Atti Accademia Nazionale Lincei Classe Scienze Fisiche Matematiche Naturali

Rendiconti Lincei Matematica e Applicazioni

Enrico Bombieri

Diophantine Equations in Low Dimensions

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Serie 9, Vol. **11** (2000), n.S1 (Mathematics Towards The Third Millenium), p. 11–29.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLIN_2000_9_11_S1_11_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni, Accademia Nazionale dei Lincei, 2000.

Rend. Mat. Acc. Lincei
s. 9, fasc. spec. 2000: 11-29

ENRICO BOMBIERI

DIOPHANTINE EQUATIONS IN LOW DIMENSION

ABSTRACT. — This lecture is a survey of recent results in the theory of diophantine equations, especially for dimension 1. The unit equation and its generalizations are examined in detail, as well as Baker's theory and the consequences of the *abc*-conjecture.

KEY WORDS: Diophantine equations; Diophantine approximation; Unit equation; Thue equation.

1. A SURVEY OF DIOPHANTINE EQUATIONS

In this lecture, we shall consider some aspects of the theory of diophantine equations, reviewing recent progress and ending with speculative thoughts about the future.

Let us consider first diophantine equations associated with integral points on curves. Perhaps the simplest example, arising from Euclid's algorithm for the greatest common divisor of two integers, is **Euclid's equation**:

The linear equation $ax - by = 1$ *with* a, b *coprime integers, to be solved in integers* x, y.

A smallest solution (x_0, y_0) is obtained using Euclid's algorithm for the greatest common divisor of two integers; this amounts to finding the continued fraction of a/b. The general solution is in parametric form $(x, y) = (bt + x_0, at + y_0)$, with t any integer.

Another important equation is **Pell's** [1] **equation**:

$$Dx^2 + 1 = y^2 \text{ to be solved in integers } x, y,$$

D a positive integer not a square, considered by the Indian mathematicians Brahmagupta and Bhaskara in the twelfth century, and by Fermat, Wallis and Brouncker in the seventeenth century. A smallest positive solution (x_0, y_0) can be found via the continued fraction of $\sqrt{D}$. The general solution is $x + \sqrt{D}y = \pm(x_0 + \sqrt{D}y_0)^m$ with $m \in \mathbb{Z}$. Solutions form an infinite abelian group of rank 1.

Integral points on general curves also pose interesting questions. An important special case is **Thue's equation**:

$$\text{The equation } a_0x^r + a_1x^{r-1}y + \cdots + a_ry^r = m \text{ in integers } x, y,$$

where the coefficients a_i are integers and $m \neq 0$. Thue [19] proved that such an equation has only finitely many solutions if the associated equation

$$a_0\xi^r + a_1\xi^{r-1} + \cdots + a_r = 0$$

[1] According to L.E. Dickson, there is no indication that John Pell ever worked on this equation, and the name comes from an erroneous attribution by Euler.

has at least three distinct complex roots ξ. Thue's theorem dates back to 1909. We had to wait until 1966 for Alan Baker to produce an algorithm for finding all solutions of a general Thue's equation.

The determination of rational points on algebraic curves is also a very classical problem. Perhaps the oldest example of a diophantine equation, known to Babylonian mathematicians, is the equation of **Pythagorean triples**, namely

$$\textit{The equation } x^2 + y^2 = z^2 \textit{ in non-zero integers } x, y, z,$$

which corresponds to finding rational points on the unit circle. The general solution is given in parametric form by

$$(a, b, c) = (m(p^2 - q^2), 2mpq, m(p^2 + q^2)),$$

with m, p and q arbitrary integers.

A natural, and historically intractable, generalization of the Pythagoric equation is the notorious **Fermat's equation**:

$$x^n + y^n = z^n \textit{ in non-zero integers } x, y, z,$$

famous for Fermat's brief statement that he had found a «truly marvellous proof» that it had no solutions for $n \geq 3$. Fermat himself gave a proof for an equation which covered the case $n = 4$ using, for the first time, his celebrated *method of descent.* Attempts to prove Fermat's statement led to the development of algebraic number theory (Kummer, Lamé, Cauchy, Dedekind). Eventually, Fermat's statement was solved in the affirmative by A. Wiles and R. Taylor in 1995 [22, 18], using deep new methods from the theory of modular forms and Galois representations, after 360 years of failed attempts by hundreds of mathematicians and thousands of amateurs.

Rational points on elliptic curves were studied already in antiquity, with the Greek mathematician Diophantus. The associated equation, for an elliptic curve in Weierstrass form, is

$$\textit{the cubic } y^2 = x^3 - ax - b \textit{ to be solved in rational numbers } x, y,$$

(with the non-singularity condition $\Delta := 4a^3 + 27b^2 \neq 0$, the case $\Delta = 0$ is easy), and more generally one may consider non-singular cubic equations $f(x, y) = 0$ with f a polynomial of degree 3. As conjectured by Poincaré and proved by Mordell and later generalized by Weil to the case of rational points on an abelian variety, solutions form an abelian group of finite rank, the Mordell-Weil group. There is no known algorithm guaranteed to find a basis of generators of the Mordell-Weil group although it is conjectured, with good evidence, that the existing algorithm, based on descent and used in practice, always works.

These equations can be viewed as special cases of:

$$\textit{the equation } f(x, y) = 0 \textit{ to be solved in rational numbers } x, y.$$

Here one has the celebrated Faltings's theorem, stating that such an equation has only finitely many solutions if the plane curve $f(x, y) = 0$ is irreducible with genus $g \geq 2$,

as conjectured by Mordell back in 1922. However, in this general situation there is no known algorithm guaranteed to find all solutions.

Let us look briefly at Thue's equation.

We may attack the problem as follows. Suppose for simplicity that $a_0 = 1$. The left-hand side is a homogeneous polynomial in two variables, so it factors over the complex numbers:

$$\prod_{i=1}^{r}(x - \alpha_i y) = m.$$

Now x and y are integers and $x - \alpha_i y$ is an algebraic integer in the number field $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$, so each $x - \alpha_i y$ is a divisor of m in the ring R of integers of K. The ring R does not in general have unique factorization, but this is a technical difficulty which can be overcome in several ways, for example by going to a larger subring $R' \subset K$ obtained by localization of R at a suitable finite set of prime ideals.

Hence assume R has unique factorization up to units (a unit in R is an element u such that both u and u^{-1} are in R). Then m has only finitely many divisors (up to units) and we must have $x - \alpha_i y = d_i u_i$ where the d_i's belong to a finite set, $d_1 d_2 \cdots d_r = m$ and the u_i's are units with $u_1 u_2 \cdots u_r = 1$.

