Math. Proc. Camb. Phil. Soc. (1976), **79**, 281
MPCPS 79–22
Printed in Great Britain

Proof of a conjecture about the distribution of divisors of integers in residue classes

BY P. ERDÖS AND R. R. HALL
Trinity College, Cambridge, and University of York

(*Received* 23 *December* 1974)

Introduction. Let k be a positive integer and $F(x,k)$ denote the number of integers $n < x$ which have a divisor in every residue class prime to k. Erdös (1) proved that for every fixed $\epsilon > 0$, we have $F(x,k) \sim x$ when

$$k < 2^{(1-\epsilon)\log\log x}, \quad x \to \infty,$$

and conjectured the following result, which we prove in this paper.

THEOREM. *Let c be any fixed real number and k and x satisfy the relation*

$$k = 2^{\log\log x + (c+o(1))\sqrt{(\log\log x)}}, \tag{1}$$

then as $x \to \infty$, we have

$$F(x,k) \sim \frac{x}{\sqrt{(2\pi)}} \int_c^\infty e^{-\frac{1}{2}v^2} dy. \tag{2}$$

Remarks. Let $\nu(n)$ denote the number of distinct prime factors of n, so that n has at least $2^{\nu(n)}$ divisors. It is well known that

$$\operatorname{card}\left\{n < x : \frac{\nu(n) - \log\log x}{\sqrt{(\log\log x)}} > c\right\} \sim \frac{x}{\sqrt{(2\pi)}} \int_c^\infty e^{-\frac{1}{2}v^2} dy, \tag{3}$$

so that an intuitive statement of the theorem is that the numbers with sufficient divisors to fill the required residue classes almost surely will do so.

The result was proved by Hall (2), subject to a hypothesis about the Siegel zero (if such exists) of the Dirichlet L-functions (mod k), which is stronger than Siegel's theorem. Precisely, if $\xi(k) \to 0$ arbitrarily slowly as $k \to \infty$, and the L-functions (mod k) have no real zero in the interval

$$(1 - \exp(-\xi(k)\log^{\frac{1}{2}} k), 1)$$

then (2) holds. In our proof we need no information about the precise location of the Siegel zero, only that there is at most one, and that it is the zero of an L-function induced by a real Dirichlet character, which is well known.

The following lemma about finite Abelian groups is the fundamental result needed in the proof.

LEMMA. *Let G be an Abelian group of even order N, and H be a subgroup of G of index* 2. *Then for any $\delta > 0$, the number of choices of t elements $g_1, g_2, \ldots, g_t$ of G of which precisely r lie in H, and such that not every $g \in G$ has a representation in the form*

$$g = \epsilon_1 g_1 + \epsilon_2 g_2 + \ldots + \epsilon_t g_t, \quad (\textit{each } \epsilon_i = 0 \textit{ or } 1),$$

does not exceed

$$\delta\binom{t}{r}\left(\frac{N}{2}\right)^t \tag{4}$$

whenever $r < t$ *and*

$$t\log 2 \geqslant \log N + \log\frac{1}{\delta} + \log\frac{\log N}{\log 2} + 5.$$

Remarks. The condition $r < t$ is plainly necessary: if $r = t$ we can only represent elements of H. If every element of G is to be represented, we must have $2^t \geqslant N$ and our condition on t is not much stronger than this.

The result is an extension to Theorem 2 of Erdös and Rényi (3) where there was no restriction on the choice of the t elements $g_1, g_2, \ldots, g_t$. The upper bound corresponding to (4) was δN^t, and the essential feature of the present result is that (except when $r = t$) the upper bound in (4) is always a proportion δ of the number of possible choices of the elements.

Proof. For any particular choice of $g_1, g_2, \ldots, g_t$ let $R(g)$ denote the number of representations of g in the required form. Then

$$R(g) = \frac{1}{N}\sum_{\chi}\overline{\chi}(g)\prod_{i=1}^{t}(1+\chi(g_i))$$

where the sum is over all characters χ of G. Hence we have

$$\sum_{g\in G}\left(R(g)-\frac{2^t}{N}\right)^2 = \frac{1}{N}\sum_{\chi\neq\chi_0}\prod_{i=1}^{t}|1+\chi(g_i)|^2,$$

where χ_0 is the principal character. Let χ_1 be the character such that $\chi_1 \neq \chi_0$ and $\chi_1(h) = 1$ for every $h \in H$. We must have $\chi_1(g) = -1$ whenever $g \notin H$ so that χ_1 is unique. For any set of t elements of G we write

