PRIME ORDER TORSION ON ELLIPTIC CURVES OVER NUMBER FIELDS PART I: ASYMPTOTICS

MAARTEN DERICKX AND MICHAEL STOLL

ABSTRACT. We study the asymptotics of the set $S(d)$ of possible prime orders of K-rational points on elliptic curves over number fields K of degree d as d tends to infinity. Assuming some conjectures on the sparsity of newforms of weight 2 and prime level with unexpectedly high analytic rank, we show that $\max S(d) \leq 3d + 1$ for sufficiently large even d and $\max S(d) = o(d)$ for odd d.

1 Introduction

This paper builds on [DKSS23] by the present authors together with Kamienny and Stein. For the convenience of the reader, we introduce the relevant context here.

Let K be an algebraic number field and let E be an elliptic curve over K. Then by work of Mordell [Mor22] and Weil [Wei29] the group $E(K)$ of K-rational points on E is a finitely generated abelian group; in particular, its torsion subgroup $E(K)_{\text{tors}}$ is a finite abelian group (this can also be shown in a number of more elementary ways than relying on the Mordell-Weil theorem), and one can ask which finite abelian groups can occur as the torsion subgroup of $E(K)$ for some elliptic curve over some number field K of some fixed degree d.

For $K = \mathbb{Q}$ (equivalently, $d = 1$), Mazur [Maz77, Maz78] famously proved that there are only finitely many possibilities for the torsion subgroup and confirmed that the conjectured list is complete. Later, Merel [Mer96] extended this by showing that for any given degree d, there are only finitely many possibilities for $E(K)_{\text{tors}}$ when $[K : \mathbb{Q}] = d$. These have been determined explicitly for $d = 2$ by Kamienny [Kam92] building on work by Kenku and Momose [KM88], for $d = 3$ by Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown [DEvH$^+$21] building on previous work of Jeon, Kim and Schweizer [JKS04] and Bruin and Najman [BN15], and very recently also for $d = 4$ by Derickx and Najman [DN25].

One key step in these finiteness results is to show that there are only finitely many prime numbers p that can divide the order of $E(K)_{\text{tors}}$, i.e., can occur as the order of an element of $E(K)$, for K of degree d. This motivates the following definition (following [KM95]).

Definition 1.1. Let $n \geq 1$ be an integer. Then we define $S(d)$ to be the set of all prime numbers p such that there exists a number field K of degree d, an elliptic curve E over K and a point $P \in E(K)$ such that P has order p.

Following [DKSS23], we write $\text{Primes}(x)$ for the set of all prime numbers p such that $p \leq x$.

Date: May 19, 2025.
2020 *Mathematics Subject Classification.* Primary 11G05, 11G18, Secondary 14G05, 14G25, 14G35.
Key words and phrases. Elliptic curve, torsion point, number fields.

The following values of $S(d)$ are known.

Theorem 1.2.

$$\begin{aligned} S(1) &= \mathrm{Primes}(7) && \text{[Maz77, Maz78]},\\ S(2) &= \mathrm{Primes}(13) && \text{[Kam92]},\\ S(3) &= \mathrm{Primes}(13) && \text{[Par00, Par03]},\\ S(4) &= \mathrm{Primes}(17) && \text{[DKSS23]},\\ S(5) &= \mathrm{Primes}(19) && \text{[DKSS23]},\\ S(6) &= \mathrm{Primes}(19) \cup \{37\} && \text{[DKSS23]},\\ S(7) &= \mathrm{Primes}(23) && \text{[DKSS23]}, \quad \textit{and}\\ S(8) &= \mathrm{Primes}(23) && \text{[Kha24]}. \end{aligned}$$

The recent determination of $S(8)$ by Khawaja follows the approach taken in [DKSS23]. In the second part of this series we will give an alternative proof that requires less computation.

It is much easier to determine the set $S'(d)$ of primes p such that there are *infinitely many* elliptic curves E over number fields K of degree d with distinct j-invariants that have a K-point of order p. This is mostly a question about the gonality of the modular curve $X_1(p)$. The following is known.

Proposition 1.3.

$$\begin{aligned} &S'(1) = \mathrm{Primes}(7), && S'(2) = \mathrm{Primes}(13), && S'(3) = \mathrm{Primes}(13), && S'(4) = \mathrm{Primes}(17),\\ &S'(5) = \mathrm{Primes}(19), && S'(6) = \mathrm{Primes}(19), && S'(7) = \mathrm{Primes}(23), && S'(8) = \mathrm{Primes}(23). \end{aligned}$$

For $d = 1, 2, 3, 4$, this is shown in [Maz77, Kam92, JKL11a, JKL11b], respectively; for $5 \le d \le 8$, this follows from [DvH14, Thm. 3].

The gonality of $X_1(p)$ grows like p^2 [Abr96]; this implies that $S'(d) \subset \mathrm{Primes}\big(O(\sqrt{d})\big)$; see Proposition 3.6 below. On the other hand, denoting by $S_{\mathrm{CM}}(d)$ the set of primes that can occur as orders of points on elliptic curves with complex multiplication over a number field of degree d, the results of [CCS13] show that $S_{\mathrm{CM}}(s) \subset \mathrm{Primes}\big(O(d)\big)$ and that $3d+1 \in S_{\mathrm{CM}}(d)$ when $3d+1$ is prime. (Let $p = 3d+1$. There is a pair of quadratic points defined over $\mathbb{Q}(\sqrt{-3})$ with j-invariant zero on $X_0(p)$. The set-theoretic preimage gives a Galois orbit of points of degree $2 \cdot \frac{p-1}{2} \cdot \frac{1}{3} = d$ on $X_1(p)$, since the covering $X_1(p) \to X_0(p)$ ramifies with index 3 above the points with j-invariant zero.) So we will certainly have $S'(d) \subsetneq S(d)$ for infinitely many d. The data in [vH14] suggest that this is the case for all $d \ge 9$; by [DKSS23, Prop. 1.4], we know that $S(6) \setminus S'(6) = \{37\}$.

It is perhaps tempting to assume that for large enough d, the only sporadic points of degree d on $X_1(p)$ are CM points, as this seems to be the expectation for rational points on modular curves in general. This would imply that $S(d) \subseteq \mathrm{Primes}(3d+1)$ for large d. However, consulting the table in [vH14], it appears that there are many sporadic non-CM points (like the degree 6 points on $X_1(37)$ mentioned above). Still, the bound $p \le 3d+1$ is consistent with this information for $d \ge 13$. One of our aims in this paper is to show that such a bound for large d is implied by conjectures on the sparsity of newforms of prime level and weight 2 that have unexpectedly large analytic rank.

For the necessary background on modular curves, in particular the definition of the modular curve X_H between $X_1(p)$ and $X_0(p)$, where H is a subgroup of $\mathrm{Aut}(X_1(p)/X_0(p)) = (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$, see [DI95] or [DKSS23, Section 2].

In this first part of a pair of papers, we will focus on the asymptotic behavior of the set $S(d)$ as d tends to infinity. The second part will consider specific small values of d.

Acknowledgments

We would like to thank Drew Sutherland for fruitful discussions and in particular for his very valuable help with the computational aspects of this study and Loïc Merel for some information around the gonality lower bound.

2 Kernels of Hecke correspondences

Let $N \geq 1$ be an integer and fix a subgroup $H \subseteq G := (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. X_H will denote the modular curve $X_1(N)/H$. We denote by $C_H \subseteq X_H$ the subscheme consisting of the (finitely many) cusps.

We recall [DKSS23, Prop. 2.3], slightly strengthened using the observation that the rational cusps on X_H are killed by $T_q - \langle q \rangle - q$ when $q \nmid N$.

Proposition 2.1. *Let $q \nmid N$ be a prime and $P \in J_H(\mathbb{Q})_{\mathrm{tors}}$ such that q is odd or P is a sum of a point of odd order and a point in the subgroup generated by differences of rational cusps. Then $(T_q - \langle q \rangle - q)(P) = 0$.*

The following is a more general version of [DKSS23, Prop. 2.4].

Proposition 2.2. *Let $N \geq 1$ be an integer and fix a subgroup $H \subseteq G := (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$. Let $h_1, h_2 \in \mathbb{Z}_{\geq 0}[G/H][x]$ be polynomials whose coefficients are linear combinations of diamond operators on X_H with nonnegative integer coefficients. We assume that h_1 is monic and that $\deg(h_1) > \deg(h_2) \geq 0$. Let $q \nmid N$ be a prime. Then $t_1 = h_1(T_q)$ and $t_2 = h_2(T_q)$ can be considered as (effective) correspondences on X_H, and so $t = t_1 - t_2$ induces an endomorphism of the divisor group of X_H over $\mathbb{C}$. If D is a divisor on X_H such that $t(x) = 0$, then D is supported in cusps.*

Proof. We set $d_1 = \deg(h_1)$ and $d_2 = \deg(h_2)$.

A non-cuspidal point $x \in X_H(\mathbb{C})$ corresponds to an elliptic curve E over $\mathbb{C}$ with additional structure. The point $\langle a \rangle(x)$ corresponds to the same curve E (with modified extra structure), and $T_q(x)$ is a sum of points corresponding to all the elliptic curves that are q-isogenous to E. We define the q-*isogeny graph* G_q to have as vertices the isomorphism classes of all elliptic curves over $\mathbb{C}$; two vertices are connected by an edge when there is a q-isogeny between the corresponding curves. There is a natural map γ from $X_H(\mathbb{C}) \setminus C_H(\mathbb{C})$ to the vertex set of G_q. Let x be a non-cuspidal point in the support of a divisor D on X_H and let $G_{q,x}$ be the connected component of G_q containing $\gamma(x)$. Let E be the elliptic curve given by x. We distinguish two cases.

First, assume that E does not have CM. Then $G_{q,x}$ is an infinite $(q+1)$-regular tree. The image under γ of the support of $h_1(T_q)(x)$ is contained in the d_1-ball around $\gamma(x)$ and contains all the vertices at distance d_1 from $\gamma(x)$, whereas the image of the support of $h_2(T_q)(x)$ is contained in the d_2-ball and (since $d_2 < d_1$) does not contain vertices at distance d_1 from $\gamma(x)$. Now consider a vertex v of G_x that has maximal possible distance from $\gamma(x)$ among all vertices of the form $\gamma(y)$ for a non-cuspidal point y in the support of D. Let $y_1, \dots, y_n$ be the points in the support of D such that $\gamma(y_j) = v$, and let $w \in G_x$ be a point at distance d_1 from v whose distance from $\gamma(x)$ is larger by d_1 than that of v. Each $h_1(T_q)(y_j)$ contains precisely one point y_j' such that $\gamma(y_j') = w$, and these points are distinct for distinct points y_j (since the map from X_H to the j-line is étale above the points in G_x). Then w is not of the form $\gamma(z)$ for a point z in the support of $h_2(T_q)(D)$. This shows that $t(D)$ has non-empty support, so $t(D)$ cannot be zero when D has non-CM non-cuspidal points in its support.

