Effective results for unit equations over finitely generated domains

Jan-Hendrik Evertse
Universiteit Leiden

Joint work with Kálmán Győry (Debrecen)

Paul Turán Memorial Conference, Budapest
August 22, 2011
Let $A$ be a \textit{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 $A$.

\begin{center}
\textbf{Theorem (Siegel, Mahler, Parry, Lang)}
\end{center}

\textit{Let $a, b, c$ be non-zero elements of $A$. Then the equation}

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

\textit{has only finitely many solutions}.

Siegel (1921): $A = O_K$ = ring of integers in a number field $K$,
Mahler (1933): $A = \mathbb{Z}[1/p_1 \cdots p_t]$, $p_i$ primes,
Parry (1950): $A = O_S$ = ring of $S$-integers in a number field $K$,
Lang (1960): $A$ arbitrary finitely generated domain over $\mathbb{Z}$

The proofs of Siegel, Mahler, Parry, Lang are \textit{ineffective}. 
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 \( F(X, Y) = a_0 X^n + a_1 X^{n-1} Y + \cdots + a_n Y^n \in A[X, Y] \) be a square-free binary form of degree \( n \geq 3 \) and \( \delta \in A \setminus \{0\} \). Then

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

has only finitely many solutions.
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

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

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 $B = A[a_0^{-1}, \delta^{-1}, \beta_1, \ldots, \beta_n]$. Then for any solution $(x, y)$ of (2) we have

$$(\beta_2 - \beta_3) \frac{x - \beta_1 y}{x - \beta_3 y} + (\beta_3 - \beta_1) \frac{x - \beta_2 y}{x - \beta_3 y} = \beta_2 - \beta_1, \quad \frac{x - \beta_1 y}{x - \beta_3 y}, \quad \frac{x - \beta_2 y}{x - \beta_3 y} \in B^*.$$
Effective results for S-unit equations (I)

Let $K$ be an algebraic number field and $S = \{p_1, \ldots, p_t\}$ a finite set of prime ideals of $O_K$. Define $O_S = O_K[(p_1 \cdots p_t)^{-1}]$. Then $O_S^*$ consists of all elements of $K$ composed of prime ideals from $S$.

For $\alpha \in \overline{\mathbb{Q}}$ with minimal polynomial $a_0X^d + \cdots + a_d \in \mathbb{Z}[X]$ with $\gcd(a_0, \ldots, a_d) = 1$, we define its logarithmic height $h(\alpha) := \log \max |a_i|$.

**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

$$(3) \quad ax + by = c, \quad x, y \in O_S^*$$

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).
Let $K$ be an algebraic number field, $S = \{p_1, \ldots, p_t\}$ 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 $\Delta$, $\max_i N_{K/\mathbb{Q}} p_i \leq P$, and $\max (h(a), h(b), h(c)) \leq h$.

**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 $\mathbb{Z}$. 
The general effective result

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,

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

**Remark.** A domain, $A \supset \mathbb{Z} \iff f_1, \ldots, f_m$ generate a prime ideal of $\mathbb{Q}[X_1, \ldots, X_r]$ not containing 1. There are various algorithms to check this for given $f_1, \ldots, f_m$.

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

**Theorem 1 (Győry, E., to appear)**

*Given $f_1, \ldots, f_m$ and representatives for $a, b, c$, one can effectively determine representatives for all solutions of*

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

Let $A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$ be a domain with $A \supset \mathbb{Z}$ and $a, b, c \in A \setminus \{0\}$. For $f \in \mathbb{Z}[X_1, \ldots, X_r]$ define

$$\deg f := \text{total degree of } f,$$
$$h(f) := \log \max |\text{coefficients of } f| \quad \text{(logarithmic height)},$$
$$s(f) := \max(1, \deg f, h(f)) \quad \text{(size)}.$$

**Theorem 2 (Győry, E.)**

Let $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}[X_1, \ldots, X_r]$ be representatives for $a, b, c$. Suppose that $f_1, \ldots, f_m, \tilde{a}, \tilde{b}, \tilde{c}$ 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 $\tilde{x}, \tilde{y}$ such that

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

where $\kappa$ is an effectively computable absolute constant $> 1$. 

We need the following result:

**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

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

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

\[
\begin{align*}
    \deg g_i & \leq (d + 2)^r \kappa^r \log(r+1) (h + 1), \\
    h(g_i) & \leq (d + 2)^r \kappa^r \log(r+1) (h + 1)^{r+1}
\end{align*}
\]

for $i = 1, \ldots, m$, where $\kappa$ is an effectively computable absolute constant $> 1$.

