A GENERALIZATION OF PRIMITIVE ROOTS

SHUGUANG LI AND CARL POMERANCE

Abstract. We survey a few results and conjectures on a natural generalization of primitive roots. In the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ one may look at elements whose order is the maximum over all elements in the group. If the group is cyclic, this concept is exactly the same as a primitive root. Here we look at the issue for general numbers n, continuing to call an element of maximal order a primitive root for n. Some of the traditional problems and results for primitive roots, including the number of them and Artin's conjecture, continue to make sense in this expanded context, but we shall see that the situation is considerably stranger.

1. Introduction

For a prime p, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Number theorists refer to any cyclic generator of this group as a primitive root modulo p. There are many attractive theorems and conjectures concerning primitive roots, and these are discussed in other chapters. It is our intention to broaden the playing field, so to speak, and introduce the concept of a primitive root for a composite modulus n. It is well-known that for most numbers n, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic (namely, $(\mathbb{Z}/n\mathbb{Z})^*$ is not cyclic for any number $n > 4$ that is not of the form $p^j, 2p^j$ for p an odd prime). So what then do we mean by a primitive root for n? In any finite group G one may look at elements whose order is the maximum order over all elements in G. We do precisely this, and say that such elements for the group $G = (\mathbb{Z}/n\mathbb{Z})^*$ are primitive roots modulo n. In Martin [20], these are called λ-roots for n, but regardless of the name, we shall see that they contain a few surprises.

Setting some notation, for $n \geq 2$ let $\lambda(n)$ denote the size of the largest cyclic subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$, so that $a \in (\mathbb{Z}/n\mathbb{Z})^*$ is a primitive

Date: April 2, 2025.

Parts of this article appeared in "New Aspects of Analytic Number Theory" (RIMS Kokyuroku No. 1274), 2002 and in Dev. Math. **8**, pp. 219–231, Kluwer Academic Publishers, Dordrecht 2002, with the title "Primitive roots: a survey."

root for n if and only if its order is $\lambda(n)$. Let $R(n)$ denote the number of primitive roots for n. By convention we take $\lambda(1) = R(1) = 1$.

2. The number of primitive roots for a given modulus

One might wonder if $R(n)$ is multiplicative. It is not, but it does have some structure, it is sub-multiplicative, see the discussion below. A basic question that one might ask is a formula for $R(n)$ and beyond that, a study of the order of magnitude of $R(n)$ as a function of n. For primes, the situation is straightforward. If g is a primitive root modulo p then all of the primitive roots for p are of the form g^j where j is coprime to $p-1$. Thus $R(p) = \varphi(p-1)$. This fact is well-known, but less well-known is that $\varphi(p-1)/(p-1)$ has a continuous distribution function. That is, let $D(u)$ denote the relative asymptotic density in the set of all primes of the set $\{p \text{ prime} : R(p)/(p-1) \le u\}$. Then $D(u)$ exists for every real number u, $D(u)$ is a continuous function of u, and $D(u)$ is strictly increasing on $[0, 1/2]$, with $D(0) = 0, D(1/2) = 1$. This beautiful result, which echoes Schoenberg's theorem on $\varphi(n)/n$, is due to Kátai [8] (also see [2] and [4]).

It is not so easy to get a formula for $R(n)$ in general. It may be instructive to first consider the case of a general finite abelian group G. Write G as a product of cyclic groups of prime power order. For each prime p dividing the order of G, let p^{λ_p} be the highest power of p that appears as an order of one of these cyclic factors, and let Δ_p be the number of times that this cyclic factor appears. Then the maximal order of an element in G is

$$\prod_{p\,|\,|G|} p^{\lambda_p}$$

and the number of elements of G with this order is

$$|G| \prod_{p\,|\,|G|} \left(1 - p^{-\Delta_p}\right)$$

To see the latter assertion, note that an element g will have p^{λ_p} dividing its order if and only if at least one of its projections in the Δ_p cyclic factors of order p^{λ_p} has order p^{λ_p}. The chance that one particular projection does not have this order, that is, it is killed by the exponent $p^{\lambda_p - 1}$, is $1/p$. Thus, the fraction of elements g for which each of the Δ_p projections is killed by the exponent $p^{\lambda_p - 1}$ is $p^{-\Delta_p}$, so the fraction for which at least one projection has order p^{λ_p} is $1 - p^{-\Delta_p}$. The assertion follows.

