Subgroups of the multiplicative group

Greg Martin
University of British Columbia

joint work with Lee Troupe

Analytic Number Theory
2017 CMS Winter Meeting
University of Waterloo
December 10, 2017

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

Outline

1. Background, and distribution of (ϕ-)additive functions
2. Results on the distribution of the number of subgroups of $\mathbb{Z}_n^\times$
3. Outline of the proofs

Our objects of study

Definition

The "multiplicative group" (or unit group) modulo n is $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of reduced residue classes under multiplication $(\mathrm{mod}\ n)$.

$\mathbb{Z}_n^\times$ is some finite abelian group with $\phi(n)$ elements (usually not cyclic). Questions about its structure often turn into number theory (example: its exponent is the Carmichael λ-function).

Overarching question (I heard it from Shparlinski)

How many subgroups does $\mathbb{Z}_n^\times$ usually have?

Notation (used throughout the talk)

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups (that is, subgroups not up to isomorphism).

Our objects of study

Definition

The "multiplicative group" (or unit group) modulo n is $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of reduced residue classes under multiplication $\pmod{n}$.

$\mathbb{Z}_n^\times$ is some finite abelian group with $\phi(n)$ elements (usually not cyclic). Questions about its structure often turn into number theory (example: its exponent is the Carmichael λ-function).

Overarching question (I heard it from Shparlinski)

How many subgroups does $\mathbb{Z}_n^\times$ usually have?

Notation (used throughout the talk)

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups (that is, subgroups not up to isomorphism).

Our objects of study

Definition

The "multiplicative group" (or unit group) modulo n is $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of reduced residue classes under multiplication $(\mathrm{mod}\ n)$.

$\mathbb{Z}_n^\times$ is some finite abelian group with $\phi(n)$ elements (usually not cyclic). Questions about its structure often turn into number theory (example: its exponent is the Carmichael λ-function).

Overarching question (I heard it from Shparlinski)

How many subgroups does $\mathbb{Z}_n^\times$ usually have?

Notation (used throughout the talk)

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups (that is, subgroups not up to isomorphism).

Our objects of study

Definition

The “multiplicative group” (or unit group) modulo n is $\mathbb{Z}_n^\times = (\mathbb{Z}/n\mathbb{Z})^\times$, the group of reduced residue classes under multiplication $\pmod n$.

$\mathbb{Z}_n^\times$ is some finite abelian group with $\phi(n)$ elements (usually not cyclic). Questions about its structure often turn into number theory (example: its exponent is the Carmichael λ-function).

Overarching question (I heard it from Shparlinski)

How many subgroups does $\mathbb{Z}_n^\times$ usually have?

Notation (used throughout the talk)

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups (that is, subgroups not up to isomorphism).

Distribution results: different strengths

By way of analogy: some historical results about the distribution of $\omega(n)$, the number of distinct prime factors of n.

- The average value of $\omega(n)$ is $\log\log n$.

  — requires an asymptotic formula for $\sum_{n\le x}\omega(n)$
- The normal order (typical size) of $\omega(n)$ is $\log\log n$.

  — requires estimate for variance $\sum_{n\le x}\big(\omega(n)-\log\log n\big)^2$
- Erdős–Kac theorem: $\omega(n)$ is asymptotically distributed like a normal random variable with mean $\log\log n$ and variance $\log\log n$. (More precise statement on next slide.)

  — requires asymptotic formulas for all central moments $\sum_{n\le x}\big(\omega(n)-\log\log n\big)^k$

Distribution results: different strengths

By way of analogy: some historical results about the distribution of $\omega(n)$, the number of distinct prime factors of n.

- The average value of $\omega(n)$ is $\log\log n$.

  — requires an asymptotic formula for $\sum_{n\le x}\omega(n)$
- The normal order (typical size) of $\omega(n)$ is $\log\log n$.

  — requires estimate for variance $\sum_{n\le x}\big(\omega(n)-\log\log n\big)^2$
- Erdős–Kac theorem: $\omega(n)$ is asymptotically distributed like a normal random variable with mean $\log\log n$ and variance $\log\log n$. (More precise statement on next slide.)

  — requires asymptotic formulas for all central moments $\sum_{n\le x}\big(\omega(n)-\log\log n\big)^k$

Distribution results: different strengths

By way of analogy: some historical results about the distribution of $\omega(n)$, the number of distinct prime factors of n.

- The average value of $\omega(n)$ is $\log\log n$.

  — requires an asymptotic formula for $\sum_{n\le x}\omega(n)$
- The normal order (typical size) of $\omega(n)$ is $\log\log n$.

  — requires estimate for variance $\sum_{n\le x}\big(\omega(n)-\log\log n\big)^2$
- Erdős–Kac theorem: $\omega(n)$ is asymptotically distributed like a normal random variable with mean $\log\log n$ and variance $\log\log n$. (More precise statement on next slide.)

  — requires asymptotic formulas for all central moments $\sum_{n\le x}\big(\omega(n)-\log\log n\big)^k$

Distribution results: different strengths

By way of analogy: some historical results about the distribution of $\omega(n)$, the number of distinct prime factors of n.

- The average value of $\omega(n)$ is $\log\log n$.

  — requires an asymptotic formula for $\sum_{n\le x} \omega(n)$
- The normal order (typical size) of $\omega(n)$ is $\log\log n$.

  — requires estimate for variance $\sum_{n\le x} \big(\omega(n) - \log\log n\big)^2$
- Erdős–Kac theorem: $\omega(n)$ is asymptotically distributed like a normal random variable with mean $\log\log n$ and variance $\log\log n$. (More precise statement on next slide.)

  — requires asymptotic formulas for all central moments $\sum_{n\le x} \big(\omega(n) - \log\log n\big)^k$

Erdős–Kac laws

Definition

A function $f(n)$ satisfies an Erdős–Kac law with mean $\mu(n)$ and variance $\sigma^2(n)$ if

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x\colon \frac{f(n)-\mu(n)}{\sigma(n)} < u\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt$$

for every real number u.

