# The universal invariant profile of the multiplicative group

Greg Martin
University of British Columbia

joint work with Reginald M. Simpson

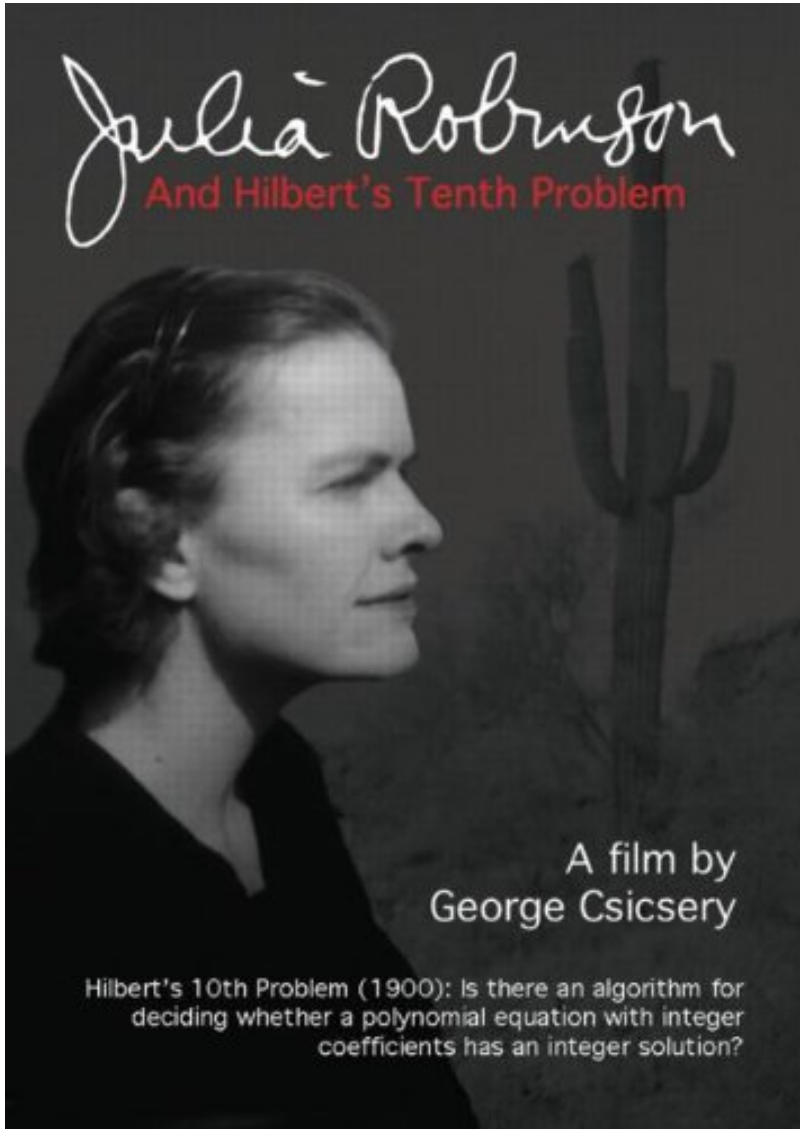
Canadian Mathematical Society Winter Meeting
Toronto, ON
December 9, 2019

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

# Yu–Ru Liu, Stanley Xiao, and Asif Zaman

Thank you for organizing this session!

# You don't look a day over 100 (... although you are)




Julia Robinson (Dec. 8, 1919—July 30, 1985)

Superhero of logic and computability theory, most notably for contributions to Hilbert's 10th problem

# Outline

# The multiplicative group

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

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

## Overarching question

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

Example: $M_n$ is cyclic if and only if $n$ has a primitive root.

## Methodology—analytic number theory

Choose a numerical statistic of $M_n$, and investigate the distribution of that statistic when $n$ is "chosen at random".

Example: Distribution of $\frac{\phi(n)}{n}$ known (Schoenberg, 1928).

