

On the equation $y^m = P(x)$

by

A. SCHINZEL (Warszawa) and R. TIJDEMAN (Leiden)

The aim of this paper is to prove the following

THEOREM. *If a polynomial $P(x)$ with rational coefficients has at least two distinct zeros then the equation*

$$(1) \quad y^m = P(x), \quad x, y \text{ integers, } |y| > 1,$$

implies $m < c(P)$ where $c(P)$ is an effectively computable constant.

For a fixed m the diophantine equation (1) has been thoroughly investigated before (see [1] and [4]) and the known results together with the above theorem imply immediately

COROLLARY 1. *If a polynomial $P(x)$ with rational coefficients has at least two simple zeros then the equation (1) has only finitely many integer solutions m, x, y with $m > 2$, $|y| > 1$ and these solutions can be found effectively.*

COROLLARY 2. *If a polynomial $P(x)$ with rational coefficients has at least three simple zeros then the equation (1) has only finitely many integer solutions m, x, y with $m > 1$, $|y| > 1$ and these solutions can be found effectively.*

A simple proof of the special case of Corollary 1 that $P(x)$ has at least two simple rational zeros can be found in a survey paper by the second named author [6]. Corollary 2 is a step towards the following

CONJECTURE. *If a polynomial $P(x)$ with rational coefficients has at least three simple zeros then the equation $y^2 z^3 = P(x)$ has only finitely many solutions in integers x, y, z with $yz \neq 0$.*

This conjecture lies rather deep, since it implies the existence of infinitely many primes p such that $2^{p-1} \not\equiv 1 \pmod{p^2}$.

The proof of the theorem is based on Baker's work [2] and on two lemmata. We denote by $\|x\|$ the distance from x to the nearest integer.

LEMMA 1. For any complex numbers X, Y different from 0, a positive integer h and any choice of the roots $X^{1/h}, Y^{1/h}$ we have

$$(2) \quad |X^{1/h} - Y^{1/h}| \geq \max(|X|, |Y|)^{1/h} \cdot \begin{cases} \left(1 - \frac{1}{e}\right) \min\left(1, \frac{1}{h} \left|\log |XY^{-1}|\right|\right) & \text{if } |X| \neq |Y|, \\ \frac{4}{h} \left\| \frac{\log XY^{-1}}{2\pi i} \right\| & \text{if } |X| = |Y|. \end{cases}$$

Proof. We can assume without loss of generality that

$$|X| \geq 1 = |Y|.$$

If $|X| > 1$ we have

$$|X^{1/h} - 1| \geq |X^{1/h}| - 1 = |X|^{1/h} (1 - |X|^{-1/h}),$$

and if $|X| \geq e^h$ the inequality (2) follows immediately. To settle the case $e^h > |X| > 1$ we verify by differentiation that the function

$$f(t) = (1 - t^{-1}) / \log t$$

is decreasing in the interval $(1, e)$. Since $f(e) = 1 - e^{-1}$, (2) follows on taking $t = |X|^{1/h}$.

Suppose now that $|X| = 1$,

$$X = \cos \varphi + i \sin \varphi, \quad \varphi = i^{-1} \log X.$$

Then

$$X^{1/h} = \cos \frac{\varphi + 2\pi j}{h} + i \sin \frac{\varphi + 2\pi j}{h} \quad \text{for some integer } j$$

and

$$|X^{1/h} - 1| = 2 \left| \sin \frac{\varphi + 2\pi j}{2h} \right|.$$

However, $\sin \psi / \psi$ is decreasing on $(0, \pi/2)$. Hence for all real ψ

$$|\sin \psi| \geq 2 \left\| \frac{\psi}{\pi} \right\|$$

and

$$|X^{1/h} - 1| \geq 4 \left\| \frac{\varphi + 2\pi j}{2\pi h} \right\| \geq \frac{4}{h} \left\| \frac{\log X}{2\pi i} \right\|.$$

In the following lemma we denote the height of an algebraic number α by $H(\alpha)$.

