ACTA ARITHMETICA
109.4 (2003)

Average multiplicative orders of elements modulo n

by

Florian Luca (Morelia) and Igor E. Shparlinski (Sydney)

1. Introduction and notation. Let n be a positive integer. In [8], the function $\alpha(n)$ which gives the average additive order of elements modulo n has been considered, and several of its properties have been investigated, such as mean value, minimal and maximal order, and so on. The behaviour of this function restricted only to shifted primes (say, only to positive integers n of the form $p-1$ with p a prime number), or to numbers of the form 2^n-1 has been investigated in [8] and [13].

In this paper, we take a positive integer n and denote by $u(n)$ the average multiplicative order of invertible elements modulo n. That is, let $U_n := U(\mathbb{Z}_n)$ denote the group of invertible elements modulo n. This is an abelian group of order $\varphi(n)$, where φ is the Euler function. The *exponent* of U_n, that is, the maximal order of elements in U_n, is the Carmichael function $\lambda(n)$. If

$$n := \prod_{p^\alpha \,\|\, n} p^\alpha$$

then

$$\lambda(n) := \operatorname{lcm}(\lambda(p^\alpha) \mid p^\alpha \,\|\, n),$$

where $\lambda(p^\alpha) = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$ if p is odd, and $\lambda(2)=1,\ \lambda(4)=2$, and $\lambda(2^\alpha)=2^{\alpha-2}$ when $\alpha \ge 3$, and as usual $p^\alpha \,\|\, n$ means $p^\alpha \mid n$ but $p^{\alpha+1} \nmid n$.

For every $d \mid \lambda(n)$ we write $a(d)$ for the number of elements of U_n whose order is precisely d. Then

$$u(n) := \frac{1}{\varphi(n)} \sum_{d \mid \lambda(n)} d a(d).$$

For any positive integer n we also use $\sigma(n)$, $\omega(n)$, $\Omega(n)$ with their usual meanings, as the sum of all positive integer divisors of n, the number of distinct prime divisors of n, and the total number of prime divisors of n (that is, counted with multiplicities), respectively.

2000 *Mathematics Subject Classification*: Primary 11N37, 11N64; Secondary 20K01.

For every positive integer n we let $\mathrm{rad}(n)$ stand for the *radical* of n, that is,

$$\mathrm{rad}(n) = \prod_{p|n} p$$

is the largest square-free divisor of n. We also use the Landau symbols O and o as well as the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings.

Moreover, for any positive integer k and any positive real number x, we define recursively the function $\log_k x$ as being $\log_1 x := \max\{\log x, 1\}$ and $\log_k x := \max\{\log(\log_{k-1} x), 1\}$, where $\log x$ stands for the natural logarithm of x. We write $\log_1 x$ as $\log x$ and thus we always have $\log x \ge 1$.

We use some basic properties of prime numbers as well as their asymptotic growth. We also need a couple of more advanced tools.

One of them is *Chen's theorem* which we present in the form in which it appears in [9]:

> Let k be an even positive integer. Then there exists $x_0(k)$ so that for $x > x_0(k)$ the interval $[x, 2x]$ contains at least $T \gg x/\log^2 x$ prime numbers p such that $p-1 = kl$ and l is divisible by at most two distinct primes, each exceeding $x^{1/4}$.

The other one is *Linnik's theorem* which we present in the explicit form given in [10]:

> Let $k \ge 1$ and $a \ge 1$ be coprime integers. Then there exists a prime number $p \equiv a \pmod k$ which satisfies $p = O(k^{5.5})$.

Moreover, for one of our results we need Theorem 2.1 of [1] showing that for most of the progressions the constant 5.5 can be replaced with $12/5 + \varepsilon$ for any fixed $\varepsilon > 0$.

Acknowledgements. The authors would like to thank Joachim von zur Gathen whose question initiated this work. A substantial part of this work was done during a visit by the second author to UNAM, whose hospitality and excellent working conditions are very much appreciated. The first author acknowledges support from Grant SEP-CONACyT 37259-E.

2. Average orders in arbitrary finite abelian groups. In this section, we aim at giving a general formula for the average order of elements in an arbitrary finite abelian group, and in the next section we shall specialize this result to the case of the group U_n.

Let G be a finite abelian group (written multiplicatively); we use 1 to refer to the identical element in G. We also use $\#G$ to denote the order of G, and $\lambda(G)$ for the *exponent* of G, that is, the maximal order of elements in G. For every $d \mid \lambda(G)$ we write $b_G(d)$ for the number of elements in G of exponent d (that is, the number of elements $x \in G$ such that $x^d = 1$), and $a_G(d)$ for the number of elements of order precisely d. We find it useful to extend the two functions $d \mapsto b_G(d)$ and $d \mapsto a_G(d)$ to the set of all positive integers by setting for an arbitrary positive integer n, $b_G(n) := b_G(\gcd(\lambda(G), n))$ and $a_G(n) := 0$ if $n \nmid \lambda(G)$. It is now clear that

$$b_G(n) = \sum_{d|n} a_G(d) \tag{1}$$

for all positive integers n. Finally, we use $u(G)$ for the average order of elements in G:

$$u(G) := \frac{1}{\#G} \sum_{d|\lambda(G)} d a_G(d).$$

LEMMA 1. *Both functions a_G and b_G are multiplicative.*

Proof. The formula (1) shows that b_G is the convolution of a_G with the function which associates to any positive integer n the constant value 1. Thus, it suffices to show that b_G is multiplicative. Let m and n be two coprime positive integers and to any pair (x, y) of elements in G, x of exponent m and y of exponent n, we associate the element xy. Clearly, xy has exponent mn and so it is counted by $b_G(mn)$. It is clear that this association is injective. Indeed, if (X, Y) is another pair of such elements so that $XY = xy$, then $f := Xx^{-1} = Y^{-1}y$, and therefore the order of f divides both the order of Xx^{-1} (which divides m) as well as the order of $Y^{-1}y$ (which divides n); hence, $f = 1$. Thus, $X = x$ and $Y = y$. To see that this association is also surjective, let z be any element whose exponent is mn, construct two integers u and v such that $um + vn = 1$ (which is possible because m and n are coprime), set $x := z^{vn}$ and $y := z^{um}$ and notice that $z = z^1 = z^{um+vn} = xy$. Moreover, since $z^{mn} = 1$, it follows that $x^m = (z^{vn})^m = z^{vmn} = 1$ and $y^n = (z^{um})^n = z^{umn} = 1$, which shows that x and y have exponents m and n respectively. So, this association is surjective as well, and therefore we deduce that $b_G(mn) = b_G(m)b_G(n)$; hence, b_G is multiplicative. ∎

LEMMA 2. *For every prime number $p \mid \#G$ let G_p be the p-Sylow subgroup of G. Then $b_G(p^\alpha) = b_{G_p}(p^\alpha)$ and $a_G(p^\alpha) = a_{G_p}(p^\alpha)$ for all $\alpha \geq 0$, and*

$$u(G) = \prod_{p|\#G} u(G_p).$$

Proof. It is clear that $b_G(1) = a_G(1) = 1$ for all groups G, so we may consider only the case $\alpha \geq 1$. If $p \mid \#G$ and x is an element counted by either $b_G(p^\alpha)$ or $a_G(p^\alpha)$, then $x^{p^\alpha} = 1$, therefore $x \in G_p$. Conversely, every element of exponent (or order) p^α in G_p can be regarded as an element of the same exponent (or order) in G. This shows that both $b_G(p^\alpha) = b_{G_p}(p^\alpha)$ and $a_G(p^\alpha) = a_{G_p}(p^\alpha)$. We now assume that $p_1 < \ldots < p_t$ are all the distinct primes dividing $\#G$. Since a_G is multiplicative, and $a_G(n)=0$ if there is no element of order n in G, we have

$$\begin{aligned}u(G)&=\frac{1}{\#G}\sum_{d\mid\#G}da_G(d)=\frac{1}{\#G}\sum_{\beta_1\ge0,\dots,\beta_t\ge0}\Big(\prod_{i=1}^{t}p^{\beta_i}\Big)a_G\Big(\prod_{i=1}^{t}p^{\beta_i}\Big)\\&=\frac{1}{\#G}\sum_{\beta_1\ge0,\dots,\beta_t\ge0}\prod_{i=1}^{t}p_i^{\beta_i}a_{G_{p_i}}(p^{\beta_i})=\prod_{i=1}^{t}\bigg(\frac{1}{\#G_{p_i}}\sum_{\beta_i\ge0}p^{\beta_i}a_{G_{p_i}}(p^{\beta_i})\bigg)\\&=\prod_{p\mid\#G}u(G_p),\end{aligned}$$

which concludes the proof. ■

Lemma 2 reduces the problem of understanding $u(G)$ for an arbitrary finite abelian group to a finite abelian p-group. From now on we write G_p for a finite abelian p-group. We also write

$$G_p:=\mathbb{Z}_{p^{\alpha_1}}\times\ldots\times\mathbb{Z}_{p^{\alpha_t}},\tag{2}$$

where $1\le\alpha_1\le\ldots\le\alpha_t$. This representation is not unique, but the numbers t and $\alpha_1,\dots,\alpha_t$ are uniquely determined by G_p. We think of $x\in G_p$ as a vector $x:=(x_1,\dots,x_t)$ where $x_i\in\mathbb{Z}_{p^{\alpha_i}}$. It is clear that the order of x is the maximum of the orders of all x_i in the cyclic groups $\mathbb{Z}_{p^{\alpha_i}}$. Moreover, $\lambda(G_p)=p^{\alpha_t}$ and $\#G=p^{\alpha}$, where $\alpha:=\sum_{i=1}^{t}\alpha_i$.