Standard notation

$\omega(n)$ is the number of distinct prime factors of n.
$\Omega(n)$ is the number of prime factors of n counted with multiplicity.

Theorem (Erdős–Kac, 1940)

Both $\omega(n)$ and $\Omega(n)$ satisfy Erdős–Kac laws with mean $\log\log n$ and variance $\log\log n$.

Erdős–Kac laws

Definition

A function $f(n)$ satisfies an Erdős–Kac law with mean $\mu(n)$ and variance $\sigma^2(n)$ if

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x \colon \frac{f(n)-\mu(n)}{\sigma(n)} < u\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt$$

for every real number u.

Standard notation

$\omega(n)$ is the number of distinct prime factors of n.
$\Omega(n)$ is the number of prime factors of n counted with multiplicity.

Theorem (Erdős–Kac, 1940)

Both $\omega(n)$ and $\Omega(n)$ satisfy Erdős–Kac laws with mean $\log\log n$ and variance $\log\log n$.

Erdős–Kac laws

Definition

A function $f(n)$ satisfies an Erdős–Kac law with mean $\mu(n)$ and variance $\sigma^2(n)$ if

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x \colon \frac{f(n)-\mu(n)}{\sigma(n)} < u \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2} \, dt$$

for every real number u.

Standard notation

$\omega(n)$ is the number of distinct prime factors of n.
$\Omega(n)$ is the number of prime factors of n counted with multiplicity.

Theorem (Erdős–Kac, 1940)

Both $\omega(n)$ and $\Omega(n)$ satisfy Erdős–Kac laws with mean $\log\log n$ and variance $\log\log n$.

Erdős–Kac laws

Definition

A function $f(n)$ satisfies an Erdős–Kac law with mean $\mu(n)$ and variance $\sigma^2(n)$ if

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x\colon \frac{f(n)-\mu(n)}{\sigma(n)} < u\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt$$

for every real number u.

Standard notation

$\omega(n)$ is the number of distinct prime factors of n.
$\Omega(n)$ is the number of prime factors of n counted with multiplicity.

Theorem (Erdős–Kac, 1940)

Both $\omega(n)$ and $\Omega(n)$ satisfy Erdős–Kac laws with mean $\log\log n$ and variance $\log\log n$.

Erdős–Kac laws

Definition

A function $f(n)$ satisfies an Erdős–Kac law with mean $\mu(n)$ and variance $\sigma^2(n)$ if

$$\lim_{x\to\infty} \frac{1}{x}\#\left\{n \le x \colon \frac{f(n)-\mu(n)}{\sigma(n)} < u\right\} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt$$

for every real number u.

Standard notation

$\omega(n)$ is the number of distinct prime factors of n.
$\Omega(n)$ is the number of prime factors of n counted with multiplicity.

Theorem (Erdős–Kac, 1940)

Both $\omega(n)$ and $\Omega(n)$ satisfy Erdős–Kac laws with mean $\log\log n$ and variance $\log\log n$.

Other functions with Erdős–Kac laws

The paper of Erdős–Kac establishes these normal-distribution laws for a large class of additive functions: if $n = p_1^{r_1} \cdots p_k^{r_k}$, then $f(n) = f(p_1^{r_1}) + \cdots + f(p_k^{r_k})$. Examples of non-additive functions:

Liu (2007)

On GRH, $\omega(\#E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean $\log\log p$ and variance $\log\log p$.

Erdős–Pomerance (1985)

$\omega(\phi(n))$ and $\Omega(\phi(n))$ satisfy Erdős– Kac laws with mean $\frac{1}{2}(\log\log n)^2$ and variance $\frac{1}{3}(\log\log n)^3$.

$\Omega(\phi(n))$ is not additive, but is "ϕ-additive": if $\phi(n) = p_1^{r_1} \cdots p_k^{r_k}$, then $\Omega(\phi(n)) = \Omega(p_1^{r_1}) + \cdots + \Omega(p_k^{r_k})$.

Other functions with Erdős–Kac laws

The paper of Erdős–Kac establishes these normal-distribution laws for a large class of additive functions: if $n = p_1^{r_1} \cdots p_k^{r_k}$, then $f(n) = f(p_1^{r_1}) + \cdots + f(p_k^{r_k})$. Examples of non-additive functions:

Liu (2007)

On GRH, $\omega(\#E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean $\log\log p$ and variance $\log\log p$.

Erdős–Pomerance (1985)

$\omega(\phi(n))$ and $\Omega(\phi(n))$ satisfy Erdős– Kac laws with mean $\frac{1}{2}(\log\log n)^2$ and variance $\frac{1}{3}(\log\log n)^3$.

$\Omega(\phi(n))$ is not additive, but is "ϕ-additive": if $\phi(n) = p_1^{r_1} \cdots p_k^{r_k}$, then $\Omega(\phi(n)) = \Omega(p_1^{r_1}) + \cdots + \Omega(p_k^{r_k})$.

Other functions with Erdős–Kac laws

The paper of Erdős–Kac establishes these normal-distribution laws for a large class of additive functions: if $n = p_1^{r_1} \cdots p_k^{r_k}$, then $f(n) = f(p_1^{r_1}) + \cdots + f(p_k^{r_k})$. Examples of non-additive functions:

Liu (2007)

On GRH, $\omega(\#E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean $\log\log p$ and variance $\log\log p$.

Erdős–Pomerance (1985)

$\omega(\phi(n))$ and $\Omega(\phi(n))$ satisfy Erdős– Kac laws with mean $\frac{1}{2}(\log\log n)^2$ and variance $\frac{1}{3}(\log\log n)^3$.

$\Omega(\phi(n))$ is not additive, but is "ϕ-additive": if $\phi(n) = p_1^{r_1} \cdots p_k^{r_k}$, then $\Omega(\phi(n)) = \Omega(p_1^{r_1}) + \cdots + \Omega(p_k^{r_k})$.

