Effective results for Diophantine equations over finitely generated domains

Jan-Hendrik Evertse
Universiteit Leiden

Joint work with Attila Bérczes, Kálmán Győry (Debrecen)

12th Colloquiumfest on Algebra and Logic
9th Polish, Slovak and Czech conference on Number Theory
Ostravice, June 12, 2012

The subject of our lecture

Let A be a *finitely generated domain over* $\mathbb{Z}$, that is a commutative integral domain containing $\mathbb{Z}$ which is finitely generated as a $\mathbb{Z}$-algebra.

We have $A = \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ with the z_i algebraic or transcendental over $\mathbb{Q}$.

We consider certain classes of Diophantine equations with unknowns taken from A.

We are interested in *effective* finiteness results, these are results which imply that the equation has only finitely many solutions and provide a method to determine all solutions in principle.

Thue equations

Let

$$F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in \mathbb{Z}[X,Y]$$

be a *square-free* binary form of degree $n \geq 3$
(i.e., not divisible by $G(X,Y)^2$ for some binary form $G(X,Y) \in \mathbb{Q}[X,Y]$ of positive degree).

Let b be a non-zero integer.

Theorem (Thue, 1909)

The equation

$$F(x,y) = b \quad \textit{in } x, y \in \mathbb{Z}$$

has only finitely many solutions.

Thue's proof is *ineffective*.

Thue equations over finitely generated domains

Theorem (Lang, 1960)

Let A be a finitely generated domain over $\mathbb{Z}$, $F(X,Y) \in A[X,Y]$ a square-free binary form of degree $n \geq 3$ and $b \in A \setminus \{0\}$.

Then the equation

$$F(x,y) = b \quad \text{in } x, y \in A$$

has only finitely many solutions.

This extends work of

Siegel (1921): $A = O_K =$ ring of integers of number field K;

Mahler (1933): $A = \mathbb{Z}_S = \mathbb{Z}[(p_1 \cdots p_t)^{-1}]$ ($S = \{p_1, \ldots, p_t\}$ set of primes)

Parry (1950): $A = O_S = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}]$ ($S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ set of pr. ideals)
(ring of S-integers in number field K)

The proofs of Siegel, Mahler, Parry, Lang are also *ineffective*.

Baker's Theorem

Theorem (A. Baker, 1967/68)

Let $F(X,Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^i \in \mathbb{Z}[X,Y]$ be a square-free binary form of degree $n \geq 3$ and $b \in \mathbb{Z} \setminus \{0\}$. Then for the solutions of

$$F(x,y) = b \quad \text{in } x, y \in \mathbb{Z}$$

we have

$$\max(|x|,|y|) \leq C,$$

where C is an effectively computable number depending only on the coefficients of F and of b and n.

Baker's proof is based on his own lower bounds for linear forms in logarithms of algebraic numbers.

One may take

$$C = \exp\left\{ 10^{30(n+1)} n^{32n} \left(\max_i |a_i| \right)^{2n} \cdot \log|2b| \right\} \quad \text{(Bugeaud, 1998).}$$

Effective Thue's theorem over the S-integers

Let K be an algebraic number field and $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ a finite set of prime ideals of O_K.

Theorem (Kotov, Sprindžuk, 1975)

Let $F \in O_S[X, Y]$ be a square-free binary form of degree $n \geq 3$ and $b \in O_S \setminus \{0\}$. Then the solutions of

$$F(x, y) = b, \quad x, y \in O_S \tag{1}$$

have heights $H(x), H(y) \leq C$, where C is an effectively computable number depending only on K, S, n, the coefficients of F and b.

Effective Thue's theorem over the S-integers

Let K be an algebraic number field and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ a finite set of prime ideals of O_K.

Theorem (Kotov, Sprindžuk, 1975)

Let $F \in O_S[X, Y]$ be a square-free binary form of degree $n \geq 3$ and $b \in O_S \setminus \{0\}$. Then the solutions of

$$F(x, y) = b, \quad x, y \in O_S \tag{1}$$

have heights $H(x), H(y) \leq C$, where C is an effectively computable number depending only on K, S, n, the coefficients of F and b.

Thus, given (suitable representations for) K, S, b and the coefficients of F, one can determine effectively (suitable representations for) the solutions of (1).

