Proceedings of the International Congress of Mathematicians
Helsinki. 1978

Exponential Diophantine Equations

R. Tijdeman

1. Historical introduction. Many questions in number theory concern perfect powers, numbers of the form a^b where a and b are rational integers with $a>1$, $b>1$. To mention a few:

(a) Is it possible that for $n\geqslant 3$ the sum of two nth powers is an nth power?

(b) Is 8, 9 the only pair of perfect powers which differ by 1?

(c) Is it possible that the product of consecutive integers, $(x+1)(x+2)\ldots(x+m)$, is a perfect power?

(d) Does a given polynomial with integer coefficients represent (infinitely many) perfect powers at integer points?

(e) Can a number with identical digits in the decimal scale be a perfect power?

A common feature of these problems is that they can be restated in the form of a diophantine equation in which exponents occur as variables. Problem (a) leads to the equation $x^n+y^n=z^n$ in integers $n\geqslant 3$, $x>1$, $y>1$, $z>1$ which is still unsolved in spite of Fermat's claim and all efforts thereafter. Problem (b) was posed by Catalan in 1844 and corresponds to the equation $x^m-y^n=1$ in integers $m>1$, $n>1$, $x>1$, $y>1$. Problem (c) goes back to Liouville who gave a partial solution in 1857. The complete solution was obtained by Erdős and Selfridge in 1975. They showed that $\prod_{j=1}^{m}(x+j)=y^n$ has no solutions in integers $m>1$, $n>1$, $x\geqslant 1$, $y>1$. Problem (d) is stated here in a general form, but special cases were investigated long ago. In 1850 V. A. Lebesgue proved that x^2+1 is never a perfect power for integral x. It follows from a more general result of Legendre in 1798 that x^3-y^3 is not a power of 2 for $x>y>1$. Ramanujan conjectured in 1913 that $2^3, 2^4, 2^5, 2^7$ and 2^{15} are the only powers of 2 assumed by the polynomial x^2+7 for integral x. In 1948 Nagell proved that the corresponding equation $x^2+7=2^n$ in integers $n>1$, $x\geqslant 1$ indeed has no further solutions. Problem (e) is still open. In 1810 P. Barlow stated that no square has all its digits alike. It follows from the work of Ljunggren, Obláth, Shorey and Tijdeman that the corresponding equation $a(10^m-1)/(10-1)=y^n$ in integers $1\leqslant a<10$, $m>1$, $n>1$, $y>1$ has no solutions unless $a=1$ and $n\geqslant 23$.

2. Methods for solving exponential diophantine equations. We consider equations $f(x_1^{m_1}, x_2^{m_2}, \dots, x_k^{m_k})=0$ in positive integers $m_1, m_2, \dots, m_k, x_1, x_2, \dots, x_k$ subject to certain conditions, where f is a polynomial with integer coefficients. In this section we distinguish three different approaches to such equations and give some examples of results obtained in that way. The most elementary attack to find all solutions of an exponential equation is the use of

(i) *Divisibility properties of rational integers.* The solution of Problem (c) by Erdős and Selfridge belongs to this type. In 1952 LeVeque proved that for fixed a, b the equation $a^x-b^y=1$ has at most one solution $x\geqslant 1$, $y\geqslant 1$ except for the case $a=3$, $b=2$. In this case there are exactly two solutions, as was proved by Lewi Ben Gerson (1288–1344). It was only in 1964 that Chao Ko proved that x^2-1 is never a perfect power if $x>3$. The corresponding results for x^2+1 and $x^3\pm 1$ had been proved by V. A. Lebesgue in 1850 and Nagell in 1921 respectively, but in their methods certain irrational numbers play a role.

