MANY OLD AND ON SOME NEW PROBLEMS

OF MINE IN NUMBER THEORY

Paul Erdös   Hungarian Academy of Sciences

I kept notebooks since July 1933. I only stated there problems and results, proofs are practically never given. In rereading them, many turn out to be trivial, false or well known, but some of them still seem interesting to me. Not to make this paper too long, I will usually restrict myself to those which have been more or less forgotten sometimes even by myself. I will give proofs only rarely sometimes to save space but (unfortunately) more often because I can not settle the problems.

In the first chapter, I discuss problems on primes and related topics.

I

1. First, let me state an ill-fated conjecture of Straus and myself. Is it true that for all $n > n_0$ there is an i so that

$$(1) \qquad p_n^2 < p_{n+i}\, p_{n-i} \;.$$

Selfridge always disbelieved (1) and had a heuristic argument that (1) fails not only for primes but much more general sequences. Independently Pomerance disproved (1) on the lines suggested by Selfridge. Pomerance and I tried unsuccessfully to prove that the density of integers n for which (1) does not hold is 0. This conjecture certainly must be true.

Pomerance and I considered the following further problems: Put

$$M(n) = \max p_{n+i}\, p_{n-i} \;.$$

Is it true that there is an $\varepsilon > 0$ so that for infinitely many n

$$(2) \qquad M(n) > p_n^2 + n^{1+\varepsilon} \;?$$

Congressus Numerantium, Vol. 30 (1981), pp. 3- 27

Is it true that the number of distinct integers of the form $p_{n+i}+p_{n-i}$ is $> c\, n/\log n$? Denote by $f(n)$ the maximum in A of the number of solutions in i of $p_{n+i}+p_{n-i}=A$. Probably $f(n)\to\infty$, $\limsup f(n)=\infty$ is not difficult. As far as we know there are no nontrivial upper bounds known for $f(n)$.

Put $$h(n) = \min\, (p_{n+i}+p_{n-i}-2p_n) \quad .$$

Is it true that $\limsup h(n)=\infty$?

C. Pomerance, The prime number graph, Math. Comp. 33 (1979), 339 - 408.

2. Let $f(n)$ be the smallest integer so that for every choice of the primes $q_1, \ldots, q_r$ for which for every i $(1 \le i \le f(n))$ there is a j, $1 \le j \le r$ satisfying $n+i \equiv 0 \pmod{q_j}$ we have

$$\sum_{j=1}^{r} \frac{1}{q_j} > 1. \tag{1}$$

I proved that for infinitely many n

$$f(n) > \exp c(\log n \log\log n)^{1/2} \quad . \tag{2}$$

(2) follows from the fact that for infinitely many n ($P(m)$ is the greatest, $p(n)$ the least, prime factor of n)

$$\min_{1\le i\le L_n} P(n+i) > \exp(c\,(\log n \log\log n)^{1/2}) \tag{3}$$

where $L_n = \exp c_1\left(\frac{\log n}{\log\log n}\right)^{1/2}$. Denote by $\psi(x,y)$ the number of integers $\le x$ all prime factors of which are $\le y$. (3) follows easily from the classical results of de Bruijn on $\psi(x,y)$.

$f(n) = o(n)$ is easy to prove and can be slightly strengthened. I have no non trivial upper bounds and no non trivial lower bounds valid for all n.

Denote by $f_1(n) = t_n$ the smallest integer for which

$$\sum_{1\le i\le t_n} \frac{1}{P(n+1)} > 1 \quad . \tag{4}$$

Clearly $f_1(n) \geq f(n)$. It would be of interest to decide whether $f_1(n) > f(n)$ holds for all sufficiently large n. Let $f_2(n)$ be the smallest integer for which for every choice of $d_1 < d_2 < \ldots$

$$\sum_{n<p\leq n+f_2(n)} \frac{1}{p} + \sum \frac{1}{d_i} > 1$$

where every non prime $n + j$, $1 \leq j \leq f_2(n)$ has a proper divisor among the d's. Clearly $f_2(n) \geq f_1(n)$. Is it true that for every sufficiently large n $f_2(n) > f_1(n)$?

N. G. de Bruijn, On the number of positive integers $\leq x$ and free of prime factor $>y$. Indg. Math. 13 (1951), 50 - 60.

3. Selfridge and I proved the following curious result. There are k^2 primes $p_1 > \ldots > p_{k^2}$ and an interval (a,b) of length $(3 - \varepsilon)\, p_1$ so that the number of integers u, $a < u < b$ which are multiples of at least one of the p_i, $1 \leq i \leq k^2$ is $2k$. It is easy to see that it can not be less than $2k$.

I just proved that for an interval of length $(3 + \varepsilon)p_1$ the number of multiples is at least $[6^{1/2} k]$, but I can not exclude the possibility that in fact it is more than εk^2.

P. Erdos, Problems and results in combinatorial analysis and combinatorial number theory, Proc. Ninth Southeastern Conf. on Combinatorics ... Cong. Num. XXI Florida Atlantic University 1978, 29 - 40, see p. 35 - 38.

4. Denote by $L(n)$ the smallest integer for which for every $(a,n) = 1$ there is a prime $p \leq L(n)$, $p \equiv a \pmod n$. Linnik proved that there is an absolute constant c so that for all n $L(n) < n^c$. Probably for $n > n_0(\varepsilon)$ $L(n) < n^{1+\varepsilon}$. Schinzel proved (improving a previous result of Prachar) that for infinitely many n

$$L(n) > c \log n \ \log\log n \ \log\log\log\log n \ (\log\log\log n)^{-2}$$

It seems certain that

$$(1) \qquad \lim_{n\to\infty} L(n)/_{n \log n} = \infty \ .$$

Very likely there are constants $1 < \alpha < \beta$ for which

$$(2) \qquad c_1 \, n(\log n)^{\alpha} < L(n) < c_2 \, n(\log n)^{\beta} \ .$$

but (1) and (2) seem to be unattackable at present. I expect that

$$(3) \qquad \sum_{n=2}^{\infty} \frac{1}{L(n)} < \infty \ .$$

(3) would of course follow from (2), but (3) also seems to be unattackable at present.

