Astérisque

PAUL ERDÖS

Some unconventional problems in number theory

Astérisque, tome 61 (1979), p. 73-82

<http://www.numdam.org/item?id=AST_1979__61__73_0>

© Société mathématique de France, 1979, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Société Mathématique de France
Astérisque 61 (1979) p. 73-82

SOME UNCONVENTIONAL PROBLEMS IN NUMBER THEORY

by

Paul ERDÖS

I have several papers with a similar title which will be published soon - at least one of them is a joint paper with R.R. Hall. The number of unsolved problems is so large that I can keep the overlap to a minimum.

First of all I state a very old conjecture of mine : the density of integers n which have two divisors d_1 and d_2 satisfying $d_1 < d_2 < 2 d_1$ is 1 . I proved long ago [1] that the density of these numbers exists but I have never been able to prove that it is 1 . I claimed [2] that I proved that almost all integers n have two divisors

$$(1) \qquad d_1 < d_2 < d_1 \left(1 + \left(\frac{e}{3}\right)^{1 - \eta \log\log n}\right)$$

and that (1) is best possible, namely it fails if $1 - \eta$ is replaced by $1 + \eta$. R.R. Hall and I confirmed this later statement but unfortunately we cannot prove (1) . We are fairly sure that (1) is true and perhaps it is not hopeless to prove it by methods of probabilistic number theory which are at our disposal.

Denote by $d^+(n)$ the number of integers k for which n has a divisor d satisfying $2^k < d \leq 2^{k+1}$. I conjecture that for almost all n

$$d^+(n) / d(n) \to 0$$

which of course implies that almost all integers have two divisors satisfying $d_1 < d_2 < 2 d_1$. It would be of some interest to get an asymptotic formula for

$$\sum_{n=1}^{X} d^+(n) = F(X) \quad .$$

It is easy to prove that $F(X) / X \log X \to 1$.

Another interesting and unconventional problem states as follows : let $1 = d_1 < d_2 < \ldots < d_{\tau(n)} = n$ be the set of divisors of n .

Put :

$$G(n) = \sum_{i=1}^{\tau(n)-1} d_i / d_{i+1} \quad .$$

I conjecture that $\varphi(n) \to \infty$ if we disregard a sequence of integers n of density 0. This again would imply the conjecture on $d_1 < d_2 < 2d_1$, but needless to say I cannot prove it.

It would be of interest to determine the normal order of $d^+(n)$ and $\varphi(n)$ (or at least of $\log \varphi(n)$ and $\log d^+(n)$). Also an asymptotic formula for

$$\sum_{n=1}^{x} \varphi(n)$$

would be of interest. It is easy to prove that $\frac{1}{x} \sum_{n=1}^{x} \varphi(n) \to \infty$.

Let $p_1 < \ldots < p_{V(n)}$ be the consecutive prime factors of n. Alladi and I proved that (unpublished):

$$f(n) = \sum_{i=1}^{V(n)-1} p_i/p_{i+1}$$

has a distribution function and a bounded average.

A well-known theorem of Hardy and Ramanujan states that the normal order of $V(n)$ (the number of prime factors of n) is $(1 + o(1))\log\log n$. A special case of our well-known theorem with Kac [3] states that

$$\frac{V(n) - \log\log n}{(\log\log n)^{1/2}}$$

has normal distribution.

More than 40 years ago I proved that if $p_1^{(n)} < \ldots < p_{V(n)}^{(n)}$ are the consecutive prime factors of n, then for almost all n the v-th prime factor of n satisfies

$$\log\log p_v^{(n)} = (1 + o(1))v \tag{2}$$

More precisely: the every $\varepsilon > 0$, $\eta > 0$ there is an $\ell_0 = \ell_0(\varepsilon, \eta)$ so that the density of integers n for which for every $\ell_0 < v \leq V(n)$

$$v(1 - \varepsilon) < \log\log p_v^{(n)} < (1 + \varepsilon)v \tag{2'}$$

is greater than $1 - \eta$ [4]. I do not prove (2) in [4], I only indicate that it is a special case of a result which can easily be deduced by methods of probabilistic number theory.