Now consider the case that E has CM by an order $\mathcal{O}$ in an imaginary quadratic field. If q is inert in $\mathcal{O}$, then $G_{q,x}$ is a $(q+1)$-regular tree again, and we can argue as before. Otherwise, $G_{q,x}$ has the structure of a "volcano"; see [Sut13]. For a CM elliptic curve over $\mathbb{C}$, this volcano has infinite depth. Concretely, this means that it consists of a number of rooted $(q+1)$-regular trees whose roots form a cycle (of length ≥ 1). We can now argue as in the first case by choosing v to be a vertex of maximal level (i.e., distance from the root cycle) and w to be at distance d_1 from v and level larger by d_1. This shows that there can be no CM points in the support of D as well. If $j(x) = 0$ (so $\operatorname{disc}(\mathcal{O}) = -3$) or $j(x) = 1728$ (so $\operatorname{disc}(\mathcal{O}) = -4$), the structure of $G_{q,x}$ is slightly different. It should be considered as a directed graph (with edges directed according to the direction of the isogeny); then the difference is that the edges pointing away from the root cycle have multiplicity 3 (resp., 2), whereas all other edges are simple. The map from X_H to the j-line is étale away from the root cycle, so in particular at the vertex w, and it is still true that $t(D)$ has positive coefficients at some points mapping to w.

The only points that we have not excluded from the support of D are the cusps; this proves the claim. □

3 Gonality of modular curves

One of our workhorse results, Proposition 4.1, is based on a lower bound for the gonality of the modular curve we want to apply it to. Recall the following definition.

Definition 3.1. Let X be a smooth projective and geometrically irreducible curve over a field k. The k-*gonality of* X, $\operatorname{gon}_k(X)$, is the smallest degree of a non-constant rational function on X defined over k.

Clearly, if $k \subseteq K$ is a field extension, then $\operatorname{gon}_k(X) \geq \operatorname{gon}_K(X)$.

We write $X^{(d)}$ for the dth symmetric power of a curve X. Its points classify effective divisors of degree d on X; in particular, the points in $X^{(d)}(K)$ correspond to K-rational effective divisors of degree d on X. We will identify effective divisors and points on $X^{(d)}$ in this paper without further mention. We write $[D]$ for the linear equivalence class of a divisor D.

The following is a trivial consequence of the definition above.

Lemma 3.2. *Let X be a smooth projective and geometrically irreducible curve over a field k and let $x, y \in X^{(d)}(k)$ be two points such that $[x - y] = 0$ in the Jacobian of X. If $d < \operatorname{gon}_k(X)$, then $x = y$.*

Proof. The assumption $[x - y] = 0$ says that $x - y$, considered as a divisor of degree zero, is the divisor of some rational function $f \in k(X)^\times$. If f were non-constant, it would follow that $\deg(f) \leq d < \operatorname{gon}_k(X)$, a contradiction. So f must be constant, which implies that $x - y = 0$. □

We need some information on the gonality of the curves X_H.

Theorem 3.3 (Yau, Abramovich, Kim-Sarnak). *Let p be a prime number and let $H \subseteq (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ be a subgroup. Then*

$$\operatorname{gon}_{\mathbb{Q}}(X_H) \geq \gamma \frac{p^2-1}{2\#H} \qquad \textit{with} \qquad \gamma = \frac{325}{2^{15}}.$$

In particular,

$$\operatorname{gon}_{\mathbb{Q}}(X_1(p)) \geq \gamma \frac{p^2-1}{2} \qquad \textit{and} \qquad \operatorname{gon}_{\mathbb{Q}}(X_0(p)) \geq \gamma(p+1).$$

Proof. By [Abr96] and the fact that $(p^2-1)/(2\#H)$ is the degree of the map from X_H to the j-line, we have that

$$\operatorname{gon}_{\mathbb{Q}}(X_H) \geq \operatorname{gon}_{\mathbb{C}}(X_H) \geq \frac{\lambda_1}{24} \frac{p^2-1}{2\#H},$$

where λ_1 is the smallest positive eigenvalue of the Laplace operator on $X_H(\mathbb{C})$, and by [Kim03], $\lambda_1 \geq 975/4096$. □

The argument given in Abramovich's paper is originally due to Yau (unpublished).

Remark 3.4. Selberg's Conjecture says that $\lambda_1 \geq \frac{1}{4}$. If it holds, then we can take $\gamma = \frac{1}{96}$ in the bound above.

Derickx and van Hoeij [DvH14] have determined the $\mathbb{Q}$-gonality of $X_1(N)$ for $N \leq 40$. In these cases, the $\mathbb{Q}$-gonality is achieved by a modular unit, i.e., a function on $X_1(N)$ whose zeros and poles are cusps. We propose the following conjecture (compare Question 1 in [DvH14]).

Conjecture 3.5. *Let p be a prime. There is a modular unit f defined over $\mathbb{Q}$ on $X_1(p)$ such that $\operatorname{gon}_{\mathbb{Q}}(X_1(p)) = \deg f$.*

According to [DvH14, p. 57][1], we have the upper bound (writing $\lfloor a \rceil$ for the integer closest to a)

$$\operatorname{gon}_{\mathbb{Q}}(X_1(p)) \leq \left\lfloor \frac{11(p^2-1)}{840} \right\rceil.$$

In fact, at the time of writing, only three values of p are known for which $X_1(p)$ has a $\mathbb{Q}$-rational function of degree $< \left\lfloor \frac{11(p^2-1)}{840} \right\rceil$. These values are $\{31, 67, 101\}$, in which case a function of degree $\left\lfloor \frac{11(p^2-1)}{840} \right\rceil - 1$ is known according to the table in [DvH14].

In this light it is interesting to ask the question whether the limit

$$\lim_{p \to \infty} \frac{\operatorname{gon}_{\mathbb{Q}}(X_1(p))}{p^2-1}$$

exists. And if it exists, wether it is close to the upper bound $\frac{11}{840} \approx 0.0131$ or to the lower bound $\frac{325}{2^{16}} \approx 0.00496$ (or $\frac{1}{192} \approx 0.00521$ under Selberg's Conjecture).

[1] Actually there it is mentioned that $\operatorname{gon}_{\mathbb{Q}}(X_1(p)) \leq \left\lfloor \frac{11p^2}{840} \right\rceil$, but these values are equal as can be seen by studying the possible values of $11p^2$ modulo 840.

The known growth of the gonality of $X_1(p)$ implies the following.

Proposition 3.6. *There are constants $C_1' \geq C_1 > 0$ such that for all $d \geq 1$,*

$$\mathrm{Primes}(\sqrt{C_1 d + 1}) \subset S'(d) \subset \mathrm{Primes}(\sqrt{C_1' d + 1}).$$

Proof. By a result of Frey [Fre94], $p \in S'(d)$ implies $\mathrm{gon}_{\mathbb{Q}}(X_1(p)) \leq 2d$. Combined with Theorem 3.3, this gives the upper bound (with $C_1' = 4\gamma^{-1}$). Conversely, if X is a curve of genus g over $\mathbb{Q}$ with a rational point, then the Riemann-Roch Theorem implies that there are functions in $\mathbb{Q}(X)^\times$ of exact degree d for each $d \geq 2g - 1$, so there are infinitely many points of degree d on X (this uses the Hilbert Irreducibility Theorem). Since the genus of $X_1(p)$ is $\leq (p^2-1)/24$, this gives the lower bound (with $C_1 = 12$). □

4 A criterion for ruling out moderately large primes

In [DKSS23, Prop. 7.1], we gave a criterion in terms of the gonality and the degree of a point on $X_1(p)$ to arise as a pull-back from an intermediate modular curve. We extend this result to intermediate curves X_H and more general not necessarily prime level N, which we anticipate will be useful for future applications (although we will only require the case $X_1(p)$ with p prime in this paper).

Proposition 4.1. *Let $d \geq 1$, let N be an integer, $\ell \nmid N$ a prime and let H be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$ containing -1. Let $a \in \big((\mathbb{Z}/N\mathbb{Z})^\times/\{\pm1\}\big)/H$ be such that*

$$A := (\langle a \rangle - 1)(J_H(\mathbb{Q}))$$

is finite. When $\ell = 2$, we additionally assume that $A[2]$ is killed by $T_2 - \langle 2 \rangle - 2$ (by Proposition 2.1, this follows when $A[2]$ is contained in the subgroup generated by differences of rational cusps). We set

$$n = \begin{cases} 2\ell + 1 & \text{if } a \in \{\ell, \ell^{-1}\}, \\ 2\ell + 2 & \text{if } a \notin \{\ell, \ell^{-1}\}. \end{cases}$$

Then any rational point on $X_H^{(d)}$ of degree $d < \mathrm{gon}_{\mathbb{Q}}(X_H)/n$ and without cusps in its support is a sum of orbits under $\langle a \rangle$.

Remark 4.2. By Theorem 3.3, the inequality $d < \mathrm{gon}_{\mathbb{Q}}(X_H)/n$ above holds when $N = p$ is prime and

$$d < \frac{325}{2^{15}} \frac{p^2 - 1}{2n \cdot \#H}.$$

We note that when $N = p > 3$ is prime, we can always take $\ell = 3$; then $n \leq 8$.

Proof. Compare the proof of [DKSS23, Prop. 7.1]. Our assumptions together with Proposition 2.1 imply that $T_\ell - \langle \ell \rangle - \ell$ kills A. Let $x \in X_H^{(d)}(\mathbb{Q})$ without cusps in its support. Then as in [DKSS23] we obtain the linear equivalence of effective divisors on X_H

$$(\langle a \rangle T_\ell + \langle \ell \rangle + \ell) \cdot x \sim (T_\ell + \langle \ell a \rangle + \ell \langle a \rangle) \cdot x.$$

If $a \in \{\ell, \ell^{-1}\}$, then we can cancel $\langle \ell \rangle x$ or x, so that the divisors involved have degree $(2\ell + 1)d$; otherwise they have degree $(2\ell + 2)d$. In both cases, the degree is nd. By Lemma 3.2, it follows that both sides are equal as divisors, so

$$(T_\ell - \langle \ell \rangle - \ell) \cdot (\langle a \rangle x - x) = 0.$$

Then Proposition 2.2 implies that $\langle a\rangle x - x$ is supported on cusps. As x does not contain cusps in its support by assumption, it follows that $\langle a\rangle x = x$, which is equivalent to saying that x is a sum of orbits of $\langle a\rangle$. □

Regarding the extra condition when $\ell = 2$ in the case $X_H = X_1(p)$, we quote the following, which is Conjecture 6.2.2 in [CES03].

Conjecture 4.3. *Let p be a prime. Then the rational torsion subgroup of $J_1(p)$ is generated by differences of rational cusps.*

Remark 4.4. In [CES03], this is shown for all primes $p \le 157$ with the exception of

$$p \in \{29, 97, 101, 109, 113\},$$

and in these cases, they bound the index of the subgroup generated by differences of rational cusps by 2^6, 17, 2^4, 3^7, and $2^{12} \cdot 3^2$, respectively. In [DKSS23, Thm. 3.2], the conjecture is shown for $p = 29$. Davide De Leo establishes the conjecture for the remaining open cases (for $p \le 157$) in his Master's thesis [DL24, DLS25]. This implies that the 2-primary part of $J_1(p)(\mathbb{Q})_{\mathrm{tors}}$ is contained in the subgroup generated by differences of rational cusps for all $p \le 157$.

