Glasgow Math. J. **47** (2005) 517–528. © 2005 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089505002752. Printed in the United Kingdom

SOME DIVISIBILITY PROPERTIES OF THE EULER FUNCTION

WILLIAM D. BANKS
Department of Mathematics, University of Missouri, Columbia, MO 65211 USA
e-mail: bbanks@math.missouri.edu

FLORIAN LUCA
Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089,
Morelia, Michoacán, México
e-mail: fluca@matmor.unam.mx

and IGOR E. SHPARLINSKI
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au

(Received 22 February, 2005; accepted 16 May, 2005)

Abstract. Let $\varphi(\cdot)$ denote the Euler function, and let $a > 1$ be a fixed integer. We study several divisibility conditions which exhibit typographical similarity with the standard formulation of the Euler theorem, such as $a^n \equiv 1 \pmod{\varphi(n)}$, and we estimate the number of positive integers $n \le x$ satisfying these conditions.

2000 *Mathematics Subject Classification.* 11A07, 11N37.

1. Introduction. Let $a > 1$ be an integer and let $\varphi(\cdot)$ denote the *Euler function*, whose value $\varphi(m)$ at any positive integer m is the cardinality of the group $(\mathbb{Z}/m\mathbb{Z})^*$. The classical theorem of Euler asserts that

$$n \mid a^{\varphi(n)} - 1 \tag{1}$$

provided that a and n are coprime. It is a well-known and amusing fact that one can "accidentally misplace" the location of the symbol φ in Euler's theorem and still obtain a valid mathematical statement:

$$n \mid \varphi(a^n - 1) \qquad \text{for every } a > 1;$$

see [**14**] for an even stronger statement. In this paper, we study the validity of other divisibility properties of the Euler function with a form similar to (1).

More precisely, let $\mathcal{F}_a(x)$ denote the set of positive integers $n \le x$ that satisfy the condition

$$\varphi(n) \mid a^n - 1, \tag{2}$$

and let $\mathcal{G}_a(x)$ denote the set of positive integers $n \le x$ for which

$$n \mid \varphi(n)^a - 1. \tag{3}$$

We show that both $\mathcal{F}_a(x)$ and $\mathcal{G}_a(x)$ are rather "thin" sets.

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

THEOREM 1. *For a fixed integer $a > 1$, the following estimate holds:*

$$\#\mathcal{F}_a(x) \le x\ \exp\left(-\left(2^{-1/2}+o(1)\right)\sqrt{\log x \log\log\log x}\right),$$

where the function implied by $o(1)$ depends only on a.

THEOREM 2. *Let $a > 1$ be a fixed integer. If a is even, then the estimate*

$$\#\mathcal{G}_a(x) = \pi(x) + O\left(x \exp\left(-\left(2^{-1/2}+o(1)\right)\sqrt{\log x \log\log x}\right)\right),$$

holds, where $\pi(x)$ is the number of primes $p \le x$. If a is odd, then

$$\#\mathcal{G}_a(x) \le x \exp\left(-\left(2^{-1/2}+o(1)\right)\sqrt{\log x \log\log x}\right).$$

Here, the functions implied by $o(1)$ and the constant implied by O depend only on a.

We also investigate the set of positive integers n for which (2) holds for *all* integers a coprime to $\varphi(n)$, which is equivalent to the divisibility condition

$$\lambda(\varphi(n)) \mid n. \tag{4}$$

Here, $\lambda(\cdot)$ denotes the *Carmichael function*, whose value $\lambda(m)$ at a positive integer m is the exponent of the group $(\mathbb{Z}/m\mathbb{Z})^*$, that is, $\lambda(m)$ is the largest multiplicative order of any element in $(\mathbb{Z}/m\mathbb{Z})^*$. More explicitly, for a prime power p^ν, one has

$$\lambda(p^\nu) = \begin{cases} p^{\nu-1}(p-1), & \text{if } p \ge 3 \text{ or } \nu \le 2;\\ 2^{\nu-2}, & \text{if } p = 2 \text{ and } \nu \ge 3;\end{cases}$$

and for an arbitrary integer $m \ge 2$,

$$\lambda(m) = \operatorname{lcm}\left[\lambda\left(p_1^{\nu_1}\right), \dots, \lambda\left(p_k^{\nu_k}\right)\right],$$

where $m = p_1^{\nu_1} \cdots p_k^{\nu_k}$ is the prime factorization of m. Also, $\lambda(1) = 1$.

Let $\mathcal{H}(x)$ denote the set of positive integers $n \le x$ satisfying (4). Clearly, the bound $\#\mathcal{H}(x) \le \#\mathcal{F}_a(x)$ holds for every fixed integer $a > 1$. However, we give a much sharper estimate on $\#\mathcal{H}(x)$ than the one that follows from this inequality and Theorem 1.

