Statistics of the multiplicative group

Greg Martin
University of British Columbia

joint work with Ben Chang

Canadian Undergraduate Mathematics Conference
University of Victoria
July 15, 2016

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

Outline

1. Ring ring: cyclic groups C_n and multiplicative groups M_n
2. Using the Euler ϕ-function to illustrate this talk's themes
3. Structure theorems: facial recognition software for finite abelian groups
4. Divide and conquer: primitive roots, the Chinese remainder theorem, and calculating the structure of M_n
5. The number of invariant factors of M_n, the number of prime factors of n, and the Erdős–Kac theorem
6. Other examples (as time permits)

The additive group

One ring to rule them all

- For every integer $n \geq 2$, we have a natural example of a (qoutient) ring with n elements, namely $\mathbb{Z}/n\mathbb{Z}$.
- The elements can be written as $0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $\ldots$, $(n-1) + n\mathbb{Z}$ (or just $0, 1, \ldots, n-1$ if we're lazy).
- We add and multiply these elements by doing arithmetic modulo n.

The additive group

- Ignore multiplication and look at addition: we get a group.
- This group is actually a cyclic group with n elements: every element can be written as $1 + 1 + \cdots$.
- We call this cyclic group with n elements C_n.

The additive group

One ring to rule them all

- For every integer $n \geq 2$, we have a natural example of a (qoutient) ring with n elements, namely $\mathbb{Z}/n\mathbb{Z}$.
- The elements can be written as $0 + n\mathbb{Z}$, $1 + n\mathbb{Z}$, $\ldots$, $(n-1) + n\mathbb{Z}$ (or just $0, 1, \ldots, n-1$ if we're lazy).
- We add and multiply these elements by doing arithmetic modulo n.

The additive group

- Ignore multiplication and look at addition: we get a group.
- This group is actually a cyclic group with n elements: every element can be written as $1 + 1 + \cdots$.
- We call this cyclic group with n elements C_n.

The additive group

C_n when $n = 12$

$+$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

What is the multiplicative group?

$\mathbb{Z}/n\mathbb{Z}$ is a ring, and its additive group C_n is cyclic.

The multiplicative group

- If we ignore addition and just look at multiplication, we don't get a group: most axioms are satisfied, but some elements (such as 0) don't have multiplicative inverses.
- We repair this by considering only the units: those elements with multiplicative inverses. As it happens, this means keeping the elements $0 \le a \le n-1$ where $\gcd(a,n) = 1$.
- There are $\phi(n)$ units (the Euler phi-function), and they do form a group under multiplication.
- We call this multiplicative group M_n.

What is the multiplicative group?

$\mathbb{Z}/n\mathbb{Z}$ is a ring, and its additive group C_n is cyclic.

The multiplicative group

- If we ignore addition and just look at multiplication, we don't get a group: most axioms are satisfied, but some elements (such as 0) don't have multiplicative inverses.
- We repair this by considering only the units: those elements with multiplicative inverses. As it happens, this means keeping the elements $0 \le a \le n-1$ where $\gcd(a,n) = 1$.
- There are $\phi(n)$ units (the Euler phi-function), and they do form a group under multiplication.
- We call this multiplicative group M_n.

What is the multiplicative group?

M_n when $n = 12$

$\times$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

What is the multiplicative group?

M_n when $n = 12$

$\times$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Multiplicative groups are isomorphic to additive groups

M_5 on the left, M_{12} on the right

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

C_4 on the left, $C_2 \oplus C_2$ on the right (only groups of size 4)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Multiplicative groups are isomorphic to additive groups

M_5 on the left, M_{12} on the right

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

C_4 on the left, $C_2 \oplus C_2$ on the right (only groups of size 4)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Multiplicative groups are isomorphic to additive groups

M_5 on the left, M_{12} on the right

$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
3	3	1	2	4
4	4	3	1	2

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

C_4 on the left, $C_2 \oplus C_2$ on the right (only groups of size 4)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Multiplicative groups are isomorphic to additive groups

M_5 on the left, M_{12} on the right

$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
3	3	1	2	4
4	4	3	1	2

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

C_4 on the left, $C_2 \oplus C_2$ on the right (only groups of size 4)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Multiplicative groups are isomorphic to additive groups

M_5 on the left, M_{12} on the right

$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

C_4 on the left, $C_2 \oplus C_2$ on the right (only groups of size 4)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Multiplicative groups are isomorphic to additive groups

M_5 on the left, M_{12} on the right

$\times$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

C_4 on the left, $C_2 \oplus C_2$ on the right (only groups of size 4)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

What are we doing here again?

Two themes for this talk

1. Lots of questions about the multiplicative groups M_n turn into questions in number theory.
2. What sorts of questions (and answers) are number theorists interested in?

Note: there are lots of different kinds of number theory. This topic might be called multiplicative analytic number theory.

Example: the size of M_n

- What is the size of M_n?—the Euler phi-function $\phi(n)$.
- How big and small can $\phi(n)$ get?
- How big do we expect $\phi(n)$ to be if we "pick n at random"?

What are we doing here again?

Two themes for this talk

1. Lots of questions about the multiplicative groups M_n turn into questions in number theory.
2. What sorts of questions (and answers) are number theorists interested in?

Note: there are lots of different kinds of number theory. This topic might be called multiplicative analytic number theory.

Example: the size of M_n

- What is the size of M_n?—the Euler phi-function $\phi(n)$.
- How big and small can $\phi(n)$ get?
- How big do we expect $\phi(n)$ to be if we "pick n at random"?

What are we doing here again?

Two themes for this talk

1. Lots of questions about the multiplicative groups M_n turn into questions in number theory.
2. What sorts of questions (and answers) are number theorists interested in?

Note: there are lots of different kinds of number theory. This topic might be called multiplicative analytic number theory.

Example: the size of M_n

- What is the size of M_n?—the Euler phi-function $\phi(n)$.
- How big and small can $\phi(n)$ get?
- How big do we expect $\phi(n)$ to be if we "pick n at random"?

What are we doing here again?

Two themes for this talk

1. Lots of questions about the multiplicative groups M_n turn into questions in number theory.
2. What sorts of questions (and answers) are number theorists interested in?

Note: there are lots of different kinds of number theory. This topic might be called multiplicative analytic number theory.

Example: the size of M_n

- What is the size of M_n?—the Euler phi-function $\phi(n)$.
- How big and small can $\phi(n)$ get?
- How big do we expect $\phi(n)$ to be if we "pick n at random"?

Euler ϕ-function: the big and the small

$$\phi(n) = \#\{1 \le a \le n : \gcd(a,n) = 1\}$$

Maximal order

- Clear from its definition: $\phi(n) \le n-1$ for $n \ge 2$.
- If n is prime, then $\phi(n) = n-1$.
- There are infinitely many primes.

Minimal order

- $\phi(n) > \dfrac{n}{7\ln(\ln n)}$ for every $n \ge 4$.
- There are infinitely many n for which $\phi(n) < \dfrac{n}{1.78\ln(\ln n)}$.

Euler ϕ-function: the big and the small

$$\phi(n) = \#\{1 \le a \le n : \gcd(a,n) = 1\}$$

Maximal order

- Clear from its definition: $\phi(n) \le n - 1$ for $n \ge 2$.
- If n is prime, then $\phi(n) = n - 1$.
- There are infinitely many primes.

Minimal order

- $\phi(n) > \dfrac{n}{7 \ln(\ln n)}$ for every $n \ge 4$.
- There are infinitely many n for which $\phi(n) < \dfrac{n}{1.78 \ln(\ln n)}$.

Euler ϕ-function: the big and the small

$$\phi(n) = \#\{1 \le a \le n : \gcd(a,n) = 1\}$$

Maximal order

- Clear from its definition: $\phi(n) \le n - 1$ for $n \ge 2$.
- If n is prime, then $\phi(n) = n - 1$.
- There are infinitely many primes.

