# TORSION POINTS ON ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION (WITH AN APPENDIX BY ALEX RICE)

PETE L. CLARK, BRIAN COOK, AND JAMES STANKEWICZ

Abstract. We present seven theorems on the structure of prime order torsion points on CM elliptic curves defined over number fields. The first three results refine bounds of Silverberg and Prasad-Yogananda by taking into account the class number of the CM order and the splitting of the prime in the CM field. In many cases we can show that our refined bounds are optimal or asymptotically optimal. We also derive asymptotic upper and lower bounds on the least degree of a CM-point on $X_1(N)$. Upon comparison to bounds for the least degree for which there exist infinitely many rational points on $X_1(N)$, we deduce that, for sufficiently large $N$, $X_1(N)$ will have a rational CM point of degree smaller than the degrees of at least all but finitely many non-CM points.

## 1. Introduction

### 1.1. Notation.

For $d \in \mathbb{Z}^+$, we define the following quantities:

$T(d)$: the supremum of the orders of the groups $E(K)[\text{tors}]$ as $K$ ranges over all number fields of degree $d$ and $E$ ranges over all elliptic curves defined over $K$.

$N(d)$: the supremum of all orders of $K$-rational torsion points $P \in E(K)$, with $K$ and $E$ varying as above. (Equivalently, the supremum of all *exponents* of groups $E(K)[\text{tors}]$).

$P(d)$: the supremum of all prime orders of $K$-rational torsion points $P \in E(K)$, with $K$ and $E$ varying as above.

We shall have occasion to consider analogues $T_\bullet(d)$, $N_\bullet(d)$, $P_\bullet(d)$ of the above quantities, which are defined by restricting to some subset of elliptic curves $E_{/K}$. Specifically we will be interested in the set of all elliptic curves with integral modulus $j(E)$ and also the set of all elliptic curves with complex multiplication.

### 1.2. Background on torsion.

Since the torsion subgroup of an elliptic curve over a number field is a finite abelian group with at most two generators, we have

$$P(d) \le N(d) \le T(d) \le N(d)^2. \tag{1}$$

*Date*: June 3, 2015.

The **uniform boundedness theorem** of L. Merel [Mer96] asserts $T(d) < \infty$ for all $d \in \mathbb{Z}^+$. The finiteness of $P(d)$ and $N(d)$ follows immediately.

Merel's proof gives an explicit upper bound on $T(d)$, which was then improved by work of Merel, Oesterlé and Parent. For instance, Parent showed [Par99] that if a power $p^a$ of a prime $p > 3$ divides the order of the torsion subgroup of an elliptic curve over a degree $d$ number field, then

$$p^a \leq 65(3^d - 1)(2d)^6.$$

However, it is a "folk conjecture" that there exists a constant $\alpha$ such that $T(d) = O(d^\alpha)$. In other words, it is believed that Merel's bounds are a full exponential away from the truth. In fact, we record here a more precise conjecture:

**Conjecture 1.**
*There is a* $C_2 > 0$ *such that* $T(d) \leq C_2 d \log\log d$ *for all* $d \in \mathbb{Z}^+$.

Conjecture 1 is very close to being the most ambitious conceivable one: we shall show (Theorem 6) that there is a positive constant $C_1$ and a strictly increasing sequence $\{d_n\}_{n=1}^{\infty}$ of positive integers such that $N(d_n) > C_1 d_n \sqrt{\log\log d_n}$ for all $n$.

The only values of $d$ for which any of $T(d)$, $N(d)$, $P(d)$ are known are:

$T(1) = 16$, $N(1) = 12$, $P(1) = 7$ ([Maz77]).

$T(2) = 24$, $N(2) = 18$, $P(2) = 13$ ([Kam86], [Kam92], [KM88]).

$P(3) = 13$ ([Par03]).

While this article was in revision, M. Stoll announced that he, together with S. Kamienny and W. Stein, have computed that $P(4) = 17$, but the proof has not yet appeared in finished form. Maarten Derickx is currently completing a master's thesis computing $P(5)$ and getting certain (new) bounds on $P(6)$ and $P(7)$. This exciting recent work has pushed the boundary of what is known, but computation of $P(n)$ for moderately large $n$ – let alone for all $n$ at once – seems well out of current reach. So it seems natural to find some more tractable sub-problem and examine the extent to which it is representative of the general case.

One approach is to concentrate on the case of elliptic curves with algebraic integral $j$-invariant (henceforth **integral modulus**). In this case we write $T_{\mathrm{IM}}(d)$, $N_{\mathrm{IM}}(d)$, $P_{\mathrm{IM}}(d)$ for the order, exponent and largest prime dividing the order of an elliptic curve $E$ with integral modulus defined over any number field of degree $d$. For such curves the uniform boundedness is much easier to prove. Moreover, in the integral modulus case the computation of all torsion subgroups over $\mathbb{Q}$ was done by G. Frey in 1977 [Fre77]. Analogous computations in higher degree are significantly more difficult and have been the subject of several papers of H. Zimmer and his collaborators: the 1976 paper [Zim76] lays foundations by giving a generalization of the Lutz-Nagell restrictions on torsion points to arbitrary number fields; the 1989 paper [MSZ89] enumerates the torsion subgroups of elliptic curves with integral modulus over quadratic fields ($d = 2$); special kinds of cubic fields ($d = 3$) were considered in 1990 [FSWZ90] and the case of a general cubic field was completed in 1997 [PWZ97]. Only a very restricted class of quartic fields has ever been considered in the case of integral modulus, so already the case $d = 4$ seems to be out of reach.

However, Hindry and Silverman have shown [HS99] that

$$\forall d \in \mathbb{Z}^+, T_{\mathrm{IM}}(d) \leq 1977408 d \log d, \tag{2}$$

$$\forall d \geq 25, T_{\mathrm{IM}}(d) \leq 498240 d \log d. \tag{3}$$

Another approach is to search for all finite groups $G$ which arise as the torsion subgroup of *infinitely* many elliptic curves defined over (varying) number fields of degree $d$. In this case the computations in degree up to $d = 4$ have been done by Jeon, Kim, Park and Schweizer [JKS04], [JK06], [JKP06], and reasonably good asymptotic bounds can be obtained by applying theorems of Faltings and Abramovich. This work is described in more detail below.

In this paper we shall usually restrict to elliptic curves with complex multiplication. This is a very special subclass of the class of integral moduli curves, comprising for each degree $d$ only finitely many j-invariants (but infinitely many nonisomorphic *twists* for a given $j$-invariant). Accordingly, we are able to derive more precise results than in the general case. We also take up the task of relating the special case of CM points to the general case.

### 1.3. **Prior results.**

Let $F$ be a field of characteristic 0 and $E_{/F}$ an elliptic curve. We say that $E$ has **complex multiplication** (henceforth **CM**) if the ring $\operatorname{End} E$ of endomorphisms of $E$ defined over an algebraic closure $\overline{F}$ of $F$ is strictly larger than $\mathbb{Z}$. In this case, $\operatorname{End}^0(E) := \operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and $\operatorname{End}(E)$ is an order in $\operatorname{End}^0(E)$.

As alluded to above, we write $T_{\mathrm{CM}}(d)$, $N_{\mathrm{CM}}(d)$, $P_{\mathrm{CM}}(d)$ for, respectively, the largest order, exponent and prime dividing the order of any CM elliptic curve defined over any number field of degree $d$.

The $j$-invariant of a CM elliptic curve is an algebraic integer [Sil94, Thm. II.6.1], so that by (2), (3) we have $\#E(F)[\mathrm{tors}] = O(d \log d)$. If we restrict to the order of a single torsion point – i.e., to $N_{\mathrm{CM}}(d)$ rather than $T_{\mathrm{CM}}(d)$ – we can do qualitatively better: one knows that $N_{\mathrm{CM}}(d) = o(d \log d)$. More precisely:

**Theorem.** *(Silverberg* [Sbg88] [Sbg92]*, Prasad-Yogananda* [PY01]*) Let $F$ be a number field of degree $d$, and let $E_{/F}$ be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in the imaginary quadratic field $K$. Let $w = w(\mathcal{O}) = \#\mathcal{O}^\times$ (so $w = 2$, 4 or 6) and let $e$ be the exponent of $E(F)[\mathrm{tors}]$. Then:*
*a) $\varphi(e) \leq wd$ ($\varphi$ is Euler's totient function).*
*b) If $F \supseteq K$, then $\varphi(e) \leq \frac{wd}{2}$.*
*c) If $F$ **does not** contain $K$, then $\varphi(\#E(F)[\mathrm{tors}]) \leq wd$.*

Applying the theorem necessitates separate consideration of three cases:

Case 1: $\mathcal{O} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, of discriminant $-3$ and $w(\mathcal{O}) = 6$. We get

$$\varphi(e) \leq 6d. \tag{4}$$

Case 2: $\mathcal{O} = \mathbb{Z}[\sqrt{-1}]$, of discriminant $-4$ and $w(\mathcal{O}) = 4$. We get

$$\varphi(e) \leq 4d. \tag{5}$$

Case 3: For every other order, $w(\mathcal{O}) = 2$. We get

$$\varphi(e) \leq 2d. \tag{6}$$

Let us call (4), (5) and (6) the **SPY bounds**.

Recall the classical result $\varphi(N) \gg \frac{N}{\log \log N}$ (e.g., [HW, Thm. 328]). From this and the SPY bounds we deduce that there exists a positive constant $C$ such that

$$N_{\mathrm{CM}}(d) \leq Cd \log \log d. \tag{7}$$

This improves upon what one gets by applying (2):

$$N_{\mathrm{CM}}(d) \leq N_{\mathrm{IM}}(d) \leq T_{\mathrm{IM}}(d) \leq 1977408 d \log d.$$

Theorem 6 below asserts $N_{\mathrm{CM}}(d) \neq o(d\sqrt{\log \log d})$, so that our understanding of the true lower order of magnitude of $N_{\mathrm{CM}}(d)$ is rather good. On the other hand, it is vexing that we cannot get any improvement on

$$T_{\mathrm{CM}}(d) \leq T_{\mathrm{IM}}(d) = O(d \log d)$$

by applying the methods of SPY, or indeed by any other means that we know.

### 1.4. **Computational results.**

We briefly report on some calculations done by the University of Georgia Number Theory VIGRE Research Group, which has implemented an algorithm (c.f. [Cla04]) to do the following: given a positive integer $d$, compute the complete list of isomorphism classes of finite abelian groups which arise as the full torsion subgroup of some CM elliptic curve with defined over any number field of degree $d$.

This algorithm requires knowledge of the CM j-invariants (more precisely, their minimal polynomials) of degree $d'$ *strictly dividing* $d$, so in full generality requires an enumeration of the set of imaginary quadratic fields with any given class number, i.e., an effective solution of the **Gauss class number problem**. Work of M. Watkins [Wat04] gives a solution to this problem up to class number 100, so the data from *ibid.* enable us, in theory, to run the algorithm for all degrees up to $d = 201$. In fact this is more class number data than we have been able to use: one of the steps in our algorithm is the computation of an explicit polynomial $P_N(x, y) = 0$ which (birationally) defines the modular curve $X_1(N)$, a computation which became prohibitively expensive for us around $N = 79$. For further information on the computation of equations for $X_1(N)$, the reader is encouraged to see A. Sutherland's tables [S12].

The complete list of possible torsion subgroups of CM elliptic curves defined over any degree $d$ number field has been computed by our VIGRE research group for $1 \leq d \leq 13$, as will be described elsewhere. The case of $d = 1$ is a 1974 result of L. Olson [Ols74]. For $d = 2$ and 3 the results are subsumed by the calculations of [MSZ89], [PWZ97]. To the best of our knowledge the cases $4 \leq d \leq 13$ had not been computed before.

Upon restriction from $T_{\mathrm{CM}}(d)$ to $P_{\mathrm{CM}}(d)$, the above problem can be rephrased as follows: for a fixed $d$, find all prime numbers $N$ such that the modular curve

$X_1(N)$ has a CM point of degree $d$. It is natural to consider also the following "converse problem": for fixed prime $N$, find the smallest degree of a CM point on $X_1(N)$. Our algorithm works equally well on this converse problem, and we present the solution, for all $N \leq 79$, in the following table:[1]

**TABLE 1**

| $N$ | $d$ | $D$ |
|---|---|---|
| 2 | 1 | -3, -4,-7, -8, -12, -16, -28 |
| 3 | 1 | -3, -12, -27 |
| 5 | 2 | -4 |
| 7 | 2 | -3 |
| 11 | 5 | -11 |
| 13 | 4 | -3 |
| 17 | 8 | -4 |
| 19 | 6 | -3 |
| 23 | 22 | -7, -11, -19, -28, -43, -67 |
| 29 | 14 | -4 |
| 31 | 10 | -3 |
| 37 | 12 | -3 |
| 41 | 20 | -4 |
| 43 | 14 | -3 |
| 47 | 46 | -11, -19, -43, -67, -163 |
| 53 | 26 | -4 |
| 59 | 58 | -8, -11, -43, -67 |
| 61 | 20 | -3 |
| 67 | 22 | -3 |
| 71 | 70 | -7, -11, -28, -67, -163 |
| 73 | 24 | -3 |
| 79 | 26 | -3 |

Looking through the data one observes that much, but not all, of the time, the SPY bounds are not sharp, so it is natural to ask for refinements. In the next section we shall present several such results. Theorem 2 refines the SPY bounds, by including a factor of the class number $h(D)$ as well as giving a much larger lower bound in case $(\frac{D}{N}) = -1$. Theorem 3 gives conditions under which one gets an extra factor of 2 in the SPY-type bounds. Moreover, for $N$ sufficiently large compared to $D$, the bounds of Theorem 3 are optimal.

