ON THE INTEGERS OF THE FORM x^k+y^k

P. Erdös*.

In a previous paper, which I wrote in collaboration with Mahler†, it was proved that, if $f(x, y)$ is a binary form of degree $k \geqslant 3$ with integer coefficients and non-vanishing discriminant, then the number of integers not exceeding n representable by the binary form with positive x and y is $\Omega(n^{2/k})$. The proof was simple but not elementary. For the special form x^k+y^k, k odd, I have found an elementary proof which may be of some interest.

So far as I know, the first non-trivial estimation of the number of integers not exceeding n of the form x^k+y^k is due to Landau‡. He proved that for even k the number of integers in question is $\Omega(n^{2/k}/\log n)$. Later this result was improved by S. S. Pillai§ to $\Omega\{n^{2/k}/(\log n)^a\}$, $0<a<1$, in the cases $k\equiv 1, 2, 3 \pmod 4$. The method used in this paper is a refinement of that of Pillai.

First we prove five lemmas.

Lemma 1. *Let A and B be arbitrary positive integers, $A<B$. Write*

$$(1)\qquad x^k+(A-x)^k=y^k+(B-y)^k,\quad 0<x<\tfrac{1}{2}A,\quad 0<y<\tfrac{1}{2}B.$$

Then y is a convex function of x.

Proof‖. We note first that y is an increasing function of x, since the left-hand side of (1) is a decreasing function of x, while the right-hand side is a decreasing function of y. Considering y as a function of x and B, we obtain

$$\frac{\partial y}{\partial B}=\frac{1}{1-(y/B-y)^{k-1}}.$$

Differentiating this equation with respect to x, we obtain

$$\frac{\partial^2 y}{\partial B\,\partial x}=\frac{1}{\{1-(y/B-y)^{k-1}\}^2}(k-1)\left(\frac{y}{(B-y)}\right)^{k-2}\frac{B}{(B-y)^2}\frac{\partial y}{\partial x}.$$

* Received 24 February, 1939; read 23 March, 1939.

† P. Erdös and K. Mahler, *Journal London Math. Soc.*, 13 (1938), 134–139.

‡ E. Landau, *Journal London Math. Soc.*, 1 (1926), 72–74.

§ S. S. Pillai, *Journal London Math. Soc.*, 3 (1928), 56–61.

‖ This proof is due to Dr. W. Strodt.

Hence $\frac{\partial}{\partial B}\left(\log\frac{\partial y}{\partial x}\right)$ increases with x for any value of B. Integrating with respect to B, from A to $B_0 > A$, we conclude that

$$\log\frac{\partial y}{\partial x}\Big|_A^{B_0}$$

increases with x. Since $y = x$ when $B = A$, this implies that

$$\frac{\partial y}{\partial x}\Big|_{B=B_0}$$

increases with x, so that (1) defines as a convex function of x.

LEMMA 2. *The number of solutions in integers x and y of* (1) *is less than* $7A^{\frac{2}{3}}$.

Proof. First we show that, if (1) is solvable, $2A > B$. It is evident that both $f(A, x) = x^k+(A-x)^k$ and $f(B, y) = y^k+(B-y)^k$ are monotonously decreasing for $0 < x < \frac{1}{2}A$, $0 < y < \frac{1}{2}B$, and that $f(A, u) < f(B, u)$. Thus, if (1) holds, $y > x$, $A-x > B-y$, i.e. $2A > B$.

Let now (x_1, y_1), (x_2, y_2), ..., (x_r, y_r) be the solutions of (1). From Lemma 1 it follows that

$$\frac{y_{i+1}-y_i}{x_{i+1}-x_i} > \frac{y_i-y_{i-1}}{x_i-x_{i-1}}. \tag{2}$$

We now split the (x_i, y_i)'s into two classes. In the first class we put the (x_i, y_i) for which one of the equations $y_{i+1}-y_i > 2A^{\frac{1}{3}}$, $x_{i+1}-x_i > 2A^{\frac{1}{3}}$ holds, and in the second class all the other (x_i, y_i). Obviously the number of the (x_i, y_i) of the first class is less than $2A^{\frac{2}{3}}$. Thus, if the result is false, the second class contains at least $5A^{\frac{2}{3}}(x_i, y_i)$. Thus we obtain from (2) that there are at least $5A^{\frac{2}{3}}$ different fractions u_i/v_i with $u_i \leqslant 2A^{\frac{1}{3}}$, $v_i \leqslant 2A^{\frac{1}{3}}$, an obvious contradiction.