By the assumption of Thue's theorem, we may assume that α_1, α_2, α_3 are distinct. But then we have three distinct linear forms $x - \alpha_i y$ in only two variables, so they must be linearly dependent over K. This gives a relation

$$ad_1 u_1 + bd_2 u_2 = cd_3 u_3$$

and, after dividing by $cd_3 u_3$, we get the **unit equation**

$$AX + BY = 1, \quad \text{with } X, Y \text{ units in the ring } R.$$

The group U of units of R is a finitely generated abelian group (Dirichlet) so the problem consists in studying the intersection of the subvariety $AX + BY = 1$ of the commutative algebraic group $XY \neq 0$ with the finitely generated subgroup $\Gamma = U \times U$. If $g_1, \ldots, g_s$ are generators of U we get the **exponential diophantine equation**

$$Ag_1^{m_1} g_2^{m_2} \cdots g_s^{m_s} + Bg_1^{n_1} g_2^{n_2} \cdots g_s^{n_s} = 1.$$

More generally, we may consider a subvariety X of a multiplicative group G, a finitely generated subgroup Γ and ask about the structure of the intersection $X \cap \Gamma$.

We may also view the problem of determining the rational points on a curve of genus $g \geq 2$ as a far deeper generalization of the above setting. Any curve C of genus $g \geq 2$ can be embedded as a proper subvariety of the jacobian $J(C)$, and the set of rational points of C can be recovered as the intersection $C \cap \Gamma$ where Γ is the finitely generated Mordell-Weil group of the abelian variety $J(C)$.

More generally, we may ask about the structure of the set $X \cap \Gamma$ where X is a proper subvariety of an abelian variety A and Γ is a finitely generated subgroup of A.

This is summarized as follows:

MULTIPLICATIVE GROUPS	ABELIAN VARIETIES
ANALOGIES:	
affine	compact
integral points	rational points
FINITENESS for the rank:	
yes (Dirichlet)	yes (Mordell-Weil)
FINITENESS for $X \cap \Gamma$, $\dim(X) = 1$:	
yes (Thue, Siegel)	yes (Faltings)
FINITENESS for $X \cap \Gamma$, $\dim(X) > 1$:	
yes (Schmidt)	yes (Faltings)
ALGORITHMS for generators:	
yes (Dirichlet)	?
ALGORITHMS for $X \cap \Gamma$, $\dim(X) = 1$:	
yes (Baker)	?
ALGORITHMS for $X \cap \Gamma$, $\dim(X) > 1$:	
?	?

The finiteness results in higher dimension are as follows. Let G be either a multiplicative group $\mathbb{G}_m^n$ or an abelian variety A defined over a number field K. Translates of algebraic subgroups H of G provide obvious examples of subvarieties of G which may have infinite intersection with a finitely generated subgroup Γ. It may happen that a subvariety $X \subset G$ contains such a translate of an algebraic subgroup H, so we want to remove them from X. We define

$$X^\circ = X - \bigcup \{gH : gH \subset X,\ g \in G,\ \dim(H) \geq 1\}.$$

THEOREM 1. *If Γ is a finitely generated subgroup of G, then $X^\circ \cap \Gamma$ is finite.*

This deep theorem is due to Schlickewei and Schmidt if $G = \mathbb{G}_m^n$ and to Faltings [11] in the much more difficult case $G = A$.

If $G = \mathbb{G}_m^n$, one can say something more about the structure of $Y := X - X^\circ$. After a coordinate change compatible with the group structure on G, the set Y becomes a finite union of cartesian products $H \times Z$ with H a subgroup of G of positive dimension and Z a subvariety of G. Moreover, the degrees of the coordinate changes, of H and of Z are bounded solely in terms of the degree of X and the dimension n.

Once this is done, we can study Z, and so on.

The most important case for applications is that of a linear subvariety X, giving the **general unit equation**

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1\,, \quad \mathbf{x} \in \Gamma.$$

The component Y which must be removed to obtain finiteness is simply the set of points for which there is a vanishing subsum

$$a_{j_1}x_{j_1} + a_{j_2}x_{j_2} + \cdots + a_{j_s}x_{j_s} = 0.$$

Solutions with vanishing subsums are in a certain sense degenerate solutions.

The theorem of Schlickewei and Schmidt shows that the general unit equation has only a finite number of non-degenerate solutions.

Conversely, the special case of the general unit equation implies the full result of Schmidt and Schlickewei. The idea is simple: To study the polynomial equation (in multi-index notation $a_J\mathbf{x}^J = a_{j_1,\ldots,j_n}x_1^{j_1}\cdots x_n^{j_n}$)

$$\sum_J a_J\mathbf{x}^J = 1\,,$$

one introduces new variables x_J and solves first for

$$\sum_J a_Jx_J = 1$$

and afterwards for the system $\mathbf{x}^J = x_J$.

Unfortunately, no algorithm is known for solving explicitly the unit equation in dimension $n > 2$. The question of finding effective algorithms for the Mordell-Weil theorem, Faltings's theorem and the theorem of Schlickewei and Schmidt represents a major challenge in the theory of diophantine equations.

There are also extensions of these results to more general classes of commutative algebraic groups, but we will not discuss them in this expository paper.

2. The unit equation in dimension 2

If $n = 2$ we know a fair amount of precise information about the unit equation. This involves

a) Upper and lower bounds for the number of solutions.
b) Upper bounds for the size of solutions.
c) Location of solutions: gaps and clustering.

We begin with four examples of equations with many solutions.

Example 1. An example of Erdös, Stewart and Tijdeman of a subgroup of $\mathbb{Q}^*$ yielding a large number of solutions. Let $N \geqq 2$ and let $\mathcal{M}$ be the set of integers up

to x whose prime factors do not exceed $x^{1/N}$. Then

$$|\mathcal{M}| \geqq \frac{\pi(x^{1/N})^N}{N!} > 2x/(\log x)^N$$

if $x \geqq 17^N$. Consider the $|\mathcal{M}|^2$ sums $n + n'$ with $n, n' \in \mathcal{M}$. At least one sum $n + n' = b$ occurs $|\mathcal{M}|^2/(2x) > x/(\log x)^{2N}$ times.

It follows that if $\Gamma = U \times U$ with U the group $U = \langle b, p \leq x^{1/N} \rangle$ then there is a unit equation in Γ with $x/(\log x)^{2N}$ solutions, provided $x \geqq 17^N$. By the Prime Number Theorem, Γ has rank $r \sim 2Nx^{1/N}/\log x$. If we choose N in an optimal way, we easily verify that the number of solutions is at least

$$e^{(c+o(1))\sqrt{r/\log r}}$$

for a positive constant c.

