On the Catalan equation over algebraic number fields

By *B. Brindza, K. Győry* at Debrecen and *R. Tijdeman* at Leiden

1. Introduction

In 1844 Catalan [4] conjectured that 8 and 9 are the only consecutive positive integers which both are perfect powers. Cassels [3] made the weaker conjecture that the equation

$$x^p - y^q = 1 \tag{1}$$

has only finitely many solutions in positive integers $x>1$, $y>1$, $p>1$, $q>1$. The latter conjecture was proved by Tijdeman [14]. He showed that an upper bound for the solutions of (1) can be computed by using Baker's method for estimating linear forms in logarithms of algebraic numbers. Langevin [8] followed Tijdeman's proof to show that (1) implies

$$y^q < x^p < \exp\exp\exp\exp(730)\ ^1).$$

For the further history of the problem and related results we refer to Ribenboim [10], Shorey and Tijdeman [13], Chapter 12 and Tijdeman [14], [16].

In the present paper we shall give a generalization of Tijdeman's result to the case that the ground ring is the ring of integers of an arbitrary algebraic number field. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$. Further, let $\lceil\alpha\rceil$ denote the maximum absolute value of the conjugates of an arbitrary algebraic number α.

Theorem. *There exists an effectively computable number C which depends only on K such that all solutions of the equations*

$$x^p \pm y^q = 1 \quad \text{in} \quad x, y \in \mathcal{O}_K,\ p, q \in \mathbb{N} \tag{2}$$

with x, y not roots of unity and $p>1$, $q>1$, $pq>4$ satisfy

$$\max(\lceil x\rceil, \lceil y\rceil, p, q) < C. \tag{3}$$

In other words, (2) has only finitely many non-trivial solutions and all these can be, at least in principle, effectively determined.

[1]) The assertion on the bound in Tijdeman [15], p. 386 is incorrect.

The restrictions on x, y, p, q in the theorem are necessary. If x or y is a root of unity, then $\max(\lceil x \rceil, \lceil y \rceil)$ is bounded, but p or q may be arbitrarily large. If p or q equals 1, then clearly there are infinitely many solutions. Finally, if $p=q=2$ and if K has infinitely many units and 2 splits into $[K:\mathbb{Q}]$ distinct prime ideals (this is the case, for example, when $K=\mathbb{Q}(\sqrt{7})$), then all units ε in $\mathcal{O}_K$ satisfy $\varepsilon \equiv 1 \pmod 2$. Hence, for any unit $\varepsilon \in \mathcal{O}_K$ there are $x, y \in \mathcal{O}_K$ such that $\varepsilon + \varepsilon^{-1} = 2x$, $\varepsilon - \varepsilon^{-1} = 2y$ and so $x^2 - y^2 = 1$. Thus the equation $x^2 - y^2 = 1$ has infinitely many solutions $x, y \in \mathcal{O}_K$.

We also note that the dependence of C on K cannot be relaxed to dependence on the degree of K only, since for any q we can choose arbitrary $x \in \mathbb{Q}$, $p \in \mathbb{N}$ and define y such that $x^p \pm y^q = 1$.

As in the rational case, the constant 1 at the right hand side of (2) is essential for the argument. Pillai [9] conjectured that for given non-zero rational integers a, b, k the more general equation

$$ax^p - by^q = k \tag{4}$$

has only finitely many solutions in rational integers $x>1$, $y>1$, $p>1$, $q>1$ with $pq>4$. The conjecture is still open, but the assertion has been proved under the condition that at least one of the numbers x, y, p or q is fixed (cf. Shorey and Tijdeman [13], Theorems 12. 1, 12. 2). A natural extension of Pillai's conjecture is the problem if, for given non-zero $a, b, k \in \mathcal{O}_K$, equation (4) has only finitely many solutions $x, y \in \mathcal{O}_K$, $p, q \in \mathbb{N}$ with $xy \neq 0$, x and y no roots of unity and $p>1$, $q>1$, $pq>4$. It is easy to show that the latter assertion is true if at least one of the numbers x, y, p or q is fixed. If p or q is fixed, then apply Lemmas 8 and 7 stated in § 2. If x or y is fixed and both are units, then apply Lemma 5. If x or y is fixed and one of them is not a unit, then Lemma 6 implies that q or p is bounded and then the argument for fixed p or q can be applied.

The proof of the Theorem is not merely a straightforward generalization of the rational case. In the general case new arguments were needed to deal with the cases that p or q is bounded and that x or y is a unit or has a bounded norm. Furthermore, the case that the linear form vanishes requires a new argument.

2. Lemmas

To prove the theorem we shall need some lemmas. Let K be an algebraic number field of degree n with ring of integers $\mathcal{O}_K$.

Lemma 1. *Let $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$, α not a root of unity. There exists an effectively computable positive number C_1 depending only on n such that*

$$\lceil \alpha \rceil > 1 + C_1.$$

Proof. This result is due to Schinzel and Zassenhaus [11]. They gave an explicit value for C_1 which was improved upon, at least asymptotically, by Dobrowolski [5] and Cantor and Straus [2].

For any algebraic number α, we denote by $H(\alpha)$ the height of α, i.e. the maximal absolute value of the coefficients of the minimal defining polynomial of α over $\mathbb{Z}$. Without further reference we shall use the following inequalities (cf. [7], § 1. 1).