# The invariant factor decomposition

## Two forms that answers to the question can take

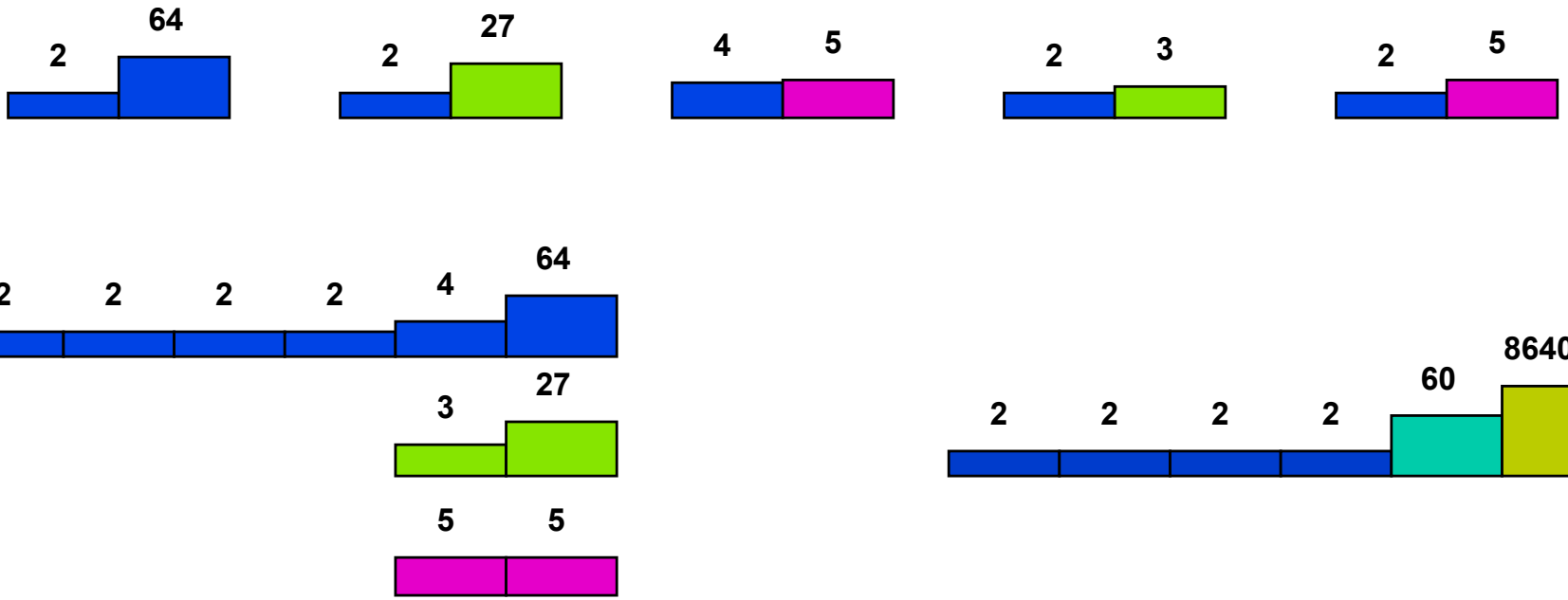
- Primary decomposition: for $G$ finite abelian,
$$G \cong C_{p_1^{r_1}} \oplus \cdots \oplus C_{p_k^{r_k}},$$
where the $p_j^{r_j}$ are prime powers (unique up to reordering)
- Invariant factors: for $G$ finite abelian,
$$G \cong C_{\lambda_1} \oplus \cdots \oplus C_{\lambda_\ell},$$
where $\lambda_1 \mid \lambda_2 \mid \cdots \mid \lambda_\ell$ (unique)

## Another object in analytic number theory

The largest invariant factor $\lambda_\ell$ of $M_n$ equals the Carmichael function $\lambda(n)$, whose distribution has also been investigated (Erdős/Pomerance/Schmutz, 1991).

