

ON A FAMILY OF SUBGROUPS OF THE MULTIPLICATIVE GROUP MOD n

CARL POMERANCE

ABSTRACT. For each pair j, n with $n > j$, we consider the subgroup of the multiplicative group mod n of residues with order dividing $n - j$. We generalize some results in the case $j = 1$ due to Erdős and the current author. The case $j = 0$ is of particular interest.

1. INTRODUCTION

For each integer j and positive integer n with $n > j$, let

$$G_j(n) = \{a \bmod n : a^{n-j} \equiv 1 \pmod{n}\}, \quad F_j(n) = \#G_j(n).$$

Then $G_j(n)$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, so that $F_j(n) \mid \varphi(n)$, where φ is Euler's function. The case $j = 1$ has been studied in [2] and elsewhere. There are some results in the literature corresponding to some other values of j ; see [4], [9], and [11]. The case of $j = 0$ is connected to results on conditions for a ring to be commutative and was mentioned to me by Lenstra. The sequence $F_0(n)$ for $n = 1, 2, \dots$ is A072994 in oeis, computed by Cloitre. Lenstra (private communication) asked about the average order of $F_0(n)$. In this note we obtain some results about the average order and the normal order. We also look at the more general problem of $F_j(n)$.

2. THE AVERAGE ORDER OF $F_0(n)$

We reserve the letter p for a prime variable. As is common, we write $p^i \parallel n$ if $p^i \mid n$ and $p^{i+1} \nmid n$. Let $\text{rad}(n) = \prod_{p \mid n} p$, the squarefree kernel of n . By the Chinese remainder theorem we have

$$F_0(n) = \prod_{p^i \parallel n} \#\{a \bmod p^i : a^n \equiv 1 \pmod{p^i}\} = \prod_{p^i \parallel n} p^{i-1}(p-1, n) = \frac{n}{\text{rad}(n)} \prod_{p \mid n} (p-1, n).$$

This formula is to be contrasted with

$$\varphi(n) = \frac{n}{\text{rad}(n)} \prod_{p \mid n} (p-1).$$

Let $\lambda(n)$ denote the exponent of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$. Known as Carmichael's function, we have $\lambda(n)$ equal to the lcm of the numbers $\lambda(p^i)$ for $p^i \parallel n$. Further, for a prime power p^i , we have $\lambda(p^i) = \varphi(p^i)$ except if $p = 2, i \geq 3$, and then $\lambda(2^i) = \frac{1}{2}\varphi(2^i) = 2^{i-2}$. We will use the function

$$L(x) = \exp(\log x \log_3 x / \log_2 x),$$

Date: June 29, 2026.

2010 Mathematics Subject Classification. 11A05, 11N45.

Key words and phrases. multiplicative group, average order, normal order.

where \log_k is the k -fold iterate of \log . Note that $L(x) = x^{o(1)}$ as $x \rightarrow \infty$, but $L(x) > (\log x)^m$ for any m and x sufficiently large depending on m .

Theorem 1. *As $x \rightarrow \infty$, we have $\sum_{n \leq x} F_0(n) \leq x^2/L(x)^{1+o(1)}$.*

Proof. Suppose $n \leq x$ and let $k = k(n) = \varphi(n)/F_0(n)$. We consider 3 cases:

- (i) $k(n) > L(x)$;
- (ii) $k(n) \leq L(x)$ and $\lambda(n) > L(x)^3$;
- (iii) $k(n) \leq L(x)$ and $\lambda(n) \leq L(x)^3$.

For $n \leq x$ we have $F_0(n) = \varphi(n)/k(n) \leq x/k(n)$, so that for case (i) we have

$$\sum_{\substack{n \leq x \\ k(n) > L(x)}} F_0(n) \leq \sum_{n \leq x} \frac{x}{L(x)} \leq \frac{x^2}{L(x)}. \quad (1)$$

We now assume that $k(n) \leq L(x)$. Let $u = (n, \lambda(n))$ and write $n = uv$. We have

$$k = \frac{\varphi(n)}{F_0(n)} = \prod_{p|n} \frac{p-1}{(p-1, n)}.$$

Thus, for $p | n$, we have

$$p-1 = (p-1, n) \frac{p-1}{(p-1, n)} \mid (p-1, n)k \mid nk.$$

Thus, if $p^i \parallel n$, we have $p^{i-1}(p-1) \mid nk$, which implies that $\lambda(n) \mid nk$. This then implies that

$$\lambda(n) = (nk, \lambda(n)) \mid (n, \lambda(n))k = uk. \quad (2)$$

Now consider those $n \leq x$ in case (ii), say there are N of them. That is,

$$N := \sum_{\substack{n \leq x \\ k(n) \leq L(x) \\ \lambda(n) > L(x)^3}} 1.$$

For each such n , (2) implies that $(n, \lambda(n)) \geq \lambda(n)/k > L(x)^2$. Since $(n, \lambda(n)) \leq (n, \varphi(n))$, we have

$$\sum_{n \leq x} (n, \varphi(n)) \geq NL(x)^2.$$

Note that Theorem 11 in [3] is that

$$\sum_{n \leq x} (n, \varphi(n)) \leq xL(x)^{1+o(1)},$$

from which we deduce that $N \leq x/L(x)^{1+o(1)}$, so that

$$\sum_{\substack{n \leq x \\ k(n) \leq L(x) \\ \lambda(n) > L(x)^3}} F_0(n) \leq x^2/L(x)^{1+o(1)}. \quad (3)$$

