ARKIV FÖR MATEMATIK Band 4 nr 35

Communicated 13 January 1960 by T. NAGELL

The diophantine equation $2^n = x^2 + 7$

By L. J. MORDELL

This paper deals with the following

Theorem. *The only solutions in integers $x > 0$ of the equation*

$$2^n = x^2 + 7 \tag{1}$$

are given by

$$\begin{aligned} &n = 3, x = 1,\\ &n = 4, x = 3,\\ &n = 5, x = 5,\\ &n = 7, x = 11,\\ &n = 15, x = 181. \end{aligned} \tag{2}$$

In 1913, Ramanujan gave these values (2) in Problem (465), page 120 of Vol. 5 of the *Journal of the Indian Mathematical Society*, and asked whether there were other values of n. In Ramanujan's collected works, there is a reference on page 327 to "Solution by K. J. Sanjana and T. P. Trevedi on pages 227, 228 also of Vol. 5." This, however, is merely a verification for some values of n.

On page 272 of Nagell's *Introduction to Number Theory,* the theorem is set as a problem. The enunciation is preceded by the problem, to show by considering the quadratic field $R(\sqrt{-7})$ in which factorization is unique, that the only rational integer solutions of

$$x^2 + x + 2 = y^3 \tag{3}$$

are given by $y = 2$. It seems to be implied that the same method will suffice for a proof of the theorem.

The theorem was proved by Chowla, D. J. Lewis, and Skolem in a joint paper submitted in 1958 for publication in the *Proceedings of the American Mathematical Society.*[1] The question was brought to my notice by Professor Chowla. I have found the present solution which is entirely different from theirs, which I had not seen when this paper was written.

[1] It has since appeared in Vol. 10 (1959) 663–669. Professor Nagell now informs me that he published (in Norwegian) a simple proof of the theorem in the Norsk Matematisk Tidsskrift 30 (1948) 62–64.

We note first that the only even value of n occurs when $n=4$. For then

$$(2^{\frac{1}{2}n}+x)(2^{\frac{1}{2}n}-x)=7,$$

and so $$2^{\frac{1}{2}n}+x=7,\ 2^{\frac{1}{2}n}-x=1,\ 2^{\frac{1}{2}n}=4,$$

and $$n=4,\ x=3.$$

This is also the only solution for which $x \equiv 0 \pmod 3$.
For then, all to mod 3,

$$2^n-1\equiv 0,$$

or $$(-1+3)^n-1\equiv 0,\ (-1)^n-1\equiv 0,$$

and so n is even.

We now investigate the solutions for which n is odd and $x \not\equiv 0 \pmod 3$. Corresponding to the cases $n=3m,\ 3m+1,\ 3m+2$, we have the respective equations,

$$y^3-7=x^2, \tag{4}$$

$$2y^3-7=x^2, \tag{5}$$

$$4y^3-7=x^2, \tag{6}$$

where $y=2^m$.

The equation (6) becomes Nagell's (3) when x in (6) is replaced by $2x+1$. Since x is odd, $\frac{1}{2}(x\pm\sqrt{-7})$ are coprime integers in the field $R(\sqrt{-7})$. Factorization is unique in this field, and the only units are ± 1. Hence,

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right)=y^3,$$

and so $$\frac{x+\sqrt{-7}}{2}=\left(\frac{a+b\sqrt{-7}}{2}\right)^3,$$

where a, b are rational integers and $a\equiv b \pmod 2$.
This gives

$$4=3a^2b-7b^3. \tag{7}$$

Since the right-hand side factorizes, we have

$$b=\pm 1,\ \pm 2,\ \pm 4;\ 3a^2-7b^2=\pm 4,\ \pm 2,\ \pm 1.$$

Hence $b=-1$, $a=\pm 1$, and $y=2$. Then $n=5$, $x=5$.

The field $R(\sqrt{-7})$ does not seem useful for equations (4), (5). Thus in (4), put $y=2z$, and so

$$\frac{x+\sqrt{-7}}{2}\cdot\frac{x-\sqrt{-7}}{2}=2z^3.$$

Since $$2=\left(\frac{1+\sqrt{-7}}{2}\right)\left(\frac{1-\sqrt{-7}}{2}\right),$$

we have now $$\frac{x+\sqrt{-7}}{2}=\left(\frac{1\pm\sqrt{-7}}{2}\right)\left(\frac{a+b\sqrt{-7}}{2}\right)^3,$$

or $$8=a^3-21ab^2\pm(3a^2b-7b^3).$$

It suffices to take the positive sign, and putting $a=X-2Y$, $y=Y$, we have

$$X^3-6XY^2+2Y^3=1. \tag{8}$$

The number θ defined by $\theta^3-6\theta+2=0$ has discriminant $\Delta(\theta)=4\cdot 6^3-27\cdot 2^2=4\cdot 9\cdot 21$, and so the study of the units in the field defined by θ, and this is required by (8), may not be simple.