$$s = \sum_{i=1}^{t}\chi_1(g_i)$$

so that $s = 2r - t$ if and only if precisely r of these elements belong to H. We now form the sum

$$\Sigma z^s \sum_{g\in G}\left(R(g)-\frac{2^t}{N}\right)^2,$$

where the sum is over all choices of t elements of G, and s and R refer to the particular choice. From the above, this is equal to

$$\frac{1}{N}\sum_{\chi\neq\chi_0}\left[\sum_{g\in G} z^{\chi_1(g)}|1+\chi(g)|^2\right]^t$$

and the inner sum is equal to $N(z+1/z)$ if $\chi \neq \chi_1$ (since χ is then non-principal as a character of H), and equal to $2Nz$ when $\chi = \chi_1$. Therefore

$$\Sigma z^s \sum_{g\in G}\left(R(g)-\frac{2^t}{N}\right)^2 = \left(1-\frac{2}{N}\right)N^t\left(z+\frac{1}{z}\right)^t + N^{t-1}(2z)^t.$$

For convenience we refer to a set of t elements of G of which precisely r belong to H as a (t,r)-set, and we denote by $\Sigma_{(r)}$ summation over all (t,r)-sets. Equating

coefficients of z^{2r-t} in the above, we deduce that

$$\Sigma_{(r)} \sum_{g \in G} \left(R(g) - \frac{2^t}{N}\right)^2 = \binom{t}{r}\left(1 - \frac{2}{N}\right) N^t, \quad (r < t),$$

and

$$\Sigma_{(t)} \sum_{g \in G} \left(R(g) - \frac{2^t}{N}\right)^2 = \left(1 - \frac{2}{N}\right) N^t + 2^t N^{t-1}.$$

It follows from the first relation that provided $r < t$, the number of (t, r)-sets which fail to represent at least $\lambda N^2 2^{-t}$ elements of G does not exceed

$$\frac{1}{\lambda}\binom{t}{r}\left(\frac{N}{2}\right)^t \tag{5}$$

for any $\lambda > 0$. Notice that this is a proportion $1/\lambda$ of the total number of (t, r)-sets.

The idea of the remainder of the proof is as follows. We begin by considering (t_1, r_1)-sets, where $r_1 < t_1 < t$: given such a set, which we suppose already represents a large number of elements of G, we add $t - t_1$ further elements to the set one at a time, at each stage considering how many more elements of G may be represented. We can expect that the number of elements represented is about doubled at each stage. In order to fix our ideas, we suppose that the (t, r)-set is constructed by choosing the elements which do not belong to H first: we are interested in the case $r < t$ and so when we have chosen t_1 of the elements we have a (t_1, r_1)-set where

$$r_1 = \max(0, t_1 - (t - r)) < t_1$$

as specified above.

We use a counting argument and the language of probability is appropriate. The elements $g_1, \ldots, g_t$ are chosen independently of each other, the first $t - r$ at random from the complement of H and the remainder at random from H itself. Within H or its complement, any element has an equal probability of being chosen.

$P(\ldots)$ denotes the probability of the event in brackets, and $E(\ldots)$ the expectation of the random variable in brackets. $P(\ldots \mid A)$ and $E(\ldots \mid A)$ are conditional on the event A.

Let $\delta > 0$ be fixed and d be a positive integer, which will depend on δ only. Set

$$t_1 = \left[\frac{\log N}{\log 2}\right] + d + 1, \quad \lambda = 2/\delta.$$

It follows from (5), substituting t_1 and r_1 for t and r, that if N_1 is the number of elements of G not represented by a (t_1, r_1)-set then

$$P\left(N_1 \geqslant \lambda \frac{N^2}{2^{t_1}}\right) \leqslant \frac{1}{\lambda}.$$

Denote by A_1 the event

$$N_1 < \lambda \frac{N^2}{2^{t_1}} \leqslant \frac{\lambda N}{2^d},$$

and choose a further element g_{t_1+1} at random from H or its complement as the case may be, denoting by N_2 the number of elements of G which still cannot be represented. If g is one of these elements, neither g nor $g - g_{t_1+1}$ could be represented by the original

(t_1, r_1)-set, and for fixed g, the probability that $g - g_{t_1+1}$ could not be represented does not exceed $2N_1/N$. Hence

$$E(N_2 \mid N_1) \leqslant 2N_1^2/N$$

and

$$E(N_2 \mid A_1) \leqslant 2\lambda^2 N/2^{2d}.$$

It follows from Markoff's inequality that

$$P\left(N_2 \geqslant \frac{4\lambda^3 N}{2^{2d}} \,\middle|\, A_1\right) \leqslant \frac{1}{2\lambda}.$$

