Anatomy of the mulitplicative group

Greg Martin
University of British Columbia

Pacific Northwest Number Theory Conference
University of Idaho
May 19, 2012

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

Outline

1. What do we want to know about multiplicative groups $(\mathrm{mod}\ n)$?
2. Distribution of the number of prime factors of n
3. Other invariants of the multiplicative groups
4. Counting certain elements, and subgroups, of multiplicative groups

The main characters

Notation

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $\mathbb{Z}_n$. It enjoys both addition and multiplication.

If we ignore multiplication:

The additive group $\mathbb{Z}_n^+$ is the set $\mathbb{Z}_n$ with the ring's addition operation. It is always a cyclic group with n elements.

If we instead ignore addition:

The multiplicative group $\mathbb{Z}_n^\times$ is the set $(\mathbb{Z}_n)^\times$ of invertible elements in $\mathbb{Z}_n$, with the ring's multiplication operation. It is a finite abelian group with $\phi(n)$ elements.

The main characters

One ring to rule them all . . .

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $\mathbb{Z}_n$. It enjoys both addition and multiplication.

If we ignore multiplication:

The additive group $\mathbb{Z}_n^+$ is the set $\mathbb{Z}_n$ with the ring's addition operation. It is always a cyclic group with n elements.

If we instead ignore addition:

The multiplicative group $\mathbb{Z}_n^\times$ is the set $(\mathbb{Z}_n)^\times$ of invertible elements in $\mathbb{Z}_n$, with the ring's multiplication operation. It is a finite abelian group with $\phi(n)$ elements.

The main characters

One ring to rule them all . . .

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $\mathbb{Z}_n$. It enjoys both addition and multiplication.

If we ignore multiplication:

The additive group $\mathbb{Z}_n^+$ is the set $\mathbb{Z}_n$ with the ring's addition operation. It is always a cyclic group with n elements.

If we instead ignore addition:

The multiplicative group $\mathbb{Z}_n^\times$ is the set $(\mathbb{Z}_n)^\times$ of invertible elements in $\mathbb{Z}_n$, with the ring's multiplication operation. It is a finite abelian group with $\phi(n)$ elements.

The main characters

One ring to rule them all . . .

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ will be denoted by $\mathbb{Z}_n$. It enjoys both addition and multiplication.

If we ignore multiplication:

The additive group $\mathbb{Z}_n^+$ is the set $\mathbb{Z}_n$ with the ring's addition operation. It is always a cyclic group with n elements.

If we instead ignore addition:

The multiplicative group $\mathbb{Z}_n^\times$ is the set $(\mathbb{Z}_n)^\times$ of invertible elements in $\mathbb{Z}_n$, with the ring's multiplication operation. It is a finite abelian group with $\phi(n)$ elements.

How to find the structure of $\mathbb{Z}_n^\times$

Chinese remainder theorem, and primitive roots

If the prime factorization of n is $p_1^{r_1} \times \cdots \times p_k^{r_k}$, then

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^\times \cong \mathbb{Z}^+_{p_1^{r_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}^+_{p_k^{r_k-1}(p_k-1)}.$$

Confession

I'm lying slightly about the prime $p = 2$. I'll keep doing so throughout the talk when making general statements about $\mathbb{Z}_n^\times$.

Example (with $n = 11!$)

$$\begin{aligned}\mathbb{Z}_{11!}^\times &\cong \mathbb{Z}_{2^8}^\times \oplus \mathbb{Z}_{3^4}^\times \oplus \mathbb{Z}_{5^2}^\times \oplus \mathbb{Z}_7^\times \oplus \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_2^+ \oplus \mathbb{Z}_{64}^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+\end{aligned}$$

How to find the structure of $\mathbb{Z}_n^\times$

Chinese remainder theorem, and primitive roots

If the prime factorization of n is $p_1^{r_1} \times \cdots \times p_k^{r_k}$, then

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^\times \cong \mathbb{Z}^+_{p_1^{r_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}^+_{p_k^{r_k-1}(p_k-1)}.$$

Confession

I'm lying slightly about the prime $p = 2$. I'll keep doing so throughout the talk when making general statements about $\mathbb{Z}_n^\times$.

Example (with $n = 11!$)

$$\begin{aligned}\mathbb{Z}_{11!}^\times &\cong \mathbb{Z}_{2^8}^\times \oplus \mathbb{Z}_{3^4}^\times \oplus \mathbb{Z}_{5^2}^\times \oplus \mathbb{Z}_7^\times \oplus \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_2^+ \oplus \mathbb{Z}_{64}^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+\end{aligned}$$

How to find the structure of $\mathbb{Z}_n^\times$

Chinese remainder theorem, and primitive roots

If the prime factorization of n is $p_1^{r_1} \times \cdots \times p_k^{r_k}$, then

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^\times \cong \mathbb{Z}_{p_1^{r_1-1}(p_1-1)}^+ \times \cdots \times \mathbb{Z}_{p_k^{r_k-1}(p_k-1)}^+.$$

Confession

I'm lying slightly about the prime $p = 2$. I'll keep doing so throughout the talk when making general statements about $\mathbb{Z}_n^\times$.

Example (with $n = 11!$)

$$\begin{aligned}\mathbb{Z}_{11!}^\times &\cong \mathbb{Z}_{2^8}^\times \oplus \mathbb{Z}_{3^4}^\times \oplus \mathbb{Z}_{5^2}^\times \oplus \mathbb{Z}_7^\times \oplus \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_2^+ \oplus \mathbb{Z}_{64}^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+\end{aligned}$$

How to find the structure of $\mathbb{Z}_n^\times$

Chinese remainder theorem, and primitive roots

If the prime factorization of n is $p_1^{r_1} \times \cdots \times p_k^{r_k}$, then

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^\times \cong \mathbb{Z}^+_{p_1^{r_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}^+_{p_k^{r_k-1}(p_k-1)}.$$

Confession

I'm lying slightly about the prime $p = 2$. I'll keep doing so throughout the talk when making general statements about $\mathbb{Z}_n^\times$.