For equations (4), (5), we use the cubic fields $R\left(\sqrt[3]{7}\right)$, $R\left(\sqrt[3]{28}\right)$, respectively. We recall that for the cubic field $R\left(\sqrt[3]{fg^2}\right)$, where f and g are square free and relatively prime, the integers are given by

$$a+b\sqrt{fg^2}+c^3\sqrt{f^2g},\ 1/3\left(a+b\sqrt[3]{fg^2}+c\sqrt[3]{f^2g}\right),$$

respectively according as $fg^2\not\equiv\pm 1$ or $fg^2\equiv\pm 1 \pmod 9$. Here, a, b, c are integers which when $fg^2\equiv\pm 1 \pmod 9$ are subjected to congruences (mod 3) which do not matter here. There is only one fundamental unit ε, say, and all the units are given by $\pm\varepsilon^r$ for integers r. The number[1] of classes of ideals in each of our two fields is 3, and so an equation $AB=C^2$, in integers, or in ideals

$$[AB]=[C]^2,$$

where $[A]$ and $[B]$ are principal ideals relatively prime to each other, and $[C]$ is a principal ideal, gives first $[A]=C_1^2$, $[B]=C_2^2$, where C_1, C_2 are ideals, and then since the class number is odd, C_1, C_2 are principal ideals. Hence we have an equation

$$A=\pm\varepsilon^r C_1^2,$$

where A, C_1 are integers, and on absorbing powers of ε in C_1, it suffices to consider only

$$A=\pm\varepsilon^r C_1^2,\ \text{where } r=0,1. \tag{9}$$

We note that the fundamental units in $R\left(\sqrt[3]{7}\right)$, $R\left(\sqrt[3]{28}\right)$, are

$$\varepsilon_1=2-\sqrt[3]{7},\ \varepsilon_2=1/3\left(-1-\sqrt[3]{28}+\sqrt[3]{98}\right),\ \text{respectively.} \tag{10}$$

We come back to equation (4). Here

$$\left(y-\sqrt[3]{7}\right)\left(y^2+\sqrt[3]{7}y+\sqrt[3]{49}\right)=x^2.$$

[1] A table of class numbers and fundamental units is given by Cassels for $R\left(\sqrt[3]{D}\right)$ with $D\leqslant 50$ in the *Acta Mathematica* (82) 1950, page 270.

The two factors here are relatively prime since x is prime to 21. Hence (9) gives

$$\pm\left(y - \sqrt[3]{7}\right) = \varepsilon_1^r \left(a + b\sqrt[3]{7} + c\sqrt[3]{49}\right)^2, \ (r = 0,1). \tag{11}$$

When $r = 0$, we have

$$\pm\left(y - \sqrt[3]{7}\right) = a^2 + 14\,b\,c + \sqrt[3]{7}\,(2\,a\,b + 7\,c^2) + \sqrt[3]{49}\,(b^2 + 2\,a\,c). \tag{12}$$

Hence $b^2 + 2\,a\,c = 0$, $2\,a\,b + 7\,c^2 = \pm 1$. Since $(b, c) = 1$, $c = \pm 1$, $a\,b = -3$, or -4, and it suffices to take $c = 1$, $b = 2$, $a = -2$, and then $\pm y = a^2 + 14\,b\,c$, and so $y = 32$, $n = 15$, and $x = 181$. Suppose next $r = 1$ in (11). Then multiplying (12) by $2 - \sqrt[3]{7}$, we have

$$\pm\left(y - \sqrt[3]{7}\right) = 2\,a^2 + 28\,b\,c - 7\,b^2 - 14\,a\,c + \sqrt[3]{7}\,(4\,a\,b + 14\,c^2 - a^2 - 14\,b\,c) + \\ + \sqrt[3]{49}(2\,b^2 + 4\,a\,c - 2\,a\,b - 7\,c^2).$$

Hence

$$\pm y = 2\,a^2 + 28\,b\,c - 7\,b^2 - 14\,a\,c, \tag{13}$$

$$\mp 1 = 4\,a\,b + 14\,c^2 - a^2 - 14\,b\,c, \tag{14}$$

$$0 = 2\,b^2 + 4\,a\,c - 2\,a\,b - 7\,c^2. \tag{15}$$

Equation (14) shows that a is odd, and equation (15) that c is even. Then equation (13) gives $\pm y \equiv 2 + b^2 \pmod 4$. Since $y = 2^m$, the only possibility is $y = 2$, $n = 3$, $x = 1$.

We now come to (5), which we write as $8\,y^3 - 28 = 4\,x^2$, i.e., say,

$$Y^3 - 28 = X^2, \tag{16}$$

or

$$\left(Y - \sqrt[3]{28}\right)\left(Y^2 + \sqrt[3]{28}\,Y + \sqrt[3]{28^2}\right) = X^2. \tag{17}$$

In the field $R\left(\sqrt[3]{28}\right)$, 2 becomes an ideal cube, and we have $2 = \left(2, \sqrt[3]{98}\right)^3 = P^3$, say. Since

$$Y^2 + \sqrt[3]{28}\,Y + \sqrt[3]{28^2} = \left(Y - \sqrt[3]{28}\right)^2 + 3\sqrt[3]{28}\,Y,$$

on noting that $X \not\equiv 0 \pmod 3$ but that X is even, we see that the only common ideal factor of the left-hand factors of (17) is P^2. This can be absorbed in the square of an ideal, and so

$$\pm\left(Y - \sqrt[3]{28}\right) = \varepsilon_2^r \left(\frac{a + b\sqrt[3]{28} + c\sqrt[3]{98}}{3}\right)^2, (r = 0,1). \tag{18}$$