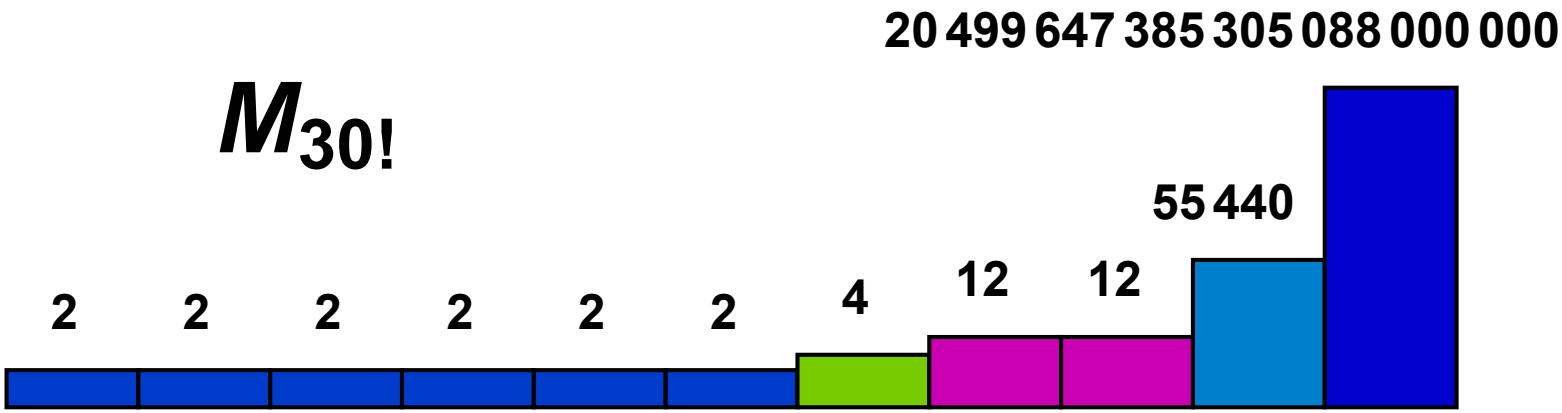
## Example: $M_n$ when $n = 11! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$

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



## Work in progress with Jenna Downey

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




## Theorem (Ben Chang–M., 2019+)

*The number of integers $n \le x$ for which the least invariant factor of $M_n$ does* not *equal 2 is $\sim Cx/\sqrt{\log x}$ for a certain $C > 0$.*

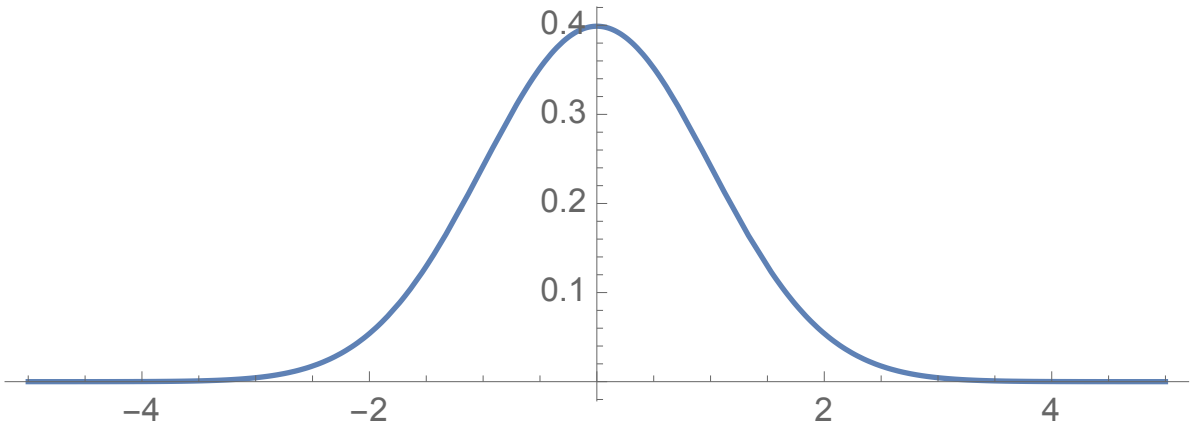
# Connection to $\omega(n)$

**Theorem (Erdős–Kac theorem)**

*The limiting distribution of the normalized statistic*

$$\frac{(\text{number of prime factors of } n) - \log\log n}{(\log\log n)^{1/2}}$$

*is the standard normal random variable.*



# Connection to $\omega(n)$

**Theorem (Erdős–Kac theorem)**

*The limiting distribution of the normalized statistic*

$$\frac{(\text{number of prime factors of } n) - \log\log n}{(\log\log n)^{1/2}}$$

