Pure and Applied Mathematics Quarterly
Volume 4, Number 4
(*Special Issue: In honor of
Jean-Pierre Serre, Part 1 of 2*)
1317—1326, 2008

# Minimal CM Liftings of Supersingular Elliptic Curves

**Tonghai Yang**

*Dedicated to J.-P. Serre*

**Abstract:** In this paper, we prove that if every supersingular elliptic curve over $\mathbb{F}_p$ can be lifted to a CM elliptic curve by an imaginary order $\mathcal{O}_D$ for some $D \ll p^\theta$, then $\theta \geq \frac{1}{2}$. We also prove that if every supersingular elliptic curve over $\bar{\mathbb{F}}_p$ can be lifted to a CM elliptic curve by an imaginary order $\mathcal{O}_D$ for some $D \ll p^\theta$, then $\theta \geq \frac{2}{3}$ as suggested by Elkies.
**Keywords:** Supersingular elliptic curve, complex multiplication, quaternion algebra, maximal order, optimal embedding, quadratic forms

## 1. Introduction

Let $E$ be a rational elliptic curve, and let $\pi_0(x)$ is the number of primes $p < x$ such that $E \mod p$ is supersingular, i.e., $p$ is a supersingular prime of $E$. Then a well-known conjecture of Lang and Trotter [LT] claims that

$$\pi_0(x) = (C + o(1))\frac{x^{\frac{1}{2}}}{\log x} \tag{1.1}$$

for some explicit constant $C > 0$ depending on the elliptic curve $E$. A famous result of Elkies asserts that $\pi_0(x)$ goes to infinity as $x$ goes to infinity [El1]. Later He and Murty [El2] observed that if for every supersingular prime $p$ of $E$, $E \mod p$ can be lifted to a CM elliptic curve with CM by an imaginary order $\mathcal{O}_D$ for some $D \ll p^\theta$, then $\pi_0(x) \ll x^{\frac{3}{2}\theta}$. Combining this observation with the following result of Kaneko [Kan], they proved that $\pi_0(x) \ll x^{\frac{3}{4}}$.

Received January 9, 2007.
*2000 Mathematics Subject Classification.* 11G15, 11F41, 14K22.
Partially supported by NSF grants DMS-0302043, 0354353, a NSA grant, and NSFC-10628103.

**Theorem 1.1.** *(Kaneko) Every supersingular elliptic curve $E$ defined over $\mathbb{F}_p$ can be lifted to a CM elliptic curve with CM by an imaginary quadratic order $\mathcal{O}_D$ (of discriminant $-D$) for some $D < \frac{4}{\sqrt{3}} p^{\frac{1}{2}}$.*

An improvement of Kaneko's result in terms of the exponent $\theta$ would get us closer to the Long-Trotter conjecture, and $\theta = \frac{1}{3}$ would almost give the Lang-Trotter conjecture. So a natural and interesting question is how far we can improve the result of Kaneko. The main purpose of this paper is to show that Kaneko's result is the best possible. Indeed, we will prove the following theorems in Sections 4 and 5.

**Theorem 1.2.** *For every $\kappa < \frac{4}{\sqrt{3}}$, there is $N = N(\kappa) > 0$ such that for every prime $p \equiv 3 \mod 4$ with $p > N$, there is a supersingular elliptic curve over $\mathbb{F}_p$ which can not be lifted to a CM elliptic curve by an imaginary order $\mathcal{O}_D$ with $D < \kappa p^{\frac{1}{2}}$.*

**Theorem 1.3.** *For every $\kappa < \frac{\pi}{6}$, there is $N = N(\kappa) > 0$ such that for every prime $p \equiv 1 \mod 4$ with $p > N$, there is a supersingular elliptic curve over $\mathbb{F}_p$ which can not be lifted to a CM elliptic curve by an imaginary order $\mathcal{O}_D$ with $D < \kappa p^{\frac{1}{2}}$.*

