The unit equation over $\mathbb{Q}_\infty$

Samir Siksek (Warwick)
joint work with Nuno Freitas (ICMAT–Madrid), Alain Kraus (Sorbonne) and Robin Visser (Warwick)

15 September 2023

$\mathbb{Z}_\ell$-extensions of $\mathbb{Q}$

Let ℓ be an odd prime and $n \geq 1$. Then

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^{n+1}})/\mathbb{Q}) \quad \cong \quad (\mathbb{Z}/\ell^{n+1}\mathbb{Z})^\times \quad \cong \quad \mathbb{Z}/\ell^n\mathbb{Z} \times (\mathbb{Z}/\ell\mathbb{Z})^\times.$$

Thus $\mathbb{Q}(\zeta_{\ell^{n+1}})$ has a subfield denoted by $\mathbb{Q}_{n,\ell}$ satisfying

1. $[\mathbb{Q}_{n,\ell} : \mathbb{Q}] = \ell^n$;
2. $\mathbb{Q}_{n,\ell}$ is totally real and Galois;
3. $\mathrm{Gal}(\mathbb{Q}_{n,\ell}/\mathbb{Q}) \cong \mathbb{Z}/\ell^n\mathbb{Z}$;
4. ℓ is totally ramifies in $\mathbb{Q}_{n,\ell}$, and all other primes are unramified.

Let

$$\mathbb{Q}_{\infty,\ell} \;=\; \bigcup_{n=1}^{\infty} \mathbb{Q}_{n,\ell} \qquad \text{(cyclotomic } \mathbb{Z}_\ell\text{-extension of } \mathbb{Q}).$$

Then

$$\mathrm{Gal}(\mathbb{Q}_{\infty,\ell}/\mathbb{Q}) \;\cong\; \mathbb{Z}_\ell.$$

Sometimes write $\mathbb{Q}_n = \mathbb{Q}_{n,\ell}$ and $\mathbb{Q}_\infty = \mathbb{Q}_{\infty,\ell}$.

Asymptotic Fermat over ℓ-extensions

$K/\mathbb{Q}$ is an ℓ-extension if it is Galois and $[K : \mathbb{Q}] = \ell^n$.

Theorem (Freitas, Kraus and S.)

Let $\ell \geq 5$ be prime. Let K be an ℓ-extension of $\mathbb{Q}$ such that

- *K is totally real;*
- *ℓ is totally ramified in K;*
- *2 is inert in K.*

Then the asymptotic Fermat's Last Theorem holds for K: i.e. there is a constant C_K such that if $p > C_K$ is prime and $x^p + y^p + z^p = 0$ with x, y, $z \in K$ then $xyz = 0$.

Hypotheses are satisfied for $K = \mathbb{Q}_{n,\ell}$, with $\ell \geq 5$, provided $2^{\ell-1} \not\equiv 1 \pmod{\ell^2}$.

Asymptotic Fermat over ℓ-extensions

$K/\mathbb{Q}$ is an ℓ-extension if it is Galois and $[K:\mathbb{Q}] = \ell^n$.

Theorem (Freitas, Kraus and S.)

Let $\ell \geq 5$ be prime. Let K be an ℓ-extension of $\mathbb{Q}$ such that

- *K is totally real;*
- *ℓ is totally ramified in K;*
- *2 is inert in K.*

Then the asymptotic Fermat's Last Theorem holds for K: i.e. there is a constant C_K such that if $p > C_K$ is prime and $x^p + y^p + z^p = 0$ with x, y, $z \in K$ then $xyz = 0$.

Hypotheses are satisfied for $K = \mathbb{Q}_{n,\ell}$, with $\ell \geq 5$, provided $2^{\ell-1} \not\equiv 1 \pmod{\ell^2}$.

A key step is showing that the **unit equation**

$$\varepsilon + \delta = 1, \qquad \varepsilon,\ \delta \in \mathcal{O}_K^\times$$

has no solutions.

The unit equation in ℓ-extensions

Lemma

- *Let K be an ℓ-extension, $[K:\mathbb{Q}] = \ell^n$.*
- *Suppose ℓ is totally ramified:*

$$\ell\mathcal{O}_K = \lambda^{\ell^n}.$$

Then $\varepsilon \equiv \pm 1 \pmod{\lambda}$ for all $\varepsilon \in \mathcal{O}_K^\times$.

Proof.

Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then $G = I(\lambda/\ell)$ (the inertia group).
Hence

$$\varepsilon^\sigma \equiv \varepsilon \pmod{\lambda}, \qquad \forall \sigma \in G.$$

Thus

$$\pm 1 = \mathrm{Norm}(\varepsilon) = \prod_{\sigma \in G} \varepsilon^\sigma \equiv \varepsilon^{\ell^n} \equiv \varepsilon \pmod{\lambda},$$

since $\mathcal{O}_K/\lambda \cong \mathbb{F}_\ell$. □

The unit equation in ℓ-extensions

Theorem

Let $\ell \neq 3$.

- *Let K be an ℓ-extension, $[K : \mathbb{Q}] = \ell^n$.*
- *Suppose ℓ is totally ramified:* $\ell \mathcal{O}_K = \lambda^{\ell^n}$.

Then the unit equation

$$\varepsilon + \delta = 1, \qquad \varepsilon,\ \delta \in \mathcal{O}_K^\times$$

has no solutions.

Proof.

True since $\pm 1 \pm 1 \not\equiv 1 \pmod{\ell}$. □

- Proof doesn't work for $\ell = 3$ as $-1 - 1 \equiv 1 \pmod 3$.
- Unable to prove FLT over $\mathbb{Q}_{n,3}$.
- Does the the unit equation have infinitely or finitely many solutions over $\mathbb{Q}_{\infty,3}$?

Some major theorems in Diophantine geometry

	K a number field
A/K abelian variety	**Mordell–Weil Theorem** $A(K)$ is finitely generated
A, B/K abelian varieties	**Tate Conjecture (Faltings)** $\mathrm{Hom}_{G_K}(T_\ell(A), T_\ell(B)) \cong \mathrm{Hom}_K(A, B) \otimes \mathbb{Z}_\ell$
S finite set of $\mathcal{O}_K$-primes $n \geq 1$	**Shafarevich Conjecture (Faltings)** $\exists$ finitely many isom classes of dim n p.p. abelian varieties A/K with good reduction outside S
C/K curve of genus ≥ 2	**Mordell Conjecture (Faltings)** $C(K)$ is finite
S finite set of $\mathcal{O}_K$-primes	**Siegel's Theorem** $\varepsilon + \delta = 1$ has finitely many solutions with $\varepsilon, \delta \in \mathcal{O}_S^\times$

Győry (1974): effective Siegel.

Mordell–Weil, Shafarevich, Mordell: ineffective.

Replacing number field with $\mathbb{Q}_\infty$

	$K = \mathbb{Q}_\infty$
A/K abelian variety	**Analogue of Mordell–Weil: Mazur Conjecture** $A(K)$ is finitely generated
A, B/K abelian varieties	**Analogue of Tate: Zarhin's Theorem** $\mathrm{Hom}_{G_K}(T_\ell(A), T_\ell(B)) \cong \mathrm{Hom}_K(A, B) \otimes \mathbb{Z}_\ell$
S finite set of $\mathcal{O}_K$-primes $n \geq 1$	**Analogue of Shafarevich??** Can we say anything about dim n p.p.a.v. A/K with good reduction outside S?
C/K curve of genus ≥ 2	**Analogue of Mordell: Parshin Conjecture** $C(K)$ is finite
S finite set of $\mathcal{O}_K$-primes	**Analogue of Siegel??** Does $\varepsilon + \delta = 1$ have only finitely many solutions with ε, $\delta \in \mathcal{O}_S^\times$?

Mazur Conjecture

Conjecture (Mazur)

Let A be an abelian variety over $\mathbb{Q}_\infty$. Then $A(\mathbb{Q}_\infty)$ is finitely generated.

Theorem (Kato)

Let $A/\mathbb{Q}$ be a factor of $J_1(N)$. Then $A(\mathbb{Q}_\infty)$ is finitely generated.

Wiles: If $E/\mathbb{Q}$ is an elliptic curve then E is a factor of $J_1(N)$.

Conjecture (Mazur)

Let A be an abelian variety over $\mathbb{Q}_\infty$. Then $A(\mathbb{Q}_\infty)$ is finitely generated.

Conjecture (Parshin)

Let $C/\mathbb{Q}_\infty$ be a curve of genus ≥ 2. Then $C(\mathbb{Q}_\infty)$ is finite.

Theorem (Greenberg)

Mazur $\implies$ Parshin

Proof.

