 \qquad \varphi \approx 1.$$

— It is at once clear that 9.15.7 implies 9.15.11, if we substitute the different possibilities 9.3.4 for s and t in 9.15.9 and use the relation $\lambda^2 = -3\varrho$. — On the other hand, if we substitute $\varphi = 1$ and $\alpha = U + V\varrho$ in 9.15.9, we find by comparing the real and complex parts:

$$X(X + Y)^2 = A^2(-U^3 + 3U^2V - V^3), \quad Y(X + Y)^2 = A^2(-U^3 + 3UV^2 - V^3),$$
$$\text{i.e.} \quad (X + Y)^3 = A^2(-2U^3 + 3U^2V + 3UV^2 - 2V^3).$$

This shows that $A \mid X + Y$, and we must consequently have a descent of the type 9.3.3. Substituting this in 9.15.9 (with $\varphi = 1$), we see that $\varepsilon = 1$ is the only possibility, q.e.d.

Faddeev considers only the case $A = p$ *or* p^2, $p \neq 3$ a prime. There are then no equations of the form

$$9.15.12 \quad ax^3 + by^3 + cz^3 = 0, \quad abc = A, \quad 1 \leqq a < b < c, \quad (a, b) = (a, c) = (b, c) = 1,$$

and the descent 9.15.7 will then lead only to the case 9.15.8, i.e. a triplication. But *Faddeev's method applies without modifications whenever all equations* 9.15.12 *(if any) can be proved insoluble one way or other.*

We shall say that the descent 9.15.12 (and the corresponding solutions (X, Y, Z)) are of *Type I*, and then have

Lemma 3 *(Faddeev). When no descent of Type I exists, then* 9.15.11 *is the necessary and sufficient condition for* (X, Y, Z) *to be the triplication of another solution.*

Let next (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) be two solutions with elliptic arguments ζ_1 and ζ_2 respectively. We form the solution (X, Y, Z) with the argument

$$\zeta_1 - \zeta_2 = -(-\zeta_1) - \zeta_2$$

by means of the formulae 9.15.2, applied to $(\underbrace{Y_1, X_1}, Z_1)$ and (X_2, Y_2, Z_2). From the two formulae 9.15.5 (the first one squared) we conclude that

$$3^3(X_1 + Y_1)^2(Y_1 + X_1\varrho)(X_2 + Y_2)^2(X_2 + Y_2\varrho)(X + Y)^2(X + Y\varrho) = \alpha^3, \quad \alpha \in K(\varrho).$$

But

$$(X_1 + Y_1)(X_1 + Y_1\varrho)(X_1 + Y_1\varrho^2) = X_1^3 + Y_1^3 = A Z_1^3,$$

and so

$$\frac{(X_2 + Y_2)^2(X_2 + Y_2\varrho)}{(X_1 + Y_1)^2(X_1 + Y_1\varrho)} \cdot (X + Y)^2(X + Y\varrho) = \varrho^2 A^2 \left\{\frac{\alpha}{3 A Z_1 (X_1 + Y_1)}\right\}^3 =$$

$$= \varrho^2 A^2 \alpha_1^3, \quad \alpha_1 \in K(\varrho).$$

A comparison with Lemma 3 gives

Lemma 4 *(Faddeev). When no descent of Type I exists, then* 9.15.10 *is the necessary and sufficient condition for* $\zeta_1 - \zeta_2$ *to give the triplication of another solution.* — It is further an easy deduction that *addition of elliptic arguments corresponds to multiplication of Faddeev-constants.*

We can now divide the solutions of $X^3 + Y^3 = A Z^3$ in *classes* according to their Faddeev-constants; two solutions belong to the same class if and only if they are F-equivalent. (We still suppose that no descent of Type I exists.). The relations 9.15.4—5 show that *the classes form an abelian group, isomorphic with the multiplicative group formed by the corresponding Faddeev-constants.*

We know that the number of *basic solutions* of $X^3 + Y^3 = A Z^3$, represented by the elliptic arguments

$$\zeta_1, \zeta_2, \ldots \zeta_\varrho$$

is *finite.* (Faddeev gives a special proof for this, independently of earlier, general proofs. We return to this in § 18 below.)

If we consider the elliptic arguments

9.15.13 $$n_1\zeta_1 + n_2\zeta_2 + \cdots + n_g\zeta_g, \quad n_1, n_2, \ldots n_g = 0, 1, 2,$$

in number 3^g, it is clear that they all represent *inequivalent* solutions. On the other hand, any solution $m_1\zeta_1 + m_2\zeta_2 + \cdots + m_g\zeta_g$ differs from one of the forms 9.15.13 by the triplication of a solution, on taking the residues mod 3 of $m_1, m_2, \ldots m_g$. There is consequently a *one-one-correspondence* between the elliptic arguments 9.15.13 and the classes of solutions; in particular, the number of such classes is always *a power of* 3.

The number of classes is now easily found by counting the soluble descents different from 9.15.7 (cf. 9.6.1):

9.15.14 $$\begin{cases} X + Y = sA_1w^3, \quad X + Y\varrho = t\lambda(a + b\varrho)(u + v\varrho)^3, \quad a + b\varrho \neq \pm 1, \\ \text{where } A = A_1 \cdot N(a + b\varrho). \text{ A change of sign for } a + b\varrho \text{ is not} \\ \text{considered, and conjugate values } a + b\varrho \text{ and } a + b\varrho^2 \text{ are not} \\ \text{counted separately.} \end{cases}$$

We shall say that this descent (and the corresponding solutions (X, Y, Z)) are of *Type II.* — There can be no confusion with the a and b of 9.15.12.

We have seen that this descent will lead to an equation 9.6.3 (Table 5), where we must now include the possibility $a = 0$, $b = 1$, i.e. the equations 9.5.3—4 (Table 3).

It is clear that the different cases I—III of 9.3.4 (for the same value of $a + b\varrho$) will not themselves lead to different classes, since the values $s^2t = 3^4, 3^{-2}$ and 3^{-2} (cf. 9.15.9) *differ only by cubes.* (Such a combination of cases can occur only when $A \equiv \pm 2 \pmod 9$, i.e. $a + b\varrho$ in primary form, when both cases I and II are possible, cf. the beginning of § 8 above.) But different values of $a + b\varrho$ will obviously correspond to different classes. So will also *conjugate* values, hence each possibility 9.15.14 must be counted *twice.* Finally there is always *one* descent 9.15.7 (the triplication case), and we can therefore enunciate the following

Theorem XIII[1]. *When no soluble equation* 9.15.12 *exists, the number of soluble descents* 9.15.14 *is always of the form*

9.15.15 $$\frac{1}{2}(3^g - 1),$$

[1] The second sentence of this theorem is due to Faddeev, and the first is an immediate consequence of his methods.

where g is the number of generators for the equation $X^3 + Y^3 = AZ^3$. If in particular $A = p$ or p^2, $p \neq 3$ a prime, then

9.15.16
$$\begin{cases} g = 0 & \text{for} \quad p \equiv 2 \text{ or } 5 & (\text{mod } 9) \\ g \leqq 1 & \text{''} \quad p \equiv 4,\ 7 \text{ or } 8 & \text{''} \\ g \leqq 2 & \text{''} \quad p \equiv 1 & \text{''} \end{cases}$$

The cases $p \equiv 2$ or 5 are covered by Th. VIII, $p \equiv 4$ or 7 by § 9, 1. (Table 5), $p \equiv 8$ by Th. X (Table 3) and $p \equiv 1$ by a combination of the last two cases. We never find $g = 1$ when $p \equiv 1 \pmod 9$ and $A \leqq 500$ (but $g = 0$ for the values of Table 4[f]). In no case have I been able to show that $g = 0$ when $p \equiv 4$, 7 or 8 (but there are some unsolved equations with $A = p \equiv 4$ and $\leqq 500$ in 9.11.1).

The number 9.15.15 takes the values 0, 1, 4, 13, ... For $A \leqq 500$ (the combined Tables 3 and 5), the maximum attained is 4.

§ 16. Faddeev's method fails when there are soluble equations 9.15.12 (descents of Type I). We must then find a way of *classifying* such equations, analogous to Faddeev-equivalence for the descents 9.15.14 (Type II).

I define by

9.16.1
$$\varkappa = \frac{a}{b} \sim \frac{b}{c} \sim \frac{c}{a} \sim \frac{u}{v}$$

the "*characteristic ratio*" (c.r.) for an equation $ax^3 + by^3 + cz^3 = 0$, $abc = A$. The sign of equivalence stands for *equality when rational cubes and powers of A are ignored.* Thus for instance

$$\frac{a}{b} = A \cdot \left(\frac{1}{b}\right)^3 \cdot \frac{b}{c} \sim \frac{b}{c}.$$

The u and v are those of 9.4.1.

A *cyclic permutation* of the terms ax^3, by^3 and cz^3 leaves both the c.r. and the formulae 1.2.4 unaltered. (This corresponds to using the *automorphisms* 9.11.3 in the descent 9.15.7.) But a *transposition* of the terms implies inversion of the c.r., and at the same time an interchange of X and Y in 1.2.4, which means a change of sign in the elliptic argument ζ. (This corresponds to replacing $u + v\varrho$ by its *conjugate*, combined with an automorphism if necessary.)

It is clear that two different factorizations $A = abc$ correspond to inequivalent c.r. Each such factorization gives *two (reciprocal) values*, except in the case 9.15.8, when the only value is $\varkappa \sim 1$.