Minimal order

- $\phi(n) > \dfrac{n}{7 \ln(\ln n)}$ for every $n \ge 4$.
- There are infinitely many n for which $\phi(n) < \dfrac{n}{1.78 \ln(\ln n)}$.

Euler ϕ-function: the big and the small

$$\phi(n) = \#\{1 \le a \le n : \gcd(a,n) = 1\}$$

Maximal order

- Clear from its definition: $\phi(n) \le n - 1$ for $n \ge 2$.
- If n is prime, then $\phi(n) = n - 1$.
- There are infinitely many primes.

Minimal order

- $\phi(n) > \dfrac{n}{7 \ln(\ln n)}$ for every $n \ge 4$. $\qquad \ln(\ln 10^{80}) \approx 5.2$
- There are infinitely many n for which $\phi(n) < \dfrac{n}{1.78 \ln(\ln n)}$.

You can pick your friends . . .

. . . but you can't pick a positive integer uniformly at random. (Infinitely many things can't all have the same positive probability.)

When number theorists say "pick an integer at random":

1. Let $x \geq 1$ be a temporary parameter.
2. Pick an integer uniformly at random from $\{1, 2, \ldots, x\}$; answer whatever question we want to ask (the answer will depend on x).
3. Take the limit of the answer as $x \to \infty$.

Since $\phi(n)$ is close to n, let's look instead at $\frac{\phi(n)}{n}$, which is between 0 and 1.

Question: What is the expected value of $\frac{\phi(n)}{n}$?

You can pick your friends . . .

. . . but you can't pick a positive integer uniformly at random. (Infinitely many things can't all have the same positive probability.)

When number theorists say "pick an integer at random":

1. Let $x \geq 1$ be a temporary parameter.
2. Pick an integer uniformly at random from $\{1, 2, \ldots, x\}$; answer whatever question we want to ask (the answer will depend on x).
3. Take the limit of the answer as $x \to \infty$.

Since $\phi(n)$ is close to n, let's look instead at $\frac{\phi(n)}{n}$, which is between 0 and 1.

Question: What is the expected value of $\frac{\phi(n)}{n}$?

You can pick your friends . . .

. . . but you can't pick a positive integer uniformly at random. (Infinitely many things can't all have the same positive probability.)

When number theorists say "pick an integer at random":

1. Let $x \geq 1$ be a temporary parameter.
2. Pick an integer uniformly at random from $\{1, 2, \ldots, x\}$; answer whatever question we want to ask (the answer will depend on x).
3. Take the limit of the answer as $x \to \infty$.

Since $\phi(n)$ is close to n, let's look instead at $\frac{\phi(n)}{n}$, which is between 0 and 1.

Question: What is the expected value of $\frac{\phi(n)}{n}$?

What is the expected value of $\frac{\phi(n)}{n}$?

For any fixed $x \geq 1$:

- The expected value of $\frac{\phi(n)}{n}$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\frac{1}{x}\sum_{n=1}^{x} \frac{\phi(n)}{n}$.
- We know how to show that $\sum_{n=1}^{x} \frac{\phi(n)}{n} = \frac{6x}{\pi^2} + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq 2 \ln x$.
- Therefore the "expected value of $\frac{\phi(n)}{n}$" is

$$\lim_{x\to\infty} \frac{1}{x}\left(\frac{6x}{\pi^2} + \varepsilon(x)\right) = \frac{6}{\pi^2} \approx 0.608.$$

$\phi(n)$ is $\frac{6}{\pi^2}n$ on average

What is the expected value of $\frac{\phi(n)}{n}$?

For any fixed $x \geq 1$:

- The expected value of $\frac{\phi(n)}{n}$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\displaystyle\frac{1}{x}\sum_{n=1}^{x}\frac{\phi(n)}{n}$.
- We know how to show that $\displaystyle\sum_{n=1}^{x}\frac{\phi(n)}{n} = \frac{6x}{\pi^2} + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq 2\ln x$.
- Therefore the "expected value of $\frac{\phi(n)}{n}$" is

$$\lim_{x\to\infty}\frac{1}{x}\left(\frac{6x}{\pi^2}+\varepsilon(x)\right) = \frac{6}{\pi^2} \approx 0.608.$$

$\phi(n)$ is $\frac{6}{\pi^2}n$ on average

What is the expected value of $\frac{\phi(n)}{n}$?

For any fixed $x \geq 1$:

- The expected value of $\frac{\phi(n)}{n}$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\frac{1}{x} \sum_{n=1}^{x} \frac{\phi(n)}{n}$.
- We know how to show that $\sum_{n=1}^{x} \frac{\phi(n)}{n} = \frac{6x}{\pi^2} + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq 2 \ln x$.
- Therefore the "expected value of $\frac{\phi(n)}{n}$" is

$$\lim_{x \to \infty} \frac{1}{x} \left(\frac{6x}{\pi^2} + \varepsilon(x) \right) = \frac{6}{\pi^2} \approx 0.608.$$

$\phi(n)$ is $\frac{6}{\pi^2} n$ on average

What is the expected value of $\frac{\phi(n)}{n}$?

For any fixed $x \geq 1$:

- The expected value of $\frac{\phi(n)}{n}$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\frac{1}{x}\sum_{n=1}^{x} \frac{\phi(n)}{n}$.
- We know how to show that $\sum_{n=1}^{x} \frac{\phi(n)}{n} = \frac{6x}{\pi^2} + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq 2 \ln x$.
- Therefore the "expected value of $\frac{\phi(n)}{n}$" is

$$\lim_{x\to\infty} \frac{1}{x}\left(\frac{6x}{\pi^2} + \varepsilon(x)\right) = \frac{6}{\pi^2} \approx 0.608.$$

$\phi(n)$ is $\frac{6}{\pi^2}n$ on average

Statistics of $\frac{\phi(n)}{n}$

- Expected value (mean): $\frac{6}{\pi^2}$
- Variance: some funny constant near 0.0587.

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left(\frac{\phi(n)}{n}-\frac{6}{\pi^2}\right)^2\right)$$

- Median: open problem! Provably less than $\frac{1}{2}$; but maybe around $\frac{1}{2}-10^{-20}$.

Cumulative distribution function

- For a random variable X, the CDF is $f(u)=\operatorname{Prob}(X<u)$
- For a number theory statistic like $\frac{\phi(n)}{n}$, the CDF is

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

- Schoenberg proved (1928) that $\frac{\phi(n)}{n}$ has a cumulative distribution function that is continuous, but totally singular (derivative equals 0 almost everywhere) . . .

Statistics of $\frac{\phi(n)}{n}$

- Expected value (mean): $\frac{6}{\pi^2}$
- Variance: some funny constant near 0.0587.

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left(\frac{\phi(n)}{n}-\frac{6}{\pi^2}\right)^2\right)$$

- Median: open problem! Provably less than $\frac{1}{2}$; but maybe around $\frac{1}{2}-10^{-20}$.

Cumulative distribution function

- For a random variable X, the CDF is $f(u)=\operatorname{Prob}(X<u)$
- For a number theory statistic like $\frac{\phi(n)}{n}$, the CDF is

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

- Schoenberg proved (1928) that $\frac{\phi(n)}{n}$ has a cumulative distribution function that is continuous, but totally singular (derivative equals 0 almost everywhere) . . .

Statistics of $\frac{\phi(n)}{n}$

- Expected value (mean): $\frac{6}{\pi^2}$
- Variance: some funny constant near 0.0587.

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left(\frac{\phi(n)}{n}-\frac{6}{\pi^2}\right)^2\right)$$

- Median: open problem! Provably less than $\frac{1}{2}$; but maybe around $\frac{1}{2}-10^{-20}$.

Cumulative distribution function

- For a random variable X, the CDF is $f(u)=\operatorname{Prob}(X<u)$
- For a number theory statistic like $\frac{\phi(n)}{n}$, the CDF is

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

- Schoenberg proved (1928) that $\frac{\phi(n)}{n}$ has a cumulative distribution function that is continuous, but totally singular (derivative equals 0 almost everywhere) . . .

