Some remarks concerning points of finite order on elliptic curves over global fields

Gerhard Frey

Introduction

Using the reduction theory of Néron we give necessary conditions for the existence of points of order q on elliptic curves E rational over global fields. An application is the determination of all elliptic curves $/\mathbf{Q}$ with integer j and torsion points, generalizing Olson [8]. Another application is a theorem about semistable reduction whose consequences generalize a theorem of Olson [9] ($K=\mathbf{Q}$) and give divisibility conditions for the discriminant and the coefficients of E related with the paper of Zimmer [13] as well as "diophantine" equations related with Fermat's equation that are discussed for $K=\mathbf{Q}$ and K a function field.

We are interested in elliptic curves over global fields K (i.e.: K is a finite number field or K is a function field of one variable over a finite field) and especially in the torsion group of $E(K)$, where $E(K)$ is the group of K-rational points of E.

It is well known that $E(K)$ is finitely generated, it is conjectured that if K is a number field then the order of the torsion group of $E(K)$ is bounded by some number depending only on K (cf. Demjanenko [1]). In any case in order to handle with $E(K)$ the first step is to determine the torsion group. In principle this is not so difficult; if one uses the results of Lutz [6] and Zimmer [13], one sees immediately that for every E there exist points of q-power-order only for a finite number of primes q, as the equations for points of order q are known (in principle) one has only to test what orders really occur. But as the computational work grows very rapidly with q it is usefull to look for sharper necessary conditions, and this shall be done in this paper.

The method is to use the classification of reduction types given by Néron [7]. Then the local result is that for nearly all primes $\mathfrak{p}$ (the exception set is in the case of a number field only depending on the ramification of $K/\mathbf{Q}$) E has to have semistable reduction in $\mathfrak{p}$ if $E(K_\mathfrak{p})$ has a point of order q. (Lemma 1 and lemma 2).

In the global situation the reduction theory is used at first to determine all elliptic curves defined of $\mathbf{Q}$ with integer j and torsion points, this generalizes a result of Olson [8] who deals with curves with complex multiplication (Theorem 1). Then we use the global version (Theorem 2) of the local reduction lemmas to prove another result that for $K=\mathbf{Q}$ is found in Olson [9]: For given j there are only finitely many elliptic curves with points of an order greater than 2. If q is great enough and $E(K)$ contains a point of order q then E has to have semistable reduction in all primes of K, and this implies a "diophantine" divisor equation for the discriminant of E together with some divisibility conditions (proposition 1 and corollaries) from which results as contained in Zimmer [13] can be concluded. The results are more manageable if we treat the special case $K=\mathbf{Q}$ (Theorem 3), for instance: If $E(\mathbf{Q})$ contains a point of order q^i ($q\geqq 5$, $q^i\geqq 11$) then E has semistable reduction in all primes, and for all primes p with $v_p(j)<0$ and $p\not\equiv\pm 1 \bmod q^i$ we have:

$p^{q^i}|\Delta$ (Δ the discriminant of E). If $i=2l$ then the equation:

$U^3-V^2=12^3Z^{q^l}$ has an integer relatively prime solution, and if E has a point of order $2q^{2l}$ rational over $\mathbf{Q}$ then the equation: $A_0^2=Z_1^{q^l}+2^6Z_2^{q^l}$ has such a solution (Theorem 4). These equations are related with Fermat's equation; this is not too astonishing in view of the results of Hellegouarche [4] and Demjanenko [1]. [1])

A natural question is the converse problem: If one has a solution of the equations above. Does this imply the existence of an elliptic curve over $\mathbf{Q}$ with a torsion point of order q^l. This question leads to difficult realization problems over $\mathbf{Q}$: If the answer is negative then there exists an extension $K/\mathbf{Q}$ with Galoisgroup $\mathrm{Gl}(2, q)$ unramified over $\mathbf{Q}(\zeta_q)$.

In the last paragraph we assume that K is a function field and give a short discussion of the results one has to expect in this case.

The methods used in this paper are elementary except the reduction theory of Néron and the theory of Tate curves that enable us to avoid nearly all computations occuring in the papers of Olson and Zimmer. So we never use explicitely the addition formulas and the coordinates of the points of order q, we only need the Tate parametrization of these points in the places with bad reduction. The price we must pay for this is a loss of information about the points of order q (cf. Hellegouarche [4]), we only get information about the coefficients and the discriminant of the equation. But in practice this disadvantage is perhaps not so bad: Given an elliptic curve the only accessible things are just the coefficients, and the necessary criterions for the existence of torsion points given in this paper may help to exclude a lot of primes from the concurrence.

---

[1]) Added in proof: Recently B. Mazur proved that there are no torsion points of order greater than 12 rational over $\mathbf{Q}$ and hence the assumptions of Theorem 3 and 4 can never be satisfied.

1. Local theory

Let K be a field complete with respect to a discrete valution v with residue field k, k being perfect, and of characteristic $p \geqq 0$. Let E be an elliptic curve defined over K with absolute invariant j and Hasse-Invariant δ. For simplicity we assume: $p \neq 2, 3$, and then we can find a Weierstraß normal form for E:

$$Y^2 = X^3 - g_2 X - g_3, \quad j = 12^3 \cdot 4 \cdot g_2^3 \Delta^{-1}, \quad \Delta = 4g_2^3 - 27g_3^2,$$

if $j \neq 0, 12^3$: $\delta \equiv -1/2\, g_2 \cdot g_3 \mod K^{*2}$.

Without any loss of generality we may always assume: $v(g_2) \geqq 0$, $v(g_3) \geqq 0$. If L is an overfield of K, then $E(L)$ is the group of L-rational points of E.

Néron [7] proves the existence of a minimal model E^* of E lying in some (possibly) high dimensional projective space and defining a group scheme over the ring of integers of K. We will use the following properties of E^*: Let $E_0^*(L)$ be the kernel of the reduction map mod v, and E^{*0} the group scheme over k corresponding to the special fiber of E^* (the "reduction" of E^*), then we have the exact sequence

$$0 \to E_0^*(K) \to E^*(K) \to E^{*0}(k) \to 0$$

$E_0^*(K)$ has a natural filtration $\ldots E_i^*(K) \supset E_{i+1}^*(K) \supset \ldots$ with $E_i^*(K)/E_{i+1}^*(K) \cong k^+$. If C^0 is the connected component of E^{*0}, then C^0 is isomorphic as algebraic group either to an elliptic curve, or to the multiplicative group G_m (possibly after a quadratic extension of k) or to the additive group G_a. In the first case it follows that E^{*0} is connected, we say: E has good reduction. In the second case: $E^{*0}/C^0 \cong$ $\cong \mathbf{Z}/m$ with $m = -v(j)$, E has reduction of multiplicative type, which is said to be split iff $C^0 \cong G_m$.

In the third case the table in Néron [7] shows that if $v(j) < 0$, then $|E^{*0}(k)/C^0(k)| \leqq 4$, and if $v(j) \geqq 0$ then

$$E^{*0}(k)/C^0(k) \subset \begin{cases} \mathbf{Z}/3 \\ \mathbf{Z}/2 \times \mathbf{Z}/2. \end{cases}$$

We can use j, Δ and δ to characterize the reduction types if char $(k) \neq 2, 3$:

If $v(j) < 0$ then we have reduction of multiplicative type iff $K(\sqrt{\delta})/K$ is unramified. It is split iff $K(\sqrt{\delta}) = K$.

If $v(j) \geqq 0$ then we have good reduction iff $v(\Delta) \equiv 0 \mod 12$. So after a finite totally ramified extension of K of degree dividing 12 we get an elliptic curve with either good reduction or with reduction of multiplicative type.

Definition. E has semistable reduction with respect to v iff E has good reduction or E has reduction of multiplicative type. E has potentially good reduction iff $v(j) \geqq 0$.

