Irish Debbarma

Department of Mathematics
Indian Institute of Science

भारतीय विज्ञान संस्थान

# Finiteness of Integral points on Elliptic Curves

From Dirchlet and Thue-Roth to Siegel, Šafarevič and Faltings

Elliptic Curves–Course Presentation, Dept. of Mathematics, 2023

# Outline

# Notation

- $K$ is a global field (finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$ where $q$ is a prime power),
- $K_v$ is the completion of $K$ at a place $v \in M_K$, and thus is a local field,
- For $S \subseteq M_K$ a finite set of places of $K$ containing all the infinite primes, the $x \in K$ such that

$$|x|_v \leq 1$$

  is called an $S$-unit and the group of $S$-units is denoted by $\mathbb{Z}_S$.

## Overview

**Siegel Theorem**

Let $E/K$ be an elliptic curve with Weierstrass coordinate function $x, y$, let $S \subseteq M_K$ be a finite set of places of $K$ containing $M_K^{\infty}$. If $\mathbb{Z}_S$ is the set of $S$-integers of $K$, then

$$\{P \in E(K) : x(P) \in \mathbb{Z}_S\}$$

is finite.

Or, more generally

**Siegel Theorem (General form)**

Let $P \in \mathbb{Q}[x, y]$ be an irreducible polynomial of two variables, such that the affine part $C := \{(x, y) : P(x, y) = 0\}$ either has genus atleast $1$, or has atleast three points on the line at infinity, or both. Then, $C$ can have only finitely many points $(x, y) \in \mathbb{Z}^2$.

## Overview

**Faltings Theorem**

Let $C/K$ be a non-singular curve defined over $K$ of genus atleast $2$, then the full set of rational points $C(K)$ is finite.

**Šaferevič Theorem**

Let $S \subseteq M_K$ be a finite set of places containing $M_K^\infty$. Then, upto isomorphism over $K$, there are only finitely many elliptic curves $E/K$ having good reduction at all primes not in $S$.

# Diophantine approximation

## Approximation of real numbers [Dirichlet]

Let $\alpha \in \mathbb{R} \backslash \mathbb{Q}$. Then, there are infinitely many rational numbers $p/q \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$$

Along the same lines, we have

## Approximation of algebraic numbers [Liouville]

Let $\alpha \in \overline{\mathbb{Q}}$ with degree $d \geq 2$ over $\mathbb{Q}$. Then, there is a constant $C(\alpha)$ such that for all rational numbers $p/q$

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C(\alpha)}{q^d}$$

## Approximation exponent

### Definition

Consider the property:
Let $\alpha \in \overline{K}, d = [K(\alpha) : K]$, and let $v \in M_K$ be an absolute value on $K$ that has been extended to $K(\alpha)$. Then, for any constant $C$ there exist only finitely many $x \in K$ satisfying the inequality:

$$|x - \alpha|_v < \frac{C}{H_K(x)^{\tau(d)}}$$

$K$ is said to have approximation exponent $\tau$ if it has the above property.

### Progress Report

- Liouville, $1851$: $\tau(d) = d + \epsilon$ is an approximation exponent for every $\epsilon > 0$
- Thue, $1909$: $\tau(d) = d/2 + 1 + \epsilon$ for every $\epsilon > 0$
- Siegel, $1921$: $\tau(d) = 2\sqrt{d} + \epsilon$ for every $\epsilon > 0$
- Gelfond, Dyson, $1947$: $\tau(d) = \sqrt{2d} + \epsilon$ for every $\epsilon > 0$
- Roth, $1955$: $\tau(d) = 2 + \epsilon$ for every $\epsilon > 0$

## Diophantine approximation applied to estimate integral points

Consider the Pell equation

$$x^3 - 2y^3 = a$$

with solutions $(x, y) \in \mathbb{Z}^2$, and $a \in \mathbb{Z}$. Suppose $(x, y)$ is a solution and $y \neq 0$, and $\omega$ is a primitive $3$-rd root of unity. Now, if we factor the equation as

$$\left(\frac{x}{y} - \sqrt[3]{2}\right)\left(\frac{x}{y} - \sqrt[3]{2}\omega\right)\left(\frac{x}{y} - \sqrt[3]{2}\omega^2\right) = \frac{a}{y^3}$$

Since $\omega^j \sqrt[3]{2}, j = 1, 2$ is not real, therefore the two terms on the right in the product is bounded away from $0$, and thus we have the estimate

$$\left(\frac{x}{y} - \sqrt[3]{2}\right) \leq \frac{C}{y^3}$$

for some constant $C$ independent of $x, y$. Now, using Roth's theorem or even Thue, we can conclude that there are only finitely many integral solutions to the Pell equation.