Statistics of $\frac{\phi(n)}{n}$

- Expected value (mean): $\frac{6}{\pi^2}$
- Variance: some funny constant near 0.0587.

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left(\frac{\phi(n)}{n}-\frac{6}{\pi^2}\right)^2\right)$$

- Median: open problem! Provably less than $\frac{1}{2}$; but maybe around $\frac{1}{2}-10^{-20}$.

Cumulative distribution function

- For a random variable X, the CDF is $f(u)=\operatorname{Prob}(X<u)$
- For a number theory statistic like $\frac{\phi(n)}{n}$, the CDF is

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

- Schoenberg proved (1928) that $\frac{\phi(n)}{n}$ has a cumulative distribution function that is continuous, but totally singular (derivative equals 0 almost everywhere) . . .

Statistics of $\frac{\phi(n)}{n}$

- Expected value (mean): $\frac{6}{\pi^2}$
- Variance: some funny constant near 0.0587.

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left(\frac{\phi(n)}{n}-\frac{6}{\pi^2}\right)^2\right)$$

- Median: open problem! Provably less than $\frac{1}{2}$; but maybe around $\frac{1}{2}-10^{-20}$.

Cumulative distribution function

- For a random variable X, the CDF is $f(u)=\operatorname{Prob}(X<u)$
- For a number theory statistic like $\frac{\phi(n)}{n}$, the CDF is

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

- Schoenberg proved (1928) that $\frac{\phi(n)}{n}$ has a cumulative distribution function that is continuous, but totally singular (derivative equals 0 almost everywhere) . . .

Statistics of $\frac{\phi(n)}{n}$

- Expected value (mean): $\frac{6}{\pi^2}$
- Variance: some funny constant near 0.0587.

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left(\frac{\phi(n)}{n}-\frac{6}{\pi^2}\right)^2\right)$$

- Median: open problem! Provably less than $\frac{1}{2}$; but maybe around $\frac{1}{2}-10^{-20}$.

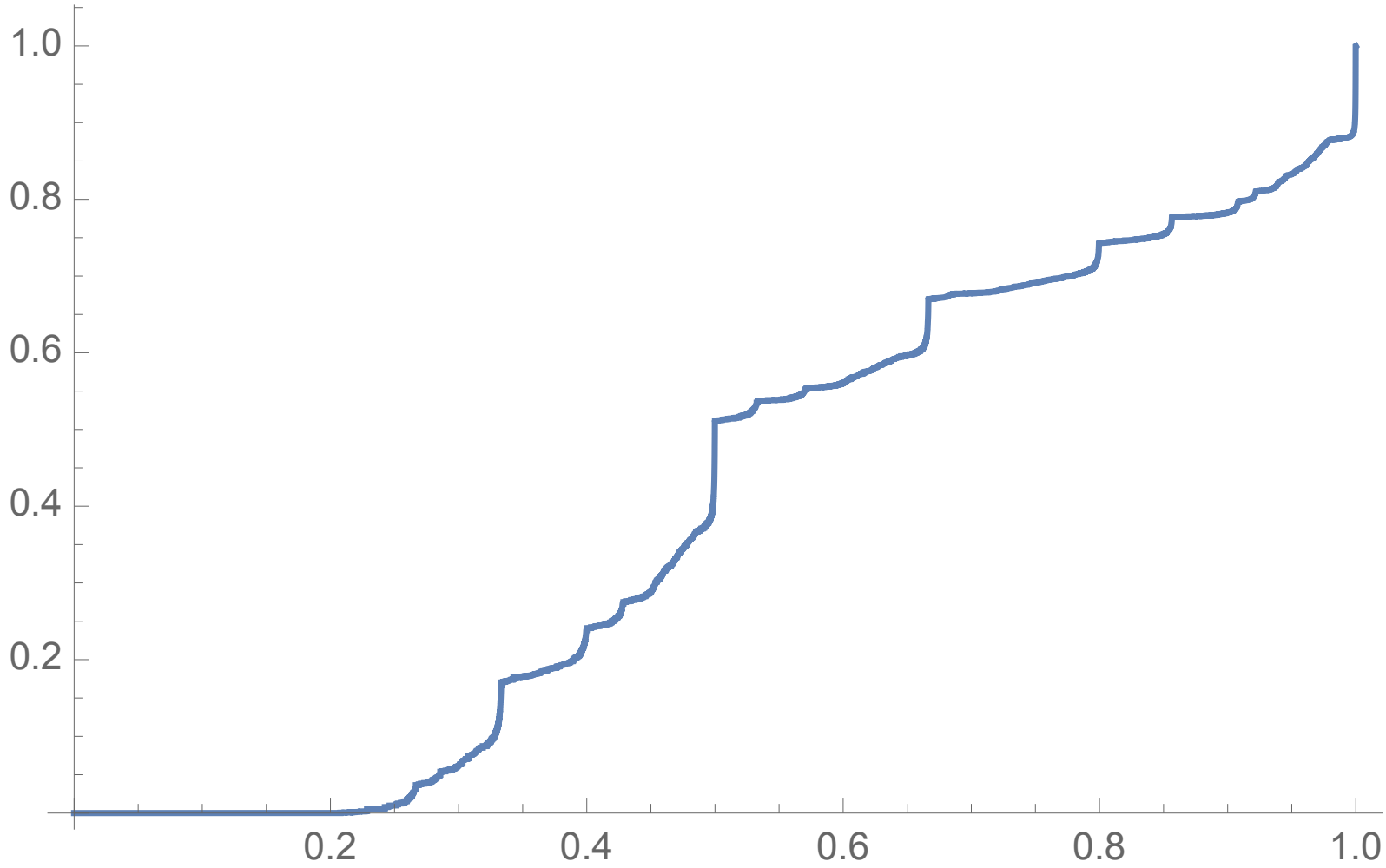
Cumulative distribution function

- For a random variable X, the CDF is $f(u)=\operatorname{Prob}(X<u)$
- For a number theory statistic like $\frac{\phi(n)}{n}$, the CDF is

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

- Schoenberg proved (1928) that $\frac{\phi(n)}{n}$ has a cumulative distribution function that is continuous, but totally singular (derivative equals 0 almost everywhere) ...

The cumulative distribution function for $\frac{\phi(n)}{n}$



Identifying finite abelian groups

We saw earlier that:

- both $\phi(5) = 4$ and $\phi(12) = 4$, but
- $M_5 \cong C_4$ while $M_{12} \cong C_2 \oplus C_2$.
- (And this matters, because $C_4 \ncong C_2 \oplus C_2$.)

Question

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

Before answering that question, we have to answer another question:

Question

What does "which finite abelian group" even mean?

Identifying finite abelian groups

We saw earlier that:

- both $\phi(5) = 4$ and $\phi(12) = 4$, but
- $M_5 \cong C_4$ while $M_{12} \cong C_2 \oplus C_2$.
- (And this matters, because $C_4 \ncong C_2 \oplus C_2$.)

Question

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

Before answering that question, we have to answer another question:

Question

What does "which finite abelian group" even mean?

Identifying finite abelian groups

We saw earlier that:

- both $\phi(5) = 4$ and $\phi(12) = 4$, but
- $M_5 \cong C_4$ while $M_{12} \cong C_2 \oplus C_2$.
- (And this matters, because $C_4 \ncong C_2 \oplus C_2$.)

Question

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

Before answering that question, we have to answer another question:

Question

What does "which finite abelian group" even mean?

A tool for identifying isomorphic groups

The Chinese remainder theorem

If m and n are positive integers with $\gcd(m,n) = 1$, then the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic.

In particular, if $\gcd(m,n) = 1$ ("m and n are relatively prime"):

- The additive groups C_{mn} and $C_m \oplus C_n$ are isomorphic.
- The multiplicative groups M_{mn} and $M_m \times M_n$ are isomorphic.

