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

Journées Arithmétiques 2023

Robin Visser
(joint work with Samir Siksek)

Mathematics Institute
University of Warwick

7 July 2023

Motivation

- Let K be a number field and S a finite set of places of K.

Motivation

- Let K be a number field and S a finite set of places of K.

Theorem (Mordell 1922, Weil 1928)

For any abelian variety A/K, its K-rational points $A(K)$ are finitely generated.

Motivation

- Let K be a number field and S a finite set of places of K.

Theorem (Mordell 1922, Weil 1928)

For any abelian variety A/K, its K-rational points $A(K)$ are finitely generated.

Theorem (Siegel 1929, Mahler 1933)

Let $a, b \in K^\times$. There are only finitely many S-units x, y in K such that $ax + by = 1$.

Motivation

- Let K be a number field and S a finite set of places of K.

Theorem (Mordell 1922, Weil 1928)

For any abelian variety A/K, its K-rational points $A(K)$ are finitely generated.

Theorem (Siegel 1929, Mahler 1933)

Let $a, b \in K^\times$. There are only finitely many S-units x, y in K such that $ax + by = 1$.

Theorem (Faltings 1983; conjectured by Mordell 1922)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Motivation

- Let K be a number field and S a finite set of places of K.

Theorem (Mordell 1922, Weil 1928)

For any abelian variety A/K, its K-rational points $A(K)$ are finitely generated.

Theorem (Siegel 1929, Mahler 1933)

Let $a, b \in K^\times$. There are only finitely many S-units x, y in K such that $ax + by = 1$.

Theorem (Faltings 1983; conjectured by Mordell 1922)

Any smooth curve C/K of genus at least 2 has only finitely many K-rational points.

Theorem (Faltings 1983; conjectured by Shafarevich 1962)

Let $d \geq 1$ be a positive integer. Then there are only finitely many K-isomorphism classes of (p.p.) abelian varieties A/K of dimension d with good reduction outside S.

Motivation

- What if K is “bigger” than a number field?

Motivation

- What if K is "bigger" than a number field?

$\mathbb{Z}_\ell$-cyclotomic extension of K

Let K be a number field and ℓ a fixed prime. For each $n \geq 1$, let ζ_{ℓ^n} be a primitive ℓ^n-th root of unity and let $\mathbb{Q}_{n,\ell}$ be the unique cyclic degree ℓ^n totally real subfield of $\mathbb{Q}(\zeta_{\ell^{n+2}})$. Let $\mathbb{Q}_{\infty,\ell} = \cup_{n=1}^{\infty} \mathbb{Q}_{n,\ell}$. The $\mathbb{Z}_\ell$-**cyclotomic extension of** K is the field $K \cdot \mathbb{Q}_{\infty,\ell}$.

Motivation

- What if K is "bigger" than a number field?

$\mathbb{Z}_\ell$-cyclotomic extension of K

Let K be a number field and ℓ a fixed prime. For each $n \geq 1$, let ζ_{ℓ^n} be a primitive ℓ^n-th root of unity and let $\mathbb{Q}_{n,\ell}$ be the unique cyclic degree ℓ^n totally real subfield of $\mathbb{Q}(\zeta_{\ell^{n+2}})$. Let $\mathbb{Q}_{\infty,\ell} = \cup_{n=1}^{\infty} \mathbb{Q}_{n,\ell}$. The $\mathbb{Z}_\ell$-**cyclotomic extension of** K is the field $K \cdot \mathbb{Q}_{\infty,\ell}$.

- $\mathrm{Gal}(\mathbb{Q}_{n,\ell}/\mathbb{Q}) \cong \mathbb{Z}/\ell^n\mathbb{Z}$ and $\mathrm{Gal}(K_{\infty,\ell}/K) \cong \mathbb{Z}_\ell$.

Motivation

- What if K is "bigger" than a number field?

