INTEGRAL POINTS ON GALOIS COVERS

Yuri Bilu

1. Introduction

Let C be a smooth projective curve of genus $\boldsymbol{g} = \boldsymbol{g}(C)$, defined over the field of rationals $\mathbb{Q}$, and $x \in \mathbb{Q}(C)$ a non-constant rational function on C. Let

$$C(x, \mathbb{Z}) := \{P \in C(\mathbb{Q}) : \ x(P) \in \mathbb{Z}\}$$

be the set of x-integral points on C. Siegel [26] has proved the following remarkable theorem.

Theorem 1.1 (Siegel). *Assume that either $\boldsymbol{g}(C) \geq 1$ or x has at least 3 distinct poles defined over $\bar{\mathbb{Q}}$. Then $|C(x, \mathbb{Z})| < \infty$.*

In the remaining case, where $\boldsymbol{g}(C) = 0$ and x has at most 2 poles, it is easy to decide whether the set $C(x, \mathbb{Z})$ is finite or infinite.

Indeed, assume first that x has only one pole, and denote it by P_0. Then P_0 is defined over $\mathbb{Q}$. Since $\boldsymbol{g}(C) = 0$, there exists $t \in \mathbb{Q}(C)$ such that $\mathbb{Q}(C) = \mathbb{Q}(t)$ and the pole of t is P_0. The function t is integral over $\mathbb{Q}[x]$. After multiplying t by a suitable integer, we may assume that t is integral over $\mathbb{Z}[x]$. So for any $P \in C(x, \mathbb{Z})$ we have $t(P) \in \mathbb{Z}$.

On the other hand, x is integral over $\mathbb{Q}[t]$. It follows that $ax = f(t)$ for some non-zero $a \in \mathbb{Z}$ and $f(t) \in \mathbb{Z}[t]$. Hence the set $C(x, \mathbb{Z})$ is infinite if the congruence

$$f(t) \equiv 0 \pmod{a}$$

has a solution, and $C(x, \mathbb{Z}) = \emptyset$ otherwise.

If x has exactly two distinct poles P_1 and P_2 then they are defined over a number field K of degree at most 2 over $\mathbb{Q}$. But, there is $t \in K(C)$ such that $\operatorname{div}(t) = P_1 - P_2$. After multiplying by an appropriate integer, we may assume that t is integral over $\mathbb{Z}[x]$. Also, there is a non-zero integer a such that at^{-1} is integral over $\mathbb{Z}[x]$. Hence for any $P \in C(x, \mathbb{Z})$

$$t(P) \in \mathcal{O}_K \text{ and } t(P) \text{ divides } a.$$

It follows that there are only finitely many possibilities for $t(P)$ when $K = \mathbb{Q}$ or K is an imaginary quadratic field. Therefore in these cases $C(x, \mathbb{Z})$ is finite.

In the remaining case, when K is a real quadratic field, denote by η its fundamental unit. Then there exists an effectively computable finite set $M \subset \mathcal{O}_K$ such that for any $P \in C(x, \mathbb{Z})$ we have $t(P) = \mu\eta^n$, where $\mu \in M$ and $n \in \mathbb{Z}$. Since x is integral over $K[t, at^{-1}]$, there exists $F(U, V) \in \mathcal{O}_K[U, V]$ and $\beta \in \mathcal{O}_K$ such that $\beta x = F(t, at^{-1})$. If for some $\mu \in M$ the exponential congruence

$$F(\mu\eta^n, a\mu^{-1}\eta^{-n}) \equiv 0 \pmod{\beta}$$

has a solution $n \in \mathbb{Z}$ then the set $C(x, \mathbb{Z})$ is infinite; otherwise, it is empty.

Thus, Siegel's theorem gives a criterion for the finiteness of the set of integral points.

In this context one should mention Mordell's conjecture, proved by Faltings [16]:

Theorem 1.2 (Faltings). *If $\boldsymbol{g}(C) \geq 2$ then $|C(\mathbb{Q})| < \infty$.*

The results of both Siegel and Faltings extend to arbitrary number fields and their rings of integers (or S-integers).

Unfortunately, all known proofs of Siegel's and Faltings' theorems are **non-effective**. This means that they give estimates for the **number** of integral (or rational) points[1], but nor for their **size**.

[1] We refer to Pacheco's contribution [19] for a survey of results on this topic. Mention only that Bombieri's [11] "elementary" proof of Mordell conjecture implies very explicit bounds for the number of rational points.