The basic idea to prove Theorems 1.2 and 1.3 is as follows. It is well-known (see Section 3) that a supersingular elliptic curve $E$ can be lifted to a CM elliptic curve by $\mathcal{O}_D$ if and only if there is an optimal embedding $\mathcal{O}_D \hookrightarrow \mathcal{O}_E = \mathrm{End}(E)$, or equivalently the Gross lattice

$$\mathcal{L}_E = \{x \in \mathbb{Z} + 2\mathcal{O}_E : \mathrm{tr}\, x = 0\}, \quad Q(x) = -x^2 \tag{1.2}$$

represents $D$. Moreover, $\mathcal{O}_E$ is a maximal order of $B_p$, and every maximal order with an element $w^2 = -p$ is conjugate to some $\mathcal{O}_E$. Here $B_p$ is the unique rational quaternion algebra ramified exactly at $p$ and infinity. Serre [El2] observes that the orthogonal complement of $w$ in $\mathcal{L}_E$ is a binary quadratic lattice of discriminant of size about $p$, and thus represents some integer about the size $\sqrt{p}$, which gives a simple proof of Kaneko's result. Our idea is to reverse the procedure, starting with binary quadratic forms of discriminant $p$ (or $4p$ for $p \equiv 1 \mod 4$) which do not represent 'small' integers, we construct maximal orders of $B_p$ whose associated Gross orders do not represent small integers either.

As a related question, one might ask what can be said about integers $D_0$ such that every supersingular elliptic curve over $\bar{\mathbb{F}}_p$ can be lifted to a CM elliptic curve by $\mathcal{O}_D$ for some $D \le D_0$. Elkies showed that $D_0 = 2p^{\frac{2}{3}}$ is enough and mentioned in a private email to the author that the exponent $\frac{2}{3}$ should be the best possible. We confirm his claim by counting in Section 2.

**Proposition 1.4.** *If there are positive constants $\theta$ and $C$ such that every supersingular elliptic curve over $\bar{\mathbb{F}}_p$ can be lifted to a CM elliptic curve over some number field with CM by $\mathcal{O}_D$ with $D \le Cp^\theta$, then $\theta \ge \frac{2}{3}$.*

Another natural question is for what $D_0 = D_0(p)$, every supersingular elliptic curve over $\bar{\mathbb{F}}_p$ can be lifted to a CM elliptic curve by $\mathcal{O}_D$ for every fundamental discriminant $-D \le -D_0$ with $(\frac{-D}{p}) \ne 1$. This was studied by Duke [Du], Michele [Mi], Elkies, Ono, and the author [EOY] ineffectively, and by Kane [Ka] effectively (assuming GRH).

**Acknowledgement**: The project was inspired by a private email communication from Elkies in early 2005, and the proof of the main theorem was inspired by Serre's proof [El2] of Kaneko's result. We thank both for their inspirations. We thank W. Duke, T. Ibukiyama, B. Kane, M. Kaneko, K. Ono, J. Rouse, and L. Washington for their helpful discussion and comments.

## 2. Proof of Proposition 1.4

**Proof of Proposition 1.4**: Let

$$S_p(x) = \prod_{E s.s.} (x - j(E)) \tag{2.1}$$

be the supersingular polynomial, where the product runs over all supersingular elliptic curves (up to isomorphism) over $\bar{\mathbb{F}}_p$. Let

$$P_D(x) = \prod_{\text{End } A = \mathcal{O}_D} (x - j(A))$$

be the class polynomial of discriminant $-D \equiv 0, 1 \mod 4$. Here the product runs over all elliptic curves over $\mathbb{C}$ with End $A = \mathcal{O}_D$ (up to isomorphism), i.e., all CM elliptic curves with CM by $\mathcal{O}_D$. When $D \equiv 1, 2 \mod 4$, we set $P_D(x) = 1$. Since an elliptic curve is determined by its $j$-invariants (up to isomorphism), it is clear that the condition in Proposition 1.4 is equivalent to

$$S_p(x) | \prod_{D \le Cp^\theta} P_D(x).$$

So

$$\deg S_p(x) \le \sum_{D \le Cp^\theta} \deg P_D(x). \tag{2.2}$$

A classical result of Deuring ([Si, Theorem 4.1]) asserts

$$\deg S_p(x) = \frac{p}{12} + \epsilon_p, \quad -1 \le \epsilon_p \le 2.$$

On the other hand, the theory of complex multiplication implies that $\det P_D(x) = h_D$ is the ideal class number of the imaginary quadratic order $\mathcal{O}_D = \mathbb{Z}[\frac{D+\sqrt{-D}}{2}]$. It is well known that

$$h_D \ll D^{\frac{1}{2}+\epsilon}$$

for every $\epsilon > 0$. So we have by (2.2)

$$\frac{p}{12} \ll \sum_{D \le Cp^\theta} D^{\frac{1}{2}+\epsilon} \ll p^{\frac{3}{2}\theta+\theta\epsilon}.$$

Since $\epsilon$ can be arbitrarily small and $p$ can be arbitrarily large, we have $\theta \ge \frac{2}{3}$. This proves Proposition 1.4.

