Effective results for Diophantine equations over finitely generated domains

A. Bérczes

Nancy, 2023

1. Introduction
   - Finitely generated domains
   - Results over arbitrary finitely generated domains

2. Some words on the proofs
   - Some words about the proof of the Theorem on division points

Topic of the talk

- Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be an integral domain of characteristic 0 which is finitely generated over $\mathbb{Z}$.
- Assume that $r > 0$.
- We considered several types of Diophantine problems over A:
  - Thue equations
  - hyper- and superelliptic equations
  - the Schinzel-Tijdeman equation
  - unit points on curves
  - division points on curves

Main goal

Prove effective results for such equations, i.e. results which imply that these equations have finitely many solutions and provide a theoretical way to find all these solutions

Historical remarks

- Győry in the 1980's introduced effective specializations to prove effective results over a special type of finitely generated domain
- Using this method Győry proved effective results over special finitely generated domains for
    - unit equations
    - norm form equations
    - index form equations
    - discriminant form equations
    - polynomials and integral elements of given discriminant
- Brindza, Pintér, Végső and others used this method to prove results for several other types of equations
- In 2013 Evertse and Győry combined the method of Győry with results of Aschenbrenner and proved effective results for unit equations in two unknowns over arbitrary finitely generated domains.

Historical remarks – The new method of Evertse and Győry

- In 2013 Evertse and Győry combined the method of Győry with results of Aschenbrenner and proved effective results for unit equations in two unknowns over arbitrary finitely generated domains.
- Using this new method general effective results have been proved for several types of equations over arbitrary finitely generated domains
  - Thue equations (B., Evertse, Győry)
  - hyper- and superelliptic equations (B., Evertse, Győry)
  - the Schinzel-Tijdeman equation (B., Evertse, Győry)
  - unit points on curves (B.)
  - division points on curves (B.)
  - the Catalan equation (Koymans)
  - discriminant form and discriminant eqiations (Evertse, Győry)
  - norm form equations (Evertse, Győry)
  - decomposable form equations (Evertse, Győry)

The finitely generated domain A

- Let $A = \mathbb{Z}[z_1, \ldots, z_r]$ be as above, and put

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

Then we have

$$A \cong \mathbb{Z}[X_1, \ldots, X_r]/I.$$

Further, the ideal I is finitely generated, say

$$I = (f_1, \ldots, f_t).$$

- We may view $f_1, \ldots, f_t$ as a representation for A.
- A is a domain of char 0 $\iff$ I is a prime ideal with $I \cap \mathbb{Z} = (0)$
- Given a set of generators $\{f_1, \ldots, f_t\}$ for I this can be checked effectively

Representing elements of A

Let A be as above and let K be its quotient field.

- For $\alpha \in A$, we call f a *representative* for α, or we say that f represents α, if $f \in \mathbb{Z}[X_1, \dots, X_r]$ and $\alpha = f(z_1, \dots, z_r)$.
- Further, for $\alpha \in K$ we call (f, g) a *representation pair* for α, or say that (f, g) represents α if $f, g \in \mathbb{Z}[X_1, \dots, X_r]$, $g \notin I$ and $\alpha = f(z_1, \dots, z_r)/g(z_1, \dots, z_r)$.
- Using an ideal membership algorithm for $\mathbb{Z}[X_1, \dots, X_r]$ one can decide effectively
  - whether two polynomials $f', f'' \in \mathbb{Z}[X_1, \dots, X_r]$ represent the same element of A, i.e., $f' - f'' \in I$
  - whether two pairs $(f', g'), (f'', g'')$ in $\mathbb{Z}[X_1, \dots, X_r]$ represent the same element of K, i.e., $g' \notin I$, $g'' \notin I$ and $f'g'' - f''g' \in I$

Effective computations in A

- Based on results of Aschenbrenner one can perform arithmetic operations on A and K by using representatives.
- For $0 \neq f \in \mathbb{Z}[X_1, \ldots, X_r]$, denote by
  - $\deg f$ the total degree of f
  - $h(f)$ the logarithmic height of f, i.e. the logarithm of the maximum of the absolute values of its coefficients.
  - $s(f)$ the *size* of f, which is defined by

$$s(f) := \max(1, \deg f, h(f)) \qquad \text{for} \quad f \neq 0$$
$$s(0) := 1$$

- It is clear that there are only finitely many polynomials in $\mathbb{Z}[X_1, \ldots, X_r]$ of size below a given bound, and these can be determined effectively.