THEOREM 3. *The following estimate holds*:

$$\#\mathcal{H}(x) \le \exp\left(O\left((\log x)^{3/4}\right)\right),$$

where the constant implied by O is absolute.

Finally, recall that the famous *Lehmer conjecture* asserts that $\varphi(n) \mid n-1$ if and only if n is a prime number; see [**12**, **13**]. For a fixed polynomial $f(X) \in \mathbb{Z}[X]$, let $\mathcal{L}_f(x)$ denote the set of positive integers $n \le x$ with the property:

$$\varphi(n) \mid f(n). \tag{5}$$

We show that $\lim_{x\to\infty} \mathcal{L}_f(x)/\pi(x)$ exists and is a rational number. More precisely, we show:

THEOREM 4. *Let $f(X) \in \mathbb{Z}[X]$ be a polynomial. For each root m of $f(X)$, there exist certain residue classes $\{\alpha_{j,m} \pmod{\varphi(m)} : j = 1, \dots, r_m\}$ for which the following estimate*

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

holds:

$$\begin{aligned}\#\mathcal{L}_f(x) = \sum_{f(m)=0} \sum_{j=1}^{r_m} \pi(x/m; \varphi(m), \alpha_{j,m}) \\ + O\big(x \exp\big(-\big(2^{-1/2} + o(1)\big)\sqrt{\log x \log\log x}\,\big)\big),\end{aligned}$$

where the function implied by $o(1)$ *and the constant implied by* O *depend only on* f.

In the statement above, $\pi(z; q, \alpha)$ denotes (as usual) the number of primes $p \le z$ in the congruence class $p \equiv \alpha \pmod q$. We now recall the result of Walfisz [**18**], which asserts for every fixed modulus $q \ge 1$, the estimate

$$\pi(z; q, \alpha) = \frac{\pi(z)}{\varphi(q)} + O\left(z \exp\left(-C(q)\frac{(\log z)^{3/5}}{(\log\log z)^{1/5}}\right)\right) \tag{6}$$

holds for some constant $C(q) > 0$ depending only on q (in fact, the earlier result of Tatuzawa [**16**] suffices for our application). Using (6) together with Theorem 4, it follows that for any polynomial $f(X) \in \mathbb{Z}[X]$, there exists a rational number $\kappa_f \ge 0$, depending only on f, such that

$$\#\mathcal{L}_f(x) = \kappa_f \pi(x) + O\big(x \exp\big(-\big(2^{-1/2} + o(1)\big)\sqrt{\log x \log\log x}\,\big)\big).$$

Moreover, if f has no positive integer root, then $\kappa_f = 0$.

For a slightly restricted class of polynomials, using ideas from [**12**], we obtain the following stronger statement.

THEOREM 5. *Let* $f(X) \in \mathbb{Z}[X]$ *be a polynomial of degree* k, *with* $f(0) \ne 0$, *whose roots all have multiplicity at most* ν. *For each root* m *of* $f(X)$, *there exist certain residue classes* $\{\alpha_{j,m} \pmod{\varphi(m)} : j = 1, \dots, r_m\}$ *for which the following estimate holds*:

$$\begin{aligned}\#\mathcal{L}_f(x) = \sum_{f(m)=0} \sum_{j=1}^{r_m} \pi(x/m; \varphi(m), \alpha_{j,m}) \\ + O\big(x^{1-1/(2\nu+1)+o(1)} + x^{1-1/(k+1)+o(1)}\big),\end{aligned}$$

where the function implied by $o(1)$ *and the constant implied by* O *depend only on* f.

Under the conditions of Theorem 5, from (6) we derive the estimate

$$\#\mathcal{L}_f(x) = \kappa_f \pi(x) + O\left(x \exp\left(-C_f \frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right)$$

for some constants κ_f and $C_f > 0$ that depend only on f. Moreover, under the *Extended Riemann Hypothesis*, it follows that

$$\#\mathcal{L}_f(x) = \kappa_f \pi(x) + O\big(x^{1-1/(2\nu+1)+o(1)} + x^{1-1/(k+1)+o(1)}\big).$$

Throughout this paper, the letters p, q and r are always used to denote prime numbers. We use the Vinogradov symbols $\ll$ and $\gg$, and the Landau symbols O and o with their usual meanings; *the implied constants may depend, where obvious, on the integer* a *or the polynomial* f.

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

For a positive real number x, we write $\log x$ for the maximum of the natural logarithm of x and 1. For a positive integer n, $P(n)$ denotes the largest prime factor of n (and $P(1) = 1$).

Our arguments rely on several well-known results about the distribution of *smooth numbers*, that is, positive integers $n \le x$ with $P(n) \le y$; see, for example, [**6**, **8**, **17**] for exhaustive accounts of such results. We also apply recent results about smooth values of the Euler function; see [**1**].