(ii) *Algebraic methods.* Divisibility properties of numbers in certain algebraic number fields are used in several solutions of exponential equations. Most proofs of Ramanujan's assertion on the equation $x^2+7=2^n$ are based on properties of numbers in $Q(\sqrt{-7})$, a field with unique factorization. Another useful tool is the p-adic method of Skolem. It was exploited by Skolem, Chowla and Lewis in 1959 to give another solution of the equation $x^2+7=2^n$ and in 1945 by Skolem to give an algorithm for determining all solutions of certain equations of the form $a_1^{m_1}\dots a_k^{m_k}-b_1^{n_1}\dots b^{n_l}=c$ in positive integers $m_1, \dots, m_k, n_1, \dots, n_l$, where $a_1, \dots, a_k$, $b_1, \dots, b_l$, c are given positive integers. The finiteness of the number of solutions had been proved by Pólya in 1918 who applied a third type of methods.

(iii) *Approximation methods.* Pólya showed that his assertion is an immediate consequence of a result of Thue on binary forms. Thue's work was improved by Siegel in 1921. In 1933 Mahler proved a p-adic analogue of Siegel's result and deduced that the equation $x+y=z$ in coprime integers x, y, z composed of fixed primes has only finitely many solutions. In 1955 Roth improved upon Siegel's work and this was generalized by W. M. Schmidt in 1970. Six years later Dubois and Rhin and Schlickewei showed that a p-adic analogue of Schmidt's result implies that the equation $x_1+x_2+\dots+x_n=0$ in integers which are pairwise coprime and composed of fixed integers, has only finitely many solutions. A disadvantage of the method is that it is ineffective; no upper bounds for the solutions can be obtained by the Thue–Siegel–Roth–Schmidt method.

Siegel, and later Baker, developed work of Thue based on hypergeometric functions. Their results were applied by Inkeri in 1972 and by Shorey and Tijdeman in 1976 to the equation $(x^m-1)/(x-1)=y^n$. Very recently Beukers obtained a further extension, which enabled him to prove that the equation $x^2+D=p^n$ in integers $n>1$, $x\geqslant 1$ has at most four solutions when $D\neq 0$ and p is a prime, $p\nmid D$, and at most one solution when $p=2$, $D>0$, $D\neq 7$, 23, 2^k-1 for some $k\geqslant 4$. This method is effective only if an exceptionally large solution of a related equation is known.

An important effective method in transcendental number theory was developed by Gelfond and Schneider. It was applied by Gelfond in 1940 to the equation $\alpha^x+\beta^y=\gamma^z$ in integers x, y, z, where α, β, γ are fixed real algebraic numbers. In 1961 Cassels used it to give an effective proof of Pólya's result mentioned at the end of (ii). In 1968 Schinzel gave several other applications, for example to the equation $x^2+D=p^n$. About at the same time A. Baker found an ingenious generalization of Gelfond's method, which led to important new results on diophantine equations. They will be discussed later, but we note that it was used to prove that there are only finitely many solutions to problems (b), (e) and, under suitable conditions, problem (d). As to problem (a) no more than a partial result has been obtained.

3. Linear forms in logarithms of algebraic numbers. All presented applications of Baker's method to diophantine equations can be deduced from the following theorem and its p-adic analogue proved by van der Poorten in 1977.

THEOREM 1 (BAKER 1973, 1977). *Let* $0<\delta<\frac{1}{2}$. *Let* α_j *denote an algebraic number, not* 0 *or* 1, *with height at most* A_j $(\geqslant 4)$ *for* $j=1, \dots, n$. *Put* $\Omega'=\prod_{j=1}^{n-1}\log A_j$. *Let* d *denote the degree of the field generated by the* α*'s over the rationals. Let* $b_1, \dots, b_n$ *be nonzero rational integers with absolute values at most* B $(\geqslant 4)$. *Put* $\Lambda=b_1\log\alpha_1+\dots+b_n\log\alpha_n$, *where the logarithms have their principal values. If* $\Lambda\neq 0$, *then*

$$\text{(a)}\qquad |\Lambda|>B^{-(16nd)^{200n}\Omega'\log\Omega'\log A_n},$$

$$\text{(b)}\qquad |\Lambda|>(\delta/|b_n|)^{C\log A_n}e^{-\delta B},$$

where $C>0$ *depends only on* d, n *and* $A_1, \dots, A_{n-1}$.