Hence it can be decided effectively whether (4) is solvable.

This is an analogue of earlier results of Hermann (1926) and Seidenberg (1972) on linear equations over $F[X_1, \ldots, X_r]$, $F$ any field.
Theorem 2 $\iff$ Theorem 1 (II)

**Corollary (Ideal membership algorithm)**

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 (Ideal membership algorithm)

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 $\iff$ Theorem 1 (II)

**Corollary (Ideal membership algorithm)**

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 $A$

$\iff$

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

$\iff$

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

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

$\square$
Theorem 2 $\implies$ Theorem 1 (III)

Let $f_1, \ldots, f_m$ such that $A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$, and let $\tilde{a}, \tilde{b}, \tilde{c}$ 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) \hspace{1cm} ax + by = c, \hspace{0.5cm} x, y \in A^*$

has representatives $\tilde{x}, \tilde{y}$ of size $\leq C$. 
Theorem 2 $\iff$ Theorem 1 (III)

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

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

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

has representatives $\tilde{x}, \tilde{y}$ of size $\leq C$.

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

Check for each pair $\tilde{x}, \tilde{y} \in \mathbb{Z}[X_1, \ldots, X_r]$ of size $\leq C$ whether

$$
\tilde{a} \cdot \tilde{x} + \tilde{b} \cdot \tilde{y} - \tilde{c} \in (f_1, \ldots, f_m),
$$

$\tilde{x}, \tilde{y}$ represent elements of $A^*$.

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

15/24
Exponential equations

Let \( A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m) \) be a domain with \( A \supset \mathbb{Z} \), \( a, b, c \in A \setminus \{0\} \), and \( \gamma_1, \ldots, \gamma_s \) multiplicatively independent elements of \( A \setminus \{0\} \). Consider

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

**Theorem 3 (Győry, E.)**

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

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

where \( \kappa \) is an effectively computable absolute constant \( > 1 \).
An effective criterion for multiplicative (in)dependence

Let $f_1, \ldots, f_m$ be such that $A \cong \mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_m)$, let $\gamma_1, \ldots, \gamma_s$ be non-zero elements of $A$, and choose representatives $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_s$ for $\gamma_1, \ldots, \gamma_s$.

Suppose that $f_1, \ldots, f_m, \tilde{\gamma}_1, \ldots, \tilde{\gamma}_s$ 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 $\kappa$ is an effectively computable absolute constant $> 1$.***
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 $\gamma_1, \ldots, \gamma_s \in A^*$ 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) \[ ax + by = c \quad \text{in } x, y \in A^* \]

can be rewritten as an exponential equation

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

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).
Let $A = \mathbb{Z}[z_1, \ldots, z_r]$. We can map

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

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

$$\varphi : A \rightarrow \overline{\mathbb{Q}} : z_i \mapsto \xi_i \in \overline{\mathbb{Q}} \quad (i = 1, \ldots, r).$$
Idea of proof of Theorem 2

Let \( A = \mathbb{Z}[z_1, \ldots, z_r] \). We can map

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

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 \( \varphi \), to effective upper bounds for the logarithmic heights \( h(\varphi(x)) \) and \( h(\varphi(y)) \).
Idea of proof of Theorem 2

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$. We can map

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

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 $\varphi$, 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 determine effective upper bounds for the function field heights $h_f(x)$, $h_f(y)$, using Stothers’ and Mason’s effective abc-Theorem for function fields.
Idea of proof of Theorem 2

Let $A = \mathbb{Z}[z_1, \ldots, z_r]$. We can map

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

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 $\varphi$, 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 determine effective upper bounds for the function field heights $h_f(x)$, $h_f(y)$, using Stothers’ and Mason’s effective abc-Theorem for function fields.

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

□
Effective results over finitely generated domains $A$ (with effective upper bounds for the sizes of the solutions) for

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

- Hyper- and superelliptic equations $y^m = f(x)$ in $x, y \in A$ ($f \in A[X], m \geq 2$);

- Discriminant form equations $\text{Discr}_{L/K}(\alpha_1x_1 + \cdots + \alpha_mx_m) = \delta$ in $x_1, \ldots, x_m \in A$ ($K$ quotient field of $A$, $L$ finite extension of $K$, $\alpha_1, \ldots, \alpha_m \in L, \delta \in A \setminus \{0\}$).
J.-H. Evertse, K. Győry,
*Effective results for unit equations over finitely generated domains,*