*is the standard normal random variable.*

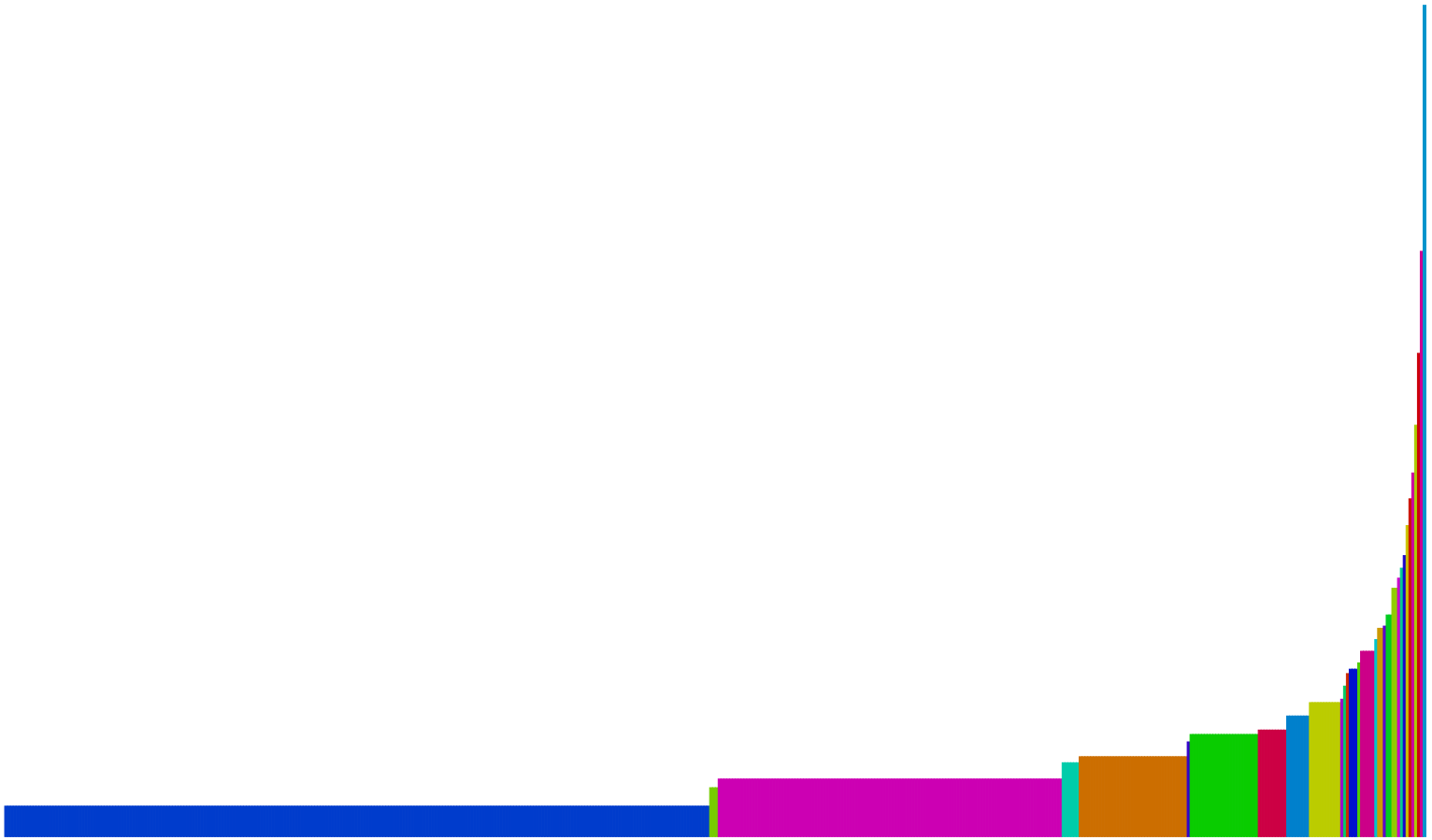
**Theorem (M.–Lee Troupe 2018, answering a question of Vukoslavcevic and Shparlinski)**