Denote by $Q(n)$ the smallest integer so that for every a, (a,n) squarefree, there is a squarefree q satisfying $q \equiv a (\text{mod } n)$, $q \le Q(n)$. Warlimont and I proved, (unpublished), that for every n

$$(4) \qquad Q(n) > c \, n \log n/_{\log\log n} \ .$$

Sharpening a previous result of Prachar, I proved $Q(n) = o(n^{3/2})$. No doubt $Q(n) < n^{1+\varepsilon}$. I can not decide whether $\sum \frac{1}{Q(n)}$ converges or not.

Iu. V. Linnik, On the least prime number in an arithmetic progression: I The basic theorem, Mat. Sbornik 15 (1947), 139 - 178, II. The Deuring-Heillbronn phenomenon, ibid 347 - 368.

For an easily accessible exposition of the work of Linnik see Prachar's book: Primzahlverteilung Berlin 1959, Springer Verlag.

For a simpler proof of Linik's theorem see:

P. Turán, On a density theorem of Ju. V. Linnik, Publ. Math. Inst. Hung. Acad. 6 (1961), 165 - 178, and S. Knapowski, On Linnik's theorem concerning exceptional L-zeroes, Publ. Math.

Deleven 9(1962), 168–178. See also P. Turán, Über die Primzahlen der arithmetischen Progression, Acta., Szeged, 8(1937), 226–235.
C. Pomerance, A note on the least prime in an arithmetic progression, J. Number Theory 12 (1980), 218–223.

A. Schinzel, Remark on the paper of K. Prachar, "Über die kleinste Trimzahl einer arithmetischen Reiche, J. rein u angew Math 210 (1962), 121–122.

P. Erdös, Über die kleinste quadratfreie zahl einer arithmetischen Reiche, Monatshefte der Math. 64(1960), 314–315.

5. Let $p_1 < p_2 < \dots$ be the sequence of consecutive primes, put $d_n = p_{n+1} - p_n$. An old (and at present hopeless) conjecture states that d_n assumes all even values. Put

$$D_n = \max_{m \le n} d_m$$

and let n_k be the smallest integer with $D_{n_k} > D_{n_{k-1}}$. Perhaps

$$(1) \qquad D_{n_k}/D_{n_{k-1}} \to 1, \quad \text{and } n_k > (1+c)n_{k-1} .$$

The first conjecture of (1) is probably true. I am less sure about the second and can not even exclude the possibility that $n_k - n_{k-1} = 1$ has infinitely many solutions. I am sure that the density of the integers D_{n_k} is 0 and perhaps $D_{n_{k+1}} - D_{n_k} \to \infty$.

Put $L_n = \log n \ \log\log n \ \log\log\log\log n \ (\log\log\log n)$? Rankin proved that for infinitely many n

$$(2) \qquad d_n > c\, L_n$$

(2) has not been improved since 1938 (except for the value of the constant c). The proof of

$$(3) \qquad \limsup d_n/L_n = \infty$$

would probably involve new ideas and I offered (and offer) 10^4 dollars for a proof (3). I am so sure that (3) is true that I did not say "proof or disproof" but will of course pay for a disproof too.

I conjectured that for every $k \geq 1$ and infinitely many n

$$(4) \qquad \min_k(d_n, d_{n+1}, \ldots, d_{n+k}) > c_k L_n .$$

I proved (4) for $k = 1$ and very recently Meyer proved (4) in a surprisingly ingenious way. I further conjectured that for every $k \geq 0$

$$(5) \qquad \max_k(d_n, \ldots, d_{n+k}) < (1 - c_k)\log n$$

has infinitely many solutions. I proved (5) only for $k = 0$, and as far as I know (5) is still open for all $k \geq 1$.

Ricci and I proved that the set of limit point of $d_n/\log n$ form a set of positive measure, but no finite limit point is known. No doubt every $\alpha, 0 \leq \alpha \leq \infty$ is a limit point of $d_n/\log n$.

As I stated in the previous paragraph (2) is no doubt very far from being best possible. In fact a classical conjecture of Cramer states that

$$(6) \qquad \limsup d_n/(\log n)^2 = 1$$

(6) is completely unattackable by the methods at our disposal and the decision must no doubt be left to the distant future. A slightly stronger form of (6) states:

$$\lim D_n/(\log n)^2 = 1$$

Probably

$$(7) \qquad \max_{m<n} \min(d_m, d_{m+1})/D_n = 0 .$$

Turán and I conjectured that for every $k, d_m > \dots > d_{n+k}$ has infinitely many solutions. We could not even prove that $(-1)^n(d_{n+1}d_n)$ changes sign infinitely often. We have no non-trivial upper bound for the longest sequence

$$(8) \qquad d_n > \dots > d_{n+k} \ .$$

surely $k = o(n^{\varepsilon})$ and perhaps $k = o(\log n)$.

Let $q_1 < q_2 < \dots$ be the sequence of consecutive squarefree numbers. Put

$$q_{n+1} - q_n = t_n, \quad \max_{1 \le m \le n} t_m = T_n \ .$$

The behaviour of t_n and T_n is simpler to study than that of d_n and D_n but many unsolved problems remain, e.g. very little is known about T_n and I cannot decide whether

$$\max_{m<n} \min(t_m, t_{m+1})/T_n \to 0$$

holds. (It almost certainly does).

