ON A SPECIAL CLASS OF DIOPHANTINE EQUATIONS: II

KURT MAHLER†.

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

In this second paper I generalize the result of Paper I, and prove the following theorem:

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 is bounded. Then the curve is given parametrically by

$$x = as^n, \quad y = g(s),$$

where $a \neq 0$ is an integer, n is a non-negative integer, and $g(s)$ is a polynomial in s with rational coefficients.

While the first part depended on the Thue-Siegel theorem, this paper uses the deeper theorem of Siegel about the lattice points on algebraic curves.

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

1. Suppose that $f(x, y)$ is an irreducible polynomial with rational coefficients, and that the equation

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

has an infinite set S of different integer solutions (x, y), such that x is divisible only by a finite system of prime numbers $P_1, P_2, \ldots, P_t$. This condition is satisfied, for instance, in the two cases

$$f(x, y) \equiv x - a \quad \text{and} \quad f(x, y) \equiv y - b,$$

where $a \neq 0$ and b are fixed integers; these two trivial cases will be excluded from what follows.

Then, for the elements (x, y) of S,

$$x = \epsilon P_1^{u_1} P_2^{u_2} \ldots P_t^{u_t},$$

where $\epsilon = \pm 1$, and $u_1, u_2, \ldots, u_t$ are integers greater than or equal to zero. Let N be a positive integer and write u_τ as

$$u_\tau = u_\tau' N + u_\tau'' \quad (\tau = 1, 2, \ldots, t),$$

where the u_τ' are non-negative integers, while each of the residues u_τ'' has one of the values

$$0, 1, 2, \ldots, N-1.$$

Since the system of numbers $\epsilon, u_1'', \ldots, u_t''$ has only $2N^t$ different possibilities, there is an infinite subset S_N of S, for the elements (x, y) of which

$$\epsilon = \epsilon^*, \quad u_1'' = u_1^*, \quad u_2'' = u_2^*, \quad \ldots, \quad u_t'' = u_\tau^*$$

have always constant values. Hence, when

$$X = P_1^{u_1'} P_2^{u_2'} \ldots P_t^{u_t'}, \quad A = \epsilon^* P_1^{u_1^*} P_2^{u_2^*} \ldots P_t^{u_t^*},$$

so that A is a constant integer, while the integer X depends on x and tends to ∞ with x, then, for the elements of S_N,

$$x = AX^N.$$

Hence there is, in particular, an infinite set of solutions of

$$f(AX^N, y) = 0$$

in integers X, y.

2. Now, by a theorem due to Siegel†, there can be an infinity of lattice points on an algebraic curve only when this curve is of genus zero. Hence, we get the following two results:

---

† *Abh. Preussische Akad. Wiss.* (1929), *Math.-Phys. Kl.*, Nr. 1, Zweiter Teil.

(*a*) Both coordinates x, y of the curve $f(x, y) = 0$ are non-constant rational functions

(1) $$x = r(t), \quad y = r_1(t)$$

of a parameter t, and this parameter can be chosen in such a way that it is itself a rational function

(2) $$t = r_2(x, y)$$

of x and y.

(*b*) For every positive integer N, the coordinates $X = (x/A)^{1/N}$ and y on the curve $f(AX^N, y) = 0$, and therefore also $x^{1/N}$ and y, are rational functions

(3) $$x^{1/N} = R_1(T), \quad y = R_2(T)$$

of a second parameter T.

Hence, in particular,

(4) $$t = r_2\Big(R_1(T)^N, R_2(T)\Big) = R(T)$$

say, must be a rational function of T.

Therefore, corresponding to the given rational function $r(t)$ and to every given positive integer N, there must exist a non-constant rational function $R(T)$, such that $r\Big(R(T)\Big)$ is the exact N-th power of a rational function of T. This gives an infinity of different algebraic conditions for $r(t)$. In general, as we shall see, these conditions cannot be satisfied.