We fix $N = p$ to be a prime. Then the orbits under $\langle a\rangle$ on $X_1(p)$ have length $\operatorname{ord}(a)$ (the order of a as an element of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$) unless

- $3 \mid \operatorname{ord}(a)$, so necessarily $p \equiv 1 \bmod 6$, and the points map on $X_0(p)$ to points corresponding to pairs (E, C) with $j(E) = 0$ and C the kernel of an element $\pi \in \operatorname{End}_{\mathbb{C}}(E) \simeq \mathbb{Z}[\omega]$ of norm p, where ω is a primitive cube root of unity; such an orbit has length $\operatorname{ord}(a)/3$, or
- $2 \mid \operatorname{ord}(a)$, so necessarily $p \equiv 1 \bmod 4$, and the points map on $X_0(p)$ to points corresponding to pairs (E, C) with $j(E) = 1728$ and C the kernel of an element $\pi \in \operatorname{End}_{\mathbb{C}}(E) \simeq \mathbb{Z}[i]$ of norm p, where i is a primitive fourth root of unity; such an orbit has length $\operatorname{ord}(a)/2$.

We consider the case that $x \in X_1(p)^{(d)}(\mathbb{Q})$ comes from a non-cuspidal point of degree d on $X_1(p)$, say corresponding to the pair (E, P) of an elliptic curve E defined over a number field K of degree d and a point $P \in E(K)$ of order p, such that $K = \mathbb{Q}(E, P)$. Then the conclusion of Proposition 4.1 implies that for every $m \in \mathbb{Z}$ with $p \nmid m$ such that the image of m in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ is in the subgroup generated by a, (E, mP) is isomorphic to a Galois conjugate of (E, P). This fact can be expressed as follows. Recall that we can always take ($\ell = 3$ and) $n = 8$ in Proposition 4.1.

Corollary 4.5. *Let $d \ge 1$ be an integer and let p be a prime such that $8d < \operatorname{gon}_{\mathbb{Q}}(X_1(p))$. Assume that there is some nontrivial subgroup H of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ such that all simple factors of $J_1(p)$ of positive (analytic) rank are factors of J_H.*

Let $x \in X_1(p)^{(d)}(\mathbb{Q})$ be a point without cusps in its support. Then either x contains points with j-invariant 0 or 1728, or $d = m \cdot \#H$ for some integer m and x arises as the pull-back of a point in $X_H^{(m)}(\mathbb{Q})$.

Proof. We take a to be a generator of (the cyclic group) H; then A in Proposition 4.1 is finite by assumption. The gonality condition in Proposition 4.1 is also satisfied by assumption. So x is a sum of H-orbits. If the support of x does not contain points with j-invariant 0 or 1728, then all these H-orbits in x have length $\#H$, which shows that

$d = m \cdot \#H$ for some integer m. This also implies that x is the pull-back of a point in $X_H^{(m)}(\mathbb{Q})$. □

We would like to take $H = (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. We can do that unless there is a positive-rank factor of $J_1(p)$ that corresponds to an orbit of newforms with nontrivial character. Such an orbit exists by definition if and only if p is strange in the sense of Section 5 below. We will come back to the implications for $S(d)$ in Section 7.

5 Strange primes

In view of the criterion discussed in Section 4, we make the following definition. We state it for general levels N, even though we will be only concerned with prime levels in this paper.

Definition 5.1. Let $N \geq 1$ be an integer, χ a Dirichlet character of modulus N and let f be a newform for $\Gamma_1(N)$ of weight 2 and character χ.

(1) The newform f is *strange*, if χ is nontrivial and $L(f, 1) = 0$, i.e., the analytic rank of the associated abelian variety A_f is positive.
(2) The character χ is *strange*, if there exists a divisor $M \mid N$ and a strange newform f of weight 2 on $\Gamma_1(M)$ with character χ' such that χ is the induction of χ'.
(3) N is *strange* if there is a strange newform whose level divides N.
(4) The *strangeness* $\mathrm{str}(N)$ of N is the order of the group generated by all strange characters mod N. In particular, $\mathrm{str}(N) > 1$ if and only if N is strange.
(5) The *new strangeness dimension* $\mathrm{strdim}_{\mathrm{new}}(N)$ of N is the number of strange newforms at level N.
(6) The *strangeness dimension* $\mathrm{strdim}(N)$ is defined as

$$\mathrm{strdim}(N) = \sum_{M \mid N} \tau(N/M)\, \mathrm{strdim}_{\mathrm{new}}(M)\,,$$

where $\tau(n)$ denotes the number of divisors of n. In particular, $\mathrm{strdim}(N) > 0$ if and only if N is strange.

The formula for the definition of strdim in terms of $\mathrm{strdim}_{\mathrm{new}}$ is motivated by the Atkin-Lehner-Li decomposition

$$S_k(\Gamma_1(N)) \cong \bigoplus_{M \mid N} \bigoplus_{d \mid N/M} S_K(\Gamma_1(M))_{\mathrm{new}}\,.$$

It counts a strange newform of level $M \mid N$ with the multiplicity it occurs in $S_2(\Gamma_1(N))$.

Since there are no newforms of level 1 and weight 2 it follows that for a prime p one has $\mathrm{strdim}(p) = \mathrm{strdim}_{\mathrm{new}}(p)$.

The LMFDB has complete data of all newforms of weight 2 up to level 1000. In this range, there are only nine strange primes p, and for each of these primes, there is exactly one Galois orbit of strange newforms. They are given in Table 1. The column labeled "ord(χ)" gives the order of the associated character, which is equal to the index of the largest subgroup H we can take in Corollary 4.5 for the prime p. We also give the order of H.

We have extended the range of the LMFDB data by a computation, as follows. Let p be the prime we want to test for strangeness. Pick a (reasonably large, but not too large,

level	ord(χ)	dim A_f	#H
61	6	2	5
97	12	4	8
101	10	4	5
181	6	2	15
193	12	4	8
409	12	4	17
421	6	2	35
733	6	2	61
853	6	2	71

TABLE 1. Newforms f of weight 2, nontrivial character χ and prime level $p < 1000$ such that $L(f, 1) = 0$.

say below 2^{30}) prime $q \equiv 1 \bmod p - 1$. Working mod q, all the Dirichlet characters mod p take values in $\mathbb{F}_q^\times$. So we can compute the space of modular symbols over $\mathbb{F}_q$ associated to any given (even) Dirichlet character χ mod p (we take the subspace fixed by the star involution). We know that $(T_\ell - \ell\langle\ell\rangle - 1)(T_\ell - \langle\ell\rangle - 1)$ maps the modular symbol $-\{0, \infty\}$ into the cuspidal subspace, for every prime ℓ. We find the first ℓ such that the resulting element is nonzero (almost always $\ell = 2$). Write $\mathbf{e}'$ for this element of the cuspidal subspace. Then we find the smallest prime ℓ' such that $T_{\ell',\mathbb{F}_q}$ has squarefree characteristic polynomial on the cuspidal subspace. We then check whether $\mathbb{F}_q[T_{\ell'}] \cdot \mathbf{e}'$ is the full cuspidal subspace. If it is, then the projection of the winding element $\mathbf{e}$ into any of the newform spaces associated to χ (over $\mathbb{Q}$) is nonzero, and it follows that χ is not strange. If, on the other hand, we obtain a smaller subspace, then it is quite likely that χ is indeed strange (since q is taken to be reasonably large); to rigorously prove that, we perform a similar (but much slower) computation in characteristic zero.

Drew Sutherland, using code written by the first author of this paper, found all candidates for strange characters modulo primes $p < 10^5$. The second author used independently written code to corroborate these results for $p < 50\,000$ and to verify that candidates for strange characters are indeed strange. These computations were done using the Modular Symbols functionality of Magma [BCP97]. They result in the following.

Proposition 5.2. *Let $p < 100\,000$ be a prime and let χ be an even Dirichlet character modulo p. The character χ is strange if and only if p and the order of χ are listed in Table 2.*

There are just 74 strange primes up to 10^5. Why should we expect strange primes to be rare? The L-series of a newform f for $\Gamma_0(p)$ satisfies a functional equation $L(f, 2 - s) = \pm L(f, s)$ with sign the negative of the eigenvalue of f under the Fricke involution w_p. So the analytic rank must be odd when f is invariant under w_p. When the character χ of f is nontrivial, however, the coefficient field of f is no longer totally real, but instead totally complex (this follows from the relation $a_\ell = \chi(\ell)\bar{a}_\ell$ for primes $\ell \neq p$; see [Rib77, page 21]), and the functional equation has the form $L(\bar{f}, 2 - s) = \varepsilon L(f, s)$ with $|\varepsilon| = 1$. So the functional equation does not force a zero at $s = 1$, and we can expect it to be rare for a zero to occur, and particularly so when the Galois orbit of f is large.

p	61	97	101	181	193	409	421	733	853
$\mathrm{ord}(\chi)$	6	12	10	6	12	12	6	6	6
$\mathrm{strdim}(p)$	2	4	4	2	4	4	2	2	2

p	1021	1777	1801	1861	2377	2917	3229	3793	4201
$\mathrm{ord}(\chi)$	30	3	5	6	12	6	3	12	3
$\mathrm{strdim}(p)$	8	2	4	6	4	2	2	4	2

p	4733	5441	5821	5953	6133	6781	7477	8681	8713
$\mathrm{ord}(\chi)$	7	10	6	3	6	6	14	10	4, 12
$\mathrm{strdim}(p)$	6	4	2	2	2	2	6	4	$4+4$

p	10093	11497	12941	14533	15061	15289	17041	17053	17257
$\mathrm{ord}(\chi)$	6	3	10	6	6	12	3	6	12
$\mathrm{strdim}(p)$	2	2	4	2	4	4	2	2	4

p	18199	20341	22093	23017	23593	26161	26177	28201	29569
$\mathrm{ord}(\chi)$	3	6	6	12	12	3	4	3	2
$\mathrm{strdim}(p)$	4	2	2	4	4	2	4	2	2

p	31033	31657	32497	35521	35537	36373	39313	41081	41131
$\mathrm{ord}(\chi)$	3	3	3	3	4	6	12	5	3
$\mathrm{strdim}(p)$	2	2	2	2	4	2	4	4	2

p	41593	42793	48733	52561	52691	53113	53857	63313	63901
$\mathrm{ord}(\chi)$	12	3	6	3	5	12	12	12	6
$\mathrm{strdim}(p)$	4	2	2	2	4	4	4	4	2

p	65171	65449	66973	68737	69061	69401	69457	73009	86113
$\mathrm{ord}(\chi)$	5	12	6	12	6	5	4	12	12
$\mathrm{strdim}(p)$	4	4	2	4	2	4	4	4	4

p	86161	96289							
$\mathrm{ord}(\chi)$	4	12							
$\mathrm{strdim}(p)$	4	4							

TABLE 2. Strange primes $p < 100\,000$, orders of strange characters mod p, and the strangeness dimension of p.

One can also use similar heuristics as in Section 8 below: A strong version of the analogue of Maeda's Conjecture for the newforms of level p with a given non-trivial character would say that there should only be few small Galois orbits and one very large one (which is consistent with experimental observations), and there may be reason to believe that the total size of the small orbits grows only slowly or is even uniformly bounded. An analogue of the result of Iwaniec and Sarnak mentioned in Section 8 would then imply that $\mathrm{strdim}(p)$ is bounded by the total size of the small orbits.

Based on the data and heuristics above, we propose the following conjecture.

Conjecture 5.3.