At present, no general effective method for the study of **rational** points is known, and effective bound for the size of rational points are obtained only in a few non-trivial cases, the most celebrated being Wiles' proof of Fermat's Last Theorem. (By "trivial" we mean the case when there is an "obvious" local obstruction, like for the curve $x^2 + x^4 + x^8 + y^6 + y^{10} = 0$.)

However, for integral points there is a quite powerful **method of Gelfond-Baker**, based on the following **Baker's inequality**:

Theorem 1.3 (Baker [1]). *Let $\alpha_1 \ldots \alpha_n \in$ be algebraic numbers distinct from 0 and 1, and $\varepsilon > 0$. Then there exists an effective constant c_{eff}, which depends on $\alpha_1 \ldots \alpha_n$ and ε, such that for any $b_1 \ldots b_n \in \mathbb{Z}$ one has either $\alpha_1^{b_1} \cdots \alpha_n^{b_n} = 1$ or*

$$\begin{gathered} \left|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1\right| \geq c_{\text{eff}} e^{-\varepsilon B}. \\ B = \max(|b_1| \ldots |b_n|) \end{gathered} \tag{1}$$

(Note that inequality $|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq e^{-c_{\text{eff}} B}$ is a trivial consequence of the product formula; Baker's main contribution was to replace B by εB.)

Many authors, including Baker himself, Feldman, Stark, Waldschmidt, Wüstholz, and others, worked on quantitative versions of Baker's inequality. The best result we know is due to Baker-Wüstholz [4] and Waldschmidt [31]:

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq e^{-c(n,d)\Omega \log B}, \tag{2}$$

where

$$\begin{aligned} d &= [\mathbb{Q}(\alpha_1 \ldots \alpha_n) \colon \mathbb{Q}], \\ \Omega &= \min\left(1, h(\alpha_1) \cdots h(\alpha_n)\right), \\ c(n,d) &= (nd)^{c'n}. \end{aligned}$$

Here $h(\cdot)$ stands for the absolute logarithmic height, and c' is an absolute effective constant.

Using Baker's inequality, Baker and others obtained effective upper bounds for the size of integral points on certain curves. For instance, Siegel's theorem is effective when $\boldsymbol{g}(C) \leq 1$:

Theorem 1.4. *If either*

$$\boldsymbol{g}(C) = 1$$

or

$$\boldsymbol{g}(C) = 0 \text{ and } x \text{ has at least } 3 \text{ poles}$$

then

$$\max_{P \in C(x,\mathbb{Z})} |x(P)| \leq c_{\text{eff}}(C, x) \tag{3}$$

The case $\boldsymbol{g}(C) = 1$ is due to Baker and Coates [3]. They obtained a huge explicit value for the constant $c_{\text{eff}}(C, x)$, which was improved by many authors, see [17, 23, 6]. The case "$\boldsymbol{g}(C) = 0$ and x has at least 3 poles" is a part of the folklore, though the first explicit bound was written down quite recently by Poulakis [21] (see also [6]).

When $\boldsymbol{g}(C) \geq 2$ only partial results are known. For instance, consider solutions $(x, y) \in \mathbb{Z} \times \mathbb{Q}$ of the **superelliptic equation**

$$ay^n = f(x), \tag{4}$$

where $f(x) = a_m x^m + \cdots + a_0 \in \mathbb{Z}[x]$ and $a \in \mathbb{Z} \setminus \{0\}$.

Theorem 1.5 (Baker [2], Brindza [12]) *Let C be a smooth model of the plane curve (4). If C has genus at least* 1 *then*

$$\max_{\substack{(x,y) \in \mathbb{Z} \times \mathbb{Q} \\ ay^n = f(x)}} |x| \leq c_{\text{eff}}(f, a, n). \tag{5}$$

An explicit expression for $c_{\text{eff}}(f, a, n)$ was obtained by many people, see [20, 25, 27, 28, 29]. The best published result is due to Voutier [30]:

$$c_{\text{eff}}(f, a, n) = e^{c_{\text{eff}}(m,n) H^{O_{\text{eff}}(m^8 n^2)}}, \tag{6}$$

where $H = \max(|a|, |a_0| \ldots |a_m|)$, and O_{eff} implies an absolute effective constant.