EXAMPLE 2. This example is due to J. Berstel (see [4] for references on this and related results). Consider the equation $a\xi^m + b\eta^m = 1$ for varying m, corresponding to a group $\Gamma = (\xi, \eta)^{\mathbb{Z}}$ of rank 1. We want to find a, b, ξ, η such that it has the maximum number of solutions for $m \in \mathbb{Z}$. We may assume that $m = 0$ is a solution. Suppose that $m = 1$ is also a solution, so the equation becomes $(\eta - 1)\xi^m + (1 - \xi)\eta^m - (\eta - \xi) = 0$. If we fix two other solutions, say m_1 and m_2, we determine pairs (ξ, η) as common points of the two curves

$$(y - 1)x^{m_1} + (1 - x)y^{m_1} - (y - x) = 0,$$

$$(y - 1)x^{m_2} + (1 - x)y^{m_2} - (y - x) = 0.$$

For general m_1 and m_2, this gives a group Γ of rank 1 such that the equation $a\xi^m + b\eta^m = 1$ has the four solutions $0, 1, m_1, m_2$.

Remarkably, the choice $m_1 = 4$ and $m_2 = 6$ yields two additional solutions $m = 13$ and $m = 52$ and in the end an equation $a\xi^m + b\eta^m = 1$ with the six solutions $0, 1, 4, 6, 13, 52$.

EXAMPLE 3. The following example gives an equation $u + v = 1$ with at least 2532 solutions $u, v \in \Gamma$, and $\operatorname{rank}(\Gamma) = 5$. Let $K = \mathbb{Q}(\alpha)$ with α the real root $\alpha > 1$ of the Lehmer equation

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1 = 0.$$

This equation has another real root $1/\alpha$ and 8 complex roots all of absolute value 1; we shall refer to the map $\alpha \mapsto 1/\alpha$ as real conjugation in $\mathbb{Q}(\alpha)$. The Mahler height of α is $M(\alpha) = \alpha = 1.176281^+$ and is widely conjectured to be the infimum of the Mahler height of an algebraic number not a root of unity – the so-called Lehmer Conjecture. The group Γ of units of K has rank 5: $\Gamma = \{\pm 1\} \times \langle \alpha, 1 - \alpha, 1 + \alpha, 1 + \alpha + \alpha^2, 1 + \alpha - \alpha^3 \rangle$. Now an extensive computer search for solutions of the corresponding unit equation produced a remarkable total of 2532 solutions.

EXAMPLE 4. The following remark is due to H.W. Lenstra. For a prime p, consider the cyclotomic field $\mathbb{Q}(\sqrt[p]{1})$ and the corresponding unit equation. If $u + v = 1$ and u,

v are not real then $\overline{u} + \overline{v} = 1$ is another solution of the unit equation. Now $\varepsilon := \overline{u}/u$ is an algebraic integer all of whose conjugates have absolute value 1 so, by a theorem of Kronecker, ε and, similarly, $\varepsilon' := \overline{v}/v$ are roots of unity in $\mathbb{Q}(\sqrt[p]{1})$. Solving the system $u + v = 1$, $\varepsilon u + \varepsilon' v = 1$ we get $u = (\varepsilon' - 1)/(\varepsilon' - \varepsilon)$, $v = (1 - \varepsilon)/(\varepsilon' - \varepsilon)$. Conversely, given distinct roots of unity ε, ε' in $\mathbb{Q}(\sqrt[p]{1})$, not equal to 1, we obtain a solution u, v of the unit equation. Thus the number of complex solutions of the unit equation $x + y = 1$ in $\mathbb{Q}(\sqrt[p]{1})$ is $(p-1)(p-2)$.

The number of solutions in the maximal real subfield K_p of $\mathbb{Q}(\sqrt[p]{1})$ is much larger. A computer search using cyclotomic units produced 3 solutions in K_5, 42 solutions in K_7, 570 solutions in K_{11}, 1830 solutions in K_{13}, 11700 solutions in K_{17} and 28398 solutions in K_{19}.

Thus the question arises of determining the maximal number of solutions for the equation $ax + by = 1$ with (x, y) in a multiplicative group Γ of fixed rank r. We begin with a nice result of Beukers and Schlickewei [4].

THEOREM 2. *Let Γ be a subgroup of $(\overline{\mathbb{Q}}^*)^2$ with $\operatorname{rank}(\Gamma) = r < \infty$. Then the equation*

$$ax + by = 1, \qquad (x, y) \in \Gamma$$

has at most 512^{r+1} solutions.

By refining their methods, K.K. Choi has obtained the improved bound 241×70^r. It is noteworthy that the number of solutions is bounded solely in terms of the rank r and is independent of the field of definition and heights of generators of the group Γ.

Theorem 2 has been extended to the higher dimensional case by Evertse, Schlickewei and Schmidt [10], proving the uniform bound $\exp((6n)^{3n}(r+1))$ for the number of non-degenerate solutions, in a multiplicative group of rank r, of the unit equation in n variables. The analogous result for abelian varieties lies even deeper and it has been recently obtained by Rémond [15].

Let $N(r)$ be the maximum number of solutions of such an equation. By Example 1 and Theorem 2 we have

$$\sqrt{r/\log r} \ll \log N(r) \ll r.$$

Beukers and Schlickewei have proved that $N(1) \leq 61$. Examples 2, 3 and 4 give $N(1) \geq 6$, $N(2) \geq 42$, $N(8) \geq 570$, $N(10) \geq 2532$, $N(14) \geq 11700$, $N(16) \geq \geq 28398$.

Perhaps $\log N(r) \gg r^{1-\varepsilon}$ for any $\varepsilon > 0$.

The proof of Theorem 2 depends on a clever use of hypergeometric identities to obtain a gap principle sufficient to give a bound for the number of solutions (x, y) with large height $h(x) + h(y)$. A bound for the number of solutions with small height is obtained using an important result of S. Zhang [24], together with a classical covering argument. A special case of Zhang's result is as follows.

THEOREM 3 (Zhang). *There are two absolute constants $c > 0$ and $N_0 > 0$ with the following property. Let $ab \neq 0$. Then there are at most N_0 algebraic number solutions (x, y) of $ax + by = 1$ with $h(x) + h(y) \leq c$.*

Zhang's proof of Theorem 3 is not elementary, but elementary proofs leading to good values of N_0 and c have been found by several authors. The following extension of Theorem 3 is due to Bombieri and Zannier [8].

THEOREM 4. *There are two constants $c > 0$ and $N_0 > 0$, depending only on n and d, with the following property. Let X be a subvariety of $\mathbb{G}_m^n$ of degree d. Then there are at most N_0 points $\mathbf{x} = (x_1, \dots, x_n)$ in X° with algebraic coordinates and height $h(\mathbf{x}) = h(x_1) + \cdots + h(x_n) \le c$.*

How does one approach such a result? It is a simple consequence of the following equidistribution theorem due to Bilu [5].