CRT extends to more than two integers

If $n_1, n_2, \ldots, n_k$ are positive integers, any pair of which are relatively prime, then the rings $\mathbb{Z}/n_1 n_2 \cdots n_k\mathbb{Z}$ and $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_k\mathbb{Z}$ are isomorphic.

Example

$$\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

A tool for identifying isomorphic groups

The Chinese remainder theorem

If m and n are positive integers with $\gcd(m,n) = 1$, then the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic.

In particular, if $\gcd(m,n) = 1$ ("m and n are relatively prime"):

- The additive groups C_{mn} and $C_m \oplus C_n$ are isomorphic.
- The multiplicative groups M_{mn} and $M_m \times M_n$ are isomorphic.

CRT extends to more than two integers

If $n_1, n_2, \ldots, n_k$ are positive integers, any pair of which are relatively prime, then the rings $\mathbb{Z}/n_1 n_2 \cdots n_k\mathbb{Z}$ and $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_k\mathbb{Z}$ are isomorphic.

Example

$$\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

A tool for identifying isomorphic groups

The Chinese remainder theorem

If m and n are positive integers with $\gcd(m,n) = 1$, then the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ are isomorphic.

In particular, if $\gcd(m,n) = 1$ ("m and n are relatively prime"):

- The additive groups C_{mn} and $C_m \oplus C_n$ are isomorphic.
- The multiplicative groups M_{mn} and $M_m \times M_n$ are isomorphic.

CRT extends to more than two integers

If $n_1, n_2, \ldots, n_k$ are positive integers, any pair of which are relatively prime, then the rings $\mathbb{Z}/n_1 n_2 \cdots n_k\mathbb{Z}$ and $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_k\mathbb{Z}$ are isomorphic.

Example

$$\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

A larger example

Claim: The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- The Chinese remainder theorem lets us split apart some of the additive groups in group A into pairs of additive groups in group B.
- CRT also allows us to gather together certain additive groups from group B to make group C.

We have to remember though:

The integers involved all have to be relatively prime. Among the groups $C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and $C_4 \oplus C_4$ and C_{16} and $C_2 \oplus C_8$, none of them are isomorphic to one another.

Canonical forms for finite abelian groups

Theorem (Primary decomposition)

Every finite abelian group G can be uniquely written as the direct sum of cyclic groups of prime-power order:

$$G \cong C_{p_1^{r_1}} \oplus C_{p_2^{r_2}} \oplus \cdots \oplus C_{p_k^{r_k}}$$

where $p_1, p_2, \ldots, p_k$ are primes, $r_1, r_2, \ldots, r_k$ are positive integers, and $p_1^{r_1} \le p_2^{r_2} \le \cdots \le p_k^{r_k}$.

Theorem (Invariant factor decomposition)

Every finite abelian group G can be uniquely written as the direct sum of cyclic groups of orders dividing one another:

$$G \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_\ell}$$

where $d_1, d_2, \ldots, d_k$ are positive integers and d_1 divides d_2, which divides d_3, and so on.

Canonical forms for finite abelian groups

Theorem (Primary decomposition)

Every finite abelian group G can be uniquely written as the direct sum of cyclic groups of prime-power order:

$$G \cong C_{p_1^{r_1}} \oplus C_{p_2^{r_2}} \oplus \cdots \oplus C_{p_k^{r_k}}$$

where $p_1, p_2, \ldots, p_k$ are primes, $r_1, r_2, \ldots, r_k$ are positive integers, and $p_1^{r_1} \le p_2^{r_2} \le \cdots \le p_k^{r_k}$.

Theorem (Invariant factor decomposition)

Every finite abelian group G can be uniquely written as the direct sum of cyclic groups of orders dividing one another:

$$G \cong C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_\ell}$$

where $d_1, d_2, \ldots, d_k$ are positive integers and d_1 divides d_2, which divides d_3, and so on.

The example we already saw

The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- Group B is in primary decomposition form: each index is a power of a prime, and they're sorted in ascending order.
- Group C is in invariant factor form: each index divides the one after it.
- So the primary decomposition of group A is group B, while the invariant factor decomposition of group A is group C.

The example we already saw

The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- Group B is in primary decomposition form: each index is a power of a prime, and they're sorted in ascending order.
- Group C is in invariant factor form: each index divides the one after it.
- So the primary decomposition of group A is group B, while the invariant factor decomposition of group A is group C.

The example we already saw

The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- Group B is in primary decomposition form: each index is a power of a prime, and they're sorted in ascending order.
- Group C is in invariant factor form: each index divides the one after it.
- So the primary decomposition of group A is group B, while the invariant factor decomposition of group A is group C.

The example we already saw

The following three groups are all isomorphic.

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

- Group B is in primary decomposition form: each index is a power of a prime, and they're sorted in ascending order.
- Group C is in invariant factor form: each index divides the one after it.
- So the primary decomposition of group A is group B, while the invariant factor decomposition of group A is group C.

Greater context

Primary importance of these canonical forms

To see whether two finite abelian groups are isomorphic, just write them both in primary decomposition form (or both in invariant factor form) and see if the two expressions are identical.

This seems a little familiar. . .

The proofs of these facts about canonical forms often falls under a much more general theorem called the "structure theorem for finitely generated modules over a PID", of which finite(ly generated) abelian groups are an example.

Now we can return to the question:

Question

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

Let's start with an important special subquestion:

Question

When is the multiplicative group M_n cyclic? (If it is cyclic, it will be isomorphic to $C_{\phi(n)}$.)

Alternatively: when does M_n have a generator—an integer a such that $a, a^2, \ldots, a^{\phi(n)}$ run over all of the elements of M_n?

It turns out that number theorists have a complete answer to this question! (We call those generators "primitive roots".)

Now we can return to the question:

Question

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

Let's start with an important special subquestion:

Question

When is the multiplicative group M_n cyclic? (If it is cyclic, it will be isomorphic to $C_{\phi(n)}$.)

Alternatively: when does M_n have a generator—an integer a such that $a, a^2, \ldots, a^{\phi(n)}$ run over all of the elements of M_n?

It turns out that number theorists have a complete answer to this question! (We call those generators "primitive roots".)

When n is a prime power

If p is an odd prime:

- M_p is always cyclic: $M_p \cong C_{\phi(p)} = C_{p-1}$. Example:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	16	32	64	128	256	512	1024
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

- M_{p^r} is cyclic for all $r \geq 1$: $M_{p^r} \cong C_{\phi(p^r)} = C_{p^{r-1}(p-1)}$.

2 is the oddest prime of all

- Small groups are boring: $M_2 \cong C_1$ and $M_4 \cong C_2$
- If $r \geq 3$, then $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$. (as close to being cyclic as you can get without being cyclic)

M_n is cyclic if and only if n is a power of an odd prime, or twice a power of an odd prime, or 1, 2, or 4

When n is a prime power

If p is an odd prime:

- M_p is always cyclic: $M_p \cong C_{\phi(p)} = C_{p-1}$. Example:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	16	32	64	128	256	512	1024
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

- M_{p^r} is cyclic for all $r \geq 1$: $M_{p^r} \cong C_{\phi(p^r)} = C_{p^{r-1}(p-1)}$.

2 is the oddest prime of all

- Small groups are boring: $M_2 \cong C_1$ and $M_4 \cong C_2$
- If $r \geq 3$, then $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$. (as close to being cyclic as you can get without being cyclic)

M_n is cyclic if and only if n is a power of an odd prime, or twice a power of an odd prime, or 1, 2, or 4

When n is a prime power

If p is an odd prime:

- M_p is always cyclic: $M_p \cong C_{\phi(p)} = C_{p-1}$. Example:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	16	32	64	128	256	512	1024
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

- M_{p^r} is cyclic for all $r \geq 1$: $M_{p^r} \cong C_{\phi(p^r)} = C_{p^{r-1}(p-1)}$.