### 1.5. **Theoretical results I: Optimal bounds on prime order torsion points.**

**Theorem 1.**
*a) For every prime $N \equiv 1 \pmod 3$, there exists an elliptic curve $E$ over a number field $K$ of degree $\frac{N-1}{3}$, with $j(E) = 0$, and with a $K$-rational $N$-torsion point.*
*b) There exists an absolute constant $N_0$ such that for all primes $N \geq N_0$:*
*(i) if $X_1(N)$ has a CM point of degree $d$, then $d \geq \frac{N-1}{3}$;*

[1]Some preliminary calculations were done by the first author. The calculations were rechecked and completed by Steve Lane, who also pointed out – several times – an error in the preliminary calculations at $N = 11$, which turned out to be very interesting and significant.

*(ii) if $X_1(N)$ has a CM point of degree $d < \frac{N-1}{2}$ then $N \equiv 1 \pmod 3$, $d = \frac{N-1}{3}$ and $j(E) = 0$.*
*(iii) If $N \equiv -1 \pmod 3$ and $X_1(N)$ has a CM point of degree $d < N-1$, then $N \equiv 1 \pmod 4$, $d = \frac{N-1}{2}$ and $j(E) = 1728$.*

Remark 1.1: The data suggests that it may be possible to take $N_0 = 5$.

**Theorem 2.** *Let $\mathcal{O}_K$ be the maximal order in $K = \mathbb{Q}(\sqrt{D})$, $F$ a number field, and $E_{/F}$ an elliptic curve with $\mathcal{O}_K$ multiplication. Let $w(K) = \#\mathcal{O}_K^\times$. Suppose that $E(F)[\mathrm{tors}]$ contains an element of odd prime order $N$.*
*a) $(\frac{D}{N}) = 1$, then*

$$(N-1) \cdot \frac{2h(K)}{w(K)} \mid [KF:\mathbb{Q}].$$

*b) If $(\frac{D}{N}) = -1$, then*

$$(N^2-1) \cdot \frac{2h(K)}{w(K)} \mid [KF:\mathbb{Q}].$$

**Theorem 3.** *Let $\mathcal{O}$ be an order in the field $K = \mathbb{Q}(\sqrt{D})$, $w(\mathcal{O}) = \#(\mathcal{O}^\times)$ and $h(\mathcal{O}) = \#\operatorname{Pic}(\mathcal{O})$ the class number of $\mathcal{O}$. Then:*
*a) For every odd prime $N$ which splits in $K$, there exists an $\mathcal{O}$-CM elliptic curve defined over a number field of degree $2(N-1) \cdot \frac{h(\mathcal{O})}{w(\mathcal{O})}$ with a rational $N$-torsion point.*
*b) There is an $N_0 = N_0(D)$ such that for $N \geq N_0$, the least degree of an $\mathcal{O}(D)$-CM point on $X_1(N)$ is at least $2(N-1) \cdot \frac{h(\mathcal{O})}{w(\mathcal{O})}$ if $N$ splits in $K$ and at least $\left(N^2-1\right) \frac{h(\mathcal{O})}{w(\mathcal{O})}$ otherwise.*

Remark 1.2: Taking $\mathcal{O}$ to be the quadratic order of discriminant $-3$ in Theorem 3a), we recover Theorem 1a). As we shall see, the other parts of Theorem 1 are quick consequences of Theorem 3 together with the SPY-bounds, but it seemed worthwhile to call attention to the extremal behavior coming from the quadratic orders with nontrivial units.

### 1.6. Theoretical results II: CM points of small degree on $X_1(N)$.

Throughout this section $N$ denotes a prime number different from 2 and 3.

Define $d_{\mathrm{CM}}(N)$ to be the least degree of a CM point on $X_1(N)$.

Theorem 1 shows that the smallest (resp. second smallest) possible degree of a CM point on $X_1(N)$ is $\frac{N-1}{3}$ (resp. $\frac{N-1}{2}$), and shows that this degree can be attained iff $N \equiv 1 \pmod 3$ (resp. $N \equiv 1 \pmod 4$). In particular, as $N$ ranges over all primes $N$ which are **not** $11 \pmod{12}$, the least degree of a CM point on $X_1(N)$ is linear in $N$. Notice that the excluded set of primes $N \equiv 11 \pmod{12}$ has density $\frac{1}{4}$ in the set of all primes. By Theorem 2, the problem of bounding the upper order of $d_{\mathrm{CM}}(N)$ as $N$ ranges over prime numbers, comes down to finding, for a given prime $N$, an imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ such that $(\frac{D}{N}) = -1$ and with class number $h(D)$ as small as possible. By applying what is known about these elementary – but difficult! – analytic problems, we arrive at the following result.

**Theorem 4.** *Put $c = \frac{1}{4}e^{-\frac{1}{2}}$: "Burgess's constant".*
*a) For any $\epsilon > 0$, there exists $C_\epsilon$ such that for any prime $N$, the curve $X_1(N)$ has*

*a CM point of degree less than* $C_\epsilon N^{1+c/2+\epsilon} = C_\epsilon N^{1.078\ldots+\epsilon}$.
*b) Assuming the Generalized Riemann Hypothesis (GRH), the least degree of a CM point on* $X_1(N)$ *is* $O(N \log N \log\log N)$.

However, $d_{\mathrm{CM}}(N)$ is not bounded by a linear function of $N$.

**Theorem 5.** *For any* $C > 0$*, there is a positive density set* $\mathcal{P}$ *of prime numbers such that for all* $N \in \mathcal{P}$*, the least degree of a CM point on* $X_1(N)$ *exceeds* $CN$.

**Theorem 6.** *a) There exists* $C > 0$ *such that for any* $F/\mathbb{Q}$ *with* $[F : \mathbb{Q}] = d$ *and any CM elliptic curve* $E_{/F}$*, one has* $\exp(E(F)[\mathrm{tors}]) \leq Cd \log\log d$.
*b) There exists a sequence* $F_n$ *of number fields, of degree* $d_n = [F_n : \mathbb{Q}]$ *tending to infinity, and CM elliptic curves* $E_n/F_n$ *such that*

$$\exp(E_n(F_n)[\mathrm{tors}]) \gg d_n \sqrt{\log\log d_n}.$$

We have already seen that part a) is a consequence of the SPY bounds; we repeat it here for the sake of parallelism. Neither is part b) very difficult: all in all Theorems 4 and 5 seem to lie significantly deeper.

## 1.7. Theoretical results III: small degree points on $Y_1(N)$: comparison with non-CM case.

The overarching problem is to understand all points of degree $d$ on the family of modular curves $Y_1(N)$. Merel's theorem asserts that for fixed $d$ the set of all such points on all curves $Y_1(N)$ is finite, so it is natural to enumerate this list. Conversely, one can fix $N$ and ask for the least degree of a noncuspidal point on $X_1(N)$. In the previous section we presented results giving rather tight estimates on the least degree of a noncuspidal CM point. Therefore the key issue is: how many *non*-CM points are there of small degree?

The next result gives a precise sense in which $d \approx N^2$ is the threshold between small degree and large degree:

**Theorem 7.** *Let* $N > 3$ *be a prime number. Then:*
*a) The set of points of* $X_1(N)$ *of degree less than* $\lceil \frac{7}{3200}(N^2-1) \rceil$ *is finite. Assuming Selberg's eigenvalue conjecture the bound can be improved to* $\lceil \frac{1}{384}(N^2-1) \rceil$.
*b) The set of points of* $X_1(N)$ *of degree at most* $\frac{N^2-12N+11}{12}$ *is infinite.*

Remark 1.3: The proof of part a) uses deep theorems of Faltings, Frey and Abramovich, but the deduction itself is now routine. Essentially the same result appears as [JKS04, Cor. 1.4], the only difference being that we get a sharper bound by restricing to prime $N$. Part b) is much more elementary. Nevertheless, it is in the spirit of this paper to pursue quantitative rather than just qualitative results, and in this regard the fact that we can compute the "threshold" value of $d$ sharply to within a factor of 32 seems interesting. For instance, it raises the question of whether the truth lies closer to $\frac{1}{384}N^2$ or to $\frac{1}{12}N^2$.

Remark 1.4: Selberg's eigenvalue conjecture states that for a modular curve $Y(\Gamma) := \Gamma\backslash\mathcal{H}$ associated to a congruence subgroup $\Gamma \subset PSL_2(\mathbb{Z})$, the least positive eigenvalue $\lambda_1$ of the hyperbolic Laplacian on $Y(\Gamma)$ satisfies $\lambda_1 \geq \frac{1}{4}$. Selberg himself showed $\lambda_1 \geq \frac{3}{16}$; in 1994, Luo, Rudnick and Sarnak showed $\lambda_1 \geq \frac{21}{100}$; this the bound we use in our unconditional estimate. As of this writing, the best known estimate on $\lambda_1$ is due to Kim and Sarnark: $\lambda_1 \geq \frac{975}{4096} > 0.238$. Thus the improvement in the upper bound of part a) gained by assuming Selberg's conjecture is small compared to the discrepancy between the upper bound of part a) and the lower bound of part b).

Application: For $N = 127$ the least degree of a rational CM point is 42, whereas – assuming Selberg's eigenvalue conjecture – the bound of Theorem 7a) gives that there are only finitely many points (if any, of course!) on $Y_1(127)$ of any smaller degree. For all larger $N \equiv 1 \pmod 3$, the set of points whose degree is less than or equal to the minimal degree of a CM point is finite.

On the other hand, Theorem 7b) guarantees that there are infinitely many points of degree less than the smallest CM point for $N \leq 13$. When $N = 17$ the bound ensures infinitely many points of degree at most 8, and the table above shows that the least degree of a rational CM point is 8. But in fact there exists a degree 4 map from $X_1(17)$ to the projective line, so that there are infinitely many rational points of degree at most 4. This suggests that there is room for improvement in the bound of Theorem 7b).

Finally we note that it is possible to show that if $N > 911$, there are only finitely many points of degree less than the least degree of a CM point on $X_1(N)$. This result may be found in Appendix A.

### 1.8. **Dramatis Personae and Acknowledgments.**

The 2007-2008 UGA VIGRE research group in number theory included:

Group leaders (year long):
Pete L. Clark (assistant professor), Patrick Corn (postdoc)
Graduate students (year long):
Steve Lane, Jim Stankewicz, Nathan Walters, Steve Winburn, Ben Wyser
Graduate students (spring semester only): Brian Cook
Undergraduate student (year long): Alex Rice.

Many of the participants were assigned specific subproblems which they wrote up formally and have been incorporated into this paper. Specifically, we wish to acknowledge the contributions of Steve Lane in computing Table 1, of Alex Rice in §2.4, of Jim Stankewicz in §5.1 and of Brian Cook in §8.

The first author would like to thank all the participants in the seminar for an enlightening and stimulating experience; this paper represents a substantial advancement of his prior work in this area, which would probably not have been done were it not for the interest and involvement of the students.

## 2. Background on elliptic curves and complex multiplication

2.1. **Some facts about elliptic curves with complex multiplication.** Let $E$ be an elliptic curve over any field $K$. The neutral point for the group law will be denoted by $O$. A $K$-rational endomorphism of $E$ is a morphism of $K$-varieties

$\varphi\colon E \to E$ such that $\varphi(O) = O$. Then $\varphi$ induces an endomorphism (i.e., self-homomorphism) on the group $E(L)$ of $L$-rational points, for any field extension $L$ of $K$. By definition, the **endomorphism ring** of $E$ is the set of all $\overline{K}$-rational endomorphisms of $E$, endowed with the structure of a ring under pointwise addition and composition. As for any ring, there is a natural homomorphism $\iota\colon \mathbb{Z} \to \mathrm{End}(E)$, in which the image of $n$ is the multiplication by $n$ map on $E$, traditionally denoted $[n]$.

In all cases $\varphi$ is an injection and $\mathrm{End}(E)$, as an abelian group, is a free $\mathbb{Z}$-module of rank 1, 2 or 4 [Sil86, §$III$.9]. When $\mathrm{End}(E)$ has rank 4, the endomorphism ring is noncommutative, an order in a definite rational quaternion algebra. Such an elliptic curve is said to be **supersingular**; supersingular elliptic curves over $K$ exist iff $K$ has positive characteristic. So if $K$ has characteristic 0, we have either $\mathrm{End}(E) = \mathbb{Z}$, or $\mathrm{End}(E) \cong \mathbb{Z}^2$ as a free abelian group; in the latter case $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ of an imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$, and "thus" we say that $E$ has **complex multiplication**. More precisely, we say $E$ has $\mathcal{O}$-CM if $\mathrm{End}(E) \cong \mathcal{O}$. Since the ring $\mathcal{O}$ has exactly one nontrivial automorphism – complex conjugation – if $\mathrm{End}(E) \cong \mathcal{O}$, there are two such isomorphisms.