Again, let A_2 be the event

$$N_2 < \frac{4\lambda^3 N}{2^{2d}}.$$

By a similar argument, if we add another element at random (from the appropriate part of G) to our set and suppose that N_3 elements of G remain which cannot be represented, then

$$E(N_3 \mid A_1 A_2) \leqslant \frac{32\lambda^6 N}{2^{4d}},$$

and

$$P\left(N_3 \geqslant \frac{128\lambda^7 N}{2^{4d}} \,\middle|\, A_1 A_2\right) \leqslant \frac{1}{4\lambda}.$$

We continue this process. Let A_k denote the event

$$N_k < M_k = \frac{2^{(2^k+2^{k-1}-k-2)}\lambda^{2^{k-1}} N}{2^{(2^k-1)d}}.$$

Then we have

$$P(N_k \geqslant M_k \mid A_1 A_2 \ldots A_{k-1}) \leqslant \frac{1}{2^{k-1}\lambda}.$$

The joint event $A_1 A_2 \ldots A_k$ occurs with probability exceeding

$$1 - \frac{1}{\lambda} - \frac{1}{2\lambda} - \ldots - \frac{1}{2^{k-1}\lambda} > 1 - \delta,$$

and in this event,

$$N_k < M_k < \left(\frac{4\lambda}{2^d}\right)^{2^{k-1}} N.$$

We choose d so that $2^d \geqslant 8\lambda = 16/\delta$, i.e.

$$d = \left[\frac{\log 1/\delta}{\log 2}\right] + 5,$$

and

$$k = \left[\frac{1}{\log 2} \log\left(\frac{\log N}{\log 2}\right)\right] + 1,$$

and we deduce that with probability exceeding $1-\delta$, we have the event $N_k < 1$, that is, every element of G is represented by the set constructed; but this is a random (t, r)-set where $t = t_1 + k$, and this is the result stated.

Proof of the theorem. This is modelled on the proof of Theorem 1 in Erdös (1). Let $I(x)$ be the interval $(g, h]$ where

$$\log g = (\log\log x)^3, \quad \log h = \frac{\log x}{(\log\log x)^3},$$

and for each $n < x$ set

$$f(n) = \prod_{p \in I, p^a \| n} p^a.$$

We may assume in the following that $f(n)$ is squarefree, indeed that its prime factors lie in distinct residue classes (mod k), since the number of integers $n < x$ for which this is false is $o(x)$. Moreover the familiar variance method of Turán shows that $\nu(n) - \nu(f(n))$ has normal order $6 \log\log\log n$, hence we may assume that

$$\nu(n) - \nu(f(n)) < 7 \log\log\log x.$$

Those numbers $n < x$ with fewer than $\phi(k)$ divisors cannot contribute to $F(x, k)$. Since the number of divisors of n is at most $2^{\omega(n)}$ where $\omega(n)$ is the number of prime factors of n counted according to multiplicity, and $\phi(k)$ satisfies (1) whenever k does (since $k/\phi(k) = O(\log\log k)$), we may restrict our attention to the integers $n < x$ such that

$$\omega(n) > \log\log x + (c + o(1))\sqrt{(\log\log x)}.$$

The simple estimate

$$\sum_{n<x} \{\omega(n) - \nu(n)\} = O(x)$$

implies that $\omega(n) - \nu(n) = o(\sqrt{(\log\log x)})$ for all but $o(x)$ integers $n < x$, hence we need only consider those $n < x$ for which

$$\log\log x + (c + o(1))\sqrt{(\log\log x)} < \nu(n) < 2 \log\log x, \tag{6}$$

the upper bound being permissible as the normal order of $\nu(n)$ is $\log\log n$. Since (2) is an asymptotic formula for the number of such integers, it will be sufficient to show that almost all of them contribute to $F(x, k)$. Since the $o(\sqrt{(\log\log x)})$ term in (6) does not affect the final formula (2), and in view of all the remarks above, it will be sufficient for our theorem to deal with just those integers $n < x$ such that

$$\log \phi(k) + \log^{\frac{1}{2}} \phi(k) < \nu(f(n)) < 3 \log \phi(k), \tag{7}$$

where $f(n)$ is assumed to have all the properties specified above.

