Linear forms in logarithms and integral points on varieties

Aaron Levin

Michigan State University

Second Annual Upstate Number Theory Conference

Faltings' and Siegel's Theorem

Diophantine Equations

- Basic object of interest: The set of solutions to a system of polynomial equations over a number field k,

$$f_1(x_1,\ldots,x_n) = 0,$$
$$\vdots$$
$$f_m(x_1,\ldots,x_n) = 0,$$

  where the solutions are taken in one of the following rings:
  - $x_1,\ldots,x_n \in k$ (rational solutions)
  - $x_1,\ldots,x_n \in \mathcal{O}_k$, the ring of integers of k (integral solutions)
  - More generally, $x_1,\ldots,x_n \in \mathcal{O}_{k,S}$, the ring of S-integers (S-integral solutions).
- Geometric viewpoint: The system of polynomial equations defines a geometric object in affine space or projective space (if the polynomials are homogeneous).

- Philosophy: Geometry determines arithmetic.
- Let $X \subset \mathbb{A}^n$ be an affine variety over a number field k. Then we're interested in the set of (S-)integral points

$$X(\mathcal{O}_{k,S}) = \{(x_1, \ldots, x_n) \in X \mid x_1, \ldots, x_n \in \mathcal{O}_{k,S}\}.$$

- Note: This set depends not just on X, but on the embedding of X in $\mathbb{A}^n$.
- Similarly, we can study the set of rational points $X(k)$.

Faltings' Theorem

- If $X = C$ is a nonsingular projective curve, there is a fundamental geometric invariant: the genus. This is the number of "holes" in the corresponding Riemann surface.
- For curves, this single invariant, the genus, controls the qualitative behavior of rational points.

Theorem (Faltings, formerly the Mordell Conjecture)

Let C be a curve defined over a number field k. If the (geometric) genus g of C satisfies $g \geq 2$ then $C(k)$ is finite.

- Conversely, curves of genus 0 and genus 1 may have infinitely many rational points (rational and elliptic curves).

Siegel's Theorem

- For affine curves, there is an additional geometric invariant: the number of points of the curve “at infinity"
- The fundamental finiteness result for integral points on affine curves is the 1929 theorem of Siegel.

Theorem (Siegel)

Let $C \subset \mathbb{A}^n$ be an affine curve defined over k. Let $\tilde{C}$ be a projective closure of C. If either

- *$\tilde{C}$ has positive genus*

or

- *C is rational with more than two points at infinity ($\#\tilde{C} \setminus C \geq 3$)*

then the set of integral points $C(\mathcal{O}_{k,S})$ is finite (for any S).

- The hypothesis that $\#\tilde{C} \setminus C \geq 3$ when C is rational is necessary.

An example

- Consider the rational affine curve C defined by $x^2 - 3y^2 = 1$.
- We have $C \subset \widetilde{C}$, where $\widetilde{C}$ is the projective plane curve $\widetilde{C} : x^2 - 3y^2 = z^2$.
- The points at infinity $\widetilde{C} \setminus C$ correspond to the points on $\widetilde{C}$ with $z = 0$. There are two such points $[x : y : z] = [\pm\sqrt{3} : 1 : 0]$.
- So Siegel's theorem does not apply.
- C does in fact have infinitely many $\mathbb{Z}$-integral points. C is defined by a so-called Pell equation. If $n \in \mathbb{N}$,

$$x + \sqrt{3}y = (2 + \sqrt{3})^n,$$

then (x, y) will be an integral point on C.

Effectivity

- Faltings' theorem and Siegel's theorem both have one major defect: all of the known proofs of these theorems are ineffective.
- No known algorithm which, in general, can provably find the finitely many points in either theorem
- This would typically be done by bounding the height of the points.
- For curves with certain special properties there do exist effective techniques for finding the finitely many rational/integral points.

Linear Forms in Logarithms

Baker's theorem

- By far, the most powerful and widely used effective technique for integral points comes from Baker's theory of linear forms in logarithms.

Theorem (Baker)

Let $\alpha_1, \ldots, \alpha_m$ be nonzero algebraic numbers, $b_1, \ldots, b_m$ integers, and $\epsilon > 0$. Suppose that

$$0 < |b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m| < e^{-\epsilon B},$$

where $B = \max\{|b_1|, \ldots, |b_m|\}$. Then $B \leq B_0$, where B_0 is an effectively computable constant depending on $\alpha_1, \ldots, \alpha_m, \epsilon$.

- In fact, one can replace $e^{-\epsilon B}$ on the right-hand side by B^{-C} for some effective constant C.

