Arithmetic of punctured curves and punctured abelian varieties

Samir Siksek (Warwick)

14 May 2021

What is an integral point?

- K be a number field; $\mathcal{O}_K$ ring of integers of K;
- S a finite set of places of K;
- $\mathcal{O}_S = \{\alpha \in K \ : \ \mathrm{ord}_{\mathfrak{p}}(\alpha) \geq 0, \qquad \text{for all } \mathfrak{p} \notin S\}$.
- V/K a smooth projective irreducible variety;
- W a subvariety defined over K.

Define

$$(V - W)(\mathcal{O}_S) = \{P \in V(K) \ : \ (P \bmod \mathfrak{p}) \notin W \text{ for all } \mathfrak{p} \notin S\}.$$

Example. Let a, $b \in \mathbb{Z}$ with $4a^3 + 27b^2 \neq 0$. Let

$$E \ : \ \{Y^2 = X^3 + aX + b\} \cup \{\infty\}$$

$$\begin{aligned}(E - \infty)(\mathbb{Z}) &= \{(\alpha, \beta) \in E(\mathbb{Q}) \ : \ \mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta) \geq 0 \text{ for all primes } p\} \\ &= \{(\alpha, \beta) \in \mathbb{Z}^2 \ : \ \beta^2 = \alpha^3 + a\alpha + b\}.\end{aligned}$$

(But $\qquad E(\mathbb{Z}) = E(\mathbb{Q}) \qquad V = E, \ W = \emptyset$.)

Let C/K be a smooth projective curve. Let $P_1, \ldots, P_r \in C(K)$. Let

$$C' = C - \{P_1, P_2, \ldots, P_r\} \qquad C \textbf{ punctured} \text{ at } P_1, \ldots, P_r.$$

The **Euler characteristic** of C' is $\quad \chi(C') = 2 - 2g(C) - r.$

Theorem (Faltings–Siegel)

If C' is hyperbolic (i.e. $\chi(C') < 0$) then $C'(\mathcal{O}_K)$ is finite.

Example

- If $g(C) \geq 2$ then C' is hyperbolic.
- $E - \infty$ is hyperbolic.
- $\mathbb{P}^1 - \{0, 1, \infty\}$ is hyperbolic.

Integral points on $\mathbb{P}^1 - \{0, 1, \infty\}$

$$\mathbb{P}^1(\mathcal{O}_K) = \mathbb{P}^1(K) = K \cup \infty.$$

$$(\mathbb{P}^1 - \infty)(\mathcal{O}_K) = \mathcal{O}_K.$$

$$(\mathbb{P}^1 - \{0, \infty\})(\mathcal{O}_K) = \mathcal{O}_K^\times.$$

$$(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}_K) = \{\varepsilon \in \mathcal{O}_K^\times \ : \ \varepsilon - 1 \in \mathcal{O}_K^\times\}.$$

We obtain a $1-1$ correspondence between $(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}_K)$ and solutions to the **unit equation**:

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

Arithmetic Puncturing Problem

- K be a number field; $\mathcal{O}_K$ ring of integers of K;
- V/K a smooth projective irreducible variety;
- W a subvariety defined over K.

Arithmetic Puncturing Problem (Hassett and Tschinkel, 2001).

- Suppose $\mathrm{codim}(V, W) \geq 2$.
- Suppose the rational points of V are potentially dense: i.e. there is a finite extension F/K such that $V(F)$ is Zariski dense in V.
- Is the set of integral points on $V - W$ potentially dense?
  i.e. Is there a finite extension L/K, and a finite set of places T such that $(V - W)(\mathcal{O}_{L,T})$ is Zariski dense in V?

Example

(Hassett and Tschinkel) Let A be an abelian variety. Suppose $\mathrm{End}(A)^\times$ is infinite. Then the integral points on $A - 0$ are potentially dense.

Arithmetic Puncturing Problem

- K be a number field; $\mathcal{O}_K$ ring of integers of K;
- V/K a smooth projective irreducible variety;
- W a subvariety defined over K.