(1) *(Weak form)*

$$\lim_{p\to\infty} \frac{\mathrm{strdim}(p)}{\log p} = 0$$

as p *runs through all prime numbers.*

(2) *(Strong form) The strangeness dimension* $\mathrm{strdim}(p)$ *is uniformly bounded as* p *runs through all prime numbers.*

Part (2) of this conjecture implies that $\mathrm{str}(p)$ is uniformly bounded for all primes p, since the size of the Galois orbit of a strange newform is a multiple of $\varphi(\mathrm{ord}(\chi))$, where χ is the associated strange character and φ is the Euler totient function. So a bound on $\mathrm{strdim}(p)$ implies a bound on $\mathrm{ord}(\chi)$ and therefore also a bound on $\mathrm{str}(p)$.

The strangeness dimensions of all primes below 10^5 are bounded by 8 (which occurs only twice, 6 occurs three times, and all other strangeness dimensions are at most 4; this holds for $p > 10\,000$), and the characters have order bounded by 30 (occurring once; 14 occurs once, all other orders are at most 12). From the data, it therefore appears to be possible that

$$\max_p \mathrm{str}(p) = 30 \qquad \text{and} \qquad \limsup_{p\to\infty} \mathrm{str}(p) = 12$$

and that

$$\max_p \mathrm{strdim}(p) = 8 \qquad \text{and} \qquad \limsup_{p\to\infty} \mathrm{strdim}(p) = 4.$$

6 A source of strange primes

In the following, we describe a source of strange primes p such that the character of the strange newforms has order 6 and the Galois orbit of these newforms has length 2. This case occurs a number of times in Table 2, including for fairly large primes.

Consider a curve X of genus 2 over $\mathbb{Q}$ such that X has an automorphism σ of order 3 defined over $\mathbb{Q}$. Denote the Jacobian variety of X by J. Since the hyperelliptic involution ι of X is in the center of the automorphism group, σ induces an automorphism of order 3 of $\mathbb{P}^1_{\mathbb{Q}}$. We can take this automorphism to be given by $x \mapsto \frac{1}{1-x}$. Then the curve X has a model of the form

$$y^2 = rF_1(x,z)^2 + sF_1(x,z)F_2(x,z) + tF_2(x,z)^2 \tag{6.1}$$

with $r, s, t \in \mathbb{Z}$ and

$$F_1(x,z) = xz(x-z) \qquad \text{and} \qquad F_2(x,z) = x^3 - x^2z - 2xz^2 + z^3.$$

The action of σ is $(x : y : z) \mapsto (z : y : z - x)$; σ has four fixed points (satisfying $x^2 - xz + z^2 = 0$), so the quotient curve $X/\langle\sigma\rangle$ has genus 0. This implies that all divisors of the form $P + \sigma(P) + \sigma^2(P)$ (where P is a point on X) are linearly equivalent. This means that $\sigma^2 + \sigma + 1 = 0$ in $\mathrm{End}(J)$, so that $\mathbb{Z}[\omega] \subseteq \mathrm{End}_{\mathbb{Q}}(J)$, where ω is a primitive cube root of unity. In particular, if J is simple, then J is an abelian surface of GL_2-type and therefore occurs as a simple factor of $J_1(N)$ for some N such that the conductor of J is N^2; see [Rib04, KW09a, KW09b]. Since the endomorphism algebra contains the CM field $\mathbb{Q}(\omega)$, the associated character must be nontrivial. So if we can arrange for J to have conductor p^2 for some prime p and to have positive (analytic) rank, then the associated pair of newforms for $\Gamma_1(p)$ will be strange.

The discriminant of the model of X given in (6.1) above is

$$\Delta(r,s,t) = 2^8(s^2-4rt)^3\left(\tfrac{1}{4}((2r+s-13t)^2+27(s+t)^2)\right)^2.$$

If the right hand side in (6.1) is a square modulo 4, then we can "un-complete the square" and get a new model that is still integral and whose discriminant is $\Delta(r,s,t)/2^{20}$. If we assume that not all of r,s,t are divisible by 4, then we are in this case exactly when

$$(r,s,t) \equiv (0,0,1), \quad (1,0,0) \quad \text{or} \quad (1,2,1) \bmod 4.$$

In this case, $2^4 \mid s^2-4rt$ (and the last factor in the expression for $\Delta(r,s,t)$ above is an integer).

Let $p \equiv 1 \bmod 6$ be a prime. To get a curve X with (minimal) discriminant $\pm p^2$, we can set

$$s^2-4rt = \pm 2^4 \qquad \text{and} \qquad (2r+s-13t)^2+27(s+t)^2 = 4p.$$

Then, up to perhaps a common sign change, (r,s,t) satisfy one of the congruences above, and we do obtain a curve with discriminant $\pm p^2$. Since $p \equiv 1 \mod 3$, we can always write $4p = u^2+27v^2$, and u and v are uniquely determined up to sign. Expressing r and s in terms of u, v and t, the first equation becomes

$$27t^2+2ut-v^2 \pm 2^4 = 0.$$

The discriminant of this quadratic equation in t is

$$4(u^2+27v^2 \mp 2^4\cdot 27) = 4^2(p \mp 108).$$

So if there is to be a solution, $p \mp 108 = m^2$ must be a square. The solutions are then

$$t = \frac{-u \pm 2m}{27},$$

and since $u^2+27v^2 = 4p = 4m^2 \pm 432$, we have that $u \equiv \pm 2m \mod 27$, so that one of the two possibilities will lead to an integral solution. We summarize the discussion so far. Note that the conductor of J must be p^2 if the discriminant of X is $\pm p^2$, since the conductor must be a square and it divides the discriminant.

Proposition 6.1. *Let $m \in \mathbb{Z}$ be such that $p = m^2 \pm 108$ is a prime. Write $4p = u^2+27v^2$ with $u, v \in \mathbb{Z}$ such that $u \equiv 2m \bmod 27$ and set $t = (2m-u)/27 \in \mathbb{Z}$. Then the curve X in (6.1) with $r = (u-v)/2+7t$, $s = v-t$ and t or their negatives (so that $r \equiv 1 \bmod 4$ or $t \equiv 1 \bmod 4$) has minimal discriminant $\pm p^2$. If its Jacobian J is simple, it occurs as a simple factor of $J_1(p)$ with nontrivial character.*

In the case $p = m^2+108 = m^2+27\cdot 2^2$, we must have $u = 2m$ and $v = \pm 4$, because u and v are essentially unique. We then obtain $t = 0$ and $r = \pm m - 2$, $s = 4$, with the sign chosen so that $r \equiv 1 \bmod 4$. (The alternative $r = \pm m + 2$, $s = -4$ leads to an isomorphic curve). The right hand side splits as a product of $xz(x-z)$ and a cubic (with cyclic Galois group). Since u and v are even, 2 is a cubic residue mod p by a famous result due to Gauss.

In the other case, $t \neq 0$, since $u = 2m$ would force v^2 to be negative.

We note that there are two primes, $p = 733$ and $p = 2917$ that can be written as m^2+108 and as m^2-108 (with different m). For these primes, we obtain two non-isomorphic curves.

The list of all primes $p < 10^5$ such that $p = m^2 + 108$ is as follows.

109, 157, 229, 277, 397, 733, 1069, 1789, 2917, 4597, 5437, 6037, 6997, 7333, 8389,
9133, 15733, 19429, 24133, 26029, 27997, 28669, 32869, 37357, 38917, 39709,
43789, 51637, 55333, 58189, 60133, 67189, 72469, 76837, 87133, 90709, 93133.

The list of all primes $p < 10^5$ such that $p = m^2 - 108$ is as follows.

13, **61**, **181**, **421**, **733**, **853**, 1117, 1741, 2293, **2917**, 3373, 3613, 4933, **5821**, **6133**,
6781, **10093**, 10501, **14533**, **17053**, 17581, 18661, 19213, **20341**, **22093**, 23917,
30517, 32653, **36373**, 43573, **48733**, 51421, 54181, 55117, 57973, 60901, **63901**,
66973, **69061**, 70117, 72253, 78853, 82261, 89293, 97861.

The numbers in boldface are those for which there is a pair of strange newforms; these newforms all have character of order 6, and all these newforms are associated to curves X of the type considered here. Somewhat surprisingly, none of the primes of the form $m^2 + 108$ in this range lead to Jacobian of positive rank.

If we assume that the "probability" that a number of the form $N = m^2 - 108$ is prime is a constant multiple of $1/\log N$ (which seems reasonable), then we expect the sum over $\log p$ for such primes $p < B$ to grow like a constant times $\sqrt{B}$. If we assume that all strange characters of order 6 are obtained in this way, then the corresponding sum over the associated primes will grow at most like a constant times $\sqrt{B}$.

Question 6.2. Is it true that *every* pair of strange newforms with character of order 6 is associated to the Jacobian of a curve of the form above?

Question 6.3. Is it true that a curve as above associated to a prime $p = m^2 + 108$ always has Jacobian with Mordell-Weil rank zero?

Question 6.4. Are there similar explanations for the other cases that seem to occur relatively frequently? This refers to pairs of newforms with character of order 3 and to quadruples of newforms with character of order 4, 5, or 12.

Assuming Bunyakovsky's conjecture, we can at least show that there are infinitely many strange primes of the type considered above.

Proposition 6.5. *Let w be a positive integer. If*

$$p = w^4 + 2w^3 + 23w^2 + 22w + 13 = (w^2 + w + 11)^2 - 108 \tag{6.2}$$

is a prime, then there is a pair of strange characters of order 6 at level p; in particular, p is strange.

Proof. We set

$$u = 2w^2 + 2w - 5, \quad v = 2w + 1, \quad t = 1,$$

so

$$r = w^2 + 4, \quad s = 2w, \quad t = 1.$$

Then the curve

$$X_p \colon y^2 = rF_1(x, z)^2 + sF_1(x, z)F_2(x, z) + tF_2(x, z)^2$$

is of the type above for the prime p, and it contains the rational point $P = (0 : 1 : 1)$. Denoting by ι the hyperelliptic involution, we show that $P - \iota(P)$ represents a point Q of infinite order on the Jacobian J_p of X_p. Reducing mod 3 and mod 5, we find that the point has order 19 mod 3 when $3 \mid w^2 + w$ and order 3 otherwise, and it has order 19 mod 5 when $5 \mid w^2 + w$ and order 6 or 9 otherwise. If 15 does not divide $w^2 + w$, this implies that the orders of the reduced points differ. Since the reduction modulo an odd prime is injective on the torsion subgroup, these orders must agree when the point has finite order in $J_p(\mathbb{Q})$. This shows that the point must have infinite order. If $15 \mid w^2 + w$ and Q has finite order, P must have order 19. We can construct the curve above with w an indeterminate and compute 19 times the image of Q on the associated Kummer surface. If this is to be the origin, the first three of the four coordinates must vanish simultaneously, which results in a polynomial equation w has to satisfy; it turns out that the only such (integral) values are $w \in \{-1, 0\}$, which are excluded by our assumptions.

So $J_p(\mathbb{Q})$ has positive rank. All possible reductions mod 11 of X_p (for $w \not\equiv 5 \bmod 11$; otherwise the expression for p is divisible by 11) have a zeta function with irreducible numerator, so J_p must be simple over $\mathbb{Q}$. Since J_p is a simple factor of $J_1(p)$ of positive rank, by [KL89] and [Kat04], it follows that the two associated newforms have positive analytic rank. This shows that the characters of order 6 mod p are strange. □

Remark 6.6. Note that for $w \in \{-1, 0\}$, we have $p = 13$, and the resulting curve is $X_1(13)$, whose Jacobian has rank zero and rational torsion of order 19.