- Let J be the Jacobian of C.
- $J(\mathbb{Q}_\infty) = J(\mathbb{Q}_n)$ for some n, by Mazur.
- Enlarge n so that $C(\mathbb{Q}_n) \neq \emptyset$.
- By Abel–Jacobi, $C(\mathbb{Q}_\infty) \subset J(\mathbb{Q}_\infty) = J(\mathbb{Q}_n)$.
- Thus $C(\mathbb{Q}_\infty) = C(\mathbb{Q}_n)$.
- $C(\mathbb{Q}_n)$ is finite by Faltings.

□

No Siegel over $\mathbb{Q}_\infty$

Theorem (S.–Visser)

Let $K = \mathbb{Q}_{\infty,3}$. Then

$$\varepsilon + \delta = 1, \qquad \varepsilon,\ \delta \in \mathcal{O}_K^\times$$

has infinitely many solutions.

Theorem (S.–Visser)

Let $\ell = 2$, 5 or 7 and $K = \mathbb{Q}_{\infty,\ell}$. Let υ_ℓ be the unique prime above ℓ. Let $S = \{\upsilon_\ell\}$. Then

$$\varepsilon + \delta = 1, \qquad \varepsilon,\ \delta \in \mathcal{O}_S^\times$$

has infinitely many solutions.

Cyclotomic Units from Cyclotomic Polynomials

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

$$X^m - 1 \;=\; \prod_{d|m} \Phi_d(X), \qquad \Phi_m(X) \;=\; \prod_{d|m} (X^d - 1)^{\mu(m/d)}$$

Can conclude

$$\mathrm{Cyc}_n \;=\; \left\langle \zeta, \quad \Phi_m(\zeta) \quad : \quad 1 < m < \frac{\ell^{n+1}}{2},\; \ell \nmid m \right\rangle$$

cyclotomic units in $\mathbb{Q}(\zeta_{\ell^{n+1}})$

$$\mathrm{SCyc}_n \;=\; \left\langle \zeta, \quad \Phi_m(\zeta) \quad : \quad 1 \le m < \frac{\ell^{n+1}}{2},\; \ell \nmid m \right\rangle$$

cyclotomic υ_ℓ-units in $\mathbb{Q}(\zeta_{\ell^{n+1}})$

Write $\mathrm{SCyc}_n^+ = \mathbb{Q}(\zeta_{\ell^{n+1}})^+ \cap \mathrm{SCyc_n}$.

Kummer–Sinnott: $[\mathcal{O}_{\upsilon_\ell}^\times : \mathrm{SCyc}_n^+] \;=\; h_n^+ \;:=\; \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_{\ell^{n+1}})^+)$.

Let $\ell = 5$. Let $\zeta = \zeta_{5^{n+1}}$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}_{n,5})$ is cyclic and generated by

$$\sigma_a : \zeta \mapsto \zeta^a, \qquad a^2 \equiv -1 \pmod{5^{n+1}}.$$

Let

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

- $F + G = 2H$.
- F, G, H are invariant under $x_1 \mapsto x_2 \mapsto x_3 \mapsto x_4 \mapsto x_1$.
- $F(\zeta, \zeta^a, \zeta^{a^2}, \zeta^{a^3}) \in \mathcal{O}(\mathbb{Q}_{n,5})^\times$. Same for G, H.
- $\therefore \varepsilon + \delta = 2$ has infinitely many solutions in $\mathcal{O}(\mathbb{Q}_{\infty,5})^\times$.

No Shafarevich over $\mathbb{Q}_\infty$

Let

$$E \; : \; Y^2 = X^3 - X.$$

- Let $\varepsilon \in \mathcal{O}(\mathbb{Q}_\infty)^\times$. Let

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

  Then E_ε has good reduction away from primes above 2.
- $E_\varepsilon \cong_{\mathbb{Q}_\infty} E_\delta \qquad \iff \qquad \varepsilon/\delta \in (\mathcal{O}^\times)^2$.
- $\#\mathcal{O}^\times/(\mathcal{O}^\times)^2 = \infty$
- We obtain infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}_\infty$ with good reduction away from 2.
- $E_\varepsilon \cong_{\overline{\mathbb{Q}}} E$.

No Shafarevich over $\mathbb{Q}_\infty$

Theorem (S.–Visser)

Let $\ell \geq 11$ be an odd prime and let $g = \lfloor \frac{\ell-3}{4} \rfloor$.

- *There is an infinite family of genus g hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ with good reduction away from $\{v : v \mid 2\ell\}$.*
- *The curves are pairwise non-isomorphic over $\overline{\mathbb{Q}}$.*
- *The Jacobians have good reduction away from $\{v : v \mid 2\ell\}$, and are pairwise non-isomorphic over $\overline{\mathbb{Q}}$.*
- *Moreover, if*

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

then the Jacobians are pairwise non-isogenous over $\mathbb{Q}_{\infty,\ell}$.

