COMPOSITIO MATHEMATICA

JAN-HENDRIK EVERTSE

On the equation $ax^n - by^n = c$

Compositio Mathematica, tome 47, n° 3 (1982), p. 289-315
<http://www.numdam.org/item?id=CM_1982__47_3_289_0>

COMPOSITIO MATHEMATICA, Vol. 47, Fasc. 3, 1982, pag. 289–315

ON THE EQUATION $ax^n - by^n = c$

Jan-Hendrik Evertse

§1. Introduction

We deal with the diophantine equation

$$ax^n - by^n = c \tag{1}$$

in integers x, y. Let $R(n, c)$ denote the number of residue classes $z \pmod c$ satisfying $z^n \equiv 1 \pmod c$. We shall derive upper bounds for the number of solutions of (1) in terms of $R(n, c)$.

THEOREM 1: *The number of solutions of*

$$|ax^n - by^n| = c \tag{2}$$

$$(a, b, c, n \text{ integers with } a > 0, b \neq 0, c > 0, n \geq 3)$$

in positive integers x, y with $(x, y) = 1$ is bounded above by

$$\begin{aligned} &2R(3, c) + 6 \text{ if } n = 3, \\ &R(4, c) + 3 \text{ if } n = 4, \\ &R(5, c) + 2 \text{ if } n = 5 \ (R(5, c) + 1 \text{ if } c \geq 220), \\ &R(6, c) + 2 \text{ if } n = 6 \ (R(6, c) + 1 \text{ if } c \geq 9), \\ &R(n, c) + 1 \text{ if } n \geq 7. \end{aligned}$$

If c has many prime divisors one of which is large, we can derive a better result from the following theorem.

THEOREM 2: *The number of solutions of*

$$ax^n - by^n = dz \tag{3}$$

$$(a, b, d, n \text{ integers with } a > 0, b \neq 0, d > 0, n \geq 3, (a, d) = (b, d) = 1)$$

0010-437X/82090289–27$00.20/0

in integers x, y, z *with* $x > 0, y > 0, (x, y) = 1, 0 < |z| \leq d^{2n/5-1}$ *is bounded above by*

$$\begin{aligned} &3R(3,d) + 6 \text{ if } n = 3,\\ &2R(4,d) + 2 \text{ if } n = 4,\\ &2R(n,d) + 1 \text{ if } n \in \{5,6\},\\ &R(7,d) + 3 \text{ if } n = 7,\\ &R(n,d) + 2 \text{ if } n \geq 8. \end{aligned}$$

To avoid confusion, we agree that by solutions of (2), respectively (3), we shall always mean solutions in integers x, y, respectively x, y, z with $x > 0$, $y > 0$, $(x, y) = 1$, $z \neq 0$.

It is possible to give a simple upper bound for $R(n, c)$. For fixed n, $R(n, m)$ is a multiplicative function of m. Let $m = 2^{k_0}m'$, where k_0 is a non-negative integer, $m' = p_1^{k_1}, p_2^{k_2}, \ldots, p_t^{k_t}$ for distinct odd primes $p_1, p_2, \ldots, p_t$ and positive integers $k_1, k_2, \ldots, k_t$. Then

$$R(n, m) = R(n, 2^{k_0}) \prod_{i=1}^{t} R(n, p_i^{k_i}).$$

We denote Euler's totient-function by ϕ and the number of prime divisors of m by $\omega(m)$. Then we have $R(n, p_i^{k_i}) = (n, \phi(p_i^{k_i}))$ for $i \in \{1, 2, \ldots, t\}$. Hence $R(n, m')$ divides

$$(n^t, \prod_{i=1}^{t} \phi(p_i^{k_i})) = (n^{\omega(m')}, \phi(m')). \tag{4}$$

Further we have $R(n, 2^{k_0}) = 1$ if $k_0 \in \{0, 1\}$ and $R(n, 2^{k_0}) = (n, 2)(n, 2^{k_0-2})$ if $k_0 \geq 2$. Hence $R(n, 2^{k_0})$ divides $((n, 2)n, \phi(2^{k_0}))$. Together with (4) this implies that $R(n, m)$ divides $((n, m, 2)n^{\omega(m)}, \phi(m))$. Substituting this into theorem 1 and 2 we obtain:

COROLLARY 1: (i) (2) *has at most* $2n^{\omega(c)} + 6$ *solutions,*
(ii) (3) *has at most* $4n^{\omega(d)} + 3$ *solutions with* $|z| \leq d^{2n/5-1}$

As a consequence of corollary 1, (ii) we obtain

COROLLARY 2: *Put* $c_1 = c/(c, [a, b])$, *where* $[a, b]$ *denotes the positive lcm of* a *and* b. *Suppose there is a prime power* P *dividing* c_1 *such that* $P^n \geq c_1^{5/2}$. *Then* (2) *has at most* $4n + 3$ *solutions.*

If $(a, c) = (b, c) = 1$ then corollary 2 follows at once from corollary

1, (ii), by putting $d = P$, $|z| = c/d$. The following lemma, which will be proved in §2, shows that the assumption that $(a, c) = (b, c) = 1$ is no restriction.

LEMMA 1: *Let a, b, c, n be integers with the same meaning as in* (2) *and let c_1 be defined as in corollary* 2. *There are non-zero integers a_1, b_1 with $(a_1, c_1) = (b_1, c_1) = 1$, having the same signs as a, b respectively, such that the number of solutions of* (2) *does not exceed the number of solutions of $|a_1 x^n - b_1 y^n| = c_1$ in positive integers x, y with $(x, y) = 1$.*

Note that lemma 1 shows, together with the inequality $R(n, c_1) \leq R(n, c)$ that we may assume that $(a, c) = (b, c) = 1$ in the proof of theorem 1.

Let $R \geq 1$ be some constant. Any pair (x_0, y_0) such that (x_0, y_0) is a solution of (2) or (x_0, y_0, z_0) is a solution of (3) for a suitable value of z_0 with $|z_0| \leq R$, satisfies both a diophantine inequality

$$0 < |ax^n - by^n| \leq C \text{ in } x, y \in \mathbb{N} \text{ with } (x, y) = 1, \tag{5}$$

and a congruence equation

$$ax^n - by^n = 0 (\mathrm{mod}\, m) \text{ in } x, y \in \mathbb{N} \text{ with } (x, m) = (y, m) = 1, \tag{6}$$

where $C \geq 1$ is a real number and a, b, m are integers with $a > 0$, $b \neq 0$, $m > 0$, $(a, m) = (b, m) = 1$. We obtain (2) by taking $C = m = c$ and (3) by taking $C = dR, m = d$. By congruence considerations we shall estimate the number of pairs (x, y) satisfying both (5) and (6) for which $\max(ax^n, |by^n|)$ is "small". By an approximation method we shall show that (5) cannot have many "large" solutions.

THEOREM 3: *Let M_n, A_n be given by the following table:*

n	3	4	5	6	7	≥ 8
M_n	1.71×10^7	1449	57	135	32	$8.4n$
A_n	11	5	3.25	2.67	2.4	2.4

Then the number of solutions of (5) *with $\max(ax^n, |by^n|) \geq M_n C^{A_n}$ is at most* 3 *if $n = 3$ and at most* 1 *if $n \geq 4$.*

The main tools in the proof of theorem 3 are hypergeometric functions. Using properties of these functions, Siegel [6] showed that (5) has

at most one solution if

$$|ab|^{n/2-1} \geq 4(n\prod_{p|n} p^{1/(p-1)})^n C^{2n-2},$$

where $\prod_{p|n}$ denotes the product over all primes dividing n. Hyyrö ([3], Satz 1, p. 11) generalized Siegel's result in the following way: there are constants $\sigma_0 = \sigma_0(n) \in (0, 1]$, $C_0 = C_0(n, ab) > 0$ with the following property: for any pair of real numbers σ, C with $\sigma_0 \leq \sigma \leq 1$, $C > 0$ such that $\sigma = \sigma_0$, $C > C_0$ do not hold simultaneously, the diophantine equation

$$|ax^n - by^n| = z \qquad (a, b, n \in \mathbb{N},\ n \geq 3)$$

has at most one solution in integers x, y, z with $x \geq 1$, $y \geq 1$, $(x, y) = 1$, $z < C \max(ax^n, by^n)^{1-\sigma}$ and $\max(ax^n, by^n) > G = G(n, \sigma, C, ab)$. By choosing $\sigma = 1$ for those values of n for which $\sigma_0(n) < 1$, i.e. $n \geq 4$, Hyyrö derives a corollary from his general result (cf. [3], Satz 5, p. 30) which does not differ much from our theorem 3. For $n \in \{4, 5\}$ our result is slightly better and for $n \geq 8$ theorem 3 gives bounds which are worse than the bounds given by Hyyrö but more convenient for our purposes. Although our method of proof is similar to that of Hyyrö, we shall give the complete proof of theorem 3 for convenience of the reader.

