Effective results for unit equations over finitely generated domains

Jan-Hendrik Evertse
Universiteit Leiden

Joint work with Kálmán Győry (Debrecen)

Intercity Number Theory Seminar, CWI
March 16, 2012

Unit equations in two unknowns

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 $\mathbb{Q}$.

Denote by A^* the unit group of A.

Theorem (Siegel, Mahler, Parry, Lang)

Let a, b, c be non-zero elements of A. Then the equation

$$ax + by = c \quad \text{in } x, y \in A^* \tag{1}$$

has only finitely many solutions.

The proofs of Siegel, Mahler, Perry, Lang are *ineffective*.

We will focus on *effective* results, which give a method to determine (in principle) all solutions of (1).

History

Ineffective finiteness proofs for the number of solutions were given by

Siegel (1921): $ax + by = c$ in $x, y \in O_K^*$,
O_K is ring of integers of number field K.

Mahler (1933): $ax + by = c$ in $x, y \in \mathbb{Z}_S^*$,
$\mathbb{Z}_S = \mathbb{Z}[(p_1 \cdots p_t)^{-1}]$ ($S = \{p_1, \dots, p_t\}$ set of primes),
$\mathbb{Z}_S^* = \{\pm p_1^{z_1} \cdots p_t^{z_t} : z_i \in \mathbb{Z}\}$.

Parry (1950): $ax + by = c$ in $x, y \in O_S^*$,
$O_S = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}]$ ($S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ set of prime ideals),
$O_S^* = \{x \in K^* : (x) = \mathfrak{p}_1^{z_1} \cdots \mathfrak{p}_t^{z_t} : z_i \in \mathbb{Z}\}$.

Lang (1960): $ax + by = c$ in $x, y \in A^*$,
A arbitrary finitely generated domain over $\mathbb{Z}$.

Application: Thue equations

Let $A = \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be a finitely generated domain over $\mathbb{Z}$, and K its quotient field.

Theorem

Let $F(X, Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X, Y]$ be a square-free binary form of degree $n \geq 3$ and $\delta \in A \setminus \{0\}$. Then

$$F(x, y) = \delta \quad \text{in } x, y \in A \tag{2}$$

has only finitely many solutions.

This was proved by A. Thue (1909) for $A = \mathbb{Z}$.

Application: Thue equations

Let $A = \mathbb{Z}[z_1, \dots, z_r] \supset \mathbb{Z}$ be a finitely generated domain over $\mathbb{Z}$, and K its quotient field.

Theorem

Let $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n \in A[X,Y]$ be a square-free binary form of degree $n \geq 3$ and $\delta \in A \setminus \{0\}$. Then

$$F(x,y) = \delta \quad \textit{in } x, y \in A \tag{2}$$

has only finitely many solutions.

Idea of proof.

Assume wlog $a_0 \neq 0$ and factor F in a finite extension of K as $F = a_0 \prod_{i=1}^{n}(X - \beta_i Y)$. Take $B = A[a_0^{-1}, \delta^{-1}, \beta_1, \dots, \beta_n]$.
Then for any solution (x,y) of (2) we have

$$(\beta_2 - \beta_3)\frac{x - \beta_1 y}{x - \beta_3 y} + (\beta_3 - \beta_1)\frac{x - \beta_2 y}{x - \beta_3 y} = \beta_2 - \beta_1, \quad \frac{x - \beta_1 y}{x - \beta_3 y}, \frac{x - \beta_2 y}{x - \beta_3 y} \in B^*.$$

□

Effective results for S-unit equations (I)

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. Define $O_S = O_K[(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^{-1}]$.

For $\alpha \in \overline{\mathbb{Q}}$ with minimal polynomial $a_0 X^d + \cdots + a_d \in \mathbb{Z}[X]$ with $\gcd(a_0, \ldots, a_d) = 1$, we define its logar. height $h(\alpha) := \log \max_i |a_i|$.

Theorem (Győry, 1979)

Let $a, b, c \in O_S \setminus \{0\}$. There is an effectively computable number C depending on K, S, a, b, c, such that for every pair x, y with

$$ax + by = c, \quad x, y \in O_S^* \tag{3}$$

we have $h(x), h(y) \leq C$.

Thus, given (suitable representations for) K, S, a, b, c, one can determine effectively (suitable representations for) the solutions of (3).