Hyperelliptic Construction

- Let $\zeta = \zeta_{\ell^{n+1}}$. Let $\alpha = \zeta^i$, $\beta = \zeta^j$

  $$(\alpha + \alpha^{-1}) - (\beta + \beta^{-1}) \;=\; \alpha^{-1} \cdot (1 - \alpha\beta) \cdot (1 - \alpha\beta^{-1}) \;\in\; \mathrm{SCyc}_n^+$$

  unless $\alpha = \beta^{\pm 1}$.
- Let $\gamma_1 = \zeta + \zeta^{-1}$ and let $\gamma_1, \ldots, \gamma_{(\ell-1)/2}$ be the conjugates of γ_1 in $\mathbb{Q}(\zeta)^+/\mathbb{Q}_{n,\ell}$.
- Let $C_n \;:\; Y^2 = (X - \gamma_1)(X - \gamma_2)\cdots(X - \gamma_{(\ell-1)/2})$.
- $C_n/\mathbb{Q}_n$.
- $\Delta(\mathrm{pol}) = \prod_{i<j}(\gamma_i - \gamma_j)^2 \in \mathrm{SCyc}_n^+$.
- $C_n/\mathbb{Q}_n$ has genus $\lfloor(\ell-3)/4\rfloor$, has good reduction away from $\{\upsilon \;:\; \upsilon \mid 2\ell\}$.

J_m, J_n are non-isogenous for $m > n$ (sketch)

- Let ℓ, q be odd primes, such that $\ell = 2q + 1$, $\mathbb{F}_q^\times = \langle 2 \rangle$.
- $\Omega_\infty^+ = \cup_k \mathbb{Q}(\zeta_{\ell^k} + \zeta_{\ell^k}^{-1})$, $[\Omega_\infty^+ : \mathbb{Q}_\infty] = q$.
- $C_n \ : \ Y^2 = (X - \gamma_1)(X - \gamma_2) \cdots (X - \gamma_q)$. $\gamma_1 = \zeta_{\ell^{n+1}} + \zeta_{\ell^{n+1}}^{-1}$.
- $C_m \ : \ Y^2 = (X - \delta_1)(X - \delta_2) \cdots (X - \delta_q)$. $\delta_1 = \zeta_{\ell^{m+1}} + \zeta_{\ell^{m+1}}^{-1}$.
- Write $J_n = \mathrm{Jac}(C_n)/\mathbb{Q}_\infty$. Then $J_n[2]$ is irreducible as $G_{\mathbb{Q}_\infty}$-module.
- Suppose $\phi : J_n \to J_m$ is an isogeny, defined over $\mathbb{Q}_\infty$ of minimal degree. **Want a contradiction**.
- As $J_n[2]$ is irreducible, ϕ has odd degree.
- Hence $\mathbb{Q}_\infty(J_n[2^r]) = \mathbb{Q}_\infty(J_m[2^r])$ for all $r \geq 1$.
- Plan A: compute $\mathbb{Q}_\infty(J_n[2])$, $\mathbb{Q}_\infty(J_m[2])$. If different then have a contradiction.
- Bad news: $\mathbb{Q}_\infty(J_n[2]) = \mathbb{Q}_\infty(\gamma_1) = \Omega_\infty^+ = \mathbb{Q}_\infty(J_m[2])$. No contradiction.

J_m, J_n are non-isogenous for $m > n$ (sketch)

- Let ℓ, q be odd primes, such that $\ell = 2q + 1$, $\qquad \mathbb{F}_q^\times = \langle 2 \rangle$.
- $\Omega_\infty^+ = \cup_k \mathbb{Q}(\zeta_{\ell^k} + \zeta_{\ell^k}^{-1})$, $\qquad [\Omega_\infty^+ : \mathbb{Q}_\infty] = q$.
- $C_n \ : \ Y^2 = (X - \gamma_1)(X - \gamma_2) \cdots (X - \gamma_q)$. $\gamma_1 = \zeta_{\ell^{n+1}} + \zeta_{\ell^{n+1}}^{-1}$.
- $C_m \ : \ Y^2 = (X - \delta_1)(X - \delta_2) \cdots (X - \delta_q)$. $\delta_1 = \zeta_{\ell^{m+1}} + \zeta_{\ell^{m+1}}^{-1}$.
- Plan B: compute $\mathbb{Q}_\infty(J_n[4])$, $\mathbb{Q}_\infty(J_m[4])$. If different then have a contradiction.
- $\mathbb{Q}_\infty(J_n[4]) = \Omega_\infty^+(\sqrt{\gamma_i - \gamma_j} : 1 \le i, j \le q)$. Suppose fields of 4-torsion are same:
- $\Omega_\infty^+(\sqrt{\gamma_i - \gamma_j} : 1 \le i, j \le q) \ = \ \Omega_\infty^+(\sqrt{\delta_i - \delta_j} : 1 \le i, j \le q)$.
- $\langle \gamma_i - \gamma_j : 1 \le i, j \le q \rangle = \langle \delta_i - \delta_j : 1 \le i, j \le q \rangle$ in $\Omega_\infty^+/(\Omega_\infty^+)^2$.
- We obtain a relation between elements of SCyc_m^+ up to the square of $\mu \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^{m+1}})^+)_S^\times$.

