COMPOSITIO MATHEMATICA

NOAM D. ELKIES

Supersingular primes for elliptic curves over real number fields

Compositio Mathematica, tome 72, n° 2 (1989), p. 165-172

<http://www.numdam.org/item?id=CM_1989__72_2_165_0>

Compositio Mathematica **72**: 165–172, 1989.

Supersingular primes for elliptic curves over real number fields

NOAM D. ELKIES*

Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA

Received 19 November 1988; accepted 2 March 1989

0. Introduction

Let E be a fixed elliptic curve defined over a number field K. In [3] we showed that E has infinitely many primes of supersingular reduction in the case $K = \mathbf{Q}$, or more generally when K is an extension of odd degree of $\mathbf{Q}$. Here we use a similar technique to extend this result to any number field K with at least one real embedding:

THEOREM. *Let E be a fixed elliptic curve defined over a number field K with at least one real embedding. Let S be any finite set of primes of K. Then E has a supersingular prime outside S.*

The exposition of the proof is organized as follows: Section 1 introduces complex multiplication and the polynomials P_D, Section 2 describes the factorization of P_D over the finite fields of characteristic $l|D$, Section 3 treats the factorization of P_D over $\mathbf{R}$, and Section 4 applies these results to prove the infinitude of supersingular primes.

REMARK. The heuristic of [5] for the distrbution of supersingular primes for an elliptic curve over $\mathbf{Q}$ extends to supersingular primes of prime residue field for an elliptic curve over any number field: the number of such primes of norm up to x should be $(C_E + o(1))\sqrt{x}/\log x$ for some C_E depending explicitly on E. Unfortunately, the argument that $C_E > 0$ ([5, p. 37]) only applies when K has a real embedding; indeed one can find curves over totally complex number fields (such as the curve with j-invariant $2^{14}/(i-4)$ of [3]) for which $C_E = 0$, so their supersingular primes are expected to be much rarer – on the order of $\log\log x$ of norm less than x – and cannot be detected by the methods of [3] and the present paper. Thus our apparently artificial restriction to number fields with a real embedding seems to reflect a genuine new difficulty for totally complex fields. However, I can neither prove that all curves with $C_E > 0$ have infinitely many

*NSF Grant DMS-87-18965.

supersingular primes nor construct an elliptic curve over a totally complex number field that can be proved to have only finitely many such primes.

1. Preliminary notions[1]

For a prime π of K at which E has food reduction let E_π be the reduction of E mod π. An elliptic curve over any field F will be said to have complex multiplication by the quadratic order

$$O_D = \mathbf{Z}[\tfrac{1}{2}(D + \sqrt{-D})] \qquad (D \equiv 0 \text{ or } -1 \bmod 4)$$

of discriminant $-D$ if O_D is maximally embedded in its $\bar{F}$-endomorphism ring A, that is, if there exists an embedding $\iota: O_D \hookrightarrow A$ such that

$$\iota(O_D) = A \cap (\iota(O_D) \otimes \mathbf{Q}).$$

Now E_π is supersingular if and only if it has complex multiplication by some O_D such that the residual characteristic p of π is ramified or inert in $\mathbf{Q}(\sqrt{-D})$ (see [2]). Let us denote a positive rational prime congruent to 1 or 3 mod 4 by l_1 or l_3 respectively. In [3] we proved the case $K = \mathbf{Q}$ of the Theorem by forcing E_π to have complex multiplication by O_D for some $D = l_3$ or $4l_3$ with $(-D/p) \neq 1$. To prove it in general we shall use instead D of the form $l_1 l_3$ or $4l_1 l_3$ for suitable l_1, l_3.