Let $D_0$ be a **fundamental imaginary quadratic discriminant**, i.e., the discriminant of the full ring of integers of some imaginary quadratic field. More concretely, $D_0$ is a negative integer which is either (i) congruent to $1 \pmod 4$ and squarefree, or (ii) congruent to $0 \pmod 4$ and such that $\frac{D_0}{4}$ is squarefree. Put

$$\tau_{D_0} = \frac{D_0 + \sqrt{D_0}}{2}.$$

Every imaginary quadratic order $\mathcal{O}$ in $\mathbb{Q}(\sqrt{D_0})$ is of the form $\mathbb{Z}[f\tau_{D_0}]$ for a uniquely determined $f \in \mathbb{Z}^+$, the **conductor** of $\mathcal{O}$. Thus an order is determined by its fundamental discriminant $D_0$ – the discriminant of the full ring of integers of $\mathcal{O} \otimes \mathbb{Q}$ – and $f$. On the other hand, an order is also determined by its **discriminant** $D = f^2 D_0$. This means that for any imaginary quadratic discriminant $D$ – i.e., an integer $D$ with $D < 0$ and $D \equiv 0, 1 \pmod 4$ – there exists a unique (up to isomorphism) imaginary quadratic order $\mathcal{O}(D)$ of discriminant $D$.

For any integral domain $R$, one may consider its **Picard group** $\mathrm{Pic}(R)$, of rank one locally free $R$-modules under tensor product. Otherwise put, $\mathrm{Pic}(R)$ is the quotient of the group of invertible fractional $R$-ideals by the subgroup of principal $R$-ideals. The **class number** $h(R)$ is the cardinality of $\mathrm{Pic}(R)$. For an arbitrary domain $R$, the class number may well be infinite, but it is finite when $R$ is an order in any algebraic number field, so in particular when $R = R(n, d)$ is an imaginary quadratic order. When $R$ is a Dedekind domain all nonzero fractional ideals are invertible, and $\mathrm{Pic}(R) = \mathrm{Cl}(R)$ is the usual ideal class group.

We abbreviate $h(\mathcal{O}(D))$ to $h(D)$, and if $K = \mathbb{Q}(D_0)$ is an imaginary quadratic field, then the class number of $K$, denoted $h(K)$, means the class number of the maximal order $\mathcal{O}_K$ of $K$.

Until further notice we fix an imaginary quadratic order $\mathcal{O}(D)$, of discriminant $D$, and with quotient field $K = \mathbb{Q}(\sqrt{D_0})$.

**Fact 1.** *a) There exists at least one complex elliptic curve with $\mathcal{O}$-CM.*
*b) Let $E$, $E'$ be any two complex elliptic curves with $\mathcal{O}(D)$-CM. The $j$-invariants $j(E)$ and $j(E')$ are Galois conjugate algebraic integers. In other words, $j(E)$ is a root of some monic polynomial with $\mathbb{Z}$-coefficients, and if $P(t)$ is the minimal such polynomial, $P(j'(E)) = 0$ also.*
*c) Thus there is a unique irreducible, monic polynomial $H_D(t) \in \mathbb{Z}[t]$ whose roots are the $j$-invariants of the various non-isomorphic $\mathcal{O}(D)$-CM complex elliptic curves. We write $j_D$ for a root of this polynomial.*
*d) The degree of $H_D(t)$ is the class number $h(\mathcal{O}) = h(D)$ of the order $\mathcal{O}$, so when $\mathcal{O}$ is the full ring of integers of its quotient field $K$, $\deg(H_D(t)) = h(K)$, the class number of $K$.*
*e) Let $F_D := \mathbb{Q}[t]/H_D(t)$. Then $F_D$ can be embedded in the real numbers, so in particular is linearly disjoint from the imaginary quadratic field $K$. Let $K_D$ denote the compositum of $F_D$ and $K$. Then $K_D/K$ is abelian, with Galois group canonically isomorphic to $\operatorname{Pic}(\mathcal{O})$. Moreover, $K_D/\mathbb{Q}$ is Galois and the exact sequence*

$$1 \to \operatorname{Gal}(K_D/K) \to \operatorname{Gal}(K_D/\mathbb{Q}) \to \operatorname{Gal}(K/\mathbb{Q}) \to 1$$

*splits, i.e., $\operatorname{Gal}(K_D/\mathbb{Q})$ is up to isomorphism the semidirect product of $\operatorname{Pic}(\mathcal{O})$ with the cyclic group $Z_2$ of order 2, where the map $Z_2 \to \operatorname{Aut}(\operatorname{Pic}(\mathcal{O}))$ takes the nontrivial element of $Z_2$ to inversion: $x \mapsto x^{-1}$.*

References for this fact include: Cox [Cox89] and Silverman II [Sil94].

It follows from Fact 1 that one can define an $\mathcal{O}(D)$-CM elliptic curve over a number field $F$ iff $F \supset F_D$. In particular, one can define an $\mathcal{O}(D)$-CM elliptic curve over $\mathbb{Q}$ iff $h(D) = 1$, which by the Heegner-Baker-Stark theorem is known to occur for exactly 13 values of $D$:

$$D = -3, -4, -7, -8, -11, -12, -16, -27, -28, -19, -43, -67, -163.$$

Let $E\colon y^2 = x^3 + Ax + B$ be a complex elliptic curve in Weierstrass form. We define a **Weber function** $h$ on $E$, as:

$\mathfrak{h}(x, y) = x$ if $AB \neq 0$,
$\mathfrak{h}(x, y) = x^2$ if $B = 0$,
$\mathfrak{h}(x, y) = x^3$ if $A = 0$.

The point of the Weber function is to make explicit the quotient map $E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1$. See [Sil94, Ch. II] for more details.

If $E$ is defined over some subfield $K$ of $\mathbb{C}$, let $K(E[N])$ be the field extension of $K$ obtained by adjoining the coordinates of all the $N$-torsion points on $E$.

**Theorem 8** (Weber)**.** *Let $D$ be an imaginary quadratic discriminant, $K = \mathbb{Q}(\sqrt{D})$, and $E_{/\mathbb{C}}$ an $\mathcal{O}_K$-CM elliptic curve. For any positive integer $N$, the field $\mathbb{Q}(\sqrt{D}, j(E), \mathfrak{h}(E[N]))$ is the $N$-ray class field of $K$.*

*Proof.* See e.g., [Sil94, Thm. II.5.6]. □

**Corollary 9.** *Let $K = \mathbb{Q}(\sqrt{D_0})$ be an imaginary quadratic field, and let $E_{/F(D_0)}$ be an elliptic curve with $\mathcal{O}_K$-CM. Let $N$ be an odd prime and $D = N^2 D_0$. Then*

$$[K_D(\mathfrak{h}(E[N])) : K_D] =$$

$$[\mathbb{Q}(\sqrt{D_0}, j(E), \mathfrak{h}(E[N])) : \mathbb{Q}(\sqrt{D_0}, j(E))] = \left(\frac{N-1}{w(K)}\right)\left(N - \left(\frac{D_0}{N}\right)\right).$$

*Proof.* We deduce the corollary from the theorem using the description of the $N$-ray class field $K(N)$ of $K$ provided by class field theory. Namely, consider the $N$-**ring class field** $L(N)$, a subextension of $K(N)/K$. Recalling $D = N^2 \cdot D_0$, we have

$$\mathrm{Gal}(L(N)/K) \cong \mathrm{Pic}(\mathcal{O}(D)),$$

whereas

$$\mathrm{Gal}(K(N)/L(N)) \cong (\mathbb{Z}/N\mathbb{Z})^\times/\pm 1.$$

Recall the relative class number formula [Cox89, Thm. 7.24]

$$\frac{h(N^2D_0)}{h(D_0)} = \frac{N - \left(\frac{D_0}{N}\right)}{[\mathcal{O}_K^\times : \mathcal{O}^\times]},$$

Thus

$$[\mathbb{Q}(\sqrt{D_0}, j(E), \mathfrak{h}(E[N]) : \mathbb{Q}(\sqrt{D_0}, j(E))] = [K(N) : K(1)]$$

$$= \frac{[K(N) : K]}{[K(1) : K]} = \frac{h(N^2D_0)(N-1)}{2h(D_0)} = \frac{N-1}{w(K)} \cdot \left(N - \left(\frac{D_0}{N}\right)\right).$$

□

2.2. **The Galois representation.** Let $F$ be a field of characteristic 0, $E_{/F}$ an elliptic curve, and $N$ a positive integer. Let $\sigma \in \mathrm{Gal}_F = \mathrm{Aut}(\overline{F}/F)$. Let $E[N]$ be the set of $N$-torsion points on $E$ over $\overline{F}$; the action of $\mathrm{Gal}_F$ is seen to be $\mathbb{Z}/N\mathbb{Z}$-linear, so $E[N]$ may naturally be viewed as a $\mathbb{Z}/N\mathbb{Z}[\mathrm{Gal}_F]$-module. Recall that, as a $\mathbb{Z}/N\mathbb{Z}$-module, $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ [Sil86]. It is notationally convenient to choose such an isomorphism – i.e., to choose an ordered $\mathbb{Z}/N\mathbb{Z}$-basis $\{e_1, e_2\}$ of $E[N]$. The $\mathbb{Z}/N\mathbb{Z}[\mathrm{Gal}_F]$-module structure is then given by a homomorphism

$$\rho_N\colon \mathrm{Gal}_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

called the **mod N Galois representation** associated to $E$. Let $M = F(E[N])$ be the field extension obtained by adjoining to $F$ the $x$ and $y$ coordinates of all the $N$-torsion points. Then the kernel of $\rho_N$ is nothing else than $\mathrm{Gal}(\overline{F}/M) = \mathrm{Gal}_M$, so $\rho_N$ factors through to give an embedding

$$\rho_N\colon \mathrm{Gal}(M/F) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

There is "a piece" of $\rho_N$ which is well understood in all cases. Namely, composing with the determinant map $\det\colon \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^\times$, we get a homomorphism

$$\det(\rho_N)\colon \mathrm{Gal}(M/F) \to (\mathbb{Z}/N\mathbb{Z})^\times.$$

This homomorphism evidently cuts out an abelian extension of $F$, so can be viewed as a character of the group $\mathrm{Gal}(M/F)$. More precisely:

**Theorem 10.** *We have* $\det(\rho_N) = \chi_N$*, where* $\chi_N$ *is the mod* $N$ ***cyclotomic character****, defined as follows:*

$$\chi_N\colon \mathrm{Gal}_F \to \mathrm{Gal}(F(\zeta_N)/F) \to (\mathbb{Z}/N\mathbb{Z})^\times,$$

*where* $\alpha \in \mathrm{Gal}_F \mapsto \alpha \in \mathrm{Gal}(F(\zeta_N)/F)$*, an automorphism which is determined by its effect on a primitive* $N$*th root of unity:*

$$\zeta_N \mapsto \alpha(\zeta_N) = \zeta_N^{\chi_N(\alpha)},$$

*for a uniquely determined element* $\chi_N(\alpha) \in \mathbb{Z}/N\mathbb{Z}^\times$*.*

*Proof.* See [Sil86, Ch. III]. □

**Corollary 11.** *We have* $\det(\rho_N(\mathrm{Gal}_F)) = 1$ *iff* $F$ *contains the* $N$*th roots of unity.*

**Theorem 12** (Serre's Open Image Theorem, non-CM Case [S72])**.** *Let* $E$ *be an elliptic curve defined over a number field* $F$*, and suppose that* $E$ ***does not*** *have complex multiplication.*
*a) For all sufficiently large prime numbers* $\ell$*,* $\rho_\ell\colon \mathrm{Gal}_F \to GL_2(\mathbb{Z}/\ell\mathbb{Z})$ *is surjective.*
*b) There exists a fixed number* $B$ *such that for all* $N \in \mathbb{Z}^+$*,*

$$\#\operatorname{coker}(\rho_N) := \frac{\# GL_2(\mathbb{Z}/N\mathbb{Z})}{\#\rho_N(\mathrm{Gal}_F)} \leq B.$$

2.3. **Galois representation in the CM case.**

Our interest here is in the fact that this result fails in the presence of CM.

We assume that $N$ is an **odd prime**.

Suppose first that $E/F$ is a $\mathcal{O}(D)$-CM elliptic curve and that $F$ contains the CM field $K = \mathbb{Q}(\sqrt{D})$, so that the action of $\mathcal{O}(D)$ is defined and rational over $F$. Then, in additional to its $\mathbb{Z}/N\mathbb{Z}[\mathrm{Gal}_F]$-module structure, $E[N]$ also has the structure of an $\mathcal{O}(D)$-module. Morever, the $F$-rationality of the endomorphisms means precisely that for all $\sigma \in \mathrm{Gal}_F$ and $\varphi \in \mathcal{O}(D)$, we have $\sigma\varphi = \varphi\sigma$, i.e., the two actions commute with each other.[2] In fact, since $N = 0$ in $E[N]$, $E[N]$ is naturally a $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z} = \mathcal{O}(D)/N\mathcal{O}(D)$-module.

