Algebra & Number Theory

Volume 19
2025
No. 1

Curves with few bad primes over cyclotomic $\mathbb{Z}_\ell$-extensions

Samir Siksek and Robin Visser

msp

ALGEBRA AND NUMBER THEORY 19:1 (2025)
https://doi.org/10.2140/ant.2025.19.113

Curves with few bad primes over cyclotomic $\mathbb{Z}_\ell$-extensions

Samir Siksek and Robin Visser

Let K be a number field, and S a finite set of nonarchimedean places of K, and write $\mathcal{O}^\times$ for the group of S-units of K. A famous theorem of Siegel asserts that the S-unit equation $\varepsilon+\delta=1$, with $\varepsilon, \delta \in \mathcal{O}^\times$, has only finitely many solutions. A famous theorem of Shafarevich asserts that there are only finitely many isomorphism classes of elliptic curves over K with good reduction outside S. Now instead of a number field, let $K=\mathbb{Q}_{\infty,\ell}$ which denotes the $\mathbb{Z}_\ell$-cyclotomic extension of $\mathbb{Q}$. We show that the S-unit equation $\varepsilon+\delta=1$, with $\varepsilon, \delta \in \mathcal{O}^\times$, has infinitely many solutions for $\ell \in \{2, 3, 5, 7\}$, where S consists only of the totally ramified prime above ℓ. Moreover, for every prime ℓ, we construct infinitely many elliptic or hyperelliptic curves defined over K with good reduction away from 2 and ℓ. For certain primes ℓ we show that the Jacobians of these curves in fact belong to infinitely many distinct isogeny classes.

1. Introduction

Let ℓ be a rational prime and r a positive integer. Write $\mathbb{Q}_{r,\ell}$ for the unique degree ℓ^r totally real subfield of $\bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_n)$, where μ_n denotes the set of ℓ^n-th roots of 1. We let $\mathbb{Q}_{\infty,\ell}=\bigcup_r \mathbb{Q}_{r,\ell}$; this is the $\mathbb{Z}_\ell$-cyclotomic extension of $\mathbb{Q}$, and $\mathbb{Q}_{r,\ell}$ is called the r-th layer of $\mathbb{Q}_{\infty,\ell}$. Now let K be a number field, and write $K_{\infty,\ell}=K \cdot \mathbb{Q}_{\infty,\ell}$ and $K_{r,\ell}=K \cdot \mathbb{Q}_{r,\ell}$. To ease notation we shall sometimes write K_∞ for $K_{\infty,\ell}$. We write $\mathcal{O}_\infty$ (or $\mathcal{O}_{\infty,\ell}$) for the integers in K_∞ (i.e., the integral closure of $\mathbb{Z}$ in K_∞), and write $\mathcal{O}_r$ (or $\mathcal{O}_{r,\ell}$) for the integers of $K_{r,\ell}$. Clearly $\mathcal{O}_{\infty,\ell}=\bigcup_r \mathcal{O}_{r,\ell}$. The motivation for the present paper is a series of conjectures and theorems that suggest that the arithmetic of curves (respectively abelian varieties) over K_∞ is similar to the arithmetic of curves (respectively abelian varieties) over K. One of these is the following conjecture of Mazur [1972], which in essence says that the Mordell–Weil theorem continues to hold over K_∞.

Conjecture (Mazur). *Let A/K_∞ be an abelian variety. Then $A(K_\infty)$ is finitely generated.*

Another is a conjecture of Parshin and Zarhin [1989, page 91] which is the analogue of Faltings' theorem (Mordell conjecture) over K_∞.

Conjecture (Parshin and Zarhin). *Let X/K_∞ be a curve of genus ≥ 2. Then $X(K_\infty)$ is finite.*

Siksek is supported by the EPSRC grant *Moduli of Elliptic curves and Classical Diophantine Problems* (EP/S031537/1). Visser is supported by an EPSRC studentship (EP/V520226/1).
MSC2020: primary 11G10; secondary 11G05.
Keywords: Shafarevich conjecture, Abelian varieties, cyclic fields, cyclotomic fields, integral points.

© 2025 MSP (Mathematical Sciences Publishers). Distributed under the Creative Commons Attribution License 4.0 (CC BY). Open Access made possible by subscribing institutions via Subscribe to Open.

A third is the following theorem of Zarhin [2010, Corollary 4.2], which asserts that the Tate homomorphism conjecture (also a theorem of Faltings [1983] over number fields) continues to hold over K_∞.

Theorem (Zarhin). *Let A, B be abelian varieties defined over $K_{\infty,\ell}$, and denote their respective ℓ-adic Tate modules by $T_\ell(A)$, $T_\ell(B)$. Then the natural embedding*

$$\mathrm{Hom}_{K_\infty}(A, B) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{K_\infty}/K_\infty)}(T_\ell(A), T_\ell(B))$$

is a bijection.

Mazur's conjecture is now known to hold for certain elliptic curves. For example, if E is an elliptic curve defined over $\mathbb{Q}$ then $E(\mathbb{Q}_\infty)$ is finitely generated thanks to theorems of Kato, Ribet and Rohrlich [Greenberg 2001, Theorem 1.5]. From this one can deduce [Greenberg 2001, Theorem 1.24] that $X(\mathbb{Q}_\infty)$ is finite for curves $X/\mathbb{Q}$ of genus ≥ 2 equipped with a nonconstant morphism to an elliptic curve $X \to E$ defined over $\mathbb{Q}$. We also note that the conjecture of Parshin and Zarhin follows easily from Mazur's conjecture and Faltings' theorem. Indeed, using the Abel–Jacobi map we can deduce from Mazur's conjecture that $X(K_\infty) = X(K_r)$ for suitably large r, and we know that $X(K_r)$ is finite by Faltings' theorem.

It is natural to wonder whether other standard conjectures and theorems concerning the arithmetic of curves and abelian varieties over number fields continue to hold over K_∞. The purpose of this paper is to give counterexamples to potential generalizations of certain theorems of Siegel and Shafarevich to K_∞. A theorem of Siegel (e.g., [Abramovich 2009, Theorem 0.2.8]) asserts that $(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}_{K,S})$ is finite for any number field K and any finite set of primes S; modern proofs can be found in [Kim 2005; Lawrence and Venkatesh 2020; Poonen 2021]. We show that the corresponding statement over $\mathbb{Q}_{\infty,\ell}$ is false, at least for $\ell = 2, 3, 5, 7$. We denote by υ_ℓ the totally ramified prime of $\mathbb{Q}_{\infty,\ell}$ above ℓ (the precise meaning of primes in infinite extensions of $\mathbb{Q}$ is clarified in Section 2).

Theorem 1. *Let $\ell = 2, 3, 5$ or 7. Let*

$$S = \begin{cases} \{\upsilon_\ell\} & \text{if } \ell = 2, 5, 7, \\ \varnothing & \text{if } \ell = 3. \end{cases} \tag{1}$$

Let $\mathcal{O}_S$ denote the S-integers of $\mathbb{Q}_{\infty,\ell}$. Then $(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}_S)$ is infinite.

Remarks. • There have been several recent papers showing that $\mathbb{P}^1 - \{0, 1, \infty\}$ and other punctured curves have no or few integral points over various infinite families of number fields e.g., [Freitas et al. 2020; 2021a; 2021b; 2022; Triantafillou 2021]. In particular, it is shown in [Freitas et al. 2020] that $(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}_\infty) = \varnothing$ for $\ell \neq 3$. The obstruction given in [loc. cit.] for $\ell \neq 3$ is local in nature. In essence, Theorem 1 complements this result, showing that we can obtain infinitely many integral or S-integral points in the absence of the local obstruction. The proof of Theorem 1 is constructive.

• Theorem 1 strongly suggests that the conjecture of Parshin and Zarhin does not admit a straightforward generalization to the broader context of integral points on hyperbolic curves. We also remark that there is a critical difference over K_∞ between complete curves X of genus ≥ 2 and $\mathbb{P}^1 - \{0, 1, \infty\}$. For the former, the group of K_∞-points of the Jacobian is expected to be finitely generated by Mazur's conjecture. For the latter, the analogue of the Jacobian is the generalized Jacobian which is $\mathbb{G}_m \times \mathbb{G}_m$, and its group of K_∞-points is $(\mathbb{G}_m \times \mathbb{G}_m)(K_\infty) = \mathcal{O}_\infty^\times \times \mathcal{O}_\infty^\times$, which is infinitely generated.

Variants of the proof of Theorem 1 give the following.

Theorem 2. *Let $\ell = 2, 3$ or 5. Let $S = \{\upsilon_\ell\}$ and write $\mathcal{O}_S$ for the S-integers of $\mathbb{Q}_{\infty,\ell}$. Let*

$$k \in \begin{cases} \{1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 24\} & \text{if } \ell = 2, 3, \\ \{1, 2, 4\} & \text{if } \ell = 5. \end{cases}$$

Then $(\mathbb{P}^1 - \{0, k, \infty\})(\mathcal{O}_S)$ is infinite.

Let ζ_{ℓ^n} denote a primitive ℓ^n-th root of 1, and write $\Omega_{n,\ell} = \mathbb{Q}(\zeta_{\ell^n})$, and $\Omega_{n,\ell}^+ = \mathbb{Q}(\zeta_{\ell^n} + \zeta_{\ell^n}^{-1})$. Let

$$\Omega_{\infty,\ell} = \bigcup_{n=1}^{\infty} \Omega_{n,\ell}, \qquad \Omega_{\infty,\ell}^+ = \bigcup_{n=1}^{\infty} \Omega_{n,\ell}^+.$$

We note the inclusions $\Omega_{\infty,\ell} \supset \Omega_{\infty,\ell}^+ \supset \mathbb{Q}_{\infty,\ell}$. Nagell [1969, page 181] points out that $1 + \zeta_{\ell^n}$ is a unit for ℓ odd, and that therefore the equation $\varepsilon + \delta = 1$ has the solution $\varepsilon = -\zeta_{\ell^n}$, $\delta = 1 + \zeta_{\ell^n}$ in units belonging to $\Omega_{n,\ell}$. It follows straightforwardly from this (see the beginning of Section 3) that $\mathbb{P}^1 - \{0, 1, \infty\}$ has infinitely many integral points defined over $\Omega_{\infty,\ell}$. Many of our constructions of S-integral points on $\mathbb{P}^1 - \{0, 1, \infty\}$ apply in greater generality to the fields $\Omega_{\infty,\ell}$ and $\Omega_{\infty,\ell}^+$, where the statements are in fact much cleaner. For example, we prove the following theorem.

Theorem 3. *Let ℓ be an odd prime. Then $(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}(\Omega_{\infty,\ell}^+))$ is infinite.*

Here $\mathcal{O}(\Omega_{\infty,\ell}^+)$ denotes the integers of $\Omega_{\infty,\ell}^+$.

Shafarevich's conjecture asserts that for a number field K, a dimension n, a degree d, and a finite set of places S, there are only finitely many isomorphism classes of polarized abelian varieties defined over K of dimension n with degree-d polarization and with good reduction away from S. This conjecture was proved by Shafarevich for elliptic curves (i.e., $n = 1$) and by Faltings [1983] in complete generality. If we replace K by $\mathbb{Q}_{\infty,\ell}$ then the Shafarevich conjecture no longer holds. For example, consider

$$E_\varepsilon : \varepsilon Y^2 = X^3 - X,$$

where $\varepsilon \in \mathcal{O}_\infty^\times$. This elliptic curve has good reduction away from the primes above 2. Moreover, E_ε, E_δ are isomorphic over $\mathbb{Q}_\infty$ if and only if ε/δ is a square in $\mathcal{O}_\infty^\times$. As $\mathcal{O}_\infty^\times/(\mathcal{O}_\infty^\times)^2$ is infinite, we deduce that there are infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}_\infty$ with good reduction away from the primes above 2. It is however natural to wonder if a sufficiently weakened version of the Shafarevich conjecture continues to hold over $\mathbb{Q}_\infty$. Indeed, the curves E_ε in the above construction form a single $\overline{\mathbb{Q}}$-isomorphism class. This it is natural to ask if, for suitable ℓ and finite set of primes S, does the set of elliptic curves over $\mathbb{Q}_\infty$ with good reduction outside S form infinitely many $\overline{\mathbb{Q}}$-isomorphism classes?

Theorem 4. *Let $\ell = 2, 3, 5$, or 7. Let S be given by (1) and let $S' = S \cup \{\upsilon_2\}$ where υ_2 is the unique prime of $\mathbb{Q}_{\infty,\ell}$ above 2. Then, there are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over $\mathbb{Q}_{\infty,\ell}$ with good reduction away from S' and with full 2-torsion in $\mathbb{Q}_{\infty,\ell}$. Moreover, these elliptic curves form infinitely many distinct $\mathbb{Q}_{\infty,\ell}$-isogeny classes.*

Remarks. • By [Freitas et al. 2020, Lemma 2.1], a rational prime $p \neq \ell$ is inert in $\mathbb{Q}_{\infty,\ell}$ if and only if $p^{\ell-1} \not\equiv 1 \pmod{\ell^2}$. It follows from this that 2 is inert in $\mathbb{Q}_{\infty,\ell}$ for $\ell = 3, 5, 7$ and 11.

• Faltings' proof [1983] of the Mordell conjecture can be considered to have three major steps. In the first step, Faltings proves the Tate homomorphism conjecture. In the second step, Faltings derives the Shafarevich conjecture from the Tate homomorphism conjecture, and in the final step Faltings uses the "Parshin trick" to deduce the Mordell conjecture from the Shafarevich conjecture. Although Zarhin has extended the Tate homomorphism conjecture to K_∞, Theorem 4 suggests that there is no plausible strategy for proving the conjecture of Parshin and Zarhin by mimicking Faltings' proof of the Mordell conjecture.

It is natural to wonder if the isogeny classes appearing in the proof of Theorem 4 are finite or infinite. Rather reassuringly they turn out to be finite.

Theorem 5. *Let E be an elliptic curve over $\mathbb{Q}_{\infty,\ell}$ without potential complex multiplication. Then the $\mathbb{Q}_{\infty,\ell}$-isogeny class of E is finite.*

The original version of Shafarevich's conjecture [1963] (also proved by Faltings [1983, Korollar 1]) states that for a given number field K, a genus g and a finite set of places S, there are only finitely many isomorphism classes of genus-g curves C/K with good reduction away from S. Again this statement becomes false if we replace K by $\mathbb{Q}_{\infty,\ell}$ for any prime ℓ.

Theorem 6. *Let $g \geq 2$ and let $\ell = 3, 5, 7, 11$ or 13. There are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of genus-g hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ with good reduction away from $\{\upsilon_2, \upsilon_\ell\}$.*

Theorem 7. *Let $\ell \geq 11$ be an odd prime and let $g = \lfloor \frac{\ell-3}{4} \rfloor$. There are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of genus-g hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ with good reduction away from $\{\upsilon_2, \upsilon_\ell\}$. Moreover, if*

$$\ell \in \{11, 23, 59, 107, 167, 263, 347, 359\},$$

then the Jacobians of these curves form infinitely many distinct $\mathbb{Q}_{\infty,\ell}$-isogeny classes.