For any positive $D \equiv 0$ or $-1 \bmod 4$, let $P_D(X) \in \mathbf{Z}[X]$ be the irreducible monic polynomial whose roots are the j-invariants of elliptic curves over $\bar{\mathbf{Q}}$ with complex multiplication by O_D. The roots of $P_D(X)$ in characteristic p are then j-invariants of curves with an endomorphism $(D + \sqrt{-D})/2$ and thus with complex multiplication by $O_{D'}$ for some factor D' of D such that D/D' is a perfect square. Now let $j_E \in K$ be the j-invariant of E. Given j_E, we can always find an elliptic curve of j-invariant j_E defined over $\mathbf{Q}(j_E)$ that is isomorphic to E over $\bar{\mathbf{Q}}$, and since supersingularity depends only on the j-invariant we may and henceforth will assume $K = \mathbf{Q}(j_E)$. Then E_π has complex multiplication by $O_{D'}$ for some D' as above if j_E is a root of $P_D(X) \bmod \pi$, that is, if $P_D(j_E)$ has a positive π-valuation. If, furthermore, $-D$ (thus also $-D'$) is not a p-adic square, then π is a supersingular prime for E.

Our strategy for constructing a new supersingular prime π for E is to find $D = -l_1 l_3$ or $-4l_1 l_3$ such that $P_D(X)$ must have positive π-valuation for some

[1] We retain the notations of [3], except that j-invariants are denoted only by lower-case j's and the notations for primes are adapted to the case of a general number field.

$\pi \notin S$ whose residual characteristic p is ramified or inert in $\mathbf{Q}(\sqrt{-l_1 l_3})$, or equivalently has $\chi_{l_1 l_3}(p) \neq +1$ where $\chi_{l_1 l_3}$ is the Jacobi character $(\cdot/l_1 l_3)$. Let $N_D(j_E)$ be the absolute value of the numerator of the norm $\mathbf{N}_{\mathbf{Q}}^{K} P_D(j_E)$ of $P_D(j_E)$, and denote by $\mathbf{N}_{\mathbf{Q}}^{K}(S)$ the set of rational primes lying under primes in S. Then it will suffice to ensure that $N_D(j_E)$ is not divisible by any $p \in \mathbf{N}_{\mathbf{Q}}^{K}(S)$ and that $\chi_{l_1 l_3}(N_D(j_E)) \neq +1$, since then $N_D(j_E)$ is necessarily divisible by some rational prime $p \notin \mathbf{N}_{\mathbf{Q}}^{K}(S)$ ramified or inert in $\mathbf{Q}(\sqrt{-D})$, whence $P_D(j_E)$ has positive valuation at some new supersingular prime $\pi \notin S$ lying above p. To evaluate $\chi_{l_1 l_3}(N_D(j_E))$, we shall use information on the factorization of $P_D(X)$ in characteristics l_1 and l_3 and over $\mathbf{R}$; we obtain this information in the next two Sections.

2. Factorization of $P_D(X)$ modulo primes l ramified in $\mathbf{Q}(\sqrt{-D})$

Let D be any positive integer congruent to 0 or 1 mod 4, and l a prime ramified in $\mathbf{Q}(\sqrt{-D})$. We then have the following generalization of the Proposition in Sect. 2 of [3]:

PROPOSITION 1. *All the roots of* $P_D(X)$ mod l, *except possibly* 1728, *occur with even multiplicity.*

Proof (with B. Gross): We first observe that these roots are all supersingular j-invariants mod l by [2]. In particular if $l = 2$ or 3 then the only supersingular j-invariant is $0 = 1728$ and the Proposition is trivial. Thus we may and will henceforth assume $l > 3$.

Consider first the case that $-D$ is a fundamental discriminant. Let λ be a prime of the splitting field L of $P_D(X)$ which lies over l and let $\mathscr{E}$ be any supersingular elliptic curve defined over the residue field F of λ. We shall show that, unless $\mathscr{E}$ has an automorphism of order 4 ($\Leftrightarrow$ $\mathscr{E}$ has complex multiplication by $O_4 = \mathbf{Z}[\sqrt{-1}] \Leftrightarrow \mathscr{E}$ has j-invariant 1728), liftings of $\mathscr{E}$ to an elliptic curve in characteristic zero with complex multiplication by O_D come naturally in pairs.