Lemma 3. *With the previous notations we have*

$$u(G_p)=\lambda(G_p)\bigg(1-\frac{p-1}{\lambda(G_p)\#G_p}\sum_{\beta=0}^{\alpha_t-1}p^{\beta}\prod_{i=1}^{t}p^{\min\{\beta,\alpha_i\}}\bigg).$$

Proof. Clearly, $a_{G_p}(1)=b_{G_p}(1)=1$ and

$$a_{G_p}(p^{\beta})=b_{G_p}(p^{\beta})-b_{G_p}(p^{\beta-1}),\qquad\beta=1,\dots,\alpha_t.$$

Thus,

$$\begin{aligned}u(G_p)&=\frac{1}{\#G_p}\sum_{d\mid\lambda(G_p)}da_{G_p}(d)=\frac{1}{\#G_p}\sum_{\beta=0}^{\alpha_t}p^{\beta}a_{G_p}(p^{\beta})\\&=\frac{1}{\#G_p}\Big(1+\sum_{\beta=1}^{\alpha_t}p^{\beta}(b_{G_p}(p^{\beta})-b_{G_p}(p^{\beta-1}))\Big)\\&=\frac{1}{\#G_p}\Big(\lambda(G_p)\#G_p-(p-1)\sum_{\beta=0}^{\alpha_t-1}p^{\beta}b_{G_p}(p^{\beta})\Big)\\&=\lambda(G_p)\bigg(1-\frac{p-1}{\lambda(G_p)\#G_p}\sum_{\beta=0}^{\alpha_t-1}p^{\beta}b_{G_p}(p^{\beta})\bigg).\end{aligned}$$

It remains to compute $b_{G_p}(p^\beta)$ for $0 \le \beta < \alpha_t$. Fix such a β and look at $x = (x_1, \dots, x_t)$ such that $x^{p^\beta} = 1$. Clearly, if $\alpha_i \le \beta$, then x_i can be any element in $\mathbb{Z}_{p^{\alpha_i}}$, while if $\alpha_i > \beta$, then $x_i \in p^{\alpha_i - \beta}\mathbb{Z}_{p^{\alpha_i}}$ and for such i there are only p^β possibilities for x_i. This shows that

$$b_{G_p}(p^\beta) = \prod_{i=1}^{t} p^{\min\{\beta, \alpha_i\}},$$

and we have concluded the proof. ■

Let us see how Lemma 3 compares with the formula from [8] which gives the average order of elements in a cyclic group $\mathbb{Z}_n$. Write $n = \prod_{p|n} p^\alpha$; if $G := \mathbb{Z}_n$, then $G_p := \mathbb{Z}_{p^\alpha}$ for all primes $p \mid n$. In this case, G_p is cyclic, so $t = 1$, $\#G_p = \lambda(G_p) = p^\alpha$, and Lemma 3 asserts that

$$\begin{aligned} u(G_p) &= p^\alpha \biggl(1 - \frac{p-1}{p^{2\alpha}} \sum_{\beta=0}^{\alpha-1} p^{2\beta}\biggr) \\ &= p^\alpha \biggl(1 - \frac{(p-1)(p^{2\alpha}-1)}{p^{2\alpha}(p-1)}\biggr) = p^\alpha \biggl(1 - \frac{p^{2\alpha}-1}{(p+1)p^{2\alpha}}\biggr). \end{aligned}$$

The last expression can be rewritten as

$$u(G_p) = \frac{p^{\alpha+1}}{p+1} + \frac{1}{p^\alpha(p+1)}$$

and in this form it appears as Lemma 1 in [8].

Lemma 3 could be a convenient tool for studying various questions about the behaviour of $u(G)$. For example, let G be a finite abelian group. Then $\lambda(G)$ represents the size of the largest cyclic subgroup of G. One can ask how $u(G)$ compares to $u(\mathbb{Z}_{\lambda(G)})$. Or fix n and let G run over all the finite abelian groups of order n. Clearly, the cyclic group is the unique one realizing the maximum of $\lambda(G)$ (which is $\lambda(G) = n$), but one can ask about the maximum of $u(G)$ when G runs over these subgroups. The next statement answers some of these questions.

Let E_n be the elementary abelian group of order $n \ge 1$. That is, if $n = p_1^{\gamma_1} \dots p_s^{\gamma_s}$, then $E_n = \mathbb{Z}_{p_1}^{\gamma_1} \times \dots \times \mathbb{Z}_{p_s}^{\gamma_s}$. Equivalently, E_n is the unique abelian group G of order n having $\lambda(G) = \mathrm{rad}(n)$.

Theorem 1. (i) *$u(G) \ge u(\mathbb{Z}_{\lambda(G)})$ for all finite abelian groups G, with equality if and only if G is cyclic.*

(ii) *$u(\mathbb{Z}_n) \ge u(G)$ for every abelian group G of order n, with equality if and only if G is cyclic.*

(iii)
$$\frac{u(E_n)}{\lambda(E_n)} \ge \frac{u(G)}{\lambda(G)} \ge \frac{u(\mathbb{Z}_n)}{\lambda(\mathbb{Z}_n)}$$

for all abelian groups G of order n, with equality on the left or on the right if and only if G coincides with the corresponding group.

Proof. Both u and λ are multiplicative at the level of Sylow subgroups, meaning that

$$u(G) = \prod_{p \mid \# G} u(G_p) \quad \text{and} \quad \lambda(G) = \prod_{p \mid \# G} \lambda(G_p).$$

Thus, with the Chinese Remainder Theorem to deal with the cases of equalities, it suffices to prove the theorem for p-groups. So, from now on we work with a p-group G_p given by (2).

(i) From Lemma 3 we obtain

$$\begin{aligned} u(G_p) &= \lambda(G_p)\left(1 - \frac{p-1}{\lambda(G_p)\# G_p} \sum_{\beta=0}^{\alpha_t - 1} p^{\beta} \prod_{i=1}^{t} p^{\min\{\beta, \alpha_i\}}\right) \\ &= \lambda(G_p)\left(1 - \frac{p-1}{p^2} \sum_{\beta=0}^{\alpha_t - 1} \frac{1}{p^{2(\alpha_t - 1 - \beta)}} \prod_{i=1}^{t-1} \frac{1}{p^{\alpha_i - \min\{\beta, \alpha_i\}}}\right). \end{aligned}$$

Clearly,

$$\prod_{i=1}^{t-1} \frac{1}{p^{\alpha_i - \min\{\beta, \alpha_i\}}} \le 1$$

for all $\beta \le \alpha_t - 1$, and if $t > 1$ then this inequality is strict for at least one β (for example, for $\beta = 0$). This shows that

$$\begin{aligned} u(G_p) &\ge \lambda(G_p)\left(1 - \frac{p-1}{p^2} \sum_{\beta=0}^{\alpha_t - 1} \frac{1}{p^{2(\alpha_t - 1 - \beta)}}\right) \\ &= \lambda(G_p)\left(1 - \frac{p^{2\alpha_t} - 1}{(p+1)p^{2\alpha_t}}\right) = u(\mathbb{Z}_{\lambda(G_p)}), \end{aligned}$$

and the above inequality is strict unless $t = 1$, that is, unless G_p is cyclic.

(ii) Assume that $p^{\gamma} \parallel n$ and let G_p be the p-group given by (2) of order p^{α} and let $\lambda(G_p) = p^{\alpha_t}$. Clearly, $\alpha_t < \gamma$ is equivalent to $t \ge 2$. We may also assume that $\gamma > 1$, otherwise G_p is cyclic anyway. By (i), we have

$$p^{\alpha_t} = \lambda(G_p) > u(G_p) \ge u(\mathbb{Z}_{p^{\alpha_t}}) = \frac{p^{\alpha_t + 1}}{p+1} + \frac{1}{p^{\alpha_t}(p+1)}.$$

Since

$$\frac{p^{k+1}}{p+1} + \frac{1}{p^k(p+1)} > p^{k-1}$$

for all primes p and for any positive integer k, it follows that if $\alpha_t < \gamma$, then choosing $\widetilde{G}_p$ to be any p-group of order p^{γ} and exponent $\lambda(\widetilde{G}_p) = p^{\alpha_t + 1}$, we have

$$u(\widetilde{G}_p) \geq \frac{p^{\alpha_t+2}}{p+1} + \frac{1}{p^{\alpha_t+1}(p+1)} > p^{\alpha_t} = \lambda(G_p) > u(G_p),$$

so G_p cannot realize the maximum of u among all the p-groups of order p^γ. This shows that $u(\mathbb{Z}_{p^\gamma}) \geq u(G_p)$, with equality if and only if G_p is cyclic.

