MODULAR PARAMETRIZATIONS OF NEUMANN–SETZER ELLIPTIC CURVES

WILLIAM STEIN AND MARK WATKINS

ABSTRACT. Suppose p is a prime of the form $u^2 + 64$ for some integer u, which we take to be 3 mod 4. Then there are two Neumann–Setzer elliptic curves E_0 and E_1 of prime conductor p, and both have Mordell–Weil group $\mathbb{Z}/2$. There is a surjective map $X_0(p) \xrightarrow{\pi} E_0$ that does not factor through any other elliptic curve (i.e., π is optimal), where $X_0(p)$ is the modular curve of level p. Our main result is that the degree of π is odd if and only if $u \equiv 3 \pmod 8$. We also prove the prime-conductor case of a conjecture of Glenn Stevens, namely that that if E is an elliptic curve of prime conductor p then the optimal quotient of $X_1(p)$ in the isogeny class of E is the curve with minimal Faltings height. Finally we discuss some conjectures and data about modular degrees and orders of Shafarevich–Tate groups of Neumann–Setzer curves.

1. Introduction

Let p be a prime of the form $u^2 + 64$ for some integer u, which we take to be 3 modulo 4. Neumann and Setzer [Neu71, Set75] considered the following two elliptic curves of conductor p (note that Setzer chose $u \equiv 1 \pmod 4$ instead):

$$E_0: \quad y^2 + xy = x^3 - \frac{u+1}{4}x^2 + 4x - u, \tag{1.1}$$

$$E_1: \quad y^2 + xy = x^3 - \frac{u+1}{4}x^2 - x. \tag{1.2}$$

For E_1 we have $c_4 = p - 16$ and $c_6 = u(p+8)$ with $\Delta = p = u^2 + 64$, while for E_0 we have $c_4 = p - 256$ and $c_6 = u(p + 512)$ with $\Delta = -p^2$. Thus each E_i is isomorphic to a curve of the form $y^2 = x^3 - 27c_4x - 54c_6$ for the indicated values of c_4 and c_6. The curves E_0 and E_1 are 2-isogenous and one can show using Lutz-Nagell and descent via 2-isogeny that $E_0(\mathbb{Q}) = E_1(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ (see [Set75]). Moreover, if E is *any* elliptic curve over $\mathbb{Q}$ of prime conductor with a rational point of order 2 then E is a Neumann–Setzer curve or has conductor 17.

Let $X_0(p)$ be the modular curve of level p. By [Wil95] there is a surjective map $\pi : X_0(p) \to E_0$, and by [MO89, §5, Lem. 3] we may choose π to be optimal, in the sense that π does not factor through any other elliptic curve. The *modular degree* of E_0 is $\deg(\pi)$.

We prove in Section 2 that the modular degree of E_0 is odd if and only if $u \equiv 3 \pmod 8$. Our proof uses results from Mazur [Maz77]. In Section 3 we show that E_1 is the curve of minimal Faltings height in the isogeny class $\{E_0, E_1\}$ of E_1 and prove that E_1 is an optimal quotient of $X_1(p)$, which is enough to prove the prime-conductor case of a conjecture of Stevens [Ste89] (this case is not covered by the results of Vatsal [Vat03]). Finally, in Section 4 we give evidence for our conjecture that there are infinitely many elliptic curves with odd modular degree, and give a

Date: December 2003.

conjectural refinement of Theorem 2.1. We also present some data about p-divisibility of conjectural orders of Shafarevich–Tate groups of Neumann–Setzer curves.

1.1. **Notation.** Let p be a prime and n be the numerator of $(p-1)/12$.