Fix algebraic closures $\bar{L}, \bar{F}$ of L and F, and an embedding of O_D into $\bar{L}$ (so, reducing mod λ, also a homomorphism of O_D to $\bar{F}$). Then define an embedding of O_D into the endomorphism ring of an elliptic curve over L (or F) to be *normalized* if each $\alpha \in O_D$ induces multiplication by the image of α under this embedding (resp. homomorphism) on the tangent space of the curve. Let $\mathscr{A}$ be the $\bar{F}$-endomorphism ring of $\mathscr{E}$; $\mathscr{A}$ is a maximal order in a quaternion algebra over $\mathbf{Q}$ ramified at $\{p, \infty\}$. From any lifting of $\mathscr{E}$ to a curve E_1 in characteristic zero with complex multiplication by O_D we obtain an embedding $\iota: O_D \hookrightarrow \mathscr{A}$ by reduction mod λ. This embedding will be normalized if we choose our action of O_D on E_1 to be normalized. Conversely, we have the following refinement

[4, Prop. 2.7] of Deuring's Lifting Lemma [2, p. 259]:

Every normalized embedding $\iota: O_D \hookrightarrow \mathscr{A}$ lifts, uniquely up to isomorphism,[2] *to a normalized action of O_D on a curve E_1 in characteristic zero.*

All of this is true for every D such that $-D$ is a fundamental discriminant. The additional assumption that l ramifies in $\mathbf{Q}(\sqrt{-D})$ means that normalized embeddings $O_D \hookrightarrow \mathscr{A}$ come in pairs: if ι is such an embedding, so is its conjugate $\bar{\iota}$, and it lifts to another curve E_2 in characteristic zero. It remains to show that, provided $\mathscr{E}$ does not have j-invariant 1728, the j-invariants of E_1 and E_2 are distinct, or equivalently that E_1 and E_2 are not isomorphic over $\bar{L}$. But such an isomorphism would reduce mod λ to an automorphism $\varepsilon \in \mathscr{A}^\times$ such that $\alpha\varepsilon = \varepsilon\bar{\alpha}$ for all $\alpha \in \iota(O_D)$, whence ε is a square root of -1, and $\mathscr{E}$, having complex multiplication by O_4, would have j-invariant 1728. This proves the Proposition when $-D$ is a fundamental discriminant.

Now if $-D$ is not a fundamental discriminant then $D = c^2 D_1$ where $-D_1$ is a fundamental discriminant. The zero divisor of P_D is then a linear combination with integral coefficients of the divisors obtained from the zero divisor of P_{D_1} by the Hecke correspondences T_d, $d|c$. [The correspondence T_d sends the j-invariant of an elliptic curve E_0 to the formal sum of the j-invariants of the curves E_0/G, G ranging over the $\sigma(d)$ cyclic order-d subgroups of E_0. In characteristic zero, if E_0 has complex multiplication by O_{D_1} for some fundamental discriminant D_1, each of the curves $E_1 = E_0/G$ will have complex multiplication by the quadratic order of discriminant $d'^2 D_1$ for some $d'|d$; conversely, for any such d', the j-invariant of any curve E_1 with complex multiplication by $O_{d'^2 D_1}$ occurs $M(D_1, d, d')$ times this way, with $M(D_1, d, d) = 1$, and in general $M(D_1, d, d')$ depending on the factorization in O_{D_1} of the rational primes dividing d, d', but not on the choice of E_1. It then follows by induction on the number of prime factors of c that the zero divisor of $P_{c^2 D_1}$ may be obtained from the zero divisor of P_{D_1} by the application of a $\mathbf{Z}$-linear combination of the correspondences T_d for $d|c$.] Thus, since all the coefficients of the divisor $T_d(1728)$ are even with the possible exception of the coefficient of 1728 itself,[3] we obtain the Proposition for all discriminants from the fundamental ones. Q.E.D.

COROLLARY. *$P_{l_1 l_3}(X)$ and $P_{4l_1 l_3}(X)$ are perfect squares modulo both l_1 and l_3.*

Proof. In view of Proposition 1 it suffices to show that the degrees of $P_{l_1 l_3}(X)$

[2] That is, if E_1 and E_2 are two such lifts of $\mathscr{E}$, there is an isomorphism between E_1 and E_2 that commutes with the action of O_D. For our purposes we need only that each embedding ι corresponds to a unique j-inariant in characteristic zero.