EQUIDISTRIBUTION THEOREM (Bilu). *Let $\{\xi_i\}$ be an infinite sequence of distinct non-zero algebraic numbers of degree d_i and suppose that*

$$\lim_{i\to\infty} h(\xi_i) = 0.$$

Let $K_i = \mathbb{Q}(\xi_i)$. Then the sequence of probability measures

$$\mu_i := \frac{1}{d_i} \sum_{\sigma: K_i \to \mathbb{C}} \delta_{\sigma\xi_i}$$

converges in the weak topology to the uniform probability measure on the unit circle $\mathbb{T}$.*

An analogous statement for abelian varieties is a hard theorem of Szpiro, Ullmo and Zhang [17].

3. BOUNDS FOR SOLUTIONS

As mentioned before, Baker showed how to solve effectively a general unit equation in two variables. He obtained his result as an application of his theory of linear forms in logarithms. In its simplest version, one can state it as follows. Let $\alpha_i \in \mathbb{C}$, $i = 1, \dots, n$ be non-zero algebraic numbers and let us fix a determination $\log\alpha_i$ of their logarithms. Consider a non-zero linear combination

$$\Lambda := b_1 \log\alpha_1 + b_2 \log\alpha_2 + \cdots + b_n \log\alpha_n$$

with integer coefficients b_i. We want to get non-trivial lower bounds for $|\Lambda|$. We have

$$\alpha := e^\Lambda = \alpha_1^{b_1}\alpha_2^{b_2}\cdots\alpha_n^{b_n}$$

therefore

$$0 < |\alpha - 1| \le |\Lambda| e^{|\Lambda|}.$$

A trivial lower bound for $|\alpha - 1|$ is readily obtained (take the norm over $\mathbb{Q}$ of the algebraic number $\alpha - 1$). If we define, for ξ algebraic of degree d, the modified height

$$h'(\xi) = \max\left(h(\xi), \frac{1}{d}|\log\xi|, \frac{1}{d} \right)$$

then we have

$$\log|\Lambda| \geq -d^2 \max(B, e)(h'(\alpha_1) + \cdots + h'(\alpha_n) + \log 2)$$

where $B = \max |b_i|$. We refer to this as the trivial estimate, of order $-CB$ as $B \to \infty$.

A non-trivial estimate is an estimate of order $-o(B)$ as $B \to \infty$.

A. Baker [1] in 1966 obtained for the first time explicit non-trivial lower bounds for $\log|\Lambda|$ in the general case (2) which were remarkably good with respect to B, in fact of order $(\log B)^{cn}$.

Many mathematicians, besides Baker himself, have contributed to the theory of linear forms in logarithms. I may mention here Stark (introduction of Kummer extensions), Feldman (introduction of better bases for polynomials), Wüstholz, Masser and Philippon (sharp zero estimates), Waldschmidt and his school (precise numerical estimates for $n = 1, 2$ particularly useful in applications), Van der Poorten, Kunrui Yu (linear forms in p-adic logarithms, which have important applications of their own), Masser, Wüstholz, Hirata-Kohno (linear forms in elliptic and abelian logarithms).

THEOREM 5 (Baker and Wüstholz [2]). *With the notation as before we have*

$$\log|\Lambda| \geq -2400(15nd)^{2n+4}(\log(eB)) \prod_{i=1}^{n} h'(\alpha_i).$$

The proof is quite difficult involving functions of several complex variables, a delicate extrapolation technique, algebraic number theory, and «zero estimates» on general commutative algebraic groups. Kunruy Yu [23] has recently obtained the extension of this result to the p-adic case, where new difficulties have to be overcome.

The applications of Baker's theory are legion. To mention a few:

1) the solution of the class number 1 and class number 2 problems;

2) the effective solution of the unit equation $x + y = 1$, and in turn the solution of Thue's equation and of the hyperelliptic and superelliptic diophantine equations

$$y^m = a_0 x^n + a_1 x^{n-1} + \cdots + a_n;$$

3) an effective improvement of Liouville's lower bound for the approximation of a real algebraic number α of degree d, namely the Baker-Feldman theorem [12] that

$$|\alpha - p/q| \geq c(\alpha) q^{-d+\delta(\alpha)}$$

for suitable (small) computable positive constants $c(\alpha)$, $\delta(\alpha)$;

4) the theorem of Tijdeman [20] showing that the Catalan equation $x^m - y^n = 1$ has only finitely many solutions in positive (x, y, m, n) with $m, n \geq 2$.

One may ask how far we are from proving Catalan's conjecture that $9 = 3^2$ and $8 = 2^3$ are the only non-trivial consecutive powers. The proof of Tijdeman's theorem requires Baker's theorem with $n = 3$ and the very delicate $O(\log B)$ dependence on B.

(2) Before Baker's work, there were non-trivial estimates only for forms in two logarithms, with the work of Gelfond and Schneider around 1930. Baker's success in the general case was a real breakthrough.

This is not easy to obtain and the proof in the end leads to huge bounds for m, n. The best bounds obtained so far by these methods are (one may assume m, n prime numbers) of order 10^{31}.

There are applications to other areas, such as algebra, algebraic topology, dynamical systems and ordinary and partial differential equations.

Recently, an alternative approach to effective methods has been obtained through techniques of diophantine approximation, see [6, 7]. Let $g_1, \dots, g_n$ be multiplicatively independent algebraic numbers in a field K of degree d and let

$$\Gamma = \langle g_1, \dots, g_n \rangle \oplus \mathrm{tors}(K),$$

so Γ has rank n. We want to know how close elements Ag of a coset $A\Gamma$ can come to 1, assuming $Ag \neq 1$. An easy lower bound is

$$|Ag - 1| \geq (2H(Ag))^{-d}$$

and the goal is to improve it to

$$|Ag - 1| \geq (2H(Ag))^{-\kappa d}$$

for any $\kappa > 0$, provided $H(Ag)$ is sufficiently large. The basic idea is a reduction to the case $n = 1$ (linear forms in only two logarithms!), which is achieved by means of an elementary trick as follows.

Write $g = \varepsilon g_1^{m_1} \dots g_n^{m_n}$. Now let Q, N be positive integers and let $L = \mathrm{lcm}(1, 2, \dots, Q)$. By Dirichlet's theorem on simultaneous approximation, there are integers p_i and q, $1 \leq q \leq Q$, such that

$$\left| \frac{m_i}{LN} - \frac{p_i}{q} \right| \leq \frac{1}{Q^{1/n} q}, \quad i = 1, \dots, n.$$

Now $r = L/q$ is an integer, therefore we have the following statement:

there exists an integer r with $LN \leq r \leq QLN$ such that $|m_i - rp_i| \leq rQ^{-1/n}$ for $i = 1, \dots, n$.

This means that if we set $a = \varepsilon A \prod g_i^{m_i - rp_i}$ and $g' = \prod g_i^{p_i}$ we have

$$|a(g')^r - 1| = |Ag - 1|,$$

whence

$$|a^{1/r} g' - 1| \ll H(a^{1/r} g')^{-\kappa dr}$$

if the inequality we want to prove is not satisfied. This means that $(g')^{-1}$ is a remarkably good approximation to $a^{1/r}$.