J_m, J_n are non-isogenous for $m > n$ (sketch continued)

- Let ℓ, q be odd primes, such that $\ell = 2q+1$, $\quad \mathbb{F}_q^\times = \langle 2 \rangle$.
- $\Omega_\infty^+ = \cup_k \mathbb{Q}(\zeta_{\ell^k} + \zeta_{\ell^k}^{-1})$, $\quad [\Omega_\infty^+ : \mathbb{Q}_\infty] = q$.
- $C_n \;:\; Y^2 = (X-\gamma_1)(X-\gamma_2)\cdots(X-\gamma_q)$. $\gamma_1 = \zeta_{\ell^{n+1}} + \zeta_{\ell^{n+1}}^{-1}$.
- $C_m \;:\; Y^2 = (X-\delta_1)(X-\delta_2)\cdots(X-\delta_q)$. $\delta_1 = \zeta_{\ell^{m+1}} + \zeta_{\ell^{m+1}}^{-1}$.
- $\langle \gamma_i - \gamma_j : 1 \le i,j \le q \rangle = \langle \delta_i - \delta_j : 1 \le i,j \le q \rangle$ in $\Omega_\infty^+/(\Omega_\infty^+)^2$.
- $\delta_1 - \delta_2 \;=\; \mu^2 \cdot \prod_{i<j} (\gamma_i - \gamma_j)^{x_{i,j}} \qquad x_{i,j} \in \{0,1\}$.
- We obtain a relation between elements of SCyc_m^+ up to the square of $\mu \in \mathcal{O}(\mathbb{Q}(\zeta_{\ell^{m+1}})^+)_S^\times$.
- Recall $[\mathcal{O}(\mathbb{Q}(\zeta_{\ell^{m+1}})^+)_S^\times : \mathrm{SCyc}_m^+] = h_m^+ := \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_{\ell^{m+1}})^+)$.
- **If $2 \nmid h_m^+$ then $\mu \in \mathrm{SCyc}_m^+$, can obtain a contradiction!**

$h_m^+ := \#\,\mathrm{Cl}(\mathbb{Q}(\zeta_{\ell^{m+1}})^+)$. Want values of ℓ such that $2 \nmid h_m^+$ for all $m \geq 0$. Recall $h_m^+ \mid h_m$.

Theorem (Estes, Stevenhagen, 1994)

Let ℓ, q be odd primes, such that $\ell = 2q+1$, and $\mathbb{F}_q^\times = \langle 2 \rangle$. Then h_0 is odd.

Theorem (Washington, 1978)

Let $p \neq \ell$. Then $\mathrm{ord}_p(h_m)$ is bounded as $m \to \infty$.

Theorem (Ichimura and Nakajima, 2012)

Let $\ell \leq 509$. Then h_m/h_0 is odd for all m.

No Shafarevich over $\mathbb{Q}_\infty$

Theorem (S.–Visser)

Let $\ell \geq 11$ be an odd prime and let $g = \lfloor \frac{\ell-3}{4} \rfloor$.

- *There is an infinite family of genus g hyperelliptic curves over $\mathbb{Q}_{\infty,\ell}$ with good reduction away from $\{\upsilon : \upsilon \mid 2\ell\}$.*
- *The curves are pairwise non-isomorphic over $\overline{\mathbb{Q}}$.*
- *The Jacobians have good reduction away from $\{\upsilon : \upsilon \mid 2\ell\}$, and are pairwise non-isomorphic over $\overline{\mathbb{Q}}$.*
- *Moreover, if*

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

then the Jacobians are pairwise non-isogenous over $\mathbb{Q}_{\infty,\ell}$.