2. Preliminaries.

We need the following result of Canfield, Erdős and Pomerance [**3**] on smooth numbers (see also Hildebrand [**7**] for a similar estimate in a wider range):

Lemma 6. *Uniformly for* $\exp(\sqrt{\log x}\,) \le y \le x$, *the set*

$$\mathcal{S}(x, y) = \{n \le x : P(n) \le y\}$$

has the cardinality

$$\#\mathcal{S}(x, y) = x \exp(-(1 + o(1))u \log u),$$

where $u = (\log x)/(\log y)$.

We also need the following simplified version of Theorem 3.1 in [**1**]:

Lemma 7. *Uniformly for* $\exp(\sqrt{\log x}\,) \le y \le x$, *the set*

$$\mathcal{T}(x, y) = \{n \le x : P(\varphi(n)) \le y\}$$

has its cardinality bounded by

$$\#\mathcal{T}(x, y) \le x \exp(-(1 + o(1))\, u \log\log u),$$

provided that $u = (\log x)/(\log y) \to \infty$.

Finally, we need the following simple estimate, which is an immediate consequence of the *Prime Number Theorem* together with partial summation:

Lemma 8. *Uniformly for* $x \ge y \ge 2$, *the set*

$$\mathcal{U}(x, y) = \{n \le x : p^2 \mid n \textit{ for some prime } p \ge y\}$$

has its cardinality bounded by

$$\#\mathcal{U}(x, y) \ll \frac{x}{y \log y}.$$

3. Proof of Theorem 1.

Let x be a large positive real number, and put

$$y = \exp(\sqrt{2 \log x \log\log\log x}\,).$$

By Lemma 7, we have the estimate

$$\#\mathcal{T}(x, y) \le x \exp(-\sqrt{(0.5 + o(1)) \log x \log\log\log x}\,), \tag{7}$$

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

and by Lemma 8, the following estimate holds:

$$\#\mathcal{U}(x,y) \le x\exp(-\sqrt{(2+o(1))\log x \log\log\log x}). \tag{8}$$

Now let $\mathcal{N}$ be the set of positive integers $n \le x$ that satisfy (2) but do not lie in $\mathcal{T}(x,y)\cup\mathcal{U}(x,y)$. For every $n\in\mathcal{N}$, since $n\notin\mathcal{T}(x,y)$, it follows that the prime $p = P(\varphi(n))$ has the properties:

(i) $p > y$;
(ii) $p \mid \varphi(n)$;
(iii) $p \mid a^n - 1$.

As $p^2 \nmid n$ (since $n \notin \mathcal{U}(x,y)$), there exists a prime $q \equiv 1 \pmod p$ such that $q \mid n$. If t_p denotes the order of a modulo p (note that we can assume that x is large enough so that a is not divisible by any prime $p > y$), then from (iii) we deduce that $t_p \mid n$. Clearly, $t_p < p < q \le n \le x$, and therefore $\gcd(q, t_p) = 1$; consequently, $n \equiv 0 \pmod{q\cdot t_p}$. Thus,

$$\#\mathcal{N} \le \sum_{p>y}\sum_{\substack{q\le x\\ q\equiv 1 \pmod p}} \frac{x}{qt_p} = x\sum_{p\ge y}\frac{1}{t_p}\sum_{\substack{q\le x\\ q\equiv 1 \pmod p}}\frac{1}{q}.$$

Applying the well-known bound

$$\sum_{\substack{q\le x\\ q\equiv 1 \pmod p}}\frac{1}{p} \ll \frac{\log\log x}{p},$$

(see, for example, the proof of Theorem 3.4 in [**5**], or that of Lemma 2 in [**11**]), we deduce that

$$\begin{aligned}\#\mathcal{N} &\ll x\log\log x\sum_{p>y}\frac{1}{pt_p} = x\log\log x\sum_{j=0}^{\infty}\sum_{2^jy<p\le 2^{j+1}y}\frac{1}{pt_p}\\ &\le \frac{x\log\log x}{y}\sum_{j=0}^{\infty}2^{-j}\sum_{2^jy<p\le 2^{j+1}y}\frac{1}{t_p} \le \frac{x\log\log x}{y}\sum_{j=0}^{\infty}2^{-j}\sum_{t=1}^{\infty}\frac{1}{t}R_j(t),\end{aligned}$$

where $R_j(t)$ is the number of primes p with $2^jy < p \le 2^{j+1}y$ and $t_p = t$. Since $p \mid a^t - 1$ whenever $t_p = t$, it follows that we have $R_j(t) \ll t/\log(2^jy)$. If $T_j < 2^{j+1}y$, then

$$\begin{aligned}\sum_{t=1}^{\infty}\frac{1}{t}R_j(t) &= \sum_{t\le 2^{j+1}y}\frac{1}{t}R_j(t) \le \sum_{t\le T_j}\frac{1}{t}R_j(t) + \frac{1}{T_j}\sum_{T_j<t\le 2^{j+1}y}R_j(t)\\ &\ll \sum_{t\le T_j}\frac{1}{\log(2^jy)} + \frac{1}{T_j}\pi(2^{j+1}y) \ll \frac{T_j}{\log(2^jy)} + \frac{2^jy}{T_j\log(2^jy)}.\end{aligned}$$