(2) seems to me to be interesting and has many applications, thus at the end of this paper I give a direct and simple proof of (2) . A similar proof of (2) is outlined in a forthcoming paper of S. Wagstaff and myself. This paper also deals with an unconventional problem. Let B_n be the n-th Bernoulli number and

$$\frac{a_n}{b_n} = \sum_{p-1 \mid n} \frac{1}{p}$$

its fractional part. Let n be the smallest integer with this fractional part. Then the density d_n of integers m with fractional part a_n/b_n exists and $\sum_n' d_n = \infty$ where the dash indicates that the summation is only extended over the n which have fractional part a_n/b_n and are minimal (our paper will soon appear in Illinois J. of Math.).

Denote by $d_v(p)$ the density of the integers n whose v- th prime factor is n . $d_v(p)$ can easily be calculated by the exclusion - inclusion principle (essentially the sieve of Eratosthenes). By (2), for almost all integers, $p_v^{(n)}$ is about expexp v . On the other hand, it is easy to see that the largest value of $d_v(p)$ is assumed for much smaller values of p , in fact for

$$e^{v(1-\varepsilon)} < p < e^{v(1+\varepsilon)}$$

by more careful computation it would easily be possible to obtain better estimates. The simple explanation for this apparent paradox is that there are very much more values of p at e^{e^v} than at e^v . It is not impossible that $d_v(p)$ is unimodular, i.e. it first increases with p then assumes its maximum and then decreases. I in fact doubt that $d_v(p)$ behaves so regularly but have not disproved it. The same problems arise if $d_v(n)$ denotes the density of the integers m whose v-th divisor is n . Here we obtain that if $D_1 < D_2$ are the consecutive divisors of n then for all but εX integers $n < X$ for $v > v_0(\varepsilon, n)$

$$\exp(v^{1/\log 2 - \varepsilon}) < D_v < \exp(v^{1/\log 2 + \varepsilon}) \quad .$$

On the other hand, for fixed v , $d_v(n)$ is maximal for

$$\exp((1-\varepsilon)\log v \ \log\log v) < D_v < \exp((1+\varepsilon)\log v \ \log\log v).$$

It can be shown that $d_v(n)$ is not unimodular.

I now state some further results on the prime factors of integers which can be obtained by the methods of probabilistic number theory or also by more elementary but longer computations. Some of these results have been stated in [5] .

For almost all integers n :

$$\sum' \frac{1}{v} = (\frac{1}{2} + o(1)) \operatorname{loglog} n$$

where the dash indicates that the summation is extended over the v satisfying $\operatorname{loglog} p_v^{(n)} > v$.

Similarly, for almost all n :

$$\sum_{p_v^{(n)} > p_v^{(n+1)}} \frac{1}{v} = (\frac{1}{2} + o(1)) \operatorname{loglog} n .$$

On the other hand, it is not hard to show that it is not true that for almost all n :

$$\sum' 1 = (\frac{1}{2} + o(1)) \operatorname{loglog} n$$

On the other hand, if $v_{i+1} > (1 + c) v_i$, then for almost all n :

$$(3) \qquad \sum_{\operatorname{loglog} p_{v_i}^{(n)} > v_i} 1 = (\frac{1}{2} + o(1)) \sum_{v_i < \operatorname{loglog} n} 1$$

It easily follows from the methods of [3] that

$$\frac{\operatorname{loglog} p_v^{(n)} - v}{v^{1/2}}$$

has normal distribution, and that if $v_1/v_2 \to \infty$, then

$$\frac{\operatorname{loglog} p_{v_1}^{(n)} - v_1}{v_1^{1/2}} \quad \text{and} \quad \frac{\operatorname{loglog} p_{v_2}^{(n)} - v_2}{v_2^{1/2}}$$

are asymptotically independent. (3) follows from this without too much difficulty.

For further results of this type see [5] . Here we just make two more remarks. (2) does not mean that $p_v^{(n)}$ is really close to e^{e^v} . In fact, the following results hold.

Let $\alpha(v)$ tend to 0 monotonically as v tends to infinity. Denote by $h_\alpha(n)$ the number of v-s for which the v-th prime factor $p_v^{(n)}$ of n satisfies :

$$v - \alpha(v) < \log\log p_v^{(n)} < v + \alpha(v)$$

Then, if $\sum_{v=1}^{\infty} \alpha(v)/v^{1/2} < \infty$, for every k the density β_k of integers n for which $h_\alpha(n) = k$ exists and $\sum_{k=1}^{\infty} \beta_k = 1$ (or roughly speaking $h_\alpha(n)$ is almost always bounded and $h_\alpha(n)$ has a distribution function).