The paper is structured as follows. In Section 2 we recall basic results on units and S-units of the cyclotomic field $\mathbb{Q}(\zeta_{\ell^n})$. In Sections 3–6 we employ identities between cyclotomic polynomials to give constructive proofs of Theorems 1, 2 and 3. Section 7 gives a proof of Theorem 5, making use of a deep theorem of Kato to control the $\mathbb{Q}_{\infty,\ell}$-points on certain modular curves. Section 8 uses the integral and S-integral points on $\mathbb{P}^1 - \{0, 1, \infty\}$ furnished by Theorem 1 to construct infinite families of elliptic curves over $\mathbb{Q}_{\infty,\ell}$ for $\ell = 2, 3, 5, 7$, with good reduction away from $\{\upsilon_2, \upsilon_\ell\}$, which are used to give a proof of Theorem 4. Sections 9 and 10 give proofs of Theorems 6 and 7, making use of the relation, due to Kummer, between the class number of $\mathbb{Q}(\zeta_{\ell^n})^+$, and the index of cyclotomic units in the full group of units.

2. Units and S-units of $\mathbb{Q}(\zeta)$

Let K be a subfield of $\overline{\mathbb{Q}}$. We denote the integers of K (i.e., the integral closure of $\mathbb{Z}$ in K) by $\mathcal{O}(K)$. Let p be a rational prime. By a *prime of K above p* we mean a map $\upsilon : K \to \mathbb{Q} \cup \{\infty\}$ satisfying the following:

- $\upsilon(p) = 1$, $\upsilon(0) = \infty$.
- $\upsilon|_{K^\times} : K^\times \to \mathbb{Q}$ is a homomorphism.
- $\upsilon(1 + b) = 0$ whenever $\upsilon(b) > 0$.

Suppose $K = \bigcup K_n$ where $K_0 \subset K_1 \subset K_2 \subset \cdots$ is a tower of number fields (i.e., finite extensions of $\mathbb{Q}$), with $K_0 = \mathbb{Q}$. One sees that the primes of K above p are in one-to-one correspondence with sequences $\{\mathfrak{p}_n\}$ where:

- $\mathfrak{p}_n$ is a prime ideal of $\mathcal{O}(K_n)$.
- $\mathfrak{p}_{n+1} \mid \mathfrak{p}_n \mathcal{O}(K_{n+1})$.
- $\mathfrak{p}_0 = p\mathbb{Z}$.

Indeed, from υ one obtains the corresponding sequence $\{\mathfrak{p}_n\}$ via the formula $\mathfrak{p}_n = \{\alpha \in \mathcal{O}(K_n) : \upsilon(\alpha) > 0\}$. Given a sequence $\{\mathfrak{p}_n\}$, we can recover the corresponding υ by letting

$$\upsilon(\alpha) = \operatorname{ord}_{\mathfrak{p}_n}(\alpha) / \operatorname{ord}_{\mathfrak{p}_n}(p)$$

whenever $\alpha \in K_n^\times$. Given a finite set of primes S of K, we define the S-integers of K to be the set $\mathcal{O}(K, S)$ of all $\alpha \in K$ such that $\upsilon(\alpha) \geq 0$ for every prime $\upsilon \notin S$. We let $\mathcal{O}(K, S)^\times$ be the unit group of $\mathcal{O}(K, S)$; this is precisely the set of $\alpha \in K^\times$ such that $\upsilon(\alpha) = 0$ for every prime $\upsilon \notin S$. If $S = \varnothing$ then $\mathcal{O}(K, S) = \mathcal{O}(K)$ are the integers of K and $\mathcal{O}(K, S)^\times = \mathcal{O}(K)^\times$ are the units of K.

Fix a rational prime ℓ. For a positive integer n, let ζ_{ℓ^n} denote a primitive ℓ^n-th root of 1 which is chosen so that

$$\zeta_{\ell^{n+1}}^{\ell} = \zeta_{\ell^n}.$$

Let $\Omega_{n,\ell} = \mathbb{Q}(\zeta_{\ell^n})$; this has degree $\varphi(\ell^n)$, where φ is Euler totient function. Let

$$\Omega_{\infty,\ell} = \bigcup_{n=1}^{\infty} \Omega_{n,\ell}.$$

The prime ℓ is totally ramified in each $\Omega_{n,\ell}$, and we denote by λ_n the unique prime ideal of $\mathcal{O}(\Omega_{n,\ell})$ above ℓ. Thus

$$\ell \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{\varphi(\ell^n)}. \tag{2}$$

We write υ_ℓ for the unique prime of $\Omega_{\infty,\ell}$ above ℓ. For now fix $n \geq 1$ if $\ell \neq 2$ and $n \geq 2$ if $\ell = 2$. We recall that $\lambda_n = (1 - \zeta_{\ell^n}) \cdot \mathcal{O}(\Omega_{n,\ell})$. If $\ell \nmid s$ then $(1 - \zeta_{\ell^n}^s) \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n$; we can see this by applying the automorphism $\zeta_{\ell^n} \mapsto \zeta_{\ell^n}^s$ to (2).

Lemma 8. *Let s be an integer and let $t = \mathrm{ord}_\ell(s)$. Suppose $t < n$. Then*

$$(1-\zeta_{\ell^n}^s)\cdot\mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{\ell^t}.$$

Moreover,

$$\upsilon_\ell(1-\zeta_{\ell^n}^s) = \frac{1}{\ell^{n-1-t}(\ell-1)}.$$

Proof. Write $\zeta = \zeta_{\ell^n}$. Note that ζ^s is a primitive ℓ^{n-t}-th root of 1. Thus

$$(1-\zeta^s)\cdot\mathcal{O}(\Omega_{n-t,\ell}) = \lambda_{n-t}.$$

As ℓ is totally ramified in $\Omega_{n,\ell}$, we have

$$(1-\zeta^s)\cdot\mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{[\Omega_{n,\ell}:\Omega_{n-t,\ell}]} = \lambda_n^{\ell^t}.$$

For the final part of the lemma,

$$\upsilon_\ell(1-\zeta^s) = \frac{\mathrm{ord}_{\lambda_n}(1-\zeta^s)}{\mathrm{ord}_{\lambda_n}(\ell)} = \frac{\ell^t}{\varphi(\ell^n)} = \frac{1}{\ell^{n-1-t}(\ell-1)}. \qquad \square$$

Cyclotomic units and S-units. Write V_n for the subgroup of $\mathcal{O}(\Omega_n, \{\upsilon_\ell\})^\times$ generated by

$$\{\pm\zeta_{\ell^n}, 1-\zeta_{\ell^n}^k : 1 \le k < \ell^n\}$$

and let

$$C_n = V_n \cap \mathcal{O}(\Omega_n)^\times.$$

The group C_n is called [Washington 1997, Chapter 8] the group of *cyclotomic units* in Ω_n. We will often find it more convenient to work with the group V_n.

Lemma 9. *The abelian group $V_n/\langle\pm\zeta_{\ell^n}\rangle$ is free with basis*

$$\{1-\zeta_{\ell^n}^k : 1 \le k < \ell^n/2, \ell \nmid k\}. \tag{3}$$

Proof. The torsion subgroup of V_n is the torsion subgroup of $\Omega_n^\times$ which is $\langle\pm\zeta_{\ell^n}\rangle$. Thus $V_n/\langle\pm\zeta_{\ell^n}\rangle$ is torsion free. By definition of V_n, the group $V_n/\langle\pm\zeta_{\ell^n}\rangle$ is generated by $1-\zeta_{\ell^n}^k$ with $\ell^n \nmid k$. Write $k = \ell^r d$ with $\ell \nmid d$; thus $r < n$. Suppose $r \ge 1$. Then,

$$\begin{aligned} 1-\zeta_{\ell^n}^k &= 1-\zeta_{\ell^n}^{\ell^r d} \\ &= \prod_{i=0}^{\ell^r-1}(1-\zeta_{\ell^n}^d\zeta_{\ell^r}^i) \quad \text{using} \quad 1-X^{\ell^r} = \prod_{i=0}^{\ell^r-1}(1-\zeta_{\ell^r}^i X) \\ &= \prod_{i=0}^{\ell-1}(1-\zeta_{\ell^n}^{d+i\ell^{n-r}}). \end{aligned}$$

It follows that $V_n/\langle\pm\zeta_{\ell^n}\rangle$ is generated by $1-\zeta_{\ell^n}^k$ with $\ell \nmid k$. If $\ell^n/2 < k < \ell^n$ and $\ell \nmid k$ then

$$1-\zeta_{\ell^n}^k = -\zeta_{\ell^n}^k(1-\zeta_{\ell^n}^{\ell^n-k}). \tag{4}$$

Thus (3) certainly generates $V_n/\langle \pm\zeta_\ell^n \rangle$. Note that (3) has cardinality $\varphi(\ell^n)/2$ where φ is the Euler totient function. It therefore suffices to show that V_n has rank $\varphi(\ell^n)/2$. A well-known theorem [Washington 1997, Theorem 8.3] states that C_n has finite index in $\mathcal{O}(\Omega_n)^\times$ and thus, by Dirichlet's unit theorem, C_n has rank $-1+\varphi(\ell^n)/2$. We note that C_n is the kernel of the surjective homomorphism $V_n \to \mathbb{Z}$, sending μ to $\mathrm{ord}_{\lambda_n}(\mu)$. Thus V_n has rank $\varphi(\ell^n)/2$ completing the proof. □

Lemma 10. *Let $n \geq 2$ if $\ell \neq 2$ and $n \geq 3$ if $\ell = 2$. Then $V_{n-1} \subset V_n$. Moreover,*

$$\prod_{\substack{1 \leq k < \ell^n/2 \\ \ell \nmid k}} (1-\zeta_{\ell^n}^k)^{c_k} \in \langle \pm\zeta_{\ell^n}, V_{n-1} \rangle$$

if and only if $c_k = c_m$ whenever $k \equiv m \pmod{\ell^{n-1}}$.

Proof. The group V_{n-1} is generated, modulo roots of unity, by $1-\zeta_{\ell^{n-1}}^d$ with $\ell \nmid d$. By the proof of Lemma 9,

$$1-\zeta_{\ell^{n-1}}^d = 1-\zeta_{\ell^n}^{\ell d} = \prod_{i=0}^{\ell-1}(1-\zeta_{\ell^n}^{d+i\ell^{n-1}}).$$

The lemma follows from Lemma 9. □

Given $a \in \mathbb{Z}_\ell$, it makes sense to reduce a modulo ℓ^n and therefore it makes sense to write $\zeta_{\ell^n}^a$. We write $\{a\}_n$ for the unique integer satisfying

$$0 \leq \{a\}_n < \ell^n/2, \quad \{a\}_n \equiv \pm a \pmod{\ell^n}.$$

Lemma 11. *Let $a_1, \dots, a_r \in \mathbb{Z}_\ell$ and $c_1, \dots, c_r \in \mathbb{Z}$. Suppose:*

(i) $c_1 \neq 0$.

(ii) $a_1 \not\equiv 0 \pmod{\ell}$.

(iii) $a_1 \not\equiv \pm a_2, \pm a_3, \dots, \pm a_r \pmod{\ell^n}$.

Write

$$\varepsilon_n = \prod_{1 \leq i \leq r} (1-\zeta_{\ell^n}^{a_i})^{c_i}. \tag{5}$$

Then, $\varepsilon_n \notin \langle \pm\zeta_{\ell^n}, V_{n-1} \rangle$ for all sufficiently large n.

Proof. If $a_j \equiv 0 \pmod{\ell}$ then $(1-\zeta_{\ell^n}^{a_j}) \in V_{n-1}$. We may therefore suppose $a_j \not\equiv 0 \pmod{\ell}$ for all j. Write

$$\delta_n = \prod_{1 \leq i \leq r} (1-\zeta_{\ell^n}^{\{a_i\}_n})^{c_i}.$$

In view of the identity (4) it will be sufficient to show that $\delta_n \notin \langle \pm\zeta_{\ell^n}, V_{n-1} \rangle$ for n sufficiently large. Also, in view of Lemma 10, it is sufficient to show for sufficiently large n that $\{a_1\}_n \not\equiv \{a_j\}_n \pmod{\ell^n}$ for all $2 \leq j \leq n$. This is equivalent to $a_1 \neq \pm a_j$ for $2 \leq j \leq n$ which is hypothesis (iii). This completes the proof. □

The following corollary easily follows from Lemma 11.

Corollary 12. *Let $a_1, \dots, a_r \in \mathbb{Z}_\ell$ and $c_1, \dots, c_r \in \mathbb{Z}$. Suppose*:

(i) $c_1 \equiv 1 \pmod 2$.

(ii) $a_1 \not\equiv 0 \pmod \ell$.

(iii) $a_1 \neq \pm a_2, \pm a_3, \dots, \pm a_r \pmod{\ell^n}$.

Let ε_n be as in (5). *Then, $\varepsilon_n \notin \langle \pm\zeta_{\ell^n}, V_{n-1}, V_n^2 \rangle$ for all sufficiently large n.*

Units and S-units from cyclotomic polynomials. For $m \geq 1$, let $\Phi_m(X) \in \mathbb{Z}[X]$ be the *m-th cyclotomic polynomial* defined by

$$\Phi_m(X) = \prod_{\substack{1 \leq i \leq m \\ (i,m)=1}} (X - \zeta_m^i).$$

These satisfy the identity [Washington 1997, Chapter 2]

$$X^m - 1 = \prod_{d \mid m} \Phi_d(X). \tag{6}$$

It follows from the Möbius inversion formula that

$$\Phi_m(X) = \prod_{d \mid m} (X^d - 1)^{\mu(m/d)}, \tag{7}$$

where μ denotes the Möbius function.

Lemma 13. *Let ℓ be a prime and $n \geq 1$. Let $m \geq 1$, and suppose $\ell^n \nmid m$*:

(a) $\Phi_m(\zeta_{\ell^n}) \in V_n \subseteq \mathcal{O}(\Omega_{n,\ell}, S)^\times$, *where $S = \{\upsilon_\ell\}$.*

(b) *If $m \neq \ell^u$ for all $u \geq 0$, then $\Phi_m(\zeta_{\ell^n}) \in C_n \subseteq \mathcal{O}(\Omega_{n,\ell})^\times$.*

Moreover,

$$\upsilon_\ell(\Phi_{\ell^t}(\zeta_{\ell^n})) = \begin{cases} 1/(\ell^{n-1}(\ell-1)), & t = 0, \\ 1/\ell^{n-t}, & 1 \leq t \leq n-1. \end{cases}$$

Proof. Let $t = \operatorname{ord}_\ell(m) < n$. Observe that $\Phi_m(X) \mid (X^m - 1)$. Hence $\Phi_m(\zeta_{\ell^n}) \cdot \mathcal{O}(\Omega_{n,\ell})$ divides $(1 - \zeta_{\ell^n}^m) \cdot \mathcal{O}(\Omega_{n,\ell})$. By Lemma 8 we have $(1 - \zeta_{\ell^n}^m) \cdot \mathcal{O}(\Omega_{n,\ell}) = \lambda_n^{\ell^t}$, giving (a).

