SOME REMARKS ON NUMBER THEORY

BY

P. ERDÖS

ABSTRACT

This note contains some disconnected minor remarks on number theory.

I. Let

$$|z_j| = 1, \ 1 \leqq j < \infty \tag{1}$$

be an infinite sequence of numbers on the unit circle. Put

$$s(k,n) = \sum_{j=1}^{n} z_j^k, \quad A_k = \limsup_{k=\infty} |s(k,n)|$$

and denote by B_k the upper bound of the numbers $|s(k,n)|$. If $z_j = e^{2\pi i j \alpha}$ $\alpha \neq 0$ then all the A_k's are finite and if the continued fraction development of α has bounded denominators then $A_k < ck$ holds for every k ($c, c_1, \cdots$ will denote suitable positive absolute constants not necessarily the same at every occurrence). In a previous paper [2] I observed that for every choice of the numbers (1), $\limsup_{k=\infty} B_k = \infty$, but stated that I can not prove the same result for A_k. I overlooked the fact that it is very easy to show the following

THEOREM. *For every choice of the numbers* (1) *there are infinitely many values of* k *for which*

$$A_k > c_1 \log k. \tag{2}$$

To prove (2) observe that it immediately follows from the classical theorem of Dirichlet that if $|y_i| = 1, 1 \leqq i \leqq n$ are any n complex numbers, then there is an integer $1 \leqq k \leqq 10^n$ so that ($R(z)$ denotes the real part of z)

$$R(y_i^k) > \frac{1}{2}, \quad 1 \leqq i \leqq n. \tag{3}$$

Apply (3) to the n numbers $z_{rn+1}, \cdots, z_{(r+1)n}$, $0 \leqq r < \infty$. We obtain that there is a $k \leqq 10^n$ for which there are infinitely many values of r so that

$$R\left(\sum_{l=1}^{n} z_{rn+l}^k\right) > \frac{n}{2}. \tag{4}$$

Received February 10, 1965.

(4) immediately implies $A_k \geqq n/4$, thus by $k \leqq 10^n$ (2) follows, and our Theorem is proved.

Perhaps $A_k \geqq ck$ holds for infinitely many values of k*. In this connection I would like to mention the following question: Denote by $f(n,c)$ the smallest integer so that if $|z_i| \geqq 1$, $1 \leqq i \leqq n$ are any n complex numbers, there always is an integer $1 \leqq k \leqq f(n,c)$ for which

$$\left| \sum_{i=1}^{n} z_i^k \right| \geqq c.$$

A very special case of the deep results of Turán [8] is that $f(n,1) = n$. Rényi and I [3] obtain some crude upper bounds for $f(n,c,)$ if $c > 1$, but our results are too weak to improve (2).

II. Is it true that to every $\varepsilon > 0$ there is a k so that for $n > n_0$ every interval $(n, n(1+\varepsilon))$ contains a power of a prime $p_i \leqq p_k$? It easily follows from the theorem of Dirichlet quoted in I that the answer is negative for every $\varepsilon < 1$, since the above theorem implies that to every $\eta > 0$ there are infinitely many values of m so that all primes $p_i \leqq p_k$ have a power in the interval $(m, m(1+\eta))$ and then the interval $(m(1+\eta), 2m)$ must be free of these powers. Let us call an increasing function $g(n)$ good if to every $\eta > 0$ there are infinitely many values of n so that all the primes $p_i \leqq g(n)$ have a power in $(n, n(1+\eta))$. It easily follows from the theorem of Dirichlet and $\pi(x) < cx/\log x$ that if

$$g(n) = o\left(\frac{\log\log n \cdot \log\log\log n}{\log\log\log\log n}\right) \tag{5}$$

then $g(n)$ is good. I leave the straightforward proof to the reader. I can obtain no non-trivial upper bound for $g(n)$.

