Torsion subgroups of elliptic curves over number fields

Andrew V. Sutherland

December 24, 2012

Abstract

This is an extended version of an expository talk given at a seminar[1] on Mazur's torsion theorem, summarizing work on generalizations to number fields and related results.

Introduction

These notes contain a summary of work on generalizations of Mazur's theorem [33, 32, Thm. 8] classifying the possible (rational) torsion subgroups of an elliptic curve defined over $\mathbb{Q}$. The primary goal of the work surveyed here is to classify the possible torsion subgroups that can arise among elliptic curves defined over number fields of degree $d > 1$. So far this goal has been fully achieved only for $d = 2$, but there is a surprising amount that can be said about $d > 2$, much of it based on very recent work.

These notes are surely incomplete, and there is a lot of work currently in progress; any comments, corrections, and additions are welcome. For the benefit of those looking for research topics, **open questions** have been highlighted throughout this document.

1 Generalizing Mazur's Theorem to number fields

1.1 Quadratic Fields ($d = 2$)

As noted above, other than $\mathbb{Q}$ itself, quadratic extensions of $\mathbb{Q}$ are the only cases that are completely understood.

[1] See `http://www.math.harvard.edu/~chaoli/MazurTorsionSeminar.html`.

1.1.1 Possible torsion subgroups over quadratic fields

There is a direct analog of Mazur's theorem for quadratic fields.

Theorem 1 (Kamienny-Kenku-Momose). *Let E be an elliptic curve over a quadratic field K. Then the torsion subgroup $E(K)_{\text{tors}}$ is isomorphic to one of the following* 26 *groups:*

$$\begin{array}{rl} \mathbb{Z}/m\mathbb{Z}, & \textit{for } 1 \le m \le 18, m \ne 17, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & \textit{for } 1 \le m \le 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}, & \textit{for } 1 \le m \le 2, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array}$$

This theorem was proven through a long series of papers by Kenku, Momose, and Kamienny, including [17, 18, 19, 20, 21, 22, 25, 26, 27, 28, 29, 37, 38], culminating in a 1988 paper by Kenku and Momose [29] that proposed the above list of groups and a 1992 paper by Kamienny that finally proved that the list is complete [22]. This work relied extensively on the techniques developed by Mazur in [33, 34], but they were more special cases to consider, and many of them were more difficult. The key step by Kamienny involved a non-trivial extension of Mazur's ideas that allowed him to prove the (strong) *Uniform Boundedness Conjecture* for quadratic fields. In [22] Kamienny proves an absolute upper bound on the cardinality of $|E(K)_{\text{tors}}|$ valid for all quadratic fields K by showing that the largest possible prime divisor of $|E(K)_{\text{tors}}|$ is 13. The crux of his proof lies in the following proposition, which gives an analog of the formal immersion used in Mazur's proof.

Proposition 2. *Let N be a prime greater than* 61 *and different from* 71. *Let X denote the symmetric square of $X_0(N)$, viewed as a smooth scheme over $S = \operatorname{Spec} \mathbb{Z}[\frac{1}{N}]$, and let J denote the Eisenstein quotient of $J_0(N)$, as defined in [33, Ch. II, §10]. Then the map*

$$f : X_{/S} \to J_{/S}$$

is a formal immersion along (∞, ∞) away from characteristic $2, 3$, and 5.

Kamienny proves this proposition using a pair of weight-2 newforms for $\Gamma_0(N)$ attached to J, with integral Fourier coefficients. He then shows that for primes N satisfying the hypothesis of the proposition, the existence of an elliptic curve E/K with a rational point of order N implies the existence of a point $(x, x^\sigma) \ne (\infty, \infty)$ on X for which $f(x, x^\sigma)_{/7} = f(\infty, \infty)_{/7}$, which is a contradiction. Kamienny later generalized some of these ideas to higher degree number fields, provided that one can find a suitable set of newforms attached to J; see [23].

Table 1: Modular curves parametrizing elliptic curves with torsion subgroups that occur over quadratic fields but not over $\mathbb{Q}$.

genus	modular curves
0	$X(3), X_1(3,6), X(4)$
1	$X_1(11), X_1(14), X_1(15), X_1(2,10), X_1(2,12)$
2	$X_1(13), X_1(16), X_1(18)$

1.1.2 Realizing torsion subgroups over quadratic fields

Recall that for each of the 15 torsion subgroups that can arise over $\mathbb{Q}$ we have explicit parametrizations due to Kubert that allow us to construct infinitely many non-isomorphic examples of each case; see [30, Table 3]. This is also true for the torsion subgroups that can occur over quadratic fields, *provided we are prepared to vary the field K*; see [48] for a detailed description of these parametrizations. The key point is that the modular curves in question all have genus $g \leq 2$.

Let $Y_1(M, N)$ denote the affine modular curve that parameterizes isomorphism classes of triples (E, P_M, P_N), where P_M and P_N are points on the elliptic curve E such that $\langle P_M \rangle \times \langle P_N \rangle \simeq \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ with $M|N$. Let $X_1(M, N)$ be the compactification of $Y_1(M, N)$ obtained by adding the cusps. Table 1 lists the 11 modular curves that correspond to torsion subgroups listed in Theorem 1 but not in Mazur's theorem, sorted by genus.

The genus 0 curves $X(3), X_1(3,6)$, and $X(4)$ have no rational points over $\mathbb{Q}$ because the existence of the Weil pairing implies that if the N-torsion points of an elliptic curve E/K are all rational, then K must contain the Nth roots of unity. Thus the only quadratic field over which the torsion subgroups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ can arise is $K = \mathbb{Q}(\sqrt{-3})$, and for $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ we must have $K = \mathbb{Q}(i)$; there are then infinitely many non-isomorphic examples in each case.

For modular curves X of genus 1 and 2 we can always find an affine model for X of the form $y^2 = f(x)$, where $f(x)$ is a polynomial over $\mathbb{Q}$.[2] If we then pick an arbitrary $x_0 \in \mathbb{Q}$, let $y_0 = \sqrt{f(x_0)}$, and let $K = \mathbb{Q}(y_0)$, then (x_0, y_0) is a K-rational point on X. There are infinitely many such points (over different fields K), only finitely many of which correspond to cusps. Thus for almost all choices of x_0 we obtain a point (x_0, y_0) that can be used

[2] In genus 2 these models will necessarily be singular (they can be desingularized by embedding them in $\mathbb{P}^3$), but this does not pose a problem for our intended application.

to construct an elliptic curve $E/\mathbb{Q}(y_0)$ with the desired torsion subgroup.

As an example, let us consider the genus 2 modular curve $X_1(13)$, which has a hyperelliptic model

$$X_1(13)\colon \qquad y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1.$$

If we pick $x_0 = 2$, and set $y_0 = \sqrt{17}$, then (x_0, y_0) is a point on our model of $X_1(13)$ over the quadratic field $K = \mathbb{Q}(\sqrt{17})$. If we then apply the formulas

$$r = \frac{x^4 - x^3 + xy - x + 2}{2}, \quad s = \frac{x^4 - x^2 + xy - x + y + 1}{x^3 - x^2 + y + 1}$$

$$c = s(r-1), \qquad b = cr$$

with $x = x_0$ and $y = y_0$, we obtain the values

$$b_0 = b(x_0, y_0) = 18\sqrt{17} + 74 \qquad \text{and} \qquad c_0 = c(x_0, y_0) = 2\sqrt{17} + 10.$$

These coordinates define an elliptic curve in Tate normal form:

$$E(b,c)\colon \qquad y^2 + (1-c)xy - by = x^3 = bx^2.$$

The elliptic curve $E(b_0, c_0)$over $\mathbb{Q}(\sqrt{17})$ has $(0,0)$ as a point of order 13, and in fact its torsion subgroup is $\mathbb{Z}/13\mathbb{Z}$. For an explanation of how one can construct such models of $X_1(N)$, along with the necessary maps $r(x,y)$ and $s(x,y)$, see [49, 55].