We use standard notation for modular forms, modular curves, and Hecke algebras, as in [1] or [Maz77]. In particular, let $X_0(p)$ be the compactified coarse moduli space of elliptic curves with a cyclic subgroup of order p. Then $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$. Let $J = J_0(p)$ be the Jacobian of $X_0(p)$, and let $\mathbb{T} = \mathbb{Z}[T_2, T_3, \ldots] \subset \mathrm{End}(J)$ be the Hecke algebra. Also, let $X_1(p)$ be the modular curve the classifies isomorphism classes of pairs (E, P), where $P \in E$ is a point of order p.

To each newform $f \in S_2(\Gamma_0(p))$, there is an associated abelian subvariety $A = A_f \subset J_0(p)$. We call the kernel Ψ_A of the natural map $A \hookrightarrow J \to A^\vee$ the *modular kernel*. For example, when A is an elliptic curve, this map is induced by pullback followed by push forward on divisors and Ψ_A is multiplication by $\deg(X_0(p) \to A)$. The *modular degree* of A is the square root of the degree of Ψ_A. (This definition makes sense even when $\dim(A) > 1$, since the degree of a polarization is the square of its Euler characteristic, which is a perfect square.)

If $I \subset \mathbb{T}$ is an ideal, let

$$A[I] = \{x \in A(\overline{\mathbb{Q}}) : Ix = 0\} \qquad \text{and} \qquad A[I^\infty] = \bigcup_n A[I^n].$$

1.2. **Acknowledgements.** The authors would like to thank AIM for hospitality while they worked on this paper, NSF for financial support, and Matt Baker, Barry Mazur, and Frank Calegari for helpful conversations.

2. Determination of the Parity of the Modular Degree

Let p, u, E_0, J and n be as in Section 1, and fix notation as in Section 1.1. In this section we prove the following theorem.

Theorem 2.1. *The modular degree of E_0 is odd if and only if $u \equiv 3 \pmod 8$.*

Before proving the theorem we prove a number of lemmas. These lemmas all follow relatively easily from the general ideas of [Maz77], but we give complete proofs for the convenience of the reader.

Let m be the modular degree of E_0, and let

$$B = \ker(J \xrightarrow{\pi} E_0).$$

Lemma 2.2. *We have $m^2 = \#(B \cap E_0)$.*

Proof. As mentioned in Section 1.1, the composition $E_0 \to J \to E_0$ is multiplication by the degree of $X_0(p) \to E_0$, i.e., multiplication by the modular degree of E_0. The lemma follows since multiplication by m on E_0 has degree m^2. □

The *Eisenstein ideal* $\mathcal{I}$ of $\mathbb{T}$ is the ideal generated by $T_\ell - (\ell + 1)$ for $\ell \neq p$ and $1 - T_p$. By hypothesis, there is a Neumann–Setzer curve of conductor p, which implies that the numerator n of $(p-1)/12$ is even (we do the elementary computation that shows this in the proof of Theorem 2.1 below). As discussed in [Maz77, Prop. II.9], the 2-Eisenstein prime $\mathfrak{m} = (2) + \mathcal{I}$ of $\mathbb{T}$ is a maximal ideal of T, with $\mathbb{T}/\mathfrak{m} \cong \mathbb{F}_2$.

Lemma 2.3. *We have $E_0[\mathfrak{m}] = E_0[2]$.*

Proof. By [Maz77, Prop. II.11.1, Thm. III.1.2], the Eisenstein ideal $\mathcal{I}$ annihilates $J(\mathbb{Q})_{\mathrm{tor}}$, so $\mathfrak{m}$ annihilates $J(\mathbb{Q})_{\mathrm{tor}}[2]$. Since $J(\mathbb{Q})_{\mathrm{tor}}$ is cyclic of order n (by [Maz77, Thm. III.1.2]), $J(\mathbb{Q})_{\mathrm{tor}}[2]$ has order 2, so $J(\mathbb{Q})_{\mathrm{tor}}[2] = E_0(\mathbb{Q})_{\mathrm{tor}}[2]$, hence $E_0(\mathbb{Q})[\mathfrak{m}] \neq 0$. The Hecke algebra $\mathbb{T}$ acts on E_0 through $\mathrm{End}(E_0) \cong \mathbb{Z}$, so each element of $\mathbb{T}$ acts on E_0 as an integer; in particular, the elements of $\mathfrak{m}$ all act as multiples of 2 (since $E_0[\mathfrak{m}] \neq 0$ and $2 \in \mathfrak{m}$), so $E_0[\mathfrak{m}] = E_0[2]$ since $2 \in \mathfrak{m}$. □

