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

Samir Siksek, Robin Visser

Mathematics Institute, University of Warwick, Coventry, UK

s.siksek@warwick.ac.uk, robin.visser@warwick.ac.uk

WARWICK THE UNIVERSITY OF WARWICK

1) Introduction

Let ℓ be a rational prime and r a positive integer. We write $\mathbb{Q}_{r,\ell}$ for the unique degree ℓ^r totally real subfield of $\cup_{n=1}^{\infty}\mathbb{Q}(\mu_n)$, where μ_n denotes the set of ℓ^n-th roots of 1. We let $\mathbb{Q}_{\infty,\ell} = \cup_r \mathbb{Q}_{r,\ell}$; this is the **$\mathbb{Z}_\ell$-cyclotomic extension of $\mathbb{Q}$**. Furthermore, for any number field K, we write $K_{\infty,\ell} = K \cdot \mathbb{Q}_{\infty,\ell}$ (also denoted K_∞ for brevity).

The motivation for the present paper is a series of conjectures and theorems by Mazur, Parshin and Zarhin that suggest that the arithmetic of curves (respectively abelian varieties) over K_∞ is similar to the arithmetic of curves (respectively abelian varieties) over K.

- **Conjecture** (Mazur [1]). *Let A/K_∞ be an abelian variety. Then $A(K_\infty)$ is finitely generated.*
- **Conjecture** (Parshin and Zarhin [2, page 91]) *Let X/K_∞ be a curve of genus ≥ 2. Then $X(K_\infty)$ is finite.*
- **Theorem** (Zarhin [3, Corollary 4.2]) *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.

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. [4, 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. We show that the corresponding statement over $\mathbb{Q}_{\infty,\ell}$ is false, at least for $\ell = 2,\ 3,\ 5,\ 7$.

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

For a rational prime ℓ, we denote by υ_2 the inert prime of $\mathbb{Q}_{\infty,\ell}$ above 2, and υ_ℓ the totally ramified prime of $\mathbb{Q}_{\infty,\ell}$ above ℓ. Most of our constructions for counterexamples to Siegel and Shafarevich use properties of $\Phi_m(X)$; the **m-th cyclotomic polynomial** given by

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

At the heart of our constructions is the following lemma asserting that $\Phi_m(X)$ evaluated at ζ_{ℓ^n} is either a unit or $\{\upsilon_\ell\}$-unit of $\mathbb{Q}(\zeta_{\ell^n})$.

Lemma 1 *Let ℓ be a prime and $n \geq 1$. Let $m \geq 1$, and suppose $\ell^n \nmid m$.*
(a) $\Phi_m(\zeta_{\ell^n}) \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$, where $S = \{\upsilon_\ell\}$.
(b) If $m \neq \ell^u$ for all $u \geq 0$, then $\Phi_m(\zeta_{\ell^n}) \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}))^\times$.

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

Theorem 2 *Let $\ell = 2, 3, 5$ or 7. Let $S = \{\upsilon_\ell\}$ and write $\mathcal{O}_S$ for the S-integers of $\mathbb{Q}_{\infty,\ell}$. Let $k \in \{1,2,3,4,5,6,7,8,10,12,24\}$ if $\ell = 2,3$, or $k \in \{1,2,4\}$ if $\ell = 5$, or $k = 1$ if $\ell = 7$. Then $(\mathbb{P}^1 - \{0,k,\infty\})(\mathcal{O}_S)$ is infinite.*

Construction for $\ell = 2,3$. For each k given above, we found a ternary relation of the form $f_1 \cdots f_\alpha - g_1 \cdots g_\beta = kXh_1 \cdots h_\gamma$ where each f_i, g_i, h_i is a cyclotomic polynomial. The theorem follows by applying Lemma 1 to these relations. E.g. for $k = 10$, a short computer search found the following ternary relation:

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

Therefore, for each $n \geq 1$, by letting

$$\varepsilon_n = \frac{\Phi_2(\zeta_{\ell^n})^4\Phi_5(\zeta_{\ell^n})}{\zeta_{\ell^n}\Phi_4(\zeta_{\ell^n})^3}, \qquad \delta_n = \frac{-\Phi_1(\zeta_{\ell^n})^4\Phi_{10}(\zeta_{\ell^n})}{\zeta_{\ell^n}\Phi_4(\zeta_{\ell^n})^3}.$$

we have the S-unit equation $\varepsilon_n + \delta_n = 10$, noting that $\varepsilon_n, \delta_n \in \mathcal{O}_S$ by Lemma 1. It can also be shown using properties of cyclotomic units in $\mathbb{Q}(\zeta_{\ell^n})^+$ [5, Chapter 8] that $\varepsilon_n \neq \varepsilon_m$ for any $m < n$.