Remark 3. As in the case $d = 1$, every torsion subgroup that occurs when $d = 2$ can be realized by an elliptic curve without complex multiplication. This follows immediately from the fact that there are infinitely many non-isomorphic examples of each case, whereas the total number of isomorphism classes of CM elliptic curves defined over a quadratic field is finite (there are exactly 71, of which 13 are defined over $\mathbb{Q}$). This situation does not hold over number fields of sufficiently high degree; see §4.

1.1.3 Addressing particular quadratic fields

Theorem 1 gives the torsion subgroups that can arise over quadratic fields in general, but one might also ask which torsion subgroups can arise over a given quadratic field K. This problem is addressed in a recent paper by Kamienny and Najman [24], which also determines the quadratic field of minimal discriminant over which each torsion subgroup can be realized.

For modular curves of genus 0 the situation is clear: the cases that also arise over $\mathbb{Q}$ occur infinitely often over every quadratic field, while the curves $X(3), X_1(3,6)$ (resp. $X(4)$) have non-cuspidal rational points only over $\mathbb{Q}(\sqrt{-3})$ (resp. $\mathbb{Q}(i)$), where they have infinitely many.[3] For modular curves of genus 2 the situation is also clear: Faltings' theorem implies that there are only finitely many points on $X_1(13)$, $X_1(16)$, and $X_1(18)$ over any particular quadratic field. Determining whether this finite number is zero or nonzero is a non-trivial problem, but there are tools for doing so.

The situation for modular curves of genus 1 is more interesting. Depending on the field K, the number of non-cuspidal K-rational points may be zero, positively finite, or infinite. A detailed analysis is given in [24]. Najman has also determined the number of points on the genus 1 curves in Table 1, as well as the genus 1 curves $X_1(3,9)$, $X_1(4,8)$ and $X(6)$, over number fields of degree 3, 4, and arbitrary prime degree [39, 40, 41].[4]

1.2 Cubic fields ($d = 3$)

Over cubic fields we do not yet have an exact analog of Mazur's theorem. But we may be getting close. The part of the problem that was most difficult for $d \leq 2$ has been solved. The largest prime that can divide the order of the torsion subgroup of an elliptic curve defined over a cubic number field is 13. This was proved by Pierre Parent in a pair of papers published in 2000 and 2003 [44, 45].

We also know all of the torsion subgroups that arise for an infinite number of non-isomorphic elliptic curves over cubic fields. The list

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z}, & \text{for } 1 \leq m \leq 20, m \neq 17, 19, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & \text{for } 1 \leq m \leq 7, \end{array}$$

was determined by Jeon, Kim and Schweizer in [14], and Jeon, Kim, and Lee give explicit parameterizations for each case in [15]. Based on our experience with $d \leq 2$, we might be tempted to conjecture that is a complete list of the torsion subgroups that can arise over cubic fields. But we would be wrong!

As recently announced by Najman [42], the elliptic curve

$$y^2 + xy + y = x^3 - x^2 - 5x + 5,$$

(curve 162b1 in Cremona's Tables [5]), has torsion subgroup $\mathbb{Z}/21\mathbb{Z}$ over the cubic subfield of $\mathbb{Q}(\zeta_9)$. This is our first example of a *sporadic* point

[3] The genus 0 curve $X(5)$ does not appear in Table 1 because no quadratic field contains the fifth roots of unity, but we will see it when we consider quartic fields.

[4] The genus 1 curves $X_1(3,9)$, $X_1(4,8)$ and $X(6)$ do not appear in Table 1 because they happen to have no non-cuspidal rational points over $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(i)$. But over quartic fields containing $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ there may be infinitely many rational points on these curves; see [39] for a detailed analysis.

on $X_1(N)$. The elliptic curve 162b1 corresponds to a non-cuspidal point on $X_1(21)$ defined over a cubic field, but the total number of such points over all cubic fields is finite. In fact, this may be the only one; Najman proves that at least there are no others arising from an elliptic curve that can be defined over $\mathbb{Q}$ (but this does not rule out other sporadic points arising from elliptic curves defined over cubic fields). We remark that curve 162b1 does not have complex multiplication (CM): its j-invariant -140625/8 is not an algebraic integer.

In [42] Najman also determines exactly which torsion subgroups can arise for an elliptic curve $E/\mathbb{Q}$ that has been base extended to a cubic field. Other than $\mathbb{Z}/21\mathbb{Z}$, every other case occurs infinitely often and is already included in the list of Jeon, Kim, and Schweizer.

So the remaining **open question** for $d = 3$ is whether there are any other sporadic points of degree 3 on $X_1(N)$ or $X_1(2, N)$, where the prime divisors of N can be at most 13, and we know that the corresponding elliptic curves cannot be defined over $\mathbb{Q}$.[5]

1.3 Quartic fields ($d = 4$)

The situation over quartic fields is similar to the case of cubic fields. It was recently proved that 17 is the largest prime that can divide $|E(K)_{\text{tors}}|$ over any quartic field K. This result is based on work by Sheldon Kamienny, William Stein, and Michael Stoll that was announced at the 2010 Algorithmic Number Theory Symposium (ANTS IX) [54]. Jeon, Kim, and Park have determined the list of torsion subgroups with infinitely many non-isomorphic examples arising over quartic fields [13], see Table 2, and Jeon, Kim, and Lee have found explicit parameterizations for each case [16].

It is an **open question** whether any sporadic points of degree 4 exist on $X_1(N)$ or $X_1(2, N)$. It is possible that the list in Table 2 includes every torsion subgroup that can arise over a quartic field, but based on our experience with $d = 3$ it would seem rash to make such a conjecture.

1.4 Quintic fields ($d = 5$)

The largest prime that can divide $|E(K)_{\text{tors}}|$ over any quintic field K is 19. This recent result of Derickx, Kamienny, Stein, and Stoll was announced (and partially proved) in Maarten Derickx master's thesis [8]. A paper

[5] The list of possible N is finite (by Parent's theorem), and ruling out degree 3 points on $X_1(N)$ for $N = 25, 27, 32, 49, 121, 169$ would leave a pretty short list, but I don't know the current state of knowledge here; I expect at least some of this work has been done.

Table 2: Torsion subgroups arising infinitely often over quartic fields.

$\mathbb{Z}/m\mathbb{Z}$,	for $1 \le m \le 24, m \ne 19, 23$,
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$,	for $1 \le m \le 9$,
$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$,	for $1 \le m \le 3$,
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}$	for $1 \le m \le 2$,
$\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$	
$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	

containing a complete proof is currently in preparation, and the same set of authors also plan to publish a proof of the analogous bound of 17 for quartic fields that was announced at ANTS.

