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

by

A. SCHINZEL (Warszawa) and J. 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

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

implies \( m < o(P) \) where \( o(P) \) 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 \( y^3 = P(x) \) 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 \( 2^p - 1 \equiv 1 \pmod{p^3} \).

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

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

if $|X| \neq |Y|$, and

$$\frac{4}{h} \log \frac{|XY|}{2\pi i}$$

if $|X| = |Y|$. 

Proof. We can assume without loss of generality that $|X| > 1 = Y^{1/h}$.

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

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

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

Suppose now that $|X| = 1$, then

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

Then

$$X^{1/h} = \cos \frac{\varphi + 2\pi j}{h} + i \sin \frac{\varphi + 2\pi j}{h}$$

for some integer $j$ and

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

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

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

and

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

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

Lemma 2. If $\gamma_1, \gamma_2$ are algebraic integers of a field $K$ of degree $d$ then

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

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

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

Proof. Clearly $\gamma_1/\gamma_2$ satisfies the equation

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

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

$$F(x) = N_{K \cap \mathbb{Q}(\gamma_1, \gamma_2)} f(x),$$

where $f$ is the minimal polynomial of $\gamma_1/\gamma_2$. By Gauss's lemma $F(x) = g(x)^r$, where $g$ is an integer, $h$ has integral coefficients and is irreducible as a constant multiple of $f$. By an inequality of Gel'fond ([3], p. 139) we have

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

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

On the other hand,

$$H(F) \leq \sum_{\omega} \max \{|\gamma_1|, |\gamma_2|\} \leq 2^{d} \max \{|\gamma_1|, |\gamma_2|\}.$$ 

This implies (3). Now if $K = \mathbb{Q}$ we have $|\gamma_1| = \gamma_2 x_k K (i = 1, 2)$. Hence

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

$$= 3d2^d \max \{|\gamma_1 |^2, |\gamma_2 |^2\} \cdot \max \{|\gamma_1 |^2, |\gamma_2 |^2\}^2.$$ 

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

$$bP(x) = \prod_{i=1}^n (x - \alpha_i)^{r_i}$$

have integral coefficients. It follows from (1) that

$$\prod_{i=1}^n (x - \alpha_i)^{r_i} = ba^{N-1} y^n, \quad N = \sum_{i=1}^n r_i,$$
where the numbers $a_{k_i}$ are algebraic integers. Since for integer $s$
\[(ax - a_1, ax - a_2) = (a_1 - a_2),\]
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
\[\Delta = \prod_{i < j < m} (a_i - a_j).\]
Hence, for each $i \leq n$ we have
\[(ax - a_i)^t = \mathfrak{b}c^m \]
for some ideals $\mathfrak{b}$ and $c$ such that $\mathfrak{b}$ is composed exclusively of prime
factors of $\mathfrak{a}d$ and $(c, \mathfrak{a}d) = 1$. If $p$ is a prime ideal and $p^{\alpha} | c^m$ then clearly
$\mathfrak{m}|t$ and by (5) $r_i|t$, thus $[m, r_i]|t$. It follows that
\[\frac{m}{(m, r_i)} \frac{t}{r_i}.\]
Moreover $\mathfrak{b} = b_i^\alpha$ and we get from (5)
\[(ax - a_i) = b_i^\alpha, \quad b = \left(\frac{m}{(m, [r_1, \ldots, r_m])}\right).\]
Let $p_1, \ldots, p_k$ be all prime ideal divisors of $\mathfrak{a}d$ in $K$ and let $b$ be the
class number of $K$. We have
\[p_i^b = (p_i) \quad (1 \leq j \leq k),\]
\[c = (c) \quad (1 \leq i \leq n),\]
and by (6) for suitable integer exponents $y_j \geq 0$
\[(ax - a_i)^b = \left(\prod_{j=1}^k p_i^{y_j} c_j\right).\]
If $e_0, e_1, \ldots, e_s$ are a basis for the group of units in $K$ we get
\[(ax - a_i)^b = \prod_{i=1}^s e_i^{\alpha_i} \prod_{i=1}^k p_i^{y_i} c_i \quad (1 \leq i \leq m),\]
where we can suppose without loss of generality that
\[0 \leq s_i < e_i, \quad 0 \leq y_i < s,\]
since any product
\[\prod_{i=1}^s e_i^s \prod_{i=1}^k p_i^{y_i}\]
with $s_i = y_i = 0 \pmod{s}$, $y_i \geq 0$,
can be incorporated in $y_i$.

