ACTA ARITHMETICA
XXVIII (1975)

Some properties of the sequence $\{p-1\}$

by

R. R. Hall (Heslington)

Introduction. It is sometimes necessary to have information about the divisors, and in particular, the prime divisors, of the number $p-1$, where p itself is prime. Erdös [1] proved that the number of these prime factors has normal order $\log\log p$ (whether counted multiply or not), and used the fact that for almost all primes, $p-1$ has a prime factor as large as

$$p^{1/20\log\log p}. \tag{1}$$

The greatest prime factor of $p-1$, and more generally $p+a$, has received the attention of Goldfeld [5] and Hooley [8], in particular Hooley proved that for every fixed $\alpha < 5/8$, and every a, there are infinitely many primes for which $p+a$ has a prime factor exceeding p^{α}.

The estimate from below (1) can be improved by means of Selberg's method, and we have

Theorem 1. *Let $\varepsilon_p \to 0$ arbitrarily slowly as $p \to \infty$ through the sequence of primes. Then for almost all primes, $p-1$ has a prime factor exceeding p^{ε_p}.*

By "almost all primes" I mean that the number of exceptional primes upto x is $o\big(\pi(x)\big)$ as $x \to \infty$.

Theorem 1 implies the following result.

Corollary. *Provided $\varepsilon_n \to 0$ as $n \to \infty$, $\varphi(n)$ has a prime factor exceeding n^{ε_n} for almost all integers n.*

Let $V(x)$ denote the number of distinct values of $\varphi(n) < x$. A more difficult result which I could not prove, would be that $\big(1+o(1)\big)V(x)$ of these values have a prime factor exceeding x^{ε} when $\varepsilon \to 0$ as $n \to \infty$. $V(x)$ is surprizingly small: Erdös and Hall [3] obtained the estimate

$$V(x) \ll \pi(x)\exp\{B\sqrt{\log\log x}\}$$

for each fixed $B > 2\sqrt{2/\log 2}$.

Although Theorem 1 is a consequence of Selberg's method, it may be readily derived from the following result. Goldfeld [5] proved this in the case $u = 1/2$, but the full result is implicit in his method.

THEOREM. *Let $P(x, u)$ denote the number of primes $p \leqslant x$ such that $p-1$ has no prime factor exceeding x^u. Then provided $u \leqslant 1/2$,*

$$P(x, u) \leqslant \frac{ux}{\log x} + O\left(\frac{x}{\log^2 x}(1+u\log\log x)\right). \tag{2}$$

The limitation $u \leqslant 1/2$ arises from Bombieri's theorem, and the estimation of $P(x, u)$ for $u > 1/2$ is much more difficult, as indicated by Hooley's theorem mentioned above.

Suppose that almost all integers n have some property which is preserved when n is multiplied by a prime q, perhaps restricted in some way relative to n. Then we can often use Theorem 1 to show that $p-1$ has the same property, for almost all primes. I would like to mention two results of this type.

THEOREM 2. *For every $\eta > 0$ and $\alpha \in R$, and almost all primes p, $p-1$ has divisors d_1, d_2, d_3 satisfying*

(i) $0 < \|\log d_1 - \alpha\| < 2^{-(1-\eta)\log\log p}$,

(ii) $0 < \|\log d_2 - \log d_3\| < 3^{-(1-\eta)\log\log p}$,

where $\|x\|$ denotes the distance from x to the nearest integer to it.

THEOREM 3. *For every fixed $A > 3/e$, and almost all primes p,*

$$\sup_z \Big|\sum_{\substack{d\mid p-1\\ d<z}} \mu(d)\Big| < A^{\nu(p-1)}$$

where $\nu(p-1)$ denotes the number of distinct prime factors of $p-1$. The result also holds if $\mu(d)$ is replaced by any multiplicative function $f(d)$ such that for all d, $|f(d)| \leqslant 1$ and

$$\sum\left\{\frac{1}{p}: f(p) = -1\right\} = \infty.$$

The two parts of Theorem 2 are derived from similar results concerning almost all integers n proved by Erdös and Hall [2] and Hall [7]. The analogue of Theorem 3 for almost all integers was proved by Erdös and Kátai [4] in the case $A > \sqrt{2}$, and for $A > 3/e$ by Hall [6]. It is quite possible that this is not the best possible constant here: maybe the result is true for $A > 1$.