C has been made explicit by Kotov & Sprindžuk (1975),…, Győry & Yu (2006).

Extension to finitely generated domains

In 1983/84 Győry extended the result of Kotov and Sprindzŭk to an effective finiteness result for Thue equations

$$F(x, y) = b \quad \text{in } x, y \in A$$

for domains of the shape

$$A = O_K[z_1, \ldots, z_q, y, g^{-1}]$$

where K is a number field, $z_1, \ldots, z_q$ are algebraically independent, y is integral over $O_K[z_1, \ldots, z_q]$, and $g \in O_K[z_1, \ldots, z_q] \setminus \{0\}$.

Aim:

An effective finiteness result for Thue equations over *arbitrary* finitely generated domains over $\mathbb{Z}$.

Representation for finitely generated domains

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be an arbitrary finitely generated domain over $\mathbb{Z}$. The ideal

$$I := \{f \in \mathbb{Z}[X_1, \ldots, X_r] : \ f(z_1, \ldots, z_r) = 0\}$$

is finitely generated, say $I = (f_1, \ldots, f_m)$. Thus,

$$A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m).$$

By a *representative* for $a \in A$, we mean a polynomial $\widetilde{a} \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $a = \widetilde{a}(z_1, \ldots, z_r)$ (or $a = \widetilde{a} \bmod I$).

Representation for finitely generated domains

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be an arbitrary finitely generated domain over $\mathbb{Z}$. The ideal

$$I := \{f \in \mathbb{Z}[X_1, \ldots, X_r] : \, f(z_1, \ldots, z_r) = 0\}$$

is finitely generated, say $I = (f_1, \ldots, f_m)$. Thus,

$$A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m).$$

By a *representative* for $a \in A$, we mean a polynomial $\widetilde{a} \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $a = \widetilde{a}(z_1, \ldots, z_r)$ (or $a = \widetilde{a} \bmod I$).

Remark

A domain, $A \supset \mathbb{Z} \iff$

I prime ideal of $\mathbb{Z}[X_1, \ldots, X_r]$ with $I \cap \mathbb{Z} = (0) \iff$

$f_1, \ldots, f_m$ generate a prime ideal of $\mathbb{Q}[X_1, \ldots, X_r]$ not containing 1.

There are various algorithms to check this for given $f_1, \ldots, f_m$.

The general effective result

Theorem 1 (Bérczes, Győry, E., to appear)

Given $f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_r]$ *such that*

$$A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m) \text{ is a domain with } A \supset \mathbb{Z},$$

and given representatives for $b \in A \setminus \{0\}$ *and for the coefficients of a square-free binary form* $F \in A[X, Y]$ *of degree* ≥ 3*,*

one can effectively determine a list, consisting of one pair of representatives for each solution of

$$F(x, y) = b, \quad x, y \in A.$$

A quantitative result

For $f = \sum_{\mathbf{i}} c_{\mathbf{i}} X_1^{i_1} \cdots X_r^{i_r} \in \mathbb{Z}[X_1, \ldots, X_r]$ define

$$\deg f := \max\{i_1 + \cdots + i_r : c_{\mathbf{i}} \neq 0\} \quad \text{(total degree)},$$
$$h(f) := \log \max |c_{\mathbf{i}}| \quad \text{(logarithmic height)}.$$

Let $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ be a domain with $A \supset \mathbb{Z}$, $F = \sum_{i=0}^{n} a_i X^{n-i} Y^i \in A[X, Y]$ a square-free binary form of degree $n \geq 3$ and $b \in A \setminus \{0\}$. Choose representatives $\widetilde{a}_i$, $\widetilde{b}$ for the a_i and b.

Theorem 2 (Bérczes, Győry, E.)

Suppose that $f_1, \ldots, f_m$, the $\widetilde{a}_i$ and $\widetilde{b}$ have total degrees at most d and logarithmic heights at most h. Then each solution of

$$F(x, y) = b, \quad x, y \in A$$

has representatives $\widetilde{x}$, $\widetilde{y}$ such that

$$\deg(\widetilde{x}), h(\widetilde{x}), \quad \deg(\widetilde{y}), h(\widetilde{y}) \leq \exp\left\{(n!)^3 n^5 (d+2)^{\kappa^r} (h+1)\right\},$$

where κ is an effectively computable absolute constant > 1.