For (b), write $m = \ell^t k$ where $k > 1$. Then $\Phi_m(X)$ divides the polynomial $(X^m - 1)/(X^{\ell^t} - 1)$. Therefore $\Phi_m(\zeta_{\ell^n}) \cdot \mathcal{O}(\Omega_{n,\ell})$ divides

$$\frac{(1 - \zeta_{\ell^n}^m)}{(1 - \zeta_{\ell^n}^{\ell^t})} \cdot \mathcal{O}(\Omega_{n,\ell}) = \frac{\lambda_n^{\ell^t}}{\lambda_n^{\ell^t}} = 1 \cdot \mathcal{O}(\Omega_{n,\ell}).$$

Thus $\Phi_m(\zeta_{\ell^n})$ is a unit, giving (b).

The final part of the lemma follows from Lemma 8, and the formulae

$$\Phi_{\ell^t}(X) = \begin{cases} X - 1, & t = 0, \\ (X^{\ell^t} - 1)/(X^{\ell^{t-1}} - 1), & t \geq 1. \end{cases}$$

□

Lemma 14. *Let $n \geq 2$ if $\ell \neq 2$ and $n \geq 3$ if $\ell = 2$. Then $V_n/\langle \pm\zeta_{\ell^n}\rangle$ is free with basis*

$$\{\Phi_m(\zeta_{\ell^n}) : 1 \leq m < \ell^n/2, \ell \nmid m\}.$$

Proof. This follows from Lemma 9 thanks to identities (6) and (7). □

3. The S-unit equation over $\mathbb{Q}(\zeta_{\ell^n})^+$

We continue with the notation of the previous section. In particular, let K be a subfield of $\overline{\mathbb{Q}}$ and S be a finite set of primes of K. Let k be a nonzero rational integer. We shall make frequent use of the correspondence between elements of $(\mathbb{P}^1 - \{0, k, \infty\})(\mathcal{O}(K, S))$ and the set of solutions to the S-unit equation

$$\varepsilon + \delta = k, \quad \varepsilon, \delta \in \mathcal{O}(K, S)^\times,$$

sending $\varepsilon \in (\mathbb{P}^1 - \{0, k, \infty\})(\mathcal{O}(K, S))$ to $(\varepsilon, \delta) = (\varepsilon, k - \varepsilon)$.

Now, as before, let ℓ be a rational prime and n is a positive integer. If $\ell = 2$ suppose $n \geq 2$. Let $\zeta = \zeta_{\ell^n}$, and write $\Omega^+_{n,\ell} = \mathbb{Q}(\zeta + 1/\zeta)$ for the index-2 totally real subfield of $\Omega_{n,\ell}$. Let

$$\Omega^+_{\infty,\ell} = \bigcup_{n=1}^{\infty} \Omega^+_{n,\ell}.$$

In this section, for suitable S, we produce solutions to S-unit equations over $\Omega^+_{\infty,\ell}$.

As before, Φ_m denotes the m-cyclotomic polynomial. It is convenient to record the first few Φ_m:

$$\Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1,$$
$$\Phi_4 = X^2 + 1, \quad \Phi_5 = X^4 + X^3 + X^2 + X + 1, \quad \Phi_6 = X^2 - X + 1,$$
$$\Phi_7 = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, \quad \Phi_8 = X^4 + 1,$$
$$\Phi_9 = X^6 + X^3 + 1, \quad \Phi_{10} = X^4 - X^3 + X^2 - X + 1.$$

We shall call a polynomial $F \in \mathbb{Z}[X]$ *supercyclotomic* if it is of the form $X^m f_1 f_2 \cdots f_k$ where each $f_i(X)$ is a cyclotomic polynomial. We know, thanks to Lemma 13, that if F is supercyclotomic and ℓ is a prime, then $F(\zeta_{\ell^n}) \in \mathcal{O}(\Omega_n, \{\upsilon_\ell\})^\times$ for n sufficiently large. We wrote a short computer program that lists all supercyclotomic polynomials of degree at most 20 and searches for ternary relations of the form $F - G = kH$ with F, G, H supercyclotomic, $\gcd(F, G, H) = 1$ and k is a positive integer. Note that any such relation $F - G = kH$ gives points

$$\varepsilon_n = F(\zeta_{\ell^n})/H(\zeta_{\ell^n}) \in (\mathbb{P}^1 - \{0, k, \infty\})(\mathcal{O}(\Omega_n, \{\upsilon_\ell\})),$$

for n sufficiently large. We found the following ternary relations between supercyclotomic polynomials:

$$\Phi_2(X)^2 - \Phi_3(X) = X, \tag{8}$$

$$\Phi_2(X)^2 - \Phi_4(X) = 2X, \tag{9}$$

$$\Phi_2(X)^2 - \Phi_6(X) = 3X, \tag{10}$$

$$\Phi_2(X)^2 - \Phi_1(X)^2 = 4X, \tag{11}$$

$$\Phi_2(X)^4 - \Phi_{10}(X) = 5X\Phi_3(X), \tag{12}$$

$$\Phi_2^2(X)\Phi_3(X) - \Phi_1(X)^2\Phi_6(X) = 6X\Phi_4(X), \tag{13}$$

$$\Phi_7(X) - \Phi_1(X)^6 = 7X\Phi_6(X)^2, \tag{14}$$

$$\Phi_2(X)^4 - \Phi_1(X)^4 = 8X\Phi_4(X), \tag{15}$$

$$\Phi_2(X)^4\Phi_5(X) - \Phi_1(X)^4\Phi_{10}(X) = 10X\Phi_4(X)^3. \tag{16}$$

From the identities (6) and (7) one easily sees that $F(X^k)$ is supercyclotomic for any supercyclotomic polynomial F and any positive integer k; thus each of the nine identities above in fact yields an infinite family of identities. We pose the following open problems:

- Are there ternary linear relations between supercyclotomic polynomials that are outside these nine families?
- Classify all ternary linear relations between supercyclotomic polynomials.

Lemma 15. *Let $c : \Omega_\ell \to \Omega_\ell$ denote complex conjugation. Let $n \ge 1$ and let $\zeta = \zeta_{\ell^n}$ be an ℓ^n-th root of* 1. *Let $m \ge 1$ and suppose $\ell^n \nmid m$. Then*

$$\frac{\Phi_m(\zeta)^c}{\Phi_m(\zeta)} = \begin{cases} \zeta^{-\varphi(m)}, & m \ge 2, \\ -\zeta^{-1}, & m = 1. \end{cases}$$

Proof. Note that $\zeta^c = \zeta^{-1}$. So

$$\frac{\Phi_1(\zeta)^c}{\Phi_1(\zeta)} = \frac{\zeta^{-1}-1}{\zeta-1} = -\zeta^{-1}, \qquad \frac{\Phi_2(\zeta)^c}{\Phi_2(\zeta)} = \frac{\zeta^{-1}+1}{\zeta+1} = \zeta^{-1}.$$

Let $m \ge 3$. The polynomial Φ_m is monic of degree $\varphi(m)$, and its roots are the primitive m-th roots of 1 which come in distinct pairs η, η^{-1}. Thus the trailing coefficient is 1. It follows that $X^{\varphi(m)}\Phi_m(X^{-1})$ is monic and has the same roots as Φ_m, therefore

$$\Phi_m(X) = X^{\varphi(m)}\Phi_m(X^{-1}).$$

Hence

$$\frac{\Phi_m(\zeta)^c}{\Phi_m(\zeta)} = \frac{\Phi_m(\zeta^{-1})}{\Phi_m(\zeta)} = \zeta^{-\varphi(m)}. \qquad \square$$

Lemma 16. *Let ℓ be a prime. Let $F \in \mathbb{Z}[X]$ be a product of powers of cyclotomic polynomials. Suppose that the exponents of $\Phi_1(X)$ and $\Phi_2(X)$ in the factorization of F are both even. Then F has even degree and, for suitably large n, we have*

$$\zeta^{-\deg(F)/2}F(\zeta) \in \mathcal{O}(\Omega_{n,\ell}^+, S)^\times,$$

where $\zeta = \zeta_{\ell^n}$ and $S = \{\upsilon_\ell\}$.

Proof. We note that Φ_m has degree $\varphi(m)$ which is even for $m \ge 3$. It follows from this that F has even degree. From Lemma 13 we have $\zeta^{-\deg(F)/2}F(\zeta) \in \mathcal{O}(\Omega_{n,\ell}, S)^\times$ for suitably large n. To prove the lemma we need to show that $\zeta^{-\deg(F)/2}F(\zeta)$ is fixed by complex conjugation. Let G be either Φ_1^2, or Φ_2^2, or Φ_m with $m \ge 3$. We claim that $\zeta^{-\deg(G)/2}G(\zeta)$ is fixed by complex conjugation. Since F is a product of such G, the lemma follows from our claim. The claim is trivially true for $G = \Phi_1^2$ and $G = \Phi_2^2$, and follows immediately from Lemma 15 for $G = \Phi_m$ with $m \geq 3$. □

Lemma 17. *Let* $S = \{\upsilon_\ell\}$. *Let*

$$k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}.$$

Then $(\mathbb{P}^1 - \{0, k, \infty\})(\mathcal{O}(\Omega^+_{\infty,\ell}, S))$ *is infinite.*

Proof. The proof makes use of identities (8)–(16). Each identity has the form $P - Q = kXR$, where P, Q, and R are supercyclotomic polynomials. Let n be sufficiently large so that ζ_{ℓ^n} is not a root of PQR, and write

$$\varepsilon_n = \frac{P(\zeta_{\ell^n})}{\zeta_{\ell^n} R(\zeta_{\ell^n})}, \quad \delta_n = \frac{-Q(\zeta_{\ell^n})}{\zeta_{\ell^n} R(\zeta_{\ell^n})}.$$

From the identity $P - Q = kXR$ we see that $\varepsilon_n + \delta_n = k$. We note the following features of the triples (P, Q, R) common to all the identities (8)–(16):

- In every case, P, Q, R are products of powers of cyclotomic polynomials where the exponents of Φ_1 and Φ_2 are both even.
- Write $d = \deg(P)$. Then $\deg(Q) = d$ and $\deg(R) = d - 2$. Indeed as supercyclotomic polynomials are monic, the relation $P - Q = kXR$ forces P and Q to have the same degree as soon as $k \geq 2$.

We may rewrite ε_n as

$$\varepsilon_n = \frac{\zeta_{\ell^n}^{-d/2} P(\zeta_{\ell^n})}{\zeta_{\ell^n}^{-(d-2)/2} R(\zeta_{\ell^n})}, \quad \delta_n = \frac{-\zeta_{\ell^n}^{-d/2} Q(\zeta_{\ell^n})}{\zeta_{\ell^n}^{-(d-2)/2} R(\zeta_{\ell^n})}.$$

By Lemma 16, we have $\varepsilon_n, \delta_n \in \mathcal{O}(\Omega^+_{n,\ell}, S)^\times$ for n suitably large, and therefore ε_n is an $\mathcal{O}(\Omega^+_{\infty,}, S)$-point on $\mathbb{P}^1 - \{0, k, \infty\}$. To complete the proof we need to show that we obtain infinitely many distinct points as we vary n. We will do this for $k = 10$. The other cases are similar. Note that

$$\varepsilon_n = \frac{\Phi_2(\zeta_{\ell^n})^4 \Phi_5(\zeta_{\ell^n})}{\zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3} = \frac{(1 - \zeta_{\ell^n}^2)^7 (1 - \zeta_{\ell^n}^5)}{\zeta_{\ell^n}(1 - \zeta_{\ell^n})^5 (1 - \zeta_{\ell^n}^4)^3} \in V_n.$$

To show that we obtain infinitely many distinct ε_n it is enough to show that $\varepsilon_n \notin V_{n-1}$ for n sufficiently large. This follows by an easy application of Lemma 10; to illustrate this let $\ell = 5$ and suppose $\varepsilon_n \in V_{n-1}$. Note that $1 - \zeta_{5^n}^5 \in V_{n-1}$. It follows that

$$(1 - \zeta_{5^n})^{-5} (1 - \zeta_{5^n}^2)^7 (1 - \zeta_{5^n}^4)^{-3} \in \langle \pm\zeta_{\ell^n}, V_{n-1} \rangle.$$

Now in the product on the left the exponent of $1 - \zeta_{5^n}$ is -5 whereas the exponent of $1 - \zeta_{5^n}^{1+5^{n-1}}$ is 0, contradicting Lemma 10. The proof is similar for $\ell = 2$, and for $\ell \neq 2, 5$. It follows that we have infinitely many $\mathcal{O}(\Omega^+_{\infty,\ell}, S)$-points on $\mathbb{P}^1 - \{0, 10, \infty\}$. □

Proof of Theorem 2 for $\ell = 2$ and 3. For $\ell = 2, 3$, we have $\Omega^+_{\infty,\ell} = \mathbb{Q}_{\infty,\ell}$. Indeed, if $\ell = 2$ then $\mathbb{Q}_{n,2} = \Omega^+_{n+2,2}$ and if $\ell = 3$ then $\mathbb{Q}_{n,3} = \Omega^+_{n+1,3}$. Therefore Theorem 2 with $\ell = 2$ and 3 follows immediately from Lemma 17 for $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$.

