Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Journal of Number Theory 113 (2005) 208–225
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Supersingular primes for points on $X_0(p)/w_p$

David Jao

Microsoft Research, 1 Microsoft Way, Redmond, WA 98052, USA

Received 10 May 2004
Available online 2 December 2004
Communicated by B. Poonen

Abstract

For small odd primes p, we prove that most of the rational points on the modular curve $X_0(p)/w_p$ parametrize pairs of elliptic curves having infinitely many supersingular primes. This result extends the class of elliptic curves for which the infinitude of supersingular primes is known. We give concrete examples illustrating how these techniques can be explicitly used to construct supersingular primes for such elliptic curves. Finally, we discuss generalizations to points defined over larger number fields and indicate the types of obstructions that arise for higher level modular curves.

MSC: 11G05

Keywords: Supersingular primes; Modular curves; Elliptic curves; Atkin–Lehner involutions

1. Introduction

Let E be an elliptic curve defined over a number field. It is conjectured that E has infinitely many prime ideals of supersingular reduction. For curves E with complex multiplication, a classical result of Deuring [4] states that the supersingular primes have density 1/2. More recently, Elkies proved that E always has infinitely many supersingular primes whenever it is defined over a real number field [6], or when the absolute norm of $j(E) - 1728$ has a prime factor congruent to $1 \bmod 4$ and occurring

E-mail address: davidjao@microsoft.com

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2004.09.002

with odd exponent [5]. In this article we prove that the number of supersingular primes is infinite for certain elliptic curves which do not satisfy any of the above conditions, thereby providing the first new examples of such curves since the work of Elkies.

Specifically, for p prime, let w_p be the unique Atkin–Lehner involution [1] on the modular curve $X_0(p)$, and write $X_0^*(p)$ for the quotient curve $X_0(p)/w_p$. Then $X_0^*(p)$ is a moduli space parameterizing unordered pairs of elliptic curves $\{E, E'\}$ together with a cyclic p-isogeny $\phi: E \to E'$. The main result of this paper is the following:

Theorem 1.1. *Suppose p is equal to* 3, 5, 7, 11, 13, *or* 19. *Let $\{E, E'\}$ be a pair of elliptic curves parametrized by a rational point on the moduli space $X_0^*(p)$, and suppose E does not have supersingular reduction mod p. Then E has infinitely many supersingular primes.*

For pairs E, E' whose j-invariants are imaginary quadratic conjugates, the theorem provides new examples of ordinary elliptic curves with infinitely many supersingular primes. In Section 2, we introduce the Heegner point analogues of Hilbert class polynomials that enable the proof of Theorem 1.1. Section 3 analyzes the real roots of these polynomials, and Section 4 gives the proof of the theorem. Section 5 explains the precise relationship between the curves E of Theorem 1.1 and the curves of [5,6].

2. Class polynomial calculations

Fix an odd prime p such that $X_0^*(p)$ has genus 0. In this section we do not impose any other conditions on p. Therefore p is one of 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, or 71. Under these conditions, we will construct a sequence of polynomials for $X_0^*(p)$ which are analogues to the Hilbert class polynomials for $X(1)$. Instead of using CM points on $X(1)$ we will use Heegner points on $X_0^*(p)$. We then describe how our variant class polynomials factor into near perfect squares modulo primes $\ell \neq p$ and later modulo $\ell = p$. We also classify all of the real roots of these polynomials. Taken together, these properties of the class polynomials can be used to construct supersingular primes for points on $X_0^*(p)$. For $\ell = p$, our square factorization results only hold for small values of p, which explains why Theorem 1.1 is restricted to these values.

The case $p = 2$ is omitted because its Heegner points exhibit very different behavior from the odd case. A discussion of this case can be found in [9].

For negative integers $D \equiv 0$ or $1 \bmod 4$, write $\mathcal{O}_D$ for the unique imaginary quadratic order of discriminant D. We assume throughout this chapter that D is of the form $-p\ell$ or $-4p\ell$ for some prime $\ell \neq p$. For either choice of D, we denote by $\mathfrak{p}$ the ideal of $\mathcal{O}_D$ generated by p and $\sqrt{D}$.

Lemma 2.1. *Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_D$. There is exactly one p-torsion subgroup of E which is annihilated by the ideal $\mathfrak{p} \subset \mathcal{O}_D$.*

Proof. An elliptic curve E with CM by $\mathcal{O}_D$ corresponds to a quotient of the complex plane $\mathbb{C}$ by a lattice L which is homothetic to an ideal class in $\mathcal{O}_D$. By scaling L

appropriately, we may assume $L = \langle 1, \tau \rangle$ where $\tau = \frac{-b+\sqrt{b^2-4ac}}{2a}$ is in the upper half plane $\mathbf{H}$, with $b^2 - 4ac = D$.

The p-torsion subgroups of E are generated in $\mathbb{C}/L$ by $1/p$, τ/p, $(\tau+1)/p, \ldots,$ $(\tau+(p-1))/p$. For z to be annihilated by $\mathfrak{p}$ means exactly that the $\mathbb{R}$-linear combination $\sqrt{D}z = z_1 \cdot 1 + z_2 \cdot \tau$ has integer coefficients. We have the equations:

$$\sqrt{D} \cdot \frac{1}{p} = \frac{b}{p} + \frac{2a}{p}\tau, \tag{1}$$

$$\sqrt{D} \cdot \frac{\tau+k}{p} = \frac{bk-2c}{p} + \frac{2ak-b}{p}\tau \quad (k = 0, 1, 2, \ldots, p-1). \tag{2}$$

Suppose first that $p \mid a$. Then the equation $D = b^2 - 4ac$ means that $p \mid b$, so Eq. (1) shows that $1/p$ is annihilated by $\mathfrak{p}$. By Eq. (2), in order for $(\tau+k)/p$ to be annihilated by $\mathfrak{p}$ it would have to be the case that $p \mid (bk - 2c)$, but this cannot happen since $p \mid b$ and $p \nmid c$.

Conversely, if $p \nmid a$ then Eq. (1) shows that $1/p$ is not annihilated by $\mathfrak{p}$, and one easily checks using Eq. (2) that $(\tau + k)/p$ is annihilated if and only if $k \equiv b/2a \pmod{p}$. $\square$

One consequence of Lemma 2.1 is that, if $\phi\colon E \to E'$ is the unique cyclic p-isogeny whose kernel is the p-torsion subgroup of Lemma 2.1, then E' also has CM by $\mathcal{O}_D$. Indeed, the lattice L' generated by L and this p-torsion subgroup is closed under multiplication by both 1 and $\mathfrak{p}$, which additively generate all of $\mathcal{O}_D$. In the case where $D = -p\ell$ and hence $\mathcal{O}_D$ is a maximal order, it follows immediately that L' has complex multiplication by $\mathcal{O}_D$. When $D = -4p\ell$, we have to make sure that the CM ring is not an order strictly containing $\mathcal{O}_{-4p\ell}$, of which the only one is $\mathcal{O}_{-p\ell}$. But the discriminants of the endomorphism rings of two p-isogenous CM elliptic curves can only differ by a multiple of p if they differ at all [10], and we have assumed that p is odd, so the discriminants cannot differ by factors of 2.

