MATHEMATICA BALCANICA
4.32 (1974) 197—202

ERDÖS, P. (Budapest, Hungary)

REMARKS ON SOME PROBLEMS IN NUMBER THEORY*

I discuss in this note several disconnected problems in number theory. I have written several such papers but here I will give details (or at least outlines) of the proofs and will not concentrate on stating unsolved problems (except in III). Several of the problems which I discuss were suggested by questions in other branches of mathematics.

I. Denote by $S(x)$ the number of integers $n<x$ for which there is a non-cyclic simple group of order n. The well known classical result of FEIT and THOMSON states that every such number must be even. DORNHOFF proved that $S(x)=o(x)$ and DORNHOFF and SPITZNAGEL proved $S(x)<c_1 x\left(\frac{\log\log\log x}{\log\log x}\right)^{1/2}$. ($c_1$, c_2, ... denote absolute constants.)

I proved in a paper dedicated to the memory of the well known Indian mathematician D. D. KOSAMBI that

$$S(x)<x\exp\left(-\left(\frac{1}{2}+o(1)\right)\quad(\log x\log\log x)^{1/2}\right). \tag{1}$$

dince the paper where I proved (1) is not easily available, I will outline the sroof of (1) and discuss a few related results and conjectures.

Let V be the sequence of integers $v_1<v_2<\cdots$ having the property that for every $p\mid v_i$ v_i has a divisor $t_i\equiv 1 \pmod p$, $t_i>1$. U is the sequence of integers $u_1<u_2<\cdots$ where the above property only has to hold for the largest prime factor $p_i=P(u_i)$ of u_i. Clearly $U\supset V$.

It follows from the classical results on non-cyclic simple groups that if there is a non-cyclic group of order s then $s\in V$. For if $p^a\mid s$, $p^{a+1}\nmid s$ then the number of SYLOW subgroups $t(\alpha, p)$ of order p^a is a divisor of s and further $t(\alpha, p)>1$ and $t(\alpha, p)\equiv 1 \pmod p$. Thus clearly $S(x)\leqslant V(x)\leqslant U(x)$ and (1) will follow from ($A(x)$ is the number of integers not exceeding x of the sequence A)

$$U(x)<x\exp\left(-\left(\frac{1}{2}+o(1)\right)\quad(\log x\log\log x)^{1/2}\right) \tag{2}$$

To prove (2) denote by $\psi(x, y)$ the number of integers not exceeding x all whose prime factors are $\leqslant y$. Put $y^z=x$ and assume $z<y^{1/2}\log y$ A theorem of DE BRUIJN then states that

$$\psi(x, y)<c_2\, x(\log x)^2\exp(-z\log z-z\,\mathrm{loglog}\, z+c_3 z). \tag{3}$$

---

* Presented at the 5th Balkan Mathematical Congress (Beograd, 24—30. 06. 1974)

(3) now easily implies (2) and (1). We split the integers $u_i < x$ into two classes. In the first class are the integers $u_i < x$ all whose prime factors are less than $\exp \frac{1}{2} (2 \log x \log\log x)^{1/2}$. In the second class are the other u's. $U_i(x)$, $i = 1, 2$ denotes the number of u's in the i-th class. From (3) we obtain by a simple computation that here $\left(z = \left(\frac{2 \log x}{\log\log x} \right)^{1/2} \right)$

$$U_1(x) < x \exp \left(-\left(\frac{1}{2} + o(1) \right) \quad (\log x \log\log x)^{1/2} \right). \tag{4}$$

For the u's of the second class we evidently have $\left(\text{in } \sum' \text{ the summation is extended over the primes } p > \exp \left(\frac{1}{2} \log x \log\log x \right)^{1/2} \right)$

$$U_2(x) < \sum_p' \sum_{t=1}^{\infty} \left[\frac{x}{p(tp+1)} \right] \leq \sum_p' \sum_{t=1}^{x} \frac{x}{p(tp+1)} \tag{5}$$
$$< \sum' \frac{x}{p^2} \sum_{t=1}^{x} \frac{1}{t} < 2x \log x \sum' \frac{1}{p^2} < x \exp - \left(\frac{1}{2} + o(1) \right) (\log x \log\log x)^{1/2}$$

(4) and (5) proves (2) and (1). With a little more trouble I could prove

$$S(x) \leq U(x) = x \exp - \left(1 + o(1) \right) \quad (\log x \log\log x)^{1/2}. \tag{6}$$

We suppress the details. The principal tool is again a result of DE BRUIJN, namely $\psi(x, y) > \frac{x}{(z!)^{1+\varepsilon}}$.