We can say that $\varkappa$ is the c.r. also for the solution (X, Y, Z) leading to the descent 9.15.7. It then follows from Lemmas 1—2 that *the conditions* 9.15.11 ($\varphi \approx 1$) *and*

9.16.2 $$\varkappa \sim 1$$

are the necessary and sufficient conditions for (X, Y, Z) *to be the triplication of another solution.*

Let us first suppose that *no soluble descent of Type II exists;* the condition 9.15.11 is then automatically satisfied. — We have already noticed that a change of sign in the elliptic argument ζ corresponds to *inversion* of the characteristic ratio $\varkappa$. We shall also see that addition of elliptic arguments corresponds to *multiplication* of characteristic ratios. This follows from the

Lemma 5. *Let* (x_1, y_1, z_1) *and* (x_2, y_2, z_2) *be solutions of the equations*

$$a_1 x^3 + b_1 y^3 + c_1 z^3 = 0, \quad a_1 b_1 c_1 = A, \quad \text{and}$$
$$a_2 x^3 + b_2 y^3 + c_2 z^3 = 0, \quad a_2 b_2 c_2 = A$$

respectively, and let $P_1(X_1, Y_1, Z_1)$ *and* $P_2(X_2, Y_2, Z_2)$ *be the corresponding points* (*by* 1.2.4) *on the curve* $X^3 + Y^3 = A Z^3$. *Then*

9.16.3 $$\begin{cases} x = a_1 x_1^2 y_2 z_2 - a_2 x_2^2 y_1 z_1, \quad y = b_1 y_1^2 z_2 x_2 - b_2 y_2^2 z_1 x_1, \\ z = c_1 z_1^2 x_2 y_2 - c_2 z_2^2 x_1 y_1 \end{cases}$$

is a solution of the equation

9.16.4 $$\frac{x^3}{a_1 a_2} + \frac{y^3}{b_1 b_2} + \frac{z^3}{c_1 c_2} = 0.$$

Further the corresponding point $P(X, Y, Z)$ *on* $X^3 + Y^3 = A Z^3$ *is the third intersection of the chord through* P_1 *and* P_2. (This lemma is of course valid whether or not descents of Type II exist.)

The multiplicative property of the characteristic ratio is an immediate consequence, since the c.r. for the equation 9.16.4 is

$$\varkappa = \frac{\frac{1}{a_1 a_2}}{\frac{1}{b_1 b_2}} = \frac{1}{\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}} = \frac{1}{\varkappa_1 \varkappa_2},$$

and the elliptic argument ζ of P equals

$$\zeta = -(\zeta_1 + \zeta_2).$$

It is easily verified by straightforward calculation that 9.16.3 gives a solution of the equation 9.16.4. The product of the coefficients is here $\frac{1}{A^2} = \frac{A}{A^3}$, and the equation can thus be given the form $a_3 x'^3 + b_3 y'^3 + c_3 z'^3 = 0$, $a_3 b_3 c_3 = A$, $(a_3, b_3) = (a_3, c_3) = (b_3, c_3) = 1$. — We note that 9.16.3 coincides with *Desboves'* formulae 1.5.3 when $a_1 = a_2 = a$, $b_1 = b_2 = b$ and $c_1 = c_2 = c$.

The last sentence of the Lemma can also be verified by straightforward calculations. These become very tedious, but can be facilitated by means of the second formula 9.15.5, where we substitute

$$X_1 + Y_1\varrho = \lambda(u_1 + v_1\varrho)^3, \quad X_2 + Y_2\varrho = \lambda(u_2 + v_2\varrho)^3, \quad X + Y\varrho = C\lambda(u + v\varrho)^3;$$
$$Z_1 = 3w_1 \cdot N(u_1 + v_1\varrho), \quad Z_2 = 3w_2 \cdot N(u_2 + v_2\varrho).$$

Here $C = (X, Y)$ is the unknown common factor of the formulae 9.15.2. We can always use the values $s = 9$, $t = 1$ of *case I*, if we keep a common factor 9 in a solution of case II.

It follows from 9.15.5 that C is divisible by $9A$ (cf. 9.18.7), and further from a comparison of the cubes that

9.16.5 $$C' \cdot (u + v\varrho) = w_2(u_2 + v_2\varrho^2)(u_1 + v_1\varrho)^2 - w_1(u_1 + v_1\varrho^2)(u_2 + v_2\varrho)^2,$$

where C' is some unspecified rational integer. A possible unit $\varepsilon = 1$, ϱ or ϱ^2 can be absorbed in $u + v\varrho$, because of the automorphisms 9.11.3.

The relation 9.16.5 is now rather easily verified on equating real and complex parts and making the substitution

$$u_1 = -a_1 x_1^3, \quad v_1 = b_1 y_1^3, \quad w_1 = -x_1 y_1 z_1; \quad u_2 = -a_2 x_2^3, \quad v_2 = b_2 y_2^3, \quad w_2 = -x_2 y_2 z_2;$$
$$u = -\frac{1}{a_1 a_2}(a_1 x_1^2 y_2 z_2 - a_2 x_2^2 y_1 z_1)^3, \quad v = \frac{1}{b_1 b_2}(b_1 y_1^2 z_2 x_2 - b_2 y_2^2 z_1 x_1)^3,$$

cf. 9.4.1 and 9.16.3—4. — This concludes the proof of Lemma 5.

The formulae 9.16.3 fail in the *duplication* case (since then $x = y = z = 0$). But it is easily verified by means of 1.5.2 and 9.15.1 that corresponding solutions (by 1.2.4) of the two equations $ax^3 + by^3 + cz^3 = 0$ and $X^3 + Y^3 = abcZ^3 = AZ^3$ have corresponding tangentials. (As above, the verification can be simplified by use of the second formula 9.15.4.) The multiplicative property of $\varkappa$ still holds, since a tangential for $X^3 + Y^3 = AZ^3$ has an elliptic argument $-2\zeta \equiv +\zeta \pmod{3\zeta}$.

Like the Faddeev-constants φ of the last paragraph, the characteristic ratios $\varkappa$ thus form *a multiplicative abelian group.* In particular, we conclude in analogy with Lemma 4 that $\varkappa_1 \sim \varkappa_2$ *is the necessary and sufficient condition for* $\zeta_1 - \zeta_2$ *to give the triplication of another solution.*

The classification of the soluble equations $ax^3 + by^3 + cz^3 = 0$ is now complete, and the arguments that led to Th. XIII can be repeated. They show that *when no descent of Type II exists, the number of soluble equations* 9.15.12 *is always of the form*

$$\frac{1}{2}(3^g - 1), \tag{9.16.6}$$

where g *is the number of generators for the equation* $X^3 + Y^3 = AZ^3$.

We must finally *combine* the Types I and II of descent, and divide the basic solutions (in finite number) between the two types:

$$\underbrace{\zeta_1, \zeta_2, \ldots \zeta_{g_1}}_{\text{Type I}}; \quad \underbrace{\zeta'_1, \zeta'_2, \ldots \zeta'_{g_2}}_{\text{Type II}}.$$

We first note that the Types I and II have a Faddeev-constant $\varphi \equiv 1$ and $\varphi' \not\equiv 1$ respectively. It follows that when there are descents of Type II, there must be at least one generator ζ'. We can further suppose that all the ζ' are F-inequivalent, since ζ'_1 and $\zeta'_2 \equiv \zeta'_1$ can be replaced by ζ'_1 and $\zeta'_1 - \zeta'_2$, where the latter is of Type I.

If we consider the elliptic arguments 9.15.13:

$$\begin{cases} \zeta = \underbrace{n_1\zeta_1 + \cdots + n_{g_1}\zeta_{g_1}}_{\text{Type I}} + \underbrace{n'_1\zeta'_1 + \cdots + n'_{g_2}\zeta'_{g_2}}_{\text{Type II}}, \\ n_1, \ldots n_{g_1};\ n'_1, \ldots n'_{g_2} = 0, 1, 2, \end{cases} \tag{9.16.7}$$

then the Faddeev-constant φ of ζ will depend only on the coefficients n', and not on the n. Further $\varphi \equiv 1$ (Type I) if and only if all $n' = 0$. The arguments that led to Th. XIII can now be repeated, showing that the number of soluble descents of Type II is still of the form 9.15.15 (with $g = g_2$).

Equating all the n' to zero, we can then study the distribution of the generators of Type I by varying the coefficients n. (There must be at least one generator ζ, when there are descents of this type.) We are again led to 9.16.6 (with $g = g_1$), and can consequently enunciate the following

Theorem XIV. *The number of soluble equations* 9.15.12 *and the number of soluble descents* 9.15.14 *are always of the forms*

$$\frac{1}{2}(3^{g_1}-1) \quad \textit{and} \quad \frac{1}{2}(3^{g_2}-1)$$

respectively. Here

$$g = g_1 + g_2$$

is the number of generators of infinite order for the equation $X^3 + Y^3 = AZ^3$. *The basic solutions can be chosen so that there are* g_1 *and* g_2 *generators respectively resulting from the two different types of descent.*

Of course other choices of generators are possible when $g_1, g_2 > 0$, cf. the concluding remarks of the next paragraph.

The solutions of Type I, together with the triplications, are characterized by $\varphi \equiv 1$, and thus form a *subgroup* of the group of all solutions. It is very striking that such an arithmetically defined subgroup should exist.

§ 17. The *basic solutions* of $X^3 + Y^3 = AZ^3$ for (cubefree) $A \leqq 500$ can now be found by Th. XIV from Table 2^b (Th. I), Table 3 (Th. X) and Table 5 (the formulae 9.6.2). A list of the basic solutions is given in *Table 6*, which also contains a column for the maximum number g of generators. This number is obtained in nearly all cases; the only undecided (unsolved) equations, given in (10) of the Introduction, correspond to 7.4.2 and 9.11.1. Since these have $A = 473 = 11 \cdot 43$ in common, $g \leqq 2$ in this case. In the remaining undecided cases, $g \leqq 1$. *As stated earlier, I believe that the maximum number of generators is really obtained in all cases.*

In particular, I can decide solubility and the number of generators in *all* cases when

9.17.1 $$A < 283.$$

Sylvester ([1] pp. 313 and 316) stated that he knew whether or not any number $A \leqq 100$ is a sum of two cubes, except perhaps $A = 66$ (which is insoluble by Table 4^b; also proved by Cassels [1]). Sylvester's statement is partly based on the inaccurate communication from *Pépin*, mentioned above in connection with 9.4.5. But there is one insoluble value of $A \leqq 100$, namely $A = 73$ (Table 4^f), which has never been noticed in earlier papers. I suspect that Sylvester has taken the solubility of 9.5.3 with $A = 73$ for granted.

The basic solutions of Table 6 for $A \leqq 50$ are also given by Faddeev [1] (but I choose the solutions differently for $A = 19$ and 37). Some of the remaining

solutions in Table 6 were given by LENHART (see DICKSON [1], Ch. XXI, ref. 186), but most of them have been found by me.