How fast must $f(n)$ tend to infinity $(f(n) = o(n))$ so that

$$\pi(n + f(n)) - \pi(n) = (1 + o(1)) \frac{f(n)}{\log n} \ ?$$

Perhaps $f(n) > (\log n)^{2+\varepsilon}$ suffices for (7), but as far as I know it never has been disproved that $f(n) > (\log n)^{1+\varepsilon}$ does not suffice. In fact I do not see a proof that $f(n)/L(n) \to \infty$ does not suffice for (7) (see (2) and (3)).

R. A. Rankin, The difference between consecutive prime numbers. J. London Math. Soc. 13 (1938), 242-247.

P. Erdös and P. Turán, On some new questions on the distribution of prime numbers, Bull. Amer. Math. Soc. 54 (1948), 685-692.

P. Erdös, The difference of consecutive primes, Duke Math. J. 6 (1940), 438-441, and Problems and results on the difference of consecutive primes, Publ. Math. Debrecem 1 (1949), 33-37.

G. Ricci, Recherches sur l'allure de la nute $(p_{n+1}-p_n)/\log p_n'$ Coll. sur la theorie des nombres, Bruxelles 1955, 93-96, Sull. andamento della differenza di numeri primi consecutive, Riv. Math. Univ. Parma, 5(1954), 3-54. My proof appeared in 1955 in lecture notes held at Lake Como.

P. Erdös, Some problems and results in elementary number theory, Publ. Math. Debreen 2(1951), 103-109; On the difference of consecutive primes, Bull. Amer. Math. Soc. 54 (1948), 885-889.

6. To end this chapter, I state a few miscellaneous problems on primes. Let $f(x;n)$ be the number of distinct integers $x < m < x+n$ for which there is a prime $p, \frac{n}{3} < p < \frac{n}{2}$ satisfying $p|m$ is it true that for every $x \geq 0$

$$(1) \qquad f(x;n) > c\,\frac{n}{\log n} \quad ?$$

It is rather annoying that I got nowhere with this harmless looking problem. It is easy to see that $f(x;n) > c\,n^{1/2}(\log n)^{-1/2}$, but I do not see how to prove $f(x;n) > n^{1-\varepsilon}$ for every $\varepsilon > 0$ and $n > n_0(\varepsilon)$. Observe that for suitable x there is only one integer m, $x < x + m < x + n$ which has a prime factor $p, \frac{n}{2} < p < n$. Trivially for $x = 0$

$$(2) \qquad f(0,n) < \left(\frac{1}{3} + o(1)\right)\frac{n}{\log n}$$

and Straus and I just observed that there is an $x = x(n)$ which gives

$$(3) \qquad f(x,n) \leq \left(\frac{1}{6} + o(1)\right)\frac{n}{\log n} \quad .$$

It is not impossible that the method of Selfridge and I (used in 3) will improve (3) and perhaps can lead to a disproof of (1).

It seems that $p_k = 7$ is the largest prime for which the sequence $p_k, p_{k+1}, \ldots, p_{k+p_k-1}$ forms a complete set of residues mod p_k. This question is almost certainly unattackable. It seems I was wrong here, Promerance just proved this.

What can one say about the smallest r for which for at least one ℓ, $k \le \ell \le k + r$ the primes $p_k, p_{k+1}, \ldots p_{k+r}$ contain a complete set of residues mod p_ℓ? It will not be easy to get upper and lower bounds for r. I expect that infinitely often, but not always, $\ell = k$.

What is the largest $s = s(k)$ so that

$$p_j \equiv p_\ell \pmod{p_i}, \quad k \le i < j < \ell \le s$$

never holds? For almost all k no doubt $s \le (2 + \varepsilon)k$, but exceptionally s can perhaps be much larger.

These problems become easy if the primes are replaced by squarefree numbers, e.g., it is easy to prove that if $q_1 < q_2 \ldots$ is the sequence of squarefree numbers then for $k > k_0$, $q_k, q_{k+1}, \ldots q_{k+q_k-1}$ does not form a complete set of residues mod q_k.

On the other hand it is not hard to prove that for every k there are q_k consecutive squarefree numbers which form a complete set of residues mod q_k. I am sure that for every prime p there are infinitely many $(p-1)$-tuples of consecutive primes which form a complete set of reduced residues mod p.

This conjecture is almost certainly unattackable at present.

Many years ago, S. Golomb and I conjecture that

$$\sum_p \sum_{q \mid (2^p-1)} \frac{1}{q} < \infty; \qquad p,q \text{ primes.} \tag{2}$$

(2) does not seem hopeless and is perhaps not difficult. When I found (2) a few days ago in my old notes I tried it again and failed. Schnizel observed that the number of primes $q < x$ which occur in the sum (1) is $o\left(\frac{x}{\log x}\right)$.

Is there any prime p for which

$$(3) \qquad \sum_{q \mid (2^p-1)} \frac{1}{q} > \frac{1}{p} \quad ?$$

Find the smallest prime (if any) which satisfies (3). I doubt very much if there is such a prime. (Pomerance just convinced me [1980 XII 18] that such primes indeed exist and can be found [in principle] in a finite number of steps), but there probably are integers n for which

$$\sum{}' \frac{1}{q} > \frac{1}{n}$$

where in $\sum{}'$ the summation is extended over the primes $q \mid 2^n-1$, $q \nmid 2^m-1$ for $m < n$.

Is it true that $\frac{\sigma(2^n + 1)}{2^n}$ and $\frac{\sigma(2^n - 1)}{2^n}$ are both everywhere dense in $(1,\infty)$?

Let $p_1 < p_2 < \dots$ be an infinite sequence of primes satisfying $p_k \equiv 1 (\mathrm{mod}\ p_{k-1})$. It is true that $p_k^{1/k} \to \infty$?

I can not even prove $\limsup p_k/p_{k-1} = \infty$.

The same questions can be asked if we insist that p_k is the smallest prime $\equiv 1(\mathrm{mod}\ p_{k-1})$. It is not impossible (but I am doubtful) that $p_k/p_{k-1} \to \infty$ for this sequence.