2 is the oddest prime of all

- Small groups are boring: $M_2 \cong C_1$ and $M_4 \cong C_2$
- If $r \geq 3$, then $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$. (as close to being cyclic as you can get without being cyclic)

M_n is cyclic if and only if n is a power of an odd prime, or twice a power of an odd prime, or 1, 2, or 4

When n is a prime power

If p is an odd prime:

- M_p is always cyclic: $M_p \cong C_{\phi(p)} = C_{p-1}$. Example:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	16	32	64	128	256	512	1024
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

- M_{p^r} is cyclic for all $r \geq 1$: $M_{p^r} \cong C_{\phi(p^r)} = C_{p^{r-1}(p-1)}$.

2 is the oddest prime of all

- Small groups are boring: $M_2 \cong C_1$ and $M_4 \cong C_2$
- If $r \geq 3$, then $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$. (as close to being cyclic as you can get without being cyclic)

M_n is cyclic if and only if n is a power of an odd prime, or twice a power of an odd prime, or 1, 2, or 4

When n is a prime power

If p is an odd prime:

- M_p is always cyclic: $M_p \cong C_{\phi(p)} = C_{p-1}$. Example:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	16	32	64	128	256	512	1024
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

- M_{p^r} is cyclic for all $r \geq 1$: $M_{p^r} \cong C_{\phi(p^r)} = C_{p^{r-1}(p-1)}$.

2 is the oddest prime of all

- Small groups are boring: $M_2 \cong C_1$ and $M_4 \cong C_2$
- If $r \geq 3$, then $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$. (as close to being cyclic as you can get without being cyclic)

M_n is cyclic if and only if n is a power of an odd prime, or twice a power of an odd prime, or 1, 2, or 4

When n is a prime power

If p is an odd prime:

- M_p is always cyclic: $M_p \cong C_{\phi(p)} = C_{p-1}$. Example:

k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	16	32	64	128	256	512	1024
$2^k \pmod{11}$	2	4	8	5	10	9	7	3	6	1

- M_{p^r} is cyclic for all $r \geq 1$: $M_{p^r} \cong C_{\phi(p^r)} = C_{p^{r-1}(p-1)}$.

2 is the oddest prime of all

- Small groups are boring: $M_2 \cong C_1$ and $M_4 \cong C_2$
- If $r \geq 3$, then $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$. (as close to being cyclic as you can get without being cyclic)

M_n is cyclic if and only if n is a power of an odd prime, or twice a power of an odd prime, or 1, 2, or 4

Identifying the group M_n

From the previous slide:

- If p is an odd prime and $r \geq 1$, then $M_{p^r} \cong C_{p^{r-1}(p-1)}$
- $M_2 \cong C_1$ and $M_4 \cong C_2$
- $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$ when $r \geq 3$

Algorithm for identifying M_n

- Factor n into prime powers: $n = p_1^{r_1} p_2^{r_2} \cdots p_2^{r_k}$
- Chinese remainder theorem: $M_n \cong M_{p_1^{r_1}} \times M_{p_2^{r_2}} \times \cdots \times M_{p_k^{r_k}}$
- For each piece: use the known isomorphisms above
- Convert the resulting group to one of the canonical forms

Identifying the group M_n

From the previous slide:

- If p is an odd prime and $r \geq 1$, then $M_{p^r} \cong C_{p^{r-1}(p-1)}$
- $M_2 \cong C_1$ and $M_4 \cong C_2$
- $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$ when $r \geq 3$

Algorithm for identifying M_n

- Factor n into prime powers: $n = p_1^{r_1} p_2^{r_2} \cdots p_2^{r_k}$
- Chinese remainder theorem: $M_n \cong M_{p_1^{r_1}} \times M_{p_2^{r_2}} \times \cdots \times M_{p_k^{r_k}}$
- For each piece: use the known isomorphisms above
- Convert the resulting group to one of the canonical forms

Identifying the group M_n

From the previous slide:

- If p is an odd prime and $r \geq 1$, then $M_{p^r} \cong C_{p^{r-1}(p-1)}$
- $M_2 \cong C_1$ and $M_4 \cong C_2$
- $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$ when $r \geq 3$

Algorithm for identifying M_n

- Factor n into prime powers: $n = p_1^{r_1} p_2^{r_2} \cdots p_2^{r_k}$
- Chinese remainder theorem: $M_n \cong M_{p_1^{r_1}} \times M_{p_2^{r_2}} \times \cdots \times M_{p_k^{r_k}}$
- For each piece: use the known isomorphisms above
- Convert the resulting group to one of the canonical forms

Identifying the group M_n

From the previous slide:

- If p is an odd prime and $r \geq 1$, then $M_{p^r} \cong C_{p^{r-1}(p-1)}$
- $M_2 \cong C_1$ and $M_4 \cong C_2$
- $M_{2^r} \cong C_2 \oplus C_{2^{r-2}}$ when $r \geq 3$

Algorithm for identifying M_n

- Factor n into prime powers: $n = p_1^{r_1} p_2^{r_2} \cdots p_2^{r_k}$
- Chinese remainder theorem: $M_n \cong M_{p_1^{r_1}} \times M_{p_2^{r_2}} \times \cdots \times M_{p_k^{r_k}}$
- For each piece: use the known isomorphisms above
- Convert the resulting group to one of the canonical forms

Let's do an example!

Consider $n = 39{,}916{,}800 = 11!$ (really easy to factor).

Identifying $M_{11!}$

- Factor into prime powers: $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$
- CRT: $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$
- Isomorphisms: $M_{11!} \cong M_{2^8} \times C_{3^3 \cdot 2} \oplus C_{5 \cdot 4} \oplus C_6 \oplus C_{10}$

By sheer coincidence:

- This is "group A" from earlier in the talk:
  $M_{11!} \cong C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$
- Primary decomposition:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$
- Invariant factor form:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Let's do an example!

Consider $n = 39{,}916{,}800 = 11!$ (really easy to factor).

Identifying $M_{11!}$

- Factor into prime powers: $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$
- CRT: $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$
- Isomorphisms: $M_{11!} \cong M_{2^8} \times C_{3^3 \cdot 2} \oplus C_{5 \cdot 4} \oplus C_6 \oplus C_{10}$

By sheer coincidence:

- This is "group A" from earlier in the talk:
  $M_{11!} \cong C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$
- Primary decomposition:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$
- Invariant factor form:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Let's do an example!

Consider $n = 39{,}916{,}800 = 11!$ (really easy to factor).

Identifying $M_{11!}$

- Factor into prime powers: $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$
- CRT: $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$
- Isomorphisms: $M_{11!} \cong M_{2^8} \times C_{3^3 \cdot 2} \oplus C_{5 \cdot 4} \oplus C_6 \oplus C_{10}$

By sheer coincidence:

- This is "group A" from earlier in the talk:
  $M_{11!} \cong C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$
- Primary decomposition:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$
- Invariant factor form:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Let's do an example!

Consider $n = 39{,}916{,}800 = 11!$ (really easy to factor).

Identifying $M_{11!}$

- Factor into prime powers: $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$
- CRT: $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$
- Isomorphisms: $M_{11!} \cong C_2 \oplus C_{2^6} \oplus C_{3^3 \cdot 2} \oplus C_{5 \cdot 4} \oplus C_6 \oplus C_{10}$

By sheer coincidence:

- This is "group A" from earlier in the talk:
  $M_{11!} \cong C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$
- Primary decomposition:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$
- Invariant factor form:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Let's do an example!

Consider $n = 39{,}916{,}800 = 11!$ (really easy to factor).

Identifying $M_{11!}$

- Factor into prime powers: $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$
- CRT: $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$
- Isomorphisms: $M_{11!} \cong C_2 \oplus C_{2^6} \oplus C_{3^3 \cdot 2} \oplus C_{5 \cdot 4} \oplus C_6 \oplus C_{10}$

By sheer coincidence:

- This is "group A" from earlier in the talk:
  $M_{11!} \cong C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$
- Primary decomposition:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$
- Invariant factor form:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Let's do an example!