Theorem 2 $\Longrightarrow$ Theorem 1

Let $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ be a domain with $A \supset \mathbb{Z}$, $b \in A \setminus \{0\}$, $F = \sum_{i=0}^{n} a_i X^{n-i} Y^i \in A[X, Y]$ the binary form under consideration, $\widetilde{a}_i, \widetilde{b} \in \mathbb{Z}[X_1, \ldots, X_r]$ the representatives, and $\widetilde{F}(X, Y) = \sum_{i=0}^{n} \widetilde{a}_i X^{n-i} Y^i$.

By Theorem 2, there is an effectively computable number C such that all $x, y \in A$ with $F(x, y) = b$ have representatives $\widetilde{x}, \widetilde{y} \in \mathbb{Z}[X_1, \ldots, X_r]$ of total degrees and logarithmic heights at most C.

Theorem 2 $\Longrightarrow$ Theorem 1

Let $A = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$ be a domain with $A \supset \mathbb{Z}$, $b \in A \setminus \{0\}$, $F = \sum_{i=0}^{n} a_i X^{n-i} Y^i \in A[X, Y]$ the binary form under consideration, $\widetilde{a}_i, \widetilde{b} \in \mathbb{Z}[X_1, \dots, X_r]$ the representatives, and $\widetilde{F}(X, Y) = \sum_{i=0}^{n} \widetilde{a}_i X^{n-i} Y^i$.

By Theorem 2, there is an effectively computable number C such that all $x, y \in A$ with $F(x, y) = b$ have representatives $\widetilde{x}, \widetilde{y} \in \mathbb{Z}[X_1, \dots, X_r]$ of total degrees and logarithmic heights at most C.

There exist algorithms which for given $f_1, \dots, f_m,\ g \in \mathbb{Z}[X_1, \dots, X_r]$ decide whether g belongs to the ideal of $\mathbb{Z}[X_1, \dots, X_r]$ generated by $f_1, \dots, f_m$ (Simmons (1970); Aschenbrenner (2004)).

Theorem 2 $\Longrightarrow$ Theorem 1

Let $A = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$ be a domain with $A \supset \mathbb{Z}$, $b \in A \setminus \{0\}$, $F = \sum_{i=0}^n a_i X^{n-i} Y^i \in A[X, Y]$ the binary form under consideration, $\widetilde{a}_i, \widetilde{b} \in \mathbb{Z}[X_1, \dots, X_r]$ the representatives, and $\widetilde{F}(X, Y) = \sum_{i=0}^n \widetilde{a}_i X^{n-i} Y^i$.

By Theorem 2, there is an effectively computable number C such that all $x, y \in A$ with $F(x, y) = b$ have representatives $\widetilde{x}, \widetilde{y} \in \mathbb{Z}[X_1, \dots, X_r]$ of total degrees and logarithmic heights at most C.

There exist algorithms which for given $f_1, \dots, f_m,\ g \in \mathbb{Z}[X_1, \dots, X_r]$ decide whether g belongs to the ideal of $\mathbb{Z}[X_1, \dots, X_r]$ generated by $f_1, \dots, f_m$ (Simmons (1970); Aschenbrenner (2004)).

Using such an algorithm, check for all polynomials $\widetilde{x}, \widetilde{y} \in \mathbb{Z}[X_1, \dots, X_r]$ of total degrees and logarithmic heights $\leq C$ whether

$$\widetilde{F}(\widetilde{x}, \widetilde{y}) \equiv \widetilde{b} \pmod{(f_1, \dots, f_m)}.$$

From the pairs $(\widetilde{x}, \widetilde{y})$ satisfying this test, select a maximal subset of pairs that are different modulo $(f_1, \dots, f_m)$. $\square$

Hyper/superelliptic equations

Let $f \in \mathbb{Z}[X]$, b a non-zero integer, and m an integer ≥ 2. Consider

$$by^m = f(x) \quad \text{in } x, y \in \mathbb{Z}. \tag{2}$$

Theorem (A. Baker, 1968/69)

Assume that f has no multiple roots, and f has degree ≥ 3 if $m = 2$ and degree ≥ 2 if $m \geq 3$.