If $\sum_{v=1}^{\infty} \alpha(v)/v^{1/2} = \infty$, then $h_\alpha(n) \to \infty$ for almost all n .

In particular, for almost all n ,

$$\sum{}' 1/v^{1/2} = (1 + o(1))\, c \log\log\log n$$

where the summation is extended over the v for which $v < \log\log p_v^{(n)} < v + 1$. On the other hand, it is not true that for almost all n

$$\sum{}' 1 = (1 + o(1))\, c_1 (\log\log n)^{1/2} \qquad (4)$$

.

The order of magnitude of the left side of (4) is $(\log\log n)^{1/2}$ and with more trouble the distribution function could be calculated.

Let $p_1 < p_2 < \ldots$ be an infinite sequence of primes, it is quite easy to prove that

$$\sum 1/p_i = \infty$$

is the necessary and sufficient condition that almost all integers n should have a prime factor p_i . It seems very difficult to obtain a necessary and sufficient condition that if $a_1 < \ldots$ is a sequence of integers then almost all integers n should be a multiple of one of the a's . I just want to illustrate the difficulty by a simple example : let $n_{i+1} > (1 + c)\, n_i$. Consider the integers m which have a divisor d satisfying $n_k < d < n_k (1 + \eta_k)$.

If $\sum_{h=1}^{\infty} \eta_k < \infty$ then it is easy to see that the density of these integers exists and is less than 1 .

If $\sum_{h=1}^{\infty} \eta_k = \infty$ it seems difficult to get a general result, e.g. if $\eta_k = \frac{1}{k}$ the density in question exists and is less than 1 .

It seems certain that there is an α, $0 < \alpha < 1$ so that if $\beta < \alpha$ and $\eta_k = 1/k^\beta$ the density of the m having a divisor d, $n_k < d < n_k(1 + 1/k^\beta)$ is 1 and if $\beta > \alpha$ it is less than 1.

Denote by $\varepsilon(n, m)$ the density of integers having a divisor d satisfying $n < d < m$ and by $\varepsilon'(n, m)$ the density of integers having precisely one divisor d, $n < d < m$. Besicovitch proved $\liminf \varepsilon(n, 2n) = 0$ and I proved that if $\log m/\log n \to 1$, then $\lim \varepsilon(n, m) = 0$ [6].

It is easy to see that this result is best possible, i.e. $\lim \varepsilon(n, m) = 0$ implies $\log m/\log n \to 1$.

Further, I can prove that :

$$\varepsilon'(n, m) < c/(\log n)^\alpha$$

for a certain $0 < \alpha < 1$. Perhaps $\varepsilon'(n, m)$ is unimodular for $m > n + 1$, but I know nothing about this. I don't know where $\varepsilon'(n, m)$ assumes its maximum.

I am sure that :

$$\varepsilon'(n, m) / \varepsilon(n, m) \to 0$$

for $m = 2n$. If $m - n$ is small, then clearly $\varepsilon'(n, m) / \varepsilon(n, m) \to 1$ and I don't know where the transition occurs.

Some time ago the following question occured to me : let k be given $n > n_0(k)$. Is there an absolute constant α so that for every $n < m < n^k$ there is a t, $0 < t < (\log n)^\alpha$ so that $m + t$ has a divisor in $(n, 2n)$?

More generally : if $n + 1 = a_1 < a_2 < \dots$ is the sequence of integers which have a divisor d, $n < d < 2n$. Determine or estimate $\max_{a_i < n^k} (a_{i+1} - a_i)$.

Now we prove (2) and (2') . Denote by $V(n)$ the number of prime factors of n and by $V_{T(n)}$ the number of prime factors of n exceeding T. The well known inequality of Turán [7] implies

$$(5) \qquad \sum_{n=1}^{X} (V_T(n) - \operatorname{loglog} T)^2 < C X \operatorname{loglog} T,$$

where C is an absolute constant. From (5) we immediately obtain by the Tchebicheff inequality that the number of integers $n < X$ satisfying

$$(6) \qquad |V_T(n) - \operatorname{loglog} T| < Z(\operatorname{loglog} T)^{1/2}$$

is less than $C X/Z^2$.

