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

Conference for Young Number Theorists in Bonn

Robin Visser
(joint work with Samir Siksek)
Mathematics Institute
University of Warwick

11 September 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?

\[ \mathbb{Z}_\ell \text{-cyclotomic extension of } K \]

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

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

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

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

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

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

• If $\ell = 2$, then $\mathbb{Q}_{n,2} = \mathbb{Q}(\zeta_{2^{n+2}})^+ = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})$, so $\mathbb{Q}_{\infty,2} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{2^n})^+$. 

Motivation

• What if \( K \) is “bigger” than a number field?

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

Let \( K \) be a number field and \( \ell \) a fixed prime. For each \( n \geq 1 \), let \( \zeta_{\ell^n} \) be a primitive \( \ell^n \)-th root of unity and let \( \mathbb{Q}_{n,\ell} \) be the unique cyclic degree \( \ell^n \) totally real subfield of \( \mathbb{Q}(\zeta_{\ell^{n+2}}) \).

Let \( \mathbb{Q}_{\infty,\ell} = \bigcup_{n=1}^{\infty} \mathbb{Q}_{n,\ell} \). The \( \mathbb{Z}_\ell \)-\textbf{cyclotomic extension of} \( K \) is the field \( K \cdot \mathbb{Q}_{\infty,\ell} \).

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

• If \( \ell = 2 \), then \( \mathbb{Q}_{n,2} = \mathbb{Q}(\zeta_{2^{n+2}})^+ = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}) \), so \( \mathbb{Q}_{\infty,2} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{2^n})^+ \).

• If \( \ell = 3 \), then \( \mathbb{Q}_{n,3} = \mathbb{Q}(\zeta_{3^{n+1}})^+ = \mathbb{Q}(\zeta_{3^{n+1}} + \zeta_{3^{n+1}}^{-1}) \), 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 $\geq 2$. 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 $\geq 2$. 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 $\ell$-adic Tate modules by $T_\ell(A)$, $T_\ell(B)$. Then the natural embedding

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

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 $\geq 2$. 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 $\ell$-adic Tate modules by $T_\ell(A)$, $T_\ell(B)$. Then the natural embedding

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

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 \( \zeta_m \) 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:

• \( X^m - 1 = \Phi_d(X) \Phi_m(X) \) and \( \Phi_m(X) = \Phi_{d}(X^{\phi(m)/\phi(d)}) \).

• For prime \( \ell \), \( \Phi_{\ell^k}(X) = \ell^{k-1}(X^{\ell^{k-1}} - 1) \), thus \( \Phi_{\ell}(1) = \ell - 1 \).
Cyclotomic polynomials

Cyclotomic polynomial

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

\[
\Phi_m(X) := \prod_{1 \leq i \leq m \atop (i,m)=1} (X - \zeta_m^i).
\]

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 $\zeta_m$ 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 $\ell$ 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 $\ell$ (and unramified above any $p \neq \ell$).
- Let $\nu_\ell$ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above $\ell$. 

Lemma

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

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

Corollary (the "cyclotomic $\{\nu_\ell\}$-unit generator")

Let $F(X) := \Phi_m^1(X)\Phi_m^2(X)\cdots\Phi_m^k(X)$ for some integers $m \geq 0, m^1, \ldots, m^k \geq 1$.

Then $F(\zeta_{\ell^n})$ is a $\{\nu_\ell\}$-unit, for sufficiently large $n$. 

Cyclotomic polynomials

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

**Lemma**

Let $\ell$ be a prime and $n, m \geq 1$ such that $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\nu_{\ell}\}$-unit in $\mathbb{Q}(\zeta_{\ell^n})$. 
Cyclotomic polynomials

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

Lemma

Let $\ell$ be a prime and $n, m \geq 1$ such that $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\nu_\ell\}$-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 $\ell$ (and unramified above any $p \neq \ell$).
• Let $\nu_\ell$ be the unique prime in $\mathbb{Q}(\zeta_{\ell^n})$ lying above $\ell$.