(iii) By (i), we have

$$\frac{u(G)}{\lambda(G)} \geq \frac{u(\mathbb{Z}_{\lambda(G)})}{\lambda(G)}$$

and reducing the problem again to $G = G_p$ where G_p is given by (2) we have

$$\frac{u(G_p)}{\lambda(G_p)} \geq \frac{u_{\mathbb{Z}_{p^{\alpha_t}}}}{p^{\alpha_t}} = 1 - \frac{p^{2\alpha_t} - 1}{p^{2\alpha_t}(p+1)} \geq 1 - \frac{p^{2\gamma} - 1}{p^{2\gamma}(p+1)} = \frac{u(\mathbb{Z}_{p^\gamma})}{\lambda(\mathbb{Z}_{p^\gamma})}.$$

Finally, suppose again that $G = G_p$ is the p-group (2) and let τ denote the number of integers α_i such that $\alpha_i = \alpha_t$. That is, $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_{t-\tau} < \alpha_{t-\tau+1} = \alpha_{t-\tau+2} = \ldots = \alpha_t$. Lemma 3 shows that

$$\frac{u(G_p)}{\lambda(G_p)} \leq 1 - \frac{p-1}{p^{\tau+1}},$$

with equality if and only if $\tau = t$ and $\alpha_t = 1$. Since clearly,

$$\frac{u(E_{p^\gamma})}{\lambda(E_{p^\gamma})} = 1 - \frac{p-1}{p^{\gamma+1}} \geq 1 - \frac{p-1}{p^{\tau+1}}$$

the left inequality asserted at (iii) follows. ■

We now denote by $\gamma(G)$ the number of elements of maximal order $\lambda(G)$ in G. In [8], together with the function $\alpha(n)$, which gives the average value of additive orders of elements modulo n, the function $\alpha(n)/\varphi(n)$ has also been investigated. To understand this function in a more general context, let us look at the ratios $\alpha(n)/n$ and $\varphi(n)/n$. The first measures how far away the average value of additive orders of elements modulo n is from the maximal order n, while the second represents the proportion of all elements of maximal additive order modulo n to all the elements in the group. For arbitrary groups, the natural analogues of $\alpha(n)/n$ and $\varphi(n)/n$ are $u(G)/\lambda(G)$ and $\gamma(G)/\#G$, respectively. Thus, the analogue of the function $\beta(n) = \alpha(n)/\varphi(n)$ seems to be

$$v(G) = \frac{u(G)\#G}{\lambda(G)\gamma(G)}.$$

In what follows the following constant plays an important role:

$$A := \frac{\zeta(2)\zeta(3)}{\zeta(6)} = \frac{315\zeta(3)}{2\pi^4} \cong 1.94359\ldots \tag{3}$$

Here, we prove an analogue of Theorem 1 from [8] for the general setting:

Theorem 2. *Let A be given by* (3).

(i) $\liminf_{\#G\to\infty} v(G) = 1$.
(ii) $\limsup_{\#G\to\infty} v(G) = A$.
(iii) $1 < v(G) < A$ *for any group G with* $\#G > 1$.

Proof. To establish the minimal and maximal orders, we need some analytic arguments. Clearly $\gamma(G) = a_G(\lambda(G))$ is also multiplicative at the level of Sylow subgroups, that is, $\gamma(G) = \prod_{p\|\#G}\gamma(G_p)$, and so it is again enough to study $\gamma(G_p)$, where G_p is the p-group (2). It is known that if we denote again by τ the number of integers α_i such that $\alpha_i = \alpha_t$, then

$$\frac{\gamma(G_p)}{\#G_p} = 1 - \frac{1}{p^\tau}. \tag{4}$$

This formula appears, for example, in [3, 11, 15]. From Lemma 3 and (4), we get

$$v(G_p) = \frac{u(G_p)\#G_p}{\lambda(G_p)\gamma(G_p)} = \left(1-\frac{1}{p^\tau}\right)^{-1}\left(1-\frac{p-1}{\lambda(G_p)\#G_p}\sum_{\beta=0}^{\alpha_t-1}p^\beta\prod_{i=1}^{t}p^{\min\{\beta,\alpha_i\}}\right).$$

To see that $v(G)$ can tend to 1 choose a large number τ and consider the group $G := G_p = E_{p^\tau} = \mathbb{Z}_p^\tau$. Then

$$v(G) = \left(1-\frac{1}{p^\tau}\right)^{-1}\left(1-\frac{p-1}{p^{\tau+1}}\right),$$

and letting τ tend to infinity (and keeping p fixed), we obtain (i). We point out that the fact that the lower limit in (i) is exactly 1 (once we know that it is at least 1) follows also from Theorem 1 of [8] where it is shown that the limit value 1 can be achieved for cyclic groups. We also notice that

$$v(G_p) \le \left(1-\frac{1}{p^\tau}\right)^{-1}\left(1-\frac{p-1}{p^{\tau+1}}\right). \tag{5}$$

Indeed, (5) follows from Lemma 3 by noticing that

$$\begin{aligned}\frac{u(G_p)}{\lambda(G_p)} &\le 1-\frac{p-1}{\lambda(G_p)\#G_p}\cdot p^{\alpha_t-1}\cdot\prod_{i=1}^{t}p^{\min\{\alpha_t-1,\alpha_i\}}\\ &= 1-\frac{(p-1)p^{(\alpha_t-1)+\tau(\alpha_t-1)+\sum_{\alpha_i<\alpha_t}\alpha_i}}{p^{\alpha_t+\tau\alpha_t+\sum_{\alpha_i<\alpha_t}\alpha_i}} = 1-\frac{p-1}{p^{\tau+1}}.\end{aligned}$$

Moreover, from what we have previously said, the equality in (5) occurs for the elementary abelian group G with p^τ elements. It is easily checked that for any fixed $p \ge 2$, the right hand side of (5) is decreasing as a function of τ, and therefore

$$v(G_p) \le \left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{p-1}{p^2}\right),$$

with equality, of course, for the cyclic group of order p. Thus,

$$\begin{aligned} v(G) &\le \prod_{p\mid \#G}\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{p-1}{p^2}\right)\\ &= \prod_{p\mid \#G}\left(1-\frac{1}{p^2}\right)^{-1}\left(1-\frac{1}{p^3}\right)^{-1}\left(1-\frac{1}{p^6}\right). \end{aligned}$$

In particular,

$$v(G) < \prod_{p\ge 2}\left(1-\frac{1}{p^2}\right)^{-1}\left(1-\frac{1}{p^3}\right)^{-1}\left(1-\frac{1}{p^6}\right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)},$$

and the limit in (ii) can be achieved by setting $G := G(r) = \times_{p<r}\mathbb{Z}_p$ and letting r tend to infinity.

The fact that $v(G) > 1$ if $\#G > 1$ is trivial to see from

$$\sum_{d\mid \lambda(G)} d a_G(d) > \lambda(G) a_G(\lambda(G)) = \lambda(G)\gamma(G),$$

therefore

$$u(G) > \frac{\lambda(G)\gamma(G)}{\#G},$$

which is equivalent to $v(G) > 1$. Because the identity element is never of maximal order in G if G is non-trivial, we have $v(G) < A$ and thus (iii) is established. ∎

3. Multiplicative orders of elements of $\mathbb{Z}_n$. Here, we apply our previous results to the function giving the average order of all invertible elements modulo n. For any n, we write $\lambda(n)$ for the Carmichael function of n, and $u(n)$ for the average multiplicative order of elements in $G := U(\mathbb{Z}_n)$. To keep with the notation from [8], we also write $\alpha(n)$ for the average additive order of elements modulo n. From Theorem 1 we immediately derive

THEOREM 3. *For any positive integer n we have*

$$\alpha(\lambda(n)) \le u(n) \le \lambda(n).$$

Because of Theorem 3, it makes sense to look at $u(n)/\lambda(n)$ and to ask about the properties of this function. In the next statement, we find the minimal and maximal order of this function, as well as its range. We remark that Theorem 7(iii) below implies that $u(n)/\lambda(n)$ does not have a distribution function.

THEOREM 4.

(i) $$\liminf_{n\to\infty}\frac{u(n)\log_2 n}{\lambda(n)} = \frac{e^{-\gamma}\pi^2}{6} \quad \textit{and} \quad \limsup_{n\to\infty}\frac{u(n)}{\lambda(n)} = 1.$$

(ii) *The sequence $u(n)/\lambda(n)$ is dense in* $[0,1]$.

