Statistics of the multiplicative group

Greg Martin
University of British Columbia

joint work with Ben Chang, Jenna Downey, and Lee Troupe (in parallel)

UNSW–Sydney Number Theory Seminar
November 21, 2018

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

Outline

What is the multiplicative group?

The finite ring $\mathbb{Z}/n\mathbb{Z}$ has:

- a cyclic additive group $C_n = (\mathbb{Z}/n\mathbb{Z})^+$ with n elements;
- an abelian multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$ with $\phi(n)$ elements.

Overarching question

Which abelian group of $\phi(n)$ elements is M_n?

For example, M_n being cyclic is equivalent to n having a primitive root.

Two forms that answers to the question can take

- primary decomposition: $G \cong C_{p_1^{r_1}} \oplus \cdots \oplus C_{p_k^{r_k}}$, where the $p_j^{r_j}$ are prime powers (unique up to reordering)
- invariant factors: $G \cong C_{m_1} \oplus \cdots \oplus C_{m_\ell}$, where $m_1 \mid m_2 \mid \cdots \mid m_\ell$ (unique)

What is the multiplicative group?

The finite ring $\mathbb{Z}/n\mathbb{Z}$ has:

- a cyclic additive group $C_n = (\mathbb{Z}/n\mathbb{Z})^+$ with n elements;
- an abelian multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$ with $\phi(n)$ elements.

Overarching question

Which abelian group of $\phi(n)$ elements is M_n?

For example, M_n being cyclic is equivalent to n having a primitive root.

Two forms that answers to the question can take

- primary decomposition: $G \cong C_{p_1^{r_1}} \oplus \cdots \oplus C_{p_k^{r_k}}$, where the $p_j^{r_j}$ are prime powers (unique up to reordering)
- invariant factors: $G \cong C_{m_1} \oplus \cdots \oplus C_{m_\ell}$, where $m_1 \mid m_2 \mid \cdots \mid m_\ell$ (unique)

What is the multiplicative group?

The finite ring $\mathbb{Z}/n\mathbb{Z}$ has:

- a cyclic additive group $C_n = (\mathbb{Z}/n\mathbb{Z})^+$ with n elements;
- an abelian multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$ with $\phi(n)$ elements.

Overarching question

Which abelian group of $\phi(n)$ elements is M_n?

For example, M_n being cyclic is equivalent to n having a primitive root.

Two forms that answers to the question can take

- primary decomposition: $G \cong C_{p_1^{r_1}} \oplus \cdots \oplus C_{p_k^{r_k}}$, where the $p_j^{r_j}$ are prime powers (unique up to reordering)
- invariant factors: $G \cong C_{m_1} \oplus \cdots \oplus C_{m_\ell}$, where $m_1 \mid m_2 \mid \cdots \mid m_\ell$ (unique)

What is the multiplicative group?

The finite ring $\mathbb{Z}/n\mathbb{Z}$ has:

- a cyclic additive group $C_n = (\mathbb{Z}/n\mathbb{Z})^+$ with n elements;
- an abelian multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$ with $\phi(n)$ elements.

Overarching question

Which abelian group of $\phi(n)$ elements is M_n?

For example, M_n being cyclic is equivalent to n having a primitive root.

Two forms that answers to the question can take

- primary decomposition: $G \cong C_{p_1^{r_1}} \oplus \cdots \oplus C_{p_k^{r_k}}$, where the $p_j^{r_j}$ are prime powers (unique up to reordering)
- invariant factors: $G \cong C_{m_1} \oplus \cdots \oplus C_{m_\ell}$, where $m_1 \mid m_2 \mid \cdots \mid m_\ell$ (unique)

Number theory within a computation of M_n

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

$$\begin{aligned} M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\ &\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\ &\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\ &\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640} \end{aligned}$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$
\begin{aligned}
M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\
&\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\
&\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\
&\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\
&\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\
&\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}
\end{aligned}
$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$\begin{aligned} M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\ &\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\ &\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\ &\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640} \end{aligned}$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$
\begin{aligned}
M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\
&\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\
&\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\
&\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\
&\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\
&\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}
\end{aligned}
$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$\begin{aligned} M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\ &\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\ &\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\ &\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640} \end{aligned}$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$\begin{aligned} M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\ &\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\ &\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\ &\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640} \end{aligned}$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$\begin{aligned} M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\ &\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\ &\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\ &\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\ &\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640} \end{aligned}$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

Number theory within a computation of M_n

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

$$
\begin{aligned}
M_{11!} &\cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11} \\
&\cong (C_2 \oplus C_{64}) \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10} \\
&\cong (C_2 \oplus C_{64}) \oplus (C_2 \oplus C_{27}) \\
&\qquad \oplus (C_4 \oplus C_5) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_5) \\
&\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus (C_4 \oplus C_3 \oplus C_5) \oplus (C_{64} \oplus C_{27} \oplus C_5) \\
&\cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}
\end{aligned}
$$

Largest invariant factor

$8{,}640 = \lambda(11!)$ (Carmichael lambda-function)

Number of invariant factors

- When n odd: exactly $\omega(n) = \#\{p \mid n\}$
- When n even: $\omega(n) - 1$ or $\omega(n)$ or $\omega(n) + 1$

What's known about $\lambda(n)$

For purposes of comparison

$\phi(n)$ is never smaller than $(e^{-\gamma} + o(1))n/\log\log n$.

Theorem (Erdős/Pomerance/Schmutz, 1991)

For almost all integers n,

$$\lambda(n) = n/\exp\big((1+o(1))\log n \log\log n\big).$$

In other words, the normal order of $\log\big(n/\lambda(n)\big)$ is $\log n \log\log n$.

Drive-by question

What about the second-largest invariant factor, $\lambda_2(n)$?

- $\lambda(n) = \min\big\{k \ge 1 : a^k \in \langle 1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.
- Pick a reduced residue a_1 of order $\lambda(n)$. Then $\lambda_2(n) = \min\big\{k \ge 1 : a^k \in \langle 1, a_1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.

What's known about $\lambda(n)$

For purposes of comparison

$\phi(n)$ is never smaller than $(e^{-\gamma} + o(1))n/\log\log n$.

Theorem (Erdős/Pomerance/Schmutz, 1991)

For almost all integers n,

$$\lambda(n) = n/\exp\big((1+o(1))\log n \log\log n\big).$$

In other words, the normal order of $\log\big(n/\lambda(n)\big)$ is $\log n \log\log n$.