Other functions with Erdős–Kac laws

The paper of Erdős–Kac establishes these normal-distribution laws for a large class of additive functions: if $n = p_1^{r_1} \cdots p_k^{r_k}$, then $f(n) = f(p_1^{r_1}) + \cdots + f(p_k^{r_k})$. Examples of non-additive functions:

Liu (2007)

On GRH, $\omega(\#E(\mathbb{F}_p))$ satisfies an Erdős–Kac law with mean $\log\log p$ and variance $\log\log p$.

Erdős–Pomerance (1985)

$\omega(\phi(n))$ and $\Omega(\phi(n))$ satisfy Erdős– Kac laws with mean $\frac{1}{2}(\log\log n)^2$ and variance $\frac{1}{3}(\log\log n)^3$.

$\Omega(\phi(n))$ is not additive, but is "ϕ-additive": if $\phi(n) = p_1^{r_1} \cdots p_k^{r_k}$, then $\Omega(\phi(n)) = \Omega(p_1^{r_1}) + \cdots + \Omega(p_k^{r_k})$.

The number of subgroups has a similar property

Reminder of notation

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups.

Every finite abelian group is the direct sum of its p-Sylow subgroups, so consequently:

If $G_p(n)$ denotes the number of subgroups of the p-Sylow subgroup of $\mathbb{Z}_n^\times$, then $G(n) = \prod_{p \mid \#\mathbb{Z}_n^\times} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

And similarly for $I(n)$.

In particular, both $I(n)$ and $G(n)$ are “ϕ-multiplicative” functions; so we might hope to get strong distributional information for the ϕ-additive functions $\log I(n)$ and $\log G(n)$.

The number of subgroups has a similar property

Reminder of notation

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups.

Every finite abelian group is the direct sum of its p-Sylow subgroups, so consequently:

If $G_p(n)$ denotes the number of subgroups of the p-Sylow subgroup of $\mathbb{Z}_n^\times$, then $G(n) = \displaystyle\prod_{p \mid \#\mathbb{Z}_n^\times} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

And similarly for $I(n)$.

In particular, both $I(n)$ and $G(n)$ are "ϕ-multiplicative" functions; so we might hope to get strong distributional information for the ϕ-additive functions $\log I(n)$ and $\log G(n)$.

The number of subgroups has a similar property

Reminder of notation

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups.

Every finite abelian group is the direct sum of its p-Sylow subgroups, so consequently:

If $G_p(n)$ denotes the number of subgroups of the p-Sylow subgroup of $\mathbb{Z}_n^\times$, then $G(n) = \prod_{p \mid \#\mathbb{Z}_n^\times} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

And similarly for $I(n)$.

In particular, both $I(n)$ and $G(n)$ are "ϕ-multiplicative" functions; so we might hope to get strong distributional information for the ϕ-additive functions $\log I(n)$ and $\log G(n)$.

The number of subgroups has a similar property

Reminder of notation

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups.

Every finite abelian group is the direct sum of its p-Sylow subgroups, so consequently:

If $G_p(n)$ denotes the number of subgroups of the p-Sylow subgroup of $\mathbb{Z}_n^\times$, then $G(n) = \prod_{p \mid \#\mathbb{Z}_n^\times} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

And similarly for $I(n)$.

In particular, both $I(n)$ and $G(n)$ are "ϕ-multiplicative" functions; so we might hope to get strong distributional information for the ϕ-additive functions $\log I(n)$ and $\log G(n)$.

The number of subgroups has a similar property

Reminder of notation

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$.
$G(n)$ is the number of subsets of $\mathbb{Z}_n^\times$ that are subgroups.

Every finite abelian group is the direct sum of its p-Sylow subgroups, so consequently:

If $G_p(n)$ denotes the number of subgroups of the p-Sylow subgroup of $\mathbb{Z}_n^\times$, then $G(n) = \displaystyle\prod_{p \mid \#\mathbb{Z}_n^\times} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

And similarly for $I(n)$.

In particular, both $I(n)$ and $G(n)$ are "ϕ-multiplicative" functions; so we might hope to get strong distributional information for the ϕ-additive functions $\log I(n)$ and $\log G(n)$.

Erdős–Kac laws for the number of subgroups

Theorem (M.-Troupe, submitted)

$\log I(n)$ *satisfies an Erdős–Kac law with mean* $\frac{\log 2}{2}(\log\log n)^2$ *and variance* $\frac{\log 2}{3}(\log\log n)^3$.

How did we prove this?

We showed that $\omega(\phi(n))\log 2 \le \log I(n) \le \Omega(\phi(n))\log 2$, and then quoted Erdős–Pomerance. $\square$

Theorem (M.-Troupe, submitted)

$\log G(n)$ *satisfies an Erdős–Kac law with mean* $A(\log\log n)^2$ *and variance* $C(\log\log n)^3$, *for certain constants* A *and* C.

$\frac{\log 2}{2} \approx 0.34657$ while $A \approx 0.72109$, so typically $G(n) \approx I(n)^{2.08}$.

Erdős–Kac laws for the number of subgroups

Theorem (M.-Troupe, submitted)

$\log I(n)$ *satisfies an Erdős–Kac law with mean* $\frac{\log 2}{2}(\log\log n)^2$ *and variance* $\frac{\log 2}{3}(\log\log n)^3$.

How did we prove this?

We showed that $\omega(\phi(n))\log 2 \le \log I(n) \le \Omega(\phi(n))\log 2$, and then quoted Erdős–Pomerance. $\square$

Theorem (M.-Troupe, submitted)

$\log G(n)$ *satisfies an Erdős–Kac law with mean* $A(\log\log n)^2$ *and variance* $C(\log\log n)^3$*, for certain constants* A *and* C.

$\frac{\log 2}{2} \approx 0.34657$ while $A \approx 0.72109$, so typically $G(n) \approx I(n)^{2.08}$.