Also, if $\ell=2$, then the infinitely many solutions $\varepsilon+\delta=6$ yield infinitely many solutions for $2\varepsilon+2\delta=12$ and $4\varepsilon+4\delta=24$. And if $\ell=3$, then the infinitely many solutions $\varepsilon+\delta=4$ yield infinitely many solutions $3\varepsilon+3\delta=12$, and similarly the infinitely many solutions $\varepsilon+\delta=8$ yield infinitely many solutions $3\varepsilon+3\delta=24$. This proves Theorem 2 for $\ell=2$, 3 and $k\in\{12,24\}$. □

Proof of Theorem 1 for $\ell=2$. Theorem 1 for $\ell=2$ is simply a special case of Theorem 2. □

4. The unit equation over $\mathbb{Q}(\zeta_{\ell^n})^+$

For roots of unity α, β, we let

$$E(\alpha,\beta)=\frac{\alpha^2+\alpha^{-2}}{(\alpha\beta^{-1}+\alpha^{-1}\beta)(\alpha\beta+\alpha^{-1}\beta^{-1})}=\frac{\Phi_8(\alpha)}{\Phi_4(\alpha\beta)\Phi_4(\alpha/\beta)},$$
$$F(\alpha,\beta)=\frac{\beta^2+\beta^{-2}}{(\alpha\beta^{-1}+\alpha^{-1}\beta)(\alpha\beta+\alpha^{-1}\beta^{-1})}=\frac{\Phi_8(\beta)}{\Phi_4(\alpha\beta)\Phi_4(\beta/\alpha)}.$$

We easily check that

$$E(\alpha,\beta)+F(\alpha,\beta)=1. \tag{17}$$

Lemma 18. *Suppose ℓ is odd and $n\geq 1$. Let $\zeta=\zeta_{\ell^n}$. Let i, j be integers satisfying i, j, $i+j$, $i-j\not\equiv 0 \pmod{\ell^n}$. Then $E(\zeta^i,\zeta^j)$, $F(\zeta^i,\zeta^j)\in\mathcal{O}(\Omega_{n,\ell}^+)^\times$, and satisfy the unit equation*

$$\varepsilon+\delta=1,\quad \varepsilon,\delta\in\mathcal{O}(\Omega_{n,\ell}^+)^\times. \tag{18}$$

Moreover,

$$\upsilon_\ell(E(\zeta^i,\zeta^j)-F(\zeta^i,\zeta^j))=\frac{\ell^{\mathrm{ord}_\ell(i+j)}+\ell^{\mathrm{ord}_\ell(i-j)}}{\ell^{n-1}(\ell-1)}. \tag{19}$$

Proof. It is clear that $E(\zeta^i,\zeta^j)$, $F(\zeta^i,\zeta^j)$ are fixed by complex conjugation $\zeta\mapsto\zeta^{-1}$ and so belong to $\Omega_{n,\ell}^+$. By Lemma 13, $E(\zeta^i,\zeta^j)$ and $F(\zeta^i,\zeta^j)$ are units. It remains to check (19). We observe

$$E(\zeta^i,\zeta^j)-F(\zeta^i,\zeta^j)=\frac{(\zeta^{i-j}-\zeta^{j-i})(\zeta^{i+j}-\zeta^{-i-j})}{(\zeta^{i-j}+\zeta^{j-i})(\zeta^{i+j}+\zeta^{-i-j})}=\frac{(\zeta^{2(i-j)}-1)(\zeta^{2(i+j)}-1)}{\Phi_4(\zeta^{i-j})\Phi_4(\zeta^{i+j})}.$$

The denominator is a unit by Lemma 13. Now (19) follows from Lemma 8. □

Proof of Theorem 3. We deduce this from Lemma 18. Let us take for example $i=2$ and $j=1$. Let $n\geq 2$ and let

$$\varepsilon_n=E(\zeta_{\ell^n}^2,\zeta_{\ell^n}),\qquad \delta_n=F(\zeta_{\ell^n}^2,\zeta_{\ell^n}).$$

By Lemma 18, ε_n, $\delta_n\in\mathcal{O}(\Omega_{\infty,\ell}^+)^\times$ and satisfy $\varepsilon_n+\delta_n=1$. Thus $\varepsilon_n\in(\mathbb{P}^1-\{0,1,\infty\})(\mathcal{O}(\Omega_{\infty,\ell}^+))$. Moreover,

$$\upsilon_\ell(2\varepsilon_n-1)=\upsilon_\ell(\varepsilon_n-\delta_n)=\begin{cases}2/(\ell^{n-1}(\ell-1)), & \ell>3,\\ 2/3^{n-1}, & \ell=3,\end{cases}$$

by (19). Thus $\varepsilon_n\neq\varepsilon_m$ whenever $n\neq m$. Hence $(\mathbb{P}^1-\{0,1,\infty\})(\mathcal{O}(\Omega_{\infty,\ell}^+))$ is infinite. □

Remark. Theorem 3 applies only for ℓ odd; for $\ell = 2$ it is easy to show that the statement is false. Indeed, let η_n be the prime ideal of $\mathcal{O}(\Omega^+_{n,2})$ above 2. Then $\mathcal{O}(\Omega^+_{n,2})/\eta_n \cong \mathbb{F}_2$, and a solution to $\varepsilon + \delta = 1$ with ε, $\delta \in \mathcal{O}(\Omega^+_{n,2})^\times$ reduced modulo η_n gives $1 + 1 \equiv 1 \pmod 2$ which is impossible.

Proof of Theorem 1 for $\ell = 3$. We recall that $\mathbb{Q}_{\infty,3} = \Omega^+_{\infty,3}$. Therefore Theorem 1 for $\ell = 3$ follows immediately from Theorem 3. □

5. The *S*-unit equation over $\mathbb{Q}_{\infty,5}$

The purpose of the is section is to prove Theorems 1 and 2 for $\ell = 5$. These in fact follow immediately from the following lemma.

Lemma 19. *Let υ_5 be the unique prime of $\mathbb{Q}_{\infty,5}$ above 5, and write $S = \{\upsilon_5\}$. Then*:

(i) $(\mathbb{P}^1 - \{0, k, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty,5}, S))$ *is infinite for* $k = 1, 4$.

(ii) $(\mathbb{P}^1 - \{0, 2, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty,5}))$ *is infinite.*

Proof. Let $a \in \mathbb{Z}_5^\times$ be the element satisfying

$$a^2 = -1, \quad a \equiv 2 \pmod 5;$$

such an element exists and is unique by Hensel's lemma. Let $\sigma : \Omega_{\infty,5} \to \Omega_{\infty,5}$ be the field automorphism satisfying

$$\sigma(\zeta_{5^n}) = \zeta_{5^n}^a$$

for $n \geq 1$. Note that σ is an automorphism of order 4, and fixes a subfield of $\Omega_{\infty,5}$ of index 4. This subfield is precisely $\mathbb{Q}_{\infty,5}$.

Let

$$F = (x_1x_2^2 + x_3x_4^2)(x_1^2x_4 + x_2x_3^2),$$
$$G = (x_1^2x_2 + x_3^2x_4)(x_1x_4^2 + x_2^2x_3),$$
$$H = (x_1 - x_3)(x_2 - x_4)(x_1x_2 - x_3x_4)(x_1x_4 - x_2x_3).$$

Observe F, G, H are invariant under the 4-cycle (x_1, x_2, x_3, x_4). One can check that $F - G = H$. Let $n \geq 2$ and write $\zeta = \zeta_{5^n}$. Let

$$\varepsilon_n = \frac{F(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}{H(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}, \quad \delta_n = -\frac{G(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}{H(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3})}.$$

From the identity $F - G = H$ we have $\varepsilon_n + \delta_n = 1$. We shall show that $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times$.

Since σ cyclically permutes $\zeta, \zeta^a, \zeta^{-1}, \zeta^{-a}$ we conclude that $f(\zeta, \zeta^a, \zeta^{-1}, \zeta^{-a}) \in \mathbb{Q}_{\infty,5}$ for $f = F$, G, H. Thus $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5}$. Moreover,

$$F = x_2x_3^3x_4^2 \cdot \Phi_2(x_1x_2^2/x_3x_4^2)\Phi_2(x_1^2x_4/x_2x_3^2),$$
$$G = x_2^2x_3^3x_4 \cdot \Phi_2(x_1^2x_2/x_3^2x_4)\Phi_2(x_1x_4^2/x_2^2x_3),$$
$$H = x_2x_3^3x_4^2 \cdot \Phi_1(x_1/x_3) \cdot \Phi_1(x_2/x_4) \cdot \Phi_1(x_1x_2/x_3x_4) \cdot \Phi_1(x_1x_4/x_2x_3).$$

Hence

$$\varepsilon_n = \frac{\Phi_2(\zeta^{2+4a})\Phi_2(\zeta^{4-2a})}{\Phi_1(\zeta^2)\Phi_1(\zeta^{2a})\Phi_1(\zeta^{2+2a})\Phi_1(\zeta^{2-2a})}$$
$$= \frac{(1-\zeta^{4+8a})(1-\zeta^{8-4a})}{(1-\zeta^2)(1-\zeta^{2a})(1-\zeta^{2+2a})(1-\zeta^{2-2a})(1-\zeta^{2+4a})(1-\zeta^{4-2a})}.$$

and

$$\delta_n = \frac{-\zeta^{2a}\Phi_2(\zeta^{4+2a})\Phi_2(\zeta^{2-4a})}{\Phi_1(\zeta^2)\Phi_1(\zeta^{2a})\Phi_1(\zeta^{2+2a})\Phi_1(\zeta^{2-2a})}$$
$$= \frac{-\zeta^{2a}(1-\zeta^{8+4a})(1-\zeta^{4-8a})}{(1-\zeta^2)(1-\zeta^{2a})(1-\zeta^{2+2a})(1-\zeta^{2-2a})(1-\zeta^{4+2a})(1-\zeta^{2-4a})}.$$

We checked, using the fact that $a \equiv 7 \pmod{25}$, that the exponents of ζ in the above expressions for ε_n and δ_n all have 5-adic valuation 0 or 1. It follows from this that $\varepsilon_n, \delta_n \in V_n \subseteq \mathcal{O}(\Omega_n, S)^\times$ for $n \geq 2$. Hence $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5} \cap \mathcal{O}(\Omega_n, S)^\times = \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times$ for $n \geq 2$. To complete the proof of the lemma for $k = 1$ it is enough to show that $\varepsilon_n \neq \varepsilon_m$ for $n > m$, and for this it is enough to show that $\varepsilon_n \notin \langle \pm\zeta_{5^n}, V_{n-1}\rangle$ for $n \geq 2$. Since $a \equiv 7 \pmod{25}$ we see that

$$4+8a \equiv 10, \quad 8-4a \equiv 5, \quad 2+4a \equiv 5, \quad 4-2a \equiv 15 \pmod{25}.$$

Thus the factors

$$1-\zeta^{4+8a}, \quad 1-\zeta^{8-4a}, \quad 1-\zeta^{2+4a}, \quad 1-\zeta^{4-2a}$$

all belong to V_{n-1}. Hence it is enough to show that

$$(1-\zeta^2)(1-\zeta^{2a})(1-\zeta^{2+2a})(1-\zeta^{2-2a}) \tag{20}$$

does not belong to $\langle \pm\zeta_{5^n}, V_{n-1}\rangle$. However, the exponents 2, $2a$, $2+2a$, $2-2a$ are respectively 2, 4, 1, 3 modulo 5, and hence certainly distinct modulo 5^{n-1}. It follows from Lemma 10 that the product (20) does not belong to $\langle \pm\zeta_{5^n}, V_{n-1}\rangle$ completing the proof for $k = 1$.

The proof for $k = 2$ is similar, and is based on the identity $F - G = 2H$, where

$$F = (x_1^2 + x_1x_3 + x_3^2)(x_2^2 + x_2x_4 + x_4^2) = x_3^2x_4^2 \cdot \Phi_3(x_1/x_3) \cdot \Phi_3(x_2/x_4),$$
$$G = (x_1^2 - x_1x_3 + x_3^2)(x_2^2 - x_2x_4 + x_4^2) = x_3^2x_4^2 \cdot \Phi_6(x_1/x_3) \cdot \Phi_6(x_2/x_4),$$
$$H = (x_1x_4 + x_2x_3)(x_1x_2 + x_3x_4) = x_2x_3^2x_4 \cdot \Phi_2(x_1x_4/x_2x_3) \cdot \Phi_2(x_1x_2/x_3x_4),$$

and likewise the proof for $k = 4$ is based on the identity $F - G = 4H$, where

$$F = (x_1 + x_3)^2(x_2 + x_4)^2 = x_3^2x_4^2 \cdot \Phi_2(x_1/x_3)^2\Phi_2(x_2/x_4)^2,$$
$$G = (x_1 - x_3)^2(x_2 - x_4)^2 = x_3^2x_4^2 \cdot \Phi_1(x_1/x_3)^2\Phi_1(x_2/x_4)^2,$$
$$H = (x_1x_2 + x_3x_4)(x_1x_4 + x_2x_3) = x_2x_3^2x_4 \cdot \Phi_2(x_1x_2/x_3x_4)\Phi_2(x_1x_4/x_2x_3).$$ □

Remark. It is appropriate to remark on how the identities in the above proof were found. Write

$$\Psi_m(X, Y) = Y^{\varphi(m)}\Phi_m(X/Y)$$

for the homogenization of the m-th cyclotomic polynomial. Now consider

$$f(x_1, x_2, x_3, x_4) = \Psi_m(u, v),$$

where u, v are monomials in variables x_1, x_2, x_3, x_4. Let ℓ be a prime. We see that evaluating any such f at $(\zeta^\alpha, \zeta^\beta, \zeta^\gamma, \zeta^\delta)$ gives an element of V_n (provided that it does not vanish). We considered products of such f of total degree up to 20 and picked out ones that are invariant under the 4-cycle (x_1, x_2, x_3, x_4), and searched for ternary relations between them. This yielded the identities used in the above proof.

Proof of Theorems 1 and 2 for $\ell = 5$. Theorems 1 and 2 for $\ell = 5$ follow immediately from Lemma 19. □

6. The S-unit equation over $\mathbb{Q}_{\infty,7}$

Lemma 20. *Let υ_7 be the unique prime of $\mathbb{Q}_{\infty,7}$ above 7, and write $S = \{\upsilon_7\}$. Then*

$$(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}(\mathbb{Q}_{\infty,7}, S))$$

is infinite.

Proof. In view of the proof of Lemma 19, it would be natural to seek polynomials F, G, H in variables $x_1, \dots, x_6$ satisfying the following properties:

- $F \pm G = H$.
- F, G, H are invariant under the 6-cycle $(x_1, x_2, \dots, x_6)$.
- Each is a product of polynomials

  $$f(x_1, x_2, \dots, x_6) = \Psi_m(u, v),$$

  with u, v monomials in $x_1, \dots, x_6$.

Unfortunately, an extensive search has failed to produce any such triple of polynomials. We therefore need to proceed a little differently.