# Distance Functions

## Definition

Let $C/K$ be a curve, let $v \in M_K$, and fix a point $Q \in C(K_v)$. Choose a function $t_Q \in K_v(C)$ that has a zero of order $e \geq 1$ at $Q$ and no other zeros. Then, for $P \in C(K_v)$, we define the $v$-adic distance from $P$ to $Q$ by

$$d_v(P, Q) = \min\left\{|t_Q(P)|_v^{1/e}, 1\right\}$$

(If $t_Q$ has a pole at $P$, we formally set $|t_Q(P)| = \infty$, so $d_v(P, Q) = 1$)

## Proposition

Let $Q \in C(K_v)$ and let $f \in K_v(C)$ be a function that vanishes at $Q$. Then, the limit

$$\lim_{P \in C(K_v), P \xrightarrow{v} Q} \frac{\log |f(P)|_v}{\log d_v(P, Q)} = \mathrm{ord}_Q(f)$$

exists and is independent of the choice of the function $t_Q$ used to define $d_v(P, Q)$.

# Restatement of Roth's theorem

## Proposition

Let $C_1/K$ and $C_2/K$ be two curves, and let $\phi : C_1 \to C_2$ be a finite map defined over $K$. Let $Q \in C_1(K_v)$ and let $e_\phi(Q)$ be the ramification index of $\phi$ at $Q$. Then,

$$\lim_{P \in C_1(K_v), P \xrightarrow{v} Q} \frac{\log d_v(\phi(P), \phi(Q))}{\log d_v(P, Q)} = e_\phi(Q)$$

Now, we can interpret Roth's theorem in terms of distance functions.

## Corollary

Fix an absolute value $v \in M_K$. Let $C/K$ be a curve, let $f \in K(C)$ be a non-constant function, and let $Q \in C(\overline{K})$. Then,

$$\liminf_{P \in C(K), P \xrightarrow{v} Q} \frac{\log d_v(P, Q)}{\log H_K(f(P))} \geq -2$$

# Siegel's theorem

## Lemma

Let $E/K$ be an elliptic curve with $\#E(K) = \infty$. Fix a point $P \in E(\overline{K})$, a non-constant even function $f \in E(K)$, and an absolute value $v \in M_{K(Q)}$. Then,

$$\lim_{P \in C(K_v), P \xrightarrow{v} Q} \frac{\log d_v(P, Q)}{\log h_f(P)} = 0$$

## Siegel's Theorem

Let $E/K$ be an elliptic curve with Weierstrass coordinate function $x, y$, let $S \subseteq M_K$ be a finite set of places of $K$ containing $M_K^\infty$. If $\mathbb{Z}_S$ is the set of $S$-integers of $K$, then

$$\{P \in E(K) : x(P) \in \mathbb{Z}_S\}$$

is finite.

## Proof of Siegel's theorem

1. We wish to apply the lemma to $f = x$.
2. Suppose there is a sequence of points $P_i \in E(K)$ such that $x(P_i) \in \mathbb{Z}_S$
3. $h_x(P_i) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S} \log \max\{1, |x(P_i)|_v^{n_v}\}$ since for $v \notin S$, we have $|x(P_i)|_v \leq 1$.
4. In particular, we can find a subsequence of points $P_i$ (relabel if necessary) such that $h_x(P_i) \leq \#S \cdot \log |x(P_i)|_v$ (note that $n_v \leq [K:\mathbb{Q}]$)
5. This allows us to conclude that $|x(P_i)|_v \to \infty$, and since $O$ is the only pole of $x$, we can conclude that $d_v(P_i, O) \to \infty$
6. The function $x$ has a pole of order $2$ and no other poles, so we may take our distance function to be $d_v(P_i, O) = \min\{|x(P_i)|_v^{-1/2}, 1\}$
7. Then, for sufficiently large $i$, we have
$$-\frac{\log d_v(P_i, O)}{h_x(P_i)} \geq \frac{1}{2\#S}$$
8. This contradicts our lemma, which says that the LHS goes to $0$ as $i$ goes to infinity.