We now choose $T_j = (2^jy)^{1/2}$ (to balance the last two terms), substitute the resulting bound into the preceding estimate for $\#\mathcal{N}$, and sum over j, obtaining:

$$\#\mathcal{N} \ll \frac{x\log\log x}{y^{1/2}\log y} \le x\exp(-\sqrt{(0.5+o(1))\log x\log\log\log x}). \tag{9}$$

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

Inserting the bounds (7), (8) and (9) into the inequality

$$\#\mathcal{F}_a(x) \le \#\mathcal{T}(x, y) + \#\mathcal{U}(x, y) + \#\mathcal{N},$$

we finish the proof. □

4. Proof of Theorem 2. Let x be a large positive real number, and put

$$y = \exp(\sqrt{0.5 \log x \log\log x}).$$

From Lemma 6, it follows that

$$\#\mathcal{S}(x, y) = x \exp(-\sqrt{(0.5 + o(1)) \log x \log\log x}), \tag{10}$$

and by Lemma 8, we have the bound:

$$\#\mathcal{U}(x, y) \le x \exp(-\sqrt{(0.5 + o(1)) \log x \log\log x}). \tag{11}$$

Now let $\mathcal{N}$ be the set of positive integers $n \le x$ that satisfy (3) but do not lie in $\mathcal{S}(x, y) \cup \mathcal{U}(x, y)$. For every $n \in \mathcal{N}$, write $n = pm$ with $p = P(n)$. Since $n \notin \mathcal{S}(x, y) \cup \mathcal{U}(x, y)$, it follows that $p > y$ and $p^2 \nmid n$; thus,

$$p \mid \varphi(pm)^a - 1 = (p - 1)^a \varphi(m)^a - 1,$$

and therefore,

$$p \mid \varphi(m)^a - (-1)^a.$$

Note that if a is even and $\varphi(m) = 1$, this condition is always satisfied; on the other hand, if $m = 2$, then $n = 2p$ cannot divide the odd number $\varphi(n)^a - 1$.

Now let $\mathcal{Q}$ be defined as the empty set $\varnothing$ if a is odd, and as the set of primes $p \le x$ if a is even. In each case, one has $\mathcal{Q} \subset \mathcal{G}_a(x)$, and therefore,

$$\#\mathcal{G}_a(x) = \#\mathcal{Q} + O\left(\#\mathcal{S}(x, y) + \#\mathcal{U}(x, y) + \#\left(\mathcal{N} \setminus \mathcal{Q}\right)\right). \tag{12}$$

If $n = pm$ lies in $\mathcal{N} \setminus \mathcal{Q}$, then $m < x/y$, and a is odd or $\varphi(m) > 1$; in particular, $m \ge 3$ and $\varphi(m)^a - (-1)^a \ne 0$. On the other hand, for fixed m in the range $3 \le m < x/y$, there are at most

$$\omega\left(\varphi(m)^a - (-1)^a\right) \ll \frac{\log x}{\log\log x}$$

choices of a prime $p > P(m)$ for which $n = pm$ lies in $\mathcal{N} \setminus \mathcal{Q}$, where $\omega(N)$ is the number of distinct prime factors of an integer $N \ge 1$. Consequently,

$$\begin{aligned}\#\left(\mathcal{N} \setminus \mathcal{Q}\right) &\le \sum_{3 \le m < x/y} \omega\left(\varphi(m)^a - (-1)^a\right)\\ &\ll \frac{x \log x}{y \log\log x} \le x \exp(-\sqrt{(0.5 + o(1)) \log x \log\log x}).\end{aligned}$$

Substituting this bound together with (10) and (11) into the estimate (12), we finish the proof. □

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

5. Proof of Theorem 3. We begin with the following statement, which may be of independent interest; our proof uses *Rankin's method* (see, for example, Chapter III.5 in [**17**]).

Lemma 9. *Let $\mathcal{P}$ be a finite set of odd primes, and let $\mathcal{Q}_{\mathcal{P}}$ be the set of odd primes q with the property that if a prime p divides $q-1$, then $p=2$ or $p \in \mathcal{P}$. Finally, let $\mathcal{M}_{\mathcal{P}}$ be the set of squarefree positive integers m with the property that if a prime q divides m, then $q \in \mathcal{Q}_{\mathcal{P}}$. Then*

$$\#\{m \in \mathcal{M}_{\mathcal{P}} : m \le x\} \le \exp\big(O\big((\log x)^{(\#\mathcal{P}+1)/(\#\mathcal{P}+2)}\big)\big),$$

where the implied constant depends only on $\#\mathcal{P}$.