Let $a \in \mathbb{Z}_7$ be the element satisfying

$$a^2 + a + 1 = 0, \quad a \equiv 2 \pmod 7;$$

such an element exists and is unique by Hensel's lemma. Let $\sigma, c : \Omega_{\infty,7} \to \Omega_{\infty,7}$ be the field automorphisms satisfying

$$\sigma(\zeta_{7^n}) = \zeta_{7^n}^a, \quad c(\zeta_{7^n}) = \zeta_{7^n}^{-1}$$

for $n \geq 1$. Then $\mathbb{Q}_{\infty,7}$ is the field fixed by the subgroup of $\mathrm{Gal}(\Omega_{\infty,7}/\mathbb{Q})$ generated by σ and c. We work with polynomials in variables x_1, x_2, x_3. Let

$$F = (x_1x_2^2 + x_3^3)(x_2x_3^2 + x_1^3)(x_3x_1^2 + x_2^3),$$
$$G = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_1x_2 - x_3^2)(x_2x_3 - x_1^2)(x_3x_1 - x_2^2),$$
$$H = (x_1^2x_2 + x_3^3)(x_2^2x_3 + x_1^3)(x_3^2x_1 + x_2^3).$$

These satisfy the identity $F - G = H$. Moreover, they are invariant under the 3-cycle (x_1, x_2, x_3) and all the factors are of the form $\Psi_m(u, v)$ where $m = 1$ or 2, and where u, v are suitable monomials in x_1, x_2, x_3. Evaluating any of F, G, H at $(\zeta, \zeta^a, \zeta^{a^2})$ yields an S-unit belonging to $\Omega_{n,7}^{\langle\sigma\rangle}$. Now we let

$$F' = \frac{F(x_1^2, x_2^2, x_3^2)}{x_1^6 x_2^6 x_3^6}, \quad G' = \frac{G(x_1^2, x_2^2, x_3^2)}{x_1^6 x_2^6 x_3^6}, \quad H' = \frac{H(x_1^2, x_2^2, x_3^2)}{x_1^6 x_2^6 x_3^6}.$$

Observe that the rational functions F', G', H' satisfy $F' - G' = H'$ and are moreover invariant under the 3-cycle (x_1, x_2, x_3). Moreover, F', G', H' evaluated at $(\zeta, \zeta^a, \zeta^{a^2})$ yield S-units belonging to $\Omega_{n,7}^{\langle\sigma\rangle}$. We need to check that these in fact belong to $\mathbb{Q}_{n-1,7} = \Omega_{n,7}^{\langle\sigma,c\rangle}$ and so we need to check that these expressions are invariant under c. This follows immediately on observing that F', G', H' may be rewritten as

$$\begin{aligned} F' &= \left(\frac{x_1 x_2^2}{x_3^3} + \frac{x_3^3}{x_1 x_2^2}\right)\left(\frac{x_2 x_3^2}{x_1^3} + \frac{x_1^3}{x_2 x_3^2}\right)\left(\frac{x_3 x_1^2}{x_2^3} + \frac{x_2^3}{x_3 x_1^2}\right), \\ G' &= \left(\frac{x_1}{x_2} - \frac{x_2}{x_1}\right)\left(\frac{x_2}{x_3} - \frac{x_3}{x_2}\right)\left(\frac{x_3}{x_1} - \frac{x_1}{x_3}\right)\left(\frac{x_1 x_2}{x_3^2} - \frac{x_3^2}{x_1 x_2}\right)\left(\frac{x_2 x_3}{x_1^2} - \frac{x_1^2}{x_2 x_3}\right)\left(\frac{x_3 x_1}{x_2^2} - \frac{x_2^2}{x_3 x_1}\right), \\ H' &= \left(\frac{x_1^2 x_2}{x_3^3} + \frac{x_3^3}{x_1^2 x_2}\right)\left(\frac{x_2^2 x_3}{x_1^3} + \frac{x_1^3}{x_2^2 x_3}\right)\left(\frac{x_3^2 x_1}{x_2^3} + \frac{x_2^3}{x_3^2 x_1}\right). \end{aligned}$$

Thus F', G', H' evaluated at $(\zeta, \zeta^a, \zeta^{a^2})$ yield elements of $\mathcal{O}(\mathbb{Q}_{\infty,7}, S)^\times$. We write

$$\varepsilon_n = \frac{F'(\zeta, \zeta^a, \zeta^{a^2})}{H'(\zeta, \zeta^a, \zeta^{a^2})}, \quad \delta_n = -\frac{G'(\zeta, \zeta^a, \zeta^{a^2})}{H'(\zeta, \zeta^a, \zeta^{a^2})}.$$

Then ε_n, δ_n belong to $\mathcal{O}(\mathbb{Q}_{\infty,7}, S)^\times$ and satisfy $\varepsilon_n + \delta_n = 1$. In fact it is straightforward to check that $\varepsilon_n \notin \langle \pm\zeta_{7^n}, V_{n-1}\rangle$, from which it follows that $\varepsilon_n \neq \varepsilon_m$ for $n > m$. The details are similar to those of the proof of Lemma 19 and we omit them. □

7. Isogeny classes of elliptic curves over $\mathbb{Q}_{\infty,\ell}$

The purpose of this section is to prove Theorem 5. Since isogenous elliptic curves share the same set of bad primes, the corresponding theorem over number fields is an immediate consequence of Shafarevich's theorem. However, as we intend to show in the following section, Shafarevich's theorem does not generalize to elliptic curves over $\mathbb{Q}_{\infty,\ell}$. We shall instead rely on a theorem of Kato to control $\mathbb{Q}_{\infty,\ell}$-points on certain modular Jacobians.

Our first lemma shows that there are only finitely many primes that can divide the degree of a cyclic isogeny of E.

Lemma 21. *Let ℓ be a prime and let $E/\mathbb{Q}_{\infty,\ell}$ be an elliptic curve without potential complex multiplication. Then there is a constant B, depending on E, such that for primes $p \geq B$, the elliptic curve E has no p-isogenies defined over $\mathbb{Q}_{\infty,\ell}$.*

Proof. Let n be the least positive integer such that E admits a model defined over $\mathbb{Q}_{n,\ell}$. By a famous theorem of Serre [1972], there is a constant B, depending on E, such that for $p \geq B$ the mod p

representation

$$\bar{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{n,\ell}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is surjective. We may suppose that $B \geq 5$. Thus, for $p \geq B$, the Galois group $\mathrm{Gal}(\mathbb{Q}_{n,\ell}(E[p])/\mathbb{Q}_{n,\ell})$ is isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$ which is nonsolvable. We will show that E has no p-isogeny defined over $\mathbb{Q}_{\infty,\ell}$. Suppose otherwise. Then such an isogeny is in fact defined over $\mathbb{Q}_{m,\ell}$ for some $m \geq n$. It follows that the extension $\mathbb{Q}_{m,\ell}(E[p])/\mathbb{Q}_{m,\ell}$ has Galois group isomorphic to a subgroup of a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, with is solvable. As the extension $\mathbb{Q}_{m,\ell}/\mathbb{Q}_{n,\ell}$ is cyclic, we conclude that $\mathbb{Q}_{m,\ell}(E[p])/\mathbb{Q}_{n,\ell}$ is solvable. However, this contains the nonsolvable subextension $\mathbb{Q}_{n,\ell}(E[p])/\mathbb{Q}_{n,\ell}$, giving a contradiction. □

We shall make use of the following theorem of Kato [2004, Theorem 14.4] building on work of Rohrlich [1984].

Theorem 22 (Kato). *Let ℓ be a prime. Let A be an abelian variety defined over $\mathbb{Q}$ and admitting a surjective map $J_1(N) \to A$ for some $N \geq 1$. Then $A(\mathbb{Q}_{\infty,\ell})$ is finitely generated.*

Lemma 23. *Let p, ℓ be primes. Let E be an elliptic curve defined over $\mathbb{Q}_{\infty,\ell}$ without potential complex multiplication. Then, for m sufficiently large, E has no p^m-isogenies defined over $\mathbb{Q}_{\infty,\ell}$.*

Proof. Let r be the least positive integer such that the modular curve $X = X_0(p^r)$ has genus at least 2, and write $J = J_0(p^r)$ for the corresponding modular Jacobian. It follows from Kato's theorem that $J(\mathbb{Q}_{\infty,\ell})$ is finitely generated, and therefore that $J(\mathbb{Q}_{\infty,\ell}) = J(\mathbb{Q}_{n,\ell})$ for some $n \geq 1$. Consider the Abel–Jacobi map

$$X \hookrightarrow J, \quad P \mapsto [P - \infty]$$

where $\infty \in X(\mathbb{Q})$ denotes the infinity cusp. It follows from this embedding that $X(\mathbb{Q}_{\infty,\ell}) = X(\mathbb{Q}_{n,\ell})$. By Faltings' theorem, this set is finite.

Let $k = \#X(\mathbb{Q}_{\infty,\ell})$ and let $s = kr$. To prove the lemma we in fact show that E has no cyclic isogenies of degree p^s defined over $\mathbb{Q}_{\infty,\ell}$. Suppose otherwise, and let $\psi : E \to E'$ be a cyclic isogeny of degree p^s defined over $\mathbb{Q}_{\infty,\ell}$. Then, we may factor ψ into a sequence of cyclic isogenies defined over $\mathbb{Q}_{\infty,\ell}$

$$E = E_0 \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} E_2 \cdots \xrightarrow{\psi_k} E_k = E',$$

where ψ_i is of degree p^r. Note that E_i and E_j are nonisomorphic over $\overline{\mathbb{Q}}$ for $i \neq j$; indeed they are related by a cyclic isogeny and E does not have potential complex multiplication. Thus the elliptic curves $E_0, E_1, \ldots, E_k$ support distinct $\mathbb{Q}_{\infty,\ell}$-points on $X = X_0(p^r)$. This contradicts the fact that $\#X(\mathbb{Q}_{\infty,\ell}) = k$. □

Remark. A famous theorem of Serre [1968, Section 2.1] asserts that the p-adic Tate module of a non-CM elliptic curve defined over a number field is irreducible. It is in fact possible to deduce Lemma 23 from Serre's theorem for $\ell \neq p$, but we have been unable to do this for $\ell = p$.

Proof of Theorem 5. Let E' belong to the $\mathbb{Q}_{\infty,\ell}$-isogeny class of E. Let $\psi : E \to E'$ be an isogeny defined over $\mathbb{Q}_{\infty,\ell}$. This has kernel of the form $\mathbb{Z}/a \times \mathbb{Z}/ab$ where a, b are positive integers, and so it can be factored into a composition

$$E \to E/E[a] \cong E \to E',$$

where the final morphism is cyclic of degree b. Thus to prove the proposition, it is enough to show that E has finitely many cyclic isogenies defined over $\mathbb{Q}_{\infty,\ell}$. The degree of any such isogeny is divisible by primes $p < B$ where B is as in Lemma 21. Also, for any $p < B$, we know the exponent of p in the degree of a cyclic isogeny $E \to E'$ is bounded by Lemma 23. Thus there are finitely many cyclic isogenies of E defined over $\mathbb{Q}_{\infty,\ell}$. □

8. From S-unit equations to elliptic curves

The aim of this section is to prove Theorem 4. We start by recalling a few facts about Legendre elliptic curves; see Proposition III.1.7 of [Silverman 1986] and its proof. Let K be a field of characteristic $\neq 2$ and let $\lambda \in (\mathbb{P}^1 - \{0, 1, \infty\})(K)$. Associated to λ is the Legendre elliptic curve

$$E_\lambda : Y^2 = X(X-1)(X-\lambda).$$

This model respectively has discriminant and j-invariant

$$\Delta = 16\lambda^2(1-\lambda)^2, \quad j = \frac{64(\lambda^2-\lambda+1)^3}{\lambda^2(1-\lambda)^2}. \tag{21}$$

Moreover, for $\lambda, \mu \in (\mathbb{P}^1 - \{0, 1, \infty\})(K)$, the Legendre elliptic curves E_λ and E_μ are isomorphic over K (or over $\overline{K}$) if and only if

$$\mu \in \left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}\right\}.$$

Now let K be a number field and S a finite set of nonarchimedean places. We let S' be the set of nonarchimedean places which are either in S or above 2. We let $\lambda \in (\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}(K, S))$. Then λ, $1-\lambda \in \mathcal{O}(K, S)^\times$. It follows from the expression for the discriminant that E_λ has good reduction away from S'.

Proof of Theorem 4. Let $\ell = 2, 3, 5$ or 7. Let S be given by (1) and let $S' = S \cup \{\upsilon_2\}$ as in the statement of Theorem 4. In proving Theorem 1 we constructed, for each positive integer n, elements ε_n, $\delta_n = 1-\varepsilon_n$, belonging $\mathbb{Q}_{\infty,\ell} \cap V_n \subseteq \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$, and moreover verified, for $n \geq 2$, that $\varepsilon_n \notin \langle \zeta_{\ell^n}, V_{n-1}\rangle$. We let

$$E_n : Y^2 = X(X-1)(X-\varepsilon_n).$$

Then E_n is defined over $\mathbb{Q}_{\infty,\ell}$ and has good reduction away from S'. We claim, for $n > m$, that E_n and E_m are not isomorphic, even over $\overline{\mathbb{Q}}$. To see this, suppose E_n and E_m are isomorphic. Then ε_n equals one of $\varepsilon_m^{\pm 1}$, $\delta_m^{\pm 1}$, $(-\varepsilon_m\delta_m)^{\pm 1}$. This gives a contradiction as all of these belong to $\langle \pm\zeta_{\ell^n}, V_{n-1}\rangle$. This proves the claim.

It remains to show that the E_n form infinitely many isogeny classes over $\mathbb{Q}_{\infty,\ell}$. However, this immediately follows from Theorem 5 and the following lemma. □

Lemma 24. *For n sufficiently large, E_n does not have potential complex multiplication.*

Proof. Suppose E_n has potential complex multiplication by an order R in an imaginary quadratic field K. Write $j = j(E_n)$. We claim that $\mathbb{Q}(j)/\mathbb{Q}$ is a cyclic Galois extension of order ℓ^n for some n. Note that $\mathbb{Q}(j)$ is a subextension of $\mathbb{Q}_{\infty,\ell}$ of finite degree, and is thus contained in $\mathbb{Q}_{m,\ell}$ for some m. Hence $\mathbb{Q}(j)$ is the fixed field of some subgroup H (say) of $G = \mathrm{Gal}(\mathbb{Q}_{m,\ell}/\mathbb{Q})$. As G is cyclic, the group H is a normal subgroup, and therefore $\mathbb{Q}(j)/\mathbb{Q}$ is a Galois extension. Moreover, $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \cong G/H$ which is cyclic of order ℓ^n for some n, proving our claim.

