# ON THE DIOPHANTINE EQUATION $ay^2+by+c = dx^n$

By EDMUND LANDAU and ALEXANDER OSTROWSKI.

(Communicated by G. H. HARDY.)

[Received December 19th, 1919.—Read February 12th, 1920.]

1. We owe to Mr. A. Thue* the important theorem:

*If $F(u, v)$ is a homogeneous form with rational integral coefficients, and is not a power of a linear or quadratic form, then the equation*

$$F(u, v) = f$$

*has, for every $f \neq 0$, at most a finite number of rational integral solutions.*

It was shown by Landau,† in response to a question‡ in *l'Intermédiaire des Mathématiciens*, and by use of the particular case of Thue's theorem in which $F$ is a cubic form, that the equation $y^2-2 = x^3$ has only a finite number of solutions. The method may be extended, by the aid of considerations drawn from the theory of ideals, so as to lead to the following theorem:

*The equation*

$$ay^2+by+c = dx^n, \tag{1}$$

*where $n \geqslant 3$, $a \neq 0$, $b^2-4ac \neq 0$, $d \neq 0$, and all the letters denote rational integers, has at most a finite number of solutions.*

* "Om en general i store hele tal ulösbar ligning," *Skrifter udgivne af Videnskabs-Selskabet i Christiania*, 1908 I, Mathematisk-Naturvidenskabelig Klasse (1909), No. 7, 15 S.; "Über Annäherungswerte algebraischer Zahlen," *Journal für die reine und angewandte Mathematik*, Bd. 135 (1909), S. 284-305. In the second memoir the theorem is proved only for an irreducible $F(u, v)$; but the extension to the general case (treated in the first memoir) is immediate.

† *L'Intermédiaire des Mathématiciens*, t. 8 (1901), pp. 145-147, and t. 20 (1913), p. 154.

‡ 1360.

This theorem, the proof of which is the object of the present note, is new only when $n > 3$, for when $n = 3$ it results immediately from a combination of Thue's theorem with the results obtained by Mr. Mordell, from the theory of numbers and the theory of invariants, in his memoir "Indeterminate equations of the third and fourth degrees."*

In the special case when $a = 1$, $b = 0$, $d = 1$, $n \geqslant 3$, our theorem shows that:

*If all squares and all n-th powers $\geqslant 0$ are arranged together in order of magnitude, numbers which are both squares and n-th powers occurring only once, in a series*

$$z_1(=0),\ z_2(=1),\ z_3(=4),\ \ldots,\ z_m,\ z_{m+1},\ \ldots,$$

*then $z_{m+1}-z_m$ tends to infinity with m.*

This special case is trivial† when $n$ is even; it may be expressed, when $n$ is odd, in the form:

*If $\vartheta(t)$ denotes the distance of t from the nearest rational integer, and x runs through all rational integers $\geqslant 0$ which are not squares, then*

$$x^{\frac{1}{2}n}\,\vartheta(x^{\frac{1}{2}n}) \rightarrow \infty .$$

[For, if the sign is chosen appropriately,

$$\left(x^{\frac{1}{2}n} \pm \vartheta(x^{\frac{1}{2}n})\right)^2 = x^n \pm 2x^{\frac{1}{2}n}\,\vartheta(x^{\frac{1}{2}n}) + \left(\vartheta(x^{\frac{1}{2}n})\right)^2$$

is a square, whose distance from $x^n$ is

$$\left| \pm 2x^{\frac{1}{2}n}\,\vartheta(x^{\frac{1}{2}n}) + \left(\vartheta(x^{\frac{1}{2}n})\right)^2 \right| \leqslant 2x^{\frac{1}{2}n}\,\vartheta(x^{\frac{1}{2}n}) + \tfrac{1}{4},$$

and tends to infinity.]

2. *Proof of the theorem.*—The equation (1) may be written

$$(2ay+b)^2-(b^2-4ac) = 4adx^n.$$

Hence, if (1) has an infinity of solutions, so has an equation

$$(2) \qquad y^2-k = lx^n \quad (k \neq 0,\ l \neq 0).$$

We need therefore only consider the equation (2). There are two cases.