Unit points on curves

- $A := \mathbb{Z}[z_1, \ldots, z_r]$ a domain which is finitely generated over $\mathbb{Z}$, as $\mathbb{Z}$-algebra
- K the quotient field of A
- $\overline{K}$ the algebraic closure of K
- A^*, K^*, $\overline{K}^*$ denotes the unit group of A, K, $\overline{K}$, respectively.
- Γ a finitely generated subgroup of K^*
- $\overline{\Gamma}$ the division group of Γ
- $F(X, Y) \in A[X, Y]$ a polynomial, such that F is not divisible by any polynomial of the form

$$X^m Y^n - \alpha \qquad \text{or} \qquad X^m - \alpha Y^n \tag{1}$$

for any $m, n \in \mathbb{Z}_{\geq 0}$, not both zero, and any $\alpha \in A$.

Consider the equation

$$F(x, y) = 0 \quad \text{in } x, y \in \Gamma \tag{2}$$

Historical remarks for unit points and division points on curves

Let

$$\mathcal{C} := \{(x, y) \in (\mathbb{C}^*)^2 \mid f(x, y) = 0\}$$

- Lang (1960) – finiteness of $\mathcal{C} \cap \Gamma^2$ (ineffective)
- Liardet (1974) – finiteness of $\mathcal{C} \cap \overline{\Gamma}^2$ (ineffective)
- Bombieri and Gubler (2006) – effective finiteness of $\mathcal{C} \cap \Gamma^2$ in the algebraic case
- B., Evertse and Győry (2009) – explicit effective finiteness of $\mathcal{C} \cap \overline{\Gamma}^2$ in the algebraic case

Goal:

Prove effective versions of the results of Lang and Liardet in the case of arbitrary finitely generated groups.

Recall that

- $A = \mathbb{Z}[z_1, \ldots, z_r]$ integral domain finitely generated over $\mathbb{Z}$
- We assume that $r > 0$
- $A \cong \mathbb{Z}[X_1, \ldots, X_r]/\mathcal{I}$ for
  $\mathcal{I} := \{f \in \mathbb{Z}[X_1, \ldots, X_r] \mid f(z_1, \ldots, z_r) = 0\}$
- we have $\mathcal{I} = (f_1, \ldots, f_t)$

Let $I \subset \mathbb{Z}^2_{\geq 0}$ be a non-empty set, and let

$$F(X,Y) = \sum_{(i,j)\in I} a_{ij} X^i Y^j \in A[X,Y]$$

be a polynomial which fulfils the following condition:

F **is not divisible by** any non-constant polynomial of the form

$$X^m Y^n - \alpha \quad \text{or} \quad X^m - \alpha Y^n, \text{where } m, n \in \mathbb{Z}_{\geq 0} \text{ and } \alpha \in \overline{K}^*. \tag{3}$$

Unit points on curves over finitely generated domains

- F is given by representatives $\tilde{a}_{ij} \in \mathbb{Z}[X_1, \ldots, X_r]$ of its coefficients $a_{ij} \in A$
- We assume that $d > 1$ and $h > 1$ are real numbers with

$$\begin{cases} \deg f_1, \ldots, \deg f_t, \deg \tilde{a}_{ij} \leq d \quad \text{for every} \quad (i,j) \in I \\ h(f_1), \ldots, h(f_t), h(\tilde{a}_{ij}) \leq h \quad \text{for every} \quad (i,j) \in I. \end{cases} \tag{4}$$

Theorem (Bérczes, 2015)

If A is a finitely generated domain as above, and F fulfils the condition (3) then for all elements (x, y) of the set

$$\mathcal{C} := \{(x,y) \in (A^*)^2 | F(x,y) = 0\} \tag{5}$$

there exist representatives $\tilde{x}$, $\tilde{y}$, $\tilde{x}'$ and $\tilde{y}'$ of x, y, x^{-1} and y^{-1}, respectively, with their sizes bounded by

$$\exp\left\{(2d)^{\exp O(r)}(2N)^{(\log^* N)\cdot \exp O(r)} \cdot (h+1)^3\right\}.$$

Effectiveness of the above Theorem

The above result is effective, i.e. it provides an algorithm to determine, at least in principle, all elements of the set $\mathcal{C}$.