If $v(j)<0$ one has a very explicit description of $E(K)$ due to Tate (cf. Roquette [12], Frey [2]): If $K_1 = K(\sqrt{\delta})$ then there is a canonical isomorphism

$$\varphi\colon E(K_1) \xrightarrow{\sim} K_1^*/\langle Q_v\rangle$$

where $Q_v \in K$ and $j = \frac{1}{Q_v} + \sum_{i\geqq 0} a_i Q_v^i$ with $a_i \in \mathbf{Z}$. (So $v(Q_v) = -v(j)$).

If $G(K_1/K) = \langle\sigma\rangle \neq 1$, then

$$(\varphi\circ\sigma)(P) = ((\sigma\circ\varphi)(P))^{-1} \quad \text{for all} \quad P \in E(K_1). \tag{1}$$

We want to use these informations to determine the torsion points $E(K)_t$ of $E(K)$.

Lemma 1. *If $v(j)<0$ and E has not semistable reduction then $|E(K)_t/W| \leqq 4$, where W is the p-primary part of the group of roots of unity in K_1 in the kernel of the norm map from K_1 to K.*

Proof. (1) implies: $E(K) = \{a \in K_1^*/Q_v,\ N_{K_1/K} a \equiv 1 \bmod Q_v\}$, and so:

$$\begin{aligned} E(K)_t &= \{a \in K_1,\ \exists n\colon a^n = Q_v^s,\ N_{K_1/K} a = Q_v^t\}/\langle Q_v\rangle = \\ &= \{\zeta \in K_1,\ N_{K_1/K}\zeta = 1\} \cup \{a \in K_1,\ a^2 = \zeta\cdot Q_v,\ N_{K_1/K} a = Q_v\} \end{aligned}$$

(ζ a root of unity).

So $E(K)_t/\varphi^{-1}\{\zeta \in K_1,\ N_{K_1/K}(\zeta) = 1\} \subset \mathbf{Z}/2$, and so the assertion follows.

Corollary. *If $v(j)<0$, E not semistable and* char $(K) = p > 0$ *or* char $(K) = 0$ *and $v(p) = e$ is not divisible by $\frac{p-1}{2}$*, then $|E(K)_t| \leqq 4$.

Now let us look at an elliptic curve E with potential good reduction. For simplicity assume: $p \neq 2, 3$. Let be $v(\Delta) = l$ with $0 < l < 12$.[1]) After a ramified extension L/K with $[L:K] = n \leqq 6$ we find an elliptic curve E'/L isomorphic to E over L with good reduction: If we give E' again in Weierstraß normal form

$$Y'^2 = X'^3 - g_2' X - g_3'$$

then an isomorphism $\varphi'\colon E \underset{L}{\xrightarrow{\sim}} E'$ is given by

$$(X, Y) \to (t^2 X, t^3 Y)$$

with $v_L(t) = -\frac{n\cdot l}{12}$ (v_L = normed valuation of L).

Now let $P = (x, y)$ be a point of order m of $E(K)$ with $(m, 6) = 1$.

Let E^* be the minimal model of E with respect to v, and P^{*0} the reduction of P mod v.

---

[1]) l may be equal to 2, 3, 4, 6, 8, 9, 10 (Neron [7]).

As the order of P^{*0} is prime to 6, $P^{*0} \in C^0(k)$, and so the order of P^{*0} is a power of p. By Hensel's Lemma the order of P is a power of p, say: p^i.

Now by looking at the proof of Néron [7] for the existence of minimal models (pp. 106—120) one easily verifies that the fact that P^{*0} lies in $C^0(k)$ implies: $v(x) \leqq 0$. Hence: $\varphi(P)=(x', y')$ lies in the kernel of the reduction map with respect to v_L. But this has consequences: Let be char$(K)=0$. Then $p^{i-1}|v(p)=e$, and $p^{i-1}(p-1) \leqq v_L(p)=n \cdot e \leqq 6e$. (See Lutz [6] or Serre [11], the reason for the inequalities is the fact that the kernel of the reduction of E' is a formal group of height 1 or 2).

Let be char$(K)=p>0$. Let be (X', Y') a generic point of E', $(X'_p, Y'_p)= =p \cdot (X', Y')$, and

$$\frac{X'_p}{Y'_p} = c_p \left(\frac{X'}{Y'}\right)^p + \sum\nolimits_{i=p+1}^{\infty} c_i \left(\frac{X'}{Y'}\right)^i$$

the expansion of X_p/Y_p. The coefficients c_i are integral with respect to v. c_p is called the Hasse-Invariant (not to confuse with δ) of E'. $c_p=0$ iff E is supersingular.

The existence of the point of order p^i in the kernel now implies $p^i(p-1) \leqq \leqq v_L(c_p)$ and $p^i|v_L(c_p)$. (cf. Frey [3].)

So we proved

Lemma 2. *Assume: $p \neq 2, 3$, and E has potential good reduction but not good reduction. Let L be an overfield of K, totally ramified, of degree $n \leqq 6$, such that E is isomorphic to E' over L and E' has good reduction. If* char$(K)=p>0$ *let c_p be the Hasse-Invariant concerning the points of order p of E'. Assume:*

If char$(K)=0$ *then $p^{i-1} \nmid v(p)$ or $(p-1)p^{i-1}>6v(p)$.*

If char$(K)=p$ *then $p^i \nmid v_L(c_p)$ or $(p-1)p^i > v_L(c_p)$.*

Then $|E(K)_t| \subset \mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}/3 \times (\mathbf{Z}/p^{i-1})^2$.

2. Global applications

We now assume that K is a global field, that is: K is a finite extension of $\mathbf{Q}$ or a function field of one variable over a finite field. We give now some applications of the local theory described above.

If v is a valuation of K, let K_v be the completion of K with respect to v.

§ 1. Torsion of elliptic curves over Q with integer j

We look at E: $Y^2=X^3-g_2X-g_3$, $g_2, g_3\in\mathbf{Z}$, and

$$j = 12^3\cdot 4\frac{g_2^3}{\Delta}\in\mathbf{Z}.$$

If q is a prime, and v_q the q-adic valuation, then $v_q(j)\geqq 0$, so E has everywhere potentially good reduction.

We begin with $p=2$. If E has good reduction in $p=2$, it follows from Riemann's hypothesis that the order of the group of torsion points with order prime to 2 is at most 5. If E has bad reduction in $p=2$ it follows that beside of points with an order divisible by 2 there is at most a point of order 3.

Next we look at $p=3$. If E has good reduction in $p=3$ then the order of the group of torsion points with order prime to 3 is at most 7. If E has bad reduction in $p=3$ then there are only points of order $3^n\cdot 2$.

The prime $p=5$ gives in the same manner: The group of torsion points with order prime to 5 has at most 10 elements. If we combine the statements above we have:

The torsion group $E(\mathbf{Q})_t$ of $E(\mathbf{Q})$ is
either equal to $\mathbf{Z}/5$ (0)
or contained in $\mathbf{Z}/6$ (1)
or equal to $\mathbf{Z}/4$ (2)
or equal to $\mathbf{Z}/2\times\mathbf{Z}/2$ (3)

We now want to show that the case (0) does not occur. Assume that $E(\mathbf{Q})_t=\mathbf{Z}/5$. Then it follows from above that E has good reduction in all primes except $p=5$.

We choose g_2 and g_3 such that $|\Delta|$ is minimal in $\mathbf{N}$, so: $\Delta=\pm 2^8 5^n$. $j\in\mathbf{Z}$ implies $5^n|g_2^3$, so: $5^n\|g_3^2$, $n\equiv 0 \bmod 2$. We have: $12^3\cdot g_2^3-3^6\cdot 4^2\cdot g_3^2=\pm 12^3 4^3 5^n$, or:

$$A^3-B^2 = \pm 12^3 4^3 5^n \quad \text{with} \quad A, B\in\mathbf{Z}.$$

If $n\equiv 0 \bmod 6$ it is well known that then $B=0$, $A=\pm 3\cdot 4^2\cdot 5^{n/3}$, and so: $j=12^3$. But if $g_3=0$, E has always the point of order 2 given by $(0, 0)$, and this is a contradiction.