It is also possible to estimate the number of solutions in terms of c and not in terms of a, b, n:

COROLLARY 3: *Let $\varepsilon > 0$. The number of solutions of* (1) *in integers x, y is bounded above by $C(\varepsilon)|c|^{\varepsilon}$, where $C(\varepsilon)$ is a constant depending only on ε and not on a, b, c, n.*

This corollary will be proved in §6. By a result of Baker [1] on lower bounds for linear forms in logarithms, (1) is only solvable in integers x, y with $|xy| \geq 2$ if n is less then some constant depending on a, b, c which can be given explicitly. Using this fact in combination with corollary 3, we obtain

THEOREM 4: *Let $\varepsilon > 0$. The number of solutions of*

$$ax^z - by^z = c \quad (a, b, c \text{ integers with } abc \neq 0) \tag{7}$$

in integers x, y, z with $|xy| \geq 2$ and $z \geq 3$ is bounded above by

$$D(\varepsilon) \log M (\log\log M)^2 |c|^{\varepsilon},$$

where $M = \max(3, |a|, |b|)$ and $D(\varepsilon)$ is a constant depending only on ε.

§2. Lemmas and special cases

In this section we shall prove some auxiliary results for the proofs of theorems 1, 2 and 3. We shall also deal with some special cases of these theorems. First of all, we shall prove lemma 1.

PROOF OF LEMMA 1: We may assume that $(a, b) = 1$ for otherwise put $d = (a, b)$, $a = da'$, $b = db'$, $c = dc'$. Then

$$c_1 = \frac{c'd}{(c'd, a'b'd)} = \frac{c'}{(c', a'b')}$$

and the number of solutions of (2) does not change if a, b, c are replaced by a', b', c' respectively. Hence it suffices to prove the lemma with a', b', c' instead of a, b, c.

Let (x_0, y_0) be a solution of (2). Put $f_1 = (a, c)$, $f_2 = (b, c)$. From $(a, b) = 1$ and $(x_0, y_0) = 1$ it follows easily that $(a, y_0^n) = f_1$, $(b, x_0^n) = f_2$, $(ax_0^n, by_0^n) = (a, y_0^n)(b, x_0^n) = f_1 f_2 = (ab, c)$. Let F_1, F_2 be the smallest positive integers such that $f_1 | F_1^n$, $f_2 | F_2^n$. Then $F_1 | y_0$, $F_2 | x_0$. Put $a_1 = aF_2^n / f_1 f_2$, $b_1 = bF_1^n / f_1 f_2$. Then a_1, b_1 are non-zero integers having the same signs as a, b respectively such that $(a_1, c_1) = (b_1, c_1) = 1$. Furthermore, every solution (x_0, y_0) of $|ax^n - by^n| = c$ corresponds to a solution $(x_0/F_2, y_0/F_1)$ of $|a_1 x^n - b_1 y^n| = c_1$. Hence the number of solutions of (2) is at most equal to the number of solutions of $|a_1 x^n - b_1 y^n| = c_1$ in positive integers x, y with $(x, y) = 1$ which proves our lemma. □

As we have noticed before, we may assume that $(a, c) = (b, c) = 1$ in the proof of theorem 1. We shall distinguish between the cases $b > 0$ and $b < 0$. There we use the fact that the numbers a_1, b_1 mentioned in lemma 1 have the same signs as a, b respectively.

In the sequel the constants a, b, c, d, m, n, C will have the same meaning as in (2), (3), (5), (6). For convenience we repeat the conditions which must be imposed on these constants.

$$\begin{cases} a, b, c, d, m, n \in \mathbb{Z}, C \in \mathbb{R}, a > 0, b \neq 0, c > 0, d > 0, m > 0, n \geq 3, C \geq 1, \\ (a, c) = (b, c) = 1 \text{ in (2)}, (a, d) = (b, d) = 1 \text{ in (3)}, (a, m) = (b, m) = 1 \text{ in (6)}. \end{cases} \tag{8}$$

Further we define the set

$$S(m) = \{(x, y) | x, y \in \mathbb{N}, (x, m) = (y, m) = 1, m \in \mathbb{N}\}.$$

On $S(m)$ we define the following congruence relation: (x_1, y_1) and (x_2, y_2)

are congruent mod m if $x_1y_2 \equiv x_2y_1 \pmod{m}$, i.e. if $x_1/y_1 \equiv x_2/y_2 \pmod{m}$. We denote this by $(x_1, y_1) \equiv (x_2, y_2) \pmod{m}$.

LEMMA 2: *The solutions of* (6) *belong to at most* $R(n, m)$ *congruence classes* mod m.

PROOF: Let (x_0, y_0) be a fixed solution of (6). Then $(x_0, y_0) \in S(m)$ and since also $(a, m) = (b, m) = 1$ we have

$$\left(\frac{x_0}{y_0}\right)^n \equiv \frac{b}{a} \pmod{m}.$$

Let (x, y) be an arbitrary solution of (6). Then

$$\left(\frac{xy_0}{yx_0}\right)^n \equiv 1 \pmod{m}.$$

This shows that the number of congruence classes of solutions of (6) is at most equal to the number of solutions of the congruence equation $z^n \equiv 1 \pmod{m}$ in residue classes $z \pmod{m}$, i.e. $R(n, m)$.

We put $w(x) = ax^n$ for every positive integer x, and $w(x, y) = \max(ax^n, |by^n|)$ for every pair of positive integers x, y.

LEMMA 3: *Let* (x_1, y_1), (x_2, y_2) *be pairs satisfying both* (5) *and* (6) *such that* $(x_1, y_1) \equiv (x_2, y_2) \pmod{m}$ *and* $w(x_2) \geq w(x_1)$.

If $ab = 1$ *then* $w(x_2) \geq m^n/2C$ *and if* $ab \neq 1$ *then* $w(x_2) \geq m^n/C$.

PROOF: We have $ax_1^n - by_1^n = r_1$, $ax_2^n - by_2^n = r_2$, $|r_1| \leq C$, $|r_2| \leq C$. On solving b from this system of linear equations, we obtain

$$b = \frac{r_2x_1^n - r_1x_2^n}{x_2^n y_1^n - x_1^n y_2^n}.$$

Since x_2y_1, x_1y_2 are positive integers with $|x_1y_2 - x_2y_1| \geq m$ we have $|x_2^n y_1^n - x_1^n y_2^n| \geq m^n$, hence

$$|r_2w(x_1) - r_1w(x_2)| \geq |ab| m^n.$$

For $b > 0$ we have $|r_2w(x_1) - r_1w(x_2)| \leq C(w(x_1) + w(x_2)) \leq 2Cw(x_2)$, hence

$$w(x_2) \geq \frac{ab}{2} \frac{m^n}{C}.$$

If $b < 0$ then both r_1 and r_2 are positive and we even have

$$|r_2 w(x_1) - r_1 w(x_2)| \leq C w(x_2),$$

hence

$$w(x_2) \geq |ab| \frac{m^n}{C}.$$

Since $ab \neq 1$ for $b < 0$, this proves our lemma. □

LEMMA 4: *If* (x, y) *is a solution of* (5), *then*

$$w(x, y) < C \text{ if } b < 0 \text{ and } w(x, y) < C^{n/(n-1)}/2 \text{ if } a = b = 1.$$

PROOF: The lemma is trivial if $b < 0$. If $a = b = 1$, we may assume that $x > y$. Then we have

$$C \geq x^n - y^n \geq x^n - (x-1)^n.$$

Hence it suffices to show that $x^n - (x-1)^n > 2^{1-1/n} x^{n-1}$ for all $x \geq 2$, $n \geq 3$. The function $f(z) = (z^n - (z-1)^n) z^{-n+1}$ has the derivative $(z^n - (z-1)^n - n(z-1)^{n-1}) z^{-n}$. For all $z > 1$ this derivative is positive, hence $f(z)$ is increasing. This implies that

$$(x^n - (x-1)^n) x^{-n+1} \geq (2^n - 1) 2^{-n+1}$$

for all $x \geq 2$, $n \geq 3$. But from this fact our lemma follows immediately, since

$$(2^n - 1) 2^{-n+1} = 2(1 - 2^{-n}) > 2 \exp(-(2^n - 1)^{-1}) > 2^{1-1/n}$$

for all $n \geq 3$. □

We see that theorem 3 is valid if $ab \leq 1$. We shall now prove theorem 1 and theorem 2 in this case.

LEMMA 5: *If* $ab \leq 1$, *then* (2) *has at most* $R(n, c)$ *solutions.*

PROOF: Since $(a, c) = (b, c) = 1$ by (8), it suffices to show that (2) has at most one solution in each congruence class mod c, i.e. that for any two distinct solutions (x_1, y_1), (x_2, y_2) of (2) we have $(x_1, y_1) \not\equiv (x_2, y_2)$ (mod c).

