ON THE NUMBER OF INTEGERS WHICH CAN BE REPRESENTED BY A BINARY FORM

P. ERDÖS *and* K. MAHLER*.

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

Let $F(x, y)$ be a binary form of degree $n \geqslant 3$ with integer coefficients and non-vanishing discriminant, and let $A(u)$ be the number of different positive integers $k \leqslant u$, for which $|F(x, y)| = k$ has at least one solution in integers x, y. We prove that

(a) $$\liminf_{u \to \infty} A(u)\, u^{-2/n} > 0.$$

The proof is simple, but not elementary, since it depends on the p-adic generalization of the Thue-Siegel theorem. The result remains true when x and y are restricted by conditions

$$x \geqslant 0, \quad \alpha x \leqslant y \leqslant \beta x \quad (\alpha, \beta \text{ constants}).$$

* Received 15 December, 1937; read 16 December, 1937.

Thus, for instance, when $F(x, y)$ is not negative definite, and $A(u)$ is now the number of positive integers $k \leqslant u$, for which $F(x, y) = k$ has at least one solution, then again (a) is true. In the special case $F(x, y) = x^n + y^n$, $n \geqslant 3$ and odd, one of us (Erdös) had already found an elementary proof for (a) some weeks ago, but this proof could not be generalized.

1. The following notation will be used:

$F(x, y) = \sum_{h=0}^{n} a_h x^{n-h} y^h$ $(a_0 a_n \neq 0)$ is a binary form of degree $n \geqslant 3$ with integer coefficients and discriminant $d \neq 0$.

x, y are two integers, for which $F(x, y) \neq 0$.

$|x, y| = \max(|x|, |y|)$.

N is a sufficiently large positive integer.

A is an integer not zero with sufficiently large modulus $|A|$.

ϑ is a number satisfying $0 < \vartheta \leqslant 1$, to be assigned later.

$c_0, c_1, \ldots$ are positive numbers, which depend only on the form F.

$\gamma = \max(|a_0|, |d|, n)$.

p is a prime number satisfying $\gamma < p \leqslant N^\vartheta$.

P is a prime number satisfying either $P \leqslant \gamma$ or $P > N^\vartheta$.

$p^a \| A$ denotes that A is divisible by p^a, but not by p^{a+1}.

$g(A)$ is the arithmetical function defined by $g(A) = \prod_{\substack{\gamma < p \leqslant N^\vartheta \\ p^a \| A \\ p^a \leqslant N^\vartheta}} p^a$.

2. LEMMA 1. *For sufficiently large* N

$$G(N) = \prod_{\substack{|x, y| \leqslant N \\ F(x, y) \neq 0}} g\Big(F(x, y)\Big) \leqslant N^{8\vartheta n (2N+1)^2}.$$

Proof. By definition, $p > n$ and p is prime to a_0 and d. Hence, for given a and y, there are at most n incongruent values of x (mod p^a), for which $F(x, y) \equiv 0$ (mod p^a). Therefore, for given p and a with

$$\gamma < p \leqslant p^a \leqslant N^\vartheta,$$

the conditions

$$|x, y| \leqslant N, \quad F(x, y) \neq 0, \quad F(x, y) \equiv 0 \pmod{p^a}$$

have at most

$$n(2N+1)\left\{\left[\frac{2N+1}{p^a}\right]+1\right\} \leqslant \frac{2n(2N+1)^2}{p^a}$$

solutions x, y. It follows that the exponent b, with $p^b \| G(N)$, satisfies the inequality

$$b \leqslant \sum_{a=1}^{\infty} \frac{2n(2N+1)^2}{p^a} = \frac{2n(2N+1)^2}{p-1} \leqslant \frac{4n(2N+1)^2}{p}.$$

Hence, for sufficiently large N,

$$G(N) \leqslant \exp\left\{ \sum_{\gamma < p \leqslant N^\vartheta} \frac{4n(2N+1)^2}{p} \log p \right\} \leqslant N^{2\vartheta \cdot 4n(2N+1)^2},$$

since

$$\sum_{p \leqslant u} \frac{\log p}{p} \leqslant 2 \log u$$

for sufficiently large u.

LEMMA 2. *If μ is the number of pairs x, y with*

$$|F(x, y)| \leqslant N^{\frac{1}{2}}, \quad |x, y| \leqslant N,$$

then $\mu \leqslant \frac{1}{3}N^2$ for sufficiently large N.