Now let $n\not\equiv 0 \bmod 3$. We look for a solution $B^2=A^3\pm 3\cdot 4^2\cdot 5^n$ with $5|A$, $5^n\|B^2$. But as 12 is no square mod 5 there is no such solution, and we are done.

A short look at the table in Néron [7] shows that the case 2 can only occur if E has everywhere good reduction except at $p=2$. The same arguments as in 2) together with a study of the list of curves having a point of order 2 show: j has to be equal 12^3 or $2^3 3^3 11^3$.

Now we handle with the case 3. Let be given E by:

$$Y^2 = aX(X-1)(X-\mu) \quad \text{with} \quad \mu \in \mathbf{Q}^* \setminus \{1\}, \quad a \in \mathbf{Q}$$

(After a transformation over $\mathbf{Q}$ we always may assume that E has such an equation, if E has 4 points of order 2 over $\mathbf{Q}$.)

This equation implies:

$$j = 4^4 \cdot (1-\mu+\mu^2)^3 \cdot (1-\mu)^{-2} \cdot \mu^{-2}.$$

$j \in \mathbf{Z}$, hence: $2^4 \cdot \mu \in \mathbf{Z}$. With $\varepsilon = 2^4 \cdot \mu$ we have:

$$j = (2^8 - 2^4\varepsilon + \varepsilon^2)^3 \cdot \varepsilon^{-2}(2^4-\varepsilon)^{-2}.$$

As $\varepsilon \cdot (2^4-\varepsilon) | (2^8-2^4\varepsilon+\varepsilon^2)^3$, we have: $\varepsilon \cdot (2^4-\varepsilon) | 2^{8\cdot 3}$, and hence: ε and $(2^4-\varepsilon)$ are powers of 2. So $\varepsilon = -2^4$ or 2^3 and $j = 12^3$.

So we have the result that E fulfils case 3 only if $j=12^3$. On the other hand Olson [8] has the result: If $j=12^3$ then case 2 or case 3 may happen, and if $j = 2^3 \cdot 3^3 \cdot 11^3$, case 2 may happen, with an exact description what points will really occur (depending on the Hasse-Invariant), so we can say that we exactly know the curves E with $|E(\mathbf{Q})| = 4$.

Now let E fulfil the case 1.

Firstly we look for points of order 3.

A slight computation shows that E has a point of order 3 rational over $\mathbf{Q}$ iff E has an equation: $Y^2 = X^3 + A^2X^2 + 2A \cdot CX + C^2$, with $A, C \in \mathbf{Z}$. For $A=0$ we get: $j=0$. From now on we assume: $A \neq 0$.

The substitution $X \to A^{-2}X$, $Y \to A^{-3}Y$ gives the equation:

$$Y^2 = X^3 + X^2 + 2C'X + C'^2$$

with $C' \in \mathbf{Q}$. We get a Weierstraß normal form:

$$Y^2 = X^3 + (2C' - 1/3)X + C'^2 - 2/3C' + 2/27,$$

and so

$$j = 4^4(1-6C')^3(4-27C')^{-1} \cdot C'^{-3}.$$

$v_p(C') > 0$ implies:

$$v_p(j) = 8v_p(2) - 3v_p(C') - v_p(4-27C'),$$

hence: For $p \neq 2$: $v_p(C') \leqq 0$, for $p=2$: $v_2(C') \leqq 1$, so: $2 \cdot C'^{-1} = \mu \in \mathbf{Z}$.

This gives:

$$j = 2^4(\mu-12)^3 \cdot \mu \cdot (2\mu-27)^{-1}.$$

If $\mu - 12 \neq 0$, then: $(2\mu-27, \mu)$ and $((\mu-12), (2\mu-27))$ are powers of 3 and we must have:

$$2\mu - 27 = \pm 3^n,$$

or:

$$\mu = (1/2)(\pm 3^n + 27).$$

Hence:

$$j = 3^{6-n}\cdot(1+3^{n-1})^3\cdot(1+3^{n-3}), \quad \text{or:} \quad j = 3^{6-n}(1-3^{n-1})^3(3^{n-3}-1),$$

for $n=0, \ldots, 6$, $C'=4\cdot(27+3^n)^{-1}$ resp. $C'=4\cdot(27-3^n)^{-1}$, $n\neq 3$.

Next we want to compute all elliptic curves with exactly two points of order 2. The cases $j=0$ and $j=12^3$ are known (cf. Olson [8]), and so we assume from now on that $j\neq 0, 12^3$.

E has exactly two points of order 2 iff E admits an equation:

$$Y^2 = X(X^2-2aX+a^2-b^2d)$$

with $a, b, c, d\in\mathbf{Z}$, d squarefree, $abd\neq 0$.

Then a Weierstraß normal form of E is:

$$Y^2 = X^3-(1/3a^2+b^2d)X-(2/3ab^2d-2/27a^3).$$

Hence:

$$j = 4^3(a^2+3b^2d)^3(b^2d\cdot(a^2-b^2d)^2)^{-1}.$$

Let be $p\neq 2$. If $v_p(a^2)<v_p(b^2d)$, then $v_p(j)<0$, a contradiction. If $p=2$, it follows in the same way:

$$v_2(a^2)+6 \geqq v_2(b^2d),$$

hence:

$$b^2d|2^6a^2.$$

Let be $\mu\in\mathbf{Z}$ so that $\mu\cdot b^2d=2^6a^2$. Then we get:

$$j = (\mu+3\cdot 2^6)^3(\mu-2^6)^{-2}.$$

From this we conclude that μ has to be equal to $2^6\pm 2^n$, and this gives:

$$j = 2^{24-2n}(1\pm 2^{n-8})^3.$$

j is an integer iff $0\leqq n\leqq 12$.

$2^6\pm 2^n$ is no square for $0\leqq n\leqq 12$, except for $n=9$: $2^6+2^9=24^2$ and $n=6$. In all other cases choose $b\in\mathbf{Z}\setminus\{0\}$ and d square free so that $(2^6\pm 2^n)b^2d$ is a square $(=a^2)$.

We see in this way that we find for all admissible j an elliptic curve that has a point of order 2. But for $j\neq 0, 12^3$ all elliptic curves with the same absolute invariant have the same number of points of order 2. So we have exactly determined all elliptic curves with exactly two points of order 2, and taking all considerations together we have proved the following

Theorem 1. *Let E be an elliptic curve defined over $\mathbf{Q}$ with $j\in U$. Then either $E(\mathbf{Q})_t=\{0\}$ or E is one of the curves listed in the following table.*

$E(\mathbf{Q})_t$	j	Equation
$=\mathbf{Z}/2\times\mathbf{Z}/2$	12^3	$Y^2=X^3-g_2X,\ g_2\in\mathbf{Z}^2$
$=\mathbf{Z}/4$	12^3 $2^3 3^3 11^3$	$Y^2=X^3+4X$ $Y^2=X^3-11D^2X+14D^3$, $D=1,2$
$\mathbf{Z}/2\subset E(\mathbf{Q})_t\subset\mathbf{Z}/6$	0 12^3 $2^{24-2n}(1\pm 2^{n-8})^3$ $(0\leqq n\leqq 12)$	$Y^2=X^3+k,\ k\in\mathbf{Z}^3$ any equation with admissible j not appearing in line 1 or 2
$\mathbf{Z}/3\subset E(\mathbf{Q})_t\subset\mathbf{Z}/6$	0 $3^{6-n}(1+3^{n-1})^3(1+3^{n-3})$ $0\leqq n\leqq 6$ $3^{6-n}(1-3^{n-1})^3(3^{n-3}-1)$ $(0\leqq n\leqq 6, n\neq 3)$	$Y^2=X^3+k,\ k\in\mathbf{Z}^2$ $Y^2=X^3+X^2+$ $+\frac{8}{27+3^n}X+\frac{4^2}{(27+3^n)^2}$ $Y^2=X^3+X^2+$ $+\frac{8}{27-3^n}X+\frac{4^2}{(27-3^n)^2}$
$=\mathbf{Z}/6$	0 $2^4 3^3 5^3$	$Y^2=X^3+1$ $Y^2=X^3+X^2+\frac{-4}{27}X+\left(\frac{2}{27}\right)^2$

§ 2. Necessary conditions for the existence of torsion points

Let K be a global field. If $\operatorname{char}(K)=p>0$ then assume that $p\neq 2,3$. If $\operatorname{char}(K)=0$ and q a prime we define:

$e_q=\{\min_{\mathfrak{Q}|q}\{e_{\mathfrak{Q}}\}\}$, where $\mathfrak{Q}$ is a place of K and $e_{\mathfrak{Q}}$ the ramification of $\mathfrak{Q}$ over $\mathbf{Q}$.