Example (with $n = 11!$)

$$\begin{aligned}\mathbb{Z}_{11!}^\times &\cong \mathbb{Z}_{2^8}^\times \oplus \mathbb{Z}_{3^4}^\times \oplus \mathbb{Z}_{5^2}^\times \oplus \mathbb{Z}_7^\times \oplus \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_2^+ \oplus \mathbb{Z}_{64}^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+\end{aligned}$$

How to find the structure of $\mathbb{Z}_n^\times$

Chinese remainder theorem, and primitive roots

If the prime factorization of n is $p_1^{r_1} \times \cdots \times p_k^{r_k}$, then

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^\times \cong \mathbb{Z}^+_{p_1^{r_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}^+_{p_k^{r_k-1}(p_k-1)}.$$

Confession

I'm lying slightly about the prime $p = 2$. I'll keep doing so throughout the talk when making general statements about $\mathbb{Z}_n^\times$.

Example (with $n = 11!$)

$$\begin{aligned}\mathbb{Z}_{11!}^\times &\cong \mathbb{Z}_{2^8}^\times \oplus \mathbb{Z}_{3^4}^\times \oplus \mathbb{Z}_{5^2}^\times \oplus \mathbb{Z}_7^\times \oplus \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_2^+ \oplus \mathbb{Z}_{64}^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+\end{aligned}$$

How to find the structure of $\mathbb{Z}_n^\times$

Chinese remainder theorem, and primitive roots

If the prime factorization of n is $p_1^{r_1} \times \cdots \times p_k^{r_k}$, then

$$\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{r_1}}^\times \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^\times \cong \mathbb{Z}^+_{p_1^{r_1-1}(p_1-1)} \times \cdots \times \mathbb{Z}^+_{p_k^{r_k-1}(p_k-1)}.$$

Confession

I'm lying slightly about the prime $p = 2$. I'll keep doing so throughout the talk when making general statements about $\mathbb{Z}_n^\times$.

Example (with $n = 11!$)

$$\begin{aligned}\mathbb{Z}_{11!}^\times &\cong \mathbb{Z}_{2^8}^\times \oplus \mathbb{Z}_{3^4}^\times \oplus \mathbb{Z}_{5^2}^\times \oplus \mathbb{Z}_7^\times \oplus \mathbb{Z}_{11}^\times \\ &\cong (\mathbb{Z}_2^+ \oplus \mathbb{Z}_{64}^+) \oplus \mathbb{Z}_{54}^+ \oplus \mathbb{Z}_{20}^+ \oplus \mathbb{Z}_6^+ \oplus \mathbb{Z}_{10}^+\end{aligned}$$

Two standard forms

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

Example (with $n = 11!$)

$$\mathbb{Z}_{11!}^\times \cong \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_{60}^+ \oplus \mathbb{Z}_{8640}^+$$

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{q_1^{r_1}}^+ \oplus \mathbb{Z}_{q_2^{r_2}}^+ \oplus \cdots \oplus \mathbb{Z}_{q_\ell^{r_\ell}}^+$ where each q_j is prime. (unique up to reordering)

Two standard forms

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

Example (with $n = 11!$)

$$\mathbb{Z}_{11!}^\times \cong \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_{60}^+ \oplus \mathbb{Z}_{8640}^+$$

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{q_1^{r_1}}^+ \oplus \mathbb{Z}_{q_2^{r_2}}^+ \oplus \cdots \oplus \mathbb{Z}_{q_\ell^{r_\ell}}^+$ where each q_j is prime. (unique up to reordering)

Two standard forms

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

Example (with $n = 11!$)

$$\mathbb{Z}_{11!}^\times \cong \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_2^+ \oplus \mathbb{Z}_{60}^+ \oplus \mathbb{Z}_{8640}^+$$

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{q_1^{r_1}}^+ \oplus \mathbb{Z}_{q_2^{r_2}}^+ \oplus \cdots \oplus \mathbb{Z}_{q_\ell^{r_\ell}}^+$ where each q_j is prime. (unique up to reordering)

Two standard forms

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

Example (with $n = 11!$)

$$\mathbb{Z}_{11!}^\times \cong (\mathbb{Z}_2^+)^4 \oplus \mathbb{Z}_{60}^+ \oplus \mathbb{Z}_{8640}^+$$

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{q_1^{r_1}}^+ \oplus \mathbb{Z}_{q_2^{r_2}}^+ \oplus \cdots \oplus \mathbb{Z}_{q_\ell^{r_\ell}}^+$ where each q_j is prime. (unique up to reordering)

Two standard forms

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

Example (with $n = 11!$)

$$\mathbb{Z}_{11!}^\times \cong (\mathbb{Z}_2^+)^4 \oplus \mathbb{Z}_{60}^+ \oplus \mathbb{Z}_{8640}^+$$

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{q_1^{r_1}}^+ \oplus \mathbb{Z}_{q_2^{r_2}}^+ \oplus \cdots \oplus \mathbb{Z}_{q_\ell^{r_\ell}}^+$ where each q_j is prime. (unique up to reordering)

Two standard forms

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

Example (with $n = 11!$)

$$\mathbb{Z}_{11!}^\times \cong (\mathbb{Z}_2^+)^4 \oplus \mathbb{Z}_4^+ \oplus \mathbb{Z}_{64}^+ \oplus \mathbb{Z}_3^+ \oplus \mathbb{Z}_{27}^+ \oplus (\mathbb{Z}_5^+)^2$$

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{q_1^{r_1}}^+ \oplus \mathbb{Z}_{q_2^{r_2}}^+ \oplus \cdots \oplus \mathbb{Z}_{q_\ell^{r_\ell}}^+$ where each q_j is prime. (unique up to reordering)

Reasons to look at the multiplicative group

We study $\mathbb{Z}_n^\times$ because of its:

Ubiquity

Modular arithmetic shows up everywhere in number theory.