Put $T_i = (\exp\exp i^4)$. From (6) we obtain that the number of integers $n < X$ for which some $i > i_o$

$$(7) \qquad |V_{T_i}(n) - \log\log T_i| > (\log\log T_i)^{3/4}$$

is less than

$$(8) \qquad C X \sum_{i > i_o} \frac{1}{i^2} < \varepsilon X$$

for every $\varepsilon > 0$ if $i_o > i_o(\varepsilon)$. To complete our proof observe that $V_T(n)$ is nondecreasing in T . Thus, if $T_i < T < T_{i+1}$ and n satisfies (7), we have

$$(9) \qquad |V_T(n) - \log\log T| < (\log\log T_i)^{3/4} + \log\log T_{i+1}$$

$$\log\log T_i < 10\,(\log\log T)^{3/4} \ .$$

Thus, from (7), (8) and (9) it follows that (2) and (2') are satisfied for almost all n and our proof is complete.

Finally I state an old problem of mine which is probably very difficult and which seems to be unattackable by the methods of probabilistic number theory : denote by $P(n)$ the greatest prime factor of n . Is it true that the density of integers n satisfying $P(n+1) > P(n)$ is $\frac{1}{2}$? Is it true that the density of integers for which

$$(10) \qquad P(n+1) > P(n)\, n^{\alpha}$$

exists for every α ? Pomerance and I proved (our paper will soon appear in Aequationes Mathematica) that if $\varepsilon_n \to 0$ then the upper density of the integers satisfying

$$n^{-\varepsilon_n} < \frac{P(n+1)}{P(n)} < n^{\varepsilon_n}$$

tends to 0 as n tends to ∞ .

To end this note, I state a few unrelated unconventional problems. Denote by $\Phi(X)$ the number of integers $n < X$ for which $\varphi(m) = n$ is solvable ($\varphi(n)$ is Euler's φ function). The sharpest current bounds for $\Phi(X)$ are due to R.R. Hall and myself [8].

We prove (for every $\varepsilon > 0$ and $X > X_0(\varepsilon)$)

$$(11) \qquad \frac{X}{\log X} \exp((\log\log\log X)^2) < \Phi(X) < \frac{X}{\log X} \exp(C_1 (\log\log X)^{1/2}) .$$

It seems to us that the upper bound in (11) is closer to the truth, in fact we believe that for every $\varepsilon > 0$ and $X > X_0(\varepsilon)$

$$\Phi(X) > \frac{X}{\log X} \exp(C_2 (\log\log X)^{1/2}) .$$

It is not certain that there is a genuine asymptotic formula for $\Phi(X)$ but perhaps $\Phi(CX)/\Phi(X) \to C$ holds for every $C > 0$.

Denote $\Phi_K(X)$ the number of distinct integers n of the form $\varphi(kX + t)$, $1 \le t \le X$. For "small" k all the $\Phi_K(X)$ probably have a similar asymptotic behaviour, but of course I can prove nothing. I have no idea how many new integers appear amongst the $\varphi(kX + t)$, $1 \le t \le X$. In other words : estimate the number of integers $n < X$ for which the smallest solution of $\varphi(m) = n$ satisfies $kX < m \le (k+1)X$. I can at the moment say nothing interesting about this problem.

Denote by m_X the largest integer for which $\varphi(m_X) \le X$ and by m'_X the largest integer for which $\varphi(m'_X) \le X$ and for which there is no $u < m'_X$ with $\varphi(u) = \varphi(m'_X)$. In other words m'_X is the largest integer for which $\varphi(m'_X) \le X$ and which gives a new number of the form $\varphi(m)$. I hope that $m'_X/m_X \to 1$ but I do not see how to prove this. Perhaps $m'_X = m_X$ holds for infinitely many X .