Again the same question can be asked if $q_1 < q_2 < \dots$ is a sequence of squarefree numbers satisfying $q_k \equiv 1(\mathrm{mod}\ q_{k-1})$. I would expect that $q_k^{1/k} < c$ is possible, but probably $\limsup q_k/q_{k-1} = \infty$ remains true.

Let $p_1 = 3, p_2 = 5, \ldots, p_{k+1}$ is the least prime for which $(p_{k+1} - 2) | p_1, \ldots, p_k$. Is this sequence infinite?

Is it true that for every c and $n > n_0(c)$ there is a composite $m > n + c$ for which $m - p(m) < n$? ($p(m)$ is the least prime factor of m.) I have no proof even if we assume $c = 0$. It might be of some interest to study the sequence of composite integers $m_1 < m_2 < \ldots$ where m_1 is the least integer greater than m_{i-1} so that $n > m_i$, $n - p(n) > m_i - p(m_i)$. p^2 clearly is an m_i and probably all the m_i have two prime factors.

Put

$$n - f(n,c) = \min_{m>n+c} (m - p(m)), \quad m \text{ composite.}$$

A stronger form of my conjecture states that $f(n;c) \to \infty$ as $n \to \infty$. I can not prove this even for $c = 0$. If the conjecture is correct one could try to estimate $f(n,c)$ from above and below.

Denote by $d_{p-1}(n)$ the number of divisors of n of the form $p - 1$. Prachar proved that for infinitely many n

$$d_{p-1}(n) > n^{c/(\log\log n)^2} . \tag{4}$$

Very recently Odlyzko replaced in (4) $n^{c/(\log\log n)^2}$ by $n^{c/\log\log n}$ which apart from the value of c is best possible. Put

$$D_{p-1}(x) = \max_{n\le x} d_{p-1}(x), \quad D(x) = \max_{n\le x} d(n) .$$

Is it true

$$D_{p-1}(x)/D(x) \to 0, \text{ but } D_{p-1}(x) > D(x)^{1-\varepsilon} \text{ for } x > x_0(\varepsilon) ? \tag{5}$$

The first conjecture in (5) is perhaps easy, but I expect that the second is very difficult.

Prachar and I studied the variation of p_k/k. We obtained various inequalities but did not prove the following very plausible conjecture: Is it true that there are only a finite number of indices k so that for every $j < k < \ell$

$$p_{j/j} < p_{k/k} < p_{\ell/\ell} \quad ?$$

K. Prachar, Über die Anzahl der Teiler einer Natürlichen Zahl, welche die Form p-1 haben, Monatshefte Math. 59 (1955), 91-97. The proof of Odlyzko will appear in a forthcoming paper of L. M. Adleman, C. Pomerance and R. C. Rumely, On distinguishing prime numbers from composite numbers.

P. Erdös and K. Prachar, Sätze und Probleme über p_k/k Math. Sem. Univ. Hamburg 25 (1962), 51-56.

II

In this chapter I discuss problems on consecutive integers.

1. Two old problems on consecutive integers were settled in the last decade. Catalan conjectured about 100 years ago that 8 and 9 are the only consecutive powers. Tijdeman proved that there is a computable constant c so that two consecutive integers greater than c can not both be powers. c is too large to prove that 8 and 9 are the only exceptional cases, but I am sure that this soon will be done.

Selfridge and I proved that the product of consecutive integers is never a power. This was conjectured more than 100 years ago.

Both results can probaly be strengthened. Denote by $x_1 < x_2 < \dots$ the sequence of consecutive powers. Is it true that $x_{k+1} - x_k \to \infty$? or sharper $x_{k+1} - x_k > x_k^\varepsilon$? Choodnovsky may have a proof of the first conjecture, the second is quite unattackable at present.

Put $\Pi(n,k) = (n+1) \dots (n+k)$. Is it true that for $k > 2$ there always is a $p \geq k$ for which $p \| \Pi(n,k)$? We can not even prove that for $k > 2$ there is always a $p \| \Pi(n;k)$.

P. Erdös and J. Selfridge, The product of consecutive integers is never a power, Illinois J. Math 19 (1975), 292-301. In this paper a short outline of the history of the problem and some references are given.

R. Tijdeman, On the equation of Catalan, Acta Arith. 29 (1976), 197 - 209.

2. Put ($P(n)$ is the greatest, $p(n)$ the least prime factor of n),

$$n+i = a_i^{(n)} \cdot b_i^{(n)}, \ 1 \leq i \leq k, \ \ P(a_i^{(n)}) < k, \ p(b_i^{(n)}) \geq k .$$

Define

$$f(n;k) = \min_{1 \leq i \leq k} a_i^{(n)}, \quad F(n;k) = \max_{1 \leq i \leq k} a_i^{(n)} .$$

By a simple averaging process I proved that

$$f(n;k) < c\, k$$

and conjectured

$$(1) \qquad f(n;k) = o(k) .$$

(1) seems to me to be a very attractive conjecture unfortunately I got nowhere with it. A stronger conjecture than (1) states that

$$\sum_{i=1}^{k} \frac{1}{a_i^{(n)}} \to \infty \text{ or perhaps even } \sum_{i=1}^{k} \frac{1}{a_i^{(n)}} \geq (1+o(1)) \log k .$$

It would be very interesting if one could determine the true order of magnitude of $f(n;k)$. I expect that much more than (1) is true, perhaps $f(n;k) = o(k^{\varepsilon})$.

I can prove that $f(n;k) \to \infty$ as k tends to infinity, but I do not think that I can get a good lower bound for $f(n;k)$.