Lemma 2.4. *Suppose $A \subset J_0(p)$ is a $\mathbb{T}$-stable abelian subvariety and $\wp \subset \mathbb{T}$ is a maximal ideal such that $A[\wp^\infty] \neq 0$. Then $A[\wp] \neq 0$. Also $A[\wp^\infty]$ is infinite.*

Proof. Arguing as in [Maz77, §II.14, pg. 112], we see that for any r, $A[\wp^r]/A[\wp^{r+1}]$ is isomorphic to a direct sum of copies of $A[\wp]$. If $A[\wp] = 0$, then since $A[\wp^\infty] \neq 0$, there must exist an r such that $A[\wp^r]/A[\wp^{r+1}] \neq 0$. But then $A[\wp^r]/A[\wp^{r+1}]$ is a direct sum of copies of 0, a contradiction.

To see that $A[\wp^\infty]$ is infinite, note that if ℓ is the residue characteristic of $\wp$ and $\mathrm{Tate}_\ell(A)$ is the Tate module of A at ℓ, then

$$\varprojlim_r A[\wp^r] = \mathrm{Tate}_\ell(A) \otimes \mathbb{T}_\wp$$

is infinite. (For more details, see the proof of [RS01, Prop. 3.2].) □

The analogues of Lemmas 2.5–2.7 below are true, with the same proofs, for $\mathfrak{m}$ any Eisenstein prime. We state and prove them for the 2-Eisenstein prime, since that is the main case of interest to us. Let $\tilde{J}^{(2)}$ be the 2-Eisenstein quotient of J associated to $\mathfrak{m}$, where $\tilde{J}^{(2)}$ is as defined in [Maz77, §II.10]. More precisely, we have the following description of $\tilde{J}^{(2)}$:

Lemma 2.5. *The simple factors of $\tilde{J}^{(2)}$ correspond to the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of newforms f such that $A_f[\mathfrak{m}] \neq 0$ (equivalently, $A_f^\vee[\mathfrak{m}] \neq 0$).*

Proof. On page 97 of [Maz77] we find that the $\mathbb{C}$-simple factors of $\tilde{J}^{(2)}$ are in one-to-one correspondence with the irreducible components $\mathrm{Spec}(I_f)$ of $\mathrm{Spec}(\mathbb{T})$ which meet the support of the ideal $\mathfrak{m}$. Since $\mathfrak{m}$ is maximal, this means the ideals I_f that are contained in $\mathfrak{m}$. If $I_f \subset \mathfrak{m}$ and $A_f[\mathfrak{m}] = 0$ then $A_f[\mathfrak{m}^\infty] = 0$ by Lemma 2.4. Since $\mathbb{T}/I_f$ acts faithfully on A_f it would follow that the image of $\mathfrak{m}$ in $\mathbb{T}/I_f$ is the unit ideal, a contradiction. Conversely, if $A_f[\mathfrak{m}] \neq 0$, then the image of $\mathfrak{m}$ in $\mathbb{T}/I_f$ is not the unit ideal, so $I_f \subset \mathfrak{m}$. Finally, note that the same argument applies to $A_f^\vee$, since $\mathbb{T}/I_f$ also acts faithfully on $A_f^\vee$. □

Lemma 2.6. *Suppose A and B are abelian varieties equipped with an action of the Hecke ring $\mathbb{T}$ and that $\varphi : A \to B$ is a $\mathbb{T}$-module isogeny. If $\wp \subset \mathbb{T}$ is a maximal ideal and $B[\wp] \neq 0$, then also $A[\wp] \neq 0$.*