There are never more than 2 generators when $A \leqq 500$. The smallest value of A with $g > 2$ is

9.17.2 $$A = 657 = 9 \cdot 73,$$

where $3\,(R)\,73$ (cf. § 9, 3.). We then get the one soluble equation $x^3 + 9y^3 + 73z^3 = 0$, and four soluble descents 9.15.14, corresponding to $a + b\varrho = \varrho$, π_{73}, $\varrho\,\pi_{73}$ and $\varrho^2\,\pi_{73}$. There are thus *three* basic solutions, which can be chosen as

9.17.3 $(X, Y, Z) = (10, -7, 1)$, $(17, 7, 2)$ and $(2971, -2890, 147)$.

Most of the soluble $A \leqq 500$ have $g = 1$, resulting from one equation in Table 2^b, 3 *or* 5. The values of $A \leqq 500$ with 2 generators are distributed as follows:

Table 2^b alone gives rise to $g = 2$ (4 equations) in 13 cases, and Table 5 alone in 3 cases ($A = 91$, 217 and 469, all of the form $A = r_1 r_2 \equiv 1 \pmod 9$, r_1 and $r_2 \not\equiv 1 \pmod 9$ and not both cubic residues of each other).

The combined Tables 3 and 5 give $g = 2$ (4 equations) for 8 primes $r \equiv +1 \pmod 9$, cf. 9.15.16.

The values $A = 153$ and 477 (both of the form $A = 9q$, $q \equiv -1 \pmod 9$) have $g = 2$, resulting from one equation in each of the Tables 2^b and 3.

The remaining cases with $g = 2$ all result from one equation in each of the Tables 2^b and 5:

5 values $A = 3R$, $3\,(R)\,r$;

12 values $A = QR \not\equiv \pm 1 \pmod 9$, $q\,(R)\,r$ (and possibly also $A = 473 = 11 \cdot 43$, where no solution has been found); and finally

7 values of A with 3 different prime factors.

In the cases where there are two basic solutions, resulting from one equation in Table 2^b and one in Table 3 or 5, the solution of the latter equation (Type II) will usually lead to the smaller basic solution (X, Y, Z). In most cases the smallest values of the second basic solution, as given in Table 6, is calculated from another solution of the same type of descent (not given in Tables 3 or 5). The solution (X, Y, Z) resulting from Table 2^b (Type I) then usually corresponds to one of the elliptic arguments $\pm\zeta_1 \pm \zeta_2$.

§ 18. We must also ensure that the solutions of Table 6, found by the descents 9.15.12 and 9.15.14, are really *basic*. — The principles to be used are

given by *Faddeev*, in his proof that the number of generators is finite. His result is as follows:

Let (X_i, Y_i, Z_i), $i = 1, 2, \ldots 3^g - 1$, represent one solution from each of the classes defined by 9.16.7; the triplication class (all n and $n' = 0$) need not be considered. Let further L denote the maximum of all $|X_i|$, $|Y_i|$ and $|Z_i|$. Any solution (X, Y, Z) can then be expressed as a combination (in elliptic arguments) of the solutions (X_i, Y_i, Z_i) and a finite number of other solutions (X', Y', Z') such that

9.18.1 $$|X'| + |Y'| < 4 A^{\frac{1}{18}} L^{\frac{1}{3}}.$$

The possible basic solutions not contained among the (X_i, Y_i, Z_i) can thus be found in a finite number of steps.

Faddeev's inequality 9.18.1 is based on rather rough approximations. I will show that his method can be refined, leading to an improvement of both coefficient and exponent in 9.18.1.

I prefer to deal with the *norm* $N(X + Y\varrho) = X^2 - XY + Y^2$ of a solution (X, Y, Z), instead of with $|X|$ and $|Y|$. For a solution of Type II, resulting from a descent 9.15.14, we have

9.18.2 $$N(X + Y\varrho) = 3t^2 \cdot N(a + b\varrho) \cdot N(u + v\varrho)^3,$$

where u and v are the solutions of the corresponding equation 9.6.3.

For a solution of Type I, resulting from a descent 9.15.7 and leading to an equation 9.15.12, we have by 9.4.1:

9.18.3 $$N(X + Y\varrho) = 3t^2 \cdot N(u + v\varrho)^3 = 3t^2 \cdot N(-ax^3 + by^3\varrho)^3.$$

For both types of descent, the value of $N(u + v\varrho)$ for a known solution must be calculated anyway as a factor of Z in 9.3.3 or 9.6.1. The value of t to be used (cf. 9.3.4) depends on the solution (X, Y, Z).

It is further easily seen that we have the inequalities:

9.18.4 $$\text{Max } \{|u|, |v|\} \leqq \sqrt{\frac{4}{3} N(u + v\varrho)}; \text{ in particular}$$

9.18.5 $$\text{Max } \{|ax^3|, |by^3|, |cz^3|\} \leqq \sqrt{\frac{4}{3} N(-ax^3 + by^3\varrho)}.$$

Let (X_i, Y_i, Z_i), $i = 1, 2, \ldots 3^g - 1$, have the same meaning as above, and let now

$$M = \text{Max } \{N(X_i + Y_i\varrho)\}.$$

Let further (X, Y, Z), with elliptic argument ζ, be any solution different from $(1, -1, 0)$ and from the (X_i, Y_i, Z_i), and not a triplication of another solution (x, y, z). (If (X, Y, Z) is such a triplication, we deal with (x, y, z) instead.) There is then always one (X_i, Y_i, Z_i), with argument ζ_i, such that $\zeta - \zeta_i = -(-\zeta) - \zeta_i$ gives the triplication (X_3, Y_3, Z_3) of another solution. Since (X_3, Y_3, Z_3) can be obtained by applying 9.15.2 to (Y, X, Z) and (X_i, Y_i, Z_i), we get from 9.15.5:

9.18.6 $$3(Y + X\varrho)(X_i + Y_i\varrho)(X_3 + Y_3\varrho) = A[Z_i(Y + X\varrho) - Z(X_i + Y_i\varrho)]^3.$$

As already mentioned, the formulae 9.15.2 will usually give a rather big common factor C. It is easily seen that C is always divisible by

9.18.7 $$C_1 = \text{greatest common factor of all } sA_1$$

(in the expression for $X + Y$) in all soluble descents 9.15.7 (where $A_1 = A$) and 9.15.14. In particular, C_1 *will contain all prime factors* $q \equiv -1 \pmod 3$ *of* A. — It follows from 9.15.5 that possible factors of C prime to $3A$ always occur as *cubes*, but nothing more can be said in general about such factors.

Let (X_3', Y_3', Z_3') be the solution with the factor C removed. Since $|Y + X\varrho| = |X + Y\varrho|$, 9.18.6 gives the inequality

$$3|X + Y\varrho| \cdot |X_i + Y_i\varrho| \cdot |X_3' + Y_3'\varrho| \leqq C_1^{-1} A[|Z_i| \cdot |X + Y\varrho| + |Z| \cdot |X_i + Y_i\varrho|]^3.$$

Further

$$|Z|^3 = \frac{|X^3 + Y^3|}{A} = \frac{|X + Y| \cdot |X + Y\varrho|^2}{A} \leqq \frac{2|X + Y\varrho|^3}{A}, \quad \text{i.e.}$$

$$|Z| \leqq \sqrt[3]{\frac{2}{A}} \cdot |X + Y\varrho|, \quad |Z_i| \leqq \sqrt[3]{\frac{2}{A}} \cdot |X_i + Y_i\varrho|.$$

Substituting this, we find that

$$|X_3' + Y_3'\varrho| \leqq \frac{2^4}{3} C_1^{-1} \cdot |X_i + Y_i\varrho|^2 \cdot |X + Y\varrho|^2.$$

Now the norm is the square of the modulus, and so

9.18.8 $$N(X_3' + Y_3'\varrho) \leqq \frac{2^8}{3^2} C_1^{-2} \cdot M^2 \cdot N(X + Y\varrho)^2.$$

Let (X_3', Y_3', Z_3') be the triplication of a solution (x, y, z), given by the expressions 9.15.3. It is easily verified by the second formula 9.15.6 that $N(x + y\varrho)$

has a maximum for fixed $N(X_3' + Y_3'\varrho)$ when

$$x = -y, \quad N(x + y\varrho) = 3x^2, \quad N(X_3' + Y_3'\varrho) = 3x^{18}.$$

But we must remember that the formulae 9.15.3 can give a common factor 9 when $A \equiv \pm 2 \pmod 9$. Since the possibility $x = -y$ is excluded, we thus get an inequality:

$$\frac{N(x + y\varrho)}{3} < \sqrt[9]{C_2 \cdot \frac{N(X_3' + Y_3'\varrho)}{3}}, \quad \text{where}$$

9.18.9 $\qquad C_2 = 1 \quad \text{if} \quad A \not\equiv \pm 2, \quad C_2 = 3^4 \quad \text{if} \quad A \equiv \pm 2 \pmod 9.$

Combining this with 9.18.8, we see that

$$N(x + y\varrho) < \left\{\frac{2^8 \cdot 3^6 \cdot C_2}{C_1^2}\right\}^{\frac{1}{9}} \cdot M^{\frac{2}{9}} \cdot N(X + Y\varrho)^{\frac{2}{9}}.$$

We now apply the same process to the solution (x, y, z), and can continue with this principle *until we get, either to one of the given solutions* (X_i, Y_i, Z_i), *or to a solution* (X', Y', Z') *such that*

9.18.10 $$N(X' + Y'\varrho) < \left\{\frac{2^8 \cdot 3^6 \cdot C_2}{C_1^2}\right\}^{\frac{1}{7}} \cdot M^{\frac{2}{7}}.$$

Here C_1 and C_2 are given by 9.18.7 and 9.18.9. — This is the improved form of the inequality 9.18.1.

When the limit of 9.18.10 has been calculated, the search for possible solutions (X', Y', Z') can be quickly performed by the formulae 9.18.2—3. These will in most cases give very narrow limits for the $|u|$ and $|v|$ of 9.18.4, or for the $|ax^3|$, $|by^3|$ and $|cz^3|$ of 9.18.5. The value of t to be used in these inequalities is usually uniquely determined by the type of descent and the residue of A mod 9. The only ambiguity arises for $A \equiv \pm 2 \pmod 9$, when both cases I and II are possible; we must then use the most unfavourable value $t = \frac{1}{9}$ (case II) in the expression for $N(X' + Y'\varrho)$.

