BULLETIN DE LA S. M. F.

SHELDON KAMIENNY

Torsion points on elliptic curves over all quadratic fields. II

Bulletin de la S. M. F., tome 114 (1986), p. 119-122

<http://www.numdam.org/item?id=BSMF_1986__114__119_0>

Bull. Soc. math. France,
114, 1986,

TORSION POINTS ON ELLIPTIC CURVES OVER ALL QUADRATIC FIELDS II

BY

SHELDON KAMIENNY (*)

RÉSUMÉ. – Soit K un corps quadratique, et soit E une courbe elliptique définie sur K. Nous prouvons que $E(K)$ ne possède pas un point d'ordre $N=41$, 47, 59, ou 71.

ABSTRACT. – Let K be any quadratic field, and let E be any elliptic curve defined over K. We prove that $E(K)$ cannot possess a point of order $N=41$, 47, 59, or 71.

1. Introduction

In [1] we proved that there is no quadratic field K over which is defined a pair $(E, \mathbf{P})/K$ consisting of an elliptic curve E and a K-rational point $\mathbf{P}$ of order p for $p=17$, 19, 23, 29, or 31. Our proof depended on the existence of a non-hyperelliptic quotient (of genus $\geqslant 2$) of $X_1(p)$ whose jacobian has finite Mordell-Weil group over $\mathbf{Q}$. In this note we extend the results of [1] to include the cases $p=41$, 47, 59, and 71. In these cases our proof depends on the fact that $X_0(p)$ is hyperellipic, and that the hyperelliptic involution coincides with the Atkin-Lehner involution. By combining the ideas of [1] with the ideas of this paper it is an easy matter to see that the above result extends to all natural numbers $N(\neq 40, 48$, or 30, 33, 45, 60) such that $X_0(N)$ is of genus $\geqslant 2$, and $J_0(N)(\mathbf{Q})$ is finite. The first two exceptional cases $N=40$, 48 are the values of N for which $X_0(N)$ is hyperelliptic, but the hyperelliptic involution is not of Atkin-Lehner type (this is also the case when $N=37$, however, $J_0(37)(\mathbf{Q})$ has rank 1). The other exceptional cases are the values of N for which the analogue of Lemma 3.1 (*see* §3) may fail to be true. We also show that our methods can be made to yield information about elliptic curves with rational p-torsion over certain quartic extensions of $\mathbf{Q}$.

(*) Texte reçu le 1er février 1985.

S. KAMIENNY, Department of Mathematics, 231, West 18th Avenue, Columbus, Ohio 43210, U.S.A. Partially supported by N.S.F. Grant.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE – 0037-9484/1986/01 119 4/$ 2.40

I would like to thank A. Ogg and K. Rubin for some invaluable conversations.

2. Modular curves

Let K be a number field, p a prime $\geqslant 5$, and let $Y_0(p)/\mathbf{Q}$ denote the curve whose K-rational points classify isomorphism classes of pairs $(E, C)/K$ where E/K is an elliptic curve, and C is a K-rational subgroup of E of order p. Denote by $X_0(p)/\mathbf{Q}$ the complete curve obtained by adjoining the cusps 0 and ∞ to $Y_0(p)/\mathbf{Q}$. Similarly, let $Y_1(p)/\mathbf{Q}$ be the curve whose K-rational points classify isomorphism classes of pairs $(E, \mathbf{P})/K$ where E/K is an elliptic curve, and $\mathbf{P}$ is a K-rational p-torsion point of E. Finally, let $X_1(p)/\mathbf{Q}$ denote the complete curve obtained from $Y_1(p)/\mathbf{Q}$ by adjoining the $p-1$ cusps. The curve $Y_1(p)/\mathbf{Q}$ is naturally a cyclic cover of $Y_0(p)/\mathbf{Q}$ of degree $(p-1)/2$. The covering map $Y_1(p) \to Y_0(p)$ is given by sending an elliptic curve and a point to the elliptic curve and the subgroup generated by that point. The covering map extends to a map

$$\Pi : X_1(p)/\mathbf{Q} \to X_0(p)/\mathbf{Q}$$

that is unramified at the cusps.

We denote by $J_0(p)/\mathbf{Q}$ the Jacobian of $X_0(p)/\mathbf{Q}$. The abelian variety $J_0(p)$ is semi-stable over $\mathbf{Q}$, and has good reduction at all primes l different from p. If we embed $X_0(p)/\mathbf{Q}$ into $J_0(p)/\mathbf{Q}$ sending ∞ to zero then the class of $0-\infty$ generates a $\mathbf{Q}$-rational subgroup C of $J_0(p)/\mathbf{Q}$ of order $n = \text{num}\ (p-1)/12$. For $p = 23$, 29, 31, 41, 47, 59, and 71 MAZUR [2] has shown that C is the entire Mordell-Weil group $J_0(p)(\mathbf{Q})$.

The Atkin-Lehner involution w_p of $X_0(p)$ induces an involution (that we again denote by w_p) of $J_0(p)/\mathbf{Q}$. The cusps 0 and ∞ are interchanged by w_p. OGG [4] has determined the complete set of N for which $X_0(N)$ is hyperelliptic. For three of these values ($N = 37$, 40, and 48) the hyperelliptic involution is not of Atkin-Lehner type. For the remaining sixteen values of N the hyperelliptic involution is of Atkin-Lehner type. In particular, this is the case for $p = 23$, 29, 31, 41, 47, 59, and 71. Since p is prime in each of these cases, the hyperelliptic involution is w_p.