Proof. Let $\psi : B \to A$ be the isogeny complementary to φ, so ψ is the unique isogeny such that $\psi \circ \varphi$ is multiplication by $\deg(\varphi)$. Then ψ is also a $\mathbb{T}$-module homomorphism (one can see this in various ways; one way is to use the rational representation on homology to view the endomorphisms as matrices acting on lattices, and to note that if matrices M and N commute, then M^{-1} and N also commute). By Lemma 2.4, the union $B[\wp^\infty]$ is infinite, so $\psi(B[\wp^\infty]) \neq 0$. Since $\psi(B[\wp^\infty]) \subset A[\wp^\infty]$, Lemma 2.4 implies that $A[\wp] \neq 0$, as claimed. □

Lemma 2.7. *Suppose $B \subset J_0(p)$ is a sum of abelian subvarieties A_f attached to newforms. If $B[\mathfrak{m}] \neq 0$, then there is some $A_f \subset B$ such that $A_f[\mathfrak{m}] \neq 0$.*

Proof. There is something to be proved because if $x \in B[\mathfrak{m}]$ it could easily be the case that $x = y + z$ with $y \in A_f$ and $z \in A_g$, but $x \notin A_h$ for any h. Let $C = \oplus A_f$, where the $A_f \subset J_0(p)$ are simple abelian subvarieties of B corresponding to newforms. Then there is an isogeny $\varphi : C \to B$ given by $\varphi(x_1, \ldots, x_n) = x_1 + \cdots + x_n$, where the sum is in $B \subset J_0(p)$. By Lemma 2.6, we see that $C[\mathfrak{m}] \neq 0$ as well. Since $C[\mathfrak{m}] \cong \oplus A_f[\mathfrak{m}]$, it follows that $A_f[\mathfrak{m}] \neq 0$ for some $A_f \subset B$. $\square$

Lemma 2.8. *If* $4 \mid n$, *then* $\dim \tilde{J}^{(2)} > 1$.

Proof. This follows from the remark on page 163 of [Maz77]. Since the proof is only sketched there, we give further details for the convenience of the reader. Because $4 \mid n$, the cuspidal subgroup C, which is generated in $J_0(p)$ by $(0) - (\infty)$ and is cyclic of order n, contains an element of order 4. Let $C(2)$ be the 2-primary part of C, and let $D = \ker(J_0(p) \to \tilde{J}^{(2)})$. If there is a nonzero element in the kernel of the homomorphism $C(2) \to \tilde{J}^{(2)}$, then $D[\mathfrak{m}] \neq 0$, where $\mathfrak{m}$ is the 2-Eisenstein prime. But then by Lemma 2.7, there is an $A_f \subset D$ such that $A_f[\mathfrak{m}] \neq 0$. By Lemma 2.5, $A_f^\vee$ is a quotient of $\tilde{J}^{(2)}$, so $A_f \subset (\tilde{J}^{(2)})^\vee$ so A_f cannot be in D. This contradiction shows that the map $C(2) \to \tilde{J}^{(2)}$ is injective, so $\tilde{J}^{(2)}$ contains a rational point of order 4. However, as mentioned in the introduction, $E_0(\mathbb{Q})$ has order 2, so $\tilde{J}^{(2)} \neq E_0$. Thus $\tilde{J}^{(2)}$ has dimension bigger than 1. $\square$

Note that the converse of Lemma 2.8 is also true, as we note in the second part of the proof of the theorem below.

Having established the above lemmas, we are now ready to deduce the theorem.

Proof of Theorem 2.1. ($\Longrightarrow$) *Odd modular degree implies* $u \equiv 3 \pmod 8$*:* We prove this by proving the converse, i.e., that if $u \equiv 7 \pmod 8$ then the modular degree of E_0 is even. Writing $u = 8k + 7$ we see that $p = (8k + 7)^2 + 64 \equiv 1 \pmod{16}$, so $16 \mid (p - 1)$ hence $4 \mid n$.

