ACTA ARITHMETICA
XXVIII (1975)

The divisors of integers II

by

R. R. Hall (Heslington)

Introduction. This paper is concerned with the distribution (mod 1) of the numbers $\log d$, where d runs through the divisors of an integer n. This was the topic of my previous paper [4], also of Erdös and Hall [3].

We may think of this distribution in terms of the points

$$d^{2i\pi}, \qquad (d\,|\,n)$$

lying on the unit circle — I proved in [4] that as n tends to infinity through a suitable sequence of asymptotic density 1, these points are asymptotically uniformly distributed; an estimate for the discrepancy was given.

We can ask about the maximum and minimum spacing between the points. Theorem 3 [3] applies to the first question: if $f(n)\to\infty$ arbitrarily slowly as $n\to\infty$ then for almost all n,

$$\sup_{d_1|n}\ \inf_{\substack{d_2|n\\ d_2\neq d_1}} \|\log d_1-\log d_2\| < 2^{-\log\log n+f(n)\sqrt{\log\log n}},$$

where $\|x\|$ denotes the distance from x to the nearest integer. I will prove the following result concerning the minimum spacing:

THEOREM. *Let*

$$g(n) = \inf\|\log d_1-\log d_2\|, \qquad d_1, d_2\,|\,n,\ d_1\neq d_2.$$

Then for every fixed $\varepsilon>0$ and almost all n,

$$3^{-(1+\varepsilon)\log\log n} < g(n) < 3^{-(1-\varepsilon)\log\log n}.$$

This is related to a result of Erdös [1]: if

$$g_1(n) = \inf|\log d_1-\log d_2|, \qquad d_1, d_2\,|\,n,\ d_1\neq d_2$$

the same conclusion holds for $g_1(n)/\log n$ in place of $g(n)$.

Proof of the theorem. We begin with the right-hand inequality, and we need the following result:

LEMMA. *Let δ and η be any fixed positive numbers and r be a prime number. Then for all but possibly*

$$o\left(\binom{r}{t}\right)$$

exceptional choices of the t distinct residue classes $h_1, h_2, \ldots, h_t \pmod r$ the number of solutions $N(b)$ of the congruence

$$\varepsilon_1 h_1 + \varepsilon_2 h_2 + \ldots + \varepsilon_t h_t \equiv b \pmod r, \text{ each } \varepsilon_i = 0 \text{ or } \pm 1,$$

satisfies

$$(1-\eta)\frac{3^t}{r} < N(b) < (1+\eta)\frac{3^t}{r}$$

for every integer b, provided $t\log 3 \geqslant (1+\delta)\log r$.

We shall only use the fact that provided $\eta < 1$, this implies $N(b)$ is always positive, and I think a similar argument to that of Erdös and Rényi [2] would give this; the result which I have stated may be deduced from a theorem of K. Wild [6].

The argument now follows [3] in some respects, and I will be able to suppress several details. For each $x > 3$, let $I(x)$ be the interval

$$\left(\exp\left((\log\log x)^3\right), x^{1/(\log\log x)^2}\right)$$

and suppose that the integer $n \leqslant x$ has t prime factors $p_1, \ldots, p_t$ lying in $I(x)$. For all but $o(x)$ such n, these primes will be distinct, moreover the familiar variance method of Turán [5] for estimating the normal order of an additive function shows that t will satisfy

$$\log\log x - (\log\log x)^{2/3} < t < 2\log\log x.$$

We restrict our attention to these n, neglecting a sequence of zero density. Now let r be a prime satisfying

$$\tfrac{1}{2}\cdot 3^{(1-\varepsilon/2)\log\log x} < r \leqslant 3^{(1-\varepsilon/2)\log\log x}$$

so that for $x \geqslant x_0(\varepsilon)$ we have

$$t\log 3 \geqslant \left(1-\frac{\varepsilon}{4}\right)\log 3\cdot\log\log x \geqslant \left(1+\frac{\varepsilon}{4}\right)\log r$$

and suppose that for $1 \leqslant i \leqslant t$,

$$[r\log p_i] \equiv h_i \pmod r.$$

We set $\delta = \varepsilon/4$, $\eta = 1/2$ and note that t and r satisfy the requirements of the lemma. Assume for the moment that the residue classes h_i defined above are distinct and unexceptional in the sense of the lemma. Then $N(1) > 0$, that is, there exist $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_t$ each equal to 0 or ± 1 (and plainly not all zero) such that

$$\varepsilon_1 h_1 + \varepsilon_2 h_2 + \ldots + \varepsilon_t h_t \equiv 1 \pmod r$$

and so

$$r(\varepsilon_1\log p_1 + \varepsilon_2\log p_2 + \ldots + \varepsilon_t\log p_t) \equiv a \pmod r$$

where

$$1-t \leqslant a \leqslant 1+t.$$

Now let d_1 be the product of those p_i for which $\varepsilon_i = +1$, and d_2 the product of the primes p_j with $\varepsilon_j = -1$. Empty products are taken to be 1 – in view of the fact that the ε's are not all zero not both d_1 and d_2 equal 1, in fact they are distinct divisors of n satisfying

$$\|\log d_1 - \log d_2\| \leqslant \frac{2t}{r} \leqslant \frac{8\log\log x}{3^{(1-\varepsilon/2)\log\log x}}.$$