**Lemma 13.** *(*[Pari89, Lemma 1]*) The* $N$*-torsion group* $E[N]$ *is free of rank* 1 *as a (right)* $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z}$*-module, i.e., isomorphic to* $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z}$ *itself.*

In particular, the natural $\mathbb{Z}/N\mathbb{Z}$-linear action of $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z}$ on $E[N]$ is faithful, so we have an embedding of $\mathbb{Z}/N\mathbb{Z}$-algebras

$$\iota\colon \mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z} \hookrightarrow \operatorname{End}(E[N]) \cong M_2(\mathbb{Z}/N\mathbb{Z}).$$

Let us denote the image of $\iota$ by $C_N$. Now, for any $\sigma \in \mathrm{Gal}_F$, the matrix $\rho_N(\sigma)$ gives an invertible $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z}$-linear map of $E[N]$. Since the $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z}$-linear endomorphisms of the free one-dimensional module $E[N]$ are precisely multiplication by an element of $\mathcal{O}(D) \otimes \mathbb{Z}/N\mathbb{Z}$ and the invertible ones are elements of the unit group of this ring, we conclude

$$\rho_N(\mathrm{Gal}_F) \subset C_N^\times.$$

This shows that the CM case is much different, because the Galois extension $F(E[N])/F$ is in this case **abelian** and has size at most $\# C_N^\times$, or approximately $N^2$, whereas Serre's theorem asserts that in the non-CM case $\rho_N(\mathrm{Gal}_F)$ has, for sufficiently large prime $N$, size $\#\,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) = (N^2-1)(N^2-N) \sim N^4$.

To give more precise results, we must consider separately whether $N$ splits, stays inert or ramifies in $\mathcal{O}(D)$.

Case 1 (split case): $(\frac{D}{N}) = 1$. Then one sees (e.g., by direct computation) that

[2] This can be expressed more concisely as the fact that $E[N]$ is a $(\mathbb{Z}/N\mathbb{Z}[\mathrm{Gal}_F], \mathcal{O}(D))$-bimodule, but we find no particular advantage to using this terminology here.

$C_N$, as an $\mathbb{F}_N$-algebra, is isomorphic to $\mathbb{F}_N \oplus \mathbb{F}_N$; therefore the unit group $C_N^\times$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times \oplus (\mathbb{Z}/N\mathbb{Z})^\times$. Thus there are precisely two one-dimensional subspaces $V_1$, $V_2$ of $E[N]$ which are simultaneous eigenspaces for $C_N$. By taking generators $e_1$ of $V_1$ and $e_2$ of $V_2$ as basis, we get

$$C_N \cong \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{F}_N \right\}.$$

The same considerations show that there is, up to conjugacy, a unique subalgebra of $M_2(\mathbb{F}_N)$ isomorphic to $\mathbb{F}_N \oplus \mathbb{F}_N$; such an algebra is called a **split Cartan subalgebra** and its unit group a **split Cartan subgroup**.

Case 2 (inert case): $(\frac{D}{N}) = -1$. Then one sees that $C_N \cong \mathbb{F}_{N^2}$, a finite field of order $N^2$, so that $C_N^\times$ is cyclic of order $N^2 - 1$. Again ones sees that $\mathbb{F}_{N^2}$ is unique up to conjugacy as a subalgebra of $M_2(\mathbb{F}_N)$ (e.g., the result is a special case of the Skolem-Noether theorem on simple subalgebras of central simple algebras; or just do a direct computation). Such an algebra is called a **nonsplit Cartan subalgebra** and the unit group is called a **nonsplit Cartan subgroup**.

Case 3 (ramified case): $N$ divides $D$. Then $C_N \cong \mathbb{F}_N[t]/(t^2)$, i.e., is generated over the center (the scalar matrices) by a single nilpotent matrix $g$. Since the eigenvalues of $g$ are $\mathbb{F}_N$-rational, we can put $g$ in Jordan canonical form, and this gives a choice of basis such that

$$C_N \cong \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{F}_N \right\}.$$

Again $C_N$ is unique up to conjugacy; for lack of a better name, we shall call it a **pseudo-Cartan subalgebra**. Evidently $C_N^\times \cong Z_{N-1} \oplus Z_N \cong Z_{N^2-N}$.

We now introduce a third operator on $E[N]$. By Fact 1 above, we can choose an embedding of $K_D$ into $\mathbb{C}$ which carries $\mathbb{Q}(j_D)$ into the real numbers. Then complex conjugation $c$ induces a $\mathbb{Z}/N\mathbb{Z}$-linear automorphism of $E[N]$.

**Lemma 14.** *Let $N \in \mathbb{Z}^+$ be odd. The characteristic polynomial of complex conjugation acting on the $\mathbb{Z}/N\mathbb{Z}$-module $E[N]$ is $t^2 - 1$.*

*Proof.* Clearly $c$ satisfies the polynomial $t^2 - 1$, so we must show $c \neq \pm 1$. If $c = 1$ then $c$ acts trivially on each $N$-torsion point and we would have $\dim_{\mathbb{Z}/N\mathbb{Z}} E[N](\mathbb{R}) = 2$. If $c = -1$ then (since $N$ is odd), $c$ acts nontrivially on each $N$-torsion point, and we would have $\dim_{\mathbb{Z}/N\mathbb{Z}} E[N](\mathbb{R}) = 0$. But in fact $\dim_{\mathbb{Z}/N\mathbb{Z}} E[N](\mathbb{R}) = 1$: the one-dimensional compact real Lie group $E(\mathbb{R})$ is isomorphic either to $S^1$ (if a Weierstrass cubic has one real root) or to $S^1 \times \mathbb{Z}/2\mathbb{Z}$ (if all 2-torsion points (if a Weierstrass cubic has three real roots), and either way $E[N](\mathbb{R}) \cong \mathbb{Z}/N\mathbb{Z}$. □

**Lemma 15.** *Let $D$ be an imaginary quadratic discriminant, $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field, $F$ a number field, and $E_{/F}$ a $K$-CM elliptic curve. Suppose that $N$ is an odd prime which does not ramify in $K$. Then:*
*a) We have $F(E[N]) \supset \mathbb{Q}(\sqrt{D})$.*
*b) For any $\mathcal{O}(D)$-CM elliptic curve $E/\mathbb{Q}(j_D)$, we have $\mathbb{Q}(j_D, E[N]) \supset \mathbb{Q}(\sqrt{D})$.*

*Proof.* Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field, let $F$ be a number field, and let $E_{/F}$ be a $K$-CM elliptic curve. Let $\rho_N^\infty \colon \operatorname{Gal}_F \to \operatorname{Aut}(T_N E)$ be the $N$-adic

Galois representation on $E/F_D$, and let $\mathcal{G}_N$ be its image. By [S66, Thm. 5], $\mathcal{G}_N$ is commutative iff $\mathbb{Q}(\sqrt{D}) \subset F$. If $\mathbb{Q}(\sqrt{D}) \subset F$ then part a) holds trivially, so assume otherwise and hence that $\mathcal{G}_N$ is not commutative but has an index 2 commutative subgroup $\mathcal{H}$, namely the image of $\rho_{N^\infty}$ restricted to $F(\sqrt{D})$. Thus when we adjoin to $F$ the coordinates of all $N$-power torsion points, we get $\mathbb{Q}(\sqrt{D})$. However, the Galois group $F(E[N^\infty])/F(E[N]))$ is a pro-$N$-group so contains no elements of order 2. Therefore we must have gained the quadratic extension $F(\sqrt{N})/F$ by adjoining the $N$-torsion, establishing part a). Part b) follows immediately. $\square$

There is also a natural nontrivial action of complex conjugation on $\mathcal{O}(D)$, and the homomorphism $\iota\colon \mathcal{O}(D) \to \mathrm{End}(E[N])$ is $c$-equivariant: $\iota \circ c = c \circ \iota$. This, together with the nontriviality of the $c$-action on $\mathcal{O}(D)$, is equivalent to the fact that conjugation by $c$ stabilizes $C_N$ and induces a nontrivial involution on it.

In the split case we find that, with respect to the chosen basis $e_1$, $e_2$ of $C_N$-eigenspaces, $c$ is equal to either permutation matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ or its negative. Either way, the effect of conjugation by $c$ is $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mapsto \begin{bmatrix} b & 0 \\ 0 & a \end{bmatrix}$. Explicit computation shows that the Cartan subgroup $C_N^\times$ has index 2 in its normalizer $N(C_N^\times)$.

In the inert case, conjugation by $c$ stablizes $C_N \cong \mathbb{F}_{N^2}$ and induces the unique nontrivial Galois automorphism, the Frobenius map: $\mathrm{Frob}_N\colon x \mapsto x^N$. The elements of $N(C_N^\times) \setminus C_N^\times$ correspond to $\mathrm{Frob}_N$-semilinear automorphisms of the 1-dimensional $\mathbb{F}_{N^2}$-vector space $V = E[N]$, i.e., maps $\sigma\colon V \to V$ such that for $v, w \in V$, $\sigma(vw) = \mathrm{Frob}_N(v)\sigma(w)$. Such a map is uniquely specified by $\sigma(1)$, so that $\# N(C_N^\times) \setminus C_N^\times = N^2 - 1$, i.e., $[N(C_N^\times) : C_N^\times] = 2$.

In the ramified case, complex conjugation induces a nontrivial involution of the (non-semisimple) $\mathbb{F}_N$-algebra $C_N \cong \mathbb{F}_N[t]/(t^2)$. The automorphism group $\mathrm{Aut}(C_N/\mathbb{F}_N)$ is isomorphic to $Z_{N-1}$ so has a unique element of order 2, $t \mapsto -t$. Therefore conjugation by $c$ has the effect $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mapsto \begin{bmatrix} a & -b \\ 0 & a \end{bmatrix}$. Note that this case is different from the previous two in that the normalizer of $C_N^\times$ is the entire Borel subgroup $\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \mid a, b, c \in \mathbb{F}_N, ac \neq 0\}$.

Given all this, one readily deduces the following result:

**Theorem 16.** *Let $F$ be a number field, and $E_{/F}$ an elliptic curve with $\mathcal{O}(D)$-CM. Let $M = F(E[N])$ be the field extension of $F$ obtained by adjoining $x$ and $y$ coordinates of all the $N$-torsion points of $E$.*
*a) The CM field $K = \mathbb{Q}(\sqrt{D})$ is contained in $M$, so we get a short exact sequence*

$$1 \to \mathrm{Gal}(M/KF) \to \mathrm{Gal}(M/F) \to \mathrm{Gal}(KF/F) \to 1. \tag{8}$$

*b) Under the natural embedding $\rho_N\colon \mathrm{Gal}(M/F) \hookrightarrow GL_2(\mathbb{F}_N)$, the subgroup $\mathrm{Gal}(M/KF)$ embeds in the unit group $C_N^\times$.*
*c) The sequence (8) splits, with a splitting given by a choice of an involution $c \in N(C^\times) \setminus C^\times$.*

This result gives upper bounds on the the degree $[F(E[N]) : F]$ which improve upon the obvious bound of $\# \mathrm{GL}_2(\mathbb{F}_N)$:

**Corollary 17.** *a) If* $(\frac{D}{N}) = 1$*, then* $[F(E[N]) : F] \mid 2(N-1)^2$.
*b) If* $(\frac{D}{N}) = -1$*, then* $[F(E[N]) : F] \mid 2(N^2-1)$.
*c) If* $(\frac{D}{N}) = 0$*, then* $[F(E[N]) : F] \mid 2(N^2-N)$.

*Proof.* Using the exact sequence (8) we see that

$$\# \mathrm{Gal}(M/F) = \# \mathrm{Gal}(M/KF) \cdot \# \mathrm{Gal}(K/F) \mid \#(C_N)^{\times} \cdot 2.$$

And we know that $C_N^{\times}$ has order $(N-1)^2$, $(N^2-1)$ or $N^2-N$ according to whether $N$ splits, is inert, or is ramified in $\mathcal{O}(D)$. □

The slogan is that the image of the Galois representation $\rho_N$ should be "as large as possible", up to a factor which is uniformly bounded as $N$ varies. But in the CM case $GL_2(\mathbb{F}_N)$ is impossibly large. The correct answer is again due to Serre:

**Theorem 18.** *(Open Image Theorem, CM case* [S72, §4.5]*) Let $F$ be a number field and $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve. For all sufficiently large primes $N$:*
- $\rho_N(\mathrm{Gal}_F)) = N(C_N)$*, if* $K = \mathbb{Q}(\sqrt{D})$ *is not contained in* $F$,
- $\rho_N(\mathrm{Gal}_F) = C_N^{\times}$*, if* $K \subset F$.

Since Theorem 18 only holds for sufficiently large primes $N$, the case of $N \mid D$ can be completely ignored. Nevertheless Theorem 18 tells us to "expect" that the $N$-torsion fields will be as large as possible. In the next section we use elementary group theory to deduce consequences for the least degree of an $N$-torsion point.

## 2.4. Orbits under $C_N^{\times}$ and applications.

We maintain the notation of the previous section: $E_{/F}$ is an elliptic curve with $\mathcal{O}(D)$-CM, $N$ is an odd prime number, $C_N = \iota(\mathcal{O} \otimes \mathbb{Z}/N\mathbb{Z}) \subset \mathrm{End}(E[N])$, $C_N^{\times}$ is the unit group of $C_N$, and $N(C_N^{\times})$ is its normalizer.