For most values of n and k $f(n;k) = 1$ i.e. usually k consecutive integers contain an integer all prime factors of which are not less than k. More precisely: denote by ε_k the density of integers n for which $(n+i,(k-1)!) > 1$ for every $i \le k$. It is easy to see that $\varepsilon_k \to 0$. Estimate how fast. I expect that ε_k tends to 0 exponentially or at least not much slower. Denote by $r(n;k)$ the number of integers i, $1 \le i \le k$ for which $(n+i,k!) = 1$. It easily follows from Turán's method that for almost $n (k \to \infty)$.

$$r(n;k) = (1 + o(1))k \prod_{p \le k} \left(1 - \frac{1}{p}\right)$$

The smallest possible value for $F(n;k)$ is clearly k, but usually $F(n;k)$ is very much larger. I expect that the density for integers n for which

$$F(n;k) < k^{(1-\varepsilon)\log k\,(\log\log k)^{-1}}$$

goes to 0 as k tends to infinity. It follows from the results of de Bruijn (on $\psi(x,y)$ quoted in the first chapter) that for almost all n

$$f(n;k) < k^{\log k/\log\log k} .$$

Denote by $G(k)$ the largest integer for which there are $G(k)$ consecutive integers $1 \le i \le G(k)$ so that for some of the integers $a_i^{(n)}$ $1 \le i \le G(k)$ are all different. Basil Gordon and I proved that $G(k) \le (2 + o(1))k$. I am convinced that

(2) $$G(k) = (1 + o(1))k.$$

It is rather annoying that we got nowhere with (2), which seems a simple and natural conjecture, perhaps we overlooked a simple agrument. Let $2 = p_1 < p_2 < \ldots < p_s \le k < p_{s+1} < p_{s+2}$ be the sequence of consecutive primes. It seemed to me that $G(k) = p_{s+2}-2$, but I seem to remember that a counterexample was found. Perhaps $G(k) = p_{s+s}-2$ holds for all sufficiently large k.

Denote by $h(n;k)$ the number of distinct values of the $a_i^{(n)}$, $1 < i < k$. $\max_n h(n;k) = k$ is obvious. Put $\min_n h(n;k) = H(k)$. I conjecture that $H(k) > ck$ and perhaps

(3) $$\lim_k H(k)/k = C.$$

At present I can not attack these conjectures. It is easy to prove that

$$(4) \qquad H(k) \quad c\left(\frac{k}{\log k}\right)^{1/2}$$

To prove (4) let $2 < 3 \ldots < p_r$ be the primes not exceeding $k/2$. Each p_i has at least two multiples in $(n+1, n+k)$. If every $n < u \le n+k$ is divisible by at most $r^{1/2}$ of the p_i then clearly at least $r^{1/2}$ of the $a_j^{(n)}$, $1 \le j \le k$ are distinct. If there is a u, $n < u \le n+k$ which is divisible by more than $r^{1/2}$ primes $p_{i_1}, p_{i_2}, \ldots, p_{i_s}$, $s > r^{1/2}$, then if $u < n + \frac{k}{2}$ all the $u + p_{i_j}$, $1 \le j \le s$ are $\le n+k$ and the $a_{u+p_j}^{(n)}$ are all distinct ($a_{u+p_{i_j}}^{(n)}$ is a multiple of p_{i_j} and of no other p_{i_j}). If $u > n + \frac{k}{2}$ then we consider the numbers $u - p_{i_j} > n$ and the proof goes as before.

If (1) of I, 6 holds $\left(f(x,n) > \frac{cn}{\log n}\right)$ then this proof easily give $H(k) > c\,\frac{k}{\log k}$. At the moment I have no idea how to approach (4).

By a combinatorial argument I can show that for $k > k_0(r)$ the number of integers $n < m \le n+k$ which have a prime divisor p, $k^{1/r} < p < 2k^{1/r}$ is greater than $c_r k^{1-\frac{1}{r}+\frac{1}{r^2}}$. Perhaps this can be improved to $c_r k/\log k$. The difficulty of getting an estimation of $H(k)$ is that for m_1 and m_2, $m_1 \ne m_2$ the a_i's may be the same.

Put

$$P(n;k) = \max p^{\alpha}, \; p^{\alpha} \| a_i^{(n)}, \quad 1 \le i \le k \quad .$$

In view of the difficulty of estimating the order of magnitude of $F(n;k)$ for almost all n, it might be worth while to observe that for almost all n $P(n;k)$ is of the order of magnitude $\frac{k^2}{(\log k)^2}$. In fact a simple sieve argument gives that the density of the integers n for which $P(n;k) \frac{c\,k^2}{(\log k)^2}$ tends to a distribution function $f(c)$ as $k \to \infty$.

Let $G_1(k)$ be the largest integer ℓ for which there is an n so that

$$a_1^{(n)} < a_2^{(n)} < \ldots < a_\ell^{(n)}, \quad \ell = G_1(k).$$

I am sure that $G_1(k) = (1+o(1))k$. This should be much easier to prove than $G(k) = (1+o(1))k$. In fact perhaps $G_1(k) = p_{s+1}-1$ where p_{s+1} is the least prime greater than k.

To finish this chapter I state a few more questions. It seems to me that I can prove (I did not carry out all the details) that there is a distribution function $f(\alpha)$ so that the density of integers n for which the number of indices $i(1 \le i \le k)$ for which $a_i^{(n)} > n^\alpha$, tends tends to $f(\alpha)$ as k tends to infinity.

Denote by $P(a_i^{(n)})$ the product of all the distinct prime factor of $a_i^{(n)}$ and by $Q(a_i^{(n)})$ the squarefree part of $a_i^{(n)}$ i.e. $p|Q(a_i^{(n)})$ if an only if the exact power of p dividing $a_i^{(n)}$ is odd. One can ask the same questions about $P(a_i^{(n)})$ and $Q(a_i^{(n)})$ which we asked about $a_i^{(n)}$ e.g. for how many consecutive integers $n+1, n+2, \ldots$ can they be distinct and how many of the integers $P(a_i^{(n)})$ (or $Q(a_i^{(n)})$, $(1 \le i \le k)$ must be different. I needed some results of this type in my old proof that the product of consecutive integers is never square.