Proofs of the theorems. Theorem 1 is immediate from (2) so I will go straight on to the corollary. We set

$$\varepsilon = \varepsilon(x) = \sup\{\varepsilon_n: \sqrt{x} \leqslant n \leqslant x\}$$

so that it will be sufficient to prove that the number of integers $n < x$ such that $\varphi(n)$ has a prime factor exceeding x^ε is $(1+o(1))x$. Now choose the positive function $\delta(x)$ so that

$$\delta^2(x) = \max\left(\frac{1}{\log x}, \sup\{\varepsilon(y): y \geqslant x\}\right).$$

Note that $\delta(x)$ is decreasing and tends to zero. Let E denote the set of primes p in the interval

$$x^{\delta(x)} < p \leqslant x$$

such that $p-1$ has a prime factor as large as $p^{\delta(p)}$. By Theorem 1,

$$\sum_{p\in E}\frac{1}{p} \geqslant \sum_{p\in E}\int_p^x \frac{dt}{t^2} \geqslant \int_{x^\delta}^x \big(1+o(1)\big)\pi(t) - \pi(x^\delta)\frac{dt}{t^2}$$
$$\geqslant \big(1+o(1)\big)\log\frac{1}{\delta(x)} + O\left(\frac{1}{\delta(x)\log x}\right)$$

so that

$$\prod_{p\in E}\left(1-\frac{1}{p}\right) \to 0 \quad \text{as} \quad x\to\infty.$$

If the integer $n < x$ has a prime factor $p \in E$, $\varphi(n)$ being divisible by $p-1$ has a prime factor as large as

$$p^{\delta(p)} \geqslant (x^{\delta(x)})^{\delta(x)} \geqslant x^{\varepsilon(x)}.$$

The number of $n < x$ with no prime factor in E is

$$\ll x\prod_{p\in E}\left(1-\frac{1}{p}\right) = o(x)$$

by a theorem of van Lint and Richert [9]. This completes the proof.

Next, we prove Theorem 2. First, for almost all primes, $p-1$ is free of prime factors exceeding $p^{1-\varepsilon_p}$ provided $\varepsilon_p \to 0$ as $p\to\infty$. For let $p < x$ be exceptional: we have $p-1 = qm$ and either

$$p < \sqrt{x} \quad \text{or} \quad m < x^\varepsilon, \quad \varepsilon = \sup\{\varepsilon_p: \sqrt{x} < p < x\}.$$

The number of such primes is

$$\leqslant \sqrt{x} + \sum_{m<x^\varepsilon}\ \sum_{\substack{q<x/m\\ mq+1 \text{ prime}}} 1 \ll \sqrt{x} + \frac{x}{\log^2 x}\sum_{m<x^\varepsilon}\frac{1}{\varphi(m)}$$

by Satz 4.5 (p. 51) of Prachar [10], and this is $o\big(\pi(x)\big)$. In view of Theorem 1, we deduce that for almost all primes p, we may write $p-1 = nq$ where

$$p^{\varepsilon_p} < q \leqslant p^{1-\varepsilon_p}, \quad q \text{ prime}.$$

If now n has divisors d_1, d_2, d_3 satisfying

$$0 < \|\log d_1 - \alpha\| < 2^{-(1-\eta/2)\log\log n}, \tag{3}$$
$$0 < \|\log d_2 - \log d_3\| < 3^{-(1-\eta/2)\log\log n},$$

on observing that $n \geqslant \frac{1}{2}p^{\varepsilon_p}$ and so

$$(1-\eta/2)\log\log n \geqslant (1-\eta/2)\log\log p - \log\frac{1}{\varepsilon_p} + O(1) \geqslant (1-\eta)\log\log p$$

when $\varepsilon_p \to 0$ sufficiently slowly, we see that $p-1$ has divisors d_1, d_2, d_3 with the required properties. Next, by the results of Erdös and Hall [2], [7], the sequence of integers n without divisors satisfying (3) has zero asymptotic density, and therefore has zero logarithmic density. That is to say that if $\sum'$ denotes summation over this sequence then

$$\sum_{n<x}{}' \frac{1}{n} = g(x)\log x, \qquad g(x) = o(1).$$

It follows from Cauchy's inequality that

$$\sum_{n<x}{}' \frac{1}{\varphi(n)} \ll \sqrt{g(x)}\log x.$$

We may now estimate the number of primes $p < x$ which are exceptional in the sense of the theorem. Write

$$2\varepsilon_1 = 2\varepsilon_1(x) = \inf\{\varepsilon_p : \sqrt{x} < p < x\}.$$

