Werk

Titel: Torsion points on elliptic curves over fileds of low degree.

Autor: Kamienny, S.

Jahr: 1989

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0065|log26

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 65, 349 - 355 (1989)

manuscripta
mathematica

TORSION POINTS ON ELLIPTIC CURVES OVER FIELDS OF LOW DEGREE

S. Kamienny[1]

In [7] and [8] we proved, for certain small primes p, the non-existence of elliptic curves with rational p-torsion defined over any quadratic field. In this note we give various extensions of this result.

1. Modular Curves

Let p be a prime ≥ 5. If K is any number field we let $Y_0(p)_{/\mathbf{Q}}$ denote the affine curve whose K-rational points classify isomorphism classes of pairs $(E,C)_{/K}$ where E is an elliptic curve over K, and C is a K-rational subgroup of E of order p. We let $X_0(p)_{/\mathbf{Q}}$ denote the complete curve obtained by adjoining the cusps 0 and ∞ to $Y_0(p)_{/\mathbf{Q}}$. Similarly, we let $Y_1(p)_{/\mathbf{Q}}$ be the curve whose K-rational points classify isomorphism classes of pairs $(E,P)_{/K}$ where $E_{/K}$ is an elliptic curve, and P is a K-rational p-torsion point of E. Finally, we let $X_1(p)_{/\mathbf{Q}}$ denote the complete curve obtained from $Y_1(p)_{/\mathbf{Q}}$ by adjoining the p - 1 cusps.

[1]Partially supported by an N.S.A. grant

The curve $Y_1(p)_{/\mathbf{Q}}$ is naturally a cyclic cover of $Y_0(p)_{/\mathbf{Q}}$ of degree $\frac{p-1}{2}$. The covering map $Y_1(p) \to Y_0(p)$ is given by mapping an elliptic curve and a point to the elliptic curve and the subgroup generated by that point. The covering map extends to a map $\Pi: X_1(p) \to X_0(p)$ that is unramified at the cusps. It is known [9] that the cusps of $X_0(p)$ are not Weierstrass points.

We let $J_0(p)$ denote the jacobian of $X_0(p)_{/\mathbf{Q}}$. The abelian variety $J_0(p)$ has good reduction at all primes $l \neq p$. If we embed $X_0(p)$ into $J_0(p)$, sending the cusp ∞ to zero, then the class of $(0 - \infty)$ generates a $\mathbf{Q}$-rational subgroup C of $J_0(p)$ of order num $\left(\frac{p-1}{12}\right)$. For $p = 23, 29, 31, 41, 47, 59$ and 71 Mazur [10] has shown that C is the entire Mordell-Weil group $J_0(p)(\mathbf{Q})$. In general, Mazur has shown that C is the torsion subgroup of $J_0(p)(\mathbf{Q})$.

The Atkin-Lehner involution w acts on $X_0(p)_{/\mathbf{Q}}$ as follows:

$$w(0) = \infty$$

$$w(E,C) = (E/C, C') \text{ where } C' = E[p]/C.$$

This induces an involution (which we again denote by w) of $J_0(p)$.

2. Elliptic Curves and Rational p-torsion

We write g for the genus of $X_0(p)$. In this section K denotes a field of degree $d \leq g$. The table below gives the value of g for some small values of p.

p	g
41	3
47	4
59	5
71	5

Table 2.1

The object of this section is to prove the following:

THEOREM 2.2: *Let* K *be a galois extension of* $\mathbf{Q}$ *of degree* d $\leq$ g. *Then no elliptic curve over* K *can possess a* K*-rational point of order* p (*where* p *and* g *are given in Table* 2.1).

PROOF: We suppose that there exists a pair $(E,P)_{/K}$ consisting of an elliptic curve and a K-rational p-torsion point. The point (E,P) gives us a K-rational point $y \in X_1(p)$, and by projection, a point $x = \Pi(y) \in X_0(p)(K)$. If $\sigma \in Gal(K/\mathbf{Q})$ then x^σ also is a point in $X_0(p)(K)$. Moreover, the class of $\left(\sum_{\sigma \in Gal(K/\mathbf{Q})} x^\sigma - d\infty \right)$ is a $\mathbf{Q}$-rational point on $J_0(p)$. For $p = 47$, 59, or 71 we let $\wp$ denote a prime of K above 2. For $p = 41$ we let $\wp$ denote a prime of K above 3. Let f denote the residue class degree of $\wp$.

LEMMA 2.3: *The point* x^σ *reduces modulo* $\wp$ *to the cusp* $\infty_{/\wp}$.