If $\operatorname{char}(K)=p>0$ and E/K is an elliptic curve with discriminant Δ, then we define: $L:=K(\Delta^{1/12})$, let E'/L be an elliptic curve isomorphic to E over L with good reduction in all places q with $v_q(j)>0$ with Hasse-Invariant $c_p\in L$. Let $\mathfrak{C}$ be the divisor of c_p.

Theorem 2. *If $E(K)$ contains a point of order q^i (q a prime $\geqq 5$) then E has semistable reduction in all places $\mathfrak{P}$ of K whose residue field has a characteristic different from q. Let $\mathfrak{Q}$ be a place of K with residue field $k_{\mathfrak{Q}}$ and* $\operatorname{char}(k_{\mathfrak{Q}})=q$. *Then E has semistable reduction in $\mathfrak{Q}$ if*

i) $\mathfrak{Q}^{q^i(q-1)}\nmid\mathfrak{C}$ *(regarded as divisors of L) if* $\operatorname{char}(K)=q>0$.

ii) $q^{i-1}\nmid e_q$ *or* $q^{i-1}(q-1)>6e_q$ *if* $\operatorname{char}(K)=0$.

Proof. Just apply Lemma 1 and Lemma 2.

Corollary 1. *For given $j \neq 0$, 12^3 there are only finitely many elliptic curves with points of an order greater than* 2.

Proof. Let E_1, E_2 be elliptic curves with absolute invariant j and Hasse-Invariant δ_1 resp. δ_2.

Firstly assume: char $(K)=0$.

If E_1 and E_2 have both points of prime order greater than 3 then E_1 and E_2 have semistable reduction outside the finite set of places $\mathfrak{Q}$ with $e_q > 1$, or $\mathfrak{Q} | 2 \cdot 3 \cdot 5 \cdot 7$. We claim: $K_{12} = K\left(\sqrt{\frac{\delta_1}{\delta_2}}\right)$ is unramified in all such places. To see this let be $\mathfrak{Q}$ so that $v_{\mathfrak{Q}}(j) < 0$. Then $K(\sqrt{\delta_i})$ is unramified in $\mathfrak{Q}$, and so K_{12} is unramified in $\mathfrak{Q}$.

If $v_{\mathfrak{Q}}(j) \geqq 0$ then E_1 and E_2 have good reduction in $\mathfrak{Q}$, and we can choose equations for E_1 and for E_2 with discriminants Δ_1 and Δ_2 such that $v_{\mathfrak{Q}}(\Delta_1) = v_{\mathfrak{Q}}(\Delta_2) = v_{\mathfrak{Q}}\left(\left(\frac{\delta_2}{\delta_1}\right)^6 \cdot \Delta_1\right) = 0$, so as $\mathfrak{Q} \nmid 2$ K_{12} is unramified in $\mathfrak{Q}$.

If E_1 has a point of order 4 then $v_{\mathfrak{Q}}(j) \geqq 0$ and $\mathfrak{Q} \nmid 2$ implies: E_1 has good reduction in $\mathfrak{Q}$, and we can argue as above for $\mathfrak{Q} \nmid 2$.

If E_1 has a point of order 3 and if E_1 has potentially good reduction in $\mathfrak{Q}$ $(\mathfrak{Q} \nmid 2, 3)$ then we have

$$v_{\mathfrak{Q}}(\Delta(E_1)) \equiv \begin{cases} 0 \\ 4 \bmod 12. \quad \text{(c.f. [7], p. 124)} \\ 8 \end{cases}$$

But since $v_{\mathfrak{Q}}(\Delta(E_2)) \equiv v_{\mathfrak{Q}}(\Delta(E_1)) \bmod 6$, E_2 has a point of order 3 only if $v_{\mathfrak{Q}}(\delta_1) \equiv v_{\mathfrak{Q}}(\delta_2) \bmod 2$ in all $\mathfrak{Q}$ with $v_{\mathfrak{Q}}(j) \geqq 0$. Hence there are only finitely many curves $E_1, \ldots, E_s$ with invariant j having a point of order 3. So choose $\mathfrak{Q}$ such that

i) $\mathfrak{Q} \nmid 2 \cdot 3 \cdot 5 \cdot 7$,

ii) $E_1, \ldots, E_s$ have good reduction in $\mathfrak{Q}$ and

ii) $e_q = 1$.

Then if E, E' are elliptic curves with invariant j, Hasse-Invariants δ_1 and δ_2 and points of order greater than 2, then $K(\sqrt{\delta_1/\delta_2})/K$ is unramified in $\mathfrak{Q}$. As there are only finitely many extensions of degree 2 over K with this property we are done.

Now assume: char $(K) = p > 3$. Let E_1, E_2 be as above. Again we claim: $K\left(\sqrt{\frac{\delta_1}{\delta_2}}\right)$ is unramified outside a finite set depending only on E_1:

Let $\mathfrak{Q}$ be a place of K with $v_{\mathfrak{Q}}(j) \geqq 0$ and $\mathfrak{Q} \nmid \mathfrak{C}_1$.

If $v_{\mathfrak{Q}}(\mathfrak{C}_2) > 0$ then the reduction of E_2' (defined as in the theorem) is supersingular. But then the reduction of E_1 is supersingular too, and this gives a contradiction. Hence $v_{\mathfrak{Q}}(\mathfrak{C}_2)=0$, and so E_2 has to have good reduction in $\mathfrak{Q}$, especially: $K\left(\sqrt{\frac{\delta_1}{\delta_2}}\right)\Big/K$ is unramified in $\mathfrak{Q}$.

Corollary 2. *Let E have a point of order q^i with $q\geqq 5$, $q\neq \operatorname{char}(K)$, $q^i\geqq 11$ and $q^{i-1}\nmid e_q$ or $e_q<q^{i-1}\dfrac{q-1}{6}$. Let $Y^2=X^3-g_2X-g_3$ be a Weierstraß equation for E. Then if $\mathfrak{P}$ divides both (g_2) and (g_3) and $\mathfrak{P}\nmid 6$ we have $w_{\mathfrak{P}}(g_2)\equiv 0 \bmod 4$ or $w_{\mathfrak{P}}(g_3)\equiv 0 \bmod 6$. Moreover we can choose g_2 and g_3 such that for all $\mathfrak{P}\nmid 6$ with $v_{\mathfrak{P}}(j)<0$ we have $v_{\mathfrak{P}}(g_2)=v_{\mathfrak{P}}(g_3)=0$.*

Proof. E has semistable reduction in all places of K. Let be $v_{\mathfrak{P}}(j)\geqq 0$. In the completion $K_{\mathfrak{P}}$ we find g_2', g_3' defining an elliptic curve isomorphic to E over $K_{\mathfrak{P}}$ with $v_{\mathfrak{P}}(\Delta)=0$. So $v_{\mathfrak{P}}(g_2')=0$ or $v_{\mathfrak{P}}(g_3')=0$. But as $g_2'=\alpha^4g_2$ and $g_3'=\alpha^6g_3$ for some $\alpha\in K_{\mathfrak{P}}$ the corollary follows.