We have seen that $g = 1$ or 2 for all soluble $A \leqq 500$. When $g = 2$, the solutions of the descents 9.15.12 and/or 9.15.14 are usually so simple that the basic ones are easily recognized. When however $g = 1$, the one basic solution (X_1, Y_1, Z_1) is sometimes big, and must be checked by 9.18.10. The solutions (X_i, Y_i, Z_i) can then be chosen as (X_1, Y_1, Z_1) and $(X_2, Y_2, Z_2) = (Y_1, X_1, Z_1)$, i.e. $M = N(X_1 + Y_1\varrho)$.

Table I[a].

The residues mod 9 of $N(u + v\vartheta + w\vartheta^2) = u^3 + mv^3 + m^2w^3 - 3muvw$.

	1	ϑ	ϑ^2	$1+\vartheta$	$1-\vartheta$	$1+\vartheta^2$	$1-\vartheta^2$	$\vartheta+\vartheta^2$	$\vartheta-\vartheta^2$	$1+\vartheta+\vartheta^2$	$1-\vartheta-\vartheta^2$	$1-\vartheta+\vartheta^2$	$1+\vartheta-\vartheta^2$
$m\equiv 1 \pmod 9$	1	1	1	2	0	2	0	2	0	0	−4	4	4
$m\equiv 2$ "	1	2	4	3	−1	−4	−3	−3	−2	1	−2	0	−4
$m\equiv 3$ "	1	3	0	4	−2	1	1	3	3	4	−2	−2	4
$m\equiv 4$ "	1	4	−2	−4	−3	−1	3	2	−3	0	−4	−2	1

Table I[b].

Possible combinations mod 3 of v and $\eta = \varepsilon_m^i$.

		$n\equiv 0 \pmod 9$			$n\equiv 1 \pmod 9$			$n\equiv 2 \pmod 9$		
	$v\equiv$	$1-\vartheta$	$1-\vartheta^2$	$\vartheta-\vartheta^2$	1	ϑ	ϑ^2	$1+\vartheta$	$1+\vartheta^2$	$\vartheta+\vartheta^2$
$m\equiv 1 \pmod 9$	$\eta\equiv 1$	×			×	×		×		
	$\eta\equiv\vartheta$		×		×		×		×	
	$\eta\equiv\vartheta^2$			×		×	×			×

		$n\equiv 1 \pmod 9$			$n\equiv 2 \pmod 9$			$n\equiv 3 \pmod 9$		
	$v\equiv$	1	$-1+\vartheta$	$1+\vartheta+\vartheta^2$	ϑ	$-\vartheta+\vartheta^2$	$-1+\vartheta+\vartheta^2$	$1+\vartheta$	$-1+\vartheta^2$	$-\vartheta-\vartheta^2$
$m\equiv 2 \pmod 9$	$\eta\equiv 1$	×	×		×			×		
	$\eta\equiv -1+\vartheta$	×		×			×			×
	$\eta\equiv 1+\vartheta+\vartheta^2$		×	×		×			×	

		$n\equiv 1 \pmod 9$			$n\equiv 2 \pmod 9$			$n\equiv 4 \pmod 9$		
	$v\equiv$	1	$1+\vartheta^2$	$1-\vartheta^2$	$-1+\vartheta$	$-1+\vartheta+\vartheta^2$	$-1+\vartheta-\vartheta^2$	$1+\vartheta$	$1+\vartheta+\vartheta^2$	$1+\vartheta-\vartheta^2$
$m\equiv 3 \pmod 9$	$\eta\equiv 1$	×			×			×		
	$\eta\equiv 1+\vartheta^2$			×		×				×
	$\eta\equiv 1-\vartheta^2$		×				×		×	

		$n\equiv 1 \pmod 9$			$n\equiv 3 \pmod 9$			$n\equiv 4 \pmod 9$		
	$v\equiv$	1	$-1-\vartheta^2$	$1+\vartheta-\vartheta^2$	$-1+\vartheta$	$1-\vartheta^2$	$-\vartheta+\vartheta^2$	ϑ	$-1-\vartheta$	$-1+\vartheta+\vartheta^2$
$m\equiv 4 \pmod 9$	$\eta\equiv 1$	×			×			×	×	
	$\eta\equiv -1-\vartheta^2$			×		×		×		×
	$\eta\equiv 1+\vartheta-\vartheta^2$		×				×		×	×

Table 1c.

Effective cubic residues for $m \equiv \pm 1 \pmod 9$.

	$m=10$	$m=17$	$m=19$	$m=26$	$m=28$
Class 4 (mod 27)	$\frac{1+\vartheta-2\vartheta^2}{3}$	$\frac{32+4\vartheta-\vartheta^2}{3}$	$\frac{-1+2\vartheta+8\vartheta^2}{3}$	$\frac{16-\vartheta+10\vartheta^2}{3}$	$\frac{20-\vartheta+8\vartheta^2}{3}$
Class 6 (mod 9)	$\frac{7+\vartheta-2\vartheta^2}{3}$	$\frac{8+4\vartheta-\vartheta^2}{3}$	$\frac{-7+2\vartheta+8\vartheta^2}{3}$	$\frac{4-\vartheta+10\vartheta^2}{3}$	$\frac{5-\vartheta+8\vartheta^2}{3}$
	$m=35$	$m=37$	$m=44$	$m=46$	
Class 4 (mod 27)	$\frac{1+11\vartheta+\vartheta^2}{3}$	$\frac{31-5\vartheta+\vartheta^2}{3}$	$\frac{31+5\vartheta+\vartheta^2}{3}$	$\frac{1-11\vartheta+\vartheta^2}{3}$	
Class 6 (mod 9)	$\frac{7+11\vartheta+\vartheta^2}{3}$	$\frac{1-5\vartheta+\vartheta^2}{3}$	$\frac{1+5\vartheta+\vartheta^2}{3}$	$\frac{7-11\vartheta+\vartheta^2}{3}$	

Table 1d.

The cubic residues $td+\vartheta \pmod{q_q}$ in $K(\vartheta)$.
" " " $t+\varrho \pmod q$ " $K(\varrho)$.

$m=$		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$q=47$	m^{-1}	1	−23	16	12	19	8	−20	6	21	−14	−17	4	−18	−10	22	3	−11	−13	5	−7	9	15	−2
	d	1	21	−19	18	−8	−23	16	2	−15	20	−12	−13	10	7	11	−5	4	14	−6	−3	−22	−17	−9
$q=41$	m^{-1}	1	−20	14	−10	−8	7	6	−5	−9	−4	15	−17	19	3	11	18	−12	16	13	−2			
	d	1	5	−14	−16	20	12	−17	2	−9	18	6	19	15	−3	7	10	−13	−4	11	8			
$q=29$	m^{-1}	1	−14	10	−7	6	5	−4	11	13	3	8	−12	9	−2									
	d	1	−3	−11	9	−7	4	−13	2	5	−8	−14	−12	6	10									
$q=23$	m^{-1}	1	−11	8	6	−9	4	10	3	−5	7	−2												
	d	1	−7	−11	3	−4	8	−9	2	6	5	10												
$q=17$	m^{-1}	1	−8	6	−4	7	3	5	−2															
	d	1	8	7	−4	−6	5	−3	2															
$q=11$	m^{-1}	1	−5	4	3	−2																		
	d	1	−4	−2	5	3																		
$q=5$	m^{-1}	1	−2																					
	d	1	−2																					

Values of t:

$q=5$: $t=$ 3

$q=11$: $t=$ 3, 6, 9

$q=17$: $t=$ 0, 1, 2, 9, 16

$q=23$: $t=$ 3, 4, 10, 12, 14, 20, 21

$q=29$: $t=$ 5, 8, 10, 12, 15, 18, 20, 22, 25

$q=41$: $t=$ 4, 5, 8, 12, 14, 17, 21, 25, 28, 30, 34, 37, 38

$q=47$: $t=$ 8, 9, 10, 13, 17, 18, 23, 24, 25, 30, 31, 35, 38, 39, 40

Table 2[b].

Non-excluded equations $ax^3 + by^3 + cz^3 = 0$
with $abc = A$ cubefree and $\leqq 500$;
$1 \leqq a < b < c$, $(a, b) = (a, c) = (b, c) = 1$.

A	a	b	c	x	y	z	A	a	b	c	x	y	z
6	1	2	3	1	1	−1	132	1	3	44	−5	3	1
12	1	3	4	1	1	−1		1	4	33	1	2	−1
15	1	3	5	−2	1	1		1	11	12	1	1	−1
20	1	4	5	1	1	−1		3	4	11	1	7	−5
22	1	2	11	−3	2	1	140	1	7	20	−3	1	1
30	1	2	15	1	−2	1	141	1	3	47	1	5	−2
	1	3	10	1	−3	2	142	1	2	71	−5	3	1
	1	5	6	1	1	−1	153	1	9	17	2	1	−1
	2	3	5	1	1	−1	156	1	12	13	1	1	−1
33	1	3	11	2	1	−1	159	1	3	53	7	3	−2
34	1	2	17	1	2	−1	164	1	4	41	11	−7	1
42	1	6	7	1	1	−1	166	1	2	83	9	38	−11
50	1	2	25	−3	1	1	170	1	10	17	−3	1	1
51	1	3	17	4	−3	1	177	1	3	59	17	−16	5
58	1	2	29	3	1	−1	178	1	2	89	7	−6	1
65	1	5	13	2	1	−1	180	4	5	9	1	1	−1
68	1	4	17	−5	3	1	182	1	13	14	1	1	−1
69	1	3	23	1	−2	1	183	1	3	61	−4	1	1
70	2	5	7	1	1	−1	186	1	2	93	−7	5	1
75	1	3	25	1	2	−1	187	1	11	17	5	1	−2
78	2	3	13	−2	1	1	195	1	5	39	1	−2	1
84	3	4	7	1	1	−1	198	2	9	11	1	1	−1
85	1	5	17	1	3	−2	201	1	3	67	4	1	−1
86	1	2	43	3	2	−1	202	1	2	101	3	−4	1
87	1	3	29	10	−7	1	203	1	7	29	3	−2	1
90	1	9	10	1	1	−1	205	1	5	41	1	2	−1
92	1	4	23	−3	1	1	209	1	11	19	2	1	−1
94	1	2	47	−63	50	1	210	1	6	35	−11	6	1
105	1	7	15	2	1	−1		1	14	15	1	1	−1
106	1	2	53	1	−3	1		2	5	21	2	1	−1
110	1	2	55	1	3	−1		3	7	10	1	1	−1
	1	5	22	−3	1	1	212	1	4	53	19	−12	1
	1	10	11	1	1	−1	213	1	3	71	250	−231	67
	2	5	11	−2	1	1	214	1	2	107	7	−19	5
114	2	3	19	2	1	−1	218	1	2	109	−5	2	1
115	1	5	23	−7	4	1	219	1	3	73	2	−3	1
123	1	3	41	16	7	−5	222	1	6	37	5	−3	1
124	1	4	31	3	1	−1	228	1	12	19	−7	3	1
126	2	7	9	1	1	−1	231	3	7	11	3	1	−2
130	1	5	26	−7	3	2	236	1	4	59	3	2	−1

Table 2^b (continued).