The true order of magnitude of $S(x)$ is probably much smaller. It is generally conjectured by group theorists that $S(x) < x^{1-\varepsilon}$ and perhaps even $S(x) = o(x^{1/3})$, but our methods are far too crude to prove this. Using $V(x)$ instead of $U(x)$ it should be possible to improve (6) a little bit. Unfortunately not very much since I can show that

$$V(x) > x \exp - c_3 (\log x)^{1/2} \log\log x. \tag{7}$$

I am sure that (7) gives the right order of magnitude for $V(x)$ and in fact that there is a constant c_5 so that

$$V(x) = x \exp - \left(1 + o(1) \right) \; c_5 (\log x)^{1/2} \log\log x$$

but so far I have not been able to prove (7).

References. N. G. DE BRUIJN, *On the number of uncanceled elements in the sieve of Eratosthenes*, Indag. Math. **12** (1950) 247—250, see also: *Of the number of positive integers* $\leq x$ *and free of prime factors* $> y$, ibid. **13**) 1951), 50—60.

L. DORNHOFF, *Simple groups are scarce*, Proc. Amer. Math. Soc. **19** (1968), 692—696.

L. DORNHOFF and E. E. SPITZNAGEL JR., *Density of finite simple group orders*, Math-Zeitschrift, **106** (1968), 175—177.

II. The following problem is due to H. HADWIGER: Denote by $D(n)$ the set of integers with the property that if $k \in D(n)$ then the n-dimensional unit cube can be decomposed into k homothetic n-dimensional cubes. C. MEIER denotes by $c(n)$ the *smallest* integer so that every $k \geqslant c(n)$ belongs to $D(n)$. He proves

$$c(n) \leqslant (2^n-2)\left((2^n-1)^n-(2^n-2)^n-1\right)+1. \tag{1}$$

Earlier W. PLÜSS gave a somewhat greater upper bound. It is easy to see that $c(2)=6$ and in fact $k \in D(2)$ except if $k=2, 3$ or 5. MEIER conjectures $c(3)=48$ and asks for an improvement of (1). He remarks that the problem is attractive because of the interplay of geometric and number theoretic ideas. I agree with him.

First of all *I* give an improvement due to BURGESS and myself of (1). We prove

$$c(n) \leqslant (2^n-2)\left((n+1)^n-2)\right)-1. \tag{2}$$

To prove (2) we first show the following

Lemma. The set of integers k^n-1, $2 \leqslant k \leqslant n+1$ is relatively prime.

Observe that if $p \mid k^n-1$, $2 \leqslant k \leqslant n+1$ we clearly must have $p > n+1$. Thus the congruence $x^n-1 \equiv 0 \pmod p$ has the roots $k=1, 2, \ldots, n+1$ which is a contradiction since it can have at most n roots. This contradiction proves the Lemma.

To prove (2) observe that in the decomposition of the unit cube into smaller cubes, a cube of the decomposition can always be replaced by k^n smaller cubes. Thus every integer of the form

$$\sum_{k=2}^{n+1} c_k (k^n-1), \qquad c_k \geqslant 1$$

belongs to $D(n)$. A well known theorem of A. BRAUER states that if $(a_0, \ldots, a_l) = 1$, $a_1 < \cdots < a_l$ then every integer greater than $(a_1-1)(a_l-1)-1$ can be expressed in the form $\sum_{i=1}^{k} c_i a_i$, $c_i \geqslant 0$, which proves (2).

(2) can in fact be improved. Put $d_k = (a_1, \ldots, a_k)$. A. BRAUER proved that if $d_n=1$ then every integer $\geqslant \sum a_{k+1} d_k/d_{k+1}$ is of the form $\sum_{k=1}^{n} c_k a_k$, $c_k \geqslant 0$, and it is not hard to prove that this gives $c(n) < \alpha n^{n+1}$ for some absolute constant α. I am certain that if $n+1$ is a prime $c(n) > n^n$ but as far as I know HADWIGER's result $c(n) \geqslant 2^n + 2^{n-1}$ is the only lower bound for $c(n)$.