LEMMA 2. If γ_1, γ_2 are algebraic integers of a field K of degree d then

$$(3) \quad H(\gamma_1/\gamma_2) \leq 3d2^d \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|),$$

where σ runs through all the isomorphic injections of K into the complex field. Moreover, if $K = \bar{K}$ (the bar denoting complex conjugation) then

$$H(|\gamma_1/\gamma_2|^2) \leq 3d2^d \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|)^2.$$

Proof. Clearly γ_1/γ_2 satisfies the equation

$$F(x) = \prod_{\sigma} (\gamma_2^{\sigma} x - \gamma_1^{\sigma}) = 0.$$

$F(x)$ has rational integral coefficients, but it may be reducible. We have

$$F(x) = N_{K/\mathbb{Q}} \gamma_2 \cdot f(x)^r,$$

where f is the minimal polynomial of γ_1/γ_2 . By Gauss's lemma $F(x) = c \cdot g(x)^r$, where c is an integer, g has integral coefficients and is irreducible as a constant multiple of f . By an inequality of Gelfond ([3], p. 139) we have

$$H(F) \geq \frac{1}{3d} H(g)^r \geq \frac{1}{3d} H(g),$$

where $H(P)$ denotes the height of the polynomial P .

On the other hand,

$$H(F) \leq \prod_{\sigma} (|\gamma_1^{\sigma}| + |\gamma_2^{\sigma}|) \leq 2^d \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|).$$

This implies (3). Now if $K = \bar{K}$ we have $|\gamma_i^{\sigma}| = \gamma_i \bar{\gamma}_i \in K$ ($i = 1, 2$). Hence

$$\begin{aligned} H(|\gamma_1/\gamma_2|^2) &\leq 3d2^d \prod_{\sigma} \max(|\gamma_1^{\sigma} \bar{\gamma}_1^{\sigma}|, |\gamma_2^{\sigma} \bar{\gamma}_2^{\sigma}|) \\ &\leq 3d2^d \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|) \cdot \prod_{\sigma} \max(|\bar{\gamma}_1^{\sigma}|, |\bar{\gamma}_2^{\sigma}|) \\ &= 3d2^d \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|)^2. \end{aligned}$$

Proof of the Theorem. Let K be the splitting field of P and let

$$bP(x) = a \prod_{i=1}^n (x - a_i)^{r_i} \quad (a_i \text{ distinct, } b \text{ integer})$$

have integral coefficients. It follows from (1) that

$$(4) \quad \prod_{i=1}^n (ax - a_i)^{r_i} = bu^{N-1} y^m, \quad N = \sum_{i=1}^n r_i,$$

where the numbers aa_i are algebraic integers. Since for integer x

$$(ax - aa_i, ax - aa_j) \mid (aa_i - aa_j),$$

the highest common ideal divisor of any two factors on the left-hand side of (4) is composed exclusively of prime ideals of K dividing

$$\Delta = \prod_{1 \leq i < j \leq n} (aa_i - aa_j).$$

Hence, for each $i \leq n$ we have

$$(5) \quad (ax - aa_i)^{r_i} = \mathfrak{d}c^m$$

for some ideals \mathfrak{d} and c such that \mathfrak{d} is composed exclusively of prime factors of $ab\Delta$ and $(c, ab\Delta) = 1$. If \mathfrak{p} is a prime ideal and $\mathfrak{p}^t \parallel c^m$ then clearly $m \mid t$ and by (5) $r_i \mid t$, thus $[m, r_i] \mid t$. It follows that $\frac{m}{(m, r_i)} \mid \frac{t}{r_i}$. Moreover $\mathfrak{d} = \mathfrak{d}_i^{r_i}$ and we get from (5)

$$(6) \quad (ax - aa_i) = \mathfrak{d}_i c_i^s, \quad s = \frac{m}{(m, [r_1, \dots, r_n])}.$$