Drive-by question

What about the second-largest invariant factor, $\lambda_2(n)$?

- $\lambda(n) = \min\big\{k \ge 1 : a^k \in \langle 1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.
- Pick a reduced residue a_1 of order $\lambda(n)$. Then $\lambda_2(n) = \min\big\{k \ge 1 : a^k \in \langle 1, a_1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.

What's known about $\lambda(n)$

For purposes of comparison

$\phi(n)$ is never smaller than $(e^{-\gamma} + o(1))n/\log\log n$.

Theorem (Erdős/Pomerance/Schmutz, 1991)

For almost all integers n,

$$\lambda(n) = n/\exp\big((1+o(1))\log n \log\log n\big).$$

In other words, the normal order of $\log\big(n/\lambda(n)\big)$ is $\log n \log\log n$.

Drive-by question

What about the second-largest invariant factor, $\lambda_2(n)$?

- $\lambda(n) = \min\big\{k \ge 1 : a^k \in \langle 1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.
- Pick a reduced residue a_1 of order $\lambda(n)$. Then $\lambda_2(n) = \min\big\{k \ge 1 : a^k \in \langle 1, a_1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.

What's known about $\lambda(n)$

For purposes of comparison

$\phi(n)$ is never smaller than $(e^{-\gamma} + o(1))n/\log\log n$.

Theorem (Erdős/Pomerance/Schmutz, 1991)

For almost all integers n,

$$\lambda(n) = n/\exp\big((1+o(1))\log n \log\log n\big).$$

In other words, the normal order of $\log\big(n/\lambda(n)\big)$ is $\log n \log\log n$.

Drive-by question

What about the second-largest invariant factor, $\lambda_2(n)$?

- $\lambda(n) = \min\big\{k \ge 1 : a^k \in \langle 1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.
- Pick a reduced residue a_1 of order $\lambda(n)$. Then $\lambda_2(n) = \min\big\{k \ge 1 : a^k \in \langle 1, a_1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.

What's known about $\lambda(n)$

For purposes of comparison

$\phi(n)$ is never smaller than $(e^{-\gamma} + o(1))n/\log\log n$.

Theorem (Erdős/Pomerance/Schmutz, 1991)

For almost all integers n,

$$\lambda(n) = n/\exp\big((1+o(1))\log n \log\log n\big).$$

In other words, the normal order of $\log\big(n/\lambda(n)\big)$ is $\log n \log\log n$.

Drive-by question

What about the second-largest invariant factor, $\lambda_2(n)$?

- $\lambda(n) = \min\big\{k \ge 1 : a^k \in \langle 1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.
- Pick a reduced residue a_1 of order $\lambda(n)$. Then $\lambda_2(n) = \min\big\{k \ge 1 : a^k \in \langle 1, a_1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.

What's known about $\lambda(n)$

For purposes of comparison

$\phi(n)$ is never smaller than $(e^{-\gamma} + o(1))n/\log\log n$.

Theorem (Erdős/Pomerance/Schmutz, 1991)

For almost all integers n,

$$\lambda(n) = n/\exp\big((1+o(1))\log n \log\log n\big).$$

In other words, the normal order of $\log\big(n/\lambda(n)\big)$ is $\log n \log\log n$.

Drive-by question

What about the second-largest invariant factor, $\lambda_2(n)$?

- $\lambda(n) = \min\big\{k \ge 1 : a^k \in \langle 1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.
- Pick a reduced residue a_1 of order $\lambda(n)$. Then $\lambda_2(n) = \min\big\{k \ge 1 : a^k \in \langle 1, a_1\rangle \pmod n \text{ for all } (a,n)=1\big\}$.

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 $\sum_{n\le x}\bigl(\omega(n)-\log\log n\bigr)^2$
- 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 $\sum_{n\le x}\bigl(\omega(n)-\log\log n\bigr)^k$

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 $\sum_{n\le x}\bigl(\omega(n)-\log\log n\bigr)^2$
- 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 $\sum_{n\le x}\bigl(\omega(n)-\log\log n\bigr)^k$

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

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

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

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

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

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

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

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

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

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

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

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

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 $\Omega(\phi(n)) = \Omega(p_1^{r_1}) + \cdots + \Omega(p_k^{r_k})$.

A different question about the multiplicative group

Notation reminder

$M_n = \mathbb{Z}_n^\times$, an abelian group with $\phi(n)$ elements.

Question (Vukoslavcevic and Shparlinski, 2010)

How many subgroups does M_n have?

Notation (used throughout this section of the talk)

- $I(n)$ is the number of isomorphism classes of subgroups of M_n.
- $G(n)$ is the number of subsets of M_n that are subgroups (that is, subgroups not up to isomorphism).

A different question about the multiplicative group

Notation reminder

$M_n = \mathbb{Z}_n^\times$, an abelian group with $\phi(n)$ elements.

Question (Vukoslavcevic and Shparlinski, 2010)

How many subgroups does M_n have?

Notation (used throughout this section of the talk)

- $I(n)$ is the number of isomorphism classes of subgroups of M_n.
- $G(n)$ is the number of subsets of M_n that are subgroups (that is, subgroups not up to isomorphism).

A different question about the multiplicative group

Notation reminder

$M_n = \mathbb{Z}_n^\times$, an abelian group with $\phi(n)$ elements.

Question (Vukoslavcevic and Shparlinski, 2010)

How many subgroups does M_n have?

Notation (used throughout this section of the talk)

- $I(n)$ is the number of isomorphism classes of subgroups of M_n.
- $G(n)$ is the number of subsets of M_n that are subgroups (that is, subgroups not up to isomorphism).

A different question about the multiplicative group

Notation reminder

$M_n = \mathbb{Z}_n^\times$, an abelian group with $\phi(n)$ elements.

Question (Vukoslavcevic and Shparlinski, 2010)

How many subgroups does M_n have?

Notation (used throughout this section of the talk)

- $I(n)$ is the number of isomorphism classes of subgroups of M_n.
- $G(n)$ is the number of subsets of M_n that are subgroups (that is, subgroups not up to isomorphism).

