ON THE SUM $\sum_{t<N^{1/k}} d(N-t^k)$

by SEAN McDONAGH

(Received 12th July 1966)

Erdős (1) has proved the following result:

Theorem A. *Every integral polynomial $g(n)$ of degree $k \geqq 3$, represents for infinitely many integers n a $(k-1)$th power-free integer provided, in the case where k is a power of 2, there exists an integer n such that $g(n) \not\equiv 0 \pmod{2^{k-1}}$.*

He conjectures that by similar methods it should be possible to prove that every sufficiently large integer N is representable in the form

$$N = t^k + m, \tag{1}$$

where m is $(k-1)$th power-free, that is, that the polynomial $N-t^k$ represents, for large N and some integer t, $1 \leqq t < N^{\omega}$, where $\omega = 1/k$, a $(k-1)$th power-free integer. In his proof of Theorem A, Erdős uses the following theorem of Van der Corput (3).

Theorem B. *If $g(n)$ is an integral polynomial, l a positive integer and $x \geqq 3$, then there exists a constant c, $c > 1$, independent of x, such that*

$$\sum_{1 \leqq n \leqq x,\ g(n) \neq 0} d^l(|g(n)|) \leqq x(\log x)^c$$

where $d(n)$, as usual, denotes the number of divisors of a positive integer n.

As we will now show, a similar result does hold for the divisor function of $N-t^k$ summed over integers t satisfying $1 \leqq t < N^{\omega}$. We let $c_1, c_2, \ldots,$ denote positive constants independent of N. Using Van der Corput's method we prove

Theorem C. *If N, k and l are positive integers, with $N \geqq 2$ then there exists c_1 such that*

$$S = \sum_{1 \leqq t < N^{\omega}} d^l(N-t^k) \leqq N^{\omega}(\log N)^{c_1}.$$

If $k = 1$, the result is true since

$$\sum_{1 \leqq t < N} d^l(N-t) = \sum_{t<N} d^l(t) \leqq N(\log N)^{2^l-1}.$$

Suppose $k \geqq 2$. We then define $r_x(v)$ to be the number of solutions of the congruence

$$t^k \equiv N \pmod{v} \tag{2}$$

satisfying $1 \leqq t \leqq x$ and we write $r(v) = r_v(v)$. It is well known that $r(v)$ is a multiplicative function of v, that is, if $(v_1, v_2) = 1$, then $r(v_1v_2) = r(v_1)r(v_2)$. This is proved, for example, in Hardy and Wright (4), Theorem 122. Clearly, if $v \leqq x$, then

$$r_x(v) \leqq \frac{2x}{v} r(v).$$

In the proof of Theorem C we need the following Lemma.

Lemma. *If p denotes a prime then the function $r(p^\alpha)$ has the following properties*:

$$r(p^\alpha) < c_2, \text{ if } p \nmid N, \tag{3}$$

and, if $p^\beta \parallel N$, $\beta \geqq 1$, then

$$r(p^\alpha) \begin{cases} = p^{\alpha-1}, \text{ if } \alpha \leqq k \text{ and } \beta \geqq \alpha, \\ = 0, \text{ if } \alpha \leqq k \text{ and } \beta < \alpha, \\ = 0, \text{ if } \alpha > k,\ \beta < \alpha \text{ and } k \nmid \beta, \\ \leqq c_2 p^{\beta - \beta\omega}, \text{ if } \alpha > k,\ \beta < \alpha \text{ and } k | \beta, \\ \leqq p^{\alpha - \alpha\omega}, \text{ if } \alpha > k \text{ and } \beta \geqq \alpha. \end{cases} \tag{4}$$

Proof. (3) follows from consideration of indices. If $p \nmid N$, $p > 2$, let ind t, $t \not\equiv 0 \pmod p$ denote the index of $t \pmod{p^\alpha}$. If $t^\kappa = N \pmod{p^\alpha}$, then $t \not\equiv 0 \pmod p$ and k ind $t \equiv$ ind $N(\bmod\, p^{\alpha-1}(p-1))$ and so there are at most k values for ind t. Thus $r(p^\alpha) \leqq k$.

If $p \nmid N$ and $p = 2$, (3) is obvious if $\alpha \leqq 2$. If $\alpha > 2$ let $N \equiv (-1)^{\gamma_1} 5^{\gamma_2} \pmod{2^\alpha}$. If $t^\kappa \equiv N \pmod{2^\alpha}$, then $2 \nmid t$ and, if $t \equiv (-1)^{\delta_1} 5^{\delta_2} \pmod{2^\alpha}$, we must have $\delta_1 k = \gamma_1 \pmod 2$ and $\delta_2 k = \gamma_2 \pmod{2^{\alpha-2}}$. Hence there is one possible choice for δ_1, and, at most, k for δ_2. This establishes (3).