A point on $X_0(p)$ that parameterizes isogenous curves of the same CM order is called a Heegner point [8]. We have just showed that every E with CM by $\mathcal{O}_D$ lifts to a unique Heegner point on $X_0(p)$.

Definition 2.2. For any elliptic curve E with *CM* by $\mathcal{O}_D$, let $\tilde{E}$ denote the Heegner point on $X_0(p)$ corresponding to the isogeny $E \to E'$ whose kernel is the p-torsion subgroup of Lemma 2.1.

Let j_p denote a Hauptmodul on $X_0^*(p)$, i.e., a rational coordinate function on $X_0^*(p)$ with a simple pole of residue 1 at ∞. Such a function exists since the curve $X_0^*(p)$ always has a rational cusp and we are assuming its genus is 0.

Proposition 2.3. *For each ideal $\mathfrak{a}$ of $\mathcal{O}_D$, let $E_{\mathfrak{a}}$ denote the elliptic curve corresponding to $\mathbb{C}/\mathfrak{a}$. For $|D|$ sufficiently large, the minimal polynomial of $j_p(\tilde{E}_{\mathfrak{p}})$ over $\mathbb{Q}$*

is given by

$$P_D(X) := \left(\prod_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)} (X - j_p(\tilde{E}_{\mathfrak{a}})) \right)^{1/2},$$

where the product is taken over all ideal classes of $\mathcal{O}_D$.

Proof. First, note that $(X - j_p(\tilde{E}_{\mathfrak{p}}))$ is one of the factors in the product. To get the other factors, start from the known formula

$$H_D(X) := \prod_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)} (X - j(E_{\mathfrak{a}}))$$

for the Hilbert class polynomial $H_D(X)$, which by Cox [3] is the minimal polynomial of the j-invariant of $E_{\mathfrak{p}}$. Let G be the absolute Galois group of $\mathbb{Q}$. For every $\sigma \in G$, we have $\sigma(j(E_{\mathfrak{p}})) = j(E_{\mathfrak{a}})$ for some ideal class $\mathfrak{a}$ of $\mathcal{O}_D$ appearing in the above product. We claim that $\sigma(j_p(\tilde{E}_{\mathfrak{p}})) = j_p(\tilde{E}_{\mathfrak{a}})$ as well, or equivalently, the map $\sigma\colon E_{\mathfrak{p}} \to E_{\mathfrak{a}}$ sends the distinguished p-torsion subgroup of $E_{\mathfrak{p}}$ from Lemma 2.1 to that of $E_{\mathfrak{a}}$. But σ sends the endomorphism ring of $E_{\mathfrak{p}}$ into the endomorphism ring of $E_{\mathfrak{a}}$, and in both cases there are only two conjugate embeddings of $\mathcal{O}_D$ into the endomorphism ring of the elliptic curve, with either choice resulting in the same action of $\mathfrak{p}$ and hence in the same distinguished p-torsion subgroup.

From this claim we see that the set of Galois conjugates of $j_p(\tilde{E}_{\mathfrak{p}})$ is exactly $\{j_p(\tilde{E}_{\mathfrak{a}}) \mid \mathfrak{a} \subset \mathcal{O}_D\}$, and so the minimal polynomial contains all the factors in the product.

We now prove that each linear factor in the product occurs with multiplicity two. For any ideal class $[\mathfrak{a}]$, the Atkin–Lehner image of $\tilde{E}_{\mathfrak{a}}$ is $\tilde{E}_{\mathfrak{a}'}$ for some other ideal class $[\mathfrak{a}'] \in \mathrm{Cl}(\mathcal{O}_D)$ (by the remarks following Lemma 2.1). The ideal classes $[\mathfrak{a}]$ and $[\mathfrak{a}']$ are not identical since the 2-1 covering map $\pi\colon X_0(p) \to X_0^*(p)$ has only finitely many branch points, and we can avoid these branch points by choosing $|D|$ sufficiently large. Hence $j_p(\tilde{E}_{\mathfrak{a}}) = j_p(\tilde{E}_{\mathfrak{a}'})$, and since π is 2 to 1, these are the only equalities among the roots of the factors in the product. □

From now on, we will assume that $|D|$ is large enough to satisfy the hypothesis of Proposition 2.3.

Lemma 2.4. *Let* $\mathfrak{P}$ *be a prime of the splitting field* K *of* $P_D(X)$ *lying over* ℓ, *with residue field* k. *Let* $\mathcal{E}$ *be an elliptic curve defined over* k, *and fix an embedding* $\mathcal{O}_D \hookrightarrow \mathrm{End}(\mathcal{E})$. *Then there is exactly one* p-*torsion subgroup of* $\mathcal{E}$ *which is annihilated by* $\mathfrak{p} \subset \mathcal{O}_D$.

Proof. By Deuring's lifting lemma [4], there is exactly one lifting of $\mathcal{E}$ to an elliptic curve E over K with CM by $\mathcal{O}_D$ such that reduction mod $\mathfrak{P}$ induces the embedding $\mathcal{O}_D \hookrightarrow \mathrm{End}(\mathcal{E})$. The p-torsion lattices of E and $\mathcal{E}$ are isomorphic via reduction [14], so the unique p-torsion subgroup of E from Lemma 2.1 descends to a unique p-torsion subgroup on $\mathcal{E}$. □

As in Definition 2.2, we denote by $\tilde{\mathcal{E}}$ the point on $X_0(p) \bmod \mathfrak{P}$ corresponding to the elliptic curve $\mathcal{E}$ together with the cyclic p-isogeny whose kernel is the subgroup determined by Lemma 2.4.

Proposition 2.5. *Suppose the odd prime ℓ splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$ (equivalently, $-p$ is a quadratic residue modulo ℓ). Then, modulo ℓ, all roots of the polynomial $P_D(X)$ occur with even multiplicity, except possibly those corresponding to elliptic curves with $j \equiv 1728 \bmod \ell$ when $D = -p\ell$, or elliptic curves which are 2-isogenous to those curves when $D = -4p\ell$.*

Proof. Assume first that D is a fundamental discriminant. We show that the points $\tilde{E}$ corresponding to roots away from $j(E) = 1728$ occur naturally in pairs modulo ℓ. We begin with the following facts from [6] concerning the Hilbert class polynomial $H_D(X)$ defined in the proof of Proposition 2.3. Each root of $H_D(X)$ corresponds to an isomorphism class of elliptic curves E with complex multiplication by $\mathcal{O}_D$. The reduction of this root modulo ℓ corresponds to a reduction of E to a supersingular elliptic curve $\mathcal{E}$ in characteristic ℓ, or equivalently an embedding $\iota\colon \mathcal{O}_D \hookrightarrow \mathrm{End}(\mathcal{E})$. Since ℓ ramifies in $\mathcal{O}_D$, the conjugate $\bar{\iota}$ of ι is again an embedding of $\mathcal{O}_D$ into $\mathrm{End}(\mathcal{E})$, and $\mathcal{E}$ lifts by way of $\bar{\iota}$ to an elliptic curve E' in characteristic zero, which is not isomorphic to E provided that $j(E) \not\equiv 1728 \pmod{\ell}$.