# Corollary of Siegel theorem

**Corollary**

Let $C/K$ be a curve of genus one, let $f \in K(C)$ be a non-constant function, and let $S$ and $\mathbb{Z}_S$ be as defined before. Then,

$$\{P \in C(K) : f(P) \in \mathbb{Z}_S\}$$

is a finite set.

## Application

Consider the Diophantine equation

$$y^2 = x^3 + Ax + B$$

where $A, B \in \mathbb{Z}$ and $4A^3 + 27B^2 \neq 0$. Suppose there are infinitely many rational points $P_1, P_2, \ldots \in E(K)$ (reorder them if necessary so that they are in order of non-decreasing height of $x$-coordinate) and write

$$x(P_i) = a_i/b_i$$

in lowest terms. Take a subsequence $P_{i_j}$ of integral points, then $|a_{i_j}| \geq |b_{i_j}| = 1$.
The function $x$ has pole of order $2$ at $O$. Therefore, $x^{-1}$ must have zero of order $2$ at $O$.

## Application contd..

Take $Q = O$ in our distance formula to obtain

$$\begin{aligned}\log d_v(P_{i_j}, O) &= \log \min\{|x(P_{i_j})|^{-1/2}, 1\} \\ &= \frac{1}{2}\log \min\left\{\frac{1}{|a_{i_j}|}\right\} \\ &= -\frac{1}{2}\log |a_{i_j}|\end{aligned}$$

But, by definition $h_x(P_{i_j}) = \log \max\{|a_{i_j}|, 1\} = \log |a_{i_j}|$. Therefore, $\log d_v(P_{i_j}, O)/h_x(P_{i_j}) \to -1/2$ as $j \to \infty$. This is a contradiction to our lemma. Hence, proved.

## Quantitative Siegel's theorem

Siegel's theorem is not effective! A conjecture of Serge Lang tries to study the relationship between the number of integral points and rank of the Mordell-Weil group:

**Conjecture [Lang]**

Let $E/K$ be an elliptic curve, and choose a quasiminimal Weierstrass equation for $E/K$,

$$E : y^2 = x^3 + Ax + B$$

Let $S \subseteq M_K$ be a finite set of places of $M_K$ containing the infinite places, and $\mathbb{Z}_S$ the set of $S$-integers of $K$. There exists a constant $C$, depending only on $K$, such that

$$\#\{P \in E(K) : x(P) \in \mathbb{Z}_S\} \leq C^{\#S + \operatorname{rank} E(K)}$$

# Lang's conjecture in specific cases

The conjecture of Lang is known to be true in case of elliptic curves with integral $j$-invariant. More generally,

**Theorem [Silverman]**

There is a constant $C$ depending only on $[K:\mathbb{Q}]$ and on the number of places $v \in M_k^0$ with $\mathrm{ord}_v(j_E) < 0$, such that

$$\#\{P \in E(K) : x(P) \in \mathbb{Z}_S\} \leq C^{\#S + \mathrm{rank} E(K)}$$

**Theorem [Hindry-Silverman]**

Assume that the ABC conjecture is true for the field $K$. Then, there is a constant $C$, depending only on $[K:\mathbb{Q}]$ and the constants appearing in the ABC conjecture, such that

$$\#\{P \in E(K) : x(P) \in \mathbb{Z}_S\} \leq C^{\#S + \mathrm{rank} E(K)}$$

## $S$-unit equation

The second idea is to reduce the problem of finding $S$-integral points on a curve to the problem of solving several equations of the form

$$ax + by = 1$$

in $S$-units

**Lemma**

Let $S \subseteq M_K$ be a finite set of places, and let $a, b \in K^\times$. Then, the equation

$$ax + by = 1$$

has only finitely many solutions in $S$-units $x, y \in \mathbb{Z}_S^\times$.

The proof of the lemma is ineffective because it uses Roth theorem, however it is indeed possible to make it *quantitative*, i.e., to give an upper bound on the number of solutions as in Lang's conjecture.

# Siegel's second theorem

**Theorem [Evertse]**

Let $S \subseteq M_K$ be a finite set of places containing $M_K^\infty$, and let $a, b \in K^\times$. Then, the equation

$$ax + by = 1$$

has atmost $3 \times 7^{[K:\mathbb{Q}]+2\#S}$ solutions in $S$-units $x, y \in \mathbb{Z}_S^\times$.

**Theorem [Siegel]**

Let $f(x) \in K[x]$ be a polynomial of degree $d \geq 3$ with distinct roots in $\overline{K}$. Then, the equation

$$y^2 = f(x)$$

has only finitely many solutions in $\mathbb{Z}_S$.