There are numerous results which give refinements, often under suitable conditions. I may refer to recent work of van der Poorten, Loxton, Waldschmidt and Mignotte. For our purpose it is important to note that in (i) the best present methods yield an exponent not better than, say, $-10^6(10nd)^n\Omega'\log\Omega'\log A_n$.

4. Applications to polynomial diophantine equations. Baker, Coates, Feldman, Sprindžuk and others have used estimates for linear forms to give upper bounds for solutions of polynomial diophantine equations. In these cases it was already known by the Thue–Siegel–Mahler method that there are only finitely many solutions. We restrict our attention here to two results which are important for the applications to exponential equations.

Theorem 2 (Baker, 1968). *Let $f(x, y)$ be an irreducible binary form with degree $n \geqslant 3$ and with integer coefficients having absolute values at most H. Let c denote any positive integer. Then all solutions of $f(x, y)=c$ satisfy*

$$\max(|x|, |y|) < \exp\{(nH)^{(10n)^5}+(\log c)^{2n}\}.$$

For our purpose later improvements are not significant, since the dependence on n is not better than $\exp\{n^n\}$ because of the fact noted at the end of § 3. Coates and Sprindžuk have given p-adic analogues of Theorem 2.

Theorem 3 (Baker, 1969). *Let m be an integer, $m \geqslant 3$. Let $f(x)$ be a polynomial with degree $n \geqslant 2$ and with integer coefficients having absolute values at most H. Suppose that f has at least two simple zeros. Then all solutions of $f(x)=y^m$ satisfy*

$$\max(|x|, |y|) < \exp\exp\{(5m)^{10} n^{10n^3} H^{n^2}\}.$$

Moreover, if f has at least three simple zeros, then all solutions of $f(x)=y^2$ satisfy

$$\max(|x|, |y|) < \exp\exp\exp\{n^{10n^3} H^{n^2}\}.$$

Improvements of the last inequality were obtained by Sprindžuk in 1976 and by Choodnovsky (to appear).

5. Applications to exponential diophantine equations. The p-adic analogues of Theorem 2 given by Coates and Sprindžuk already deal with exponential polynomials, namely with the equation $f(x, y)=cp_1^{z_1} \dots p_s^{z_s}$ in integers $x, y, z_1, \dots, z_s$, where f and c are as in Theorem 2 and $p_1, \dots, p_s$ are fixed primes. It follows that under the conditions of Theorem 2 the greatest prime factor $P[f(x, y)]$ of $f(x, y)$ tends to ∞ when $\max(|x|, |y|) \to \infty$, $(x, y)=1$. Completing results of Sprindžuk and Kotov, Shorey, van der Poorten, Tijdeman and Schinzel obtained the following estimate.

Theorem 4 (Shorey *et. al.*, 1977). *Let $f(x, y) \in \mathbf{Z}[x, y]$ be a binary form such that among the linear factors in the factorization of f at least three are distinct. Then for all pairs x, y with $(x, y)=1$*

$$P[f(x, y)] \gg_f \log\log(\max(|x|, |y|)).$$

($G \gg_a H$ means that there is a constant $c > 0$ depending only on a such that $G \geqslant cH$.)

It is an almost trivial consequence of Theorems 1 and 2 that for fixed integers a, b and $c \neq 0$ the equation $ax^n - by^n = c$ in integers $x > 1, y > 1$ *and* $n > 2$ has only finitely many solutions. A much stronger result was established by Stewart.