Since $h(a^{1/r}) \leq (1/r)h(A) + nQ^{-1/n} \max h(g_i)$ is also small we have good control on the height of the number to be approximated and direct methods based on diophantine approximation can be used here.

The method works equally well in the p-adic case.

As an example, one can prove the following theorem.

THEOREM 6. *Let K be a number field of degree d and let v be a place of K, dividing a rational prime p in the case where v is a finite place.*

Let Γ *be a finitely generated subgroup of* K^* *and let* $g_1, \ldots, g_n$ *be generators of* Γ/tors. *Let* $g \in \Gamma$, $A \in K^*$ *and* $\kappa > 0$ *be such that*

$$0 < |1 - Ag|_v < H(Ag)^{-\kappa}.$$

Define $Q = \prod h'(g_i)$. *Then we have*

$$h(Ag) \leq c(\kappa, n, d, v) Q \max(h'(A), Q)$$

where $c(\kappa, n, d, v)$ *is an explicit function of* κ, n, d *and* v.

As an application one obtains the Baker-Feldman theorem in the following form.

THEOREM 7. *Let* K *be a number field,* v *a place of* K *and* α *an algebraic number of degree* $d \geq 3$ *over* K *which is also an element of the complete field* K_v. *Then we have for* $\beta \in K$ *the effective lower bound*

$$|\alpha - \beta|_v \gg H(\beta)^{-d+\delta/R}$$

where R *is the regulator of the field* K *and* $\delta > 0$ *depends only on* v, d *and the degree of* K *over* $\mathbb{Q}$.

4. THE FUTURE: THE *abc*-CONJECTURE

The *abc*-conjecture of Masser and Oesterlé is a typical example of a simple statement which can be used to unify and motivate a number of results in number theory, which otherwise would be scattered statements without a common link.

Although a pessimist may conclude that the ease with which the *abc*-conjecture may be applied to solve notoriously difficult problems is only a reflection of how difficult its proof is likely to be, one should keep in mind that its function field analogue is quite easy to prove, thus providing a unified method of attack for many problems in the arithmetic of function fields. Moreover, whatever its status may be in the classical case, it is likely that exceptions, if any, will be extremely rare and therefore most of the conclusions obtained by its application are also likely to be valid, and provable in some instances by using different methods.

The *abc*-conjecture is also a useful tool for guessing the right answer when analyzing specific problems, hence its significance should not be too easily discounted.

***abc*-conjecture (strong form).** *Let* $\varepsilon > 0$ *be a positive real number. Then there is a constant* $C(\varepsilon)$ *with the following property:*

For any triple a, b, c *of coprime positive integers with* $a + b = c$, *we have*

$$c \leq C(\varepsilon) \Big(\prod_{p \mid abc} p \Big)^{1+\varepsilon},$$

where $\prod_p$ *ranges over the distinct prime divisors of* abc.

Here 'strong' refers to the fact that this statement is supposed to hold for every positive ε. If we assume that it only holds for some fixed $\varepsilon > 0$, *e.g.* $\varepsilon = 1$, then we refer to it as the weak *abc*-conjecture.

In this respect, we note that the weak *abc*-conjecture appears to be almost as useful as the strong form of it. The statement:

$$(*) \qquad a + b \leqq \Big(\prod_{p \mid ab(a+b)} p \Big)^2$$

for every pair a, b of positive coprime integers has in fact been conjectured by several authors as a likely explicit form of the weak *abc*-conjecture.

In what follows, the conductor $\mathrm{Cond}(N)$ of an integer N is the product of all distinct primes dividing N:

$$\mathrm{Cond}(N) = \prod_{p \mid N} p.$$

Suppose $x^n + y^n = z^n$ is a non-trivial solution in coprime positive integers of the famous Fermat equation. Let us take $a = x^n$, $b = y^n$, $c = z^n$. Since $ab(a + b) = (xyz)^n$ we deduce

$$z^n \leqq \Big(\prod_{p \mid (xyz)^n} p \Big)^2 = \Big(\prod_{p \mid xyz} p \Big)^2 \leqq (xyz)^2 \leqq z^6.$$

Since $z > 1$, this implies $n \leqq 6$. It is well-known that the Fermat equation has no non-trivial solutions for $n = 3$ (Euler), $n = 4$ (Fermat), $n = 5$ (Dirichlet), therefore we see that $(*)$ implies Fermat's Last Theorem.

The same argument applies to the Catalan conjecture that 8 and 9 are the only two consecutive perfect powers in the sequence of natural integers. If we apply $(*)$ to the Catalan equation $x^m + 1 = y^n$, we find

$$y^n \leqq (xy)^2 < y^{2\frac{n}{m}+2}$$

and $n(m - 2) < 2m$. This leaves us with the possibilities $m = 2$, or $n = 2$, or both $n \leqq 5$ and $m \leqq 5$, which can be analyzed directly.

Another application concerns Marshall Hall's conjecture on the size of integer solutions of the Mordell equation $y^2 = x^3 + k$, namely $x \ll_\varepsilon |k|^{2+\varepsilon}$, $y \ll_\varepsilon |k|^{3+\varepsilon}$.

The following more explicit statement has been proposed by Baker.

CONJECTURE (Baker). *There is an absolute constant K, such that if a, b, c are three coprime integers with $a + b + c = 0$ we have*

$$\max(|a|, |b|, |c|) \leqq K \cdot \Big(\prod_{p \mid abc} (p/\varepsilon) \Big)^{1+\varepsilon}$$

for every ε with $0 < \varepsilon \leqq 1$.

The example $2 + 109 \times 3^{10} = 23^5$ has a very high *abc*-**ratio** $\log c / \log(\prod_{p \mid abc} p)$, namely 1.62991. This was found by E. Reyssat, by searching for very good rational

approximations to numbers of type $a^{1/n}$. Note

$$109^{\frac{1}{5}} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{77733 + \ldots}}}}$$

A beautiful application of a strong form of the *abc*-conjecture (however, over number fields) was given by Elkies [9], who showed that it implies the Mordell conjecture. A key step of the proof consists in extending it to general polynomial equations $f(a, b) = 0$; this was also independently done by Langevin. We describe the ideas involved here, since they are quite striking.

We begin with the following result due to G.V. Belyĭ [3].

BELYĬ'S LEMMA. *Let $g : C \to C'$ be a non-constant morphism between two non-singular curves C, C', defined over a number field K. Let S be any finite set of points on $C(\overline{K})$. Then there is a non-constant rational function $h : C' \to \mathbb{P}^1$, defined over K, such that the composite morphism $f = h \circ g : C \to \mathbb{P}^1$ is ramified only over $0, 1, \infty$ and moreover $f(S) \subseteq \{0, 1, \infty\}$.*

PROOF.