*For certain constants $A, B > 0$, the limiting distribution of*

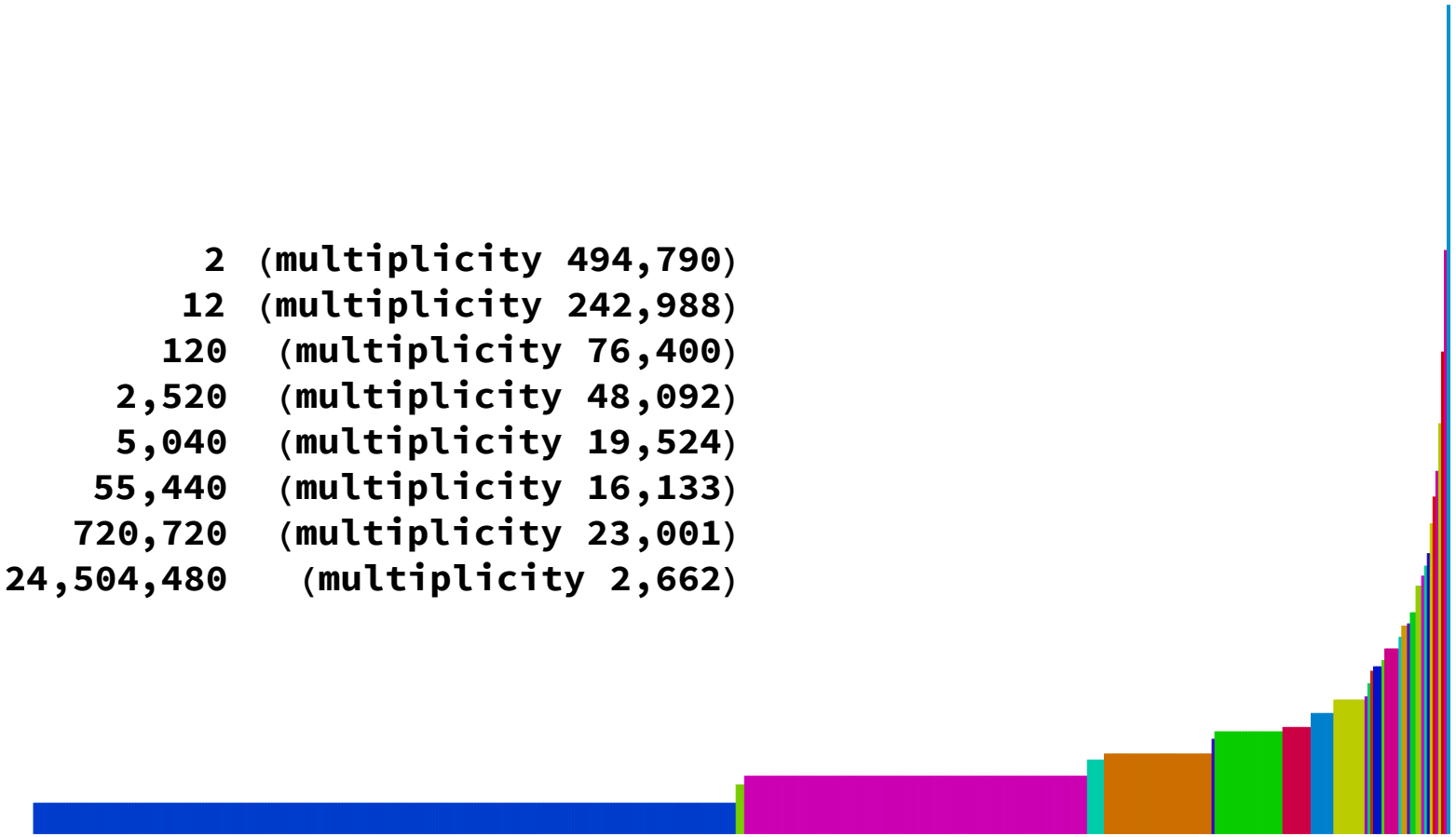
$$\frac{\log(\text{number of subgroups of } M_n) - A(\log\log n)^2}{(B(\log\log n)^3)^{1/2}}$$