Typicality

$\mathbb{Z}_n^\times$ is representative of finite abelian groups in general.

Fun exercise

Every finite abelian group is a subgroup of $\mathbb{Z}_n^\times$ for infinitely many integers n.

Reasons to look at the multiplicative group

We study $\mathbb{Z}_n^\times$ because of its:

Ubiquity

Modular arithmetic shows up everywhere in number theory.

Typicality

$\mathbb{Z}_n^\times$ is representative of finite abelian groups in general.

Fun exercise

Every finite abelian group is a subgroup of $\mathbb{Z}_n^\times$ for infinitely many integers n.

Reasons to look at the multiplicative group

We study $\mathbb{Z}_n^\times$ because of its:

Ubiquity

Modular arithmetic shows up everywhere in number theory.

Typicality

$\mathbb{Z}_n^\times$ is representative of finite abelian groups in general.

Fun exercise

Every finite abelian group is a subgroup of $\mathbb{Z}_n^\times$ for infinitely many integers n.

Reasons to look at the multiplicative group

We study $\mathbb{Z}_n^\times$ because of its:

Ubiquity

Modular arithmetic shows up everywhere in number theory.

Typicality

$\mathbb{Z}_n^\times$ is representative of finite abelian groups in general.

Fun exercise

Every finite abelian group is a subgroup of $\mathbb{Z}_n^\times$ for infinitely many integers n.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

Questions to ask about $\mathbb{Z}_n^\times$

If we "choose n at random", what is the distribution of:

- the number of invariant factors?
- the largest invariant factor?
- the number of terms in the primary decomposition?
- the largest term in the primary decomposition?
- the number of elements of order 2 (square roots of $1 \pmod n$)? (and generalizations)
- the number of subgroups?

Choosing n at random means:

Choose n uniformly at random from an initial interval $\{1, 2, \dots, x\}$, understand the distribution as a function of x, and see what happens as $x \to \infty$.

The number of invariant factors

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The number of invariant factors equals $\omega(n)$, the number of distinct prime factors of n. (This is again a slight lie: if n is even, then it might be $\omega(n) \pm 1$.)

Theorem (Average order of $\omega(n)$)

$$\frac{1}{x}\sum_{n\le x}\omega(n) = \frac{1}{x}\sum_{n\le x}\sum_{p\mid n}1 = \frac{1}{x}\sum_{p\le x}\sum_{\substack{n\le x\\ p\mid n}}1 \sim \frac{1}{x}\sum_{p\le x}\frac{x}{p} \sim \log\log x.$$

- *new improvements in error term (M.–Naslund, 2012+)*

The number of invariant factors

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The number of invariant factors equals $\omega(n)$, the number of distinct prime factors of n. (This is again a slight lie: if n is even, then it might be $\omega(n) \pm 1$.)

Theorem (Average order of $\omega(n)$)

$$\frac{1}{x}\sum_{n\le x}\omega(n) = \frac{1}{x}\sum_{n\le x}\sum_{p\mid n}1 = \frac{1}{x}\sum_{p\le x}\sum_{\substack{n\le x\\ p\mid n}}1 \sim \frac{1}{x}\sum_{p\le x}\frac{x}{p} \sim \log\log x.$$

- *new improvements in error term (M.–Naslund, 2012+)*

The number of invariant factors

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The number of invariant factors equals $\omega(n)$, the number of distinct prime factors of n. (This is again a slight lie: if n is even, then it might be $\omega(n) \pm 1$.)

Theorem (Average order of $\omega(n)$)

$$\frac{1}{x}\sum_{n\le x}\omega(n) = \frac{1}{x}\sum_{n\le x}\sum_{p\mid n}1 = \frac{1}{x}\sum_{p\le x}\sum_{\substack{n\le x\\ p\mid n}}1 \sim \frac{1}{x}\sum_{p\le x}\frac{x}{p} \sim \log\log x.$$

- *new improvements in error term (M.–Naslund, 2012+)*

The number of invariant factors

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The number of invariant factors equals $\omega(n)$, the number of distinct prime factors of n. (This is again a slight lie: if n is even, then it might be $\omega(n) \pm 1$.)

Theorem (Average order of $\omega(n)$)

$$\frac{1}{x}\sum_{n\le x}\omega(n) = \frac{1}{x}\sum_{n\le x}\sum_{p\mid n}1 = \frac{1}{x}\sum_{p\le x}\sum_{\substack{n\le x\\ p\mid n}}1 \sim \frac{1}{x}\sum_{p\le x}\frac{x}{p} \sim \log\log x.$$

- *new improvements in error term (M.–Naslund, 2012+)*

The number of invariant factors

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The number of invariant factors equals $\omega(n)$, the number of distinct prime factors of n. (This is again a slight lie: if n is even, then it might be $\omega(n) \pm 1$.)

Theorem (Average order of $\omega(n)$)

$$\frac{1}{x}\sum_{n\le x}\omega(n) = \frac{1}{x}\sum_{n\le x}\sum_{p\mid n}1 = \frac{1}{x}\sum_{p\le x}\sum_{\substack{n\le x\\ p\mid n}}1 \sim \frac{1}{x}\sum_{p\le x}\frac{x}{p} \sim \log\log x.$$

- *new improvements in error term (M.–Naslund, 2012+)*

The number of invariant factors

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The number of invariant factors equals $\omega(n)$, the number of distinct prime factors of n. (This is again a slight lie: if n is even, then it might be $\omega(n) \pm 1$.)