A	a	b	c	x	y	z	A	a	b	c	x	y	z
238	1	7	34	3	1	−1	357	3	7	17	−2	1	1
246	1	2	123	−5	1	1	358	1	2	179	5	3	−1
	1	3	82	1	3	−1	363	1	3	121	23	−16	1
	1	6	41	7	−4	1	366	1	3	122	−5	1	1
	2	3	41	52	1	−19	370	1	10	37	3	1	−1
249	1	3	83	−1867	49	428	372	1	4	93	−5	2	1
254	1	2	127	5	1	−1	380	1	19	20	1	1	−1
258	1	2	129	1	4	−1	382	1	2	191			
265	1	5	53	43	−39	16	385	1	7	55	1	−2	1
267	1	3	89	2	3	−1	390	1	5	78	1	−5	2
273	1	13	21	2	1	−1		2	3	65	2	−3	1
274	1	2	137	−165	59	31		2	13	15	1	1	−1
275	1	11	25	−9	4	1		3	10	13	1	1	−1
282	1	2	141	5	2	−1	391	1	17	23	41	8	−15
	1	3	94	−73	11	16	393	1	3	131	176	−169	41
	1	6	47	1	−2	1	394	1	2	197	−13	10	1
	2	3	47	−4	3	1	396	1	9	44	7	1	−2
284	1	4	71	691	714	−293	399	1	7	57	1	2	−1
285	3	5	19	−2	1	1	402	1	3	134	83	−63	11
286	2	11	13	1	1	−1	407	1	11	37	−5	2	1
294	1	6	49	1	2	−1	411	1	3	137	−8	5	1
295	1	5	59	−4	1	1	414	1	9	46	5	3	−2
303	1	3	101	−5	2	1	418	1	11	38	3	1	−1
306	1	17	18	1	1	−1	420	1	15	28	−13	3	4
308	4	7	11	1	1	−1		1	20	21	1	1	−1
309	1	3	103	1	13	−4		3	4	35	1	2	−1
310	1	2	155	3	4	−1		5	7	12	1	1	−1
319	1	11	29	45	−119	86	425	1	17	25	2	1	−1
321	1	3	107	11	−9	2	428	1	4	107	1	−3	1
322	2	7	23	2	1	−1	429	3	11	13	−2	1	1
330	5	6	11	1	1	−1	430	1	2	215	−7	4	1
335	1	5	67	3	2	−1	435	1	3	145	4	3	−1
339	1	3	113	5	−7	2		1	5	87	17	−10	1
342	1	18	19	1	1	−1		1	15	29	17	−7	2
345	1	3	115	−17	11	2		3	5	29	2	1	−1
	1	5	69	4	1	−1	436	1	4	109	1	3	−1
	1	15	23	2	1	−1	438	1	3	146	−13	7	2
	3	5	23	−6	5	1	444	3	4	37	−17	8	7
346	1	2	173				445	1	5	89			
348	1	3	116	7	27	−8	446	1	2	223	3	−5	1
	1	4	87	−7	4	1	447	1	3	149	5	2	−1
	1	12	29	−5	2	1	450	2	9	25	2	1	−1
	3	4	29	1	−2	1	452	1	4	113	109	49	−25
355	1	5	71	4	−3	1	453	1	3	151	−7	4	1
356	1	4	89	589	183	−137	454	1	2	227	−20331	15485	1627

Table 2^b (continued).

A	a	b	c	x	y	z	A	a	b	c	x	y	z
460	4	5	23	1	−5	3	483	1	7	69	−5	2	1
462	1	6	77	−5	2	1	484	1	4	121	−5	1	1
	1	21	22	1	1	−1	490	2	5	49	−3	1	1
	2	7	33	2	5	−3	493	1	17	29	32	7	−11
	3	11	14	1	1	−1	495	1	9	55	−4	1	1
465	1	15	31	−22	1	7	497	1	7	71	4	1	−1
466	1	2	233	119	138	−31	498	1	2	249	1	−5	1
468	4	9	13	1	1	−1		1	3	166	−11	1	2
473	1	11	43					1	6	83	67	−38	7
474	2	3	79	1	−3	1		2	3	83	1	3	−1
477	1	9	53	−5	2	1							

Table 2^c.

Values of $A \leqq 1000$ with 13 possible equations $ax^3 + by^3 + cz^3 = 0$, $abc = A$, only one of which is soluble.

A	a	b	c	x	y	z
$330 = 2 \cdot 3 \cdot 5 \cdot 11$	5	6	11	1	1	−1
$510 = 2 \cdot 3 \cdot 5 \cdot 17$	2	15	17	1	1	−1
$660 = 3 \cdot 4 \cdot 5 \cdot 11$	4	11	15	1	1	−1
$690 = 2 \cdot 3 \cdot 5 \cdot 23$	1	2	345	7	1	−1
$870 = 2 \cdot 3 \cdot 5 \cdot 29$	1	29	30	1	1	−1

Table 3.

The equation $u^3 - 3u^2v + v^3 = 3^\lambda p w^3$, $\lambda = 0$ or 1, $9^{1-\lambda} p \leqq 500$.
Crosses: insoluble equations.

	p	u	v	w	p	u	v	w	p	u	v	w
$\lambda = 1$	1	1	2	1	163	1	8	1	$17 \cdot 19$	11	1	1
	17	5	1	1	179	283	86	17	359	49	731	71
	19	7	2	1	181		×		19^2		×	
	37	1	5	1	197	20	31	1	379	25	8	1
	53	29	10	1	199		×		397	13	2	1
	71	8	13	1	233	77	118	1	431	11	19	1
	73		×		251	38	13	1	433	1	11	1
	89	2	7	1	269	2189	757	37	449	5	13	1
	107	8	1	1	271	10	17	1	467	23	7	1
	109		×		17^2	4	11	1	487		×	
	127	16	5	1	307		×					
$\lambda = 0$	1	1	0	1	19	1	3	1	53	1	4	1
	17	4	1	0	37	5	8	1				

Table 4.

Cubefree values of $A \leqq 500$ for which the equation

$$X^3 + Y^3 = AZ^3$$

has only the trivial solution with $Z = 0$.

4a. Values covered by Theorem VIII.

$A = 3$

$A = q_1 \equiv 2 \pmod 9$: (2), 11, 29, 47, 83, 101, 137, 173, 191, 227, 263, 281, 317, 353, 389, 443, 461, 479

$A = q_2 \equiv 5 \pmod 9$: 5, 23, 41, 59, 113, 131, 149, 167, 239, 257, 293, 311, 347, 383, 401, 419, 491

$A = q_1^2$: $2^2 = 4$, $11^2 = 121$

$A = q_2^2$: $5^2 = 25$

Other combinations.

	2	9	11	5^2	29	47	83	101
2^2	—	36	44	100	116	188	332	404
5	10	45	55	—	145	235	415	
9	18	—	99	225	261	423		
23	46	207	253					
41	82	369	451					
59	118							
113	226							
11^2	242							
131	262							
149	298							
167	334							
239	478							

4b. Values of A with 4 possible equations

$$ax^3 + by^3 + cz^3 = 0,\ abc = A,$$

which have all been proved insoluble (Theorem IX).

60, 66, 102, 138, 150, 165, 174, 204, 220, 230, 255, 276, 290, 300, 318, 340, 354, 374, 410, 426, 470, 492

4^c. Combinations covered by Theorem XI.

	2	3	2^2	5	11	17	23	5^2	47	53
7	14	21	—	—	77	119	—	175	329	371
13	—	39	52	—	—	221	299	—		
19	38	57	76	95	—	—	437	475		
31	—	93	—	155						
37	74	111	148	185						
43	—	129	—	—						
7^2	—	147	196	245						
61	122	—	—	—						
67	—	—	268	—						
73	146	—	292	365						
79	158	237	—							
97	194	291	—							
103	—	—	412							
109	—	327								
127	—	381								
139	—	417								
151	302	—								
157	—	471								
163	326	489								
13^2	338									
181	362									
199	398									
241	482									

4^d. Values of A covered by Theorem XII.

$234 = 9 \cdot 2 \cdot 13$ $\quad$ $154 = 2 \cdot 11 \cdot 7$
$252 = 9 \cdot 2^2 \cdot 7$ $\quad$ $190 = 2 \cdot 5 \cdot 19$
$315 = 9 \cdot 5 \cdot 7$ $\quad$ $260 = 2^2 \cdot 5 \cdot 13$
$350 = 2 \cdot 5^2 \cdot 7$
$406 = 2 \cdot 29 \cdot 7$
$442 = 2 \cdot 17 \cdot 13$
$476 = 2^2 \cdot 17 \cdot 7$

4^e. Values of A with two prime factors $r \equiv 1 \pmod 3$.

$266 = 2 \cdot 7 \cdot 19$ $\quad$ $364 = 2^2 \cdot 7 \cdot 13$ $\quad$ $434 = 2 \cdot 7 \cdot 31$ $\quad$ $455 = 5 \cdot 7 \cdot 13$

4^f. Values of A with four possible but insoluble descents 9.6.1, including $a + b\varrho = \varrho$ (identical with the crossed values of Table 3).