Proof. For a given m with $|m| \leqslant N^{\frac{1}{2}}$ and a given y with $|y| \leqslant N$, the equation $F(x, y) = m$ has at most n integer solutions x, and therefore

$$\mu \leqslant n(2\sqrt{N}+1)(2N+1) \leqslant \tfrac{1}{3}N^2.$$

LEMMA 3. *For sufficiently large N, there are at least $\frac{4}{3}N^2$ pairs of integers x, y with $|x, y| \leqslant N$ and $(x, y) = 1$.*

Proof. Obviously, the number of these pairs is at least $4M$, where M denotes the number of pairs with $1 \leqslant x \leqslant N$, $1 \leqslant y \leqslant N$, $(x, y) = 1$, so that

$$M \geqslant N^2 - \sum_p \frac{N^2}{p^2} \geqslant N^2\left(2 - \sum_{h=1}^{\infty} \frac{1}{h^2}\right) = N^2\left(2 - \frac{\pi^2}{6}\right) \geqslant \frac{N^2}{3}.$$

LEMMA 4. *For sufficiently large N, there are at least $\frac{1}{2}N^2$ pairs of integers x, y with*

$$|x, y| \leqslant N, \quad F(x, y) \neq 0, \quad (x, y) = 1, \quad g\big(F(x, y)\big) \leqslant |F(x, y)|^{160\vartheta n}.$$

Proof. By Lemmas 2 and 3, there are at least $\frac{4}{3}N^2 - \frac{1}{3}N^2 = N^2$ pairs x, y with

$$|x, y| \leqslant N, \quad |F(x, y)| \geqslant N^{\frac{1}{2}}, \quad (x, y) = 1.$$

Hence, if Lemma 4 were false, there would be more than $N^2 - \frac{1}{2}N^2 = \frac{1}{2}N^2$ pairs x, y with

$$g\big(F(x, y)\big) \geqslant |F(x, y)|^{160\vartheta n} \geqslant N^{80\vartheta n},$$

and therefore

$$G(N) \geqslant N^{80\vartheta \cdot n \frac{1}{2}N^2} > N^{8\vartheta n(2N+1)^2},$$

in contradiction to Lemma 1.

Lemma 5. *For all x and y,*

$$|F(x, y)| \leqslant c_1 |x, y|^n.$$

Proof. Obvious with $c_1 = |a_0| + \ldots + |a_n|$.

Lemma 6. *For sufficiently large N, there are at least $\frac{1}{2}N^2$ pairs of integers x, y with*

$$(1) \qquad |x, y| \leqslant N, \quad F(x, y) \neq 0, \quad (x, y) = 1,$$

such that $|F(x, y)| = k_1 k_2$, where k_1 and k_2 are positive integers such that k_1 is divisible by at most c_2 different primes, and $k_2 \leqslant |F(x, y)|^{\frac{1}{7}}$.

Proof. We apply Lemma 4 with $\vartheta = 1/(1120n)$ and

$$k_2 = g\Big(F(x, y)\Big), \quad k_1 = \frac{|F(x, y)|}{k_2}.$$

k_1 and k_2 are positive integers, since $g\Big(F(x, y)\Big)$ is a positive integer which divides $F(x, y)$. By Lemma 4, for at least $\frac{1}{2}N^2$ pairs x, y satisfying (1),

$$k_2 \leqslant |F(x, y)|^{160\vartheta n} = |F(x, y)|^{\frac{1}{7}}.$$

The other factor k_1 is divisible only by prime numbers of the form P with either $P \leqslant \gamma$ or $P > N^{\vartheta}$. But there are at most γ primes of the first form, and, since by Lemma 5

$$|F(x, y)| \leqslant c_1 N^n,$$

there are at most $1200n^2$ different primes of the second form, which can divide $F(x, y)$, for sufficiently large N.

3. To conclude the proof we use the following generalization of the Thue-Siegel theorem*:

Lemma 7. *Suppose that x and y are integers with*

$$F(x, y) \neq 0, \quad (x, y) = 1,$$

that $P_1, P_2, \ldots, P_t$ are t different prime numbers, and that

$$Q(x, y) = P_1^{h_1} P_2^{h_2} \ldots P_t^{h_t}$$

* See K. Mahler, *Math. Annalen*, 108 (1933), 51, Satz 6, from which Lemma 7 is a trivial consequence, if $F(x, y)$ is irreducible. But Satz 6 remains true when $F(x, y)$, though reducible, has a non-vanishing discriminant, if only the representations of $k = 0$ are excluded; a proof for this generalized theorem and so for the general case of Lemma 7 will be published in the near future.

is the greatest product of powers of these primes which divides $F(x, y)$. Then the inequality

$$\frac{|F(x, y)|}{Q(x, y)} \leqslant |x, y|^{\frac{1}{2}n-1-\frac{1}{28}}$$

has at most c_3^{t+1} solutions in different pairs x, y.