Proof. For an arbitrary real number $c > 0$, we have the bound

$$\#\{m \in \mathcal{M}_{\mathcal{P}} : m \le x\} = \sum_{\substack{m \le x \\ m \in \mathcal{M}_{\mathcal{P}}}} 1 \le \sum_{\substack{m \le x \\ m \in \mathcal{M}_{\mathcal{P}}}} \left(\frac{x}{m}\right)^c \le x^c \sum_{\substack{m \in \mathcal{M}_{\mathcal{P}} \\ q \mid m \;\Rightarrow\; q \le x}} \frac{1}{m^c}$$
$$= x^c \prod_{\substack{q \le x \\ q \in \mathcal{Q}_{\mathcal{P}}}} \left(1 + \frac{1}{q^c}\right) \le x^c \exp\left(\sum_{\substack{q \le x \\ q \in \mathcal{Q}_{\mathcal{P}}}} \frac{1}{q^c}\right).$$

Moreover,

$$\sum_{\substack{q \le x \\ q \in \mathcal{Q}_{\mathcal{P}}}} \frac{1}{q^c} \le \sum_{\substack{q \le x \\ q \in \mathcal{Q}_{\mathcal{P}}}} \frac{1}{(q-1)^c}$$
$$\le \left(1 + \frac{1}{2^c} + \frac{1}{2^{2c}} + \cdots\right) \prod_{p \in \mathcal{P}} \left(1 + \frac{1}{p^c} + \frac{1}{p^{2c}} + \cdots\right)$$
$$= (1-2^{-c})^{-1} \prod_{p \in \mathcal{P}} (1-p^{-c})^{-1} \le (1-2^{-c})^{-(\#\mathcal{P}+1)}.$$

Now choose c such that

$$(1-2^{-c})^{-1} = (\log x)^{1/(\#\mathcal{P}+2)}.$$

Then, from the preceding estimate, we have

$$\sum_{\substack{q \le x \\ q \in \mathcal{Q}_{\mathcal{P}}}} \frac{1}{q^c} \le (\log x)^{(\#\mathcal{P}+1)/(\#\mathcal{P}+2)}.$$

Also,

$$c \log 2 = -\log\big(1 - (\log x)^{-1/(\#\mathcal{P}+2)}\big) = O\big((\log x)^{-1/(\#\mathcal{P}+2)}\big),$$

where the implied constant depends only on $\#\mathcal{P}$; thus,

$$x^c = \exp(c \log x) = \exp\big(O\big((\log x)^{(\#\mathcal{P}+1)/(\#\mathcal{P}+2)}\big)\big).$$

The result follows. □

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

We now turn to the proof of Theorem 3. Let $n \in \mathcal{H}(x)$ be fixed, and let $n = 2^\alpha \prod_{\ell=1}^{L} p_\ell^{\beta_\ell}$ be its prime factorization. Since $\lambda(\varphi(n))$ is odd only for $n \in \{1, 2, 3, 4, 6\}$, we can assume that $\alpha \geq 1$ in what follows. We can further assume that $L \geq 1$, since the set of integers in $\mathcal{H}(x)$ of the form $n = 2^\alpha$ has at most $O(\log x)$ elements.

Let $\mathcal{P} = \{p_1, \dots, p_L\}$ be the set of odd primes p that divide n, and let $\mathcal{Q}$ be the set of odd primes q that divide $\varphi(n)$ but not n. Assuming $p_1 < \cdots < p_L$, we write

$$p_\ell - 1 = 2^{\alpha_\ell} \prod_{j=1}^{\ell-1} p_j^{\gamma_{\ell,j}} \prod_{q \in \mathcal{Q}} q^{\delta_{\ell,q}}, \qquad 1 \leq \ell \leq L, \tag{13}$$

where $\gamma_{\ell,j} \geq 0$ and $\delta_{\ell,q} \geq 0$ (for example, p_1 must be a Fermat prime). We also put $\gamma_{\ell,j} = 0$ for $j \geq \ell$. For all choices of ℓ, j, q, we obtain that

$$\begin{aligned}\varphi(n) &= 2^{\alpha-1} \prod_{\ell=1}^{L} p_\ell^{\beta_\ell - 1}(p_\ell - 1) = 2^{\alpha-1} \prod_{\ell=1}^{L} p_\ell^{\beta_\ell - 1} \left(2^{\alpha_\ell} \prod_{j=1}^{L} p_j^{\gamma_{\ell,j}} \prod_{q \in \mathcal{Q}} q^{\delta_{\ell,q}} \right) \\ &= 2^{\alpha-1+A} \prod_{j=1}^{L} p_j^{\beta_j - 1 + C_j} \prod_{q \in \mathcal{Q}} q^{D_q},\end{aligned}$$

where

$$\begin{aligned} A &= \sum_{\ell=1}^{L} \alpha_\ell, \\ C_j &= \sum_{\ell=1}^{L} \gamma_{\ell,j}, \qquad 1 \leq j \leq L, \\ D_q &= \sum_{\ell=1}^{L} \delta_{\ell,q}, \qquad q \in \mathcal{Q}. \end{aligned}$$