By standard CM theory [Shimura 1971, Theorem 5.7], we know that $\mathrm{Gal}(K(j)/K) \cong \mathrm{Pic}(R)$ and $[\mathbb{Q}(j) : \mathbb{Q}] = [K(j) : K]$. Since in our case $\mathbb{Q}(j)/\mathbb{Q}$ is Galois, $\mathrm{Gal}(\mathbb{Q}(j)/\mathbb{Q}) \cong \mathrm{Gal}(K(j)/K) \cong \mathrm{Pic}(R)$. However, $\mathbb{Q}(j) \subset \mathbb{Q}_{\infty,\ell}$ is totally real. It follows [Shimura 1971, page 124] that $\mathrm{Pic}(R)$ is an elementary abelian 2-group. However $\mathbb{Q}(j)/\mathbb{Q}$ is cyclic of order ℓ^n. Thus, $j \in \mathbb{Q}$ if $\ell \neq 2$, and $j \in \mathbb{Q}_{1,2} = \mathbb{Q}(\sqrt{2})$ if $\ell = 2$. However, from the expression for j in (21) we know that $[\mathbb{Q}(\varepsilon_n) : \mathbb{Q}(j)] \leq 6$. Thus ε_n belongs to a subfield of $\mathbb{Q}_{\infty,\ell}$ of degree at most 12. The lemma follows since, by Siegel's theorem, the S-unit equation has only finitely many solutions in any number field. □

9. Hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ with few bad primes

Let ℓ be an odd prime. Let $g \geq 2$ be an integer satisfying

$$\begin{cases} g \equiv (\ell-3)/4 \text{ or } -1 \pmod{(\ell-1)/2} & \text{if } \ell \equiv 3 \pmod 4, \\ g \equiv -1 \pmod{(\ell-1)/4} & \text{if } \ell \equiv 1 \pmod 4. \end{cases} \tag{22}$$

Then there is a positive integer k such that

$$k \cdot \left(\frac{\ell-1}{2}\right) = \begin{cases} 2g+1 \text{ or } 2g+2 & \text{if } \ell \equiv 3 \pmod 4, \\ 2g+2 & \text{if } \ell \equiv 1 \pmod 4. \end{cases} \tag{23}$$

Let $n \geq 2$ be a positive integer satisfying

$$\ell^{n-1} \geq k. \tag{24}$$

In this section we construct a hyperelliptic D_n curve of genus g defined over $\mathbb{Q}_{n-1,\ell}$ with good reduction away from the primes above 2, ℓ.

Write

$$\mathcal{Z}_n = \{\zeta \in \Omega_{n,\ell} : \zeta^{\ell^n} = 1, \zeta^{\ell^i} \neq 1 \text{ if } i < n\}$$

for the set of primitive ℓ^n-th roots of 1. Write

$$\mathcal{Z}_n^+ = \{\zeta + \zeta^{-1} : \zeta \in \mathcal{Z}_n\} \subset \Omega_{n,\ell}^+.$$

We note that any element of $\mathcal{Z}_n^+$ generates $\Omega_{n,\ell}^+$.

Lemma 25. $$\#\mathcal{Z}_n^+ = \tfrac{1}{2}\ell^{n-1}(\ell-1).$$

Proof. We note that $\#\mathcal{Z}_n = \varphi(\ell^n) = \ell^{n-1}(\ell-1)$. Suppose $\alpha, \beta \in \mathcal{Z}_n$. Then

$$(\alpha+\alpha^{-1}) - (\beta+\beta^{-1}) = \alpha^{-1}\cdot(1-\alpha\beta)\cdot(1-\alpha\beta^{-1}). \tag{25}$$

Thus $\alpha+\alpha^{-1} = \beta+\beta^{-1}$ if and only if $\alpha=\beta$ or $\alpha=\beta^{-1}$. The lemma follows. □

Write

$$G_n = \mathrm{Gal}(\Omega_{n,\ell}^{+}/\mathbb{Q}_{n-1,\ell}), \quad H_n = \mathrm{Gal}(\Omega_{n,\ell}^{+}/\Omega_{n-1,\ell}^{+}).$$

We note that these are both cyclic subgroups of $\mathrm{Gal}(\Omega_{n,\ell}^{+}/\mathbb{Q})$ having orders

$$\#G_n = (\ell-1)/2, \quad \#H_n = \ell.$$

Lemma 26. *Fix $\zeta \in \mathcal{Z}_n$. Let*

$$\eta_i = \zeta^{1+\ell^{n-1}(i-1)} + \zeta^{-1-\ell^{n-1}(i-1)}, \quad 1 \le i \le \ell. \tag{26}$$

Then $\eta_1, \dots, \eta_\ell \in \mathcal{Z}_n^{+}$ form a single orbit under the action of H_n, but have pairwise disjoint orbits under the action of G_n.

Proof. Let $\kappa \in \mathrm{Gal}(\Omega_{n,\ell}/\mathbb{Q})$ be given by $\kappa(\zeta) = \zeta^{1+\ell^{n-1}}$. We note that κ has order ℓ and fixes $\Omega_{n-1,\ell}$. We denote the restriction of κ to $\Omega_{n,\ell}^{+}$ by τ; this is a cyclic generator of H_n. Note that

$$\eta_i = \tau^{i-1}(\zeta+\zeta^{-1}), \quad 1 \le i \le \ell.$$

Let $\sigma_1, \sigma_2 \in G_n$. Let $1 \le i < j \le \ell$ and suppose $\sigma_1(\eta_i) = \sigma_2(\eta_j)$. Thus $\sigma_1\tau^{i-1}(\eta_1) = \sigma_2\tau^{j-1}(\eta_1)$, so $\tau^{1-j}\sigma_2^{-1}\sigma_1\tau^{i-1}$ fixes η_1. As η_1 generates $\Omega_{n,\ell}^{+}$, we have $\tau^{1-j}\sigma_2^{-1}\sigma_1\tau^{i-1} = 1$ is the identity element in $\mathrm{Gal}(\Omega_{n,\ell}^{+}/\mathbb{Q})$. However, $\mathrm{Gal}(\Omega_{n,\ell}^{+}/\mathbb{Q})$ is abelian, so

$$\tau^{i-j} = \sigma_1^{-1}\sigma_2 \in G_n \cap H_n = \{1\}.$$

Since $1 \le i \le j \le \ell$ and τ has order ℓ we have $i = j$. □

The Galois group G_n acts faithfully on $\mathcal{Z}_n^{+}$. This action has ℓ^{n-1} orbits. Assumption (24) ensures that the number of orbits is at least k. If $k > \ell$, then we *extend* the list $\eta_1, \dots, \eta_\ell \in \mathcal{Z}_n^{+}$ to $\eta_1, \dots, \eta_k \in \mathcal{Z}_n^{+}$, so that the η_i continue to have disjoint orbits under the action of G_n; if $\ell = 3$ the choice of η_4 will be important later, and we choose $\eta_4 = \zeta^2 + \zeta^{-2}$. Consider the curve

$$D_n : Y^2 = \prod_{j=1}^{k} \prod_{\sigma \in G_n} (X - \eta_j^{\sigma}). \tag{27}$$

Lemma 27. *The curve D_n is hyperelliptic of genus g, is defined over $\mathbb{Q}_{n-1,\ell}$, and has good reduction away from the primes above 2 and ℓ.*

Proof. Our assumption on the orbits ensures that the polynomial on the right hand-side of (27) is separable. By (23), the degree of the polynomial is either $2g+1$ or $2g+2$. Thus D_n is a hyperelliptic curve of genus g. A priori, D_n is defined over $\Omega_{n,\ell}^{+}$. However, the roots of the hyperelliptic polynomial are permuted by the action of $G_n = \mathrm{Gal}(\Omega^+_{n,\ell}/\mathbb{Q}_{n-1,\ell})$ and so the polynomial belongs to $\mathbb{Q}_{n-1,\ell}[X]$. Hence D_n is defined over $\mathbb{Q}_{n-1,\ell}$.

Let $u_1, \dots, u_d$ be the roots of the hyperelliptic polynomial. Then the discriminant of hyperelliptic polynomial is

$$\prod_{1\le i<j\le d} (u_i - u_j)^2.$$

However, u_i, u_j are distinct elements of $\mathcal{Z}_n^+$. Thus there are $\alpha, \beta \in \mathcal{Z}_n$ with $\alpha \ne \beta, \beta^{-1}$ such that $u_i = \alpha + \alpha^{-1}$, $u_j = \beta + \beta^{-1}$. From the identity (25),

$$u_i - u_j = \alpha^{-1}(1 - \alpha\beta^{-1})(1 - \alpha\beta).$$

Since $\alpha\beta$ and $\alpha\beta^{-1}$ are nontrivial ℓ-power roots of 1, we see that $u_i - u_j$ is a $\{\upsilon_\ell\}$-unit, and hence the discriminant of the hyperelliptic polynomial of D_n is a $\{\upsilon_\ell\}$-unit. □

Given four pairwise distinct elements z_1, z_2, z_3, z_4 of a field K, we shall employ the notation $(z_1, z_2; z_3, z_4)$ to denote the *cross ratio*

$$(z_1, z_2; z_3, z_4) = \frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)}.$$

We extend the cross ratio to four distinct elements z_1, z_2, z_3, z_4 of $\mathbb{P}^1(K)$ in the usual way. We let $\mathrm{GL}_2(K)$ act on $\mathbb{P}^1(K)$ via fractional linear transformations

$$\gamma(z) = \frac{az+b}{cz+d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

It is well-known and easy to check that these fractional linear transformations leave the cross ratio unchanged:

$$(\gamma(z_1), \gamma(z_2); \gamma(z_3), \gamma(z_4)) = (z_1, z_2; z_3, z_4).$$

Lemma 28. *Let $\overline{K}$ be an algebraically closed field of characteristic* 0. *Let*

$$D : Y^2 = \prod_{i=1}^{d} (X - a_i), \quad D' : Y^2 = \prod_{i=1}^{d} (X - b_i)$$

be genus-g curves defined over $\overline{K}$ where the polynomials on the right are separable. If D, D' are isomorphic then there is some permutation $\mu \in S_d$ such that for all quadruples of pairwise distinct indices $1 \le r, s, t, u \le d$

$$(a_r, a_s; a_t, a_u) = (b_{\mu(r)}, b_{\mu(s)}; b_{\mu(t)}, b_{\mu(u)}).$$

Proof. We shall make use of the following standard description (e.g., [Baker et al. 2005, Proposition 6.11]) of isomorphisms of hyperelliptic curves: every isomorphism $\pi : D \to D'$ is of the form

$$\pi(X, Y) = \left(\frac{aX+b}{cX+d}, \frac{eY}{(cX+d)^{g+1}} \right)$$

for some

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\overline{K}), \quad e \in \overline{K}^{\times}.$$

Observe that $\pi(a_i, 0)$ has Y-coordinate 0; thus

$$\{\gamma(a_1), \dots, \gamma(a_d)\} = \{b_1, \dots, b_d\}.$$

Hence there is a permutation $\mu \in S_d$ such that $\gamma(a_i) = b_{\mu(i)}$. The lemma follows from the invariance of the cross ratio under the action of $\mathrm{GL}_2(\overline{K})$. □

Lemma 29. *Let $\ell \geq 11$ be prime. Then there is some $a \in \mathbb{Z}_\ell^\times$ of order $\ell - 1$ such that*

$$1+a^2 \not\equiv 0, \pm(1-a^2), \ \pm(a+a^3), \ \pm(a-a^3), \pm(1+a^3), \ \pm(1-a^3), \ \pm(a+a^2), \ \pm(a-a^2) \pmod{\ell}. \quad (28)$$

Proof. Making use of the fact that a polynomial of degree n has at most n roots, we see that the number of $a \in \mathbb{F}_\ell$ that *do not satisfy* (28) is (very crudely) bounded by 37. An element $a \in \mathbb{Z}_\ell^\times$ of order $\ell - 1$ is the unique Hensel lift of an element $a \in \mathbb{F}_\ell^\times$ of order $\ell - 1$. There are precisely $\varphi(\ell - 1)$ elements of order $\ell - 1$ in $\mathbb{F}_\ell^\times$. A theorem of Shapiro [1943, page 23], asserts that $\varphi(n) > n^{\log 2/\log 3}$ for $n \geq 30$. We note that if $\ell \geq 317$ then $\varphi(\ell - 1) \geq 316^{\log 2/\log 3} \approx 37.8$, and so the lemma holds for $\ell \geq 317$. For the range $11 \leq \ell \leq 317$ we checked the lemma by brute force computer enumeration. □

Lemma 30. *Let $n > m$ be sufficiently large. Then D_n and D_m are nonisomorphic, even over $\overline{\mathbb{Q}}$.*

Proof. Note that all roots of the hyperelliptic polynomial for D_n in (27) belong to $\mathcal{Z}_n^+$. It follows from (25) that the cross ratio of any four of them belongs to V_n. Suppose D_n and D_m are isomorphic. Let u_1, u_2, u_3, u_4 be any distinct roots of the hyperelliptic polynomial for D_n given in (27). Then, by Lemma 28,

$$(u_1, u_2; u_3, u_4) \in V_m \subseteq V_{n-1}.$$

We shall obtain a contradiction through a careful choice of the four roots $u_1, \dots, u_4$.

We first suppose that $k \geq 2$ and $\ell \geq 5$. Let $\zeta = \zeta_{\ell^n}$ and $b = 1 + \ell^{n-1}$. Then, by Lemma 26, $\eta_1 = \zeta + \zeta^{-1}$ and $\eta_2 = \zeta^b + \zeta^{-b}$. Let $a \in \mathbb{Z}_\ell^\times$ have order $\ell - 1$. Let $\kappa \in \mathrm{Gal}(\Omega_{n,\ell}/\mathbb{Q}_{n-1,\ell})$ be given by $\kappa(\zeta) = \zeta^a$. Then κ is a cyclic generator for $\mathrm{Gal}(\Omega_{n,\ell}/\mathbb{Q}_{n-1,\ell})$. We shall denote the restriction of κ to $\Omega_{n,\ell}^+$ by μ. Then μ is a cyclic generator for $G_n = \mathrm{Gal}(\Omega_{n,\ell}^+/\mathbb{Q}_{n-1,\ell})$ having order $(\ell - 1)/2$. We shall take

$$u_1 = \eta_1 = \zeta + \zeta^{-1}, \quad u_2 = \mu(\eta_1) = \zeta^a + \zeta^{-a}, \quad u_3 = \eta_2 = \zeta^b + \zeta^{-b}, \quad u_4 = \mu(\eta_2) = \zeta^{ab} + \zeta^{-ab}.$$

We compute the cross ratio with the help of identity (25), finding

$$(u_1, u_2; u_3, u_4) = \frac{(1 - \zeta^{1+b})(1 - \zeta^{1-b})(1 - \zeta^{a+ab})(1 - \zeta^{a-ab})}{(1 - \zeta^{1+ab})(1 - \zeta^{1-ab})(1 - \zeta^{a+b})(1 - \zeta^{a-b})}.$$

As $b \equiv 1 \pmod{\ell}$, and clearly $a \not\equiv \pm 1 \pmod{\ell}$, it is easy to check that $1 + b$ is the only one out of the eight exponents of ζ above that is $\pm 2 \pmod{\ell}$. Therefore by Lemma 11, the cross ratio is not an element of $\langle \pm\zeta_{\ell^n}, V_{n-1} \rangle$ for n sufficiently large, giving a contradiction for the case $k \geq 2$ and $\ell \geq 5$.