Now we make a few purely number theoretic observations. Denote by $h(n)$ the smallest integer for which the numbers

$$\{2^n-1, 3^n-1, \ldots, h(n)^n-1\}$$

are relatively prime If $n+1=p$ is a prime then $h(n)=n+1$, and it is easy to see that conversely if $h(n)=n+1$ then $n+1=p$. To see this observe that if $p \mid k^n-1$ for every $1 \leqslant k \leqslant n$ then $x^n-1 \equiv 0 \pmod p$ can not have any other roots, but this is possible only if $p=n+1$ (for odd n $(n+1)^n \equiv 1 \pmod p$ and for even n $(n+2)^n \equiv 1 \pmod p$).

Denote by $A(n)$ the greatest prime q_k for which $q_k - 1 \mid n$. Clearly $h(n) \geq q_{k+1}$. But $h(n)$ can be much larger e.g. $h(15) = 5$ and $A(15) = A(2n + 1) = 2$. It is easy to see that for odd n $h(n)$ is unbounded.

I proved (unpublished) that the density of integers n with $A(n) = q_k$ exists. Denote this density by ε_k, $\sum_{k=1}^{\infty} \varepsilon_k = 1$. I can not prove that the density δ_k of integers with $h(n) = q_k$ exists. I am sure that the density exists and $\sum_{k=1}^{\infty} \delta_k = 1$.

It is possible that if $A(n)$ is large (say $> n^{\varepsilon}$) then $A(n) = h(n)$. I can not prove that $h(n)$ does not tend to infinity.

Define now $H(n) = l$ as the least integer so that there is a $k < l$ with $(k^n - 1, l^n - 1) = 1$. Clearly $H(n) \geq h(n)$. Probably $(2^n - 1, 3^n - 1) = 1$ holds for infinitely many n or $H(n) = h(n) = 3$ infinitely often. but I can not prove that $H(n) = h(n)$ holds for infinitely many n. On the other hand I prove that $H(n)$ can be unexpectedly large for suitable values of n. In fact I prove that for infinitely many n $(\exp x = e^x)$

$$H(n) > \exp n^{c_1/(\log\log n)^2}. \tag{3}$$

To prove (3) we use the folloving theorem of PRACHAR. For infinitely many n, n has more than $\exp n^{c_2/(\log\log n)^2}$ divisors of the form $p-1$. Let $p_1^{(n)}, \ldots, p_s^{(n)}$, $s > \exp n^{c_2/(\log\log n)^2}$ be the primes p with $p - 1 \mid n$. Clearly if $(k^n - 1, l^n - 1) = 1$ we must have $kl \equiv 0 \mod \prod_{i=1}^{s} p_i^{(n)}$ or by the prime number theorem $kl \geq \prod_{i=1}^{s} p_i^{(n)} \geq \exp(1 + o(1)) s \log s$ which proves (3).

I have no good upper bound for $H(n)$. It seems likely that there is an absolute constant c so that for every $\varepsilon > 0$

$$H(n) > \exp(n^{(c-\varepsilon)/\log\log n}) \tag{4}$$

holds for infinitely many values of n but for all $n > n_0(\varepsilon)$

$$H(n) < \exp(n^{(c+\varepsilon)/\log\log n}), \tag{5}$$

but I am very far from being able to prove (4) or (5).

Denote by $H_1(n)$ the smallest integer k for which $(k^n - 1, 2^n - 1) = 1$.

Clearly $H_1(n) \geq H(n)$, nevertheless it seems likely that (5) holds for $H_1(n)$ too. I can prove that there is a $c > 0$ so that for $n > n_0(c)$

$$H_1(n) < \exp n^{1-c}. \tag{6}$$

The proof of (6) uses BRUN's method and is somewhat complicated. I do not give it since it seems to fall so far from the final truth.

It might be of interest to investigate the distribution function of the functions $H(n)$ and $H_1(n)$, but I have no results in this direction at present.

References. C. MEIER, *Decomposition of a cube into smaller cubes*, Amer. Math. Monthly **81** (1974), 630—631.