Erdős–Kac laws for the number of subgroups

Theorem (M.-Troupe, submitted)

$\log I(n)$ *satisfies an Erdős–Kac law with mean* $\frac{\log 2}{2}(\log\log n)^2$ *and variance* $\frac{\log 2}{3}(\log\log n)^3$.

How did we prove this?

We showed that $\omega(\phi(n))\log 2 \le \log I(n) \le \Omega(\phi(n))\log 2$, and then quoted Erdős–Pomerance. $\square$

Theorem (M.-Troupe, submitted)

$\log G(n)$ *satisfies an Erdős–Kac law with mean* $A(\log\log n)^2$ *and variance* $C(\log\log n)^3$*, for certain constants* A *and* C.

$\frac{\log 2}{2} \approx 0.34657$ while $A \approx 0.72109$, so typically $G(n) \approx I(n)^{2.08}$.

Erdős–Kac laws for the number of subgroups

Theorem (M.-Troupe, submitted)

$\log I(n)$ *satisfies an Erdős–Kac law with mean* $\frac{\log 2}{2}(\log\log n)^2$ *and variance* $\frac{\log 2}{3}(\log\log n)^3$.

How did we prove this?

We showed that $\omega(\phi(n))\log 2 \le \log I(n) \le \Omega(\phi(n))\log 2$, and then quoted Erdős–Pomerance. $\square$

Theorem (M.-Troupe, submitted)

$\log G(n)$ *satisfies an Erdős–Kac law with mean* $A(\log\log n)^2$ *and variance* $C(\log\log n)^3$, *for certain constants* A *and* C.

$\frac{\log 2}{2} \approx 0.34657$ while $A \approx 0.72109$, so typically $G(n) \approx I(n)^{2.08}$.

We had to look at these constants, so you do too

Definition

$$A_0 = \frac{1}{4} \sum_p \frac{p^2 \log p}{(p-1)^3 (p+1)}$$

$$A = \frac{\log 2}{2} + A_0 \approx 0.72109$$

$$B = \frac{1}{4} \sum_p \frac{p^3 (p^4 - p^3 - p^3 - p - 1)(\log p)^2}{(p-1)^6 (p+1)^2 (p^2 + p + 1)}$$

$$C = \frac{(\log 2)^2}{3} + 2A_0 \log 2 + 4A_0^2 + B \approx 3.924$$

(The two sums are convergent sums over all primes p.)

How many subgroups can there be?

Theorem (M.-Troupe, submitted)

The order of magnitude of the maximal order of $\log I(n)$ *is* $\log n/\log\log n$. *More precisely,*

$$\frac{\log 2}{5}\frac{\log x}{\log\log x} \lesssim \max_{n\le x}\big(\log I(n)\big) \lesssim \pi\sqrt{\frac{2}{3}}\frac{\log x}{\log\log x}.$$

Theorem (M.-Troupe, submitted)

The order of magnitude of the maximal order of $\log G(n)$ *is* $(\log n)^2/\log\log n$. *More precisely,*

$$\frac{1}{16}\frac{(\log x)^2}{\log\log x} \lesssim \max_{n\le x}\big(\log G(n)\big) \lesssim \frac{1}{4}\frac{(\log x)^2}{\log\log x}.$$

Consequence: $G(n)$ can be superpolynomially large

There are infinitely many integers n with $G(n) > n^{2017!}$ …

How many subgroups can there be?

Theorem (M.-Troupe, submitted)

The order of magnitude of the maximal order of $\log I(n)$ *is* $\log n/\log\log n$. *More precisely,*

$$\frac{\log 2}{5}\frac{\log x}{\log\log x} \lesssim \max_{n\le x}\big(\log I(n)\big) \lesssim \pi\sqrt{\frac{2}{3}}\frac{\log x}{\log\log x}.$$

Theorem (M.-Troupe, submitted)

The order of magnitude of the maximal order of $\log G(n)$ *is* $(\log n)^2/\log\log n$. *More precisely,*

$$\frac{1}{16}\frac{(\log x)^2}{\log\log x} \lesssim \max_{n\le x}\big(\log G(n)\big) \lesssim \frac{1}{4}\frac{(\log x)^2}{\log\log x}.$$

Consequence: $G(n)$ can be superpolynomially large

There are infinitely many integers n with $G(n) > n^{2017!}$ …

How many subgroups can there be?

Theorem (M.-Troupe, submitted)

The order of magnitude of the maximal order of $\log I(n)$ *is* $\log n / \log\log n$. *More precisely,*

$$\frac{\log 2}{5} \frac{\log x}{\log\log x} \lesssim \max_{n \le x} \big(\log I(n) \big) \lesssim \pi \sqrt{\frac{2}{3}} \frac{\log x}{\log\log x}.$$

Theorem (M.-Troupe, submitted)

The order of magnitude of the maximal order of $\log G(n)$ *is* $(\log n)^2 / \log\log n$. *More precisely,*

$$\frac{1}{16} \frac{(\log x)^2}{\log\log x} \lesssim \max_{n \le x} \big(\log G(n) \big) \lesssim \frac{1}{4} \frac{(\log x)^2}{\log\log x}.$$

Consequence: $G(n)$ can be superpolynomially large

There are infinitely many integers n with $G(n) > n^{2017!}$ …

Finite abelian groups and partitions

Facts about finite abelian p-groups

- Every finite abelian group of size p^m can be written uniquely as $\mathbb{Z}_{p^{\boldsymbol{\alpha}}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_\ell}}$ for some partition $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_\ell)$ of m (so $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_\ell$).
- So the number of isomorphism classes of subgroups of $\mathbb{Z}_{p^\alpha}$ is exactly the number of subpartitions $\beta \preceq \alpha$ …

… which is somewhere between 2 and 2^m inclusive.

In other words:

$\log \#\{$subpartitions of $\alpha\}$ is between $\log 2$ and $m \log 2$.