As far as I know, the list of torsion subgroups that can arise infinitely often over quintic fields has yet to be determined, and no sporadic points of degree 5 are known (these are both **open questions**).

2 Uniform Boundedness

The analog of Mazur's theorem for quadratic fields is remarkable in that it gives a universal upper bound on the size of the torsion subgroups of elliptic curves that can arise over any of the infinitely many number fields of degree $d = 2$. It is reasonable to ask, as Kamienny did, whether this holds for $d > 2$. This is known as the (strong) *Uniform Boundedness Conjecture*, and it is no longer a conjecture; it was proved in 1994 by Merel [35].[6]

Theorem 4 (Merel)**.** *For every positive integer d there is a constant $B(d)$ such that for every elliptic curve E/K with $[K : \mathbb{Q}] = d$ we have*

$$|E(K)_{\mathrm{tors}}| \le B(d).$$

The bound in Merel's proof is not effective (it relies on Faltings' theorem), but he did prove an explicit bound of d^{3d^2} on the largest prime divisor of $|E(K)_{\mathrm{tors}}|$ for all $d > 1$. This bound was later improved by Oesterlé to $(1 + 3^{d/2})^2$ [1994, unpublished!].[7] Parent then proved an explicit upper

[6] The *weak* Uniform Boundedness conjecture allows the bound to vary with the field.

[7] Oesterlé's bound plays a critical role in several of the results discussed here; it is quite unfortunate that no proof has been published. The work of Parent in [43] implies that Oesterlé's bound holds for all sufficiently large d, but we are typically interested in particular small values of d (e.g. $d = 5, 6, 7$). There is current work in progress aimed at addressing this gap in the literature [6].

bound on the largest prime power that can divide $|E(K)_{\mathrm{tors}}|$, yielding an explicit value for $B(d)$. The following theorem appears in [43, Thm. 1.2].

Theorem 5 (Parent)**.** *Let E be an elliptic curve over a number field K of degree d with a rational point of order p^n. Then*

$$p^n \leq \begin{cases} 129(3^d-1)(3d)^6 & \text{if } p=2, \\ 65(5^d-1)(2d)^6 & \text{if } p=3, \\ 65(3^d-1)(2d)^6 & \text{if } p\geq 5. \end{cases}$$

Applying these results to the case $d=2$, we find that the prime divisors of $|E(K)_{\mathrm{tors}}|$ are bounded by $(1+3^{2/2})^2=16$, which is essentially tight (we know that 13 does occur), but the value of $B(d)$ we get by naïvely applying Parent's theorem is

$$129(3^2-1)6^6\cdot 65(5^2-1)4^6\cdot(65(3^2-1)4^6)^4\approx 6.3\times 10^{39},$$

far larger than the known value 24. One can improve the naïve bound in many cases, see [46] for example, but all the general bounds we know are still exponential in d. But it is generally believed that $B(d)$ should grow polynomially with d. Proving such a bound is an **open problem**.

2.1 The set of prime torsion orders $S(d)$

Closely related to the bound $B(d)$, and a necessary first step in proving analogs of Mazur's theorem over number fields of degree $d>1$, is the problem of determining the set of primes $S(d)$ that can arise as the order of a rational point on an elliptic curve over a number field of degree d.

Let $\mathsf{Primes}(n)$ denote the set of primes bounded by n. We know from Oesterlé's bound that

$$S(d)\subseteq \mathsf{Primes}((3^{d/2}+1)^2).$$

The exact value of the set $S(d)$ is currently known only for $d\leq 5$, but reasonably good bounds on $S(6)$ and $S(7)$ are given in [8, Thm. 3.1][8], and the bound on $S(6)$ has very recently been sharpened [7]. Table 3 gives a summary of what is currently known.

[8] Derickx's bounds depend on Oesterlé's bound, the truth of which he conservatively includes as a hypothesis of his theorem; c.f. footnote 5.

Table 3: Bounds on $S(d)$ for $d \leq 7$

$S(1) = \mathsf{Primes}(7)$	[Mazur 1977].
$S(2) = \mathsf{Primes}(13)$	[Kamienny 1992]
$S(3) = \mathsf{Primes}(13)$	[Parent 2003]
$S(4) = \mathsf{Primes}(17)$	[Kamienny-Stein-Stoll 2010]
$S(5) = \mathsf{Primes}(19)$	[DKSS 2012]
$S(6) \subseteq \mathsf{Primes}(19) \cup \{37, 73\}$	[Derickx 2012]*
$S(7) \subseteq \mathsf{Primes}(43) \cup \{59, 61, 67, 73, 113, 127\}$	[Derickx 2012]

*It is known that $S(6)$ contains $\mathsf{Primes}(19) \cup \{37\}$, only 73 is in question.

Remark 6. In [8] and [54], a broader definition of $S(d)$ is used that includes all prime orders of torsion points on elliptic curves defined over number fields of degree *at most* d, but we prefer the more precise definition that requires the degree to be *exactly* d, as is used elsewhere in the literature [44, 45]. It turns out that $S(1) \subseteq S(2) \subseteq S(3) \subseteq S(4) \subseteq S(5)$, so this distinction has no impact on any of the results listed in Table 3. It is also known that $S(5) \subseteq S(6)$, but it may very well be that $S(6) \not\subseteq S(7)$.

Remark 7. One can also consider the subset of $S_{\mathbb{Q}}(d) \subseteq S(d)$ corresponding to points on an elliptic curve that is actually defined over $\mathbb{Q}$, that is,

$$S_{\mathbb{Q}}(d) := \{p : E(K)[p] \neq \{0\} \text{ with } j(E) \in \mathbb{Q} \text{ and } [K : \mathbb{Q}] = d\},$$

where p is a prime and E is an elliptic curve. It is known that

$$S_{\mathbb{Q}}(d) \subseteq \mathsf{Primes}(13) \cup \{37\} \cup \mathsf{Primes}(2d+1),$$

and exact values of $S_{\mathbb{Q}}(d)$ are known for $d \leq 42$; see [31]. For $1 \leq d \leq 7$:

$$S_{\mathbb{Q}}(d) = \begin{cases} \mathsf{Primes}(7) & \text{if } d = 1, 2, \\ \mathsf{Primes}(7) \cup \{13\} & \text{if } d = 3, 4, \\ \mathsf{Primes}(13) & \text{if } d = 5, 6, 7. \end{cases}$$

3 Gonality bounds for $X_1(N)$

The *gonality* (or *K-gonality*) $\gamma(X)$ of a curve X/K is the minimum degree among all dominant morphisms $\pi\colon X \to \mathbb{P}^1_K$ (rational maps to $\mathbb{P}^1$ with dense image). We are specifically interested in the $\mathbb{Q}$-gonality $\gamma(N)$ of the modular curve $X_1(N)$, because the morphism π allows us to construct infinitely many non-isomorphic elliptic curves with a point of order N over number fields of degree $\gamma(N)$. We saw an example of this earlier when we used a hyperelliptic model $y^2 = f(x)$ of $X_1(13)$ to construct an elliptic curve over a quadratic field with a rational point of order 13; the map $(x, y) \mapsto x$ is a dominant morphism from $X_1(13)$ to $\mathbb{P}^1_{\mathbb{Q}}$ of degree 2, the gonality of $X_1(13)$.