In order to show that the root $j_p(\tilde{\mathcal{E}})$ occurs twice in $P_D(X)$ modulo ℓ, we must show that the two curves E and E' from the previous paragraph correspond to two different roots of $P_D(X)$ in characteristic zero, and that they both reduce to $\tilde{\mathcal{E}}$ modulo ℓ. To prove the second fact, observe that the embeddings ι and $\bar{\iota}$ both determine the same p-torsion subgroup of $\mathcal{E}$ under Lemma 2.4, since $\mathfrak{p}$ equals itself under conjugation, so $\tilde{E}$ and $\tilde{E}'$ both reduce to $\tilde{\mathcal{E}}$. As for the first fact, we have $E \neq E'$ provided that $j(E) \not\equiv 1728 \bmod \ell$, so $\tilde{E} \neq \tilde{E}'$. The only other way E and E' could be equal on $X_0^*(p)$ is if $w_p(\tilde{E}) = \tilde{E}'$. But if these two were equal, then in particular their reductions mod ℓ would be equal, so $w_p(\tilde{\mathcal{E}}) = \tilde{\mathcal{E}}'$. On the other hand, we have just showed that $\tilde{\mathcal{E}} = \tilde{\mathcal{E}}'$. Putting the two equations together yields $w_p(\tilde{\mathcal{E}}) = \tilde{\mathcal{E}}$. We show that this cannot happen.

Let $\phi\colon \mathcal{E} \to \mathcal{E}'$ be the cyclic p-isogeny corresponding to $\tilde{\mathcal{E}}$. The equation $w_p(\tilde{\mathcal{E}}) = \tilde{\mathcal{E}}$ implies that the dual isogeny $\hat{\phi}$ of ϕ is isomorphic to ϕ, or that there exist isomorphisms $\psi_1\colon \mathcal{E} \to \mathcal{E}'$ and $\psi_2\colon \mathcal{E}' \to \mathcal{E}$ making the diagram

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\phi} & \mathcal{E}' \\ {\scriptstyle\psi_1}\downarrow & & \downarrow{\scriptstyle\psi_2} \\ \mathcal{E}' & \xrightarrow{\hat{\phi}} & \mathcal{E} \end{array}$$

commute. Since p is prime, the equation $\hat{\phi}\phi = [p]$ at once implies that $\psi_2\phi$ is not equal to multiplication by any integer, which in turn means that $\psi_2\phi$ algebraically generates an imaginary quadratic order $\mathcal{O}$ inside $\mathrm{End}(\mathcal{E})$. But we also have $(\psi_2\phi)^2 = u[p]$ for some $u \in \operatorname{Aut}(\mathcal{E})$ (specifically, $u = \psi_2\psi_1$), from which we conclude that $\mathcal{O}$ contains a square root of $-p$, and thus that $\mathcal{E}$ has CM by either $\mathcal{O}_{-p}$ or $\mathcal{O}_{-4p}$. Moreover, since ℓ splits in these orders by hypothesis, the curve $\mathcal{E}$ must have ordinary reduction mod ℓ. On the other hand, by Deuring [4] every root of $H_D(X) \bmod \ell$ (and hence every root of $P_D(X) \bmod \ell$) corresponds to an elliptic curve of supersingular reduction mod ℓ, which provides our contradiction.

For the non-fundamental discriminant $D = -4p\ell$, set $D' := -p\ell$ for convenience. Let ε be 0, 1, or 2 according as 2 is inert, ramified or split in $\mathcal{O}_{D'}$. Then the divisor of zeros $(P_D)_0$ of P_D in characteristic ℓ or 0 is equal to the Hecke correspondence T_2 on $X_0^*(p)$ applied to the divisor of zeros $(P_{D'})_0$ of $P_{D'}$, minus ε times the divisor $(P_{D'})_0$. That is,

$$(P_D)_0 = T_2((P_{D'})_0) - \varepsilon(P_{D'})_0. \tag{3}$$

Every zero of $P_{D'}$, except for the divisors with j-values of 1728, appears in $(P_{D'})_0$ with even coefficient in characteristic ℓ, and hence also appears in $(P_D)_0$ with even coefficient by (3). The only divisors unaccounted for are those with j-values of 1728, and the images of such divisors under T_2, so the Proposition is proved. $\square$

3. Real roots of $P_D(X)$

We find the real roots of the class polynomial $P_D(X)$. A real root of $P_D(X)$ corresponds to an unordered pair $\{E, E'\}$ of cyclic p-isogenous elliptic curves which is fixed under complex conjugation. Choose an ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_D)$ representing E; then $[\mathfrak{a}\mathfrak{p}]$ represents E'. For $\{E, E'\}$ to be fixed under complex conjugation means that

$$\{[\mathfrak{a}], [\mathfrak{a}\mathfrak{p}]\} = \{[\overline{\mathfrak{a}}], [\overline{\mathfrak{a}\mathfrak{p}}]\},$$

where the bar denotes complex conjugation. This can happen in two ways: either $[\mathfrak{a}] = [\overline{\mathfrak{a}}]$, or $[\mathfrak{a}\mathfrak{p}] = [\overline{\mathfrak{a}}]$.

Definition 3.1. With notation as above, a real root of $P_D(X)$ is said to be *unbounded* if $[\mathfrak{a}] = [\overline{\mathfrak{a}}]$, and *bounded* if $[\mathfrak{a}\mathfrak{p}] = [\overline{\mathfrak{a}}]$.

For the primes $p \equiv 1 \bmod 4$, the behavior of the real roots of $P_D(X)$ closely resembles the case of $H_D(X)$ which was treated in [5]. This is not surprising if one observes that $X(1) = X_0(1)$ is a degenerate case of $X_0(p)$ where $p \equiv 1 \bmod 4$. However, when $p \equiv 3 \bmod 4$, the real roots of $P_D(X)$ exhibit very different behavior. It is therefore necessary to treat the two cases separately.

3.1. *The case* $p \equiv 1 \bmod 4$

In this section, we assume that $p \equiv 1 \pmod 4$ and that D is equal to $-p\ell$ or $-4p\ell$, where ℓ is chosen to be a prime congruent to $3 \bmod 4$ which splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$.

An unbounded real root of $P_D(X)$ corresponds to an isogeny $E \to E'$ which is isomorphic to itself under complex conjugation, meaning that $\tilde{E}$ is a real point on

$X_0(p)$. Since the covering $X_0(p) \to X(1)$ is defined over $\mathbb{Q}$, each such real point $\tilde{E}$ has $j(E)$ real, so we can count these points by counting the ideal classes $[\mathfrak{a}]$ for which $j(\mathfrak{a})$ is real. By genus theory [3], there are two such ideal classes for $\mathcal{O}_{-p\ell}$ and two for $\mathcal{O}_{-4p\ell}$, corresponding to the quadratic forms

$$x^2 + xy + \left(\frac{p\ell + 1}{4}\right) y^2,$$

$$px^2 + pxy + \left(\frac{p + \ell}{4}\right) y^2$$

for $D = -p\ell$, and

$$x^2 + p\ell y^2,$$

$$px^2 + \ell y^2$$

for $D = -4p\ell$.