Theorem (Average order of $\omega(n)$)

$$\frac{1}{x}\sum_{n\le x}\omega(n) = \frac{1}{x}\sum_{n\le x}\sum_{p\mid n}1 = \frac{1}{x}\sum_{p\le x}\sum_{\substack{n\le x\\ p\mid n}}1 \sim \frac{1}{x}\sum_{p\le x}\frac{x}{p} \sim \log\log x.$$

- *new improvements in error term (M.–Naslund, 2012+)*

The variance of $\omega(n)$

$\omega(n) =$ number of distinct prime factors of n

Theorem (Turán, 1934)

$$\frac{1}{x}\sum_{n\le x}\bigl(\omega(n)-\log\log x\bigr)^2 \sim \log\log x.$$

So there can't be too many integers n with $\omega(n)$ far from $\log\log n$. For example, the number of integers $n \le x$ with $\bigl|\omega(n)-\log\log x\bigr| > (\log\log x)^{0.52}$ is less than $x/(\log\log x)^{0.03}$.

Theorem (Hardy–Ramanujan, 1917)

The normal order *of* $\omega(n)$ *is* $\log\log n$. *In other words, if* $n \in \{1,2,\dots,x\}$ *is chosen uniformly at random, then the probability that* $\omega(n) \sim \log\log n$ *tends to* 1 *as* $x \to \infty$.

The variance of $\omega(n)$

$\omega(n) =$ number of distinct prime factors of n

Theorem (Turán, 1934)

$$\frac{1}{x}\sum_{n\le x}\big(\omega(n)-\log\log x\big)^2 \sim \log\log x.$$

So there can't be too many integers n with $\omega(n)$ far from $\log\log n$. For example, the number of integers $n \le x$ with $\big|\omega(n)-\log\log x\big| > (\log\log x)^{0.52}$ is less than $x/(\log\log x)^{0.03}$.

Theorem (Hardy–Ramanujan, 1917)

The normal order *of* $\omega(n)$ *is* $\log\log n$. *In other words, if* $n \in \{1,2,\dots,x\}$ *is chosen uniformly at random, then the probability that* $\omega(n) \sim \log\log n$ *tends to* 1 *as* $x \to \infty$.

The variance of $\omega(n)$

$\omega(n) =$ number of distinct prime factors of n

Theorem (Turán, 1934)

$$\frac{1}{x}\sum_{n\le x}\bigl(\omega(n)-\log\log x\bigr)^2 \sim \log\log x.$$

So there can't be too many integers n with $\omega(n)$ far from $\log\log n$. For example, the number of integers $n \le x$ with $\bigl|\omega(n)-\log\log x\bigr| > (\log\log x)^{0.52}$ is less than $x/(\log\log x)^{0.03}$.

Theorem (Hardy–Ramanujan, 1917)

The normal order *of* $\omega(n)$ *is* $\log\log n$. *In other words, if* $n \in \{1,2,\dots,x\}$ *is chosen uniformly at random, then the probability that* $\omega(n) \sim \log\log n$ *tends to* 1 *as* $x \to \infty$.

The variance of $\omega(n)$

$\omega(n) =$ number of distinct prime factors of n

Theorem (Turán, 1934)

$$\tfrac{1}{x} \sum_{n \le x} \big(\omega(n) - \log\log x\big)^2 \sim \log\log x.$$

So there can't be too many integers n with $\omega(n)$ far from $\log\log n$. For example, the number of integers $n \le x$ with $\big|\omega(n) - \log\log x\big| > (\log\log x)^{0.52}$ is less than $x/(\log\log x)^{0.03}$.

Theorem (Hardy–Ramanujan, 1917)

The normal order *of* $\omega(n)$ *is* $\log\log n$. *In other words, if* $n \in \{1, 2, \dots, x\}$ *is chosen uniformly at random, then the probability that* $\omega(n) \sim \log\log n$ *tends to* 1 *as* $x \to \infty$.

A Gaussian distribution?!

Definition (Standard normal distribution/bell curve)

$$\Phi(\alpha) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\,dt$$

Theorem (Erdős–Kac, 1940)

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} < \alpha \right\} = \Phi(\alpha).$$

"The number of prime factors of n has a normal distribution with mean $\log\log n$ and standard deviation $\sqrt{\log\log n}$."

A Gaussian distribution?!

Definition (Standard normal distribution/bell curve)

$$\Phi(\alpha) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\, dt$$

Theorem (Erdős–Kac, 1940)

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x : \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} < \alpha \right\} = \Phi(\alpha).$$

"The number of prime factors of n has a normal distribution with mean $\log\log n$ and standard deviation $\sqrt{\log\log n}$."

A Gaussian distribution?!

Definition (Standard normal distribution/bell curve)

$$\Phi(\alpha) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\, dt$$

Theorem (Erdős–Kac, 1940)

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \le x : \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} < \alpha \right\} = \Phi(\alpha).$$

"The number of prime factors of n has a normal distribution with mean $\log\log n$ and standard deviation $\sqrt{\log\log n}$."

A Gaussian distribution?!

Definition (Standard normal distribution/bell curve)

$$\Phi(\alpha) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\,dt$$

Theorem (Erdős–Kac, 1940)

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} < \alpha \right\} = \Phi(\alpha).$$

"The number of prime factors of n has a normal distribution with mean $\log\log n$ and standard deviation $\sqrt{\log\log n}$."

Good luck testing this emperically . . .

Even if we could reliably factor numbers around 10^{100}, the quantity $\log\log 10^{100}$ isn't even up to 5.5 yet.

An application: the Erdős multiplication table problem

Question:

How many distinct integers are in the $N \times N$ multiplication table?

$\times$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

An application: the Erdős multiplication table problem

Question:

How many distinct integers are in the $N \times N$ multiplication table?

$\times$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

An application: the Erdős multiplication table problem

Question:

How many distinct integers are in the $N \times N$ multiplication table?

$\times$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

Spot the trend

N	# of distinct integers in $N \times N$ table	% of distinct integers in $N \times N$ table
10	42	42.0%
$10^{1.5}$	339	33.9%
10^2	2,906	29.0%
$10^{2.5}$	26,643	26.6%
10^3	248,083	24.8%
$10^{3.5}$	2,346,562	23.5%
10^4	22,504,348	22.5%

Time to vote:

The percentage does tend to a limit as $N \to \infty$. Is that limit positive or zero?