The number of subgroups has a similar property

Getting used to the notation

$I(n)$ is the number of isomorphism classes of subgroups of M_n.
$G(n)$ is the number of subsets of M_n 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 M_n, then $G(n) = \prod_{p \mid \#M_n} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

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

Getting used to the notation

$I(n)$ is the number of isomorphism classes of subgroups of M_n.
$G(n)$ is the number of subsets of M_n 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 M_n, then $G(n) = \prod_{p \mid \#M_n} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

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

Getting used to the notation

$I(n)$ is the number of isomorphism classes of subgroups of M_n.
$G(n)$ is the number of subsets of M_n 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 M_n, then $G(n) = \prod_{p|\#M_n} G_p(n) = \prod_{p|\phi(n)} G_p(n)$.

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

Getting used to the notation

$I(n)$ is the number of isomorphism classes of subgroups of M_n.
$G(n)$ is the number of subsets of M_n 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 M_n, then $G(n) = \prod_{p \mid \#M_n} G_p(n) = \prod_{p \mid \phi(n)} G_p(n)$.

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

Getting used to the notation

$I(n)$ is the number of isomorphism classes of subgroups of M_n.
$G(n)$ is the number of subsets of M_n 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 M_n, then $G(n) = \prod_{p|\#M_n} G_p(n) = \prod_{p|\phi(n)} G_p(n)$.

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, to appear in the Journal of the Australian Mathematical Society)

$\log I(n)$ 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. □

Theorem (M.–Troupe)

$\log G(n)$ 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, to appear in the Journal of the Australian Mathematical Society)

$\log I(n)$ 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. □

Theorem (M.–Troupe)

$\log G(n)$ 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, to appear in the Journal of the Australian Mathematical Society)

$\log I(n)$ 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. □

Theorem (M.–Troupe)

$\log G(n)$ 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, to appear in the Journal of the Australian Mathematical Society)

$\log I(n)$ *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. □

Theorem (M.–Troupe)

$\log G(n)$ *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)

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)

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 $G(n) > n^{2018!}$ ...

How many subgroups can there be?

Theorem (M.–Troupe)

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)

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 $G(n) > n^{2018!}$ ...

How many subgroups can there be?

Theorem (M.–Troupe)

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)

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 $G(n) > n^{2018!}$ ...

Finite abelian groups and partitions

Facts about finite abelian p-groups

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

... 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 $C_{p^{\boldsymbol{\alpha}}} = C_{p^{\alpha_1}} \oplus C_{p^{\alpha_2}} \oplus \cdots \oplus C_{p^{\alpha_\ell}}$ for some partition $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_\ell)$ of m (so $\alpha_1 \ge \alpha_2 \ge \cdots \ge \alpha_\ell$).
- So the number of isomorphism classes of subgroups of $C_{p^{\boldsymbol{\alpha}}}$ is exactly the number of subpartitions $\boldsymbol{\beta} \preceq \boldsymbol{\alpha}$ ...

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

In other words:

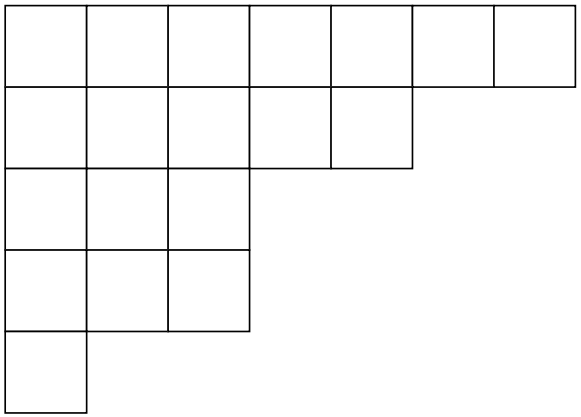
$\log \#\{\text{subpartitions of } \boldsymbol{\alpha}\}$ is between $\log 2$ and $m \log 2$.

Finite abelian groups and partitions

Facts about finite abelian p-groups

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

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



In other words:

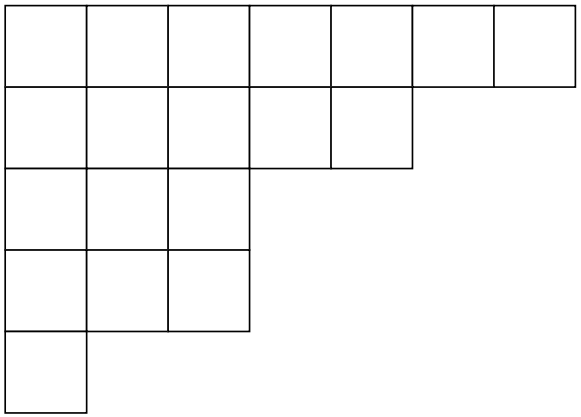
$\log \#\{\text{subpartitions of } \boldsymbol{\alpha}\}$ is between $\log 2$ and $m \log 2$.

Finite abelian groups and partitions

Facts about finite abelian p-groups

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

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



In other words:

$\log \#\{\text{subpartitions of } \boldsymbol{\alpha}\}$ 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 M_n

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$ 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 M_n

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$ 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 M_n

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$ 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 M_n

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$ 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 M_n

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$ 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 M_n

More notation

Let $\phi(n) = \prod_{p|\phi(n)} p^{m(p)}$, so that $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$ 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.

How many subgroups of each shape?

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

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 $C_{p^{\boldsymbol{\alpha}}}$ that are isomorphic to $C_{p^{\boldsymbol{\beta}}}$.

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: $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_\ell)$, $C_{p^{\boldsymbol{\alpha}}} = C_{p^{\alpha_1}} \oplus \cdots \oplus C_{p^{\alpha_\ell}}$

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 $C_{p^{\boldsymbol{\alpha}}}$ that are isomorphic to $C_{p^{\boldsymbol{\beta}}}$.

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 $C_{p^{\boldsymbol{\alpha}}}$ isomorphic to $C_{p^{\boldsymbol{\beta}}}$.

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 C_{p^α} is dominated by this special $\beta = \text{“}\frac{1}{2}\alpha\text{”}$.

Lemma

For any prime p and any partition α,

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

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 $C_{p^{\boldsymbol{\alpha}}}$ isomorphic to $C_{p^{\boldsymbol{\beta}}}$.

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 $C_{p^{\boldsymbol{\alpha}}}$ is dominated by this special $\boldsymbol{\beta} = \text{“}\frac{1}{2}\boldsymbol{\alpha}\text{”}$.