To prove (4), we first consider the case $\alpha \leqq k$. If $t^\kappa = N \pmod{p^\alpha}$, we must have $t \equiv 0 \pmod p$, since $N \equiv 0 \pmod p$. Hence $t^\kappa \equiv 0 \pmod{p^\kappa}$ and so $t^\kappa \equiv 0 \pmod{p^\alpha}$. If $\beta \geqq \alpha$, then $N \equiv 0 \pmod{p^\alpha}$ and $r(p^\alpha)$ is the number of integers t such that $1 \leqq t \leqq p^\alpha$ and $t \equiv 0 \pmod p$, that is $p^{\alpha-1}$. If $\beta < \alpha$ then $r(p^\alpha) = 0$, since $N \not\equiv 0 \pmod{p^\alpha}$.

When $\alpha > k$ we write $N = p^\beta N_0$ so that $p \nmid N_0$. If $\beta < \alpha$ and $k \nmid \beta$ then $t^\kappa \equiv p^\beta N_0 \pmod{p^\alpha}$ cannot have a solution because p divides t^κ to a power which, being a multiple of k, cannot be equal to β, making an equation $t^\kappa = p^\beta N_0 + ap^\alpha$ impossible for integral a. Such an equation is possible, if $\beta < \alpha$ and $k \mid \beta$, only if $p^\beta \parallel t^\kappa$. Writing $\beta = k\beta_0$ we see that if t satisfies $t^\kappa \equiv N \pmod{p^\alpha}$ then $t \equiv 0 \pmod{p^{\beta_0}}$. Hence, if $\beta < \alpha$ and $k \mid \beta$, the integers t, $1 \leqq t \leqq p^\alpha$, which satisfy $t^\kappa \equiv N \pmod{p^\alpha}$ are in the form $t = p^{\beta_0} y$, with $1 \leqq y \leqq p^{\alpha - \beta_0}$ and $y^\kappa \equiv N_0 \pmod{p^{\alpha-\beta}}$. By (3) there are less than

$$c_2 p^{\alpha-\beta_0} . p^{-(\alpha-\beta)} = c_2 p^{\beta - \beta\omega}$$

such integers. Finally, if $\alpha > k$ and $\beta \geqq \alpha$, then $N \equiv 0 \pmod{p^\alpha}$. Thus the only solutions of $t^\kappa \equiv N \pmod{p^\alpha}$ are those integers t which are divisible by $p^{\alpha\omega}$, if $k \mid \alpha$, or $p^{[\alpha\omega]+1}$, if $k \nmid \alpha$. There are less than $p^{\alpha-\alpha\omega}$ such integers $(\bmod\, p^\alpha)$ which establishes (4).

It follows from (4) that, if $p \mid N$, we have

$$r(p^\alpha) \leqq \begin{cases} p^{\alpha-1}, \text{ if } \alpha \leqq k, \\ c_2 p^{\alpha-\alpha\omega}, \text{ if } \alpha > k. \end{cases} \tag{5}$$

We write

$$S = \sum_{t<N^\omega} d^l(N-t^k) = \sum_{1 \leqq y \leqq N} d^l(y)T(y)$$

where

$$T(y) = \begin{cases} 1, \text{ if } y = N-t^k \text{ for some } t,\ 1 \leqq t < N^\omega, \\ 0, \text{ otherwise.} \end{cases}$$

Hence

$$\sum_{y<N} T(y) \leqq N^\omega$$

and, if $v < N^\omega$ we have

$$\sum_{y<N,\ y \equiv 0 \pmod{v}} T(y) = r_{N^\omega}(v) \leqq \frac{2N^\omega}{v} r(v).$$

Each y, $1 \leqq y \leqq N$, is uniquely decomposed in the form

$$y = p_1 p_2 \dots p_m v_1 v_2 \dots v_n,$$

where an empty product is defined to be 1. Here, if $m \neq 0$, p_j is prime and $p_j \geqq N^\omega$, $j = 1, 2, \dots, m$, while if $n \neq 0$, v_1 is the largest integer less than N^ω which divides y, and, in general, v_i is the largest integer less than N^ω which divides $y/p_1p_2\dots p_m v_1 v_2 \dots v_{i-1}$. Since $y \leqq N$ we have $m \leqq k$ and since at most one of the v's is less than $N^{\omega/2}$ we have $n \leqq 2k+1$. Thus

$$d^l(y) \leqq 2^{ml} d^l(v_1) d^l(v_2) \dots d^l(v_n) \leqq 2^{kl} \sum_{1 \leqq i \leqq n} d^{l(2k+1)}(v_i).$$