Arithmetic Puncturing Problem (Hassett and Tschinkel, 2001).

- Suppose $\mathrm{codim}(V, W) \geq 2$.
- Suppose the rational points of V are potentially dense: i.e. there is a finite extension F/K such that $V(F)$ is Zariski dense in V.
- Is the set of integral points on $V - W$ potentially dense?
  i.e. Is there a finite extension L/K, and a finite set of places T such that $(V - W)(\mathcal{O}_{L,T})$ is Zariski dense in V?

Theorem (McKinnon and Roth)

Let V be a surface with negative Kodaira dimension. Then the integral points on $V - W$ are potentially dense.

Theorem (Triantafillou, March 2020)

Let $n = [K : \mathbb{Q}]$. Suppose

- $3 \nmid n$;
- *3 splits completely in K.*

Then the unit equation

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

has no solutions.

Proof.

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the primes above 3. Then $\mathcal{O}_K/\mathfrak{p}_i = \mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{-1}\}$. Suppose (ε, δ) is a solution to (1). Then

$$1 = \varepsilon + \delta \equiv (\pm 1) + (\pm 1) \pmod{\mathfrak{p}_i}.$$

Hence $\varepsilon \equiv \delta \equiv -1 \pmod{\mathfrak{p}_i}$. Thus

$$\varepsilon = -1 + 3\phi, \qquad \delta = -1 + 3\psi, \qquad \phi,\ \psi \in \mathcal{O}_K.$$

Assumptions:

- $3 \nmid n$;
- 3 splits completely in K.
- $\varepsilon + \delta = 1, \qquad \varepsilon,\ \delta \in \mathcal{O}_K^\times$.

Then

$$1 = \varepsilon + \delta \equiv (\pm 1) + (\pm 1) \pmod{\mathfrak{p}_i}.$$

Hence $\varepsilon \equiv \delta \equiv -1 \pmod{\mathfrak{p}_i}$. Thus

$$\varepsilon = -1 + 3\phi, \qquad \delta = -1 + 3\psi, \qquad \phi,\ \psi \in \mathcal{O}_K.$$

$$1 = \varepsilon + \delta = -2 + 3(\phi + \psi) \qquad \Longrightarrow \qquad \phi + \psi = 1.$$

But ε is a unit, so

$$\pm 1 = \mathrm{Norm}(\varepsilon) = \mathrm{Norm}(-1+3\phi) \equiv (-1)^n + (-1)^{n-1} \times 3 \times \mathrm{Trace}(\phi) \pmod 9.$$

$$\therefore \qquad \mathrm{Trace}(\phi) \equiv \mathrm{Trace}(\psi) \equiv 0 \pmod 3.$$

$$\therefore \qquad n = [K : \mathbb{Q}] = \mathrm{Trace}(1) = \mathrm{Trace}(\phi + \psi) \equiv 0 \pmod 3$$

Contradiction! $\square$

Theorem (Triantafillou, March 2020)

Suppose

- $3 \nmid [K : \mathbb{Q}]$;
- 3 *splits completely in* K.

Then the unit equation

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

has no solutions.

Theorem (Triantafillou, March 2020)

Suppose

- $3 \nmid [K : \mathbb{Q}]$;
- 3 *splits completely in* K.

Then the unit equation

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

has no solutions.

Theorem (Corollary to Triantafillou's proof)

Suppose

- $3 \nmid [K : \mathbb{Q}]$;
- 3 *splits completely in* K.

Let $V = \{\varepsilon \in K^* \ :\ \mathrm{ord}_{\mathfrak{p}}(\varepsilon) = 0$ *for all* $\mathfrak{p} \mid 3$ *and* $\mathrm{Norm}(\varepsilon) \equiv \pm 1 \bmod 9\}$.
Then the equation

$$\varepsilon + \delta = 1, \qquad \varepsilon,\ \delta \in V$$

has no solutions.

Local Obstructions to the Unit Equation (jt wk with A. Kraus and N. Freitas)

Let $K/\mathbb{Q}$ be Galois.