More generally, if we have an irreducible plane model $f(x, y) = 0$ of $X_1(N)$ with $d = \min(\deg_x f, \deg_y f)$, we can use it to construct infinitely many elliptic curves over number fields of degree d with a rational point of order N. In the case that $d = \deg y$, if x_0 is a generic element of $\mathbb{Q}$ and y_0 is a root of $f(x_0, y)$, then the point (x_0, y_0) on $X_1(N)$ is defined over the number field $\mathbb{Q}(y_0)$ of degree d; this also gives us the upper bound $\gamma(N) \le d$, via the morphism $(x, y) \mapsto x$

3.1 General bounds on $\gamma(N)$

Provided that X has a rational point (true for $X_1(N)$, since we always have cusps), we have $\gamma(X) \le g + 1$, where g is the genus of X, and for $g > 1$ we have $\gamma(X) \le g$; see Appendix A of Poonen's paper [47] for this and other useful facts about gonalities. The genus $g(N)$ of $X_1(N)$ can be computed using the general formula for a modular curve X_Γ defined by a congruence subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$:

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2},$$

see [51, Prop. 1.40] or any standard reference. Here μ is the index of Γ in $\mathrm{PSL}_2(\mathbb{Z})$, ν_2 and ν_3 count elliptic points of orders 2 and 3, respectively, while ν_∞ counts cusps, all up to Γ-equivalence. In the case of $X_1(N)$, for $N > 4$ we have $\nu_2 = \nu_3 = 0$,

$$\mu = \frac{N^2}{2} \prod_{p|N} (1 - p^{-2}),$$

$$\nu_\infty = \frac{1}{2} \sum_{n|N, n>0} \phi(n)\phi(N/n),$$

see [36, §4.2]. If $N > 4$ is prime we have $\mu = (N^2 - 1)/2$ and $\nu_\infty = N - 1$, and otherwise $\mu \le (N^2 - 4)/2$ and $\nu_\infty \ge N - 2$. In either case

$$g(N) \le 1 + \frac{N^2 - 1}{24} - \frac{N - 1}{2} \le \frac{N^2 - 1}{24}$$

for all $N > 4$. For $N > 12$ we have $g(N) > 1$, in which case

$$\gamma(N) \leq g(N) \leq \frac{1}{24}N^2 - \frac{1}{2}N + \frac{35}{24} \tag{1}$$

For any field extension L of K, the L-gonality of the base extension X_L is a lower bound on the K-gonality of X_K. Applying $\mathbb{C}$-gonality bounds for modular curves due to Abramovich [1], one obtains a lower bound on the $\mathbb{Q}$-gonality of $X_1(N)$. This yields[9]

$$\gamma(N) \geq \frac{7}{1600}(N^2 - 1) \geq \frac{21}{200}g(N), \tag{2}$$

for all $N > 12$. The bounds (1) and (2) imply that $\gamma(N)$ is asymptotically quadratic in N, as is $g(N)$, but $\gamma(N)$ may vary within the range

$$\frac{21}{200}g(N) \leq \gamma(N) \leq g(N) \qquad (N > 12).$$

Asymptotically, we can improve the bound $\gamma(N) \leq g(N)$ by a significant constant factor. The parametrization

$$r = (x^2y - xy + y - 1)/(x^2y - x), \qquad s = (xy - y + 1)/(xy)$$

yields a plane model $f_N(x,y) = F_N(r,s) = 0$ for $X_1(N)$, where $F_N(r,s)$ is as defined in [55, §2]; A table of $f_N(x,y)$ for $N < 190$ can be found at [56]. Elkies finds that $\deg_x f_N \to \frac{11}{35}g(N)$ as $N \to \infty$ [10], which implies

$$\limsup_{N\to\infty} \gamma(N) \leq \frac{11}{35}g(N).$$

When N is divisible by 2 or 3 one can do better. Using parameterizations from [12], Elkies has shown [10]

$$\limsup_{M\to\infty} \gamma(2M) \leq \frac{3}{10}g(2M),$$
$$\limsup_{M\to\infty} \gamma(3M) \leq \frac{1}{4}g(3M).$$

It is not known whether the asymptotic upper bound $\frac{11}{35}g(N)$ is optimal. The lower bound $\frac{21}{200}g(N)$ (or $\frac{1}{8}g(N)$ under the Selberg eigenvalue conjecture) is almost surely not asymptotically optimal.[10] Improving these bounds is an **open problem**. A better lower bound would be particularly useful.

[9] Under Selberg's eigenvalue conjecture the constants 7/1600 and 21/200 improve to 1/192 and 1/8, respectively; see [1].

[10] But $\frac{1}{8}g(N)$ might well be an optimal lower bound on the quantity $\delta(N)$ defined in §4.

Table 4: Gonality $\gamma = \gamma(N)$ and genus $g = g(N)$ of $X_1(N)$.

N	γ	g	N	γ	g	N	γ	g	N	γ	g
1	1	0	11	2	1	21	4	5	31	12	26
2	1	0	12	1	0	22	4	6	32	8	17
3	1	0	13	2	2	23	7	12	33	10	21
4	1	0	14	2	1	24	4	5	34	10	21
5	1	0	15	2	1	25	5	12	35	12	25
6	1	0	16	2	2	26	6	10	36	8	17
7	1	0	17	4	5	27	6	13	37	18	40
8	1	0	18	2	2	28	6	10	38	12	28
9	1	0	19	5	7	29	11	22	39	14	33
10	1	0	20	3	3	30	6	9	40	12	25

3.2 Specific bounds on $\gamma(N)$

Unlike the genus $g(N)$, computing the gonality $\gamma(N)$ of $X_1(N)$ is a hard problem. Until recently the exact value of $\gamma(N)$ was known for less than 20 values of N. Thanks to work by Maarten Derickx and Mark van Hoeij, we now know $\gamma(N)$ for all $N \leq 40$; these are listed in the Online Encyclopedia of Integers Sequences [52] as sequence A146879 (see A029937 for $g(N)$). A complete write-up of this work is still in progress, but for the odd values of N see [8, Appendix A], and supporting computational data for all $N \leq 40$ can be found in [9]. The first 40 values of $\gamma(N)$ and $g(N)$ are listed in Table 4.

The method used to prove these bounds begins by computing the $\mathbb{F}_p$-gonality of the reduction of $X_1(N)$ modulo a prime $p \nmid N$, which yields a lower bound on $\gamma(N)$; see [8, Thm. 2.5]. This lower bound is not necessarily tight, but in practice it often is. One can also vary the prime p in the hope of finding a better bound, but it is not known whether for every N there exists a prime p that will yield a tight bound; this is an **open question**. In principle, computing the $\mathbb{F}_p$-gonality of a curve is a finite computation. In practice, many optimizations are needed to make this practical for N up to 40, even for $p = 2$; see [8, §2.3] for details.

Assuming one has a tight lower bound (and there is really no way of knowing this *a priori*), one then looks for a matching upper bound. Currently this is done by attempting to construct a dominant morphism whose degree matches the lower bound (a *gonal morphism*). There is unfortunately no systematic method known for doing this. Instead we rely on various *ad hoc* approaches, such as the optimization algorithms described in [3, 55], and techniques developed by Elkies and by van Hoeij. But in many cases some manual effort and ingenuity is still required; it is more of an art than a science. Developing better methods to compute gonalities and to explicitly construct gonal morphisms is a major **open problem** (one with applications far beyond our current topic).