The author [5] and Dvornicich & Zannier [13] proved independently the following effective version of Siegel's theorem for Galois coverings:

Theorem 1.6. *If $\boldsymbol{g}(C) \geq 1$ and $\bar{\mathbb{Q}}(C)$ is a Galois extension of $\bar{\mathbb{Q}}(x)$ then*

$$\max_{P \in C(x,\mathbb{Z})} |x(P)| \leq c_{\mathrm{eff}}(C, x). \tag{7}$$

Baker's result on the superelliptic equation is a particular case of Theorem 1.6.

The author [9] obtained a quantitative version of Theorem 1.6. Let $y \in \mathbb{Q}(C)$ be such that $\mathbb{Q}(C) = \mathbb{Q}(x, y)$, and let the (x, y)-plane model of C be defined by $f(x, y) = 0$, where

$$f(X, Y) = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} X^i Y^j \in \mathbb{Z}[X, Y].$$

Theorem 1.7. *Assuming the hypothesis of Theorem 1.6, one has (7) with*

$$c_{\mathrm{eff}}(C, x) = e^{c_{\mathrm{eff}}(m,n) H^{O_{\mathrm{eff}}(mn^7 + m^2 n^4)}},$$

where $H = \max |a_{ij}|$, and O_{eff} means an absolute effective constant.

In particular, this improves on the bound (6) of Voutier.

However, more important than the improvement of (6) by Theorem 1.7 is the fact that this theorem gives a sharp quantitative result in a more general set-up.

We refer to [9] for a complete proof of this theorem. There we prove it for an arbitrary number field and a ring of S-integers in it.

The main novelty of our approach is reducing the problem directly to Baker's inequality, without the intermediate use of "linear unit equations", as it was customary before. This method was elaborated in our thesis [6], see also [8]. Recently we were able to apply it to numerical solution of certain Diophantine equations, see [7, 10].

Some further improvements are due to clever use of the Galois action, an idea which goes back to Voutier [30].

In the next section we indicate the main steps of the proof.

2. Proof of Theorem 1.7 (a sketch)

Step 1

For any $\alpha \in \bar{\mathbb{Q}} \cup \infty$ the field $\bar{\mathbb{Q}}(C)$ has the same ramification e_α over $\bar{\mathbb{Q}}(x)$ at all places above α (this is the point where we use the Galois condition). Hence by the Riemann-Hurwitz formula

$$0 \le 2\boldsymbol{g} - 2 = \sum_{\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}} \frac{n}{e_\alpha}(e_\alpha - 1) - 2n, \tag{8}$$

whence

$$\sum_{\alpha \in \bar{\mathbb{Q}} \cup \{\infty\}} (1 - e_\alpha^{-1}) \ge 2,$$

and so

$$\sum_{\alpha \in \bar{\mathbb{Q}}} (1 - e_\alpha^{-1}) > 1.$$

Therefore one of the following conditions is true:

(a) there exist distinct $\alpha, \beta \in \bar{\mathbb{Q}}$ such that $e_\alpha \ge 3$ and $e_\beta \ge 2$;

(b) there exist pairwise distinct $\alpha, \beta, \gamma \in \bar{\mathbb{Q}}$ such that $e_\alpha = e_\beta = e_\gamma = 2$.

By an easy Galois argument, one concludes further that one of the following conditions is true:

(a1) there exist distinct $\alpha, \beta \in \bar{\mathbb{Q}}$, conjugate over $\mathbb{Q}$, such that $e_\alpha = e_\beta \ge 3$.

(a2) there exist distinct $\alpha \in \mathbb{Q}$ and $\beta \in \bar{\mathbb{Q}}$ such that $e_\alpha \ge 3$, $e_\beta \ge 2$ and $[\mathbb{Q}(\beta)\colon \mathbb{Q}] \le 2$.

(b1) there exist pairwise distinct $\alpha, \beta, \gamma \in \bar{\mathbb{Q}}$, conjugate over $\mathbb{Q}$ such that $e_\alpha = e_\beta = e_\gamma = 2$.

(b2) there exist pairwise distinct $\alpha \in \mathbb{Q}$ and $\beta, \gamma \in \bar{\mathbb{Q}}$, such that $e_\alpha = e_\beta = e_\gamma = 2$, and $[\mathbb{Q}(\beta)\colon \mathbb{Q}] = [\mathbb{Q}(\gamma)\colon \mathbb{Q}] \le 2$.

In the sequel we assume (a1) (the other cases are treated similarly).