K. PRACHAR, *Über die Anzahl der Teiler einer natürlichen Zahl welche die Form p—1 haben*, Monatshefte für Math. **59** (1954), 91—97.

III. Denote by $\sigma(n)$ the sum of divisors of n and by $\varphi(n)$ EULER's φ function. I state some solved and unsolved problems on these functions. Unless stated otherwise the results are true for both $\sigma(n)$ and $\varphi(n)$. In some cases the behavior of $\sigma(n)$ is more complicated. Denote by $f(x)$ the number of integers $m<x$ for which $\varphi(n)=m$ is solvable. R. R. HALL and I proved that for every k and $\varepsilon>0$ **[1]**

$$\frac{x}{\log x}(\log\log x)^k<f(x)<\frac{x}{\log x}e^{(\log\log x)^{1/2+\varepsilon}}. \tag{1}$$

Probably the upper bound in (1) is close to being best possible but we are far from being able to prove this. Recently HALL proved

$$f(x)>\frac{x}{\log x}(\log\log x)^{c\ \log\log\log x}. \tag{2}$$

It is not immediately clear if there is an asymptotic formula for $f(x)$ in terms of elementary functions. I can not prove that $\lim_{x=\infty} f(2x)/f(x)$ exists; if it exists it must be 2.

I have no nontrivial estimation for the number $A(x)$ of integers $n<x$ for which $\varphi(m)=n$ is solvable only in integers $m>x$. In particular, I do not know if

$$\lim_{x=\infty} A(x)/f(x) \tag{3}$$

exists, also I can not decide if the limit could be 0 or infinity.

Denote by $g(n)$ the number of solutions of $\varphi(m)=n$. SIVASANKARANARAYANA PILLAI proved that $\lim\sup g(n)=\infty$ and I proved that there is an absolute constant $c>0$ so that for infinitely many integers n, $g(n)>c$ **[2]**. I am certain that this holds for every $c<1$ i.e. infinitely often $g(n)>n^{1-\varepsilon}$. This result would follow if one could prove that for every $\varepsilon>0$ the number of primes $p<x$ for which all prime factors of $p-1$ is less that p^ε is greater than $c_\varepsilon x/\log x$, but this conjecture though no doubt true is certainly very deep.

I can not prove that the equation $\sigma(n)=\varphi(m)$ has infinitely many solutions, though this certainly must be true. I proved that there are infinitely many even numbers not of the form $\sigma(n)-n$ [3] but can not prove that there are infinitely many even numbers not of the form $n-\varphi(n)$. I can not prove that the density of integers of the form $n+\varphi(n)$ (and $n+\sigma(n)$) is positive. I can not prove that for every $\alpha\geqslant 1$ there is a sequence of integers n_k and m_k satisfying $n_k/m_k\to\alpha$, $\sigma(n_k)=\sigma(m_k)$ (it is easy to prove the analogous result for $\varphi(n)$). I can not prove that there is a $\beta>1$ for which

$$|\sigma(n)-\beta_n|\to\infty \text{ as } n\to\infty.$$

In a previous paper **[4]**, I state the following question: Denote by $h(x)$ the number of solutions of $\sigma(a)=\sigma(b)$, $(a,b)=1$, $a<b<x$.

Prove that $h(x)/x\to\infty$.

I sketch a proof of

$$\limsup_{x=\infty} \frac{h(x)}{x} = \infty. \tag{4}$$

The proof of $\frac{h(x)}{x} \to \infty$ can be produced with a little more trouble.

Observe that if a and b are squarefree and $\sigma(a) = \sigma(b)$, then there are uniquely determined integers $a_1, b_1, (a_1, b_1) = 1, a = a_1 t, b = b_1 t$ and of course $\sigma(a_1) = \sigma(b_1)$. Thus if $h(y) < c$ for every y then the number $R(x)$ of solutions of the equation

$$\sigma(a) = \sigma(b), \quad a < b < x, \quad a, b \text{ squarefree} \tag{5}$$

is easily seen to be less than $cx \log x$.