Proof. (i) By Theorem 3 and the formula for α, which can be recovered from Lemma 3 and from the fact that $\alpha(n) = u(\mathbb{Z}_n)$, we have

$$\begin{aligned}\frac{u(n)\log_2 n}{\lambda(n)} &\geq \frac{\alpha(\lambda(n))\log_2 \lambda(n)}{\lambda(n)}\\ &= \log_2 \lambda(n) \prod_{p^{\beta_p}\|\lambda(n)} \left(\frac{p}{p+1} + \frac{1}{p^{2\beta_p}(p+1)}\right)\\ &\geq \log_2(\mathrm{rad}(\lambda(n))) \prod_{p|\lambda(n)} \left(\frac{p}{p+1}\right).\end{aligned}$$

This shows that

$$\liminf_{n\to\infty} \frac{u(n)\log_2 n}{\lambda(n)} \geq \liminf_{\substack{n\to\infty\\ |\mu(n)|=1}} \frac{n\log_2 n}{\sigma(n)} = \frac{e^{-\gamma}\pi^2}{6},$$

where the last limit follows easily from

$$\prod_{p\leq z}\left(1-\frac{1}{p^2}\right) \to \zeta(2)^{-1} = \frac{6}{\pi^2} \quad \text{as } z\to\infty$$

and the Mertens formula

$$\prod_{p\leq z}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log z} + O(\log^{-2} z).$$

To see that this is in fact an equality, for sufficiently large x define $t := \lfloor 2\log x\rfloor + 1$, set

$$R_x := \prod_{p<x} p \quad \text{and} \quad Q_x := (R_x)^t,$$

and choose P_x to be the first prime in the arithmetic progression $1 \pmod{Q_x}$. By Linnik's theorem, $P_x = O(Q_x^{11/2})$ and clearly $P_x > Q_x$. Thus $\log_2 P_x = \log_2 Q_x + O(1)$. We also have

$$\log_2 Q_x = \log(t\log(R_x)) = \log t + \log_2 R_x = \log x + o(\log x)$$

because $\log R_x = x + o(x)$. Therefore

$$\frac{\log_2 P_x}{\log x} = 1 + o(1). \tag{6}$$

We shall show that

$$\frac{u(P_x)\log_2 P_x}{\lambda(P_x)} \to \frac{e^{-\gamma}\pi^2}{6} \quad \text{as } x\to\infty.$$

Since $U(\mathbb{Z}_{P_x}) = \mathbb{Z}_{P_x-1}$ is cyclic, it follows that $u(P_x) = \alpha(P_x-1)$ and

$\lambda(P_x) = P_x - 1$, and using (6) we conclude that it suffices to show that

$$\lim_{x\to\infty} \frac{\alpha(P_x-1)\log x}{P_x-1} = \frac{e^{-\gamma}\pi^2}{6}.$$

Now

$$\frac{\alpha(P_x-1)}{P_x-1} = \prod_{p^\beta \| P_x-1} \left(\frac{p}{p+1} + \frac{1}{p^{2\beta}(p+1)}\right) = VW, \tag{7}$$

where

$$\begin{aligned} V &:= \prod_{\substack{p^\beta \| P_x-1 \\ p<x}} \left(\frac{p}{p+1} + \frac{1}{p^{2\beta}(p+1)}\right) = \prod_{p<x} \left(\frac{p}{p+1} + \frac{1}{p^{2\beta}(p+1)}\right), \\ W &:= \prod_{\substack{p^\beta \| P_x-1 \\ p\ge x}} \left(\frac{p}{p+1} + \frac{1}{p^{2\beta}(p+1)}\right). \end{aligned}$$

We have

$$\begin{aligned} V &= \prod_{p<x} \left(\frac{p}{p+1}\right)(1+O(p^{-2t-1})) = \prod_{p<x} \left(\frac{p}{p+1}\right)(1+O(2^{-2t})) \\ &= \exp(O(\pi(x)2^{-2t})) \prod_{p<x} \frac{p}{p+1} = (1+o(1)) \prod_{p<x} \frac{p}{p+1}. \end{aligned}$$

On the other hand,

$$\begin{aligned} W &= \prod_{\substack{p^\beta \| P_x-1 \\ p\ge x}} \left(\frac{p}{p+1}\right)(1+O(p^{-3})) \\ &= \exp\Big(O\Big(\sum_{p\ge x} p^{-3}\Big)\Big) \prod_{\substack{p^\beta \| P_x-1 \\ p\ge x}} \frac{p}{p+1} = (1+o(1)) \prod_{\substack{p^\beta \| P_x-1 \\ p\ge x}} \frac{p}{p+1}. \end{aligned}$$

Since $P_x - 1 < P_x = O(Q_x^{11/5}) < \exp(O(xt))$, it follows that

$$\omega(P_x) \ll \frac{\log P_x}{\log_2 P_x} \ll \frac{xt}{\log x} \ll x.$$

In particular, from the prime number theorem, we derive that for some constant $C > 0$ we have

$$\begin{aligned} \sum_{\substack{p \mid P_x-1 \\ p>x}} \frac{1}{p} &< \sum_{x<p<Cx\log x} \frac{1}{p} = \log_2(Cx\log x) - \log_2 x + o(1) \\ &= \log(\log x + \log(C\log^2 x)) - \log(\log x) + o(1) = o(1). \end{aligned}$$

Therefore

$$\prod_{\substack{p \mid P_x - 1\\ p > x}} \frac{p}{p+1} = 1 + o(1),$$

and we see that $W = 1 + o(1)$. Putting everything into (7) we get

$$\frac{\alpha(P_x - 1)}{P_x - 1} = (1 + o(1)) \prod_{p<x} \frac{p}{p+1}.$$

Thus,

$$\begin{aligned} \lim_{x\to\infty} \frac{\alpha(P_x - 1)\log_2 P_x}{P_x - 1} &= \lim_{x\to\infty} \frac{\alpha(P_x - 1)\log x}{P_x - 1} = \lim_{x\to\infty} \log x \prod_{p<x} \frac{p}{p+1} \\ &= \lim_{x\to\infty} \log x \prod_{p<x} \left(1 - \frac{1}{p}\right) \prod_{p<x} \left(1 - \frac{1}{p^2}\right)^{-1} \\ &= e^{-\gamma}\zeta(2) = e^{-\gamma}\pi^2/6. \end{aligned}$$

Notice that $u(n)/\lambda(n) \le 1$, and so the right limit in (i) can be at most 1 and (ii) would imply that it is exactly 1.

(ii) Here we use the well known (and easy to prove) fact that for every $\delta \in [0,1]$ there exists a sequence $(m_k)_k$ of odd square-free numbers with $\omega(m_k) \to \infty$ such that

$$\lim_{k\to\infty} \frac{m_k}{\sigma(m_i)} = \lim_{k\to\infty} \prod_{p \mid m_k} \frac{p}{p+1} = \delta \tag{8}$$

(see [16] for a quantitative form of this statement). We fix δ, select an odd square-free number $m = p_1 \ldots p_t$ belonging to the sequence $(m_k)_k$, and let s be a large integer.

For each $i = 1, \ldots, t$ we apply Chen's theorem for $k := k_i = 2p_i^s$ to find a number $x_0(p_i^s)$ so that for $x > x_0(p_i^s)$ the interval $[x, 2x]$ contains a prime q_i so that $q_i - 1 = 2p_i^s l_i$, where l_i is divisible by at most two primes, each larger than $x^{1/4}$. Set $x_0(s) := \max\{x_0(p_i^s),\ i = 1, \ldots, t\}$ and assume that x is so large that $x > p_i^4$ for all $i = 1, \ldots, t$. So, all the primes q_i are in $[x, 2x]$, and they are also distinct. Construct the number

$$n := \prod_{i=1}^{t} q_i.$$

For the group $G(n) := U(\mathbb{Z}_n)$ we certainly have

$$\begin{aligned} G(n) = U(\mathbb{Z}_n) &= \mathbb{Z}_{q_1 - 1} \times \ldots \times \mathbb{Z}_{q_t - 1} \\ &= (\mathbb{Z}_2 \times \mathbb{Z}_{p_1^s} \times \mathbb{Z}_{l_1}) \times \ldots \times (\mathbb{Z}_2 \times \mathbb{Z}_{p_t^s} \times \mathbb{Z}_{l_t}). \end{aligned}$$

We also notice that:

- $G_2(n) = \mathbb{Z}_2^t$.
- $G_{p_i}(n) = \mathbb{Z}_{p_i^s}$ for $i = 1, \ldots, t$.
- Except for the primes 2 and p_i for $i = 1, \ldots, t$, all the other primes that divide $\#G$ exceed $x^{1/4}$, and there are at most $2t$ of them.