Lemma

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

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

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 $C_{p^{\boldsymbol{\alpha}}}$ isomorphic to $C_{p^{\boldsymbol{\beta}}}$.

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 $C_{p^{\boldsymbol{\alpha}}}$ is dominated by this special $\boldsymbol{\beta} = \text{“}\frac{1}{2}\boldsymbol{\alpha}\text{”}$.

Lemma

For any prime p and any partition α,

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

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 $C_{p^{\boldsymbol{\alpha}}}$ isomorphic to $C_{p^{\boldsymbol{\beta}}}$.

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 $C_{p^{\boldsymbol{\alpha}}}$ is dominated by this special $\boldsymbol{\beta} = \text{“}\frac{1}{2}\boldsymbol{\alpha}\text{”}$.

Lemma

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

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

If $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$, 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 $\big(\omega_p(n), \omega_{p^2}(n), \dots\big)$.

Lemma

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

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

If $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$, 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 $\big(\omega_p(n), \omega_{p^2}(n), \dots\big)$.

Lemma

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

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

If $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$, 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 $\big(\omega_p(n), \omega_{p^2}(n), \dots\big)$.

Lemma

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

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

If $M_n \cong \bigoplus_{p|\phi(n)} C_{p^{\alpha(p)}}$, 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 $\big(\omega_p(n), \omega_{p^2}(n), \dots\big)$.

Lemma

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

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 (just submitted!) 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 (just submitted!) 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 (just submitted!) 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 (just submitted!) 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.

Prohibited prime factors: related problems

Let q be a fixed odd prime.

Definition

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

Question (Colin Weir, 2017)

If we fix our favorite prime q and our favorite group G, how often will we get G as the exact q-Sylow subgroup of M_n?

Definition

$S_{q,G}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

Prohibited prime factors: related problems

Let q be a fixed odd prime.

Definition

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

Question (Colin Weir, 2017)

If we fix our favorite prime q and our favorite group G, how often will we get G as the exact q-Sylow subgroup of M_n?

Definition

$S_{q,G}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

Prohibited prime factors: related problems

Let q be a fixed odd prime.

Definition

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

Question (Colin Weir, 2017)

If we fix our favorite prime q and our favorite group G, how often will we get G as the exact q-Sylow subgroup of M_n?

Definition

$S_{q,G}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

The trivial example

Another translation of algebra to number theory

$$\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\}$$
$$= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.$$

Example (when $G = \{1\}$ is trivial)

$$S_{q,\{1\}}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}:$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\}$$
$$= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.$$

Example (when $G = \{1\}$ is trivial)

$$S_{q,\{1\}}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}\colon$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\}$$
$$= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.$$

Example (when $G = \{1\}$ is trivial)

$$S_{q,\{1\}}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}\colon$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\}$$
$$= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.$$

Example (when $G = \{1\}$ is trivial)

$$S_{q,\{1\}}(x) = \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\}$$
$$= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}\colon$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\begin{aligned}\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} &= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\} \\ &= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.\end{aligned}$$

Example (when $G = \{1\}$ is trivial)

$$\begin{aligned}S_{q,\{1\}}(x) &= \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} \\ &= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}:\end{aligned}$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\begin{aligned}\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} &= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\} \\ &= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.\end{aligned}$$

Example (when $G = \{1\}$ is trivial)

$$\begin{aligned}S_{q,\{1\}}(x) &= \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} \\ &= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}:\end{aligned}$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\begin{aligned}\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} &= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\} \\ &= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.\end{aligned}$$

Example (when $G = \{1\}$ is trivial)

$$\begin{aligned}S_{q,\{1\}}(x) &= \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} \\ &= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}:\end{aligned}$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$.

Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

The trivial example

Another translation of algebra to number theory

$$\begin{aligned}\{n\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} &= \{n\colon q \text{ does not divide } \#M_n = \phi(n)\} \\ &= \{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}.\end{aligned}$$

Example (when $G = \{1\}$ is trivial)

$$\begin{aligned}S_{q,\{1\}}(x) &= \#\{n \le x\colon \text{the } q\text{-Sylow subgroup of } M_n \text{ is trivial}\} \\ &= \#\{n\colon \big(p \mid n \implies p \not\equiv 1 \pmod q\big) \text{ and } q^2 \nmid n\}:\end{aligned}$$

we prohibit prime factors from a set of relative density $1/(q-1)$.

General philosophy

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $S_{q,\{1\}}(x) \asymp x/(\log x)^{1/(q-1)}$.

Analytic number theorists can do this

Theorems of this type go back to Landau; today it would be deemed a standard application of the Selberg–Delange method; this particular application (other than the extra $q^2 \nmid n$) was carried out by Ford/Luca/Moree (Math Comp., 2014).

Theorem

$$S_{q,\{1\}} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})}\left(1-\frac{1}{q^2}\right)\frac{x}{(\log x)^{1/(q-1)}};$$

here

$$C_q = \left((1-\tfrac{1}{q})\prod_{\chi\neq\chi_0} L(1,\chi)\right)^{-1/(q-1)} \prod_{p\not\equiv 0,1 \pmod q}\left(1-\frac{1}{p^{k_p}}\right)^{-1/k_p},$$

where k_p is the multiplicative order of p modulo q.

Analytic number theorists can do this

Theorems of this type go back to Landau; today it would be deemed a standard application of the Selberg–Delange method; this particular application (other than the extra $q^2 \nmid n$) was carried out by Ford/Luca/Moree (Math Comp., 2014).

Theorem

$$S_{q,\{1\}} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})}\left(1-\frac{1}{q^2}\right)\frac{x}{(\log x)^{1/(q-1)}};$$

here

$$C_q = \left((1-\tfrac{1}{q})\prod_{\chi\neq\chi_0} L(1,\chi)\right)^{-1/(q-1)} \prod_{p\not\equiv 0,1 \pmod q}\left(1-\frac{1}{p^{k_p}}\right)^{-1/k_p},$$

where k_p is the multiplicative order of p modulo q.

Analytic number theorists can do this

Theorems of this type go back to Landau; today it would be deemed a standard application of the Selberg–Delange method; this particular application (other than the extra $q^2 \nmid n$) was carried out by Ford/Luca/Moree (Math Comp., 2014).