Suppose to the contrary that (2) has two congruent solutions mod c, (x_1, y_1), (x_2, y_2) say, ordered such that $w(x_1) \leq w(x_2)$. Then it follows from lemma 3, applying it with $m = C = c$, that $w(x_2) \geq c^{n-1}$ if $b < 0$ and $w(x_2) \geq c^{n-1}/2$ if $a = b = 1$. But this is contradictory to lemma 4 since $c^{n-1} \geq c$, $c^{n-1}/2 \geq c^{n/(n-1)}/2$ for all $c \geq 1$, $n \geq 3$. □

LEMMA 6: (i) *If* $b < 0$, *then* (3) *has at most* $R(n, d)$ *solutions for which* $|z| \leq d^{n/2-1}$.

(ii) *If* $a = b = 1$, *then* (3) *has at most* $R(n, d)$ *solutions for which*

$$|z| \leq d^{(n^2-3n+1)/(2n-1)}.$$

PROOF: By (8) we have $(a, d) = (b, d) = 1$, hence it suffices to show that (3) has at most one solution in each congruence class mod d, i.e. that for any two distinct solutions (x_1, y_1, z_1), (x_2, y_2, z_2) of (3) satisfying the conditions imposed on z in lemma 6, we have $(x_1, y_1) \not\equiv (x_2, y_2) \pmod{d}$.

Just as in the proof of lemma 5 we suppose that there is a congruence class mod d containing at least two solutions, (x_1, y_1, z_1), (x_2, y_2, z_2) say, ordered such that $w(x_2) \geq w(x_1)$. We apply lemma 3 with $C = d^{n/2}$ if $b < 0$, $C = d^{n(n-1)/(2n-1)}$ if $a = b = 1$ and $m = d$. Then we have $w(x_2) \geq d^{n/2}$ if $b < 0$ and $w(x_2) \geq d^{n^2/(2n-1)}/2$ if $a = b = 1$. But this contradicts lemma 4 for $d \geq 1$, $n \geq 3$. □

Note that lemma 6 proves theorem 2 when $ab \leq 1$, since $2n/5 - 1 \leq n/2 - 1$ and $2n/5 - 1 \leq (n^2 - 3n + 1)/(2n - 1)$ for all $n \geq 3$. Thus we proved theorems 1, 2 and 3 for $ab \leq 1$, so we may assume that $ab \geq 2$.

LEMMA 7: *Let* β, f *be constants,* $\beta > 1$, $f \geq 1$. *Put* $\nu = n^{-1}$, $\kappa = (n-1)/2$.

(i) *If* (x, y) *is a solution of* (5) *for which* $w(x) \geq \beta C$, *then*

$$\left|1 - \left(\frac{b}{a}\right)^{\nu} \frac{y}{x}\right| < \frac{C(\beta/(\beta-1))^{\kappa\nu}}{nw(x)}. \tag{9}$$

(ii) *If* (x_1, y_1), (x_2, y_2) *are two solutions of* (5) *with* $|x_1y_2 - x_2y_1| \geq f$, $w(x_2) \geq w(x_1) \geq \beta C$, *then*

$$w(x_2) \geq 2\left(\frac{nf}{2C}\right)^n \left(\frac{\beta-1}{\beta}\right)^{\kappa} w(x_1)^{n-1}. \tag{10}$$

PROOF: (i) We have

$$|a^\nu x - b^\nu y| = \frac{|ax^n - by^n|}{(ax^n)^{(n-1)\nu} + (ax^n)^{(n-2)\nu}(by^n)^\nu + \ldots + (by^n)^{(n-1)\nu}}.$$

Using the inequality of the arithmetic and the geometric mean, it follows that

$$|a^\nu x - b^\nu y| < \frac{C}{n(ax^n)^{\kappa\nu}(by^n)^{\kappa\nu}},$$

hence

$$\left|1 - \left(\frac{b}{a}\right)^\nu \frac{y}{x}\right| < \frac{C}{n(ax^n)^{(n+1)\nu/2}(by^n)^{\kappa\nu}}.$$

Since $ax^n/by^n \leq \beta/(\beta - 1)$ this implies that

$$\left|1 - \left(\frac{b}{a}\right)^\nu \frac{y}{x}\right| < \frac{C(\beta/(\beta-1))^{\kappa\nu}}{nw(x)}.$$

(ii) We have by (i)

$$\begin{aligned}\frac{f}{w(x_1)^\nu w(x_2)^\nu} &\leq \frac{|x_1y_2 - x_2y_1|}{a^{2\nu}x_1x_2} = a^{-2\nu}\left|\frac{y_1}{x_1} - \frac{y_2}{x_2}\right| \\ &\leq a^{-2\nu}\left(\frac{a}{b}\right)^\nu\left(\left|1 - \left(\frac{b}{a}\right)^\nu \frac{y_1}{x_1}\right| + \left|1 - \left(\frac{b}{a}\right)^\nu \frac{y_2}{x_2}\right|\right) \\ &\leq (ab)^{-\nu}\nu C(\beta/(\beta-1))^{\kappa\nu}(w(x_1)^{-1} + w(x_2)^{-1}) \\ &\leq 2^{1-\nu}\nu C(\beta/(\beta-1))^{\kappa\nu}w(x_1)^{-1}\end{aligned}$$

by $ab \geq 2$. Hence

$$w(x_2) \geq 2\left(\frac{nf}{2C}\right)^n\left(\frac{\beta-1}{\beta}\right)^\kappa w(x_1)^{n-1}. \qquad \square$$

§3. Proof of Theorem 3

In this section we shall use the same notations as in §2. Thus a, b, n, C are constants with the same meaning as in (5) and in particular $n \geq 3$, $C \geq 1$. Further we shall assume that $ab \geq 2$ which is no restriction by lemma 4.

In fact we shall prove slightly more than theorem 3. Put

$$T_n = n\prod_{p|n} p^{1/(p-1)},\ \mu_3 = 2^5 T_3^8,$$
$$\mu_n = \max((2^{3/2}T_n^{n/2+1})^{1/(n-3)}, (4T_n^n)^{1/(n-2)}) \text{ for } n \geq 4,$$
$$\alpha_3 = 11, \alpha_n = \max((2n-2)/(n-2), (3n/2-1)/(n-3)) \text{ for } n \geq 4.$$

We shall show that the number of solutions of (5) for which

$$w(x,y) \geq \mu_n C^{\alpha_n} \tag{11}$$

is at most 3 if $n = 3$ and at most 1 if $n \geq 4$. This implies theorem 3. For if $n \leq 7$ we have $\mu_n \leq M_n$, $\alpha_n \leq A_n$. If $n \geq 8$ we may assume that (5) has at most one solution for which $w(x,y) \geq \mu_d C^{\alpha_d}$ where d is the smallest divisor of n with $d \geq 7$. Then d is a prime or $d \in \{8, 9, 10, 12, 15, 25\}$. For $n \geq 7$ we have $\mu_n = (4T_n^n)^{1/(n-2)}$, since $n/(n-2) \geq (n/2+1)/(n-3)$ and $2/(n-2) \geq 3/2(n-3)$. If d is a prime with $d \geq 7$ then

$$\mu_d/d = (4d^{3+1/(d-1)})^{1/(d-2)}.$$

This function is decreasing for $d \geq 7$, hence $\mu_d/d \leq \mu_7/7 < 8.4$. For all other values of d given above it is easy to check that also $\mu_d/d < 8.4$. Hence

$$\mu_d < 8.4d \leq 8.4n = M_n$$

for all $n \geq 8$. For all $n \geq 8$ we have also

$$\alpha_d = (2d-2)/(d-2) \leq \alpha_7 = 2.4 = A_n.$$

It is clear that this implies theorem 3.

The following lemma is fundamental in the proof of theorem 3. It is due to Siegel [6]. Our proof is simpler than his.