Alternative formulations

- An alternative formulation avoiding logarithms and with arbitrary absolute values (van der Poorten, Yu) is the following:

Theorem

Let $\alpha_1, \dots, \alpha_m$ be algebraic numbers, $b_1, \dots, b_m$ integers, and $\epsilon > 0$. Let v be a place of k. Suppose that

$$0 < |\alpha_1^{b_1} \cdots \alpha_m^{b_m} - 1|_v < e^{-\epsilon B},$$

where $B = \max\{|b_1|, \dots, |b_m|\}$. Then $B \leq B_0$, where B_0 is an effectively computable constant depending on $\alpha_1, \dots, \alpha_m, v, \epsilon$.

Heights

- Denote the absolute logarithmic height by $h(x)$.
- Recall that for a rational number $\frac{a}{b} \in \mathbb{Q}$, $(a, b) = 1$, the height is given by

$$h\left(\frac{a}{b}\right) = \log \max\{|a|, |b|\}.$$

- We can also define local heights. For k a number field, $\alpha \in k$, and v a place of k, define the local height (or local Weil function) with respect to α by

$$h_{\alpha,v}(x) = \frac{[k_v : \mathbb{Q}_v]}{[k : \mathbb{Q}]} \log \frac{\max\{|x|_v, 1\}}{|x - \alpha|_v}, \quad \forall x \in k, x \neq \alpha.$$

- This measures how v-adically close x is to α (being large when x is close to α).

Height formulation

- In terms of heights, we can reformulate Baker's theorem as

Theorem

Let k be a number field, S a finite set of places of k containing the archimedean places, $v \in S$, $\alpha \in k^*$, and $\epsilon > 0$. Then there exists an effective constant C such that

$$h_{\alpha,v}(x) \leq \epsilon h(x) + C$$

for all $x \in \mathcal{O}_{k,S}^*$, $x \neq \alpha$.

Applications to curves

- Baker's method allows one to effectively solve, for instance, the following:
  - The S-unit equation: for fixed $a, b, c \in k^*$,

$$au + bv = c, \quad u, v \in \mathcal{O}_{k,S}^*.$$

  - The Thue-Mahler equation:

$$F(x, y) \in \mathcal{O}_{k,S}^*, \quad x, y \in \mathcal{O}_{k,S},$$

    where $F(x, y) \in k[x, y]$ is a binary form such that $F(x, 1)$ has at least 3 distinct roots in $\bar{k}$.
  - The hyperelliptic equation:

$$y^2 = f(x), \qquad x, y \in \mathcal{O}_{k,S},$$

    where $f(x) \in k[x]$ has no repeated roots and degree ≥ 3.
- All of these equations correspond to integral points on certain curves (e.g., the unit equation corresponds to integral points on $\mathbb{P}^1$ minus three points).

Effective Results in Higher Dimensions

The general unit equation

- The (two-variable) unit equation can be generalized to sums of more units:

Theorem (Evertse, van der Poorten and Schlickewei)

All but finitely many solutions of the equation

$$a_0u_0 + a_1u_1 + \ldots + a_nu_n = a_{n+1} \quad \text{in } u_0, \ldots, u_n \in \mathcal{O}_{k,S}^*,$$

where $a_0, \ldots, a_{n+1} \in k^*$, satisfy an equation of the form $\sum_{i \in I} a_iu_i = 0$, where $I \subset \{0, \ldots, n\}$.

- Solutions to this equation yield integral points on $\mathbb{P}^n$ minus $n+2$ hyperplanes in general position (the coordinate hyperplanes and the hyperplane $a_0x_0 + \cdots + a_nx_n = 0$).
- For $n \geq 2$, the proofs of the theorem aren't effective.
- There is a bound for the number of nondegenerate solutions, however, and this bound depends only on $|S|$ and n!

Vojta's Theorem

- In his thesis, Vojta proved:

Theorem (Vojta)

Let k be a number field and S a finite set of places of k containing the archimedean places. Suppose that $|S| \leq 3$. Let $a_1, a_2, a_3, a_4 \in k^*$. Then there exists an effectively computable constant C such that every solution to

$$a_1 u_1 + a_2 u_2 + a_3 u_3 = a_4, \quad u_1, u_2, u_3 \in \mathcal{O}_{k,S}^*$$

with $a_i u_i + a_j u_j \neq 0$, $1 \leq i < j \leq 3$, satisfies $h(u_i) \leq C$, $i = 1, 2, 3$.