3.3 The quantity $\delta(N)$ and a theorem of Frey

Let us call a non-cuspidal point on a modular curve X that is defined over a number field of degree d a *degree d point* on X. We have observed that for $d = \gamma(N)$ there are infinitely many degree d points on $X_1(N)$. It is natural to ask whether the converse holds. The answer is almost certainly no. As a possible counterexample, Derickx has shown that there is a degree 130 map from $X_1(131)$ to an elliptic curve with positive rank [6]; such a map can be used to construct infinitely many degree 130 points on $X_1(131)$. But the genus of $X_1(131)$ is 651, which makes it very likely that $\gamma(131) > 130$; we do not know of any examples where $g(N)/\gamma(N)$ exceeds 4, let alone 5. For comparison, the best known upper bound on $\gamma(131)$ is 225; see [56].

Let us define $\delta(N)$ to be the least integer d for which $X_1(N)$ has infinitely many degree d points. We clearly have $\delta(N) \leq \gamma(N)$, and we suspect that this inequality may be strict in some cases (possibly in general). However, the following theorem of Frey [11] implies that $\gamma(N) \leq 2\delta(N)$. It can be viewed as a corollary of Faltings' theorem.

Theorem 8 (Frey)**.** *Let C/k be a projective absolutely irreducible nonsingular curve with a k-rational point. If there are infinitely many points on C defined over extensions K/k of degree at most d, then $\gamma(C) \leq 2d$.*

In our setting $k = \mathbb{Q}$ and $C = X_1(N)$ has a $\mathbb{Q}$-rational point (take any cusp), so Frey's theorem applies.

Remark 9. The bound in Frey's theorem is tight for certain modular curves. As computed by Derickx [6], for $N \in \{53, 61, 65, 79, 83, 89, 101, 131\}$ the curve $X_0(N)$ has $\mathbb{Q}$-gonality 4, but these curves are all known to have infinitely many degree 2 points [2, Thm. 4.3].

Based on the data in Table 4 and our knowledge of which torsion subgroups arise infinitely often for $d \leq 4$ (see §1), we can say that $\delta(N) = \gamma(N)$ for all $N \leq 25$. We also know that if $\delta(N) < \gamma(N)$, then the Jacobian $J_1(N)$ of $X_1(N)$ has positive rank over $\mathbb{Q}$.[11] For $N \leq 40$ the only case where $J_1(N)$

[11] As pointed out to me by Maarten Derickx, if we fix a rational point P on $X_1(N)$,

has positive rank is $N = 37$. Thus we know that $\delta(N) = \gamma(N)$ for all $N \leq 40$, but for $N = 37$ this is an **open question**, as is the more general problem of understanding exactly how and when we can have $\delta(N) < \gamma(N)$ for arbitrary N. It would be especially useful to be able to make this determination without knowing the exact values of $\delta(N)$ and $\gamma(N)$.

Combining Frey's theorem with the lower bounds on $g(N)$ derived form Abramovich's bound, we have

$$\delta(N) \geq \frac{7}{3200}(N^2 - 1). \tag{3}$$

This inequality not only gives a lower bound on $\delta(N)$, we may also view it as an upper bound on N. For any fixed degree d, the largest integer N for which $\delta(N) \leq d$ must satisfy

$$N \leq \sqrt{\frac{3200}{7}d + 1}. \tag{4}$$

This bound is dramatically better than Oesterlé's $N \leq (1 + 3^{d/2})^2$ bound on the largest prime N for which $X_1(N)$ has any degree d points at all. This makes bounding the primes (or arbitrary) N for which $X_1(N)$ has infinitely many degree d points a much easier problem than bounding the set $S(d)$.

Let us define $S^\infty(d)$ as the set of primes N for which $X_1(N)$ has infinitely many degree d points. We saw in §1 that $S^\infty(d) = S(d)$ for all $d \leq 4$, and in fact we also have $S^\infty(5) = S(5)$ (for each $N \in S(5) = \mathsf{Primes}(19)$ one can construct a dominant morphism to $\mathbb{P}^1_\mathbb{Q}$ of degree 5). But this dos not hold for $d = 6$, due to the sporadic point of degree 6 on $X_1(37)$. We can say more: for $d = 6$ the bound in (4) yields $N < 52$, hence $S^\infty(6)$ cannot contain 73. It is not difficult to show that there are infinitely many degree 6 points on $X_1(N)$ for all $N \in \mathsf{Primes}(19)$, thus $S^\infty(6) = \mathsf{Primes}(19)$. For $d = 7$ we get $N < 56$, so from Table 3 we must have $S^\infty(7) \subseteq \mathsf{Primes}(43)$; if any of the primes in $\{59, 61, 67, 73, 113, 127\}$ lie in $S(7)$ it can only be due to the existence of sporadic points.

4 Sporadic points on $X_1(N)$

In §1.2 we defined a *sporadic point* on $X_1(N)$ as a point of degree less than $\delta(N)$, and we saw an example of a sporadic point of degree 3 on $X_1(21)$,

then for all $d < \gamma(N)$ there is an injective map from the dth symmetric power $X_1^{(d)}(N)$ to $J_1(N)$ that sends each rational degree d divisor D to the class $[D - dP]$.

with $\delta(21) = \gamma(21) = 4$. This is the lowest possible degree of any sporadic point, since we know that over number fields of degree $d \le 2$ every torsion subgroup that can occur at all occurs infinitely often.

Only a handful of sporadic points are known that do not correspond to elliptic curves with complex multiplication (we will shortly see how to construct infinitely many sporadic CM points). As observed by van Hoeij in [57], the curve $X_1(37)$ has a point of degree 6. From Table 4, we have $\gamma(37) = 18$, which implies $\delta(N) \ge \gamma(N)/2 = 9 > 6$, thus this point is sporadic. It corresponds to one of two exceptional isomorphism classes of elliptic curves over $\mathbb{Q}$ that admit a rational isogeny of degree 37, the one with j-invariant -9317 (the other isomorphism class has j-invariant -162677523113838677 and does not yield a sporadic point). In the same article van Hoeij also lists points of degrees 9 and 10 on $X_1(29)$, which has $\mathbb{Q}$-gonality 11, and points of degrees 9, 10, and 11 on $X_1(31)$, which has $\mathbb{Q}$-gonality 12. Since $\delta(29) = \gamma(29)$ and $\delta(31) = \gamma(31)$, these are also sporadic points.

As a slightly weaker notion, we may also consider *low degree points* on $X_1(N)$, defined as points of degree $d < \gamma(N)$. Every sporadic point is a low degree point, but the converse need not hold (although we do not yet know of any cases where it does not). In cases where $\delta(N) < \gamma(N)$ there will be infinitely many low degree points on $X_1(N)$. So far no such N is known, but as noted above, $N = 131$ seems a likely candidate, and this may well be the general case.