- there are only finitely many polynomials of $\mathbb{Z}[X_1, \ldots, X_r]$ below our bound in the theorem
- $(x, y) \in \mathcal{C}$ is clearly fulfilled if and only if there are polynomials $\tilde{x}, \tilde{y}, \tilde{x}', \tilde{y}' \in \mathbb{Z}[X_1, \ldots, X_r]$ with their sizes below the bound (1), which fulfil

$$\tilde{x} \cdot \tilde{x}' - 1,\ \ \tilde{y} \cdot \tilde{y}' - 1,\ \ \tilde{F}(\tilde{x}, \tilde{y}) \in \mathcal{I}. \tag{6}$$

- so we can enlist all 4-tuples $(\tilde{x}, \tilde{y}, \tilde{x}', \tilde{y}')$ with $s(\tilde{x}), s(\tilde{y}), s(\tilde{x}'), s(\tilde{y}')$ being smaller than our bound
- using an ideal membership algorithm check if (6) is fulfilled
- finally, group all the tuples in which $(\tilde{x},\ \tilde{y})$ represent the same pair $(x, y) \in (A^*)^2$ and pick out one pair from each group
- so we get a list consisting of one representative for each element of the set $\mathcal{C}$.

Assumptions for the results on division points

- $F(X,Y) \in A[X,Y]$ is a polynomial as above
- $\gamma_1, \dots, \gamma_s \in K^*$ are arbitrary non-zero elements of K
- they are given by corresponding representation pairs $(g_1, h_1), \dots, (g_s, h_s)$
- $\Gamma := \left\{ \gamma_1^{l_1} \dots \gamma_s^{l_s} \mid l_1, \dots, l_s \in \mathbb{Z} \right\}$
- $\overline{\Gamma} := \{ \delta \in \overline{K} \mid \exists\, m \in \mathbb{Z}_{>0} : \ \delta^m \in \Gamma \}$

Further, we assume that

$$\deg f_1, \dots, \deg f_t, \deg g_1, \dots, \deg g_s, \deg h_1, \dots, \deg h_s, \deg \tilde{a}_{ij} \leq d$$
$$h(f_1), \dots, h(f_t), h(g_1), \dots, h(g_s), h(h_1), \dots, h(h_s), h(\tilde{a}_{ij}) \leq h,$$

where $(i,j) \in I$ and d, h are real numbers with $d > 1$ and $h > 1$.

Division points on curves I.

Theorem (Theorem for division points on curves – part (i))

(i) *Let* A, $\overline{\Gamma}$, *and* F *be as specified above. Define the set*

$$\mathcal{C} := \{(x, y) \in (\overline{\Gamma})^2 | F(x, y) = 0\}. \quad (7)$$

Then there exists a suitably large effectively computable constant C_1 *such that for*

$$M_0 := \left[N^6 (2d)^{\exp\{C_1(r+s)\}} (h+1)^{4s} \right]$$

and $m := \text{lcm}(1, \ldots, M_0)$ *we have*

$$x^m \in \Gamma \qquad \textit{and} \qquad y^m \in \Gamma,$$

for every $(x, y) \in \mathcal{C}$.

Division points on curves II.

Theorem (Theorem for division points on curves – part (ii))

(ii) *Let m be the exponent fixed in part (i) and recall that*

$$\mathcal{C} := \{(x, y) \in (\overline{\Gamma})^2 | F(x, y) = 0\}. \tag{8}$$

Then there exists an effectively computable constant C_2 *and integers* $t_{1,x}, \ldots, t_{s,x}, t_{1,y}, \ldots, t_{s,y}$ *with*

$$|t_{i,x}|, |t_{i,y}| \leq \exp\left\{\exp\left\{N^{12}(2d)^{\exp\{C_2(r+s)\}}(h+1)^{8s}\right\}\right\} \tag{9}$$

for $i = 1, \ldots, s$*, such that*

$$x^m = \gamma_1^{t_{1,x}} \ldots \gamma_s^{t_{s,x}}, \qquad y^m = \gamma_1^{t_{1,y}} \ldots \gamma_s^{t_{s,y}}. \tag{10}$$

