MATH. SCAND. 10 (1962), 163–170

ON THE INTEGERS RELATIVELY PRIME TO n AND ON A NUMBER-THEORETIC FUNCTION CONSIDERED BY JACOBSTHAL

P. ERDÖS

Dedicated to E. Jacobsthal for his 80th birthday

Let n be any integer. Jacobsthal [6] defines $g(n)$ to be the least integer so that amongst any $g(n)$ consecutive integers $a,\ a+1,\ldots,a+g(n)-1$ there is at least one which is relatively prime to n. He further defines

$$(1) \qquad \max g(n) = C(r)+1\ ,$$

where on the left hand side the maximum is taken over all the integers n with $\nu(n)=r$, $\nu(n)$ denoting the number of distinct prime factors of n. The growth of the function $g(n)$ is very irregular and even the growth of $C(r)$ is very difficult to study. We have (throughout this paper $c_1, c_2, \ldots,$ denote positive absolute constants)

$$(2) \qquad \frac{c_1 r(\log r)^2 \log\log\log r}{(\log\log r)^2} < C(r) < c_2 r^{c_3}\ .$$

The left hand side of (2) is a result of Rankin [8] and the right hand side follows easily from Brun's method.

Jacobsthal asked (in a letter) if

$$(3) \qquad C(r) < c_4 r^2$$

is true. The exponent c_3 can be reduced by Selberg's improvement of Brun's method, but it seems hopeless at present to decide about (3). Jacobsthal also informed me that for $r \leqq 10$ the value of $C(r)$ is determined by $n_r = 2, 3, \ldots p_r,$ the p's being the consecutive primes, and that this perhaps holds for all values of r. Possibly the value of $g(n_r')$ for $n_r' = \prod_{i=1}^{r} p_{2i+1}$ is already considerably smaller than $C(r)$. In a previous paper [4] I estimated $g(n)$ for integers n of a certain special form, e.g. if n is the product of the first r consecutive primes $\equiv 3 \pmod 4$.

It is easy to see that for almost all integers satisfying $\nu(n)=r$ we have

Received May 26, 1961.

$g(n) = r+1$. To see this observe that the number of integers $n \leqq x$ with $\nu(n) = r$ is by a well known theorem of Landau (cf. [7, vol. 1, p. 211]).

$$(4) \qquad \big(1+o(1)\big)\frac{x(\log\log x)^{r-1}}{(r-1)!\,\log x}.$$

Further Jacobsthal [6] observed that if $\nu(n) = r$ and all prime factors of n are greater than r, then $g(n) = r+1$. Now from (4) we obtain by a simple computation that the number of integers $n \leqq x$ with $\nu(n) = r$, whose smallest prime factor is not greater than r, is less than (c_5 depends on r)

$$(5) \qquad c_5 x(\log\log x)^{r-2}/\log x \;=\; o\big(x(\log\log x)^{r-1}/\log x\big)\,.$$

(4) and (5) complete the proof of our assertion.

In the present note we shall prove that for almost all integers n

$$(6) \qquad g(n) \;=\; \big(1+o(1)\big)n\,\log\log n/\varphi(n)\,,$$

where $\varphi(n)$ denotes Euler's φ-function. In other words, for every ε the density of integers for which

$$(1-\varepsilon)n\,\log\log n/\varphi(n) \;<\; g(n) \;<\; (1+\varepsilon)n\,\log\log n/\varphi(n)\,,$$

is not satisfied, is 0. In fact we shall prove somewhat stronger theorems.

Denote by $1 = a_1 < \ldots < a_{\varphi(n)} = n-1$ the $\varphi(n)$ integers relatively prime to n. Some time ago I conjectured [3] that

$$(7) \qquad \sum_{k=1}^{\varphi(n)-1} (a_{k+1}-a_k)^2 \;<\; c_6 n^2/\varphi(n)\,.$$

I have been unable to prove or disprove (7). In the present note I shall outline a proof (Theorem III) that to every $\varepsilon > 0$ and $\eta > 0$ there exists an $A_0(\varepsilon,\eta)$ so that for every $A > A_0(\varepsilon,\eta)$ the number of integers x, $1 \leqq x \leqq n$, for which

$$(1-\varepsilon)A \;<\; \varphi_n\big(x, x+An/\varphi(n)\big) \;<\; (1+\varepsilon)A\,,$$

is not satisfied, is less than ηn. ($\varphi_n(x, x+B)$ denotes the number of integers $x < m \leqq x+B$ with $(m,n) = 1$). This result seems to indicate that (7) is true, but (7) is deeper and I have not yet been able to prove it.