If $x > x_1(\varepsilon)$ and $n \leqslant x$, this implies that

$$g(n) \leqslant \|\log d_1 - \log d_2\| < 3^{-(1-\varepsilon)\log\log n}.$$

To complete the proof that this inequality holds for almost all n, it is sufficient to show that from the set of $x + o(x)$ integers $n \leqslant x$ under consideration, we can find a sub-set, again with cardinality $x + o(x)$ such that the residue classes h_i corresponding to n are distinct and unexceptional in the sense of the lemma. This part of the proof is very similar to the argument following Lemma 2 [3] and need not be repeated here.

It remains to show that for fixed $\varepsilon > 0$ and almost all n,

$$g(n) > 3^{-(1+\varepsilon)\log\log n}.$$

Evidently it will be sufficient to show that if we define

$$\mu(x) = 3^{-(1+\varepsilon/2)\log\log x}$$

then the number of integers $n \leqslant x$ with $g(n) < \mu(x)$ is $o(x)$. We define

$$T(y) = \inf\|\log d_1 - \log d_2\|, \quad d_1 \leqslant y,\ d_2 \leqslant y,\ d_1 \neq d_2;$$

since e is transcendental, $T(y) > 0$ although $T(y) \to 0$ as $y \to \infty$. We suppose that y tends to infinity as a function of x, in such a way that $T(y) > \mu(x)$. Let $\mathcal{D}(u)$ denote the set of integers with no prime factor exceeding u; we begin by estimating the number of integers $n \leqslant x$ with distinct divisors d_1, d_2 satisfying

$$d_1 \in \mathcal{D}(u),\ d_2 \in \mathcal{D}(u), \quad \|\log d_1 - \log d_2\| < \mu(x).$$

These conditions will still be satisfied if we remove any common factor of d_1 and d_2, or transpose them, so we may assume that $(d_1, d_2) = 1$ and $d_1 < d_2$. Since $\mu(x) < T(y)$, we have $d_2 > \max(d_1, y) = d_1(y)$ say. Now $(d_1, d_2) = 1$ implies that $d_1 d_2 | n$, hence the number of integers $n \leqslant x$ with such divisors does not exceed

$$x\sum\frac{1}{d_1 d_2}$$

the summation conditions imposed on d_1, d_2 being all those above, except that for the purpose of estimating this sum from above, we drop the condition $(d_1, d_2) = 1$. We set

$$u = \exp\big((\log\log x)^3\big), \qquad H = \exp\big((\log\log x)^{10}\big)$$

and show first that the contribution to the sum above from those $d_2 > H$ is negligible. For

$$\sum_{\substack{d_2\in\mathscr{D}(u)\\ d_2>H}}\frac{1}{d_2} < \frac{1}{\log H}\sum_{d_2\in\mathscr{D}(u)}\frac{\log d_2}{d_2} = \frac{1}{\log H}\prod_{p\leqslant u}\left(1-\frac{1}{p}\right)^{-1}\sum_{p\leqslant u}\frac{\log p}{p-1}$$
$$= O\left(\frac{\log^2 u}{\log H}\right),$$

and so

$$x\sum_{d_1\in\mathscr{D}(u)}\frac{1}{d_1}\sum_{\substack{d_2\in\mathscr{D}(u)\\ d_2>H}}\frac{1}{d_2} = O\left(x\,\frac{\log^3 u}{\log H}\right) = O\left(\frac{x}{\log\log x}\right).$$

Therefore

$$(1)\qquad x\sum\frac{1}{d_1 d_2} \leqslant x\sum_{d_1\in\mathscr{D}(u)}\frac{1}{d_1}\sideset{}{'}\sum_{d_1(y)<d_2\leqslant H}\frac{1}{d_2} + o(x)$$

where $\sum'$ denotes that d_2 satisfies

$$(2)\qquad m-\mu(x) < \log d_2 - (\log d_1) < m+\mu(x)$$

for some integer m; $(\log d_1)$ is the fractional part of $\log d_1$ and we drop the condition $d_2 \in \mathscr{D}(u)$.

