Statistics of the multiplicative group

Greg Martin
University of British Columbia

UBC Number Theory Seminar
November 2, 2023

slides can be found on my web page
`www.math.ubc.ca/∼gerg/index.shtml?slides`

Outline

Introducing the multiplicative group

Notation

- For every positive integer n, the integers have a quotient ring $\mathbb{Z}/n\mathbb{Z}$ with n elements.
- If we ignore multiplication, we get the additive group $\mathbb{Z}_n^+$. It is always a cyclic group of order n.
- If we instead ignore addition: the multiplicative group $\mathbb{Z}_n^\times$ is the set $(\mathbb{Z}/n\mathbb{Z})^\times$ of invertible elements in $\mathbb{Z}/n\mathbb{Z}$ under its multiplication. It is some finite abelian group with $\phi(n)$ elements.

Overarching theme

Questions about the family $\{\mathbb{Z}_n^\times\}_{n=1}^\infty$ of multiplicative groups are usually analytic number theory opportunities in disguise.

The Euler phi-function

Definition

The Euler totient function $\phi(n)$ is the number of integers in $\{1, \dots, n\}$ that are relatively prime to n.

Statistics we care about

- The maximal order of $\phi(n)$ is $n-1$
- The minimal order of $\phi(n)$ is $(e^{-\gamma} + o(1))\dfrac{n}{\log\log n}$
- The average order of $\phi(n)$ is $\dfrac{6}{\pi^2}n$, meaning that

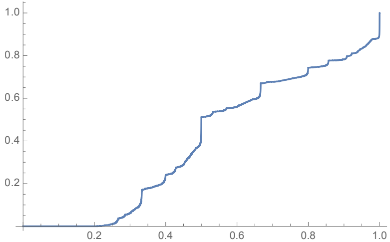
$$\sum_{n\le x} \phi(n) = \left(\frac{3}{\pi^2} + o(1)\right)x^2 = \sum_{n\le x} \frac{6}{\pi^2}n$$

What is the distribution of $\phi(n)$?

Since $\phi(n) \to \infty$, it doesn't have a limiting distribution as is. But if we normalize $\phi(n)$ by dividing it by n, we can obtain a limiting distribution.

The result

The graph shows the cumulative distribution function $F(t)$ for $\phi(n)/n$.



$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x \colon \frac{\phi(n)}{n} \le t \right\} = F(t)$$

An unusual function

$F(t)$ is continuous everywhere, but it is a singular function—its derivative equals 0 almost everywhere.

The structure of the multiplicative group

Other questions depend on the structure of $\mathbb{Z}_n^\times$, not just its size.

Square roots of unity

The number of solutions to $x^2 \equiv 1 \pmod{n}$ is $2^{\omega(n)}$ *when n is odd*.

- Here $\omega(n)$ is the number of distinct prime factors of n.

Theorem (Finch & M. & Sebah, 2010)

The average order of the number of solutions to $x^k \equiv 1 \pmod{n}$ is $\frac{1}{x}\sum_{n\le x} \#\{x^k \equiv 1 \pmod{n}\} \sim C_k(\log x)^{\tau(k)-1}$, where $\tau(k)$ is the number of positive divisors of k (and C_k is an explicit constant).

- Note: this is also the average order of the number of Dirichlet characters $\pmod{n}$ of order k

One canonical form: primary decomposition

Theorem

Every finite abelian group has a unique primary factor decomposition (or elementary divisor decomposition) as the direct sum of cyclic groups of prime-power order.

Example: $n = 11!$

$$\mathbb{Z}_{11!}^\times \cong \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_3^+ \oplus \mathbb{Z}_4^+ \oplus \mathbb{Z}_5^+ \oplus \mathbb{Z}_5^+ \oplus \mathbb{Z}_{27}^+ \oplus \mathbb{Z}_{64}^+$$

How do we get that?

It turns out to be straightforward to determine the primary decomposition of $\mathbb{Z}_n^\times$, using the Chinese remainder theorem and the fact that odd prime powers always have primitive roots.

- even prime powers are understood, but irritating

Primary decomposition example

Example: $n = 11! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$

By the Chinese remainder theorem,

$$\mathbb{Z}_{11!}^\times \cong \mathbb{Z}_{2^8}^\times \times \mathbb{Z}_{3^4}^\times \times \mathbb{Z}_{5^2}^\times \times \mathbb{Z}_7^\times \times \mathbb{Z}_{11}^\times.$$

For each odd prime power, $\mathbb{Z}_{p^r}^\times$ is cyclic of order $\phi(p^r)$:

$$\mathbb{Z}_{11!}^\times \cong (\mathbb{Z}_{64}^+ \oplus \mathbb{Z}_2^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+.$$