The following theorem easily implies formula (2) in [3].

THEOREM I. *For all n*

$$g(n) \;>\; \frac{n}{\varphi(n)}\,\nu(n)\left(1-\frac{c_7\log\log v(n)}{\log v(n)}\right).$$

First we need a lemma which is substantially due to Chang [1].

LEMMA 1. *Let A be any integer and $q_1, q_2, \dots q_k$ be any primes. Then there exists an integer $x_k = x_k(u_k)$, $u_k = \prod_{i=1}^{k} q_i$, so that*

$$\varphi_{u_k}(x_k, x_k + A) \leqq A \prod_{i=1}^{k} (1 - q_i^{-1}) ,$$

$\varphi_{u_k}(x_k, x_k + A)$ denoting the number of integers $x_k < m \leqq x_k + A$ for which $(m, u_k) = 1$.

We use induction with respect to k. Lemma 1 clearly holds if $k = 1$. Suppose that it holds for $k-1$. Then there exists an integer $x_{k-1} = x_{k-1}(u_{k-1})$, $u_{k-1} = \prod_{i=1}^{k-1} q_i$, so that

$$\varphi_{u_{k-1}}(x_{k-1}, x_{k-1} + A) \leqq A \prod_{i=1}^{k-1} (1 - q_i^{-1}) .$$

Denote by $x_{k-1} + j_l$, $1 \leqq l \leqq r$, $r \leqq A \prod_{i=1}^{k-1} (1 - q_i^{-1})$ the integers in $(x_{k-1}, x_{k-1} + A)$ which are relatively prime to u_{k-1}. At least one residue class $(\bmod q_k)$ contains at least r/q_k of these numbers, let this residue class be α_k. Let now

$$x_k \equiv x_{k-1} \pmod{u_{k-1}}, \qquad x_k \equiv -\alpha_k + x_{k-1} \pmod{q_k} .$$

In $(x_k, x_k + A)$ there clearly are at least r/q_k integers which are relatively prime to u_{k-1} and are multiples of q_k. Thus

$$\varphi_{u_k}(x_k, x_k + A) \leqq A \prod_{i=1}^{k} (1 - q_i^{-1}) ,$$

which proves Lemma 1.

PROOF OF THEOREM I. Let $p_1 < \dots < p_{\nu(n)}$ be the distinct prime factors of n and let p_k be the largest prime factor of n which is less than $\nu(n)$. From the prime number theorem (or from the more elementary results of Tschebycheff) we easily obtain by a simple computation that

$$\prod_{i=k+1}^{\nu(n)} (1 - p_i^{-1}) \geqq \prod_{i=1}^{\nu(n)} (1 - r_i^{-1}) > 1 - c_8 \frac{\log\log \nu(n)}{\log \nu(n)}, \tag{8}$$

where $r_1 < r_2 < \dots$, are the consecutive primes $\geqq \nu(n)$. Put

$$A = \frac{n}{\varphi(n)} \nu(n) \left(1 - \frac{c_7 \log\log \nu(n)}{\log \nu(n)}\right).$$

From (8) and Lemma 1 it follows that there exists an integer (or rather a residue class $\bmod v_k$, $v_k = \prod_{i=1}^{k} p_i$) for which

$$\varphi_{v_k}\left(x_k, x_k+A\right) \leqq A \prod_{i=1}^{k} (1-p_i^{-1}\Big)$$

$$= A\,\frac{\varphi(n)}{n} \prod_{i=k+1}^{\nu(n)} (1-p_i^{-1})^{-1}$$

$$(9) \qquad < A\,\frac{\varphi(n)}{n}\left(1-c_8\,\frac{\log\log\nu(n)}{\log\nu(n)}\right)^{-1}$$