By Lemma 2.8, the dimension of $\tilde{J}^{(2)}$ is bigger than 1. By Lemma 2.3 and Lemma 2.5, since $4 \mid n$ we have that E_0 is a factor of $\tilde{J}^{(2)}$. Thus there is an A_f distinct from E_0 such that $A_f[\mathfrak{m}] \neq 0$. Since $A_f \subset B = \ker(J_0(p) \to E_0)$, it follows that $B[\mathfrak{m}] \neq 0$. As discussed on page 38 of [Maz77], $J[\mathfrak{m}]$ has dimension 2 over $\mathbb{F}_2$ so $E_0[\mathfrak{m}] = J[\mathfrak{m}]$, hence $B[\mathfrak{m}] \subset E_0[\mathfrak{m}]$. It follows that $2 \mid \#(B \cap E_0)$, so E_0 has even modular degree.

($\Longleftarrow$) $u \equiv 3 \pmod 8$ *implies odd modular degree:* Next suppose that $u \equiv 3 \pmod 8$. Then n is exactly divisible by 2 because when $u = 8k+3$ we have $p = (8k+3)^2+64 \equiv 9 \pmod{16}$, so that $8 \mid\mid (p - 1)$.

Since $8 \mid\mid (p-1)$, [Maz77, Prop. III.7.5] implies that $\tilde{J}^{(2)} = E_0$. We will now show that if the modular degree were even, then $\tilde{J}^{(2)}$ would have to have dimension bigger than 1. Thus assume for the sake of contradiction that the modular degree m of E_0 is even. Letting $B = \ker(J_0(p) \to E_0)$ we have $E_0 \cap B \cong \ker(E_0 \to J_0(p) \to E_0)$, so $\Psi := E_0 \cap B = E_0[m]$. Lemma 2.3 and our assumption that m is even imply that

$$E_0[\mathfrak{m}] = E_0[2] \subset E_0[m] = \Psi,$$

so $\Psi[\mathfrak{m}] \neq 0$. Since $\Psi[\mathfrak{m}] \neq 0$, and $\Psi \subset B$, we have $B[\mathfrak{m}] \neq 0$. By Lemma 2.7, there is some $A_f \subset B$ such that $A_f[\mathfrak{m}] \neq 0$. Then by Lemma 2.5 we see that A_f is an isogeny factor of $\tilde{J}^{(2)}$, which contradicts the fact that $\tilde{J}^{(2)}$ has dimension 1. Our assumption that m is even must be false. $\square$

Remark 2.9. Frank Calegari pointed out to us that Lemma 2.8 and its converse also follow from conditions (i) and (v) of Théorème 3 of [Mer96].

3. The Stevens Conjecture for Neumann–Setzer Curves is True

Let E be an arbitrary elliptic curve over $\mathbb{Q}$ of conductor N. Stevens conjectured in [Ste89] that the optimal quotient of $X_1(N)$ in the isogeny class of E is the curve in the isogeny class of E with minimal Faltings height. In this section we explain why this conjecture is true when N is prime.

Let $p = u^2 + 64$ be prime and E_1 and E_0 be as in Section 1. In this section we verify that the curve E_1 has smaller Faltings height than E_0, then show that E_1 is $X_1(p)$-optimal. The Stevens conjecture asserts that the $X_1(p)$-optimal curve is the curve of minimal Faltings height in an isogeny class, so our results verify the conjecture for Neumann–Setzer curves. In fact, the Stevens conjecture is true for all isogeny classes of elliptic curves of prime conductor. For if E is an elliptic curve of prime conductor, then by [Set75] there is only one curve in the isogeny class of E, unless E is a Neumann–Setzer curve or the conductor of E is 11, 17, 19, or 37. When the isogeny class of E contains only one curve, that curve is obviously both X_1-optimal and of minimal Faltings height. The conjecture is also well-known to be true for curves of conductor 11, 17, 19, or 37 (see [Ste89]). We note that Vatsal [Vat03] has recently extended results of Tang [Tan97] that make considerable progress toward the Stevens conjecture, but his work is not applicable to Neumann–Setzer curves.