Let $q(n;k)$ be the smallest prime which does not divide $\prod_{i=1}^{k}(n+i)$. $f(n) = \max_k g(n;k)/k$. What can be said about $f(n)$ for all or almost all n? In particular if $k = [\log n]$ is $f(n) > 2+\varepsilon$ possible? Pomerance observed that if true this is best possible, since if $n+1$ is the product of primes in $(\log n, 2 \log n)$ $f(n) = 2+o(1)$.

Szemeredi and I proved that for $k > k_0$ and $n > e^k$ ($\omega(n)$ is the number of distinct prime factors of n)

$$(5) \qquad \omega\left(\binom{n}{k}\right) \geq k \quad ,$$

but probably (5) holds already for much smaller values of n.

Put

$$M_n(k) = \prod_{\substack{p \leq k \\ p^\alpha \| \binom{n}{k}}} p^\alpha \quad .$$

It is well known that $p^\alpha \leq n$, thus $M_n(k) < n^{\pi(k)}$. Perhaps

$$(6) \qquad M_n(k) < e^k \, n(\log n)^c$$

holds for all n and k. The conjecture (6) is perhaps a bit too optimistic.

P. Erdös, On consecutive integers, Nieuw Arch. Wisk 3(1955), 124-128.

P. Erdös and J. Selfridge, Some problems on the prime factors of consecutive integers, Illinois J. Math. 11(1967), 428-430; Complete prime subsets of consecutive integers, Proc. Manitoba Conf. on Num. Math., Univ. of Manitoba, Winnipeg 1971, 1-14, Some problems on the prime factors of consecutive integers II Proc. Wash. State Conf. on Number Theory 1971, 13-21.

P. Erdös and R. L. Graham, On the prime factor of $\binom{n}{k}$, Fibonacci Quart. 14 (1976), 348-352.

III

In this final chapter I discuss some miscellaneous problems.

1. Let S_r be a measurable set in a circly of radius $r (r \to \infty)$. Assume that S_r does not contain the vertices of an equilateral

triangle of side >1. Is it true that the measure of S_r is $o(r^2)$? If we would insist that S_r contains no equilateral triangle at all then it follows from the density theorem of Lebesgue that the measure of S_r is 0.

Straus suggested that perhaps the measure of S_r is less than cr.

2. Problem of Szemeredi and myself. Let $x_1, \ldots, x_n$ be n points in the unit circle. Denote by $D(x_1, \ldots x_n)$ the smallest distance between two of the x_i's and by $\alpha(x_1, \ldots, x_n)$ the size of the smallest angle determined by our points. It is well known and easy to see that

$$D(x_1, \ldots, x_n) < c\, n^{-1/2}, \quad \alpha(x_1, \ldots, x_n) < c\, n^{-1} .$$

It is true that

$$\alpha(x_1, \ldots, x_n) \cdot D(x_1, \ldots, x_n) = o(n^{-3/2}) \quad ?$$

Perhaps

$$\alpha(x_1, \ldots, x_n) \cdot D(x_1, \ldots, x_n) < c\, n^{-2} .$$

The regular n-gon shows that if (1) is true it is best possible.

3. Harzheim and I considered the following problem: Let $1 \le a_1 \le a_2 \ldots$ be an infinite sequence of integers, assume that no a is the sum of consecutive a's (i.e. $a_j \neq a_r + \ldots + a_s$). Is it then true that the upper density of the a's is $\le \frac{1}{2}$? Is the lower density 0? Is the logarithmic density 0? An older question of Andrews asked: Let $x_1 \le x_2 \ \ldots$ be a sequence of integers where x_n is the smallest integer which can not be written in the from $x_i + x_{i+1} + \ldots + x_j$. What can be said about the asymptotic properties of x_n? It is quite possible that the density of this sequence is 0. Nevertheless it is easy to see that in our modification of Andrews' problem the upper density can $\frac{1}{2}$.

To see this suppose that $1 \le a_1 < \dots < a_k$ is already defined. Then $a_{k+1} = a_k^4$, $a_{k+2} = a_k^4 + a_k^2$, $a_{k+2+i} = a_k^4 + a_k^2 + i$, $1 \le i < a_k^4 - a_k^2$. Clearly the upper density of this sequence is $\frac{1}{2}$ and no $\underline{a}$ is the sum of consecutive a's.

Perhaps $\sum_k \frac{1}{a_k} < \infty$, but this I can not prove. All I can show is that

$$(1) \qquad \sum_{x<a_k<x^2} \frac{1}{a_k} < c .$$

The proof of (1) is easy. Let $x < a_k < a_{k+1} < \dots < a_\ell < x^2$ be the a's in (x,x^2). Observe that all the sums $\sum_u^v a_i$, $v - u \le x$ are all all distinct and are all less than x^3. Thus

$$(2) \qquad \sum_{\substack{k<u<v<\ell \\ v-u\le x}} \frac{1}{\sum_u^v a_i} < \sum_{t<x^3} \frac{1}{t} < 3 \log x + c \quad .$$

Now clearly $\sum_u^v a_i < (v-u)\, a_v$. Thus

$$(3) \qquad \sum_{k<u<v<\ell} \frac{1}{\sum_u^v a_i} > \left(1 + \frac{1}{2} + \dots \frac{1}{x}\right)\left(\frac{1}{a_{k+x}} + \frac{1}{a_{k+x+1}} + \dots + \frac{1}{a_\ell}\right)$$

(2) and (3) gives

$$\frac{1}{a_{k+x}} + \dots + \frac{1}{a_\ell} < 3 + o(1) \quad \text{or} \quad \sum_{x<a_k<x^2} \frac{1}{a_k} < 4 + o(1)$$

which proves (1). The best value of c in (1) could perhaps be determined.