Lemma

Let $\ell$ be a prime and $n, m \geq 1$ such that $\ell^n \nmid m$. Then $\Phi_m(\zeta_{\ell^n})$ is a $\{\nu_\ell\}$-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 $\{\nu_\ell\}$-unit.  

Corollary (the "cyclotomic $\{\nu_\ell\}$-unit generator")

Let $F(X) := \Phi_{m_1}(X)\Phi_{m_2}(X)\cdots\Phi_{m_k}(X)$ for some integers $m \geq 0, m_1, \ldots, m_k \geq 1$.

Then $F(\zeta_{\ell^n})$ is a $\{\nu_\ell\}$-unit, for sufficiently large $n$.  

□
Cyclotomic polynomials

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

**Lemma**

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

**Proof:**

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

**Corollary (the “cyclotomic $\{\nu_\ell\}$-unit generator”)**

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 $\{\nu_\ell\}$-unit, for sufficiently large $n$. 
Problem (Siegel–Mahler for $\mathbb{Q}_\infty, \ell$)

For some fixed integer $k \in \mathbb{Z}$, can we find infinitely many $\{\nu_\ell\}$-units $\varepsilon, \delta \in \mathbb{Q}_\infty, \ell$ such that $\varepsilon + \delta = k$?
**S-unit equations**

**Problem (Siegel–Mahler for \( \mathbb{Q}_\infty, \ell \))**

For some fixed integer \( k \in \mathbb{Z} \), can we find infinitely many \( \{v_\ell\}\)-units \( \varepsilon, \delta \in \mathbb{Q}_\infty, \ell \) such that \( \varepsilon + \delta = k \)?

*Idea:* Use cyclotomic polynomials as a machine to generate infinitely many \( \{v_\ell\}\)-units!

\[ X^{a_0} \Phi^{a_1}(X) \Phi^{a_2}(X) \cdots \Phi^{a_r}(X) - X^{b_0} \Phi^{b_1}(X) \Phi^{b_2}(X) \cdots \Phi^{b_s}(X) = k X^{c_0} \Phi^{c_1}(X) \Phi^{c_2}(X) \cdots \Phi^{c_t}(X) \]

for some nonnegative integers \( a_i, b_i, c_i \geq 0 \).

Then, for each \( n \geq 1 \) we can define

\[ \varepsilon_n := X^{a_0} \Phi^{a_1}(\zeta_\ell^n) \Phi^{a_2}(\zeta_\ell^n) \cdots \Phi^{a_r}(\zeta_\ell^n) \]

\[ \delta_n := -X^{b_0} \Phi^{b_1}(\zeta_\ell^n) \Phi^{b_2}(\zeta_\ell^n) \cdots \Phi^{b_s}(\zeta_\ell^n) \]

where \( \varepsilon_n, \delta_n \) are \( \{v_\ell\}\)-units in \( \mathbb{Q}(\zeta_\ell^n) \) such that \( \varepsilon_n + \delta_n = k \) (for sufficiently large \( n \)).
Problem (Siegel–Mahler for $\mathbb{Q}_\infty, \ell$)

For some fixed integer $k \in \mathbb{Z}$, can we find infinitely many $\{\nu_\ell\}$-units $\varepsilon, \delta \in \mathbb{Q}_\infty, \ell$ such that $\varepsilon + \delta = k$?

Idea: Use cyclotomic polynomials as a machine to generate infinitely many $\{\nu_\ell\}$-units!

I.e. search for cyclotomic relations of the form

$$X^{a_0} \Phi_{a_1}(X) \Phi_{a_2}(X) \cdots \Phi_{a_r}(X) - X^{b_0} \Phi_{b_1}(X) \Phi_{b_2}(X) \cdots \Phi_{b_s}(X) = k X^{c_0} \Phi_{c_1}(X) \Phi_{c_2}(X) \cdots \Phi_{c_t}(X)$$

for some nonnegative integers $a_i, b_i, c_i \geq 0$. 
**S-unit equations**

### Problem (Siegel–Mahler for $\mathbb{Q}_{\infty,\ell}$)

For some fixed integer $k \in \mathbb{Z}$, can we find infinitely many $\{\nu_\ell\}$-units $\varepsilon, \delta \in \mathbb{Q}_{\infty,\ell}$ such that $\varepsilon + \delta = k$?