Let $1 < \alpha < 2$ and put

$$A(n,\alpha) = \sum{}' 1/p \tag{6}$$

where in $\sum'$ the summation is extended over all primes p for which $n < p^\beta < \alpha n$ for some integer $\beta \geqq 1$. (5) and $\sum_{p<y} 1/p = \log\log\, y + 0(1)$ implies that for infinitely many n

$$A(n,\alpha) > \log\log\log\log n + 0(1). \tag{7}$$

Now we are going to prove

$$\liminf_{n=\infty} A(n,\alpha) = 0. \tag{8}$$

To prove (8) we shall show that to every $\varepsilon > 0$ there are arbitrarily large values of n for which

$$A(n,\alpha) < \varepsilon. \tag{9}$$

* By a remark of Clunie, we certainly must have $c \leqq 1$. Added in proof: Clunie proved $f(n,c) < g(c)\, n \log n$, $A_k > c k^{\frac{1}{2}}$.

Let $k = k(\varepsilon)$ be sufficiently large. Consider $\sum' A(2^l, \alpha)$ where in $\sum'$ the summation is extended over those $l, 1 \leqq l \leqq x$ for which the interval $(2^l, \alpha 2^l)$ does not contain any powers of the primes $p_i, 1 \leqq i \leqq k$. Put

$$D(\alpha, k) = \prod_{i=2}^{k} \left(1 - \frac{\log(1+\alpha)}{\log p_k}\right).$$

Let $\alpha_1, \cdots, \alpha_k$ be positive numbers which are such that for every choice of the rational numbers $r_1, \cdots, r_k$ not all 0, $\sum_{i=1}^{k} r_i \alpha_i$ is irrational. The classical theorem of Kronecker-Weyl states that if we denote by $x_n, 1 \leqq n < \infty$ the point in the k dimensional unit cube whose coordinates are the fractional parts of $n\alpha_i, 1 \leqq i \leqq k$ then the sequence x_n is uniformly distributed in the k dimensional unit cube. From this theorem is easily follows that the number of summands in $\sum' A(2^l, \alpha)$ is $(1 + o(1)) x D(\alpha, k)$. Thus to prove (9) it will suffice to show that for every sufficiently large x

$$\sum' A(2^l, \alpha) < \frac{\varepsilon}{2} D(\alpha, k) x. \tag{10}$$

We evidently have

$$\sum' A(2^l, \alpha) = \sum_{p_k < p_j \leqq 2^x} \frac{u(j, x)}{p_j}$$

where $u(j, x)$ denotes the number of those integers $1 \leqq l \leqq x$ for which the interval $(2^l, \alpha 2^l)$ contains a power of p_j, but does not contain any power of p_i, $1 \leqq i \leqq k$. For fixed j we obtain again from the Kronecker-Weyl theorem

$$u(j, x) = (1 + o(1)) D(\alpha, k) \frac{\log(1+\alpha)}{\log p_j} x. \tag{11}$$

Put

$$\sum' A(2^l, \alpha) = \sum_{p_k < p_j \leqq 2^x} \frac{u(j, x)}{p_j} = \sum_1 + \sum_2 \tag{12}$$

where in $\sum_1$ $p_k < p_j \leqq T = T(k, \varepsilon)$ and in $\sum_2$ $T < p_j \leqq 2^x$. From (11) and (12) we have for sufficiently large k

$$\sum_1 < (1 + o(1)) \, D(\alpha, k) \, \log(1+\alpha) \, x \sum_{j=k+1}^{\infty} 1 / p_j \log p_j < \frac{\varepsilon}{4} D(\alpha, k) x \tag{13}$$

since $\sum 1 / p_j \log p_j$ converges. To estimate $\sum_2$ observe that there are $[x \log 2 / \log p_j]$ powers of p_j not exceeding 2^x, thus for every j and x

$$u(j, x) \leqq x \log 2 / \log p_j. \tag{14}$$

From (14) we have for sufficiently large $T = T(k, \varepsilon_p c)$

$$\sum_2 \leqq x \log 2 \sum_{p_j > T} 1 / p_j \log p_j < \frac{\varepsilon}{4} D(\alpha, k) x \tag{15}$$

(10) follows from (12) (13) and (15). By a refinement of this method one could perhaps prove that for infinitely many n

$$A(n,\alpha) < c\,/\,\text{logloglog}\; n.$$

Using the classical result of Hoheisel [6]

$$\pi(x + x^{1-\varepsilon}) - \pi(x) > cx^{1-\varepsilon}/\log x$$

we obtain by a simple computation that for all n

$$c_1\,/\,\text{loglog}\; n < A(n,\alpha) < c_2\; \text{logloglog}\; n.$$

III Sivasankaranarayana, Pillai and Szekeres proved that for $1 \leqq l \leqq 16$ any sequence of l consecutive integers always contains one which is relatively prime to the others, but that this is in general not true for $l = 17$, the integers $2184 \leqq t \leqq 2200$, giving the smallest counter example. Later A. Brauer and Pillai [1] proved that for every $l \geqq 17$ there are l consecutive integers no one of which is relatively prime to all the others.