Let be $v_{\mathfrak{P}}(j)<0$. As $v_{\mathfrak{P}}(j)=3v_{\mathfrak{P}}(g_2)-v_{\mathfrak{P}}(\Delta)$ and $v_{\mathfrak{P}}(\Delta)\geqq \min\{3v_{\mathfrak{P}}(g_2), 2v_{\mathfrak{P}}(g_3)\}$, we have:

$3v_{\mathfrak{P}}(g_2)=2v_{\mathfrak{P}}(g_3)$. As $\delta=-1/2g_2\cdot g_3$, and as $K(\sqrt{\delta})/K$ is unramified it follows that $v_{\mathfrak{P}}(g_2)\equiv v_{\mathfrak{P}}(g_3) \bmod 2$.

Hence $v_{\mathfrak{P}}(g_2)\equiv 0 \bmod 4$ and $v_{\mathfrak{P}}(g_3)\equiv 0 \bmod 6$. The approximation theorem in K gives the corollary.

What happens if $\mathfrak{P}|6$. (Automatically K is a number field then.) We are interested in the case that $v_{\mathfrak{P}}(j)<0$ if $\mathfrak{P}|6$. At first assume: $\mathfrak{P}|2$. Then we have: $3v_{\mathfrak{P}}(g_2)+2v_{\mathfrak{P}}(2)=2v_{\mathfrak{P}}(g_3)$ and $v_{\mathfrak{P}}(g_2)+v_{\mathfrak{P}}(2)\equiv v_{\mathfrak{P}}(g_3) \bmod 2$. This implies:

We can choose g_2 and g_3 such that $v_{\mathfrak{P}}(g_2)=0$, $v_{\mathfrak{P}}(g_3)=v_{\mathfrak{P}}(2)$. Now assume: $\mathfrak{P}|3$. We have: $3v_{\mathfrak{P}}(g_2)=3v_{\mathfrak{P}}(3)+2v_{\mathfrak{P}}(g_3)$ and $v_{\mathfrak{P}}(g_2)\equiv v_{\mathfrak{P}}(g_3) \bmod 2$. Hence: We can choose g_2 and g_3 such that $v_{\mathfrak{P}}(g_2)=v_{\mathfrak{P}}(3)+2$, $v_{\mathfrak{P}}(g_3)=3$, if $v_{\mathfrak{P}}(3)\equiv 1 \bmod 2$, or $v_{\mathfrak{P}}(g_2)=v_{\mathfrak{P}}(3)$, $v_{\mathfrak{P}}(g_3)=0$, if $v_{\mathfrak{P}}(3)\equiv 0 \bmod 2$.

With $U=3^{-1}\cdot g_2$, $V=2^{-1}\cdot g_3$ we get

$$j = 12^3\cdot 4\,\frac{3^3U^3}{3^3\cdot 4U^3-27\cdot 4V^2} = 12^3\cdot U^3(U^3-V^2)^{-1}$$

or

$$(j) = (12^3\cdot U^3)\mathfrak{D}_0^{-1}\cdot\mathfrak{D}_1^{-12}$$

with $\mathfrak{D}_0, \mathfrak{D}_1$ divisors in K with $\mathfrak{D}_0\cdot\mathfrak{D}_1^{12}=(U^3-V^2)$, $\mathfrak{D}_0\geqq 1$ and $v_{\mathfrak{P}}(j)<0$ iff $v_{\mathfrak{P}}(\mathfrak{D}_0)>0$, $(\mathfrak{D}_0, \mathfrak{D}_1)=1$ and the common divisors of V, $\mathfrak{D}_0$ resp. U, $\mathfrak{D}_0$ divide 3, and if $v_{\mathfrak{P}}(U)\neq 0$, $v_{\mathfrak{P}}(V)\neq 0$ then $v_{\mathfrak{P}}\big((3)\mathfrak{D}_1\big)\neq 0$. [1])

[1]) If one would push the discussion a little bit further at this point one would get results similar to the results in Zimmer [13].

We know even a little more about $\mathfrak{P}|\mathfrak{D}_0$: If there are no roots of unity of order q^i in $K_{\mathfrak{P}}(\sqrt{\delta})$, for example if $|k_{\mathfrak{P}}| \not\equiv \pm 1 \mod q^i$ then the point of order q^i corresponds to an element $a \in K_{\mathfrak{P}}(\sqrt{\delta})^*$ with $a^{q^i} \equiv Q_{\mathfrak{P}}^s$, where $(s, q)=1$ and $Q_{\mathfrak{P}}$ is the period of E at $\mathfrak{P}$. Hence:

$K_{\mathfrak{P}}(\sqrt{\delta})=K_{\mathfrak{P}}$ and $q^i|v_{\mathfrak{P}}(j)$, and so $q^i|v_{\mathfrak{P}}(\mathfrak{D}_0)-3v_{\mathfrak{P}}(12U)$. The Riemann hypotheses implies that $\mathfrak{P}|\mathfrak{D}_0$ if $2\sqrt{|k_{\mathfrak{P}}|}+|k_{\mathfrak{P}}|<q^i-1$. From above we conclude: If $2\sqrt{|k_{\mathfrak{P}}|}+1+|k_{\mathfrak{P}}|<q^i$ then q^i divides $v_{\mathfrak{P}}(\mathfrak{D}_0)-3v_{\mathfrak{P}}(12\cdot U)$.

We summarize these facts in

Proposition 1. *Assume E fulfils the conditions of Corollary 2 of Theorem 2 and has bad reduction in all primes $\mathfrak{P}$ that divide 6.*

Then $(j)=(12U)^3\mathfrak{D}_0^{-1}\mathfrak{D}_1^{-12}$ with $\mathfrak{D}_0\mathfrak{D}_1^{12}=(U^3-V^2)$, $(\mathfrak{D}_0, \mathfrak{D}_1)=1$, $\mathfrak{D}_0 \geqq 1$ $((U), \mathfrak{D}_0)|(3)$, $v_{\mathfrak{P}}(j)<0$ iff $v_{\mathfrak{P}}(\mathfrak{D}_0)>0$, and $q^i|v_{\mathfrak{P}}(\mathfrak{D}_0)-3v_{\mathfrak{P}}(12U)$ if $|k_{\mathfrak{P}}| \not\equiv \pm 1 \mod q^i$.

Corollary 1. *If K is a number field and U, V are choosen to be integers in K (this can always be done) then $N_{K/\mathbf{Q}}(\Delta)=d_0\cdot d_1^{12}$, and if $\mathfrak{P}|p$ and $2\sqrt{|k_{\mathfrak{P}}|}+|k_{\mathfrak{P}}|+1<q^i$ then $p^{q^i}|d_0$.*

To sharpen the situation assume: $i=2l$. Let P_i be a point of order q^i in $E(K)$, and $P_l=q^l\cdot P_i$, this is a point of order q^l.

If $\mathfrak{P}$ is a place of K with $v_{\mathfrak{P}}(j)<0$ then

$$E(K_{\mathfrak{P}}(\sqrt{\delta})) \overset{\varphi}{\simeq} K_{\mathfrak{P}}^*(\sqrt{\delta})/\langle Q_{\mathfrak{P}}\rangle.$$

If $\varphi(P_l)=a_l\cdot Q_{\mathfrak{P}}^s$ with $0\leqq v_{\mathfrak{P}}(a_l)<v_{\mathfrak{P}}(Q_{\mathfrak{P}})$ then $\varphi(P_i)=a_i\cdot Q_{\mathfrak{P}}^t$ with $0\leqq v_{\mathfrak{P}}(a_i)< <v_{\mathfrak{P}}(Q_{\mathfrak{P}})$, and $q^l v_{\mathfrak{P}}(a_i)\equiv v_{\mathfrak{P}}(a_l) \mod v_{\mathfrak{P}}(Q_{\mathfrak{P}})$.

Let be $q^{r_{\mathfrak{P}}}$ minimal such that $q^{r_{\mathfrak{P}}}v_{\mathfrak{P}}(a_l)\equiv 0 \mod v_{\mathfrak{P}}(Q_{\mathfrak{P}})$. Then if $r_{\mathfrak{P}}>0$ then $q^{r_{\mathfrak{P}}+l}$ is minimal with $q^{r_{\mathfrak{P}}+l}v_{\mathfrak{P}}(a_i)\equiv 0 \mod v_{\mathfrak{P}}(Q_{\mathfrak{P}})$.