(5) $$\lceil\alpha\rceil \leqq 2H(\alpha), \quad H(\alpha) \leqq (2\lceil\alpha\rceil)^n \quad \text{for} \quad \alpha \in \mathcal{O}_K,$$

(6) $$H(\alpha/\beta) \leqq (\lceil\alpha\rceil + \lceil\beta\rceil)^n \quad \text{for} \quad \alpha, \beta \in \mathcal{O}_K, \quad \beta \neq 0.$$

Let $\alpha_1, \ldots, \alpha_k$ ($k \geqq 2$) be algebraic numbers in K with heights at most $A_1, \ldots, A_k$, respectively, and suppose $A_j \geqq 2$ ($j = 1, \ldots, k$). Put

$$\Omega' = \prod_{j=1}^{k-1} \log A_j, \quad \Omega = \Omega' \log A_k.$$

Lemma 2. *There exist effectively computable absolute constants $C_2 > 0$ and $C_3 > 0$ such that the inequalities*

$$0 < |\alpha_1^{b_1} \cdots \alpha_k^{b_k} - 1| < \exp\{-(C_2 k n)^{C_3 k} \Omega \log \Omega' \log B\}$$

have no solutions in rational integers $b_1, \ldots, b_k$ with absolute values at most B ($\geqq 2$).

Proof. This profound result is a direct consequence of Baker [1], Theorem 2; cf. Shorey, van der Poorten, Tijdeman and Schinzel [12], p. 66.

As to the proofs of Lemmas 3—8, first references concern the book of Shorey and Tijdeman which also contains historical data. Second references concern refinements of the lemmas due to Győry. These refinements provide explicit values for the computable numbers occurring in the lemmas. Let r denote the unit rank of K.

Lemma 3. *There are independent units $\eta_1, \ldots, \eta_r$ in $\mathcal{O}_K$ such that*

$$\max_i \lceil\eta_i\rceil \leqq C_4$$

and that every unit $\eta \in \mathcal{O}_K$ can be written as $\eta = \eta' \eta_1^{a_1} \cdots \eta_r^{a_r}$ with $a_1, \ldots, a_r \in \mathbb{Z}$ and $\lceil\eta'\rceil \leqq C_5$, where C_4 and C_5 are effectively computable numbers depending only on K.

Proof. See [13], Corollaries A.4 and A.5 or [6], Lemma 3.

There are n isomorphisms $\sigma_1, \ldots, \sigma_n$ of K into the complex numbers; denote the images of an element α of K under these isomorphisms by $\sigma_i(\alpha) = \alpha^{(i)}$ for $i = 1, \ldots, n$.

Lemma 4. *Let $0 \neq \alpha \in K$ with $|N_{K/\mathbb{Q}}(\alpha)| = m$. Then there exists a $\beta \in K$ associated to α such that*

$$|\log(m^{-\frac{1}{n}} |\beta^{(i)}|)| \leqq C_6 \quad \text{for} \quad i = 1, \ldots, n,$$

where C_6 is an effectively computable number which depends only on K.

Proof. See [13], Lemma A.15 or [6], Lemma 3.

Lemma 5. *Let γ_1, γ_2 and γ be non-zero elements of $\mathcal{O}_K$. If $\varepsilon_1, \varepsilon_2$ are units in $\mathcal{O}_K$ such that $\gamma_1 \varepsilon_1 + \gamma_2 \varepsilon_2 = \gamma$, then*

$$\max(\lceil\varepsilon_1\rceil, \lceil\varepsilon_2\rceil) < C_7$$

where C_7 is an effectively computable number which depends only on K and $\gamma_1, \gamma_2, \gamma$.

Proof. [13], Theorem 1.3, [6], Theorem and its Corollary.

Let $v \geqq 1$ and $s \geqq 0$ be rational integers. Let $\{\pi_1, \ldots, \pi_s\}$ be a set of non-zero non-units of $\mathcal{O}_K$. Denote by $S_0 = \mathcal{S}_{K,v}(\pi_1, \ldots, \pi_s)$ the set of all non-zero elements of $\mathcal{O}_K$ of the form $\mu \pi_1^{v_1} \cdots \pi_s^{v_s}$ where $v_1, \ldots, v_s$ are non-negative rational integers and $\mu \in \mathcal{O}_K$ with $\boxed{\mu} \leqq v$. Consider the equation

$$\varepsilon_1 \gamma_1 + \varepsilon_2 \gamma_2 = \gamma y^q \quad \text{in} \quad \varepsilon_1, \varepsilon_2, y \in \mathcal{O}_K, \ \gamma_1, \gamma_2, \gamma \in S_0, \ q \in \mathbb{N} \tag{7}$$

with $\varepsilon_1, \varepsilon_2$ units and $y \neq 0$.

Lemma 6. *Let y be a non-zero non-unit in $\mathcal{O}_K$. Let $\tau \geqq 0$. Suppose*

$$\min(\mathrm{ord}_{\mathfrak{p}}(\gamma_1), \mathrm{ord}_{\mathfrak{p}}(\gamma_2)) \leqq \tau \tag{8}$$

for every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. Then equation (7) implies that the greatest prime factor of q is bounded by an effectively computable number depending only on τ, K and S_0.

Proof. [13], Theorem 9. 3.

Let $f \in K[X]$ be a monic polynomial with splitting field L over K, and let $n \geqq 2$ be a rational integer. Consider the equation

$$f(x) = y^n \quad \text{in} \quad x, y \in \mathcal{O}_K. \tag{9}$$

Lemma 7. *Suppose that $f(X)$ has at least two simple roots if $n \geqq 3$, and at least three simple roots if $n = 2$. If $x, y \in \mathcal{O}_K$ satisfy (9) then*

$$\max(\boxed{x}, \boxed{y}) \leqq C_8$$

with some effectively computable number C_8 depending only on n, f and L.

Proof. [13], Theorems 6. 1 and 6. 2.

