ON A RESULT OF CASSELS

R. T. WORLEY

(Received 5 February 1969)

Communicated by E. S. Barnes

Let α be an irrational algebraic number of degree k over the rationals. Let K denote the field generated by α over the rationals and let $\mathfrak{a}$ denote the ideal denominator of α. Then Cassels [3] has shown that for sufficiently large integral $N > 0$ distinctly more than half the integers n,

$$N < n \leqq N+[10^{-6}N]$$

are such that $(n+\alpha)\mathfrak{a}$ is divisible by a prime ideal $\mathfrak{p}_n$ which does not divide $(m+\alpha)\mathfrak{a}$ for any integer $m \neq n$ satisfying $N < m \leqq N+[10^{-6}N]$. The purpose of this note is to point out that minor modification of Cassel's proof enables the extension of the interval for n from $N < n \leqq N+[10^{-6}N]$ to $0 \leqq n \leqq N$, and to derive results on the proportion of values n, $0 \leqq n \leqq N$ for which the values $f(n)$ of a given integral polynomial in n are divisible by a prime $p > N$.

THEOREM. *The proportion* $\rho(\alpha, N)$ *of integers* n, $0 \leqq n \leqq N$, *for which* $(n+\alpha)\mathfrak{a}$ *is divisible by a prime ideal* $\mathfrak{p}_n$ *not dividing* $(m+\alpha)\mathfrak{a}$ *for integral* $m \neq n$, $0 \leqq m \leqq N$, *has the properties*

(i) $\liminf_{N\to\infty} \rho(\alpha, N) > \frac{1}{2}$.

(ii) $\liminf_{N\to\infty} \rho(\alpha, N) \geqq 1-\dfrac{1}{2k}+O(k^{-\frac{3}{2}})$ *as* $k \to \infty$.

PROOF. The proof is basically that of Cassels with $N \log N$ for M instead of $[10^{-6}N]$ and with the estimate cn^k as a lower bound for norm $\{(n+\alpha)\mathfrak{a}\}$ instead of cn^2. For simplicity we prove (i) and (ii) for $\sigma(\alpha, N)$ which denotes the proportion of integers $n, N < n \leqq N \log N$, for which $(n+\alpha)\mathfrak{a}$ is divisible by a prime ideal $\mathfrak{p}_n$ not dividing $(n+\alpha)\mathfrak{a}$ for integral $m \neq n$, $N < m \leqq N \log N$. Plainly

$$\liminf_{N\to\infty} \rho(\alpha, N) = \liminf_{N\to\infty} \sigma(\alpha, N).$$

As in Cassels' proof $\mathfrak{p}$ shall denote a prime ideal of K which is of the first degree and unambiguous i.e. $\mathfrak{p}^2$ does not divide $p = \text{norm}\, \mathfrak{p}$ and if

$\mathfrak{p} | (n+\alpha)\mathfrak{a}$ for any integer n then $(n+\alpha)\mathfrak{a}$ is not divisible by any $\mathfrak{p}' \neq \mathfrak{p}$ with norm $\mathfrak{p}' = p$. For any integer n,

$$(n+\alpha)\mathfrak{a} = \mathfrak{b} \prod_{\mathfrak{p}} \mathfrak{p}^{u(\mathfrak{p})} \tag{1}$$

where the $u(\mathfrak{p})$ are integers and $\mathfrak{b}$ contains all the factors of $(n+\alpha)\mathfrak{a}$ which are not $\mathfrak{p}$'s. Norm $\mathfrak{b}$ is bounded and norm $\{(n+\alpha)\mathfrak{a}\} > cn^k$ where $c > 0$ is independent of n provided n is large enough. Hence on taking logarithms

$$\sum u(\mathfrak{p}) \log p \geqq k \log n - C \tag{2}$$

where C is independent of n (n large enough).

Denote by $\mathfrak{S} = \mathfrak{S}_N$ the set of all n in the range $N < n \leqq N \log N$ with the property that

$$p^{u(\mathfrak{p})} < N \log N \tag{3}$$

for all $\mathfrak{p}$ in the factorization (1). An upper bound for the number $S = \rho N \log N$ of elements of $\mathfrak{S}$ is found as follows.

For any $\mathfrak{p}$ and integral $v > 0$ write

$$\phi(\mathfrak{p}^v, n) = \begin{cases} \log p & \text{if } \mathfrak{p}^v | (n+\alpha)\mathfrak{a} \\ 0 & \text{otherwise} \end{cases}$$

and

$$\sigma(n) = \sum \phi(\mathfrak{p}^v, n)$$

where the summation is over all $\mathfrak{p}$ and v with $p^v < N \log N$. Take $\varepsilon > 0$ arbitrarily — then $\log N > (1-\varepsilon) \log (N \log N)$ for sufficiently large N. From (2) and (3) we therefore obtain

$$\sigma(n) \geqq (k-\varepsilon) \log (N \log N)$$

for all $n \in \mathfrak{S}$ and

$$\sum_{n \in \mathfrak{S}} \sigma(n) \geqq (k-\varepsilon) S \log (N \log N) \tag{4}$$

for N sufficiently large.