*is the standard normal random variable.*

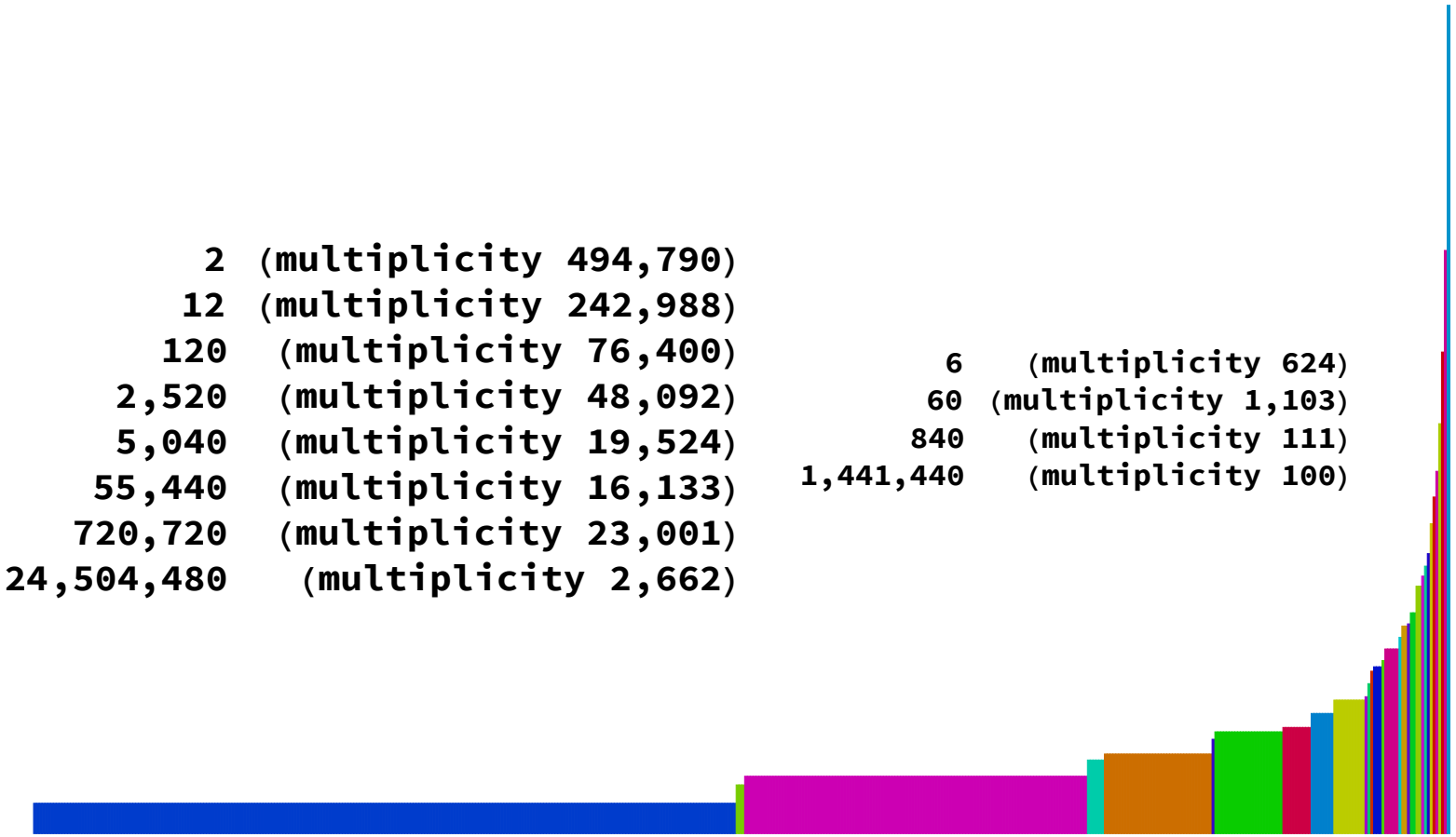
# $M_n$ for a random integer $n$ near $e^{e^{1,000,000}}$