**Lemma 19.** *a) The orbits of $C_N^{\times}$ on $E[N] \setminus \{0\}$ are as follows:*
*(i) If $(\frac{D}{N}) = 1$, the two one-dimensional eigenspaces for $C_N$ give two orbits of size $N-1$; all the remaining points lie in a single orbit of size $(N-1)^2$.*
*(ii) If $(\frac{D}{N}) = -1$, $E[N] \setminus \{0\}$ forms a single $C_N^{\times}$-orbit.*
*(iii) If $(\frac{D}{N}) = 0$, the unique one-dimensional eigenspace for $C_N$ gives an orbit of size $N-1$; the remaining points form a single orbit of size $N^2-N$.*
*b) If $(\frac{D}{N}) = 1$, the two orbits of size $N-1$ for $C_N^{\times}$ form a single orbit for $N(C_N^{\times})$.*

*Proof.* This is a pleasant elementary computation that we leave to the reader. □

In the statement of the following result we employ the following convention: if $p$ and $q$ are nonzero rational numbers, we say $p \mid q$ if $\frac{q}{p} \in \mathbb{Z}$.

**Corollary 20.** *Let $E_{/F}$ be an $\mathcal{O}(D)$-CM elliptic curve defined over a number field $F$. Suppose that the image $\rho_N(\mathrm{Gal}_{KF})$ of the mod $N$ Galois representation has index $I$ in $C_N^{\times}$. Let $P \in E(\mathbb{C})$ be any point of exact order $N$, and let $F(P)$ be the extension of $F$ obtained by adjoining the coordinates of $P$.*
*(i) If $(\frac{D}{N}) = 1$ and $\sqrt{D} \in F$, then $\frac{1}{I}(N-1) \mid [F(P) : F]$*
*(ii) If $(\frac{D}{N}) = 1$ and $\sqrt{D}$ is not in $F$, then $\frac{2}{I}(N-1) \mid [F(P) : F]$.*

*(iii) If* $(\frac{D}{N}) = -1$*, then* $\frac{1}{I}(N^2-1) \mid [F(P):F]$.
*(iv) If* $(\frac{D}{N}) = 0$*, then* $\frac{1}{I}(N-1) \mid [F(P):F]$.

*Proof.* Consider the tower of field extensions $F \subset F(P) \subset F(E[N])$. Then $F(E[N])/F(P)$ is Galois, with Galois group canonically isomorphic to $\rho_N(\mathrm{Gal}_F) \cap G(P)$, where $G(P) \subset \mathrm{GL}_2(\mathbb{F}_N)$ is the stabilizer of the point $P$. By the orbit-stabilizer theorem, $[F(P):F]$ is equal to the orbit of $P$ under the action of $\mathrm{Gal}_F$.

In case (i) we have $\sqrt{D} \in F$, so that the image of Galois lies in the split Cartan subgroup $C_N^\times \cong \mathbb{F}_N^\times \oplus \mathbb{F}_N^\times$. By Lemma 19 the full $C_N^\times$-orbits have sizes $N-1$ and $(N-1)^2$. Since we are assuming that $[C_N^\times : \rho_N(\mathrm{Gal}_F)] \mid I$, it follows that every $\rho_N(\mathrm{Gal}_F)$-orbit has size a multiple of $\frac{N-1}{I}$. Case (ii) is similar except in this case replace the gcd of all sizes of $C_N^\times$ orbits with the gcd of all sizes of $N(C_N^\times)$-orbits, which according to Lemma 19 is $2(N-1)$. Parts (iii) and (iv) are similar, except here it does not matter whether $\sqrt{D}$ lies in the ground field $F$: in case (iii) this is because the orbit size for $C_N^\times$ is already as large as possible; in case (iv) this is because the minimal $C_N^\times$-orbit is stable under complex conjugation. □

## 3. Proof of Theorem 1

a) Theorem 1a) is precisely the $D = -3$ case of Theorem 3a). Indeed, for $D = -3$, $w(D) = 6$, and an odd prime splits completely in $\mathbb{Q}(\sqrt{-3})$ iff $N \equiv 1 \pmod 3$.
b) Suppose we have an $\mathcal{O}(D)$-CM point on $X_1(N)$ of degree $D$.
Case 1 ($D = -3$): By Theorem 3, if $N$ is greater than or equal to some absolute constant $N_1$, we have $d \geq \frac{N-1}{3}$ if $N \equiv 1 \pmod 3$ and $d \geq \frac{N^2-1}{6}$ if $N \equiv -1 \pmod 3$.
Case 2 ($D = -4$): We have $w(-4) = 4$, and then Theorem 3 says that for $N$ greater than or equal to another absolute constant $N_2$, we have $d \geq \frac{N-1}{2}$ if $N \equiv 1 \pmod 4$ and $d \geq \frac{N^2-1}{4}$ if $N \equiv -1 \pmod 4$.
Case 3 ($D < -4$): We have $w(D) = 2$, and then by the Theorem of Silverberg and Prasad-Yogananda, $d \geq \frac{N-1}{2}$. Altogether we see that if $N \geq \max(5, N_1, N_2)$ then $d \geq \frac{N-1}{3}$ in all cases, equality can be met iff $N \equiv 1 \pmod 3$ (necessarily for an $\mathcal{O}(-3)$-CM elliptic curve of $j$-invariant 0). Moreover, the next smallest possible degree is $\frac{N-1}{2}$, for an $\mathcal{O}(-4)$-CM elliptic curve of $j$-invariant 1728, a bound which can be attained iff $N \equiv 1 \pmod 4$. In all other cases, the degree is at least $N-1$. This completes the proof of Theorem 1.

## 4. Proof of Theorem 2

Let $N$ be an odd prime number; let $D$ be a fundamental imaginary quadratic discriminant, $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field; and let $E_{/F}$ be an $\mathcal{O}_K$-CM elliptic curve. Suppose that there exists a point $P \in E(F)$ of order $N$.

Split case: $(\frac{D}{N}) = 1$. We may assume $K \subset F$ and show $\frac{2h(K)(N-1)}{w(K)} = \frac{[K(1):\mathbb{Q}](N-1)}{w(K)} \mid [F:\mathbb{Q}]$, or equivalently, $\frac{N-1}{w(K)} \mid [F:K(1)]$. Using Lemma 19, let $Q \in E(\mathbb{C})$ be a point of order $N$ lying in a one-dimensional eigenspace having Galois orbit of size dividing $N-1$ and linearly independent from $P$, so $[F(Q):F] \mid N-1$ and thus $[F(Q):K(1)] \mid (N-1)[F:K(1)]$. Since $F(Q)$ contains $P$ and $Q$, it contains

$\mathfrak{h}(E[N])$, and thus

$$\frac{(N-1)^2}{w(K)} = [K(1)\mathfrak{h}(E[N]) : K(1)] \mid [F(Q) : K(1)] \mid (N-1)[F : K(1)],$$

so indeed $\frac{N-1}{w(K)} \mid [F : K(1)]$.

Inert case: $(\frac{D}{N}) = -1$. We may assume $K \subset F$ and show $\frac{2h(K)(N^2-1)}{w(K)} = \frac{[K(1):\mathbb{Q}](N-1)}{w(K)} \mid [F : \mathbb{Q}]$, or equivalently, $\frac{N^2-1}{w(K)} \mid [F : K(1)]$.

In this case, by Corollary 20(iii), as soon as there is one $N$-torsion point we have $I = N^2 - 1$ and the Galois action is trivial. By Corollary 9, we get

$$\frac{N^2-1}{w(K)} = [K(1)\mathfrak{h}(E[N]) : K(1)] \mid [F : K(1)].$$

## 5. Proof of Theorem 3

### 5.1. **A technical lemma.**

Let $w$ be a positive even integer, and let $\zeta = \zeta_w = e^{2\pi i/w}$ be a primitive $w$th root of unity. Let $G = \langle \sigma \mid \sigma^w = 1 \rangle$ be a cyclic group of order $w$. Let $M$ be an abelian group endowed with the following additional structures:

- a $\mathbb{Z}$-linear action of $G$, and
- A ring homomorphism $\mathbb{Z}[\zeta] \to \mathrm{End}(M)$.

We require first that $\zeta^{\frac{w}{2}} \cdot x = -x$ for all $x \in M$. We also require that these two actions commute with each other: for all $x \in M$, $\zeta\sigma x = \sigma\zeta x$.

For $i \in \mathbb{Z}/w\mathbb{Z}$, we define $M_i = \{x \in M \mid \sigma x = \zeta^i x\}$, and

$$\mathbf{M} = \bigoplus_{i \in \mathbb{Z}/w\mathbb{Z}} M_i.$$

Consider the $\mathbb{Z}$-module homomorphism $\Phi \colon \mathbf{M} \to M$ given $(x_i) \mapsto \sum_i x_i$. Let $\tilde{\Phi} = \Phi \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{w}] \colon \mathbf{M}' = \mathbf{M} \otimes \mathbb{Z}[\frac{1}{w}] \to M' = M \otimes \mathbb{Z}[\frac{1}{w}]$.

**Lemma 21.** *Both* $\ker(\Phi)$ *and* $\mathrm{coker}(\Phi)$ *are $w$-torsion $\mathbb{Z}$-modules. It follows that:*
*a) The map $\tilde{\Phi}$ is an isomorphism of $\mathbb{Z}[\frac{1}{w}]$-modules.*
*b) We have* $\dim_{\mathbb{Q}}(\boldsymbol{M} \otimes \mathbb{Q}) = \dim_{\mathbb{Q}}(M \otimes \mathbb{Q})$*, and for any prime $p$ not dividing $w$, $\Phi$ induces an isomorphism from the $p$-primary torsion subgroup $\boldsymbol{M}[p^\infty]$ of $\boldsymbol{M}$ to the $p$-primary torsion subgroup $M[p^\infty]$ of $M$.*

*Proof.* It is enough to show that the kernel and cokernel of $\Phi$ are $w$-torsion; for if so, tensoring the short exact sequences

$$0 \to \ker(\Phi) \to \mathbf{M} \xrightarrow{\Phi} \Phi(\mathbf{M}) \to 0$$

and

$$0 \to \mathbf{M}/\ker(\Phi) \xrightarrow{\Phi} M \to \mathrm{coker}(\Phi) \to 0$$

of $\mathbb{Z}$-modules with the flat $\mathbb{Z}$-module $\mathbb{Z}[\frac{1}{w}]$ shows that $\tilde{\Phi}$ is an isomorphism.

Step 1: We show $\ker(\Phi) = \ker(\Phi)[w]$. Let $P = (P_0, \ldots, P_{w-1})$ be an element of $\ker \Phi$, so that

$$P_0 + \cdots + P_{w-1} = 0.$$

Applying $\sigma$, we obtain

$$P_0 + \zeta P_1 + \cdots + \zeta^{w-1} P_{w-1} = 0.$$

Applying $\sigma$ $w-2$ more times, we arrive at the matrix equation $AP = 0$, where

$$A = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \zeta & \ldots & \zeta^{w-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{w-1} & \ldots & \zeta^{(w-1)(w-1)} \end{pmatrix}.$$

It is therefore also a solution to $A^2 P = 0$, where

$$A^2 = \begin{pmatrix} w & 0 & \ldots & \ldots & 0 \\ 0 & 0 & \ldots & 0 & w \\ \vdots & \vdots & \iddots & w & 0 \\ \vdots & 0 & \iddots & \iddots & \vdots \\ 0 & w & 0 & \ldots & 0 \end{pmatrix}.$$

Thus $wP_0 = wP_{w-1} = \cdots = wP_1 = 0$, i.e., $wP = 0$.

Step 2: We show $\operatorname{coker}(\Phi) = \operatorname{coker}(\Phi)[w]$. Let $P \in M$. Define a $w \times w$ matrix

$$B = \begin{pmatrix} P & \sigma(P) & \sigma^2(P) & \ldots & \sigma^{w-1}(P) \\ P & \zeta^{-1}\sigma(P) & \zeta^{-2}\sigma^2(P) & \ldots & \zeta^{-(w-1)}\sigma^{w-1}(P) \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ P & \zeta^{-(w-1)}\sigma(P) & \zeta^{-2(w-1)}\sigma^2(P) & \ldots & \zeta^{-(w-1)(w-1)}\sigma^{w-1}(P) \end{pmatrix}.$$

Notice that the sum of all the entries of $B$ is $wP$: indeed, this is the sum of the entries in the first column, and since for any $j \neq 0 \pmod{w}$ we have $\sum_{i=1}^{w-1} \zeta^{-ji} = 0$, each of the other columns sums to 0. Now for $1 \leq i \leq w$, put

$$P_{i-1} = \sum_{k=0}^{w-1} \zeta^{-ki} \sigma^k(P).$$

Then

$$\sigma(P_{i-1}) = \sum_{k=0}^{w-1} \zeta^{-ki} \sigma^{k+1}(P) = \zeta^i \sum_{k=0}^{w-1} \zeta^{-(k+1)i} \sigma^{k+1}(P) = \zeta^i P_{i-1},$$

so $P_{i-1} \in M_i$. Therefore

$$wP = \Phi((P_0, \ldots, P_{w-1})) \in \Phi(\mathbf{M}).$$

$\square$

5.2. **Application to the proof of Theorem 3.**

Now let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D$, $K = \mathbb{Q}(\sqrt{D})$, and let $N > w = w(\mathcal{O})$ be a prime which splits in $K$. Let $K_D = K(j_D)$, and let $E/K_D$ be an $\mathcal{O}$-CM elliptic curve. By the work of §2.3, we know that there exists an extension $K_D(P)/K_D$, which is cyclic of degree dividing $N-1$, such that over $K_D(P)$ $E$ has a point $P$ of exact order $N$. Let us first assume that $[K_D(P) : K_D] = N-1$; afterwards we will discuss how to modify the argument to deal with the case in which the degree strictly divides $N-1$.