Consider $n = 39{,}916{,}800 = 11!$ (really easy to factor).

Identifying $M_{11!}$

- Factor into prime powers: $11! = 2^8 \times 3^4 \times 5^2 \times 7 \times 11$
- CRT: $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$
- Isomorphisms: $M_{11!} \cong C_2 \oplus C_{2^6} \oplus C_{3^3 \cdot 2} \oplus C_{5 \cdot 4} \oplus C_6 \oplus C_{10}$

By sheer coincidence:

- This is "group A" from earlier in the talk:
  $M_{11!} \cong C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$
- Primary decomposition:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$
- Invariant factor form:
  $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Our second statistic of M_n

Example: the number of invariant factors of M_n

- Define $\#IF(n)$ to be the number of invariant factors of M_n.
- How big and small can $\#IF(n)$ get?
- What do we expect $\#IF(n)$ to be if we "pick n at random"?

The calculation for $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Each odd prime dividing n contributes exactly one C_{2^r} to the primary decomposition; so there must be (at least) this many invariant factors.

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Our second statistic of M_n

Example: the number of invariant factors of M_n

- Define $\#IF(n)$ to be the number of invariant factors of M_n.
- How big and small can $\#IF(n)$ get?
- What do we expect $\#IF(n)$ to be if we "pick n at random"?

The calculation for $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Each odd prime dividing n contributes exactly one C_{2^r} to the primary decomposition; so there must be (at least) this many invariant factors.

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Our second statistic of M_n

Example: the number of invariant factors of M_n

- Define $\#IF(n)$ to be the number of invariant factors of M_n.
- How big and small can $\#IF(n)$ get?
- What do we expect $\#IF(n)$ to be if we "pick n at random"?

The calculation for $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Each odd prime dividing n contributes exactly one C_{2^r} to the primary decomposition; so there must be (at least) this many invariant factors.

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Our second statistic of M_n

Example: the number of invariant factors of M_n

- Define $\#IF(n)$ to be the number of invariant factors of M_n.
- How big and small can $\#IF(n)$ get?
- What do we expect $\#IF(n)$ to be if we "pick n at random"?

The calculation for $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Each odd prime dividing n contributes exactly one C_{2^r} to the primary decomposition; so there must be (at least) this many invariant factors.

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Our second statistic of M_n

Example: the number of invariant factors of M_n

- Define $\#IF(n)$ to be the number of invariant factors of M_n.
- How big and small can $\#IF(n)$ get?
- What do we expect $\#IF(n)$ to be if we "pick n at random"?

The calculation for $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Each odd prime dividing n contributes exactly one C_{2^r} to the primary decomposition; so there must be (at least) this many invariant factors.

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Our second statistic of M_n

Example: the number of invariant factors of M_n

- Define $\#IF(n)$ to be the number of invariant factors of M_n.
- How big and small can $\#IF(n)$ get?
- What do we expect $\#IF(n)$ to be if we "pick n at random"?

The calculation for $M_{11!} \cong M_{2^8} \times M_{3^4} \times M_{5^2} \times M_7 \times M_{11}$

A. $C_2 \oplus C_{64} \oplus C_{54} \oplus C_{20} \oplus C_6 \oplus C_{10}$

B. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_5 \oplus C_{27} \oplus C_{64}$

C. $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$

Each odd prime dividing n contributes exactly one C_{2^r} to the primary decomposition; so there must be (at least) this many invariant factors.

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Steal what number theorists know

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Minimal order

- If M_n is cyclic (for example, if n is prime), then $\#IF(n) = 1$.
- There are (still) infinitely many primes.

Maximal order

- $\#IF(n) < \dfrac{2\ln n}{\ln(\ln n)}$ for every $n \geq 4$.
- There are infinitely many n for which $\#IF(n) > \dfrac{\ln n}{\ln(\ln n)}$.

Steal what number theorists know

$\#IF(n)$ is the number of prime factors of n, or else off by ± 1

Minimal order

- If M_n is cyclic (for example, if n is prime), then $\#IF(n) = 1$.
- There are (still) infinitely many primes.

Maximal order

- $\#IF(n) < \dfrac{2 \ln n}{\ln(\ln n)}$ for every $n \geq 4$.
- There are infinitely many n for which $\#IF(n) > \dfrac{\ln n}{\ln(\ln n)}$.

What is the expected size of $\#IF(n)$?

For any fixed $x \geq 1$:

- The expected value of $\#IF(n)$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\dfrac{1}{x}\displaystyle\sum_{n=1}^{x} \#IF(n)$.
- We know how to show that $\displaystyle\sum_{n=1}^{x} \#IF(n) = x\ln(\ln x) + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq x/\ln x$.
- Therefore the "expected size of $\#IF(n)$" is $\ln(\ln n)$:

$$\lim_{x\to\infty} \frac{1}{x}\left(\sum_{n=1}^{x} \big(\#IF(n) - \ln(\ln n)\big)\right) = 0.$$

$\#IF(n)$ is $\ln(\ln n)$ on average

What is the expected size of $\#IF(n)$?

For any fixed $x \geq 1$:

- The expected value of $\#IF(n)$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\dfrac{1}{x}\displaystyle\sum_{n=1}^{x} \#IF(n)$.
- We know how to show that $\displaystyle\sum_{n=1}^{x} \#IF(n) = x\ln(\ln x) + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq x/\ln x$.
- Therefore the "expected size of $\#IF(n)$" is $\ln(\ln n)$:

$$\lim_{x\to\infty} \frac{1}{x}\left(\sum_{n=1}^{x} \big(\#IF(n) - \ln(\ln n)\big)\right) = 0.$$

$\#IF(n)$ is $\ln(\ln n)$ on average

What is the expected size of $\#IF(n)$?

For any fixed $x \geq 1$:

- The expected value of $\#IF(n)$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\dfrac{1}{x}\displaystyle\sum_{n=1}^{x} \#IF(n)$.
- We know how to show that $\displaystyle\sum_{n=1}^{x} \#IF(n) = x\ln(\ln x) + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq x/\ln x$.
- Therefore the "expected size of $\#IF(n)$" is $\ln(\ln n)$:

$$\lim_{x\to\infty} \frac{1}{x}\left(\sum_{n=1}^{x} \big(\#IF(n) - \ln(\ln n)\big)\right) = 0.$$

$\#IF(n)$ is $\ln(\ln n)$ on average

What is the expected size of $\#IF(n)$?

For any fixed $x \geq 1$:

- The expected value of $\#IF(n)$, when n is chosen uniformly at random from $\{1, 2, \ldots, x\}$, is exactly $\dfrac{1}{x}\displaystyle\sum_{n=1}^{x} \#IF(n)$.
- We know how to show that $\displaystyle\sum_{n=1}^{x} \#IF(n) = x\ln(\ln x) + \varepsilon(x)$, where $\varepsilon(x)$ is a function satisfying $|\varepsilon(x)| \leq x/\ln x$.
- Therefore the "expected size of $\#IF(n)$" is $\ln(\ln n)$:

$$\lim_{x\to\infty} \frac{1}{x}\left(\sum_{n=1}^{x} \big(\#IF(n) - \ln(\ln n)\big)\right) = 0.$$

$\#IF(n)$ is $\ln(\ln n)$ on average

Statistics of $\#IF(n)$

- Expected size: about $\ln(\ln n)$
- Variance: also about $\ln(\ln n)$:

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left\{\Big(\#IF(n)-\ln(\ln n)\Big)^2-\ln(\ln n)\right\}\right)=0$$

How can we investigate the "distribution of $\#IF(n)$"?

Normalization

Create a normalized statistic by subtracting the expectation and dividing by the "standard deviation":

$$NIF(n)=\frac{\#IF(n)-\ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Forces the expectation and variance of $NIF(n)$ to both be 1.