LEMMA 8: *Let* $r \in \mathbb{N}$. *Put*

$$q_r = (n^r, r!),\ s_r = \binom{2r}{r} q_r n^r,\ t_r = q_r n^r \prod_{m=1}^{r} (1 - \nu m^{-1}),$$
$$G_r(x) = q_r n^r \sum_{m=0}^{r} \binom{r+\nu}{m}\binom{r-\nu}{r-m}(1-x)^m,$$
$$H_r(x) = q_r n^r \sum_{m=0}^{r} \binom{r-\nu}{m}\binom{r+\nu}{r-m}(1-x)^m.$$

Then the polynomials $G_r(x), H_r(x)$ have the following properties:

(i) *$G_r(x), H_r(x)$ have integral coefficients,*

(ii) $0 < G_r(x) < s_r$ *for* $x \in (0, 1)$, (12)

(iii) $0 < G_r(x) - (1-x)^v H_r(x) < t_r x^{2r+1}$ *for* $x \in (0, 1)$, (13)

(iv) $G_{r+1}(x)H_r(x) \neq G_r(x)H_{r+1}(x)$ *for* $x \in (0, 1)$. (14)

PROOF: The hypergeometric series $F(\alpha, \beta, \gamma, x)$ is defined by

$$F(\alpha, \beta, \gamma, x) = 1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1 \cdot 2 \cdot \gamma(\gamma+1)} x^2 + \ldots \quad (\alpha, \beta, \gamma \in \mathbb{C})$$

where the series truncates after the last term of which the coefficient has non-zero numerator. α, β, γ should be such that the coefficients in the series do not have a denominator which is equal to 0. We have

$$x(x-1)y'' + ((1 + \alpha + \beta)x - \gamma)y' + \alpha\beta y = 0 \tag{15}$$

if $y(x) = F(\alpha, \beta, \gamma, x)$. By computing the constant terms and the quotients of two consecutive coefficients of $G_r(1-x)$, $H_r(1-x)$ respectively, one can verify easily that

$$\begin{aligned} G_r(x) &= t_r F(-v-r, -r, 1-v, 1-x), \\ H_r(x) &= u_r F(v-r, -r, 1+v, 1-x), \end{aligned} \tag{16}$$

where

$$u_r = q_r n^r \prod_{m=1}^{r} (1 + vm^{-1}).$$

First of all we prove (i). It suffices to show that

$$Q(m) := q_r n^r \binom{r+v}{m} \binom{r-v}{r-m}$$

is a p-adic integer for all primes p and for all m with $0 \leq m \leq r$. Note that

$$Q(m) = \frac{q_r}{r!} \binom{r}{m} d(m)$$

for some integer $d(m)$, hence $Q(m)$ is a p-adic integer for all primes p dividing n. For the primes p not dividing n, $\binom{r+v}{m}$ and $\binom{r-v}{r-m}$ are p-adic integers, so $Q(m)$ is also p-adically integral for these primes p.

By equating the coefficients of x^r in the identity in power series $(1+x)^{2r} = (1+x)^{r+v}(1+x)^{r-v}$ we obtain

$$\binom{2r}{r} = \sum_{m=0}^{r} \binom{r+v}{m}\binom{r-v}{r-m},$$

hence

$$G_r(0) = H_r(0) = s_r. \tag{17}$$

This implies (ii), for by the fact that $G_r(1-x)$ has positive coefficients, we have

$$0 < G_r(x) < G_r(0)$$

for all $x \in (0,1)$.

To prove (iii) and (iv), we infer from (15) and (16) that the three functions $G_r(x)$, $(1-x)^v H_r(x)$ and $x^{2r+1}F_r(x)$, where $F_r(x) = F(-v+r+1, r+1, 2r+2, x)$, satisfy the differential equation

$$x(x-1)y'' + ((1-v-2r)x + 2r)y' + r(v+r)y = 0.$$

This implies that $G_r(x)$, $(1-x)^v H_r(x)$ and $x^{2r+1}F_r(x)$ are linearly dependent, hence there are constants ρ_r, σ_r, τ_r, not all equal to 0, such that

$$\rho_r G_r(x) + \sigma_r(1-x)^v H_r(x) + \tau_r x^{2r+1}F_r(x) \equiv 0.$$

It follows from (17), by taking $x = 0$, that $\rho_r + \sigma_r = 0$. Since $F_r(x)$ is not identically equal to 0, the coefficients ρ_r, σ_r are both non-zero. Hence there is a constant ω_r such that

$$G_r(x) - (1-x)^v H_r(x) = \omega_r x^{2r+1}F_r(x). \tag{18}$$

Put $U_r(x) = G_r(x) - (1-x)^v H_r(x)$. Then $U_r(1) = G_r(1) = t_r > 0$, hence $U_r(x)$ assumes a positive value for some $x \in (0,1)$. But since $F_r(x)$ has positive coefficients and converges for all $x \in (0,1)$, we have $\omega_r > 0$. Hence, by (18), $U_r(x)x^{-2r-1}$ increases monotonically on $(0,1)$. It follows that

$$U_r(x)x^{-2r-1} < U_r(1) = t_r$$

for all $x \in (0,1)$ which is equivalent to (iii).

To prove (iv) we eliminate $(1-x)^v$ from

$$G_r(x) - (1 - x)^v H_r(x) = \omega_r x^{2r+1} F_r(x),$$
$$G_{r+1}(x) - (1 - x)^v H_{r+1}(x) = \omega_{r+1} x^{2r+3} F_{r+1}(x).$$

It follows that

$$G_r(x)H_{r+1}(x) - G_{r+1}(x)H_r(x) = C_r(x)x^{2r+1} \tag{19}$$

for a power series $C_r(x)$. But the degree of the left-hand side of (19) is at most $2r + 1$, hence $C_r(x)$ is a constant. Since $G_r(1)H_{r+1}(1) \neq G_{r+1}(1)H_r(1)$ this constant is nonzero. This implies (iv). □

We make the following assumptions.

$$\begin{cases} \text{(i) } \textit{If } n = 3 \textit{ then } (5) \textit{ has at least four solutions satisfying } (11). \\ \text{(ii) } \textit{If } n \geq 4 \textit{ then } (5) \textit{ has at least two solutions satisfying } (11). \end{cases} \tag{20}$$

We shall show that (20), (i) and (20), (ii) are impossible.

LEMMA 9: *Let* $(x_1, y_1), (x_2, y_2)$ *be distinct solutions of* (5), *satisfying* (11) *and ordered such that* $w(x_1, y_1) \leq w(x_2, y_2)$. *Then* $w(x_1) \leq w(x_2)$.

PROOF: Suppose that $w(x_2) < w(x_1)$. Then we have

$$w(x_2) \geq w(x_2, y_2) - C \geq w(x_2, y_2) - C^{\alpha_n} \geq (1 - \mu_n^{-1})w(x_2, y_2) \geq (\mu_n - 1)C.$$

Applying (10) with $\beta = \mu_n - 1$, $f = 1$, we obtain, by $\mu_n \geq 3$,

$$\begin{aligned} w(x_2, y_2) &\geq w(x_1, y_1) \geq w(x_1) \geq 2\left(\frac{n}{2C}\right)^n \left(\frac{\mu_n - 2}{\mu_n - 1}\right)^\kappa w(x_2)^{n-1} \\ &\geq 2\left(\frac{n}{2C}\right)^n \left(\frac{\mu_n - 2}{\mu_n - 1}\right)^\kappa \left(\frac{\mu_n - 1}{\mu_n}\right)^{n-1} w(x_2, y_2)^{n-1} \\ &\geq 2\left(\frac{n}{2C}\right)^n 2^{-\kappa}(2/3)^{n-1} w(x_2, y_2)^{n-1} \\ &= n^n(3\sqrt{2})^{-n+1} C^{-n} w(x_2, y_2)^{n-1} \\ &\geq C^{-n} w(x_2, y_2)^{n-1} \end{aligned}$$

for all $n \geq 3$. Hence

$$w(x_2, y_2) \leq C^{n/(n-2)} < \mu_n C^{\alpha_n},$$

a contradiction. □

If $n \geq 4$, let (x_1, y_1), (x_2, y_2) be two solutions of (5) such that $w(x_2, y_2) \geq w(x_1, y_1) \geq \mu_n C^{\alpha_n}$, if $n = 3$ let (x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4) be four solutions of (5) such that $w(x_2, y_2) \geq w(x_4, y_4) \geq$ $\geq w(x_3, y_3) \geq w(x_1, y_1) \geq \mu_3 C^{\alpha_3}$. We may assume that $w(x_1, y_1) = w(x_1)$. By lemma 9 we have $w(x_2) \geq w(x_1)$ if $n \geq 4$ and $w(x_2) \geq w(x_4) \geq$ $\geq w(x_3) \geq w(x_1)$ if $n = 3$. We apply (10) thrice if $n = 3$ and once if $n \geq 4$. We take $f = 1$ and since $w(x_1) \geq \mu_n C^{\alpha_n}$ we may take $\beta = \mu_n$. Put

$$\sigma_n = (\mu_n/(\mu_n - 1))^{\kappa v}, \quad w_1 = w(x_1), w_2 = w(x_2).$$

Then

$$\begin{cases} w_2 \geq 2^7 \cdot (3/2\sigma_3 C)^{21} w_1^8 & \text{if } n = 3, \\ w_2 \geq 2 \cdot (n/2\sigma_n C)^n \quad w_1^{n-1} & \text{if } n \geq 4. \end{cases} \tag{21}$$

Put $z = 1 - by_1^n/ax_1^n$, $V_r = x_2^{-1} y_2 G_r(z) - x_1^{-1} y_1 H_r(z)$.