Since $\mathcal{P} \cap \mathcal{Q} = \varnothing$, it follows that

$$\lambda(\varphi(n)) = \mathrm{lcm}\Big[\lambda\left(2^{\alpha-1+A}\right), \left\{\lambda\left(p_j^{\beta_j-1+C_j}\right)\right\}_{1\leq j\leq L}, \left\{\lambda\left(q^{D_q}\right)\right\}_{q\in\mathcal{Q}}\Big],$$

and therefore,

$$\mathrm{lcm}\Big[\lambda\left(2^{\alpha-1+A}\right), \left\{\lambda\left(p_j^{\beta_j-1+C_j}\right)\right\}_{1\leq j\leq L}, \left\{\lambda\left(q^{D_q}\right)\right\}_{q\in\mathcal{Q}}\Big] \,\Big|\, 2^\alpha \prod_{\ell=1}^{L} p_\ell^{\beta_\ell}. \tag{14}$$

Using properties of the Carmichael function, it is easy to see that

(i) $A \leq 3$;

(ii) $C_j \leq 2$ for $1 \leq j \leq L$;

(iii) $D_q \leq 1$ for $q \in \mathcal{Q}$.

Note that the condition (i) implies that $L \leq 3$.

We claim that each $D_q = 1$. Indeed, if $q \in \mathcal{Q}$, then

$$q \mid 2^{\alpha-1} \prod_{\ell=1}^{L} p_\ell^{\beta_\ell - 1}(p_\ell - 1), \qquad \text{and} \qquad q \nmid 2^\alpha \prod_{\ell=1}^{L} p_\ell^{\beta_\ell}.$$

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

Hence, $q \mid (p_\ell - 1)$ for some ℓ, which implies that $\delta_{\ell,q} \geq 1$. The claim now follows from (iii).

Using (14) and the fact that $D_q = 1$ for every $q \in \mathcal{Q}$, it follows that

$$(q-1) \,\Big|\, 2^\alpha \prod_{\ell=1}^{L-1} p_\ell^{\beta_\ell}, \qquad q \in \mathcal{Q}.$$

Here, we have used the fact that $p_L \nmid (q-1)$, which follows from the factorization (13). Defining $\mathcal{P}^* = \{p_1, \ldots, p_{L-1}\}$, it is clear that $\mathcal{Q}$ is a subset of the set $\mathcal{Q}_{\mathcal{P}^*}$ defined in Lemma 9 (with $\mathcal{P}$ replaced by $\mathcal{P}^*$). Moreover, each quantity $\prod_{q\in\mathcal{Q}} q^{\delta_{\ell,q}}$ that occurs in (13) clearly lies in the set $\mathcal{M}_{\mathcal{P}^*}$. By (i) and (ii), the exponents α_ℓ and $\gamma_{\ell,j}$ in (13) are all less than or equal to 3. Since $\#\mathcal{P}^* = L - 1 \leq 2$, Lemma 9 now implies that each prime p_j can be chosen in at most $\exp(O((\log x)^{3/4}))$ different ways, and the result follows. □

6. Proof of Theorem 4. As in Section 4, we put

$$y = \exp(\sqrt{0.5 \log x \log\log x}).$$

Thus, we can again use the estimates (10) and (11).

Let $\mathcal{N}$ be the set of positive integers $n \leq x$ that satisfy (5) but do not lie in $\mathcal{S}(x, y) \cup \mathcal{U}(x, y)$. For every $n \in \mathcal{N}$, we write $n = pm$ where $p = P(n)$. Since $\gcd(p, m) = 1$, we have $\varphi(n) = (p-1)\varphi(m)$. In particular, from (5) we derive that

$$f(m) \equiv f(pm) = f(n) \equiv 0 \pmod{p-1}.$$

Hence, for each fixed $m \leq x/y$ such that $f(m) \neq 0$, there are at most $\tau\,(|f(m)|)$ possible choices for a prime p for which $n = pm$ lies in $\mathcal{N}$, where $\tau(N)$ is the number of positive integer divisors of $N \geq 1$. The classical result of van der Corput (see [**4**, **10**]) shows that

$$\sum_{\substack{m<x/y\\ f(m)\neq 0}} \tau\,(|f(m)|) \ll \frac{x(\log x)^{K_f}}{y} \ll x\exp(-\sqrt{(0.5 + o(1))\log x \log\log x}),$$

where K_f is a constant depending only on f.