3. Obviously, t is determined except for an arbitrary linear transformation. Therefore, without loss of generality, we may suppose that $r(t)$ is regular and not zero for $t = \infty$, so that

(5) $$r(t) = a \prod_{k=1}^{m} (t - a_k)^{n_k},$$

where $a \neq 0$ is a constant, $a_1, a_2, \ldots, a_m$ are the different zeros and poles of $r(t)$, and $n_1, n_2, \ldots, n_m$ are non-vanishing integers with a sum

(6) $$n_1 + n_2 + \ldots + n_m = 0.$$

Since $r(t)$ is not a constant, it must have at least one zero and one pole, and therefore $m \geqslant 2$.

The second rational function $R(T)$ can be written as a quotient

$$R(T) = \frac{p(T)}{q(T)}$$

of two coprime polynomials $p(T)$ and $q(T)$, of which at least one is not a constant. Then, by (6),

$$r\big(R(T)\big) = a \prod_{k=1}^{m} \left(\frac{p(T)}{q(T)} - a_k\right)^{n_k} = a \prod_{k=1}^{m} \big(p(T) - a_k q(T)\big)^{n_k},$$

and this must be the exact N-th power of a rational function. Now, since all the a_k are different, no two of the m polynomials

$$p(T) - a_k q(T) \quad (k = 1, 2, \ldots, m)$$

vanish together or are both constants. Hence $r\big(R(T)\big)$ is an exact N-th power, if and only if all m polynomials

$$(7) \qquad p(T) - a_k q(T) = P_k(T)^N \quad (k = 1, 2, \ldots, m)$$

are the N-th powers of certain polynomials $P_k(T)$, and here no two of these $P_k(T)$ have a common zero or are both constants.

Suppose, in particular, that $m \geqslant 3$. Then, by eliminating $p(T)$ and $q(T)$ from the first three equations (7), we have

$$\left\{\sqrt[N]{\left(\frac{a_3 - a_2}{a_1 - a_2}\right)} \frac{P_1(T)}{P_3(T)}\right\}^N + \left\{\sqrt[N]{\left(\frac{a_1 - a_3}{a_1 - a_2}\right)} \frac{P_2(T)}{P_3(T)}\right\}^N = 1.$$

identically in T, so that the coordinates of points of the curve

$$\xi^N + \eta^N = 1$$

are represented as rational, non-constant functions of a parameter. But, for $N \geqslant 3$, this curve is at least of genus one, since it has no singular points. Therefore, the assumption $m \geqslant 3$ leads to a contradiction.

4. Hence, necessarily, $m = 2$, $n_1 = -n_2 = n$, and

$$r(t) = a\left(\frac{t - a_1}{t - a_2}\right)^n = as^n,$$

with the new parameter $s = (t - a_1)/(t - a_2)$. The constant $a \neq 0$ is still arbitrary; we choose it as an integer in such a way that there is an infinite set S^* of lattice points (x, y) on the curve

$$(8) \qquad f(x, y) = 0,$$

for which $x = as^n$ with integer s; this is possible by § 1. Then, by § 2,

$$x = as^n, \quad y = g(s)$$

identically in s on our curve (8), where $g(s)$ is a rational function of s. By considering the elements of S^*, it follows that $g(s)$ is an integer for infinitely many integer values of s; therefore its coefficients may be taken to be rational numbers, and we can write

$$g(s) = g_1(s) + g_2(s),$$

where $g_1(s)$ is a polynomial with rational coefficients, while $g_2(s)$ is a rational function which vanishes for $s = \infty$. Hence there is a positive integer h, such that $hg_1(s)$ has integer values for all integers s. Also, if $g_2(s)$ does not vanish identically, then $0 < |g(s)| < 1/h$ for all sufficiently large s; and so, for sufficiently large s, $g(s)$ cannot be an integer. Therefore $g(s) = g_1(s)$ is a polynomial with rational coefficients, and the theorem is proved†.

Mathematical Department,
The University,
Manchester.

† I wish to express my thanks to Prof. Mordell for his help with the manuscript of both parts of this paper.

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