**Remark 2.1.** Similar argument would give the following assertion. If every supersingular elliptic curve over $\mathbb{F}_p$ can be lifted to a CM elliptic curve with CM by $\mathcal{O}_D$ for some $D \le Cp^\theta$, then $\theta \ge \frac{1}{3}$. Theorem 1.2 asserts $\theta \ge \frac{1}{2}$.

## 3. Maximal Orders and Optimal Embeddings

For a prime number $p$, let $B_p$ be the unique quaternion algebra over $\mathbb{Q}$ ramified exactly at $p$ and $\infty$. It is a well-known fact, due to Deuring [De], that every maximal order of $B_p$ is conjugate to $\mathcal{O}_E = \mathrm{End}_{\bar{\mathbb{F}}_p}(E)$ for some supersingular elliptic curve $E$ over $\bar{\mathbb{F}}_p$. Two maximal orders $\mathcal{O}_E$ and $\mathcal{O}_{E'}$ are conjugate to each other if and only if $E' \cong E$ or $E' \cong E^{(p)}$, the Frobenius of $E$. $E \cong E^{(p)}$ if and only if $E$ is defined over the prime field $\mathbb{F}_p$. In such a case, the Frobenius gives an element $w \in \mathcal{O}_E$ such that $w^2 = -p$. The converse is also true, a maximal order containing an element $w$ with $w^2 = -p$ comes from a supersingular elliptic curve over $\mathbb{F}_p$ (up to conjugation). Deuring [De] also proved that a supersingular elliptic curve $E$ can be lifted to an elliptic curve over a number field with complex multiplication (CM) exactly by an imaginary quadratic order $\mathcal{O}_D = \mathbb{Z}[\frac{-D+\sqrt{-D}}{2}]$ if and only if there is an optimal embedding from $\mathcal{O}_D$ into $\mathcal{O}_E$, i.e., an embedding $f : K = \mathbb{Q}(\sqrt{-D}) \hookrightarrow B_p$ such that $f^{-1}(\mathcal{O}_E) = \mathcal{O}_D$. Next, for an order $\mathcal{O}$ of $B_p$, let

$$\mathcal{L}_{\mathcal{O}} = \{x \in \mathbb{Z} + 2\mathcal{O} : \mathrm{tr}\, x = 0\} \tag{3.1}$$

be its Gross quadratic (ternary) lattice with quadratic form $Q(x) = -x^2$, the reduced norm of $x$. Then Gross proved in [Gr] that $\mathcal{L}_{\mathcal{O}}$ represents $D$ if and only if $\mathcal{O}_D$ embeds into $\mathcal{O}$, or equivalently, some order $\mathcal{O}_{D'}$ with $D = D'n^2$ embeds optimally into $\mathcal{O}$. So we have

**Proposition 3.1.** *Let $E$ be a supersingular elliptic curve over $\bar{\mathbb{F}}_p$ and $D_0$ be a positive integer. Then the following are equivalent.*

*(1) $E$ can be lifted to a CM elliptic curve with CM by $\mathcal{O}_D$ for some $D \le D_0$.*

*(2) There is an (optimal) embedding of $\mathcal{O}_D$ into $\mathcal{O}_E$ for some $D \le D_0$.*

*(3) The Gross lattice of $\mathcal{O}_E$ represents $D$ for some $D \le D_0$.*

## 4. Proof of Theorem 1.2

To a primitive positive definite binary quadratic form $Q = [a, b, c] = ay^2 + byz + cz^2$ of discriminant $d = 4ac - b^2 > 0$, we associate a ternary quadratic lattice

$$L = L(Q) = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3, \tag{4.1}$$

with quadratic form

$$Q_L((x, y, z)) = x^2 + ay^2 + byz + cz^2. \tag{4.2}$$

Then it is well-known that the even Clifford algebra of $L$ is actually a quaternion algebra $B = B(L) = B(Q)$ with a $\mathbb{Q}$-basis $\{v_0 = 1, v_1 = e_2e_3, v_2 = e_3e_1, v_3 = e_1e_2\}$ and the following multiplication table.