Lemma 8. *Suppose $f(X)$ has at least two distinct roots. Further, assume $0 \neq y \in \mathcal{O}_K$ is not a root of unity. Then (9) implies that n is bounded by an effectively computable number C_9 depending only on f and L.*

Proof. [13], Theorem 10. 5. Take $\gamma = z = 1$, $\tau = 0$.

Remarks. 1. The dependence on S_0 in Lemma 6 is actually dependence on $K, v, \pi_1, \ldots, \pi_s$. By [13], Corollary A.2 the algebraic integers $\delta \in K$ with $\boxed{\delta} \leqq D$ belong to a computable finite set which depends only on K and D. We can therefore reduce the dependence on S_0 in Lemma 6 to dependence on $K, v, \boxed{\pi_1}, \ldots, \boxed{\pi_s}$. In this way we shall apply Lemma 6 in section 3.

2. The dependence on L in Lemmas 7 and 8 is actually dependence on the degree and the discriminant of L only. (Cf. the Notes of Chapters 6 and 10 of [13].) By applying [13], Corollary A.7 we infer that the dependence on L of C_8 and C_9 can be reduced to dependence on K and f. In section 3 we shall apply Lemma 7 with C_8 depending only on n, f and K and Lemma 8 with C_9 depending only on f and K.

3. Proof of the Theorem

In the proof $c_1, c_2, \ldots$ denote effectively computable numbers which depend only on K. Further, C_1, C_4 will denote the constants occurring in Lemma 1 and Lemma 3, respectively. As in Lemma 4, $\alpha^{(1)}, \ldots, \alpha^{(n)}$ will signify the images of $\alpha \in K$ under the corresponding isomorphisms of K into $\mathbb{C}$.

A) Let x, y, p, q be a solution of (2) satisfying the restrictions of the theorem. We first show that we can make certain assumptions without loss of generality.

It suffices to prove the theorem in case p and q are primes with $p > c_1$, $q > c_1$ where c_1 is some large number satisfying the conditions stated below. Indeed, if e.g. p has a prime factor p_1 such that $p_1 \leqq c_1$, then (2) implies

$$\pm((x^{\frac{p}{p_1}})^{p_1} - 1) = y^q. \tag{10}$$

By assumption x and y are not roots of unity, hence $xy \neq 0$. By applying Lemmas 8 and 7 with $f(X) = \pm(X^{p_1} - 1)$ to (10), we obtain that $q, \lceil y \rceil$ and $\lceil x^{\frac{p}{p_1}} \rceil = \lceil x \rceil^{\frac{p}{p_1}}$ are bounded by c_2. But then, by Lemma 1, $\max(\lceil x \rceil, p) < c_3$ and (3) follows with an appropriate C. We may therefore assume that p has a prime factor $p_1 > c_1$ and that q has a prime factor $q_1 > c_1$. Then (2) implies

$$(x^{\frac{p}{p_1}})^{p_1} \pm (y^{\frac{q}{q_1}})^{q_1} = 1.$$

Hence, if the assertion of the theorem is proved for primes p, q larger than c_1, then the theorem holds true in the general case.

If q is a prime with $q > 2$, then q is odd. Hence we can restrict our attention to the equation

$$x^p + y^q = 1 \quad \text{in} \quad x, y \in \mathcal{O}_K, \; p, q \in \mathbb{N} \tag{11}$$

with p and q primes, $p > c_1$, $q > c_1$, since we can replace y by $-y$ when necessary.

It is further no restriction to assume that neither x nor y is a unit in $\mathcal{O}_K$. Indeed, if both x and y are units, then (11) and Lemma 5 with $\gamma_1 = \gamma_2 = \gamma = 1$ imply $\lceil x \rceil^p \leqq c_4$ and $\lceil y \rceil^p \leqq c_4$, whence (3) follows with an appropriate C. If exactly one of x, y is a unit, x say, then, by applying Lemma 6 with $\gamma_1 = \gamma_2 = \gamma = 1$, $\varepsilon_1 = -x^p$, $\varepsilon_2 = 1$ to $-x^p + 1 = y^q$, we obtain $q \leqq c_5$. This is excluded by taking $c_1 > c_5$.

We may also assume that $\lceil x \rceil > 3$ and $\lceil y \rceil > 3$. Indeed, if e.g. $\lceil y \rceil \leqq 3$ then Lemma 6 with $s = 1$, $\pi_1 = y$, $\mu = v = 1$, $\varepsilon_1 = -1$, $\varepsilon_2 = \gamma_2 = \gamma = 1$ implies $p \leqq c_6$. This is excluded by taking $c_1 > c_6$. We shall show that the condition $\min(\lceil x \rceil, \lceil y \rceil) > 3$ implies that

$$\text{if} \quad |x^{(j)}| = \lceil x \rceil \quad \text{then} \quad |y^{(j)}| \geqq \frac{1}{2}\lceil y \rceil. \tag{12}$$

It follows from (11) that

$$(x^{(j)})^p + (y^{(j)})^q = 1 \qquad (j = 1, \ldots, n)$$

which gives

$$\lceil x \rceil^p \leqq |y^{(j)}|^q + 1.$$

Further, by (11), $\lceil y \rceil^q \leqq \lceil x \rceil^p + 1$. Consequently

$$\frac{|y^{(j)}|^q}{\lceil y \rceil^q} \geqq \frac{\lceil x \rceil^p - 1}{\lceil x \rceil^p + 1} \geqq \frac{1}{2} > \left(\frac{1}{2}\right)^q,$$

whence (12). Similarly,

$$\text{if} \quad |y^{(i)}| = \lceil y \rceil \quad \text{then} \quad |x^{(i)}| \geqq \frac{1}{2}\lceil x \rceil. \tag{12'}$$

Finally, if $p=q$ then x^p, $-xy$ is a solution of the equation

$$u(u-1)=v^p \quad \text{in} \quad u, v \in \mathcal{O}_K.$$

But xy is not a root of unity, hence, by Lemma 8, we have $p \leqq c_7$. By taking $c_1 > c_7$, this is excluded. Hence we may assume without loss of generality that $p > q$.