$\mathbb{Z}_\ell$-cyclotomic extension of K

Let K be a number field and ℓ a fixed prime. For each $n \geq 1$, let ζ_{ℓ^n} be a primitive ℓ^n-th root of unity and let $\mathbb{Q}_{n,\ell}$ be the unique cyclic degree ℓ^n totally real subfield of $\mathbb{Q}(\zeta_{\ell^{n+2}})$. Let $\mathbb{Q}_{\infty,\ell} = \cup_{n=1}^{\infty} \mathbb{Q}_{n,\ell}$. The **$\mathbb{Z}_\ell$-cyclotomic extension of K** is the field $K \cdot \mathbb{Q}_{\infty,\ell}$.

- $\mathrm{Gal}(\mathbb{Q}_{n,\ell}/\mathbb{Q}) \cong \mathbb{Z}/\ell^n\mathbb{Z}$ and $\mathrm{Gal}(K_{\infty,\ell}/K) \cong \mathbb{Z}_\ell$.
- If $\ell = 2$, then $\mathbb{Q}_{n,2} = \mathbb{Q}(\zeta_{2^{n+2}})^+ = \mathbb{Q}(\zeta_{2^{n+2}} + 1/\zeta_{2^{n+2}})$, so $\mathbb{Q}_{\infty,2} = \displaystyle\bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{2^n})^+$.

Motivation

- What if K is "bigger" than a number field?

$\mathbb{Z}_\ell$-cyclotomic extension of K

Let K be a number field and ℓ a fixed prime. For each $n \geq 1$, let ζ_{ℓ^n} be a primitive ℓ^n-th root of unity and let $\mathbb{Q}_{n,\ell}$ be the unique cyclic degree ℓ^n totally real subfield of $\mathbb{Q}(\zeta_{\ell^{n+2}})$. Let $\mathbb{Q}_{\infty,\ell} = \cup_{n=1}^{\infty} \mathbb{Q}_{n,\ell}$. The **$\mathbb{Z}_\ell$-cyclotomic extension of K** is the field $K \cdot \mathbb{Q}_{\infty,\ell}$.

- $\mathrm{Gal}(\mathbb{Q}_{n,\ell}/\mathbb{Q}) \cong \mathbb{Z}/\ell^n\mathbb{Z}$ and $\mathrm{Gal}(K_{\infty,\ell}/K) \cong \mathbb{Z}_\ell$.
- If $\ell = 2$, then $\mathbb{Q}_{n,2} = \mathbb{Q}(\zeta_{2^{n+2}})^+ = \mathbb{Q}(\zeta_{2^{n+2}} + 1/\zeta_{2^{n+2}})$, so $\mathbb{Q}_{\infty,2} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{2^n})^+$.
- If $\ell = 3$, then $\mathbb{Q}_{n,3} = \mathbb{Q}(\zeta_{3^{n+1}})^+ = \mathbb{Q}(\zeta_{3^{n+1}} + 1/\zeta_{3^{n+1}})$, so $\mathbb{Q}_{\infty,3} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{3^n})^+$.

Motivation

Conjecture (Mazur 1972)

Let $A/K_{\infty,\ell}$ be an abelian variety. Then $A(K_{\infty,\ell})$ is finitely generated.

Motivation

Conjecture (Mazur 1972)

Let $A/K_{\infty,\ell}$ be an abelian variety. Then $A(K_{\infty,\ell})$ is finitely generated.

Conjecture (Parshin–Zarhin 2009)

Let $X/K_{\infty,\ell}$ be a curve of genus ≥ 2. Then $X(K_{\infty,\ell})$ is finite.

Motivation

Conjecture (Mazur 1972)

Let $A/K_{\infty,\ell}$ be an abelian variety. Then $A(K_{\infty,\ell})$ is finitely generated.

Conjecture (Parshin–Zarhin 2009)

Let $X/K_{\infty,\ell}$ be a curve of genus ≥ 2. Then $X(K_{\infty,\ell})$ is finite.

Theorem (Zarhin 2010)

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

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

is a bijection.