To apply this result to $G = (\mathbb{Z}/n\mathbb{Z})^*$ we must compute the numbers $\Delta_p = \Delta_p(n)$ for this group. By the Chinese remainder theorem, G has

a decomposition into the product of the groups $(\mathbb{Z}/q^j\mathbb{Z})^*$, where q is prime and $q^j \| n$. Further, the groups $(\mathbb{Z}/q^j\mathbb{Z})^*$ are themselves cyclic unless $q = 2$ and $j \geq 3$, in which case $(\mathbb{Z}/2^j\mathbb{Z})^*$ is the product of a cyclic group of order 2 and a cyclic group of order 2^{j-2}. It is thus a simple task to further refine the decomposition afforded by the Chinese remainder theorem into a factorization of $(\mathbb{Z}/n\mathbb{Z})^*$ into cyclic groups of prime power order. We thus can work out a formula, albeit not so simple, for $R(n)$: If the prime factorization of n is $\prod_{i=1}^{k} q_i^{a_i}$, and p is a prime with $p \mid \varphi(n)$, let $\lambda_p = \lambda_p(n)$ be such that $p^{\lambda_p} \| \lambda(n)$, so it is the largest number such that $p^{\lambda_p} \mid \lambda\left(q_i^{a_i}\right)$ for some i. If p is odd, let Δ_p be the number of i 's with $p^{\lambda_p} \mid \lambda\left(q_i^{a_i}\right)$. If $p = 2$ and either $\lambda_2 > 1$ or $n \not\equiv 8 \pmod{16}$, the definition of Δ_2 is the same. If $p = 2, \lambda_2 = 1$, and $n \equiv 8 \pmod{16}$, then $\Delta_2 = k + 1$. Then

$$R(n) = \varphi(n) \prod_{p \mid \varphi(n)} \left(1 - p^{-\Delta_p}\right).$$

We can use this formula to prove that

$$R(mn) \geq R(m)R(n) \tag{1}$$

for all positive integers m, n with equality if and only if one of m, n is 1, one of m, n is 2 with the other odd, or $m = n = 2$. This extends a result from [7]. To prove this, we consider the contribution of various primes p to $R(mn)/R(m)R(n)$. Assume $p \mid \gcd(m, n)$. The contribution of p to $\varphi(mn)/\varphi(m)\varphi(n)$ is $p/(p-1)$, while the contribution of p to the three products over primes dividing $\varphi(m), \varphi(n), \varphi(mn)$ is $\geq 1 - p^{-\Delta_p(mn)} \geq 1 - 1/p$, and so the total contribution is ≥ 1, and it is > 1 if $p \mid \varphi(m)\varphi(n)$. Now suppose that $p \nmid \gcd(m, n)$, but $p \mid \gcd(\varphi(m), \varphi(n))$. Then the contribution of p to the φ factors is 1 and $\nu_p(mn) = \max\{\nu_p(m), \nu_p(n)\}$. If $\nu_p(m) < \nu_p(n)$, then $\Delta_p(mn) = \Delta_p(n)$ and the p contribution is > 1. Similarly if $\nu_p(n) < \nu_p(m)$. So, assume that $\nu_p(m) = \nu_p(n) > 0$. Then $\Delta_p(mn) = \Delta_p(m) + \Delta_p(n)$ and the p contribution is

$$\frac{1 - p^{-\Delta_p(mn)}}{(1 - p^{-\Delta_p(m)})(1 - p^{-\Delta_p(n)})} = \frac{p^{\Delta_p(m)+\Delta_p(n)} - 1}{(p^{\Delta_p(m)} - 1)(p^{\Delta_p(n)} - 1)} > 1.$$

