ARKIV FÖR MATEMATIK Band 4 nr 17

Communicated 14 September 1960 by T. NAGELL

On a class of exponential equations

By J. W. S. CASSELS

In this note I shall prove the following theorem.

Theorem. *Let Π_1, Π_2 be two finite sets of rational prime numbers and let $\boldsymbol{P}_1, \boldsymbol{P}_2$ be the sets of positive integers all of whose prime factors are in Π_1, Π_2 respectively. Then for any fixed integer $C \neq 0$ there are only a finite number of solutions of*

$$X - Y = C, \qquad X \in \boldsymbol{P}_1,\ Y \in \boldsymbol{P}_2. \tag{1}$$

These can all be determined in a finite number of steps.

The novelty of the theorem lies only in the last sentence. Without it, the theorem is a well-known consequence of the theorem of Thue about the approximation of algebraic numbers by rationals which was subsequently improved by Siegel and Roth. We shall use instead a result (Lemma 1, below), given by Gelfond [2], which is related to Mahler's p-adic analogue of the Gelfond–Schneider theorem about the transcendence of α^β, where α and β are algebraic.

For the earlier history of the problem solved by our theorem we refer to Nagell [1] § 1. Nagell's formulation is different from ours, but the two formulations are readily seen to be identical.

The result which we require is given on page 157 of Gelfond's book, and may be formulated for our purposes as follows.

Lemma 1. *Let a, b be elements of some algebraic number field $\mathcal{K}$. Suppose that*

$$a^u = b^v \tag{2}$$

with rational integers u, v implies that $u = v = 0$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{K}$ for which a and b are $\mathfrak{p}$-adic units. Then there is a number $x_0 = x_0(a, b, \mathfrak{p})$, which can be determined in a finite number of steps, with the following property:

For any $x \geqslant x_0$ the congruence

$$a^u \equiv b^v \pmod{\mathfrak{p}^m} \tag{3}$$

is insoluble in rational integers u, v, m with

$$|u| + |v| \leqslant x, \qquad m \geqslant [\log^7 x]. \tag{4}$$

We shall need to supplement this by the trivial Lemma 2.

Lemma 2. *Let a, b be elements of some algebraic number field $\mathcal{K}$. Suppose that $b \neq 1$ and that there is a pair of coprime integers U, V such that*

$$a^U = b^V. \tag{5}$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{K}$ for which a and b are $\mathfrak{p}$-adic units. Then there exists a constant $\phi = \phi(a, b, \mathfrak{p})$, which can be determined in a finite number of steps, with the following property:

If the integers u, v, m are such that

$$a^u \equiv b^v \pmod{\mathfrak{p}^m} \tag{6}$$

and

$$m > \phi^2 - \phi \max(\log|u|, \log|v|), \tag{7}$$

then

$$u = tU, \qquad v = tV \tag{8}$$

for some rational integer t.

We sketch the simple proof. From (5) and (6) it follows that

$$b^w \equiv 1 \pmod{\mathfrak{p}^m}, \tag{9}$$

where

$$w = Vu - Uv.$$

If (7) is true, we have

$$\begin{aligned} |w| &\leqslant 2 \max(|U|, |V|) \max(|u|, |v|) \\ &\leqslant 2 \max(|U|, |V|) \exp(-\phi + \phi^{-1} m). \end{aligned} \tag{10}$$

Here $2 \max(|U|, |V|)$ is fixed. The theory of the $\mathfrak{p}$-adic logarithm now shows immediately that (9) and (10) together imply $w = 0$, provided that ϕ is chosen large enough.

We are now in a position to prove the following lemma, of which the theorem is an easy consequence.

Lemma 3. *Let Π be a finite set of rational primes and let $\mathbf{P}$ be the set of positive integers all of whose prime factors are in Π. Let $D > 0$ and $E \neq 0$ be rational integers and suppose that no prime factors of E is in Π. Then there are only a finite number of solutions Z, Y of the equation*

$$Z^2 - DY^2 = E, \tag{11}$$

where Z is a rational integer and $Y \in \mathbf{P}$. These can all be obtained in a finite number of steps.

