Effective results for Diophantine equations over finitely generated domains

Jan-Hendrik Evertse (Universiteit Leiden)

(Joint work with Attila Bérczes, Kálmán Győry)

Let $A = \mathbb{Z}[z_1, \ldots, z_q] \supset \mathbb{Z}$ be an integral domain which is finitely generated over $\mathbb{Z}$. Then

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

where $f_1, \ldots, f_s$ is a system of generators for the ideal of $f \in \mathbb{Z}[X_1, \ldots, X_r]$ with $f(z_1, \ldots, z_r) = 0$. We want to give effective finiteness results for certain classes of Diophantine equations with unknowns taken from the domain A.

To state our results, we need some terminology. Given $a \in A$, we call $\widetilde{a} \in \mathbb{Z}[X_1, \ldots, X_r]$ a *representative* for a if $\widetilde{a}(z_1, \ldots, z_s) = a$. There exist algorithms with which one can decide for given $f, f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_r]$ whether $f \in (f_1, \ldots, f_s)$ (see Simmons [13, 1970], Aschenbrenner [1, 2004]). With the help of this, one can decide effectively whether two polynomials $f, g \in \mathbb{Z}[x_1, \ldots, X_r]$ represent the same element of A.

For $f \in \mathbb{Z}[X_1, \ldots, X_r]$, let $\deg f$ denote its total degree and $h(f)$ its logarithmic height (i.e., the maximum of the logarithms of the absolute values of its coefficients), and define its size $s(f) := \max(1, \deg f, h(f))$. Then we define the size of $x \in A$ by the minimum of the quantities $s(\widetilde{x})$, taken over all representatives $\widetilde{x} \in \mathbb{Z}[X_1, \ldots, X_r]$ for x.

Notice that if $F \in A[Y_1, \ldots, Y_t]$ is a polynomial with coefficients in A, and we are given $\widetilde{F} \in \mathbb{Z}[X_1, \ldots, X_r][Y_1, \ldots, Y_t]$ whose coefficients represent those of F, then in order to determine effectively all solutions of the equation $(*)$ $F(y_1, \ldots, y_t) = 0$ in $y_1, \ldots, y_t \in A$, it suffices to give a number C such that $\max_i s(y_i) \leq C$ for all solutions $(y_1, \ldots, y_t)$ of $(*)$. Indeed, one simply needs to check for all polynomials $\widetilde{y_1}, \ldots, \widetilde{y_t} \in \mathbb{Z}[X_1, \ldots, X_r]$ of size $\leq C$ whether $\widetilde{F}(\widetilde{y_1}, \ldots, \widetilde{y_t}) \in (f_1, \ldots, f_s)$.

Recently, Győry and the author [8, 2011] proved the following result on unit equations over A in two unknowns:

Let a, b, c be non-zero elements of A and let be given representatives $\widetilde{a}, \widetilde{b}, \widetilde{c}$ for a, b, c. Suppose that $f_1, \ldots, f_s$ and $\widetilde{a}, \widetilde{b}, \widetilde{c}$ have total degrees at most d and logarithmic heights at most h where $d, h \geq 1$. Then for the solutions

x, y of

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

we have

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

where κ is an effectively computable absolute constant.

The method of proof of this result can be applied to other classes of Diophantine equations as well. To illustrate this, we give some effective results for Thue equations and hyper- and superelliptic equations over A, obtained jointly with Bérczes and Győry. We always use κ to denote an effectively computable absolute constant, but at each occurrence, its value may be different.