B) By A) we may restrict our attention to equation (11) in non-zero non-units $x, y \in \mathcal{O}_K$ with $\overline{x} > 3$ and $\overline{y} > 3$ and primes p, q with $p > q > c_1 \geqq 2$. We first deal with the special case that

$$(x-1)^p + (y-1)^q = 0 \tag{13}$$

which requires another treatment than the general case.

If $\mathfrak{p} \mid x-1$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, then (13) implies $\mathfrak{p} \mid y-1$. But it follows then from (11) that $\mathfrak{p} \mid x$. Hence $\mathfrak{p} \mid 1$ which is impossible. Thus $x-1$ is a unit in $\mathcal{O}_K$ and, by (13), $y-1$ is also a unit in $\mathcal{O}_K$.

Subsequently we show that there is a unit ε in $\mathcal{O}_K$ such that

$$x = 1-\varepsilon^q \quad \text{and} \quad y = 1+\varepsilon^p.$$

Let w be a complex number such that $w^q = 1-x$. Then $w^{pq} = (y-1)^q$. Hence $w^p = \varrho(y-1)$ with ϱ a qth root of unity. For any qth root of unity ζ we have $(\zeta w)^q = 1-x$ and $(\zeta w)^p = \zeta^p \varrho (y-1)$. By $(p, q) = 1$ we can choose ζ such that $\zeta^p = \varrho^{-1}$. Put $\varepsilon = \zeta w$. Then $\varepsilon^q = 1-x$ and $\varepsilon^p = y-1$. Hence $\varepsilon^p, \varepsilon^q \in K$. Since $(p, q) = 1$, we find $\varepsilon \in K$ by applying Euclid's algorithm to the exponents. But ε^p is a unit, thus ε is also a unit in $\mathcal{O}_K$. Further, since by assumption $\overline{y} > 3$, we have $\overline{\varepsilon} > 1$, hence ε is not a root of unity. Therefore we have by Lemma 1

$$\overline{\varepsilon} > 1 + C_1. \tag{14}$$

Let $\mathfrak{p}$ be an arbitrary prime ideal divisor of q in $\mathcal{O}_K$. (11) and (13) imply that

$$(x-1)^p \equiv 1 - y^q \equiv x^p \pmod{\mathfrak{p}}. \tag{15}$$

Since $x-1$ is a unit, $\mathfrak{p} \nmid x-1$ and so, by (15), $\mathfrak{p} \nmid x$. There is an $x' \in \mathcal{O}_K$ with $\mathfrak{p} \nmid x'$ and $xx' \equiv 1 \pmod{\mathfrak{p}}$. Hence (15) gives

$$((x-1)x')^p \equiv 1 \pmod{\mathfrak{p}}.$$

Here $(x-1)x' \equiv 1-x' \not\equiv 0$ and $\not\equiv 1 \pmod{\mathfrak{p}}$. This means that p is the smallest positive integer t for which

$$(1-x')^t \equiv 1 \pmod{\mathfrak{p}}.$$

But

$$(1-x')^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}},$$

hence $p \mid N(\mathfrak{p}) - 1$ in $\mathbb{Z}$. Since $N(\mathfrak{p}) = q^f$ with some positive integer $f \leqq n$, we obtain

$$p \leqq q^n. \tag{16}$$

Using (14) and (16), we shall now prove that q is bounded. We may assume without loss of generality that $\overline{\varepsilon}$ is $|\varepsilon|$. Put

$$f(z) = (1-z^q)^p + (1+z^p)^q - 1.$$

Then

$$0 = f(\varepsilon) = \sum_{k=0}^{p} \binom{p}{k} (-\varepsilon^q)^k + \sum_{l=0}^{q} \binom{q}{l} \varepsilon^{pl} - 1.$$

The leading term of f is $pz^{(p-1)q}$. We have

$$p|\varepsilon|^{(p-1)q} = \left|\sum_{k=0}^{p-2}\binom{p}{k}(-\varepsilon^q)^k + \sum_{l=0}^{q-1}\binom{q}{l}\varepsilon^{pl} - 1\right|$$
$$\leqq q|\varepsilon|^{p(q-1)} + \sum_{k=0}^{p-2}\binom{p}{k}|\varepsilon|^{kq} + \sum_{l=1}^{q-2}\binom{q}{l}|\varepsilon|^{lp}.$$

By $p>q$ and (14), we obtain

$$1 \leqq |\varepsilon|^{q-p} + \frac{1}{p}\sum_{k=0}^{p-2}\binom{p}{k}|\varepsilon|^{(k-p+1)q} + \frac{1}{p}\sum_{l=1}^{q-2}\binom{q}{l}|\varepsilon|^{(l-q)p+q}$$
$$\leqq \frac{1}{|\varepsilon|} + \frac{1}{p}\sum_{k=1}^{p-1}\binom{p}{k+1}|\varepsilon|^{-kq} + \frac{1}{p}\sum_{l=1}^{q-2}\binom{q}{l+1}|\varepsilon|^{-lp}$$
$$< \frac{1}{|\varepsilon|} + \sum_{k=1}^{\infty} p^k|\varepsilon|^{-kq} + \sum_{l=1}^{\infty} q^l|\varepsilon|^{-lp}.$$

