ACTA ARITHMETICA
XXXI (1976)

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*

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

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 $y^2z^3 = P(x)$ 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*

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

Proof. We can assume without loss of generality that

$$|X|\geqslant 1 = Y^{1/h}.$$

If $|X|>1$ we have

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

and if $|X|\geqslant e^h$ 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 $|X|=1$,

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

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

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

and

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

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

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

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

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

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

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

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

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 Gel'fond ([3], p. 139) we have

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

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

On the other hand,

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

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

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

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

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

where the numbers $a\alpha_i$ are algebraic integers. Since for integer x

$$(ax-a\alpha_i,\ ax-a\alpha_j) \mid (a\alpha_i-a\alpha_j),$$

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

$$\Delta = \prod_{1\leqslant i<j\leqslant n} (a\alpha_i-a\alpha_j).$$

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

$$(ax-a\alpha_i)^{r_i} = \mathfrak{d}\mathfrak{c}^m \tag{5}$$

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

$$(ax-a\alpha_i) = \mathfrak{d}_i\mathfrak{c}_i^s, \qquad s = \frac{m}{(m, [r_1, \ldots, r_n])}. \tag{6}$$

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

$$\mathfrak{p}_j^h = (\pi_j) \qquad (1 \leqslant j \leqslant k),$$
$$\mathfrak{c}_i^h = (\gamma_i) \qquad (1 \leqslant i \leqslant n),$$

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

$$(ax-a\alpha_i)^h = \Big(\prod_{j=1}^{k} \pi_j^{y_{ij}} \gamma_i^s\Big).$$

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

$$(ax-a\alpha_i)^h = \prod_{q=0}^{r} \varepsilon_q^{x_{iq}} \prod_{j=1}^{k} \pi_j^{y_{ij}} \gamma_i^s \qquad (1 \leqslant i \leqslant n), \tag{7}$$

where we can suppose without loss of generality that

$$0 \leqslant x_{iq} < s, \qquad 0 \leqslant y_{ij} < s, \tag{8}$$

since any product

$$\prod_{q=0}^{r} \varepsilon_q^{x_q} \prod_{j=1}^{k} \pi_j^{y_j} \quad \text{with } x_q \equiv y_j \equiv 0 \pmod{s},\ y_j \geqslant 0,$$

can be incorporated in γ_i.

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

$$(ax-a\alpha_1)^h = (ax-a\alpha_2)^h$$

and it follows, from $\alpha_1 \neq \alpha_2$, that $ax-a\alpha_1 = e^{2\pi i g/h}(ax-a\alpha_2)$, $0 < g < h$, and

$$|x| \leqslant \frac{|\alpha_1|+|\alpha_2|}{2\sin(\pi/h)}.$$

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

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

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

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

$$\begin{aligned}|a\alpha_1-a\alpha_2| &= |X^{1/h}-Y^{1/h}| \\ &> c_4 \max(|X|, |Y|)^{1/h} \prod_{\sigma} \max(|\gamma_1^\sigma|, |\gamma_2^\sigma|)^{-c_5\log s} \\ &> c_6^{-s} \max(|\gamma_1|, |\gamma_2|)^{s/h} \prod_{\sigma} \max(|\gamma_1^\sigma|, |\gamma_2^\sigma|)^{-c_5\log s}\end{aligned}$$

for some constant $c_6 > 1$.

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

$$|a\alpha_1^\tau - a\alpha_2^\tau| > c_6^{-s} \max(|\gamma_1^\tau|, |\gamma_2^\tau|)^{s/h} \prod_{\sigma} \max(|\gamma_1^\sigma|, |\gamma_2^\sigma|)^{-c_5\log s}.$$

On taking the product over all automorphisms τ we obtain

$$|N_{K/Q}(a\alpha_1-a\alpha_2)| > c_6^{-ds} \prod_{\sigma} \max(|\gamma_1^\sigma|, |\gamma_2^\sigma|)^{s/h-c_5 d\log s}.$$

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

$$\prod_{\sigma} \max(|\gamma_1^\sigma|, |\gamma_2^\sigma|) < c_6^{2dh}.$$

In the former case we have $m \leqslant c_7[r_1, \ldots, r_n]$, in the latter case, by (

$$N_{K/Q}(ax-aa_1)^h(ax-aa_2)^h = \pm \prod_{j=1}^{k} N(\pi_j)^{y_{1j}+y_{2j}}\mathscr{G}^s, \quad (9)$$

where $\mathscr{G} = |N\gamma_1\gamma_2| < c_6^{4dh}$. The greatest prime factor of the right-ha side of (9) is bounded by $ab\Delta c_6^{4dh}$. The left-hand side of (9) is a polynom in x with integer coefficients and at least two distinct zeros. It has be proved by the first named author, M. Keates, S. V. Kotov and V. Sprindžuk (see [5]) that the greatest prime factor of such a polynom exceeds $c_8 \log\log|x|$. So we obtain $|x| \leqslant c_9$ and in view of (1) with $|y| >$ $m \leqslant c_{10}$.

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 equatio Current problems of analytic number theory*, Proc. Summer School Analy Number Theory Minsk 1972 (Russian). Izdat. "Nauka i Technika", Minsk 19 pp. 199–222.
[6] R. Tijdeman, *Applications of the Gel'fond-Baker method to rational num 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, R. U. LEIDEN
Leiden, Netherlands

Received on 10. 6. 1975 (7