[3] This is because if E has j-invariant 1728, and so has complex multiplication by $O_4 = \mathbf{Z}[i]$, then $G \longleftrightarrow iG$ is an involution of its cyclic subgroups G of order d preserving $j(\mathscr{E}/G)$, and if $G = iG$ then $\mathscr{E}/G$ inherits complex multiplication by O_4 and so has j-invariant 1728 as well. Note that the coefficient of (1728) in $T_d(1728)$ is even as well for $d > 2$ because deg T_d is even unless $d = 1$ or 2.

and $P_{4l_1l_3}$ are even. But, for any D, the degree of P_D is the class number of O_D, and $O_{l_1l_3}, O_{4l_1l_3}$ have even class numbers by genus theory.

3. The real roots of $P_D(X)$

The complex roots of $P_D(X)$ are j-invariants of elliptic curves with models $\mathbf{C}/I$ where I represents an ideal class of O_D. The complex conjugate of such a root is the j-invariant of $\mathbf{C}/I^{-1}$. The root is real if and only if it is equal to its complex conjugate, that is, if the curves $\mathbf{C}/I$ and $\mathbf{C}/I^{-1}$ are isomorphic, or equivalently I and I^{-1} are in the same ideal class. Thus the real roots of $P_D(X)$ are in one-to-one correspondence with ideal classes in the 2-torsion of the ideal class group of O_D. In particular, we know how many real roots there are from genus theory; in the case $D = l_1l_3$ or $D = 4l_1l_3$ we find that $P_D(X)$ has two real roots. To locate these roots on the real line we identify the corresponding ideal classes of O_D. Recall that the j-invariant of $\mathbf{C}/L$, where L is a lattice in $\mathbf{C}$ homothetic to $\mathbf{Z} + \mathbf{Z}\tau$ and τ has positive imaginary part, is given by the modular function

$$j(\tau) = q^{-1} + 744 + 196884q + \cdots, \qquad q = e^{2\pi i\tau}.$$

The principal ideal class of O_D is represented by $I = O_D$ itself, whence $\mathbf{C}/I$ has j-invariant

$$j(\tfrac{1}{2}(1 + i\sqrt{l_1l_3})),\ j(i\sqrt{l_1l_3})$$

for $D = l_1l_3$, $D = 4l_1l_3$ respectively. Let $r = l_1/l_3$; then the nonprincipal 2-torsion ideal class of $O_{l_1l_3}$ is represented by

$$I = \mathbf{Z}l_3 + \mathbf{Z}(l_3 + i\sqrt{l_1l_3})/2$$

and so corresponds to the real root

$$j(\tfrac{1}{2}(1 + i\sqrt{l_1/l_3})) = j(\tfrac{1}{2}(1 + i\sqrt{r}))$$

of $P_{l_1l_3}$, while the nonprincipal 2-torsion ideal class of $O_{4l_1l_3}$ is represented by

$$I = \mathbf{Z}l_3 + \mathbf{Z}(i\sqrt{l_1l_3})$$

and so yields the real root

$$j(i\sqrt{l_1/l_3}) = j(i\sqrt{r})$$

of $P_{4l_1l_3}$. Let $f^{\pm}: (0, \infty) \to \mathbf{R}$ be the functions defined by

$$f^{+}(t) = j(it),\ f^{-}(t) = j(\tfrac{1}{2}(1 + it)).$$

Then we have:

PROPOSITION 2. (a) *The real roots of* $P_{l_1l_3}$ *are* $f^{-}(\sqrt{l_1l_3})$ *and* $f^{-}(\sqrt{r})$; *the real roots of* $P_{4l_1l_3}$ *are* $f^{+}(\sqrt{l_1l_3})$ *and* $f^{+}(\sqrt{r})$. (b) *The functions* $f^{\pm}$ *are continuous and satisfy*

$$f^{\pm}(1) = 1728, \quad f^{\pm}(1/t) = f^{\pm}(t), \quad \lim_{t \to 0} f^{\pm}(t) = \lim_{t \to \infty} f^{\pm}(t) = \pm\infty;$$

$f^{+}(t)$ (*resp.* $f^{-}(t)$) *is monotone increasing* (*decreasing*) *on* $t \in (1, \infty)$, *and monotone decreasing* (*increasing*) *on* $t \in (0, 1)$.