Proof.

Lower bounds for linear forms in ordinary and p-adic logarithms (Baker, Coates, van der Poorten, Yu). □

Effective results for S-unit equations (II)

Let K be an algebraic number field, $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ a finite set of prime ideals of O_K, and $a, b, c \in O_S \setminus \{0\}$.

Suppose that $[K : \mathbb{Q}] = \delta$, K has discriminant Δ, $\max_i N_{K/\mathbb{Q}}\mathfrak{p}_i \leq P$, and $\max\big(h(a), h(b), h(c)\big) \leq h$.

Theorem (Győry, Yu, 2006; weaker version)

For every pair x, y with

$$ax + by = c, \quad x, y \in O_S^*$$

we have $h(x), h(y) \leq C$ with

$$C = 2^{35}(\delta(\delta + t))^{2(\delta+t)+5}|\Delta|^{1/2}(\log|2\Delta|)^{\delta}\, P^{t+1}(h+1).$$

Unit equations over arbitrary finitely generated domains

In 1983/84 Győry extended his effective result on S-unit equations from 1979 to an effective result for equations

$$ax + by = c \quad \text{in } x, y \in A^*$$

for a special class of finitely generated domains $A = \mathbb{Z}[z_1, \ldots, z_r]$ with some of the z_i transcendental.

Aim:
Prove an effective result for unit 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 $f \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $a = f(z_1, \ldots, z_r)$ (or $a = f \mod I$).

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 $f \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $a = f(z_1, \ldots, z_r)$ (or $a = f \mod I$).

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 (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 $a, b, c \in A$*, one can effectively determine a list, containing one pair of representatives for each solution* (x, y) *of*

$$ax + by = c \quad \text{in } x, y \in A^*.$$

A quantitative result

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

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

Let $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ be a domain with $A \supset \mathbb{Z}$ and $a, b, c \in A \setminus \{0\}$. Choose representatives $\widetilde{a}, \widetilde{b}, \widetilde{c} \in \mathbb{Z}[X_1, \ldots, X_r]$ for a, b, c.

Theorem 2 (Győry, E.)

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

$$ax + by = c \quad \text{in } x, y \in A^*$$

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

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

where κ is an effectively computable absolute constant > 1.

Theorem 2 $\Longrightarrow$ Theorem 1 (I)

We need the following result:

Theorem (Aschenbrenner, 2004)

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

$$(4) \qquad g_1 f_1 + \cdots + g_m f_m = b, \quad g_1, \dots, g_m \in \mathbb{Z}[X_1, \dots, X_r].$$

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

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

where κ *is an effectively computable absolute constant* > 1*.*
Hence it can be decided effectively whether (4) *is solvable.*

This is an analogue of results of Hermann (1926) and Seidenberg (1972) on linear equations over $F[X_1, \dots, X_r]$, F any field.

Theorem 2 $\Longrightarrow$ Theorem 1 (II)

Corollary (Ideal membership algorithm for $\mathbb{Z}[X_1, \ldots, X_r]$)

Given $f_1, \ldots, f_m, b \in \mathbb{Z}[X_1, \ldots, X_r]$ *it can be decided effectively whether* $b \in (f_1, \ldots, f_m)$.

Theorem 2 $\Longrightarrow$ Theorem 1 (II)

Corollary (Ideal membership algorithm for $\mathbb{Z}[X_1, \ldots, X_r]$)

Given $f_1, \ldots, f_m, b \in \mathbb{Z}[X_1, \ldots, X_r]$ *it can be decided effectively whether* $b \in (f_1, \ldots, f_m)$.

Corollary (Unit decision algorithm)

Given $b, f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_r]$ *it can be decided effectively whether* b *represents a unit of* $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$.

Theorem 2 $\Longrightarrow$ Theorem 1 (II)

Corollary (Ideal membership algorithm for $\mathbb{Z}[X_1, \ldots, X_r]$)

Given $f_1, \ldots, f_m, b \in \mathbb{Z}[X_1, \ldots, X_r]$ it can be decided effectively whether $b \in (f_1, \ldots, f_m)$.

Corollary (Unit decision algorithm)

Given $b, f_1, \ldots, f_m \in \mathbb{Z}[X_1, \ldots, X_r]$ it can be decided effectively whether b represents a unit of $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$.