Finally, if $p \nmid \gcd(m, n)$ and p divides exactly one of $\varphi(m), \varphi(n)$ then the p contribution is 1. This proves the inequality (1) holds. The cases for equality are clear, but it remains to show there are no other cases where equality holds. We saw above that there was a strict inequality if $\gcd(\varphi(m), \varphi(n)) > 1$. Since $\varphi(k)$ is even for $k \geq 3$, we always have this unless $\min\{m, n\} \leq 2$. We may assume one of m, n is 2 and the other even and > 2, since the other cases have equality. We saw above that

if $\gcd(m, n, \varphi(m)\varphi(n)) > 1$ the inequality is strict, so this completes the proof.

There is a more conceptual proof of (1) in the case that $\gcd(m, n) = 1$. Then $(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ and if a, b are primitive roots mod m, n respectively, then the element c corresponding to (a, b) is a primitive root mod mn. Moreover, if $\min\{m, n\} \geq 3$ and $\nu_2(m) \leq \nu_2(n)$, then (a^2, b) also corresponds to a primitive root mod mn, so we have a strict inequality, with the same in the analogous case that $\nu_2(n) \leq \nu_2(m)$.

In analogy with Kátai's theorem about $R(p)/(p-1)$, one might ask if $R(n)/\varphi(n)$, has a distribution function. That is, for a given real number u does the set

$$\mathcal{R}_u := \{n : R(n)/\varphi(n) \leq u\}$$

have a natural density? Our first surprise is that the answer is no. It is shown by the first-named author in [13], [14] that there are values of u so that $\mathcal{R}_u$ does not have a natural density. In fact, there is a small positive number δ such that for every $u > 0, \mathcal{R}_u$ has upper density at least δ, but the lower density tends to 0 as $u \to 0$.

There are other naturally occurring sets in number theory where there is no natural density. For example, consider the set of integers n with an even number of decimal digits. While the natural density does not exist (the fraction of numbers in the set at 10^{2n} is at least $9/10$ while the fraction in the set at 10^{2n+1} is at most $1/10$), note that this set does have a logarithmic density. That is, the sum of the reciprocals of the numbers in the set that are $\leq x$, when divided by $\log x$, approaches a limit, namely $1/2$. (It is interesting to note that logarithmic density is equivalent to the concept of Dirichlet density from analytic number theory.)

Well, perhaps the set of numbers with an even number of decimal digits is not so natural a concept. But also consider the set of integers n with $\pi(n) > \mathrm{li}(n)$. (Here, $\pi(x)$ is the number of primes in the interval $[1, x]$ and $\mathrm{li}(x) = \int_0^x dt/\log t$, where the principal value is taken for the singularity at $t = 1$.) It was once thought that there should be no values of n with $\pi(n) > \mathrm{li}(n)$, until Littlewood showed that there are infinitely many, and also infinitely many with the reverse inequality. It is shown in Rubinstein and Sarnak [23] that assuming reasonable conjectures concerning the zeroes of the Riemann zeta function, the set of integers n with $\pi(n) > \mathrm{li}(n)$ does not have a natural density, but it does have a logarithmic density. Similar results pertain to the set of integers n with $\pi(n; 4, 1) > \pi(n; 4, 3)$, where $\pi(x; k, l)$ denotes the number of primes p in $[1, x]$ that are in the residue class $l \pmod k$.

So maybe the sets $\mathcal{R}_u$ have a logarithmic density? Alas, the answer is again no, as is shown in [13]. In fact, the oscillation persists at even the double logarithmic density (where one sums $1/a \log a$ for members a of the set that are in $[2, x]$ and divides the sum by $\log \log x$). Maybe the triple logarithmic density exists: In [13] it is shown that at the triple level, $\mathcal{R}_u$ has upper density tending to 0 as $u \to 0$.