Then for each solution $x, y \in \mathbb{Z}$ of (2) we have

$$\max(|x|, |y|) \leq C,$$

where C is an effectively computable number depending on f, b, m.

This effective result has been generalized by Brindza (1989) to equations $by^m = f(x)$ in $x, y \in A$ where A belongs to the restricted class of finitely generated domains considered by Győry.

Hyper/superelliptic equations with varying exponent

Let $f \in \mathbb{Z}[X]$ and b a non-zero integer.

Theorem (Schinzel, Tijdeman, 1976)

Assume that f has no multiple roots and $\deg f \geq 2$. Then there is an effectively computable number C' depending only on f, b such that if

$$m > C'$$

then $by^m = f(x)$ has no solutions $x, y \in \mathbb{Z}$ with $y \neq 0, \pm 1$.

This has been generalized by Végső (1994) to equations $by^m = f(x)$ in $x, y \in A$ where A belongs to the restricted class of finitely generated domains considered by Győry.

Hyper/superelliptic equations over arbitrary finitely generated domains: fixed exponent

Let $A = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$ be a domain containing $\mathbb{Z}$.
Let $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ and $b \in A \setminus \{0\}$.

Choose representatives $\widetilde{a_i}, \widetilde{b}$ for the a_i and b.

Suppose that $f_1, \dots, f_m$, the $\widetilde{a_i}$ and $\widetilde{b}$ have total degrees at most d and logarithmic heights at most h.

Theorem 3 (Bérczes, Győry, E.)

Assume f has no multiple roots, and degree $n \geq 3$ if $m = 2$ and $n \geq 2$ if $m \geq 3$. Then each solution of

$$by^m = f(x), \quad x, y \in A$$

has representatives $\widetilde{x}, \widetilde{y}$ with

$$\deg \widetilde{x}, h(\widetilde{x}), \ \ \deg \widetilde{y}, h(\widetilde{y}) \ \leq \exp\left\{ m^2 n^5 (d+2)^{\kappa^r} (h+1) \right\},$$

where κ is an effectively computable absolute constant > 1.

Hyper/superelliptic equations over arbitrary finitely generated domains: varying exponent

Let $A = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$ be a domain containing $\mathbb{Z}$.
Let $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ and $b \in A \setminus \{0\}$.

Choose representatives $\widetilde{a_i}, \widetilde{b}$ for the a_i and b.

Suppose that $f_1, \dots, f_m$, the $\widetilde{a_i}$ and $\widetilde{b}$ have total degrees at most d and logarithmic heights at most h.

Theorem 4 (Bérczes, Győry, E.)

Assume f has no multiple zeros, and degree $n \geq 2$. If

$$m > \exp\left\{n^5 (d+2)^{\kappa^r} (h+1)\right\}$$

then

$$by^m = f(x)$$

has no solutions with $x, y \in A$, $y \neq 0$, $y \neq$ root of unity.
Here κ is an effectively computable absolute constant > 1.

An important tool: Aschenbrenner's Theorem

Theorem (Aschenbrenner, 2004)

Let $f_1, \ldots, f_m, b \in \mathbb{Z}[X_1, \ldots, X_r] \setminus \{0\}$ *of total degrees at most* d *and logarithmic heights at most* h*. Suppose there are* $g_1, \ldots, g_m$ *such that*

$$(3) \qquad g_1 f_1 + \cdots + g_m f_m = b, \quad g_1, \ldots, g_m \in \mathbb{Z}[X_1, \ldots, X_r].$$

Then there are such $g_1, \ldots, g_m$ *with*

$$\left.\begin{array}{rcl} \deg g_i & \leq & (d+2)^{\kappa^{r \log(r+1)}}(h+1), \\ h(g_i) & \leq & (d+2)^{\kappa^{r \log(r+1)}}(h+1)^{r+1} \end{array}\right\} \text{ for } i = 1, \ldots, m$$

where κ *is an effectively computable absolute constant* > 1*.*
Hence it can be decided effectively whether (3) *is solvable.*

Outline of the proof of Theorem 2 on Thue equations

Let $A = \mathbb{Z}[z_1, \ldots, z_r] = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ and

$$\varphi : A \to \overline{\mathbb{Q}} : \ z_i \mapsto \xi_i \in \overline{\mathbb{Q}} \quad (i = 1, \ldots, r)$$

a specialization homomorphism. Then $\varphi(A)$ is contained in the ring of S-integers O_S for a finite set of prime ideals S in some number field K.