#### Idea:
Use cyclotomic polynomials as a machine to generate infinitely many $\{\nu_\ell\}$-units!
I.e. search for cyclotomic relations of the form

$$X^{a_0}\Phi_{a_1}(X)\Phi_{a_2}(X)\cdots\Phi_{a_r}(X) - X^{b_0}\Phi_{b_1}(X)\Phi_{b_2}(X)\cdots\Phi_{b_s}(X) = k X^{c_0}\Phi_{c_1}(X)\Phi_{c_2}(X)\cdots\Phi_{c_t}(X)$$

for some nonnegative integers $a_i, b_i, c_i \geq 0$. Then, for each $n \geq 1$ we can define

$$\varepsilon_n := \frac{X^{a_0}\Phi_{a_1}(\zeta_{\ell^n})\Phi_{a_2}(\zeta_{\ell^n})\cdots\Phi_{a_r}(\zeta_{\ell^n})}{X^{c_0}\Phi_{c_1}(\zeta_{\ell^n})\Phi_{c_2}(\zeta_{\ell^n})\cdots\Phi_{c_t}(\zeta_{\ell^n})}, \quad \delta_n := -\frac{X^{b_0}\Phi_{b_1}(\zeta_{\ell^n})\Phi_{b_2}(\zeta_{\ell^n})\cdots\Phi_{b_s}(\zeta_{\ell^n})}{X^{c_0}\Phi_{c_1}(\zeta_{\ell^n})\Phi_{c_2}(\zeta_{\ell^n})\cdots\Phi_{c_t}(\zeta_{\ell^n})},$$

where $\varepsilon_n, \delta_n$ are $\{\nu_\ell\}$-units in $\mathbb{Q}(\zeta_{\ell^n})$ such that $\varepsilon_n + \delta_n = k$ (for sufficiently large $n$).
$S$-unit equations

- A quick computer search yields the following relations:
S-unit equations

- A quick computer search yields the following relations:

\[
\begin{align*}
\Phi_2(X)^2 - \Phi_3(X) &= X, \\
\Phi_2(X)^2 - \Phi_4(X) &= 2X, \\
\Phi_2(X)^2 - \Phi_6(X) &= 3X, \\
\Phi_2(X)^2 - \Phi_1(X)^2 &= 4X, \\
\Phi_2(X)^4 - \Phi_{10}(X) &= 5X\Phi_3(X), \\
\Phi_2^2(X)\Phi_3(X) - \Phi_1(X)^2\Phi_6(X) &= 6X\Phi_4(X), \\
\Phi_7(X) - \Phi_1(X)^6 &= 7X\Phi_6(X)^2, \\
\Phi_2(X)^4 - \Phi_1(X)^4 &= 8X\Phi_4(X), \\
\Phi_2(X)^4\Phi_5(X) - \Phi_1(X)^4\Phi_{10}(X) &= 10X\Phi_4(X)^3.
\end{align*}
\]
S-unit equations

• A quick computer search yields the following relations:

\[ \Phi_2(X)^2 - \Phi_3(X) = X, \]
\[ \Phi_2(X)^2 - \Phi_4(X) = 2X, \]
\[ \Phi_2(X)^2 - \Phi_6(X) = 3X, \]
\[ \Phi_2(X)^2 - \Phi_1(X)^2 = 4X, \]
\[ \Phi_2(X)^4 - \Phi_{10}(X) = 5X\Phi_3(X), \]
\[ \Phi_2^2(X)\Phi_3(X) - \Phi_1(X)^2\Phi_6(X) = 6X\Phi_4(X), \]
\[ \Phi_7(X) - \Phi_1(X)^6 = 7X\Phi_6(X)^2, \]
\[ \Phi_2(X)^4 - \Phi_1(X)^4 = 8X\Phi_4(X), \]
\[ \Phi_2(X)^4\Phi_5(X) - \Phi_1(X)^4\Phi_{10}(X) = 10X\Phi_4(X)^3. \]