We note that Proposition 6.5 explains the strange primes

$$p = 61, 181, 421, 853, 6781, 10093, 14533, 20341, 48733$$

in our list (where $w = 1, 2, 3, 4, 8, 9, 10, 11, 14$, respectively).

Assuming Bunyakovsky's conjecture for the polynomial in w in (6.2), Proposition 6.5 implies that there are infinitely many strange primes.

7 Behavior of $S(d)$ for large d

We now consider what we can say about $S(d)$ when d gets large.

Since it is more convenient to work with points of exact degree d on $X_1(p)$, we make the following definition.

Definition 7.1. Let $d \geq 1$ be an integer. Then $S_{\mathrm{new}}(d)$ denotes the subset of $S(d)$ consisting of primes p such that $X_1(p)$ has a non-cuspidal point of exact degree d.

So $p \in S_{\mathrm{new}}(d)$ means that there is a pair (E, P) consisting of en elliptic curve E over $\bar{\mathbb{Q}}$ and a point $P \in E$ of order p such that the field of definition of (E, P) (i.e., the fixed field of the stabilizer of (E, P) in the absolute Galois group of $\mathbb{Q}$) is an algebraic number field of degree d.

Remark 7.2. We have $S(d) = \bigcup_{d' \mid d} S_{\mathrm{new}}(d')$, where the union is over all (positive) divisors d' of d.

We have the following consequence of Proposition 4.1.

Corollary 7.3. *Let p be an odd prime. Let H be the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ that is the intersection of the kernels of all strange characters for p (then the index of H is $\mathrm{str}(p)$). Pick a generator a of H and let n be as in Proposition 4.1 for a and $X_1(p)$ (with $\ell = 2$ if possible, else $\ell = 3$). Let $d \geq 1$ be an integer. If $p \in S_{\mathrm{new}}(d)$, then one of the following holds.*

(a) $d \geq \mathrm{gon}_{\mathbb{Q}}(X_1(p))/n$.
(b) $p \equiv 1 \bmod 6$ *and* $d = (p-1)/3$.
(c) $p \equiv 1 \bmod 4$ *and* $d = (p-1)/2$.
(d) d *is a multiple of* $\#H = (p-1)/(2\,\mathrm{str}(p))$, *say* $d = m \cdot \#H$, *and there is a non-cuspidal point of degree* m *on* X_H.

Proof. Since $p \in S_{\mathrm{new}}(d)$, there is a point $x \in X_1(p)^{(d)}(\mathbb{Q})$ coming from a non-cuspidal degree d point P on $X_1(p)$. We assume that $nd < \mathrm{gon}_{\mathbb{Q}}(X_1(p))$, so that we are not in case (a). Then by Proposition 4.1, x is a sum of orbits of H. Since orbit length is stable under the action of the Galois group, all orbits occurring in x have the same length. This length can be $\#H$, $\#H/2$, or $\#H/3$.

(i) If the orbit length is $\#H$, then $d = m \cdot \#H$ for some integer $m \geq 1$. Each H-orbit in the support of x is the pull-back of a point of degree m on X_H, so we are in case (d).
(ii) If the orbit length is $\#H/2$, then $p \equiv 1 \bmod 4$, and P maps to a point on $X_0(p)$ corresponding to an elliptic curve E with j-invariant 1728 together with one of the two subgroups of E of order p stable under $\mathbb{Z}[i]$. Such a point has field of definition $\mathbb{Q}(i)$, which is the CM-field of E. So $\mathbb{Q}(i)$ is contained in the field of definition of P; in particular, d is even. By [Sil88], it follows that $p - 1 \leq 2d$. On the other hand, there are exactly $(p-1)/2$ points on $X_1(p)$ above the two relevant points on $X_0(p)$ ($(p-1)/4$ above each of the two; the covering is ramified with index 2 at these points). This implies that $d = (p-1)/2$, and we are in case (c).
(iii) If the orbit length is $\#H/3$, then $p \equiv 1 \bmod 6$, and we can argue as in the previous case with $j = 0$ in place of $j = 1728$ and $\mathbb{Z}[\omega]$ (and $\mathbb{Q}(\omega)$) in place of $\mathbb{Z}[i]$ (and $\mathbb{Q}(i)$) to deduce that we must be in case (b). □

At the cost of a worse bound on d, we can work with a generator a of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ even when p is a strange prime. The bound depends on the strangeness dimension of p, $\mathrm{strdim}(p)$.

Corollary 7.4. *Let* $p > 3$ *be an odd prime. Pick a generator* a *of* $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$ *and let* n *be as in Proposition 4.1 for* a *and* $X_1(p)$ *(with* $\ell = 2$ *if possible, else* $\ell = 3$*). Let* $d \geq 1$ *be an integer. If* $p \in S_{\mathrm{new}}(d)$*, then one of the following holds.*

(a) $d \geq \dfrac{\mathrm{gon}_{\mathbb{Q}}(X_1(p))}{n\left\lfloor (2\sqrt{2}+3)^{\mathrm{strdim}(p)} \right\rfloor}$.
(b) $p \equiv 1 \bmod 6$ *and* $d = (p-1)/3$.
(c) $p \equiv 1 \bmod 4$ *and* $d = (p-1)/2$.
(d) d *is a multiple of* $(p-1)/2$, *say* $d = m(p-1)/2$, *and there is a non-cuspidal point of degree* m *on* $X_0(p)$.

Proof. Let $f_1, \dots, f_m$, with $m = \mathrm{strdim}(p)$, be the strange newforms at level p, and set $h = \prod_{j=1}^{m}(x - a_2(f_j)) \in \mathbb{Z}[x]$. This polynomial has roots bounded in absolute value by $2\sqrt{2}$, so the coefficient h_j of x^j is bounded by $\binom{m}{j}(2\sqrt{2})^{m-j}$. Similarly to our previous considerations in the proof of Proposition 4.1, it follows that

$$t = (T_\ell - \langle \ell \rangle \ell - 1)h(T_2)(\langle a \rangle - 1)$$

annihilates $J_1(p)(\mathbb{Q})$ (with $\ell = 2$ or 3). It is then easy to see that t can be written as a difference of effective correspondences of degree

$$n \sum_{j=0}^{m} |h_j| 3^j \leq n \left\lfloor \sum_{j=0}^{m} \binom{m}{j} 3^j (2\sqrt{2})^{m-j} \right\rfloor = n \left\lfloor (2\sqrt{2}+3)^m \right\rfloor .$$

(In concrete cases, the degree can be smaller.) When we are not in case (a), then it follows as in the proof of Proposition 4.1 that x must be a sum of orbits of $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. The remainder of the proof then is as for Corollary 7.3 with $H = (\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. □

Fixing d instead of p, we obtain the following.

Corollary 7.5. *Let $d \geq 1$ be an integer. If $p \in S_{\mathrm{new}}(d)$ is a prime, then one of the following holds.*

(a) $p \leq \sqrt{Cd+1}$ *with* $C = 2^{19}/325 \approx 1613.2$.
(b) d *is even and* $p = 2d+1$.
(c) d *is even and* $p = 3d+1$.
(d) $p-1$ *divides* $2\,\mathrm{str}(p)d$, *and there are non-cuspidal points of degree* $2\,\mathrm{str}(p)d/(p-1)$ *on the subcover of degree* $\mathrm{str}(p)$ *above* $X_0(p)$ *of* $X_1(p) \to X_0(p)$. *If*

$$p > \sqrt{C \left\lfloor (2\sqrt{2}+3)^{\mathrm{strdim}(p)} \right\rfloor d + 1}, \tag{7.1}$$

then $(p-1)/2$ *divides* d, *and there are non-cuspidal points of degree* $2d/(p-1)$ *on* $X_0(p)$.

Conversely, we have for any even d *that* $2d+1 \in S_{\mathrm{new}}(d)$ *when* $2d+1$ *is prime and that* $3d+1 \in S_{\mathrm{new}}(d)$ *when* $3d+1$ *is prime.*

Proof. The first statement follows from Corollaries 7.3 and 7.4, together with the gonality lower bound in Theorem 3.3; note that we can always take $n = 8$ in Proposition 4.1.

For the second statement, note that we obtain a point of degree d on $X_1(p)$ for $p = 2d+1$ or $p = 3d+1$ when p is prime and d is even by taking a preimage in $X_1(p)$ of one of the quadratic points on $X_0(p)$ with j-invariant 1728 or 0, respectively. □

Remark 7.6. If we are in case (d) in Corollary 7.5 and p satisfies the bound (7.1), then $p = \frac{2d}{m} + 1$ for some $m \geq 1$ and there are non-cuspidal points of degree m on $X_0(p)$. Since $X_0(p)$ has no non-cuspidal rational points when $p > 163$ by [Maz78], it follows that $m \geq 2$, and therefore $p \leq d+1$.

More generally, we have the following.

Theorem 7.7. *Assume Conjecture 5.3 (1). Then for sufficiently large* d, *we have that*

$$S_{\mathrm{new}}(d) \subseteq \mathrm{Primes}(d+1) \cup \{2d+1, 3d+1\},$$

and $2d+1 \in S_{\mathrm{new}}(d)$ *(resp.,* $3d+1 \in S_{\mathrm{new}}(d)$*) if and only if* d *is even and* $2d+1$ *is prime (resp.,* $3d+1$ *is prime).*

Proof. By Conjecture 5.3 (1), $p > \left\lfloor (2\sqrt{2}+3)^{\mathrm{strdim}(p)} \right\rfloor^2$ when p is sufficiently large. For such p, we then have that the bound (7.1) is satisfied if $p > (Cd+1)^{2/3}$. Take d large enough so that $d+1 > \max\{163, (Cd+1)^{2/3}\}$. For such d, Corollary 7.5 and Remark 7.6 show that $p \in S_{\mathrm{new}}(d)$ implies that either $p \leq (Cd+1)^{2/3} < d+1$, or

$p = (2d/m) + 1 \leq d + 1$ for some $m \geq 2$, or else $p \in \{2d+1, 3d+1\}$ if d is even. Corollary 7.5 also gives us that $p \in S_{\text{new}}(d)$ when d is even and $p \in \{2d+1, 3d+1\}$. □

Corollary 7.8. *Assume Conjecture 5.3 (1).*

(1) *For sufficiently large odd d, we have that*

$$S(d) \subseteq \text{Primes}(d+1)\,.$$

(2) *For sufficiently large even d, we have that*

$$S(d) \subseteq \text{Primes}(d+1) \cup \left\{\tfrac{3}{2}d+1, 2d+1, 3d+1\right\}\,.$$

Proof. This follows from Theorem 7.7 together with $S(d) = \bigcup_{d'|d} S_{\text{new}}(d')$. □

To obtain more precise results, we note that we can mimic for $S_2(\Gamma_0(p))$ and the eigenspaces of the Atkin-Lehner involution what we did in Section 5 using the splitting of $S_2(\Gamma_1(p))$ according to characters. We do this in the next section.

8 Small degree points on $X_0(p)$

Let w denote the Fricke (= Atkin-Lehner) involution on $X_0(p)$. Then the sign in the functional equation of $L(f,s)$, for f a weight 2 newform for $\Gamma_0(p)$, is the negative of the eigenvalue of w on f. So the simple factors of $J_0(p)$ on which w acts as multiplication by -1 have analytic rank an even multiple of their dimension (assuming that the analytic rank of a newform is invariant under the Galois action, which is known when the analytic rank is 0 or 1), whereas the simple factors of the w-invariant part $J_0(p)^+$ (which is the Jacobian of $X_0(p)^+ = X_0(p)/\langle w\rangle$) have analytic rank an odd multiple of their dimension.