We now consider those $n \leq x$ in case (iii), so that $k \leq L(x)$ and $\lambda(n) \leq L(x)^3$. For these n we have $u = (n, \lambda(n)) \leq L(x)^3$ and from (2), $\lambda(n) \mid uk$. With $n = uv$, we have $v \leq x/u$. Further, $\lambda(v) \mid \lambda(n) \mid uk$. For a divisor d of uk , the number of integers $v \leq x/u$ with $\lambda(v) = d$

is at most $(x/u)/L(x/u)^{1+o(1)}$ uniformly. Here we have used [10, Lemma 5.2]. Since u is small, we have $L(x/u) = L(x)^{1+o(1)}$, so that our count is bounded above by $(x/u)/L(x)^{1+o(1)}$. We have this for each $d \mid uk$ so our count in this case is at most

$$\sum_{u \leq L(x)^3} \frac{\tau(uk)}{u} \frac{x}{L(x)^{1+o(1)}} \leq \tau(k) \frac{x}{L(x)^{1+o(1)}}.$$

Now for each n counted, we have $F_0(n) \leq x/k$, so the contribution of these n 's is at most

$$\sum_{k \leq L(x)} \frac{\tau(k)}{k} \frac{x^2}{L(x)^{1+o(1)}} \leq \frac{x^2}{L(x)^{1+o(1)}}.$$

With the estimates (1) and (3), the proof is complete. \square

3. THE AVERAGE ORDER OF $F_j(n)$ FOR $j \neq 0, 1$

It was shown in [2] that

$$\sum_{\substack{n \leq x \\ n \text{ composite}}} F_1(n) \leq \frac{x^2}{L(x)^{1+o(1)}}, \quad x \rightarrow \infty. \quad (4)$$

It's clear that we should restrict to n composite since if n is prime, we have $F_1(n) = n - 1$, so that $\sum_{n \leq x} F_1(n) \sim \frac{1}{2}x^2/\log x$ as $x \rightarrow \infty$. We even have a name for members of $G_1(n)$ when n is composite: these are the bases for which n is a *pseudoprime*.

When $j > 1$ there is a similar special case. For a prime $p > j$ we have $F_j(jp)$ a multiple of $p - 1$ and a divisor of $\varphi(jp)$ (see (5) below), so $\sum_{p \leq x/j} F_j(jp) \asymp_j x^2/\log x$. Hence in this case we only consider values of n that are not j times a prime.

Theorem 2. *For each fixed integer $j \neq 0, 1$ we have*

$$\sum_{\substack{|j| < n \leq x \\ j \mid n \implies n/j \text{ composite}}} F_j(n) \leq \frac{x^2}{L(x)^{1+o(1)}}, \quad x \rightarrow \infty.$$

Proof. The argument is similar to the proof of (4). Fix an integer $j \neq 0, 1$. We have

$$F_j(n) = \prod_{p^i \parallel n} \sum_{\substack{a \pmod{p^i} \\ a^{n-j} \equiv 1 \pmod{p^i}}} 1 = \left(\frac{n}{\text{rad}(n)}, j \right) \prod_{p \mid n} (p - 1, n - j). \quad (5)$$

As discussed in the Introduction, $G_j(n)$ a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, say it has index $k = k(n)$, so that $F_j(n) = \varphi(n)/k$. We have

$$\prod_{p \mid n} \frac{p - 1}{(p - 1, n - j)} \mid k,$$

and so each $p - 1$ divides $(n - j)k$. Thus,

$$\lambda(\text{rad}(n)) \mid (n - j)k. \quad (6)$$

Since $F_j(n) = \varphi(n)/k(n) < x/L(x)$ for $k(n) > L(x)$, we may assume that $k \leq L(x)$. Now assume that $n \leq x$ is divisible by a prime $p > kL(x)$. Write $n = mp$ where $1 \leq m \leq x/p$. We have $(mp - j)k \equiv 0 \pmod{p-1}$, so that

$$m - j \equiv 0 \pmod{\frac{p-1}{(p-1, k)}}.$$

Note that if $j > 0$ we are assuming that $m \neq j$. Thus, $m \geq j + (p-1)/(p-1, k)$ and m is in a residue class mod $(p-1)/(p-1, k)$, so that the number of choices for m is at most $kx/p(p-1) + |j|k/(p-1)$. Summing this for $p > kL(x)$ we get $o_j(x/L(x))$ for the count, and so $o_j(x^2/L(x))$ for the contribution to the sum in the theorem.