Let $F(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_0Y^n \in A[X,Y]$ be a binary form of degree $n \geq 3$ without multiple factors, and let $b \in A \setminus \{0\}$. Consider the equation

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

Baker [2, 1968] gave in the case $A = \mathbb{Z}$ an effective proof that (1) has only finitely many solutions. This was extended by Coates [7, 1968/69] to the case $A = \mathbb{Z}[(p_1 \cdots p_t)^{-1}]$ where the p_i are distinct primes and by Kotov and Sprindzhuk [10, 1973] to the case that A is the ring of S-integers in a number field. Győry [9, 1983] extended this effective finiteness result further to integral domains of the special shape $\mathbb{Z}[z_1, \ldots, z_q, w, g^{-1}]$, where $z_1, \ldots, z_q$ are algebraically independent, w is integral over $A_0 := \mathbb{Z}[z_1, \ldots, z_q]$, and $g \in A_0$. In his proof, Győry developed a specialization method, which we managed to extend to arbitrary finitely generated domains. This led to the following general result for Thue equations. As before, A is an integral domain containing $\mathbb{Z}$, isomorphic to $\mathbb{Z}[X_1, \ldots, X_r]/(f_1, \ldots, f_s)$.

Theorem 1 (Bérczes, E., Győry). *Let $\widetilde{a_0}, \ldots, \widetilde{a_n}, \widetilde{b}$ be representatives for the coefficients $a_0, \ldots, a_n$ of F and of b, and assume that these representatives, as well as $f_1, \ldots, f_s$, have total degrees $\leq d$ and logarithmic heights at most h. Then for the solutions of (1) we have*

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

Now let $F(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$, $b \in A \setminus \{0\}$, $m \in \mathbb{Z}_{\geq 2}$ and consider the hyper-/superelliptic equation

$$by^m = F(x) \quad \text{in } x, y \in A. \tag{2}$$

Assume that F has no multiple roots, and that F has degree $n \geq 3$ if $m = 2$ and degree $n \geq 2$ if $m \geq 3$. Again Baker[3, 1969] was the first to give an effective finiteness proof for the set of solutions of (2), in the case $A = \mathbb{Z}$. This was extended by Brindza [4, 1984] to the case that A is the ring of S-integers of a number field, and further[6, 1989] to the special class of finitely generated domains mentioned above considered by Győry. In the case $A = \mathbb{Z}$, Schinzel and Tijdeman [12, 1976] proved that if (2) has a solution $x, y \in \mathbb{Z}$ with $y \neq 0, \pm 1$, then m is bounded above by an effectively computable number depending only on F and b. Brindza [5, 1987] extended this to the case that A is the ring of S-integers in a number field, and Végső [14, 1994] to the class of domains considered by Győry.

Theorem 2 (Bérczes, E., Győry). *Let $\widetilde{a}_0, \ldots, \widetilde{a}_n, \widetilde{b}$ be representatives for the coefficients $a_0, \ldots, a_n$ of F and of b, and assume that these representatives, as well as $f_1, \ldots, f_s$, have total degrees $\leq d$ and logarithmic heights at most h. Then for the solutions of (2) we have*

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

Further, if (2) has a solution $x, y \in A$ with y not equal to 0 or to a root of unity, then

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

We sketch the proof of Theorem 1; the proof of Theorem 2 is essentially similar. Let as before $A = \mathbb{Z}[z_1, \ldots, z_r] \supset \mathbb{Z}$ be an integral domain. Assume that $z_1, \ldots, z_q$ are linearly independent, and that $z_{q+1}, \ldots, z_r$ are algebraic over $K_0 := \mathbb{Q}(z_1, \ldots, z_q)$. Choose $w \in A$ integral over $A_0 := \mathbb{Z}[z_1, \ldots, z_q]$ and choose $g \in A_0$ such that $A \subseteq B := \mathbb{Z}[z_1, \ldots, z_q, w, g^{-1}]$. Assume that w has degree D over K_0. Given $\mathbf{u} = (u_1, \ldots, u_q) \in \mathbb{Z}^q$ with $g(\mathbf{u}) \neq 0$, we can define a specialization homomorphism $\varphi_{\mathbf{u}} : B \to \overline{\mathbb{Q}}$ by mapping z_i to u_i for $i = 1, \ldots, q$. Then $\varphi_{\mathbf{u}}$ maps the Thue equation (1) over A to a Thue equation ($1_{\mathbf{u}}$) over the ring of $S_{\mathbf{u}}$-integers $O_{S_{\mathbf{u}}}$ in a number field $K_{\mathbf{u}}$, where both the number field $K_{\mathbf{u}}$ and the set of places $S_{\mathbf{u}}$ may depend on $\mathbf{u}$.