Question: Do there exist any cyclotomic relations for \( k \notin \{1, 2, 3, 4, 5, 6, 7, 8, 10\} \)?
Theorem (Siksek–V. 2023)

Let $\ell = 2$ or $3$ and let $S = \{\nu_\ell\}$ be the unique prime above $\ell$ 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 $\varepsilon_n, \delta_n \in \mathbb{Q}(\zeta_{\ell^n})$ as
  
  $\varepsilon_n = \Phi_2(\zeta_{\ell^n})^4 \Phi_5(\zeta_{\ell^n}) \zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3$, $\delta_n = -\Phi_1(\zeta_{\ell^n})^4 \Phi_{10}(\zeta_{\ell^n}) \zeta_{\ell^n} \Phi_4(\zeta_{\ell^n})^3$.

  noting that $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)$ and $\varepsilon_n + \delta_n = 10$.

• As $\Phi_m(X) = X^{\varphi(m)} \Phi_m(X - 1)$, this implies $\varepsilon_c = \varepsilon_n$ and $\delta_c = \delta_n$, thus $\varepsilon_n, \delta_n \in \mathbb{Q}_\infty,\ell$.

• Using a multiplicative basis for the cyclotomic units, one can show $\varepsilon_n$ is not generated by $\{\pm \zeta_{\ell^n} - 1, 1 - \zeta_{k \ell^n} - 1, 1 \leq k < \ell^n - 1\}$, and so $\varepsilon_m \neq \varepsilon_n$ for any $m < n$. 


**Theorem (Siksek–V. 2023)**

Let $\ell = 2$ or $3$ and let $S = \{\nu_\ell\}$ be the unique prime above $\ell$ 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 $\varepsilon_n, \delta_n \in \mathbb{Q}(\zeta_{\ell^n})$ as
  
  $$\varepsilon_n = \frac{\Phi_2(\zeta_{\ell^n})^4\Phi_5(\zeta_{\ell^n})}{\zeta_{\ell^n}\Phi_4(\zeta_{\ell^n})^3}, \quad \delta_n = \frac{-\Phi_1(\zeta_{\ell^n})^4\Phi_{10}(\zeta_{\ell^n})}{\zeta_{\ell^n}\Phi_4(\zeta_{\ell^n})^3}.$$ 

  noting that $\varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times$ and $\varepsilon_n + \delta_n = 10$. 

Theorem (Siksek–V. 2023)

Let \( \ell = 2 \) or \( 3 \) and let \( S = \{ v_\ell \} \) be the unique prime above \( \ell \) 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 \( \varepsilon_n, \delta_n \in \mathbb{Q}(\zeta_{\ell^n}) \) as

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

noting that \( \varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^{\times} \) and \( \varepsilon_n + \delta_n = 10 \).

- 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 \( S = \{\nu_\ell\} \) be the unique prime above \( \ell \) 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 \( \varepsilon_n, \delta_n \in \mathbb{Q}(\zeta_{\ell^n}) \) as
  \[
  \varepsilon_n = \Phi_2(\zeta_{\ell^n})^4\Phi_5(\zeta_{\ell^n}) \quad \text{and} \quad \delta_n = -\Phi_1(\zeta_{\ell^n})^4\Phi_{10}(\zeta_{\ell^n}) / \zeta_{\ell^n}\Phi_4(\zeta_{\ell^n})^3.
  \]
  noting that \( \varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^n}), S)^\times \) and \( \varepsilon_n + \delta_n = 10 \).

- 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 a multiplicative basis for the cyclotomic units, one can show \( \varepsilon_n \) is not generated by \( \{\pm \zeta_{\ell^{n-1}}, 1 - \zeta_{\ell^{n-1}}^k, 1 \leq k < \ell^{n-1}\} \), and so \( \varepsilon_m \neq \varepsilon_n \) for any \( m < n \). □
For each \( n \geq 1 \), let \( G_n := \text{Gal}(\mathbb{Q}(\zeta_5^n)/\mathbb{Q}_{n-1,5}) \). This is a cyclic group of order 4, generated by some \( \sigma \in G_n \) where \( \sigma(\zeta_5^n) = \zeta_5^{an} \) for some integer \( a \).
For each $n \geq 1$, let $G_n := \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}_{n-1,5})$. This is a cyclic group of order 4, generated by some $\sigma \in G_n$ where $\sigma(\zeta_n) = \zeta_n^a$ for some integer $a$.

