ON THE REPRESENTATION OF AN INTEGER AS THE SUM OF k k-TH POWERS

PAUL ERDÖS*.

[*Extracted from the Journal of the London Mathematical Society, Vol.* 11, 1936.]

1. Let $f(m)$ denote the number of representations of m as the sum of k k-th powers of non-negative integers. Hardy and Littlewood† conjectured ("Hypothesis K") that $f(m) = O(m^{\epsilon})$ for every $\epsilon > 0$. In the opposite direction, Chowla has recently proved‡ that, for fixed $k \geqslant 5$, $f(m) \neq O(1)$. In this note I give a simple proof that, for an infinity of m,

$$f(m) > e^{c_1 (\log m / \log\log m)}, \tag{1}$$

where c_1 (as also c_2, ...) is a positive number depending only on k§.

Dr. Mahler has just proved that, for $k = 3$, $f(m^{12}) > c_2 m$, which shows that Hypothesis K is false for $k = 3$.

2. We first suppose that k is odd.

LEMMA 1. *If* $p \nmid k$, *and* $(p-1, k) = 1$, *then for every* $x \not\equiv 0 \pmod p$ *there exists exactly one* $y \pmod{p^k}$ *such that* $y^k \equiv x \pmod{p^k}$.

Proof. It suffices to prove that, if $y_1 y_2 \not\equiv 0 \pmod p$ and $y_1 \not\equiv y_2 \pmod{p^k}$, then $y_1^k \not\equiv y_2^k \pmod{p^k}$. Hence it suffices to prove that $z^k \equiv 1 \pmod{p^k}$ implies $z \equiv 1 \pmod{p^k}$. This is clear, since $z^{p^k - p^{k-1}} \equiv 1 \pmod{p^k}$ and $(k, p^k - p^{k-1}) = 1$.

* Received 10 December, 1935; read 12 December, 1935.

† *Math. Zeitschrift*, 23 (1925), 1–37.

‡ *Indian Physico-Mathematical Journal*, 6 (1935), 65–68.

§ Since writing this paper, I have heard from Prof. Chowla that he has also proved (1).

Let $p_1, p_2, \ldots, p_r$ be consecutive primes greater than k for which $(p-1, k) = 1$. Let $A = p_1 p_2 \ldots p_r$, $n = A^k$, $B \mid A$, $A = BC$. Let S_B denote the number of solutions of

$$x_i \leqslant n, \quad x_i \equiv 0 \pmod{B} \quad (i = 1, 2, \ldots, k), \tag{2}$$

$$x_1{}^k + \ldots + x_k{}^k \equiv 0 \pmod{n}, \tag{3}$$

$$(x_1{}^k + \ldots + x_{k-1}^k, C) = 1, \tag{4}$$

in non-negative integers $x_1, \ldots, x_k$.

LEMMA 2. $$S_B > \frac{c_3 n^{k-1}}{\log p_r}.$$

Proof. For each of $x_1, \ldots, x_{k-2}$ there are n/B values to satisfy (2). When $x_1, \ldots, x_{k-2}$ have been chosen, there are $(n/B) \prod_{p \mid C} (1-p^{-1})$ values for x_{k-1} to satisfy (2), (4). When $x_1, x_2, \ldots, x_{k-1}$ have been chosen, x_k is uniquely determined mod BC^k by (2), (3), and so can be given n/BC^k values.

Hence $$S_B \geqslant \frac{n^k}{B^k C^k} \prod_{p \mid C} (1-p^{-1}) > \frac{c_3 n^{k-1}}{\log p_r}.$$

To prove (1), we now observe that the number of solutions of

$$x_i \leqslant n, \quad x_1{}^k + \ldots + x_k{}^k \equiv 0 \pmod{n} \tag{5}$$

is at least $$\sum_{B \mid A} S_B > \frac{c_3 2^r n^{k-1}}{\log p_r},$$

since the same value of x_k cannot arise from two different B's. Hence there is an $m \leqslant kn^k$ which has at least

$$\frac{c_3 2^r n^{k-1}}{\log p_r} \frac{1}{kn^{k-1}}$$

representations as the sum of k k-th powers. Now, by the prime number theorem for arithmetic progressions, $p_r < c_4 r \log r$, and

$$\log n = k (\log p_1 + \ldots + \log p_r) < c_5 r \log r,$$

so that $$r > c_6 \frac{\log n}{\log \log n}.$$

Hence m has at least $e^{c_1 (\log n / \log \log n)}$ representations as the sum of k k-th powers, which establishes (1) for odd k.