Finite abelian groups and partitions

Facts about finite abelian p-groups

- Every finite abelian group of size p^m can be written uniquely as $\mathbb{Z}_{p^{\boldsymbol{\alpha}}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_\ell}}$ for some partition $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_\ell)$ of m (so $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_\ell$).
- So the number of isomorphism classes of subgroups of $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ is exactly the number of subpartitions $\boldsymbol{\beta} \preceq \boldsymbol{\alpha}$ ...

... which is somewhere between 2 and 2^m inclusive.

In other words:

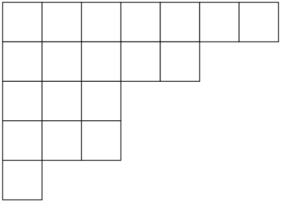
$\log \#\{\text{subpartitions of } \alpha\}$ is between $\log 2$ and $m \log 2$.

Finite abelian groups and partitions

Facts about finite abelian p-groups

- Every finite abelian group of size p^m can be written uniquely as $\mathbb{Z}_{p^{\boldsymbol\alpha}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_\ell}}$ for some partition $\boldsymbol\alpha = (\alpha_1, \alpha_2, \dots, \alpha_\ell)$ of m (so $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_\ell$).
- So the number of isomorphism classes of subgroups of $\mathbb{Z}_{p^{\boldsymbol\alpha}}$ is exactly the number of subpartitions $\boldsymbol\beta \preceq \boldsymbol\alpha$ …

… which is somewhere between 2 and 2^m inclusive.



In other words:

$\log \#\{\text{subpartitions of } \alpha\}$ is between $\log 2$ and $m \log 2$.

Finite abelian groups and partitions

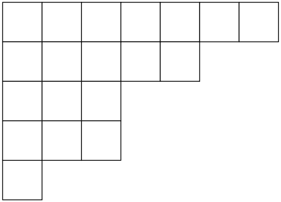
Facts about finite abelian p-groups

- Every finite abelian group of size p^m can be written uniquely as $\mathbb{Z}_{p^{\boldsymbol\alpha}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \mathbb{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_\ell}}$ for some partition $\boldsymbol\alpha = (\alpha_1, \alpha_2, \dots, \alpha_\ell)$ of m (so $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_\ell$).
- So the number of isomorphism classes of subgroups of $\mathbb{Z}_{p^{\boldsymbol\alpha}}$ is exactly the number of subpartitions $\boldsymbol\beta \preceq \boldsymbol\alpha$ …

… which is somewhere between 2 and 2^m inclusive.

In other words:

$\log \#\{$subpartitions of $\boldsymbol\alpha\}$ is between $\log 2$ and $m \log 2$.



Application to distribution of $I(n)$

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $\mathbb{Z}_n^\times \cong \bigoplus_{p|\phi(n)} \mathbb{Z}_{p^{\boldsymbol{\alpha}(p)}}$ for some partitions $\boldsymbol{\alpha}(p)$ of $m(p)$.

Then $\log I(n) = \sum_{p|\phi(n)} \log \#\{$subpartitions of $\alpha_p\}$ and hence

$$\sum_{p|\phi(n)} \log 2 \le \log I(n) \le \sum_{p|\phi(n)} m(p) \log 2$$

$$\omega(\phi(n)) \log 2 \le \log I(n) \le \Omega(\phi(n)) \log 2$$

Upper bound seems very wasteful, yet still good enough!

"Anatomy of integers" techniques show: most primes dividing $\phi(n)$ do so only once.

Application to distribution of $I(n)$

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $\mathbb{Z}_n^\times \cong \bigoplus_{p|\phi(n)} \mathbb{Z}_{p^{\alpha(p)}}$ for some partitions $\alpha(p)$ of $m(p)$.

Then $\log I(n) = \sum_{p|\phi(n)} \log \#\{\text{subpartitions of } \alpha_p\}$ and hence

$$\sum_{p|\phi(n)} \log 2 \le \log I(n) \le \sum_{p|\phi(n)} m(p) \log 2$$

$$\omega(\phi(n)) \log 2 \le \log I(n) \le \Omega(\phi(n)) \log 2$$

Upper bound seems very wasteful, yet still good enough!

"Anatomy of integers" techniques show: most primes dividing $\phi(n)$ do so only once.

Application to distribution of $I(n)$

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $\mathbb{Z}_n^\times \cong \bigoplus_{p|\phi(n)} \mathbb{Z}_{p^{\alpha(p)}}$ for some partitions $\alpha(p)$ of $m(p)$.

Then $\log I(n) = \sum_{p|\phi(n)} \log \#\{\text{subpartitions of } \alpha_p\}$ and hence

$$\sum_{p|\phi(n)} \log 2 \le \log I(n) \le \sum_{p|\phi(n)} m(p) \log 2$$

$$\omega(\phi(n)) \log 2 \le \log I(n) \le \Omega(\phi(n)) \log 2$$

Upper bound seems very wasteful, yet still good enough!

"Anatomy of integers" techniques show: most primes dividing $\phi(n)$ do so only once.

Application to distribution of $I(n)$

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$

More notation

Let $\phi(n) = \prod_{p\mid\phi(n)} p^{m(p)}$, so that $\mathbb{Z}_n^\times \cong \bigoplus_{p\mid\phi(n)} \mathbb{Z}_{p^{\boldsymbol\alpha(p)}}$ for some partitions $\boldsymbol\alpha(p)$ of $m(p)$.

Then $\log I(n) = \sum_{p\mid\phi(n)} \log \#\{\text{subpartitions of } \boldsymbol\alpha_p\}$ and hence

$$\sum_{p\mid\phi(n)} \log 2 \le \log I(n) \le \sum_{p\mid\phi(n)} m(p) \log 2$$

$$\omega(\phi(n)) \log 2 \le \log I(n) \le \Omega(\phi(n)) \log 2$$

Upper bound seems very wasteful, yet still good enough!

"Anatomy of integers" techniques show: most primes dividing $\phi(n)$ do so only once.

Application to distribution of $I(n)$

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $\mathbb{Z}_n^\times \cong \bigoplus_{p|\phi(n)} \mathbb{Z}_{p^{\boldsymbol{\alpha}(p)}}$ for some partitions $\boldsymbol{\alpha}(p)$ of $m(p)$.