The sum of the reciprocals of the integers d_2 in such a range is

$$\leqslant \mu(x) + e^{-m}$$

and m must lie in the range

$$\log d_1(y) + O(1) \leqslant m \leqslant \log H + O(1)$$

in view of (2). Hence

$$\sideset{}{'}\sum_{d_1(y)<d_2\leqslant H}\frac{1}{d_2} \leqslant \mu(x)\log H + \frac{1}{d_1(y)},$$

and

$$\sum_{d_1\in\mathscr{D}(u)}\frac{1}{d_1}\sideset{}{'}\sum_{d_1(y)<d_2\leqslant H}\frac{1}{d_2} \leqslant \mu(x)(\log H)\log u + \frac{\log y}{y}.$$

Substituting this in (1), and comparing μ, H and u, we have

$$x\sum\frac{1}{d_1 d_2} = o(x)$$

as $y\to\infty$ with x. We therefore have to estimate next the number of integers $n \leqslant x$ with a pair of coprime divisors d_1 and d_2, at least one of which has a prime factor exceeding u, and satisfying

$$\|\log d_1 - \log d_2\| < \mu(x).$$

For convenience we refer to such integers as belonging to Class 1. We may assume that n has a prime factor exceeding

$$w = x^{1/\log\log x},$$

the number of exceptional integers $n \leqslant x$ being $o(x)$ by Selberg's method, also that n has at most

$$t_0 = 1 + \frac{\varepsilon}{4}\log\log x$$

prime factors, counted according to multiplicity. We can write $n = mp$, $p > w$, and we say that n belongs to Class 2 if m itself belongs to Class 1. We begin by estimating the cardinality of Class 2. This is at most

$$\sideset{}{'}\sum_{m\leqslant x/w}\pi\left(\frac{x}{m}\right) \leqslant \frac{x}{\log w}\sideset{}{'}\sum\frac{1}{m}$$

where $\sum'$ refers to summation over Class 1 — we have to show that the sum on the right is $o(\log w)$.

We may write $m = qp_1p_2\dots p_t$ where $p_1, \dots, p_t$ are the prime factors of m exceeding u, in increasing order. We may assume they are distinct, the contribution of the exceptional m's being

$$\leqslant \sum_{p>u}\frac{\log x}{p^2} \leqslant \frac{\log x}{u} = o(\log w).$$

Next, if $d_1, d_2 | m$,

$$d_1/d_2 = (f_1/f_2)p_1^{\varepsilon_1}p_2^{\varepsilon_2}\dots p_t^{\varepsilon_t}, \qquad \varepsilon_i = 0 \text{ or } \pm 1,$$

where f_1 and f_2 are divisors of q, of which there are $\tau^2(q)$ pairs. The ε's are not all zero, if

$$(3) \qquad \|\log d_1 - \log d_2\| < \mu(x),$$

by the definition of Class 1. Suppose $\varepsilon_j = \pm 1$ for some j, $1 \leqslant j \leqslant t$. Then $(\log p_j)$ is determined by (3) to lie in the union of $3^{t-1}\tau^2(q)$ sub-intervals of $[0, 1)$, each of length $2\mu(x)$. By Lemma 2 [3], the sum of the reciprocals of such p_j's is

$$\sum\nolimits^{*} \frac{1}{p_j} \ll 3^{t-1}\tau^2(q)\mu(x)\log\log x.$$

Next, $t \leqslant t_0$. Thus

$$\sum\nolimits' \frac{1}{m} \leqslant o(\log w) + \sum_{q\in\mathscr{D}(u)} \frac{1}{q} \sum_{1\leqslant t\leqslant t_0} \sum_{j=1}^{t} \sum\nolimits'' \frac{1}{p_1 \cdots p_{j-1}p_{j+1} \cdots p_t} \sum\nolimits^{*} \frac{1}{p_j}$$

where $\sum''$ denotes that the primes p_i are distinct, and do not exceed x. Plainly

$$\sum\nolimits'' \frac{1}{p_1 \cdots p_{j-1}p_{j+1} \cdots p_t} \leqslant \frac{\big(\log\log x + O(1)\big)^{t-1}}{(t-1)!} \ll \frac{(\log\log x)^{t-1}}{(t-1)!}$$

since $t \leqslant 2\log\log x$. Therefore

$$\begin{aligned}\sum\nolimits' \frac{1}{m} &\ll o(\log w) + 3^{t_0}\mu(x) \sum_{q\in\mathscr{D}(u)} \frac{\tau^2(q)}{q} \sum_{t\leqslant t_0} \frac{t(\log\log x)^t}{(t-1)!}\\ &\ll o(\log w) + 3^{t_0}\mu(x)(\log\log x)^2(\log x) \prod_{p\leqslant u}\left(1-\frac{4}{p}\right)^{-1}\\ &\ll o(\log w) + 3^{-\frac{\varepsilon}{4}\log\log x}(\log x)(\log\log x)^{14} = o(\log w).\end{aligned}$$