Since the first two forms above are Atkin–Lehner images of each other, and the last two are Atkin–Lehner images of each other, the first pair of real points on $X_0(p)$, upon quotienting by w_p, yields one real root of $P_{-p\ell}(X)$, and the second pair yields a real root for $P_{-4p\ell}(X)$. For $D = -p\ell$, the quadratic form $x^2 + xy + \left(\frac{p\ell+1}{4}\right) y^2$ has the root $\tau = (-1 + \sqrt{-p\ell})/2$ in the upper half plane, and

$$\lim_{\ell \to \infty} j_p \left(\frac{-1 + \sqrt{-p\ell}}{2}\right) = -\infty.$$

Similarly, for $D = -4p\ell$, the quadratic form $x^2 + p\ell y^2$ has the root $\tau = \sqrt{-p\ell}$ with $\lim_{\ell \to \infty} j_p(\tau) = \infty$. The divergence of the roots $j_p(\tau)$ of $P_D(X)$, as $\ell \to \infty$, justifies the terminology "unbounded."

A bounded real root of $P_D(X)$ occurs when $[\mathfrak{a}\mathfrak{p}] = [\overline{\mathfrak{a}}]$, or equivalently $[\mathfrak{p}] = [\overline{\mathfrak{a}}]^2$. Viewing each ideal class as a quadratic form, a bounded root exists if and only if the quadratic form $px^2 + \ell y^2$ (for $D = -4p\ell$) or $px^2 + pxy + \frac{p+\ell}{4} y^2$ (for $D = -p\ell$) is equal to the direct composition of some quadratic form $ax^2 + bxy + cy^2$ with itself. In particular, this implies by definition of composition that there exists a nonzero integer z satisfying the Diophantine equation $px^2 + \ell y^2 = z^2$ in the $D = -4p\ell$ case, or $px^2 + pxy + \frac{p+\ell}{4} y^2 = z^2$ in the $D = -p\ell$ case. We show that this cannot happen in our situation.

Lemma 3.2. *The Diophantine equations $px^2 + \ell y^2 = z^2$ and $px^2 + pxy + \frac{p+\ell}{4} y^2 = z^2$ have no nonzero solutions $x, y, z \in \mathbb{Z}$.*

Proof. Suppose there were a nonzero solution. We may assume $y \not\equiv 0 \pmod{p}$, or else descent yields a contradiction. Then reducing the equations modulo p, we get that ℓ is a perfect square mod p, which contradicts the assumptions that $\ell \equiv 3 \bmod 4$ and that ℓ splits in $\mathcal{O}_{-p}$. $\square$

We conclude that the polynomial $P_D(X)$ has one unbounded real root and no bounded real roots, with the bounded real root diverging to ∞ for $D = -4p\ell$ and $-\infty$ for $D = -p\ell$, as $\ell \to \infty$.

3.2. The case $p \equiv 3 \bmod 4$

We assume that $p \equiv 3 \pmod 4$ and that $D = -4p\ell$, where $\ell \equiv 1 \bmod 4$ and ℓ splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$. Using genus theory as before, the unbounded real root of $P_D(X)$ is represented by the pair of ideals corresponding to the two w_p-equivalent quadratic forms

$$x^2 + p\ell y^2,$$
$$px^2 + \ell y^2.$$

Hence the polynomial $P_D(X)$ has one unbounded real root, which approaches ∞ as ℓ becomes large.

A bounded real root corresponds to an equivalence class of quadratic forms $ax^2 + bxy + cy^2$ whose square in the form class group is equal to the form $px^2 + \ell y^2$. There is at most one such form class, because a second one would result in more 2-torsion classes in the ideal class group of $\mathcal{O}_D$ than were found in the preceding analysis of the unbounded roots.

To show the existence of such a quadratic form, it suffices to construct a quadratic form $pax^2 + bxy + ay^2$ of discriminant D with p dividing b. Indeed, the Dirichlet composition [3] of $pax^2+bxy+ay^2$ with itself is $a^2x^2+bxy+py^2$, which is properly equivalent to $px^2 + \ell y^2$ since $p \mid b$ and the discriminants of the two forms match.

To find such a quadratic form, choose integers A and B such that $\ell = A^2 - pB^2 = (A + B\sqrt{p})(A - B\sqrt{p})$. Such integers exist because ℓ splits in $\mathbb{Q}(\sqrt{p})$, and all such representations of ℓ differ by a factor of $\pm\varepsilon^n$ where $\varepsilon := c + d\sqrt{p}$ is the fundamental unit of $\mathbb{Q}(\sqrt{p})$. Note that c and d are integers, since $p \equiv 3 \bmod 4$, and that c is even and d is odd. Accordingly, multiplication by ε changes the parity of A, so there exist representations with A even and with A odd. Choose A to be odd, and set $a = A$, $b = 2pB$ to obtain a quadratic form $pax^2 + bxy + ay^2$ of discriminant $-4p\ell$.

We now find the minimal possible value for B (equivalently, the minimal possible b), subject to the constraint that A is odd. This value for B is determined by the requirement that multiplication by ε^2 must increase the size of the coefficients of the factor $A - B\sqrt{p}$. We compute these coefficients to be:

$$(A - B\sqrt{p})(c + d\sqrt{p})^2 = (Ac^2 - 2Bcdp + Ad^2p) + (2Acd - Bc^2 - Bd^2p)\sqrt{p}.$$

The requirement is thus $B < (2Acd - Bc^2 - Bd^2p)$, or

$$\frac{B}{A} < \frac{2cd}{c^2 + d^2p + 1} = \frac{d}{c} \cdot \frac{2c^2}{c^2 + d^2p + 1}.$$

But $d^2p = c^2-1$, so the fraction $(2c^2)/(c^2+d^2p+1)$ equals 1, whence our condition on B is just $B/A < d/c$. One could have done the same computation using the inequality on A given by the other coefficient; the reader can verify that doing so produces the same inequality.

Now, if b is chosen to be minimal and of the above form (i.e., $cB < dA$, or equivalently $cb < 2pda$, and A is odd), then the root $\tau = \frac{-b+\sqrt{D}}{2pa}$ of the quadratic form $pax^2 + bxy + ay^2$ lying in the upper half plane has absolute value $1/\sqrt{p}$ and real part between $-d/c$ and 0 (since $-d/c < -B/A < 0$). Denote the set of all such complex numbers in the upper half plane by S. Since all of the points on the circular arc S are distinct in $X_0^*(p)$, the function $j_p(z)$ is monotonic (and, of course, real valued) in the clockwise direction along this circular arc. From q-expansions we see that $j_p(z)$ is in fact increasing clockwise along the arc S. We claim that, for random large values of ℓ, the locations of the corresponding roots τ (as a function of ℓ) are uniformly distributed along the arc S in a weak sense to be made precise in Lemma 3.3. It follows that the bounded real root of the polynomial $P_D(X)$ is uniformly distributed along the real interval $j_p(S)$ as D varies.