Again we use the Chinese remainder theorem on each factor:

$$\mathbb{Z}_{11!}^\times \cong (\mathbb{Z}_{64}^+ \oplus \mathbb{Z}_2^+) \oplus (\mathbb{Z}_{27}^+ \oplus \mathbb{Z}_2^+) \oplus (\mathbb{Z}_5^+ \oplus \mathbb{Z}_4^+) \oplus (\mathbb{Z}_3^+ \oplus \mathbb{Z}_2^+) \oplus (\mathbb{Z}_5^+ \oplus \mathbb{Z}_2^+).$$

Another canonical form: invariant factor decomposition

Theorem

Every finite abelian group has a unique invariant factor decomposition as the direct sum of cyclic groups $\mathbb{Z}_{d_1}^+, \dots, \mathbb{Z}_{d_k}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_k$.

Example: $n = 11!$

$$\begin{aligned}
\mathbb{Z}_{11!}^\times \cong\ & \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_4^+ \oplus \mathbb{Z}_{64}^+ \\
& \oplus \mathbb{Z}_3^+ \oplus \mathbb{Z}_{27}^+ \\
& \oplus \mathbb{Z}_5^+ \oplus \mathbb{Z}_5^+ \\
\cong\ & \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_{12}^+ \oplus \mathbb{Z}_{60}^+ \oplus \mathbb{Z}_{8640}^+
\end{aligned}$$

The Carmichael lambda-function

Invariant factor decomposition

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_k}^+ \text{ where } d_1 \mid d_2 \mid \cdots \mid d_k$$

The largest invariant factor

d_k equals the Carmichael function value $\lambda(n)$, which is the largest order of any element of $\mathbb{Z}_n^\times$ (the “exponent” of $\mathbb{Z}_n^\times$).

Theorem (Erdős & Pomerance, 1991)

For almost all integers n, we have $\lambda(n) = n/(\log n)^{\log\log\log n + O(1)}$.

- much smaller than $\phi(n) \gg n/\log\log n$

Theorem (M. & Pomerance, 2005)

$\lambda(\lambda(n)) = n/(\log n)^{(1+o(1))(\log\log\log n)^2}$ for almost all integers n.

The number of prime factors

Length of the invariant factor decomposition

If $\mathbb{Z}_n^\times \cong \mathbb{Z}_{d_1}^+ \oplus \cdots \oplus \mathbb{Z}_{d_k}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_k$, then $k = \omega(n)$ (the number of distinct prime factors of n) *when n is odd*.

The size of $\omega(n)$

- maximal order: $(1 + o(1))\dfrac{\log n}{\log\log n}$
- average order: $\dfrac{1}{x}\displaystyle\sum_{n \le x} \omega(n) \sim \log\log x$.

Its sibling

$\Omega(n)$: the number of prime factors of n counted with multiplicity.

- same average order as $\omega(n)$; maximal order $\dfrac{\log n}{\log 2}$

The number of prime factors

The Hardy–Ramanujan theorem (1917)

The normal order of $\omega(n)$ is $\log\log n$: for every $\varepsilon > 0$, the set $\{n \in \mathbb{N} : (1-\varepsilon)\log\log n < \omega(n) < (1+\varepsilon)\log\log n\}$ has density 1.

- $\omega(n) \sim \log\log n$ for almost all integers n

The Erdős–Kac theorem (1940)

$\omega(n)$ acts like a normal random variable with mean $\log\log n$ and variance $\log\log n$: the cumulative distribution function of $(\omega(n) - \log\log n)/\sqrt{\log\log n}$ is

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x : \frac{\omega(n) - \log\log n}{(\log\log n)^{1/2}} < t\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t} e^{-u^2/2}\,du.$$

- Both statements remain true with $\Omega(n)$ in place of $\omega(n)$

How many terms in the primary decomposition?

Exercise

If the finite abelian group G has m elements, then the number of terms in the primary decomposition of G is at least $\omega(m)$ and at most $\Omega(m)$. In particular, the length of the primary decomposition of $\mathbb{Z}_n^\times$ is between $\omega(\phi(n))$ and $\Omega(\phi(n))$.

Theorem (Erdős & Pomerance, 1985)

$\omega(\phi(n))$ and $\Omega(\phi(n))$ each acts like a normal random variable with mean $\frac{1}{2}(\log\log n)^2$ and variance $\frac{1}{3}(\log\log n)^3$:

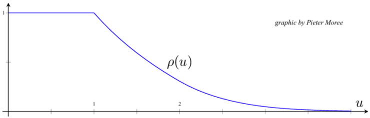
$$\frac{1}{x}\#\left\{n \le x \colon \frac{\omega(\phi(n)) - \frac{1}{2}(\log\log n)^2}{\sqrt{\frac{1}{3}(\log\log n)^3}} < t\right\} \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t} e^{-u^2/2}\,du.$$

Therefore the same is true of the length of the primary decomposition of $\mathbb{Z}_n^\times$.