## Proof

1. Enlarging $K$ and $S$ clearly proves something stronger. So, we may assume that $f(x)$ splits over $K$, as

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$$

   with $\alpha_i \in K$
2. Enlarge $S$ so that
   2.1 $a \in \mathbb{Z}_S^\times$
   2.2 $\alpha_i - \alpha_j \in \mathbb{Z}_S^\times$ for $i \neq j$
   2.3 $\mathbb{Z}_S$ is a PID
3. Take a field extension $L/K$ obtained by adjoining to $K$ the square root of every element in $\mathbb{Z}_S^\times$. This is a finite extension by Dirichlet's $S$-unit theorem.
4. Let $T$ be the set of places of $L$ lying above $S$ and $\mathbb{Z}_T$ the corresponding set of integers.
5. Let $(x, y) \in \mathbb{Z}_S$ be a solution of $y^2 = f(x)$. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_S$. Then, $\mathfrak{p}$ divides atmost one $x - \alpha_i$. And, $\mathfrak{p}$ does not divide $a$.

## Proof contd..

6. It follows from the equation

$$y^2 = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_d)$$

that $\operatorname{ord}_{\mathfrak{p}}(x-\alpha_i)$ is even. Therefore, there are ideals $\mathfrak{a}_i$ such that

$$(x-\alpha_i)\mathbb{Z}_S = \mathfrak{a}_i^2$$

7. Since $\mathbb{Z}_S$ is a PID, therefore there is a $z_i \in \mathbb{Z}_S$ such that $\mathfrak{a}_i = z_i\mathbb{Z}_S$. Hence, there are units $u_i \in \mathbb{Z}_S^\times$ such that

$$x-\alpha_i = u_i z_i^2$$

8. In the extension $L$, $u_i$ is a square, so $u_i = v_i^2$ and thus

$$x-\alpha_i = (w_i := v_i z_i)^2$$

9. Taking the difference gives us

$$\alpha_i - \alpha_j = w_i^2 - w_j^2 = (w_i + w_j)(w_i - w_j)$$

10. Since $\alpha_i - \alpha_j$ is an unit, the two terms in the RHS of the product must be units as well.

## Proof contd..

11. Now, we use Siegel's identity:

$$\frac{w_1 + w_2}{w_1 - w_3} - \frac{w_2 + w_3}{w_1 - w_3} = 1$$

There are only finitely many values for the above equation and similarly, there are only finitely many values for the equation

$$\frac{w_1 - w_2}{w_1 - w_3} + \frac{w_2 - w_3}{w_1 - w_3} = 1$$

12. The above allows us to conclude that there are only finitely many values for the equation

$$\frac{w_1 + w_2}{w_1 - w_3} \times \frac{w_1 + w_2}{w_1 - w_3} = \frac{w_1^2 - w_2^2}{(w_1 - w_3)^2} = \frac{\alpha_2 - \alpha_1}{(w_1 - w_3)^2}$$

Therefore, there are only finitely many values for $w_1 - w_3$.

## Proof contd..

13. Hence, finitely many solutions

$$\frac{1}{2}\left((w_1 - w_3) + \frac{\alpha_3 - \alpha_1}{w_1 - w_3}\right) = w_1$$

14. But, $x = \alpha_1 + w_1^2$. Thus, there are only finitely many values of $x$, and each $x$ value gives at most two values of $y$. This completes the proof.

## Classical results

**Theorem [Gelfond-Schneider]**

Let $\alpha, \beta \in \overline{\mathbb{Q}}$ with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$. Then, $\alpha^\beta$ is transcendental.

**Theorem [Baker]**

Let $\alpha_1, \ldots, \alpha_n \in K^\times$, and let $\beta_1, \ldots, \beta_n \in K$. For any constant $\kappa$, define

$$\tau(\kappa) = \tau(\kappa; \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n) = h([1, \beta_1, \ldots, \beta_n])h([1, \alpha_1, \ldots, \alpha_n])^\kappa$$

The heights are logarithmic heights. Fix an embedding $K \hookrightarrow \mathbb{C}$ and let $|\cdot|$ be the corresponding absolute value. Assume that

$$\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0$$

Then, there are effectively computable constants $C > 0, \kappa > 0$, depending only on $n$ and $[K : \mathbb{Q}]$, such that

$$|\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n| > C^{-\tau(\kappa)}$$

## Effective methods using Baker's theorem

Now, we can give an *effective* bound on the $S$-unit equation in the following theorem:

**Theorem**

Fix $a, b \in K^{\times}$. There exists an effectively computable constant $C = C(K, S, a, b)$ such that any solution $(\alpha, \beta) \in \mathbb{Z}_S^{\times} \times \mathbb{Z}_S^{\times}$ to the $S$-unit equation

$$a\alpha + b\beta = 1$$

satisfies $H(\alpha) < C$.