Spot the trend

N	# of distinct integers in $N \times N$ table	% of distinct integers in $N \times N$ table
10	42	42.0%
$10^{1.5}$	339	33.9%
10^2	2,906	29.0%
$10^{2.5}$	26,643	26.6%
10^3	248,083	24.8%
$10^{3.5}$	2,346,562	23.5%
10^4	22,504,348	22.5%

Time to vote:

The percentage does tend to a limit as $N \to \infty$. Is that limit positive or zero?

Table trouble

Theorem (Erdős, 1960)

The percentage of distinct integers in the $N \times N$ multiplication table tends to 0% as $N \to \infty$.

Four-sentence proof

Almost all integers between 1 and N have about $\log\log N$ prime factors. Hence almost all products in the $N \times N$ table have about $2\log\log N$ prime factors. But almost all potential entries between 1 and N^2 have only about $\log\log(N^2) \sim \log\log N$ prime factors. Thus almost no potential entries actually appear.

Theorem (Ford, 2009)

There are about $N^2/(\log N)^\delta(\log\log N)^{3/2}$ distinct integers in the $N \times N$ table, where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$.

Table trouble

Theorem (Erdős, 1960)

The percentage of distinct integers in the $N \times N$ multiplication table tends to 0% as $N \to \infty$.

Four-sentence proof

Almost all integers between 1 and N have about $\log\log N$ prime factors. Hence almost all products in the $N \times N$ table have about $2\log\log N$ prime factors. But almost all potential entries between 1 and N^2 have only about $\log\log(N^2) \sim \log\log N$ prime factors. Thus almost no potential entries actually appear.

Theorem (Ford, 2009)

There are about $N^2/(\log N)^\delta(\log\log N)^{3/2}$ distinct integers in the $N \times N$ table, where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$.

Table trouble

Theorem (Erdős, 1960)

The percentage of distinct integers in the $N \times N$ multiplication table tends to 0% as $N \to \infty$.

Four-sentence proof

Almost all integers between 1 and N have about $\log\log N$ prime factors. Hence almost all products in the $N \times N$ table have about $2\log\log N$ prime factors. But almost all potential entries between 1 and N^2 have only about $\log\log(N^2) \sim \log\log N$ prime factors. Thus almost no potential entries actually appear.

Theorem (Ford, 2009)

There are about $N^2/(\log N)^\delta(\log\log N)^{3/2}$ distinct integers in the $N \times N$ table, where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$.

Table trouble

Theorem (Erdős, 1960)

The percentage of distinct integers in the $N \times N$ multiplication table tends to 0% as $N \to \infty$.

Four-sentence proof

Almost all integers between 1 and N have about $\log\log N$ prime factors. Hence almost all products in the $N \times N$ table have about $2\log\log N$ prime factors. But almost all potential entries between 1 and N^2 have only about $\log\log(N^2) \sim \log\log N$ prime factors. Thus almost no potential entries actually appear.

Theorem (Ford, 2009)

There are about $N^2/(\log N)^\delta(\log\log N)^{3/2}$ distinct integers in the $N \times N$ table, where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$.

Table trouble

Theorem (Erdős, 1960)

The percentage of distinct integers in the $N \times N$ multiplication table tends to 0% as $N \to \infty$.

Four-sentence proof

Almost all integers between 1 and N have about $\log\log N$ prime factors. Hence almost all products in the $N \times N$ table have about $2\log\log N$ prime factors. But almost all potential entries between 1 and N^2 have only about $\log\log(N^2) \sim \log\log N$ prime factors. Thus almost no potential entries actually appear.

Theorem (Ford, 2009)

There are about $N^2/(\log N)^\delta(\log\log N)^{3/2}$ distinct integers in the $N \times N$ table, where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$.

Table trouble

Theorem (Erdős, 1960)

The percentage of distinct integers in the $N \times N$ multiplication table tends to 0% as $N \to \infty$.

Four-sentence proof

Almost all integers between 1 and N have about $\log\log N$ prime factors. Hence almost all products in the $N \times N$ table have about $2\log\log N$ prime factors. But almost all potential entries between 1 and N^2 have only about $\log\log(N^2) \sim \log\log N$ prime factors. Thus almost no potential entries actually appear.

Theorem (Ford, 2009)

There are about $N^2/(\log N)^\delta(\log\log N)^{3/2}$ distinct integers in the $N \times N$ table, where $\delta = 1 - (1 + \log\log 2)/\log 2 \approx 0.086$.

The largest invariant factor

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The largest invariant factor d_m is the exponent of the group G (the largest order of any element). The exponent of the multiplicative group $\mathbb{Z}_n^\times$ is called the Carmichael lambda function $\lambda(n)$ (and is a divisor of $\phi(n)$).

Theorem (Erdős–Pomerance–Schmutz, 1991)

For almost all integers n,

$$\lambda(n) \approx \frac{n}{\exp(\log\log n \log\log\log n)} = \frac{n}{(\log n)^{\log\log\log n}}.$$

The largest invariant factor

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The largest invariant factor d_m is the exponent of the group G (the largest order of any element). The exponent of the multiplicative group $\mathbb{Z}_n^\times$ is called the Carmichael lambda function $\lambda(n)$ (and is a divisor of $\phi(n)$).

Theorem (Erdős–Pomerance–Schmutz, 1991)

For almost all integers n,

$$\lambda(n) \approx \frac{n}{\exp(\log\log n \log\log\log n)} = \frac{n}{(\log n)^{\log\log\log n}}.$$

The largest invariant factor

Invariant factors

Every finite abelian group G is uniquely isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}_{d_1}^+ \oplus \mathbb{Z}_{d_2}^+ \oplus \cdots \oplus \mathbb{Z}_{d_m}^+$ where $d_1 \mid d_2 \mid \cdots \mid d_m$.

The largest invariant factor d_m is the exponent of the group G (the largest order of any element). The exponent of the multiplicative group $\mathbb{Z}_n^\times$ is called the Carmichael lambda function $\lambda(n)$ (and is a divisor of $\phi(n)$).