- If $p, q \in \mathbb{Z}$ are fixed primes, an example ($k = \mathbb{Q}, S = \{\infty, p, q\}$) of such an equation is

$$p^x q^y - p^z - q^w = 1, \quad w, x, y, z \in \mathbb{Z}.$$

The projective plane

- Versions of this result were subsequently rediscovered by Skinner and by Mo and Tijdeman.
- Geometrically: S-integral points on $\mathbb{P}^2 \setminus 4$ lines in general position, $|S| < 4$. Here is a generalization:

Theorem (L.)

Let $C_1, \ldots, C_r$ be distinct curves in $\mathbb{P}^2$, defined over a number field k. Let S a finite set of places of k containing the archimedean places. Suppose that

1. *For any point $P \in \mathbb{P}^2(\bar{k})$ there are at least two curves C_i, C_j, not containing P.*
2. $|S| < r$.

Take an affine embedding of $X = \mathbb{P}^2 \setminus \cup_{i=1}^r C_i$ in some $\mathbb{A}^N$. Then the set of S-integral points $X(\mathcal{O}_{k,S}) \subset \mathbb{A}^N(\mathcal{O}_{k,S})$ is contained in an effectively computable finite union of curves in $\mathbb{P}^2$.

Higher Dimensions

Theorem (L.)

Let $D_1, \dots, D_r$ be distinct hypersurfaces in $\mathbb{P}^n$, defined over a number field k. Let m be a positive integer. Suppose that

1. *The intersection of any m distinct hypersurfaces D_i consists of a finite number of points.*
2. *For any point $P \in \mathbb{P}^n(\bar{k})$ there are at least two hypersurfaces D_i, D_j, not containing P.*
3. $(m-1)|S| < r$.

Take an affine embedding of $X = \mathbb{P}^n \setminus \cup_{i=1}^r D_i$ in some $\mathbb{A}^N$. Then the set of S-integral points $X(\mathcal{O}_{k,S}) \subset \mathbb{A}^N(\mathcal{O}_{k,S})$ is contained in an effectively computable proper closed subset of X.

- More generally: effective result for integral points on $V \setminus \cup \operatorname{Supp} D_i$, where V is a projective variety and the D_i are effective divisors that have linearly equivalent multiples.

An application

Corollary

Let $f \in k[x, y]$ be a polynomial of degree d such that $f(0, 0) \neq 0$ and x^d and y^d appear nontrivially in f. Let S be a finite set of places of k containing the archimedean places with $|S| \leq 3$. Then the set of solutions to

$$f(u, v) = w, \quad u, v, w \in \mathcal{O}_{k,S}^*,$$

can be effectively determined.

- This corresponds to applying the theorem to three lines in $\mathbb{P}^2$ ($x = 0, y = 0, z = 0$) and the curve defined by $f(x, y) = 0$. The conditions on $f(x, y)$ are equivalent to a general position assumption on the lines and the curve.
- Taking linear functions of the form $f(x, y) = a_1 x + a_2 y + a_3$, $a_1, a_2, a_3 \in k^*$, yields Vojta's effective unit theorem.

Another application

Corollary

Let S be a finite set of places of a number field k containing the archimedean places with $|S| \leq 3$. Let $a, b, c, d \in k^*$. Then the set of solutions to

$$auv + bu + cv + d = w, \quad u, v, w \in \mathcal{O}_{k,S}^*,$$

with $u \notin \{-\frac{d}{b}, -\frac{c}{a}\}$, $v \notin \{-\frac{d}{c}, -\frac{b}{a}\}$, is finite and effectively computable.

- This case wasn't covered by the last corollary. For this, one looks at integral points on

$$\mathbb{P}^1 \times \mathbb{P}^1 \setminus \{x_1x_2y_1y_2(ax_1x_2 + bx_1y_2 + cy_1x_2 + dy_1y_2) = 0\},$$

where the coordinates are $(x_1, y_1) \times (x_2, y_2)$.

Runge's method

Runge's method

- An old (1887) result of Runge proves the effective finiteness of the set of integral points on certain affine curves.
- Here's a modern formulation:

Theorem

Let k be a number field and S a set of places of k containing the archimedean places. Let $C \subset \mathbb{A}^n$ be an affine curve over k and $\tilde{C}$ a projective closure of C. Suppose that $\tilde{C} \setminus C$ contains r irreducible components over k. If $|S| < r$ then $C(\mathcal{O}_{k,S})$ is finite and effectively computable.

- Remarkably, Bombieri showed that one could prove a uniform version of Runge's theorem, allowing the number field k and set of places S to vary: $\cup_{k,|S|<r} C(\mathcal{O}_{k,S})$ is finite.