Reduction to $C = \mathbb{P}^1$ and to the identity morphism. We choose any non-constant rational function $g_1 : C' \to \mathbb{P}^1$ defined over K and replace g by the composition $g_1 \circ g$, increasing S so as to include the ramification set of $g_1 \circ g$. This reduces the original problem to the case in which $C = \mathbb{P}^1$ is the projective line defined over $\mathbb{Q}$ and g is the identity morphism.

The proof is completed by the following descending double induction on the degree and cardinality of the components of S.

Lowering the degree of a point in S. Let $\alpha \in S$ be algebraic of degree $d \geqq 2$ and let $p(x) = a_0 x^d + \cdots + a_d$ be its defining polynomial over $\mathbb{Z}$. Consider the morphism $p : \mathbb{P}^1 \to \mathbb{P}^1$. The ramification set S_1 of p consists of the roots of $p'(x) = 0$ and ∞. This allows us to replace S by the set $S' = p(S \cup S_1)$. Since $p(\alpha) = 0$ and since the degree of elements of $p(S_1)$ is at most $d - 1$, by composition of morphisms of this type we reach a situation in which S consists only of rational points and ∞.

Lowering the cardinality of S. Suppose now that S consists only of rational points and ∞ and has cardinality $|S| \geqq 4$. By applying a projective automorphism of $\mathbb{P}^1$ we may assume that S contains $0, 1, \infty$. Let $\lambda = A/(A + B)$ be a fourth point in S, where A, B are integers with $A, B, A + B \neq 0$. Consider the rational function $h(x) = cx^A(1 - x)^B$, where c is a constant to be determined. Since

$$\frac{h'}{h} = \frac{A}{x} - \frac{B}{1 - x}$$

vanishes only at $x = \infty$ or $x = A/(A + B)$, the morphism $h : \mathbb{P}^1 \to \mathbb{P}^1$ is ramified only at $0, 1, \infty$ and $A/(A + B)$. We have $h(\{0, 1, \infty\}) \subset \{0, 1, \infty\}$ because

A, B, $A+B \neq 0$, also

$$h\left(\frac{A}{A+B}\right) = c\,\frac{A^A B^B}{(A+B)^{A+B}};$$

therefore, if we choose $c = (A+B)^{A+B}A^{-A}B^{-B}$ and correspondingly

$$h(x) = \frac{(A+B)^{A+B}}{A^A B^B}\, x^A (1-x)^B,$$

we get $h(\{0, 1, \infty, \lambda\}) \subset \{0, 1, \infty\}$ and h ramifies only over 0, 1, ∞. Thus we may replace S by $\{0, 1, \infty\} \cup h(S-\lambda)$, decreasing the cardinality of S by 1, thereby completing the second induction step and the proof.

It is worth noting that this construction is not entirely of a geometric nature because the sequence of compositions of elementary maps is determined by the arithmetic.

Here is an explicit example. Consider $g : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ where $g(x) = 2x^3 - 3ax^2 + 1$, a is an integer, $a \neq 0, 1$, and take S to be the set of roots of g.

Step 1. In order to descend the field of definition of S we note that $g'(x) = 6x(x-a)$ so g is ramified at $\{0, a, \infty\}$. Now take $S' = g(S \cup \{0, a, \infty\}) = \{0, 1, \infty, 1-a^3\}$.

Step 2. Now we construct the Belyĭ map for the new set S'. Here $A = 1-a^3$, $B = a^3$, whence

$$h(x) = (1-a^3)^{-1+a^3} a^{-3a^3} x^{1-a^3} (1-x)^{a^3}$$

and $f = h \circ g$ is the desired Belyĭ map for the set S.

For example, if $a = -1$ we get

$$f(x) = \frac{(1+3x^2+2x^3)^2}{4x^2(3+2x)}$$

$$1 - f(x) = -\frac{(1+x)^4(1-2x)^2}{4x^2(3+2x)}$$

and the identity $f(x) + (1-f(x)) = 1$ can be rewritten as

$$(1+3x^2+2x^3)^2 - (1+x)^4(1-2x)^2 - 4x^2(3+2x) = 0.$$

The last identity is an example of three polynomials P, Q, R without common roots such that $P+Q+R=0$ and

$$\max(\deg(P), \deg(Q), \deg(R)) = \#\{\textit{distinct roots of } PQR\} - 1.$$

In general, the *abc*-inequality for polynomials asserts that for three polynomials P, Q, R with $P+Q+R=0$ and without common roots the number of distinct roots of PQR is at least the maximum of the degrees of P, Q, R plus 1. It is a theorem of Stothers [16] that all extremal cases (*i.e.* with the minimum number of distinct roots) originate from Belyĭ maps.

The Belyĭ construction characterizes algebraic curves defined over a number field. A precise formulation is contained in the following theorem.

THEOREM 8. *Let C be an irreducible curve defined over $\mathbb{C}$. The following conditions are equivalent:*

(a) C is isomorphic to a curve defined over $\overline{\mathbb{Q}}$.

(b) There exists a covering $C \longrightarrow \mathbb{P}^1$ unramified outside three points.

(c) There are a subgroup Γ of finite index of the principal congruence subgroup $\Gamma(2)$ of the modular group $\mathrm{SL}_2(\mathbb{Z})$ and a Zariski open set Z of C such that Z may be identified with the quotient $\mathbb{H}/\Gamma$ of the upper half-plane $\mathbb{H}$ by Γ.

Moreover, if $C/\overline{\mathbb{Q}}$ and $S \subset C(\overline{\mathbb{Q}})$ is finite, Γ can be chosen such that S is a subset of the cusps of $\mathbb{H}/\Gamma$.

The proof combines Belyĭ's Lemma, the uniformization of the sphere punctured at three points and Riemann's Existence Theorem.

The following interesting result is due independently to Elkies, Oesterlé and Langevin.

THEOREM 9. *The strong abc-conjecture over $\mathbb{Q}$ implies Roth's Theorem over $\mathbb{Q}$.*

PROOF. Let α be an algebraic number of degree $n \geqq 3$ and let $g(x)$ be its minimal polynomial over $\mathbb{Z}$. We apply Belyĭ's Lemma to the morphism $g : \mathbb{P}^1 \to \mathbb{P}^1$ and the set S consisting of the roots of $g(x)$, obtaining a rational function $h(x)$ such that the composition $f(x) = h(g(x))$ has the following properties:

(i) the morphism $f : \mathbb{P}^1 \to \mathbb{P}^1$ is unramified outside $0, 1, \infty$;

(ii) we have $f(S) = h(0) \subset \{0, 1, \infty\}$.

Without loss of generality, we may suppose that $h(0) = 0$.