Theorem

$$S_{q,\{1\}} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})}\left(1-\frac{1}{q^2}\right)\frac{x}{(\log x)^{1/(q-1)}};$$

here

$$C_q = \left((1-\tfrac{1}{q})\prod_{\chi\neq\chi_0} L(1,\chi)\right)^{-1/(q-1)} \prod_{p\not\equiv 0,1 \pmod q}\left(1-\frac{1}{p^{k_p}}\right)^{-1/k_p},$$

where k_p is the multiplicative order of p modulo q.

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The general case

Suppose now that $G = C_{q^\alpha}$:

- Typically this q-Sylow subgroup of M_n arises from a single prime $p \mid n$ with $q^\alpha \| (p-1)$, and the other factor $\frac{n}{p}$ of the form discussed in the trivial example.
- For each possible p, we thus get a contribution of $\asymp \frac{x}{p}/(\log \frac{x}{p})^{1/(q-1)}$, or more simply, $\asymp \frac{x}{p}/(\log x)^{1/(q-1)}$.
- Summing over possible p yields $\asymp \frac{\log\log x}{q^\alpha} x/(\log x)^{1/(q-1)}$.

(Need to tread more carefully; we found a nice argument using partial summation, asymptotics for hypergeometric functions.)

In general, when $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$:

Identify a prime $p \mid n$ with $q^{\alpha_\ell} \| (p-1)$; the cofactor $\frac{n}{p}$ will be an example with $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_{\ell-1}}}$; then recurse. . . .

The result

Theorem (Downey–M., 2019)

If $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$, *then*

$$S_{q,G} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})} \left(\prod_{j=1}^{\infty} \frac{1}{n_j!} \right) \left(\frac{q^2-1}{q^{2+\alpha_1+\cdots+\alpha_\ell}} \right) \frac{x(\log\log x)^\ell}{(\log x)^{1/(q-1)}},$$

where $n_j = \#\{i : \alpha_i = j\}$*; as before,*

$$C_q = \left((1-\tfrac{1}{q}) \prod_{\chi \neq \chi_0} L(1,\chi) \right)^{-1/(q-1)} \prod_{p \not\equiv 0,1 \pmod q} \left(1 - \frac{1}{p^{k_p}}\right)^{-1/k_p},$$

where k_p *is the multiplicative order of* p *modulo* q*.*

The result

Theorem (Downey–M., 2019)

If $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$, *then*

$$S_{q,G} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})} \left(\prod_{j=1}^{\infty} \frac{1}{n_j!} \right) \left(\frac{q^2-1}{q^{2+\alpha_1+\cdots+\alpha_\ell}} \right) \frac{x(\log\log x)^\ell}{(\log x)^{1/(q-1)}},$$

where $n_j = \#\{i : \alpha_i = j\}$; *as before,*

$$C_q = \left((1-\tfrac{1}{q}) \prod_{\chi \neq \chi_0} L(1,\chi) \right)^{-1/(q-1)} \prod_{p \not\equiv 0,1 \pmod q} \left(1 - \frac{1}{p^{k_p}}\right)^{-1/k_p},$$

where k_p *is the multiplicative order of* p *modulo* q.

The result

Theorem (Downey–M., 2019)

If $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$, *then*

$$S_{q,G} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})} \left(\prod_{j=1}^{\infty} \frac{1}{n_j!} \right) \left(\frac{q^2-1}{q^{2+\alpha_1+\cdots+\alpha_\ell}} \right) \frac{x(\log\log x)^\ell}{(\log x)^{1/(q-1)}},$$

where $n_j = \#\{i : \alpha_i = j\}$; *as before,*

$$C_q = \left((1-\tfrac{1}{q}) \prod_{\chi \neq \chi_0} L(1,\chi) \right)^{-1/(q-1)} \prod_{p \not\equiv 0,1 \pmod q} \left(1 - \frac{1}{p^{k_p}}\right)^{-1/k_p},$$

where k_p *is the multiplicative order of* p *modulo* q.

The result

Theorem (Downey–M., 2019)

If $G = C_{q^{\alpha_1}} \oplus \cdots \oplus C_{q^{\alpha_\ell}}$, *then*

$$S_{q,G} \sim \frac{C_q}{\Gamma(1-\frac{1}{q-1})} \left(\prod_{j=1}^{\infty} \frac{1}{n_j!} \right) \left(\frac{q^2-1}{q^{2+\alpha_1+\cdots+\alpha_\ell}} \right) \frac{x(\log\log x)^\ell}{(\log x)^{1/(q-1)}},$$

where $n_j = \#\{i : \alpha_i = j\}$; *as before,*

$$C_q = \left((1-\tfrac{1}{q}) \prod_{\chi \neq \chi_0} L(1,\chi) \right)^{-1/(q-1)} \prod_{p \not\equiv 0,1 \pmod q} \left(1 - \frac{1}{p^{k_p}} \right)^{-1/k_p},$$

where k_p *is the multiplicative order of* p *modulo* q.

An M_n with a larger least invariant factor

Recall: $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}$

Example: M_n when $n = 3^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

$$\begin{aligned} M_n &\cong M_{3^3} \times M_{7^2} \times M_{13} \times M_{19} \times M_{31} \\ &\cong C_{18} \oplus C_{42} \oplus C_{12} \oplus C_{18} \oplus C_{30} \\ &\cong (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_7) \\ &\qquad \oplus (C_4 \oplus C_3) \oplus (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_5) \\ &\cong (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \\ &\qquad \oplus (C_2 \oplus C_9) \oplus (C_4 \oplus C_9 \oplus C_5 \oplus C_7) \\ &\cong C_6 \oplus C_6 \oplus C_6 \oplus C_{18} \oplus C_{1,260}. \end{aligned}$$

We forced the least invariant factor of M_n to exceed 2 by choosing only primes congruent to $1 \pmod 6$ (other than the power of 3 dividing n).

An M_n with a larger least invariant factor

Recall: $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}$

Example: M_n when $n = 3^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

$$\begin{aligned} M_n &\cong M_{3^3} \times M_{7^2} \times M_{13} \times M_{19} \times M_{31} \\ &\cong C_{18} \oplus C_{42} \oplus C_{12} \oplus C_{18} \oplus C_{30} \\ &\cong (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_7) \\ &\qquad \oplus (C_4 \oplus C_3) \oplus (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_5) \\ &\cong (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \\ &\qquad \oplus (C_2 \oplus C_9) \oplus (C_4 \oplus C_9 \oplus C_5 \oplus C_7) \\ &\cong C_6 \oplus C_6 \oplus C_6 \oplus C_{18} \oplus C_{1,260}. \end{aligned}$$

We forced the least invariant factor of M_n to exceed 2 by choosing only primes congruent to $1 \pmod 6$ (other than the power of 3 dividing n).