Thus, φ maps the solutions of the Thue equation $F(x, y) = b$ in $x, y \in A$ to the solutions of a Thue equation over O_S.

Outline of the proof of Theorem 2 on Thue equations

Let $A = \mathbb{Z}[z_1, \ldots, z_r] = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ and

$$\varphi : A \to \overline{\mathbb{Q}} : \; z_i \mapsto \xi_i \in \overline{\mathbb{Q}} \quad (i = 1, \ldots, r)$$

a specialization homomorphism. Then $\varphi(A)$ is contained in the ring of S-integers O_S for a finite set of prime ideals S in some number field K.

Thus, φ maps the solutions of the Thue equation $F(x, y) = b$ in $x, y \in A$ to the solutions of a Thue equation over O_S.

1. Apply 'many' specializations to A and apply existing effective results to the resulting Thue equations over O_S (e.g., Győry-Yu, 2006). This gives, for each solution (x, y) and each of the specializations φ, effective upper bounds for the heights $H(\varphi(x))$ and $H(\varphi(y))$.

Outline of the proof of Theorem 2 on Thue equations

Let $A = \mathbb{Z}[z_1, \ldots, z_r] = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ and

$$\varphi : A \to \overline{\mathbb{Q}} : \ z_i \mapsto \xi_i \in \overline{\mathbb{Q}} \ \ (i = 1, \ldots, r)$$

a specialization homomorphism. Then $\varphi(A)$ is contained in the ring of S-integers O_S for a finite set of prime ideals S in some number field K.

Thus, φ maps the solutions of the Thue equation $F(x, y) = b$ in $x, y \in A$ to the solutions of a Thue equation over O_S.

1. Apply 'many' specializations to A and apply existing effective results to the resulting Thue equations over O_S (e.g., Győry-Yu, 2006). This gives, for each solution (x, y) and each of the specializations φ, effective upper bounds for the heights $H(\varphi(x))$ and $H(\varphi(y))$.

2. View the equation as an equation over the algebraic function field $\mathbb{Q}(z_1, \ldots, z_r)$ and apply effective results of Mason on Thue equations over function fields, to get upper bounds for the total degrees of representatives for x, y.

Outline of the proof of Theorem 2 on Thue equations

Let $A = \mathbb{Z}[z_1, \dots, z_r] = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$ and

$$\varphi : A \to \overline{\mathbb{Q}} : \ z_i \mapsto \xi_i \in \overline{\mathbb{Q}} \ \ (i = 1, \dots, r)$$

a specialization homomorphism. Then $\varphi(A)$ is contained in the ring of S-integers O_S for a finite set of prime ideals S in some number field K.

Thus, φ maps the solutions of the Thue equation $F(x, y) = b$ in $x, y \in A$ to the solutions of a Thue equation over O_S.

1. Apply 'many' specializations to A and apply existing effective results to the resulting Thue equations over O_S (e.g., Győry-Yu, 2006). This gives, for each solution (x, y) and each of the specializations φ, effective upper bounds for the heights $H(\varphi(x))$ and $H(\varphi(y))$.

2. View the equation as an equation over the algebraic function field $\mathbb{Q}(z_1, \dots, z_r)$ and apply effective results of Mason on Thue equations over function fields, to get upper bounds for the total degrees of representatives for x, y.

3. Combine 1) and 2) with Aschenbrenner's theorem to get effective upper bounds for the logarithmic heights of representatives for x, y. $\square$

Other equations

Our method gives also effective finiteness results for various other classes of Diophantine equations over finitely generated domains A over $\mathbb{Z}$.

Examples:

- $x^m - y^n = 1$ in $x, y \in A$, $m, n \in \mathbb{Z}$ with $m \geq 2, n \geq 2, mn \geq 6$ (extension of Tijdeman's effective result on Catalan's equation over $\mathbb{Z}$)

- special cases of $f(x, y) = 0$ in $x, y \in A$ where $f \in A[X, Y]$ (special cases of Siegel's finiteness theorem on integral points on curves)

Thank you for your attention!