4.1 Sporadic CM points

We now show how the theory of complex multiplication can be used to construct sporadic points for all sufficiently large N, following the work of Clark, Cook, and Stankewicz [4]. The basic idea is to use an N-isogeny defined over a field K to obtain torsion points defined over an extension L/K whose degree is linear in N. Since $\delta(N) \ge \gamma(N)/2$ grows quadratically with N, once N is large enough it becomes easy to find sporadic points using elliptic curves with complex multiplication: such curves admit rational isogenies of arbitrarily high degree over any extension of their CM field. The theorem below is an easy generalization of Theorem 3a in [4] to handle composite values of N. In order to facilitate the construction of explicit examples, we give a detailed proof.

Theorem 10. *Let $N > 2$ be an integer and let $\mathcal{O}$ be an imaginary quadratic order of discriminant D. Suppose that for every prime $p|N$, either p splits in $K = \mathbb{Q}(\sqrt{D})$, or p is ramified and $p^2 \nmid N$. Then there exists an elliptic* *curve E/L with an L-rational point of order N such that*

$$[L:\mathbb{Q}] \le \phi(N)\frac{2h(\mathcal{O})}{w(\mathcal{O})},$$

where $h(\mathcal{O}) = \#\mathrm{cl}(\mathcal{O})$ is the class number and $w(\mathcal{O}) = \#\mathcal{O}^\times$ is the size of the unit group.[12]

Proof. let $H(X)$ be the minimal polynomial of the algebraic integer $j(\mathcal{O})$ (the j-invariant of the lattice $\mathcal{O}$), and let $K_\mathcal{O}$ be the ring class field $K(j(\mathcal{O}))$. Let $E/K_\mathcal{O}$ be an elliptic curve whose j-invariant is a root of $H(X)$, so that E has CM by $\mathcal{O}$, and let $y^2 = x^3 + Ax + B$ be a Weierstrass equation for E, with $(A,B) = (0,1)$ if $D = -3$ and $(A,B) = (1,0)$ if $D = -4$.

Under the hypothesis of the theorem, there exists an invertible $\mathcal{O}$-ideal $\mathfrak{n}$ of norm N. By the theory of complex multiplication, the ideal group of $\mathcal{O}$ acts on the roots of $H(X)$ via isogenies; the action of $\mathfrak{n}$ corresponds to a cyclic isogeny ψ of degree N from E to an elliptic curve $E'/K_\mathcal{O}$ that also has CM by $\mathcal{O}$ (possibly $E' = E$). The isogeny ψ is defined over $K_\mathcal{O}$.

The kernel of ψ is a cyclic subgroup of $E[N]$ of order N. Let S be the subset of $\ker\psi$ consisting of the points $P = (P_x, P_y)$ of order N. The set S is invariant under the action of the absolute Galois group of $K_\mathcal{O}$, thus the polynomial $f(X) = \prod_{P\in X}(X - P_x)$ has coefficients in $K_\mathcal{O}$. The set S is also invariant under the action of $\mathrm{Aut}(E)$, whose elements are all defined over K. The action of the automorphism $(x,y) \mapsto (x,-y)$ implies that every root of $f(X)$ occurs with multiplicity 2, so $f(X)$ is a perfect square. For $D = -4$ we also have the automorphism $(x,y) \mapsto (-x, iy)$, which implies that $f(X)$ is a polynomial in X^2, and for $D = -3$ we have the automorphism $(x,y) \mapsto (\zeta_3 x, y)$, which implies that $f(X)$ is a polynomial in X^3

Thus in any case we may write $f(X)$ as $f(X) = h(X^e)^2$, with $h \in K_\mathcal{O}[X]$ and $2e = \#\,\mathrm{Aut}(E) = w(\mathcal{O})$. Now let r be a root of $h(X)$ and define the twist $\tilde{E}$ of E and the point $\tilde{P} \in \tilde{E}(K_\mathcal{O}(r))$ as follows:

- For $D = -3$, let $\tilde{E}\colon y^2 = x^3 + t^3 r^{-1}$ and $\tilde{P} = (t, t^2)$, where $t = 1 + r^{-1}$;
- For $D = -4$, let $\tilde{E}\colon y^2 = x^3 + t^2 r^{-1} x$ and $\tilde{P} = (t, t^2)$, where $t = 1 + r^{-1}$;
- For $D < -4$, let $\tilde{E}\colon y^2 = x^3 + t^2 A + t^3 B$ and $\tilde{P} = (rt, t^2)$, where $t = r^3 + Ar + B$.

[12] Recall that $w(\mathcal{O}) = 2, 4, 6$ for $D < -4$, $D = -4$, $D = -3$, respectively.

One then verifies that $\tilde{P}$ is a rational point of order N on $\tilde{E}/K_{\mathcal{O}}(r)$. The absolute degree of the field $K_{\mathcal{O}}(r)$ is

$$[K_{\mathcal{O}}(r):K_{\mathcal{O}}][K_{\mathcal{O}}:K][K:\mathbb{Q}]\ \le \frac{\phi(N)}{2e}\cdot h(\mathcal{O})\cdot 2=\phi(N)\frac{2h(\mathcal{O})}{w(\mathcal{O})},$$

as desired. □

Remark 11. The constraint that N is not divisible by the square of a ramified prime ensures that we get a *cyclic* N-isogeny. The theorem is not true without this constraint (it fails for $D=-7$ and $N=49$, for example).

Remark 12. Clark et al. prove in [4] that for any fixed D, the degree bound in Theorem 10 is tight for all sufficiently large primes N. We expect this also holds for all sufficiently large integers N satisfying the hypothesis of the theorem. For examples where the degree bound is not tight, consider $N=7,11,19,43,67,163$ and $D=-N$. In this situation the isogeny ψ in the theorem is actually defined over $\mathbb{Q}$, not just over $K=\mathbb{Q}(\sqrt{D})$, which saves a factor of 2 in the degree. But we know from Mazur's theorem on rational isogenies [34] that the list of such cases is finite and includes no $N>163$. The degree bound also fails to be tight at the composite $N=14$ with $D=-7$.

The technique used in the proof of Theorem 10 in the typical case $D<-4$ applies equally well to non-CM elliptic curves E/K that admit a K-rational isogeny of degree N. In fact, the first two non-CM sporadic points we encountered both arise from precisely this type of construction: the elliptic curve 162b used by Najman to obtain a sporadic point on $X_1(21)$ admits a $\mathbb{Q}$-rational 21-isogeny, and, as noted above, the degree 6 point on $X_1(37)$ comes from an elliptic curve that admits a $\mathbb{Q}$-rational 37-isogeny. At first glance the degree $\phi(N)/2$ of the kernel polynomial $h\in K[X]$ might seem to large to obtain these examples. But $h(X)$ need not be irreducible, and we can choose r to be a root of its smallest irreducible factor, which happens to have degree 3 (versus 6) for the sporadic point on $X_1(21)$, and degree 6 (versus 18) for the sporadic point on $X_1(37)$.

The constraints on N in Theorem 10 are not particularly restrictive. With $D=-3$ we can already construct sporadic points for all primes $N\ge 157$ congruent to 1 mod 3, and with $D=-4$ we get sporadic points for all primes $N\ge 229$ congruent to 1 mod 4. For primes $N\equiv 3 \bmod 4$, if we simply let $D=-N$ then Schur's $O(|D|\log|D|)$ bound [50] on $h(D)$ then yields $d\le h(D)N=O(N^{3/2}\log N)$, which is sub-quadratic. One can do better (especially if one is prepared to assume the GRH), but this already implies the following corollary.