Next we suppose that $k=1$. It follows from (23) that $\ell \geq 11$. We choose $a \in \mathbb{Z}_\ell^\times$ as in Lemma 29, and, as above, take μ to be the corresponding generator of G_n of order $(\ell-1)/2 \geq 5$. We take

$$u_i = \mu^{i-1}(\eta_1) = \zeta^{a^{i-1}} + \zeta^{-a^{i-1}}, \quad 1 \leq i \leq 4;$$

observe that these are four roots of the hyperelliptic polynomial of D_n given in (27). The assumption that $\ell \geq 11$ ensures that a has order ≥ 10 and so u_1, u_2, u_3, u_4 are indeed pairwise distinct. We compute the cross ratio with the help of identity (25), finding

$$(u_1, u_2; u_3, u_4) = \frac{(1-\zeta^{1+a^2})(1-\zeta^{1-a^2})(1-\zeta^{a+a^3})(1-\zeta^{a-a^3})}{(1-\zeta^{1+a^3})(1-\zeta^{1-a^3})(1-\zeta^{a+a^2})(1-\zeta^{a-a^2})}.$$

Using Lemma 10 and our choice of a given by Lemma 29 we conclude that this cross ratio does not belong to $\langle \pm\zeta_{\ell^n}, V_{n-1}\rangle$ for n sufficiently large. This gives a contradiction for the case $k=1$.

Finally, we consider $\ell=3$. It follows from (23) that $k \geq 5$. Recall our choices of η_1, η_2, η_3 in Lemma 26, and our choice of $\eta_4 = \zeta^2 + \zeta^{-2}$ in the particular case $\ell = 3$. We choose the four roots $u_i = \eta_i$ for $i = 1, \ldots, 4$, and obtain

$$(u_1, u_2; u_3, u_4) = \frac{(1-\zeta^{2+2\times 3^{n-1}})(1-\zeta^{-2\times 3^{n-1}})(1-\zeta^{3+3^{n-1}})(1-\zeta^{-1+3^{n-1}})}{(1-\zeta^3)(1-\zeta^{-1})(1-\zeta^2)(1-\zeta^{-3^{n-1}})}.$$

As before, with the help of Lemma 11, we easily verify that the cross ratio is not an element of $\langle \pm\zeta_{\ell^n}, V_{n-1}\rangle$ for n sufficiently large. This completes the proof. □

Proof of Theorem 6. If $\ell = 3$ or 5 then (22) does not impose any restriction on the genus. Therefore we obtain, as above, for every genus $g \geq 2$, infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of genus-g hyperelliptic curves, defined over $\mathbb{Q}_{\infty,\ell}$, with good reduction away from $\{\upsilon_2, \upsilon_\ell\}$.

It remains to deal with $\ell = 7$, 11 and 13. Here, (22) imposes the restriction

$$g \equiv \begin{cases} 1 \text{ or } 2 \bmod 3 & \text{if } \ell = 7, \\ 2 \text{ or } 4 \bmod 5 & \text{if } \ell = 11, \\ 2 \bmod 3 & \text{if } \ell = 13. \end{cases}$$

We very briefly sketch how to remove the restriction. Instead of D_n defined as in (27), we consider the more general

$$D_n : Y^2 = h(X) \cdot \prod_{j=1}^{k} \prod_{\sigma \in G_n} (X - \eta_j^\sigma)$$

where

- h is a monic divisor of $X(X-1)(X+1)$;
- k and h are chosen to obtain the desired genus;
- $\eta_j \in \mathcal{Z}_n^+$ are chosen as before.

These D_n are clearly defined over $\mathbb{Q}_{n-1,\ell}$. To check that they have good reduction away from $S' = \{\upsilon_2, \upsilon_\ell\}$, we need to verify that the difference of any two distinct roots u, v of the hyperelliptic polynomial belongs to $\mathcal{O}(\Omega_n, S')^\times$. The proof of Lemma 27 shows this if $u, v \in \mathcal{Z}_n^+$. For the remaining possible differences it is enough to note that

$$\alpha + \alpha^{-1} = \alpha^{-1}\Phi_4(\alpha), \quad \alpha + \alpha^{-1} + 1 = \alpha^{-1}\Phi_3(\alpha), \quad \alpha + \alpha^{-1} - 1 = \alpha^{-1}\Phi_6(\alpha),$$

which are all units by Lemma 13. We omit the remaining details. □

10. Isogeny classes of hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$

A beautiful theorem of Kummer asserts that the index of the cyclotomic units C_n in the full unit group $\mathcal{O}(\Omega_{n,\ell})^\times$ equals the class number h_n^+ of $\Omega_{n,\ell}^+$. In this section, with the help of Kummer's theorem, we prove for certain primes ℓ the existence of infinitely many isogeny classes of hyperelliptic Jacobians over $\mathbb{Q}_{\infty,\ell}$ with good reduction away from ℓ. We first prove a few elementary lemmas.

Lemma 31. *Let K be a field of characteristic not 2, and let $L = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_r})$, where $\alpha_i \in K^\times$. Then for any $x \in K$ such that $\sqrt{x} \in L$, we have*

$$x = \alpha_1^{e_1} \cdots \alpha_r^{e_r} q^2$$

for some integers $e_i \in \mathbb{Z}$ and $q \in K$.

Proof. Let M be a field of characteristic not 2, and let $d \in M$ be a nonsquare. Let $x \in M$ and suppose $\sqrt{x} \in M(\sqrt{d})$. Then $\sqrt{x} = y + z\sqrt{d}$ for some $y, z \in M$. Squaring, we deduce that $yz = 0$. Thus $x = y^2$ or $x = dz^2$.

We now prove the lemma by induction on r. The above establishes the case $r = 1$. Let $r \geq 2$, and let $x \in K$ satisfy $\sqrt{x} \in L$. Letting $M = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{r-1}})$ we see that $x \in M$ and $\sqrt{x} \in M(\sqrt{\alpha_r})$. Thus, by the above, $\sqrt{x} \in M$ or $\sqrt{x\alpha_r} \in M$. In other words,

$$\sqrt{x \cdot \alpha_r^e} \in M = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{r-1}})$$

for some $e \in \{0, 1\}$. By the inductive hypothesis, there are $e_1, \dots, e_{r-1} \in \mathbb{Z}$ and $q \in K$ such that

$$x \cdot \alpha_r^e = \alpha_1^{e_1} \cdots \alpha_{r-1}^{e_{r-1}} q^2.$$

The proof is complete on taking $e_r = -e$. □

Lemma 32. *Let ℓ be an odd prime. Let $q \in \Omega_{\infty,\ell}$ satisfy $q^2 \in V_n$. If the class number h_n^+ of $\Omega_{n,\ell}^+$ is odd, then $q \in V_n$.*

Proof. Let $q \in \Omega_{\infty,\ell}$ satisfy $q^2 \in V_n \subset \Omega_{n,\ell}$. As the extension $\Omega_{\infty,\ell}/\Omega_{n,\ell}$ is pro-ℓ, we conclude that $q \in \Omega_{n,\ell}$. However, $V_n \subseteq \mathcal{O}(\Omega_{n,\ell}, \{\upsilon_\ell\})^\times$, where, as usual, υ_ℓ denotes the prime above ℓ. Thus $q \in \mathcal{O}(\Omega_{n,\ell}, \{\upsilon_\ell\})^\times$. We claim that

$$[\mathcal{O}(\Omega_{n,\ell}, \{\upsilon_\ell\})^\times : V_n] = h_n^+.$$

The lemma follows immediately from the claim. To prove the claim, consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_n & \longrightarrow & V_n & \xrightarrow{\kappa} & \mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathcal{O}(\Omega_{n,\ell})^\times & \longrightarrow & \mathcal{O}(\Omega_{n,\ell},\{\upsilon_\ell\})^\times & \xrightarrow{\kappa} & \mathbb{Z} & \longrightarrow & 1 \end{array}$$

where $\kappa(\alpha) = \mathrm{ord}_{(1-\zeta)}(\alpha)$. By the snake lemma,

$$\mathcal{O}(\Omega_{n,\ell},\{\upsilon_\ell\})^\times / V_n \cong \mathcal{O}(\Omega_{n,\ell})^\times / C_n.$$

Write $C_n^+ = C_n \cap \Omega_{n,\ell}^+$. The aforementioned theorem of Kummer asserts that

$$[\mathcal{O}(\Omega_{n,\ell})^\times : C_n] = [\mathcal{O}(\Omega_{n,\ell}^+)^\times : C_n^+] = h_n^+;$$

see, for example, [Washington 1997, Exercise 8.5] for the first equality, and [loc. cit., Theorem 8.2] for the second. This proves the claim. □

Lemma 33. *Let K be a field of characteristic $\neq 2$. Let $f \in K[X]$ be a monic separable polynomial of odd degree $d \geq 5$. Write $f = \prod_{i=1}^d (X - \alpha_i)$ with $\alpha_i \in \overline{K}$. Let C/K be a hyperelliptic curve given by $Y^2 = f(X)$ with Jacobian J. Then*

$$K(J[2]) = K(\alpha_1, \ldots, \alpha_d), \qquad K(J[4]) = K(J[2])(\{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i,j \leq d}).$$

Proof. Write ∞ for the point at infinity on the given model for C. The expression given for $K(J[2])$ is well-known; it may be seen by observing (see, for example [Schaefer 1995]) that the classes of the classes of degree 0 divisors $[(\alpha_i, 0) - \infty]$ with $i = 1, \ldots, d$ generate $J[2]$.

Yelton [2015, Theorem 1.2.2] gives a high-powered proof of the given expression for $K(J[4])$. For the convenience of the reader we give a more elementary argument. Let $L = K(J[2])$. The theory of 2-descent on hyperelliptic Jacobians furnishes, for any field $M \supseteq L$, an injective homomorphism [Schaefer 1995; Stoll 2001]

$$J(M)/2J(M) \hookrightarrow \prod_{i=1}^{d} M^*/(M^*)^2$$

known as the $X - \Theta$-map. This in particular sends the 2-torsion point $[(\alpha_i, 0) - \infty]$ to

$$\left((\alpha_i - \alpha_1), \ldots, (\alpha_i - \alpha_{i-1}), \prod_{j \neq i} (\alpha_i - \alpha_j), (\alpha_i - \alpha_{i+1}), \ldots, (\alpha_i - \alpha_d)\right).$$

The field $K(J[4])$ is the smallest extension of M of L such that all the images of the 2-torsion generators $[(\alpha_i, 0) - \infty]$ are trivial in $\prod_{i=1}^d M^*/(M^*)^2$. This is plainly the extension

$$M = L(\{\sqrt{\alpha_i - \alpha_j}\}_{1 \leq i,j \leq d}).$$ □

Lemma 34. *Let p be a prime for which 2 is a primitive root (i.e., 2 is a generator for $\mathbb{F}_p^\times$). Let G be a cyclic group of order p, and let V be an $\mathbb{F}_2[G]$-module with $\dim_{\mathbb{F}_2}(V) = p-1$. Suppose that the action of G on $V - \{0\}$ is free. Then V is irreducible.*

Proof. Let W be a $\mathbb{F}_2[G]$-submodule of V, and write $d = \dim_{\mathbb{F}_2}(W)$. Since the action of G on $V - \{0\}$ is free, the set $W - \{0\}$ consists of G-orbits, all having size p. However, $\#(W - \{0\}) = 2^d - 1$, and so $p \mid (2^d - 1)$. By assumption, 2 is a primitive root modulo p, therefore $(p-1) \mid d$. Since W is an $\mathbb{F}_2$-subspace of V, which has dimension $p-1$, we see that $W = 0$ or $W = V$. □

Lemma 35. *Let $\ell = 2p+1$, where ℓ and p are odd primes. Suppose 2 is a primitive root modulo p. Let $g = (\ell-3)/4$. Let $n \geq 2$ and let $D_n/\mathbb{Q}_{n-1,\ell}$ be the hyperelliptic curve defined in Section 9. Let $A/\mathbb{Q}_{\infty,\ell}$ be an abelian variety and let $\phi : J(D_n) \to A$ be an isogeny defined over $\mathbb{Q}_{\infty,\ell}$. Then $\phi = 2^r \phi_{\mathrm{odd}}$ where $\phi_{\mathrm{odd}} : J(D_n) \to A$ is an isogeny of odd degree.*

We remark if ℓ and p are primes with $\ell = 2p+1$ then p is called a Sophie Germain prime, and ℓ is called as safe prime.

Proof of Lemma 35. Note that, in the notation of Section 9, $k = 1$, and the hyperelliptic polynomial for D_n has odd degree $2g+1 = (\ell-1)/2 = p$, and consists of a single orbit under action of $G_n = \mathrm{Gal}(\Omega_n^+/\mathbb{Q}_{n-1,\ell})$:

$$D_n : y^2 = \prod_{\sigma \in G_n} (X - \eta_1^\sigma), \qquad \eta_1 = \zeta_{\ell^n} + \zeta_{\ell^n}^{-1}.$$

In particular, the hyperelliptic polynomial is irreducible over $\mathbb{Q}_{\infty,\ell}$. It follows from this (e.g., [Stoll 2001, Lemma 4.3]) that $J(\mathbb{Q}_{\infty,\ell})[2] = 0$, where J denotes $J(D_n)$ for convenience. We note, by Lemma 33, that $\mathbb{Q}_{\infty,\ell}(J[2]) = \mathbb{Q}_{\infty,\ell}(\eta_1) = \Omega_{\infty,\ell}^+$. We consider the action of $G_\infty := \mathrm{Gal}(\Omega_{\infty,\ell}^+/\mathbb{Q}_{\infty,\ell})$ on $J[2]$. The group G_∞ is cyclic of order $(\ell-1)/2 = p$. Any element fixed by this action belongs to $J(\mathbb{Q}_{\infty,\ell})[2] = 0$. Thus G_∞ acts freely on $V - \{0\}$, where $V := J[2]$.

Now let $\phi : J \to A$ be an isogeny defined over $\mathbb{Q}_{\infty,\ell}$. Then $W := \ker(\phi) \cap J[2]$ is a subgroup of V stable under the action of G_∞, and therefore an $\mathbb{F}_2[G_\infty]$-submodule of the $\mathbb{F}_2[G_\infty]$-module V. Observe that $\dim_{\mathbb{F}_2}(V) = 2g = p-1$. By hypothesis, 2 is a primitive root modulo p. We apply Lemma 34 to deduce that $W = 0$ or $W = V$. Therefore, either ϕ already has odd degree, or $J[2] \subseteq \ker(\phi)$. In the latter case, observe that $\phi = 2\phi'$ where $\phi' : J \to A$ is an isogeny defined over $\mathbb{Q}_{\infty,\ell}$ of degree $\deg(\phi)/2^{2g}$. As ϕ has finite degree, by repeating the argument we eventually arrive at $\phi = 2^r \phi_{\mathrm{odd}}$. □

Lemma 36. *Let $\ell = 2p+1$, where ℓ and p are odd primes. Suppose 2 is a primitive root modulo p. Suppose that the class number h_n^+ of $\Omega_{n,\ell}^+$ is odd for all n. Let $g = (\ell-3)/4$. For $n \geq 2$ let $D_n/\mathbb{Q}_{n-1,\ell}$ be the genus-g hyperelliptic curve defined in Section 9. Let $n > m$ be sufficiently large. Then there are no isogenies $J(D_n) \to J(D_m)$ defined over $\mathbb{Q}_{\infty,\ell}$.*

The assumption that h_n^+ is odd for all n may seem at first sight very restrictive. However, it is conjectured [Buhler et al. 2004] that $h_{n+1}^+ = h_n^+$ for all but finitely many pairs (ℓ, n). Moreover, Washington [1978] has shown that $\mathrm{ord}_p(h_n)$ remains bounded as $n \to \infty$, for any fixed prime p.