# $M_n$ for a random integer $n$ near $e^{e^{1{,}000{,}000}}$

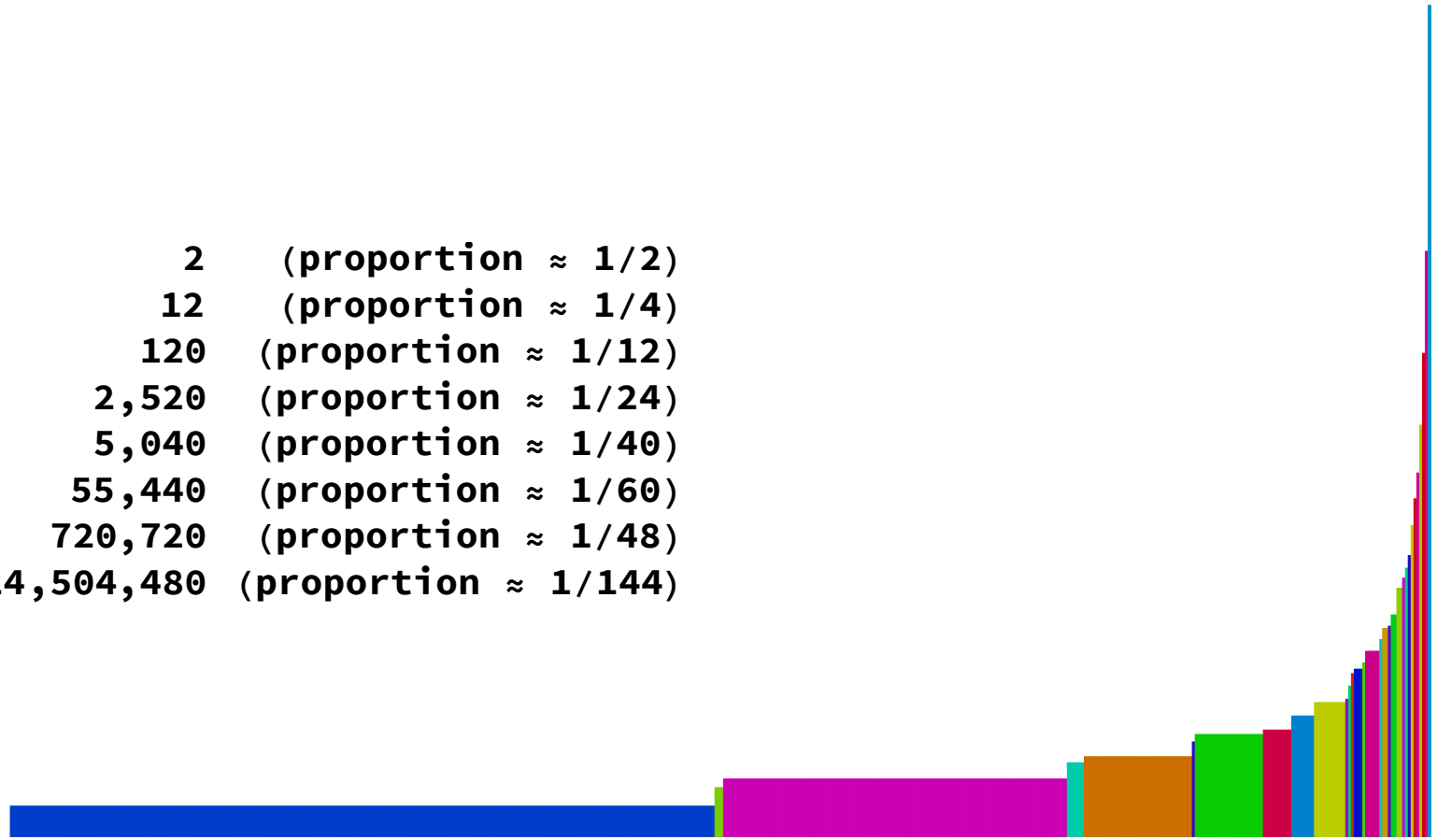


# $M_n$ for a random integer $n$ near $e^{e^{1{,}000{,}000}}$



# $M_n$ for a random integer $n$ near $e^{e^{1{,}000{,}000}}$

```
         2   (proportion ≈ 1/2)
        12   (proportion ≈ 1/4)
       120  (proportion ≈ 1/12)
     2,520  (proportion ≈ 1/24)
     5,040  (proportion ≈ 1/40)
    55,440  (proportion ≈ 1/60)
   720,720  (proportion ≈ 1/48)
24,504,480 (proportion ≈ 1/144)
```



# That integer wasn't so special after all

**Theorem (M.–Reginald M. Simpson, $> 2019$)**

*For almost all integers $n$, the multiplicative group $M_n$ has:*

- $\sim \frac{1}{2} \log\log n$ *invariant factors equal to* $2$;
- $\sim \frac{1}{4} \log\log n$ *invariant factors equal to* $12$;
- $\sim \frac{1}{12} \log\log n$ *invariant factors equal to* $120$;
- $\sim \frac{1}{24} \log\log n$ *invariant factors equal to* $2{,}520$;
- $\sim \frac{1}{40} \log\log n$ *invariant factors equal to* $5{,}040$;
- $\sim \frac{1}{60} \log\log n$ *invariant factors equal to* $55{,}440$;
- $\sim \frac{1}{48} \log\log n$ *invariant factors equal to* $720{,}720$; ...

Interpretation: The important structure arithmetic modulo $n$ seems to be encoded almost completely in the largest few invariant factors.

# What are those sequences of numbers?

## Definition: Prime-power totients

$$\{\phi(p^r) : p \text{ prime}, r \geq 1\} = \{1, 2, 4, 6, 8, 10, 12, 16, 18, 20, \ldots\}$$
$$= \{ppt_1, ppt_2, ppt_3, \ldots\}$$

## Definition: Cumulative least common multiples

$$\lambda(x) = \operatorname{lcm}[p^r : \phi(p^r) \leq x], \qquad \lambda_k = \lambda(ppt_k)$$