We want to now 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 $Q_{\infty,5}$

- For each $n \geq 1$, let $G_n := \text{Gal}(Q(\zeta_{5^n})/Q_{n-1,5})$. 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 now 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 $\{\nu_5\}$-unit in $Q_{n-1,5}$.
For each \( n \geq 1 \), let \( G_n := \text{Gal}(\mathbb{Q}(\zeta_{5^n})/\mathbb{Q}_{n-1,5}) \). 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 now 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 \( \{\sqrt[5]{5}\} \)-unit in \( \mathbb{Q}_{n-1,5} \).

\[
x_4 \Phi_2 \left( \frac{x_1 x_2^2}{x_3 x_4^2} \right) \Phi_2 \left( \frac{x_1 x_4}{x_2 x_3} \right) x_2 \Phi_2 \left( \frac{x_1 x_2}{x_3 x_4} \right) \Phi_2 \left( \frac{x_1 x_4^2}{x_2 x_3} \right) = x_4 \Phi_1 \left( \frac{x_1}{x_3} \right) \Phi_1 \left( \frac{x_2}{x_4} \right) \Phi_1 \left( \frac{x_1 x_2}{x_3 x_4} \right) \Phi_1 \left( \frac{x_1 x_4}{x_2 x_3} \right),
\]

\[
x_4 \Phi_3 \left( \frac{x_1}{x_3} \right) \Phi_3 \left( \frac{x_2}{x_4} \right) - x_4 \Phi_6 \left( \frac{x_1}{x_3} \right) \Phi_6 \left( \frac{x_2}{x_4} \right) = 2 x_2 \Phi_2 \left( \frac{x_1 x_4}{x_2 x_3} \right) \Phi_2 \left( \frac{x_1 x_2}{x_3 x_4} \right),
\]

\[
x_4 \Phi_2 \left( \frac{x_1}{x_3} \right)^2 \Phi_2 \left( \frac{x_2}{x_4} \right)^2 - x_4 \Phi_1 \left( \frac{x_1}{x_3} \right)^2 \Phi_1 \left( \frac{x_2}{x_4} \right)^2 = 4 x_2 \Phi_2 \left( \frac{x_1 x_2}{x_3 x_4} \right) \Phi_2 \left( \frac{x_1 x_4}{x_2 x_3} \right).
\]
### Theorem (Siksek–V. 2023)

Let $\ell = 5$. Let $S = \{\nu_5\}$ be the unique prime above 5 in $\mathbb{Q}_{\infty,5}$. For each $k \in \{1, 2, 4\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times$ to the $S$-unit equation $\varepsilon + \delta = k$. 

---

\[ \begin{align*}
\text{Proof for } k = 4: \\
&\quad \text{For each } n \geq 1, \text{ define } \\
&\quad \varepsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_{\infty,5}, S)^\times \text{ as } \\
&\quad \varepsilon_n = \zeta - a_5^n \Phi_2(\zeta^{2+2a_5^n}) \Phi_2(\zeta - 1 - a_5^n) \zeta^{a_5^n} \Phi_2(\zeta^2 + 2a_5^n) \Phi_2(\zeta^2 - 2a_5^n), \\
&\quad \delta_n = -\zeta - a_5^n \Phi_1(\zeta^{2+2a_5^n}) \Phi_1(\zeta - 1 - a_5^n) \zeta^{a_5^n} \Phi_2(\zeta^2 + 2a_5^n) \Phi_2(\zeta^2 - 2a_5^n),
\end{align*} \]

where we've substituted $x_1 = \zeta^{5^n}$, $x_2 = \zeta^{a_5^n}$, $x_3 = \zeta - 1^{5^n}$ and $x_4 = \zeta - a_5^n$ into the third cyclotomic relation shown previously. Therefore, $\varepsilon_n + \delta_n = 4$.