LEMMA 10: *If* $V_r \neq 0$, *then*

$$1 < (w_1 w_2/2)^v w_1^r (s_r \sigma_n C/n w_2 + t_r (C/w_1)^{2r+1}). \tag{22}$$

PROOF: Since

$$V_r = \left(\frac{a}{b}\right)^v \left(\left(\left(\frac{b}{a}\right)^v \frac{y_2}{x_2} - 1 \right) G_r(z) + G_r(z) - (1-z)^v H_r(z) \right),$$

we have by (9), (12), (13) and the fact that $z \leq C/w_1$,

$$0 < |V_r| < (a/b)^v (s_r \cdot \sigma_n C/n w_2 + t_r (C/w_1)^{2r+1}).$$

Now V_r is a fraction with denominator dividing

$$x_1 x_2 w_1^r = a^{-2v} (w_1 w_2)^v w_1^r,$$

hence

$$1 < a^{-2v} (w_1 w_2)^v w_1^r (a/b)^v (s_r \sigma_n C/n w_2 + t_r (C/w_1)^{2r+1}).$$

Since $ab \geq 2$, this proves lemma 10. □

We shall show that it is possible to choose r in such a way that

$$V_r \neq 0,$$

$$(w_1 w_2/2)^v w_1^r s_r \cdot \sigma_n C/n w_2 \leq v, \tag{23}$$

$$(w_1 w_2/2)^v w_1^r t_r (C/w_1)^{2r+1} \leq 1 - v, \tag{24}$$

which gives the desired contradiction with (22). Note that (23) is equivalent to

$$2^{\nu}\sigma_n^{-1}C^{-1}w_1^{-\nu}w_2^{1-\nu} \geq s_r w_1^r.$$

Let l be the integer defined by

$$s_l w_1^l \leq 2^{\nu}\sigma_n^{-1}C^{-1}w_1^{-\nu}w_2^{1-\nu} < s_{l+1}w_1^{l+1}. \tag{25}$$

l is well-defined since the sequence $s_k w_1^k$ increases monotonically to infinity as k tends to infinity. It is clear that (23) is equivalent to $r \leq l$.

We choose $r = l$ if $V_r \neq 0$ and $r = l - 1$ otherwise. We shall prove that $l \geq 1$ if $n \geq 4$, that $l \geq 3$ if $n = 3$ and that $V_1 \neq 0$ for $n \geq 4$. This implies that r is a positive integer with $r \geq 2$ if $n = 3$ and $r \leq l$. Hence (23) holds and by (14), we have $V_r \neq 0$.

LEMMA 11: *$l \geq 1$ if $n \geq 4$ and $l \geq 3$ if $n = 3$.*

PROOF: It suffices to show that

$$s_1 w_1 \leq 2^{\nu}\sigma_n^{-1}C^{-1}w_1^{-\nu}w_2^{1-\nu} \text{ if } n \geq 4 \text{ and}$$
$$s_3 w_1^3 \geq 2^{1/3}\sigma_3^{-1}C^{-1}w_1^{-1/3}w_2^{2/3} \text{ if } n = 3.$$

Since $s_1 = 2n$ and $s_3 = 1620$, this is equivalent to

$$w_2 \geq (2^{1-\nu}\sigma_n \cdot nC)^{n/(n-1)}w_1^{(n+1)/(n-1)} \text{ if } n \geq 4 \text{ and}$$
$$w_2 \geq (2^{-1/3}1620\,\sigma_3 C)^{3/2}w_1^5 \text{ if } n = 3.$$

It follows from (21) that it suffices to prove that

$$2\left(\frac{n}{2\sigma_n C}\right)^n w_1^{n-1} \geq (2^{1-\nu}\sigma_n nC)^{n/(n-1)}w_1^{(n+1)/(n-1)} \text{ if } n \geq 4 \text{ and}$$
$$2^7\left(\frac{3}{2\sigma_3 C}\right)^{21} w_1^8 \geq (2^{-1/3} \cdot 1620\,\sigma_3 C)^{3/2}w_1^5 \text{ if } n = 3.$$

This is equivalent to

$$w_1 \geq (2^{n-1}\sigma_n^n n^{-(n-2)}C^n)^{1/(n-3)} \text{ if } n \geq 4 \text{ and}$$
$$w_1 \geq (1620)^{1/2}2^{-5/2}(2/3)^7\sigma_3^{15/2}C^{15/2} \text{ if } n = 3.$$

Since $2(\mu_n/(\mu_n - 1))^{1/2} < 3$ for $n \geq 4$, whence

$$2^{n-1}\sigma_n^n n^{-(n-2)} < 3^{n-1}n^{-(n-2)} < 1 < \mu_n,$$

whereas

$$(1620)^{1/2}2^{-5/2}(2/3)^7\sigma_3^{15/2} < \mu_3,$$
$$n/(n-3) < \alpha_n \text{ if } n \geq 4,\ 15/2 < \alpha_3,$$

this follows immediately from $w_1 \geq \mu_n C^{\alpha_n}$.

LEMMA 12: *$V_1 \neq 0$ for $n \geq 4$.*

PROOF: Since $\mu_n > n$ for $n \geq 4$, we may assume that $z < v$. Suppose $V_1 = 0$, i.e.

$$x_2^{-1}y_2G_1(z) = x_1^{-1}y_1H_1(z).$$

Put $h = ax_1^n - by_1^n$. Since $G_1(z) = 2n - (n+1)z$, $H_1(z) = 2n - (n-1)z$, we have

$$x_2^{-1}y_2(2nw_1 - (n+1)h) = x_1^{-1}y_1(2nw_1 - (n-1)h).$$

Since $(x_2, y_2) = 1$ and since $G_1(z) > 0$ there is a positive integer d such that

$$dx_2 = x_1(2nw_1 - (n+1)h),\ dy_2 = y_1(2nw_1 - (n-1)h).$$

This implies

$$d^n ax_2^n = w_1(2nw_1 - (n+1)h)^n,\ d^n by_2^n = (w_1 - h)(2nw_1 - (n-1)h)^n,$$

hence

$$d^n(ax_2^n - by_2^n) = w_1^{n+1}(G_1(z)^n - (1-z)H_1(z)^n)$$

and therefore

$$G_1(z)^n - (1-z)H_1(z)^n \leq \frac{d^nC}{w_1^{n+1}}. \tag{26}$$

We now estimate d^n. Define u, h_0, w_0 such that $u = (h, w_1)$, $h = uh_0$, $w_1 = uw_0$. Then d^n divides

$$u^{n+1}(w_0(2nw_0 - (n+1)h_0)^n, (w_0 - h_0)(2nw_0 - (n-1)h_0)^n).$$

Using the facts that $(w_0, h_0) = 1$ and that (a_1, a_2, a_3, a_4) divides $(a_1, a_3)(a_1, a_4)(a_2, a_3)(a_2, a_4)$ for all positive integers a_1, a_2, a_3, a_4 we see that d^n divides

$$u^{n+1}(w_0, w_0 - h_0)(w_0, (2nw_0 - (n-1)h_0)^n) \times$$
$$\times (w_0 - h_0, (2nw_0 - (n+1)h_0)^n)(2nw_0 - (n+1)h_0, 2nw_0 - (n-1)h_0)^n =$$
$$= u^{n+1}(w_0, (n-1)^n)(w_0 - h_0, (n-1)^n)(2nw_0 - (n+1)h_0, 2h_0)^n.$$

Hence d^n divides $u^{n+1}(2(n-1))^n h_0^n$. Since $h = uh_0$, we conclude that d^n divides $(2(n-1))^n h^{n+1}$. Substituting this into (26), we obtain

$$G_1(z)^n - (1-z)H_1(z)^n \leq (2(n-1))^n C z^{n+1}. \tag{27}$$

In the proof of lemma 8 we saw that

$$U_1(z) = G_1(z) - (1-z)^\nu H_1(z) = z^3 K_1(z)$$

for a power series $K_1(z)$ with positive coefficients. We find, by expanding $U_1(z)$ in a Taylor series, that for $n \geq 4$

$$K_1(z) \geq K_1(0) = (n^2 - 1)/6n^2 \geq 5/32.$$

Furthermore we have, by $0 < z < \nu$,

$$(1-z)^{1-\nu} \geq 1 - z > 1 - \nu,\ H_1(z) > 2(n-1).$$

Hence

$$\begin{aligned} G_1(z)^n - (1-z)H_1(z)^n &= ((1-z)^\nu H_1(z) + z^3 K_1(z))^n - (1-z)H_1(z)^n \\ &\geq n(1-z)^{1-\nu} H_1(z)^{n-1} z^3 K_1(z) \\ &> \tfrac{5}{64} \cdot (2(n-1))^n z^3. \end{aligned}$$

A combination with (27) yields that

$$C z^{n-2} > 5/64,$$

hence

$$w_1^{n-2} < 64 C^{n-1}/5 < \mu_n^{n-2} C^{\alpha_n (n-2)}$$

for $n \geq 4$. This contradiction proves lemma 12. □

As we have noticed before, the proof of theorem 3 is complete if we

have shown that (24) holds. Therefore we need

LEMMA 13: $\sigma_n s_{r+2}(t_r/(1-v))^{n-1} < 4^{r+1} T_n^{nr+2}$.