Now we outline the proof that this is not true. In fact we show that for every k and $x > x_0(k)$

$$R(x) > x(\log x)^k. \tag{6}$$

The proof of (6) is fairly complicated thus we do not give many details. I am sure that (6) is very far from the final truth and believe that for every $\varepsilon > 0$ and $x > x_0(\varepsilon)$, $R(x) > x^{2-\varepsilon}$ and also $h(x) > x^{2-\varepsilon}$.

Denote by $v(n)$ the number of distinct prime factors of n. We first observe that for almost all n

$$v(\sigma(n)) = (1/2 + o(1)) \quad (\log\log n)^2. \tag{7}$$

The detailed proof of (7) is fairly complicated. Here is an outline of the proof. By a theorem of mine [**2**]

$$\sum{}' 1/p < \infty \tag{8}$$

where the summation is extended over the primes p for which $v(p-1) < (1-\varepsilon)\log\log p$. Another theorem of mine states that if p_k is the k-th prime factor of n then [**5**]

$$\exp\exp k(1-\varepsilon) < p_k < \exp\exp k(1+\varepsilon) \tag{9}$$

holds for all $k > k_0(\varepsilon, n)$ if we neglect ηx integers $n \leqslant x$. (7) follows from (8) and (9) without much difficulty.

(7) easily implies (6) since by a theorem of Hardy and Ramanujan [**6**] the number of integers $n < x$ for which $v(n) > \varepsilon(\log\log n)^2$ is $o\left(\frac{x}{(\log x)^k}\right)$.

[1] P. Erdös and R. R. Hall, *On the values of Euler's φ-function* Acta Arithmetica, **22** (1972), 201—206.

[2] P. Erdös, *On the nominal number of, prime factors of p-1 and some related problems concerning Euler's φ-function*, Quarterly J Math **6** (1935), 205—213

[3] P. Erdös, *Über die Zahlen der Form σ(n)−n und n−φ(n)*, Elemente der Mathematik **28** (1973), 83—86.

[4] P. Erdös, *Remarks on number theory* II. *Some problems on the σ function*, Acta Arith. **5** (1959), 171—177.

[5] P. Erdös, *On the distribution function of additive functions*, Annals of Math. **47** (1946), 1—20, see p. 3—4.

[6] Hardy and Ramanujan, Quarterly J. Math. **48** (1917), 76—92, see also Ramanujan, Collected papers.

(Došlo 04. 10. 1974)

ERDÖS P. (Budapest, Hungary)

4.33. (1974) 203—204

PROBLEMS*

4.33.1. *Problem of* S. J. BENKOSKI *and* P. ERDÖS.

Put $\sigma(n)=\sum_{d/n} d$. Is there an absolute constant C so that every integer n satisfying $\sigma(n)>Cn$ is the distinct sum of proper divisors of n?

Remarks. $\sigma(70)=144>2.70$ but 70 is not the distinct sum of proper divisors of 70, but as far as we know C could be three:

S. J. BENKOSKI and ERDÖS, *On weid and pseudoperfect numbers*, Mathematics of computation, **28** (1974), 617-623.

4.33.2. *Problem of* P. ERDÖS *and* STRAUS.

I. Are there infinitely many primes p_k so that, for every $i<k$, $p_k^2>p_{k+i}\,p_{k-i}$ (p_k is the k-*th* prime).

II. Denote by $\nu(n)$ the number of distinct prime factors of n and by $d(n)$ the number of divisors of n. Is it true that there is an infinite sequence $n_1<n_2<\cdots$ of integers satisfying

(1) $\nu(n_k+i)<c_1 i$ for every $i>0$ and c_1 is an absolute constant?

If the answer is affirmative is there an infinite sequence $m_1<m_2<\cdots$ so that

$$d(m_k+i)<c_2\,i? \tag{2}$$

(1) can perhaps be proved by an improvement of BRUNS method; (2), if true, is certainly very deep.

4.33.3. Denote by $f(n)$ the smallest integer so that every $1\leqslant m\leqslant n!$ is the sum of $f(n)$ or fewer distinct divisors of n. I proved $f(n)<n$. The proof is by induction and is simple. Prove or disprove: $f(n)<(\log n)^c$ for an absolute constant c and $n>n_0(c)$. I could not even prove $f(n)=o(n)$.