We now may assume that every prime factor of n is bounded above by $kL(x)$ and that $x/L(x) < n \leq x$. Further, if the squarefull part of n is greater than y , then the number of such $n \leq x$ is $O(x/\sqrt{y})$. We apply this with $y = L(x)^2$, and so we may assume that the squarefull part of n is at most $L(x)^2$. Since $n > x/L(x)$ is assumed, we deduce that n has a squarefree divisor d in the interval $I := (x/kL(x)^2, x/L(x)]$. For each squarefree integer d in I we count those $n \leq x$ with $n \equiv 0 \pmod{d}$ and $(n-j)k \equiv 0 \pmod{\lambda(\text{rad}(d))}$, using (6). Since d is squarefree, the second congruence reduces to $n-j \equiv 0 \pmod{\lambda(d)/(\lambda(d), k)}$. If there are any solutions at all to the two congruences, we must have the gcd of the moduli dividing j . Then the number of n in this case is at most $1 + (k, \lambda(d))|j|x/d\lambda(d)$. Letting d run over squarefree numbers in I , using [10, Lemma 5.2] and partial summation, we have

$$\sum_{d \in I} \frac{(k, \lambda(d))}{d\lambda(d)} = \sum_{l \leq x/L(x)} \frac{1}{l} \sum_{\substack{d \in I \\ \lambda(d)/(k, \lambda(d))=l}} \frac{1}{d} \leq \sum_{l \leq x/L(x)} \frac{1}{l} \sum_{u|k} \sum_{\substack{d \in I \\ \lambda(d)=ul}} \frac{1}{d} \leq \frac{\tau(k)}{L(x)^{1+o(1)}}.$$

Thus, the number of choices for n in this case is $O_j(\tau(k)x/L(x)^{1+o(1)})$, so summing $F_j(n) \leq x/k$, we get $O_j(x^2/L(x)^{1+o(1)})$. This completes the proof. \square

4. LOWER BOUNDS FOR THE AVERAGE ORDER

One may wonder how close the expression $x^2/L(x)^{1+o(1)}$ in Theorems 1, 2, and in (4) is to the true average orders. In [2, Theorem 2.1] it is shown that

$$\frac{1}{x} \sum_{\substack{n \leq x \\ n \text{ composite}}} F_1(n) > x^{15/23} \tag{7}$$

for all large x . The exponent $15/23$ depends on the existence of many primes p with $p-1$ not divisible by a large prime, and it is discussed in [2] how a certain natural conjecture about these primes leads to the assertion that we have equality in (4). For a rigorous lower bound, we have the exponent $15/23$ improving to 0.7156 using [5, Theorem 1.1].

The same goes for $F_0(n)$, namely we have

$$\frac{1}{x} \sum_{n \leq x} F_0(n) > x^{0.7156}$$

for all large x and conjecturally this average is equal to $x/L(x)^{1+o(1)}$. See the final paragraph of [7] where the distribution of those n with $\lambda(n) | n$ is discussed. Note that $\lambda(n) | n$ if and only if $F_0(n) = \varphi(n)$.

For fixed $j \neq 0, 1$ we have the same lower bound estimates for

$$\frac{1}{x} \sum_{\substack{|j| < n \leq x \\ j|n \implies n/j \text{ composite}}} F_j(n).$$

To see this one merely replaces the number 1 in [2, (2.6)] with j .

5. THE NORMAL ORDER

For each positive integer n let

$$g(n) = \sum_{d|n} \frac{\Lambda(d)}{\varphi(d)},$$

where Λ is the von Mangoldt function. We have the following theorem.

Theorem 3. *For each integer j there is a set $S_j \subset \mathbb{N}$ of asymptotic density 1 such that*

$$\frac{\log F_j(n)}{\log \log n} = g(n - j) + o(1)$$

for $n \in S_j$ and $n \rightarrow \infty$.

This theorem for $j = 1$ is [2, Theorem 4.1]. To generalize to $j \neq 1$ one need only check that we have $\log(n/\text{rad}(n))/\log \log n = o(1)$ as $n \rightarrow \infty$ in a set of asymptotic density 1.

As in [2] we have the corollary that for each j , $F_j(n) \leq (\log x)^{\psi(x)}$ for all but $o(x)$ integers $n \leq x$, where $\psi(x) \uparrow \infty$ arbitrarily slowly. In fact, from the Erdős–Wintner theorem, for each positive real number u the asymptotic density $D_j(u)$ of the set of n with $F_j(n) \leq (\log n)^u$ exists, with $D_j(u)$ continuous, strictly increasing, tending to 0 as $u \downarrow 0$ and tending to 1 as $u \uparrow \infty$.