Let $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ be all prime ideal divisors of $ab\Delta$ in K and let h be the class number of K . We have

$$\mathfrak{p}_j^h = (\pi_j) \quad (1 \leq j \leq k),$$

$$\mathfrak{c}_i^h = (\gamma_i) \quad (1 \leq i \leq n),$$

and by (6) for suitable integer exponents $y_{ij} \geq 0$

$$(ax - aa_i)^h = \left(\prod_{j=1}^k \pi_j^{y_{ij}} \gamma_i^s \right).$$

If $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_r$ are a basis for the group of units in K we get

$$(7) \quad (ax - aa_i)^h = \prod_{q=0}^r \varepsilon_q^{x_{iq}} \prod_{j=1}^k \pi_j^{y_{ij}} \gamma_i^s \quad (1 \leq i \leq n),$$

where we can suppose without loss of generality that

$$(8) \quad 0 \leq x_{iq} < s, \quad 0 \leq y_{ij} < s,$$

since any product

$$\prod_{q=0}^r \varepsilon_q^{x_{iq}} \prod_{j=1}^k \pi_j^{y_{ij}} \quad \text{with } x_{iq} \equiv y_{ij} \equiv 0 \pmod{s}, \quad y_{ij} \geq 0,$$

can be incorporated in γ_i .

By our assumption $n \geq 2$. We use (7) for $i = 1, 2$, denoting the right-hand side of (7) by X and Y , respectively. If $X = Y$ we have

$$(ax - aa_1)^h = (ax - aa_2)^h$$

and it follows, from $a_1 \neq a_2$, that $ax - aa_1 = e^{2\pi i g/h} (ax - aa_2)$, $0 < g < h$, and

$$|g| \leq \frac{|a_1| + |a_2|}{2 \sin(\pi/h)}.$$

Since $|g| > 1$, equation (1) gives $m < c_1$, where c_1 as the subsequent constants c_2, c_3, \dots depends only on P and is effectively computable.

If $X \neq Y$ we have either $|X| \neq |Y|$ or $|X| = |Y|$ and $\left\| \frac{\log XY^{-1}}{2\pi i} \right\| \neq 0$. In the former case we infer by (8) from Baker's theorem [2] that

$$|\log |XY^{-1}|| > H(|\gamma_1/\gamma_2|^2)^{-c_2 \log s},$$

in the latter case similarly

$$\left\| \frac{\log XY^{-1}}{2\pi i} \right\| > H(\gamma_1/\gamma_2)^{-c_3 \log s},$$

where in case $H(\) = 1$, it should be replaced by 2.

In virtue of Lemmata 1 and 2 we have in both cases

$$|aa_1 - aa_2| = |X^{1/h} - Y^{1/h}|$$

$$> c_4 \max(|X|, |Y|)^{1/h} \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|)^{-c_5 \log s}$$

$$> c_6^{-s} \max(|\gamma_1|, |\gamma_2|)^{s/h} \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|)^{-c_5 \log s}$$

for some constant $c_6 > 1$.

Applying any automorphism τ of K to both sides of (7) and arguing as before we get

$$|aa_1^{\tau} - aa_2^{\tau}| > c_6^{-s} \max(|\gamma_1^{\tau}|, |\gamma_2^{\tau}|)^{s/h} \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|)^{-c_5 \log s}.$$

On taking the product over all automorphisms τ we obtain

$$|N_{K/\mathcal{Q}}(aa_1 - aa_2)| > c_6^{-ds} \prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|)^{s/h - c_5 d \log s}.$$

Since the left-hand side is independent of s , this implies that either $s \leq c_7$ or

$$\prod_{\sigma} \max(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|) < c_8^{2dh}.$$



In the former case we have $m \leq c_7[r_1, \dots, r_n]$; in the latter case, by (

$$(9) \quad N_{K|\mathbb{Q}}(ax - aa_1)^h(ax - aa_2)^h = \pm \prod_{j=1}^k N(\pi_j)^{u_{1j} + u_{2j} \mathcal{G}^n},$$

where $\mathcal{G} = |N\gamma_1\gamma_2| < c_6^{abh}$. The greatest prime factor of the right-hand side of (9) is bounded by $ab\Delta c_6^{abh}$. The left-hand side of (9) is a polynomial in x with integer coefficients and at least two distinct zeros. It has been proved by the first named author, M. Keates, S. V. Kotov and V. Sprindžuk (see [5]) that the greatest prime factor of such a polynomial exceeds $c_9 \log \log |x|$. So we obtain $|x| \leq c_9$ and in view of (1) with $|y| > m \leq c_{10}$.