Hence $q^{r_{\mathfrak{P}}+l}|v_{\mathfrak{P}}(j)$.

Now let E' be the curve isogeneous to E and defined by the isogeny kernel $\langle P_l\rangle$. Then again E' is semistable and $v_{\mathfrak{P}}(j')<0$ iff $v_{\mathfrak{P}}(j)<0$. But by the local theory (Roquette [12]) one knows:

$$v_{\mathfrak{P}}(j') = q^{l-2r_{\mathfrak{P}}}\cdot v_{\mathfrak{P}}(j).$$

Hence $q^{2l-r_{\mathfrak{P}}}|v_{\mathfrak{P}}(j')$, and as $l\geqq r_{\mathfrak{P}}$:

$$q^l|v_{\mathfrak{P}}(j').$$

So we have

Corollary 2. *Under the assumptions of Corollary 1 and with $i=2l$ there exists an elliptic curve E' isogeneous to E over K, such that $\mathfrak{D}_0'=(\Pi\mathfrak{P}^6)(12^3)\cdot\mathfrak{D}_2^{q^l}$ where $\mathfrak{D}_0'$ is defined with respect to E' in the same way as $\mathfrak{D}_0$ with respect to E.*

In a special case we get a simpler result:

Corollary 3. *The same assumptions and definitions as in Corollary 2 and moreover we assume that* $\mathfrak{D}_1'$ *is a principal ideal, the class number of* K *is prime to* q, *and* $v_{\mathfrak{P}}(3) \equiv 0 \mod 2$ *for all* $\mathfrak{P}$.

Then we find U', V', *defined with respect to* E', *such that* $U'^3 - V'^2 = \varepsilon \cdot 12^3 \cdot Z^{q^l}$, *where* ε *is a unit of* K, *with* U', V', Z *relatively prime integers in* K.

§ 3. $\mathbf{K} = \mathbf{Q}$

It is now easy to get the following results: Let be E an elliptic curve defined over $\mathbf{Q}$ by the Weierstraß equation

$$Y^2 = X^3 - g_2 X - g_3$$

with $g_2, g_3 \in \mathbf{Z}$ such that $|\Delta|$ is minimal

Theorem 3. *Assume:* E *has a torsion point of order* q^i *with* $q^i > 7$.

Then:

i) E *has semistable reduction in all primes.*
ii) E *is uniquely determined by* j.
iii) $3^3 \| g_2$, $3^3 \| g_3$, $2 \| g_3$ *and* $2 \nmid g_2$. *If we define:* $U = 3^{-3} g_2$, $V = 2^{-1} \cdot 3^{-3} g_3$, *then* $(U, V) = 1$.
iv) $j = 12^3 \cdot U^3 (U^3 - V^2)^{-1}$, *and* $v_p(j) < 0$ *iff* $v_p(U^3 - V^2) > 0$.
v) *If* $v_p(j) < 0$ *and* $p \not\equiv \pm 1 \mod q^i$ *then* $q^i | v_p(j)$ *and* $p^{q^i} \left| \dfrac{(U^3 - V^2)}{12^3} \right.$. *Especially if* $p + 2\sqrt{p} + 1 < q^i$ *then* $p^{q^i} \left| \dfrac{(U^3 - V^2)}{12^3} \right.$.
vi) *If* $i = 2l$ *then there is an elliptic curve* E' *isogeneous to* E *over* $\mathbf{Q}$ *such that*

$$U'^3 - V'^2 = 12^3 \cdot Z^{q^l}$$

with U', V' *defined in the same way as* U, V; U', V', $Z \in \mathbf{Z}$, *relatively prime, and* $p | Z$.

The case that $E(\mathbf{Q})$ contains a point of order $2q^i$ $(i \geqq 2)$ has been studied by Hellegouarche [4] and Demjanenko [1], their result is that the Fermat equation

$$Z_1^q + Z_2^q = Z_3^q$$

has a solution with $q | Z_1 \cdot Z_2 \cdot Z_3$. (c.f. footnote on p. 2)

We want to look for conditions for the discriminant in this case. For this purpose we choose an equation

$$Y^2 = X^3+AX^2+BX, \quad A, B\in \mathbf{Z}$$

for E'. Then:

$$\Delta = 2^8\cdot 3^{12}\cdot Z^{q^l} = B^2(A^2-4B).$$

Using Theorem 3 we get:

$$A = 2\cdot 3^2\cdot A_0, \quad B = 3^4\cdot B_0 \quad \text{and} \quad (A_0, B_0) = 1, \quad 2\nmid A_0, \quad 2\nmid B_0 \tag{1}$$

or

$$A = 3^2\cdot A_0, \quad B = 2^4\cdot 3^4\cdot B_0, \quad (A_0, B_0) = 1, \quad 2\nmid A_0. \tag{2}$$

If A, B fulfil (1) then the elliptic curve E'' derived from E' by an isogeny of degree 2 fulfils (2) and conversely.

So we assume without any loss of generality:

A, B fulfil (1). This implies:

$$2^6\cdot Z^{q^l} = B_0^2(A_0^2-B_0)$$

and since $(B_0, A_0^2-B_0)=1$ and $(B_0, 2)=1$: $B_0=Z_1^{q^l}$ $(Z_1\in\mathbf{Z})$, and

$$A_0^2 = Z_1^{q^l}+2^6 Z_2^{q^l},$$

with $Z_i\in\mathbf{Z}$, and $Z_1^{2q^l}Z_2^{q^l}=Z^{q^l}$.

As the period of E' has to be a q^l-th power in $\mathbf{Q}_p^*$ for all p with $v_p(j)<0$ and no q^l-th root of unity in $\mathbf{Q}_p$, j has to be a q^l-th power in $\mathbf{Q}_p$ for the same primes, and this implies as one verifies easily the same conditions for A_0.

Look especially at $\mathbf{Q}_q$. If $q\nmid Z_2$ then $q|Z_1$, and so 2 has to be a q^l-th power in $\mathbf{Q}_p$, hence

$$2^{q-1}-1 \equiv 0 \bmod q^{1+l}$$

(Wieferich's condition for the solvability of the Fermat equation with a *first* type solution).

Necessarily $p\nmid Z_2$ if $v_2(Z)\not\equiv 0 \bmod 2$ and $v_q(Z)\not\equiv 0 \bmod 2$. If E' has a point of order 4 and $q\equiv 3 \bmod 4$ we find E'' isogeneous to E' such that for E'' the above conditions are fulfilled.

If Z_1 or Z_2 is a square, (say: Z_1 is a square) then to solve equation

$$A_0^2 = Z_1^{2q^l}+2^6 Z_2^{q^l}$$

is equivalent to solve

$$Z_3^{q^l} = 2^4 Z_4^{q^l}+Z_5^{q^l},$$

$Z_i\in\mathbf{Z}$, relatively prime, and

$$q|Z_3\cdot Z_4\cdot Z_5.$$

If $E(\mathbf{Q})$ contains 4 points with 2-power order then we find an elliptic curve E'' isogeneous to E' such that

$$U''^3-V''^2 = 12^3\cdot Z^{2q^l}.$$

(If all points of order 2 are in $E(\mathbf{Q})$ take $E''=E'$, if P is a point of order 4 in $E'(\mathbf{Q})$, then $E''=E'/\langle 2P\rangle$.)