- $n = [K : \mathbb{Q}]$, $\qquad G = \mathrm{Gal}(K/\mathbb{Q})$;
- $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ above rational prime p;
- $I_\mathfrak{p} := \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}} \quad \text{for all } \alpha \in \mathcal{O}_K\}$ **(inertia)**

Fact: p is totally ramified in K iff $I_\mathfrak{p} = G$.
Suppose p is totally ramified and consider

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

$$\pm 1 \ = \ \mathrm{Norm}(\varepsilon) = \prod_{\sigma \in G} \sigma(\varepsilon) = \prod_{\sigma \in I_\mathfrak{p}} \sigma(\varepsilon) \equiv \ \varepsilon^n \pmod{\mathfrak{p}}.$$

$$\therefore \quad \varepsilon^{2n} \equiv 1 \pmod{\mathfrak{p}} \qquad \text{and} \qquad (\varepsilon - 1)^{2n} \equiv 1 \pmod{\mathfrak{p}}.$$

$$\therefore \mathfrak{p} \mid \mathrm{Res}(X^{2n} - 1, (X-1)^{2n} - 1), \qquad \therefore p \mid \mathrm{Res}(X^{2n} - 1, (X-1)^{2n} - 1).$$

Conclusion: If

- $[K : \mathbb{Q}] = n$ (not necessarily Galois);
- the unit equation has solutions;
- p is totally ramified in K,

then $p \mid \mathrm{Res}(X^{2n} - 1, (X-1)^{2n} - 1)$.

Easy exercise: $\mathrm{Res}(X^{2n} - 1, (X-1)^{2n} - 1) = 0 \iff 3 \mid n$.

Theorem (Freitas, Kraus, S)

Let $\ell \neq 3$ be a prime. Then there are only finitely many degree ℓ **cyclic** *number fields K such that the unit equation has solutions in K.*

Proof.

- Let K be cyclic of degree ℓ. Let p be a rational prime.
- Let e_p be the ramification index. Then $e_p \mid \ell$. So $e_p = 1$ or $e_p = \ell$.
- Either p is unramified or it is totally ramified.
- Suppose the unit equation has solutions in K.
- $\therefore$ all ramified primes divide $\mathrm{Res}(X^{2\ell} - 1, (X-1)^{2\ell} - 1) \neq 0$.

$\square$

Theorem (Freitas, Kraus, S)

Let $\ell \neq 3$ be a prime. Then there are only finitely many degree ℓ **cyclic** *number fields K such that the unit equation has solutions in K.*

Example

Take $\ell = 5$. Then $\mathrm{Res}(X^{10} - 1, (X-1)^{10} - 1) = -3 \times 11^9 \times 31^3$.
The only cyclic degree 5 field for which the unit equation has a solution is $\mathbb{Q}(\zeta_{11})^+$.
The unit equation has 570 solutions in $\mathbb{Q}(\zeta_{11})^+$.

Nagell, 1969. Gave two infinite families of cubic fields where the unit equation has solutions. One of the two families is cyclic.

Punctured Abelian Varieties

Lemma

Let $A/\mathbb{Q}$ be an abelian variety and p be a prime of good reduction for A. Suppose

- $A(\mathbb{Q}) = 0$;
- *K is a number field, p totally ramifies in K.*
- $\gcd(n, \#A(\mathbb{F}_p)) = 1$ *where* $n = [K : \mathbb{Q}]$.

Then $(A - 0)(\mathcal{O}_K) = \emptyset$.

Proof.

Write $p\mathcal{O}_K = \mathfrak{p}^n$. Let $Q \in A(K)$. Then

$$0 \;=\; \underbrace{\mathrm{Trace}_{K/\mathbb{Q}}(Q)}_{\in A(\mathbb{Q})} \;\equiv\; nQ \pmod{\mathfrak{p}}.$$

But $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_p$.
Since $\gcd(n, \#A(\mathbb{F}_p)) = 1$, we have $Q \equiv 0 \pmod{\mathfrak{p}}$.
$\therefore\ Q \notin (A - 0)(\mathcal{O}_K)$. $\square$

Lemma

Let $A/\mathbb{Q}$ be an abelian variety and p be a prime of good reduction for A. Suppose

- $A(\mathbb{Q}) = 0$;
- *K is a number field, p totally ramifies in K.*
- $\gcd(n, \#A(\mathbb{F}_p)) = 1$ *where* $n = [K : \mathbb{Q}]$.