Theorem (Erdős–Pomerance–Schmutz, 1991)

For almost all integers n,

$$\lambda(n) \approx \frac{n}{\exp(\log\log n \log\log\log n)} = \frac{n}{(\log n)^{\log\log\log n}}.$$

Lambdas all the way down

One pseudorandom number generator repeatedly raises the previous number to the bth power modulo n; the period of the resulting "power-generator sequence" is a divisor of $\lambda(\lambda(n))$.

Theorem (M.–Pomerance, 2005)

For almost all integers n,

$$\lambda(\lambda(n)) \approx \frac{n}{\exp\left((\log\log n)^2 \log\log\log n\right)}.$$

Assuming GRH, then almost all n have at least one power-generator sequence of this length.

Higher iterates

In his PhD dissertation, Nick Harland has generalized this theorem to any higher iterate $\lambda(\lambda(\cdots\lambda(n)\cdots))$.

Lambdas all the way down

One pseudorandom number generator repeatedly raises the previous number to the bth power modulo n; the period of the resulting "power-generator sequence" is a divisor of $\lambda(\lambda(n))$.

Theorem (M.–Pomerance, 2005)

For almost all integers n,

$$\lambda(\lambda(n)) \approx \frac{n}{\exp\left((\log\log n)^2 \log\log\log n\right)}.$$

Assuming GRH, then almost all n have at least one power-generator sequence of this length.

Higher iterates

In his PhD dissertation, Nick Harland has generalized this theorem to any higher iterate $\lambda(\lambda(\cdots\lambda(n)\cdots))$.

Lambdas all the way down

One pseudorandom number generator repeatedly raises the previous number to the bth power modulo n; the period of the resulting "power-generator sequence" is a divisor of $\lambda(\lambda(n))$.

Theorem (M.–Pomerance, 2005)

For almost all integers n,

$$\lambda(\lambda(n)) \approx \frac{n}{\exp\left((\log\log n)^2 \log\log\log n\right)}.$$

Assuming GRH, then almost all n have at least one power-generator sequence of this length.

Higher iterates

In his PhD dissertation, Nick Harland has generalized this theorem to any higher iterate $\lambda(\lambda(\cdots\lambda(n)\cdots))$.

Length of the primary decomposition

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ (each q_j is prime).

The length ℓ is related to $\omega(\lambda(n))$. (To get ℓ exactly, some primes have to be counted with multiplicity.)

Theorem (Erdős–Pomerance, 1985)

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \frac{\omega(\lambda(n)) - \frac{1}{2}(\log\log n)^2}{\sqrt{\frac{1}{3}(\log\log n)^3}} < \alpha \right\}$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\, dt = \Phi(\alpha).$$

Length of the primary decomposition

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ (each q_j is prime).

The length ℓ is related to $\omega(\lambda(n))$. (To get ℓ exactly, some primes have to be counted with multiplicity.)

Theorem (Erdős–Pomerance, 1985)

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \frac{\omega(\lambda(n)) - \frac{1}{2}(\log\log n)^2}{\sqrt{\frac{1}{3}(\log\log n)^3}} < \alpha \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\,dt = \Phi(\alpha).$$

Length of the primary decomposition

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ (each q_j is prime).

The length ℓ is related to $\omega(\lambda(n))$. (To get ℓ exactly, some primes have to be counted with multiplicity.)

Theorem (Erdős–Pomerance, 1985)

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \frac{\ell - \frac12 (\log\log n)^2}{\sqrt{\frac13 (\log\log n)^3}} < \alpha \right\}$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\, dt = \Phi(\alpha).$$

Largest primary factor

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ $(q_1^{r_1} \le \cdots \le q_\ell^{r_\ell})$.

If $G = \mathbb{Z}_n^+$, then (almost all the time) the size of the largest primary factor is simply $P(n)$, the largest prime factor of n.

Theorem (Dickman–de Bruijn rho function)

The probability that $P(n)$ is less than n^α equals $\rho(1/\alpha)$, where

$$\begin{cases} \rho(u) = 1, & \text{for } 0 < u \le 1, \\ \rho'(u) = -\rho(u-1)/u, & \text{for } u > 1. \end{cases}$$

When $G = \mathbb{Z}_n^\times$ we have heuristics and conjectures (involving self-convolutions of $\rho(u)$), but the problem is still open.

Largest primary factor

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ $(q_1^{r_1} \le \cdots \le q_\ell^{r_\ell})$.

If $G = \mathbb{Z}_n^+$, then (almost all the time) the size of the largest primary factor is simply $P(n)$, the largest prime factor of n.

Theorem (Dickman–de Bruijn rho function)

The probability that $P(n)$ is less than n^α equals $\rho(1/\alpha)$, where

$$\begin{cases} \rho(u) = 1, & \text{for } 0 < u \le 1, \\ \rho'(u) = -\rho(u-1)/u, & \text{for } u > 1. \end{cases}$$

When $G = \mathbb{Z}_n^\times$ we have heuristics and conjectures (involving self-convolutions of $\rho(u)$), but the problem is still open.

Largest primary factor

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ $(q_1^{r_1} \le \cdots \le q_\ell^{r_\ell})$.

If $G = \mathbb{Z}_n^+$, then (almost all the time) the size of the largest primary factor is simply $P(n)$, the largest prime factor of n.

Theorem (Dickman–de Bruijn rho function)

The probability that $P(n)$ is less than n^α equals $\rho(1/\alpha)$, where

$$\begin{cases} \rho(u) = 1, & \text{for } 0 < u \le 1, \\ \rho'(u) = -\rho(u-1)/u, & \text{for } u > 1. \end{cases}$$

When $G = \mathbb{Z}_n^\times$ we have heuristics and conjectures (involving self-convolutions of $\rho(u)$), but the problem is still open.