Lemma 3.1. *The curve E_1 has smaller Faltings height than E_0.*

Proof. By [Ste89, Thm. 2.3, pg. 84] it is enough to exhibit an isogeny from E_1 to E_0 whose extension to Néron models is étale. Let φ be the isogeny $E_0 \to E_1$ of degree 2 whose kernel is the subgroup generated by the point whose coordinates are $(u/4, -u/8)$ in terms of the Weierstrass equation (1.1) for E_0, which is a global minimal model for E_0. The kernel of φ does not extend to an étale group scheme over $\mathbb{Z}$, since its special fiber at 2 is not étale (it has only one $\overline{\mathbb{F}}_2$-point), so the morphism on Néron models induced by $E_0 \to E_1$ cannot be étale, since kernels of étale morphisms are étale. By [Ste89, Lemma 2.5] the dual isogeny $E_1 \to E_0$ extends to an étale morphism of Néron models. $\square$

Proposition 3.2. *The curve E_1 is $X_1(p)$-optimal.*

Proof. By [MO89, §5, Lem. 3], E_0 is an optimal quotient of $X_0(p)$, so we have an injection $E_0 \hookrightarrow J_0(p)$. As in [Maz77, pg.100], let Σ be the kernel of the functorial map $J_0(p) \to J_1(p)$ induced by the cover $X_1(p) \to X_0(p)$. By [Maz77, Prop. II.11.6], Σ is the Cartier dual of the constant subgroup scheme U, which turns out to equal $J_0(p)(\mathbb{Q})_{\mathrm{tor}}$. Because $\#(E_0 \cap U) = 2$ and $E_0[2]$ is self dual, it follows that $\#(E_0 \cap \Sigma) = 2$. Thus the image of E_0 in $J_1(p)$ is the quotient of E_0 by the subgroup generated by the rational point of order 2 (note that the Cartier dual of $\mathbb{Z}/2$ is $\mu_2 = \mathbb{Z}/2$). This quotient is E_1, so $E_1 \subset J_1(p)$, which implies that E_1 is an optimal quotient of $X_1(p)$, as claimed. $\square$

Remark 3.3. The above proposition could also be proved in a slightly different manner. The Faltings height of an elliptic curve is $\sqrt{2\pi/\Omega}$ where Ω is the volume of the fundamental parallelogram associated to the curve. When the conductor is prime, we have by [AL96] that the Manin constants for $X_0(p)$ and $X_1(p)$ are 1; this says that for a G-optimal curve E, the period lattice generated by G has covolume equal to Ω_E. Since the lattice generated by $\Gamma_1(p)$ is contained in the lattice generated by $\Gamma_0(p)$ (and thus has larger covolume), the Faltings height of the $X_1(p)$-optimal curve must be less than or equal to that of the $X_0(p)$-optimal. So if these two curves differ, the $X_1(p)$-optimal curve must have smaller Faltings height.

Remark 3.4. On page 12 of [Maz98], there is a "To be removed from the final draft" comment that asks (in our notation) whether E_0 is $X_0(p)$-optimal when $p \equiv 1 \pmod{16}$. This is already answered by [MO89], whereas here we go further and show additionally that E_1 is $X_1(p)$-optimal.

4. Conjectures

4.1. **Refinement of Theorem 2.1.** The following conjectural refinement of Theorem 2.1 is supported by the experimental data of [Wat02]. It is unclear whether the method of proof of Theorem 2.1 can be extended to prove this conjecture.