Then $(A - 0)(\mathcal{O}_K) = \emptyset$.

Example

- Let $E \ : \ Y^2 = X^3 - 16$.
- Let $K = \mathbb{Q}(\sqrt{-3})$. Then $E(K) = 0$.
- Let $p \equiv 2 \pmod 3$, $p \neq 2$.
- Let K_n be the n-th layer of the anti-cyclotomic $\mathbb{Z}_p$-extension ($\mathrm{Gal}(K_n/K) = \mathbb{Z}/p^n\mathbb{Z}$).
- For every $n \geq 1$, $(E - 0)(\mathcal{O}_{K_n}) = \emptyset$.
- However, $\mathrm{rank}(E(K_n)) \to \infty$ as $n \to \infty$ (attribution?).

Theorem

Let ℓ be a rational prime. Let A be an abelian variety defined over $\mathbb{Q}$. Suppose that

(i) $A(\mathbb{Q}) = 0$;

(ii) *There is $p \equiv 1 \pmod{\ell}$ of good reduction for A such that $\ell \nmid \#A(\mathbb{F}_p)$.*

For $X > 0$, let $\mathcal{F}_\ell^{\mathrm{cyc}}(X)$ be set of cyclic number fields K of degree ℓ and conductor at most X. Then

$$\frac{\#\{K \in \mathcal{F}_\ell^{\mathrm{cyc}}(X) \ : \ (A - 0)(\mathcal{O}_K) \neq \emptyset\}}{\#\mathcal{F}_\ell^{\mathrm{cyc}}(X)} = O\left(\frac{1}{(\log X)^\gamma}\right), \qquad \gamma > 0.$$

- Assumption (ii) is equivalent to: there is an element $\sigma \in \mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q}(\zeta_\ell))$ which acts freely on $A[\ell]$.

Example

$C/\mathbb{Q}\ :\ y^2+(x+1)y = x^5-55x^4-87x^3-54x^2-16x-2$ `LMFDB 8969.a`

- Let $A = J$ the Jacobian of C.
- $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathbb{Z}$.
- $A(\mathbb{Q}) = 0$.
- Condition (ii) is satisfied for all primes ℓ (checked $\overline{\rho}_{A,\ell}$ is surjective using the method of Dieulefait for $\ell \neq 2,\ 3,\ 8969$).
- For any prime ℓ and any finite S of rational primes, $(A-0)(\mathcal{O}_{K,S}) = \emptyset$ for 100% of cyclic degree ℓ number fields K.
- For any prime ℓ and any finite S of rational primes, $(C-\infty)(\mathcal{O}_{K,S}) = \emptyset$ for 100% of cyclic degree ℓ number fields K.

Homework

- Fix $n \geq 2$. Fix prime p.
- There are finitely many degree n étale algebras $F/\mathbb{Q}_p$.
- For such F, let

$$H_F = \{\varepsilon \in \mathcal{O}_F^\times \ : \ \mathrm{Norm}(\varepsilon) = \pm 1\}.$$

- Let

$$\mathrm{Bad}_{n,p} = \{F/\mathbb{Q}_p \text{ étale of degree } n \ : \\ \text{equation } \varepsilon + \delta = 1 \text{ has solution with } \varepsilon,\, \delta \in H_F\}.$$

- Evaluate the proportion of $K/\mathbb{Q}$ of degree n with $K \otimes \mathbb{Q}_p \in \mathrm{Bad}_{n,p}$.
- This will be an upper bound for the proportion of $K/\mathbb{Q}$ of degree n such that $(\mathbb{P}^1 - \{0, 1, \infty\})(\mathcal{O}_K) \neq \emptyset$.

Thank you!