* *Quarterly Journal of Pure and Applied Mathematics*, Vol. 45 (1914), pp. 170-186. See also the note "A statement by Fermat," *Proc. London Math. Soc.* (*Records &c.*), Ser. 2, Vol. 18 (1919), pp. v-vi.

† Since then every $z_m$ is a square.

I. Let $k$ be a square $m^2$. Then

$$(y+m)(y-m) = lx^n.$$

We ignore the trivial solutions $x = 0$, $y = \pm m$. Any prime factor of $y+m$, which is not a factor of $2m$ or of $l$, occurs in $y+m$ with a multiplicity divisible by $n$, since it does not divide $y-m$, and divides $lx^n$ exactly as often as $x^n$. Hence

$$y+m = \pm p_1^{a_1} \cdots p_j^{a_j} z^n,$$

where $p_1, p_2, \ldots, p_j$ are the different prime factors of $2ml$, the exponents $a_1, \ldots, a_j$ are positive or zero, and $z$ is a rational integer. If every $a_i$ is reduced to modulus $n$, we obtain

$$(3) \qquad y+m = qu^n,$$

where $q$ can assume only a finite system of values, exclusive of zero. In exactly the same way

$$(4) \qquad y-m = rv^n,$$

where $r$ can assume only a finite system of values, exclusive of zero.

For each pair $q$, $r$, occurring in (3) and (4), the equation

$$2m = qu^n - rv^n$$

has, by Thue's theorem, at most a finite number of solutions; for the $n$ roots of $q\tau^n - r = 0$ are all different. Thus at most a finite number of values of $y$ are possible.

II. Suppose that $k$ is not a square. Then in (2) $x \neq 0$, and so the ideal equation

$$[y+\sqrt{k}][y-\sqrt{k}] = [l][x]^n$$

holds in the quadratic corpus $P(\sqrt{k})$.* Every prime ideal which divides $[y+\sqrt{k}]$, but neither $[2\sqrt{k}]$ nor $[l]$, occurs in $[y+\sqrt{k}]$ with an exponent divisible by $n$; for it does not divide $[2\sqrt{k}]$, and therefore not $[y-\sqrt{k}]$. Thus

$$[y+\sqrt{k}] = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2} \cdots \mathfrak{p}_j^{a_j}\mathfrak{z}^n,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_j$ are the different prime ideals which divide $[2\sqrt{k} \,.\, l]$, the exponents $a_1, \ldots, a_j$ are positive or zero, and $\mathfrak{z}$ is an ideal. If each $a_i$ is

* $[\alpha]$ denotes the principal ideal (Hauptideal) of the integers of the corpus divisible by $\alpha$.

reduced to modulus $n$, we obtain

$$(5) \qquad [y+\sqrt{k}] = \mathfrak{q}\mathfrak{u}^n,$$

where $\mathfrak{q}$ belongs to a finite system of ideals, and $\mathfrak{u}$ is an ideal.

It is enough to show that, for a fixed $\mathfrak{q}$, (5) can be satisfied by an ideal $\mathfrak{u}$ for at most a finite number of values of $y$. If this were not so, there would be a class of ideals $\mathfrak{K}$ such that (5) could be satisfied by an ideal $\mathfrak{u}$ of $\mathfrak{K}$ for an infinity of values of $y$. If $\mathfrak{w}$ is a fixed representative of the class inverse to $\mathfrak{K}$, so that* $\mathfrak{u}\mathfrak{w} \sim [1]$, then it follows from (5) that

$$\mathfrak{q}\mathfrak{u}^n \sim [1],$$

$$\mathfrak{q} \sim \mathfrak{q}\,(\mathfrak{u}\mathfrak{w})^n \sim \mathfrak{w}^n.$$