Our assumptions imply that $N \equiv 1 \pmod{w}$. Therefore, by Galois theory, there exists a unique subextension $K_D \subset L \subset K_D(P)$ with $G = \mathrm{Gal}(K_D(P)/L)$ cyclic of order $w$. Now we are in the setup of the previous section: take $M = E(K_D(P))$; the $G$-action is the restriction of the natural $\mathrm{Gal}(M/K_D)$-action on $E(K_D(P))$, the $\mathbb{Z}[\zeta]$-action coming from the fact that $\mathcal{O} = \mathrm{End}(E)$ contains the $w$th roots of unity, and the compatibility of these two actions is a consequence of the rationality of the endomorphisms over $K_D$ (hence also over $L$). Since $E(K_D(P))$ contains a point whose order is a prime $N$ not divisible by $w$, by Lemma 21 there exists some $i \in \mathbb{Z}/w\mathbb{Z}$ such that $M_i$ contains an element of order $N$.

Using the theory of twisting in the Galois cohomology of elliptic curves, we may interpret $M_i$ as the group of $L$-rational points on a $K_D(P)/L$-twisted form of the elliptic curve $E$. Specifically, the set of such twisted forms are parameterized by

$$H^1(\mathrm{Gal}(K_D(P)/L), \mathrm{Aut}(E)) = \mathrm{Hom}(G, \mathbb{Z}/w\mathbb{Z}) \cong \mathbb{Z}/w\mathbb{Z},$$

the last isomorphism being given by

$$(\varphi\colon G \to \mathbb{Z}/w\mathbb{Z}) \mapsto \zeta^{i_\varphi} = \varphi(\sigma).$$

Corresponding to $\zeta^i = \zeta^{i_\varphi} \in \mathbb{Z}/w\mathbb{Z}$ we build a twisted $\mathrm{Gal}(K_D(P)/L)$-action on $E(K_D(P))$:

$$\sigma \cdot_i x := \zeta^{-i}\sigma x.$$

This is exactly the relation defining $M_i$. In other words, the abstract decomposition of the $\mathbb{Z}[\frac{1}{w}]$-module $\mathbf{M'} \xrightarrow{\sim} M'$ corresponds to a decomposition of the Mordell-Weil group – up to $w$-torsion – of $E(K_D(P))$ into a direct sum of the Mordell-Weil groups of the $w$ different twists of $E_{/L}$ via the cyclic extension $K_D(P)/L$ and the automorphism group of $E$. (When $w = 2$, this result – decomposition of the Mordell-Weil group under a quadratic extension – is very well known.) Thus we have produced an $\mathcal{O}$-CM elliptic curve over a field of degree $\frac{2(N-1)}{w(\mathcal{O})}$ with a rational $N$-torsion point, giving the statement of Theorem 3a).

It remains to deal with the case in which $d = [K_D(P) : K]$ strictly divides $N-1$. If $w \mid d$, we can run through the above argument verbatim, getting in fact an $\mathcal{O}$-CM elliptic curve with a rational $N$-torsion point over a field of degree $\frac{2d}{w}$, which is *a priori* stronger than what we are trying to prove. This necessarily is the case if $w = 2$. If $w = 4$ and $d$ is a multiple of 2 but not a multiple of 4, we run through the above argument using quadratic twists instead of quartic twists. If $w = 6$ and $d$ is a multiple of 2 but not of 6, then we run through the above using quadratic twists instead of sextic twists. One sees easily that we get exactly the same bounds. This completes the proof of Theorem 3a).

Proof of Theorem 3b): Suppose first that $N$ is an odd prime with $(\frac{D}{N}) = 1$. Let

$F_D = \mathbb{Q}(j(E)) = \mathbb{Q}(j_D)$ be the number field generated by the j-invariant of the quadratic order $\mathcal{O}(D)$, and let $E_{/F_D}$ be any $\mathcal{O}(D)$-CM elliptic curve. Serre's Theorem 18 says that there exists $N_0 = N_0(D)$ such that if $N \geq N_0$, the image $\rho_N(\mathrm{Gal}_{F_D})$ in $\mathrm{GL}_2(\mathbb{F}_N)$ will be $N(C_N^{\times})$, the normalizer of a split Cartan subgroup, and then Corollary 20 applies to show that the least degree $[F_D(P) : F_D]$ is a multiple of $2(N-1)$.

Now suppose that we have any number field $F$, $E'_{/F}$ an $\mathcal{O}(D)$-CM elliptic curve with an $F$-rational point of prime order $N \geq N_0$. The theory of twisting – together with the Kummer isomorphism $H^1(\mathrm{Gal}_F, \mu_d) \cong F^{\times}/F^{\times d}$ – implies first that $F \supset F_D$, and second that there exists an extension $L$ of $F$, of degree $w(\mathcal{O})$ such that $E_{/L} \cong E'_{/L}$. Therefore, since $E'$ has an $F$-rational torsion point of order $N$, $E$ has an $L$-rational torsion point of order $N$, so

$$2(N-1) \mid [F_D : \mathbb{Q}] \mid [L : F_D][F_D : \mathbb{Q}] = [L : \mathbb{Q}] = [L : F][F : \mathbb{Q}] = w(\mathcal{O})[F : \mathbb{Q}],$$

and hence

$$\frac{2(N-1)}{w(\mathcal{O})} \mid [F : \mathbb{Q}].$$

The argument in the case $(\frac{D}{N}) = -1$ is quite similar: then there exists $N_0$ such that $N \geq N_0$ implies that, for our fixed $E_{/F_D}$ as above we have $[F_D(P) : F_D] = N^2 - 1$ (note that this is the order of the stabilizer of $P$ in all of $GL_2(\mathbb{F}_N)$, hence the largest possible order, so there is no further contribution coming from the action of complex conjugation) and arguing as before we get

$$\frac{N^2-1}{w(\mathcal{O})} \mid [F : \mathbb{Q}].$$

Since we are taking $N$ to be sufficiently large compared to $D$, we do not have to worry about the ramified case.

## 6. Proof of Theorem 4

For a negative quadratic discriminant $D$, write $d_D(N)$ for the least degree of an $\mathcal{O}(D)$-CM point on $X_1(N)$, and $d_{\mathrm{CM}}(N)$ for the least degree of a CM point on $X_1(N)$, so $d_{\mathrm{CM}}(N) = \min_D d_D(N)$.

We will need the following two estimates:

**Lemma 22.** *Suppose $D$ is a negative integer and $N$ a prime, with $(\frac{D}{N}) = 1$. Then there exists a CM point on $X_1(N)$ of degree dividing $2(N-1)h(\mathbb{Q}(\sqrt{D}))$.*

*Proof.* this is an immediate consequence of the theory of Galois representations on CM elliptic curves as recalled in §2.3. □

**Lemma 23.** *As $D$ tends to $-\infty$ through quadratic discriminants, the class number $h(D)$ of the imaginary order of discriminant $D$ is $O(\sqrt{|D|}\log|D|)$.*

*Proof.* Combine Dirichlet's class number formula (e.g. [D, p. 49])

$$h(D) = \frac{w(K)\sqrt{|D|}}{2\pi} L(1, \chi_D)$$

with the estimate (e.g. [Hu, Ch. 2]) $|L(1, \chi_D)| \leq \log(\sqrt{|D|}) + 1$. □

Proof of Theorem 4: If $N \equiv 1 \pmod 4$, by Theorem 3 we have $d_{\mathrm{CM}}(N) \leq \frac{N-1}{2}$. This is stronger than the bounds we are claiming for arbitrary $N$, so we may assume that $N \equiv -1 \pmod 4$.

For such $N$, let $D$ be a negative quadratic discriminant not divisible by $N$. Then

$$1 = \left(\frac{D}{N}\right) \iff \left(\frac{|D|}{N}\right) = -1,$$

so we are interested in the least positive integer $M$ which is first, a quadratic nonresidue modulo $N$ and second, is congruent to 0 or $-1$ modulo 4, so that $-M$ is an imaginary quadratic discriminant.

In fact this latter condition is nothing to worry about: let $M$ be the least positive quadratic nonresidue modulo $N$. Then certainly $M$ is squarefree, so $M$ is not $0 \pmod 4$. If $M \equiv -1 \pmod 4$, then $D = -M$ is the discriminant of $\mathbb{Q}(\sqrt{-M})$. If $M \equiv 1, 2 \pmod 4$, then it is not $-M$ but $-4M$ which is the discriminant of $\mathbb{Q}(\sqrt{-M})$. But if $M$ is a quadratic nonresidue modulo the odd prime $N$, so is $4M$, and if we know that $M = O(f(N))$ for some function $f$, then of course the same holds for $4M$.

Remark 6.1: The order of the least quadratic nonresidue modulo $N$ is a famous classical problem. The trivial bound – taking into account only that there are in all $\frac{N-1}{2}$ quadratic nonresidues – is $\frac{N}{2}$, but a bit of thought and experimentation suggests that $M$ should be considerably smaller than this. Long ago Vinogradov conjectured that $M = O_\epsilon(N^\epsilon)$, i.e., that $M$ grows more slowly than any power of $N$, but we are still far away from an unconditional proof of this. In 1952 N.C. Ankeny showed that, **conditionally** on GRH, $M = O((\log N)^2)$ [Ank52]. In his review of this paper [Erd52], P. Erdős remarks that it is known that $M$ is *not* $O(\log N)$, so that Ankeny's bound seems to get admirably close to the truth. Vinogradov himself was able to show unconditionally that $M = o(N)$; for more than fifty years, the best unconditional bound has been due to D.A. Burgess: $M = O_\epsilon(N^{c+\epsilon})$, where $c = \frac{e^{-1/2}}{4} = 0.15\ldots$ is "Burgess's constant" [Bur57].

So, for an odd prime $N$, let $L(N)$ be the least quadratic nonresidue modulo $N$, and put $D = -L(N)$ if $M \equiv -1 \pmod 4$ and $D = -4L(N)$ otherwise. Applying Lemma 22 and then Lemma 23, we get

$$d_{\mathrm{CM}}(N) = O(Nh(D)) = O(N\sqrt{|D|}\log|D|).$$

Substituting in the unconditional Burgess bound for $D$, we get

$$d_{\mathrm{CM}}(N) = O_\epsilon(N^{1+c/2+\epsilon/2}\log(N^{c+\epsilon})).$$

Since this holds for all $\epsilon > 0$, we get

$$d_{\mathrm{CM}}(N) = O_\epsilon(N^{1+c/2+\epsilon}).$$

Applying instead Ankeny's bound, we get, conditionally on GRH,

$$d_{\mathrm{CM}}(N) = O(N\sqrt{(\log N)^2}\log(\log N)^2 = O(N\log N\log\log N).$$

## 7. Proof of Theorem 5

Although not necessary from a logical point of view, we believe it will make for easier reading if we discuss first the special case in which the endomorphism ring is the maximal order and second the (less) special case in which the conductor of the order is prime to $N$ before discussing the general case.

**Case 1: Fundamental discriminants.** Suppose that there exists some positive number $C$ such that for every odd prime $N$, there exists a point on $X_1(N)$ with CM by the *full* ring of integers of some imaginary quadratic field, and of degree at most $CN$. We will derive a contradiction.

Put $H := 6C + 1$. Recall that the set of negative quadratic fundamental discriminants $D$ such that $h(D) \leq H$ is finite [Deu33], [Hei34], [Sie35]. Let us write out this set as $\{D_1, \ldots, D_n\}$.

Let $\mathcal{P}_1$ be the set of primes which are 1 (mod 4) and divide $D_k$ for some $1 \leq k \leq n$. Put $R = \#\mathcal{P}_1$. Similarly, let $\mathcal{P}_3$ be the set of primes which are 3 (mod 4) and divide some $D_k$. Put $S = \#\mathcal{P}_3$.

**Lemma 24.** *The set $\mathcal{P}_H$ of odd primes $N$ such that $(\frac{D}{N}) = -1$ for all $D$ with $h(D) \leq H$ is infinite; indeed it has density at least $(\frac{1}{2})^{R+S+2}$.*

*Proof.* Let $N$ be any prime number satisfying:
(i) $N \equiv 7 \pmod 8$;
(ii) $(\frac{N}{p}) = 1$ for all $p \in \mathcal{P}_1$.
(iii) $(\frac{N}{q}) = -1$ for all $q \in \mathcal{P}_3$.