Runge's method in higher dimensions

- Generalized to higher dimensions appropriately, Runge's method gives:

Theorem (L.)

Let $\tilde{X}$ be a nonsingular projective variety and $D = \sum_{i=1}^{r} D_i$ a sum of ample effective divisors on X defined over k. Let m be a positive integer and S a finite set of places of k containing the archimedean places. Suppose that

1. *The intersection of the supports of any $m+1$ distinct divisors D_i is empty.*
2. $m|S| < r$

If $X = \widetilde{X} \setminus D \subset \mathbb{A}^n$ then the set of integral points $X(\mathcal{O}_{k,S})$ is finite and effectively computable.

Comparison with Runge's method

- A quick comparison of the higher-dimensional Runge theorem with higher-dimensional results based on Baker's theorem.
- Runge's method:
  - No linear equivalence requirement.
  - Effective bounds much smaller.
  - Result is actually *uniform* in $|S|$ (finiteness even as S and k vary, subject to the key inequality $m|S| < r$).
- Our main theorem:
  - Weak intersection condition (especially on surfaces).
  - Needed inequality on $|S|$ is superior.

Proofs

Result on the projective plane

Theorem

Let $C_1, \ldots, C_r$ be distinct curves in $\mathbb{P}^2$, defined over a number field k. Let S a finite set of places of k containing the archimedean places. Suppose that

1. *For any point $P \in \mathbb{P}^2(\bar{k})$ there are at least two curves C_i, C_j, not containing P.*
2. $|S| < r$.

Take an affine embedding of $X = \mathbb{P}^2 \setminus \cup_{i=1}^r C_i$ in some $\mathbb{A}^N$. Then the set of S-integral points $X(\mathcal{O}_{k,S}) \subset \mathbb{A}^N(\mathcal{O}_{k,S})$ is contained in an effectively computable finite union of curves in $\mathbb{P}^2$.

Using the pigeonhole principle

- Throughout, the implicit constant in $O(1)$ will always be an effective constant.

Proof.

Let $d_i = \deg C_i$. We have

$$\sum_{v \in S} h_{C_i,v}(P) = d_i h(P) + O(1), \quad i = 1, \ldots, r,$$

for all $P \in X(\mathcal{O}_{k,S})$, where $h_{C_i,v}$ is a local Weil function for C. Let $P \in X(\mathcal{O}_{k,S})$. Then for each i, there exists a place $v \in S$ such that $h_{C_i,v}(P) \geq \frac{1}{|S|} h(P) + O(1)$. Since $|S| < r$, there exists a place $v \in S$ and distinct elements $i, j \in \{1, \ldots, r\}$ such that

$$\min\{h_{C_i,v}(P), h_{C_j,v}(P)\} \geq \frac{1}{|S|} h(P) + O(1).$$

$\square$

A Lemma

- The theorem is then a consequence of the following lemma.

Lemma

Let k be a number field and let $C_1, \ldots, C_r \subset \mathbb{P}^2$, $r \geq 4$, be distinct curves over k such that at most $r-2$ of the curves C_i intersect at any point of $\mathbb{P}^2(\bar{k})$. Let S be a finite set of places of k containing the archimedean places. Let $\epsilon > 0$, $i, j \in \{1, \ldots, r\}$, $i \neq j$, and $v \in S$. Let $X = \mathbb{P}^2 \setminus \cup_{i=1}^r C_i \subset \mathbb{A}^n$. Then the set of points

$$\{P \in X(\mathcal{O}_{k,S}) \mid \min\{h_{C_i,v}(P), h_{C_j,v}(P)\} > \epsilon h(P)\}$$

is effectively computable.

- Local heights associated to closed subschemes (Silverman):
- Let Y and Z be closed subschemes of a projective variety X.
- To Y and Z we can associate local heights $h_{Y,v}$, $h_{Z,v}$, $v \in M_k$, such that (up to $O(1)$):
    - If Y and Z are (Cartier) divisors on X then the local heights are the usual ones.
    - We have the following properties:

$$\begin{aligned} h_{Y\cap Z,v} &= \min\{h_{Y,v}, h_{Z,v}\} \\ h_{Y+Z,v} &= h_{Y,v} + h_{Z,v} \\ h_{Y,v} &\leq h_{Z,v}, \quad \text{if } Y \subset Z. \end{aligned}$$

    - If $\phi : W \to X$ is a morphism, $Y \subset X$, then

$$h_{Y,v}(\phi(P)) = h_{\phi^* Y,v}(P), \quad \forall P \in W(k).$$

Proof of the Lemma

Proof of the lemma.