LEMMA 3. *Let $k = r_1^{\gamma_1} r_2^{\gamma_2} \dots r_j^{\gamma_j}$, where the r's are odd primes. Then all prime factors p, $(p, k) = 1$, of*

$$\frac{x^k+y^k}{x+y}, \quad (x, y) = 1,$$

are of the form $2r_1 r_2 \dots r_j d+1$.

This result is well known*.

LEMMA 4. *Denote*† $\prod_{\substack{p^\alpha \| m \\ p \equiv 1 \ (\mathrm{mod}\ r_1 r_2 \dots r_j)}} p^\alpha$ *by* $\psi(m)$. *Then the number of integers* $m \leqslant n$ *with* $(m, k) = 1$ *and* $\psi(m) < m^{\frac{1}{10}}$ *is greater than* $c_1 n$, *where* c_1 *depends only on* k.

Proof. Consider the integers not exceeding n of the form pa, with p prime, $p > n^{\frac{10}{11}}$, $a < n^{\frac{1}{11}}$, $(a, k) = 1$, $p \not\equiv 1 \bmod (r_1 r_2 \dots r_j)$. They obviously satisfy the requirements of the lemma. We estimate the number β of these integers. Denote by $\phi(k, d)$ the number of integers not exceeding d and relatively prime to k. Then

$$\beta = \sum_{\substack{p \not\equiv 1 \ (\mathrm{mod}\ r_1 r_2 \dots r_j) \\ n \geqslant p > n^{\frac{10}{11}}}} \phi\left(k, \frac{n}{p}\right).$$

By the sieve of Eratosthenes, we get‡

$$\phi(k, d) > d \prod_{P | k} \left(1 - \frac{1}{P}\right) - 2^{\nu(k)};$$

thus
$$\beta > \prod_{P | k} \left(1 - \frac{1}{P}\right) \sum_{\substack{p \not\equiv 1 \bmod (r_1 r_2 \dots r_j) \\ n > p > n^{\frac{10}{11}}}} \frac{n}{p} - \pi(n)\, 2^k,$$

where $\pi(n)$ denotes the number of primes not exceeding n. But, by the prime number theorem or by a more elementary result,

$$\sum_{\substack{p \not\equiv 1 \bmod (r_1 r_2 \dots r_j) \\ n > p > n^{\frac{10}{11}}}} \frac{1}{p} > c_2, \qquad \pi(n) = o(n);$$

hence
$$\beta > c_2 n \prod \left(1 - \frac{1}{r_i}\right) - o(n) > c_1 n,$$

which proves the lemma.

LEMMA 5. *Let* $a_1 < a_2 \dots < a_t < m$ *be integers with* $t > c_3 m$, *then*§

$$\sum_{i=1}^{t} \phi(a_i) > c_4 m^2.$$

---

* L. Euler, *Comm. Arith. Coll.* (Petropoli, 1849), (I), 50 and (II), 523.

† $p^\alpha \| m$ means that $p^\alpha | m$ but $p^{\alpha+1} \nmid m$.

‡ $\nu(k)$ denotes the number of different prime factors of k.

§ $\phi(a_i)$ denotes Euler's ϕ-function.

Proof. First we show that the number of integers s not exceeding m for which $\phi(s) < c_5 m$ is, for suitable c_5, less than $\frac{1}{2}c_3 m$. Obviously

$$\prod_{v=1}^{m} \phi(v) = m! \prod_{p \leqslant m} \left(1-\frac{1}{p}\right)^{[m/p]} > \frac{m^m}{e^m} \prod_{p \leqslant m} \left(1-\frac{1}{p}\right)^{m/p}$$

$$> \frac{m^m}{e^m} \prod_{p=1}^{\infty} \left(1-\frac{c_6}{p^2}\right)^m > m^m c_7{}^m.$$

But if our result is not true we should have

$$\prod_{v=1}^{m} \phi(v) < m^m c_5^{\frac{1}{2}c_3 m},$$

which is impossible if $c_5^{\frac{1}{2}c_3} < c_7$.