Lemma 3.3. *Let $\mathcal{A}$ be an arithmetic progression containing infinitely many primes ℓ which are congruent to* $3 \bmod 4$ *and split in* $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$. *For any sub-arc $T \subset S$ of nonzero length, there exist infinitely many primes $\ell \in \mathcal{A}$ whose corresponding roots τ above lie in T.*

Proof. Let U be the projection of T to the real axis. Using the fact that $\mathrm{Re}(\tau) = -B/A$, we see that it suffices to show that $-B/A \in U$ for infinitely many primes $\ell \in \mathcal{A}$. Consider the function

$$\sigma(\mathfrak{a}) := \left(\frac{N(\mathfrak{a})}{N(\overline{\mathfrak{a}})}\right)^{\frac{2\pi i}{\log(\varepsilon/\overline{\varepsilon})}}$$

mapping ideals $\mathfrak{a}$ of $\mathcal{O}_p$ into complex numbers of norm 1. Let $\sigma(A, B)$ denote the value of σ on the principal ideal $(A + B\sqrt{p})$ in $\mathcal{O}_p$. Then $\sigma(A, B)$ is purely a function of B/A, and as B/A increases from 0 to d/c with B positive, the point $\sigma(A, B) \in S^1$ increases monotonically in angle from 0 to 2π. Thus it is enough to show that $\sigma(A, B)$ is equidistributed on S^1 where A, B vary as a function of $\ell \in \mathcal{A}$, with $\ell = A^2 - pB^2$. But the equidistribution of values of σ with respect to ℓ has already been proven in [11, p. 318]. $\square$

In summary, for $p \equiv 3 \bmod 4$ and $D = -4p\ell$, where $\ell \equiv 1 \bmod 4$ and ℓ splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$, the polynomial $P_D(X)$ has exactly two real roots, with the unbounded real root diverging to ∞ as ℓ increases and the bounded real root being uniformly distributed in the real interval $j_p(S)$ as the prime ℓ is varied.

4. Proof of the main theorem

4.1. Specification of Hauptmoduls

For the sake of concreteness, we will use the following Hauptmoduls for the curves $X_0^*(p)$, $p = 3, 5, 7, 11, 13, 19$. The derivation of these Hauptmoduls is discussed in [7].

For $p = 3, 5, 7, 13$, the modular curve $X_0(p)$ is a rational curve with coordinate

$$j_{p,0}(z) := \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}, \tag{4}$$

where η is the Dedekind eta function. The action of the Atkin–Lehner involution w_p is given by

$$w_p(j_{p,0}(z)) = \frac{p^{\frac{12}{p-1}}}{j_{p,0}(z)}. \tag{5}$$

For these primes, we use the Hauptmodul j_p for $X_0^*(p)$ defined by the formula

$$j_p(z) := j_{p,0}(z) + w_p(j_{p,0}(z)). \tag{6}$$

For $p = 11$ we use the Hauptmodul

$$j_{11}(z) := \left(\frac{\theta_{1,1,3}(z)}{\eta(z)\eta(11z)}\right)^2,$$

where $\theta_{a,b,c}(z)$ is defined to be the theta function

$$\theta_{a,b,c}(z) := \sum_{x,y\in\mathbb{Z}} q^{ax^2+bxy+cy^2}, \quad q := e^{2\pi i z},$$

valid for all z in the upper half plane $\mathbf{H}$.

For $p = 19$, we use the function

$$j_{19}(z) := \left(\frac{\theta_{1,1,5}(z)}{\theta^*_{1,1,5}(z)}\right)^2,$$

where now $\theta^*_{1,1,5}(z)$ is defined by

$$\theta^*_{1,1,5}(z) := \sum_{m+n\equiv 1(2)} (-1)^m q^{\frac{1}{2}(m^2+mn+5n^2)}, \quad q := e^{2\pi i z}.$$

4.2. Proof of the theorem for $p \equiv 3 \bmod 4$

We assume that p is equal to 3, 7, 11, or 19. As before, we will use the polynomials $P_D(X)$, $D = -p\ell$ or $D = -4p\ell$, where the prime ℓ is both $1 \bmod 4$ and a quadratic residue mod p. Note that $P_D(X)$ is monic (since its roots $j_p(\tilde{E})$ are algebraic integers) and each such curve E is supersingular mod p and mod ℓ (since p and ℓ ramify in D).

Proposition 4.1. *The polynomial $P_D(X)$ is a square modulo ℓ.*

Proof. By Proposition 2.5, we only have to exclude the possibility of there being roots associated to the j-invariant 1728. First consider the case $D = -p\ell$. Suppose $j_p(\tilde{E})$ were a root of $P_D(X)$, with $j(E) \equiv 1728 \bmod \ell$. Then E would be supersingular mod ℓ

and have complex multiplication by $\mathcal{O}_{-4}$. But ℓ splits in $\mathcal{O}_{-4}$, so a curve with CM by $\mathcal{O}_{-4}$ cannot be supersingular mod ℓ.

Now take $D = -4p\ell$. As in the proof of Proposition 2.5, set $D' := -p\ell$. Then, since all coefficients in the divisor of zeros $(P_{D'})_0$ are even in characteristic ℓ, the proof of Proposition 2.5 shows that every coefficient of $(P_D)_0$ is even as well. $\square$

Lemma 4.2. *For $D = -4p\ell$, the polynomial $P_D(X)$ is a square modulo p.*

Proof. Suppose first that $p = 3$ or 7. Every root of $P_D(X)$ is of the form $j_p(\tilde{E})$ where E is a supersingular elliptic curve mod p. But there is only one isomorphism class of supersingular elliptic curves mod p. It follows that $P_D(X)$ has divisor of zeros equal to $\deg(P_D) \cdot (j_p(\tilde{E}))$. Since $P_D(X) \bmod p$ is monic, has even degree, and has only one root of maximal multiplicity, it must be a perfect square.

Now suppose $p = 11$. Write $D' = -p\ell$ as before. Here there are two isomorphism classes of supersingular elliptic curves mod p, having the values 0 and -1 under the coordinate function j_{11} of Section 4.1. Using the algorithm of Pizer [13], we find that the action of the Hecke correspondence T_2, as given by the Brandt matrix $B(2)$, is represented by

$$T_2((0)) = 1 \cdot (0) + 2 \cdot (-1),$$

$$T_2((-1)) = 3 \cdot (0) + 0 \cdot (-1).$$

Since the roots of the polynomial $P_{D'}(X)$ are supersingular, the polynomial $P_{D'}(X)$ has the form $X^m(X+1)^n \bmod 11$ for some integers m and n. The above calculation of T_2, combined with Eq. (3), yields

$$P_D(X) \equiv X^{m+3n-\varepsilon m}(X+1)^{2m-\varepsilon n} \bmod 11,$$

which is a perfect square since $\deg(P_{D'}) = m + n$ is even and ε is even for all primes $\ell \equiv 1 \bmod 4$ which are squares mod p.