Let $u_1^{(n)} < \ldots < u_t^{(n)}$ be the set of integers (if they exist) for which $\varphi(u_i) = n$, $1 \le i \le t$. An old (and probably hopeless) conjecture of Carmichael states that $t \ge 1$ implies $t > 1$. It would be perhaps interesting to investigate

$$\max_{n < X} u_t^{(n)} / u_1^{(n)} .$$

One final question about the φ - function : let $p^{(n)}$ be the smallest prime $\equiv 1 \pmod n$. By a classical result of Linnik [9] $p^{(n)} < n^{1+C}$. Let u_n be the smallest integer with $\varphi(u_n) \equiv 0 \pmod n$. If $n = p - 1$ we of course have $u_n = p^{(n)}$ and it is easy to show that for infinitely many n $u_n < p^{(n)}$. $u_n/n \to \infty$ stets for almost all n . The proofs are not difficult.
I am sure that $p^{(n)}/u_n \to \infty$ holds for almost all n .

Let $q_1 < q_2 < \dots$ be a sequence of primes for which $q_{i+1} \equiv 1 \pmod{q_i}$. It easily follows from the theorem of Linnik [9] that there is an infinite sequence of such primes satisfying for every i $q_i < (\exp\exp C i)$ for some absolute constant C. In fact, there is little doubt that such a sequence exists with $q_i < \exp(i (\log i)^{1+\varepsilon})$. I am fairly certain that for every such sequence $\lim_{i=\infty} q_i^{1/i} = \infty$ but I have never been able to prove this.

Denote by $h(n)$ the largest integer ℓ for which there is a sequence of prime divisors $p_i^{(n)}$ of n for which

$$p_{i+1}^{(n)} \equiv 1 \pmod{p_i^{(n)}}, \quad 1 \le i \le \ell - 1 = h(n) - 1 .$$

It is easy to see that $h(n)$ tends to infinity for almost all n. Denote by $L(n)$ the smallest integer v for which the v-times iterated logarithm of n is less than e. It seems that the normal order of $h(n)$ is about $L(n)$ but I have not carried out all the details. Denote by $H(n)$ the largest integer u for which there is a sequence of divisors d_i of n, $1 \le i < u-1$ for which $d_{i+1} \equiv 1 \pmod{d_i}$.

I am not sure if $H(n)/h(n) \to \infty$ holds for almost all n, I am sure that $H(n)$ is not much larger than $L(n)$. The estimation of $H(n)$ is related to the following question: denote by $A(d, \alpha)$ the density of integers n which have a divisor $D \equiv 1 \pmod{d}$, $1 < D < \exp d^{\alpha}$. For $\alpha < 1$, $A(d, \alpha) \to 0$ is trivial. I can prove $A(d, 1) \to 0$ as $d \to \infty$. This last result is not quite trivial since

$$\sum{}' \frac{1}{D} = 1 + o(1)$$

where the dash indicates that $1 < D < \exp d$, $D \equiv 1 \pmod{d}$.

I believe that there is an α, $1 < \alpha < \infty$ so that for $\beta < \alpha$ $\lim_{d=\infty} A(d, \beta) = 0$ and for $\beta > \alpha$ $\lim_{d=\infty} A(d, \beta) = 1$.

REFERENCES

[1] P. Erdös On the density of some sequences of integers, Bull. Amer. Math. Soc. 54 (1948), 685-692.

[2] P. Erdös On some applications of probability to analysis and number theory, J. London Math. Soc. 39 (1964), 692-696.

[3] P. Erdös and M. Kac
The Gaussian law of errors in the theory of additive number theoretic functions, Amer. J. Math. 62 (1940), 738-742.

[4] P. Erdös On the distribution function of additive functions, Annals of Math. 47 (1946), 1-20.

[5] P. Erdös On the distribution of prime divisors, Aequationes Mathematicae 2 (1969), 177-183.

[6] See e.g. the well known book of H.H. Halberstam and K.F. Roth, Sequences, Oxford, Calenron Press 1966, Chapter V.

[7] P. Turán On a theorem of Hardy and Ramanujan, J. London Math. Soc. 9 (1934), 274-276.

[8] P. Erdös and R.R. Hall
On the values of Euler's φ function. Acta Arith. 22 (1973), 201-206 and Distinct values of Euler's φ function.

[9] K. Prachar Primzahlverteilung, Springer Verlag, 1957.

Paul ERDÖS
Mathematical Institute of the Academy
BUDAPEST
V. Realtanoda u 13-15
HONGRIE