This deals with the Class 2 integers. It remains to deal with the integers $n \leqslant x$ in Class 1 but not Class 2; such an n must have divisors $d_1 = f_1$, $d_2 = f_2 p$, where f_1 and f_2 are relatively prime divisors of m, satisfying

$$\|\log(f_1/f_2) - \log p\| < \mu(x).$$

If the prime factors of m have multiplicities $\alpha_1, \alpha_2, \ldots, \alpha_s$, the number of choices of f_1 and f_2 is

$$\prod_{i=1}^{s} (1+2\alpha_i) \leqslant \prod_{i=1}^{s} (1+2)^{\alpha_i} \leqslant 3^{t_0}.$$

Moreover, $(\log p)$ is determined by the above to lie in the union of this number of sub-intervals of $[0, 1)$ each of length $2\mu(x)$, and $w < p \leqslant x/m$.

Referring to the corollary to Lemma 3 [3], we find that the number of such primes is

$$\ll \frac{3^{t_0}\mu(x)x}{m\log w}.$$

The sum of this expression over the possible m's is

$$\ll 3^{t_0}\mu(x)x\frac{\log x}{\log w} \ll 3^{-\frac{\varepsilon}{4}\log\log x} x\log\log x = o(x)$$

and so the whole of Class 1 has cardinality $o(x)$; and this completes the proof that for almost all n, $g(n)$ satisfies the left-hand inequality stated in the theorem.

References

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

[2] — and A. Rényi, *Probabilistic methods in group theory*, Journal d'Analyse Math. 14 (1965), pp. 127–138.

[3] — and R. R. Hall, *Some distribution problems concerning the divisors of integers*, Acta Arith. 26 (1975), pp. 175–188.

[4] R. R. Hall, *The divisors of integers I*, Acta Arith. 26 (1974), pp. 41–46.

[5] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), pp. 284–286.

[6] K. Wild, *A theorem concerning products of elements of Abelian groups*, Proc. London Math. Soc. (3) 27 (1973), pp. 600–616.

Received on 5. 12. 1973 (500)

ACTA ARITHMETICA
XXVIII (1975)

A purely algebraic proof of special cases of Tchebotarev's theorem

by

J. WÓJCIK (Warszawa)

I have given in [7] a purely algebraic proof of the following

THEOREM. *Let G, J be subgroups of the multiplicative group of residues* mod m *and J be a proper subgroup of G. Then there exist infinitely many primes belonging* mod m *to $G-J$.*

The aim of the present paper is to prove on similar lines some special cases of Tchebotarev's density theorem in its qualitative form which comprise the above result. The proof is based on the upper estimate for the number of genera in a cyclic field of prime degree.

Notation. Terminology and notation are taken from [4]. In particular k denotes a fixed algebraic number field, all considered fields are extension of k unless stated to the contrary and all prime ideals are defined in k. For instance, an inclusion $\Omega \leqslant K$ means that $k \leqslant \Omega \leqslant K$. Q is the rational field, ζ_m is a primitive mth root of unity, $|\Omega| = (\Omega:Q)$. For a finite set S, $|S|$ is its cardinality. We say that the extension K/Ω is non-trivial if $K \neq \Omega$. A prime ideal of degree one means a prime ideal of degree one over Q.

THEOREM 1. *Let K be a normal non-trivial extension of k. There exist infinitely many prime ideals $\mathfrak{p}$ of degree one such that* $\left(\frac{K}{\mathfrak{p}}\right) \neq 1$.

Remark 1. For K being abelian a similar statement proved again in a purely algebraic way occurs in [1] as Corollary 8.8. However we assert in contrast to [1] that $\mathfrak{p}$ is of degree one.

LEMMA 1. *Let K be a cyclic field of prime degree and $\mathfrak{d}$ be its relative discriminant. For every positive integer M there exists a prime ideal $\mathfrak{p}$ of k prime to $\mathfrak{d}M$ such that* $\left(\frac{K}{\mathfrak{p}}\right) \neq 1$.

Proof. Let $l = (K:k)$, where l is a prime. It is well known that $\mathfrak{d} = \mathfrak{f}^{l-1}$, where $\mathfrak{f}$ is an ideal of k. Let A be the group of all classes of ideals