PROOF: We prove the lemma when $\wp$ has residue characteristic 2. When the residue characteristic is 3 the proof works mutatis mutandis. The curve E must have bad reduction at $\wp$. Otherwise, $E_{/\wp}$ is an elliptic curve over $\mathbf{F}_{2^f}$ having a rational point of order p. However, an elliptic curve over $\mathbf{F}_{2^f}$ can have at most $\left(1 + \sqrt{2^f}\right)^2$ rational points. Since $f \leq d$ and $p > \left(1 + \sqrt{2^d}\right)^2$ we see that the reduction of E cannot be an elliptic curve.

If E has additive reduction at $\wp$ then $(E_{/\wp})^0$ is an additive group, and the index of $(E_{/\wp})^0$ in $E_{/\wp}$ is ≤ 4. Thus, P^σ must specialize to $(E_{/\wp})^0$. But the additive group in characteristic 2 is killed by multiplication by 2, and so P^σ must also be killed by 2, which is clearly impossible. Then E must have multiplicative reduction at $\wp$. To see that $x^\sigma_{/\wp} = \infty_{/\wp}$ we need only check that P^σ does not specialize to $(E_{/\wp})^0$ (see [1]). Assume, to the contrary, that P^σ does specialize to

$(E_{/\wp})^0$. Over a quadratic extension k of F_{2^f} there is an isomorphism $(E_{/k})^0 \doteq G_{m_{/k}}$. Then p must divide the cardinality of k^* which is $(2^{2f} - 1)$. This is impossible with our choices of p and d.

Thus, $(\Sigma x^\sigma - d\infty)_{/\wp} = \Sigma x^\sigma_{/\wp} - d \cdot \infty_{/\wp} = 0$. However, reduction modulo $\wp$ is injective on $J_0(p)(\mathbf{Q})$, and so $(\Sigma x^\sigma - d\infty)$ must already be 0 in $J_0(p)(\mathbf{Q})$. Then there is a function g on $X_0(p)$ whose divisor is $\Sigma x^\sigma - d\infty$, i.e., ∞ is a Weierstrass point of $X_0(p)$. This contradiction proves Theorem 2.2.

3. More on Torsion Points

In this section K will denote a galois extension of $\mathbf{Q}$ of degree $\leq d$. We let G be the galois group $Gal(K/\mathbf{Q})$. As usual, $(E,P)_{/K}$ is a pair consisting of an elliptic curve E and a K-rational p-torsion point P. The relation between p and d is given in Table 3.1.

d	p
4	479 or 491
3	383 or 419
2	223, 229, 233, 239, or 241

Table 3.1

As before, the pair (E,P) gives rise to a K-rational point x on $X_0(p)$. Applying the Atkin-Lehner involution w to x we obtain another K-rational point $x^w \in X_0(p)$. We set $J_- = (1 - w)J$. For the values of p in Table 3.1 Mazur [10] has shown that $J_-(\mathbf{Q})$ is finite.

The purpose of this section is to prove the following.

THEOREM 3.2: *Let* K *be a galois extension of* $\mathbf{Q}$ *of degree* $\leq$ d. *Then no elliptic curve over* K *can possess a* K*-rational point of*

order p (*where* d *and* p *are given in Table* 3.1).

PROOF: Assume, to the contrary, that there is a pair (E,P) defined over K. Let x denote the corresponding point on $X_0(p)(K)$. The class of $z = \left(\sum_{\sigma \in G} x^\sigma - (x^w)^\sigma + d(0 - \infty) \right)$ is Q-rational and lies in J_-. For $p \neq 233$ or 241 we let $\wp$ denote a prime of K above 2. For $p = 233$ or 241 we let $\wp$ denote a prime of K above 3. Then Lemma 2.3 is still valid, so $x^\sigma_{/\wp} = \infty_{/\wp}$ and $(x^w)^\sigma_{/\wp} = 0_{/\wp}$. Thus, $z_{/\wp} = 0$. However, reduction modulo $\wp$ is injective on $J_-(Q)$, and so z must be 0. Then there is a function g on $X_0(p)$ of degree 2d. We use a trick of Ogg's (see [11]) to see that this is impossible. If $X_0(p)$ has a function of degree 2d then $X_0(p)_{/F_4}$ is a degree 2d-cover of $P^1(F_4)$. Thus, the number of F_4-rational points on $X_0(p)$ is $\leq 2d \cdot (5) = 10d$. However, Ogg has found at least $\frac{p}{12} + 2$ rational points on $X_0(p)_{/F_4}$, so $\frac{p}{12} + 2 \leq 10d$, which is impossible with our choices of p and d. This contradiction proves Theorem 3.2.

4. p-torsion Over Quadratic Extensions of $Q(\sqrt{p})$

In this section we assume that p is a prime $\equiv 1 \pmod 4$, and $p > 17$. A minor generalization of the descent argument given in [6] (this will appear in [3]) shows that there is a quotient J of $J_1(p)$ with finite Mordell-Weil group over $K = Q(\sqrt{p})$. We prove the following.