PROOF: First of all, we have

$$\mu_n \geq (4T_n^n)^{1/(n-2)} > 8$$

hence

$$\sigma_n < \left(\frac{8}{7}\right)^{\kappa v} < \frac{8}{7}.$$

If $r = 1$ we have

$$\sigma_n s_3(t_1/(1-v))^{n-1} = \sigma_n n^3 (n,6)\binom{6}{3} n^{n-1} < \frac{8}{7}\cdot 20 n^{n+2} \prod_{p|n} p^{2/(p-1)} =$$

$$= \frac{8}{7}\cdot\frac{5}{4}\prod_{p|n} p^{-n/(p-1)}\cdot 4^2 T_n^{n+2} < 4^2 T_n^{n+2}.$$

If $r \geq 2$, we use the fact that $(n^r, r!) = \prod_{p|n} p^{s_p}$, where

$$s_p = \sum_{j=1}^{\infty}\left[\frac{r}{p^j}\right] < \frac{r}{p-1}.$$

Hence

$$s_r < \binom{2r}{r} T_n^r,\ t_r < \prod_{m=1}^{r}\left(1-\frac{v}{m}\right) T_n^r \leq (1-v)\left(1-\frac{v}{2}\right) T_n^r.$$

We use also that $\binom{2k}{k} = 4^k \prod_{h=1}^{k}\left(1-\frac{1}{2h}\right)$ for all positive integers k. This gives

$$\sigma_n s_{r+2}(t_r/(1-v))^{n-1} < \frac{8}{7}\binom{2r+4}{r+2} T_n^{r+2}\left(1-\frac{v}{2}\right)^{n-1} T_n^{r(n-1)} =$$

$$= \frac{8}{7}\left(1-\frac{v}{2}\right)^{n-1} 4^{r+2} T_n^{nr+2} \prod_{h=1}^{r+2}\left(1-\frac{1}{2h}\right) \leq$$

$$\leq \frac{32}{7}\left(1-\frac{v}{2}\right)^{n-1} 4^{r+1} T_n^{nr+2} \prod_{h=1}^{4}\left(1-\frac{1}{2h}\right) =$$

$$= \frac{5}{4}\left(1-\frac{1}{2n}\right)^{n-1} 4^{r+1} T_n^{nr+2} < 4^{r+1} T_n^{nr+2},$$

since $\left(1-\frac{1}{2n}\right)^n < \exp\left(-\frac{n-1}{2n}\right) \le \exp\left(-\frac{1}{3}\right) < \frac{4}{5}$ for all $n \ge 3$.

Now we prove (24). By (25) and $l \le r+1$, we have

$$(w_1 w_2)^v < (2^{-v}\sigma_n C s_{l+1} w_1^{l+2})^{1/(n-1)} \le (2^{-v}\sigma_n C s_{r+2} w_1^{r+3})^{1/(n-1)}.$$

Using this inequality and lemma 13, we obtain

$$(w_1 w_2/2)^v w_1^r t_r (C/w_1)^{2r+1} < (\tfrac{1}{2}\sigma_n s_{r+2} t_r^{n-1} C^{(2n-2)r+n} w_1^{-(n-2)r+4-n})^{1/(n-1)} <$$
$$< R := (1-v)(\tfrac{1}{2}\cdot 4^{r+1} T_n^{nr+2} C^{(2n-2)r+n} w_1^{-(n-2)r+4-n})^{1/(n-1)}.$$

If $n \ge 4$, R is equal to

$$(1-v)(4T_n^n C^{2n-2} w_1^{-(n-2)})^{(r-1)/(n-1)} (2^{3/2} T_n^{n/2+1} C^{3n/2-1} w_1^{-(n-3)})^{2/(n-1)},$$

while if $n = 3$, R equals

$$(1-1/3)(4T_3^3 C^4 w_1^{-1})^{(r-2)/2} (2^5 T_3^8 C^{11} w_1^{-1})^{1/2}.$$

Since $r \ge 1$ if $n \ge 4$, $r \ge 2$ if $n = 3$ and $w_1 \ge \mu_n C^{\alpha_n}$, R does not exceed $1 - v$ for any $n \ge 3$. This shows (24). □

§4. Proof of Theorem 1

Let a, b, c, n be constants with the same meaning as in (2), i.e. we have $a, b, c, n \in \mathbb{Z}$, $a > 0$, $b \ne 0$, $c > 0$, $n \ge 3$. Further by lemma 1 and lemma 5 we may assume that $ab \ge 2$, $(a, c) = (b, c) = 1$. We may also assume that $a/b \ne (u/v)^n$ for all $u, v \in \mathbb{N}$ for otherwise a and b would be n-th powers which could be absorbed by x, y respectively. We may also restrict ourselves to the case $c \ge 2$. For we have, by combining some old results:

LEMMA 14: *If* $c = 1$, *then* (2) *has at most* 2 *solutions.*

Suppose $c = 1$. By considering units in the cubic field $\mathbb{Q}((a/b)^{1/3})$, Nagel [5] showed that (2) has at most one solution if $n = 3$. Ljunggren [4] showed by an investigation of the units of the field $\mathbb{Q}((a/b)^{1/4})$, that (2) has at most two solutions if $n = 4$. Finally, Domar [2] showed lemma 14 for $n \ge 5$ by refining some estimates of Siegel in [6]. Note that for $n \ge 5$, lemma 14 is an easy consequence of theorem 3. For by applying this theorem with $C = 1$ and using that $2^n < M_n < 3^n$ if

$n \in \{5, 6\}$ while $1 < M_n < 2^n$ if $n \geq 7$, we see that (2) has at most one solution with $\max(x, y) \geq 3$ if $n \in \{5, 6\}$ and $\max(x, y) \geq 2$ if $n \geq 7$. It follows immediately that (2) has at most two solutions if $n \geq 7$. If $n \in \{5, 6\}$ at most one of the pairs (1, 1), (2, 1), (1, 2) can be a solution of (2) since no system consisting of two of the linear equations $a - b = \pm 1$, $2^n a - b = \pm 1$, $a - 2^n b = \pm 1$ has integral solutions a, b. This shows that lemma 14 holds for $n \in \{5, 6\}$. □

Now we shall prove theorem 1 for $c \geq 2$. It follows from lemma 2 and lemma 3, by putting $C = m = c$, that (2) has at most $R(n, c)$ solutions for which $w(x) < c^{n-1}$. If $n = 3$ each congruence class mod c contains at most two solutions for which $w(x) < 27c^4/8$, whence (2) has at most $2R(3, c)$ solutions for which $w(x) < 27c^4/8$. For suppose (x_1, y_1), (x_2, y_2), (x_3, y_3) are solutions of (2) in the same congruence class, ordered such that $w(x_1) \leq w(x_2) \leq w(x_3)$. Then by lemma 3, with $m = C = c$, we have $w(x_2) \geq c^2$ and by (10) with $f = C = c$, $\beta = 2$, we have

$$w(x_3) \geq 2\left(\frac{3}{2}\right)^3 \cdot \frac{1}{2} w(x_2)^2 \geq 27c^4/8,$$

a contradiction.

It follows from theorem 3 that the number of solutions of (2) for which $w(x) \geq M_n c^{A_n}$ is at most 1 if $n \geq 4$ and at most 3 if $n = 3$. Hence we have only to estimate the number of solutions of (2) with $c^{n-1} \leq w(x) < M_n c^{A_n}$ if $n \geq 4$ and $27c^4/8 \leq w(x) < M_3 c^{A_3}$ if $n = 3$.

If $c^{n-1} \geq M_n c^{A_n}$ then (2) has at most $R(n, c) + 1$ solutions. This is the case if $n = 5$, $c \geq 220$, or $n = 6$, $c \geq 9$, or $n \geq 7$, $c \geq 3$, since clearly $3^{n-1} \geq 8 \cdot 4n \times 3^{2 \cdot 4}$ for all $n \geq 8$. If $n \geq 7$, $c = 2$, then $M_n c^{A_n} < 3^n$. Hence, by theorem 3, (2) has at most one solution with $\max(x, y) \geq 3$ in this case. But at most one of the pairs (1, 1), (2, 1), (1, 2) can be a solution of (2), since no system consisting of two of the linear equations $a - b = \pm 2$, $2^n a - b = \pm 2$, $a - 2^n b = \pm 2$ has integral solutions a, b. Hence (2) has at most 2 solutions if $c = 2$, $n \geq 7$ and this proves theorem 1 completely for $n \geq 7$.

In the remaining cases, i.e. $n \in \{5, 6\}$, $c^{n-1} < M_n c^{A_n}$ and $n \in \{3, 4\}$, we have to show that (2) has at most one solution if $n \in \{5, 6\}$ and at most two solutions if $n = 4$ for which $c^{n-1} \leq w(x) < M_n c^{A_n}$, and at most three solutions for which $27c^4/8 \leq w(x) < M_3 c^{A_3}$ if $n = 3$. We use the following lemma which will also be used in the proof of theorem 2.