An integer n is said to have property P if any sequence of consecutive integers which contains n also contains an integer which is relatively prime to all the others. A well known theorem of Tchebicheff states that there always is a prime between m and $2m$ and from this it easily follows that every prime has property P. Some time ago I [5] proved that there are infinitely many composite numbers which have property P. Denote in fact by $u(n)$ the least prime factor of n.n clearly has property P if there are primes p_1 and p_2 satisfying

$$(16) \qquad n - u(n) < p_1 < n; \qquad n < p_2 < n + u(n).$$

One would expect that it is not difficult to give a simple direct proof that infinitely many composite numbers satisfy (16), but I did not succeed in this. In fact I proved that there are infinitely many primes p for which $p-1$ satisfies (16) but the proof uses the Walfisz-Siegel theorem on primes in arithmetic progressions and Brun's method [5].

In fact I can prove the following

THEOREM. *The lower density α_p of the integers having property P exists and is positive.*

We will only give a brief outline of the proof, since it seems certain that the density of the integers having property P exists and our method is unsuitable to prove this fact; also our proof is probably unnecessarily complicated.

To prove our Theorem we need two lemmas.

LEMMA 1. *For a sufficiently small $\varepsilon > 0$ we have ($p_1 = 2 < p_2 < \cdots$ is the sequence of consecutive primes):*

$$\Sigma_1(p_{i+1} - p_i) > c_1 x$$

where in Σ_1 *the summation is extended over those* $p_{i+1} < x$ *for which*

(17) $$\varepsilon \log x < p_{i+1} - p_i < (1 - \varepsilon) \log x.$$

It is easy to prove the Lemma by the methods used in [4]

LEMMA 2. *Put* $N_k = \Pi_{p \leq k}\, p$ *and let* $1 = a_1 < a_2 < \cdots < a_{\phi(N_k)} = N_k - 1$ *be the integers relatively prime to* N_k. *Then for sufficiently large* k

$$\Sigma_2(a_{i+1} - a_i) < N_k / k^{\frac{1}{2}}$$

where in Σ_2 *the summation is extended over those* i's *for which* $a_{i+1} - a_i \geqq k/2$.

The Lemma can be deduced from [6] without any difficulty.

Now we can prove our Theorem. It is easy to see that if n does not have property P then it is included in a unique maximal interval of consecutive integers no one of which is relatively prime to the others. Denote these intervals of consecutive integers by $I_1, I_2 \cdots$ where I_1 are the integers $2184, 2185 \cdots 2200$. Let I_r be the last such interval which contains integers $\leqq x$. $|I|$ denotes the length of the interval I. To prove our Theorem it suffices to show

(18) $$\sum_{j=1}^{r} |I_j| < x(1 - c_2)$$

Clearly none of the intervals I_j contain any primes. To prove (18) it will suffice to show that for some $c_3 < c_1$

(19) $$\Sigma_3 |I_j| < (c_1 - c_3)x$$

where c_1 is the constant occuring in Lemma 1 and in Σ_3 the summation is extended over those I_j, $1 \leqq j \leqq r$ which are in the intervals (p_j, p_{j+1}) satisfying (17).

Let T be sufficiently large and consider in the intervals (17) those integers all whose prime factors are at least T. It easily follows from Lemma 1 and the Sieve of Eratorthenes that the number of these integers not exceeding x is at least

(20) $$(1 + o(1))c_1 x \prod_{p<T} (1 - 1/p) > c_4 x / \log T$$

Further these integers can clearly not be contained in intervals I_j with $|I_j| \leqq T$ for otherwise they would be relatively prime to all the other integers in I_j. Thus to complete the proof of our Theorem we only have to show by (20) that for sufficiently large T

(21) $$\Sigma_4 |I_j| < \frac{1}{2}\, c_4 x / \log T$$

where in Σ_4 the summation is extended over the I_j in Σ_3 for which $|I_j| > T$. The I_j in Σ_4 satisfy