From the above remarks and Lemma 3 we get

$$\frac{u(G_2(n))}{\lambda(G_2(n))} = 1 - \frac{1}{2^{t+1}}, \qquad \frac{u(G_{p_i}(n))}{\lambda(G_{p_i}(n))} = \frac{p_i}{p_i+1} + \frac{1}{p_i^{2s}(p_i+1)},$$

and

$$\frac{u(G_q(n))}{\lambda(G_q(n))} = 1 + O\biggl(\frac{1}{x^{1/4}}\biggr) \qquad \text{for } q \neq 2, p_i \text{ with } i = 1, \ldots, t.$$

So,

$$\begin{aligned}\frac{u(n)}{\lambda(n)} &= \prod_{p \mid \lambda(G(n))} \frac{u(G_p(n))}{\lambda(G_p(n))} \\ &= \biggl(1 - \frac{1}{2^{t+1}}\biggr)\biggl(1 + O\biggl(\frac{1}{x^{1/4}}\biggr)\biggr)^{2t} \prod_{i=1}^{t} \biggl(\frac{p_i}{p_i+1} + \frac{1}{p_i^{2s}(p_i+1)}\biggr).\end{aligned}$$

We first keep s and m fixed and let $x \to \infty$ to find that the set of cluster points of $\{u(n)/\lambda(n)\}_n$ contains points of the form

$$\biggl(1 - \frac{1}{2^{t+1}}\biggr) \prod_{i=1}^{t} \biggl(\frac{p_i}{p_i+1} + \frac{1}{p_i^{2s}(p_i+1)}\biggr).$$

Now the limit with respect to $s \to \infty$ shows that the set of cluster points of $\{u(n)/\lambda(n)\}_n$ contains points of the form

$$\biggl(1 - \frac{1}{2^{t+1}}\biggr) \prod_{i=1}^{t} \frac{p_i}{p_i+1}.$$

Finally, we consider the limit for the sequence $(m_k)_k$ of odd square-free numbers with $\omega(m_k) \to \infty$ and such that (8) holds to conclude that δ is indeed a cluster point of $\{u(n)/\lambda(n)\}_n$, which finishes the proof of (ii). ∎

For every n, we now use $v(n)$ to denote $v(U(\mathbb{Z}_n))$.

Theorem 5. *Let A be given by* (3).

(i) $\liminf_{n\to\infty} v(n) = 1$.
(ii) $\limsup_{n\to\infty} v(n) = A$.
(iii) $1 < v(n) < A$ *for any* $n > 1$.

Proof. The proof is based again on Chen's theorem. To see the lower limit, choose a large x and apply Chen's theorem to find at least $T \gg x/\log^2 x$ primes p in $[x, 2x]$ so that $p - 1 = 2l$, where l is divisible by at most two primes, each exceeding $x^{1/4}$. In particular, taking $t := \lfloor \log x \rfloor \le T$, we find $p_1 < \ldots < p_t$ such primes. Take $n := p_1 \ldots p_t$ and look at $G := U(\mathbb{Z}_n)$. It is clear that $G_2 = \mathbb{Z}_2^t$, all the odd primes dividing $\#G$ exceed $x^{1/4}$, and there are at most $2t$ of them. We now get

$$v(G) = v(G_2) \prod_{\substack{p \mid \lambda(n) \\ p>2}} v(G_p) = \left(1 - \frac{1}{2^t}\right)^{-1} \left(1 - \frac{1}{2^{t+1}}\right) \left(1 + O\left(\frac{1}{x^{1/4}}\right)\right)^{2t}$$

$$= \left(1 - \frac{1}{2^t}\right)^{-1} \left(1 - \frac{1}{2^{t+1}}\right) \exp\left(O\left(\frac{\log x}{x^{1/4}}\right)\right).$$

Letting $x \to \infty$ we get (i). For the upper limit, we let $x > 0$ be large, we write $Q_x := \prod_{p<x} p$, and we use Linnik's theorem to construct a prime P_x congruent to $Q_x + 1$ modulo Q_x^2, and which is $O(Q_x^{11})$. It is then immediately checked (by more or less the same arguments) that

$$v(P_x) = \frac{\alpha(P_x - 1)}{\varphi(P_x - 1)}$$

tends to A as $x \to \infty$, and the result follows. ∎

Notice that while Theorem 5 might seem to follow from Theorem 2, in the latter the limits are taken over all possible groups. In fact, Theorem 5 says that they are achieved if we consider only those groups G which can be the multiplicative groups modulo n for some n.

Using Theorems 4 and 5, we can reformulate most of the questions regarding the behaviour of $u(n)$ in terms of the behaviour of $\lambda(n)$, and the behaviour of $u(n)/\lambda(n)$ in terms of the behaviour of $r(n) := \gamma(n)/\varphi(n)$, the ratio of the number of multiplicative elements of maximal order modulo n to the number of invertible elements modulo n. In particular, from Theorem 4 we see that Theorems 1, 2 and 3 of [6] hold for $u(n)$ in place of $\lambda(n)$. More precisely, we obtain the following result.

Theorem 6. (i) *For any large real number x,*

$$u(n) \ge x/(\log x)^{\log_3 x + a + o(1)}$$

for all positive integers $n < x$ except maybe for $o(x)$ of them, where

$$a := -1 + \sum_{p\, prime} \frac{\log p}{(p-1)^2} = 0.2269\ldots$$

(ii) *For any $\varepsilon > 0$,*

$$u(n) > (\log n)^{(1/2-\varepsilon)\log_3 n}$$

for all sufficiently large n. However, there exists a constant c such that

$$u(n) < (\log n)^{c \log_3 n}$$

for infinitely many n.

(iii) *For any large real number x,*

$$\frac{1}{x}\sum_{n\le x} u(n) = \frac{x}{\log x}\exp\left(b\,\frac{\log_2 x}{\log_3 x}\,(1+o(1))\right),$$

where

$$b := e^{-\gamma}\prod_{p\,prime}\left(1-\frac{1}{(p-1)^2(p+1)}\right) = 0.3453\ldots$$

One can also replace $\lambda(n)$ with $u(n)$ in Theorem 5 of [7].

Similarly, Theorem 5 can be combined with some results of [11].

Theorem 7. (i) *For any large positive number x,*

$$\frac{u(n)}{\lambda(n)} \gg \frac{1}{\log_3 x}$$

for all positive integers $n < x$ except for $o(x)$ of them.

(ii) *There exists a constant $b > 0$ so that*

$$\liminf_{x\to\infty}\frac{1}{x}\,\#\left\{n\le x \;\middle|\; \frac{u(n)}{\lambda(n)} > \log_5^{-b} x\right\} = 0.$$

(iii) *For all real numbers w and x put*

$$\Delta(x,w) := \frac{1}{x}\,\#\left\{n\le x \;\middle|\; \frac{u(n)}{\lambda(n)} \le w\right\}.$$

Then there exists $w_0 > 0$ such that $\lim_{x\to\infty}\Delta(x,w)$ *does not exist for all* $0 < w < w_0$.

Proof. (i) Since $u(n)/\lambda(n) \gg r(n)$, it suffices to show that $r(n) \gg 1/\log_3 x$ for all $n < x$ with at most $o(x)$ exceptions. This has almost been done in [12] where it is shown that there is a positive constant x_0 such that

$$\sum_{n\le x} r(n) \gg \frac{x}{\log_3 x}$$

for $x > x_0$ (this follows by combining Lemma 2.1 with Theorem 2.3 from [12]). Here, we slightly improve on the above result from [12]. Let x be a large real number and let c be a small constant to be chosen later. Let $S(x)$ be the set of those $n < x$ such that the following two conditions are satisfied:

(1) $\lambda(n)$ is divisible by all primes $p \le g(x)$, where $g(x) := c\log_2 x/\log_3 x$ for some constant $c > 0$;

(2)
$$\sum_{\substack{p>g(x)\\ p\mid\lambda(n)}}\frac{1}{p} < \frac{\log_4 x}{\log_3 x}.$$

In [14], it is shown that for appropriate c the set $S(x)$ contains all positive integers $n < x$ except for $o(x)$ of them (see Lemmas 2 and 3 in [14]). Now if n is in $S(x)$, then

$$r(n) \ge \frac{\varphi(\lambda(n))}{\lambda(n)} = \prod_{p\mid\lambda(n)} \left(1-\frac{1}{p}\right) = VW,$$

where

$$V := \prod_{\substack{p\le g(x)\\ p\mid\lambda(n)}} \left(1-\frac{1}{p}\right) \quad\text{and}\quad W := \prod_{\substack{p> g(x)\\ p\mid\lambda(n)}} \left(1-\frac{1}{p}\right).$$

Clearly,

$$\begin{aligned} V &\gg \exp\Bigl(-\sum_{p<g(x)}\frac{1}{p}\Bigr) = \exp(-\log_2(g(x)) + O(1)) \\ &= \exp(-\log_4 x + O(1)) \gg \frac{1}{\log_3 x}, \end{aligned}$$

while

$$W \gg \exp\Bigl(-\sum_{\substack{p>g(x)\\ p\mid\lambda(n)}}\frac{1}{p}\Bigr) > \exp\Bigl(-\frac{\log_4 x}{\log_3 x}\Bigr) = 1 + o(1),$$

and we have therefore shown that $r(n) \gg 1/\log_3 x$ whenever $n \in S(x)$.