4. Mahler's problem. Mahler wrote me many years (decades) ago: Put

$$f(n) = \min \sum (x_i + y_i), \quad \text{where} \quad n = \sum_i x_i\, y_i \quad .$$

Estimate $f(n)$ as well as you can. I observed that

$$f(n) = 2\,n^{1/2} + O(n^{1/8}) \quad .$$

The exponent $\frac{1}{8}$ in the error term is probably not best possible, but I could show that is is not $o(n^{\varepsilon})$. If $\phi(n)$ is the number of summands which give the minimum, then $\limsup \phi(n) = \infty$.

5. Denote by $\sigma(n)$ the sum of divisors of n. It is easy to prove that

$$\sum_{n=1}^{x} \min \frac{1}{n} \left(\sigma(n+1), \sigma(n+2), \ldots, \sigma(n+k)\right) = c_k x + o(x) \quad .$$

It is easy to prove that c_k tends to 1 as k tends to infinity. I could not get a good estimate how fast $c_k - 1$ tends to 0. I expect that it tends to 0 exponentially or at least not much slower.

6. An old conjecture of mine states that almost all n have two divisors $d_1 < d_2 < 2d_1$. During one of my unsuccessful attempts to prove this I was lead to the following question: Denote by $f(n;k)$ the density of the integers which have a divisor in $(n,n+k)$ and by $f_1(n;k)$ which have exactly one such divisor. Is it true that $f_1(n;k)$ is unimodular? (i.e. it first increases, reaches its maximum and then decreases). For which k does $f_1(n;k)$ reach its maximum? I would of course be satisfied if this k could be determined asymptotically. Clearly for small k

$$(4) \qquad f_1(n;k) = (1 + o(1))\; f(n;k) \quad .$$

How far does (4) remain true? One would expect $k \sim n/(\log n)^{\alpha}$ for some $0 < \alpha < 1$. Probably

$$f_1(n,n) = o(f(n,n)) \quad .$$

7. Let $1 \le a_1 < \ldots < a_k \le n$. Assume that $a_i + a_j$ never

divides $a_i a_j$. I conjectured max $k = \frac{n}{2} + o(n)$. The odd numbers show that if true it is best possible. Odlyzko showed that for $n = 1000$, max $k \geq 717$ and now I am quite doubtful if my conjecture is true. Assume that no sum $a_{i_1} + \dots + a_{i_r}$ divides $a_{i_1} \dots a_{i_r}$. Is it then true that $k < \varepsilon n$ for $n > n_0(\varepsilon)$?

8. Let $f(n)$ be the smallest integer so that one can divide the integers $1, 2, \dots, n-1$ into $f(n)$ classes so that n is not the distinct sum of integers of the same class. $f(n)$ tends to infinity - but how fast?

Let $h(n;k) = \ell$ be the smallest integer so that if $1 \leq a_1 < \dots < a_\ell \leq \frac{n}{k}$ then n is the distinct sum of a's. Estimate $f(n;k)$ as well as possible.

Let $a_1 < a_2 < \dots$ be an infinite sequence of integers. Denote by $f_1(n)$ the number of solutions of $0 \leq a_i - a_j \leq n$ and $f_2(n)$ is the number of solutions of $n < a_i - a_j < 2n$. Is it true that

$$\limsup f_1^{(n)}/f_2(n) \geq 3.$$

It is easy to see that (5) if true is best possible. Is it true that

$$\liminf \sum_{0<a_i-a_j\leq n} (a_i-a_j)/n\binom{A(n)}{2}', \quad A(n) = \sum_{a_i \leq n} 1 .$$

9. Let $1 < a_1 \dots$ be an infinite sequence of integers, assume that $A(n) = \sum_{a_i<n} 1 > c\, n^{1/3}$ for every n. Denote by $H_3(n)$ the number of solutions of $0 < a_i + a_j - a_\ell < n$. Is it true that

$$\limsup H_3(n)/n = \infty \quad ? \tag{6}$$

More generally assume that $A(n) > n^{1/r}$ and denote by $H_r(n)$ the number of solutions of

$$0 < \sum_{i=1}^{r} \varepsilon_i \ a_i < n \ , \quad \varepsilon_i = \pm 1.$$

Is it true that

$$\limsup H_r(n)/n = \infty \ . \tag{7}$$

I can prove (7) only for $r = 2$. If (6) and (7) are true they would have several applications in additive number theory.

10. Let $1 \le a_1 < \ldots < a_n \le x$. Is it true that there are at least $c\, n/(\log n)^{\alpha}$ distinct integers m satisfying $m \equiv 0 (\bmod\ a_i)$ for some i, $1 \le i \le n$ and $x < m \le x + a_n$? If true then apart from the value of α this is best possible. I found this in one of my old notebooks and completely forgot about it. I ask the indulgence of the reader if it turns out to be trivial or false.

11. Let $a_k k^{-2} \to \infty$, $b_1 < b_2 < \ldots$ is the sequence of integers which are not multiples of any of the a_i. Is it true that

$$\sum_{b_k < x} (b_{k+1} - b_k)^2 < cx \ ? \tag{8}$$

It is not hard to see that $a_k > ck^2$ is not enough for (8).

12. Let $a_1 < \ldots < a_k$ be a sequence of integers. Is it true that if the number of solutions of $a_i + a_j = a_\ell$ is $> c\, k^2$ and $k > k_0(\ell)$, then the a's contain an arithmetic progression of ℓ terms? If this result is false then perhaps the assumption that the number of solutions of $a_i + a_j = a_r + a_s$ is $> c\, k^3$ will imply that our sequence contains an arithmetic progression of ℓ terms for $k > k_0(\ell)$.