An M_n with a larger least invariant factor

Recall: $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}$

Example: M_n when $n = 3^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

$$\begin{aligned} M_n &\cong M_{3^3} \times M_{7^2} \times M_{13} \times M_{19} \times M_{31} \\ &\cong C_{18} \oplus C_{42} \oplus C_{12} \oplus C_{18} \oplus C_{30} \\ &\cong (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_7) \\ &\qquad \oplus (C_4 \oplus C_3) \oplus (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_5) \\ &\cong (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \\ &\qquad \oplus (C_2 \oplus C_9) \oplus (C_4 \oplus C_9 \oplus C_5 \oplus C_7) \\ &\cong C_6 \oplus C_6 \oplus C_6 \oplus C_{18} \oplus C_{1,260}. \end{aligned}$$

We forced the least invariant factor of M_n to exceed 2 by choosing only primes congruent to $1 \pmod 6$ (other than the power of 3 dividing n).

An M_n with a larger least invariant factor

Recall: $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}$

Example: M_n when $n = 3^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

$$\begin{aligned} M_n &\cong M_{3^3} \times M_{7^2} \times M_{13} \times M_{19} \times M_{31} \\ &\cong C_{18} \oplus C_{42} \oplus C_{12} \oplus C_{18} \oplus C_{30} \\ &\cong (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_7) \\ &\qquad \oplus (C_4 \oplus C_3) \oplus (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_5) \\ &\cong (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \\ &\qquad \oplus (C_2 \oplus C_9) \oplus (C_4 \oplus C_9 \oplus C_5 \oplus C_7) \\ &\cong C_6 \oplus C_6 \oplus C_6 \oplus C_{18} \oplus C_{1,260}. \end{aligned}$$

We forced the least invariant factor of M_n to exceed 2 by choosing only primes congruent to $1 \pmod 6$ (other than the power of 3 dividing n).

An M_n with a larger least invariant factor

Recall: $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}$

Example: M_n when $n = 3^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

$$\begin{aligned} M_n &\cong M_{3^3} \times M_{7^2} \times M_{13} \times M_{19} \times M_{31} \\ &\cong C_{18} \oplus C_{42} \oplus C_{12} \oplus C_{18} \oplus C_{30} \\ &\cong (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_7) \\ &\qquad \oplus (C_4 \oplus C_3) \oplus (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_5) \\ &\cong (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \\ &\qquad \oplus (C_2 \oplus C_9) \oplus (C_4 \oplus C_9 \oplus C_5 \oplus C_7) \\ &\cong C_6 \oplus C_6 \oplus C_6 \oplus C_{18} \oplus C_{1,260}. \end{aligned}$$

We forced the least invariant factor of M_n to exceed 2 by choosing only primes congruent to $1 \pmod 6$ (other than the power of 3 dividing n).

An M_n with a larger least invariant factor

Recall: $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8,640}$

Example: M_n when $n = 3^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$

$$\begin{aligned} M_n &\cong M_{3^3} \times M_{7^2} \times M_{13} \times M_{19} \times M_{31} \\ &\cong C_{18} \oplus C_{42} \oplus C_{12} \oplus C_{18} \oplus C_{30} \\ &\cong (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_7) \\ &\qquad \oplus (C_4 \oplus C_3) \oplus (C_2 \oplus C_9) \oplus (C_2 \oplus C_3 \oplus C_5) \\ &\cong (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \oplus (C_2 \oplus C_3) \\ &\qquad \oplus (C_2 \oplus C_9) \oplus (C_4 \oplus C_9 \oplus C_5 \oplus C_7) \\ &\cong C_6 \oplus C_6 \oplus C_6 \oplus C_{18} \oplus C_{1,260}. \end{aligned}$$

We forced the least invariant factor of M_n to exceed 2 by choosing only primes congruent to $1 \pmod 6$ (other than the power of 3 dividing n).

Counting "unusually large" smallest invariant factors

The least invariant factor of M_n equals 2 for almost all integers n. But we can be more precise:

Theorem (Chang–M., 2016+)

The number of integers $n \le x$ for which the least invariant factor of M_n does not equal 2 is

$$C \frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{3/4-\varepsilon}} \right)$$

for a particular positive constant C (not the same one as before).

We also obtain the same result (with a different value of C) for integers for which the least primary-decomposition factor of M_n does not equal 2.

Counting "unusually large" smallest invariant factors

The least invariant factor of M_n equals 2 for almost all integers n. But we can be more precise:

Theorem (Chang–M., 2016+)

The number of integers $n \le x$ for which the least invariant factor of M_n does not equal 2 is

$$C\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{3/4-\varepsilon}}\right)$$

for a particular positive constant C (not the same one as before).

We also obtain the same result (with a different value of C) for integers for which the least primary-decomposition factor of M_n does not equal 2.

Counting "unusually large" smallest invariant factors

The least invariant factor of M_n equals 2 for almost all integers n. But we can be more precise:

Theorem (Chang–M., 2016+)

The number of integers $n \le x$ for which the least invariant factor of M_n does not equal 2 is

$$C\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{3/4-\varepsilon}}\right)$$

for a particular positive constant C (not the same one as before).

We also obtain the same result (with a different value of C) for integers for which the least primary-decomposition factor of M_n does not equal 2.

From group theory to analytic number theory

Lemma

Fix an even number $k \geq 4$. The least invariant factor of M_n is a multiple of k if and only if all of the following conditions hold:

1. *for primes $p \nmid k$: if $p \mid n$ then we must have $p \equiv 1 \pmod{k}$;*
2. *$4 \nmid n$;*
3. *(some condition for odd primes $p \mid k$; for example, if $3 \mid k$, then either $3 \nmid n$ or $9 \mid n$)*

Definition

$$D_k(x) = \#\{n \leq x : k \text{ divides the least invariant factor of } M_n\}$$

By the lemma, $D_k(x)$ is very similar to

$$\#\{n \leq x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

—another instance of prohibiting prime factors.