$$< \nu(n)\left(1-\frac{2}{\log\nu(n)}\right) < \nu(n)-k$$

for sufficiently large c_7. The last inequality of (9) follows from the fact that

$$k \leqq \pi\left(\nu(n)\right) < \frac{2\nu(n)}{\log\nu(n)}\,.$$

Denote now by x_k+j_l, $1 \leqq l \leqq T < \nu(n)-k$ the integers in (x_k, x_k+A) with $(x_k+j_l, v_k)=1$. By $T<\nu(n)-k$ there clearly exists an integer x_0 satisfying

$$(10 \qquad x \equiv x_k \pmod{v_k}, \qquad x+j_l \equiv 0 \pmod{p_{k+l}}, \qquad 1 \leqq l \leqq T\,.$$

From $k+T<\nu(n)$ it follows that none of the integers in $(x, x+A)$ are relatively prime to n, and this completes the proof of Theorem I.

Next we show that Theorem I is best possible for every $\nu(n)$. Let $q_1<q_2<\ldots<q_r$ be the r consecutive primes greater than r. Put $n_r=\prod_{i=1}^{r} q_i$. Clearly $g(n)=r+1$ and a simple computation (as in (8)) shows that

$$\frac{n_r}{\varphi(n_r)} > 1+\frac{c_9\log\log r}{\log r}\,.$$

Thus

$$g(n_r) = r+1 < \frac{n_r}{\varphi(n_r)}\,r\left(1-\frac{c_{10}\log\log r}{\log r}\right)$$

if c_{10} is sufficiently small, which shows that Theorem I is best possible.

It is much harder to get a good upper bound for $g(n)$. We prove

THEOREM II. *For almost all n*

$$g(n) = \frac{n}{\varphi(n)}\,\nu(n)+o(\log\log\log n)\,.$$

Since by a well known theorem of Hardy and Ramanujan (cf. [5, pp. 356–358]) $\nu(n)=(1+o(1))\,\log\log n$ for almost all n, Theorem II implies (6).

To prove Theorem II we need some simple and well known lemmas.

LEMMA 2. *For almost all* n

$$\nu(n) = \big(1+o(1)\big)\log\log n .$$

This is the theorem of Hardy and Ramanujan mentioned above (cf. [5, pp. 356–358]).

LEMMA 3. *For almost all* n

$$\sum_{\substack{p\mid n\\ p<(\log\log n)^4}} 1 = \big(1+o(1)\big)\log\log\log\log n .$$

Lemma 3 is known (cf. [2]) and can be deduced by the method of Turan [10] used in the proof of the Hardy–Ramanujan theorem.

LEMMA 4. *For almost all* n

$$n/\varphi(n) = o(\log_4 n) ,$$

where $\log_4 n$ *denotes* $\log\log\log\log n$.

LEMMA 4 is also known and follows immediately from

$$\sum_{n=1}^{x} n/\varphi(n) < c_{11}x .$$

The function $\log_4 n$ in Lemma 4 could of course be replaced by any function tending to infinity.

First we prove that for almost all n

$$g(n) < \big(n/\varphi(n)\big)\nu(n)+\varepsilon\log\log\log n = A(\varepsilon,n) , \tag{11}$$

for every $\varepsilon>0$. To prove (11) let

$$p_1 < p_2 < \dots < p_k \leqq (\log\log n)^4 < p_{k+1} < \dots < p_{\nu(n)}$$

be the prime factors of n. From the sieve of Eratosthenes we evidently have $(v_k=\prod_{i=1}^{k}p_i)$

$$\begin{aligned}\varphi_{v_k}\big(x,x+A(\varepsilon,n)\big) &> A(\varepsilon,n)\prod_{i=1}^{k}(1-p_i^{-1})-2^k \\ &> A(\varepsilon,n)\big(\varphi(n)/n\big)-2^k \\ &= \nu(n)+\varepsilon(\log\log\log n)\big(\varphi(n)/n\big)-2^k > \nu(n) .\end{aligned} \tag{12}$$

The last inequality of (12) follows from lemmas 3 and 4.