Largest primary factor

Primary decomposition

Every finite abelian group G is isomorphic to a direct sum of cyclic groups $G \cong \mathbb{Z}^+_{q_1^{r_1}} \oplus \mathbb{Z}^+_{q_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}^+_{q_\ell^{r_\ell}}$ $(q_1^{r_1} \le \cdots \le q_\ell^{r_\ell})$.

If $G = \mathbb{Z}_n^+$, then (almost all the time) the size of the largest primary factor is simply $P(n)$, the largest prime factor of n.

Theorem (Dickman–de Bruijn rho function)

The probability that $P(n)$ is less than n^α equals $\rho(1/\alpha)$, where

$$\begin{cases} \rho(u) = 1, & \text{for } 0 < u \le 1, \\ \rho'(u) = -\rho(u-1)/u, & \text{for } u > 1. \end{cases}$$

When $G = \mathbb{Z}_n^\times$ we have heuristics and conjectures (involving self-convolutions of $\rho(u)$), but the problem is still open.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of order two

Question

How many solutions are there to $x^2 \equiv 1 \pmod{n}$? Equivalently (almost), how many elements of order two are there in $\mathbb{Z}_n^\times$?

Answer, and average value

There are $2^{\omega(n)}$ solutions $\pmod{n}$; and $\frac{1}{x}\sum_{n\le x} 2^{\omega(n)} \sim \frac{6}{\pi^2}\log x$.

Paradox

For almost all integers, $2^{\omega(n)} \approx 2^{\log\log n} = (\log n)^{\log 2}$. But the average value is $\approx (\log x)^1$, which is significantly larger.

So for example, when x is large, 0.1% of the integers up to x have more than 99.9% of the total number of divisors.

Elements of a fixed order

The average number of elements of order 2 is $\frac{6}{\pi^2}\log x$.

Generalization (Finch–M.–Sebah, 2010)

There exists a constant C_k such that the average number of elements of order k in $\mathbb{Z}_n^\times$ is $C_k(\log x)^{\tau(k)-1}$, where $\tau(k)$ is the number of divisors of k. The same holds for the average number of solutions to $x^k \equiv 1 \pmod n$.

Variant (Finch–M.–Sebah)

The average number of solutions to $x^k \equiv 0 \pmod n$ is $D_k(\log x)^{k-1}$, where

$$D_k = \frac{1}{k!(k-1)!}\prod_p \left(1+\frac{k-1}{p}\right)\left(1-\frac{1}{p}\right)^{k-1}$$

Elements of a fixed order

The average number of elements of order 2 is $\frac{6}{\pi^2}\log x$.

Generalization (Finch–M.–Sebah, 2010)

There exists a constant C_k such that the average number of elements of order k in $\mathbb{Z}_n^\times$ is $C_k(\log x)^{\tau(k)-1}$, where $\tau(k)$ is the number of divisors of k. The same holds for the average number of solutions to $x^k \equiv 1 \pmod n$.

Variant (Finch–M.–Sebah)

The average number of solutions to $x^k \equiv 0 \pmod n$ is $D_k(\log x)^{k-1}$, where

$$D_k = \frac{1}{k!(k-1)!}\prod_p \left(1+\frac{k-1}{p}\right)\left(1-\frac{1}{p}\right)^{k-1}$$

Elements of a fixed order

The average number of elements of order 2 is $\frac{6}{\pi^2}\log x$.

Generalization (Finch–M.–Sebah, 2010)

There exists a constant C_k such that the average number of elements of order k in $\mathbb{Z}_n^\times$ is $C_k(\log x)^{\tau(k)-1}$, where $\tau(k)$ is the number of divisors of k. The same holds for the average number of solutions to $x^k \equiv 1 \pmod n$.

Variant (Finch–M.–Sebah)

The average number of solutions to $x^k \equiv 0 \pmod n$ is $D_k(\log x)^{k-1}$, where

$$D_k = \frac{1}{k!(k-1)!}\prod_p \left(1+\frac{k-1}{p}\right)\left(1-\frac{1}{p}\right)^{k-1}$$

Elements of a fixed order

The average number of elements of order 2 is $\frac{6}{\pi^2}\log x$.

Generalization (Finch–M.–Sebah, 2010)

There exists a constant C_k such that the average number of elements of order k in $\mathbb{Z}_n^\times$ is $C_k(\log x)^{\tau(k)-1}$, where $\tau(k)$ is the number of divisors of k. The same holds for the average number of solutions to $x^k \equiv 1 \pmod n$.

Variant (Finch–M.–Sebah)

The average number of solutions to $x^k \equiv 0 \pmod n$ is $D_k(\log x)^{k-1}$, where

$$D_k = \frac{1}{k!(k-1)!}\prod_p \left(1+\frac{k-1}{p}\right)\left(1-\frac{1}{p}\right)^{k-1}$$

Gory details: The constant C_k

Roots of unity

Average number of solutions to $x^k \equiv 1 \pmod n$ is $C_k (\log x)^{\tau(k)-1}$

$$C_k = \frac{\theta(k)}{(\tau(k)-1)!} \prod_p \left(1 + \frac{(k,p-1)}{p-1}\right)\left(1-\frac{1}{p}\right)^{\tau(k)}$$

where $\theta(k)$ is defined as follows: if $k = 2^i k_0$ with k_0 odd, then

$$\theta(k) = \begin{cases} 1, & \text{if } i = 0, \\ (i+5)/4, & \text{if } i \ge 1 \end{cases} \Bigg\} \prod_{p^j \| k_0} \left(1 + \frac{j(k,p-1)(p-1)}{p(p+(k,p-1)-1)}\right)$$

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

- $> \log n$

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

- $> \log n$
- $> \tau(n)$, which at its largest is $\approx n^{(\log 2)/\log\log n}$

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

- $> \log n$
- $> \tau(n)$, which at its largest is $\approx n^{(\log 2)/\log\log n}$
- $> \phi(n)$, which is larger than $\approx n/(\log\log n)$

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

- $> \log n$
- $> \tau(n)$, which at its largest is $\approx n^{(\log 2)/\log\log n}$
- $> \phi(n)$, which is larger than $\approx n/(\log\log n)$
- $> n^{10^{100}}$

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

- $> \log n$
- $> \tau(n)$, which at its largest is $\approx n^{(\log 2)/\log\log n}$
- $> \phi(n)$, which is larger than $\approx n/(\log\log n)$
- $> n^{10^{100}}$

There are infinitely many n . . .