We now consider the polynomial $F(X, Y) = f(XY) - f(X)$. Clearly $F(X, Y) = (Y-1)G(X, Y)$ for some $G(X, Y) \in \mathbb{Z}[X, Y]$. Thus, if $f(m) = 0$, then the condition $(p-1)\varphi(m) \mid f(pm)$ is equivalent to $\varphi(m) \mid G(m, p)$. Hence, if m is a root of f, we have that $n = pm$ lies in $\mathcal{N}$ if and only if the prime p belongs to one of the progressions $p \equiv \alpha_{j,m} \pmod{\varphi(m)}$, where $\alpha_{j,m}$, $j = 1, \ldots, r_m$, runs through all r_m roots of the congruence $G(m, r) \equiv 0 \pmod{\varphi(m)}$. Therefore, we see that for some rational number $\kappa_f \geq 0$ and real number $c_f > 0$, depending only on f, there are

$$\sum_{f(m)=0} \sum_{j=1}^{r_m} \sum_{\substack{p\leq x/m\\ p\equiv\alpha_{j,m} \pmod{\varphi(m)}}} 1 = \sum_{f(m)=0} \sum_{j=1}^{r_m} \pi(x/m; \varphi(m), \alpha_{j,m}) \tag{15}$$

integers $n = pm$ lying in $\mathcal{N}$, and we obtain the bound stated in the theorem. As it is clear that $\kappa_f = 0$ if f has no integer roots, the proof is complete. □

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

7. Proof of Theorem 5. For positive integers r and ν, we put

$$\rho_\nu(r) = \prod_{j=1}^{s} q_j^{\lceil \gamma_j/\nu \rceil},$$

where

$$r = \prod_{j=1}^{s} q_j^{\gamma_j}$$

is the prime factorization of r. We also denote by $F(X) \in \mathbb{Z}[X]$ the product of all of the irreducible divisors of $f(X)$; in particular, $f(X) \mid F(X)^\nu$. Finally, let

$$\alpha = \frac{\nu}{2\nu+1} \qquad \text{and} \qquad \beta = \frac{k}{k+1}.$$

If $p \mid n$ and $\varphi(n) \mid f(n)$, then obviously $f(m) \equiv f(n) \equiv 0 \pmod{p-1}$, where $m = n/p$. Therefore, $F(m) \equiv 0 \pmod{\rho_\nu(p-1)}$. By the *Nagell–Ore theorem* (see [**9**] for the strongest known form), we see that for every p, there are

$$M_p \ll \left(\frac{x}{p\rho_\nu(p-1)} + 1 \right) p^{o(1)}$$

values of $m \le x/p$ satisfying the last congruence. Therefore, the number of $n \le x$ such that $\varphi(n) \mid f(n)$ and also having a prime divisor p in the range $x^\alpha \le p \le x^\beta \log x$ is bounded by

$$\begin{aligned} \sum_{x^{1/(k+1)} \le p \le x^\beta \log x} M_p &\ll \sum_{x^\alpha \le p \le x^\beta \log x} \left(\frac{x}{p\rho_\nu(p-1)} + 1 \right) p^{o(1)} \\ &\ll \sum_{x^\alpha \le p \le x^\beta \log x} \left(\frac{x}{p^{1+1/\nu}} + 1 \right) p^{o(1)} \le x^{1-\alpha/\nu+o(1)} + x^{\beta+o(1)}, \end{aligned}$$

since $\rho_\nu(r) \ge r^{1/\nu}$ for any r.

Now, if $p \ge x^\beta \log x$, then $m \ll x^{1/(k+1)}(\log x)^{-1}$; hence, $f(m) \equiv 0 \pmod{p-1}$ implies that $f(m) = 0$. The contribution from such $n = pm$ is given by (15) from the proof of Theorem 4.

It remains to consider those $n \le x$ such that $P(n) \le x^\alpha$. Clearly, every such n has a divisor m with $x^\alpha \le m \le x^{2\alpha}$. Writing $n = mr$ we see that $\varphi(m) \mid f(n) = f(mr)$ implies that $F(mr) \equiv 0 \pmod{\rho_\nu(\varphi(m))}$. For fixed m, if the last congruence is solvable, then $\gcd(m, \rho_\nu(\varphi(m))) | F(0) | f(0)$. Since $f(0) \ne 0$, this shows that $\gcd(m, \rho_\nu(\varphi(m))) = O(1)$. Now, applying the Nagell–Ore theorem once more, we see that for every m, there are

$$R_m \ll \left(\frac{x}{m\rho_\nu(\varphi(m))} + 1 \right) m^{o(1)}$$

values of $r \le x/m$ with $F(mr) \equiv 0 \pmod{\rho_\nu(\varphi(m))}$. Therefore, the number of $n \le x$