Proof.

b represents a unit of A

$\Longleftrightarrow$

there is $b' \in \mathbb{Z}[X_1, \ldots, X_r]$ such that $b \cdot b' \equiv 1 \pmod{(f_1, \ldots, f_m)}$

$\Longleftrightarrow$

there are $b', g_1, \ldots, g_m \in \mathbb{Z}[X_1, \ldots, X_r]$ with

$b' \cdot b + g_1 f_1 + \cdots + g_m f_m = 1.$ □

Theorem 2 $\Longrightarrow$ Theorem 1 (III)

Let $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$, and let $\widetilde{a}, \widetilde{b}, \widetilde{c}$ be representatives for $a, b, c \in A$.

By Theorem 2 there is an effectively computable C such that each solution x, y of

$$(1) \qquad ax + by = c, \quad x, y \in A^*$$

has representatives $\widetilde{x}, \widetilde{y}$ of total degrees and logarithmic heights $\leq C$.

Theorem 2 $\Longrightarrow$ Theorem 1 (III)

Let $A = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$, and let $\widetilde{a}, \widetilde{b}, \widetilde{c}$ be representatives for $a, b, c \in A$.

By Theorem 2 there is an effectively computable C such that each solution x, y of

$$(1) \qquad ax + by = c, \quad x, y \in A^*$$

has representatives $\widetilde{x}, \widetilde{y}$ of total degrees and logarithmic heights $\leq C$.

One can find a representative for each solution of (1) as follows:

Check for each pair $\widetilde{x}, \widetilde{y} \in \mathbb{Z}[X_1, \dots, X_r]$ of total degree and logarithmic height $\leq C$ whether

$$\widetilde{a} \cdot \widetilde{x} + \widetilde{b} \cdot \widetilde{y} - \widetilde{c} \in (f_1, \dots, f_m),$$
$$\widetilde{x}, \widetilde{y} \text{ represent elements of } A^*.$$

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

Exponential equations

Let $A = \mathbb{Z}[X_1, \dots, X_r]/(f_1, \dots, f_m)$ be a domain with $A \supset \mathbb{Z}$, $a, b, c \in A \setminus \{0\}$, and $\gamma_1, \dots, \gamma_s$ *multiplicatively independent* elements of $A \setminus \{0\}$, i.e.,

$$\left\{(k_1, \dots, k_s) \in \mathbb{Z}^s : \gamma_1^{k_1} \cdots \gamma_s^{k_s} = 1\right\} = \{\mathbf{0}\}.$$

Consider

$$a\gamma_1^{u_1} \cdots \gamma_s^{u_s} + b\gamma_1^{v_1} \cdots \gamma_s^{v_s} = c \quad \text{in } u_1, \dots, v_s \in \mathbb{Z}. \tag{5}$$

Theorem 3 (Győry, E.)

Let $\widetilde{a}, \widetilde{b}, \widetilde{c}, \widetilde{\gamma}_1, \dots, \widetilde{\gamma}_s \in \mathbb{Z}[X_1, \dots, X_r]$ *be representatives for* $a, b, c, \gamma_1, \dots, \gamma_s$ *and assume that* $f_1, \dots, f_m, \widetilde{a}, \widetilde{b}, \widetilde{c}, \widetilde{\gamma}_1, \dots, \widetilde{\gamma}_s$ *have total degrees at most* d *and logarithmic heights at most* h. *Then for each solution of* (5) *we have*

$$\max(|u_1|, \dots, |v_s|) \leq \exp\left\{(d+2)^{\kappa^{r+s}}(h+1)\right\}$$

where κ *is an effectively computable absolute constant* > 1.

An effective criterion for multiplicative (in)dependence

Let $A = \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ be a domain with $A \supset \mathbb{Z}$, let $\gamma_1, \ldots, \gamma_s \in A \setminus \{0\}$, and choose representatives $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_s$ for $\gamma_1, \ldots, \gamma_s$.

Suppose that $f_1, \ldots, f_m$, $\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_s$ have total degrees at most d and logarithmic heights at most h.

Proposition 4 (Győry, E.)