We may assume $p > \sqrt{x}$ and that $p-1 = qn$ where $q > x^{\varepsilon_1}$, that is, $n < x^{1-\varepsilon_1}$, also that n is in the exceptional sequence mentioned above. So the number of these primes is

$$\leqslant \sum_{n<x^{1-\varepsilon_1}}{}' \sum_{\substack{q<x/n \\ nq+1 \text{ prime}}} 1 + o\big(\pi(x)\big) \ll \sum_{n<x^{1-\varepsilon_1}} \frac{x}{\varphi(n)\log^2 x/n} + o\big(\pi(x)\big)$$
$$\ll \frac{x\sqrt{g(x)}}{\varepsilon_1^2(x)\log x} + o\big(\pi(x)\big) = o\big(\pi(x)\big)$$

if we assume, as we may, that the sequence $\{\varepsilon_p\}$ and so $\varepsilon_1(x)$ tends to zero sufficiently slowly. This completes the proof of Theorem 2.

To prove Theorem 3 we use $\varepsilon_1(x)$ again and estimate the number of exceptional primes $p < x$. We assume once more that $\sqrt{x} < p < x$, and that $p-1 = qn$ where q is a prime exceeding x^{ε_1}. If $q \nmid n$, then

$$\sum_{\substack{d\mid p-1 \\ d<z}} f(d) = \sum_{\substack{d\mid n \\ d<z}}{}' f(d) + f(q) \sum_{\substack{d\mid n \\ d<z/q}} f(d),$$

and we may make this assumption, as the number of primes $p < x$ with $q^2 \mid p-1$, $q > x^{\varepsilon_1}$ is $o\big(\pi(x)\big)$. Thus

$$\sup_z \Big|\sum_{\substack{d\mid p-1 \\ d<z}} f(d)\Big| \leqslant 2\sup_z \Big|\sum_{\substack{d\mid n \\ d<z}} f(d)\Big|.$$

Let B be the geometric mean of $3/e$ and A. By Erdös' result cited above that $r(p-1)$ has normal order $\log\log p$, we may assume that

$$2B^{r(p-1)} \leqslant A^{r(p-1)}$$

as the number of exceptions is $o\big(\pi(x)\big)$. Hence if

$$\sup_z \Big|\sum_{\substack{d\mid n \\ d<z}} f(d)\Big| < B^{r(n)} < B^{r(p-1)} \tag{4}$$

p has the property required. Also, $B > 3/e$ so that my theorem [6] shows that (4) holds for almost all n, the exceptions having zero logarithmic density. The rest of the proof follows as in Theorem 2.

References

[1] P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quarterly Journal 6 (1935), pp. 205–213.

[2] P. Erdös and R. R. Hall, *Some distribution problems concerning the divisors of integers*, Acta Arith. 26 (1974), pp. 175–188.

[3] — — *On the values of Euler's φ-function*, Acta Arith. 22 (1973), pp. 201–206.

[4] — and I. Kátai, *Non complete sums of multiplicative functions*, Periodica Mathematica Hungarica 1 (1971), pp. 209–212.

[5] M. Goldfeld, *On the number of primes p for which $p+a$ has a large prime factor*, Mathematika 16 (1969), pp. 23–27.

[6] R. R. Hall, *A problem of Erdös and Kátai*, Mathematika 21 (1974), pp. 110–113.

[7] — *The divisors of integers, II*, Acta Arith. (to appear).

[8] C. Hooley, *On the largest prime factor of $p+a$*, Mathematika 20 (1973), pp. 135–143.

[9] J. H. van Lint and H.-E. Richert, *On primes in arithmetic progressions*, Acta Arith. 11 (1965), pp. 209–216.

[10] K. Prachar, *Primzahlverteilung*, Berlin 1957.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF YORK
England

Received on 30. 6. 1974 (534)