Take first $r = 0$, then

$$\pm 9\left(Y - \sqrt[3]{28}\right) = a^2 + 28\,b\,c + \sqrt[3]{28}\,(2\,a\,b + 7\,c^2) + \sqrt[3]{98}\,(2\,a\,c + 2\,b^2). \tag{19}$$

Hence $$ac+b^2=0,\ 2ab+7c^2=\pm 9.$$

Clearly $(b, c)=1, 3, 9$. Then $(b, c)=1$ gives, say, $c=-1$, $a=b^2$, $2b^3+7=\pm 9$, and so $b=-2$, $a=4$. Then $\pm 9Y=a^2+28bc$, and $Y=8$, $n=7$, $X=22$. If $(b, c)=3$ or 9, then $a\equiv 0 \pmod 3$ since the last term in (18) is an integer. Hence putting $a=3A$, $b=3B$, $c=3C$,

$$AC+B^2=0,\ 2AB+7C^2=\pm 1.$$

From the last equation $(B, C)=1$, and from the first $C\mid B^2$. Hence $C=\pm 1$, $A=\mp B^2$, and $\pm 2B^3+7=\pm 1$, and no solution arises.

Take next $r=1$; then multiplying (19) by $1/3\left(-1-\sqrt[3]{28}+\sqrt[3]{98}\right)$, we find

$$\pm 27Y=-a^2-28bc-14(2ac+2b^2)+14(2ab+7c^2), \tag{20}$$

$$\mp 27=-2ab-7c^2-a^2-28bc+7(2ac+2b^2), \tag{21}$$

$$0=-2ac-2b^2-2(2ab+7c^2)+a^2+28bc. \tag{22}$$

Equation (22) shows that a is even, and equation (21) that c is odd. Then (20) becomes $Y\equiv 2 \pmod 4$ and so $Y=2$ is the only possibility. This, however, is not a solution.

This completes the proof.

I remark that on writing $4y^3-7=x^2$ as $Y^3-14=2X^2$ where $Y=2y$, we could have used the cubic field $R\left(\sqrt[3]{14}\right)$. The class number is 3, and the fundamental unit is $\varepsilon=1+2\sqrt[3]{14}-\sqrt[3]{196}$. Also $2=\left[2, \sqrt[3]{14}\right]^3=P^3$, say. Then we have the ideal equation

$$\left[Y-\sqrt[3]{14}\right]=PT_1^2,$$

where T_1 is a non-principal ideal. Since $PT_1=T$ or $P^2T_1=T$, where T is a principal ideal, we have

$$2\left(Y-\sqrt[3]{14}\right)=\pm\varepsilon^r\left(a+b\sqrt[3]{14}+c\sqrt[3]{14^2}\right)^2,\ (r=0,1).$$

If $r=0$, we have

$$\pm 2\left(Y-\sqrt[3]{14}\right)=a^2+28bc+\sqrt[3]{14}\,(2ab+14c^2)+\sqrt[3]{196}\,(b^2+2ac). \tag{23}$$

Hence $ab+7c^2=\pm 1$, $b^2+2ac=0$. Since $(b, c)=1$, $c=\pm 1$, $a=\dfrac{b^2}{2}$, and no solution results.

If $r=1$, on multiplying the right-hand side of (23) by ε, we have

$$\pm 2Y=a^2+28bc+28(b^2+2ac)-14(2ab+14c^2),$$
$$\mp 2=2ab+14c^2+2(a^2+28bc)-14(b^2+2ac),$$
$$0=b^2+2ac+2(2ab+14c^2)-a^2-28bc.$$

The first equation shows that $a = 2A$ is even, the third that $b = 2B$ is even, and the second that $c = C$ is odd. Hence

$$\pm \tfrac{1}{2} Y = A^2 + 14BC + 28B^2 + 28AC - 28AB - 49C^2,$$
$$\mp 1 = 4AB + 7C^2 + 4A^2 + 56BC - 28B^2 - 28AC,$$
$$0 = B^2 + AC + 4AB + 7C^2 - A^2 - 14BC.$$

The first equation shows that $A \equiv C \pmod 2$ since $Y \equiv 0 \pmod 4$, and from the second equation C is odd. Then the third shows that B is odd. The first equation then becomes

$$\pm \tfrac{1}{2} Y \equiv 1 + 2 - 1 \pmod 4.$$

Hence the only possibility is $Y = 4$, and then $n = 5$, $x = 5$.

I remark that the same methods would apply to some other equations

$$a^n = b + x^2$$

where a, b are given integers.

University of Colorado, U.S.A. St. Johns College, Cambridge, England.

Tryckt den 29 januari 1962

Uppsala 1962. Almqvist & Wiksells Boktryckeri AB