Suppose now that k is a positive integer, for which $|F(x, y)| = k$ has at least one solution. Then, by Lemma 5,

$$c_1 |x, y|^n \geqslant k, \quad i.e. \quad |x, y| \geqslant \left(\frac{k}{c_1}\right)^{1/n},$$

so that $|x, y|$ cannot be too small. The integer $k = k_1 k_2$ is a product of two positive integers k_1 and k_2, of which k_1 has no other prime factors than $P_1, \ldots, P_t$, while k_2 is prime to $P_1, \ldots, P_t$; hence, in particular,

$$k_1 = Q(x, y), \quad k_2 = \frac{|F(x, y)|}{Q(x, y)}.$$

Suppose that
$$k_2 \leqslant k^{\frac{1}{7}},$$
so that
$$k_2 \leqslant c_1^{\frac{1}{7}} |x, y|^{\frac{1}{7}n}.$$

Since $n \geqslant 3$, we have

$$\tfrac{1}{2}n - 1 - \tfrac{1}{28} \geqslant \tfrac{1}{2}n - \tfrac{1}{3}n - \tfrac{1}{28} = \tfrac{1}{6}n - \tfrac{1}{28} \geqslant \tfrac{1}{7}n + (\tfrac{3}{6} - \tfrac{3}{7} - \tfrac{1}{28}) = \tfrac{1}{7}n + \tfrac{1}{28}.$$

Thus, when

$$k \geqslant c_1^{4n+1} = c_4, \quad i.e. \quad |x, y| \geqslant \left(\frac{k}{c_1}\right)^{1/n} \geqslant c_1^{4},$$

we get

$$c_1^{\frac{1}{7}} |x, y|^{-\frac{1}{28}} \leqslant 1, \quad \text{and} \quad k_2 \leqslant c_1^{\frac{1}{7}} |x, y|^{-\frac{1}{28}} |x, y|^{\frac{1}{7}n+\frac{1}{28}} \leqslant |x, y|^{\frac{1}{2}n-1-\frac{1}{28}}.$$

Hence Lemma 7 leads to

LEMMA 8. *If the positive integer k is larger than c_4, and if it can be written in the form $k = k_1 k_2$, where k_1 is divisible by only t different prime numbers, and where $k_2 \leqslant k^{\frac{1}{7}}$, then the equation $|F(x, y)| = k$ has not more than c_3^{t+1} different solutions x, y in relatively prime integers x and y.*

THEOREM 1. *For every sufficiently large positive u, there are at least $c_0 u^{2/n}$ different positive integers $k \leqslant u$, for which the equation $|F(x, y)| = k$ has at least one solution in relatively prime integers x and y.*

Proof. Suppose, in Lemma 6, that

$$N = \left(\frac{u}{c}\right)^{1/n}, \quad i.e. \quad |F(x, y)| \leqslant u \quad \text{for} \quad |x, y| \leqslant N.$$

Then it follows that there are at least

$$\tfrac{1}{2} c_1^{-1/n} u^{2/n}$$

different pairs of relatively prime integers x, y with $|x, y| \leqslant N$, for which

$$|F(x, y)| = k \neq 0$$

is a product of two positive integers $k = k_1 k_2$, such that k_1 is divisible by at most c_2 different primes, while $k_2 \leqslant k^{\frac{1}{7}}$. Hence, by Lemma 8, either $k \leqslant c_4$, or the number of different relatively prime solutions of $|F(x, y)| = k$ is not larger than $c_3^{c_2+1}$. Therefore, for sufficiently large u, there must be at least

$$\tfrac{1}{2} c_3^{-(c_2+1)} \cdot \tfrac{1}{2} c_1^{-1/n} u^{2/n}$$

different positive integers $k \leqslant u$, for which $|F(x, y)| = k$ has at least one solution in integers x, y with $(x, y) = 1$.

4. By a theorem of Siegel*, the inequality

$$0 < |F(x, y)| \leqslant u$$

has only $O(u^{2/n})$ solutions in integers x, y. Hence the number of integers k, with $1 \leqslant k \leqslant u$, which can be represented by $|F(x, y)|$, say the number $A(u)$, must also be $O(u^{2/n})$, and so Theorem 1 gives the exact order of this function and shows that $\liminf A(u)/u^{2/n} > 0$, while $\limsup A(u)/u^{2/n} < \infty$.

University of Manchester.

* As Prof. Siegel's proof has not been published, see K. Mahler, *Acta Math.*, 62 (1934), 92 *ff*.

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