An easy computation shows that to solve this equation is equivalent to solve

$$Z_3^{q^l} = 2^4\cdot Z_4^{q^l}+Z_5^{q^l}.$$

So we have

Theorem 4. *If $E(\mathbf{Q})$ contains a point of order $2q^{2l}$ then the equation: $A_0^2=$ $=Z_1^{q^l}+2^6Z_2^{q^l}$ has an integer relatively prime solution. If $q\nmid Z_2$ or if $E(\mathbf{Q})$ contains a point of order 4 then $2^{q-1}\equiv 1 \bmod q^{1+l}$. If E contains 4 points with 2-power order then the equation: $Z_3^{q^l}+Z_4^{q^l}=2^4Z_5^{q^l}$ has a relatively prime integer solution. For all primes p with $v_p(j)<0$ (especially $p+2\sqrt{p}+1<q^l$) and $p\not\equiv\pm 1 \bmod q^l$ or $p=q$ $p|Z_1\cdot Z_2$ resp. $p|Z_3\cdot Z_4\cdot Z_5$.*

Now assume conversely that (A_0, Z_1, Z_2) is an integer relatively prime solution of

$$A_0^2 = Z_1^q+2^6Z_2^q,\quad q|Z_1\cdot Z_2,\quad A_0\in\mathbf{Q}_q^{*q},$$

with $A=2\cdot 3^2\cdot A_0$, $B=3^4\cdot Z_1^q$. We get the elliptic curve E:

$$Y^2 = X^3+AX^2+BX$$

E is semistable in all primes and has a point of order 2.

If (U, V, Z) is an integer relatively prime solution of

$$U^3-V^2 = 12^3Z^q \quad (q|Z \text{ and } U\in\mathbf{Q}_q^{*q})$$

then again the elliptic curve E:

$$Y^2 = X^3-3^3UX-2\cdot 3^3V$$

is semistable in all primes. (If necessary replace V by $-V$.) Let E_q be the group of points of order q, and let be $K_q:=\mathbf{Q}(E_q)$, $G_q:=G(K_q/\mathbf{Q})$.

G_q is a subgroup of $Gl(2, q)$. (cf. Serre [11]), and $K_q\supset\mathbf{Q}(\zeta)$, with ζ_q a primitive q-th root of unity. If $p\neq q$ is a prime then $K_q/\mathbf{Q}$ is unramified in p, for if $v_p(j)\geqq 0$ then E has good reduction in p, and if $v_p(j)<0$ then $\mathbf{Q}_p(E_q)=\mathbf{Q}_p(\zeta_q, \sqrt[q]{j})$. But as $v_p(j)\equiv 0 \bmod q$ the assertion follows.

For $p=q$ we have $v_q(j)<0$, and $\mathbf{Q}_q(\zeta_q, \sqrt[q]{j})$ is ramified of order $q-1$.

So $K_q|\mathbf{Q}(\zeta_q)$ is unramified, and the place $\mathfrak{Q}$ of $\mathbf{Q}(\zeta_q)$ with $\mathfrak{Q}|q$ splits completely in $K_q/\mathbf{Q}(\zeta_q)$.

Assume: G_q is contained in a Borel group, let $\langle P\rangle\subset E_q$ be a G_q-invariant subspace. Then: $\mathbf{Q}(P)$ is either equal to $\mathbf{Q}(\zeta_q)$ or $\mathbf{Q}(P)/\mathbf{Q}$ is unramified, hence $\mathbf{Q}(P)=\mathbf{Q}$.

In both cases $K_q/\mathbf{Q}(\zeta)$ is an unramified extension of degree $\leqq q$, normal over $\mathbf{Q}$. An easy calculation shows that then $K_q=\mathbf{Q}(\zeta_q)$. See footnote on p. 2.

But since $\mathbf{Q}_q$ contains a point of order q it follows now that $\mathbf{Q}$ contains a point of order q.[1])

If G_q is not contained in any Borel subgroup of $Gl(2, q)$ then it is an easy consequence of the situation that $G_q = Gl(2, q)$. So we have realized $Gl(2, q)$ over $\mathbf{Q}$ by K_q such that $K_q/\mathbf{Q}(\zeta_q)$ is unramified. I ignore if this is possible.

Let be $\langle P_1 \rangle, \dots, \langle P_{q+1} \rangle$ the different cyclic subgroups of E_q; $Z_1, \dots, Z_{p+1}$ the fixed fields of the corresponding Borel subgroups of G_q.

If j_i is the absolute invariant of $E/\langle P_i \rangle$, then $Z_i = \mathbf{Q}(j_i)$ $(i=1, \dots, q+1)$. It is easy to describe the discriminant of $Z_i/\mathbf{Q}$: If $p \neq q$ then p is unramified. If $p=q$ then q has three extension to Z_i, two of them are unramified, and the third has ramification order $q-1$. (The degree of $Z_i/\mathbf{Q}$ is $q+1$.) Hence $D(Z_i/\mathbf{Q}) = \pm q^{q-2}$.

So there are only finitely many possibilities for the fields Z_i.

Let $\Phi_q(T, J)$ be the invariant polynomial of degree q. This is a polynomial defined over $\mathbf{Z}$ of degree $q+1$ in T and J. The pair (j_i, j) is a Z_i-rational place the curve defined by Φ_q. For $q \geqq 23$ the genus of this curve is greater than 1.

Proposition 2. *Let be* (A_0, Z_1, Z_2) *resp.* (U, V, Z) *as described above. Then* $E(\mathbf{Q})$ *contains a point of order* $2q$ *resp.* q *iff* $\Phi_q(T, J)$ *is reducibel over* $\mathbf{Q}$. *If there is a prime* p *with* $1+p+1/2\sqrt{p}<q$, *and* $q \nmid Z_1 \cdot Z_2$ *(resp.* Z*) then* $\Phi_q(T, j)$ *is irreducible over* $\mathbf{Q}$, *and* $G_q = Gl(2, q)$.

If the Mordell conjecture is true for Φ_q $(q \geqq 23)$ *then there are only finitely many admissible solutions* (A_0, Z_1, Z_2) *resp.* (U, V, Z).

Remark. The last part of proposition 2 is true without the condition $q|Z$ (resp. $q|Z_1 \cdot Z_2$) and $U \in \mathbf{Q}_q^{*q}$ resp. $A_0 \in \mathbf{Q}_q^{*q}$, because of the fact that in any case $Z_i/\mathbf{Q}$ is only ramified in the places dividing q, and so $D(Z_i/\mathbf{Q})$ is bounded.

§ 4. char $(K)=p$

In the following let K be a function field of one variable of the finite field k of characteristic $p \neq 2, 3$. We begin the discussion with the simplest case: $K=k(t)$, where t is transcendental over k.

Assume that E is defined over K and has semistable reduction in all places $\mathfrak{P}$ of K. Without any loss of generality we may assume: If $\mathfrak{P}_\infty$ is the unique place with $v_{\mathfrak{P}_\infty}(t)<0$ then E has good reduction in $\mathfrak{P}_\infty$. By the results of §2 we conclude: There are polynomials $U, V \in k[t]$, such that E has a Weierstraß equation

$$Y^2 = X^3 - 3^3UX - 2 \cdot 3^3V$$

with

$$(j) = (12^3U^3)\mathfrak{D}_0^{-1} \cdot \mathfrak{D}_1^{-12}.$$

[1]) Added in proof: The results of Mazur imply that always $G_q = Gl(2, q)$.

Let be $d_1 \in k[t]$ such that $(d_1) = \mathfrak{D}_1 \cdot \mathfrak{P}_\infty^s$ $(s \in \mathbf{Z})$. By the transformation $X \to d_1^{-2} X$, $Y \to d_1^{-3} Y$ we can assume:

$$(j) = (12^3 U^3) \mathfrak{D}_0^{-1} \cdot \mathfrak{P}_\infty^s$$

hence

$$j = \frac{12^3 U^3}{U^3 - V^2}$$

with $U, V \in k[t]$, relatively prime, such that $v_\mathfrak{P}(j) < 0$ iff $v_\mathfrak{P}(U^3 - V^2) > 0$. Furthermore: $3 \deg (U) \leqq (\deg (U^3 - V^2))$, and $\deg (U^3 - V^2) \equiv 0 \mod 12$. (For example: $3 \deg U < 2 \deg V$, and $\deg V \equiv 0 \mod 6$.)