Let $f(x) = u(x)/w(x)$ where u, w are polynomials with integral coefficients without common factors, and let $v(x) = w(x) - u(x)$. Let $d = \max(\deg(u), \deg(w))$ be the degree of the morphism f, let $U(X, Y) = Y^d u(X/Y)$, and similarly $V(X, Y)$ and $W(X, Y)$, be the associated homogeneous forms of degree d, and consider the factorizations of U, V, W into irreducible factors U_i, of degree n_i,

$$U(X, Y) = u_0 U_1(X, Y)^{m_1} \cdots U_r(X, Y)^{m_r}$$
$$V(X, Y) = v_0 U_{r+1}(X, Y)^{m_{r+1}} \cdots U_s(X, Y)^{m_s}$$
$$W(X, Y) = w_0 U_{s+1}(X, Y)^{m_{s+1}} \cdots U_t(X, Y)^{m_t}$$

in the ring $\mathbb{Z}[X, Y]$.

Since we assume $h(0) = 0$, we see that we may take $n_1 = n$ and $U_1(X, Y) = G(X, Y) = Y^n g(X/Y)$, the irreducible homogeneous binary form associated to the algebraic number α. The following is easy to prove.

LEMMA. *There is a positive integer D, bounded in terms of the height and degree of the rational function $f(x)$, such that if p, q are coprime integers then*

$$\mathrm{GCD}(U(p, q), V(p, q), W(p, q)) \mid D.$$

Now we complete the proof as follows.

We may suppose that α is real. Let p/q be a rational approximation to α and let

$$D_0 = \mathrm{GCD}(U(p, q), V(p, q), W(p, q)).$$

We may further assume that $U(p, q)V(p, q)W(p, q) \neq 0$. We set $a = U(p, q)/D_0$, $b = V(p, q)/D_0$, $c = W(p, q)/D_0$ and apply the *abc*-inequality to the relation $a + b = c$. The conductor $\prod_{p|abc} p$ of abc is a divisor of

$$u_0 v_0 w_0 U_1(p, q) U_2(p, q) \cdots U_t(p, q)$$

hence, recalling that $U_1(p, q) = G(p, q)$ and $U_i(p, q) \ll_f q^{\deg(U_i)}$, we get

$$\prod_{p|abc} p \ll_f |G(p, q)|\, q^K$$

where

$$K = -\deg(U_1) + \sum_{i=1}^{t} \deg(U_i) = -n + \sum_{i=1}^{t} \deg(U_i).$$

Next, we note that since $f(\alpha) = 0$ we must have that $1 - f(p/q)$ is bounded away from 0 as soon as $|\alpha - p/q|$ is sufficiently small, which we may suppose. Thus we have $|b| \gg_f q^d$, with an implied constant depending only on the height and degree of $f(x)$.

In view of these considerations, the *abc*-inequality yields

$$q^d \ll_{\varepsilon, f} (|G(p, q)|\, q^K)^{1+\varepsilon}$$

from which it follows that

$$|G(p, q)| \gg_{\varepsilon, f} q^{d - K - d\varepsilon/(1+\varepsilon)}.$$

It remains to evaluate $d - K$. To this end, we apply Hurwitz's genus formula to the ramified covering $f : \mathbb{P}^1 \to \mathbb{P}^1$. The ramification occurs only over $0, 1, \infty$, and we get

$$-2 = d \cdot (-2) + \sum_{i=1}^{t} (m_i - 1) \deg(U_i).$$

Moreover, we have

$$3d = \deg(f^{-1}(\{0, 1, \infty\})) = \sum_{i=1}^{t} m_i \deg(U_i).$$

From the last two displayed equations we find

$$\sum_{i=1}^{t} \deg(U_i) = d + 2$$

and finally $d - K = d + n - \sum \deg(U_i) = n - 2$. We conclude that

$$(**) \qquad |G(p, q)| \gg_{\varepsilon, f} q^{n - 2 - \varepsilon d/(1+\varepsilon)}.$$

Since $G(p, q) = q^n g(p/q)$ and $g(\alpha) = 0$, the mean-value theorem shows that

$$G(p, q) = q^n \left(g(p/q) - g(\alpha)\right) = q^n \left(\frac{p}{q} - \alpha\right) g'(\xi)$$

for some point ξ between p/q and α. Since p/q is close to α and $g'(\alpha) \neq 0$, we see that $g'(\xi)$ is bounded away from 0, giving

$$\left|\frac{p}{q} - \alpha\right| \gg q^{-n}|G(p, q)|.$$

Comparison with (**) yields the theorem.

As already remarked by Langevin [14], this argument proves more than Roth's Theorem, namely

THEOREM 10. *Assume the strong abc-conjecture over* $\mathbb{Q}$. *Then for a form* $F(x, y) \in \in \mathbb{Z}[x, y]$ *without square factors and of degree* $d \geq 3$, *and for all coprime integers* m, n, *we have*

$$\prod_{p|F(m,n)} p \gg_{\varepsilon, F} \max(|m|, |n|)^{d-2-\varepsilon}.$$

If we take $F(x, y) = xy(x + y)$ we recover the strong *abc*-conjecture over $\mathbb{Q}$.

A special case is

COROLLARY (Langevin). *Assume the strong abc-conjecture over* $\mathbb{Q}$. *Then for a polynomial* $f(x) \in \mathbb{Z}[x]$ *with* $f(0) \neq 0$, *without square factors and of degree* $d \geq 2$, *and for all integers* n, *we have*

$$\prod_{p|f(n)} g \gg_{\varepsilon, f} |n|^{d-1-\varepsilon}.$$

For the proof, it suffices to apply Theorem 10 to the form $F(x, y) = y^{d+1}f(x/y)$ of degree $d + 1$ and take $(x, y) = (n, 1)$.

Finally, Vojta [21] has shown how the *abc*-conjecture can be viewed as an analogue in number fields of Nevanlinna's Second Fundamental Theorem (with ramification term) for meromorphic functions, much in the same way as Roth's Theorem may be viewed as the analogue in number fields of Nevanlinna's Second Fundamental Theorem but without ramification term. This, and the coherence of the implications provided by the *abc*-conjecture may be considered as the strongest evidence up to date for its validity, at least over the rational field $\mathbb{Q}$.

5. AN UNUSUAL APPLICATION OF THE *abc*-CONJECTURE

We conclude this expository lecture with an interesting application, due to Granville [13], of the *abc*-conjecture to a classical problem of analytic number theory.

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree d without square factors and such that the sequence $\{f(n)\}$, $n = 1, 2, 3, \ldots$ has no fixed square divisor (to avoid trivial cases such as $f(x) = x(x + 1)(x + 2)(x + 3)$, which is always divisible by 4 for $x \in \mathbb{Z}$).

The following conjecture was proposed over 70 years ago in connection with applications of the theory of sieves.

CONJECTURE. *The sequence* $\{f(n)\}$ *contains infinitely many square-free integers. More*

precisely, the sequence of integers n such that $f(n)$ is square-free has positive density:

$$\#\{n \le x : f(n) \text{ is square} - \text{free}\} \sim c(f)x$$

for some constant $c(f) > 0$.