Corollary 13 (Clark-Cook-Stankewicz)**.** *There are sporadic CM points on $X_1(N)$ for all sufficiently large primes N.*

Remark 14. This result can be made effective. Alex Rice has shown that the if $d_{\mathrm{CM}}(N)$ is the least degree of a CM point on $X_1(N)$, then we must have $d_{\mathrm{CM}}(N) \leq \delta(N)$ for all primes $N > 911$; see the appendix of [4]. The fact that this inequality is not strict means that we do not necessarily get a sporadic point, but presumably only a slight increase (possibly none) in the bound 911 would make the inequality strict.

4.2 Explicit examples of sporadic CM points

Corollary 13 not withstanding, to my knowledge there is no explicit example of a sporadic CM point on $X_1(N)$ to be found in the literature. Let us now construct some examples using the method given in the proof of Theorem 10.

By examining Table 4 and recalling that $\delta(N) = \gamma(N)$ for $N \leq 40$, $N \neq 37$, we see that the least N for which the degree bound given by Theorem 10 is less than $\delta(N)$ is $N = 31$, where for $D = -3$ we obtain a point of degree $d = h(-3)\phi(31)/3 = 10$, which is less than $\delta(31) = \gamma(31) = 12$. With $D = -3$ we have $K_{\mathcal{O}} = K = \mathbb{Q}(\zeta_3)$, and we start with the curve $E\colon y^2 = x^3+1$. Over $\mathbb{Q}(\zeta_3)$ this curve admits a rational isogeny of degree 31 whose kernel contains 30 points of order 31. The polynomial $f(X)$ whose roots are the x-coordinates of these points has the form $h(X^3)^2$, where

$$\begin{aligned} h(X) = X^5 &+ (-132\zeta_3 + 20)X^4 + (336\zeta_3 + 448)X^3 + (1152\zeta_3 + 2368)X^2 \\ &+ (768\zeta_3 + 1280)X - (6144\zeta_3 + 5120)/31. \end{aligned}$$

If we now let r be a root of $h(X)$ and set $t = 1 + 1/r$, we obtain the elliptic curve

$$\tilde{E}\colon \qquad y^2 = x^3 + t^3/r$$

over the number field $L = \mathbb{Q}(\zeta_3)(r)$, with an L-rational point $\tilde{P} = (t, t^2)$ of order 31. Thus $(\tilde{E}, \tilde{P})$ is a sporadic point on $X_1(31)$ of degree 10.

By using a slightly larger value of N we can actually obtain a sporadic CM point of lower degree. For $N = 34$ and $D = -4$ we obtain a point of degree $d = h(-4)\phi(34)/2 = 8$, which is less than $\delta(34) = \gamma(34) = 10$. We now work over $K_{\mathcal{O}} = K = \mathbb{Q}(i)$ with the curve $E\colon y^2 = x^3 + x$. Over $\mathbb{Q}(i)$ this curve admits a rational isogeny of degree 34 whose kernel contains

$\phi(34) = 16$ points of order 34. The polynomial $f(X)$ whose roots are the x-coordinates of these points has the form $h(X^2)^2$, where

$$h(X) = X^4 + (-20i - 12)X^3 + (-28i - 10)X^2 + (-12i + 20)X - 4i + 1.$$

If we now let r be a root of $h(X)$ and set $t = 1 + 1/r$, we obtain the elliptic curve

$$\tilde{E}\colon \qquad y^2 = x^3 + (t^2/r)x$$

over the number field $L = \mathbb{Q}(i)(r)$, with an L-rational point $\tilde{P} = (t, t^2)$ of order 34. Thus $(\tilde{E}, \tilde{P})$ is a sporadic point on $X_1(34)$ of degree 8.

There are two other values of $N \leq 40$ for which Theorem 10 gives low degree CM points on $X_1(N)$. For $N = 39$ with $D = -3$ we get a point of degree 8, which is less than $\delta(39) = \gamma(39) = 14$ so we have a sporadic point on $X_1(39)$. For $N = 37$ and $D = -3$ we get a point of degree 12, which is less than $\gamma(37) = 18$. We do not know whether this is a sporadic point or not, since we don't know $\delta(37)$.

For $N > 40$ we do not know the value of $\delta(N)$, but we can still use Theorem 10 to construct sporadic CM points. The least N for which the theorem gives a degree d point on $X_1(N)$ with $d < \frac{7}{3200}(N^2 - 1) \leq \delta(N)$ is $N = 111$, with $D = -3$. With these parameters we should obtain a point on $X_1(N)$ of degree

$$d \leq h(-3)\phi(111)/3 = 24,$$

whereas

$$\delta(111) \geq \left\lceil \frac{7}{3200}(111^2 - 1) \right\rceil = 27.$$

Over $\mathbb{Q}(\zeta_3)$ the curve $E\colon y^2 = x^3 + 1$ admits a rational isogeny of degree 111 whose kernel contains $\phi(111) = 72$ points of order 111. The polynomial $f(X)$ whose roots are the x-coordinates of these points has the form $h(X^3)^2$, where

$$\begin{aligned} h(X) = X^{12} &+ (3696\zeta_3 + 7800)X^{11} + (587568\zeta_3 + 646848)X^{10} \\ &+ (-6811968\zeta_3 - 2738432)X^9 + (243279360\zeta_3 + 20256768)X^8 \\ &+ (996913152\zeta_3 - 7077888)X^7 + (1945497600\zeta_3 - 1971572736)X^6 \\ &+ (1713586176\zeta_3 - 5843828736)X^5 + (3137863680\zeta_3 - 2648899584)X^4 \\ &+ (868220928\zeta_3 + 336068608)X^3 + (-2938109952\zeta_3 - 1126170624)X^2 \\ &+ (-1233125376\zeta_3 - 528482304)X - 50331648\zeta_3 + 67108864. \end{aligned}$$

Picking a root r of $h(X)$ and setting $t = 1 + 1/r$, we obtain the elliptic curve $\tilde{E}\colon y^2 = x^3 + t^3/r$ over the number field $L = \mathbb{Q}(\zeta_3)(r)$, which has the

L-rational point $\tilde{P} = (t, t^2)$ of order 111. A `sage` [53] worksheet that verifies this computation is available here. Thus $(\tilde{E}, \tilde{P})$ corresponds to a degree 24 point on $X_1(111)$, and it must be sporadic since $\delta(111) \geq 27$. One can similarly construct a sporadic CM point of degree 52 on $X_1(157)$, see this `sage` worksheet for the details.

5 Acknowledgments

I am grateful to Maarten Derickx for his timely and helpful answers to questions that arose while preparing this talk, and for subsequent comments. I also thank Barry Mazur and Sheldon Kamienny for several helpful discussions, and Filip Najman for his feedback on an early draft of these notes.

References

[1] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, International Mathematics Research Notices (1996), 1005–1011.

[2] Francesc Bars, *Bielliptic modular curves*, Journal of Number Theory **76** (1999), 154–165.

[3] Peter Caday and Andrew V. Sutherland, *Optimized equations for $X_1(N)$ via simulated annealing*, poster at the Algorithmic Number Theory Symposium–ANTS IX, 2010, `http://ants9.org/slides/poster_caday.pdf`.