From group theory to analytic number theory

Lemma

Fix an even number $k \geq 4$. The least invariant factor of M_n is a multiple of k if and only if all of the following conditions hold:

1. *for primes $p \nmid k$: if $p \mid n$ then we must have $p \equiv 1 \pmod{k}$;*
2. *$4 \nmid n$;*
3. *(some condition for odd primes $p \mid k$; for example, if $3 \mid k$, then either $3 \nmid n$ or $9 \mid n$)*

Definition

$$D_k(x) = \#\{n \leq x : k \text{ divides the least invariant factor of } M_n\}$$

By the lemma, $D_k(x)$ is very similar to

$$\#\{n \leq x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

—another instance of prohibiting prime factors.

From group theory to analytic number theory

Lemma

Fix an even number $k \geq 4$. The least invariant factor of M_n is a multiple of k if and only if all of the following conditions hold:

1. *for primes $p \nmid k$: if $p \mid n$ then we must have $p \equiv 1 \pmod{k}$;*
2. $4 \nmid n$;
3. *(some condition for odd primes $p \mid k$; for example, if $3 \mid k$, then either $3 \nmid n$ or $9 \mid n$)*

Definition

$$D_k(x) = \#\{n \leq x : k \text{ divides the least invariant factor of } M_n\}$$

By the lemma, $D_k(x)$ is very similar to

$$\#\{n \leq x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

—another instance of prohibiting prime factors.

From group theory to analytic number theory

Lemma

Fix an even number $k \geq 4$. The least invariant factor of M_n is a multiple of k if and only if all of the following conditions hold:

1. *for primes $p \nmid k$: if $p \mid n$ then we must have $p \equiv 1 \pmod{k}$;*
2. *$4 \nmid n$;*
3. *(some condition for odd primes $p \mid k$; for example, if $3 \mid k$, then either $3 \nmid n$ or $9 \mid n$)*

Definition

$$D_k(x) = \#\{n \leq x : k \text{ divides the least invariant factor of } M_n\}$$

By the lemma, $D_k(x)$ is very similar to

$$\#\{n \leq x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

—another instance of prohibiting prime factors.

From group theory to analytic number theory

Lemma

Fix an even number $k \geq 4$. The least invariant factor of M_n is a multiple of k if and only if all of the following conditions hold:

1. *for primes $p \nmid k$: if $p \mid n$ then we must have $p \equiv 1 \pmod{k}$;*
2. *$4 \nmid n$;*
3. *(some condition for odd primes $p \mid k$; for example, if $3 \mid k$, then either $3 \nmid n$ or $9 \mid n$)*

Definition

$$D_k(x) = \#\{n \leq x : k \text{ divides the least invariant factor of } M_n\}$$

By the lemma, $D_k(x)$ is very similar to

$$\#\{n \leq x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

—another instance of prohibiting prime factors.

From group theory to analytic number theory

Lemma

Fix an even number $k \geq 4$. The least invariant factor of M_n is a multiple of k if and only if all of the following conditions hold:

1. *for primes $p \nmid k$: if $p \mid n$ then we must have $p \equiv 1 \pmod{k}$;*
2. $4 \nmid n$;
3. *(some condition for odd primes $p \mid k$; for example, if $3 \mid k$, then either $3 \nmid n$ or $9 \mid n$)*

Definition

$$D_k(x) = \#\{n \leq x : k \text{ divides the least invariant factor of } M_n\}$$

By the lemma, $D_k(x)$ is very similar to

$$\#\{n \leq x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

—another instance of prohibiting prime factors.

Strategy of proof

$$D_k(x) = \#\{n \le x\colon k \text{ divides the least invariant factor of } M_n\}$$

$$D_k(x) \text{ is similar to } \#\{n \le x\colon p \mid n \implies p \equiv 1 \pmod{k}\}$$

Trivially,

$$\#\{n \le x\colon \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$\le D_4(x) + D_6(x) + D_8(x) + D_{10}(x) + D_{12}(x) + \cdots.$$

General philosophy again

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $D_k(x) \asymp x/(\log x)^{1-1/\phi(k)}$.

So we expect

$$\#\{n \le x\colon \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

Strategy of proof

$$D_k(x) = \#\{n \le x\colon k \text{ divides the least invariant factor of } M_n\}$$

$$D_k(x) \text{ is similar to } \#\{n \le x\colon p \mid n \implies p \equiv 1 \pmod{k}\}$$

Trivially,

$$\#\{n \le x\colon \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$\le D_4(x) + D_6(x) + D_8(x) + D_{10}(x) + D_{12}(x) + \cdots.$$

General philosophy again

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $D_k(x) \asymp x/(\log x)^{1-1/\phi(k)}$.

So we expect

$$\#\{n \le x\colon \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

Strategy of proof

$$D_k(x) = \#\{n \le x : k \text{ divides the least invariant factor of } M_n\}$$

$$D_k(x) \text{ is similar to } \#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$$

Trivially,

$$\#\{n \le x : \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$\le D_4(x) + D_6(x) + D_8(x) + D_{10}(x) + D_{12}(x) + \cdots.$$

General philosophy again

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$.

Correspondingly, we expect $D_k(x) \asymp x/(\log x)^{1-1/\phi(k)}$.

So we expect

$$\#\{n \le x : \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

Strategy of proof

$$D_k(x) = \#\{n \le x : k \text{ divides the least invariant factor of } M_n\}$$

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$

Trivially,

$$\#\{n \le x : \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$\le D_4(x) + D_6(x) + D_8(x) + D_{10}(x) + D_{12}(x) + \cdots.$$

General philosophy again

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $D_k(x) \asymp x/(\log x)^{1-1/\phi(k)}$.

So we expect

$$\#\{n \le x : \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

Strategy of proof

$$D_k(x) = \#\{n \le x\colon k \text{ divides the least invariant factor of } M_n\}$$
$$D_k(x) \text{ is similar to } \#\{n \le x\colon p \mid n \implies p \equiv 1 \pmod{k}\}$$

Trivially,

$$\#\{n \le x\colon \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$\le D_4(x) + D_6(x) + D_8(x) + D_{10}(x) + D_{12}(x) + \cdots.$$

General philosophy again

Prohibiting prime divisors from a set of primes of relative density δ divides the counting function by a factor of $(\log x)^\delta$. Correspondingly, we expect $D_k(x) \asymp x/(\log x)^{1-1/\phi(k)}$.