The case $p = 19$ is similar: using the Hauptmodul j_{19} of Section 4.1, the Hecke correspondence mod 19 has matrix $\left[\begin{smallmatrix} 1 & 2 \\ 1 & 2 \end{smallmatrix}\right]$ with respect to the basis of supersingular invariants $\{(0), (8)\}$. Since the columns of this matrix add up to even numbers, the polynomial $P_D(X)$ is always a perfect square modulo 19 for $D = -4p\ell$ and our choices of ℓ. $\square$

Theorem 4.3. *Suppose $p = 3, 7, 11,$ or 19. Let $\{E, E'\}$ be a pair of elliptic curves, defined over K, corresponding to a rational point on $X_0^*(p)$, and assume that E is not supersingular at p. Then E has infinitely many supersingular primes.*

Proof. If E is represented by the complex lattice $\langle 1, \tau \rangle$ with $\tau \in \mathbf{H}$, the fact that $h := j_p(\tau)$ is real means that we may (cf. Section 3) take τ either on the unbounded arcs corresponding to $\mathrm{Re}(\tau) = 0$ or $\mathrm{Re}(\tau) = 1/2$, or on the bounded arc $j_p(S)$ of

Lemma 3.3. In the unbounded case, $j(\tau)$ is real and K has a real embedding, so the result follows from [6] and we do not need to do it here. We can therefore assume that $\tau \in S$ and $-d/c \leqslant \mathrm{Re}(\tau) \leqslant 0$. Moreover, we can assume these inequalities are strict, since otherwise E has CM and its supersingular primes are known to have density 1/2.

Now suppose h is rational inside the interior of the interval $j_p(S)$ and the curve E is not supersingular modulo p. Given any finite set Σ of primes of K, we construct a supersingular prime π of E outside of Σ.

Without loss of generality, suppose that Σ contains all of the primes of bad reduction of E. Choose a large prime ℓ such that

(1) $\ell \equiv 1 \bmod 4$ and ℓ splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$.
(2) $\left(\frac{v}{p\ell}\right) = 1$ for every rational prime v lying under a prime in Σ, except possibly $v = p$.
(3) $P_D(h) < 0$.

Condition 3 is satisfied as long as the bounded root r of $P_D(h)$ falls to the left of h on the real line. Since h is not on the boundary of $j_p(S)$, Lemma 3.3 assures the existence of infinitely many primes ℓ satisfying all the conditions.

The rational number $P_D(h)$ is then congruent to a perfect square mod ℓ (by Proposition 4.1) and mod p (by Lemma 4.2). However, being negative, it also contains a factor of -1, which is not a perfect square mod $p\ell$. Therefore, at least one of its prime factors q satisfies the equation $\left(\frac{q}{p\ell}\right) \neq 1$ and thus is ramified or inert in $\mathbb{Q}(\sqrt{D})$. Moreover, the denominator of $P_D(h)$ is a perfect square, since $P_D(X)$ is monic with integer coefficients and even degree. Hence we may take q to be a factor of the numerator of $P_D(h)$. Furthermore, q is not equal to p, because E is not supersingular at p and so p cannot divide $P_D(h)$.

It follows from Condition 2 that q does not lie under any prime in Σ, and h is a root of $P_D(X)$ in characteristic q. Therefore $j(E)$ is a root of $H_D(X)$ in characteristic q. Hence, for any prime $\mathfrak{q}$ of K lying over q, the reduction of E at $\mathfrak{q}$ has complex multiplication by $\mathcal{O}_{D'}$ for some factor D' of D such that D/D' is a square, and since q is not split in $\mathbb{Q}(\sqrt{D})$, it follows that there is a new supersingular prime $\pi \notin \Sigma$ lying above q. $\square$

4.3. *Proof of the theorem for $p \equiv 1 \bmod 4$*

We now give a proof of Theorem 1.1 for the primes $p = 5$ and 13. Let ℓ be a prime congruent to $3 \bmod 4$ such that ℓ splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$. Explicitly, $\ell \equiv 3, 7 \pmod{20}$ for $N = 5$, and $\ell \equiv 7, 11, 15, 19, 31, 47 \pmod{52}$ for $N = 13$. Note that Proposition 2.5 applies in this case. Throughout this section we will use the Hauptmoduls j_5 and j_{13} specified in Section 4.1.

Proposition 4.4. *For $p = 5$ and $D = -p\ell$ or $D = -4p\ell$, the polynomial $P_D(X)$ is of the form $(X + 22)R(X)^2$ modulo ℓ.*

Proof. From class number considerations we know that the class polynomial $P_D(X)$ has odd degree. We show that the only factors of $P_D(X)$ lying over $j = 1728$ are equal to $(X + 22) \bmod \ell$. This will imply that our polynomial has the required form, by Proposition 2.5.

Let $E = \mathbb{C}/L$ where $L = \mathbb{Z}[i]$. Then $j(E) = 1728$ and there are six points (counting multiplicity) of $X_0(5)$ lying over E. We compute the values under $j_{5,0}$ and j_5 for each of the choices of 5-torsion subgroup of E:

Subgroup	$j_{5,0}$	j_5
$\langle 1/5\rangle$	$125+2\sqrt{5}$	$248+126\sqrt{5}$
$\langle i/5\rangle$	$125+2\sqrt{5}$	$248+126\sqrt{5}$
$\langle (i+1)/5\rangle$	$125-2\sqrt{5}$	$248-126\sqrt{5}$
$\langle (i-1)/5\rangle$	$125-2\sqrt{5}$	$248-126\sqrt{5}$
$\langle (i+2)/5\rangle$	$-11+2i$	-22
$\langle (i-2)/5\rangle$	$-11-2i$	-22

Notice that the two subgroups G of E with $j_5(E, E/G) = -22$ are characterized by the property $G = iG$ (cf. [12, Section II.2]). We will use this characterization to prove that the roots of $P_D(X)$ over 1728 must have $j_5 = -22$.

Suppose first that $D = -5\ell$ is a fundamental discriminant. Let $j_5(\tilde{E})$ be a root of $P_D(X)$ modulo ℓ with $j(E) = 1728$ modulo ℓ. Then the reduction $\mathcal{E}$ of E modulo ℓ has quaternionic endomorphism ring A containing a subring generated by $\mathbb{Z}[I, (D+\sqrt{D})/2]$, where $I^2 = -1$ and $\sqrt{D}$ in A is obtained from the embedding $\iota\colon \mathcal{O}_D \to A$ induced by the reduction map from E to $\mathcal{E}$. Now, the reduction of the ring A modulo 5 is isomorphic to $M_{2\times 2}(\mathbb{Z}/5)$, with the isomorphism being given by the action of A on the 5-torsion group $E[5] = \mathcal{E}[5]$ of E. The element $\sqrt{D}$ has square equal to $D \equiv 0 \bmod 5$, so it is nilpotent in $M_{2\times 2}(\mathbb{Z}/5)$ with kernel equal to $\ker(5, \sqrt{D}) = \ker \mathfrak{p}$. Observe that $\ker(I\sqrt{D}I^{-1}) = I \ker(\sqrt{D}) = I \ker \mathfrak{p}$; on the other hand, $\ker(I\sqrt{D}I^{-1}) = \ker(\bar{\iota}(\sqrt{D})) = \ker(\sqrt{D}) = \ker \mathfrak{p}$. Therefore the distinguished 5-torsion subgroup $G = \ker \mathfrak{p}$ of Lemma 2.4 satisfies the equality $G = iG$, as desired.