(ii) Theorem 1.2 of [12] says that there exists a constant $b_0 > 0$ so that

$$\liminf_{x\to\infty} \frac{1}{x}\,\#\{n \le x \mid r(n) > \log_5^{-b_0} x\} = 0,$$

so Theorem 5 now shows that

$$\liminf_{x\to\infty} \frac{1}{x}\,\#\Bigl\{n \le x \Bigm| \frac{u(n)}{\lambda(n)} > \frac{1}{A}\log_5^{-b_0} x\Bigr\} = 0,$$

which implies that (ii) holds with any constant $b < b_0$.

(iii) From Theorem 5 and Corollary 5.2 of [11] we derive that for infinitely many x,

$$\Delta(x,w) \ll \frac{1}{|\log(w)|} \quad \text{for } 0 \le w \le 1/2.$$

Comparing this with (ii), as in [11], we derive the desired statement. ■

4. Arithmetic properties of the average order. Given two integer-valued arithmetic functions $f(n)$ and $g(n)$ it is natural to ask for the values of n for which $f(n)/g(n)$ is an integer. For example, the numbers n so that $\sigma(n)/n$ is an integer are called *multiply perfect*, while the composite numbers n for which $(n-1)/\lambda(n)$ is an integer are called *Carmichael numbers*. Since $u(n)$ is always a rational number, it makes sense to ask for the values of n so that $u(n)$ is an integer. Moreover, studying the smallest possible positive denominator Q_n of $u(n)$ is a natural question as well, and we address it in this section. To be more precise, for any finite abelian group G we write $S(G)$

for the sum of the orders of all elements in G, that is, $S(G) := \#G \cdot u(G)$. Accordingly, $S(n) := u(n)\varphi(n)$. In this section, we obtain various estimates on $D_n = \gcd(S(n), \varphi(n))$. In fact, our technique can be applied to the values of $u(G)$ for several other families of groups.

We start with a very simple statement describing all possible integer values of $u(n)$.

THEOREM 8. *For $n \geq 1$, $u(n)$ is integer if and only if $n \leq 2$.*

Proof. Clearly, $u(1) = u(2) = 1$. We also remark that $S(G)$ is always odd. Indeed,

$$S(G) = \prod_{p \mid \#G} S(G_p),$$

and thus it suffices to show that $S(G)$ is odd when $G := G_p$ is a p-group. We assume that G_p is given by formula (2). When $p = 2$,

$$S(G_2) = \sum_{d \mid \#G_2} d a_{G_2}(d) = 1 + \sum_{\beta \geq 1} 2^\beta a_{G_2}(2^\beta)$$

is obviously odd. For $p > 2$, the formula from Lemma 3 shows that

$$S(G_p) = \lambda(G_p)\#G_p - (p-1)\sum_{\beta=0}^{\alpha_t - 1} p^\beta \prod_{i=1}^{t} p^{\min\{\beta,\alpha_i\}},$$

which is obviously odd because $p-1$ is even and $\alpha(G_p)\#G_p = p^{\alpha+\alpha_t}$ is odd. Specializing now to $G := U(\mathbb{Z}_n)$, we conclude that $u(n) = S(U(\mathbb{Z}_n))/\varphi(n)$ cannot be an integer when $n > 2$ because $S(U(\mathbb{Z}_n))$ is odd and $\varphi(n)$ is even. ∎

It is easy to see that the proof of Theorem 8 shows that Q_n is divisible by the full power with which 2 appears in $\varphi(n)$, which immediately implies that $Q_n \gg \log n$ for almost all n. In fact, our next result shows that typically Q_n is much larger than $\log n$. In particular, it implies that for almost all n we have

$$Q_n = \varphi(n)/D_n > n \exp(-(8 + o(1)) \log_2 n \log_3 n \log_4 n).$$

THEOREM 9. *The inequality $D_n < \exp((8 + o(1)) \log_2 n \log_3 n \log_4 n)$ holds on a set of positive integers n of asymptotic density 1.*

Proof. We make use of the bound

$$\sum_{p>y} \frac{1}{p^\eta} \ll \frac{1}{y^{\eta-1}\log y},$$

which holds for any fixed $\eta > 1$ (and which we apply only with $\eta = 2$ and $\eta = 3/2$). Indeed, putting $l_0 = \lfloor \log y \rfloor$ and using the prime number theorem we obtain

$$\sum_{p>y}\frac{1}{p^\eta}\le\sum_{l\ge l_0}\sum_{e^{l+1}>p\ge e^l}\frac{1}{p^\eta}\ll\sum_{l\ge l_0}e^{-l\eta}\sum_{e^{l+1}>p\ge e^l}1\ll\sum_{l\ge l_0}e^{-l\eta}\frac{e^l}{l}$$
$$\ll\sum_{l\ge l_0}\frac{1}{e^{l(\eta-1)}l}\ll\frac{1}{e^{(\eta-1)l_0}l_0}\ll\frac{1}{y^{\eta-1}\log y}.$$

We also use the estimate

$$\sum_{\substack{q\equiv a\,(\mathrm{mod}\,k)\\ k\le q<x}}\frac{1}{q}\ll\frac{\log_2 x}{\varphi(k)}$$

for any integers a and $k\ge 1$, which follows from the Brun–Titchmarsh theorem after simple calculations. When $a=1$ it is the bound (3.1) in [4] (see also Lemma 1 of [2]) in which case the condition $q\ge k$ is redundant, of course. The general case can be proved completely analogously.

It suffices to show that $D_n<\exp((8+o(1))\log_2 n\log_3 n\log_4 n)$ for all $n\in\mathcal{N}$ except for $o(x)$ of them, where $\mathcal{N}$ is the set of integers in the interval $[x^{1/2},x]$.

Let $\mathcal{E}_1$ be the set of integers $n\in\mathcal{N}$ for which there exists $p>\log_2 x$ such that $p^2\mid n$. Obviously,

$$\#\mathcal{E}_1\le\sum_{p>\log_2 x}\frac{x}{p^2}\ll\frac{x}{\log_2 x\log_3 x}=o(x).$$

Therefore, $\#\mathcal{E}_1=o(x)$.

Let $\mathcal{E}_2$ be the set of $n\in\mathcal{N}\backslash\mathcal{E}_1$ for which there exists $p>\log_2^2 x$ such that $p^2\mid\varphi(n)$. If n is such a number, then since p^2 does not divide n, we conclude that either $q\mid n$ for some prime $q\equiv 1\pmod{p^2}$, or there exist two distinct primes q and r such that $qr\mid n$ and $q\equiv 1\pmod p$ and $r\equiv 1\pmod p$. In the first case, the total number of such n's is at most

$$\sum_{p>\log_2^2 x}\sum_{\substack{q\equiv 1\,(\mathrm{mod}\,p^2)\\ q<x}}\frac{x}{q}\ll x\log_2 x\sum_{p>\log_2^2 x}\frac{1}{p^2}\ll\frac{x}{\log_3 x}=o(x).$$

In the second case, the total number of such n's is at most

$$\sum_{p>\log_2^2 x}\sum_{\substack{q\equiv r\equiv 1\,(\mathrm{mod}\,p)\\ q\ne r\\ qr<x}}\frac{x}{qr}\ll x\sum_{p>\log_2^2 x}\Bigg(\sum_{\substack{q\equiv 1\,(\mathrm{mod}\,p)\\ q<x}}\frac{1}{q}\Bigg)^2$$
$$\ll x\log_2^2 x\sum_{p>\log_2^2 x}\frac{1}{p^2}\ll\frac{x}{\log_3 x}=o(x).$$

Therefore, $\#\mathcal{E}_2=o(x)$.

Let $\mathcal{E}_3$ be the set of $n\in\mathcal{N}\setminus(\mathcal{E}_1\cup\mathcal{E}_2)$ for which there exist two primes p and q with $p>\log_2^4 x$, $pq\mid\varphi(n)$ and $p\mid q^2-q+1$. The congruence $a^2-a+1\equiv 0\pmod p$ has either no solution (this happens precisely if -3 is not a quadratic residue modulo p, that is, if $p \equiv 2 \pmod 3$)), or exactly two distinct solutions $p > a_2(p) > a_1(p) \ge p^{1/2} > \log_2^2 x$. So, if q is a prime such that $q^2 - q + 1 \equiv 0 \pmod p$, then either $q = a_1(p)$, or $q = a_2(p)$, or $q > p$ and $q \equiv a_i(p) \pmod p$ for $i = 1$ or 2. Since $pq \mid \varphi(n)$, it follows that either n is a multiple of a prime $r \equiv 1 \pmod{pq}$, or a multiple of two distinct primes r and s with $r \equiv 1 \pmod p$ and $s \equiv 1 \pmod q$ (this is because $n \notin \mathcal{E}_1$, thus neither p^2 nor q^2 can divide n). In the first case, the total number of such numbers is at most

$$\begin{aligned}
&\sum_{p > \log_2^4 x} \sum_{i=1}^{2} \sum_{\substack{q \equiv a_i(p) \pmod p \\ q \le x/p}} \sum_{\substack{r \equiv 1 \pmod{pq} \\ r < x}} \frac{x}{r} \\
&\qquad \ll x \log_2 x \sum_{p > \log_2^4 x} \frac{1}{p} \sum_{i=1}^{2} \sum_{\substack{q \equiv a_i(p) \pmod p \\ q \le x/p}} \frac{1}{q} \\
&\qquad \le x \log_2 x \sum_{p > \log_2^4 x} \frac{1}{p} \left(\frac{1}{a_1(p)} + \frac{1}{a_2(p)} + \sum_{i=1}^{2} \sum_{\substack{q \equiv a_i(p) \pmod p \\ a_i(p) < q < x/p}} \frac{1}{q} \right) \\
&\qquad \ll x \log_2 x \sum_{p > \log_2^4 x} \frac{1}{p} \left(\frac{1}{p^{1/2}} + \frac{\log_2 x}{p} \right) \ll x \log_2 x \sum_{p > \log_2^4 x} \frac{1}{p^{3/2}} \\
&\qquad \ll \frac{x}{\log_2 x \log_3 x} = o(x).
\end{aligned}$$