Theorem 5 (Stewart, 1976). $P[ax^n - by^n] \gg_{a,b} \sqrt{n}/\log n.$

The following result can be used in combination with the proof of Theorem 3 to determine all polynomials $f(x) \in \boldsymbol{Z}[x]$ which represent infinitely many perfect powers at integer points.

THEOREM 6 (SCHINZEL AND TIJDEMAN, 1976). *If a polynomial $f(x)$ with rational coefficients has at least two distinct zeros, then the equation $y^m = f(x)$ in integers m, x, y with $|y|>1$ implies that m is bounded.*

A generalization is given by Shorey *et al.* in 1977.

It turned out that in certain cases it was even possible to prove that two exponents with unrestricted bases are bounded. So one has in connection with problem (b)

THEOREM 7 (TIJDEMAN, 1976). *The equation $x^m - y^n = 1$ in integers $m>1, n>1$, $x>1, y>1$ has only finitely many solutions.*

A p-adic result was given by van der Poorten in 1977.

To problem (e) only a partial answer could be obtained.

THEOREM 8 (LJUNGGREN, 1943, SHOREY AND TIJDEMAN, 1976). *The equation $(x^m-1)/(x-1) = y^n$ in integers $m>2$, $n>1$, $x>1$, $y>1$ with $mn>6$ has only finitely many solutions if at least one of the following conditions holds:* (a) *x is fixed,* (b) *m has a fixed prime divisor,* (c) *y has a fixed prime divisor.*

An application of Baker's method dealing with sums of equal powers of consecutive integers was obtained very recently.

THEOREM 9 (VOORHOEVE, GYŐRY AND TIJDEMAN). *Let $f(x) \in \boldsymbol{Z}[x]$ and let $a, m \in \boldsymbol{Z}$ with $a \neq 0$, $m \geqslant 2$. If the equation*

$$f(x) + 1^m + 2^m + \ldots + x^m = ay^n$$

in positive integers $n>1$, $x, y>1$ has infinitely many solutions, then

$$(m, n) \in \{(3, 2), (3, 4), (5, 2)\}.$$

The difficult part of the proof is the demonstration that the zeros of the polynomial $f(x) + 1^m + 2^m + \ldots + x^m$ have certain properties. Then Theorem 6 and a generalization of Theorem 3 can be applied.

With respect to problem (a) only partial results have been deduced. For example,

THEOREM 10 (STEWART, 1977, INKERI AND VAN DER POORTEN, *to appear*). *Let C be fixed. The equation $x^n + y^n = z^n$ has only finitely many solutions in integers $n \geqslant 3$, $x \geqslant 1$, $y \geqslant 1$, $z \geqslant 1$ with $y - x < C$.*

In both papers more information about the differences $y-x$ and $z-x$ is given.

6. Indications of some proofs. (a) *The equation $x^m - ay^m = b$ in integers $m>1$, $x>1$, $y>1$.* Note that x^m/ay^m is very close to 1 and hence $|\log a + m \log (y/x)|$ is extremely small. It follows from Theorem 1 that m is bounded and hence, from Theorem 2, that x and y are bounded.

(b) *The equation* $x^2-1=y^n$ *in integers* $n>1$, $x>1$, $y>1$. By factorizing the left side we find that both $2(x\pm1)$ and $\frac{1}{2}(x\mp1)$ are nth powers. This leads to an equation of the form $y_2^n=4y_1^n+4$ in integers $n>1, y_1>1, y_2>1$. By (a) n and $y=y_1y_2$ are bounded.

(c) *The equation* $x^m-y^n=1$ *in integers* $m>1, n>1, x>1$, $y>1$. By factorizing x^m-1 and y^n+1 we find that $x-1=\varrho y_1^n$ and $y+1=\sigma x_1^m$, where ϱ and σ are restricted in size. Hence $(\varrho y_1^n)^m/(\sigma x_1^m)^n$ is close to 1. It follows that $|m\log\varrho-n\log\sigma+mn\log(y_1/x_1)|$ is small. Now Theorem 1 can be applied to show that m and n are bounded.