\[ \begin{align*}
\text{As } \varepsilon_n \text{ and } \delta_n \text{ fixed under the action of } \text{Gal}(\mathbb{Q}_{\infty,5}/\mathbb{Q}_{5^n-1,5}), \text{ we have } \\
\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5}.
\end{align*} \]

\[ \begin{align*}
\text{A similar argument to the } \ell = 2, 3 \text{ case shows that } \\
\varepsilon_m \neq \varepsilon_n \text{ for any } m < n.
\end{align*} \]
Let $\ell = 5$. Let $S = \{\nu_5\}$ 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, $\varepsilon_n + \delta_n = 4$. 


Theorem (Siksek–V. 2023)

Let $\ell = 5$. Let $S = \{\nu_5\}$ be the unique prime above 5 in $\mathbb{Q}_{\infty,5}$. For each $k \in \{1, 2, 4\}$, there are infinitely many solutions $\varepsilon, \delta \in \mathcal{O}(\mathbb{Q}_{\infty,5})^\times$ 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

$$
\varepsilon_n = \frac{\zeta_5^{-a} \Phi_2(\zeta_5^{2n})^2 \Phi_2(\zeta_5^{1-n-a})^2}{\zeta_5^{a} \Phi_2(\zeta_5^{2+2a}) \Phi_2(\zeta_5^{2-2a})}, \quad \delta_n = \frac{-\zeta_5^{-a} \Phi_1(\zeta_5^{2n})^2 \Phi_1(\zeta_5^{-1-a})^2}{\zeta_5^{a} \Phi_2(\zeta_5^{2+2a}) \Phi_2(\zeta_5^{2-2a})}
$$

where we’ve substituted $x_1 = \zeta_5^n$, $x_2 = \zeta_5^a$, $x_3 = \zeta_5^{-1}$ and $x_4 = \zeta_5^{-a}$ into the third cyclotomic relation shown previously. Therefore, $\varepsilon_n + \delta_n = 4$.

- As $\varepsilon_n$ and $\delta_n$ fixed under the action of $\text{Gal}(\mathbb{Q}(\zeta_5^n)/\mathbb{Q}_{n-1,5})$, we have $\varepsilon_n, \delta_n \in \mathbb{Q}_{\infty,5}$.
**S-unit equation over \(Q_{\infty,5}\)**

**Theorem (Siksek–V. 2023)**

Let \(\ell = 5\). Let \(S = \{\nu_5\}\) be the unique prime above 5 in \(Q_{\infty,5}\). For each \(k \in \{1, 2, 4\}\), there are infinitely many solutions \(\varepsilon, \delta \in O(Q_{\infty,\ell}, S)^\times\) to the S-unit equation \(\varepsilon + \delta = k\).

**Proof for \(k = 4\):**

- For each \(n \geq 1\), define \(\varepsilon_n, \delta_n \in O(Q(\zeta_{5^n}), S)^\times\) 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 \(\varepsilon_n\) and \(\delta_n\) fixed under the action of \(\text{Gal}(Q(\zeta_{5^n})/Q_{n-1,5})\), we have \(\varepsilon_n, \delta_n \in Q_{\infty,5}\).
- A similar argument to the \(\ell = 2, 3\) case shows that \(\varepsilon_m \neq \varepsilon_n\) for any \(m < n\).
Elliptic curves over $\mathbb{Q}_\infty,\ell$

Theorem (Siksek–V. 2023)

Let $\ell = 2, 3, 5$ or $7$. Let $S = \{v_2, v_\ell\}$. Then there are infinitely many $\mathbb{Q}$-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 $S = \{\nu_2, \nu_\ell\}$. 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 $S = \{v_2, v_\ell\}$. Then there are infinitely many $\mathbb{Q}$-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 $\epsilon_n, \delta_n \in \mathcal{O}(\mathbb{Q}_\infty, \ell, S)^\times$ such that $\epsilon_n + \delta_n = 1$.
- We define the elliptic curve

$$E_n : Y^2 = X(X - 1)(X - \epsilon_n).$$
Elliptic curves over $\mathbb{Q}_\infty, \ell$

