ON A SPECIAL CLASS OF DIOPHANTINE EQUATIONS: I

KURT MAHLER‡.

[*Extracted from the Journal of the London Mathematical Society, Vol.* 13, 1938.]

The following theorem is proved in this paper:

Suppose that $f(x, y)$ is a polynomial in x and y with integer coefficients, which is irreducible in the field of all rational numbers, and that there is an infinity of lattice points (x, y) on the curve $f(x, y) = 0$, for which the greatest prime factor of x and y is bounded. Then

$$f(x, y) \equiv qx^m + ry^n,$$

‡ Received 19 January, 1938; read 20 January, 1938.

where q and r are non-vanishing integers, and m and n are coprime integers greater than or equal to zero, but not both zero.

This result shows that the equation

$$F(u^x, v^y) = 0,$$

where $F(x, y)$ is a polynomial with rational coefficients and where u and v are two integers greater than or equal to 2, has in general only a finite number of solutions in integers $x \geqslant 0$ and $y \geqslant 0$, and determines all exceptional cases.

1. Let $f(x, y)$ be a non-constant polynomial in x and y with integer coefficients, and suppose that on the curve C,

$$f(x, y) = 0, \tag{1}$$

there lies an infinite set S of lattice points (x, y), such that xy is divisible only by a finite number of given prime numbers $P_1, P_2, \ldots, P_t$. Curves of this kind are, *e.g.*

$$x-a = 0 \quad \text{or} \quad y-b = 0,$$

where a, b are non-vanishing integers. We exclude these trivial cases, and we also suppose, without loss of generality, that $f(x, y)$ is irreducible in the field of all rational numbers.

Then, for the elements of S, both $|x|$ and $|y|$ must tend to ∞. For, if for an infinity of elements of S, the abscissa x has the same value $c \neq 0$, then the straight line $x-c = 0$ has an infinite number of points of intersection with C, and therefore forms a part of this curve, so that $f(x, y)$ would be reducible, contrary to hypothesis; similarly with the ordinate y.

By the theory of algebraic curves, for sufficiently large x, y can be expressed as one of a finite number of descending power series

$$y = \sum_{k=0}^{\infty} a_{hk} x^{(m_h-k)/n}, \quad a_{h0} \neq 0 \quad (h = 1, 2, \ldots, H), \tag{2}$$

where n is a positive integer, $m_1, m_2, \ldots, m_H$ are integers, and the a_{hk} are algebraic numbers. Hence, to every element (x, y) of S with sufficiently large coordinates, there belongs an index $h = h(x, y)$, for which the corresponding equation (2) is satisfied. But h has only a finite number of possible values. Hence, for an infinite subset S' of S, h has always the same value, and therefore for all elements of S'

$$y = a_0 x^{m/n} + a_1 x^{(m-1)/n} + a_2 x^{(m-2)/n} + \ldots \quad (a_0 \neq 0), \tag{3}$$

where n is the same integer as in (2), m is one of the integers $m_1, m_2, \ldots, m_H$, and the a_k are the a_{hk} with a certain fixed index h. Since y is bounded for only a finite number of elements of S', the exponent m/n must be positive, and therefore m is a positive integer.

2. The coordinates of every element (x, y) of S' can be written as

$$x = \epsilon_1 P_1^{u_1} P_2^{u_2} \ldots P_t^{u_t}, \quad y = \epsilon_2 P_1^{v_1} P_2^{v_2} \ldots P_t^{v_t},$$

where $\epsilon_1 = \pm 1$, $\epsilon_2 = \pm 1$, and the u_τ, v_τ are non-negative integers. Suppose that

$$u_\tau = u_\tau' n + u_\tau'', \quad v_\tau = v_\tau' m + v_\tau'' \quad (\tau = 1, 2, \ldots, t),$$

where the u_τ', v_τ' are non-negative integers, while the u_τ'', v_τ'' are integers satisfying the inequalities

$$0 \leqslant u_\tau'' \leqslant n-1, \quad 0 \leqslant v_\tau'' \leqslant m-1 \quad (\tau = 1, 2, \ldots, t).$$