Thus we obtain

$$\sum_{i=1}^{l} \phi(a_i) > \frac{c_3 c_5}{2} m^2 = c_4 m^2,$$

which proves the lemma.

THEOREM. *The number of integers not exceeding n of the form x^k+y^k, where $k \geqslant 3$ is odd and $(x, y)=1$, is greater than $c_8 n^{2/k}$.*

Proof. Denote by $a_1 < a_2 < \dots < a_l$ the integers a with $2 < a < n^{1/k}$, $(a, k)=1$ and $\psi(a) < a^{\frac{1}{6}}$. Consider the integers

$$x^k+y^k \tag{3}$$

with $x+y=a_i$, $(x, y)=1$, $x < \frac{1}{2}a_i$ $(i=1, 2, \dots, l)$. These are obviously all less than n.

The number γ of these integers, not necessarily all different, is equal to

$$\tfrac{1}{2} \sum_{i=1} \phi(a_i) > c_9 n^{2/k},$$

by Lemmas 4 and 5.

We now estimate the number δ of solutions of

$$x^k+y^k = u^k+v^k, \tag{4}$$

with $\quad x+y=a_i, \quad (x, y)=1, \quad u+v=a_j, \quad (u, v)=1,$

$$i \leqslant j; \quad u, j=1, 2, \dots, l; \quad x \leqslant \tfrac{1}{2}a_i, \ u \leqslant \tfrac{1}{2}a_j.$$

Write (4) in the form

$$\psi(a_i)\frac{a_i}{\psi(a_i)}\frac{x^k+y^k}{x+y}=\psi(a_j)\frac{a_j}{\psi(a_j)}\frac{u^k+v^k}{u+v}. \tag{5}$$

By Lemma 3, (5) is possible only if

$$\frac{a_i}{\psi(a_i)}=\frac{a_j}{\psi(a_j)},$$

which means that, for fixed a_i, there are at most

$$\frac{n^{1/k}}{a_i/\psi(a_i)}<\frac{n^{1/k}}{a_i^{\frac{8}{15}}}$$

possible values for a_j; thus, by Lemma 2, the number δ_i of solutions of (5) for fixed a_i is less than

$$7a_i^{\frac{1}{3}}\frac{n^{1/k}}{a_i^{\frac{8}{15}}}<7\frac{n^{1/k}}{a_i^{\frac{1}{5}}}.$$

Hence, finally,

$$\delta=\sum_{i=1}\delta_i<7n^{1/k}\sum_{i\leqslant n^{1/k}}\frac{1}{i^{\frac{1}{5}}}<100n^{2/k-1/(5k)}. \tag{6}$$

Obviously the number of different integers represented by (4) is not less than*

$$\gamma-\delta>c_9 n^{2/k}-100n^{\frac{9}{5k}}>c_8 n^{2/k},$$

which proves the theorem.

By similar but slightly more complicated arguments we can prove that the number of integers not exceeding n of the form x^k+y^k, $x\geqslant y>0$, is equal to

$$\tfrac{1}{2}\sum_{x<n^{1/k}}(n-x^k)^{1/k}+o(n^{2/k}).$$

From this result it evidently follows that the number of integers m not exceeding n for which the equation $m=x^k+y^k$, $x\geqslant y>0$, has more than one solution is $o(n^{2/k})$.

The University,
Manchester.

---

* Denote by $f(m)$ the number of times that m is represented by (3). Then

$$\sum_{m=1}^{n}f(m)=\gamma \quad\text{and}\quad \sum_{m=1}^{n}\binom{f(m)}{2}=\delta \quad [\text{if } f(m)=1,\ \binom{f(m)}{2}=0];$$

thus it is clear that $\displaystyle\sum_{f(m)\neq 0}1\geqslant\gamma-\delta.$