Let $l_1, l_2, \ldots, l_t$ be distinct residue classes, prime to k. We refer to this as a good set if $l_1^{\epsilon_1} l_2^{\epsilon_2} \ldots l_t^{\epsilon_t}$ represents every residue class prime to k as the ϵ_i's vary, ($\epsilon_i = 0$ or 1 for $1 \leqslant i \leqslant t$), and say that n corresponds to this set if $f(n) = p_1 p_2 \ldots p_t$ where $p_i \equiv l_i$ (mod k) for $1 \leqslant i \leqslant t$. Plainly if n corresponds to a good set it has a divisor in all the required residue classes, so that we have to show that all but $o(x)$ of the integers $n < x$, with the properties we assume, correspond to good sets.

Let $\Sigma^{(t)}$ denote summation over bad sets of t classes, where t lies in the range given by (7). Since $p_1 p_2 \ldots p_t \leqslant h^t \leqslant x^{1/\log\log x}$ for large enough x, we may deduce as in Lemma 7 of Erdös (1) that

$$\operatorname{card}\{n < x : f(n) = p_1 \ldots p_t\} \ll \frac{x}{p_1 p_2 \cdots p_t} \prod_{p \in I(x)} \left(1 - \frac{1}{p}\right),$$

where the constant implied by Vinogradov's notation $\ll$ is absolute. Hence by Mertens' formula, the number of integers $n < x$ corresponding to bad sets is

$$\ll x\frac{\log g}{\log h}\sum_t \Sigma^{(t)}\frac{1}{t!}\prod_{i=1}^{t}\Sigma\frac{1}{p}.$$

where the innermost sum is over p in $g < p \leqslant h$ for which $p \equiv l_i \pmod k$. Next, Lemma 1 of Hall (2) states that for every l prime to k, we have that

$$\Sigma\frac{1}{p} = \frac{L}{\phi(k)}(1-\chi_1(l)M+E(l))$$

where the sum is over p in $g < p \leqslant h$, for which $p \equiv l \pmod k$, and

$$L = \int_g^h \frac{(1+\log y)\,dy}{y\log^2 y},$$

$$LM = \frac{1}{\beta}\int_g^h \frac{y^{\beta-1}(1+\log y)\,dy}{y\log^2 y}.$$

Here,

$$|E(l)| = O((\log\log x)^{-4}),$$

where the constant implied by the O-notation is independent of k and l, and β denotes the unique Siegel zero $\pmod k$ if such exists (and otherwise we put $M = 0$), that is, $L(\beta, \chi_1) = 0$ where χ_1 is a real, non-principal Dirichlet character $\pmod k$, and

$$1 - C/\log k < \beta < 1,$$

C being an absolute constant. The number of integers $n < x$ satisfying the conditions stated and corresponding to bad sets is therefore

$$\ll x\frac{\log g}{\log h}\sum_t \frac{(L/\phi(k))^t}{t!}\Sigma^{(t)}(1-M+E)^r(1+M+E)^{t-r}$$

where r is the number of l_i's in the set such that $\chi_1(l_i) = 1$, and $E \ll (\log\log x)^{-4}$.

Now let G be the group of residue classes prime to k under multiplication so that $N = \phi(k)$, and let H be the subgroup of index 2 on which χ_1 is principal. Finally set $1/\delta = \exp(\frac{1}{2}\log^{\frac{1}{2}}\phi(k))$. By the lemma,

$$\Sigma^{(t)}(1-M+E)^r(1+M+E)^{t-r} \leqslant \delta\sum_{r=0}^{t-1}\binom{t}{r}\left(\frac{\phi(k)}{2}\right)^t(1-M+E)^r(1+M+E)^{t-r}$$
$$+\left(\frac{\phi(k)}{2}\right)^t(1-M+E)^t$$
$$\leqslant \phi^t(k)\{\delta(1+E)^t + 2^{-t}(1-M+E)^t\} \ll \delta\phi^t(k)$$

since $0 \leqslant M \leqslant 1$, $Et = O(1)$, and $2^t > \phi(k)$ by (7). It follows that the number of integers corresponding to bad sets is

$$\ll \delta x\frac{\log g}{\log h}\sum_t \frac{L^t}{t!} = o(x)$$

as $L = \log(\log h/\log g) + O(1)$, $t = O(L)$, and $\delta \to 0$ as $x \to \infty$. This completes the proof.

REFERENCES

(1) Erdös, P. On the distribution of divisors of integers in residue classes (mod d). *Bull. Soc. Math. Grèce* **6** Fasc 1 (1965), 27–36.
(2) Hall, R. R. A conjecture of Erdös in number theory. *Acta Arithmetica* (to appear).
(3) Erdös, P. and Rényi, A. Probabilistic methods in group theory. *Journal Analyse Math.* **14** (1965), 127–38.