If $\gamma_1, \ldots, \gamma_s$ are multiplicatively dependent, then there are integers $k_1, \ldots, k_s$, not all 0, such that

$$\gamma_1^{k_1} \cdots \gamma_s^{k_s} = 1, \quad \max_i |k_i| \leq (d+2)^{\kappa^{r+s}} (h+1)^{s-1}$$

where κ is an effectively computable absolute constant > 1.

Unit equations vs. exponential equations

Theorem (Roquette, 1956)

Let A be a finitely generated domain over $\mathbb{Z}$. Then its unit group A^* is finitely generated, i.e., there is a finite set of generators $\gamma_1, \dots, \gamma_s \in A^*$ such that $A^* = \{\gamma_1^{u_1} \cdots \gamma_s^{u_s} : u_i \in \mathbb{Z}\}$.

By Roquette's Theorem, the unit equation

$$(1) \qquad ax + by = c \quad \text{in } x, y \in A^*$$

can be rewritten as an exponential equation

$$(5) \qquad a\gamma_1^{u_1} \cdots \gamma_s^{u_s} + b\gamma_1^{v_1} \cdots \gamma_s^{v_s} = c \quad \text{in } u_1, \dots, v_s \in \mathbb{Z}.$$

But as yet, no algorithm is known which for an arbitrary given finitely generated domain A over $\mathbb{Z}$ computes a finite set of generators for A^*.

So from an effective result on (5) one can not deduce an effective result on (1).

Idea of proof of Theorem 2

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

(1) $$ax + by = c \quad \text{in } x, y \in A^*$$

to S-unit equations in a number field by means of specializations

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

Idea of proof of Theorem 2

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

$$(1) \qquad ax + by = c \quad \text{in } x, y \in A^*$$

to S-unit equations in a number field by means of specializations

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

1. Apply 'many' specializations to (1) and apply the effective result of Győry-Yu to each of the resulting S-unit equations. This leads, for each solution x, y of (1) and each of the chosen specializations φ, to effective upper bounds for the logarithmic heights $h(\varphi(x))$ and $h(\varphi(y))$.

Idea of proof of Theorem 2

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

$$(1) \qquad ax + by = c \quad \text{in } x, y \in A^*$$

to S-unit equations in a number field by means of specializations

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

1. Apply 'many' specializations to (1) and apply the effective result of Győry-Yu to each of the resulting S-unit equations. This leads, for each solution x, y of (1) and each of the chosen specializations φ, to effective upper bounds for the logarithmic heights $h(\varphi(x))$ and $h(\varphi(y))$.

2. View (1) as an equation over the algebraic function field $\mathbb{Q}(z_1, \ldots, z_r)$ and apply Stothers' and Mason's effective abc-Theorem for function fields, to get upper bounds for the total degrees of representatives for x, y.

Idea of proof of Theorem 2

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

$$(1) \qquad ax + by = c \quad \text{in } x, y \in A^*$$

to S-unit equations in a number field by means of specializations

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

1. Apply 'many' specializations to (1) and apply the effective result of Győry-Yu to each of the resulting S-unit equations. This leads, for each solution x, y of (1) and each of the chosen specializations φ, to effective upper bounds for the logarithmic heights $h(\varphi(x))$ and $h(\varphi(y))$.

2. View (1) as an equation over the algebraic function field $\mathbb{Q}(z_1, \dots, z_r)$ and apply Stothers' and Mason's effective abc-Theorem for function fields, to get upper bounds for the total degrees of representatives for x, y.

3. Combine 1) and 2) with Aschenbrenner's theorem on linear equations over $\mathbb{Z}[X_1, \dots, X_r]$, to get effective upper bounds for the logarithmic heights of representatives for x, y. □

Work in progress (with Attila Bérczes, Kálmán Győry)

Effective results over finitely generated domains A (with effective upper bounds for the total degrees and logarithmic heights of the solutions) for

- Thue equations $F(x, y) = \delta$ in $x, y \in A$
  (F binary form in $A[X, Y]$, $\delta \in A \setminus \{0\}$);

- Schinzel-Tijdeman equation $y^m = f(x)$ in $x, y \in A$, $m \in \mathbb{Z}_{\geq 2}$
  ($f \in A[X]$)

Preprint:

J.-H. Evertse, K. Győry,
Effective results for unit equations over finitely generated domains,
arXiv:1107.5756 [math.NT] 28 July 2011