When D is a perfect square the lemma is trivial, so we may assume without loss of generality that the field $\mathcal{K} = k(D^{\frac{1}{2}})$ generated by $D^{\frac{1}{2}}$ over the rational field is a real quadratic field. Let $\eta > 1$ be the fundamental unit of $k(D^{\frac{1}{2}})$. Then (11) implies that

$$Z + Y D^{\frac{1}{2}} = \alpha \eta^n, \qquad Z - Y D^{\frac{1}{2}} = \alpha' (\eta')^n \tag{12}$$

for some rational integer n, where α is one of a finite set of integers of $k(D^{\frac{1}{2}})$ and where α', η' are the conjugates of α, η respectively. Hence

$$\alpha \eta^n - \alpha' (\eta')^n = 2 Y D^{\frac{1}{2}}. \tag{13}$$

By (12) there is a constant $\theta = \theta(\alpha, D) > 0$ such that

$$Y > \theta \eta^n. \tag{14}$$

Since $Y \in \boldsymbol{P}$, we have

$$Y = \prod_{1 \leqslant \sigma \leqslant s} p_\sigma^{a_\sigma} \tag{15}$$

for some integers $a_\sigma \geqslant 0$, where $p_1, \cdots, p_s$ are the primes in the set Π. Hence, by (14)

$$\max_{1 \leqslant \sigma \leqslant s} a_\sigma \geqslant \psi n,$$

where $\psi = \psi(\alpha, D, \Pi) > 0$. We may suppose, without loss of generality, that

$$a_1 > \psi n. \tag{16}$$

Let $\mathfrak{p}$ be a prime ideal divisor of p_1 in $k(D^{\frac{1}{2}})$. Since $E = \mathrm{Norm}\,\alpha$ and $p_1 \nmid E$, by hypothesis, it follows that α and α' are integers for $\mathfrak{p}$. Hence, by (13), (15) and (16) we have

$$a \equiv b^n \pmod{\mathfrak{p}^{\psi n}}, \tag{17}$$

where $a = \alpha/\alpha', \quad b = \eta'/\eta$

are integers for $\mathfrak{p}$.

But now

$$\psi n > \log^7 n$$

and

$$\psi n > \phi^2 + \phi \log n$$

for all sufficiently large n. Hence Lemma 3 follows from Lemma 2 or Lemma 1 according as a is an ordinary unit or not.

We can now deduce the theorem in a few lines. After dividing X, Y, C in (1) be their common divisor, we may suppose without loss of generality that X, Y, C are coprime in pairs. Hence we may suppose that the two sets Π_1, Π_2 of primes are disjoint and that C is not divisible by any prime in Π_1 or Π_2.

In (1) we may write

$$X = A X_1^2, \qquad Y = B Y_1^2,$$

where A and B are coprime. There are only a finite number of possible values for A and B. Clearly

$$X_1 \in \boldsymbol{P}_1 \qquad Y_1 \in \boldsymbol{P}_2.$$

But now

$$Z^2 - D Y_1^2 = E,$$

where $$Z = A X_1, \quad D = A B, \quad E = A C.$$

We can now apply Lemma 3 with $\Pi = \Pi_2$. Note that we do not use the fact that $X_1 \in \Pi_1$.

Trinity College, Cambridge, England.

REFERENCES

1. NAGELL, T., Sur une classe d'équations exponentielles. Ark. Mat. 3, 54 (1958).
2. ГЕЛЬФОНД, А. О. Трансцендентные и алгебраические числа; Moscow, 1952.
(Added in proof: An English translation has just appeared, published by the Dover Press.)

Tryckt den 10 december 1960

Uppsala 1960. Almqvist & Wiksells Boktryckeri AB