Writing $\sigma(n) = \sigma_1(n) + \sigma_2(n) + \sigma_3(n)$ where σ_1, σ_2, σ_3 are the sums of $\phi(\mathfrak{p}^v, n)$ with p^v in the sets

$$\sigma_1 : v > 1, p^v < N \log N$$
$$\sigma_2 : v = 1, (N \log N)^{\frac{1}{2}} \leqq p < N \log N$$
$$\sigma_3 : v = 1, p < (N \log N)^{\frac{1}{2}}$$

we obtain, as in Cassels' proof, that

$$\sum_{n \in \mathfrak{S}} \sigma_1(n) = O(M \log M), \tag{5}$$

https://doi.org/10.1017/S1446788700006376 Published online by Cambridge University Press

(6) $$\sum_{n \in \mathfrak{S}} \sigma_2(n) \leqq (\tfrac{1}{2}+o(1)) M \log M$$

and

(7) $$\sum_{n \in \mathfrak{S}} (\sigma_3(n))^2 \leqq (\tfrac{3}{8}+o(1)) M \log^2 M$$

where we have used M to denote $N \log N$ for simplicity and where $o(1)$ refers to the limit as $N \to \infty$.

Combining (4), (5) and (6) yields

(8) $$\sum_{n \in \mathfrak{S}} \sigma_3(n) \geqq ((k-\varepsilon)\rho - \tfrac{1}{2}+o(1)) M \log M.$$

Then either $(k-\varepsilon)\rho < \frac{1}{2}+o(1)$ or

$$((k-\varepsilon)\rho - \tfrac{1}{2}+o(1))^2 M^2 \log^2 M \leqq (\rho M)(\tfrac{3}{8}+o(1)) M \log^2 M,$$

from which it follows that for sufficiently large N,

(9) $$\rho \leqq \frac{k-\varepsilon+\frac{3}{8}}{2(k-\varepsilon)^2} + \frac{1}{2(k-\varepsilon)^2} (\tfrac{9}{64}+\tfrac{3}{4}(k-\varepsilon)+o(1)k^2)^{\frac{1}{2}}$$

where $o(1)$ refers to the limit as $N \to \infty$. But, as in Cassels' proof, $\sigma(\alpha, N) \geqq 1-\rho$, so the desired results follow from (9).

Corollary. *Let $f(n)$ denote a polynomial in n with integral coefficients and leading coefficients* 1, *irreducible over the rationals, and let $\rho(f, N)$ denote the number of integers n, $0 \leqq n \leqq N$, for which $f(n)$ is divisible by a prime $p > N$. Then*

(i) $\liminf_{N\to\infty} \rho(f, N) > \frac{1}{2}$.

(ii) $\liminf_{N\to\infty} \rho(f, N) \geqq 1-(1/2k)+O(k^{-\frac{3}{2}})$ *as $k \to \infty$ where k denotes the degree of f.*

Proof. Apply the theorem to $-\alpha$, where α is a root of f, noting that $f(n) = \text{norm } (n-\alpha)$.

It should be pointed out the bound on $\rho(f, N)$ seems to be much weaker than the probable bound. The argument, however implausible it may sound, that the numbers $f(0), f(1), \cdots, f(N)$ are evenly distributed amongst the numbers $1, 2, \cdots N^k$ with respect to divisibility by primes greater than N leads to the conclusion that $\lim_{N\to\infty} \rho(f, N) = 1-\rho(k)$ where $\rho(k)$ is defined as follows. Let $\psi(x, y)$ be the number of positive integers $\leqq x$ free of prime divisors $> y$ — then de Bruijn [1], Buchstab [2] Chowla and Vijayaraghavan [4] and Ramaswami [5] have shown that

$$\lim_{y\to\infty} y^{-k}\psi(y^k, y) = \rho(k)$$

where $\rho(k)$ can be calculated in an inductive manner and $\rho(k) = o(k^{-n})$ for

https://doi.org/10.1017/S1446788700006376 Published online by Cambridge University Press

all positive integers n. A limited amount of computing indicated that $1-\rho(2)$ is the correct limit for $\rho(f, N)$ for $f(n) = n^2+n+1$ and that $1-\rho(3)$ was a possible limit for $\rho(f, N)$ for $f(n) = n^3+n^2+n+2$.

References

[1] N. G. de Bruijn, 'On the number of positive integers $\leqq x$ and free of prime divisors $> y$', *Proc. K. Nederl. Akad. Wetensch.* 54 (1951) 50—60.

[2] A. A. Buchstab, 'On those numbers in an arithmetic progression all prime factors of which are small in magnitude', *Doklady Akad. Nauk SSSR* 67 (1949) 5—8.

[3] J. W. S. Cassels, 'Footnote to a note of Davenport and Heilbronn', *J. Lond. Math. Soc.* 36 (1961) 177—184.

[4] S. Chowla and T. Vijayaraghavan, 'On the largest prime divisors of numbers', *J. Ind. Math. Soc.* (N.S.) 11 (1947) 31—37.

[5] V. Ramaswami, 'The number of positive integers $< x$ and free of prime divisors $> x^c$, and a problem of S. Pillai, *Duke Math. J.* 16 (1949) 99—109.

Monash University
Clayton, Vic. 3168