Then the system of $2t$ numbers

$$u_1'', \quad u_2'', \quad \ldots, \quad u_t'', \quad v_1'', \quad v_2'', \quad \ldots, \quad v_t''$$

has only $(mn)^t$ different possibilities, and so for an infinite subset S'' of S'

$$u_\tau'' = u_\tau^*, \quad v_\tau'' = v_\tau^* \quad (\tau = 1, 2, \ldots, t),$$

where the integers u_τ^*, v_τ^* are constants. We now write

$$X = P_1^{u_1'} P_2^{u_2'} \ldots P_t^{u_t'}, \quad Y = P_1^{v_1'} P_2^{v_2'} \ldots P_t^{v_t'},$$

$$A = P_1^{u_1^*} P_2^{u_2^*} \ldots P_t^{u_t^*}, \quad B = P_1^{v_1^*} P_2^{v_2^*} \ldots P_t^{v_t^*},$$

so that

$$x = \epsilon_1 A X^n, \quad y = \epsilon_2 B Y^m. \tag{4}$$

Then A and B are positive integers, which do not depend on the elements (x, y) of S'', while X and Y are positive integers, which become arbitrarily large, and which are both divisible only by the prime numbers $P_1, P_2, \ldots, P_t$. We may suppose that ϵ_1 and ϵ_2 are independent of (x, y), that is, of (X, Y), replacing S'', if necessary, by one of its infinite subsets.

3. By formula (3), for large x,

$$y^n \sim a_0^n x^m$$

and therefore, by (4),

$$\frac{Y^{mn}}{X^{mn}} \to \frac{a_0^n (\epsilon_1 A)^m}{(\epsilon_2 B)^n}.$$

Hence we can find an infinite subset S^* of S'', for the elements of which

$$\frac{Y}{X} \to \lambda,$$

where λ is one of the real values of

$$a_0^{1/m}(\epsilon_1 A)^{1/n}(\epsilon_2 B)^{-1/m} \neq 0.$$

Obviously $$Y^m = \lambda^m X^m (1+\alpha_1 X^{-1}+\alpha_2 X^{-2}+\ldots),$$

where $$\alpha_k = \frac{a_k}{a_0}(\epsilon_1 A)^{-k/n} \quad (k=1, 2, 3, \ldots).$$

Hence

$$Y = \lambda X(1+\beta_1 X^{-1}+\beta_2 X^{-2}+\ldots), \tag{5}$$

and here the β_k are constants, which all vanish if and only if all α_k, *i.e.* all a_k $(k=1, 2, 3, \ldots)$, are zero. The power series converges when X is a sufficiently large number, and then, when X belongs to an element of S^*, gives the value of Y.

4. Suppose now that at least one of the coefficients $\beta_1, \beta_2, \beta_3, \ldots$ does not vanish, and let

$$X = (X, Y)\,\xi, \quad Y = (X, Y)\,\eta.$$

Both ξ and η have no other prime factors than $P_1, P_2, \ldots, P_t$. By (5),

$$\frac{\eta}{\xi} = \lambda(1+\beta_1 X^{-1}+\beta_2 X^{-2}+\ldots).$$

Here the right-hand side tends to the limit λ, but, by the theory of power series, it will be different from this limit, as soon as X is sufficiently large. Hence both ξ and η must tend to infinity for the elements of S^*. Thus we have obtained an infinite set of rational numbers ξ/η, for which

$$\left|\frac{\eta}{\xi} - \lambda\right| \leqslant c\,|\xi|^{-1}, \tag{6}$$

with a certain positive constant c, for $|X| \geqslant |\xi|$.

This result, however, at once leads to a contradiction. For, since the greatest prime divisor of $\xi\eta$ lies under a given bound and since λ does not vanish and is an algebraic number, the inequality (6) possesses at most a finite number of such solutions; compare Satz 3 of my previous paper†.

† *Proc. Royal Acad. Amsterdam*, 39 (1937), 633–640, 729–737.

It follows that all β_k, and therefore also all $a_1, a_2, a_3, \ldots$, must be zero. Hence, for the elements of S,

$$y^n = a_0^n x^m.$$

Suppose that m and n are chosen as coprime integers. Then obviously a_0^n is a rational number and the polynomial

$$g(x, y) = y^n - a_0^n x^m$$

is irreducible. We have proved that an infinity of lattice points on

$$f(x, y) = 0$$

lie also on the irreducible curve

$$g(x, y) = 0.$$

Hence $f(x, y)$ is divisible by $g(x, y)$, and since also $f(x, y)$ is irreducible, the polynomials can differ only by a constant, non-vanishing factor. This completes the proof.

Mathematical Department,
The University, Manchester.

Printed by C. F. Hodgson & Son, Ltd., Newton St., London, W.C.2.