73, 109, 181, 199, 307, 487 (all primes); $361 = 19^2$

4^g. A complete list of the insoluble values in the Tables 4^{a-f}.

3, 4, 5, 10, 11, 14, 18, 21, 23, 25, 29, 36, 38, 39, 41, 44, 45, 46, 47, 52, 55, 57, 59, 60, 66, 73, 74, 76, 77, 82, 83, 93, 95, 99

100, 101, 102, 109, 111, 113, 116, 118, 119, 121, 122, 129, 131, 137, 138, 145, 146, 147, 148, 149, 150, 154, 155, 158, 165, 167, 173, 174, 175, 181, 185, 188, 190, 191, 194, 196, 199

204, 207, 220, 221, 225, 226, 227, 230, 234, 235, 237, 239, 242, 245, 252, 253, 255, 257, 260, 261, 262, 263, 266, 268, 276, 281, 290, 291, 292, 293, 298, 299

300, 302, 307, 311, 315, 317, 318, 326, 327, 329, 332, 334, 338, 340, 347, 350, 353, 354, 361, 362, 364, 365, 369, 371, 374, 381, 383, 389, 398

401, 404, 406, 410, 412, 415, 417, 419, 423, 426, 434, 437, 442, 443, 451, 455, 461, 470, 471, 475, 476, 478, 479, 482, 487, 489, 491, 492

Table 5.

Non-excluded equations $3auv(u-v) + b(u^3 - 3u^2v + v^3) = \frac{s}{3t} A_1 w^3$

with $A = A_1 \cdot N(a + b\varrho)$ cubefree and $\leqq 500$, $a + b\varrho \neq \pm 1, \pm\varrho, \pm\varrho^2$

(conjugate values $a + b\varrho$ and $a + b\varrho^2$ not considered separately).

$\frac{s}{3t} = 3$ in Case I and II, $= \frac{1}{9}$ in Case III (Ch. IX, §§ 3 and 6).

A	a	b	A_1	Case	u	v	w	A	a	b	A_1	Case	u	v	w
7	1	3	1	I, II	1	2	1	127	13	6	1	I	1	6	2
13	4	3	1	I	1	0	1		6	13	1	II	1	2	1
19	5	3	1	I	1	0	1		13	7	1	II	5	4	1
	3	5	1	II	2	1	1	$133 = 7 \cdot 19$	5	3	7	I, II	2	1	1
	5	2	1	II	2	1	2	$134 = 2 \cdot 67$	9	2	2	II	2	1	2
$26 = 2 \cdot 13$	1	4	2	II	1	2	1	139	13	3	1	I	1	0	1
$28 = 2^2 \cdot 7$	3	2	4	II	2	1	1	$143 = 11 \cdot 13$	1	4	11	II	5	1	2
31	1	6	1	I	3	1	2	151	14	9	1	I, II	3	2	3
$35 = 5 \cdot 7$	3	1	5	II	2	1	1	157	13	12	1	I	43	132	28
37	7	3	1	I	1	0	1	$161 = 7 \cdot 23$	3	1	23	II	5	4	1
	3	7	1	II	1	2	1	163	14	3	1	I	1	0	1
	7	4	1	II	1	5	2		3	14	1	II	1	2	2
43	7	6	1	I, II	2	1	2		14	11	1	II	7	5	1
$49 = 7^2$	8	3	1	I	1	0	1	$169 = 13^2$	8	15	1	I, II	2	1	1
61	5	9	1	I, II	2	1	1	$172 = 2^2 \cdot 43$	7	6	4	I	3	2	1
$62 = 2 \cdot 31$	1	6	2	I	1	0	1	$182 = 2 \cdot 7 \cdot 13$	11	6	2	I, II	1	0	1
$63 = 3^2 \cdot 7$	3	1	9	III	1	0	1	$183 = 3 \cdot 61$	4	9	3	I	1	0	1
$65 = 5 \cdot 13$	4	3	5	I, II	2	1	1	193	16	9	1	I	44	227	129
67	2	9	1	I	3	8	9	$201 = 3 \cdot 67$	2	9	3	I	1	0	1
79	10	3	1	I, II	1	0	1	$203 = 7 \cdot 29$	1	3	29	I	4	1	1
$86 = 2 \cdot 43$	7	6	2	I	1	0	1	$206 = 2 \cdot 103$	11	2	2	II	1	17	5
$91 = 7 \cdot 13$	1	3	13	I	1	3	1	$209 = 11 \cdot 19$	5	3	11	I, II	3	2	1
	4	1	7	II	2	1	1	211	1	15	1	I	2	15	25
	1	10	1	II	1	2	2	$215 = 5 \cdot 43$	1	7	5	II	1	2	1
	5	11	1	II	1	2	1	$217 = 7 \cdot 31$	3	2	31	II	7	2	2
97	11	3	1	I, II	1	0	1		6	5	7	II	2	1	1
$98 = 2 \cdot 7^2$	3	8	2	II	1	2	1		8	17	1	II	1	2	1
103	11	9	1	I	1	4	3		16	3	1	I	1	0	1
$117 = 3^2 \cdot 13$	4	1	9	III	1	0	1	$218 = 2 \cdot 109$	5	12	2	I, II	1	2	1
$124 = 2^2 \cdot 31$	1	6	4	I, II	1	2	1	$219 = 3 \cdot 73$	1	9	3	I	1	0	1
$126 = 2 \cdot 3^2 \cdot 7$	3	2	18	III	1	0	1	223	17	6	1	I, II	3	2	4

Table 5 (continued).

A	a	b	A_1	Case	u	v	w	A	a	b	A_1	Case	u	v	w
229	17	12	1	I	1	4	2	$387 = 3^2 \cdot 43$	7	1	9	III	1	0	1
241	16	15	1	I, II	3	2	1	$388 = 2^2 \cdot 97$	11	8	4	II	4	17	7
$244 = 2^2 \cdot 61$	9	4	4	II	5	4	2	$395 = 5 \cdot 79$	3	10	5	II	13	23	2
$247 = 13 \cdot 19$	17	3	1	I	1	0	1	397	23	12	1	I	4	3	4
$254 = 2 \cdot 127$	13	6	2	I, II	1	0	1		12	23	1	II	2	1	1
$259 = 7 \cdot 37$	5	18	1	I, II	1	2	2		23	11	1	II	17	7	29
271	19	9	1	I	1	6	3	$399 = 3 \cdot 7 \cdot 19$	13	9	3	I	1	0	1
	9	19	1	II	1	2	1	$403 = 13 \cdot 31$	4	3	31	I, II	1	5	1
	19	10	1	II	14	1	22	$407 = 11 \cdot 37$	7	3	11	I, II	2	1	1
$273 = 3 \cdot 7 \cdot 13$	10	9	3	I	1	0	1	409	23	15	1	I			
277	19	12	1	I, II	1	5	4	$413 = 7 \cdot 59$	3	2	59	II	5	22	2
$278 = 2 \cdot 139$	13	10	2	II	2	1	2	421	1	21	1	I, II	8	19	29
$279 = 3^2 \cdot 31$	6	1	9	III	1	0	1	$422 = 2 \cdot 211$	15	14	2	II	2	1	2
283	19	6	1	I				$427 = 7 \cdot 61$	22	3	1	I	1	0	1
$287 = 7 \cdot 41$	1	3	41	I	1	4	1	433	11	24	1	I	1	0	2
$301 = 7 \cdot 43$	2	3	43	I	5	2	1		24	11	1	II	13	77	11
$305 = 5 \cdot 61$	9	5	5	II	1	5	1		24	13	1	II	1	5	1
$309 = 3 \cdot 103$	11	9	3	I	1	0	1	$436 = 2^2 \cdot 109$	5	12	4	I	1	0	1
313	19	3	1	I, II	1	0	1	439	23	18	1	I, II	7	5	2
$314 = 2 \cdot 157$	13	12	2	I	3	2	1	$441 = 3^2 \cdot 7^2$	5	8	9	III	1	0	2
$316 = 2^2 \cdot 79$	3	10	4	II	1	2	1	$446 = 2 \cdot 223$	17	6	2	I	1	0	1
$325 = 5^2 \cdot 13$	4	3	25	I	3	1	1	$453 = 3 \cdot 151$	14	9	3	I	1	0	1
331	10	21	1	I, II	1	2	1	457	7	24	1	I, II	1	0	2
$335 = 5 \cdot 67$	2	9	5	I, II	1	2	1	$458 = 2 \cdot 229$	17	12	2	I	43	31	22
337	8	21	1	I				463	22	21	1	I	1	3	1
$341 = 11 \cdot 31$	6	1	11	II	2	1	1	$468 = 2^2 \cdot 3^2 \cdot 13$	3	4	36	III	1	0	1
$342 = 2 \cdot 3^2 \cdot 19$	5	2	18	III	1	0	1	$469 = 7 \cdot 67$	3	2	67	II	1	11	2
349	20	3	1	I, II	1	0	1		9	7	7	II	7	5	1
367	22	9	1	I, II	23	1	35		13	25	1	II	2	1	1
$370 = 2 \cdot 5 \cdot 37$	7	4	10	II	2	1	1		23	3	1	I	1	0	1
373	4	21	1	I	5	2	1	$473 = 11 \cdot 43$	7	6	11	I			
$377 = 13 \cdot 29$	3	4	29	II	4	11	2	$481 = 13 \cdot 37$	5	24	1	I	1	0	2
379	22	15	1	I	1	4	1	$485 = 5 \cdot 97$	3	11	5	II	1	2	1
	15	22	1	II	2	1	2	$494 = 2 \cdot 13 \cdot 19$	5	2	26	II	5	4	1
	22	7	1	II	35	1	39	$497 = 7 \cdot 71$	1	3	71	I, II	5	1	1
$386 = 2 \cdot 193$	9	16	2	II	2	1	1	499	25	18	1	I			

Table 6.

The number g of generators and the basic solutions of the equation $X^3 + Y^3 = AZ^3$, A cubefree and $\leqq 500$.