We now assume that there are no newforms that have positive even analytic rank; equivalently, the minus part $J_0(p)^-$ with respect to the action of w has analytic rank zero and therefore by [KL89] Mordell-Weil rank zero, so that $J_0(p)^-(\mathbb{Q}) \subseteq J_0(p)(\mathbb{Q})_{\text{tors}}$. Since the torsion subgroup of $J_0(p)(\mathbb{Q})$ is cyclic and generated by the difference of the two rational cusps, it follows that $T_2 - 3$ annihilates $J_0(p)(\mathbb{Q})_{\text{tors}}$ (since T_2 acts on the cusps as multiplication by 3); therefore, $(T_2-3)(w-1)$ annihilates $J_0(p)(\mathbb{Q})$. Let $x \in X_0(p)^{(d)}(\mathbb{Q})$ be a non-cuspidal point and write $\infty \in X_0(p)(\mathbb{Q})$ for the cusp that is the image of $\infty \in \mathbb{P}^1(\mathbb{Q}) \subset \mathfrak{H}^*$. Then (arguing in a similar way as in the proof of Proposition 4.1, but in a simplified situation) $[x - d\cdot\infty] \in J_0(p)(\mathbb{Q})$, so

$$(T_2-3)(w-1)([x - d\cdot\infty]) = (T_2-3)(w-1)([x]) = 0 \in J_0(p).$$

Writing

$$(T_2-3)(w-1) = (T_2 w + 3) - (T_2 + 3w)$$

as a difference of two effective correspondences on $X_0(p)$, we have that $(T_2w+3)(x)$ is linearly equivalent to $(T_2+3w)(x)$. So if $6d$, which is the degree of these two divisors, is less than $\text{gon}_{\mathbb{Q}}(X_0(p))$, then it follows that the divisors must be the same. So we have that

$$(T_2-3)(w-1)(x) = 0$$

as divisors. Now Proposition 2.2, applied to $t = T_2 - 3$ on $X_0(p)$, shows that $w(x) = x$, since there are no cusps in the support of x. This leads to the following result.

Proposition 8.1. *Let $p > 3$ be a prime such that there are no newforms for $\Gamma_0(p)$ that have positive even analytic rank. Let $d \geq 1$ be an integer. If $d < \operatorname{gon}_{\mathbb{Q}}(X_0(p))/6$ and $P \in X_0(p)$ is a non-cuspidal point of degree d, then either P is a fixed point of the Fricke involution (and therefore corresponds to an elliptic curve with CM by an order of discriminant $-p$ or $-4p$), or else d is even and the image of P on $X_0(p)^+$ is a point of degree $d/2$.*

Proof. The discussion preceding the statement of the proposition shows that under the assumptions made, the Galois orbit of P is a union of w-orbits. Since w is defined over $\mathbb{Q}$, all these orbits have the same length. There are then two possibilities.

(1) The orbit length is 1. Then P is a fixed point of w. If (E, C) is the elliptic curve with a subgroup of order p corresponding to P, then this implies that there is an endomorphism α of E such that $\alpha^2 = \pm p$ (since $p \geq 5$, $\operatorname{Aut}(E) = \{\pm 1\}$). The positive sign is impossible, so E must have CM by an order containing $\sqrt{-p}$.

(2) The orbit length is 2. Then d is even, and the images on $X_0(p)^+$ of the Galois conjugates of P correspond to the $d/2$ orbits under w among these points. This implies that the image of P on $X_0(p)^+$ is a point of degree $d/2$. □

According to the LMFDB, exactly 111 of the 1229 primes up to 10 000 have the property that there are weight 2 newforms for $\Gamma_0(p)$ of positive even analytic rank. They are listed in Table 3. We note that Brumer [Bru95] has a table listing the nontrivial splittings into Galois orbits of newforms with negative Fricke eigenvalue; this table also gives what we denote $\dim(A)$ here as the "number of rels". Our table is consistent with his, except that he seems to have missed the positive rank factors at levels 2333 and 2381.

In most cases, there is only one Galois orbit of newforms with positive even analytic rank. The exceptions are $p = 997$ with two newforms defined over $\mathbb{Q}$, $p = 1913$ with one orbit of size 1 and one of size 2, $p = 2843$ with one orbit of size 1 and one of size 3, and $p = 9829$ with two newforms defined over $\mathbb{Q}$. Table 3 also gives the number of newforms of positive even analytic rank, which is the same as the dimension of the smallest abelian subvariety of $J_0(p)^-$ whose group of rational points has the same rank as $J_0(p)^-(\mathbb{Q})$.

When there are newforms f with positive even analytic rank, then we can use a polynomial h that has all $a_2(f)$ as roots and work with $(T_2 - 3)h(T_2)(w - 1)$. This gives the following, which is similar in spirit to Corollary 7.4.

Proposition 8.2. *Given $N \geq 0$, there is a number $\varepsilon_N > 0$ such that whenever $p > 3$ is a prime such that there are at most N weight 2 newforms for $\Gamma_0(p)$ with positive even analytic rank and $1 \leq d \leq \varepsilon_N p$ is an integer, then any non-cuspidal point P of degree d on $X_0(p)$ is either a fixed point of w (and thus a CM point) or d is even and P maps to a point of degree $d/2$ on $X_0(p)^+$. We can take*

$$\varepsilon_N = \frac{325}{3 \cdot 2^{16} \left\lfloor (2\sqrt{2}+3)^N \right\rfloor}.$$

Proof. Let p be a prime as in the statement, and let $f_1, \ldots, f_m$ be the $m \leq N$ weight 2 newforms for $\Gamma_0(p)$ that have positive even analytic rank. As in the proof of Corollary 7.4, the monic polynomial

$$h = \prod_{j=1}^{m} (x - a_2(f_j)) \in \mathbb{Z}[x]$$

p	389	433	563	571	643	709	997	1061	1171
dim(A)	1	1	1	1	1	1	2	2	1
p	1483	1531	1567	1613	1621	1627	1693	1873	1907
dim(A)	1	1	3	1	1	1	3	1	1
p	1913	1933	2027	2029	2081	2089	2251	2293	2333
dim(A)	3	1	1	2	2	1	1	2	4
p	2381	2593	2609	2617	2677	2797	2837	2843	2861
dim(A)	2	4	2	2	1	1	1	4	2
p	2953	2963	3019	3089	3271	3463	3583	3701	3779
dim(A)	1	2	2	2	3	2	2	2	1
p	3911	3943	3967	4027	4093	4139	4217	4253	4357
dim(A)	2	4	1	2	2	1	2	3	1
p	4481	4483	4547	4787	4799	4951	5003	5171	5323
dim(A)	1	2	1	2	1	2	3	1	3
p	5351	5471	5477	5737	5741	5749	5813	5821	6007
dim(A)	2	3	2	3	1	2	1	2	2
p	6011	6043	6199	6337	6571	6581	6691	6949	7019
dim(A)	1	1	1	2	1	3	1	3	1
p	7451	7541	7621	7639	7669	7753	7867	7919	7933
dim(A)	1	1	2	2	1	3	1	2	2
p	8117	8219	8363	8369	8443	8513	8699	8747	9011
dim(A)	3	1	1	2	1	3	1	1	4
p	9127	9161	9203	9277	9281	9467	9479	9781	9829
dim(A)	1	1	1	1	2	1	1	2	2
p	9857	9907	9967						
dim(A)	3	2	2						

TABLE 3. Primes $p < 10\,000$ such that there exist weight 2 newforms for $\Gamma_0(p)$ with positive even analytic rank and dimensions of the corresponding part of $J_0(p)^-$.

of degree m has roots bounded in absolute value by $2\sqrt{2}$, so the coefficient h_j of x^j is bounded by $\binom{m}{j}(2\sqrt{2})^{m-j}$. Similarly to our previous considerations, it follows that $t = (T_2 - 3)h(T_2)(w - 1)$ annihilates $J_0(p)(\mathbb{Q})$, and t can be written as a difference of effective correspondences of degree at most $6\left\lfloor(2\sqrt{2}+3)^N\right\rfloor$. The argument in the proof of Proposition 8.1 (using Proposition 2.2 with $(T_2 - 3)h(T_2)$) then shows the claim for d such that

$$d < \frac{\operatorname{gon}_{\mathbb{Q}}(X_0(p))}{6\left\lfloor (2\sqrt{2}+3)^N \right\rfloor}.$$

Together with the gonality bound from Theorem 3.3, this gives the stated value for ε_N. □

Obviously, depending on the specific $a_2(f_j)$, we may be able to improve the bound on d in concrete cases.

Definition 8.3. For a prime p, write $\operatorname{perdim}(p)$ ("positive even rank dimension") for the number of weight 2 newforms f for $\Gamma_0(p)$ such that $w(f) = -f$ and $L(f, 1) = 0$.

Similarly to Conjecture 5.3, we formulate the following conjecture.

Conjecture 8.4.

(1) *(Weak form)*

$$\lim_{p\to\infty} \frac{\operatorname{perdim}(p)}{\log p} = 0$$

as p runs through all prime numbers.

(2) *(Strong form) The positive even rank dimension $\operatorname{perdim}(p)$ is uniformly bounded as p runs through all prime numbers.*

This would give a strong form of the answer "yes" to Problem 1 in [Bru95] and to the similar question Murty asks at the end of page 264 in [RM95].

Cowan [Cow22] has computed all Galois orbits of newforms for $\Gamma_0(p)$ of weight 2 and prime level $p < 2 \cdot 10^6$. The data for $p < 10^6$ is available as part of the LMFDB. He finds that for all $10^4 < p < 10^6$, each of the two Atkin-Lehner eigenspaces contains orbits of size at most 6, together with one large orbit. There is only one orbit of size 6 (which has negative Atkin-Lehner sign) for $p = 171\,713$, there are two orbits of size 5 (both with negative Atkin-Lehner sign) for $p = 26777, 86161$, and ten of size 4, of which six have negative Atkin-Lehner sign and occur for $p = 13681, 28057, 35977, 63607, 185599, 794111$. The total size of these small orbits with negative Atkin-Lehner sign for $10^4 < p < 10^6$ is at most 7. This extends earlier work by Martin [Mar21] (who considers more general weights and levels) in the case of weight 2 and prime level. Martin formulates a conjecture (Conjecture A in loc. cit.) that essentially says (taking $r = 1$) that for 100% of the primes, each of the two Atkin-Lehner eigenspaces contains only one Galois orbit of newforms. Assuming this, [Mar21, Thm. 1] concludes that 100% of all newforms of weight 2 for $\Gamma_0(p)$ with p prime that have root number $+1$ have analytic rank zero, implying that primes p with $\operatorname{perdim}(p) > 0$ are sparse. Cowan's data may suggest that there are no further Galois orbits of size at least 5 and smaller than (say) a quarter of the number of newforms in the relevant Atkin-Lehner eigenspace, and that Galois orbits of sizes 3 or 4 are rare. The recent preprint [CM24] by Cowan and Martin has some heuristics supporting a statement along these lines.