Statistics of $\#IF(n)$

- Expected size: about $\ln(\ln n)$
- Variance: also about $\ln(\ln n)$:

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left\{\Big(\#IF(n)-\ln(\ln n)\Big)^2-\ln(\ln n)\right\}\right)=0$$

How can we investigate the "distribution of $\#IF(n)$"?

Normalization

Create a normalized statistic by subtracting the expectation and dividing by the "standard deviation":

$$NIF(n)=\frac{\#IF(n)-\ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Forces the expectation and variance of $NIF(n)$ to both be 1.

Statistics of $\#IF(n)$

- Expected size: about $\ln(\ln n)$
- Variance: also about $\ln(\ln n)$:

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left\{\Big(\#IF(n)-\ln(\ln n)\Big)^2-\ln(\ln n)\right\}\right)=0$$

How can we investigate the "distribution of $\#IF(n)$"?

Normalization

Create a normalized statistic by subtracting the expectation and dividing by the "standard deviation":

$$NIF(n)=\frac{\#IF(n)-\ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Forces the expectation and variance of $NIF(n)$ to both be 1.

Statistics of $\#IF(n)$

- Expected size: about $\ln(\ln n)$
- Variance: also about $\ln(\ln n)$:

$$\lim_{x\to\infty}\left(\frac{1}{x}\sum_{n=1}^{x}\left\{\Big(\#IF(n)-\ln(\ln n)\Big)^2-\ln(\ln n)\right\}\right)=0$$

How can we investigate the "distribution of $\#IF(n)$"?

Normalization

Create a normalized statistic by subtracting the expectation and dividing by the "standard deviation":

$$NIF(n)=\frac{\#IF(n)-\ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Forces the expectation and variance of $NIF(n)$ to both be 1.

Statistics of $\#IF(n)$

Normalization

$$NIF(n) = \frac{\#IF(n) - \ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Erdős–Kac Theorem (1940)

The cumulative distribution function for $NIF(n)$ is

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

In other words: if you pick an integer n at random, the distribution of $NIF(n)$ is the same as the distribution $\mathcal{N}(0,1)$—the standard normal distribution!

Statistics of $\#IF(n)$

Normalization

$$NIF(n) = \frac{\#IF(n) - \ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Erdős–Kac Theorem (1940)

The cumulative distribution function for $NIF(n)$ is

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

In other words: if you pick an integer n at random, the distribution of $NIF(n)$ is the same as the distribution $\mathcal{N}(0,1)$—the standard normal distribution!

Statistics of $\#IF(n)$

Normalization

$$NIF(n) = \frac{\#IF(n) - \ln(\ln n)}{\sqrt{\ln(\ln n)}}.$$

Erdős–Kac Theorem (1940)

The cumulative distribution function for $NIF(n)$ is

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

In other words: if you pick an integer n at random, the distribution of $NIF(n)$ is the same as the distribution $\mathcal{N}(0,1)$—the standard normal distribution!

Other statistics: smallest primary decomposition piece

It's really easy to get a C_2 in the primary decomposition

- If n is a multiple of 4, then M_{2^r} gives rise to a C_2
- If some prime p dividing n is of the form $p = 4k+3$, then

$$M_p \cong C_{p-1} = C_{4k+2} \cong C_2 \oplus C_{2k+1}$$

So we see:

The smallest piece in the primary decomposition for M_n is C_2, unless all the primes p dividing n satisfy $p \equiv 1 \pmod 4$. (A single factor of 2 dividing n is allowed.)

Number theorists know how to count these exceptions!

The number of integers $n \le x$ with the above property is about

$$\frac{Cx}{\sqrt{\ln x}}, \text{ where } C = \frac{9\pi}{32} \prod_{p \equiv 3 \pmod 4} \sqrt{1 - \frac{1}{p^2}} \approx 0.8175.$$

Other statistics: smallest primary decomposition piece

It's really easy to get a C_2 in the primary decomposition

- If n is a multiple of 4, then M_{2^r} gives rise to a C_2
- If some prime p dividing n is of the form $p = 4k+3$, then

$$M_p \cong C_{p-1} = C_{4k+2} \cong C_2 \oplus C_{2k+1}$$

So we see:

The smallest piece in the primary decomposition for M_n is C_2, unless all the primes p dividing n satisfy $p \equiv 1 \pmod 4$. (A single factor of 2 dividing n is allowed.)

Number theorists know how to count these exceptions!

The number of integers $n \le x$ with the above property is about

$$\frac{Cx}{\sqrt{\ln x}}, \text{ where } C = \frac{9\pi}{32} \prod_{p \equiv 3 \pmod 4} \sqrt{1 - \frac{1}{p^2}} \approx 0.8175.$$

Other statistics: smallest primary decomposition piece

It's really easy to get a C_2 in the primary decomposition

- If n is a multiple of 4, then M_{2^r} gives rise to a C_2
- If some prime p dividing n is of the form $p = 4k+3$, then

$$M_p \cong C_{p-1} = C_{4k+2} \cong C_2 \oplus C_{2k+1}$$

So we see:

The smallest piece in the primary decomposition for M_n is C_2, unless all the primes p dividing n satisfy $p \equiv 1 \pmod 4$. (A single factor of 2 dividing n is allowed.)

Number theorists know how to count these exceptions!

The number of integers $n \le x$ with the above property is about

$$\frac{Cx}{\sqrt{\ln x}}, \text{ where } C = \frac{9\pi}{32} \prod_{p \equiv 3 \pmod 4} \sqrt{1 - \frac{1}{p^2}} \approx 0.8175.$$

Other statistics: largest invariant factor

Looking back at $M_{11!}$

- The size of $M_{11!}$ is $\phi(11!) = 8{,}294{,}400$, and so $a^{8{,}294{,}400} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$ (Euler's theorem)
- However, $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$, and so actually $a^{8640} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$.

Definition

1. The exponent of a finite abelian group G is the smallest integer m such that $a^m = e$ (group identity) for every $a \in G$.

   The exponent of a finite abelian group is the same as the size of the largest invariant factor.
2. The exponent of the multiplicative group M_n is called the Carmichael lambda-function $\lambda(n)$.

Other statistics: largest invariant factor

Looking back at $M_{11!}$

- The size of $M_{11!}$ is $\phi(11!) = 8{,}294{,}400$, and so $a^{8{,}294{,}400} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$ (Euler's theorem)
- However, $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$, and so actually $a^{8640} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$.

Definition

1. The exponent of a finite abelian group G is the smallest integer m such that $a^m = e$ (group identity) for every $a \in G$.

   The exponent of a finite abelian group is the same as the size of the largest invariant factor.
2. The exponent of the multiplicative group M_n is called the Carmichael lambda-function $\lambda(n)$.

Other statistics: largest invariant factor

Looking back at $M_{11!}$

- The size of $M_{11!}$ is $\phi(11!) = 8{,}294{,}400$, and so $a^{8,294,400} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$ (Euler's theorem)
- However, $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$, and so actually $a^{8640} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$.

Definition

1. The exponent of a finite abelian group G is the smallest integer m such that $a^m = e$ (group identity) for every $a \in G$.

   The exponent of a finite abelian group is the same as the size of the largest invariant factor.
2. The exponent of the multiplicative group M_n is called the Carmichael lambda-function $\lambda(n)$.

Other statistics: largest invariant factor

Looking back at $M_{11!}$

- The size of $M_{11!}$ is $\phi(11!) = 8{,}294{,}400$, and so $a^{8{,}294{,}400} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$ (Euler's theorem)
- However, $M_{11!} \cong C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_{60} \oplus C_{8640}$, and so actually $a^{8640} \equiv 1 \pmod{11!}$ for every $a \in M_{11!}$.

Definition

1. The exponent of a finite abelian group G is the smallest integer m such that $a^m = e$ (group identity) for every $a \in G$.

   The exponent of a finite abelian group is the same as the size of the largest invariant factor.
2. The exponent of the multiplicative group M_n is called the Carmichael lambda-function $\lambda(n)$.