Then $\log I(n) = \sum_{p|\phi(n)} \log \#\{\text{subpartitions of } \boldsymbol{\alpha}_p\}$ and hence

$$\sum_{p|\phi(n)} \log 2 \le \log I(n) \le \sum_{p|\phi(n)} m(p) \log 2$$

$$\omega(\phi(n)) \log 2 \le \log I(n) \le \Omega(\phi(n)) \log 2$$

Upper bound seems very wasteful, yet still good enough!

"Anatomy of integers" techniques show: most primes dividing $\phi(n)$ do so only once.

Application to distribution of $I(n)$

$I(n)$ is the number of isomorphism classes of subgroups of $\mathbb{Z}_n^\times$

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $\mathbb{Z}_n^\times \cong \bigoplus_{p|\phi(n)} \mathbb{Z}_{p^{\boldsymbol{\alpha}(p)}}$ for some partitions $\boldsymbol{\alpha}(p)$ of $m(p)$.

Then $\log I(n) = \sum_{p|\phi(n)} \log \#\{\text{subpartitions of } \boldsymbol{\alpha}_p\}$ and hence

$$\sum_{p|\phi(n)} \log 2 \le \log I(n) \le \sum_{p|\phi(n)} m(p) \log 2$$

$$\omega(\phi(n)) \log 2 \le \log I(n) \le \Omega(\phi(n)) \log 2$$

Upper bound seems very wasteful, yet still good enough!

“Anatomy of integers” techniques show: most primes dividing $\phi(n)$ do so only once.

How many subgroups of each shape?

Notation: $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_\ell)$, $\mathbb{Z}_{p^{\boldsymbol{\alpha}}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_\ell}}$

Definition

Given a subpartition $\boldsymbol{\beta}$ of $\boldsymbol{\alpha}$ and a prime p, define $N_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ to be the number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ that are isomorphic to $\mathbb{Z}_{p^{\boldsymbol{\beta}}}$.

Some classical exact formula (don't read it)

Let $\boldsymbol{a} = (a_1, a_2, \dots, a_{\alpha_1})$ and $\boldsymbol{b} = (b_1, b_2, \dots, b_{\beta_1})$ be the conjugate partitions to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively. Then

$$N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p,$$

where $\begin{bmatrix} k \\ \ell \end{bmatrix}_p = \prod_{j=1}^{\ell} \frac{p^{k-\ell+j}-1}{p^j-1}$ is the Gaussian binomial coefficient.

How many subgroups of each shape?

Notation: $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_\ell)$, $\mathbb{Z}_{p^{\boldsymbol{\alpha}}} = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_\ell}}$

Definition

Given a subpartition $\boldsymbol{\beta}$ of $\boldsymbol{\alpha}$ and a prime p, define $N_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ to be the number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ that are isomorphic to $\mathbb{Z}_{p^{\boldsymbol{\beta}}}$.

Some classical exact formula (don't read it)

Let $\boldsymbol{a} = (a_1, a_2, \dots, a_{\alpha_1})$ and $\boldsymbol{b} = (b_1, b_2, \dots, b_{\beta_1})$ be the conjugate partitions to $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, respectively. Then

$$N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \prod_{j=1}^{\alpha_1} p^{(a_j - b_j) b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p,$$

where $\begin{bmatrix} k \\ \ell \end{bmatrix}_p = \prod_{j=1}^{\ell} \frac{p^{k-\ell+j} - 1}{p^j - 1}$ is the Gaussian binomial coefficient.

The difference between algebra and analysis

$$N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p$$

is the number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ isomorphic to $\mathbb{Z}_{p^{\boldsymbol{\beta}}}$.

It turns out that each factor is about $p^{(a_j-b_j)b_j}$, which is maximally $p^{a_j^2/4}$ when $b_j = a_j/2$, and is way smaller for noncentral values of b_j. So the total number of subgroups inside $\mathbb{Z}_{p^\alpha}$ is dominated by this special $\beta =$ "$\frac{1}{2}\alpha$".

Lemma

For any prime p and any partition α,

$$\log \#\{\textit{subgroups of } \mathbb{Z}_{p^\alpha}\} = \frac{\log p}{4} \sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

The difference between algebra and analysis

$$N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p$$

is the number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ isomorphic to $\mathbb{Z}_{p^{\boldsymbol{\beta}}}$.

It turns out that each factor is about $p^{(a_j-b_j)b_j}$, which is maximally $p^{a_j^2/4}$ when $b_j = a_j/2$, and is way smaller for noncentral values of b_j. So the total number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ is dominated by this special $\boldsymbol{\beta} =$ "$\frac{1}{2}\boldsymbol{\alpha}$".

Lemma

For any prime p and any partition α,

$$\log \#\{\textit{subgroups of } \mathbb{Z}_{p^{\alpha}}\} = \frac{\log p}{4} \sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

The difference between algebra and analysis

$$N_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \prod_{j=1}^{\alpha_1} p^{(a_j - b_j)b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p$$

is the number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ isomorphic to $\mathbb{Z}_{p^{\boldsymbol{\beta}}}$.

It turns out that each factor is about $p^{(a_j - b_j)b_j}$, which is maximally $p^{a_j^2/4}$ when $b_j = a_j/2$, and is way smaller for noncentral values of b_j. So the total number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ is dominated by this special $\boldsymbol{\beta} =$ "$\frac{1}{2}\boldsymbol{\alpha}$".

Lemma

For any prime p and any partition α,

$$\log \#\{\textit{subgroups of } \mathbb{Z}_{p^{\alpha}}\} = \frac{\log p}{4} \sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

The difference between algebra and analysis

$$N_p(\boldsymbol{\alpha},\boldsymbol{\beta}) = \prod_{j=1}^{\alpha_1} p^{(a_j-b_j)b_{j+1}} \begin{bmatrix} a_j - b_{j+1} \\ b_j - b_{j+1} \end{bmatrix}_p$$

is the number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ isomorphic to $\mathbb{Z}_{p^{\boldsymbol{\beta}}}$.