We may write

$$S = \sum_{n=0}^{2k+1} U_n$$

where U_n is the contribution to S of the y's with n v-factors. Thus

$$U_0 \leqq 2^{kl} \sum_{y=1}^{N} T(y) \leqq 2^{kl} N^\omega.$$

If $n > 0$, we have

$$U_n \leqq 2^{lk} \sum_{y=1}^{N}{}' \left(\sum_{i=1}^{n} \sum_{v_i=2}^{N^\omega} d^{l(2k+1)}(v_i) \right) T(y),$$

where the Σ' extends over the integers y, $1 \leqq y \leqq N$, having n v-factors, $v_1, v_2, \dots, v_n$. Therefore

$$U_n \leqq 2^{lk} \sum_{i=1}^{n} \sum_{v=2}^{N^\omega} d^{l(2k+1)}(v) \sum_{y=1}^{N}{}'' T(y),$$

where the Σ'' extends over the integers y, $1 \leqq y \leqq N$, having n v-factors and having v as the ith v-factor. Thus

$$U_n \leqq 2^{lk}(2k+1) \sum_{v=2}^{N^\omega} d^{l(2k+1)}(v) \sum_{\substack{y=1 \\ y \equiv 0 \pmod v}}^{N} T(y)$$

$$\leqq 2^{lk+1}(2k+1)N^\omega \sum_{v=2}^{N^\omega} \frac{d^{l(2k+1)}(v)r(v)}{v}$$

$$\leqq 2^{lk+1}(2k+1)N^\omega \prod_{p \leqq N^\omega} \left\{1+ \sum_{\alpha=1}^{\infty} \frac{d^{l(2k+1)}(p^\alpha)r(p^\alpha)}{p^\alpha}\right\}.$$

By (3), if $p \nmid N$, we have

$$\left\{1+ \sum_{\alpha=1}^{\infty} \frac{d^{l(2k+1)}(p^\alpha)r(p^\alpha)}{p^\alpha}\right\} \leqq \left\{1+ \sum_{\alpha=1}^{\infty} \frac{(\alpha+1)^{l(2k+1)}c_2}{p^\alpha}\right\} \leqq \left\{1+ \frac{c_3}{p}\right\}.$$

If $p \mid N$, we have, by (5), that

$$\left\{1+ \sum_{\alpha=1}^{\infty} \frac{d^{l(2k+1)}(p^\alpha)r(p^\alpha)}{p^\alpha}\right\} \leqq \left\{1+ \sum_{\alpha=1}^{k} \frac{(\alpha+1)^{l(2k+1)}}{p} + \sum_{\alpha=k+1}^{\infty} \frac{(\alpha+1)^{l(2k+1)}c_2}{p^{\alpha\omega}}\right\}$$

$$\leqq \left\{1+ \frac{1}{p}\left[\sum_{\alpha=1}^{k} (\alpha+1)^{l(2k+1)} + \sum_{\alpha=1}^{\infty} \frac{(\alpha+k+1)^{l(2k+1)}c_2}{2^{\alpha\omega}}\right]\right\} = \left\{1+ \frac{c_4}{p}\right\}.$$

Let $c_5 = \max(c_3, c_4)$. Then

$$U_n \leqq 2^{lk+1}(2k+1)N^\omega \prod_{p \leqq N^\omega} \left\{1+ \frac{c_5}{p}\right\}$$

$$\leqq 2^{lk+1}(2k+1)N^\omega \exp\left\{c_5 \sum_{p \leqq N^\omega} \frac{1}{p}\right\} \leqq 2^{lk+1}(2k+1)N^\omega(\log N)^{c_5}.$$

Finally, summing over n, Theorem C follows.

In the case $l = 1$, Erdős (2) has proved the following theorem which is stronger than Theorem B and which he uses to prove Theorem A.

Theorem D. *If $g(n)$ is an irreducible integral polynomial and $x \geqq 2$, there exists a constant c', independent of x, such that*

$$\sum_{n=1}^{x} d(|g(n)|) < c'x \log x.$$

If $\rho(u)$ denotes the number of solutions of the congruence

$$g(n) \equiv 0 \pmod u, \ 1 \leqq n \leqq u$$

then a powerful tool in the proof of Theorem D is the following relation (Erdős (2), Lemma 7),

$$\sum_{p \leqq x} \rho(p) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{6}$$

(6) is a consequence of the prime ideal theorem.

In order to attempt to prove Erdős' conjecture concerning the representability of every sufficiently large integer N as in (1), it is necessary to have more information about $\sum_{t<N^\omega} d(N-t^k)$, $k \geqq 3$, than is contained in Theorem C. Hooley (5) has given an asymptotic formula for $\sum_{|t|<N^{1/2}} d(N-t^2)$ but a similar estimate for $\sum_{t<N^\omega} d(N-t^k)$, $k>2$, would seem to be difficult.

Comparison of relation (6) with relations (3) and (4) would indicate that more information about $\sum_{p \leqq N^\omega,\, p \nmid N} r(p)$ than is at present available would be necessary in order to prove the conjecture of Erdős.

REFERENCES

(1) P. Erdős, Arithmetical properties of polynomials, *J. London Math. Soc.* **28** (1953), 416-425.

(2) P. Erdős, On the sum $\sum_{k=1}^{x} d(f(k))$, *J. London Math. Soc.* **27** (1952), 7-15.

(3) J. G. van der Corput, Une inégalité relative au nombres des diviseurs, *Proc. Kon. Ned. Akad. Wet. Amsterdam*, **42** (1939), 547-553.

(4) G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed. (Oxford, 1960).

(5) C. Hooley, On the representation of a number as the sum of a square and a product, *Math. Zeitschrift*, **69** (1958), 211-227.

University College
Galway