Proof. (a) This is just a restatement of our computation of the j-invariants of lattices corresponding to 2-torsion ideal classes of $O_{l_1l_3}$ and $O_{4l_1l_3}$ in terms of the functions $f^{\pm}(t)$. (b) The continuity of the functions $f^{\pm}(t)$ and their behavior as $t \to \infty$ are clear from the q-expansion of $j(\tau)$. Their $t \leftrightarrow 1/t$ invariance follows from the $\mathrm{PSL}_2(\mathbf{Z})$ invariance of $j(\tau)$:

$$f^{+}(1/t) = j(i/t) = j(-1/it) = j(it) = f^{+}(t),$$

and likewise $f^{-}(1/t) = f^{-}(t)$ follows from

$$\tfrac{1}{2}(1 + it) = \{1 - \tfrac{1}{2}(1 + it)\}/\{1 - 2[\tfrac{1}{2}(1 + it)]\}.$$

This also gives the behavior of $f^{\pm}(t)$ as $t \to 0$ once the behavior as $t \to \infty$ has been determined. That $f^{+}(1) = j(i) = 1728$ is well known; since $(1 + i)/2 = 1/(1 - i)$, the $\mathrm{PSL}_2(\mathbf{Z})$ invariance of $j(\tau)$ also gives $f^{-}(1) = j((1 + i)/2) = 1728$. Finally, to show that $f^{\pm}(t)$ are monotonic on $t \in (1, \infty)$ we need only recall that the only value that $j(\tau)$ takes with even multiplicity is 1728, and that only at values of τ in the orbit of i under the action of $\mathrm{PSL}_2(\mathbf{Z})$ on the upper half-plane; since there are no such τ of the form it or $(1 + it)/2$ for $t > 1$, then, $\mathrm{d}f^{\pm}(t)/\mathrm{d}t$ cannot change sign for $t > 1$, and the proposition is proved.

We can now determine the sign of $P_{l_1l_3}(x)$ and $P_{4l_1l_3}$ for real values of x:

COROLLARY. *For* x *real,* $P_{l_1l_3}(x) < 0$ *if and only if* $f^{-}(\sqrt{r}) > x > f^{-}(\sqrt{l_1l_3})$, *and* $P_{4l_1l_3}(x) < 0$ *if and only if* $f^{+}(\sqrt{r}) < x < f^{+}(\sqrt{l_1l_3})$.

Proof. Clearly a real monic polynomial with exactly two real roots is negative at some real x if and only if x is strictly between these roots. Thus the Corollary follows from part (a) of Proposition 2, which gives the location of the roots, and the monotonicity statement in part (b), which gives their order.

4. Proof of the Theorem

We may assume without loss of generality that S contains all of E's primes of bad reduction. If $j_E = 1728$ then E has complex multiplication by O_4, so the Theorem becomes a trivial consequence of Deuring's criterion and of Dirichlet's Theorem for the arithmetic progression $\{4k + 3\}$. Thus we may assume that $j_E \neq 1728$. Let $j_1 < j_2 < \cdots < j_k$, then, be the real conjugates of j_E, none of which equals 1728. By part (b) of Proposition 2, we may choose $r_0 > 0$ as follows: if $j_1 < 1728$, choose r_0 such that $j_1 < f^-(r_0) < j_2$; if $j_1 > 1728$ (whence also $j_k > 1728$), choose r_0 such that $j_k > f^+(r_0) > j_{k-1}$. (If $k = 1$, these conditions become simply $f^-(r_0) > j_1, f^+(r_0) < j_1$ respectively). Then, for large enough l_1 and l_3 such that $r = l_1/l_3$ is sufficiently close to r_0, it follows from the Corollary to Proposition 2 that the polynomial $P_D(X)$ (where $D = l_1 l_3$ in the former case and $D = 4l_1 l_3$ in the latter) assumes positive values at all but one of the real conjugates of j_E. Thus $\mathbf{N}_{\mathbf{Q}}^K P_D(j_E) \leqslant 0$; indeed $\mathbf{N}_{\mathbf{Q}}^K P_D(j_E)$ is the product of the values of $P_D(X)$ at all conjugates of j_E, to which each pair of complex conjugates and all but one real conjugate contributes a nonnegative real factor, and that remaining real conjugate contributes a negative factor.

