The least invariant factor of the multiplicative group

Greg Martin
University of British Columbia

joint work with Ben Chang

Canadian Number Theory Association XV Meeting
Université Laval
July 12, 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 $\omega(n) + 1$

An M_n with a larger least invariant factor

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).

An M_n with a larger least invariant factor

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).

An M_n with a larger least invariant factor

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).

An M_n with a larger least invariant factor

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).

An M_n with a larger least invariant factor

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).

The main result (of this talk, anyway)

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

Theorem (Chang–M., 2018+)

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.

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.

The main result (of this talk, anyway)

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

Theorem (Chang–M., 2018+)

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.

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.

The main result (of this talk, anyway)

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

Theorem (Chang–M., 2018+)

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.

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.

A different question about the multiplicative group

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

Question (Shparlinski)

How many subgroups does M_n have?

Theorem (M.–Troupe, 2018)

The logarithm of the number of subgroups of M_n satisfies an Erdős–Kac theorem with mean $A(\log\log n)^2$ and variance $B(\log\log n)^3$ (for certain explicit constants A, B).

Theorem (M.–Troupe, 2018)

For infinitely many n, the logarithm of the number of subgroups of M_n is $\gg (\log n)^2/\log\log n$.

In particular, M_n has more than $n^{10^{2018}}$ subgroups infinitely often!

A different question about the multiplicative group

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

Question (Shparlinski)

How many subgroups does M_n have?

Theorem (M.–Troupe, 2018)

The logarithm of the number of subgroups of M_n satisfies an Erdős–Kac theorem with mean $A(\log\log n)^2$ and variance $B(\log\log n)^3$ (for certain explicit constants A, B).

Theorem (M.–Troupe, 2018)

For infinitely many n, the logarithm of the number of subgroups of M_n is $\gg (\log n)^2/\log\log n$.

In particular, M_n has more than $n^{10^{2018}}$ subgroups infinitely often!

A different question about the multiplicative group

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

Question (Shparlinski)

How many subgroups does M_n have?

Theorem (M.–Troupe, 2018)

The logarithm of the number of subgroups of M_n satisfies an Erdős–Kac theorem with mean $A(\log\log n)^2$ and variance $B(\log\log n)^3$ (for certain explicit constants A, B).

Theorem (M.–Troupe, 2018)

For infinitely many n, the logarithm of the number of subgroups of M_n is $\gg (\log n)^2/\log\log n$.

In particular, M_n has more than $n^{10^{2018}}$ subgroups infinitely often!

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

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

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

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

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

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

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

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

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

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

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

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

Prohibited prime factors: related problems

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

$D_4(x)$ is thus similar to counting sums of two squares, since

$$\{n : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}$$
$$= \{n : p \mid n \implies p \equiv 1 \pmod 4 \text{ or } p = 2 \text{ or } \nu_p(n) \text{ is even}\}.$$

A related characterization

For any fixed odd prime q,

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

Work in progress with Jenna Downey

For any fixed finite abelian q-group G: an asymptotic formula for $\{n \le x : \text{ the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

Prohibited prime factors: related problems

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

$D_4(x)$ is thus similar to counting sums of two squares, since

$$\{n : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}$$
$$= \{n : p \mid n \implies p \equiv 1 \pmod 4 \text{ or } p = 2 \text{ or } \nu_p(n) \text{ is even}\}.$$

A related characterization

For any fixed odd prime q,

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

Work in progress with Jenna Downey

For any fixed finite abelian q-group G: an asymptotic formula for $\{n \le x : \text{ the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

Prohibited prime factors: related problems

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

$D_4(x)$ is thus similar to counting sums of two squares, since

$$\{n : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}$$
$$= \{n : p \mid n \implies p \equiv 1 \pmod 4 \text{ or } p = 2 \text{ or } \nu_p(n) \text{ is even}\}.$$

A related characterization

For any fixed odd prime q,

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

Work in progress with Jenna Downey

For any fixed finite abelian q-group G: an asymptotic formula for $\{n \le x : \text{ the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

Prohibited prime factors: related problems

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

$D_4(x)$ is thus similar to counting sums of two squares, since

$$\{n : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}$$
$$= \{n : p \mid n \implies p \equiv 1 \pmod 4 \text{ or } p = 2 \text{ or } \nu_p(n) \text{ is even}\}.$$

A related characterization

For any fixed odd prime q,

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

Work in progress with Jenna Downey

For any fixed finite abelian q-group G: an asymptotic formula for $\{n \le x : \text{ the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$

Prohibited prime factors: related problems

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

$D_4(x)$ is thus similar to counting sums of two squares, since

$$\{n : n = a^2 + b^2 \text{ for some } a, b \in \mathbb{Z}\}$$
$$= \{n : p \mid n \implies p \equiv 1 \pmod 4 \text{ or } p = 2 \text{ or } \nu_p(n) \text{ is even}\}.$$

A related characterization

For any fixed odd prime q,

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

Work in progress with Jenna Downey

For any fixed finite abelian q-group G: an asymptotic formula for

$$\{n \le x : \text{ the } q\text{-Sylow subgroup of } M_n \text{ equals } G\}$$

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

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

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

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

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

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

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

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

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

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

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

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

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

Selberg–Delange with more uniformity

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

$\#\{n \le x \colon$ 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 in Tenenbaum's book) gives

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

... 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 $\#\{n \le x \colon p \mid n \implies p \equiv 1 \pmod{k}\}$

$\#\{n \le x \colon$ 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 in Tenenbaum's book) gives

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

. . . 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 $\#\{n \le x \colon p \mid n \implies p \equiv 1 \pmod k\}$

$\#\{n \le x \colon$ 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 in Tenenbaum's book) gives

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

. . . 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 in Tenenbaum's book) gives

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

. . . 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 in Tenenbaum's book) gives

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

. . . 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 in Tenenbaum's book) gives

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

. . . 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., 2018+)

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., 2018+)

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., 2018+)

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., 2018+)

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., 2018+)

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., 2018+)

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 are available for downloading.

These slides

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