The interval $(x,x+A(\varepsilon,n))$ can clearly contain at most one integer which is a multiple of p_{k+i}, since

$$p_{k+i} > (\log\log n)^4 > A(\varepsilon,n) .$$

Thus from (12)

$$\varphi_n\big(x,x+A(\varepsilon,n)\big) > \nu(n)-\big(\nu(n)-k\big) = k > 0\,,$$

which proves (11).

PROOF OF THEOREM II. To complete the proof of Theorem II we would have to prove that for almost all n

$$g(n) > \frac{n}{\varphi(n)}\,\nu(n)-\varepsilon \log\log\log n\,.$$

In fact we shall prove very much more. We shall show that for almost all n

(13) $$g(n) > \big(n/\varphi(n)\big)\big(\nu(n)-(1+\varepsilon)\log_4 n\big) = B(\varepsilon,n)\,.$$

We will only outline the proof of (13) since it is very similar to that of Theorem I. From lemmas 3 and 4 we can show by a simple computation that there exists an integer x_k (determined mod v_k) so that

$$\begin{aligned}\varphi_{vk}\big(x,x+B(\varepsilon,n)\big) &\leqq B(\varepsilon,n)\prod_{i=1}^{k}(1-p_i^{-1})\\ &= B(\varepsilon,n)\,\varphi(n)/n+o(1)\\ &< \nu(n)-(1+\tfrac{1}{2}\varepsilon)\log_4 n < \nu(n)-k\,.\end{aligned}$$

Thus as in the proof of Theorem I we can find an x with $\varphi_n\big(x,x+B(\varepsilon,n)\big)=0$, which proves (13) and completes the proof of Theorem II.

Very likely for almost all n

$$g(n) > \big(n/\varphi(n)\big)\nu(n)\,,$$

but I have not been able to prove this.

The upper bound in Theorem II can also be considerably improved by using Brun's method, but I was unable to calculate the distribution function of $g(n)-\big(n/\varphi(n)\big)\nu(n)$, or even to prove its existence. In fact I can not guess the scale in which to measure the growth of this function, On the other hand from (6) and the well known existence (cf. [9]) of the distribution function of $n/\varphi(n)$ it immediately follows that $g(n)/\log\log n$ has a distribution function (which in fact is the same as the distribution function of $n/\varphi(n)$).

THEOREM III. *To every $\varepsilon>0$ and $\eta>0$ there exists an $A_0=A_0(\varepsilon,\eta)$, so that for every $A>A_0(\varepsilon,\eta)$*

(14) $$(1-\varepsilon)A < \varphi_n\big(x,x+An/\varphi(n)\big) < (1+\varepsilon)A$$

for all n, $1\leqq x\leqq n$, except possibly for ηn integers x.

We use the method of Turan [10], but we will suppress some of the details of the proof. Theorem III will clearly follow immediately from $(A > A_0(\varepsilon, n))$

$$I(n,A) = \sum_{x=1}^{n} \big(\varphi_n(x, x+An/\varphi(n) - A\big)^2 < \eta\varepsilon^2 A^2 n\,, \tag{15}$$

since (15) clearly implies that the number of integers x, $1 \leqq x \leqq n$, for which (14) does not hold is less than ηn. Thus we only have to prove (15). We evidently have

$$\begin{aligned} I(n,A) &= \sum_{x=1}^{n} \varphi_n\big(x, x+An/\varphi(n)\big)^2 - 2A \sum_{n=1}^{x} \varphi_n\big(x, x+An/\varphi(n)\big) + nA^2 \\ &= \sum_{x=1}^{n} \varphi_n\big(x, x+An/\varphi(n)\big)^2 - nA^2 + \alpha_n nA\,, \end{aligned} \tag{16}$$

where $|\alpha_n| < 2$, since by interchanging the order of summation we have

$$\begin{aligned} \sum_{x=1}^{n} \varphi_n\big(x, x+An/\varphi(n)\big) &= [An/\varphi(n)]\varphi(n) \\ &= An - \theta_n \varphi(n), \qquad 0 \leqq \theta_n < 1\,. \end{aligned}$$