For the non-fundamental case $D = -20\ell$, note that the Hecke correspondence T_2 applied to the value $j_5(\tilde{E}) = -22$ is a formal sum of terms all with even coefficient except for -22 itself, so by the proof of Proposition 2.5, the polynomial $P_D(X)$ is a perfect square except for a linear factor of $(X + 22)$. □

Proposition 4.5. *For $p = 13$ and $D = -p\ell$ or $D = -4p\ell$, the polynomial $P_D(X)$ is of the form $(X + 6)R(X)^2$ modulo ℓ.*

Proof. Let $j(E) = 1728$. By the same proof as in Proposition 4.4, the kernel G of $\tilde{E}$ satisfies $G = iG$. There are only two 13-torsion subgroups G of $\mathbb{C}/\mathbb{Z}[i]$ that satisfy the equation $G = iG$, and they are generated, respectively, by $(2+3i)/13$ and $(3+2i)/13$. One calculates that $j_{13,0} = -3\pm 2i$ and $j_{13} = -6$ for these points, so as in Proposition 4.4 the polynomial P_D factors as $(X + 6)$ times a perfect square. □

Define $P_\ell(X)$ to be the monic polynomial $P_{-p\ell}(X) \cdot P_{-4p\ell}(X)$. Then, by Propositions 4.4 and 4.5, the polynomial $P_\ell(X)$ is a perfect square mod ℓ, and by the classification of the real roots of $P_D(X)$ in Section 3.1, the polynomial $P_\ell(X)$ has exactly two real roots which diverge to infinity in opposite directions as $\ell \to \infty$. In particular, for any fixed real number h, the value of $P_\ell(h)$ is negative for all sufficiently large ℓ.

Lemma 4.6. *For $p = 5$ or 13, the polynomial $P_\ell(X)$ is a square modulo p.*

Proof. Since the polynomial has even degree, it suffices to prove that all roots of the polynomial are congruent mod p. But every root of $P_\ell(X) \bmod p$ is of the form $j_p(\tilde{E})$ where $\tilde{E}$ is an elliptic curve whose reduction modulo p is supersingular. For either $p = 5$ or $p = 13$, there is only one isomorphism class of supersingular j-invariants mod p, so all such curves E are isomorphic mod p and they all have the same j_p value. □

Theorem 4.7. *Suppose p equals 5 or 13. Let $\{E, E'\}$ be a pair of elliptic curves, defined over a number field K, corresponding to a rational point on the curve $X_0^*(p)$. Assume that E is not supersingular at p. Then E has infinitely many supersingular primes.*

Proof. Suppose $h := j_p(\tilde{E})$ is rational and not of supersingular reduction modulo p. Given any finite set Σ of primes of K, containing all of E's primes of bad reduction, we construct a supersingular prime π of E outside of Σ. Choose a large prime ℓ satisfying the conditions:

(1) $\ell \equiv 3 \bmod 4$ and ℓ splits in $\mathcal{O}_{-p}$ and $\mathcal{O}_{-4p}$.
(2) $\left(\frac{v}{p\ell}\right) = 1$ for every rational prime v lying under a prime in Σ (except possibly $v = p$).
(3) $P_\ell(h) < 0$.

Then the numerator z of the rational number $P_\ell(h)$ is divisible by some rational prime q which is ramified or inert in $\mathbb{Q}(\sqrt{D})$ for one of $D = -p\ell$ or $D = -4p\ell$ (equivalently, has $\left(\frac{q}{p\ell}\right) \neq 1$). Indeed, if not, then the absolute values of both the numerator and the denominator of $P_\ell(h)$ would have quadratic character 1 modulo $p\ell$. But $\left(\frac{-1}{p\ell}\right) = -1$ by our choice of ℓ, so the number $P_\ell(h)$ itself would have quadratic character -1 modulo $p\ell$, contradicting the fact that $P_\ell(h)$ is a perfect square mod p and mod ℓ. Moreover, q is not equal to p, since the assumption that E is not supersingular at p implies that p does not divide $P_\ell(h)$.

It follows that q does not lie under any prime in Σ, and h is a root of $P_\ell(X)$ in characteristic q. Therefore, for one of $D = -p\ell$ or $D = -4p\ell$, the value $j(E)$ is a root of $H_D(X)$ in characteristic q. Hence, for any prime $\mathfrak{q}$ of K lying over q, the reduction $E_\mathfrak{q}$ has complex multiplication by $\mathcal{O}_{D'}$ for some factor D' of D such that D/D' is a square, and since q is not split in $\mathbb{Q}(\sqrt{D})$, it follows that there is a new supersingular prime $\pi \notin \Sigma$ lying above q. □

5. Numerical computations

5.1. Relationship to Elkies's work

In addition to proving the infinitude of supersingular primes for elliptic curves defined over real number fields in [6], Elkies notes in [5, p. 566] that his method also works for j-invariants "such that the exponent of some prime congruent to $+1 \bmod 4$ in the absolute norm of $j - 12^3$ is odd." Thus, even for the case of elliptic curves over imaginary number fields our results do not represent the first demonstration of infinitely many supersingular primes for ordinary curves. However, one can prove by direct computation that, over non-real number fields, the set of elliptic curves given in the statement of Theorem 1.1 is disjoint from the set of curves which satisfy the property stated by Elkies above. As an illustration of this fact we will perform the computation for the case of $X_0^*(3)$.

We preserve the notation from Section 4.1. We will need the equation

$$j(z) - 1728 = \frac{(j_{3,0}(z)^2 - 486\, j_{3,0}(z) - 19683)^2}{j_{3,0}(z)^3}, \tag{7}$$

obtained as in [7] by linear algebra on the Fourier coefficients of q-expansions. Because [6] already treats the case of elliptic curves with real j-invariants, we are interested only in the case of non-real j-invariants. Eqs. (6) and (7) show that the only way a rational number $j_3(z)$ can arise from a non-real number $j(z)$ is if the two complex numbers $j_{3,0}(z)$ and $w_3(j_{3,0}(z))$ are imaginary quadratic complex conjugates of each other. When this happens, Eq. (5) then shows that the two complex conjugates multiply to 3^6, so we conclude that the norm of $j_{3,0}(z)$ must equal 3^6.