If $E(K)$ contains a point of order q^{2l}, then as before we find an elliptic curve E' isogeneous to E with:

$$U'^3 - V'^3 = c Z^{q^l}, \quad c \in k^*.$$

But as K admits no unramified extension (in the sense that for all places $\mathfrak{P}$ the value group of K has index 1 in the value group of the corresponding places of the extension) except extensions of the constant field k, we have the converse: The curve E' with

$$U'^3 - V'^2 = c Z^{q^l}, \quad U', V' \in k[t],$$

relatively prime,

$$3 \deg U' - \deg (Z^{q^l}) \equiv 0 \mod 12, \quad 3 \deg U' < \deg (Z^{q^l}), \quad c \in k^*$$

and

$$U' \in K^{*p^l} \quad \text{if} \quad q = p,$$

has all points of order q^l in $E'(K \cdot \bar{k})$.

At first assume: $q = p$.

Then it is easy to find solutions: Take $U_1, V_1 \in k[t] \setminus k$, relatively prime, $2 \deg V_1 \equiv 0 \mod 12$, $3 \deg U_1 < 2 \deg V_1$ and $Z_1 = (U_1^3 - V_1^2) c^{-1}$. By rising to the p-th power we get a solution of the desired shape. As $j^1 = 12^3 U_1^{3p} (U_1^{3p} - V_1^{2p})^{-1}$ is not constant, E' is not defined over k', and so E' is not supersingular, and hence $E'(K \cdot \bar{k})$ contains points of order p^l.

Now assume: $q \neq p$, $q \geqq 7$. Let E be an arbitrary elliptic curve with non constant invariant $j \in K$, defined over $k(j)$ with Hasse-Invariant 1. Then we can choose an equation for E such that the discriminant is:

$$\Delta = 3^3 \cdot 27^2 \cdot j^2 (j - 12^3)^{-3}.$$

Regarded over $k(j)$, E has bad reduction at the places $\mathfrak{P}$ with $v_\mathfrak{P}(j) < 0$ or $v_\mathfrak{P}(j) > 0$ or $v_\mathfrak{P}(j - 12^3) > 0$.

Let P be a point of order q of E, and K_q be equal to $k(j)(x_P)$, where x_P is the X-coordinate of P. By the local theory we conclude: K_q is ramified in these places, the ramification order is equal to q, or is divided by 3 or 2 respectively. The genus formula then gives: $g(K_q) > 0$, and $g(K_q)$ growths like $q(q-1)/6$.

Hence $K_q \not\subset K \cdot \bar{k}$.

On the other side if G_q is the Galoisgroup of $k(j)(E_q)/k(j)$ (E_q the group of points of order q of E) then $G_q \supset Sl(2, q)$, (cf. Igusa [5], the idea of the proof is that otherwise G_q would be contained in a Borel group, as G_q contains elements of order q, and this contradicts the ramification of $k(j)(E_q)/k(j)$ as one sees easily).

Now assume that $E'/K \cdot k$ has the same invariant as E and has a point of order q in $E'(K \cdot \bar{k})$. After a quadratic extension $K_1/K \cdot \bar{k}$ E' is isomorphic to E, and hence $G(K \cdot \bar{k}(E_q)/K \cdot \bar{k})$ has an order dividing $2q$. But this means that the X-coordinate of a point of order q of E has to be in $K \cdot \bar{k}$, and this is a contradiction. So we proved

Proposition 3. *If $K = k(t)$ and $q \neq p$ then there is no elliptic curve E with non constant invariant having a point of order q in $E(K \cdot \bar{k})$, and hence the equation: $U^3 - V^2 = cZ^q$ has no admissible solutions with $U, V \in k[t] \setminus k$, and* $\deg(Z^q) - 3 \deg U \equiv 0 \bmod 12$.

If $q = p$ there are always elliptic curves defined over K with non constant invariant such that $E(K \cdot \bar{k})$ contains points of order p^l ($l \in \mathbf{Z}$).

To end the discussion let K be an arbitrary function field of genus g. Let be $q \neq p$.

Just as above we conclude: There is a bound M depending on g, such that there is no non constant elliptic curve over K with a point of order q if $q \geqq M$.

Let be $U, V \in K$, such that

$$j = 12^3 \frac{U^3}{U^3 - V^2} \notin k,$$

and

$$(j) = (12^3 \cdot U^3)\mathfrak{D}_0^{-1}\mathfrak{D}_1^{12}, \quad \text{with} \quad ((U), \mathfrak{D}_0) = (1)$$

$$v_{\mathfrak{P}}(j) < 0 \quad \text{iff} \quad v_{\mathfrak{P}}(\mathfrak{D}_0) > 0, \quad \text{and then} \quad q | v_{\mathfrak{P}}(\mathfrak{D}_0).$$

Let E be the elliptic curve with absolute invariant j and Hasse-Invariant U/V. Then E is semistable in all places of K, and the adjunction of the points of order q gives an unramified extension of K. Let be $\langle P_i \rangle \subset E_q$, and j_i the invariant of $E/\langle P_i \rangle$. Then $K(j_i)/K$ is unramified and of degree $\leqq q+1$, hence there are only finitely many possibilities for $K(j_i)$. As the Mordell conjecture is true for Φ_q/K (Φ_q the invariant polynomical of degree q) (cf. Samuel [10]) we have for $q \geqq 23$: There are only finitely many elements $(U, V) \in K$ that fulfill the conditions above.

So we get

Proposition 4. *There is a bound M depending on the genus of K such that there is no elliptic curve over K with points of order q in $E(K \cdot \bar{k})$. If $q \geqq 23$, $q \neq p$ then* *there are only finitely many* $U, V \in K$ *such that*

$$j = 12^3 \frac{U^3}{U^3 - V^2} \notin k, \quad (j) = (12^3 U^3)\mathfrak{D}_0^{-1}\mathfrak{D}_1^{12} \quad \textit{with} \quad ((U), \mathfrak{D}_0) = 1,$$

$$v_{\mathfrak{P}}(j) < 0 \quad \textit{iff} \quad v_{\mathfrak{P}}(\mathfrak{D}_0) > 0, \quad \textit{and then} \quad q | v_{\mathfrak{P}}(\mathfrak{D}_0).$$

References

1. DEMJANENKO, V. A., Points of finite order on elliptic curves (Russian). *Acta Arith.*, (1971), 185—194.
2. FREY, G., Elliptische Funktionenkörper mit schlechter Reduktion und nichttrivialer Hasse-Invariante. *Archiv d. Math.*, **XXIII**, (1972), 260—268.
3. FREY, G., Elliptische Kurven über bewerteten Körpern; *Manuskript.*
4. HELLEGOUARCHE, J., Points d'ordre $2p^h$ sur les courbes elliptiques. *Acta Arith.* **26** (1975), 253—263.
5. IGUSA, J., Kroneckerian model of fields of elliptic modular functions. *Amer.* J. *Math.*, **81** (1959), 561—577.
6. LUTZ, E., Sur l'équation $Y^2 = X^3 - AX - B$ dans les corps p-adiques. J. *reine angew. Math.* **177** (1937), 238—244.
7. NERON, A., Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Publ. Math. IHES* **21** (1974).
8. OLSON, L. D., Points of finite order on elliptic curves with complex multiplication. *Manus. Math.*, **14** (1974), 195—205.
9. OLSON, L. D., Torsion points on elliptic curves with given j-invariant. *Manus. Math.* **16** (1975), 145—150.
10. SAMUEL, P., Compléments à un article de Hans Grauert sur la conjecture de Mordell. *Publ. Math. IHES* **29** (1966), 55—62.
11. SERRE, J. P., Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math.* **15** (1972), 259—331.
12. ROQUETTE, P., Analytic theory of elliptic functions over local fields. *Hamb. Math. Einzelschriften, Neue Folge*, Heft 1 (1969).
13. ZIMMER, H. G., Points of finite order on elliptic curves over number fields. *To appear in Archiv d. Math.*

Received October 13, 1975, in revised form April 21, 1976

Gerhard Frey
Mathematisches Institut
der Universität des Saarlandes
D-6600 Saarbrücken
West Germany