It turns out that each factor is about $p^{(a_j-b_j)b_j}$, which is maximally $p^{a_j^2/4}$ when $b_j = a_j/2$, and is way smaller for noncentral values of b_j. So the total number of subgroups inside $\mathbb{Z}_{p^{\boldsymbol{\alpha}}}$ is dominated by this special $\boldsymbol{\beta} =$ “$\frac{1}{2}\boldsymbol{\alpha}$”.

Lemma

For any prime p and any partition $\boldsymbol{\alpha}$,

$$\log \#\{\textit{subgroups of } \mathbb{Z}_{p^{\boldsymbol{\alpha}}}\} = \frac{\log p}{4} \sum_{j=1}^{\alpha_1} a_j^2 + O(\alpha_1 \log p).$$

If $\mathbb{Z}_n^\times \cong \bigoplus_{p\mid\phi(n)} \mathbb{Z}_{p^{\alpha(p)}}$, then which partition is $\alpha(p)$?

Notation

Let $\omega_q(n)$ denote the number of distinct prime factors of n that are congruent to $1 \pmod{q}$.

Answer (exact for odd squarefree n, up to $O(1)$ in general)

$\alpha(p)$ is the conjugate partition to $(\omega_p(n), \omega_{p^2}(n), \dots)$.

Lemma

$$\log G_p(n) \approx \frac{\log p}{4} \sum_{j=1}^{\text{“}\infty\text{”}} \omega_{p^j}(n)^2$$ *for any prime p dividing $\phi(n)$.*

Moreover, if $p \mid \phi(n)$ and $p^2 \nmid \phi(n)$, then $\log G_p(n) = \log 2$.

If $\mathbb{Z}_n^\times \cong \bigoplus_{p\mid\phi(n)} \mathbb{Z}_{p^{\boldsymbol{\alpha}(p)}}$, then which partition is $\boldsymbol{\alpha}(p)$?

Notation

Let $\omega_q(n)$ denote the number of distinct prime factors of n that are congruent to $1 \pmod{q}$.

Answer (exact for odd squarefree n, up to $O(1)$ in general)

$\boldsymbol{\alpha}(p)$ is the conjugate partition to $(\omega_p(n), \omega_{p^2}(n), \dots)$.

Lemma

$\log G_p(n) \approx \frac{\log p}{4} \sum_{j=1}^{\text{“}\infty\text{”}} \omega_{p^j}(n)^2$ *for any prime p dividing $\phi(n)$.*

Moreover, if $p \mid \phi(n)$ and $p^2 \nmid \phi(n)$, then $\log G_p(n) = \log 2$.

If $\mathbb{Z}_n^\times \cong \bigoplus_{p \mid \phi(n)} \mathbb{Z}_{p^{\alpha(p)}}$, then which partition is $\alpha(p)$?

Notation

Let $\omega_q(n)$ denote the number of distinct prime factors of n that are congruent to $1 \pmod{q}$.

Answer (exact for odd squarefree n, up to $O(1)$ in general)

$\alpha(p)$ is the conjugate partition to $(\omega_p(n), \omega_{p^2}(n), \dots)$.

Lemma

$$\log G_p(n) \approx \frac{\log p}{4} \sum_{j=1}^{\text{“}\infty\text{”}} \omega_{p^j}(n)^2$$ *for any prime p dividing $\phi(n)$.*

Moreover, if $p \mid \phi(n)$ and $p^2 \nmid \phi(n)$, then $\log G_p(n) = \log 2$.

If $\mathbb{Z}_n^\times \cong \bigoplus_{p\mid\phi(n)} \mathbb{Z}_{p^{\alpha(p)}}$, then which partition is $\alpha(p)$?

Notation

Let $\omega_q(n)$ denote the number of distinct prime factors of n that are congruent to $1 \pmod{q}$.

Answer (exact for odd squarefree n, up to $O(1)$ in general)

$\alpha(p)$ is the conjugate partition to $(\omega_p(n), \omega_{p^2}(n), \dots)$.

Lemma

$$\log G_p(n) \approx \frac{\log p}{4} \sum_{j=1}^{\text{“}\infty\text{”}} \omega_{p^j}(n)^2$$ *for any prime p dividing $\phi(n)$.*

Moreover, if $p \mid \phi(n)$ and $p^2 \nmid \phi(n)$, then $\log G_p(n) = \log 2$.

Sum the previous lemma over all primes

$$\log G(n) = \sum_{p \mid \phi(n)} \log G_p(n) \approx \sum_{\substack{p \mid \phi(n) \\ p^2 \nmid \phi(n)}} \log 2 + \sum_{p^2 \mid \phi(n)} \frac{\log p}{4} \sum_{j=1}^{\text{``}\infty\text{''}} \omega_{p^j}(n)^2.$$

For most integers n, it's acceptable to extend both sums over all primes dividing $\phi(n)$ (the last sum should be suitably truncated):

$$\log G(n) \approx \log 2 \cdot \omega(\phi(n)) + \frac{1}{4} \sum_{p^r} \omega_{p^r}(n)^2 \log p.$$

Each function here has a known normal order; plugging in gives

$$\log G(n) \approx \log 2 \cdot \frac{1}{2} (\log\log n)^2 + \frac{1}{4} \sum_{p^r} \left(\frac{\log\log n}{\phi(p^r)} \right)^2 \log p$$

for almost all integers n. And the right-hand side is $A(\log\log n)^2$.