Motivation

Conjecture (Mazur 1972)

Let $A/K_{\infty,\ell}$ be an abelian variety. Then $A(K_{\infty,\ell})$ is finitely generated.

Conjecture (Parshin–Zarhin 2009)

Let $X/K_{\infty,\ell}$ be a curve of genus ≥ 2. Then $X(K_{\infty,\ell})$ is finite.

Theorem (Zarhin 2010)

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

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

is a bijection.

- What about Siegel–Mahler's theorem or the Shafarevich conjecture over $K_{\infty,\ell}$?

Cyclotomic polynomials

Cyclotomic polynomial

Let $m \geq 1$ and let ζ_m be a primitive m-th root of unity. The ***m*-th cyclotomic polynomial** $\Phi_m(X) \in \mathbb{Z}[X]$ is

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

Cyclotomic polynomials

Cyclotomic polynomial

Let $m \geq 1$ and let ζ_m be a primitive m-th root of unity. The ***m*-th cyclotomic polynomial** $\Phi_m(X) \in \mathbb{Z}[X]$ is

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

Properties:

- $X^m - 1 = \prod_{d|m} \Phi_d(X)$ and $\Phi_m(X) = \prod_{d|m} (X^d - 1)^{\mu(m/d)}$.

Cyclotomic polynomials

Cyclotomic polynomial

Let $m \geq 1$ and let ζ_m be a primitive m-th root of unity. The ***m*-th cyclotomic polynomial** $\Phi_m(X) \in \mathbb{Z}[X]$ is

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

Properties:

- $X^m - 1 = \prod_{d|m} \Phi_d(X)$ and $\Phi_m(X) = \prod_{d|m} (X^d - 1)^{\mu(m/d)}$.
- For ℓ prime, $\Phi_{\ell^n}(X) = \sum_{i=0}^{\ell-1} X^{i\ell^{n-1}}$, thus $\Phi_{\ell^n}(1) = \ell$.

Cyclotomic polynomials

- Recall that $\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}$ is totally ramified above ℓ (and unramified above any $p \neq \ell$).
- Let v_ℓ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above ℓ.

Cyclotomic polynomials

- Recall that $\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}$ is totally ramified above ℓ (and unramified above any $p \neq \ell$).
- Let υ_ℓ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above ℓ.

Theorem

Let ℓ be a prime and $n \geq 1$. Let $m \geq 1$ and suppose $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit in $\mathbb{Q}(\zeta_{\ell^n})$.

Cyclotomic polynomials

- Recall that $\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}$ is totally ramified above ℓ (and unramified above any $p \neq \ell$).
- Let υ_ℓ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above ℓ.

Theorem

Let ℓ be a prime and $n \geq 1$. Let $m \geq 1$ and suppose $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit in $\mathbb{Q}(\zeta_{\ell^n})$.

Proof:

- Let $m = k\ell^t$ where $\ell \nmid k$. Note $\Phi_m(\zeta_{\ell^n})$ divides $\zeta_{\ell^n}^m - 1 = \zeta_{\ell^{n-t}}^k - 1$.

Cyclotomic polynomials

- Recall that $\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}$ is totally ramified above ℓ (and unramified above any $p \neq \ell$).
- Let υ_ℓ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above ℓ.

Theorem

Let ℓ be a prime and $n \geq 1$. Let $m \geq 1$ and suppose $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit in $\mathbb{Q}(\zeta_{\ell^n})$.

Proof:

- Let $m = k\ell^t$ where $\ell \nmid k$. Note $\Phi_m(\zeta_{\ell^n})$ divides $\zeta_{\ell^n}^m - 1 = \zeta_{\ell^{n-t}}^k - 1$.
- By definition, $\zeta_{\ell^{n-t}}^k - 1$ divides $\Phi_{\ell^{n-t}}(1) = \ell$, thus $\Phi_m(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit. $\square$

Cyclotomic polynomials

- Recall that $\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q}$ is totally ramified above ℓ (and unramified above any $p \neq \ell$).
- Let υ_ℓ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above ℓ.