A	g	(X, Y, Z)	A	g	(X, Y, Z)
6	1	(37, 17, 21)	90	1	(1 241, −431, 273)
7	1	(2, −1, 1)	91	2	(4, 3, 1), (6, −5, 1)
9	1	(2, 1, 1)	92	1	(25 903, −3 547, 5 733)
12	1	(89, 19, 39)	94	1	(15 642 626 656 646 177, −15 616 184 186 396 177, 590 736 058 375 050)
13	1	(7, 2, 3)			
15	1	(683, 397, 294)			
17	1	(18, −1, 7)	97	1	(14, −5, 3)
19	2	(3, −2, 1), (5, 3, 2)	98	1	(5, −3, 1)
20	1	(19, 1, 7)	103	1	(592, −349, 117)
22	1	(25 469, 17 299, 9 954)	105	1	(4 033, 3 527, 1 014)
26	1	(3, −1, 1)	106	1	(165 889, −140 131, 25 767)
28	1	(3, 1, 1)	107	1	(90, 17, 19)
30	2	(163, 107, 57), (289, −19, 93)	110	2	(181, −71, 37), (629, 251, 134)
31	1	(137, −65, 42)	114	1	(9 109, −901, 1 878)
33	1	(1 853, 523, 582)	115	1	(5 266 097, −2 741 617, 1 029 364)
34	1	(631, −359, 182)	117	1	(5, −2, 1)
35	1	(3, 2, 1)	123	1	(184 223 499 139, 10 183 412 861, 37 045 412 880)
37	2	(4, −3, 1), (10, −1, 3)			
42	1	(449, −71, 129)	124	2	(5, −1, 1), (479, −443, 57)
43	1	(7, 1, 2)	126	2	(5, 1, 1), (71, −23, 14)
49	1	(11, −2, 3)	127	2	(7, −6, 1), (121, −120, 7)
50	1	(23 417, −11 267, 6 111)	130	1	(52 954 777, 33 728 183, 11 285 694)
51	1	(730 511, 62 641, 197 028)	132	2	(2 089, −901, 399), (39 007, −29 503, 6 342)
53	1	(1 872, −1 819, 217)	133	1	(5, 2, 1)
58	1	(28 747, −14 653, 7 083)	134	1	(9, 7, 2)
61	1	(5, −4, 1)	139	1	(16, −7, 3)
62	1	(11, 7, 3)	140	1	(27 397, 6 623, 5 301)
63	1	(4, −1, 1)	141	1	(53 579 249, −52 310 249, 4 230 030)
65	2	(4, 1, 1), (191, −146, 39)	142	1	(2 454 839, 1 858 411, 530 595)
67	1	(5 353, 1 208, 1 323)	143	1	(73, 15, 14)
68	1	(2 538 163, −472 663, 620 505)	151	1	(338, −95, 63)
69	1	(15 409, −10 441, 3 318)	153	2	(70, −19, 13), (107, −56, 19)
70	1	(53, 17, 13)	156	1	(2 627, −1 223, 471)
71	1	(197, −126, 43)	157	1	(19 964 887, −19 767 319, 1 142 148)
75	1	(17 351, −11 951, 3 606)	159	1	(103 750 849, 2 269 079, 19 151 118)
78	1	(5 563, 53, 1 302)	161	1	(39, −16, 7)
79	1	(13, −4, 3)	163	2	(11, −3, 2), (17, −8, 3)
84	1	(433, 323, 111)	164	1	(311 155 001, −236 283 589, 46 913 867)
85	1	(2 570 129, −2 404 889, 330 498)			
86	2	(13, 5, 3), (10 067, −10 049, 399)	166	1	(1 374 582 733 040 071, −1 295 038 816 428 439, 136 834 628 063 958)
87	1	(1 176 498 611, −907 929 611, 216 266 610)			
89	1	(53, 36, 13)			

Table 6 (continued).

A	g	(X, Y, Z)
169	1	(8, −7, 1)
170	1	(26 353, 14 957, 5 031)
171	1	(37, 20, 7)
172	1	(139, −103, 21)
177	1	(2 419 913 540 753, 1 587 207 867 247, 468 227 201 520)
178	1	(110 623 913, 8 065 063, 19 668 222)
179	1	(2 184 480, −1 305 053, 357 833)
180	1	(901, 719, 183)
182	2	(11, 5, 2), (17, 1, 3)
183	2	(14, 13, 3), (295 579, −190 171, 46 956)
186	1	(56 182 393, 15 590 357, 9 911 895)
187	1	(336 491, −149 491, 57 070)
193	1	(135 477 799, −116 157 598, 16 825 599)
195	1	(68 561, −54 521, 9 366)
197	1	(2 339, −2 142, 247)
198	1	(1 801, −19, 309)
201	2	(16, 11, 3), (3 251, 124, 555)
202	1	(2 884 067, 257 437, 491 652)
203	2	(229, 32, 39), (2 426, −2 165, 273)
205	1	(8 191, −6 551, 1 094)
206	1	(5 211, −4 961, 455)
209	2	(52, −41, 7), (125, −26, 21)
210	2	(1 387, 503, 237), (3 961, −2 071, 633)
211	1	(74 167, 66 458, 14 925)
212	1	(337 705 939 853, −315 091 652 237, 32 429 956 428)
213	1	(64 313 150 142 602 539 525 717, 46 732 739 212 871 851 099 283, 12 000 095 230 802 028 099 750)
214	1	(307 277 703 127, −244 344 663 377, 40 697 090 945)
215	1	(6, −1, 1)
217	2	(6, 1, 1), (9, −8, 1)
218	2	(7, −5, 1), (279 469, −61 469, 46 270)
219	2	(17, 10, 3), (168 704, −36 053, 27 897)
222	1	(5 884 597, 858 653, 972 855)
223	1	(509, 67, 84)
228	1	(46 323 521, −27 319 949, 7 024 059)
229	1	(745, −673, 78)
231	1	(818 567, −369 503, 129 186)
233	1	(124 253, −124 020, 3 589)
236	1	(248 957, 209 827, 47 106)
238	1	(53 927, 3 907, 8 703)
241	1	(292, −283, 21)
244	1	(99, −67, 14)
246	2	(571 049, −511 271, 59 787), (2 043 883, −1 767 133, 230 685)
247	1	(20, −11, 3)
249	1	(275 657 307 291 045 075 203 684 958 997, −275 522 784 968 298 556 737 485 593 813, 4 974 480 998 065 387 679 603 368 524)
251	1	(4 284, −4 033, 373)
254	2	(19, −1, 3), (587, 437, 104)
258	1	(2 195 839, −2 047 231, 198 156)
259	1	(13, −5, 2)
265	1	(36 326 686 731 109 813, 9 746 422 253 537 867, 5 691 827 727 610 864)
267	1	(861 409, −342 361, 130 914)
269	1	(800 059 950, −786 434 293, 45 728 263)
271	2	(10, −9, 1), (487, −216, 73)
273	2	(19, 8, 3), (190, −163, 21)
274	1	(111 035 496 427 236 122 887, −43 257 922 194 314 055 637, 16 751 541 717 010 945 845)
275	1	(424 560 439, −309 086 839, 55 494 828)
277	1	(209, −145, 28)
278	1	(13, 3, 2)
279	1	(7, −4, 1)
282	2	(117 217, −96 913, 13 542), (2 814 607, 1 571 057, 452 772)
283	$\leqq 1$	
284	1	(7 722 630 462 000 896 449 941 136 589, −1 293 813 622 621 939 303 367 981, 1 174 877 194 362 780 234 594 343 698)
285	1	(18 989, 1 531, 2 886)
286	1	(323, −37, 49)
287	1	(248, −121, 39)
289	1	(199, 90, 31)
294	1	(124 559, −103 391, 14 118)
295	1	(34 901, −16 021, 5 068)
301	1	(382, 5, 57)
303	1	(2 659 949, 67 051, 396 030)
305	1	(86, −81, 7)
306	1	(6 697, −3 943, 921)
308	1	(199, 109, 31)
309	2	(20, 7, 3), (272 540 932, −142 217 089, 38 305 371)
310	1	(5 011 613, −190 493, 740 484)

Table 6 (continued).

A	g	(X, Y, Z)
313	1	(22, −13, 3)
314	1	(241, −223, 21)
316	1	(7, −3, 1)
319	1	(6 462 443 919 765 751 305 499, −6 182 025 219 694 143 438 499, 472 407 353 310 304 561 590)
321	1	(13 755 277 819, 8 670 272 669, 2 164 318 002)
322	1	(1 873, 703, 278)
323	1	(252, 71, 37)
325	1	(128, 97, 21)
330	1	(1 621, 1 349, 273)
331	1	(11, −10, 1)
333	1	(397, −286, 49)
335	2	(7, −2, 1), (390 997, 260 243, 61 362)
337	$\not\equiv$ 1	
339	1	(1 392 097 139, −345 604 139, 198 626 610)
341	1	(6, 5, 1)
342	2	(7, −1, 1), (1 253, −1 205, 86)
345	2	(16 543, 8 297, 2 454), (389 699, −190 979, 53 292)
346	$\not\equiv$ 1	
348	2	(40 283, −15 227, 5 622), (2 706 139, 425 861, 385 230)
349	1	(23, −14, 3)
355	1	(2 903 959, 2 617 001, 492 516)
356	1	(15 026 630 492 061 476 041 947 013, 4 709 632 110 011 335 573 393 177, 2 098 221 141 580 681 446 554 589)
357	1	(19 207, 6 497, 2 742)
358	1	(7 951 661, 2 922 589, 1 138 095)
359	1	(77 517 180, 50 972 869, 11 855 651)
363	1	(1 909 159 356 457, −1 746 345 039 913, 165 073 101 648)
366	1	(2 087 027, −1 675 277, 228 885)
367	1	(42 349, 526. 5 915)
370	2	(7, 3, 1), (70 523, 19 387, 9 891)
372	1	(2 717 893, 630 107, 379 470)
373	1	(1 604, −1 595, 57)
377	1	(469, −237, 62)
379	2	(15, −7, 2), (917, −908, 39)
380	1	(1 009, −629, 127)
382	$\not\equiv$ 1	