4.33.4. Prove that to every constant C there is an integer n for which $\sigma(n)/n>C$ and whose divisors do not give the moduli of a system of covering congruences. In other words if $1<d_1<d_2<\cdots<d_k=n$ is the set of all divisors greater than 1 of n and a_i, $1\leqslant i\leqslant k$ are arbitrary integers, there always is an integer m so that for every i, $1\leqslant i\leqslant k$ $m\not\equiv a_i \pmod{d_i}$.

4.33.5. Denote by $f(n;t)$ the smallest integer with the property that if we split the integers $1\leqslant m\leqslant n$ into two classes there always is an arithmetic progression of n terms at least t of which belongs to the same class; $f(n;n)=f(n)$ is the well known VAN DER WAERDEN function the finiteness of which is guaranteed by VAN DER WAERDEN's theorem. No satisfactory upper bound is known for $f(n)$; $f(n)\geqslant 2^{n/2}$ was proved by RADO and myself; W. SCHMIDT proved $f(n)>2^{n-c\sqrt{n\log n}}$ and BERLEKAMP proved $f(p)\geqslant p\,2^p$ for primes p. Perhaps $f(n)^{1/n}$ tends to infinity. $f(n;t)$ is interesting only for $t>\dfrac{n}{2}$. Clearly, for

* Presented the 28.06.1974 at the *problem session* of the 5th Balkan Mathematical Congress (Beograd, 24—30.06.1974)

$t \leqslant \frac{n}{2}$, $f(n;t)=n$. I proved that $f(n;t)>(1+c_\varepsilon)^n$ for $t>(1+\varepsilon)\ \frac{n}{2}$. Perhaps $f\left(n;\left[\frac{n}{2}(1+\varepsilon)\right]\right)<C_\varepsilon^n$ holds for sufficiently large C_ε if ε is sufficiently small, but I was not able to prove anything in this direction. In fact I can get no usable upper bound for $f(n;t)$ for $t=\frac{n}{2}+o(n)$. J. SPENCER proved that if $n=2^l m$ then

$$f\left(n;\left[\frac{n}{2}\right]+1\right)=2^t(n-1)+1$$

but we do not know the value of $f\left(n;\left[\frac{n}{2}\right]+2\right)$ and in fact have no satisfactory upper bound for it.

P. ERDÖS and R. RADO, *Combinatorial theorems on classifications of subsets of a given set*, Proc. London Math. Soc. **2** (1952), 417—439.

W. SCHMIDT, *Two combinatiorial theorems on arithmetic progressions*, Duke Math. J. **29** (1962), 129—140.

E. R. BERLEKAMP, *A construction for partitions which avoid long arithmetic progressions*, Bull. Canad. Math. Soc. **11** (1968), 409—414.

J. SPENCER, *Problems* 185 Bull. Canad. Math. Soc. **16** (1973), 185.

4.33.6*. Let $a_1<a_2<\cdots$ be an infinite sequence of integers for which $\sum_{i=1}^{\infty}\frac{1}{a_i}=\infty$. Then our sequence contains arbitrarily long arithmetical progressions.

I offer 2 500 dollars for a proof or disproof of this conjecture. The conjecture would imply that for every k there are k primes in an arithmetic progression.

SZEMERÉDI recently proved an old conjecture of TURÁN and myself: If $a_1<a_2<\cdots$ has positive upper density, then it contains arbitrarily arithmetic progressions. SZEMERÉDI's ingenious proof will soon appear in Acta Arithmetica.

4.33. 7*. Let E be an infinite set of real numbers. Prove that there is a set of real numbers S of positive measure which does not contain a set E' similar (in the sense of elementary geometry) to E.

We can of course assume that E is denumerable, its only limit point is 0 which is not in E.

4.33.8*. Put $\frac{n}{2^n}=\alpha_n$. **8.1** Is it true that every α_n is the finite sum of other α' s?

8.2. Is it true that $\sum_{k=1}^{\infty}\alpha_{n_k}$ is irrational if $n_k/k\to\infty$?

8.3. Is there a rational number x for which $x=\sum_{l=1}^{\infty}\alpha_{n_l}$ has $2^{\aleph_0}$ solutions.

(Došlo 04. 10. 1974).

P. Erdös
Mathematical institute
Budapest, Hungary