Theorem

Let ℓ be a prime and $n \geq 1$. Let $m \geq 1$ and suppose $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit in $\mathbb{Q}(\zeta_{\ell^n})$.

Proof:

- Let $m = k\ell^t$ where $\ell \nmid k$. Note $\Phi_m(\zeta_{\ell^n})$ divides $\zeta_{\ell^n}^m - 1 = \zeta_{\ell^{n-t}}^k - 1$.
- By definition, $\zeta_{\ell^{n-t}}^k - 1$ divides $\Phi_{\ell^{n-t}}(1) = \ell$, thus $\Phi_m(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit. $\square$

Corollary

Let $F(X) := X^m \Phi_{m_1}(X)\Phi_{m_2}(X) \cdots \Phi_{m_k}(X)$ for some integers $m \geq 0$, $m_1, \ldots, m_k \geq 1$. Then $F(\zeta_{\ell^n})$ is a $\{\upsilon_\ell\}$-unit, for sufficiently large n.

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

- We can use cyclotomic polynomials to obtain infinitely many $\{v_\ell\}$-unit solutions to $\varepsilon + \delta = k$ for various integers k. A quick computer search yields the following relations:

$$\begin{aligned}
\Phi_2(X)^2 - \Phi_3(X) &= X, \\
\Phi_2(X)^2 - \Phi_4(X) &= 2X, \\
\Phi_2(X)^2 - \Phi_6(X) &= 3X, \\
\Phi_2(X)^2 - \Phi_1(X)^2 &= 4X, \\
\Phi_2(X)^4 - \Phi_{10}(X) &= 5X\Phi_3(X), \\
\Phi_2^2(X)\Phi_3(X) - \Phi_1(X)^2\Phi_6(X) &= 6X\Phi_4(X), \\
\Phi_7(X) - \Phi_1(X)^6 &= 7X\Phi_6(X)^2, \\
\Phi_2(X)^4 - \Phi_1(X)^4 &= 8X\Phi_4(X), \\
\Phi_2(X)^4\Phi_5(X) - \Phi_1(X)^4\Phi_{10}(X) &= 10X\Phi_4(X)^3.
\end{aligned}$$

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

Theorem (Siksek–V. 2023)

Let $\ell = 2$ or 3 and let $S = \{\upsilon_\ell\}$ be the unique prime above ℓ in $\mathbb{Q}_{\infty,\ell}$. Then, for each $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

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

Theorem (Siksek–V. 2023)

Let $\ell = 2$ or 3 and let $S = \{\upsilon_\ell\}$ be the unique prime above ℓ in $\mathbb{Q}_{\infty,\ell}$. Then, for each $k \in \{1,2,3,4,5,6,7,8,10\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

Proof for $k = 10$:

- For each $n \geq 1$, define $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$ as

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

  noting that $\varepsilon_n + \delta_n = 10$.

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

Theorem (Siksek–V. 2023)

Let $\ell = 2$ or 3 and let $S = \{\upsilon_\ell\}$ be the unique prime above ℓ in $\mathbb{Q}_{\infty,\ell}$. Then, for each $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

Proof for $k = 10$:

- For each $n \geq 1$, define $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$ as
$$\varepsilon_n = \frac{\Phi_2(\zeta_{\ell^n})^4 \Phi_5(\zeta_{\ell^n})}{\zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3}, \qquad \delta_n = \frac{-\Phi_1(\zeta_{\ell^n})^4 \Phi_{10}(\zeta_{\ell^n})}{\zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3}.$$
noting that $\varepsilon_n + \delta_n = 10$.
- As $\Phi_m(X) = X^{\varphi(m)} \Phi_m(X^{-1})$, this implies $\varepsilon_n^c = \varepsilon_n$ and $\delta_n^c = \delta_n$, thus $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,\ell}$.