Let $D(X)$ be the discriminant of $f(X,Y)$ with respect to Y. Then α and β are roots of $D(X)$ of order at least $\frac{n}{p}(p-1) \geq \frac{2}{3}n$, where $p = e_\alpha$. Therefore

$$N_1 := [\mathbb{Q}(\alpha) \colon \mathbb{Q}] = [\mathbb{Q}(\beta) \colon \mathbb{Q}] \leq \frac{(2n-2)m}{(2/3)n} \leq 3m.$$

Step 2

Let ξ_p be a primitive p-th root of unity. For $k \in \{1 \ldots p\}$ put

$$\varphi_k = \left((x-\alpha)^{1/p} - \xi_p^k (x-\beta)^{1/p}\right)^p$$

This φ_k is algebraic over the field $\mathbb{Q}(C)$ of degree $N_2 \leq N_1^2 p \leq 9m^2 p$, and for any $P \in C(\mathbb{Q})$ we fix one of the N_2 possible values of $\varphi_k(P)$.

Proposition 2.1. *There exists a positive integer Δ with the following property. If $P \in C(x, \mathbb{Z})$ then $\varphi_k(P)$ belongs to a number field of discriminant dividing Δ.*

Proof. It is easy to see that the field $\bar{\mathbb{Q}}(C)(\varphi_k)$ is unramified over $\bar{\mathbb{Q}}(C)$ everywhere except may be the poles of x. Therefore the proposition is a consequence of Chevalley-Weil theorem [18, 24].

In actual estimating the Δ we heavy used of the quantitative Eisenstein theorem due to Dwork-Robba-Schmidt-van der Poorten [14, 15, 22]. This was the most involved part of the proof.

Note that Proposition 2.1 remains true with $\varphi_k = (x-\alpha)^{1/p} - \xi_p^k (x-\beta)^{1/p}$, but the degree of φ_k over $\mathbb{Q}(C)$ is bounded only by $N_1^2 p^2$. With our definition of φ_k we obtain a bound which is $1/p$ times the latter, which sharps the estimate for Δ.

Step 3

Proposition 2.2. *There exists a positive real number A, such that for any*

$P \in C(x,\mathbb{Z})$ we have $\varphi_k(P) = \mu\eta$, where η is a Dirichlet unit, and the height of the algebraic number μ does not exceed A.

Proof. We have

$$\varphi_1 \cdots \varphi_p = (\beta - \alpha)^p.$$

Since every $\varphi_k(P)$ is an algebraic integer, the result follows.

Step 4

Since $p \geq 3$, the function $\psi = (1+\xi_p)^p \varphi_1/\varphi_2$ is non-constant. Therefore there are finitely many P with $\psi(P) = 1$, and their size can be easily estimated.

Now assume that $\psi(P) \neq 1$. A trivial calculation shows that

$$\psi(P) = 1 + O_{\text{eff}}\left(x(P)^{-1}\right),$$

where all constants implied by O_{eff} or $\ll_{\text{eff}}$ depend effectively on f. On the other hand, by Propositions 2.1 and 2.2, $\psi(P)$ is the product of a bounded algebraic number by a Dirichlet unit, lying in a field of bounded discriminant, say,

$$\psi(P) = \eta_0 \eta_1^{b_1} \cdots \eta_r^{b_r}.$$

Also, it is easy to see that $B = \max(|b_1| \ldots |b_r|)$ satisfies

$$\log|x(P)| \ll_{\text{eff}} B \ll_{\text{eff}} \log|x(P)|.$$

Hence

$$|\eta_0 \eta_1^{b_1} \cdots \eta_r^{b_r} - 1| \leq e^{-O_{\text{eff}}(B)},$$

which contradicts Baker's inequality when B is large (the left-hand side is non-zero because $\psi(P) \neq 1$). We used Baker's inequality in the sharp form (2), due to Baker-Wüstholz [4], and Waldschmidt [31].

Acknowledgment. I am pleased to thank Arnaldo Garcia, Eduardo Esteves and all the organizers of the XIV-th Brazilian Algebra School, for the highly creative atmosphere of the meeting, and for having invited me to give a talk there. I am also grateful to Amilkar Pacheco for valuable discussions, and the anonymous referee for many useful comments and suggestions.

References

[1] Baker, A., *Linear forms in the logarithms of algebraic numbers I*, Mathematica 13 (1966), 204–216; II, ibid. 14 (1967), 102–107; III, ibid. 14 (1967); 220–224; IV, ibid. 15 (1968), 204–216.

[2] Baker, A., *Bounds for the solutions of the hyperelliptic equations*, Proc. Camb. Phil. Soc., 65 (1969), 439–444.