Now let $x, y \in A$ be a solution of (1). We can express x as $\sum_{i=0}^{D-1} P_i w^i / Q$, where $P_0, \ldots, P_{D-1}, Q \in \mathbb{Z}[z_1, \ldots, z_q]$. Using Mason's effective result for Thue equations over function fields [11, 1984] one can estimate the degrees of $P_0, \ldots, P_{D-1}, Q$. By applying Baker's method to the Thue equations ($1_{\mathbf{u}}$) for 'many' $\mathbf{u} \in \mathbb{Z}^q$, and then using linear algebra, one can estimate the coefficients of the P_i and Q. Up to this point, this outlines Győry's specialization method mentioned above. Using a recent effective result by

Aschenbrenner [1, 2004] for systems of inhomogeneous linear equations over polynomial rings over $\mathbb{Z}$, one can estimate the size $s(x)$ of x in terms of the total degrees and heights of the P_i and Q. The size $s(y)$ of the other unknown is estimated in the same way.

The above method of proof can by applied to various other classes of Diophantine equations. we would like to finish with an open problem. Consider the Thue-Mahler equation over an arbitrary finitely generated domain A,

$$F(x,y) \in A^* \quad \text{in } x,y \in A, \tag{3}$$

where $F \in A[X,Y]$ is a binary form of degree ≥ 3 without multiple factors. One can show that (3) has finitely many solutions $(x_1,y_1),\dots,(x_l,y_l)$, such that every other solution of (3) is expressable in the form $u(x_i,y_i)$ with $u \in A^*$, $i \in \{1,\dots,l\}$. Given an arbitrary finitely generated domain A, can one determine such (x_i,y_i) effectively?

References

[1] M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, J. Amer. Math. Soc. **17** (2004), 407–442.

[2] A. Baker, *Contributions to the theory of Diophantine equations*, Philos. Trans. Roy. Soc. London, Ser. A **263**, 173–208.

[3] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

[4] B. Brindza, *On S-integral solutions of the equation $y^m = f(x)$*, Acta Math. Hung. **44** (1984), 133–139.

[5] B. Brindza, *Zeros of polynomials and exponential diophantine equations*, Compos. Math. **61** (1987), 137–157.

[6] B. Brindza, *On the equation $f(x) = y^m$ over finitely generated domains*, Acta Math. Hung. **53** (1989), 377–383.

[7] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. **15** (1968/69), 279–305.

[8] J.-H. Evertse, K. Győry, *Effective results for unit equations over finitely generated integral domains*, submitted for publication, arXiv:1107:5756.

[9] K. Győry, *Bounds for the solutions of norm form, discriminant form and index form equations in finitely generated integral domains*, Acta Math. Hung. **42** (1983), 45–80.

[10] S.V. Kotov, V.G. Sprindzhuk, *An effective analysis of the Thue-Mahler equation in relative fields* (Russian), Dokl. Akad. Nauk. BSSR **17** (1973), 393–395; 477.

[11] R.C. Mason, *Diophantine Equations over Function Fields*, London Math. Soc. Lecure Notes Series 96, Cambridge Univ. Press, 1984.

[12] A. Schinzel, R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. **31** (1976), 199–204.

[13] H. Simmons, *The solution of a decision problem for several classes of rings*, Pacific J. Math. **34** (1970), 547–557.
[14] J. Végső, *On superelliptic equations*, Publ. Math. Debrecen **44** (1994), 183–187.