Main steps of the proof of part (i) of the Theorem on division points

- for $(x, y) \in \mathcal{C}$ we bound the degree of the field $K(x, y)$
- we estimate the smallest positive integer exponent M such that for $(x, y) \in \mathcal{C}$ we have $x^M, y^M \in \Gamma_K$, where Γ_K denotes the K closure of Γ, i.e. the largest subgroup of $\overline{\Gamma}$ which belongs to K^*
- for $\gamma \in \Gamma_K$ we estimate the smallest positive integer exponent $m(\gamma)$ such that $\gamma^{m(\gamma)} \in \Gamma$
- The number $m_0 := M \cdot m(x^M) \cdot m(y^M)$ will have the property $x^{m_0}, y^{m_0} \in \Gamma$, however it depends on (x, y).
- Since we have the estimate

$$m_0 \leq N^6 (2d)^{\exp(O(r+s))} (h+1)^{4s} := M_0.$$

the number $m := \mathrm{lcm}(1, \dots, M_0)$ will be a uniform exponent with $x^m, y^m \in \Gamma$.

Reformulation of part (ii) of the Theorem on division points

Let us fix m to be the integer specified in part (i) of our Theorem and consider the set

$$\mathcal{C}_1 := \left\{(x_0, y_0) \in \Gamma^2 \mid \exists\, x, y \in \overline{\Gamma} : x^m = x_0, y^m = y_0, F(x,y) = 0\right\}. \tag{11}$$

Proposition

Let $(x_0, y_0) \in \mathcal{C}_1$. Then there exist representatives $\tilde{x}_0$ and $\tilde{y}_0$ for x_0 and y_0, respectively, with the property

$$\begin{aligned} \deg \tilde{x}_0, \deg \tilde{y}_0 &\leq \exp\left\{N^6 (2d)^{\exp O(r+s)} (h+1)^{4s}\right\} \\ h(\tilde{x}_0), h(\tilde{y}_0) &\leq \exp\left\{\exp\left\{N^{12} (2d)^{\exp O(r+s)} (h+1)^{8s}\right\}\right\} \end{aligned} \tag{12}$$

Reducing our equation to an equation over Γ

- Let ρ be a primitive m^{th} root of unity. There exists $G(U,V)=\sum_{(i,j)\in\mathcal{J}} b_{ij}U^iV^j \in A[U,V]$ with $b_{ij}\neq 0$ and
$$G(X^m,Y^m)=\prod_{k=0}^{m-1}\prod_{l=0}^{m-1}F(\rho^kX,\rho^lY) \qquad (13)$$
and such that b_{ij} have representatives $\tilde{b}_{ij}$ with bounded size.
- $G(X,Y)$ is divisible by a non-constant polynomial of the form $X^aY^b-\alpha$ or $X^a-\alpha Y^b$ with $\alpha\in\overline{K}^*$, $a,b\in\mathbb{Z}_{\geq 0}$ if and only if $F(X,Y)$ is divisible by a non-constant polynomial of the form $X^uY^v-\beta$ or $X^u-\beta Y^v$ with $\beta\in\overline{K}^*$, $u,v\in\mathbb{Z}_{\geq 0}$.
- The set
$$\mathcal{C}_1:=\left\{(x_0,y_0)\in\Gamma^2 \mid \exists x,y\in\overline{\Gamma}: x^m=x_0, y^m=y_0, F(x,y)=0\right\}$$
is equal to the set
$$\mathcal{C}_2:=\left\{(x_0,y_0)\in\Gamma^2 \mid G(x_0,y_0)=0\right\}.$$

Effectiveness of the Theorem on division points

- Consider the above defined polynomial $G(X,Y)$
- For all values of the exponents t_{ix}, t_{iy} below the bound specified in part (ii) of our Theorem we check

$$G(\gamma_1^{t_{1x}}\dots\gamma_s^{t_{sx}}, \gamma_1^{t_{1y}}\dots\gamma_s^{t_{sy}}) = 0.$$

- If this is true then the elements

$$x_0 = \gamma_1^{t_{1x}}\dots\gamma_s^{t_{sx}}, \qquad y_0 = \gamma_1^{t_{1y}}\dots\gamma_s^{t_{sy}}$$

have at least one m^{th} root x and y, respectively, such that

$$F(x,y) = 0.$$

Further, each element of $\mathcal{C}$ can be obtained in such a way.

Thank you for your attention!