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

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
\[(ax - a_1)^b = (ax - a_2)^b\]
and it follows, from $a_1 \neq a_2$, that
\[ax - a_1 = e^{\alpha_1 b}(ax - a_2), \quad 0 \leq g < h,\]
and
\[|s| \leq \left| \frac{a_1}{a_2} \right| \frac{2}{\sin(\pi/h)} .\]
Since $|y| > 1$, equation (1) gives $m < e_1$, where $e_1$ as the subsequent constants $e_2, e_3, \ldots$ depends only on $P$ and is effectively computable.

If $X \neq Y$ we have either $|X| \neq |Y|$ or $|X| = |Y|$ and $\frac{\log|XY^{-1}|}{2\pi i} \neq 0$. In the former case we infer by (8) from Baker's theorem [2] that
\[|\log|XY^{-1}|| > H(|y_1/y_2|) - \delta_{1,\log},\]
in the latter case similarly
\[\frac{\log|XY^{-1}|}{2\pi i} > H(|y_1/y_2|) - \delta_{1,\log},\]
where in case $H(\cdot) = 1$, it should be replaced by $2$.

In virtue of Lemmata 1 and 2 we have in both cases
\[|ax - a_1| = |X^{1/s} - Y^{1/s}| > e_1 \max |X| \max |Y| \frac{1}{s} \prod_{j} \max (|y_j|, |y_j|)^{-\delta_{1,\log}}\]
\[> e_1^{-s} \max |y_j| \frac{1}{s} \prod \max (|y_j|, |y_j|)^{-\delta_{1,\log}}\]
for some constant $e_1 > 1$.

Applying any automorphism $\tau$ of $K$ to both sides of (7) and arguing
as before we get
\[|ax - a_1| > e_1^{-s} \max |y_j| \frac{1}{s} \prod \max (|y_j|, |y_j|)^{-\delta_{1,\log}}\]

On taking the product over all automorphisms $\tau$ we obtain
\[|N_{K/Q}(ax - a_1)| > e_1^{-s} \prod \max (|y_j|, |y_j|)^{-\delta_{1,\log}}\]
Since the left-hand side is independent of $s$, this implies that either $s \leq e_1$ or
\[\prod \max (|y_j|, |y_j|) < e_1^{2k} .\]
In the former case we have \( m \leq c_1 [x_1, \ldots, x_b] \), in the latter case, by (9)

\[
N_{KQ}(ax - a_1)^b(ax - a_2)^b = 2 \prod_{j=1}^{b} N(x_j)^{\nu_1^j + \nu_2^j - \delta^j},
\]

where \( \delta = |N(x_1, x_2)| < c_1^{ab} \). The greatest prime factor of the right-hand side of (9) is bounded by \( ab\delta c_1^{ab} \). 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. Kestes, S. V. Kotov and V. Sprindszuk [see (5)] that the greatest prime factor of such a polynomial exceeds \( c_1 \log|a| \). So we obtain \( |a| \leq c_2 \), and in view of (1) with \( |y| > m \leq c_3 \).

References


BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES INSTITUTE OF MATHEMATICS


MONOGRAFIE MATEMATYCZNE


New series

BANACH CENTER PUBLICATIONS

Vol. II. Mathematical foundations of computer science, in print.