So we expect

$$\#\{n \le x\colon \text{the least invariant factor of } M_n \text{ does not equal } 2\}$$
$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

Selberg–Delange with more uniformity

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$

$\#\{n \le x$: the least invariant factor of M_n does not equal $2\}$

$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

A straightforward application of the Selberg–Delange method (for example from Tenenbaum's book) gives

$$D_k(x) \sim C_k \frac{x}{(\log x)^{1-1/\phi(k)}} + O_k\left(\frac{x}{(\log x)^{2-1/\phi(k)}}\right)$$

(not the same C_k as before) . . . for any fixed k.

We have a sum over k in our error term; hence we need a version of Selberg–Delange with uniformity in k.

- uniformity of C_k: medium annoying
- uniformity of the O-constant: very annoying

Selberg–Delange with more uniformity

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$

$\#\{n \le x$: the least invariant factor of M_n does not equal $2\}$

$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

A straightforward application of the Selberg–Delange method (for example from Tenenbaum's book) gives

$$D_k(x) \sim C_k \frac{x}{(\log x)^{1-1/\phi(k)}} + O_k\left(\frac{x}{(\log x)^{2-1/\phi(k)}}\right)$$

(not the same C_k as before) . . . for any fixed k.

We have a sum over k in our error term; hence we need a version of Selberg–Delange with uniformity in k.

- uniformity of C_k: medium annoying
- uniformity of the O-constant: very annoying

Selberg–Delange with more uniformity

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod k\}$

$\#\{n \le x$: the least invariant factor of M_n does not equal $2\}$

$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

A straightforward application of the Selberg–Delange method (for example from Tenenbaum's book) gives

$$D_k(x) \sim C_k \frac{x}{(\log x)^{1-1/\phi(k)}} + O_k\left(\frac{x}{(\log x)^{2-1/\phi(k)}}\right)$$

(not the same C_k as before) . . . for any fixed k.

We have a sum over k in our error term; hence we need a version of Selberg–Delange with uniformity in k.

- uniformity of C_k: medium annoying
- uniformity of the O-constant: very annoying

Selberg–Delange with more uniformity

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$

$\#\{n \le x$: the least invariant factor of M_n does not equal $2\}$

$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

A straightforward application of the Selberg–Delange method (for example from Tenenbaum's book) gives

$$D_k(x) \sim C_k \frac{x}{(\log x)^{1-1/\phi(k)}} + O_k\left(\frac{x}{(\log x)^{2-1/\phi(k)}}\right)$$

(not the same C_k as before) . . . for any fixed k.

We have a sum over k in our error term; hence we need a version of Selberg–Delange with uniformity in k.

- uniformity of C_k: medium annoying
- uniformity of the O-constant: very annoying

Selberg–Delange with more uniformity

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$

$\#\{n \le x$: the least invariant factor of M_n does not equal $2\}$

$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

A straightforward application of the Selberg–Delange method (for example from Tenenbaum's book) gives

$$D_k(x) \sim C_k \frac{x}{(\log x)^{1-1/\phi(k)}} + O_k\left(\frac{x}{(\log x)^{2-1/\phi(k)}}\right)$$

(not the same C_k as before) . . . for any fixed k.

We have a sum over k in our error term; hence we need a version of Selberg–Delange with uniformity in k.

- uniformity of C_k: medium annoying
- uniformity of the O-constant: very annoying

Selberg–Delange with more uniformity

$D_k(x)$ is similar to $\#\{n \le x : p \mid n \implies p \equiv 1 \pmod{k}\}$

$\#\{n \le x$: the least invariant factor of M_n does not equal $2\}$

$$= D_4(x) + D_6(x) + O\big(D_8(x) + D_{10}(x) + D_{12}(x) + \cdots\big).$$

A straightforward application of the Selberg–Delange method (for example from Tenenbaum's book) gives

$$D_k(x) \sim C_k \frac{x}{(\log x)^{1-1/\phi(k)}} + O_k\left(\frac{x}{(\log x)^{2-1/\phi(k)}}\right)$$

(not the same C_k as before) . . . for any fixed k.

We have a sum over k in our error term; hence we need a version of Selberg–Delange with uniformity in k.

- uniformity of C_k: medium annoying
- uniformity of the O-constant: very annoying

That's a weird constant

Theorem (Chang–M., 2016+)

The number of integers $n \le x$ for which the least invariant factor of M_n does not equal 2 is

$$C \frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{3/4-\varepsilon}} \right)$$

where $C \approx 1.59747$ is given by

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

Theorem (Chang–M., 2016+)

Let $m \ge 4$ be even. The number of integers $n \le x$ for which the least invariant factor of M_n equals m is (for some explicit C_m)

$$C_m \frac{x}{(\log x)^{1-1/\phi(m)}} + O_m\left(\frac{x}{(\log x)^{1-1/(2\phi(m))-\varepsilon}} \right).$$

That's a weird constant

Theorem (Chang–M., 2016+)

The number of integers $n \le x$ for which the least invariant factor of M_n does not equal 2 is

$$C\frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{3/4-\varepsilon}}\right)$$

where $C \approx 1.59747$ is given by

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

Theorem (Chang–M., 2016+)

Let $m \ge 4$ be even. The number of integers $n \le x$ for which the least invariant factor of M_n equals m is (for some explicit C_m)

$$C_m \frac{x}{(\log x)^{1-1/\phi(m)}} + O_m\left(\frac{x}{(\log x)^{1-1/(2\phi(m))-\varepsilon}}\right).$$

That's a weird constant

Theorem (Chang–M., 2016+)

The number of integers $n \le x$ for which the least invariant factor of M_n does not equal 2 is

$$C \frac{x}{\sqrt{\log x}} + O\left(\frac{x}{(\log x)^{3/4-\varepsilon}} \right)$$

where $C \approx 1.59747$ is given by

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

Theorem (Chang–M., 2016+)

Let $m \ge 4$ be even. The number of integers $n \le x$ for which the least invariant factor of M_n equals m is (for some explicit C_m)

$$C_m \frac{x}{(\log x)^{1-1/\phi(m)}} + O_m\left(\frac{x}{(\log x)^{1-1/(2\phi(m))-\varepsilon}} \right).$$

The end

These slides

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

"The distribution of the number of subgroups of the multiplicative group", with Lee Troupe

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

"The distribution of sums and products of additive functions", with Lee Troupe

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

work in progress with Ben Chang and with Jenna Downey

Keep your eyes peeled on arXiv or my web page!