By the Cebotarev density theorem, the set of such primes $N$ has density $(\frac{1}{2})^{R+S+2}$. We claim that all such primes lie in $\mathcal{P}_H$. Indeed, we may write

$$D_k = (-1) \cdot 2^{a+2b} p_1 \cdots p_r q_1 \cdots q_s = (-1)^{s+1} 2^{a+2b} \prod_{i=1}^{r} p_i \prod_{j=1}^{s} (-q_j),$$

where $a, b \in \{0, 1\}$, $p_i \in \mathcal{P}_1$ and $q_j \in \mathcal{P}_3$. Then

$$\left(\frac{D_k}{N}\right) = \left(\frac{-1}{N}\right)^{s+1} \left(\frac{2}{N}\right)^{a+2b} \prod_{i=1}^{r} \left(\frac{p_i}{N}\right) \prod_{j=1}^{s} \left(\frac{-q_j}{N}\right) =$$

$$(-1)^{s+1} \cdot 1 \cdot \prod_{i=1}^{r} \left(\frac{N}{p_i}\right) \cdot \prod_{j=1}^{s} \left(\frac{N}{q_j}\right) = (-1)^{s+1}(-1)^s = -1.$$

□

Now let $N > H$ be a prime in $\mathcal{P}_H$, and let $D$ be a fundamental negative quadratic discriminant. If $(\frac{D}{N}) = -1$, then by Theorem 2 we have $d_D(N) \geq \frac{N^2-1}{6}$, which for sufficiently large $N$, is greater than $CN$. Otherwise $(\frac{D}{N}) \neq -1$, and since we are taking $N$ large we may assume $(\frac{D}{N} = 1$. Therefore, by Theorem 2 we have

$$d_D(N) \geq \frac{h(D)}{6}(N-1) > \frac{H}{6}(N-1) > CN,$$

since $N > H$.

**Case 2: Orders of conductor prime to $N$.** Suppose that $\mathcal{O}(D)$ is an order of conductor $f$ in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D_0})$; let $F$ be a number field and $E_{/F}$ be a $\mathcal{O}$-CM elliptic curve.

**Proposition 25.** *There exists an $F$-rational isogeny $\iota\colon E \to E'$, where $E'_{/F}$ is an elliptic curve with $\mathcal{O}_K$-CM. Moreover $\iota$ is cyclic of degree $f$.*

This is "well known", but lacking a convenient reference we shall sketch the proof. Over the complex numbers we may view $E$ as $\mathbb{C}/\mathcal{O}$, and then the map is just the natural map $\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{O}_K$. The rationality of the map over $F$ follows easily from the fact that $\mathcal{O}$ is the unique subring of $\mathcal{O}_K$ of index $f$.

The isogeny $\iota$ induces a homomorphism of Mordell-Weil groups $\iota(F)\colon E(F) \to E'(F)$. According to the Proposition, the kernel of $\iota(F)$ is $f$-torsion. Moreover, using the existence of a dual isogeny $\iota^\vee\colon E' \to E$ such that $\iota^\vee \circ \iota = [f]$, $\iota \circ \iota^\vee = [f]$, one sees that also the cokernel of $\iota(F)$ is $f$-torsion. In particular, if $N$ is an odd prime with $(N, f) = 1$, then

$$\iota(F) : E(F)[N] \xrightarrow{\sim} E'(F)[N].$$

In particular, if $E$ has an $F$-rational torsion point of order $N$, so does $E'$. From this it follows that – still for $N$ prime to $f$ – the least degree of an $\mathcal{O}(f^2D_0)$-CM point on $X_1(N)$ is at least as large as that of an $\mathcal{O}(D_0)$-CM point on $X_1(N)$. That is, we have succeeded in reducing Case 2 to Case 1.

**Case 3: General Case.** Finally suppose we have $D = f^2D_0$ with $N \mid f$, and consider an $\mathcal{O}(D)$-CM elliptic curve $E$ defined over a number field $F$, with an $F$-rational $N$-torsion point. To simplify the analysis, we assume $F$ contains the CM-field $K$ (this extra factor of 2 will not effect the asymptotic analysis).

The above geometric description of the isogeny $\iota$ shows that $\dim_{\mathbb{F}_N} \ker(\iota) \cap E[N] = 1$, i.e., there exists $P_0 \in E[N](\mathbb{C})$ such that $\langle P_0\rangle = \ker(\iota) \cap E[N]$. Consider first any $F$-rational $N$-torsion point $P$ which is not in $\langle P_0\rangle$. Then $\iota(P)$ is an $F$-rational point on the $\mathcal{O}(D_0)$-CM elliptic curve, i.e., we immediately reduce to Case 1. So we may assume that the point $P_0$ is $F$-rational and derive lower bounds on $[F : K]$.

As in §2.3, Case 3, the mod $N$ Galois representation $\rho_N\colon \mathrm{Gal}_F \to GL_2(\mathbb{Z}/N\mathbb{Z})$ is contained in a "pseudo-Cartan subgroup"; taking an ordered basis with $P_0$ as the first vector, we have

$$\rho(\mathrm{Gal}_F) \subset C_N^\times \cong \{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \ a \in \mathbb{F}_N^\times,\ b \in \mathbb{F}_N\}.$$

So our assumption that $P_0$ is $F$-rational means precisely that

$$\rho(\mathrm{Gal}_F) \subset \{\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \ b \in \mathbb{F}_N\}.$$

Thus $\det(\rho(\mathrm{Gal}_F)) = 1$, so by Corollary 11 we deduce $F \supset K(\zeta_N)$. Now $K(\zeta_N)$ and the ring class field $K(j(E))$ are extensions of $K$ of degrees at least $\frac{N-1}{2}$ and $\frac{N-1}{3}$ respectively. Moreover, Fact 1e) implies that, loosely speaking, these two extensions are close to being disjoint over $K$, so that $K(\zeta_N, j(E))$ has degree at least a universal constant times $(N-1)^2$.

Let us now see this in more detail: let $E''$ be an elliptic curve with $\mathcal{O}(N^2D_0)$-CM, i.e., with the same CM field but conductor $N$ instead of its multiple $f$. By class field theory $K(j(E)) \subset K(j(E''))$. But $K(j(E''))$, being the ring class field of conductor $N$, is contained in the $N$-ray class field $K(N)$, whereas explicit class field theory shows $\mathrm{Gal}(K(N)/K)$ is a finite abelian group with either 1 or two generators. Therefore the degree of the maximal exponent 2 abelian subextension of $K(j(E))/K$ is at most 4. Combining all estimates, we get

$$[F : K] \geq [K(j(E), \zeta_N) : K] \geq \frac{(N-1)^2}{24}.$$

This is obviously not $O(N)$, so the proof is complete.

## 8. Proof of Theorem 6

Here, briefly, is the idea: Start with $E/\mathbb{Q}$ of $j$-invariant 0. Enumerate the odd primes $p_n$ which are 1 mod 3 (hence split in $\mathbb{Q}(\sqrt{-3})$). Let $K_n$ be the least field over which $E$ acquires a point of order $N_n := p_1 \cdots p_n$. The degree of this field is at most

$$2\prod_{i=1}^{n}(p_i - 1) = 2\varphi(N_n),$$

and it is known that $\frac{N_n}{\varphi(N_n)} \gg \log\log N_n$.

We now begin the proof. Let $K = \mathbb{Q}(\sqrt{-3})$, and $E_{/K}$ an $\mathcal{O}(-3)$-CM elliptic curve (e.g., $y^2 = x^3 + 1$). Let $p_1 < p_2 < \ldots$ be the primes congruent to 1 (mod 3), i.e., the primes which split in $K$. It follows from the material reviewed in §2.3 that for each $i$ there is a point $P_i$ on $E$ of order $i$, such that $[K(P_i) : K] \mid (p_i - 1)$. Thus, for any positive integer $n$, the field $L_n := K(\{P_i\}_{i=1}^n)$ has a point of order $N_n = p_1 \cdots p_n$ (namely $P_1 + \ldots + P_n$) and

$$d_n := [L_n : K] \leq 2\prod_{i=1}^{n}(p_i - 1) = 2\varphi(N_n).$$

Then

$$\frac{|E(L_n)[\mathrm{tors}]|}{d_n} \geq \frac{N_n}{2\varphi(N_n)},$$

and to complete the proof it is sufficient to establish the following

Claim: There exists $C > 0$ such that for all sufficiently large $n$,

$$\frac{N_n}{2\varphi(N_n)} \geq C\sqrt{\log(\log(d_n))}.$$

The proof of the claim rests on an asymptotic formula due to Mertens, namely

$$\prod_{p \leq x} \frac{1}{1 - p^{-1}} \sim e^{-\gamma}\log(x),$$

where the product is taken over all primes less than or equal to $x$, and $\gamma$ is Euler's constant [BD04, Cor. 6.19]. From the Prime Number Theorem for Arithmetic Progressions [BD04, Thm. 9.12], it follows that

$$\prod_{p \leq x, p \equiv 1(3)} \frac{1}{(1 - p^{-1})} \sim e^{-\gamma/2}\sqrt{\log(x)}.$$

Let us now write

$$\frac{N_n}{\varphi(N_n)} = \prod_{i=1}^{n} \frac{p_i}{p_i - 1} = \prod_{p \le x(n), p \equiv 1(3)} \frac{1}{1 - p^{-1}}.$$

Then we have

$$\frac{N_n}{\varphi(N_n)} \sim e^{-\gamma/2} \sqrt{\log(x(n))}.$$

Again applying the Prime Number Theorem for Arithmetic Progressions, it follows that $\log(x(n)) \sim \log(n)$, and also that

$$\log(N_n) = \sum_{i=1}^{n} \log(p_i) \sim 2 \sum_{i=1}^{n} i \log(i) \sim 2 \log n \sum_{i=1}^{n} i = n(n+1) \log(n).$$

This implies that $\log(\log(N_n)) \sim \log(n) \sim \log(x(n))$. Thus

$$\frac{N_n}{\varphi(N_n)} \sim e^{-\gamma/2} \sqrt{\log(\log(N_n))} \ge e^{-\gamma/2} \sqrt{\log(\log(\varphi(N_n)))} \ge e^{-\gamma/2} \sqrt{\log(\log(d_n/2))},$$

which is sufficient to give the result.

Remark 8.1: The reader may be wondering whether we could have done better by applying Theorem 1, which says that we can get an $\mathcal{O}(-3)$-CM point of degree $\frac{p_i - 1}{3}$. However, the factor of 6 that we gained in the proof of this result was via our ability to make a single cyclic twist to get more torsion. However we cannot independently make cyclic twists for each prime $p_i$. Thus we could improve $d_n$ to $\frac{\varphi(p_1 \cdots p_n)}{3}$ but not to $\frac{2}{3^n} \varphi(p_1 \cdots p_n)$. In fact Serre's Theorem (Theorem 18) implies that among constructions working with a fixed elliptic curve, or even a fixed $j$-invariant, our lower bound is asymptotically optimal.

## 9. Proof of Theorem 7

**Theorem 26** (Abramovich, [Abr96])**.** *Let $\Gamma \subset PSL_2(\mathbb{Z})$ be a congruence subgroup, and $X_\Gamma = \Gamma \backslash \overline{\mathcal{H}}$ the corresponding modular curve. The gonality of $X_\Gamma$ is at least $\frac{7}{800}[PSL_2(\mathbb{Z}) : \Gamma]$.*

Remark 9.1: This result uses results of differential geometry and spectral theory, including an upper bound on the leading nontrivial eigenvalue for the Laplacian on the Riemannian manifold $X_\Gamma$: Abramovich's theorem uses the bound $\lambda_1 \le \frac{21}{100}$, due to Luo, Rudnick and Sarnak. Selberg has conjectured that $\lambda_1 \le \frac{1}{4}$, which would allow replacement of $\frac{7}{800}$ by $\frac{1}{96}$.

**Theorem 27** (Faltings, Frey [Fre94])**.** *Let $X$ be a curve defined over a number field $K$ with at least one $K$-rational point. If, for any positive integer $d$, $X_{/K}$ has infinitely many points of degree $d$, then $\frac{1}{2} \operatorname{Gon}_K(X) \le d$.*

Remark 9.2: The hypothesis is satisfied for all classical modular curves $X_\Gamma$ uniformized by congruence subgroups of $PSL_2(\mathbb{Z})$ since such curves always have a cusp rational over their "reflex field" $K$ ($K = \mathbb{Q}$ for the curves $X_1(N)$).

When $N$ is prime, the index of $\Gamma_1(N)$ in $PSL_2(\mathbb{Z})$ is $\frac{N^2-1}{2}$. Thus we get

$$\operatorname{Gon}_{\mathbb{C}}(X_1(N)) \ge \frac{7}{1600}(N^2 - 1)$$

**unconditionally**, and

$$\mathrm{Gon}_{\mathbb{C}}(X_1(N)) \geq \frac{1}{192}(N^2-1)$$

**conditionally** on Selberg's eigenvalue conjecture.

Therefore we get

$$\frac{1}{2}\,\mathrm{Gon}_{\mathbb{Q}}(X_1(N)) \geq \frac{1}{2}\,\mathrm{Gon}_{\mathbb{C}}(X_1(N)) \geq \frac{7}{3200}(N^2-1),$$

so if $d \leq [\frac{7}{3200}(N^2-1)]-1$ there are only finitely many points of degree $d$. Thus in the statement of Theorem 3 we can take for $C_1$ any constant less than $\frac{7}{3200}$, and if Selberg's eigenvalue conjecture holds, we can take any constant less than $\frac{1}{384}$.