In the second case, the total number of such n's is at most

$$\begin{aligned}
&\sum_{p > \log_2^4 x} \sum_{i=1}^{2} \sum_{\substack{q \equiv a_i(p) \pmod p \\ q \le x/p}} \sum_{\substack{r \equiv 1 \pmod p \\ s \equiv 1 \pmod q \\ rs < x}} \frac{x}{rs} \\
&\qquad \ll x \sum_{p > \log_2^4 x} \sum_{i=1}^{2} \sum_{\substack{q \equiv a_i(p) \pmod p \\ q \le x/p}} \left(\sum_{\substack{r \equiv 1 \pmod p \\ r < x}} \frac{1}{r} \right) \left(\sum_{\substack{s \equiv 1 \pmod q \\ s < x}} \frac{1}{s} \right) \\
&\qquad \ll x \log_2^2 x \sum_{p > \log_2^4 x} \frac{1}{p} \left(\frac{1}{a_1(p)} + \frac{1}{a_2(p)} + \sum_{i=1}^{2} \sum_{\substack{q \equiv a_i(p) \pmod p \\ a_i(p) < q < x/p}} \frac{1}{q} \right) \\
&\qquad \ll x \log_2^2 x \sum_{p > \log_2^4 x} \frac{1}{p} \left(\frac{1}{p^{1/2}} + \frac{\log_2 x}{p} \right) \ll x \log_2^2 x \sum_{p > \log_2^4 x} \frac{1}{p^{3/2}} \\
&\qquad \ll \frac{x}{\log_3 x} = o(x).
\end{aligned}$$

Therefore, $\#\mathcal{E}_3 = o(x)$.

Finally, for $3 \le y < x$ and an integer $n \ge 2$ write $\Omega_y(n)$ for the number of prime divisors $p \le y$ of n, counted with multiplicity. In the proof of Theorem 3.2 of [5], it is shown that there exist functions

$$\begin{aligned} E_y(x) &:= \log_2 x \log_2 y - \tfrac{1}{2} \log_2^2 y + O(\log_2 x), \\ D_y(x) &:= \log_2 x \log_2^2 y - \tfrac{2}{3} \log_2^3 y + O(\log_2 x \log_2 y), \end{aligned}$$

such that

$$\sum_{n \le x} (\Omega_y(\varphi(n)) - E_y(x))^2 \le 32 x D_y(x)$$

uniformly in $y \le x$. From the above inequality, we infer that uniformly for $y \le x$ the inequality

$$(\Omega_y(\varphi(n)) - E_y(x))^2 \ge \log_2^{1/2} x D_y(x)$$

holds for at most $O(x \log_2^{-1/2} x)$ positive integers $n < x$. Therefore

$$\Omega_y(\varphi(n)) \le (1 + O(\log_2^{-1/4} x)) \log_2 x \log_2 y \tag{9}$$

for all positive integers $n < x$ except at most $O(x \log_2^{-1/2} x)$ of them, uniformly in the range $y \le x$.

Let $\mathcal{E}_4$ be the set of $n \in \mathcal{N} \setminus (\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3)$ for which (9) fails either with $y := \log_2^2 x$ or with $y := \log_2^4 x$. Thus, $\#\mathcal{E}_4 = o(x)$.

We now define the set $\mathcal{M} = \mathcal{N} \setminus (\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \cup \mathcal{E}_4)$ of cardinality $\#\mathcal{M} = x + o(x)$. For $n \in \mathcal{M}$, we have

$$\Phi := \prod_{\substack{p^{\alpha_p} \| \varphi(n) \\ p > \log_2^2 x}} p^{\alpha_p} = \prod_{\substack{p | \varphi(n) \\ p > \log_2^2 x}} p$$

because $n \notin \mathcal{E}_1$.

For every prime $p \,|\, \varphi(n)$ we also write G_p for the p-Sylow subgroup of $U(\mathbb{Z}_n)$. Since $n \notin \mathcal{E}_2$, we obtain

$$U := \prod_{p | \Phi} S(G_p) = \prod_{p | \Phi} (p^2 - p + 1).$$

Since $n \notin \mathcal{E}_3$, we have $\gcd(U, \Psi) = 1$, where

$$\Psi := \prod_{\substack{p^{\alpha_p} \| \varphi(n) \\ p > \log_2^4 x}} p^{\alpha_p}.$$

Therefore,

$$D_n \,\Big|\, \frac{\varphi(n)}{\Psi} \cdot \frac{S(n)}{U}.$$

Thus, $\log D_n \ll \log(\varphi(n)/\Psi) + \log(S(n)/U)$. Clearly,

$$\begin{aligned}\log(\varphi(n)/\Psi) &= \sum_{\substack{p^{\alpha_p}\,\|\varphi(n)\\ p\le \log_2^4 x}} \alpha_p \log p \le 4\log_3 x \sum_{\substack{p^{\alpha_p}\,\|\varphi(n)\\ p\le \log_2^4 x}} \alpha_p\\ &\le 4\Omega_{\log_2^4 x}(\varphi(n))\log_3 x \le 4(1+o(1))\log_2 x \log_3 x \log_4 x\end{aligned}$$

because $n \notin \mathcal{E}_4$.

It is obvious that $S(G) \le \#G^2$ for any group G, therefore,

$$\begin{aligned}\log(S(n)/U) &= \sum_{\substack{p\mid\varphi(n)\\ p\le \log_2^2 x}} \log S(G_p) \le 2\sum_{\substack{p^{\alpha_p}\,\|\varphi(n)\\ p\le \log_2^2 x}} \alpha_p \log p \le 4\log_3 x \sum_{\substack{p^{\alpha_p}\,\|\varphi(n)\\ p\le \log_2^2 x}} \alpha_p\\ &= 4\Omega_{\log_2^2 x}(\varphi(n))\log_2 x \le 4(1+o(1))\log_2 x \log_3 x \log_4 x\end{aligned}$$

because $n \notin \mathcal{E}_4$, which finishes the proof. ∎

It is obvious that one can obtain explicit bounds on the size of the exceptional set.

We now turn our attention to lower bounds on D_n. Here, we adapt some arguments from [4] to show that, for almost all n, $S(n)$ contains a large smooth factor.

THEOREM 10. *There exists an absolute constant $c > 0$ such that for large x the number $S(n)$ is a multiple of all the prime numbers*

$$p < \frac{c\log_2^2 x}{\log_3 x}$$

with $p \equiv 1 \pmod 3$, *for all numbers $n < x$ with $o(x)$ exceptions.*

Proof. We set $y := \log^2 x$ and $z := \exp(\log^{1/3} x)$. For a prime $r \equiv 1 \pmod 3$ we write $\mathcal{P}_r$ for the product of all primes q in the interval $[y, z]$ with $q^2 - q + 1 \equiv 0 \pmod r$. Because the congruence $a^2 - a + 1 \equiv 0 \pmod r$ is solvable for $r \equiv 1 \pmod 3$ it is obvious that $\mathcal{P}_r > 1$ for sufficiently large x. For every integer $1 \le n \le x$ write

$$f(n) := \prod_{\substack{q\mid\varphi(n)\\ q>y}} (q^2 - q + 1),$$

and consider the sum

$$S(r,x) := \sum_{\substack{p\le x\\ r\mid f(p)}} \frac{1}{p} = \sum_{\substack{p\le x\\ \gcd(p-1,\mathcal{P}_r)>1}} \frac{1}{p}.$$

The arguments from Lemmas 3.1–3.3 and Theorem 3.4 of [4] now show that

$$S(r,x) \gg \min\left(\log_2 x, \frac{\log_2^2 x}{r}\right). \tag{10}$$

Moreover, with Brun's method (see Theorem 4.1 of [4]),

$$\sum_{\substack{n\le x\\ r\nmid f(n)}} 1 \ll x \prod_{\substack{p\le x\\ r\mid f(p)}} \left(1-\frac{1}{p}\right) \ll x\exp(-S(r,x)). \tag{11}$$