**Lemma**

Let $V$ be a finite dimensional vector space over $\mathbb{R}$. Given any basis $\mathbf{e}$ for $V$, let

$$||x||_e = ||\sum x_i e_i||_e = \max\{|x_i|\}$$

If $\mathbf{f}$ is another basis for $V$, then there are positive constants $c_1, c_2$ depending on $\mathbf{e}, \mathbf{f}$ such that for all $v \in V$,

$$c_1||x||_e \leq ||x||_f \leq c_2||x||_e$$

## Preliminaries

Now, let $S \subseteq M_K$ be a finite set of places of $M_K$ containing $M_K^\infty$. Let $s = \#S$, and choose a basis $\alpha_1, \ldots, \alpha_{s-1}$ for the free part of $\mathbb{Z}_S^\times$. Then, every $\alpha \in \mathbb{Z}_S^\times$ can be written as

$$\alpha = \zeta \cdot \alpha_1^{m_1} \cdots \alpha_{s-1}^{m_{s-1}}$$

with $m_i \in \mathbb{Z}$ and $\zeta$ a root of unity. Define the size of $\alpha$ relative to the basis by

$$m(\alpha) := \max\{|m_i|\}$$

**Lemma**

With the notations as before, there are positive constants $c_1, c_2$ depending on $K, S$ such that for all $v \in V$,

$$c_1 h(\alpha) \leq m(\alpha) \leq c_2 h(\alpha)$$

## Explicit bounds on the solutions

**Theorem [Baker]**

Let $A, B, C, D \in \mathbb{Z}$ satisfy $\max\{|A|, |B|, |C|, |D|\} \leq H$ and assume that

$$E : Y^2 = AX^3 + BX^2 + CX + D$$

is an elliptic curve. Then, any point $P = (x, y) \in E(\mathbb{Q})$ with $x, y \in \mathbb{Z}$ satisfies

$$\max\{|x|, |y|\} < \exp((10^6 H)^{10^6})$$

**Theorem [Baker-Coates]**

Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be an absolutely irreducible polynomial such that the curve $F(X, Y) = 0$ has genus one. Let $n$ be the degree of $F$, and assume that the coefficients of $F$ all have absolute value at most $H$. Then, any solution to $F(x, y) = 0$ with $x, y \in \mathbb{Z}$ satisfies

$$\max\{|x|, |y|\} < \exp\exp((2H)^{10^{n^{10}}})$$

# Šafarevič theorem

## Šafarevič

Let $S \subseteq M_K$ be a finite set of places containing $M_K^\infty$. Then, upto isomorphism over $K$, there are only finitely many elliptic curves $E/K$ having good reduction at all primes not in $S$.

## Corollary

Fix an elliptic curve $E/K$. Then, there are only finitely many elliptic curves $E'/K$ that are $K$-isogenous to $E$.

## Proof.

By Criterion of Néron-Ogg-Šafarevič, we have the corollary: If $E_1/K, E_2/K$ are elliptic curves that are isogenous over $K$, then $E_1$ has good reduction over $K$ iff $E_2$ has good reduction over $K$. Now, if $E, E'$ are isogenous, then they have the same set of primes of bad reduction. The result now follows from application of Šafarevič's theorem. □

# Corollary of Serre

**Corollary [Serre]**

Let $E/K$ be an elliptic curve with no complex multiplication. Then, for all but finitely many primes $\ell$, the group of $\ell$-torsion points $E[\ell]$ has no nontrivial $\mathrm{Gal}(\overline{K}/K)$-invariant subgroups.

**Remark**

This just means that the representation of $\mathrm{Gal}(\overline{K}/K)$ on $E[\ell]$ is irreducible.

## Over!

Thank you! Available for questions.

# References I

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry: an introduction*. Graduate texts in mathematics 201. New York: Springer, 2000. ISBN: 9780387989754 9780387989815.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. 2nd ed. Graduate texts in mathematics 106. New York, NY: Springer, 2009. ISBN: 9780387094939.