THEOREM 4.1: *Let* $p > 17$ *be a prime* $\equiv 1 \pmod 4$. *There are only finitely many elliptic curves with rational* p*-torsion defined over the totality of quadratic extensions of* $Q(\sqrt{p})$.

PROOF: We use a minor abstraction of an idea of Frey [2] (see also [5]). Assume that there are infinitely many such curves. Each curve gives us a point x on $X_1(p)$. Let F be a quadratic extension of K for which there is a pair (E,P) consisting of an elliptic curve with an F-rational p-torsion point. Let z denote the point on $X_1(p)$ corresponding to (E,P), and let $\bar{z}$ denote the conjugate of z by the

non-trivial element of $Gal(F/K)$.

Let $X^{(2)}$ denote the symmetric product of $X_1(p)$ with itself. Our assumption that there are infinitely many curves with rational p-torsion implies that $X^{(2)}(K)$ is infinite. Define a map $f:X^{(2)} \to J_1(p)$ by $f(x,y) = (x + y - z - \bar{z})$. The map f is injective as long as $X_1(p)$ is not hyperelliptic (which is the case when $p \geq 17$). We may, therefore, identify $X^{(2)}$ with its image under f. As above, we let J be a factor of $J_1(p)$ with finite Mordell-Weil group over K, and we let h denote the composition of f with the natural projection Π onto J:

$$X^{(2)} \xrightarrow{f} J_1(p) \xrightarrow{\Pi} J.$$

$$\searrow \quad \nearrow$$

$$h$$

Since $J(K)$ is finite we see that $X^{(2)}(K) \cap \operatorname{Ker} \Pi$ is infinte. Thus, $X^{(2)} \cap \operatorname{Ker} \Pi$ is a subvariety of $X^{(2)}$ whose dimension is ≤ 1 (since its Zariski closure contains infinitely many points). Moreover, $X^{(2)} \cap \operatorname{Ker} \Pi$ cannot be 2 dimensional since the image of $X^{(2)}$ in J must generate J. Thus, $X^{(2)} \cap \operatorname{Ker} \Pi$ is of dimension 1, and so must contain a curve C whose genus is ≤ 1. This curve has a function f of degree ≤ 2. We lift C to a curve $\tilde{C}$ in $X_1(p) \times X_1(p)$. Then $\tilde{C}$ is a degree 2 cover of C, and so must have a function $\tilde{f}$ of degree ≤ 4. Without loss of generality, we may assume $\tilde{C}$ projects onto the first factor of $X_1(p) \times X_1(p)$. Then the norm $N\tilde{f}$ of $\tilde{f}$ from $\tilde{C}$ to the first factor is a function on $X_1(p)$ of degree ≤ 4. If this is the case then $X_1(p)_{/\mathbb{F}_2}$ is a cover of $\mathbf{P}^1(\mathbf{F}_2)$ of degree ≤ 4. Then the cardinality of $X_1(p)_{/\mathbb{F}_2}$ is $\leq 4 \cdot 3 = 12$. However, $X_1(p)$ has $\frac{p-1}{2}$ rational cusps, and so $\frac{p^2-1}{2} \leq 12$ or $p \leq 25$, contrary to hypothesis. Thus, Ogg's trick once again proves our theorem.

References

(1) Deligne, P. and Rapoport, M.: Schémas de modules de courbes elliptiques, Lect. Notes. Math. 349, Berlin-Heidelberg-New York: Springer (1973)

(2) Frey, G.: A Remark About Isogenies of Elliptic Curves over Quadratic Fields, Comp. Math. 58, 133-134 (1986)

(3) Indik, R. and Kamienny, S.: In preparation

(4) Kamienny, S.: p-Torsion on Elliptic Curves over Subfields of $\mathbf{Q}(\mu_p)$, Math. Ann. 280, 513-519 (1988)

(5) Kamienny, S.: Points on Shimura Curves over Fields of Even Degree, to appear

(6) Kamienny, S.: Points of Order p on Elliptic Curves over $\mathbf{Q}(\sqrt{p})$, Math. Ann. 261, 413-424 (1982)

(7) Kamienny, S.: Torsion Points on Elliptic Curves over all Quadratic Fields, Duke Math. J. 53, 157-162 (1986)

(8) Kamienny, S.: Torsion Points on Elliptic Curves over all Quadratic Fields II, Bull. Soc. Math. France 114, 119-122 (1986).

(9) Lehner, J. & Newman, M.: Weierstrass points of $\Gamma_0(n)$, Ann. Math. 79, 360-368 (1964)

(10) Mazur, B.: Modular Curves and the Eisenstein Ideal, Publ. Math. I. H. E. S. 47, 33-186 (1978).

(11) Ogg, A.: Hyperelliptic modular curves, Bull. Soc. Math. France 102, 449-462 (1974)

Author's Address: Department of Mathematics
University of Arizona
Tucson, AZ 85721, USA

(Received May 2, 1989)