Sum the previous lemma over all primes

$$\log G(n) = \sum_{p \mid \phi(n)} \log G_p(n) \approx \sum_{\substack{p \mid \phi(n) \\ p^2 \nmid \phi(n)}} \log 2 + \sum_{p^2 \mid \phi(n)} \frac{\log p}{4} \sum_{j=1}^{\text{“}\infty\text{”}} \omega_{p^j}(n)^2.$$

For most integers n, it's acceptable to extend both sums over all primes dividing $\phi(n)$ (the last sum should be suitably truncated):

$$\log G(n) \approx \log 2 \cdot \omega(\phi(n)) + \frac{1}{4} \sum_{p^r} \omega_{p^r}(n)^2 \log p.$$

Each function here has a known normal order; plugging in gives

$$\log G(n) \approx \log 2 \cdot \frac{1}{2} (\log\log n)^2 + \frac{1}{4} \sum_{p^r} \left(\frac{\log\log n}{\phi(p^r)} \right)^2 \log p$$

for almost all integers n. And the right-hand side is $A(\log\log n)^2$.

Sum the previous lemma over all primes

$$\log G(n) = \sum_{p \mid \phi(n)} \log G_p(n) \approx \sum_{\substack{p \mid \phi(n) \\ p^2 \nmid \phi(n)}} \log 2 + \sum_{p^2 \mid \phi(n)} \frac{\log p}{4} \sum_{j=1}^{\text{``}\infty\text{''}} \omega_{p^j}(n)^2.$$

For most integers n, it's acceptable to extend both sums over all primes dividing $\phi(n)$ (the last sum should be suitably truncated):

$$\log G(n) \approx \log 2 \cdot \omega(\phi(n)) + \frac{1}{4} \sum_{p^r} \omega_{p^r}(n)^2 \log p.$$

Each function here has a known normal order; plugging in gives

$$\log G(n) \approx \log 2 \cdot \frac{1}{2} (\log\log n)^2 + \frac{1}{4} \sum_{p^r} \left(\frac{\log\log n}{\phi(p^r)} \right)^2 \log p$$

for almost all integers n. And the right-hand side is $A(\log\log n)^2$.

Sum the previous lemma over all primes

$$\log G(n) = \sum_{p \mid \phi(n)} \log G_p(n) \approx \sum_{\substack{p \mid \phi(n) \\ p^2 \nmid \phi(n)}} \log 2 + \sum_{p^2 \mid \phi(n)} \frac{\log p}{4} \sum_{j=1}^{\text{``}\infty\text{''}} \omega_{p^j}(n)^2.$$

For most integers n, it's acceptable to extend both sums over all primes dividing $\phi(n)$ (the last sum should be suitably truncated):

$$\log G(n) \approx \log 2 \cdot \omega(\phi(n)) + \frac{1}{4} \sum_{p^r} \omega_{p^r}(n)^2 \log p.$$

Each function here has a known normal order; plugging in gives

$$\log G(n) \approx \log 2 \cdot \frac{1}{2} (\log\log n)^2 + \frac{1}{4} \sum_{p^r} \left(\frac{\log\log n}{\phi(p^r)} \right)^2 \log p$$

for almost all integers n. And the right-hand side is $A(\log\log n)^2$.

Final sketch

Getting beyond the normal order to an Erdős–Kac law requires computing all of the central moments of this approximation to $\log G(n)$. The correlations among the additive functions $\omega_q(n)$, and their correlations with $\omega(\phi(n))$, become important.

"Sieving and the Erdős–Kac theorem" (2007)

To compute the moments, we rely on a technique of Granville and Soundararajan to reduce the complexity of identifying the main terms of these moments.

Generalizing our method

Part of $\log G(n)$ is well approximated by a sum of squares of additive functions. Troupe and I (work in progress) can obtain an Erdős–Kac law for any fixed (nonnegative) polynomial evaluated at values of (appropriate) additive functions—for example, Erdős–Kac laws for products of additive functions.

Final sketch

Getting beyond the normal order to an Erdős–Kac law requires computing all of the central moments of this approximation to $\log G(n)$. The correlations among the additive functions $\omega_q(n)$, and their correlations with $\omega(\phi(n))$, become important.

"Sieving and the Erdős–Kac theorem" (2007)

To compute the moments, we rely on a technique of Granville and Soundararajan to reduce the complexity of identifying the main terms of these moments.

Generalizing our method

Part of $\log G(n)$ is well approximated by a sum of squares of additive functions. Troupe and I (work in progress) can obtain an Erdős–Kac law for any fixed (nonnegative) polynomial evaluated at values of (appropriate) additive functions—for example, Erdős–Kac laws for products of additive functions.

Final sketch

Getting beyond the normal order to an Erdős–Kac law requires computing all of the central moments of this approximation to $\log G(n)$. The correlations among the additive functions $\omega_q(n)$, and their correlations with $\omega(\phi(n))$, become important.

"Sieving and the Erdős–Kac theorem" (2007)

To compute the moments, we rely on a technique of Granville and Soundararajan to reduce the complexity of identifying the main terms of these moments.

Generalizing our method

Part of $\log G(n)$ is well approximated by a sum of squares of additive functions. Troupe and I (work in progress) can obtain an Erdős–Kac law for any fixed (nonnegative) polynomial evaluated at values of (appropriate) additive functions—for example, Erdős–Kac laws for products of additive functions.

Final sketch

Getting beyond the normal order to an Erdős–Kac law requires computing all of the central moments of this approximation to $\log G(n)$. The correlations among the additive functions $\omega_q(n)$, and their correlations with $\omega(\phi(n))$, become important.

"Sieving and the Erdős–Kac theorem" (2007)

To compute the moments, we rely on a technique of Granville and Soundararajan to reduce the complexity of identifying the main terms of these moments.

Generalizing our method

Part of $\log G(n)$ is well approximated by a sum of squares of additive functions. Troupe and I (work in progress) can obtain an Erdős–Kac law for any fixed (nonnegative) polynomial evaluated at values of (appropriate) additive functions—for example, Erdős–Kac laws for products of additive functions.

The end

Our submitted paper "The distribution of the number of subgroups of the multiplicative group" and these slides are available for downloading.

The paper with Lee Troupe

`www.math.ubc.ca/~gerg/index.shtml?abstract=DNSMG`

These slides

`www.math.ubc.ca/~gerg/index.shtml?slides`