3. The source of the oscillation

Where does this surprising oscillation come from? The answer lies in the numbers Δ_p described above. Consider a game played with n coins: We give you n coins, and at the end of the game you will either have given us back all n of the coins, or you will have given us back $n-1$ coins, keeping one for yourself. Here's how the game is played. You flip the n coins (assume they are all fair coins with a $1/2$ probability of landing heads—the front of the coin—and a $1/2$ probability of landing tails—the back of the coin), returning to us all of the coins that land tails. If there is more than one coin left, you repeat the process. If at any time you have exactly one coin left, you get to keep it. What is the probability P_n that you win the game by getting to keep a coin? It is not so hard to work out an expression for P_n, it is

$$P_n = \sum_{k=1}^{\infty} n 2^{-k} \left(1 - 2^{1-k}\right)^{n-1}$$

Indeed, if one keeps flipping until no coins are left, and the last coin leaves on round k, with the other $n-1$ coins leaving on earlier rounds, then the probability of this is $n2^{-k}\left(1-2^{1-k}\right)^{n-1}$. (There are n choices for the "last" coin, the probability it falls heads $k-1$ straight times followed by a tails is 2^{-k}, and the probability that each of the other $n-1$ coins has at least one tails in the first $k-1$ flips is $\left(1-2^{1-k}\right)^{n-1}$.) But more interestingly, one can ask:

$$\text{What is } \lim_{n\to\infty} P_n \text{ ?}$$

It is easy to convince oneself that when n is large, the biggest contribution to the sum for P_n is from the terms k with $2^k \approx n$. Suppose $0 \le \alpha < 1$ and S_α is an infinite set of natural numbers n such that the fractional part of the base-2 logarithm for $n \in S_\alpha$ converges to α modulo 1. For example, if $\alpha = 0$, then we might take S_0 as the set of powers of 2 . Or we might also throw in the numbers of the form

$2^m - 1$ and numbers of the form $2^m + m^2$. Then

$$\lim_{n\to\infty,\, n\in S_\alpha} P_n = \sum_{j=-\infty}^{\infty} 2^{-\alpha-j} e^{-2^{1-\alpha-j}}.$$

From this result it surely looks like the limiting value of P_n actually depends on α, the limiting value of the fractional part of the base-2 logarithm of n. That is, it looks like $\lim_{n\to\infty} P_n$ does not exist!

And this is indeed the case, though the oscillation in P_n is very gentle. We have $\limsup P_n \approx 0.72135465$ which is achieved when $\alpha \approx 0.139$, and $\liminf P_n \approx 0.72134039$ which is achieved when $\alpha \approx 0.639$. That is, the oscillation is only in the fifth decimal place! (For more on this kind of oscillation in probability theory, see [1] and the references in the acknowledgment of priority therein, and [11].

It may be unclear what this game has to do with $R(n)$. Consider the number Δ_2 : If 2^{λ_2} is the highest power of 2 dividing the order of an element modulo n, then Δ_2 is the number of cyclic factors of order 2^{λ_2} in $(\mathbb{Z}/n\mathbb{Z})^*$. We might ask where these Δ_2 factors come from. But for a set of numbers n of density 0 we have Δ_2 equal to the number of primes $p \mid n$ with $p \equiv 1 \pmod{2^{\lambda_2}}$. Now think of the odd primes dividing n as the coins in the game. Those primes $p \equiv 3 \pmod 4$ are the coins that turn tails on the first round and are returned. Those primes $p \equiv 5 \pmod 8$ are returned on the second round of flips, and so on. The number of primes that are alive in the last round is Δ_p, and from our coin experience, we see that there is some oscillation for the probability that $\Delta_p = 1$. But what corresponds to the number of coins? This is the number of odd prime factors of n, which is normally about $\log\log n$. Thus the limiting probability should depend on the fractional part of $\log\log\log n/\log 2$. With all of these iterated logarithms, it may begin to be clear why the density oscillation persists at logarithmic and double logarithmic levels.