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

Theorem (Siksek–V. 2023)

Let $\ell = 2$ or 3 and let $S = \{\upsilon_\ell\}$ be the unique prime above ℓ in $\mathbb{Q}_{\infty,\ell}$. Then, for each $k \in \{1, 2, 3, 4, 5, 6, 7, 8, 10\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

Proof for $k = 10$:

- For each $n \geq 1$, define $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$ as
$$\varepsilon_n = \frac{\Phi_2(\zeta_{\ell^n})^4 \Phi_5(\zeta_{\ell^n})}{\zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3}, \qquad \delta_n = \frac{-\Phi_1(\zeta_{\ell^n})^4 \Phi_{10}(\zeta_{\ell^n})}{\zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3}.$$
noting that $\varepsilon_n + \delta_n = 10$.
- As $\Phi_m(X) = X^{\varphi(m)} \Phi_m(X^{-1})$, this implies $\varepsilon_n^c = \varepsilon_n$ and $\delta_n^c = \delta_n$, thus $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,\ell}$.
- Using properties of cyclotomic units, one can show ε_n is not generated by $\{\pm\zeta_{\ell^{n-1}}, 1 - \zeta_{\ell^{n-1}}^k, 1 \leq k < \ell^{n-1}\}$, and thus $\varepsilon_m \neq \varepsilon_n$ for any $m < n$. $\square$

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

- For each $n \geq 1$, let $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5})$. This is a cyclic group of order 4, generated by some $\sigma \in G_n$ where $\sigma(\zeta_{5^n}) = \zeta_{5^n}^a$ for some integer a.

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

- For each $n \geq 1$, let $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5})$. This is a cyclic group of order 4, generated by some $\sigma \in G_n$ where $\sigma(\zeta_{5^n}) = \zeta_{5^n}^a$ for some integer a.
- We want to find cyclotomic relations in 4 variables x_1, x_2, x_3, x_4 which are invariant under the 4 cycle $(x_1, x_2, x_3, x_4) \mapsto (x_2, x_3, x_4, x_1)$.

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

- For each $n \geq 1$, let $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5})$. This is a cyclic group of order 4, generated by some $\sigma \in G_n$ where $\sigma(\zeta_{5^n}) = \zeta_{5^n}^a$ for some integer a.
- We want to find cyclotomic relations in 4 variables x_1, x_2, x_3, x_4 which are invariant under the 4 cycle $(x_1, x_2, x_3, x_4) \mapsto (x_2, x_3, x_4, x_1)$.
- Thus, evaluating these at $(\zeta_{5^n}, \zeta_{5^n}^a, \zeta_{5^n}^{-1}, \zeta_{5^n}^{-a})$ yields an $\{v_5\}$-unit in $\mathbb{Q}_{n-1,5}$.

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

- For each $n \geq 1$, let $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5})$. This is a cyclic group of order 4, generated by some $\sigma \in G_n$ where $\sigma(\zeta_{5^n}) = \zeta_{5^n}^a$ for some integer a.
- We want to find cyclotomic relations in 4 variables x_1, x_2, x_3, x_4 which are invariant under the 4 cycle $(x_1, x_2, x_3, x_4) \mapsto (x_2, x_3, x_4, x_1)$.
- Thus, evaluating these at $(\zeta_{5^n}, \zeta_{5^n}^a, \zeta_{5^n}^{-1}, \zeta_{5^n}^{-a})$ yields an $\{\upsilon_5\}$-unit in $\mathbb{Q}_{n-1,5}$.

$$x_4\Phi_2\left(\frac{x_1x_2^2}{x_3x_4^2}\right)\Phi_2\left(\frac{x_1^2x_4}{x_2x_3^2}\right) - x_2\Phi_2\left(\frac{x_1^2x_2}{x_3^2x_4}\right)\Phi_2\left(\frac{x_1x_4^2}{x_2^2x_3}\right) = x_4\Phi_1\left(\frac{x_1}{x_3}\right)\Phi_1\left(\frac{x_2}{x_4}\right)\Phi_1\left(\frac{x_1x_2}{x_3x_4}\right)\Phi_1\left(\frac{x_1x_4}{x_2x_3}\right),$$