By (14), (16) and $q>c_1$ we have

$$\frac{p}{|\varepsilon|^p} \leqq \frac{p}{|\varepsilon|^q} \leqq \frac{q^n}{(1+C_1)^q} < \min\left(\frac{1}{2}, \frac{C_1}{4(1+C_1)}\right)$$

after taking c_1 sufficiently large. It follows that

$$\frac{C_1}{1+C_1} \leqq 1 - \frac{1}{|\varepsilon|} < \sum_{k=1}^{\infty}\left(\frac{p}{|\varepsilon|^q}\right)^k + \sum_{l=1}^{\infty}\left(\frac{p}{|\varepsilon|^p}\right)^l$$
$$\leqq \frac{2p}{|\varepsilon|^q} + \frac{2p}{|\varepsilon|^p} < \frac{C_1}{1+C_1},$$

a contradiction.

C) In view of A) and B) we restrict our further attention to equation (11) in non-zero non-units $x, y \in \mathcal{O}_K$ with $|x|>3$ and $|y|>3$ and primes p, q with $p>q>c_1 \geqq 2$ such that

$$(x-1)^p + (y-1)^q \neq 0. \tag{17}$$

For any $\alpha \in K$, we denote by $[\alpha]$ the principal ideal generated by α. We have, by (11),

$$[y]^q = [1-x]\,[1+x+\cdots+x^{p-1}] = [x-1]\,[\beta(x-1)+p]$$

for some $\beta \in \mathcal{O}_K$. We can write

$$[p] = \mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_s^{a_s}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are distinct prime ideals in $\mathcal{O}_K$, $s \leqq n$, and $a_1, \ldots, a_s$ are positive integers not exceeding n. If, for some prime ideal $\mathfrak{p}$ and positive integer a, $\mathfrak{p}^a$ is a common divisor of $[x-1]$ and $[\beta(x-1)+p]$ then $\mathfrak{p}^a \mid [p]$ and therefore $a \leqq n$. Hence we can write

$$[x-1] = \mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_s^{b_s}\mathfrak{a}^q$$

where $\mathfrak{a}$ is an integral ideal and $b_1, \ldots, b_s$ are rational integers with absolute values at most n. Since $N(\mathfrak{p}_i) = p^{f_i}$ for some positive integer $f_i \leqq n$, we have

$$p^{-c_8} \leqq N(\mathfrak{p}_i^{b_i}) \leqq p^{c_8} \quad (i=1,\ldots,s).$$

Let h denote the class number of K. We have

$$[x-1]^h=(\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_s^{b_s})^h\,\alpha^{hq}. \tag{18}$$

Here $\alpha^h=[\kappa]$ and $(\mathfrak{p}_1^{b_1}\cdots\mathfrak{p}_s^{b_s})^h=[\pi_0]$ for some $\kappa\in\mathcal{O}_K$ and $\pi_0\in K$ such that $\pi_0=\frac{\pi_1}{\pi_2}$ with $\pi_1,\pi_2\in\mathcal{O}_K$ and

$$|\log|N_{K/\mathbb{Q}}(\pi_k)||\leqq c_9\log p \qquad (k=0,1,2). \tag{19}$$

It follows from (18) that

$$(x-1)^h=\varepsilon\pi_0\kappa^q \tag{20}$$

for some unit $\varepsilon\in\mathcal{O}_K$. By virtue of Lemmas 3 and 4 and (19) and (20) there are independent units $\eta_1,\ldots,\eta_r$ in $\mathcal{O}_K$ such that $\max_i\lceil\eta_i\rceil\leqq C_4$ and that

$$(x-1)^h=\eta_1^{u_1}\cdots\eta_r^{u_r}\theta_0 w^q \tag{21}$$

where the u_i are rational integers with $0\leqq u_i<q$ for $i=1,\ldots,r$, $0\neq w\in\mathcal{O}_K$ and $0\neq\theta_0\in K$ with $\theta_0=\frac{\theta_1}{\theta_2}$ such that $\theta_1,\theta_2\in\mathcal{O}_K$ and

$$\max_{1\leqq j\leqq n}|\log|\theta_k^{(j)}||\leqq c_{10}\log p \qquad (k=0,1,2). \tag{22}$$

This gives (recall (6))

$$H(\theta_0)=H(\theta_1/\theta_2)\leqq(\lceil\theta_1\rceil+\lceil\theta_2\rceil)^n\leqq p^{c_{11}}. \tag{23}$$

Similarly, we can write

$$(1-y)^h=\eta_1^{v_1}\cdots\eta_r^{v_r}\tau_0\sigma^p \tag{24}$$

with rational integers v_i such that $0\leqq v_i<p$ for $i=1,\ldots,r$, and with $0\neq\sigma\in\mathcal{O}_K$, $0\neq\tau_0\in K$ such that

$$\max_{1\leqq j\leqq n}|\log|\tau_0^{(j)}||\leqq c_{12}\log q \tag{25}$$

and

$$H(\tau_0)\leqq q^{c_{13}}. \tag{26}$$

D) From (11) we obtain

$$(x^{(j)})^p+(y^{(j)})^q=1 \qquad (j=1,\ldots,n).$$

Hence we may assume without loss of generality that $|x|=\lceil x\rceil$. Put $X=H(x)$ and $Y=H(y)$. Since, by assumption, $\lceil x\rceil>3$, we have

$$X\leqq(2\lceil x\rceil)^n\leqq\lceil x\rceil^{2n},\quad \lceil x\rceil\leqq 2X \qquad \text{(cf. (5))} \tag{27}$$