But we noticed that the oscillation for the coin game is very slight. To see why there are great oscillations in the normal value of $R(n)$, we need to bring the other numbers Δ_p into play for higher values of p. This then suggests a game played with unfair coins, where the probability of landing heads is $1/p$. An analysis of this game shows that there is again oscillation for the probability of winning, and as p tends to infinity, the ratio of the limsup of the probability to the liminf of the probability tends to infinity. In particular, if x tends to infinity in such a way that the fractional part of $\log\log\log x/\log p$ is very nearly 1 for all small primes p, then for most numbers n up to x, the values Δ_p will frequently be 1 for these small primes p, so that $R(n) = o(\varphi(n))$ for

most numbers n up to x. But if x tends to infinity in such away that $\log\log\log x/\log p$ has fractional part about $1/2$ for all small primes p, then the values Δ_p will mostly be > 1, so that $R(n)/\varphi(n)$ is bounded away from 0 for most numbers n up to x.

4. Artin's conjecture for composite moduli

Let $N_a(x)$ denote the number of integers n in $[1, x]$ with primitive root a. In analogy with Artin's conjecture for primes, it is tempting to conjecture that if a does not lie in some exceptional set, yet to be determined, then there is a positive constant $B(a)$ with $N_a(x) \sim B(a)x$. However, considering the experience above with the normal value of $R(n)$, we might be wary of such a conjecture.

To gain some further insight, we consider averaging. Namely, what can be said about $\frac{1}{x}\sum_{1\le a\le x} N_a(x)$? As with the case for primes, we reorganize the sum, so that now we are summing over integers $n \le x$, and for each n we would like to know how many primitive roots it has in $[1, x]$. This estimate was worked out by the first-named author in [16], and sure enough, there is an oscillation. It is shown that

$$\liminf_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) = 0, \quad \limsup_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) > 0.$$

(The reason for the extra factor of $1/x$ is that it is natural to begin with the assumption that each term $N_a(x)$ is of order of magnitude x.) This result was improved by the authors, see [18], who proved the same limits but for an average over a much shorter interval of a's. Stephens [25] has a similar result in the prime case.

Before proceeding, we note that there are certain numbers a for which we always have $N_a(x) = o(x)$. Let $\mathcal{E}$ denote the set of integers a such that either a is a nontrivial power, or a is a square times –1 or a square times ± 2. Then for $a \in \mathcal{E}$, $N_a(x) = o(x)$. To get the idea of this, consider for example the case of $a = 2$, which is not exceptional when one considers prime moduli, but is exceptional for composite moduli. Since $\gcd(a, n) = 1$ and $a = 2$, we have n odd. But for a set of density 0, the highest power of 2 which divides an order of an element in $(\mathbb{Z}/n\mathbb{Z})^*$, as before call it 2^{λ_2}, has $\lambda_2 \ge 3$, since almost all numbers are divisible by a prime that is 1 (mod 8). If $p \mid n$ where $p \equiv 1 \pmod{2^{\lambda_2}}$ (at least one such prime must divide n), then necessarily, since $p \equiv 1 \pmod 8$, we have that 2 is a quadratic residue modulo p. Thus, 2^{λ_2} cannot divide the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ and so 2 cannot be a primitive root modulo n. The number of exceptional numbers $n \le x$ where this argument is not valid is $O(x/(\log x)^{1/4})$, which is $o(x)$ as claimed.

The set $\mathcal{E}$ should then stand as a candidate for the exceptional set in a generalization of Artin's conjecture for composite moduli.

But beyond this exceptional set, the first-named author in [15] was able to show that for *any* integer a, we have

$$\liminf_{x\to\infty} \frac{1}{x} N_a(x) = 0. \tag{2}$$

Moreover, this result was obtained on a set of real numbers x that is independent of the choice of a. That is, there is an unbounded set S of positive reals such that for every integer a,

$$\lim_{x\to\infty,\, x\in S} \frac{1}{x} N_a(x) = 0.$$

So, we definitely do not have $N_a(x) \sim B(a)x$ for a positive number $B(a)$, not for any integer a. (It bears remarking though that if one restricts the question to "almost primes", namely composite numbers with a fixed number of prime factors, the relative density does exist, on assumption of the GRH. See Péringuey [22].)