$$x_4\Phi_3\left(\frac{x_1}{x_3}\right)\Phi_3\left(\frac{x_2}{x_4}\right) - x_4\Phi_6\left(\frac{x_1}{x_3}\right)\Phi_6\left(\frac{x_2}{x_4}\right) = 2\,x_2\Phi_2\left(\frac{x_1x_4}{x_2x_3}\right)\Phi_2\left(\frac{x_1x_2}{x_3x_4}\right),$$

$$x_4\Phi_2\left(\frac{x_1}{x_3}\right)^2\Phi_2\left(\frac{x_2}{x_4}\right)^2 - x_4\Phi_1\left(\frac{x_1}{x_3}\right)^2\Phi_1\left(\frac{x_2}{x_4}\right)^2 = 4\,x_2\Phi_2\left(\frac{x_1x_2}{x_3x_4}\right)\Phi_2\left(\frac{x_1x_4}{x_2x_3}\right).$$

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

Theorem (Siksek–V. 2023)

Let $\ell = 5$. Let $S = \{\upsilon_5\}$ be the unique prime above 5 in $\mathbb{Q}_{\infty,5}$. For each $k \in \{1, 2, 4\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

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

Theorem (Siksek–V. 2023)

Let $\ell = 5$. Let $S = \{\upsilon_5\}$ be the unique prime above 5 in $\mathbb{Q}_{\infty,5}$. For each $k \in \{1, 2, 4\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

Proof for $k = 4$:

- For each $n \geq 1$, define $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{5^n}), S)^\times$ as

$$\varepsilon_n = \frac{\zeta_{5^n}^{-a}\Phi_2(\zeta_{5^n}^2)^2\Phi_2(\zeta_{5^n}^{-1-a})^2}{\zeta_{5^n}^{a}\Phi_2(\zeta_{5^n}^{2+2a})\Phi_2(\zeta_{5^n}^{2-2a})}, \quad \delta_n = \frac{-\zeta_{5^n}^{-a}\Phi_1(\zeta_{5^n}^2)^2\Phi_1(\zeta_{5^n}^{-1-a})^2}{\zeta_{5^n}^{a}\Phi_2(\zeta_{5^n}^{2+2a})\Phi_2(\zeta_{5^n}^{2-2a})}$$

  where we've substituted $x_1 = \zeta_{5^n}$, $x_2 = \zeta_{5^n}^a$, $x_3 = \zeta_{5^n}^{-1}$ and $x_4 = \zeta_{5^n}^{-a}$ into the third cyclotomic relation shown previously. Therefore, $\varepsilon_n + \delta_n = 4$.

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

Theorem (Siksek–V. 2023)

Let $\ell = 5$. Let $S = \{\upsilon_5\}$ be the unique prime above 5 in $\mathbb{Q}_{\infty,5}$. For each $k \in \{1,2,4\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

Proof for $k = 4$:

- For each $n \geq 1$, define $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{5^n}), S)^\times$ as

$$\varepsilon_n = \frac{\zeta_{5^n}^{-a}\Phi_2(\zeta_{5^n}^2)^2\Phi_2(\zeta_{5^n}^{-1-a})^2}{\zeta_{5^n}^a\Phi_2(\zeta_{5^n}^{2+2a})\Phi_2(\zeta_{5^n}^{2-2a})}, \quad \delta_n = \frac{-\zeta_{5^n}^{-a}\Phi_1(\zeta_{5^n}^2)^2\Phi_1(\zeta_{5^n}^{-1-a})^2}{\zeta_{5^n}^a\Phi_2(\zeta_{5^n}^{2+2a})\Phi_2(\zeta_{5^n}^{2-2a})}$$

  where we've substituted $x_1 = \zeta_{5^n}$, $x_2 = \zeta_{5^n}^a$, $x_3 = \zeta_{5^n}^{-1}$ and $x_4 = \zeta_{5^n}^{-a}$ into the third cyclotomic relation shown previously. Therefore, $\varepsilon_n + \delta_n = 4$.
- As ε_n and δ_n fixed under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5})$, we have $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5}$.