Let now $(u,n) = (v,n) = 1$, $0 < v-u \leqq An/\varphi(n)$. Then the pair (u,v) occurs in $[An/\varphi(n)] - v + u$ intervals $\big(x, x+An/\varphi(n)\big)$. Denote by $h_i(n)$ the number of solutions of

$$1 \leqq u \leqq n, \qquad (u,n) = (v,n) = 1, \qquad v-u = i\,.$$

Then by interchanging the order of summation we have

$$\begin{aligned} &\sum_{x=1}^{n} \varphi_n\big(x, x+An/\varphi(n)\big)^2 \\ &\qquad = 2 \sum_{i=1}^{[An/\varphi(n)]} \big([An/\varphi(n)] - i\big) h_i(n) + [An/\varphi(n)]\varphi(n)\,. \end{aligned} \tag{17}$$

Clearly by the sieve of Erastothenes

$$h_i(n) = n \prod_{\substack{p \mid n \\ p \nmid i}} (1 - 2p^{-1}) \prod_{p \mid (i,n)} (1 - p^{-1})\,. \tag{18}$$

Thus from (17) and (18)

$$\begin{aligned} &\sum_{x=1}^{n} \varphi_n\big(x, x+An/\varphi(n)\big)^2 \qquad (19) \\ &= 2n \sum_{i=1}^{[An/\varphi(n)]} \big([An/\varphi(n)] - i\big) \prod_{\substack{p \mid n \\ p \nmid i}} (1 - 2p^{-1}) \prod_{p \mid (i,n)} (1 - p^{-1}) + [An/\varphi(n)]\varphi(n)\,. \end{aligned}$$

Now it can be shown that for every $\delta > 0$ if $D > D_0(\delta)$ we have for a certain $|\beta_n| < \delta$

$$\sum_{i=1}^{D} (D-i) \prod_{\substack{p \mid n \\ p \nmid i}} (1-2p^{-1}) \prod_{p \mid (i,n)} (1-p^{-1}) = (\tfrac{1}{2}+\beta_n) D^2 \varphi(n)^2/n^2 . \tag{20}$$

I suppress the proof of (20) since my proof is fairly indirect, inelegant and complicated and I feel that a much simpler proof can be found. From (19) and (20) we evidently have by a simple calculation by putting $[An/\varphi(n)] = D$ for $A > A(\varepsilon, \eta)$ (if δ is sufficiently small)

$$\sum_{x=1}^{n} \varphi_n(x, x+An/\varphi(n))^2 = A^2 n + \theta_n \eta \varepsilon^2 A^2 n , \tag{21}$$

where $|\theta_n| < \frac{1}{2}$. From (21) and (16) we finally obtain

$$|I(n,A)| \leqq |\theta_n \eta \varepsilon^2 A^2 n| + |\alpha_n A n| < \eta \varepsilon^2 A^2 n$$

for $A > A(\varepsilon, \eta)$. This proves (15) and hence the proof of Theorem III is complete.

REFERENCES

1. Teh-Hsien Chang, *Über aufeinanderfolgende Zahlen, von denen jede mindestens einer von n linearen Kongruenzen genügt, deren Moduln die ersten n Primzahlen sind*, Schr. Math. Sem. Inst. Angew. Math. Univ. Berlin 4 (1938), 35–55.
2. P. Erdös, *Note on sequences of integers no one of which is divisible by another*, J. London Math. Soc. 10 (1935), 126–128.
3. P. Erdös, *The difference of consecutive primes*, Duke Math. J. 6 (1940), 438–441.
4. P. Erdös, *Some problems and results in number theory*, Publ. Math. Debrecen 2 (1951–52), 103–109.
5. G. H. Hardy and E. M. Wright, *Theory of numbers* (3rd edition), Oxford, 1954.
6. E. Jacobsthal, *Über Sequenzen ganzer Zahlen von denen keine zu n teilerfremd ist*, I–III, Norske Vidensk. Selsk. Forh. Trondheim 33 (1960), 117–139.
7. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen* I–II, Leipzig, 1909.
8. R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc. 13 (1938), 242–244.
9. I. Schoenberg, *Über die asymptotische Verteilung reeller Zahlen* mod I, Math. Z. 28 (1928), 171–199.
10. P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. 9 (1934), 274–276.

UNIVERSITY OF AARHUS, DENMARK