Conjecture 4.1. *If* $u \equiv 7 \pmod 8$*, then* 2 *exactly divides the modular degree of* E_0 *if and only if* $u \equiv 7 \pmod{16}$*.*

We can note that the pattern seems to end here; for curves with $u \equiv 15 \pmod{16}$ the data give no further information about the 2-valuation of the modular degree. For instance, with $u = -17$ we have that $[1, 1, 1, -2, 16]$ has modular degree $2^3 \cdot 3$, while with $u = 175$ the curve $[1, 1, 1, -634, -6484]$ has modular degree $2^2 \cdot 3^3 \cdot 5 \cdot 23$. Similarly, we have that $u = -33$ gives the curve $[1, -1, 1, -19, 68]$ with modular degree $2^5 \cdot 3$, while $u = 127$ gives the curve $[1, 1, 1, -332, -2594]$ of modular degree $2^2 \cdot 3^2 \cdot 5 \cdot 43$.

4.2. **The Parity of the Modular Degree.** According to Cremona's tables [Cre], of the 29755 new optimal elliptic curve quotients of $J_0(N)$ with $N < 8000$, a mere 89 have odd modular degree, which is less than 0.3%. There are 52878 non Neumann–Setzer curves in the database of [BM90] with prime conductor $N \le 10^7$; of these curves 4592, or 8%, have odd modular degree (see [Wat02]). Note that the method of [Wat02] used to compute the modular degree is rigourous when the level is prime because by [AL96] the Manin constant is 1 when the level is odd and square-free.

If $f(x) = (8x + 3)^2 + 64$, then it is a well-known conjecture (see [HL22] and e.g., [Guy94, §A1]) that there are infinitely many primes of the form $f(n)$ for some integer n, thus we make the following conjecture.

Conjecture 4.2. *There are infinitely many elliptic curves over* $\mathbb{Q}$ *with odd modular degree.*

Our data suggest that if E is of level p with $p \not\equiv 3 \pmod 8$ and E is not a Neumann–Setzer curve then the modular degree of E is even or $p = 17$. There are 23442 [BM90] curves of conductor $37 \le p \le 10^7$ with $p \equiv 3 \pmod 8$, of which 11815 have even functional equation, of which 7322 have rank 0, and 4589 have odd modular degree. The significance of the data concerning the rank is that the second author has conjectured that 2^r divides the modular degree, where r is the rank.

Conjecture 4.3. *If* E *is an optimal elliptic curve of prime conductor* p *and* E *has odd modular degree, then* $p \equiv 3 \pmod 8$ *or* E *is a Neumann–Setzer curve, or* $p = 17$*.*

4.3. **Shafarevich–Tate Groups of Neumann–Setzer Curves.** We consider the distribution of Ш in the Neumann–Setzer family (and note that similar phenomena occur in the other families). We look at u with $u^2 + 64$ prime and less than $2 \cdot 10^{12}$. We now take u to be positive, which thus replaces the restriction that u be 3 mod 4. The heuristics of [Del01] would seem to tell give us an idea of how often we expect a given prime to divide Ш. For instance, since Neumann–Setzer curves have rank 0, the prime 3 should divide Ш about 36.1% of the time. However, Table 1 gives a slightly different story with effects seen that depend on the various congruential properties of u.