Table 1. Multiplication Table

| | $v_1$ | $v_2$ | $v_3$ |
|---|---|---|---|
| $v_1$ | $bv_1 - ac$ | $-cv_3$ | $av_2 + bv_3$ |
| $v_2$ | $bv_2 + cv_3$ | $-c$ | $b - v_1$ |
| $v_3$ | $-av_2$ | $v_1$ | $-a$ |

In particular,

$$O(Q) = \oplus \mathbb{Z}v_i \tag{4.3}$$

is an order of $B(Q)$. With respect to the reduced norm (as a quadratic form), the Gram matrix of $O(Q)$ is

$$A = ((v_i, v_j)) = \begin{pmatrix} 2 & b & & \\ b & 2ac & & \\ & & 2c & -b \\ & & -b & 2a \end{pmatrix}. \tag{4.4}$$

In particular, $\det A = d^2$. Since the diagonization of $\frac{1}{2}A$ is $\mathrm{diag}(1, \frac{d}{4}, c, \frac{d}{4c})$, its local Hasse invariant is $\epsilon_l = (d, -1)_l(c, -d)_l$, where $(\ ,\ )_l$ is the local Hilbert symbol. So [Se, Theorem 6] implies

**Lemma 4.1.** *Let the notation be as above. Then*

*(1) $B(L)$ is positive definite.*

*(2) $B(L)$ is split at $l$ for every prime number $l \nmid 2d$.*

*(3) $B(L)$ is split at $l$ if and only if $(-c,-d)_l = 1$.*

**Proposition 4.2.** *Let $p \equiv 3 \mod 4$ be a prime number.*

*(1) Let $Q = [a,b,c]$ is a primitive positive definite quadratic form of discriminant $4ac - b^2 = p$. Then $B(Q) = B_p$ is the quaternion algebra ramified exactly at $p$ and $\infty$, and $O(Q)$ is a maximal order of $B_p$ with an element $w = 2v_1 - b$ satisfying $w^2 = -p$.*

*(2) The Gross lattice of $O(Q)$ is*

$$\mathcal{L}(Q) = \mathbb{Z}w + \mathbb{Z}2v_2 + \mathbb{Z}2v_3$$

*with quadratic form*

$$Q_{\mathcal{L}}(xw + y2v_2 + z2v_3) = px^2 + 4Q(z,y) = px^2 + 4(cy^2 + byz + ay^2).$$

*Proof.* (1) By Lemma 4.1, to show $B(Q) = B_p$, it is enough to verify that $B(Q)$ is split at 2, i.e., $(-c,-p)_2 = 1$. Since $4ac - b^2 = p \equiv 3 \mod 4$, $b$ is odd, and

$$4ac \equiv 1 + p \mod 8, \quad ac \equiv \frac{1+p}{4} \mod 2.$$

If $p \equiv 3 \mod 8$, then $c$ is odd, and $(-c,-p)_2 = 1$ as desired. If $p \equiv 7 \mod 8$, then $-p \equiv 1 \mod 8$ and again $(-c,-p)_2 = 1$. This proves $B(Q) = B_p$. Since the Gram matrix of $O(Q)$ has determinant $\det A = p^2$, $O(Q)$ is a maximal order of $B_p$. Finally, for $w = 2v_1 - b$, one has by Table 1

$$w^2 = 4v_1^2 - 4bv_1 + b^2 = 4bv_1 - 4ac - 4bv_1 + b^2 = -p.$$

(2) is clear from (1) and (4.4). □

Before proving Theorem 1.2, we briefly review the well-known theorem of Duke on the uniform distribution of Heegner points on modular curves. Let $X = \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^*$ be with the usual fundamental domain