Taking the norms of both sides of (7), we get

$$\begin{aligned} \mathrm{N}(j(z) - 1728) &= \frac{\mathrm{N}(j_{3,0}(z)^2 - 486\, j_{3,0}(z) - 19683)^2}{\mathrm{N}(j_{3,0}(z))^3} \\ &= \frac{\mathrm{N}(j_{3,0}(z)^2 - 486\, j_{3,0}(z) - 19683)^2}{(3^6)^3}, \end{aligned}$$

where the last equality follows from the fact that $j_{3,0}(z)$ has norm 3^6. This equation shows that the rational number $\mathrm{N}(j(z) - 1728)$ is always a perfect square, and hence it cannot satisfy the requirement of Elkies that it possess a prime factor of odd multiplicity.

5.2. Points on $X_0^*(11)$

For a numerical demonstration of our supersingular prime finding algorithm, consider the point $j_{11} = \frac{21}{2}$ on $X_0^*(11)$, having j-invariant

$$j = \frac{-489229980611 - 42355313\sqrt{-84567}}{4096},$$

with $\mathrm{N}(j-1728) = (7646751287/64)^2$. We find supersingular primes for this j-invariant using class polynomials on $X_0^*(11)$. For this we must pick primes $\ell \equiv 1 \bmod 4$ such that ℓ is a quadratic residue mod 11 and the class polynomial of discriminant -44ℓ has a real root to the left of $\frac{21}{2}$, in order to ensure that $P_D(\frac{21}{2})$ is negative.

Using $\ell = 5$, we find that

$$P_{-220}(X) = X^2 - 77X + 121.$$

The rational number $P_{-220}(\frac{21}{2}) = -2309/4$ is negative and a perfect square modulo 55, so the prime factor 2309 in the numerator is a supersingular prime for this point.

To find a new supersingular prime not equal to 2309, we need a new value of ℓ such that the Jacobi symbol $(\frac{2309}{11\ell})$ is equal to 1. Using $\ell = 37$, we have

$$\begin{aligned} P_{-1628}(X) = {} & X^8 - 101042X^7 - 2728753X^6 - 167281605X^5 \\ & +1453552981X^4 - 4464256335X^3 + 8630555868X^2 \\ & -9354295951X + 4253517961 \end{aligned}$$

and

$$P_{-1628}(\tfrac{21}{2}) = -\frac{7^2 \cdot 151 \cdot 452233314041}{256}.$$

Of the primes in the numerator, both 7 and 151 are quadratic non-residues mod $11 \cdot 37 = 407$, so our j-invariant is supersingular modulo these primes. In this case the primes are small enough to check directly against the tables of supersingular j-invariants in [2]; thus we find that $(-489229980611 - 42355313\sqrt{-84567})/4096$ is congruent to $6 \bmod 7$, and to $67 \bmod 151$ (or to $101 \bmod 151$ if the other square root is chosen), and that these values are indeed supersingular invariants modulo 7 and 151, respectively.

6. Further directions

The proofs given here are not limited to the case where $j_p(E)$ is rational. When $p \equiv 1 \bmod 4$, we can generalize Theorem 1.1 to the case of elliptic curves E whose j_p-invariant has odd algebraic degree. The proof is the same as that given in [5]: for large enough values of ℓ, the absolute norm of $P_\ell(j_p(E))$ is negative and hence has a prime factor lifting to a new supersingular prime of E. Likewise, for $p \equiv 3 \bmod 4$, we can extend our proof to all curves E for which $j_p(E)$ is real. In this case we assume that all the real conjugates of $j_p(E)$ lie inside the set $j_p(S)$ of Lemma 3.3, since otherwise we can use [6] directly. Because the bounded root of $P_D(X)$ is uniformly distributed along $j_p(S)$, there exists a value of D making $P_D(X)$ negative valued on exactly one real conjugate of $j_p(E)$. For this choice of D, the numerator of the absolute norm of $P_D(j_p(E))$ produces a new supersingular prime for E.

One might naturally ask how to prove Theorem 1.1 for the primes $p = 17$ or $p > 19$. Our proof relies on the fact that the polynomial $P_D(X)$ is a square mod p. When $X_0(p)$ has genus 0, this fact is automatic since $P_D(X)$ has only one root in characteristic p. For the genus 1 cases $p = 11$ and 19, we proved squareness using the fact that the Brandt matrix of the Hecke correspondence T_2 has column sums which are even. However, this evenness property fails in general—for instance, when $p = 23$ we have $B(2) = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 1 & 1 \\ 0 & 3 & 0 \end{bmatrix}$ which means we cannot expect $P_D(j_{23}(E))$ to be a perfect square unless the number $j_{23}(E) \bmod 23$ differs from every possible pair of supersingular j_{23}-invariants by quantities having the same quadratic character mod 23. This condition is fulfilled by about one quarter of the curves satisfying the hypotheses of Theorem 1.1, and for these curves the proof of the theorem goes through unchanged.

Even when $P_D(X)$ is not guaranteed to be a perfect square mod p, empirical evidence indicates that the polynomial is sometimes a perfect square anyway. For example, when $p = 23$, a computer search up to $\ell = 400$ indicates that the primes 101, 173, and 317 have polynomials with square factorizations. It therefore seems possible that classifying the square occurrences of $P_D(X)$ would lead to a proof of the theorem in these cases.

Acknowledgments

This paper is based upon doctoral research performed under the supervision of Noam Elkies, who first proposed to me the idea of studying the curves $X_0^*(p)$ and provided valuable insight and guidance during the time that I worked with him. The work was supported under a National Defense Science and Engineering Graduate Fellowship.

References

[1] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.
[2] B.J. Birch, W. Kuyk (Eds.), Modular functions of one variable. IV, Proceedings of the International Summer School on Modular Functions of One Variable and Arithmetical Applications, RUCA, University of Antwerp, Antwerp, July 17–August 3, 1972, Springer, Berlin, 1975 [Lecture Notes in Mathematics, vol. 476].
[3] D.A. Cox, Primes of the Form $x^2 + ny^2$, A Wiley-Interscience Publication, New York, 1989.
[4] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197–272 (German).
[5] N.D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over **Q**, Invent. Math. 89 (1987) 561–567.
[6] N.D. Elkies, Supersingular primes for elliptic curves over real number fields, Compositio Math. 72 (1989) 165–172.
[7] N.D. Elkies, Elliptic and modular curves over finite fields and related computational issues, Computational Perspectives on Number Theory (Chicago, IL, 1995), AMS/IP Studies in Advanced Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1998, pp. 21–76.
[8] B.H. Gross, Heegner points on $X_0(N)$, Modular Forms (Durham, 1983), Ellis Horwood Series in Mathematical and its Applications: Statistic in Operational Research, Horwood, Chichester, 1984, pp. 87–105.
[9] D. Jao, Supersingular primes for rational points on modular curves, Ph.D. Thesis, Harvard University, 2003.
[10] D. Kohel, Endomorphism rings of elliptic curves over finite fields, Ph.D. Thesis, University of California, Berkeley, 1996.
[11] Serge Lang, Algebraic number theory, second ed., Graduate Texts in Mathematics, vol. 110, Springer, New York, 1994.

[12] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. (1977) 33–186 (1978).
[13] A. Pizer, An algorithm for computing modular forms on $\Gamma_0(N)$, J. Algebra 64 (1980) 340–390.
[14] J.H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer, New York, 1986.