A	g	(X, Y, Z)
385	1	(20 521, −17 441, 2 054)
386	1	(9, −7, 1)
387	1	(8, −5, 1)
388	1	(4 659, −3 287, 553)
390	2	(3 043, 467, 417), (4 373, −863, 597)
391	1	(590 456 252 061 289, −171 359 229 789 289, 80 084 103 077 160)
393	1	(4 045 451 855 513 988 711 059, 2 369 372 172 284 459 347 309, 587 046 969 413 536 968 336)
394	1	(1 439 245 403, −573 627 403, 192 088 390)
395	1	(7 891, −7 851, 266)
396	1	(46 789 273, −37 009 657, 5 074 314)
397	2	(12, −11, 1), (360, 37, 49)
399	2	(22, 5, 3), (401, 328, 63)
402	1	(585 699 417 548 405 371, 102 798 361 240 815 491, 79 502 362 839 530 631)
403	1	(53, −22, 7)
407	2	(7, 4, 1), (33 733, −33 634, 939)
409	$\not\equiv$ 1	
411	1	(186 871 897, 49 864 103, 25 292 280)
413	1	(2 575, −2 103, 266)
414	1	(68 073 157, 32 528 843, 9 454 410)
418	1	(76 267, 25 307, 10 323)
420	2	(2 213, 1 567, 327), (10 459, −6 679, 1 263)
421	1	(19 690, 4 699, 2 639)
422	1	(15, 1, 2)
425	1	(2 393, 1 007, 326)
427	1	(25, −16, 3)
428	1	(1 294 057, −1 190 053, 104 013)
429	1	(16 739, 14 149, 2 598)
430	1	(5 989 967, 3 449 393, 841 204)
431	1	(701, −270, 91)
433	2	(37, 35, 6), (223, −222, 7)
435	2	(32 779, −1 459, 4 326), (3 784 049, 2 981 071, 570 276)
436	2	(19, 17, 3), (1 330 019, −1 224 071, 105 957)
438	1	(12 636 764 083, 11 127 850 973, 1 979 215 602)
439	1	(571, −563, 26)

Table 6 (continued).

A	g	(X, Y, Z)	A	g	(X, Y, Z)
441	1	(13, 11, 2)	465	1	(1 212 356 942 047, −1 197 072 217 207, 52 307 828 958)
444	1	(4 174 254 535 499, −726 500 109 131, 546 201 297 768)	466	1	(464 540 708 319 337 302 841, 88 798 763 256 715 446 551, 60 057 801 943 830 995 598)
445	$\leqq 1$				
446	2	(23, −5, 3), (4 286 417, −4 285 265, 52 212)			
447	1	(4 405 301, −382 301, 576 030)	467	1	(1 170, −703, 139)
449	1	(323, 126, 43)	468	2	(7, 5, 1), (859, −763, 74)
450	1	(21 079, 11 321, 2 886)	469	2	(13, −12, 1), (26, −17, 3)
452	1	(851 498 679 025 552 429, 224 535 817 897 760 071, 111 626 729 681 785 675)	473	$\leqq 2$	
			474	1	(568 871, −453 689, 57 627)
			477	2	(89, 70, 13), (12 040, −11 881, 523)
453	2	(23, 4, 3), (50 167 097, 39 331 207, 7 447 188)	481	1	(43, 29, 6)
			483	1	(2 401 741, 1 945 259, 352 830)
454	1	(753 389 202 595 029 867 852 290 245 746 241 110 629, −204 264 638 826 527 324 892 641 927 694 862 943 879, 97 368 775 947 767 167 139 892 682 703 702 288 385)	484	1	(236 521, −176 021, 25 235)
			485	1	(8, −3, 1)
			490	1	(193 229, −74 159, 24 039)
			493	1	(8 432 715 268 961, −1 057 596 310 369, 1 066 758 076 384)
			494	1	(59, −33, 7)
457	1	(41, 31, 6)	495	1	(342 361, −57 241, 43 212)
458	1	(953 039, −761 375, 97 482)	497	2	(55, 16, 7), (7 411, −6 772, 579)
460	1	(248 768 189, −234 795 689, 17 466 345)	498	2	(611 137, −490 123, 60 543), (15 811 001, −15 250 751, 933 765)
462	2	(3 779, 379, 489), (11 969, −7 811, 1 389)			
463	1	(403, −394, 21)	499	$\leqq 1$	

References.

Bachmann, P.: [1] "Die Lehre von der Kreistheilung", Leipzig 1872.

Billing, G.: [1] "Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins", Nova Acta Reg. Soc. Sci. Upsaliensis, Ser. IV, 11, 1938, No. 1.

Cassels, J.: [1] "The rational solutions of the Diophantine equation $Y^2 = X^3 - D$", Acta math. 82, 1950, pp. 243—73. — [2] "Addenda and corrigenda to [1]", Acta math. 84, 1951, p. 299.

Desboves, A.: [1] "Résolution, en nombres entiers et sous sa forme la plus générale, de l'équation cubique, homogène, à trois inconnues", Nouv. Ann. de Math., Ser. III, 5, 1886, pp. 545—79.

Dickson, L.: [1] "History of the theory of numbers", Vol. II (Diophantine analysis), Carnegie Publ. No. 256.

Faddeev, D.: [1] "On the equation $x^3 + y^3 = Az^3$", Trav. de l'inst. phys. math. Stekloff (Section Math.), 5, 1934, pp. 25—40 (Russian).

Gauss, C.: [1] Werke, Bd. I (Disquisitiones Arithmeticae).

HASSE, H.: [1] "Über die Riemannsche Vermutung in Funktionenkörpern", C. R. du Congr. Int. Math. Oslo 1936, Vol. I, pp. 189—206.

HOLZER, L.: [1] "Über die Gleichung $x^3 + y^3 = Cz^3$", J. f. Math. 159, 1928, pp. 93—100.

HURWITZ, A.: [1] "Über ternäre Diophantische Gleichungen dritten Grades", Vierteljahrschr. d. Naturf. Ges. in Zürich, 62, 1917, pp. 207—29. — [2] "Über die Kongruenz $ax^e + by^e + cz^e \equiv 0 \pmod{p}$", J. f. Math. 136, 1909, pp. 272—92.

KANTOR, R.: [1] "Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen", Monatshefte f. Math. u. Phys., 26, 1915, pp. 24—39.

KRAITCHIK, M.: [1] "Recherches sur la théorie des nombres", Paris 1924.

LANDAU, E.: [1] "Vorlesungen über Zahlentheorie", Bd. I, Leipzig 1927.

LEGENDRE, A.: [1] "Essai sur la théorie des nombres", 2. ed., Paris 1808.

LJUNGGREN, W.: [1] "Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante", Acta math. 75, 1942, pp. 1—21.

MARKOFF A.: [1] "Sur les nombres entiers dépendents d'une racine cubique d'un nombre entier ordinaire", Mém. de l'Acad. Imp. des Sciences de St. Pétersbourg, Ser. VII, 38, 1892, No. 9.

MORDELL, L.: [1] "A remark on indeterminate equations in several variables", Journ. London Math. Soc., 12, 1937, pp. 127—29. — [2] "The number of solutions of some congruences in two variables", Math. Zeitschr. 37, 1933, pp. 193—209.

NAGELL, T.: [1] "L'analyse indéterminée de degré supérieur", Mémorial des Sciences Math., 39, 1929. — [2] "Sur la classification des cubiques planes du premier genre par des transformations birationnelles dans un domaine de rationalité quelconque", Nova Acta Reg. Soc. Sci. Upsaliensis, Ser. IV, 12, 1941, No. 8. — [3] "Les points exceptionnels sur les cubiques planes du premier genre", II, ibid. 14, 1946, No. 3. — [4] "Sur la résolubilité des équations Diophantiennes cubiques à deux inconnues dans un domaine relativement algébrique", ibid. 13, 1942, No. 3. — [5] "Sur les propriétés arithmétiques des cubiques planes du premier genre", Acta math. 52, 1928—29, pp. 93—126. — [6] "Über die Einheiten in reinen kubischen Zahlkörpern", Skrifter Vid. Selsk. Christiania, I, Mat. nat. Kl. 1923, No. 11. — [7] "Zahlentheoretische Notizen. I—VI", ibid. No. 13.

PÉPIN, S., FATHER: [1] "Sur la décomposition d'un nombre entier en une somme de deux cubes rationnels", Journ. d. Math. (Liouville), Sér. II, 15, 1870, pp. 217—36. — [2] "Sur certains nombres complexes compris dans la formule $a + b\sqrt{-c}$", ibid. Sér. III, 1, 1875, pp. 317—72 (especially pp. 360—72). — [3] "Mémoire sur l'équation indéterminée $x^3 + y^3 = Az^3$", Atti dell' Accad. pont. de' Nuovi Lincei, 34, 1880—81, pp. 73—130. — [4] "Démonstration d'un théorème de M. Sylvester sur les diviseurs d'une fonction cyclotomique", Comptes Rendus, Vol. 90, 1880, pp. 526—28.

PODSYPANIN, V.: [1] "On the indeterminate equation $x^3 = y^2 + Az^6$", Mat. Sbornik N. S. 24 (66), 1949, pp. 391—403 (Russian).

SELMER, E.: [1] "Homogenous Diophantine equations", Comptes rendus du 11 congr. des math. scandinaves, Trondheim 22—25 août 1949, No. 42.

SKOLEM, T.: [1] "Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist", Oslo Vid. Akad. Avh., I, Mat. nat. Kl., 1942, No. 4. — [2] "Zwei Sätze über kubische Kongruenzen", Kgl. Norske Vid. Selsk. Forhandl. 10, 1937, No. 24.

SOMMER, J.: [1] "Vorlesungen über Zahlentheorie", Berlin 1907.

VON STERNECK, R.: [1] "Über die Anzahl inkongruenter Werte, die eine ganze Funktion dritten Grades annimmt", Sitz. ber. d. K. Akad. d. Wiss. Wien, Math. Nat. Kl., Bd. 116, II^a, 1907, pp. 895—904.

SYLVESTER, J.: [1] "On certain ternary cubic-form equations", Coll. Math. Papers (Cambridge 1909), Vol. III, pp. 312—91 (especially pp. 312—16 and 347—50). Originally appeared in Amer. Journ. Math., 2, 1879, pp. 280—85, 357—93, and 3, 1880, pp. 58—88, 179—89.