We now want to select l_1 and l_3 as above such that $\chi_{l_1 l_3}(q) = +1$ for each $q \in \mathbf{N}_{\mathbf{Q}}^K(S)$. These congruences conditions are compatible, despite the additional conditions on the residue class of l_1 and l_3 mod 4, because all the q's are positive. To ensure that the ratio $r = l_1/l_3$ can be made sufficiently close to r_0, we need only recall that in any arithmetic progression $\{a + md\}_{m=1}^{\infty}$ with $(a, d) = 1$ and for any $\theta > 1$ there exists $L_0 = L_0(a, d, \theta)$ such that for any $L > L_0$ the arithmetic progression contains a prime between L and θL.

REMARK. This result can be obtained either from the complex-analytic proof of Dirichlet's Theorem on primes in arithmetic progressions (see for instance [1, Ch. 20, 22]), or from later "elementary" proofs; either way we are appealing to a harder theorem than Dirichlet's original result (see [6, VI] or [1, Ch. 1]), which is all that was required for the less general Theorem 2 of [3]. In effect, Dirichlet's result required only the nonvanishing of the Dirichlet L-functions at $s = 1$, while the more precise estimate invoked here amounts to their nonvanishing anywhere on the line $\{1 + it : t \in \mathbf{R}\}$.

For the corresponding $D = l_1 l_3$ or $4l_1 l_3$ we then have

LEMMA. *$N_D(j_E)$ is divisible by a prime p ramified or inert in $\mathbf{Q}(\sqrt{-D})$.*

Proof. It suffices to show that $\chi_{l_1 l_3}(N_D(j_E)) \neq +1$. But $N_D(j_E)$ is the absolute value of the numerator of $\mathbf{N}_{\mathbf{Q}}^K P_D(j_E)$, a negative rational number which is a square modulo l_1 and l_3 (by the Corollary to Proposition 1) and whose denominator is a perfect square (because $P_D(X)$ is a monic polynomial of even degree). Since $\chi_{l_1 l_3}(-1) = -1$, then, $\chi_{l_1 l_3}(N_D(j_E))$ must be either -1 or 0, and the Lemma is thus proved.

Thus p lies under a prime π of K at which $P_D(j_E)$ has a positive valuation, so E_π has complex multiplication by $O_{l_1 l_3}$ or $O_{4l_1 l_3}$, and is therefore supersingular by Deuring's criterion. Furthermore, $\pi \notin S$ because $p \notin \mathrm{N}_{\mathbf{Q}}^{K}(S)$ by construction. It follows that π is a new supersingular prime of E. Q.E.D.

Acknowledgements

This paper is a version of Chapter 2 of my doctoral dissertation, and thus owes much to my thesis advisor Barry Mazur, who first suggested that I try to extend the results of [3] to arbitrary number fields, and helped to considerably improve the clarity of both content and form of the exposition. Benedict Gross supplied much of the present proof of the crucial Proposition 1. The referee suggested important revisions in the first draft of this paper. The dissertation was based upon work supported under a National Science Foundation Graduate Fellowship. I gratefully acknowledge also the current support of the Harvard Society of Fellows.

References

[1] H. Davenport, *Multiplicative Number Theory*, 2nd ed. New York-Heidelberg-Berlin: Springer-Verlag 1980.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* 14, (1941) 197–272.

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

[4] B.H. Gross and D. Zagier, On singular moduli. *J. Reine Angew. Math.* 335, (1985) 191–220.

[5] S. Lang and H. Trotter, Frobenius distributions in GL_2-extensions. *Lect. Notes in Math.*, vol. 504. Berlin-Heidelberg-New York: Springer 1976.

[6] J.-P. Serre, A Course in Arithmetic. New York-Heidelberg-Berlin: Springer-Verlag 1973.