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

Theorem (Siksek–V. 2023)

Let $\ell = 5$. Let $S = \{\upsilon_5\}$ be the unique prime above 5 in $\mathbb{Q}_{\infty,5}$. For each $k \in \{1, 2, 4\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ to the S-unit equation $\varepsilon + \delta = k$.

Proof for $k = 4$:

- For each $n \geq 1$, define $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{5^n}), S)^\times$ as

$$\varepsilon_n = \frac{\zeta_{5^n}^{-a}\Phi_2(\zeta_{5^n}^2)^2\Phi_2(\zeta_{5^n}^{-1-a})^2}{\zeta_{5^n}^{a}\Phi_2(\zeta_{5^n}^{2+2a})\Phi_2(\zeta_{5^n}^{2-2a})}, \quad \delta_n = \frac{-\zeta_{5^n}^{-a}\Phi_1(\zeta_{5^n}^2)^2\Phi_1(\zeta_{5^n}^{-1-a})^2}{\zeta_{5^n}^{a}\Phi_2(\zeta_{5^n}^{2+2a})\Phi_2(\zeta_{5^n}^{2-2a})}$$

  where we've substituted $x_1 = \zeta_{5^n}$, $x_2 = \zeta_{5^n}^a$, $x_3 = \zeta_{5^n}^{-1}$ and $x_4 = \zeta_{5^n}^{-a}$ into the third cyclotomic relation shown previously. Therefore, $\varepsilon_n + \delta_n = 4$.
- As ε_n and δ_n fixed under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5})$, we have $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5}$.
- A similar argument to the $\ell = 2, 3$ case shows that $\varepsilon_m \neq \varepsilon_n$ for any $m > n$. $\square$

Elliptic curves over $\mathbb{Q}_{\infty,\ell}$

Theorem (Siksek–V. 2023)

Let $\ell = 2, 3, 5$ or 7. Let $S = \{\upsilon_2, \upsilon_\ell\}$. 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.

Elliptic curves over $\mathbb{Q}_{\infty,\ell}$

Theorem (Siksek–V. 2023)

Let $\ell = 2, 3, 5$ or 7. Let $S = \{\upsilon_2, \upsilon_\ell\}$. 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.

Proof:

- For each $n \geq 1$, we have S-units $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ such that $\varepsilon_n + \delta_n = 1$.

Elliptic curves over $\mathbb{Q}_{\infty,\ell}$

Theorem (Siksek–V. 2023)

Let $\ell = 2, 3, 5$ or 7. Let $S = \{\upsilon_2, \upsilon_\ell\}$. 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.

Proof:

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

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

Elliptic curves over $\mathbb{Q}_{\infty,\ell}$

Theorem (Siksek–V. 2023)

Let $\ell = 2, 3, 5$ or 7. Let $S = \{\upsilon_2, \upsilon_\ell\}$. 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.

Proof:

- For each $n \geq 1$, we have S-units $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ such that $\varepsilon_n + \delta_n = 1$.
- We define the elliptic curve
$$E_n : Y^2 = X(X-1)(X-\varepsilon_n).$$
- This model has discriminant $\Delta = 16\varepsilon_n^2(1-\varepsilon_n)^2 = 16\varepsilon_n^2\delta_n^2$, and thus has good reduction away from S.

Elliptic curves over $\mathbb{Q}_{\infty,\ell}$

Theorem (Siksek–V. 2023)

Let $\ell = 2, 3, 5$ or 7. Let $S = \{\upsilon_2, \upsilon_\ell\}$. 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.