References

- [1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Can. Phil. Soc. 65 (1969), pp. 439-444.
- [2] — *A sharpening of the bounds for linear forms in logarithms*, Acta Arith. (1972), pp. 117-129.
- [3] A. O. Gelfond, *Transcendental and algebraic numbers* (Russian), Moscow 19 English Translation: Dover Publ., New York 1960.
- [4] W. J. LeVeque, *On the equation $y^m = f(x)$* , Acta Arith. 9 (1964), pp. 209-2
- [5] V. G. Sprindžuk, *An effective analysis of the Thue and Thue-Mahler equation* Current problems of analytic number theory, Proc. Summer School Analyt. Number Theory Minsk 1972 (Russian). Izdat. "Nauka i Technika", Minsk 19 pp. 199-222.
- [6] R. Tijdeman, *Applications of the Gelfond-Baker method to rational number theory*. Rational number theory, Proc. Conf. Debrecen 1974; Coll. Math. S. János Bolyai, to appear.

MATHEMATICAL INSTITUTE OF THE POLISH ACADEMY OF SCIENCES
Warszawa, Poland
MATHEMATICAL INSTITUTE, E. U. LEIDEN
Leiden, Netherlands

Received on 10. 6. 1975

(7)

Les volumes IV Volumes from IV Die Bände IV und Томы IV и следу-
et suivants sont on are available folgende sind zu ющие можно по-
à obtenir chez at beziehen durch лучить через

Ars Polona, Krakowskie Przedmieście 7, 00-068 Warszawa, Poland

Les volumes I-III Volumes I-III Die Bände I-III sind Томы I-III можно
sont à obtenir chez are available at zu beziehen durch получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES INSTITUTE OF MATHEMATICS

- S. Banach, *Oeuvres*, vol. I, 1967, 381 pp.
S. Mazurkiewicz, *Travaux de topologie et ses applications*, 1969, 380 pp.
W. Sierpiński, *Oeuvres choisies*, vol. I, 1974, 300 pp.; vol. II, 1975, 780 pp.;
vol. III, 1976, 688 pp.

MONOGRAFIE MATEMATYCZNE

41. H. Rasiowa and R. Sikorski, *The mathematics of metamathematics*, 3rd ed., revised, 1970, 520 pp.
43. J. Szarski, *Differential inequalities*, 2nd ed., 1967, 256 pp.
44. K. Borsuk, *Theory of retracts*, 1967, 251 pp.
45. K. Maurin, *Methods of Hilbert spaces*, 2nd ed., 1972, 552 pp.
47. D. Przeworska-Rolewicz and S. Rolewicz, *Equations in linear spaces*, 1968, 380 pp.
50. K. Borsuk, *Multidimensional analytic geometry*, 1969, 443 pp.
51. R. Sikorski, *Advanced calculus. Functions of several variables*, 1969, 460 pp.
52. W. Ślębodziński, *Exterior forms and their applications*, 1970, 427 pp.
53. M. Krzyżański, *Partial differential equations of second order I*, 1971, 562 pp.
54. M. Krzyżański, *Partial differential equations of second order II*, 1971, 407 pp.
57. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 1974, 630 pp.
58. C. Bessaga and A. Pełczyński, *Selected topics in infinite-dimensional topology*, 1975, 353 pp.
59. K. Borsuk, *Theory of shape*, 1975, 379 pp.
60. R. Engelking, *General topology*, in print.

New series

BANACH CENTER PUBLICATIONS

- Vol. I. *Mathematical control theory*, 1976, 166 pp.
Vol. II. *Mathematical foundations of computer science*, in print.