$$\mathcal{F} = \{z = x + iy : |z| \geq 1, \quad |x| \leq \frac{1}{2}\}.$$

Here $\mathbb{H}^* = \{z = x + iy : y > 0\} \cup \mathbb{Q} \cup \{i\infty\}$ is the extended upper half plane. A Heegner point in $X$ of discriminant $-d$ is a point of the form $\tau = \frac{-b+\sqrt{-d}}{2a}$ with $[a,b,c]$ being a primitive positive definite binary quadratic form of discriminant $4ac - b^2 = d$. Two primitive forms give the same Heegner points in $X$ if and only if they are equivalent, and a primitive form $Q = [a,b,c]$ gives the point $\tau_Q = \frac{-b+\sqrt{-d}}{2a}$ in the fundamental domain $\mathcal{F}$ if and only if $|b| \leq a \leq c$. i.e., $Q$ is reduced (with a couple of exceptions). Recall that a primitive form $[a,b,c]$ is reduced if and only if $|b| \leq a \leq c$ and $b > 0$ if $|b| = a$ or $c = a$. In such a case, the

smallest positive integer represented by $[a,b,c]$ is $a$. Duke proved in [Du] that the Heegner points are uniformly distributed in $X$, in the sense that for every $L^1$-function $f$ on $X$ (well-defined over Heegner points), one has

$$\lim_{d\to\infty}\frac{1}{h_d}\sum_{\tau} f(\tau)=\frac{3}{\pi}\int_{\mathcal{F}} f(z)\frac{dx\,dy}{y^2}. \tag{4.5}$$

where the sum runs over all Heegner points $\tau=\frac{-b+\sqrt{-d}}{2a}$ on $X$ of discriminant $-d$.

**Proof of Theorem 1.2**:Now we are ready to prove Theorem 1.2. For $0<\kappa<\frac{4}{\sqrt{3}}$, $\frac{2}{\kappa}>\frac{\sqrt{3}}{2}$. We define a function $f_\kappa$ on $X$ such that on the fundamental domain $\mathcal{F}$, it is given by

$$f_\kappa(z)=\begin{cases}1 & \text{if } y<\frac{2}{\kappa},\\ 0 & \text{otherwise.}\end{cases}$$

Then (4.5) gives

$$\lim_{p\to\infty}\frac{1}{h_p}\sum_{[a,b,c],a>\frac{\kappa\sqrt{p}}{4}} 1=\frac{3}{\pi}\int_{\mathcal{F}} f_\kappa(z)\frac{dx\,dy}{y^2}>0.$$

So there is a constant $N>0$ such that for every prime $p\equiv 3 \mod 4$ with $p>N$, there is a reduced form $[a,b,c]$ of discriminant $p$ with $a>\frac{\kappa\sqrt{p}}{4}$. In this case, the smallest integer represented by $Q=[a,b,c]$ is $a$. Now Proposition 4.2 implies that the smallest positive integer represented by the Gross lattice $\mathcal{L}(Q)$ is $\min(p,4a)\geq\kappa\sqrt{p}$. Let $E$ be a supersingular elliptic curve over $\mathbb{F}_p$ such that $\mathcal{O}_E$ is conjugate to $O(Q)$. Then $E$ can not be lifted to a CM elliptic curve with CM by $\mathcal{O}_D$ with $D<\kappa\sqrt{p}$ by Proposition 3.1. This proves Theorem 1.2.

## 5. Proof of Theorem 1.3

The proof of Theorem 1.3 is similar with two technical complications: not every (primitive) binary quadratic form of discriminant $4p$ for $p\equiv 1 \mod 4$ gives rise to $B_p$ using the procedure in Section 4, and the associated order $O(Q)$ (when exists) is not a maximal order of $B_p$. Let the notation be as in Section 4 but with $p\equiv 1 \mod 4$. Let $Q=[a,b,c]$ be a primitive binary quadratic form of discriminant $4ac-b^2=4p$, and let $\mathfrak{a}=[a,b/2+\sqrt{-p}]$ be an associated ideal of $\mathbb{Q}(\sqrt{-p})$. Then $Q$ is equivalent to the quadratic form on $\mathfrak{a}$ given by

$$Q(x)=\frac{N(x)}{N\mathfrak{a}}. \tag{5.1}$$

It is well-known that this gives one-to-one correspondence between the equivalence classes of primitive binary quadratic forms of fundamental discriminant $4p$ and the ideal classes of $\mathbb{Q}(\sqrt{-p})$, and between the genus classes of the quadratic

forms and the genus classes of ideals. Recall that a primitive binary quadratic form $Q$ is in the principal genus if it is equivalent to the form $[1,0,p]$ locally at every prime.