. . . for which $G_n > \exp\left(c(\log n)^2/(\log\log n)^2\right)$ . . . even if we count only subgroups that look like $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$!

The number of subgroups

Definition

Let G_n denote the number of subgroups of $\mathbb{Z}_n^\times$ (as sets, not up to isomorphism).

How big can G_n get?

- $> \log n$
- $> \tau(n)$, which at its largest is $\approx n^{(\log 2)/\log\log n}$
- $> \phi(n)$, which is larger than $\approx n/(\log\log n)$
- $> n^{10^{100}}$

There are infinitely many n . . .

. . . for which $G_n > \exp\left(c(\log n)^2/(\log\log n)^2\right)$ . . . even if we count only subgroups that look like $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$!

Relating G_n to additive functions

$$G(n) = \text{number of subgroups of } \mathbb{Z}_n^\times$$

Notation

Let $\omega_q(n)$ denote the number of primes dividing n that are congruent to $1 \pmod q$.

A sum of squares of additive functions

One can show:

$$\begin{aligned}\log G_n &\approx \tfrac14\big(\omega_2(n)^2 + \omega_3(n)^2 + \omega_4(n)^2 + \omega_5(n)^2 \\ &\qquad + \omega_7(n)^2 + \omega_8(n)^2 + \omega_9(n)^2 + \omega_{11}(n)^2 + \cdots\big) \\ &= \tfrac14 \sum\nolimits_{p^r} \omega_{p^r}(n)^2.\end{aligned}$$

Relating G_n to additive functions

$$G(n) = \text{number of subgroups of } \mathbb{Z}_n^\times$$

Notation

Let $\omega_q(n)$ denote the number of primes dividing n that are congruent to $1 \pmod q$.

A sum of squares of additive functions

One can show:

$$\begin{aligned}\log G_n &\approx \tfrac14\big(\omega_2(n)^2 + \omega_3(n)^2 + \omega_4(n)^2 + \omega_5(n)^2 \\ &\qquad + \omega_7(n)^2 + \omega_8(n)^2 + \omega_9(n)^2 + \omega_{11}(n)^2 + \cdots\big) \\ &= \tfrac14 \sum_{p^r} \omega_{p^r}(n)^2.\end{aligned}$$

Relating G_n to additive functions

$$G(n) = \text{number of subgroups of } \mathbb{Z}_n^\times$$

Notation

Let $\omega_q(n)$ denote the number of primes dividing n that are congruent to $1 \pmod q$.

A sum of squares of additive functions

One can show:

$$\begin{aligned}\log G_n &\approx \tfrac14\big(\omega_2(n)^2 + \omega_3(n)^2 + \omega_4(n)^2 + \omega_5(n)^2 \\ &\qquad + \omega_7(n)^2 + \omega_8(n)^2 + \omega_9(n)^2 + \omega_{11}(n)^2 + \cdots\big) \\ &= \tfrac14 \sum_{p^r} \omega_{p^r}(n)^2.\end{aligned}$$

Aspirations

$G(n) =$ number of subgroups of $\mathbb{Z}_n^\times$

Work currently in progress

I plan to establish an Erdős–Kac-type theorem demonstrating a Gaussian distribution not just for additive functions, but for products of additive functions, and sums of such products.

Hopeful theorem

I believe I can show:

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \log G_n - A(\log\log n)^2 < \alpha\sqrt{B(\log\log n)^3} \right\}$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\,dt = \Phi(\alpha).$$

Aspirations

$G(n) =$ number of subgroups of $\mathbb{Z}_n^\times$

Work currently in progress

I plan to establish an Erdős–Kac-type theorem demonstrating a Gaussian distribution not just for additive functions, but for products of additive functions, and sums of such products.

Hopeful theorem

I believe I can show:

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \log G_n - A(\log\log n)^2 < \alpha\sqrt{B(\log\log n)^3} \right\}$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\,dt = \Phi(\alpha).$$

Gory details: The constants A and B

Hopeful theorem

$$\lim_{x\to\infty} \frac{1}{x} \#\left\{ n \le x : \ \log G_n - A(\log\log n)^2 < \alpha\sqrt{B(\log\log n)^3} \right\}$$
$$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\alpha} e^{-t^2/2}\, dt = \Phi(\alpha)$$

$$A = \tfrac{1}{4} \sum_p \frac{p^2 \log p}{(p-1)^3(p+1)} \approx 0.374516$$

$$B = 4A^2 + \tfrac{1}{4} \sum_p \frac{p^3(p^4 - p^3 - p^2 - p - 1)(\log p)^2}{(p-1)^6(p+1)^2(p^2+p+1)} \approx 0.617393$$

The end

These slides

www.math.ubc.ca/∼gerg/index.shtml?slides

My paper with Pomerance on $\lambda(\lambda(n))$

www.math.ubc.ca/∼gerg/index.shtml?abstract=ICFNCPG

My paper with Finch and Sebah on roots of 1 and 0

www.math.ubc.ca/∼gerg/index.shtml?abstract=RUNM

The end

These slides

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

My paper with Pomerance on $\lambda(\lambda(n))$

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

My paper with Finch and Sebah on roots of 1 and 0

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

My papers on products of additive functions and subgroups of $\mathbb{Z}_n^\times$

Keep an eye on the arXiv!

The end

These slides

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

My paper with Pomerance on $\lambda(\lambda(n))$

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

My paper with Finch and Sebah on roots of 1 and 0

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

My papers on products of additive functions and subgroups of $\mathbb{Z}_n^\times$

Keep an eye on the arXiv! *(but don't hold your breath...)*