**Theorem (Siksek–V. 2023)**

Let $\ell = 2, 3, 5$ or $7$. Let $S = \{\nu_2, \nu_\ell\}$. Then there are infinitely many $\mathbb{Q}$-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 $S = \{v_2, v_{\ell}\}$. Then there are infinitely many $\mathbb{Q}$-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 $\mathbb{Q}$-isomorphism classes.
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 $\{\nu_2, \nu_\ell\}$.
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 $\{v_2, v_\ell\}$.

**Proof (sketch):**

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

13 / 15
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 $\mathbb{Q}$-isomorphism classes of genus $g$ hyperelliptic curves over $\mathbb{Q}_\infty, \ell$ with good reduction away from $\{\nu_2, \nu_\ell\}$.

Proof (sketch):  
- For $n \geq 1$, let $G_n = \text{Gal}(\mathbb{Q}(\zeta_{\ell^n})^+/\mathbb{Q}_{n-1,\ell})$; this is a cyclic subgroup of order $(\ell - 1)/2$.  
- Define the hyperelliptic curve 
  \[ D_n : Y^2 = h(X) \cdot \prod_{j=1}^{k} \prod_{\sigma \in G_n} \left( X - (\zeta_{\ell^n}^{1+\ell^n-1(j-1)} + \zeta_{\ell^n}^{-1-\ell^n-1(j-1)})^{\sigma} \right) \]
  
  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 $\mathbb{Q}$-isomorphism classes of genus $g$ hyperelliptic curves over $\mathbb{Q}_\infty, \ell$ with good reduction away from $\{\nu_2, \nu_\ell\}$.

Proof (sketch):

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

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

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

13 / 15
Summary

Conjectures/Theorems

Tate conjecture
\[ \text{Hom}_{G_K}(\ell(A), \ell(B)) \cong \text{Hom}_K(A, B) \otimes \mathbb{Z}_\ell \]

Mordell conjecture
\[ \text{genus}(C) \geq 2 \implies \#C(K) < \infty \]

Mordell–Weil
\[ (A(K) \text{ finitely generated}) \]

Siegel–Mahler
\[ \# \{ x, y \in O_{K,S}^\times : ax + by = 1 \} < \infty \]

Shafarevich (curves)
\[ \# \{ C/K : \text{genus}(C) = g \geq 2, \text{good outside } S \} < \infty \]

Shafarevich (abelian varieties)
\[ \# \{ A/K : \dim(C) = d, \text{good outside } S \} < \infty \]
### Summary

<table>
<thead>
<tr>
<th>Conjectures/Theorems</th>
<th>$K$ num field</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tate conjecture</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>$\text{Hom}<em>{G_K}(T</em>\ell(A), T_\ell(B)) \cong \text{Hom}<em>K(A, B) \otimes \mathbb{Z}</em>\ell$</td>
<td></td>
</tr>
<tr>
<td><strong>Mordell conjecture</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>$\text{genus}(C) \geq 2 \implies #C(K) &lt; \infty$</td>
<td></td>
</tr>
<tr>
<td><strong>Mordell–Weil</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>$(A(K)$ finitely generated)</td>
<td></td>
</tr>
<tr>
<td><strong>Siegel–Mahler</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>$#{x, y \in O_{K,S}^\times : ax + by = 1} &lt; \infty$</td>
<td></td>
</tr>
<tr>
<td><strong>Shafarevich (curves)</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>$#{C/K : \text{genus}(C) = g \geq 2, \text{good outside } S} &lt; \infty$</td>
<td></td>
</tr>
<tr>
<td><strong>Shafarevich (abelian varieties)</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>$#{A/K : \text{dim}(C) = d, \text{good outside } S} &lt; \infty$</td>
<td></td>
</tr>
</tbody>
</table>
### Summary

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