**Lemma 5.1.** *Let $p \equiv 1 \mod 4$ be a prime number, and let $Q=[a,b,c]$ be a primitive binary quadratic form of discriminant $-4p$. Let $B(Q)$ be the quaternion algebra constructed from $Q$ in Section 4. Then $B(Q) \cong B_p$ if and only if $Q$ is not in the principal genus.*

*Proof.* By Lemma 4.1, $B(Q)$ is split outside $2p\infty$, and is known to be ramified at $\infty$. So $B(Q) \cong B_p$ if and only if $B(Q)$ is split at 2, i.e., $(-c,-p)_2 = 1$ or equivalently $(c,-p)_2 = -1$ by the same lemma. On the other hand, it is easy to prove that two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are in the same genus if and only if $(N\mathfrak{a},-p)_l = (N\mathfrak{b},-p)_l$ for all primes $l<\infty$. Indeed, they are in the same genus if and only if $\mathfrak{a}_l = \mathfrak{b}_l\alpha_l$ (for some $\alpha_l \in \mathcal{O}_{4p}\otimes\mathbb{Z}_l$) with

$$\frac{N(x\alpha_l)}{N\mathfrak{a}} = \frac{N(x)}{N\mathfrak{b}}$$

for every $x \in \mathfrak{b}_l = \mathfrak{b}\otimes\mathbb{Z}_l$ (i.e., their associated quadratic forms are locally equivalent). This is the same as $(N\mathfrak{a},-p)_l = (N\mathfrak{b},-p)_l$. So by the comment before the lemma, $Q=[a,b,c]$ is in the principal genus if and only if $(a,-p)_l = 1$ for all $l<\infty$. It is easy to check $(a,-p)_l = 1$ for $l \nmid 2p$. Since $4ac-b^2 = 4p$, one sees that $(a,-p)_2 = (c,-p)_2$. So $Q$ is in the principal genus if and only if $(c,-p)_2 = 1$. This proves the lemma. □

**Lemma 5.2.** *Let $Q=[a,b,c]$ be a primitive binary quadratic form of discriminant $4p$ which is not in the principal genus. Let $\mathcal{O}$ be an maximal order of $B(Q)=B_p$ containing $O(Q)$, and let $\mathcal{L}_{\mathcal{O}}$ be the Gross lattice of $\mathcal{O}$. Let*

$$O(Q)^0 = \{x \in O(Q) : \operatorname{tr} x = 0\}.$$

*Then $\mathcal{L}_{\mathcal{O}} \subset O(Q)^0$, and*

$$O(Q)^0 = \mathbb{Z}w + \mathbb{Z}v_2 + \mathbb{Z}v_3$$

*with $w = v_1 - b/2$, and $v_i$ being given in Section 4.*

*Proof.* It suffices to prove $2\mathcal{O} \subset O(Q)$. First notice that $b$ has to be even. Let $b_1 = b/2$ and $w = v_1 - b_1$, then $\operatorname{tr} w = 0$ and $w^2 = -p$. Clearly $1, w, v_2$ and $v_3$ give a basis of $O(Q)$. Since the Gram matrix of $O(Q)$ has determinant $16p^2$, one

has $[\mathcal{O} : O(Q)] = 4$. If $v = x_0 + x_1 w + x_2 v_2 + x_3 v_3 \in \mathcal{O}$, then $x_i \in \frac{1}{4}\mathbb{Z}$. A simple calculation using Table 1 gives

$$v^2 = 2x_0 v - x_0^2 - x_1^2 p - x_2^2 c - x_3^2 a + 2b_1 x_2 x_3. \tag{5.2}$$

Since $v$ is integral over $\mathbb{Z}$, one has $x_0 \in \frac{1}{2}\mathbb{Z}$. The same argument with $wv \in \mathcal{O}$ gives $x_1 \in \frac{1}{2}\mathbb{Z}$. For the same reason, $v_2 v$ and $v_3 v \in \mathcal{O}$ imply

$$x_3 b_1 - c x_2, x_2 b_1 - x_3 a \in \frac{1}{2}\mathbb{Z}, \tag{5.3}$$

If $b_1$ is even, $a$ and $c$ are odd, and $x_3 b_1, x_2 b_1 \in \frac{1}{2}\mathbb{Z}$. So $x_2, x_3 \in \frac{1}{2}\mathbb{Z}$ by (5.3). If $b_1$ is odd, then $ac$ is even, say $a$ is even, and $c$ is odd (since $[a, b, c]$) is primitive). Then (5.3) implies $x_2 b_1$ and thus $x_2 \in \frac{1}{2}\mathbb{Z}$. So $x_2 b_1 - c x_2 \in \frac{1}{2}\mathbb{Z}$ and thus $x_3 \in \frac{1}{2}\mathbb{Z}$. So $\mathcal{O} \subset \frac{1}{2} O(Q)$. □