There are therefore two integers $s$ and $\gamma$, of which $s$ may be supposed rational, and both are independent of $\mathfrak{u}$, in the corpus $P(\sqrt{k})$, such that

$$[s]\,\mathfrak{q} = [\gamma]\,\mathfrak{w}^n.$$

It now follows from (5) that

$$[s][y+\sqrt{k}] = [s]\,\mathfrak{q}\mathfrak{u}^n = [\gamma]\,\mathfrak{w}^n\mathfrak{u}^n = [\gamma](\mathfrak{w}\mathfrak{u})^n = [\gamma][\xi]^n,$$

where $\xi$ is an integer of the corpus. Therefore

$$s(y+\sqrt{k}) = \epsilon\gamma\xi^n,$$

where $\epsilon$ is a unity.

If $k < 0$ the number of unities is finite, and if $k > 0$ all unities are expressible in terms of a fundamental unity $\eta$ in the form $\pm\eta^t$, where $t$ is a rational integer. Thus every unity is the product of ($a$) a unity chosen from a finite system, and ($b$) the $n$-th power of a unity. Accordingly

$$(6) \qquad s\,(y+\sqrt{k}) = \beta\zeta^n,$$

where $\beta$ belongs to a finite system of integers of the corpus, excluding zero, and $\zeta$ is an integer of the corpus. It is therefore enough to show that, for a fixed positive or negative $s$, and a fixed non-zero $\beta$, at most a finite number of values of $y$ can occur in (6).

We choose a base 1, $\omega$ of the integers of the corpus. Then

$$\zeta = u+v\omega,$$

where $u$, $v$ are rational integers. Denoting generally by $\mu'$ the number

* The symbol $\sim$ denotes equivalence.

conjugate to $\mu$, we have,[*] from (6),

$$(7) \qquad \frac{2s\sqrt{k}}{\omega-\omega'} = \frac{\beta(u+v\omega)^n-\beta'(u+v\omega')^n}{\omega-\omega'}.$$

The right-hand side is a binary form $F(u, v)$ with rational integral coefficients, since for every integer $\mu = u_0+v_0\omega$ the number $\frac{\mu-\mu'}{\omega-\omega'} = v_0$ is rational and integral. If $\delta$ is a root of $\delta^n = \beta'/\beta$, and $\rho$ runs through the $n$-th roots of unity, then

$$F(u, v) = \frac{\beta}{\omega-\omega'} \Pi_\rho \{u+v\omega-\rho\delta(u+v\omega')\}.$$

No two of the linear factors are the same, or differ only by a constant factor; for, if $\rho_1 \neq \rho_2$,

$$\begin{vmatrix} 1-\rho_1\delta, & \omega-\rho_1\delta\omega' \\ 1-\rho_2\delta, & \omega-\rho_2\delta\omega' \end{vmatrix} = \begin{vmatrix} 1, & -\rho_1\delta \\ 1, & -\rho_2\delta \end{vmatrix} \begin{vmatrix} 1, & \omega \\ 1, & \omega' \end{vmatrix} = \delta(\rho_1-\rho_2)(\omega'-\omega) \neq 0.$$

Thus Thue's theorem may be applied to (7); at most a finite number of values of $u$ and $v$, of $\zeta$, and of $y$, can occur; and our theorem is proved.

3. From our theorem it is very easy to deduce that of Pólya:[†] *the greatest prime factor of $ay^2+by+c$ ($a \neq 0$, $b^2-4ac \neq 0$) tends to infinity with $|y|$.* For if, for an infinity of values of $y$, $ay^2+by+c$ were composed only of a finite system of primes $p_1, \ldots, p_j$, then for every fixed $n$ greater than 2, and for at least one number $d$, formed by powers of these primes, the equation (1) would have an infinity of solutions.

*Göttingen, December 14th,* 1919.

[*] Compare the similar argument used by Pólya, "Zur arithmetischen Untersuchung der Polynome," *Math. Zeitschrift*, Bd. 1 (1918), S. 143-148 (S. 147).

[†] *L.c.*, S. 144.