and similarly

$$Y\leqq\lceil y\rceil^{2n},\quad \lceil y\rceil\leqq 2Y. \tag{28}$$

It follows from (11) that

$$\Lambda_1:=1-\frac{(-y)^q}{x^p}=\frac{1}{x^p}, \tag{29}$$

whence

$$|\Lambda_1| = \frac{1}{\lceil x \rceil^p} \leqq X^{-\frac{p}{2n}}. \tag{30}$$

On the other hand, by Lemma 2 and $p > q$, we have

$$|\Lambda_1| > \exp\{-c_{14}(\log X)(\log Y)(\log\log Y)(\log p)\}. \tag{31}$$

Now (30) and (31) imply

$$p \leqq c_{15}(\log Y)^2 \log p. \tag{32}$$

By estimating $\Lambda_2 := 1 - \frac{(-x)^p}{y^q} = \frac{1}{y^q}$ we can prove in a similar way that

$$q \leqq c_{16}(\log X)^2 \log p. \tag{33}$$

E) We shall now prove that

$$q < c_{17}(\log p)^{c_{18}}. \tag{34}$$

To prove this, we may assume that

$$q > \log p. \tag{35}$$

Further, we may assume that

$$\min(X, Y) > p^{c_{19}} \tag{36}$$

for some large number c_{19}, to be chosen later. Indeed, if $Y \leqq p^{c_{19}}$ then $q < p \leqq c_{20}(\log p)^3$ follows from (32), whence (34). Further, in case $X \leqq p^{c_{19}}$, (34) immediately follows from (33). Observe that (36) implies

$$\min(\lceil x \rceil, \lceil y \rceil) > p^{\frac{c_{19}}{2n}}. \tag{37}$$

By $|x| = \lceil x \rceil$ and (12), we have $|y| \geqq \frac{1}{2}\lceil y \rceil$. From (11) we obtain

$$\left| \frac{(-y)^q}{x^p} - 1 \right| = \frac{1}{\lceil x \rceil^p}. \tag{38}$$

Further, by taking c_{19} large enough, (37) and $|x| > 3$ imply

$$|x-1| \geqq \max\left(\frac{1}{2}|x|, \sqrt{|x|}\right) \geqq \max\left(\frac{1}{2}\lceil x \rceil, p\right) \tag{39}$$

and it follows that

$$\left| \frac{x^p}{(x-1)^p} - 1 \right| = \left| \frac{((x-1)+1)^p - (x-1)^p}{(x-1)^p} \right| \leqq \sum_{i=1}^{p} \frac{p^i}{|x-1|^i} \leqq \frac{p^2}{|x-1|} \leqq \frac{2p^2}{\lceil x \rceil}. \tag{40}$$

Similarly, by (11) and (37),

$$|y| \geqq \max\left(\frac{1}{2}\lceil x \rceil, q\right). \tag{41}$$

Hence we have, by taking c_{19} large enough,

$$\left|\frac{(1-y)^q}{(-y)^q}-1\right|=\left|\frac{(1-y)^q+y^q}{(-y)^q}\right|\leqq\sum_{i=1}^{q}\frac{q^i}{|y|^i}\leqq\frac{2p^2}{|x|}. \tag{42}$$

For any complex numbers z_1, z_2, z_3

$$z_1z_2z_3-1=\prod_{i=1}^{3}(z_i-1)+\sum_{1\leqq i<j\leqq 3}(z_i-1)(z_j-1)+\sum_{i=1}^{3}(z_i-1).$$

Hence (38), (40) and (42) imply

$$\left|\frac{(1-y)^q}{(x-1)^p}-1\right|\leqq\frac{c_{21}p^4}{|x|}. \tag{43}$$

Further we have, by (11), (39) and (41),

$$\left|\frac{(1-y)^q}{(x-1)^p}\right|=\left|\frac{(1-y)^q}{y^q}\right|\cdot\left|\frac{1-x^p}{(x-1)^p}\right|\leqq 2\left(1+\frac{1}{|y|}\right)^q\left(1+\frac{1}{|x-1|}\right)^p$$

$$\leqq 2\left(1+\frac{2}{|x|}\right)^{p+q}\leqq 2\left(1+\frac{2}{p}\right)^{2p}\leqq c_{22}. \tag{44}$$

For

$$\Lambda_3:=\frac{(1-y)^{qh}}{(x-1)^{ph}}-1 \tag{45}$$

we obtain, from (43) and (44),

$$|\Lambda_3|<\frac{c_{23}p^4}{|x|}. \tag{46}$$

Suppose now that $\Lambda_3\neq 0$, i.e. that $(x-1)^{ph}\neq(1-y)^{qh}$. Using (45), (21) and (24), we obtain

$$\Lambda_3=\eta_1^{e_1}\cdots\eta_r^{e_r}\tau_0^q\theta_0^{-p}\left(\frac{\sigma}{w}\right)^{pq}-1$$

where $e_i\in\mathbb{Z}$ with $|e_i|\leqq pq$ for $i=1,\ldots,r$. Put $\mathscr{H}_1=2H(\sigma)$, $\mathscr{H}_2=2H(w)$ and $\mathscr{H}_0=\max(\mathscr{H}_1,\mathscr{H}_2)$. Then

$$H\left(\frac{\sigma}{w}\right)\leqq(|\sigma|+|w|)^n\leqq(\mathscr{H}_1+\mathscr{H}_2)^n\leqq c_{24}\mathscr{H}_0^{c_{25}}. \tag{47}$$

By applying Lemma 2 to Λ_3 and using (23), (26), (47) and $p>q$ we obtain

$$|\Lambda_3|>\exp\{-c_{26}(\log p)^{c_{27}}\log\mathscr{H}_0\}.$$

This together with (46) and (27) implies

$$c_{28}\log X\leqq\log|x|\leqq c_{29}(\log p)^{c_{30}}\log\mathscr{H}_0. \tag{48}$$

If $\mathscr{H}_0\leqq c_{31}$ then (48) and (33) give (34). We therefore assume that $\mathscr{H}_0>c_{31}$ where c_{31} satisfies some conditions stated below.