(22) $$T < |I_j| < (1-\varepsilon)\log x.$$

Write

(23) $$\Sigma_4 |I_j| = \sum_r \Sigma_4^{(r)} |I_j|$$

where in $\Sigma_4^{(r)}$ we have $(r = 0, 1 \cdots)$

(24) $$2^r T < |I_j| \leqq 2^{r+1} T$$

if $2^{r+1}T > (1-\varepsilon)\log x$, then the upper bound in (24) should be replaced by $(1-\varepsilon)\log x$. Now we show that for sufficiently large T and every r

(25) $$\Sigma_4^{(r)} |I_j| < 2x/(2^r T)^{\frac{1}{2}}.$$

From (25) and (23) (21) easily follows for sufficiently large T. Thus to prove our Theorem we only have to show (25). The integers in the I_j of $\Sigma_4^{(r)}$ can not be relatively prime to $N_{2^{r+1} \cdot T}$ (N_k is the product of the primes not exceeding k) therefore if I_j is in an interval

$$(uN_{2^{r+1} \cdot T}, (u+1)N_{2^{r+1}.T})$$

I_j must lie in an interval $(a_i + uN_{2^{r+1}.T}, a_{i+1} + uN_{2^{r+1}.T})$ where

$$1 = a_1 < \cdots < a_{\phi}(N_{2^{r+1}.T)} = N_{2^{r+1}.T} - 1$$

are the integers relatively prime to $N_{2^{r+1}.T}$. Since $2^{r+1}T \leqq (1-\varepsilon)\log x$, it follows from the prime number theorem that $N_{2^{r+1}.T} = o(x)$, hence we easily obtain from Lemma 2 for sufficiently large T

$$\sum_4^{(r)} |I_j| < \left(\left[\frac{x}{N_{2^{r+1}.T}} \right] + 1 \right) N_{2^{r+1}.T}/(2^r T)^{1/2} < 2x/(2^r T)^{1/2},$$

thus (25) and hence our Theorem is proved. Unfortunately I can not handle the $|I_j| > \log x$ and thus can not prove that the density of the integers having property P exists.

COROLLARY. *There are infinitely many composite integers satisfying* (16).

By $\alpha_p > 0$ there are infinitely many composite integers having property P, and if there would be only a finite number of integers with property (1) then for sufficiently large i in the set of integers $p_i < t < p_{i+1}$ no one would be relatively prime to the other, thus only a finite number of composite integers would have property P. This contradiction proves the corollary.

Let us say that the primes have property P_0, the composite integers satisfying (16) have property P_1. By induction with respect to k we define: An integer n has property P_k if it does not have property P_j for any $j < k$, but both intervals $(n, n + u(n))$ and $(n - u(n), n)$ contains an integer having one of the properties

$P_j, 0 \leqq j < k$. It is easy to see that for every $k \geqq 0$ the integers having property P_k have property P too, and conversely every integer having property P has property P_k for some $k \geqq 0$.

It is easy to show by induction with respect to k that the integers having property P_k have density 0, hence from $\alpha_p > 0$ we obtain that for every k there are infinitely many integers having property P_k.

References

1. A. Brauer, *On a property of k consecutive integers*, Bull. Amer. Math. Soc. **47** (1941), 328–331: Sivasankaranarayana Pillai, *On m consecutive integers III*, Proc. Indian Acad. Sci. Sect. A, **12** (1940), 6–12.

2. P. Erdös, *Problems and results on diophantine approximation*, Compositio Math., **16** (1964), 52–65, see p. 52–53.

3. P. Erdös and A. Rényi, *A probabilistic approach to problems of diophantine approximation*, Illinois J. Math., **1** (1957), 303–315, see p. 314.

4. P. Erdös, *The difference of consecutive primes*, Duke Math J., **6** (1940), 438–441.

5. P. Erdös, Amer. Math. Monthly, **60** (1953), 423.

6. G. Hoheisel, *Primzahlprobleme in der Analysis*, Sitzungsber., Berlin (1930), 580–588.

7. C. Hooley, *On the difference of consecutive numbers prime to n*, Acta Arith., 8 (1962–63), 343–347.

8. P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

Technion–Israel Institute of Technology,
Haifa