LEMMA 15: *Put* $R(n) = (2^{3/2}(2^{-3/2}n)^n)^{1/(n-2)}$. *Let* C *be the constant appearing in* (5) *and let* A, B *be constants such that*

$$B > A > \max(2C, R(n)^{-1}C^{n/(n-2)}).$$

Let r be the smallest positive integer not smaller than

$$S = S(A, B, C) := \log\left(\frac{\log(R(n)C^{-n/(n-2)}B)}{\log(R(n)C^{-n/(n-2)}A)}\right)\Big/\log(n-1).$$

Then (5) *has at most r solutions for which $A \leq w(x) < B$.*

PROOF: Let $(x_1, y_1), (x_2, y_2), \ldots, (x_r, y_r)$ be solutions of (5) such that $A \leq w(x_1) \leq w(x_2) \leq \ldots \leq w(x_r) < B$. We apply (10) with $\beta = 2, f = 1$. If A is much larger than $2C$ we could have chosen a larger value for β but that does not improve our final results. For convenience, we put

$$T := R(n)C^{-n/(n-2)}.$$

Then we have for $i \in \{1, 2, \ldots, r-1\}$:

$$w(x_{i+1}) \geq 2 \cdot \left(\frac{n}{2C}\right)^n 2^{-\kappa} w(x_i)^{n-1} = T^{n-2} w(x_i)^{n-1},$$

hence

$$Tw(x_{i+1}) \geq (Tw(x_i))^{n-1}.$$

This implies that

$$TB > Tw(x_r) \geq (Tw(x_1))^{(n-1)^{r-1}} \geq (TA)^{(n-1)^{r-1}},$$

hence

$$(n-1)^{r-1} < \log TB/\log TA,$$

and therefore

$$r - 1 < \log(\log TB/\log TA)/\log(n-1),$$

which implies lemma 15.

We apply lemma 15 with $C = c$, $A = c^{n-1}$ if $n \in \{4, 5, 6\}$ but $A = 27c^4/8$ if $n = 3$, while $B = M_n c^{A_n}$. If $n \in \{4, 5, 6\}$ we have

$$S = \log\left(\frac{\log(R(n)M_n) + (A_n - n/(n-2))\log c}{\log R(n) + (n - 1 - n/(n-2))\log c}\right)\Big/\log(n-1).$$

If $n \in \{5, 6\}$ then $S < 1$, since $c \geq 2$ and

$$(n-1)(\log R(n) + (n-1-n/(n-2))\log c) \geq$$
$$\geq (n-1)\log R(n) + ((n-1)(n-1-n/(n-2)) - A_n + n/(n-2))\log 2 +$$
$$+ (A_n - n/(n-2)\log c) \geq \log(R(n)M_n + (A_n - n/(n-2))\log c\,.$$

If $n = 4$ then $S < 2$, since $R(n) = 2^{7/4}$, $M_n = 1449$, $n - 1 - n/(n-2) = 1$, $A_n - n/(n-2) = 3$, and

$$3^2(\log 2^{7/4} + \log c) > \log(2^{7/4} \times 1449) + 9\log >$$
$$> \log(2^{7/4} \times 1449) + 3\log c.$$

Finally, if $n = 3$ we have

$$S = \log\left(\frac{3\log(3/2) + \log 1.71 + 7\log 10 + 8\log c}{6\log(3/2) + \log c}\right)\Big/\log 2 < 3,$$

since $2^3 \times 6\log(3/2) > 3\log(3/2) + \log 1.71 + 7\log 10$. By lemma 15, this proves theorem 1 completely. □

§5. Proof of Theorem 2

Let a, b, d, n be constants with the same meaning as in (3), i.e. we have $a, b, d, n \in \mathbb{Z}$, $a > 0$, $b \neq 0$, $d > 0$, $n \geq 3$, $(a, d) = (b, d) = 1$. Further put $C_0 = d^{2n/5}$. By lemma 6 we may assume that $ab \geq 2$. We may also assume that (3) has solutions with $|z| \geq 2$ for otherwise we would have the same equation as (2), with d instead of c. Hence $\min(d^{2n/5-1}, d) \geq 2$, whence $\min(C_0^{2n/5-1}, C_0) \geq 2^{2n/5}$. This implies that $C_0 \geq 4$ for all $n \geq 3$.

LEMMA 16: *Define for every positive integer k:*

$$f(k) = R(n)^{(n-1)^{k-1}-1} C_0^{((n-1)^k + 2n-5)/2(n-2)}.$$

Then (3) *has at most $kR(n, d)$ solutions for which $|z| \leq d^{2n/5-1}$ and $w(x) < f(k)$.*

PROOF: Suppose (x_0, y_0, z_0), $(x_1, y_1, z_1), \ldots, (x_k, y_k, z_k)$ are solutions of (3) such that the pairs (x_0, y_0), $(x_1, y_1), \ldots, (x_k, y_k)$ are pairwise congruent mod d, that $|z_i| \leq d^{n/5-1}$ for $i \in \{0, 1, \ldots, k\}$ and ordered such that $w(x_0) \leq w(x_1) \leq \ldots \leq w(x_k)$. By lemma 3 with $C = C_0$, $m = d$, we have

$$w(x_1) \geq d^n/C_0 = C_0^{3/2} \geq 2C_0.$$

By (10) with $\beta = 2$, $f = d$, $C = C_0$, we have for $i \in \{1, 2, \ldots, k-1\}$:

$$w(x_{i+1}) \geq R(n)^{n-2}(d/C_0)^n w(x_i)^{n-1} = R(n)^{n-2} C_0^{5/2-n} w(x_i)^{n-1}.$$

Hence, similar as in the proof of lemma 15:

$$R(n)C_0^{(5/2-n)/(n-2)} w(x_k) \geq (R(n)C_0^{(5/2-n)/(n-2)} w(x_1))^{(n-1)^{k-1}}.$$

Therefore,

$$w(x_k) \geq R(n)^{(n-1)^{k-1}-1} C_0^{(5/2-n)((n-1)^{k-1}-1)/(n-2)} C_0^{3(n-1)^{k-1}/2} = f(k).$$

It follows that (3) has at most k congruent solutions mod d with $|z| \leq d^{2n/5-1}$, $w(x) < f(k)$, which proves the lemma. □

Put $k_n = 1$ if $n \geq 7$, $k_n = 2$ if $n \in \{4, 5, 6\}$, $k_n = 3$ if $n = 3$. By lemma 16 and theorem 3, it suffices to show that the number of solutions of (3) for which $|z| \leq C_0/d$ and $f(k_n) \leq w(x) < M_n C_0^{A_n}$ is at most 1 if $n \geq 8$, at most 2 if $n = 7$, 0 if $n \in \{5, 6\}$, at most 1 if $n = 4$ and at most 3 if $n = 3$. Therefore we shall apply lemma 15 with $C = C_0$, $A = f(k_n)$ and $B = M_n C_0^{A_n}$.

If $n \geq 7$ we have $A = f(1) = C_0^{3/2}$, hence

$$S = \log\left(\frac{\log(R(n)M_n) + (A_n - n/(n-2))\log C_0}{\log R(n) + (3/2 - n/(n-2))\log C_0}\right) \Big/ \log(n-1).$$

If $n \geq 8$, then $S < 1$, since

$$A_n - n/(n-2) < (n-1)(3/2 - n/(n-2)),$$
$$\log(R(n)M_n) < (n-1)\log R(n).$$

If $n = 7$, then $S < 2$, since

$$A_7 - 7/5 = 1 < 6^2(3/2 - 7/5) = 3.6, \log(R(7)M_7) < 6^2 \log R(7).$$

If $n \in \{4, 5, 6\}$ we have $A = f(2) = R(n)C_0^{n/2+1}$. If $n \in \{5, 6\}$ then

$$A = f(2) \geq R(n)C_0^{A_n + 1/4} \geq \sqrt{2}\, R(n) C_0^{A_n} \geq M_n C_0^{A_n} = B,$$

while if $n = 4$ we have

$$S = \log\left(\frac{(7/4)\log 2 + \log 1449 + 3\log C_0}{3 \times (7/4)\log 2 + \log C_0}\right) \Big/ \log 3$$

since $3^2 \times (7/4)\log 2 > (7/4)\log 2 + \log 1449$. Finally, if $n = 3$ we have $A = f(3) = (3/2)^9 C_0^{9/2}$, hence

$$S = \left(\frac{3\log(3/2) + \log 1.71 + 7\log 10 + 8\log C_0}{12\log(3/2) + (3/2)\log C_0} \right) \Big/ \log 2 < 3,$$

since $2^3 \times 12\log(3/2) > 3\log(3/2) + \log 1.71 + 7\log 10$. By lemma 15, this completes the proof of theorem 2. □

§6. Proof of Theorem 4

In this section ε will denote an arbitrary positive number, $\beta_1, \beta_2, \ldots$ will denote positive absolute constants and $\beta_1(\lambda_1, \lambda_2, \ldots, \lambda_s)$, $\beta_2(\lambda_1, \lambda_2, \ldots, \lambda_s), \ldots$ will denote positive constants depending on the parameters $\lambda_1, \lambda_2, \ldots, \lambda_s$. As was announced in §1, we shall first prove corollary 3, that is that the equation

$$ax^n - by^n = c \quad (a, b, c, n \text{ integers with } abc \neq 0, n \geq 3) \tag{1}$$

has at most $\beta_1(\varepsilon)|c|^\varepsilon$ solutions in integers x, y.