7. Upper bounds for solutions. An important feature of all proofs of the results mentioned in § 5. is that they are effective. Only in very few instances have upper bounds been computed effectively. Langevin proved that if $x^m-y^n=1$, then $x^m<\exp\exp\exp(250)$. The best we can hope for with the present methods is a bound of the order of $\exp\exp\exp(10)$. I think that with the present methods the effective solution of an exponential equation by Baker's method is nigh to hopeless, unless the bases of all exponential variables are fixed. In those cases it might be possible. For example, Hunt and van der Poorten determined all solutions of $x^2+7=2^n$ and $x^2-11=5^n$ by Baker's method. The application of Theorem 1 gives $n<10^{20}$ and the remaining values have been checked. Beukers proved by using hypergeometric functions that if $x^2+D=2^n$, $D\neq0$, then $n<500+15\log|D|$ and even $n<20+3\log|D|$ when $|D|<10^{12}$. The method works, since 181^2 is exceptionally close to 2^{15}. It is not applicable to base 5, since no square is exceptionally close to a power of 5. Baker's method is applicable to any equation $x^2+D=a^n$ in integers n, x.

8. Related results. In many cases results stated here for rational integers can actually be proved for algebraic integers in a given number field. This has been worked out by Sprindžuk and Kotov.

It is a straightforward application of Theorem 1 that in a given number field there are only finitely many units ε such that $1-\varepsilon$ is a unit. Such units were used by Lenstra in 1977 to determine Euclidean number fields.

Sprindžuk, Győry and Papp dealt with applications to norm form, discriminant form and index form equations. Győry also gave estimates for the degree of monic polynomials $f(x)\in\mathbf{Z}[x]$ with a given discriminant $D\neq0$.

Schinzel, Stewart and Győry and Kiss applied Baker's method to Lucas and Lehmer numbers. Stewart proved, for example, that there are only finitely many Lucas and Lehmer numbers of index $n>12$ which do not have a primitive divisor.

An exponential equation with algebraic integers was solved by Baker's method in order to determine all elliptic curves over $\mathbf{Q}$ of conductor 11 (Agrawal, Coates, Hunt and van der Poorten).

I thank A. J. van der Poorten for his helpful comments while I prepared this paper.

References

(The corresponding sections are given in square brackets.)

1. L. E. Dickson, *History of the theory of numbers,* I—III, 1920; reprint, Chelsea, New York, 1952. [1].

2. L. J. Mordell, *Diophantine equations.* Academic Press, London, 1969. [1, 2].

3. W. M. Schmidt, *Approximation to algebraic numbers.* L'Enseignement Math. **17** (1971), 187—253. [2].

4. A. Baker, *Effective methods in Diophantine problems,* Proc. Sympos. Pure Math., Amer. Math. Soc., Providence. R. I., vol. 20, 1971, pp. 195—205; vol. 24, 1974, pp. 1—7. [3, 4].

5. R. Tijdeman, *Hilbert's seventh problem.* Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, R. I., 1976, pp. 241—268. [3, 4].

6. *Transcendence Theory: Advances and Applications,* ed. by A. Baker and D. W. Masser, Academic Press, London, 1977, Chapters I—V. [3—6, 8].

7. V. G. Sprindžuk, *An effective analysis of the equations of Thue and Thue-Mahler,* Aktual'nye Probl. Analit. Teor. Cisel., Minsk, 1974, pp. 199—222. (Russian) [4, 8].

8. R. Tijdeman, *Some applications of Baker's sharpened bounds to diophantine equations,* Sém. Delange-Pisot-Poitou **16** (1975), No. 24 [6].

9. M. Langevin, *Quelques applications de nouveaux résultats de van der Poorten,* Sém. Delange-Pisot-Poitou **17** (1976), No. G 12 [7].

Mathematical Institute
Leiden, Netherlands