13. Let $1 \le a_1 < \ldots$ be an infinite sequence of integers for which every n is of the form $a_i\ a_j$. Clearly our sequence must contain 1 and all the primes. Is it true that is $\liminf A(x)\ x^{-1} \log x < \infty$ then $\limsup A(x)\ x^{-1} > 0$?

E. Wirsing, Über die Dichte multiplikativer Basen, Arch. Math. 8 (1957), 11-15.

14. Is it true that there is an absolute constant C so that if $a_1 < \dots < a_k < n$ is a sequence of integers which are pairwise relatively prime then

$$\sum_{i=1}^{k} \frac{1}{n-a_i} < \sum_{p<n} \frac{1}{p} + C? \tag{9}$$

(9) if true would imply

$$\sum \frac{1}{p} + C > \sum_{p<n} \frac{1}{n-p} \tag{10}$$

Problems like (9) and (10) are contained in a paper of Eggleton, Selfridge, and myself which I am afraid will only appear posthumously.

I am doubtful if (9) is true but have, of course, no counterexample. I am sure (10) is true.

Denote by $\psi(k)$ the largest integer for which there is an n and integers

$$n < a_1 < \dots < a_{\psi(k)} < n+k, \quad (a_i, a_j) = 1, \quad 1 \le i \le j \le \psi(k). \tag{11}$$

Is it true that

$$\psi(k) < (1 + o(1)) \quad \pi(k)? \tag{12}$$

$f(n) = \sum_{p<n} \frac{1}{n-p}$ has been investigated by de Bruijn, Turán and myself, but we have not even been able to prove that $\limsup f(n) = \infty$.

If the distribution of the primes is reasonably regular, then $\liminf f(n) = 1$. It is not hard to prove that

$$\sum_{n\le 1}^{x} f(n) = (1+o(1))x, \quad \sum_{n=1}^{x} f^2(n) = (1 + o(1))x \tag{13}$$

Thus $f(n) = 1 + o(1)$ for almost all n. If I remember right this was known to us (de Bruijn, Turán and myself, at the beginning of time). A few days ago Pomerance and I observed that $1+\frac{1}{k}$, $k = 1, 2, \dots$ must be limit points of $f(n)$, $n=1,2,\dots,$ but it is difficult to prove that there are other limit points. In fact if the primes satisfy

$$(14) \qquad \liminf \frac{p_{n+1}-p_n}{\log n} > 0$$

and for $y<x$, $y>x^{\varepsilon}$.

$$(15) \qquad \pi(x+y)-\pi(x) = (1+o(1))\ \frac{y}{\log x}\ ,$$

then $1+\frac{1}{k}$, $k=1,2,\dots$ are the only limit points of $f(n)$. Observe that (15) certainly holds and (14) is certainly false but both are byond our reach for the moment.

15. Let $1 \le a_1 < a_2 < \dots < a_{\phi(n)} = n-1$ be the integers relatively prime to n. An old conjecture of mine states

$$(1) \qquad \sum_{i=1}^{\phi(n)-1} (a_{i+1}-a_i)^2 < c\,\frac{n^2}{\phi(n)}\ .$$

It is very annoying that (1) is so intractable - it certainly does not look difficult at first sight. Put

$$J(n) = \max(a_{i+1}-a_i)\ .$$

$J(n)$ after Jacobstahl. Jacobstahl conjectured that $J(n) < c(\log n)^2$. This conjecture was proved by Iwaniec. Put $n_r = 2,3,\dots,p_r$ and let $m \le n_{r+1}$. Jacobstahl further conjectured that $J(m) \le J(n_{r+1})$. We are very far from being able to prove this conjecture. I wonder whether it is possible to characterize the integers n for which $J(n) > P(n)$. It is easy to see that $J(n_r) > p_{r+1}-1$. Estimate the size of the smallest $a_i^{(r)}$ ($a_1^{(r)} < \dots$ are the integers relatively prime to n_r) for which

$$a_i^{(r+1)} - a_i^{(r)} \ge p_{r+1}\ .$$

I am sure that $a_i^{(r)}$ increases "fast" i.e. faster than any fixed power of r. Unfortunately there is no hope of proving this, since it would imply $p_{k+1} - p_k < C\, p_k^{1/2}$

C. Hooley, On the differences of consecutive numbers relatively prime to n, I, II, and III, Acta Arith. 8 (1962/63), 343-344; Publ. Math. Delseven 12 (1965), 39-49; Math. Zeitschrift 90 (1965) 335-364.

16. Finally I mention a few problems on the functions $\phi(n)$ and $\sigma(n)$. I spend (wasted?) lots of time on some of these questions. One annoying problem which I could never settle is whether $\phi(n) = \sigma(m)$ has infinitely many solutions. I am sure that the answer is affirmative.

Nearly 50 years ago I stated that if $1 < a_1 < \ldots < a_k \leq n$ is a sequence of integers for which $\phi(a_1) < \ldots < \phi(a_k)$ and we make the plausible but hopeless conjecture that there always is a prime between x and $\sqrt{x} + x$ for $x > x_0$, then $k \leq \Pi(n)$. Unfortunately I was not able to reconstruct my "proof", which was probably wrong.

Let $a_1 < a_2 < \ldots < a_t < x$, $\phi(a_1) > \ldots > \phi(a_t)$. How large can $t = t_x$ be? Trivially $t_x \to \infty$.

Is there α, $1 < \alpha < \infty$ and a β, $0 < \beta < 1$ so that

$$|\sigma(n) - \alpha n| \to \infty \quad \text{and} \quad |\phi(n) - \beta n) \to \infty \;\; ?$$

(i.e.) $\frac{\sigma(n)}{n}$ is never too close to $\alpha)/$. Then max $k = \pi(n)$.

For a very large list of solved and unsolved problems see:
P. Erdos and R. L. Graham, Old and new problems and results in combinatorial number theory, Monographic N° 28 de L'Enseignement Mathematique 1980. This book contains very extensive references.