4) From S-unit equations to elliptic curves

Using the family of S-unit equations obtained from Theorem 2, we can prove that the Shafarevich conjecture for elliptic curves is false over $\mathbb{Q}_{\infty,\ell}$ for $\ell = 2,3,5,7$.

Theorem 3 *Let $\ell = 2,\ 3,\ 5$, or 7. Let $S = \{\upsilon_2, \upsilon_\ell\}$ where υ_2 and υ_ℓ are the unique primes of $\mathbb{Q}_{\infty,\ell}$ above 2 and ℓ respectively. 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 $\mathbb{Q}_{\infty,\ell}$.*

Construction. By Theorem 2, for each $n \geq 1$, we have constructed $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ such that $\varepsilon_n + \delta_n = 1$. We define the elliptic curve

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

This model for E_n has discriminant $\Delta = 16\varepsilon_n^2(1-\varepsilon_n)^2 = 16\varepsilon_n^2\delta_n^2$. Thus E_n is defined over $\mathbb{Q}_{\infty,\ell}$ and has good reduction away from $\{\upsilon_2, \upsilon_\ell\}$. As $\varepsilon_n \neq \varepsilon_m$ for $m < n$, this yields infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}_{\infty,\ell}$.

5) Hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$

Theorem 4 *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 $S = \{\upsilon_2, \upsilon_\ell\}$.*

Construction. For sufficiently large n, we define $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})^+/\mathbb{Q}_{n-1,\ell})$; this is a cyclic subgroup of order $(\ell-1)/2$. We define a set of real cyclotomic units $\eta_i \in \mathbb{Q}(\zeta_{\ell^n})^+$ given by

$$\eta_i \;=\; \zeta^{1+\ell^{n-1}(i-1)} + \zeta^{-1-\ell^{n-1}(i-1)}, \qquad 1 \leq i \leq \ell,$$

and therefore define the hyperelliptic curve D_n as

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

where $k \geq 1$ and h, a monic divisor of $X(X-1)(X+1)$, are chosen such that $\deg(h) + k(\ell-1)/2 \in \{2g+1, 2g+2\}$. The above model for D_n has discriminant $\prod_{i<j}(u_i - u_j)^2$ where $u_1, \ldots, u_d$ are the roots of the hyperelliptic polynomial in (1) Thus, to verify that D_n has good reduction away from $\{\upsilon_2, \upsilon_\ell\}$, we check that the difference of any two distinct roots u, v of the hyperelliptic polynomial belongs to $\mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$. This follows by noting the following identities,

$$\alpha + \alpha^{-1} - \beta - \beta^{-1} = \alpha^{-1}\Phi_1(\alpha/\beta)\Phi_1(\alpha\beta), \qquad \alpha + \alpha^{-1} = \alpha^{-1}\Phi_4(\alpha),$$
$$\alpha + \alpha^{-1} + 1 = \alpha^{-1}\Phi_3(\alpha), \qquad \alpha + \alpha^{-1} - 1 = \alpha^{-1}\Phi_6(\alpha),$$

and therefore, by Lemma 1, the discriminant of D_n is an element of $\mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$. A similar argument to the elliptic case proves that D_n is not $\overline{\mathbb{Q}}$-isomorphic to D_m for any $m < n$.

References and Acknowledgements

(1) B. Mazur, *Invent. Math.*, 1972, **18**, 183–266.

(2) Y. G. Zarhin and A. N. Parshin, *Finiteness Problems in Diophantine Geometry*, 2009.

(3) Y. G. Zarkhin, *Mat. Sb.*, 2010, **201**, 93–102.

(4) D. Abramovich, in *Arithmetic geometry*, Amer. Math. Soc., Providence, RI, 2009, vol. 8, pp. 335–373.

(5) L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, Second, 1997, vol. 83, pp. xiv+487.

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)