The inequality (10) shows that for an appropriate constant $c>0$ and

$$r < w := \frac{c\log_2^2 x}{\log_3 x}$$

we have

$$S(r,x) \ge 2\log_3 x,$$

and now the inequality (11) yields

$$\sum_{\substack{r\nmid f(n)\\ n\le x}} 1 \ll \frac{x}{\exp(2\log_3 x)} = \frac{x}{\log_2^2 x}.$$

Thus, the number of integers $n<x$ for which there exists $r<w$ such that $f(n)$ is not a multiple of r is at most

$$\sum_{r<w}\sum_{\substack{r\nmid f(n)\\ n\le x}} 1 \ll \frac{xw}{\log_2^2 x} = O\left(\frac{x}{\log_3 x}\right) = o(x).$$

It remains to notice that as in the proof of Theorem 9 we derive that $f(n)$ divides $S(n)$ for all $n<x$ with at most $o(x)$ exceptions. ■

THEOREM 11. *The inequalities*

$$\log D_n \gg \frac{\log_2 n}{\log_3 n} \quad \textit{and} \quad D_n \gg n^{24/67-\varepsilon}$$

hold for a set of positive integers n of asymptotic density 1 *and for infinitely many positive integers n, respectively.*

Proof. From Theorem 10 we see that $S(n)$ is a multiple of all primes $p<\log_2 x$, where $p\equiv 1 \pmod 3$. Lemma 2 of [14] shows that there exists an absolute constant c_2 such that $\varphi(n)$ is a multiple of all the prime powers $p^\beta < y := (c_2\log_2 x)/(\log_3 x)$ for all $n<x$ with $o(x)$ exceptions. Thus, D_n is a multiple of all primes $p<y$ with $p\equiv 1 \pmod 3$, and therefore

$$\log D_n \ge \sum_{\substack{p\equiv 1 \pmod 3\\ p<y}} \log p \gg y \gg \frac{\log_2 x}{\log_3 x},$$

which implies the first inequality.

To see that D_n can be large infinitely often, we recall that Theorem 2.1 of [1] implies that for any $\delta>0$ and for all primes p except $O(1)$ of them and for any integers a and $k>0$ with $\gcd(a,p)=1$ there exists a prime $q\equiv a \pmod{p^k}$ such that $q=O(p^{(12/5+\delta)k})$.

Without loss of generality we can assume that $\varepsilon < 1/3$ is sufficiently small. Select the smallest prime $p \equiv 1 \pmod 3$ for which the above estimate holds with $\delta > 0$ defined by the equation

$$\frac{24}{67+30\delta} = \frac{24}{67} - \varepsilon.$$

Since $p \equiv 1 \pmod 3$, the congruence $a^2 - a + 1 \equiv 0 \pmod p$ is solvable. Because p does not divide the discriminant -3 of $a^2 - a + 1$, using Hensel lifting we conclude that for any positive integer k there is a solution $1 \le a < p^k$ of the congruence $a^2 - a + 1 \equiv 0 \pmod{p^k}$. Choose a prime $q = O(p^{(12/5+\delta)k})$ with $q \equiv a \pmod{p^k}$ and define m from the equation

$$q^2 - q + 1 = p^k m.$$

We assume that $k \ge 3$, which implies that $q \nmid p - 1$ (for otherwise $p^k m = q^2 - q + 1 < p^2$, which is impossible for $k \ge 3$).

We now distinguish two cases:

Case 1: $q \mid \varphi(m)$. Set $n := p^{k+1}m^2$. Because $m < q^2$ we have $q \parallel \varphi(m)$, therefore $p^k m = q^2 - q + 1 \mid S(n)$. On the other hand, we also have $p^k m \mid \varphi(n)$ thus $D_n \ge p^k m > n^{1/2}$.

Case 2: $q \nmid \varphi(m)$. Set $n := p^{k+1}m^2q^2$. Then $p^k m \mid \varphi(n)$ and $q \parallel \varphi(n)$, therefore $p^k m = q^2 - q + 1 \mid S(n)$. Thus, $D_n \ge p^k m \gg q^2$. We also have

$$n = p^{k+1}m^2q^2 \ll q^6 p^{-k} \ll q^{6-5/(12+5\delta)}.$$

Therefore

$$\frac{\log D_n}{\log n} \ge \frac{2}{6 - 5/(12+5\delta)} = \frac{24+5\delta}{67+30\delta} \ge \frac{24}{67+30\delta} = \frac{24}{67} - \varepsilon.$$

Thus, the second inequality has been established. ∎

5. Concluding remarks and open problems. It would be very interesting to study the distribution of multiplicative orders of elements of $\mathbb{Z}_n$, in particular to obtain estimates for their higher moments (rather than just for the average value as we have done in this paper).

Another attractive line of research is to study orders of points on elliptic curves over finite fields. For example, given an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$, one can choose a random prime p and a random $\mathbb{F}_p$-rational point P on the reduction of $\mathcal{E}$ modulo p and study the order of P. One can also fix the prime p first, and then choose a random elliptic curve over $\mathbb{F}_p$ and ask similar questions about the average order of its points.

It is definitely tempting to suggest that $Q_n \to \infty$ as $n \to \infty$, but we believe that in fact $Q_n = 2$ infinitely often. Here we present some heuristic arguments to support this conjecture.

We believe (and it is supported by some heuristic counting arguments) that there are infinitely many finite sequences of distinct primes $p_1, \ldots, p_m$ such that

- $p_1 = 2$;
- $p_j^2 - p_j + 1 \equiv 0 \pmod{p_{j+1}}$ for every $j = 1, 2, \ldots$;
- $n = p_1 p_2 \ldots p_m + 1$ is a prime.

For each such sequence we have $Q_n = 2$.

Here are some numerical examples of integers n produced by this construction:

$$\begin{aligned} n &= 2, \\ n &= 2 \cdot 3 + 1 = 7, \\ n &= 2 \cdot 3 \cdot 7 + 1 = 43, \\ n &= 2 \cdot 3 \cdot 7 \cdot 43 \cdot 13 \cdot 157 \cdot 3499 \cdot 337 \cdot 113233 \cdot 674821003 \cdot 14724403 + 1 \\ &= 4890281893321969242411591581864107, \\ n &= 2 \cdot 3 \cdot 7 \cdot 43 \cdot 139 \cdot 19183 \cdot 2766679 \cdot 7654509922363 \cdot 93967 \cdot 1747 \\ &\quad \cdot 3050263 \cdot 769 + 1 \\ &= 39269659021529619029657646415283590328626879483, \\ n &= 2 \cdot 3 \cdot 7 \cdot 43 \cdot 139 \cdot 19183 \cdot 2766679 \cdot 7654509922363 \cdot 93967 \cdot 8581 \cdot 163 \\ &\quad \cdot 26407 \cdot 247183 \cdot 19 + 1 \\ &= 1662330489101343797227411323388048325379545079999067, \end{aligned}$$

which all have $Q_n = 2$.

References

[1] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. 140 (1994), 703–722.

[2] N. L. Bassily, I. Kátai and M. Wijsmuller, *On the prime power divisors of the iterates of the Euler-ϕ function*, Publ. Math. Debrecen 55 (1999), 17–32.

[3] T. Bier, *Some functions and numbers related to the Carmichael function*, Research Report 4/97, University of Malaya, Malaysia, 1997.

[4] P. Erdős, A. Granville, C. Pomerance and C. Spiro, *On the normal behaviour of the iterates of some arithmetic functions*, in: Analytic Number Theory, Birkhäuser, Boston, 1990, 165–204.

[5] P. Erdős and C. Pomerance, *On the normal number of prime factors of $\varphi(n)$*, Rocky Mountain J. Math. 15 (1985), 343–352.

[6] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.

[7] J. B. Friedlander, C. Pomerance and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp. 70 (2001), 1591–1605.

[8] J. von zur Gathen, A. Knopfmacher, F. Luca, L. Lucht and I. Shparlinski, *Average order in cyclic groups*, J. Théor. Nombres Bordeaux, to appear.

[9] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. 37 (1986), 27–38.

[10] —, *Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression*, Proc. London Math. Soc. 64 (1991), 265–338.

[11] S. Li, *On the number of elements with maximal order in the multiplicative group modulo n*, Acta Arith. 86 (1998), 113–132.

[12] —, *Artin's conjecture on average for composite moduli*, J. Number Theory 84 (2000), 93–118.

[13] F. Luca, *Some mean values related to average multiplicative orders of elements in finite fields*, preprint, 2002.

[14] 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.

[15] G. Martin, *The least prime primitive root and the shifted sieve*, Acta Arith. 80 (1997), 277–288.

[16] D. Wolke, *Eine Bemerkung über die Werte der Funktion $\sigma(n)$*, Monatsh. Math. 83 (1977), 163–166.

Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

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

Received on 9.7.2002
and in revised form on 3.10.2002 (4328)