By extending k and enlarging S, we easily reduce to the case where every point in $C_i \cap C_j$ is k-rational.

We have

$$\min\{h_{C_i,v}(P), h_{C_j,v}(P)\} = h_{C_i \cap C_j,v}(P).$$

Let N be an integer such that $C_i \cap C_j \subset N\,\mathrm{Supp}(C_i \cap C_j)$. Then

$$\begin{aligned} h_{C_i \cap C_j,v}(P) &\leq h_{N\,\mathrm{Supp}(C_i \cap C_j),v}(P) + O(1) \\ &\leq N \sum_{Q \in (C_i \cap C_j)(k)} h_{Q,v}(P) + O(1) \end{aligned}$$

for all $P \in \mathbb{P}^2(k) \setminus (C_i \cap C_j)$. $\square$

Proof continued

- The proof is completed using another lemma.

Lemma

Let $Q \in (C_i \cap C_j)(k)$. Let $\epsilon' > 0$. Then

$$h_{Q,v}(P) < \epsilon' h(P) + O(1)$$

for all $P \in X(\mathcal{O}_{k,S}) \setminus Z_Q$, where Z_Q is some effectively computable proper closed subset of $\mathbb{P}^2$.

- Assuming the lemma, we proceed as follows:

Proof.

Summing over all points Q in $C_i \cap C_j$, we obtain

$$\min\{h_{C_i,v}(P), h_{C_j,v}(P)\} \leq N \sum_{Q \in (C_i \cap C_j)} h_{Q,v}(P) + O(1) < \frac{\epsilon}{2} h(P) + C$$

for all $P \in X(\mathcal{O}_{k,S}) \setminus Z$, where $Z = \cup_{Q \in (C_i \cap C_j)(k)} Z_Q$ and C is an effectively computable constant. So if $P \in X(\mathcal{O}_{k,S}) \setminus Z$ satisfies

$$\min\{h_{C_i,v}(P), h_{C_j,v}(P)\} > \epsilon h(P),$$

then $h(P) < \frac{2}{\epsilon} C$. It follows that we have

$$\left\{P \in X(\mathcal{O}_{k,S}) \mid \min\{h_{C_i,v}(P), h_{C_j,v}(P) > \epsilon h(P)\right\}$$
$$\subset Z \cup \left\{P \in \mathbb{P}^2(k) \mid h(P) < \frac{2}{\epsilon} C\right\},$$

and the latter set yields a proper closed subset of X. □

Proof of the final lemma.

Let $Q \in (C_i \cap C_j)(k)$. Then there exists $l, m \in \{1, \ldots, r\}$ such that $Q \notin C_l \cup C_m$. If C_l is defined by $f_l \in k[x, y]$ and C_m by $f_m \in k[x, y]$, let $\phi = \frac{f_l^{d_m}}{f_m^{d_l}}$. So $\operatorname{div}(\phi) = d_m C_l - d_l C_m$. Let $\phi : \mathbb{P}^2 \to \mathbb{P}^1$ also denote the associated rational map. Let $R = \phi(Q)$. Since ϕ has its zeros and poles in $C_l \cup C_m$, without loss of generality, after enlarging S we can assume that $\phi(P) \in \mathcal{O}_{k,S}^*$ for all $P \in X(\mathcal{O}_{k,S})$. Now by Baker's theorem (1st inequality) and properties of heights (note: This isn't technically correct; we should really work on a blow-up of $\mathbb{P}^2$ so that ϕ lifts to a morphism, but nothing really essential changes below).

$$\begin{aligned}
h_{R,v}(\phi(P)) &< \epsilon h(\phi(P)) + O(1), \quad \forall P \in X(\mathcal{O}_{k,S}), \phi(P) \neq R, \\
h_{\phi^* R,v}(P) &< \epsilon h_{\phi^* \infty}(P) + O(1), \quad \forall P \in X(\mathcal{O}_{k,S}), \phi(P) \neq R, \\
h_{Q,v}(P) &< h_{\phi^* R,v}(P) + O(1), \quad \forall P \in X(k), \phi(P) \neq R, \\
\epsilon h_{\phi^* \infty}(P) &< d_l d_m \epsilon h(P) + O(1), \quad \forall P \in X(k).
\end{aligned}$$

Proof.

Combining the above inequalities yields

$$h_{Q,v}(P) < \epsilon h(P) + O(1)$$

for all $P \in X(\mathcal{O}_{k,S})$ with $\phi(P) \neq \phi(Q)$. So in fact Z_Q is just the closure of $\phi^{-1}(Q)$. $\square$