First suppose that $\mathscr{H}_2 > c_{31}$. Then, by (22) and (35), we have

$$\left|\frac{1}{\theta_0^{(j)}}\right| < p^{c_{32}} < c_{33}^q < \mathscr{H}_2^{\frac{q}{4n}} \quad (j=1,\ldots,n).$$

Hence we obtain, from (21) and (27),

$$|w^{(j)}|^q \leqq |x^{(j)}-1|^h \left|\frac{1}{\theta_0^{(j)}}\right| \cdot \prod_{i=1}^{r} \left|\frac{1}{\eta_i^{(j)}}\right|^{u_i}$$

$$\leqq |x^{(j)}-1|^h \mathscr{H}_2^{\frac{q}{4n}} c_{34}^q < c_{35} X^h \mathscr{H}_2^{\frac{q}{3n}} \quad (j=1,\ldots,n)$$

by making c_{31} large enough. Choosing j such that $|w^{(j)}| = \lceil w \rceil$, we obtain

$$c_{35} X^h \mathscr{H}_2^{\frac{q}{3n}} > \lceil w \rceil^q \geqq \left(\frac{1}{4} \mathscr{H}_2^{\frac{1}{n}}\right)^q > \mathscr{H}_2^{\frac{q}{2n}}$$

if c_{31} is sufficiently large. Consequently, we have

$$\log X > c_{36} q \log \mathscr{H}_2 \quad \text{if } \mathscr{H}_2 \text{ is large enough.} \tag{49}$$

By using (24) and (25) one can prove in a similar manner that

$$\log Y > c_{37} p \log \mathscr{H}_1 \tag{50}$$

if $\mathscr{H}_1 > c_{31}$ and c_{31} is sufficiently large. If $\mathscr{H}_0 = \mathscr{H}_2$ then (48) and (49) imply (34). Next suppose $\mathscr{H}_0 = \mathscr{H}_1$. From (11) we obtain $\lceil y \rceil^q \leqq 1 + \lceil x \rceil^p \leqq \lceil x \rceil^{2p}$. This together with (27) and (28) implies

$$q \log Y < c_{38} p \log X. \tag{51}$$

Now (50), (51) and (48) imply

$$c_{37} p q \log \mathscr{H}_0 < q \log Y < c_{38} p \log X < c_{39} p (\log p)^{c_{30}} \log \mathscr{H}_0,$$

whence (34) follows.

F) To prove (34) we are left with the case

$$(x-1)^{ph} = (1-y)^{qh}. \tag{52}$$

If $\mathfrak{p} \mid x-1$ for some prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, then (52) implies $\mathfrak{p} \mid y-1$. But it follows then from (11) that $\mathfrak{p} \mid x$. Thus $\mathfrak{p} \mid 1$ which is impossible. Hence $x-1$ is a unit in $\mathcal{O}_K$ and thus, by (52), $y-1$ is also a unit in $\mathcal{O}_K$. By Lemma 3 we can write

$$x-1 = \eta_1^{u_1} \cdots \eta_r^{u_r} \theta_0 w^q \tag{21'}$$

and

$$1-y = \eta_1^{v_1} \cdots \eta_r^{v_r} \tau_0 \sigma^p \tag{24'}$$

instead of (21) and (24) respectively, where $\theta_0, \tau_0, w, \sigma \in \mathcal{O}_K$ with

$$\max(\lceil \theta_0 \rceil, \lceil \tau_0 \rceil) \leqq c_{40}$$

and $u_i, v_i \in \mathbb{Z}$ with $0 \leqq u_i < q$, $0 \leqq v_i < p$ for $i = 1,\ldots,r$. We can now repeat the argument of part E) above with

$$\Lambda_4 := \frac{(1-y)^q}{(x-1)^p} - 1$$

instead of Λ_3. Since, by (17), $\Lambda_4 \neq 0$, inequality (34) follows.

G) We shall now prove that p is bounded from above by using (32), (34) and Lemma 2. Note that (32) and (34) are independent of the assumption $|x|=\lceil x\rceil$ made in D). Hence we may assume without loss of generality that, instead of this assumption, $|y|=\lceil y\rceil$. Then, by (11),

$$\left|\frac{x^p}{(1-y)^q}\right| \leqq \left|\frac{1-y^q}{(1-y)^q}\right| \leqq \frac{2|y|^q}{(|y|/2)^q} \leqq 4^q. \tag{53}$$

Hence, using again (11),

$$\left|\frac{x^p}{(1-y)^q}-1\right| = \left|\frac{x^p+(y-1)^q}{(1-y)^q}\right| \leqq \frac{c_{41}^q|y|^{q-1}}{(|y|/2)^q} \leqq \frac{c_{42}^q}{\lceil y\rceil}. \tag{54}$$