THEOREM 11. *The above conjecture is a consequence of the abc-conjecture.*

PROOF. Let D be the discriminant of f and define, for a prime p, the integer $\rho(p)$ to be the number of solutions of the congruence $f(a) \equiv 0 \pmod{p}$. If p does not divide the discriminant of f then any such solution a to the above congruence lifts uniquely to a solution mod p^2, as one sees using Hensel's Lemma.

Thus solutions mod p^2 fall into $\rho(p)$ arithmetic progressions mod p^2. The number of integers up to x not in these progressions is

$$\left(1 - \frac{\rho(p)}{p^2}\right) x + O(\rho(p))$$

and in particular such integers form a sequence of density

$$c_p(f) = 1 - \frac{\rho(p)}{p^2}.$$

Now an easy application of the inclusion-exclusion principle shows that the number of integers $n \le x$ for which $f(n)$ has no prime factors $p^2 | f(n)$ with $p \le \sqrt{\log x}$ is asymptotic to

$$\left\{ \prod_{p \nmid D} \left(1 - \frac{\rho(p)}{p^2}\right) \prod_{p | D} c_p(f) \right\} \cdot x = c(f)\, x.$$

The number of integers $n \le x$ for which $p^2 | f(n)$ and $\sqrt{\log p} < p < x$ is majorized by

$$\ll \left(\sum_{p > \sqrt{\log x}} \frac{\rho(p)}{p^2} \right) \cdot x + \sum_{p < x} \rho(p) \ll \frac{x}{\sqrt{\log x}},$$

and thus is negligible in our counting.

It remains to show that the sequence of integers n for which $p^2 | f(n)$ for some prime $p \ge x$ has zero density. Until now, sieve methods combined with various clever additional ideas have been used to prove this fact for polynomials $f(x)$ of degree at most 3, but this approach appears to fail if the degree of $f(x)$ is 4 or more. However, one can use the Corollary to Theorem 10 to conclude the proof in a single stroke.

We choose an integer m larger than the distance of any two roots of $f(x)$ and another positive integer l which is at our disposal. Consider the polynomial

$$g(x) = f(x) f(x + m) \cdots f(x + lm)$$

and note that the assumption on m ensures that $g(x)$ too has no square factor.

By Theorem 10, Corollary, the strong *abc*-conjecture implies that

$$\prod_{p | g(n)} p \gg_{g,\varepsilon} n^{\deg(g) - 1 - \varepsilon}.$$

Therefore, noting that $g(n)$ has order $n^{\deg(g)}$, we see that if $g(n) = uv^2$ we must have $uv \gg n^{\deg(g)-1-\varepsilon}$ and hence $v \ll n^{1+\varepsilon}$.

This shows that of the integers $f(n), f(n+m), f(n+2m), \ldots, f(n+lm)$ only one can be divisible by p^2 for some prime $p \geq n$ and, splitting the integers into m progressions mod m, only m of the integers $f(n), f(n+1), \ldots, f(n+lm)$ may admit such a square factor. In particular, the density of integers n for which $f(n)$ admits a square factor p^2 with $p \geq n$ is at most $m/(lm) = 1/l$. Since l can be chosen arbitrarily large, the set of such integers n has density 0, concluding the proof.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers I*. Mathematika, 13, 1966, 204-216.

[2] A. Baker - G. Wüstholz, *Logarithmic forms and group varieties*. J. reine angew. Math., 442, 1993, 19-62.

[3] G.V. Belyĭ, *On the Galois extensions of the maximal cyclotomic field*. Izv. Akad. Nauk SSSR, 1979, 267-276 (in Russian).

[4] F. Beukers - H.P. Schlickewei, *The equation $x + y = 1$ in finitely generated groups*. Acta Arithm., 78, 1996, 189-199.

[5] Yu. Bilu, *Limit distribution of small points on algebraic tori*. Duke Math. J., 89, 1997, 465-476.

[6] E. Bombieri, *Effective diophantine approximation on $\mathbb{G}_m$*. Ann. Sc. Norm. Sup. Pisa Cl. Sc., s. 4, 20, 1993, 61-89.

[7] E. Bombieri - P.B. Cohen, *Effective diophantine approximation on $\mathbb{G}_m$ II*. Ann. Sc. Norm. Sup. Pisa Cl. Sc., s. 4, 24, 1997, 205-225.

[8] E. Bombieri - U. Zannier, *Algebraic points on subvarieties of $\mathbb{G}_m^n$*. Int. Math. Res. Notices, 7, 1995, 333-347.

[9] N.D. Elkies, *ABC implies Mordell*. Int. Math. Res. Notices, 1, 1991, 127-132.

[10] J.-H. Evertse - H.P. Schlickewei - W.M. Schmidt, *Linear equations in variables which lie in a multiplicative group*. Annals of Math., submitted.

[11] G. Faltings, *Diophantine approximation an Abelian varieties*. Annals of Math., 133, 1991, 549-576.

[12] N.I. Feldman, *An effective refinement of the exponent in Liouville's theorem*. Izv. Akad. Nauk SSSR, 35, 1971, 973-990; Math. USSR Izv., 5, 1971, 985-1002.

[13] A. Granville, *ABC allows us to count squarefrees*. Int. Math. Res. Notices, 19, 1998, 991-1009.

[14] M. Langevin, *Sur quelques conséquences de la conjecture (abc) en arithmétique et logique* (Symposium on *Diophantine Problems*, Boulder, Co., 1994). Rocky Mountain J. Math., 26, 1996, 1031-1042.

[15] G. Rémond, *Décompte dans une conjecture de Lang*. Inventiones Math., to appear.

[16] W.W. Stothers, *Polynomial identities and Hauptmoduln*. Quart. J. Math. Oxford, s. (2), 32, 1981, 349-370.

[17] L. Szpiro - E. Ullmo - S. Zhang, *Equidistribution des petits points*. Inventiones Math., 127, 1997, 337-347.

[18] R. Taylor - A. Wiles, *Ring-theoretic properties of certain Hecke algebras*. Annals of Math., 142, 1995, 553-572.

[19] A. Thue, *Über Annäherungwerte algebraischer Zahlen*. J. reine angew. Math., 135, 1909, 284-305.

[20] R. Tijdeman, *On the equation of Catalan*. Acta Arithm., 29, 1976, 197-209.

[21] P. Vojta, *A more general ABC conjecture*. Int. Math. Res. Notices, 21, 1998, 1103-1116.

[22] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*. Annals of Math., 142, 1995, 443-551; Acta Arithm., 89, 1999, 337-378.

[23] K. Yu, *p-adic logarithmic forms and group varieties*. Acta Arithm., 89, 1999, 337-378.

[24] S. Zhang, *Positive line bundles on arithmetic varieties*. J. Amer. Math. Soc., 8, 1995, 187-221.

Institute for Advanced Study
Princeton, NJ 08540 (U.S.A.)