On the supersingular reduction of elliptic curves

M RAM MURTY*

Department of Mathematics, McGill University, 805 Sherbrooke Street West, Montreal, Canada H3A 2K6

Abstract. Let $a \in Q$ and denote by E_a the curve $y^2 = (x^2 + 1)(x + a)$. We prove that $E_a(F_p)$ is cyclic for infinitely many primes p. This fact was known previously only under the assumption of the generalized Riemann hypothesis.

Keywords. Supersingular reduction, elliptic curves.

Let E be an elliptic curve defined over Q. For all but finitely many primes p, E has good reduction (mod p) and it makes sense to consider E (mod p). It is classical (see [1]) that the ring $\text{End}_{\bar{F}_p}(E)$ of algebraic endomorphisms defined over $\bar{F}_p$ has Z-rank 2 or 4. In the latter case, E is said to have supersingular reduction (mod p). Our first result is:

Theorem 1. *Let E be an elliptic curve defined over Q and suppose that E has supersingular reduction* (mod p). *Then the 2-complement of $E(F_p)$ is cyclic.*

The interest of Theorem 1 lies in the following. In 1976, Lang and Trotter [4] formulated the following conjecture. Let E be an elliptic curve and suppose that the group of rational points $E(Q)$ has positive rank. Let a be a point of infinite order. Then they conjectured that the reduction of a mod (p) generates $E(F_p)$ for infinitely many primes p. This conjecture was proved in [3] for the case that E has complex multiplication, assuming the generalized Riemann hypothesis (GRH). The case when E has no complex multiplication is still open, even assuming the generalized Riemann hypothesis. As Serre observed in [6], if the conjecture of Lang and Trotter is true, then $E(F_p)$ is cyclic infinitely often. Indeed, assuming GRH, Serre showed that this was the case. In [5], the assumption of the GRH was removed in the case that E has complex multiplication (CM) by an order in an imaginary quadratic field. Thus, if E has CM, then $E(F_p)$ is cyclic infinitely often. The elimination of GRH from Serre's proof involved the use of sieve methods and an analogue of the Bombieri-Vinogradov theorem in algebraic number fields. Such an analogue is non-existent in the non-CM case and it is highly desirable to have one, for more than one reason. Moreover, sieve methods break down completely in the non-CM case.

In this paper, we will consider the following elliptic curves:

$$E_a: y^2 = (x^2 + 1)(x + a), \quad a \in Q.$$

The j-invariant of E_a denoted j_a is easily seen to be

$$j_a = 54a^4 - 738a^2 + 27a + 27.$$

There are precisely thirteen values of the j-invariant, namely

$$j = 2^6 3^3, 2^6 5^3, 0, -3^3 5^3, -2^{15}, -2^{15} 3^3,$$

$$-2^{18} 3^3 5^3, -2^{15} 3^3 5^3 11^3, -2^{18} 3^3 5^3 23^3 29^3,$$

$$2^3 3^3 11^3, 2^4 3^3 5^3, 3^3 5^3 17^3, -3^{12} 1^5 5^3,$$

for which a given elliptic curve E over Q has complex multiplication. Thus, there are only finitely many values of a for which E_a has complex multiplication. Thus, for all but finitely many values of a, E_a has no complex multiplication.

Recently, Elkies [2] proved that any elliptic curve E defined over Q has infinitely many primes p for which E has supersingular reduction (mod p). We will utilise this fact together with Theorem 1 to deduce.

Theorem 2. *Let E be the elliptic curve E_a defined above. There are infinitely many primes p such that $E(F_p)$ is cyclic.*

In order to prove these theorems, we will need the following lemma which is of interest in its own right.

Lemma 1. Let $g: E_1 \to E_2$ and $f: E_1 \to E_3$ be morphisms of elliptic curves such that $\ker g \subseteq \ker f$. Then there is a morphism $h: E_2 \to E_3$ such that $f = g \circ h$.

Proof. Let s be a section of g and define $h(x) = f(s(x))$. This is independent of the choice of section. Indeed, if t is another section of g, then $f(s(x) - t(x)) = 0$ if and only if $s(x) - t(x)$ is in the kernel of f. But by definition, $s(x) - t(x)$ is in the kernel of g, which is contained in the kernel of f, by hypothesis. This shows that h is well-defined. h is clearly a morphism of elliptic curves.

Lemma 2. Let p and q be distinct prime numbers. Suppose that $p > 2$ and that E has good reduction (mod p). Then p splits completely in $Q(E_q)$ if and only if $E(F_p)$ contains a subgroup of type (q, q).