6. THE NUMBER OF SUBGROUPS

For a finite abelian group \mathcal{G} , written multiplicatively, and m a positive integer, the sets

$$\mathcal{G}_m = \{g \in \mathcal{G} : g^m = 1\}$$

are subgroups of \mathcal{G} , call them power kernels. Let $\lambda(\mathcal{G})$ be the exponent of \mathcal{G} . It is easy to see that

$$g^m = 1 \text{ if and only if } g^{(m, \lambda(\mathcal{G}))} = 1,$$

so that $\mathcal{G}_m = \mathcal{G}_d$, where $d = (m, \lambda(\mathcal{G}))$. Applying this to the groups $G_j(n)$ we have the following, where τ is the divisor function.

Theorem 4. *For a positive integer n , let $\mathcal{G} = (\mathbb{Z}/n\mathbb{Z})^*$, with power kernels \mathcal{G}_d for $d \mid \lambda(n)$. For j an integer with $j < n$, we have $G_j(n) = \mathcal{G}_d$, where $d = (\lambda(n), n - j)$. In particular, there are exactly $\tau(\lambda(n))$ different subgroups of the form $G_j(n)$ for each positive integer n .*

It is possible to consider the count $\tau(\lambda(n))$ statistically. Its logarithm has the normal order $\frac{\log 2}{2}(\log \log n)^2$, and there is a Gaussian distribution, see [1]. One may also consider the total number of non-isomorphic subgroups of $(\mathbb{Z}/n\mathbb{Z})^*$. This was considered in [8], and their result is similar to what we have for $\tau(\lambda(n))$ in [1]. (Their paper also considered the larger statistic where one counts subsets that are subgroups.) One can also consider $\tau(\lambda(n))$ on average; for this see [6].

ACKNOWLEDGMENTS

I thank Hendrik Lenstra for introducing me to the function $F_0(n)$ and his queries about it. I also thank Florian Luca, Greg Martin, and Paul Pollack for timely help and for reminding me of some of the literature. I am grateful to the referee for a careful reading and some helpful suggestions.

REFERENCES

- [1] P. Erdős and C. Pomerance, The normal number of prime factors of $\varphi(n)$, *Rocky Mtn. J. Math.* **15** (1985), 343–352.
- [2] P. Erdős and C. Pomerance, On the number of false witnesses for a composite number, *Math. Comp.* **46** (1986), 259–279.
- [3] P. Erdős, F. Luca, and C. Pomerance, On the proportion of numbers coprime to a given integer, *Proceedings of the Anatomy of Integers Conference*, Montreal, March 2006, J.-M. De Koninck, A. Granville, F. Luca, eds., CRM Proceedings and Lecture Notes, vol. 46 (2008), 47–64.
- [4] Knödel numbers, Wolfram MathWorld, <https://mathworld.wolfram.com/KnoedelNumbers.html>
- [5] J. D. Lichtman, Primes in arithmetic progressions to large moduli, and shifted primes without large prime factors, arXiv preprint arXiv:2211.09641, (2022) 27 pp.
- [6] F. Luca and C. Pomerance, On the average number of divisors of the Euler function, *Publ. Math. Debrecen* **70** (2007), 125–148. Corrigendum, *ibid.* **89** (2016), 257–260.
- [7] F. Luca and C. Pomerance, On the range of the iterated Euler function, in *Proceedings of the Integers Conference 2007 held at the University of West Georgia*, Carrollton, GA, October 24–27, 2007. Edited by B. Landman, M. B. Nathanson, M. Nešetřil, R. J. Nowakowski, C. Pomerance and A. Robertson. Walter de Gruyter GmbH & Co. KG, Berlin, 2009, pp. 101–116.
- [8] G. Martin and L. Troupe, The distribution of the number of subgroups of the multiplicative group. *J. Aust. Math. Soc.* **108** (2020), 46–97.
- [9] D. C. Morrow, Some properties of D-numbers, *Amer. Math. Monthly* **58** (1951), 329–330.
- [10] C. Pomerance, Two methods in elementary analytic number theory, in *Number theory and applications*, R. A. Mollin, ed., Kluwer Academic Publishers, Dordrecht, 1989, pp. 135–161.
- [11] A. Rotkiewicz, On the congruence $2^{n-2} \equiv 1 \pmod{n}$, *Math. Comp.* **43** (1984), 271–272.

MATHEMATICS DEPARTMENT, DARTMOUTH COLLEGE, HANOVER, NH 03755, USA
E-mail address: carlp@math.dartmouth.edu