Firstly, we notice that it is sufficient to show that (1) has at most $\beta_2(\varepsilon)|c|^\varepsilon$ solutions in integers x, y with $(x, y) = 1$. For suppose this has been proved. Let (x_0, y_0) be a solutions of (1) with $(x_0, y_0) = d$. Then $(x_0/d, y_0/d)$ is a solution of

$$ax^n - by^n = c/d^n$$

in integers x, y with $(x, y) = 1$. Hence there are at most $\beta_2(\varepsilon/2)|c|^{\varepsilon/2}$ of such pairs (x_0, y_0) and this implies corollary 3, since the number of divisors of c, whence the number of possibilities for d, does not exceed $\beta_3(\varepsilon)|c|^{\varepsilon/2}$.

It is now clear that it suffices to show that the number of solutions of

$$|ax^n - by^n| = c \quad (a, b, c, n \text{ integers with } a \geq 0, b \neq 0, c > 0, n \geq 3) \tag{2}$$

in integers x, y with $x > 0$, $y > 0$, $(x, y) = 1$ does not exceed $\beta_4(\varepsilon)c^\varepsilon$. By corollary 1, (2) has at most $2n^{\omega(c)} + 6$ solutions. If n is large compared with c this is not sharp enough to prove corollary 3. Therefore we shall give an upper bound for the number of solutions of (2) which is better for large values of n.

By theorem 3, the number of solutions of (2) for which $\max(x, y) \geq (M_n c^{A_n})^{1/n}$ is at most 1 if $n \geq 4$ and at most 3 if $n = 3$. But we have $M_n^{1/n} \leq \beta_5$, $A_n \leq \beta_6$ and it is clear that the number of solutions of (2) for which $\max(x, y) \leq \beta_5 c^{\beta_6/n}$ does not exceed $\beta_7 c^{\beta_6/n}$. Hence (2) has at most $\beta_8 c^{\beta_6/n}$ solutions.

Put $n_0 = [\beta_6 \varepsilon^{-1}] + 1$. Then (2) has at most $\beta_8 c^{\varepsilon}$ solutions for $n \geq n_0$, while for $n < n_0$ the number of solutions of (2) does not exceed

$$2n_0^{\omega(c)} + 6 \leq \exp(\omega(c) \log \beta_9(\varepsilon)) \leq \exp(\beta_{10} \log c (\log\log 3c)^{-1} \log \beta_9(\varepsilon)) \leq$$
$$\leq \exp(\beta_{11}(\varepsilon) + \varepsilon \log c) \leq \beta_{12}(\varepsilon) c^{\varepsilon},$$

since $\omega(c) \leq \beta_{10} \log c \cdot (\log\log 3c)^{-1}$ for all positive integers c. This proves corollary 3 completely. □

Now we shall prove theorem 4, that is that the equation

$$ax^z - by^z = c \quad (a, b, c \text{ integers with } abc \neq 0) \tag{7}$$

has at most $\beta_{13}(\varepsilon) \cdot \log M (\log\log M)^2 |c|^{\varepsilon}$ solutions in integers x, y, z with $|xy| \geq 2$, $z \geq 3$, where $M = \max(3, |a|, |b|)$. Theorem 4 is a consequence of

LEMMA 17: *If* (x, y, z) *is a solution of* (7) *with* $|xy| \geq 2$, $z \geq 3$, *then*

$$z < \beta_{14} \cdot \max(\log M (\log\log M)^2, \log|2c|). \tag{28}$$

For let z be an integer satisfying (28) with $z \geq 3$. Then the number of pairs (x, y) with $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $|xy| \geq 2$ such that (x, y, z) is a solution of (7) is by corollary 3 at most $\beta_1(\varepsilon/2) \cdot |c|^{\varepsilon/2}$, while the number of integers z satisfying (28) is at most

$$\beta_{15}(\varepsilon) \log M (\log\log M)^2 |c|^{\varepsilon/2}.$$

In the proof of lemma 17 we shall use the following result of Baker. For the proof we refer to [1].

LEMMA 18: *Let* $\gamma_1, \gamma_2, \ldots, \gamma_r$ *be non-zero algebraic numbers of degrees at most* d_0, *let* $b_1, b_2, \ldots, b_r$ *be rational integers such that* $|b_i| \leq B$, $B \geq 2$. *Suppose* $\gamma_1, \gamma_2, \ldots, \gamma_r$ *have heights not exceeding* $A_1, A_2, \ldots, A_r$ *respectively,* $A_i \geq 3$ *if* $i \in \{1, 2, \ldots, r-1\}$, $A_r \geq 2$. *Put*

$$\Omega' = \log A_1 \cdot \log A_2 \cdot \ldots \cdot \log A_{r-1}, \Omega = \Omega' \log A_r,$$
$$F = b_1 \log \gamma_1 + b_2 \log \gamma_2 + \ldots + b_r \log \gamma_r.$$

Then either $F = 0$ *or*

$$|F| > \exp(-\beta_{16}(r, d_0)\Omega \log \Omega' \log B).$$

PROOF OF LEMMA 17: Let (x, y, z) be a solution of (7). We put $m_0 = \max(|x|, |y|)$. For all positive real numbers $\zeta \neq 1$ we have $|\zeta - 1| \geq 1/2$ or $|\zeta - 1| \geq |\log \zeta|/2 > 0$. Hence we have

$$|1 - by^z/ax^z| \geq |1 - |by^z/ax^z|| \geq 1/2,$$

or

$$|1 - by^z/ax^z| \geq |1 - |by^z/ax^z|| \geq |\log|by^z/ax^z||/2 = \\ = |\log|b/a| + z \log|y/x||/2 > 0.$$

Now we apply lemma 18 with $d_0 = 1$, $r = 2$, $\gamma_1 = |b/a|$, $\gamma_2 = |y/x|$, $b_1 = 1$, $b_2 = z$. Then $A_1 \leq M$, $A_2 \leq m_0$, $B = z \geq 3$, hence

$$|\log|b/a| + z \log|y/x|| \geq \\ \geq \exp(-\beta_{17} \log z \log m_0 \log M \operatorname{loglog} M) =: U.$$

Since $U < 1$, it follows that

$$|1 - by^z/ax^z| \geq U/2. \tag{29}$$

By interchanging a and b, x and y, we may also conclude that

$$|1 - ax^z/by^z| \geq U/2. \tag{30}$$

But since

$$\min(|1 - ax^z/by^z|, |1 - by^z/ax^z|) \leq c/\max(|ax^z|, |by^z|) \leq |c| \cdot m_0^{-z},$$

we have, by (29) and (30),

$$|c| m_0^{-z} \geq U/2,$$

hence

$$z \log m_0 - \log|c| \leq \beta_{18} \log z \log m_0 \log M \operatorname{loglog} M.$$

We assume that $z \geq 2 \log|c|/\log 2$, whence $\log|c| \leq (z \log m_0)/2$. Then

$$z \log m_0 \leq \beta_{19} \log z \log m_0 \log M \operatorname{loglog} M.$$

This implies that

$$z/\log z \leq \beta_{19} \log M \operatorname{loglog} M,$$

hence

$$z \leq \beta_{20} \log M (\operatorname{loglog} M)^2.$$

This proves lemma 17. □

REFERENCES

[1] A. BAKER: The theory of linear forms in logarithms. In: A. Baker and D.W. Masser (eds.), *Transcendence theory, advances and applications*, Ch. 1. Proc. Conf. Cambridge 1976, Academic Press, London.

[2] Y. DOMAR: On the diophantine equation $|Ax^n - By^n| = 1$, $n \geq 5$. *Math. Scand. 2* (1954) 29–32.

[3] S. HYYRÖ: Über die Gleichung $ax^n - by^n = z$ und das Catalansche Problem. *Ann. Ac. Scient. Fenn. Ser. A1 355* (1964).

[4] W. LJUNGGREN: Einige Eigenschaften der Einheiten reeller quadratischer and rein biquadratischer Zahlkörper. *Oslo Vid-Akad. Skrifter 1* (1936) No. 12.

[5] T. NAGELL: Über einige kubischer Gleichungen mit zwei Unbestimmten. *Math. Z. 24* (1926) 422–447.

[6] C.L. SIEGEL: Die Gleichung $ax^n - by^n = c$. *Math. Ann. 114* (1937) 57–68.

(Oblatum 4-IX-1981)

Mathematisch Instituut
Rijksuniversiteit Leiden
Leiden, The Netherlands