Proof. Let $\bar{E}$ denote the reduction of E over F_p and let π_p denote the Frobenius endomorphism of $\bar{E}$ over $\bar{F}_p$, given by $\pi_p(x) = x^p$. Then, the set of fixed points of

$$\pi_p: \bar{E} \to \bar{E}$$

constitute $E(F_p)$. Thus, $E(F_p)$ contains a subgroup of type (q, q) if and only if π_p acts trivially on the q-division points of $\bar{E}$, because the q-division points of $\bar{E}$ over $\bar{F}_p$ constitute a subgroup isomorphic to $Z/qZ \times Z/qZ$. We conclude that the decomposition group of any prime lying above p is trivial if and only if $E(F_p)$ contains a (q, q) group. This is the desired result.

COROLLARY.

Let $p > 2$. $E(F_p)$ is cyclic if and only if p does not split completely in all of the fields $Q(E_q)$ as q ranges over the primes.

Proof. $E(F_p)$ is cyclic if and only if it does not contain a (q, q) group for every prime p. For $q \not\equiv p$, the result is immediate from the lemma. Suppose therefore that $q = p$ and that $E(F_p)$ contains a subgroup of type (p, p). Then $p^2 \leqslant p + 1 + 2\sqrt{p}$ by familiar estimates for the size of $E(F_p)$. But this last inequality forces $p = 2$.

We are now ready to prove Theorem 1.

Proof of Theorem 1. If $E(F_p)$ contains a subgroup of type (q, q) for some q, then this subgroup is contained in the set of fixed points of the Frobenius endomorphism π_p. If f_q denotes the endomorphism of multiplication by q, then

$$\ker f_q \subseteq \ker(\pi_p - 1).$$

By Lemma 1, we deduce that

$$(\pi_p - 1)/q$$

is an algebraic integer. If E has supersingular reduction (mod p), then $\pi_p = \pm \sqrt{-p}$. If $q > 2$, then

$$(\pm \sqrt{-p} - 1)/q$$

is never an algebraic integer. Therefore, $E(F_p)$ does not contain a subgroup of type (q, q) when $q > 2$. Thus, the 2-complement of $E(F_p)$ is cyclic.

If E is given in Weierstrass form:

$$y^2 = x^3 + ax + b,$$

and the roots of $x^3 + ax + b = 0$ are x_1, x_2, x_3, then the 2-division points are just the points $(x_i, 0), i = 1, 2, 3$ together with the point at infinity. If p is a prime for which E has supersingular reduction, then $E(F_p)$ has size $p + 1$. By Theorem 1, we know that the 2-complement is cyclic. If $E(F_p)$ contains the 2-division points, then by lemma 2, p splits completely in $Q(E_2)$, that is, the field obtained by adjoining x_1, x_2, x_3. For the curves E_a, we have that $Q(E_2) \supset Q(\sqrt{-1})$. Therefore if p splits completely in $Q(E_2)$, it splits completely in $Q(i)$ so that $p \equiv 1 \pmod 4$ is forced. Thus, 4 cannot divide $p + 1$ and so $E(F_p)$ is cyclic. This proves Theorem 2.

It is clear from the above discussion that the same argument shows that the curve

$$E: y^2 = x^3 + ax + b, \quad a, b \in Q$$

has the property that $E(F_p)$ is cyclic whenever E has supersingular reduction (mod p) and the roots of $x^3 + ax + b = 0$ generate $Q(i)$.

It is also interesting to note that for each of the curves E_a there is no prime $p \equiv 3$ (mod 4) for which E_a has supersingular reduction.

References

[1] Deuring M, Die typen der multiplikatorenringe elliptischer funktionenkörper, *Abh. Math. Sem. Hanisischen Univ.* **14** (1941) 191–272

[2] Elkies N, The existence of infinitely many supersingular primes for every elliptic curve over Q, *Invent. Math.* **89** (1987) 561–567

[3] Gupta R and Ram Murty M, Primitive points on elliptic curves, *Compos. Math.* **58** (1986) 13–44

[4] Lang S and Trotter H, Primitive points on elliptic curves, *Bull. Am. Math. Soc.* **83** (1977) 289–292

[5] Ram Murty M, On Artin's conjecture, *J. Number Theory* **16** (1983) 147–168

[6] Serre J-P, *Resumé de cours* (1977) (Oeavres: Springer Verlag) (1986)