3. We now deal with the case in which k is even and greater than 2. It is easily seen (as in the proof of Lemma 1) that, if $p+k$ and

$(p-1, k) = 2$, every k-th power residue (mod p^k) prime to p is also a quadratic residue, and conversely.

LEMMA 3. *If C is a product of different primes, each of which satisfies $p \nmid k$, $p \equiv 3 \pmod 4$, $(p-1, k) = 2$, then the number of solutions of $x^k + y^k \equiv a \pmod{C^k}$, where $(a, C) = 1$, is*

$$C^k \prod_{p \mid C} (1+p^{-1}).$$

Proof. We shall prove that the number in question is the same as the number of solutions of $u^2+v^2 \equiv a \pmod{C^k}$, and by a well-known result*, this has the value stated. It is sufficient to prove that the congruences

$$x^k + y^k \equiv a \pmod{p^k}, \tag{6}$$

$$u^2 + v^2 \equiv a \pmod{p^k} \tag{7}$$

have the same number of solutions for every $p \mid C$. First, by the above remark, there is a (1, 1) correspondence between the solutions of (6) with $p \nmid xy$, and of (7) with $p \nmid uv$. Secondly, for any $x \equiv 0 \pmod p$, and any $u \equiv 0 \pmod p$, the number of solutions of $v^2 \equiv a - u^2 \pmod{p^k}$ and $y^k \equiv a - x^k \pmod{p^k}$ is the same, since $a - u^2 \not\equiv 0 \pmod p$ and $a - x^k \not\equiv 0 \pmod p$. Similarly for any $y \equiv 0 \pmod p$ and $v \equiv 0 \pmod p$. This exhausts the possible cases, and the lemma is proved.

Let $p_1, \ldots, p_r$ be consecutive primes greater than k, for which $p \equiv 3 \pmod 4$ and $(p-1, k) = 2$, and let A, B, C, n be as in § 2. Let S_B' denote the number of solutions of (2), (3), and

$$(x_1^k + \ldots + x_{k-2}^k,\ C) = 1. \tag{4'}$$

For each of $x_1, \ldots, x_{k-3}$ there are n/B values to satisfy (2). For x_{k-2} there are at least $(n/B) \prod_{p \mid C} (1-2p^{-1})$ values to satisfy (4′). By Lemma 3, there are $C^k \prod_{p \mid C} (1+p^{-1})$ pairs of residues (mod C^k) for x_{k-1}, x_k to satisfy (3), and so

$$\frac{n^2}{B^2 C^k} \prod_{p \mid C} (1+p^{-1})$$

pairs of values.

Hence
$$S_B' \geqslant \frac{n^k}{B^k C^k} \prod_{p \mid C} (1+p^{-1})(1-2p^{-1})$$
$$> c_7 \frac{n^{k-1}}{(\log p_r)^2}.$$

The rest of the proof now proceeds as before.

---

* Dickson, *History of the theory of numbers*, 1 (1919), 225, note [21].

4. By the same method we can prove that, if $a_1, a_2, \ldots$ are integers, and $1/k_1+\ldots+1/k_l=1$, there are an infinity of m with more than

$$e^{c\,(\log m/\log\log m)}$$

representations in the form

$$a_1 x_1^{k_1}+a_2 x_2^{k_2}+\ldots+a_l x^{k_l} \quad (x_i \geqslant 0).$$

The University,
Manchester.

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