With these thoughts in place, the first-named author in [13] made the conjecture that if a is a fixed integer not in $\mathcal{E}$, then there is a positive number $B(a)$ with

$$\limsup_{x\to\infty} \frac{1}{x} N_a(x) = B(a).$$

In [17] we were able to prove this conjecture, under assumption of the GRH[1]. In fact, we have been able to show that there is an unbounded set S' of positive reals and a positive constant c such that for each integer $a \notin \mathcal{E}$,

$$\limsup_{x\to\infty,\, x\in S'} \frac{1}{x} N_a(x) \ge c\frac{\varphi(|a|)}{|a|}. \tag{3}$$

One might ask about the weak Artin conjecture for composite moduli; that is, are there infinitely many n with a given number a as a primitive root? Actually on this question, it is indeed possible to unconditionally prove that there are infinitely many n with primitive root a for many values of a. For example, take $a = 2$. We have that 2 is a primitive root for all of the numbers 3^j. In general, if a is a primitive root for p^2, where p is an odd prime, then a is a primitive root for p^j for every j. Other examples: Any number $a \equiv \pm 3 \pmod 8$ is a primitive root for all of the numbers 2^j. What is still unsolved, and may be tractable without the GRH: Given an integer a that is not a square

[1]That is, the Riemann Hypothesis for Kummerian fields

nor –1 , are there infinitely many squarefree integers n with primitive root a ?

5. Local densities and a stronger conjecture

Let us first consider an easier question. Given a fixed prime q and a fixed integer $a \notin \mathcal{E}$, what is the distribution of the set of natural numbers n coprime to a such that the power of q in the order of a in the group $(\mathbb{Z}/n\mathbb{Z})^*$ is as large as possible over all elements in the group? Say the number of such integers $n \leq x$ is $N_a^q(x)$. This problem, see [17], can be analyzed unconditionally, giving

$$N_a^q(x) = (1 + o(1))\frac{\varphi(|a|)}{|a|} x \left(1 - F_q(x)\right)$$

where $F_q(x)$ is given by

$$\sum_{j=0}^{\infty} \left(\exp\left(-\left(\frac{1}{\varphi\left(q^j\right)} - \frac{1}{q^{j+1}} \right) \log\log x \right) - \exp\left(-\frac{1}{\varphi\left(q^j\right)} \log\log x \right) \right).$$

As with the coin-flip problem, the density $1 - F_q(x)$ does not tend to a limit as $x \to \infty$. It is possible to show that

$$\liminf_{x\to\infty} F_q(x) \sim \frac{\log q}{q^2}, \quad \limsup_{x\to\infty} F_q(x) \sim \frac{1}{eq}$$

as $q \to \infty$. By choosing a sequence of x-values where $F_q(x) \geq c/q$ occurs for many small primes q, it is possible to prove (2). It is also possible to choose a sequence of x-values where $F_q(x) = O(1/q \log q)$ for most small primes q, but this is not sufficient for (3), since larger primes q can spoil the result. To show that larger primes usually do not pose too great an influence, the GRH comes into play.

Let

$$F_q = \liminf_{x\to\infty} F_q(x) = \inf_{t>0} \sum_{j=-\infty}^{\infty} \frac{\exp\left(t/q^{j+1}\right) - 1}{\exp\left(t/\left(q^j - q^{j-1}\right)\right)} \tag{3}$$