Based on Cowan's data (as provided by the LMFDB), we determined the primes $p < 10^6$ such that $\operatorname{perdim}(p) > 4$. We found four such primes:

$$\operatorname{perdim}(86\,161) = 5, \qquad \operatorname{perdim}(89\,209) = 5,$$
$$\operatorname{perdim}(133\,117) = 5, \qquad \operatorname{perdim}(171\,713) = 6.$$

This gives some (perhaps weak) support for the strong form of the conjecture above.

There are some related results and conjectures. A result of Iwaniec and Sarnak [IS00, Theorem 6] (with $k = 2$, $D = 1$ and N running through the primes) shows that for any $\varepsilon > 0$, there is some $p_0(\varepsilon)$ such that for every prime $p > p_0(\varepsilon)$, the proportion of newforms of positive analytic rank among those of even analytic rank is at most $\frac{1}{2} + \varepsilon$. (Assuming GRH, [ILS00, (1.54)] improves this to $\frac{7}{16} + \varepsilon$. The expectation via the "Density Conjecture" is that this can be reduced to ε.) If we combine this with a version of Maeda's Conjecture in this setting (a fairly weak form of which is formulated in [Bru95, Problem 4]), which says that the newforms in each of the two Atkin-Lehner eigenspaces of cusp forms of weight 2 for $\Gamma_0(p)$ should form one large Galois orbit and only very few small ones (note that this is supported very well by Cowan's data mentioned above), we obtain that $\operatorname{perdim}(p)$ is bounded by the total size of the small Galois orbits since the large one will make up significantly more than half of the newforms, so by the Iwaniec-Sarnak result all its newforms will have analytic rank zero.

Assuming that small (say, less than a quarter the dimension of the ambient space) orbit sizes are bounded and orbits of size ≥ 2 are rare (so that the total size of small orbits of size at least 2 is bounded), $\operatorname{perdim}(p)$ is determined, up to a bounded amount, by the number of isogeny classes of elliptic curves of conductor p of positive even (analytic) rank. According to [PPVW19], the number of isogeny classes of elliptic curves of rank at least 2 and height $\leq X$ should be of the order of $X^{19/24}$, and one can expect that this should also hold for conductor $\leq X$. This would predict about a constant times $p^{-5/24}$ positive even rank elliptic curves of (prime) conductor p on average. Watkins [Wat08, Heuristic 3.1] has the more precise asymptotics $\sim X^{19/24}(\log X)^{3/5}$ (for curves with discriminant bounded by X). The LMFDB has complete data on elliptic curves of prime conductor up to 300 million. Counting positive even rank elliptic curves of prime conductors between successive multiples of a million shows good agreement with the Watkins heuristic (the constant factor derived from the data varies within a fairly small interval, with no clear tendency to grow or shrink). This then suggests that there should be only finitely many primes p such that there are five or more positive even rank elliptic curves of conductor p. Indeed, within the range of the LMFDB, there are only three such primes: $p = 4\,297\,609$ and $p = 151\,141\,051$ with five such curves, and $p = 161\,137\,637$ with six. There are six primes with four such curves, and then 109 with three and 2224 with two. We think that this is a fairly strong indication that even the strong form of Conjecture 8.4 might hold.

Theorem 8.5. *The weak form of Conjecture 8.4 implies the following.*

(i) *Fix an odd integer $d \geq 1$. There is $p_0(d)$ such that for all primes $p \geq p_0(d)$, there are no non-cuspidal points of degree d on $X_0(p)$.*

(ii) *Fix an even integer $d \geq 1$. There is $p_0(d)$ such that for all primes $p \geq p_0(d)$, every non-cuspidal point of degree d on $X_0(p)$ maps to a point of degree $d/2$ on $X_0(p)^+$.*

Proof. Take $p_0(d)$ so that $\varepsilon_{\operatorname{perdim}(p)} p > d$ for all $p \geq p_0(d)$. This is possible by assumption. (Indeed, the weaker hypothesis $\log p - \operatorname{perdim}(p) \log(2\sqrt{2} + 3) \to \infty$ as $p \to \infty$ would be sufficient.) Then Proposition 8.2 shows that a point of degree d on $X_0(p)$ is either a CM point associated to an order of discriminant $-p$ or $-4p$, or else d is even and the point maps to a point of degree $d/2$ on $X_0(p)^+$. If we increase $p_0(d)$ if necessary so that the class numbers of the orders of discriminant $-p$ or $-4p$ (when they exist) are larger than d (which is possible, since these class numbers tend to infinity with p), then the first possibility is excluded, since these points have degree equal to the class number. □

Remark 8.6. For $d = 1$, it is a theorem due to Mazur [Maz78] that the set of primes p such that there is a non-cuspidal rational point on $X_0(p)$ is

$$\mathrm{Primes}(19) \cup \{37, 43, 67, 163\};$$

for $p \in \{19, 43, 67, 163\}$, these points are fixed points of the Fricke involution.

9 Stronger results on $S(d)$ for large d

We can obtain a stronger result than Theorem 7.7 if we also assume Conjecture 8.4.

Theorem 9.1. *Assume Conjectures 5.3 (1) and 8.4 (1). Fix $m \geq 1$. Then there is $d_0(m)$ such that for integers $d \geq d_0(m)$,*

(1) *if d is odd,*

$$S_{\mathrm{new}}(d) \subseteq \mathrm{Primes}\left(\frac{d}{m}\right);$$

(2) *if d is even,*

$$S_{\mathrm{new}}(d) \subseteq \mathrm{Primes}\left(\frac{d}{m}\right) \cup \left\{\frac{d}{k} + 1 : 1 \leq k \leq m, k \mid d\right\} \cup \{2d+1, 3d+1\}\,.$$

If $d = k(p-1)$ with $1 \leq k \leq m$ and $P \in X_1(p)(K)$ is non-cuspidal with $[K : \mathbb{Q}] = d$, then K is a cyclic Galois extension of a subfield L such that $[L : \mathbb{Q}] = 2k$.

Proof. In the situation of Theorem 7.7 and its proof, we take d large enough so that $(Cd+1)^{2/3} \leq d/m$. Then for $p > d/m$ such that $p \notin \{2d+1, 3d+1\}$, we get that $p = (2d/\mu) + 1$ for some $1 \leq \mu \leq 2m$, and there are non-cuspidal points of degree μ on $X_0(p)$. If d is also sufficiently large so that for primes $p > d/m$, the conclusion of Theorem 8.5 holds for all odd degrees below $2m$, then it follows that $\mu = 2k$ must be even, hence $p = (d/k) + 1$. If d is odd, the number $(d/k) + 1$ is even, so cannot be a prime.

The statement on the fields K of definition of degree d points on $X_1(p)$ follows from the facts that $X_1(p) \to X_0(p)$ is a cyclic Galois cover over $\mathbb{Q}$ and that P maps to a point of degree $2k$ on $X_0(p)$. □

Corollary 9.2. *Assume Conjectures 5.3 (1) and 8.4 (1). Fix $m \geq 1$. Then there is $d_0(m)$ such that for integers $d \geq d_0(m)$,*

(1) *if d is odd,*

$$S(d) \subseteq \mathrm{Primes}\left(\frac{d}{m}\right);$$

(2) *if d is even,*

$$S(d) \subseteq \mathrm{Primes}\left(\frac{d}{m}\right) \cup \left\{\frac{d}{k} + 1 : 1 \leq k \leq m, k \mid d\right\}$$
$$\cup \left\{2\frac{d}{k} + 1, 3\frac{d}{k} + 1 : 1 \leq k \leq 3m, 2k \mid d\right\}.$$

In particular, we then have

$$\lim_{d\to\infty,\, d \text{ odd}} \frac{\max S(d)}{d} = 0 \qquad \textit{and} \qquad \limsup_{d\to\infty,\, d \text{ even}} \frac{\max S(d)}{d} = 3\,.$$

Proof. The upper bound for $S(d)$ follows from Theorem 9.1 and $S(d) = \bigcup_{d'|d} S_{\mathrm{new}}(d')$.

That the limit is zero for odd d follows by taking m arbitrarily large.

The statement on the limit for even d follows by observing that there are infinitely many primes $p \equiv 1 \bmod 6$, so for $d = (p-1)/3$, we have $\max S(d) = 3d+1$ if p is sufficiently large. □

Assuming the stronger forms of our conjectures, we can be more precise. Let $h(D)$ denote the class number of the quadratic order of discriminant D. We set

$$H(d) := \bigl\{p \text{ prime} : h(-4p)(p-1) = 2d \text{ or } \bigl(p \equiv 3 \bmod 4 \text{ and } h(-p)(p-1) = 2d\bigr)\bigr\}\,.$$

Remark 9.3. It is known that $h(-p), h(-4p) = p^{1/2+o(1)}$, which implies that

$$H(d) \subseteq \mathrm{Primes}(d^{2/3+o_d(1)})$$

and that the elements of $H(d)$ are bounded below by $d^{2/3-o_d(1)}$.

We also note that each prime $p \equiv 1 \bmod 4$ belongs to exactly one set $H(d)$ (for $d = h(-4p)(p-1)/2$, which is even), each prime $p \equiv 7 \bmod 8$ also belongs to exactly one set $H(d)$ (for $d = h(-4p)(p-1)/2 = h(-p)(p-1)/2$, which is odd), and each prime $p \equiv 3 \bmod 8$ (with the exception of $p = 3$, which is in $H(1)$ only) belongs to exactly two sets $H(d)$ (for $d = h(-p)(p-1)/2$ and $d = h(-4p)(p-1)/2 = 3h(-p)(p-1)/2$, which are both odd). Since the associated degrees d are roughly of size $p^{3/2}$, this implies that actually most sets $H(d)$ are empty. For example, for $d \le 10\,000$, only 233 sets $H(d)$ are nonempty, of which 8 have two elements and one has three elements (and there are no larger sets):

$$H(33) = \{23, 67\}\,, \quad H(315) = \{127, 211\}\,, \quad H(1485) = \{271, 331\}\,,$$
$$H(1701) = \{379, 487\}\,, \quad H(2625) = \{251, 1051\}\,, \quad H(4095) = \{631, 1171\}\,,$$
$$H(7875) = \{1051, 2251\}\,, \quad H(8415) = \{991, 1123, 1531\}\,, \quad H(9009) = \{859, 2003\}\,.$$

Lemma 9.4. *For all $d \ge 1$, $H(d) \subseteq S_{\mathrm{new}}(d)$.*

Proof. Let $p \in H(d)$. First assume that $h(-4p)(p-1) = 2d$. There are elliptic curves with CM by $\mathbb{Z}[\sqrt{-p}]$ defined over a number field of degree $h(-4p)$. These curves give rise to points of degree $h(-4p)$ on $X_0(p)$, which are fixed points of w_p, since they have an endomorphism of degree p (given by $\sqrt{-p}$) defined over their field of definition. Pulling back to $X_1(p)$, this gives points of degree $(p-1)/2 \cdot h(-4p) = d$, showing that $p \in S_{\mathrm{new}}(d)$.