Putting

$$\Lambda_5 := \frac{x^{ph}}{(1-y)^{qh}}-1,$$

it follows from (53) and (54) that

$$|\Lambda_5| < \frac{c_{43}^q}{\lceil y\rceil}. \tag{55}$$

Suppose that $|\Lambda_5|\neq 0$, i.e. that $x^{ph}\neq(1-y)^{qh}$. We are going to derive a lower bound for $|\Lambda_5|$. By (24) we have

$$\frac{x^{ph}}{(1-y)^{qh}} = \eta_1^{d_1}\cdots\eta_r^{d_r}\tau_0^{-q}\left(\frac{x^h}{\sigma^q}\right)^p$$

with rational integers d_i such that $|d_i|<pq$ for $i=1,\ldots,r$. Hence, by (53) and (25),

$$\left|\frac{x^h}{\sigma^q}\right| \leqq c_{44}\left(\prod_{i=1}^{r}|\eta_i|^{-d_i}\right)^{\frac{1}{p}}|\tau_0|^{\frac{q}{p}} \leqq c_{45}^q.$$

Then, by (12′), we have

$$\lceil x\rceil \leqq c_{46}|x| \leqq c_{47}^q|\sigma|^q \leqq c_{48}^q(H(\sigma))^q.$$

Put $\mathscr{H}_3=2H(\sigma)$. It follows that

$$H\left(\frac{x^h}{\sigma^q}\right) \leqq (\lceil x\rceil^h+\lceil\sigma\rceil^q)^n \leqq c_{49}^q\mathscr{H}_3^{c_{50}q}. \tag{56}$$

By applying Lemma 2 to

$$\Lambda_5 = \eta_1^{d_1}\cdots\eta_r^{d_r}\tau_0^{-q}\left(\frac{x^h}{\sigma^q}\right)^p - 1$$

and using (26) and (56), we obtain

$$|\Lambda_5| > \exp\{-c_{51}q(\log p)^{c_{52}}\log\mathscr{H}_3\}. \tag{57}$$

Comparing (55) with (57) we obtain

$$\log Y \leqq c_{53}\log\lceil y\rceil \leqq c_{54}q(\log p)^{c_{52}}\log\mathscr{H}_3. \tag{58}$$

If $\mathscr{H}_3\leqq c_{55}$ for some c_{55} then (58) together with (32) and (34) yields $p\leqq c_{56}(\log p)^{c_{57}}$ and so $p\leqq c_{58}$.

Suppose now that $\mathscr{H}_3 > c_{55}$ for some sufficiently large c_{55}. Then we have, analogously to (50),

$$\log Y > c_{59} p \log \mathscr{H}_3. \tag{59}$$

From (58), (59) and (34) it follows now again that $p \leqq c_{60}(\log p)^{c_{61}}$, whence $p \leqq c_{62}$. By taking $c_1 > c_{62}$ this is excluded.

H) We are left with the case $x^{ph} = (1-y)^{qh}$. This together with (11) gives $(1-y^q)^h = (1-y)^{qh}$. Putting $u = y^q$, $v = y(1-y)$, it follows that

$$(u(1-u))^h = v^{qh} \tag{60}$$

where $v \neq 0$. By assumption y is not a unit, hence v is not a root of unity. Applying Lemma 8 to (60), we obtain $q \leqq c_{63}$. By taking $c_1 > c_{63}$ this is excluded. The proof of the theorem is complete.

References

[1] *A. Baker*, The theory of linear forms in logarithms, Transcendence Theory: Advances and Applications, London-New York 1977, 1—27.

[2] *D. C. Cantor* and *E. G. Straus*, On a conjecture of D. H. Lehmer, Acta Arith. **42** (1982), 97—100.

[3] *J. W. S. Cassels*, On the equation $a^x - b^y = 1$, Amer. J. Math. **75** (1953), 159—162.

[4] *E. Catalan*, Note extraite d'une lettre adressée à l'éditeur, J. reine angew. Math. **27** (1844), 192.

[5] *E. Dobrowolski*, On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. **34** (1979), 391—401.

[6] *K. Győry*, On the solutions of linear diophantine equations in algebraic integers of bounded norm, Ann. Univ. Sci. Budapest. Eötvös, Sect. Math. **22—23** (1979—1980), 225—233.

[7] *K. Győry*, Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers Pure Appl. Math. **56**, Kingston, Canada, 1980.

[8] *M. Langevin*, Quelques applications de nouveaux résultats de van der Poorten, Sém. Delange-Pisot-Poitou, Paris 1975/76, Exp. G 12.

[9] *S. S. Pillai*, On the equation $2^x - 3^y = 2^X + 3^Y$, Bull. Calcutta Math. Soc. **37** (1945), 15—20.

[10] *P. Ribenboim*, Consecutive powers, Exposit. Math. **2** (1984), 193—221.

[11] *A. Schinzel* and *H. Zassenhaus*, A refinement of two theorems of Kronecker, Michigan Math. J. **12** (1965), 81—85.

[12] *T. N. Shorey*, *A. J. van der Poorten*, *R. Tijdeman* and *A. Schinzel*, Applications of the Gel'fond-Baker method to diophantine equations, Transcendence Theory: Advances and Applications, London-New York 1977, 59—77.

[13] *T. N. Shorey* and *R. Tijdeman*, Exponential diophantine equations, to appear.

[14] *R. Tijdeman*, On the equation of Catalan, Acta Arith. **29** (1976), 197—209.

[15] *R. Tijdeman*, Exponential diophantine equations, Proc. Intern. Congr. Math. Helsinki 1978, Helsinki 1980, 381—387.

[16] *R. Tijdeman*, On the Fermat-Catalan equation, Jahresber. Deutsche Math. Verein. **87** (1985), 1—18.

Mathematical Institute, Kossuth Lajos University, H-4010 Debrecen, Hungary

Mathematical Institute, R. U. Leiden, NL-2300 RA Leiden, The Netherlands

Eingegangen 22. Oktober 1985