The largest primary factor: a bit mysterious

What we do know

If $P(n)$ denotes the largest prime factor of n, then $\frac{\log n}{\log P(n)}$ has a cumulative distribution function $1-\rho(u)$, where ρ is the Dickman–de Bruijn function.



$$\rho'(u) = -\frac{\rho(u-1)}{u} \qquad (u>1)$$

What we expect

We should get the same distribution on shifted primes: $\frac{\log(p-1)}{\log P(p-1)}$.

But we don't even know that there are infinitely many p for which this is > 3.52. (Lichtman, 2022 preprint)

Largest primary factor of $\mathbb{Z}_n^\times \approx$ largest prime factor of $P(n)-1$.

- Precise conjecture can be made (essentially by Lamzouri, 2007)

The smallest invariant factor: statements

Most $\mathbb{Z}_n^\times$ have 2 as an invariant factor. In fact:

Theorem (Chang & M., 2020)

The number of integers $n \le x$ for which the least invariant factor of $\mathbb{Z}_n^\times$ does not equal 2 is $C\dfrac{x}{\sqrt{\log x}} + O\left(\dfrac{x}{(\log x)^{3/4-\varepsilon}}\right)$, where $C \approx 1.01782$ is given by

$$C = \frac{3}{2^{5/2}} \prod_{p\equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{1/2} + \frac{7}{2^{5/2}3^{3/4}} \prod_{p\equiv 5 \pmod 6} \left(1 - \frac{1}{p^2}\right)^{1/2}.$$

Further theorem

For any even $m \ge 4$, the number of integers $n \le x$ for which the least invariant factor of $\mathbb{Z}_n^\times$ equals m is $\sim C_m \dfrac{x}{(\log x)^{1-1/\phi(m)}}$ for some explicit constant C_m.

The smallest invariant factor: proof method

Application of the Selberg–Delange method

The Selberg–Delange method can be used to count integers whose prime factors all come from some set $\mathcal{S}$ of primes.

- The Dirichlet series $F_{\mathcal{S}}(s) = \sum_{\substack{n\in\mathbb{N} \\ p\mid n \implies p\in\mathcal{S}}} n^{-s} = \prod_{p\in\mathcal{S}} (1-p^{-s})^{-1}$ acts like a "fractional power of $\zeta(s)$": if $\mathcal{S}$ has density δ, then $F_{\mathcal{S}}(s)\zeta(s)^{-\delta}$ is analytic near $s=1$.
- Result: $\#\{n \le x : p \mid n \implies p \in \mathcal{S}\} \sim C_{\mathcal{S}} x/(\log x)^{1-\delta}$

Lemma

Fix an even number $m \ge 4$. The least invariant factor of $\mathbb{Z}_n^\times$ is a multiple of m if and only if all of the following conditions hold:

1. *for primes $p \nmid m$: if $p \mid n$ then we must have $p \equiv 1 \pmod{m}$;*
2. *$4 \nmid n$; and (some condition for odd primes $p \mid m$)*

The smallest primary factor: statements

Most $\mathbb{Z}_n^\times$ have 2 as a primary factor. In fact:

Theorem (M. & Nguyen, in progress)

The number of integers $n \le x$ for which the least primary factor of $\mathbb{Z}_n^\times$ does not equal 2 is $D\dfrac{x}{\sqrt{\log x}} + O\left(\dfrac{x}{(\log x)^{2/3}}\right)$*, where* $D \approx 0.490694$ *is given by* $D = \dfrac{3}{2^{5/2}} \prod_{p \equiv 3 \pmod 4} \left(1 - \dfrac{1}{p^2}\right)^{1/2}$.

Further theorem

For any prime power $q \ge 3$, the number of integers $n \le x$ for which the least primary factor of $\mathbb{Z}_n^\times$ equals q is $\sim D_q \dfrac{x}{(\log x)^{\beta_q}}$ for some explicit constants D_q and β_q.

- uses the Selberg–Delange formulation in Chang & M.

Universal profile of invariant factors (M. & Simpson)

Almost all $\mathbb{Z}_n^\times$ have among their invariant factors:

- $\sim \frac{1}{2} \log\log n$ copies of $\mathbb{Z}_2^+$,
- $\sim \frac{1}{4} \log\log n$ copies of $\mathbb{Z}_{12}^+$,
- $\sim \frac{1}{12} \log\log n$ copies of $\mathbb{Z}_{120}^+$,
- $\sim \frac{1}{24} \log\log n$ copies of $\mathbb{Z}_{2520}^+$,
- $\sim \frac{1}{40} \log\log n$ copies of $\mathbb{Z}_{5040}^+$,
- $\sim \frac{1}{60} \log\log n$ copies of $\mathbb{Z}_{55440}^+$, ...