3. Elliptic curves with rational p-torsion

In all that follows we let K be a quadratic field, and we let σ be the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$. We assume that there is an elliptic curve E/K with a K-rational point $\mathbf{P}$ of order p, where p is one of the primes 23, 29, 31, 41, 47, 59, or 71. We regard the pair $(E, \mathbf{P})$ as giving rise to a K-rational point x on $X_1(p)$, and also to a point (again denoted x) on $X_0(p)$ via the projection Π.

LEMMA 3.1. — *Let S denote the spectrum of the ring of integers of K. If $s \in S$ is a point of characteristic 3 then $x/s = \infty/s$, i.e., the point x reduces to the ∞-cusp modulo s.*

Proof. — We first note that E must have bad reduction at s. Otherwise, E/s is an elliptic curve and $\mathbf{P}/s$ is a rational point of E/s of order p. However, an elliptic curve over the field $\mathbf{F}_9$ can have at most $(1+\sqrt{9})^2 = 16$ points. Since $p \geqslant 23$ this is a contradiction. Thus, E has bad reduction at s, and we need only check that the reduction is multiplicative, and that $\mathbf{P}$ does not specialize to $(E/s)^0$. If E has additive reduction at s then $(E/s)^0$ is an additive group, and the index of $(E/s)^0$ in E/s $\leqslant 4$. Hence, our point $\mathbf{P}$ must reduce modulo s to the connected component of E/s. Thus, we have that $(\mathbf{Z}/p\mathbf{Z})/s \subset (E/s)^0$. Since the additive group in characteristic 3 is killed by multiplication by 3 we must have that $p = 3$, a contradiction. Thus, E has multiplicative reduction at s. Suppose that $\mathbf{P}$ does specialize to $(E/s)^0$. Let $k(s)$ denote the residue field at s. Over a quadratic extension F of $k(s)$ we have an isomorphism $(E/F)^0 = \mathbf{G}_m/F$, so p divides the cardinality of F^*, which must itself divide $80 = 3^4 - 1$. This contradiction proves the lemma.

LEMMA 3.2. — *If $s \in S$ is a point of characteristic 3 then reduction modulo s is injective on $J_0(p)(\mathbf{Q}) = C$.*

Since $J_0(p)$ has good reduction at 3 Lemma 4.2 of [1] applies, giving us Lemma 3.2. The lemma also follows immediately from the Specialization Lemma of RAYNAUD [5].

We now define a map

$$f: \quad X_0(p)(K) \to J_0(p)(\mathbf{Q}) \qquad \text{by} \quad f(x) = cl(x + x^\sigma - 2\infty).$$

By Lemma 3.1

$$f(x)/s = cl(x/s + x^\sigma/s - 2\infty/s) = cl(\infty/s + \infty/s - 2\infty/s) = 0.$$

By Lemma 3.2 $f(x)$ must also be zero. Thus, there is a function g on $X_0(p)$ whose divisor is $(x+x^\sigma-2\infty)$. Since g is a function of degree 2 it must be fixed by the hyperelliptic involution. Thus, the point ∞ must also be fixed by the hyperelliptic involution. But the hyperelliptic involution coincides with the Atkin-Lehner involution, and the latter interchanges the cusps 0 and ∞. This contradiction gives us the following.

THEOREM 3.3. — *Let p be one of the primes* 23, 29, 31, 41, 47, 59, *or* 71, *and let K be any quadratic field. There is no elliptic curve defined over K containing a K-rational point of order p.*

Finally, we remark that our methods can also be made to yield information about elliptic curves over certain quartic fields. Let F be a quadratic imaginary field with character χ, and assume that 3 is unramified in F. MAZUR [3] has shown that the Mordell-Weil group $J_0(p)(F)$ is finite for $p=23$, 29, 31, 41, 47, or 59 if $\chi(p)=-1$, and the class number of F is relatively prime to at least one of the prime divisors of n (a similar, although slightly more complicated, fact holds for $p=71$). If, in the preceding arguments, we replace $\mathbf{Q}$ by such an F, and K by a quadratic extension of F in which 3 has residue class degree $\leqslant 2$, we obtain the following.

THEOREM 3.4. — *Let K and F be chosen as above. There is no elliptic curve defined over F containing an F-rational point of order p.*

REFERENCES

[1] KAMIENNY (S.). — *Torsion points on elliptic curves over all quadratic fields* (to appear in Duke Math Journal.)

[2] MAZUR (B.). — *Modular curves and the Eisenstein ideal*, Publications Mathématiques I.H.E.S., Vol. 47, 1978.

[3] MAZUR (B.). — On the arithmetic of special values of L functions, *Inventiones Math.*, Vol. 55, 1979, pp. 207-240.

[4] OGG (A.). — Hyperelliptic modular curves, *Bull. Soc. Math. Fr.*, Vol. 102, 1974, pp. 449-462.

[5] RAYNAUD (M.). — Schémas en groupes de type $(p, \ldots, p)$, *Bull. Soc. Math. Fr.*, Vol. 102, 1974, pp. 241-280.