Proof:

- For each $n \geq 1$, we have S-units $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,\ell}, S)^\times$ such that $\varepsilon_n + \delta_n = 1$.
- We define the elliptic curve
$$E_n : Y^2 = X(X-1)(X-\varepsilon_n).$$
- This model has discriminant $\Delta = 16\varepsilon_n^2(1-\varepsilon_n)^2 = 16\varepsilon_n^2\delta_n^2$, and thus has good reduction away from S.
- It's j-invariant is $256(\varepsilon_n^2 - \varepsilon_n + 1)^3/\varepsilon_n^2(1-\varepsilon_n)^2$, thus yielding infinitely many $\overline{\mathbb{Q}}$-isomorphism classes. $\square$

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

Theorem (Siksek–V. 2023)

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

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

Theorem (Siksek–V. 2023)

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

Proof (sketch):

- For $n \geq 1$, let $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})^+/\mathbb{Q}_{n-1,\ell})$; this is a cyclic subgroup of order $(\ell - 1)/2$.

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

Theorem (Siksek–V. 2023)

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

Proof (sketch):

- For $n \geq 1$, let $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})^+/\mathbb{Q}_{n-1,\ell})$; this is a cyclic subgroup of order $(\ell-1)/2$.
- Define the hyperelliptic curve

$$D_n : Y^2 = h(X) \cdot \prod_{j=1}^{k} \prod_{\sigma \in G_n} \left(X - \left(\zeta_{\ell^n}^{1+\ell^{n-1}(j-1)} + \zeta_{\ell^n}^{-1-\ell^{n-1}(j-1)} \right)^{\sigma} \right)$$

where we choose some integer $k \geq 1$ and polynomial $h(X)$ dividing $X(X-1)(X+1)$ such that $\deg(h) + k(\ell-1)/2 \in \{2g+1, 2g+2\}$.

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

Theorem (Siksek–V. 2023)

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

Proof (sketch):

- For $n \geq 1$, let $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})^+/\mathbb{Q}_{n-1,\ell})$; this is a cyclic subgroup of order $(\ell-1)/2$.
- Define the hyperelliptic curve

$$D_n : Y^2 = h(X) \cdot \prod_{j=1}^{k} \prod_{\sigma \in G_n} \left(X - \left(\zeta_{\ell^n}^{1+\ell^{n-1}(j-1)} + \zeta_{\ell^n}^{-1-\ell^{n-1}(j-1)}\right)^{\sigma} \right)$$

  where we choose some integer $k \geq 1$ and polynomial $h(X)$ dividing $X(X-1)(X+1)$ such that $\deg(h) + k(\ell-1)/2 \in \{2g+1, 2g+2\}$.
- Use the identities $\alpha + \alpha^{-1} - \beta - \beta^{-1} = \alpha^{-1}\Phi_1(\frac{\alpha}{\beta})\Phi_1(\alpha\beta)$, $\alpha + \alpha^{-1} = \alpha^{-1}\Phi_4(\alpha)$, $\alpha + \alpha^{-1} + 1 = \alpha^{-1}\Phi_3(\alpha)$, and $\alpha + \alpha^{-1} - 1 = \alpha^{-1}\Phi_6(\alpha)$ to prove D_n has good reduction away from S.

Summary

Conjectures/Theorems	K num field	$K = \mathbb{Q}_{\infty,\ell}$
Tate conjecture $\mathrm{Hom}_{G_K}(T_\ell(A), T_\ell(B)) \cong \mathrm{Hom}_K(A, B) \otimes \mathbb{Z}_\ell$	Yes	Yes
Mordell conjecture $\mathrm{genus}(C) \geq 2 \implies \#C(K) < \infty$	Yes	?
Mordell–Weil $(A(K)$ finitely generated$)$	Yes	?
Siegel–Mahler $\#\{x, y \in \mathcal{O}_{K,S}^\times : ax + by = 1\} < \infty$	Yes	No
Shafarevich (curves) $\#\{C/K : \mathrm{genus}(C) = g \geq 2, \text{good outside } S\} < \infty$	Yes	No
Shafarevich (abelian varieties) $\#\{A/K : \dim(C) = d, \text{good outside } S\} < \infty$	Yes	No

Merci!