**Remark 5.3.** With a little calculation, one can show that there are two maximal orders of $B_p$ containing $O(Q)$. One can also show that every maximal order of $B_p$ with an element $w^2 = -p$ can be constructed this way.

**Proof of Theorem 1.3**: We use the same notation as in the end of Section 4. For every $0 < \kappa < \frac{\pi}{6}$, we define $f_\kappa$ on $\mathcal{F}$ as follows and extend it to an $L^1$-function on $X$.

$$f_\kappa(x + iy) = \begin{cases} 1 & \text{if } y < \frac{1}{\kappa}, \\ 0 & \text{if } y \geq \frac{1}{\kappa}. \end{cases}$$

Then applying (4.5) to $f_\kappa$ gives for $p \equiv 1 \mod 4$,

$$\lim_{p\to\infty} \frac{1}{h_{4p}} \sum_{[a,b,c], a > \kappa\sqrt{p}} 1 = \frac{3}{\pi} \int_{\mathcal{F}} f_\kappa(z) \frac{dx\, dy}{y^2} = 1 - \frac{3}{\pi}\kappa > \frac{1}{2}$$

So there is a constant $N = N(\kappa) > 0$ such that for all $p \equiv 1 \mod 4$ with $p > N$, there is a reduced form $Q = [a, b, c]$ of discriminant $4p$ not in the principal genus with $a > \kappa\sqrt{p}$. Since the smallest positive integer represented by $Q$ is $a$, the smallest positive integer represented by $O(Q)^0$ is $\min(p, a)$. So the smallest positive integer represented by $\mathcal{L}_\mathcal{O}$ is bigger than or equal to $\min(p, a) > \kappa\sqrt{p}$. Now applying Proposition 3.1, one obtains Theorem 1.3.

## References


[De] *M. Deuring*, Die Typen der Multiplikatorenringe elliptischer Funktionkörper, Abh. Math. Sem. Hamburg **14** (1941), 197-272.

[Du] *W. Duke*, *Hyperbolic distribution problems and half-integral weight Maass forms*, Invent. Math. **92** (1988), pages 73-90.

[El1] *N. Elkies*, The existence of infintiely many supersingular primes for every elliptic curves over $\mathbb{Q}$, Invent. Math. **89**(1987), 561-567.

[El2] *N. Elkies*, Distribution of supersingular primes, Astérisque **198-199-200** (1991), 127-132.

[EOY] *N. Elkies, K. Ono, and T.H. Yang*, Reduction of CM elliptic curves and modular function congruences, Int. Math. Res. Not. **44** (2005), 2695-2707.

[Gr] *B.H.Gross*, Heights and the special values of $L$-series, Canadian Math. Soc. Conf. Proc. **7**(1987), 115-187.

[Ka] *B. Kane*, Representations of integers by ternary quadratic forms and CM liftings of supersingular elliptic curves, University of Wisconsin-Madison PhD thesis, 2006.

[Kan] *M. Kaneko*, Supersingular $j$-invariants as singular moduli mod $p$, Osaka J. Math. **26**(1989), 849-855.

[LT] *S. Lang and H. Trotter*, Frobenius distributions in $GL_2$-extensions. Distribution of Frobenius automorphisms in $GL_2$-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976.

[Mi] *P. Michel*, The subconvexity problem for the Rankin-Selberg L-functions and equdistribution of Heegner points, Ann. Math. **160** (2004), 185-236.

[Si] *J. H. Silverman*, The arithmetic of elliptic curves, GTM **106**, Springer-Verlag, New York, 1996.

[Se] *J.-P. Serre*, A course in a'rithmetic, GTM **7**, Springer-Verlag, New York, 1973.

Tonghai Yang
Department of Mathematics, University of Wisconsin Madison, 480 Lincoln Dr., Madison, WI 53706, USA
E-mail: thyang@math.wisc.edu