Table 1. Frequency of a prime dividing Ш

restriction	number	$p = 3$	$p = 5$	$p = 7$	$p = 11$
$u \equiv 1 \pmod 8$	25559	33.2%	16.9%	9.2%	3.0%
$u \equiv 3 \pmod 8$	25557	39.7%	20.3%	14.3%	8.4%
$u \equiv 5 \pmod 8$	25584	36.2%	18.5%	11.5%	5.0%
$u \equiv 7 \pmod 8$	25612	34.3%	20.3%	14.3%	8.2%
$u \equiv 0 \pmod 3$	34009	36.0%	18.7%	12.1%	6.0%
$u \equiv 1 \pmod 3$	34032	35.2%	18.6%	11.5%	5.6%
$u \equiv 2 \pmod 3$	34271	36.3%	19.7%	13.3%	6.9%
$u \equiv 0 \pmod 5$	34208	33.1%	18.0%	11.4%	5.4%
$u \equiv 2 \pmod 5$	33879	37.1%	19.5%	12.8%	6.5%
$u \equiv 3 \pmod 5$	34225	37.3%	19.5%	12.7%	6.5%
total	102312	35.8%	19.0%	12.3%	6.2%
Delaunay		36.1%	20.7%	14.5%	9.2%

References

[AL96] A. Abbes, E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires* (French). Compositio Math. **103** (1996), no. 3, 269–286.

[BM90] A. Brumer, O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves.* Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382, data available online at `http://modular.fas.harvard.edu/~oisin`

[Cre] J. E. Cremona, *Elliptic Curves of conductor* $\leq$ 17000, electronic tables available online at `http://www.maths.nott.ac.uk/personal/jec/ftp/data`

[Del01] C. Delaunay, *Heuristics on Tate-Shafarevitch Groups of Elliptic Curves Defined over* **Q**. Experiment. Math. **10** (2001), no. 2, 191–196.

[Del83] P. Deligne, *Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings).* (French). Seminar Bourbaki, Vol. 1983/84. Astérisque No. 121-122, (1985), 25–41.

[1] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133.

[Eme01] M. Emerton, *Optimal Quotients of Modular Jacobians,* preprint (2001).

[Frey87] G. Frey, *Links between solutions of $A-B=C$ and elliptic curves.* In *Number Theory (Ulm, 1987),* edited by H. P. Schlickewei and E. Wirsing, 31–62, Lecture Notes in Mathematics, 1380, Springer-Verlag, New York, 1989.

[Guy94] R. K. Guy, *Unsolved problems in number theory,* Springer-Verlag, 1994.

[HL22] G. H. Hardy, J. E. Littlewood, *Some Problems of 'Partitio Numerorum.' III. On the Expression of a Number as a Sum of Primes.* Acta. Math. **44** (1922), 1–70.

[LO91] S. Ling, J. Oesterlé, The Shimura subgroup of $J_0(N)$. Astérisque **196–197** (1991), 171–203.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

[Maz98] B. Mazur, *Three Lectures about the Arithmetic of Elliptic Curves.* Rough, unedited, and preliminary notes from lectures given at the 1998 Arizona Winter School. Available at `http://swc.math.arizona.edu/notes/files/98MazurLN.ps`

[Mer96] L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$*, J. Reine Angew. Math. **477** (1996), 71–115.

[MO89] J.-F. Mestre, J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième* (French). J. Reine Angew. Math. **400** (1989), 173–184.

[Neu71] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I, II* (German). Math. Nachr. **49** (1971), 107–123, **56** (1973), 269–280.

[Ogg74] A. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France **102** (1974), 449–462.

[RS01] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232.

[Set75] B. Setzer, *Elliptic Curves of prime conductor.* J. London Math. Soc. (2), **10** (1975), 367–378.

[Ste89] G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves.* Invent. Math. **98** (1989), no. 1, 75–106.

[SW02] W. A. Stein, M. Watkins, *A Database of Elliptic Curves—First Report.* In *Algorithmic number theory* (Sydney 2002), 267–275, edited by C. Fieker and D. Kohel, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[Tan97] S.-L. Tang, *Congruences between modular forms, cyclic isogenies of modular elliptic curves, and integrality of p-adic L-function.* Trans. Amer. Math. Soc. **349** (1997), no. 2, 837–856.

[Vat03] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves,* preprint (2003).

[Wat02] M. Watkins, *Computing the modular degree of an elliptic curve,* Experiment. Math. **11** (2002), no. 4, 487–502.

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551.