These have (interesting) distributions as well

For example, the number of copies of $\mathbb{Z}_2^+$ has mean and variance $\frac{1}{2} \log\log n$ ... but the normalized number of copies doesn't tend to a normal random variable, but rather the minimum of two normal random variables!

Prohibiting a subgroup

Problem

Let q be an odd prime. How many multiplicative groups $\mathbb{Z}_n^\times$ have no subgroup isomorphic to $\mathbb{Z}_q^+$?

Translation to number theory

$\mathbb{Z}_n^\times$ has no subgroup isomorphic to $\mathbb{Z}_q^+$ if and only if both $p \mid n \implies p \not\equiv 1 \pmod{q}$ and $q^2 \nmid n$.

Counting such integers is a classic application of the Selberg–Delange method; their counting function will be asymptotically $E_q x/(\log x)^{1/\phi(q)}$ for some constant E_q.

Prescribing a subgroup

Definition (q is an odd prime throughout)

The q-Sylow subgroup of a finite abelian group G is the largest subgroup of G whose cardinality is a power of q.

- "G has no subgroup isomorphic to $\mathbb{Z}_q^+$" is the same as "the q-Sylow subgroup of G is trivial"

So the classical question of counting integers without prime factors congruent to $1 \pmod q$ can be generalized to counting integers with a specific q-Sylow subgroup. (idea: Colin Weir)

Theorem (Downey & M., 2019)

If $G = \mathbb{Z}^+_{q^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}^+_{q^{\alpha_k}}$, then the number of integers $n \le x$ such that the q-Sylow subgroup of $\mathbb{Z}_n^\times$ equals G is asymptotically $E_G \dfrac{x(\log\log x)^k}{(\log x)^{1/(q-1)}}$ for some explicit constant E_G.

How many subgroups? (I)

Definition

Let $I(n)$ denote the number of subgroups of $\mathbb{Z}_n^\times$ up to isomorphism.

M. & Troupe (2020) showed that $\frac{\log I(n)}{\log 2}$ is between $\omega(\phi(n))$ and $\Omega(\phi(n))$. An immediate consequence:

Theorem (Erdős & Pomerance, 1985)

$\omega(\phi(n))$ and $\Omega(\phi(n))$ each acts like a normal random variable with mean $\frac{1}{2}(\log\log n)^2$ and variance $\frac{1}{3}(\log\log n)^3$:

$$\frac{1}{x}\#\left\{n \le x : \frac{\omega(\phi(n)) - \frac{1}{2}(\log\log n)^2}{\sqrt{\frac{1}{3}(\log\log n)^3}} < t\right\} \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t} e^{-u^2/2}\,du.$$

Therefore the same is true of $\frac{\log I(n)}{\log 2}$.

How many subgroups? (II)

Definition

Let $G(n)$ denote the number of subgroups of $\mathbb{Z}_n^\times$, counting each subgroup separately even if some are isomorphic to others.

Theorem (M. & Troupe, 2020)

$\log G(n)$ acts like a normal random variable with mean $A(\log\log n)^2$ and variance $B(\log\log n)^3$, for certain $A, B > 0$:

$$\frac{1}{x}\#\left\{n \le x\colon \frac{\log G(n) - A(\log\log n)^2}{\sqrt{B(\log\log n)^3}} < t\right\} \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{t} e^{-u^2/2}\,du.$$

Maximal order

There are infinitely many n for which $\log G(n) > \frac{1}{17}\frac{(\log n)^2}{\log\log n}$.

- In particular, $G(n) \gg n^{2023!}$ infinitely often!

Your favourite group

A nice exercise

Show that any given finite abelian group G is a subgroup of $\mathbb{Z}_n^\times$ for infinitely many positive integers n.

Proof

Write $G \cong \mathbb{Z}_{d_1}^+ \oplus \cdots \oplus \mathbb{Z}_{d_k}^+$. There are infinitely many primes $p_j \equiv 1 \pmod{d_j}$, and for each such prime, $\mathbb{Z}_{d_j}^+$ is a subgroup of $\mathbb{Z}_{p_j}^\times \cong \mathbb{Z}_{p_j-1}^+$. Then G is a subgroup of $\mathbb{Z}_{p_1\cdots p_k}^\times \cong \mathbb{Z}_{p_1}^\times \times \cdots \times \mathbb{Z}_{p_k}^\times$.

Project for a future collaboration

But more is true: G should be a subgroup of $\mathbb{Z}_n^\times$ for almost all integers n! An asymptotic formula for the exceptions should follow from the techniques in my paper with Downey.