[3] Baker, A. and Coates, J., *Integer points on curves of genus 1*, Proc. Camb. Phil. Soc. 67 (1970), 592–602.

[4] Baker, A.; Wüstholz, G., *Logarithmic forms and Group Varieties*, J. reine und angew. Math. 442 (1993), 19–62.

[5] Bilu, Yu. (Belotserkovski), *Effective analysis of a new class of Diophantine equations (Russian)*, Vestsi Akad. Navuk BSSR, Ser. Fiz.-Math. Navuk, 1988, no. 6, 34–39, 125

[6] Bilu, Yu., *Effective analysis of integral points on algebraic curves*, thesis, Beer Sheva, 1993.

[7] Bilu, Yu., *Solving superelliptic Diophantine equations by the method of Gelfond–Baker*, preprint 94-09, Mathématiques Stochastiques, Univ. Bordeaux 2, 1994.

[8] Bilu, Yu., *Effective analysis of integral points on algebraic curves*, Israel J. Math 90 (1995), 235–252.

[9] Bilu, Yu., *Quantitative Siegel's theorem for Galois coverings*, Compositio Math., 106 (1997), 125–158.

[10] Bilu,Yu. and Hanrot, G., *Solving superelliptic Diophantine equations by Baker's method*, Compositio Math., to appear.

[11] Bombieri, E., *The Mordell conjecture revisited*, Ann. Scu. Norm. Pisa 17 (1990), 615–640.

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

[13] Dvornicich, R. and Zannier, U., *Fields containing values of algebraic functions*, Ann. Sc. Norm. Sup. Pisa Cl. Sci. Ser. IV 21 (1994), 421–443.

[14] Dwork, B.M. and Robba, B., *On natural radii of p-adic convergence*, Trans. Amer. Math. Soc. 256 (1979), 199–213.

[15] Dwork, B.M. and van der Poorten, A. J., *The Eisenstein constant*, Duke Math. J. 65(1992), 23–43; Corrections: 76 (1994), 669–672.

[16] Faltings, G., *Endlichkeitssätze für abelche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366; Erratum: 75 (1984), p.381.

[17] Kotov, S.V. and Trelina, L. A., *S-ganze Punkte auf elliptischen Kurven*, J. reine und angew. Math. 306 (1979), 28–41.

[18] Lang, S., *Fundamentals of Diophantine Geometry*, Springer, 1983.

[19] Pacheco, A., *Rational Points on Families of Curves*, this volume.

[20] Poulakis, D., *Solutions entières de l'équation $Y^m = f(x)$*, Sém. Th. Nom. Bordeaux 3 (1991), 187–199.

[21] Poulakis, D., *Points entiers sur les courbes de genre 0*, Colloquium Math. 66 (1993), 1–7.

[22] Schmidt, W. M., *Eisenstein theorem on power series expansions of algebraic functions*, Acta Arithm. 56(1990), 161–179.

[23] Schmidt, W. M., *Integer points on curves of genus 1*, Compositio Math. 81 (1992), 33–59.

[24] Serre, J.-P., *Lectures on the Mordell-Weil Theorem*, Aspects of math. E15, Vieweg 1989.

[25] Shorey, T.N. and Tijdeman, R., *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge, 1986.

[26] Siegel, S.L., *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss Akad. Wiss. Phys.-Math. Kl., 1929, Nr. 1.

[27] Sprindžuk, V. G., *The arithmetic structure of integral polynomials and class numbers* (Russian), Trudy Mat. Inst. Steklov 143 (1977), 152–174; English transl.: Proc. Steklov Inst. Math. 1980, issue 1, 163–186.

[28] Sprindžuk, V. G., *Classical Diophantine Equations in Two Unknowns* (Russian), Nauka, Moscow, 1982; English transl.: Lecture Notes in Math. 1559, Springer, 1994.

[29] Trelina, L. A., *On S-integral solutions of the hyperelliptic equation* (Russian), Dokl. Akad. Nauk BSSR 22 (1978), 881–884.

[30] Voutier, P. M., *An Upper Bound for the Size of Integral Solutions to $Y^m = f(X)$*, J. Number Theory 53 (1995), 247–271.

[31] Waldschmidt, M., *Minorations de combinaisons linéares de logarithmes de nombres algébriques*, Canadian J. Math. 45 (1993), 176–224.

Institut für Mathematik,
Technische Universität Graz,
Steyrergasse 30,
8010 Graz AUSTRIA;
e-mail: `yuri@weyl.math.tu-graz.ac.at`.