(Notice that the function of t is invariant under $t \mapsto tq$.) It seems reasonable to conjecture that the upper density $B(a)$ may be taken as $\alpha\varphi(|a|)/|a|$, where

$$\alpha := \prod_q \left(1 - F_q\right) \approx 0.326$$

a conjecture made in [17]. That is, it is conjectured that for every integer a not in $\mathcal{E}$,

$$\limsup_{x\to\infty} \frac{1}{x} N_a(x) = \alpha \frac{\varphi(|a|)}{|a|} \tag{4}$$

and that this limsup is attained on a set of positive reals independent of the choice of a. Note that for the number c in (3), we do have $c \le \alpha$; in fact this is unconditional. That is, for every integer $a \ne 0$,

$$\limsup_{x\to\infty} \frac{1}{x} N_a(x) \le \alpha \frac{\varphi(|a|)}{|a|}.$$

Let t_q be a value of t in $[1, q)$ where the infimum in (3) occurs. Then $t_q = \log q + \log\log q + o(1)$ as $q \to \infty$. If $x \to \infty$ in such a way that the fractional part of $\log\log\log x/\log q$ tends to the fractional part of $\log t_q/\log q$, then $F_q(x) \to F_q$. Part of the problem in showing the conjecture (4) is to show that there is an unbounded sequence of values of x such that simultaneously, for all small primes q, the fractional part of $\log\log\log x/\log q$ approaches the fractional part of $\log t_q/\log q$. That such a sequence of x values exists follows from Schanuel's conjecture in transcendental number theory. Indeed, from this conjecture, it follows that if $q_1, \dots, q_k$ are distinct primes, then the real numbers $\log q_1, \dots, \log q_k$ are algebraically independent. It would follow that the real numbers $1/\log q_1, \dots, 1/\log q_k$ are linearly independent over the rationals, allowing simultaneous diophantine approximation of the quantities $\log\log\log x/\log q_1, \dots, \log\log\log x/\log q_k$ modulo 1. However, even with Schanuel's conjecture and the GRH, there still seems to be some difficulties with the stronger conjecture.

Perhaps somewhat more tractable may be the conjecture from [15] that for a fixed integer a_0 not in $\mathcal{E}$, the individual count $N_{a_0}(x)$ is asymptotically equal to the average count over all integers a in $[1, x]$. That is, as $x \to \infty$,

$$N_{a_0}(x) = (1 + o(1)) \frac{1}{x} \sum_{1\le a\le x} N_a(x).$$

We close with another conjecture that is perhaps tractable:

$$\limsup_{x\to\infty} \frac{1}{x^2} \sum_{1\le a\le x} N_a(x) = \frac{6\alpha}{\pi^2}.$$

6. Average order

For a positive integer n and an integer g coprime to n, let $\ell_g(n)$ be the order of g in $(\mathbb{Z}/n\mathbb{Z})^*$. Thus, g is a primitive root for n if and only if $\ell_g(n) = \lambda(n)$. One can ask for g fixed what $\ell_g(n)$ is on average as n

runs among integers coprime to g. One can also ask about this when $n = p$ runs through primes. Let

$$A_g(x) = \frac{1}{x} \sum_{\substack{n \le x \\ \gcd(n,g)=1}} \ell_g(n), \quad A'_g(x) = \frac{1}{\pi(x)} \sum_{\substack{p \le x \\ p \nmid g}} \ell_g(p).$$

Assume $g \notin \{0, 1, -1\}$. Arnold conjectured in 2005 that $A_g(x) \sim c_g x/\log x$, where c_g is a positive constant, but this was shown to be incompatible with the GRH by Shparlinski [24]. Then in [12] it was shown, assuming the GRH, that uniformly for $|g| < \log x$,

$$A_g(x) = \frac{x}{\log x} \exp\left((B + o(1)) \frac{\log\log x}{\log\log\log x}\right)$$

as $x \to \infty$, where B is an explicitly given positive constant. The lower bound implicit in this result depended strongly on the work in [17]. The implicit upper bound is unconditional, since it had been shown in [3] in (1991) that

$$\frac{1}{x} \sum_{n \le x} \lambda(n) = \frac{x}{\log x} \exp\left((B + o(1)) \frac{\log\log x}{\log\log\log x}\right)$$

as $x \to \infty$.