Proof of Lemma 36. Write J_n for $J(D_n)$. Suppose there is an isogeny $\phi : J_n \to J_m$ defined over $\mathbb{Q}_{\infty,\ell}$. By Lemma 35 we may suppose that ϕ has odd degree, and so $\ker(\phi) \cap J_n[4] = 0$. Thus ϕ restricted to $J_n[4]$ induces an isomorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}_{\infty,\ell})$-modules $J_n[4] \cong J_m[4]$. In particular, $\mathbb{Q}_{\infty,\ell}(J_n[4]) = \mathbb{Q}_{\infty,\ell}(J_m[4])$. As in the proof of Lemma 35 we have $\mathbb{Q}_{\infty,\ell}(J_n[2]) = \mathbb{Q}_{\infty,\ell}(J_m[2]) = \Omega^+_{\infty,\ell}$. Thus, by Lemma 33, the equality $\mathbb{Q}_{\infty,\ell}(J_n[4]) = \mathbb{Q}_{\infty,\ell}(J_m[4])$ may be rewritten as

$$\Omega^+_{\infty,\ell}(\{\sqrt{\vartheta_{n,i} - \vartheta_{n,j}}\}_{1 \le i,j \le (\ell-1)/2}) = \Omega^+_{\infty,\ell}(\{\sqrt{\vartheta_{m,i} - \vartheta_{m,j}}\}_{1 \le i,j \le (\ell-1)/2}),$$

where $\vartheta_{r,i} := \mu_r^{i-1}(\zeta_{\ell^r} + \zeta_{\ell^r}^{-1})$ where μ_r is a cyclic generator of G_r. This, in particular, implies that

$$\sqrt{\vartheta_{n,2} - \vartheta_{n,1}} \in \Omega^+_{\infty,\ell}(\{\sqrt{\vartheta_{m,i} - \vartheta_{m,j}}\}_{1 \le i,j \le (\ell-1)/2}).$$

We apply Lemma 31 to obtain

$$\vartheta_{n,2} - \vartheta_{n,1} = \pm \prod_{1 \le i < j \le (\ell-1)/2} (\vartheta_{m,i} - \vartheta_{m,j})^{e_{i,j}} \cdot q^2$$

for some integers $e_{i,j} \in \mathbb{Z}$ and $q \in \Omega^+_{\infty,\ell}$. By Lemma 32, we have $q \in V_n$. The generator μ_n of G_n is given by $\mu_n(\zeta_{\ell^n} + \zeta_{\ell^n}^{-1}) = \zeta_{\ell^n}^a + \zeta_{\ell^n}^{-a}$ where $a \in \mathbb{Z}_\ell^\times$ has order $(\ell - 1)$. Note

$$\vartheta_{n,2} - \vartheta_{n,1} = \zeta_{\ell^n}^a + \zeta_{\ell^n}^{-a} - \zeta_{\ell^n} - \zeta_{\ell^n}^{-1} = \zeta_{\ell^n}^{-a}(1 - \zeta_{\ell^n}^{a+1})(1 - \zeta_{\ell^n}^{a-1}).$$

Thus,

$$(1 - \zeta_{\ell^n}^{a+1})(1 - \zeta_{\ell^n}^{a-1}) \in \langle \pm\zeta_{\ell^n}, V_m, V_n^2 \rangle.$$

However, $(a+1) \not\equiv \pm(a-1) \pmod{\ell}$. Now Corollary 12 gives a contradiction. □

Proof of Theorem 7. Let $\ell \ge 11$. Let

$$g = \left\lfloor \frac{\ell-3}{4} \right\rfloor = \begin{cases} (\ell-3)/4, & \ell \equiv 3 \pmod 4, \\ (\ell-5)/4, & \ell \equiv 1 \pmod 4. \end{cases}$$

Thus g satisfies (22). Let D_n be as in Section 9. By Lemma 27, the hyperelliptic curve $D_n/\mathbb{Q}_{n-1,\ell}$ has genus g, and good reduction away from $\{\upsilon_2, \upsilon_\ell\}$. Moreover, by Lemma 30, we have D_n and D_m are nonisomorphic, even over $\overline{\mathbb{Q}}$, for $n > m$ sufficiently large.

Now suppose

(i) $\ell = 2p + 1$ where p is also an odd prime;

(ii) 2 as a primitive root modulo p.

It then follows from Lemma 36 that $J(D_n)$ and $J(D_m)$ are nonisogenous over $\mathbb{Q}_{\infty,\ell}$ provided h_n^+ is odd for all n, where h_n^+ denotes the class number of $\Omega^+_{n,\ell}$. Write h_n for the class number of $\Omega_{n,\ell}$. It is known thanks to the work of Estes [1989] that h_1 is odd for all primes ℓ satisfying (i) and (ii); a simplified proof of this result is given Stevenhagen [1994, Corollary 2.3]. Moreover, Ichimura and Nakajima [2012] show, for primes $\ell \le 509$, that the ratio h_n/h_1 is odd for all n. The primes $11 \le \ell \le 509$ satisfying both (i) and (ii) are 11, 23, 59, 107, 167, 263, 347, 359. Thus for these primes h_n is odd for all n. As $h_n^+ \mid h_n$ (see for example [Washington 1997, Theorem 4.10]), we know for these primes that h_n^+ is odd for all n. This completes the proof. □

Remarks. • A key step in our proof of Theorem 7 is showing that $J(D_n)[2]$ is irreducible as an $\mathbb{F}_2[G_\infty]$-module whenever $\ell = 2p+1$ where p is a prime having 2 as a primitive root. It can be shown for all other ℓ that the $\mathbb{F}_2[G_\infty]$-module $J(D_n)[2]$ is in fact reducible.

• Another key step is the argument in the proof of Lemma 36 showing that for $n > m$ sufficiently large, the Jacobians $J(D_n)$ and $J(D_m)$ are not related via odd degree isogenies defined over $\mathbb{Q}_{\infty,\ell}$. This step can be made to work, with very minor modifications to the argument, for all $\ell \geq 11$, and all choices of genus g given in (22).

Acknowledgements

We are grateful to Minhyong Kim for drawing our attention to the conjecture of Parshin and Zarhin, and to Alain Kraus and David Loeffler for useful discussions. We thank the referee for many useful comments.

References

[Abramovich 2009] D. Abramovich, "Birational geometry for number theorists", pp. 335–373 in *Arithmetic geometry* (Göttingen, Germany, 2006), edited by H. Darmon et al., Clay Math. Proc. **8**, Amer. Math. Soc., Providence, RI, 2009. MR Zbl

[Baker et al. 2005] M. H. Baker, E. González-Jiménez, J. González, and B. Poonen, "Finiteness results for modular curves of genus at least 2", *Amer. J. Math.* **127**:6 (2005), 1325–1387. MR Zbl

[Buhler et al. 2004] J. Buhler, C. Pomerance, and L. Robertson, "Heuristics for class numbers of prime-power real cyclotomic fields", pp. 149–157 in *High primes and misdemeanours*, edited by A. van der Poorten and A. Stein, Fields Inst. Commun. **41**, Amer. Math. Soc., Providence, RI, 2004. MR Zbl

[Estes 1989] D. R. Estes, "On the parity of the class number of the field of qth roots of unity", *Rocky Mountain J. Math.* **19**:3 (1989), 675–682. MR Zbl

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR Zbl

[Freitas et al. 2020] N. Freitas, A. Kraus, and S. Siksek, "On asymptotic Fermat over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$", *Algebra Number Theory* **14**:9 (2020), 2571–2574. MR Zbl

[Freitas et al. 2021a] N. Freitas, A. Kraus, and S. Siksek, "Local criteria for the unit equation and the asymptotic Fermat's last theorem", *Proc. Natl. Acad. Sci. USA* **118**:12 (2021), art. id. 2026449118. MR Zbl

[Freitas et al. 2021b] N. Freitas, A. Kraus, and S. Siksek, "The unit equation over cyclic number fields of prime degree", *Algebra Number Theory* **15**:10 (2021), 2647–2653. MR Zbl

[Greenberg 2001] R. Greenberg, "Introduction to Iwasawa theory for elliptic curves", pp. 407–464 in *Arithmetic algebraic geometry* (Park City, UT, 1999), edited by B. Conrad and K. Rubin, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001. MR Zbl

[Ichimura and Nakajima 2012] H. Ichimura and S. Nakajima, "On the 2-part of the class numbers of cyclotomic fields of prime power conductors", *J. Math. Soc. Japan* **64**:1 (2012), 317–342. MR Zbl

[Kato 2004] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", pp. 117–290 in *Cohomologies p-adiques et applications arithmétiques, III*, edited by P. Berthelot et al., Astérisque **295**, Soc. Math. France, Paris, 2004. MR Zbl

[Kim 2005] M. Kim, "The motivic fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel", *Invent. Math.* **161**:3 (2005), 629–656. MR Zbl

[Lawrence and Venkatesh 2020] B. Lawrence and A. Venkatesh, "Diophantine problems and p-adic period mappings", *Invent. Math.* **221**:3 (2020), 893–999. MR Zbl

[Mazur 1972] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), 183–266. MR Zbl

[Nagell 1969] T. Nagell, "Sur un type particulier d'unités algébriques", *Ark. Mat.* **8** (1969), 163–184. MR Zbl

[Poonen 2021] B. Poonen, "The S-integral points on the projective line minus three points via finite covers and Skolem's method", pp. 583–587 in *Arithmetic geometry*, *number theory*, *and computation*, edited by J. S. Balakrishnan et al., Springer, 2021. MR Zbl

[Rohrlich 1984] D. E. Rohrlich, "On L-functions of elliptic curves and cyclotomic towers", *Invent. Math.* **75**:3 (1984), 409–423. MR Zbl

[Šafarevič 1963] I. R. Šafarevič, "Algebraic number fields", pp. 163–176 in *Proceedings of the International Congress of Mathematicians* (Stockholm, 1962), edited by V. Stenström, Mittag-Leffler, Djursholm, Sweden, 1963. In Russian; translated as pp. 25–39 in Amer. Math. Soc. Transl. (2) **31**, Amer. Math. Soc., Providence, RI, 1962. MR Zbl

[Schaefer 1995] E. F. Schaefer, "2-descent on the Jacobians of hyperelliptic curves", *J. Number Theory* **51**:2 (1995), 219–232. MR Zbl

[Serre 1968] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968. MR Zbl

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR Zbl

[Shapiro 1943] H. Shapiro, "An arithmetic function arising from the ϕ function", *Amer. Math. Monthly* **50** (1943), 18–30. MR Zbl

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Kanô Memorial Lect. **1**, Iwanami Shoten, Tokyo, 1971. MR Zbl

[Siksek 2022] S. Siksek, "Integral points on punctured abelian varieties", *Eur. J. Math.* **8**:suppl. 2 (2022), 687–703. MR Zbl

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. **106**, Springer, 1986. MR Zbl

[Stevenhagen 1994] P. Stevenhagen, "Class number parity for the pth cyclotomic field", *Math. Comp.* **63**:208 (1994), 773–784. MR Zbl

[Stoll 2001] M. Stoll, "Implementing 2-descent for Jacobians of hyperelliptic curves", *Acta Arith.* **98**:3 (2001), 245–277. MR Zbl

[Triantafillou 2021] N. Triantafillou, "There are no exceptional units in number fields of degree prime to 3 where 3 splits completely", *Proc. Amer. Math. Soc. Ser. B* **8** (2021), 371–376. MR

[Washington 1978] L. C. Washington, "The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension", *Invent. Math.* **49**:1 (1978), 87–97. MR Zbl

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Grad. Texts in Math. **83**, Springer, 1997. MR Zbl

[Yelton 2015] J. S. Yelton, *Hyperelliptic Jacobians and their associated l-adic Galois representations*, Ph.D. thesis, Pennsylvania State University, 2015, available at https://www.proquest.com/docview/1748051112.

[Zarhin 2010] Y. G. Zarhin, "Endomorphisms of abelian varieties, cyclotomic extensions, and Lie algebras", *Mat. Sb.* **201**:12 (2010), 93–102. In Russian; translated in *Sb. Math.* **201**:12 (2010), 1801–1810. MR Zbl

[Zarhin and Parshin 1989] Y. G. Zarhin and A. N. Parshin, "Finiteness problems in Diophantine geometry", pp. 35–102 in *Eight papers translated from the Russian*, edited by B. Silver, Amer. Math. Soc. Transl. (2) **143**, Amer. Math. Soc., Providence, RI, 1989. Zbl arXiv 0912.4325

Communicated by Akshay Venkatesh
Received 2023-02-05 Revised 2023-11-29 Accepted 2024-02-13

s.siksek@warwick.ac.uk *Mathematics Institute, University of Warwick, Coventry, United Kingdom*

robin.visser@warwick.ac.uk *Mathematics Institute, University of Warwick, Coventry, United Kingdom*

mathematical sciences publishers msp

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Antoine Chambert-Loir
Université Paris-Diderot
France

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Jason P. Bell	University of Waterloo, Canada
Bhargav Bhatt	University of Michigan, USA
Frank Calegari	University of Chicago, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Saclay, France
Brian D. Conrad	Stanford University, USA
Samit Dasgupta	Duke University, USA
Hélène Esnault	Freie Universität Berlin, Germany
Gavril Farkas	Humboldt Universität zu Berlin, Germany
Sergey Fomin	University of Michigan, USA
Edward Frenkel	University of California, Berkeley, USA
Wee Teck Gan	National University of Singapore
Andrew Granville	Université de Montréal, Canada
Ben J. Green	University of Oxford, UK
Christopher Hacon	University of Utah, USA
Roger Heath-Brown	Oxford University, UK
János Kollár	Princeton University, USA
Michael J. Larsen	Indiana University Bloomington, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne
Martin Olsson	University of California, Berkeley, USA
Irena Peeva	Cornell University, USA
Jonathan Pila	University of Oxford, UK
Anand Pillay	University of Notre Dame, USA
Bjorn Poonen	Massachusetts Institute of Technology, USA
Victor Reiner	University of Minnesota, USA
Peter Sarnak	Princeton University, USA
Michael Singer	North Carolina State University, USA
Vasudevan Srinivas	SUNY Buffalo, USA
Shunsuke Takagi	University of Tokyo, Japan
Pham Huu Tiep	Rutgers University, USA
Ravi Vakil	Stanford University, USA
Akshay Venkatesh	Institute for Advanced Study, USA
Melanie Matchett Wood	Harvard University, USA
Shou-Wu Zhang	Princeton University, USA

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2025 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 19 No. 1 2025