Other statistics: largest invariant factor

$\lambda(n) =$ size of largest invariant factor of M_n

$\lambda(n)$ always divides $\phi(n)$, and they are equal precisely when M_n is cyclic. However, $\lambda(n)$ can be far smaller than n.

Notation

$$F(x) = (\ln x)^{\ln(\ln(\ln x))} = \exp\big(\ln(\ln x)\ln(\ln(\ln x))\big)$$

Known facts about $\lambda(n)$

- Minimal order: $\lambda(n)$ is sometimes as small as $F(n)^{1/\ln 2}$
- Typical order: $\lambda(n)$ is usually around $n/F(n)$

Other statistics: largest invariant factor

$$\lambda(n) = \text{ size of largest invariant factor of } M_n$$

$\lambda(n)$ always divides $\phi(n)$, and they are equal precisely when M_n is cyclic. However, $\lambda(n)$ can be far smaller than n.

Notation

$$F(x) = (\ln x)^{\ln(\ln(\ln x))} = \exp\big(\ln(\ln x)\ln(\ln(\ln x))\big)$$

Known facts about $\lambda(n)$

- Minimal order: $\lambda(n)$ is sometimes as small as $F(n)^{1/\ln 2}$
- Typical order: $\lambda(n)$ is usually around $n/F(n)$

Other examples: largest primary decomposition factor

Recall that the primary decomposition factors of M_n are all cyclic groups of prime power order; and each prime power that appears divides $\phi(p^r) = p^{r-1}(p-1)$ for some p^r dividing n.

Modified problem

What is the largest prime q that divides $p-1$, where p is the largest prime dividing n? (on average, pick n at random, etc.)

Bad news all around

- We're simply ignoring prime powers.
- Even so, we want the largest prime dividing $p-1$ for some prime p dividing n; we don't know in advance whether p is the largest prime dividing n.
- Even so, the modified problem is still an open problem!

Other examples: largest primary decomposition factor

Recall that the primary decomposition factors of M_n are all cyclic groups of prime power order; and each prime power that appears divides $\phi(p^r) = p^{r-1}(p-1)$ for some p^r dividing n.

Modified problem

What is the largest prime q that divides $p-1$, where p is the largest prime dividing n? (on average, pick n at random, etc.)

Bad news all around

- We're simply ignoring prime powers.
- Even so, we want the largest prime dividing $p-1$ for some prime p dividing n; we don't know in advance whether p is the largest prime dividing n.
- Even so, the modified problem is still an open problem!

Other examples: largest primary decomposition factor

Recall that the primary decomposition factors of M_n are all cyclic groups of prime power order; and each prime power that appears divides $\phi(p^r) = p^{r-1}(p-1)$ for some p^r dividing n.

Modified problem

What is the largest prime q that divides $p-1$, where p is the largest prime dividing n? (on average, pick n at random, etc.)

Bad news all around

- We're simply ignoring prime powers.
- Even so, we want the largest prime dividing $p-1$ for some prime p dividing n; we don't know in advance whether p is the largest prime dividing n.
- Even so, the modified problem is still an open problem!

Other examples: largest primary decomposition factor

Recall that the primary decomposition factors of M_n are all cyclic groups of prime power order; and each prime power that appears divides $\phi(p^r) = p^{r-1}(p-1)$ for some p^r dividing n.

Modified problem

What is the largest prime q that divides $p-1$, where p is the largest prime dividing n? (on average, pick n at random, etc.)

Bad news all around

- We're simply ignoring prime powers.
- Even so, we want the largest prime dividing $p-1$ for some prime p dividing n; we don't know in advance whether p is the largest prime dividing n.
- Even so, the modified problem is still an open problem!

Other examples: largest primary decomposition factor

Recall that the primary decomposition factors of M_n are all cyclic groups of prime power order; and each prime power that appears divides $\phi(p^r) = p^{r-1}(p-1)$ for some p^r dividing n.

Modified problem

What is the largest prime q that divides $p-1$, where p is the largest prime dividing n? (on average, pick n at random, etc.)

Bad news all around

- We're simply ignoring prime powers.
- Even so, we want the largest prime dividing $p-1$ for some prime p dividing n; we don't know in advance whether p is the largest prime dividing n.
- Even so, the modified problem is still an open problem!

Other examples: largest primary decomposition factor

Largest prime dividing n, normalized

Define $NLP(n) = \dfrac{\log n}{\log p}$, where p is the largest prime dividing n.

$NLP(n)$ is at least 1; it equals 1 when n is prime; and it's big when n is the product of a bunch of small primes.

Cumulative distribution function

- The CDF of $NLP(n)$ is $f(u) = 1 - \rho(u)$, where $\rho(u)$ is the Dickman–de Bruijn function.
- $\rho(u)$ is defined, not by a regular differential equation, but by the differential-difference equation $\rho'(u) = -\dfrac{\rho(u-1)}{u}$!

  (continuous, with initial condition $\rho(u) = 1$ for $0 \le u \le 1$)

Other examples: largest primary decomposition factor

Largest prime dividing n, normalized

Define $NLP(n) = \dfrac{\log n}{\log p}$, where p is the largest prime dividing n.

$NLP(n)$ is at least 1; it equals 1 when n is prime; and it's big when n is the product of a bunch of small primes.

Cumulative distribution function

- The CDF of $NLP(n)$ is $f(u) = 1 - \rho(u)$, where $\rho(u)$ is the Dickman–de Bruijn function.
- $\rho(u)$ is defined, not by a regular differential equation, but by the differential-difference equation $\rho'(u) = -\dfrac{\rho(u-1)}{u}$!

  (continuous, with initial condition $\rho(u) = 1$ for $0 \le u \le 1$)

Other examples: largest primary decomposition factor

Cumulative distribution functions

- The CDF of $NLP(n)$ is $f(u) = 1 - \rho(u)$, where $\rho(u)$ is the Dickman–de Bruijn function.
- We expect that numbers of the form $p - 1$ (for p prime) are pretty representative of integers as a whole.
- In particular, we expect the CDF of $NLP(p-1)$ to be the same as the CDF of $NLP(n)$, namely $1 - \rho(u)$.

However, this is an open problem!

Our ignorance is showing

- We can't prove that the CDF of $NLP(p-1)$ is positive at all for $u < 1.4$.
- We can't even prove that there are infinitely many primes p such that $p - 1$ is divisible by a prime greater than $p^{0.7}$.

Other examples: largest primary decomposition factor

Cumulative distribution functions

- The CDF of $NLP(n)$ is $f(u) = 1 - \rho(u)$, where $\rho(u)$ is the Dickman–de Bruijn function.
- We expect that numbers of the form $p - 1$ (for p prime) are pretty representative of integers as a whole.
- In particular, we expect the CDF of $NLP(p-1)$ to be the same as the CDF of $NLP(n)$, namely $1 - \rho(u)$.

However, this is an open problem!

Our ignorance is showing

- We can't prove that the CDF of $NLP(p-1)$ is positive at all for $u < 1.4$.
- We can't even prove that there are infinitely many primes p such that $p - 1$ is divisible by a prime greater than $p^{0.7}$.

Other examples: largest primary decomposition factor

Cumulative distribution functions

- The CDF of $NLP(n)$ is $f(u) = 1 - \rho(u)$, where $\rho(u)$ is the Dickman–de Bruijn function.
- We expect that numbers of the form $p - 1$ (for p prime) are pretty representative of integers as a whole.
- In particular, we expect the CDF of $NLP(p-1)$ to be the same as the CDF of $NLP(n)$, namely $1 - \rho(u)$.

However, this is an open problem!

Our ignorance is showing

- We can't prove that the CDF of $NLP(p-1)$ is positive at all for $u < 1.4$.
- We can't even prove that there are infinitely many primes p such that $p - 1$ is divisible by a prime greater than $p^{0.7}$.

The end

These slides are available for downloading.

These slides

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