For $A'_g(x)$, after work of Murata and work of Pappalardi [21], we have $A'_g(x) \sim c_g x$ assuming the GRH. A more uniform version of this result, including the calculation of the constants c_g was worked out in [12].

One can also average the averages, namely consider $A_g(x)$ or $A'_g(x)$ for g running through an interval. See [6], [9], [10], [18], [19] for results in this vein.

References

[1] J. S. Athreya and L. M. Fidkowski, Number theory, balls in boxes, and the asymptotic uniqueness of maximal discrete order statistics, Integers **0** (2000), article A3.

[2] P. D. T. A. Elliott, On the limiting distribution of $f(p+1)$ for non-negative additive functions, Acta Arith. **25** (1974), 259–264.

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

[4] A. Hildebrand, Additive and multiplicative functions on shifted primes, Proc. London Math. Soc. 3 **59** (1989), 209–232.

[5] C. Hooley, On Artin's conjecture, J. Reine Angew. Math. **225** (1967), 209–220.

[6] Y. Hu and C. Pomerance, The average order of elements in the multiplicative group of a finite field, Involve **5** (2012), 229–236.

[7] B. Huang and S. Li, Notes on the number of primitive λ-roots mod n and its multiplicative properties, Integers, to appear.

[8] I. Kátai, On distribution of arithmetical functions on the set prime plus one, Compositio Math. **19** (1968), 278–289.
[9] S. Kim, Average results on the order of a modulo p, J. Number Theory **169** (2016), 353–368.
[10] S. Kim, Some theorems on multiplicative orders modulo p on average, J. Number Theory **208** (2020), 180–207.
[11] P. Kirschenhofer and H. Prodinger, The number of winners in a discrete geometrically distributed random sample, Ann. Appl. Probab. **6** (1996), 687-694; Addendum, ibid. 8 (1998), 647.
[12] On a problem of Arnold: the average multiplicative order of given integer, P. Kurlberg and C. Pomerance, Algebra and Number Theory **7** (2013), 981–999.
[13] S. Li, On Artin's conjecture for composite moduli, Ph. D. dissertation, University of Georgia, 1998.
[14] S. Li, On the number of elements with maximal order in the multiplicative group modulo n, Acta Arith. **86** (1998), 113-132.
[15] S. Li, On extending Artin's conjecture to composite moduli, Mathematika **46** (1999), 373-390.
[16] S. Li, Artin's conjecture on average for composite moduli, J. Number Theory **84** (2000), 93–118.
[17] S. Li and C. Pomerance, On generalizing Artin's conjecture on primitive roots to composite moduli, J. Reine Angew. Math., **556** (2003), 205–224.
[18] S. Li and C. Pomerance, The Artin–Carmichael primitive root problem on average, Mathematika **55** (2009), 167–176.
[19] F. Luca. Some mean values related to average multiplicative orders of elements in finite fields, Ramanujan J., **9** (2005),33–44.
[20] G. Martin, The least prime primitive root and the shifted sieve, Acta Arith. **80** (1997), 277–288.
[21] F. Pappalardi, On Hooley's theorem with weights, Number theory, II (Rome, 1995). Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), 375–388.
[22] P. Péringuey, Sur une généralisation de la conjecture d'Artin parmi les presque-premiers, Bull. Soc. Math. France **152** (2024), 377–442.
[23] M. Rubinstein and P. Sarnak, Chebyshev's bias, Experiment. Math. **3** (1994), 173–197.
[24] I. E. Shparlinski. On some dynamical systems in finite fields and residue rings, Discrete Contin. Dyn. Syst. **17** (2007), 901–917.
[25] P. J. Stephens, An average result for Artin's conjecture, Mathematika **16** (1969), 178–188.

Department of Mathematics, Natural Sciences Division, University of Hawaii-Hilo, 200 W. Kawili Street, Hilo, HI 96720-4091
E-mail address: shuguang@hawaii.edu

Mathematics Department, Dartmouth College, Hanover, NH 03755
E-mail address: carlp@math.dartmouth.edu