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

such that $\varphi(n) \mid f(n)$ and also having a divisor m with $x^{\alpha} \le m \le x^{2\alpha}$ is bounded by

$$\sum_{x^{\alpha} \le m \le x^{2\alpha}} R_m \ll \sum_{x^{\alpha} \le m \le x^{2\alpha}} \left(\frac{x}{m\rho_{\nu}(\varphi(m))} + 1 \right) m^{o(1)}$$
$$\ll \sum_{x^{\alpha} \le m \le x^{2\alpha}} \left(\frac{x}{m^{1+1/\nu}} + 1 \right) m^{o(1)} \le x^{1-\alpha/\nu+o(1)} + x^{2\alpha+o(1)}.$$

Recalling the choice of α and β, we obtain the desired result. □

8. Remarks. It is easy to show that, for any positive integer k, there are infinitely many integers $a > 1$ for which the lower bound

$$\mathcal{F}_a(x) \gg (\log x)^k$$

holds. Indeed, let $p_1, \dots, p_k$ be distinct primes, and suppose that the integer $s = p_1 \cdots p_k$ satisfies the condition

$$\gcd(\varphi(s), s) = 1.$$

For instance, one can choose large primes p_j such that $\max_j\{p_j\} < 2\min_j\{p_j\}$ and $P(p_j - 1) \le \sqrt{p_j}$ for each j; see [**2**]. Now let $b > 1$ be an integer such that

$$b \equiv 1 \pmod{\varphi(s)},$$

and put $a = b^{\varphi(s)}$. Then, for any integer n composed only out of the primes $p_1, \dots, p_k$, we have (2).

It is also easy to check that every positive integer n of the form $n = 2^{\alpha} \cdot 3^{\beta} \cdot 7^{\gamma} \cdot 43^{\delta}$, with arbitrary positive integer exponents $\alpha, \beta, \gamma, \delta$, satisfies the relation (4). Therefore,

$$\#\mathcal{H}(x) \gg (\log x)^4.$$

These lower bounds, however, are still far from the upper bounds given in this paper. It would be interesting to know, even conjecturally, the actual rate of growth of these functions.

Acknowledgements. The authors would like to thank Carl Pomerance whose suggestion has led to the formulation and proof of Theorem 5. During the preparation of this paper, F. L. was supported in part by grant PAPIIT IN104505, and I. S. was supported in part by ARC grant DP0211459.

REFERENCES

1. W. Banks, J. B. Friedlander, C. Pomerance and I. E. Shparlinski, Multiplicative structure of values of the Euler function, in *High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams*, Fields Institute Communications, Vol. 41 (Amer. Math. Soc., 2004), 29–48.

2. R. C. Baker and G. Harman, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331–361.

3. E. R. Canfield, P. Erdős and C. Pomerance, On a problem of Oppenheim concerning "factorizatio numerorum", *J. Number Theory* **17** (1983), 1–28.

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press

4. J. G. van der Corput, Une inégalité relative au nombre des diviseurs, *Proc. Nederl. Akad. Wetensch.* **42** (1939), 547–553.

5. P. Erdős, A. Granville, C. Pomerance and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, in *Analytic Number Theory* (Birkhäuser, 1990), 165–204.

6. A. Granville, Smooth numbers: Computational number theory and beyond, in *Proc. MSRI Conf. Algorithmic Number Theory*: *Lattices, Number Fields, Curves, and Cryptography, Berkeley 2000* (Cambridge University Press) (to appear).

7. A. Hildebrand, On the number of positive integers $\leq x$ and free of prime factors $> y$, *J. Number Theory* **22** (1986), 289–307.

8. A. Hildebrand and G. Tenenbaum, Integers without large prime factors, *J. de Théorie des Nombres de Bordeaux*, **5** (1993), 411–484.

9. M. N. Huxley, A note on polynomial congruences, in *Recent Progress in Analytic Number Theory, Vol.1* (Academic Press, 1981), 193–196.

10. B. Landreau, A new proof of a theorem of van der Corput, *Bull. London Math. Soc.* **21** (1989), 366–368.

11. F. Luca and C. Pomerance, On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions φ and σ, *Colloq. Math.* **92** (2002), 111–130.

12. C. Pomerance, On composite n for which $\varphi(n) \mid n-1$, *Acta Arith.* **28** (1976), 387–389.

13. C. Pomerance, On composite n for which $\varphi(n) \mid n-1$, II, *Pacific J. Math.* **69** (1976), 177–186.

14. A. Rotkiewicz, On the numbers $\varphi(a^n \pm b^n)$, *Proc. Amer. Math. Soc.* **12** (1961), 419–421.

15. M. V. Subbarao, On two congruences for primality, *Pacific J. Math.* **52** (1974), 261–268.

16. T. Tatuzawa, On the number of the primes in an arithmetic progression, *Jap. J. Math.* **21** (1951), 93–111.

17. G. Tenenbaum, *Introduction to analytic and probabilistic number theory* (Cambridge University Press, 1995).

18. A. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie* (VES Dentscher Verlag der Wissenschaften, Berlin, 1963).

https://doi.org/10.1017/S0017089505002752 Published online by Cambridge University Press