[4] Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, International Journal of Number Theory **9** (2013), 447–479.

[5] John E. Cremona, *Elliptic curve data for conductors up to* 300000, 2012, `http://homepages.warwick.ac.uk/~masgaj/ftp/data/INDEX.html`.

[6] Maarten Derickx, *e-mail regarding infinitely many rational points on a modular curve of degree $\mathbb{Q}$-gonality* 2, December 2012.

[7] ———, *e-mail regarding the set $S(6)$*, December 2012.

[8] ———, *Torsion points on elliptic curves and gonalities of modular curves*, Master's thesis, Mathematisch Institut, Universiteit Leiden, 2012.

[9] Maarten Derickx and Mark van Hoeij, *$X_1(N)$ gonality data for $n \leq 40$*, 2012, http://www.math.fsu.edu/~hoeij/files/X1N/gonality.

[10] Noam D. Elkies, *e-mail regarding equations for $X_1(N)$*, October 2010.

[11] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel Journal of Mathematics **85** (1994), 79–83.

[12] Sonal Jain, *Points of low height on elliptic surfaces with torsion*, LMS Journal of Computation and Mathematics **13** (2010), 370–387.

[13] Daeyeol Jeon, Chang Heon Kim, and Euisung Park, *On the torsion of elliptic curves over quartic number fields*, Journal of the London Mathematical Society **74** (2006), 1–12.

[14] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arithmetica **113** (2004), 291–301.

[15] Dayeol Joen, Change Heon Kim, and Yoonjin Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Mathematics of Computation **80** (2011), 579–591.

[16] ______, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Mathematics of Computation **80** (2011), 2395–2410.

[17] Sheldon Kamienny, *Points of order p on elliptic curves over $\mathbb{Q}(\sqrt{p})$*, Mathematische Annalen **261** (1982), 414–424.

[18] ______, *On the torsion subgroups of elliptic curves over totally real fields*, Inventiones Mathematicae **83** (1986), 545–551.

[19] ______, *Torsion points on elliptic curves over all quadratic fields*, Duke Mathematics Journal **53** (1986), 157–162.

[20] ______, *Torsion points on elliptic curves over all quadratic fields II*, Bulletin de la Société Mathématique de France **114** (1986), 119–122.

[21] ______, *Torsion points on elliptic curves*, American Mathematical Society Bulletin. New Series **23** (1990), 371–373.

[22] ______, *Torsion points on elliptic curves and q-coefficients of modular forms*, Inventiones Mathematicae **109** (1992), 221–229.

[23] ———, *Torsion points on elliptic curves over fields of higher degree*, International Mathematics Research Notices (1992), 129–133.

[24] Sheldon Kamienny and Filip Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arithmetica **152** (2012), 291–305.

[25] M. A. Kenku, *Rational* 2^n*-torsion points on elliptic curves defined over quadratic fields*, Journal of the London Mathematical Society (2) **11** (1975), 93–98.

[26] ———, *Certain torsion points on elliptic curves defined over quadratic fields*, Journal of the London Mathematical Society (2) **19** (1979), 232–240.

[27] ———, *On the modular curves* $X_0(125), X_1(25)$*, and* $X_1(49)$, Journal of the London Mathematical Society (2) **23** (1981), 415–427.

[28] ———, *Rational torsion points on elliptic curves defined over quadratic fields*, Journal of the Nigerian Mathematical Society **2** (1983), 1–16.

[29] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Naguya Mathematical Journal **109** (1988), 125–149.

[30] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proceedings of the London Mathematical Society **33** (1976), 193–237.

[31] Álvaro Lozano-Robledo, *On the field of definition of* p*-torsion points on elliptic curves over the rationals*, Mathematische Annalen **357** (2013), 279–305.

[32] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques I.H.E.S. **47** (1977), 33–186.

[33] ———, *Rational points on modular curves*, Modular forms of one variable V, Lecture Notes in Mathematics, vol. 601, Springer-Verlag, 1977, pp. 107–148.

[34] ———, *Rational isogenies of prime degree*, Inventiones Mathematicae **44** (1978), no. 2, 129–162.

[35] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Inventiones Mathematicae **124** (1996), 437–449.

[36] Toshitsune Miyake, *Modular forms*, Springer, 2006, english translation by Yoshitaka Maeda.

[37] Fumiyuki Momose, *p-torsion points on elliptic curves over quadratic fields*, Nagoya Mathematical Journal **96** (1984), 139–165.

[38] ______, *Rational points on the modular curves $X_{split}(p)$*, Compositio Mathematica **52** (1984), no. 1, 115–137.

[39] Filip Najman, *Exceptional elliptic curves over quartic fields*, International Journal of Number Theory **8** (2012), 1231–1246.

[40] ______, *On the number of elliptic curves with prescribed isogeny or torsion group over number fields of prime degree*, 2012, preprint, http://arxiv.org/abs/1109.6278.

[41] ______, *Torsion of elliptic curves over cubic fields*, Journal of Number Theory **132** (2012), 26–36.

[42] ______, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, 2012, preprint, http://arxiv.org/abs/1211.2188.

[43] Pierre Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, Journal für die Reine und Angewandte Mathematik **506** (1999), 85–116.

[44] ______, *Torsion des courbes elliptiques sur les corps cubiques*, Annales de l'Institut Fourier **50** (2000), 723–729.

[45] ______, *No 17-torsion on elliptic curves over cubic number fields*, Journal de Théorie des Nombres de Bordeaux **15** (2003), 831–838.

[46] Clayton Petsche, *Small rational points on elliptic curves over number fields*, New York Journal of Mathematics **12** (2006), 257–268.

[47] Bjorn Poonen, *Gonality of modular curves in characteristic p*, Mathematical Research Letters **14** (2007), no. 4, 691–701.

[48] F. Patrick Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arithmetica **144** (2010), 17–52.

[49] Markus A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Mathematics of Computation **46** (1986), 637–658.

[50] I. Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Polya: Über die Verteilung der quadratischen Reste und Nichtreste*, Nachr. Kon. Ges. Wiss. Göttingen, Math.-phys. Kl. (1918), 30–36, in Gesammelte Abhandlungen, vol. II, pp. 239–245, Springer, 1973.

[51] Goro Shimura, *Introduction to the theory of automorphic forms*, Princeton University Press, 1971.

[52] Neil J. A. Sloane, *The on-line encyclopedia of integer sequences*, 2012, published electronically at http://oeis.org.

[53] William A. Stein et al., *Sage Mathematics Software (Version 5.0.1)*, The Sage Development Team, 2012, http://www.sagemath.org.

[54] Michael Stoll, *Torsion points on elliptic curves over quartic number fields*, talk at the Algorithmic Number Theory Symposium — ANTS IX, 2010, http://www.mathe2.uni-bayreuth.de/stoll/talks/ANTS2010-1-EllTorsion.pdf.

[55] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Mathematics of Computation **81** (2012), 1131–1147.

[56] ———, *Defining equations for $X_1(N)$*, 2012, http://math.mit.edu/~drew/X1_altcurves.html.

[57] Mark van Hoeij, *Low degree places on the modular curve $X_1(N)$*, 2012, http://arxiv.org/abs/1202.4355.