For part b) we need two facts. First, for a curve $X$ of genus $g \geq 2$ over any field $K$, one can get a degree $2g-2$ map to the projective line by taking an element $f$ of the complete linear system associated to the canonical bundle $\Omega^1_{X/K}$, and therefore $\mathrm{Gon}_K(X) \leq 2g(X)-2$. Second, for $N \geq 5$ prime, we have $2g(X_1(N))-2 = \frac{N^2-12N+11}{12}$: see [Mi89, §4.2].

## Appendix A. The least degree of a CM point and finiteness of low-degree points on $X_1(N)$ (by Alex Rice)

The object of this appendix is to prove the following result.

**Theorem 28.** *For $N > 911$, $\{P \in X_1(N)(\overline{\mathbb{Q}}) : \deg(P) < d_{CM}(N)\}$ is finite.*

For a negative integer $D$, let $h(D) = h(\mathbb{Q}(\sqrt{D}))$. For an odd prime $N$, let $L(N)$ denote the least positive quadratic non-residue modulo $N$.

By Theorem 7(a), it suffices to show that $d_{CM}(N) < \left\lceil \frac{7}{3200}\left(N^2-1\right)\right\rceil$. By Theorem 1, if $N \equiv 1 \bmod 3$ then $d_{CM}(N) \leq \frac{N-1}{3}$ and if $N \equiv 1 \bmod 4$ then $d_{CM}(N) \leq \frac{N-1}{2}$. We now need only an upper bound on $d_{CM}(N)$ when $N \equiv 11 \bmod 12$; note that since $N \equiv -1 \pmod 4$, $\left(\frac{|D|}{N}\right) = -\left(\frac{D}{N}\right)$. By Lemma 22, if $\left(\frac{|D|}{N}\right) = -1$ then $d_{CM}(N) \leq 2(N-1)h(D)$, and thus by definition of $L(N)$ we have

$$d_{CM}(N) \leq 2(N-1)h(-L(N)). \tag{9}$$

Step 1: We reduce to a finite computation using upper bounds on $L(N)$ and $h(D)$. Recall that the "world-record" asymptotic upper bound on $L(N)$ is Burgess's bound

$$L(N) = O_\epsilon(N^{c+\epsilon}),$$

but it has proven to be difficult to determine an appropriate absolute constant for any fixed $\varepsilon$. It turns out to be easier to use a more elementary estimate given by a sharpened version of the Polya-Vinogradov inequality [Tao11, §2.5], which yields

$$L(N) \leq \sqrt{N}\log(N). \tag{10}$$

Recall Dirichlet's class number formula for an imaginary quadratic field with discriminant $D < -4$ [N, Cor. VII.5.11]:

$$h(D) = \frac{\sqrt{|D|}}{\pi}\mathrm{res}_{s=1}\zeta_{\mathbb{Q}(\sqrt{D})}, \tag{11}$$

where $\zeta_{\mathbb{Q}(\sqrt{D})}$ is the Dedekind zeta function. By [Lou01, Thm. 1],

$$\text{res}_{s=1}\zeta_k \le \frac{e \log |D|}{2}. \tag{12}$$

Since the discriminant of $\mathbb{Q}(\sqrt{-L(N)})$ is either $-L(N)$ or $-4L(N)$, we have

$$d_{CM}(N) \le \frac{2e}{\pi} N^{\frac{5}{4}} \sqrt{\log(N)} \left( \frac{\log(N)}{2} + \log\log(N) + \log(4) \right). \tag{13}$$

The right hand side is less than $\left\lceil \frac{7}{3200} \left(N^2 - 1\right) \right\rceil$ when (e.g.) $N > 10^6$.

Step 2: We will find a bound $N_0$ such that for all primes $N > N_0$ with $N \equiv 11 \pmod{12}$, there is a negative integer $D$ with $\left(\frac{|D|}{N}\right) = 1$ and $2(N-1)h(D) < \left\lceil \frac{7}{3200} \left(N^2 - 1\right) \right\rceil$. Since $h(D) \ge 1$, we certainly need to take $N_0$ large enough so that $N > N_0$ implies $2(N-1) < \left\lceil \frac{7}{3200} \left(N^2 - 1\right) \right\rceil$. This inequality holds for all primes $N \ge 919$ but not for $N = 911$, so we will need $N_0 \ge 911$.

Step 3: We implemented in SAGE [S+09] an algorithm which, for each prime $N \le 10^6$ , $N \equiv 11 \bmod 12$, computes $L(N)$ and $h(-L(N))$, and then compares $2(N-1)h(-L(N))$ to $\left\lceil \frac{7}{3200} \left(N^2 - 1\right) \right\rceil$. If the former is not smaller than the latter, $N$ is appended to a list of "bad" primes. By Step 2, the primes that are at most 911 are all "bad", and there are 12 additional "bad" primes $N < 10^6$:

$$983, 1103, 1151, 1223, 1319, 1367, 1487, 1559, 1583, 1607, 1823, 2999. \tag{14}$$

Step 4: The primes of (14) all satisfy $2(N-1) < \left\lceil \frac{7}{3200} \left(N^2 - 1\right) \right\rceil$, so by Lemma 22, it suffices to find a negative integer $D$ with $\left(\frac{|D|}{N}\right) = -1$ and $h(D) = 1$. Such a $D$ does exist for each of these "bad" primes, and thus we may take $N_0 = 911$.[3] Below is a table that shows, for each of these 12 primes, $L(N)$, $h(-L(N))$, and a $D$ with $h(D) = 1$ and $\left(\frac{|D|}{N}\right) = -1$.

| $N$ | $L(N)$ | $h(-L(N))$ | $\lvert D\rvert$ |
|---|---|---|---|
| 983 | 5 | 2 | 11 |
| 1103 | 5 | 2 | 7 |
| 1151 | 13 | 2 | 19 |
| 1223 | 5 | 2 | 19 |
| 1319 | 13 | 2 | 163 |
| 1367 | 5 | 2 | 7 |
| 1487 | 5 | 2 | 19 |
| 1559 | 17 | 4 | 19 |
| 1583 | 5 | 2 | 7 |
| 1607 | 5 | 2 | 7 |
| 1823 | 5 | 2 | 43 |
| 2999 | 17 | 4 | 19 |

[3] Since there are nine imaginary quadratic fields of class number one, the chance that $|D|$ is a quadratic nonresidue for at least one class number one field is $1 - 2^{-9} = \frac{511}{512}$. Since we only had 12 bad primes to check, this outcome was not especially fortuitious.

## References


[Abr96] D. Abramovich, *A linear lower bound on the gonality of modular curves.* Internat. Math. Res. Notices 1996, no. 20, 1005–1011.

[Ank52] N.C. Ankeny, *The least quadratic non residue.* Annals of Math. (2) 55 (1952), 65-72.

[BD04] P.T. Bateman and H.G. Diamond, *Analytic number theory. An introductory course.* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2004. xiv+360 pp.

[Bur57] D.A. Burgess, *The distribution of quadratic residues and non-residues.* Mathematika 4 (1957), 106-112.

[Cla04] P.L. Clark, *Bounds for torsion on abelian varieties with integral moduli*, 2004 preprint.

[Coh07] H. Cohen, *Number Theory. Volume I: Tools and Diophantine Equations.* Graduate Texts in Mathematics 240, Springer-Verlag, 2007.

[Cox89] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* John Wiley & Sons, New York, 1989.

[D] H. Davenport, *Multiplicative number theory.* Second edition. Revised by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York-Berlin, 1980.

[Deu33] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzahl 1.* Math. Z. 37 (1933), no. 1, 405–415.

[Erd52] P. Erdös, review of N.C. Ankeny's "The least quadratic non residue." Math reviews #MR0045159.

[Fre77] G. Frey, *Some remarks concerning points of finite order on elliptic curves over global fields.* Ark. Mat. 15 (1977), no. 1, 1–19.

[Fre94] G. Frey, *Curves with infinitely many points of fixed degree* Israel J. Math. 85 (1994), 79–83.

[FSWZ90] G. Fung, H. Ströher, H. Williams and H. Zimmer, *Torsion groups of elliptic curves with integral $j$-invariant over pure cubic fields.* J. Number Theory 36 (1990), 12-45.

[HW] G.H. Hardy, E.M. Wright, *An introduction to the theory of numbers. Fifth edition.* The Clarendon Press, Oxford University Press, New York, 1979. xvi+426 pp.

[Hei34] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields.* Quart. J. Math. Oxford Ser. 25, 150-160, 1934.

[HS99] M. Hindry and J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique.* C. R. Acad. Sci. Paris Sr. I Math. 329 (1999), no. 2, 97–100.

[Hu] L.-K. Hua, *Introduction to number theory.* Springer-Verlag, Berlin-New York, 1982.

[JK06] D. Jeon and C.H. Kim, *On the arithmetic of certain modular curves*, arXiv preprint, 2006.

[JKS04] D. Jeon, C. H. Kim and A. Schweizer, *On the torsion of elliptic curves over cubic number fields.* Acta Arith. 113 (2004) 291301.

[JKP06] D. Jeon, C.H. Kim and E. Park, *On the torsion of elliptic curves over quartic number fields.* J. London Math. Soc. (2) 74 (2006), 1-12.

[Kam86] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields.* Duke Math. J. 53 no. 1 (1986), 157–162.

[Kam92] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms.* Invent. Math. 109 (1992), no. 2, 221–229.

[KM88] M.A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Math. J. 109 (1988), 125–149.

[Lan87] S. Lang, *Elliptic functions. With an appendix by J. Tate. Second edition.* Graduate Texts in Mathematics, 112. Springer-Verlag, New York, 1987.

[Lou01] S. R. Louboutin, *Explicit Upper Bounds for Residues of Dedekind Zeta Functions and Values of L-Functions at $s = 1$, and Explicit Lower Bounds on Relative Class Numbers of CM-Fields*, Canad. J. Math. Vol. 53 (2001), pp.1194-1222.

[Maz77] B. Mazur, *Modular elliptic curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Etudes Sci. 47 (1977) 33168.

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), 437-449.

[MSZ89] H. Miller, H. Ströher and H. Zimmer, *Torsion groups of elliptic curves with integral $j$-invariant over quadratic fields.* J. Reine Angew. Math. 397 (1989), 100-161.

[Mi89] T. Miyake, *Modular forms.* Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989.

[N] J. Neukirch, *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.

[Ols74] L. Olson, *Points of finite order on elliptic curves with complex multiplication*. Manuscripta math. 14 (1974), 195-205.

[Par99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*. J. Reine Angew. Math. 506 (1999), 85–116.

[Par03] P. Parent, *No 17-torsion on elliptic curves over cubic number fields* . J. Théor. Nombres Bordeaux 15 (2003), no. 3, 831–838.

[Pari89] J.L. Parish, *Rational Torsion in Complex-Multiplication Elliptic Curves*. Journal of Number Theory 33 (1989), 257-265.

[PWZ97] A. Pethö, T. Weis and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over gneeral cubic number fields*. Internat. J. Algebra Comput. 7 (1997), 353-413.

[PY01] D. Prasad and C.S. Yogananda, *Bounding the torsion in CM elliptic curves*. C. R. Math. Acad. Sci. Soc. R. Can. 23 (2001), 1–5.

[S$^+$09] W. A. Stein et al., *Sage Mathematics Software (Version 4.0.0)*, The Sage Development Team, 2009, http://www.sagemath.org.

[S66] J.-P. Serre, *Groupes de Lie l-adiques attachés aux courbes elliptiques*. 1966 Les Tendances Géom. en Algèbre et Théorie des Nombres pp. 239–256 Éditions du Centre National de la Recherche Scientifique, Paris.

[S67] J.-P. Serre, *Complex multiplication*. 1967 Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) pp. 292–296 Thompson, Washington, D.C.

[S72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), no. 4, 259–331.

[Sie35] C.L. Siegel, *Über die Classenzahl quadtratischer Zahlkörper*. Acta Mathematica 1 (1935), 83-86.

[Sbg88] A. Silverberg, *Torsion points on abelian varieties of CM-type*. Compositio Math. 68 (1988), no. 3, 241–249.

[Sbg92] A. Silverberg. *Points of finite order on abelian varieties*. In *p-adic methods in number theory and algebraic geometry*, 175-193, Contemp. Math. 133, AMS, 1992.

[Sil86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.

[Sil94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, 1994.

[S12] A. Sutherland, *Defining Equations for* $X_1(N)$, http://math.mit.edu/~drew/X1_altcurves.html

[Tao11] T. Tao, *An epsilon of room II; pages from year three of a mathematical blog*, American Mathematical Society, Providence RI, 2011.

[Wat04] M. Watkins, *Class numbers of imaginary quadratic fields*. Math. Comp. 73 (2004), no. 246, 907–938.

[Zim76] H. Zimmer, *Points of finite order on elliptic curves over number fields*. Arch. Math. (Basel) 27 (1976), no. 6, 596–603.



Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602-7403, USA

*E-mail address*: pete@math.uga.edu

*E-mail address*: bcook@math.ubc.ca

*E-mail address*: stankewicz@gmail.com