Now assume that $p \equiv 3 \bmod 4$ and $h(-p)(p-1) = 2d$. Similarly as above, there are elliptic curves with CM by $\mathbb{Z}[(1+\sqrt{-p})/2]$ defined over a number field of degree $h(-p)$, which give rise to points of degree $h(-p)$ on $X_0(p)$ as before. Pulling back to $X_1(p)$, this gives points of degree $(p-1)/2 \cdot h(-p) = d$, again showing that $p \in S_{\mathrm{new}}(d)$. □

We also set

$$D(d) := \bigl\{p \text{ prime} : p-1 \mid d \text{ or } p = 2d+1 \text{ or } p = 3d+1\bigr\}\,.$$

Theorem 9.5. *Assume Conjecture 8.4 (2) and Conjecture 5.3 (2). Then there are constants $C_2 > C_1 > 0$ such that for all $d \ge 1$,*

(1) *when d is odd,*

$$\mathrm{Primes}(\sqrt{C_1 d + 1}) \cup H(d) \subseteq S_{\mathrm{new}}(d) \subseteq \mathrm{Primes}(\sqrt{C_2 d + 1}) \cup H(d) \subseteq \mathrm{Primes}(d^{2/3+o_d(1)})\,;$$

(2) *when* d *is even,*

$$\mathrm{Primes}(\sqrt{C_1 d + 1}) \cup H(d) \subseteq S_{\mathrm{new}}(d) \subseteq \mathrm{Primes}(\sqrt{C_2 d + 1}) \cup H(d) \cup D(d)\,.$$

Proof. The lower bound follows from Proposition 3.6 (noting that the proof actually shows that $\mathrm{Primes}(\sqrt{C_1 d + 1}) \subseteq S_{\mathrm{new}}(d)$) and Lemma 9.4.

For the upper bound, let $\alpha = \varepsilon_N^{-1}$ with ε_N as in Proposition 8.2, where N is a uniform upper bound for $\mathrm{perdim}(p)$, and let $\beta = C\lfloor(2\sqrt{2}+3)^s\rfloor$ with C as in Corollary 7.5, where s is a uniform upper bound for $\mathrm{strdim}(p)$. Assume that $p \in S_{\mathrm{new}}(d)$. Set $C_2 = \max\{2(168/167)\alpha, \beta, 163^2\}$ and assume that $p > \sqrt{C_2 d + 1}$; then $p \geq 167$. By Corollary 7.5, either d is even and $p \in \{2d+1, 3d+1\}$ (and so $p \in D(d)$), or else $p-1$ divides $2d$ and there is a non-cuspidal point P of degree $2d/(p-1)$ on $X_0(p)$. Note that

$$\frac{2d}{p-1} < \frac{2(p^2-1)}{C_2(p-1)} < \frac{p+1}{\alpha} \leq \varepsilon_N p\,,$$

so Proposition 8.2, applied with $d \leftarrow 2d/(p-1)$, tells us that P is a fixed point of w_p, which implies that $p \in H(d)$, or d is even and P comes from a point of degree $d/(p-1)$ on $X_0(p)^+$. So in this latter case, $p-1$ divides d, and we again have that $p \in D(d)$. □

To formulate the corresponding statement for $S(d)$, we set

$$\tilde{H}(d) := \bigcup_{d' \mid d} H(d') \qquad \text{and} \qquad \tilde{D}(d) := \bigcup_{d' \mid d} D(d')\,.$$

The sets $\tilde{H}(d)$ can be quite a bit larger than $H(d)$, for example,

$$\tilde{H}(6300) = \{3, 5, 7, 11, 13, 19, 29, 31, 37, 43, 61, 101, 127, 151, 181, 211, 421\}$$

has 17 elements.

Corollary 9.6. *Assume Conjecture 8.4 (2) and Conjecture 5.3 (2). Then there are constants* $C_2 > C_1 > 0$ *such that for all* $d \geq 1$*,*

(1) *when* d *is odd,*

$$\mathrm{Primes}(\sqrt{C_1 d + 1}) \cup \tilde{H}(d) \subseteq S(d) \subseteq \mathrm{Primes}(\sqrt{C_2 d + 1}) \cup \tilde{H}(d) \subseteq \mathrm{Primes}(d^{2/3+o_d(1)})\,;$$

(2) *when* d *is even,*

$$\mathrm{Primes}(\sqrt{C_1 d + 1}) \cup \tilde{H}(d) \subseteq S(d) \subseteq \mathrm{Primes}(\sqrt{C_2 d + 1}) \cup \tilde{H}(d) \cup \tilde{D}(d)\,.$$

Proof. This follows from Theorem 9.5 and $S(d) = \bigcup_{d' \mid d} S_{\mathrm{new}}(d')$. □

References

[Abr96] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **20** (1996), 1005–1011, DOI 10.1155/S1073792896000621. MR1422373 ↑1, 3

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑5

[BN15] Peter Bruin and Filip Najman, *Hyperelliptic modular curves* $X_0(n)$ *and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), no. 1, 578–602, DOI 10.1112/S1461157015000157. MR3389884 ↑1

[Bru95] Armand Brumer, *The rank of* $J_0(N)$, Astérisque **228** (1995), 3, 41–68. Columbia University Number Theory Seminar (New York, 1992). MR1330927 ↑8, 8

[CCS13] Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), no. 2, 447–479, DOI 10.1142/S1793042112501436. MR3005559 ↑1

[CES03] Brian Conrad, Bas Edixhoven, and William Stein, $J_1(p)$ *has connected fibers*, Doc. Math. **8** (2003), 331–408. MR2029169 ↑4, 4.4

[Cow22] Alex Cowan, *Computing newforms using supersingular isogeny graphs*, Res. Number Theory **8** (2022), no. 4, Paper No. 96, 23, DOI 10.1007/s40993-022-00392-z. MR4502909 ↑8

[CM24] Alex Cowan and Kimball Martin, *Counting modular forms by rationality field*, October 15, 2024. https://arxiv.org/abs/2301.10357v2. ↑8

[DL24] Davide De Leo, *On Some Open Cases of a Conjecture of Conrad, Edixhoven and Stein*, Università della Calabria, 2024. ↑4.4

[DLS25] Davide De Leo and Michael Stoll, *On Some Open Cases of a Conjecture of Conrad, Edixhoven and Stein*, May 16, 2025. https://arxiv.org/abs/2505.10777v1. ↑4.4

[DEvH$^+$21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864, DOI 10.2140/ant.2021.15.1837. MR4333666 ↑1

[DvH14] Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve* $X_1(N)$, J. Algebra **417** (2014), 52–71, DOI 10.1016/j.jalgebra.2014.06.026. MR3244637 ↑1, 3, 3

[DKSS23] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll, *Torsion points on elliptic curves over number fields of small degree*, Algebra Number Theory **17** (2023), no. 2, 267–308, DOI 10.2140/ant.2023.17.267. MR4564759 ↑1, 1.1, 1.2, 1, 1, 2, 2, 4, 4, 4.4

[DN25] Maarten Derickx and Filip Najman, *Classification of torsion of elliptic curves over quartic fields*, February 18, 2025. https://arxiv.org/abs/2412.16016v2. ↑1

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR1357209 ↑1

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83, DOI 10.1007/BF02758637. MR1264340 ↑3

[vH14] Mark van Hoeij, *Low degree places on the modular curve* $X_1(N)$, June 22, 2014. https://arxiv.org/abs/1202.4355v5. ↑1

[ILS00] Henryk Iwaniec, Wenzhi Luo, and Peter Sarnak, *Low lying zeros of families of* L*-functions*, Inst. Hautes Études Sci. Publ. Math. **91** (2000), 55–131 (2001). MR1828743 ↑8

[IS00] Henryk Iwaniec and Peter Sarnak, *The non-vanishing of central values of automorphic* L*-functions and Landau-Siegel zeros*, Israel J. Math. **120** (2000), 155–177, DOI 10.1007/s11856-000-1275-9. MR1815374 ↑8

[JKL11a] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 273, 579–591, DOI 10.1090/S0025-5718-10-02369-0. MR2728995 ↑1

[JKL11b] ———, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 276, 2395–2410, DOI 10.1090/S0025-5718-2011-02493-2. MR2813367 ↑1

[JKS04] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301, DOI 10.4064/aa113-3-6. MR2069117 ↑1

[Kam92] S. Kamienny, *Torsion points on elliptic curves and* q*-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689 ↑1, 1.2, 1

[KM95] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Astérisque **228** (1995), 3, 81–100. With an appendix by A. Granville; Columbia University Number Theory Seminar (New York, 1992). MR1330929 ↑1

[Kat04] Kazuya Kato, p*-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290 (English, with English and French summaries). Cohomologies p-adiques et applications arithmétiques. III. MR2104361 ↑6

[KM88] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149, DOI 10.1017/S0027763000002816. MR0931956 ↑1

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504, DOI 10.1007/s00222-009-0205-7. MR2551763 ↑6

[KW09b] ______, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586, DOI 10.1007/s00222-009-0206-6. MR2551764 ↑6

[Kha24] Maleeha Khawaja, *Torsion primes for elliptic curves over degree 8 number fields*, Res. Number Theory **10** (2024), no. 2, Paper No. 48, 9, DOI 10.1007/s40993-024-00533-6. MR4737399 ↑1.2

[Kim03] Henry H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, J. Amer. Math. Soc. **16** (2003), no. 1, 139–183, DOI 10.1090/S0894-0347-02-00410-1. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak. MR1937203 ↑3

[KL89] V. A. Kolyvagin and D. Yu. Logachëv, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196 (Russian); English transl., Leningrad Math. J. **1** (1990), no. 5, 1229–1253. MR1036843 ↑6, 8

[Mar21] Kimball Martin, *An on-average Maeda-type conjecture in the level aspect*, Proc. Amer. Math. Soc. **149** (2021), no. 4, 1373–1386, DOI 10.1090/proc/15328. MR4242297 ↑8

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287 ↑1, 1.2, 1

[Maz78] ______, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230 ↑1, 1.2, 7.6, 8.6

[Mer96] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449, DOI 10.1007/s002220050059 (French). MR1369424 ↑1

[Mor22] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. **21** (1922/23), 179–192, DOI 10.1080/10543406.2011.550093. MR4656011 ↑1

[RM95] M. Ram Murty, *The analytic rank of* $J_0(N)(\mathbf{Q})$, Number theory (Halifax, NS, 1994), CMS Conf. Proc., vol. 15, Amer. Math. Soc., Providence, RI, 1995, pp. 263–277. MR1353938 ↑8

[Par00] Pierre Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749 (French, with English and French summaries). MR1779891 ↑1.2

[Par03] ______, *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux **15** (2003), no. 3, 831–838 (English, with English and French summaries). MR2142238 ↑1.2

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903, DOI 10.4171/JEMS/893. MR3985613 ↑8

[Rib77] Kenneth A. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., vol. Vol. 601, Springer, Berlin-New York, 1977, pp. 17–51. MR0453647 ↑5

[Rib04] ______, *Abelian varieties over* $\mathbf{Q}$ *and modular forms*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 241–261, DOI 10.1007/978-3-0348-7919-4_15. MR2058653 ↑6

[Sil88] Alice Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), no. 3, 241–249. MR971328 ↑ii

[Str19] Marco Streng, *Generators of the group of modular units for* $\Gamma^1(N)$ *over the rationals*, February 1, 2019. https://arxiv.org/abs/1503.08127. ↑

[Sut13] Andrew V. Sutherland, *Isogeny volcanoes*, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 507–530, DOI 10.2140/obs.2013.1.507. MR3207429 ↑2

[Wat08] Mark Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125. MR2410120 ↑8

[Wei29] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315, DOI 10.1007/BF02547409 (French). MR1555278 ↑1

Department of Mathematics, University of Zagreb, Horvatovac 102a, 10000 Zagreb, Croatia
Email address: maarten@mderickx.nl

Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany.
Email address: Michael.Stoll@uni-bayreuth.de