## Theorem (M.–Reginald M. Simpson, $> 2019$)

*For almost all integers $n$, the multiplicative group $M_n$ has*

$$\sim \left( \frac{1}{ppt_k} - \frac{1}{ppt_{k+1}} \right) \log\log n$$

*invariant factors equal to $\lambda_k$ for each $k = 1, 2, 3, \ldots$.*

# Example invariant factor: $55{,}440$

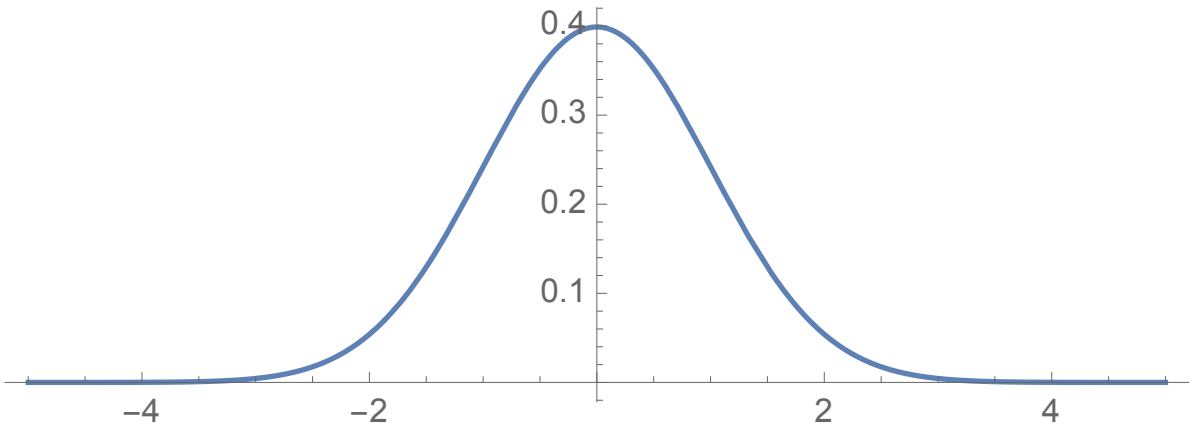
We can be more precise than $\sim \frac{1}{60} \log\log n$ about the multiplicity of the invariant factor $55{,}440$:

**Theorem (M.–Simpson, $> 2019$)**

*The limiting distribution of the normalized count*

$$\frac{(\text{multiplicity of the invariant factor } 55{,}440) - \frac{1}{60}\log\log n}{(\frac{1}{6}\log\log n)^{1/2}}$$

*is the standard normal random variable.*



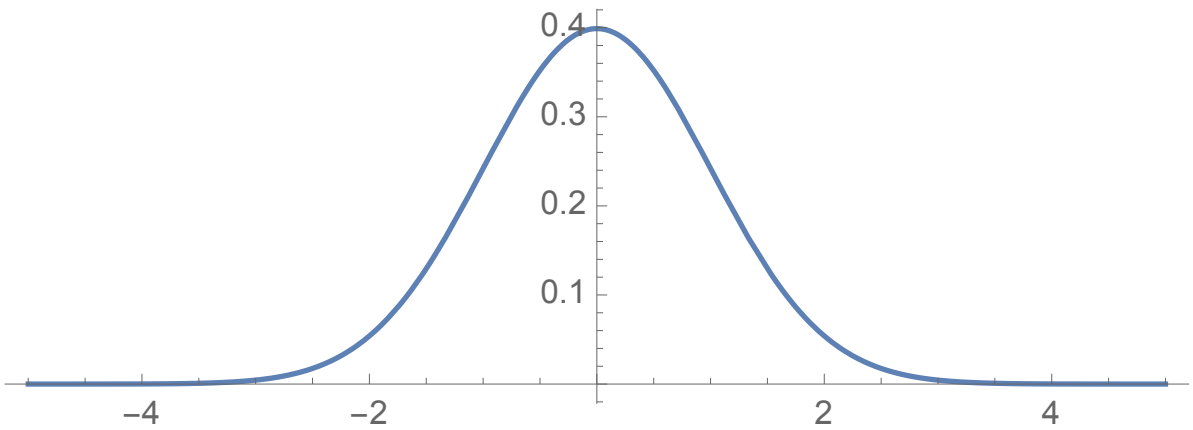
# Example invariant factor: 2 (but lying)

**Theorem (M.–Simpson, $> 2019$)**

*The limiting distribution of the normalized count*

$$\frac{(\text{multiplicity of the invariant factor } 2) - \frac{1}{2}\log\log n}{(\frac{1}{2}\log\log n)^{1/2}}$$

*is the standard normal random variable.*



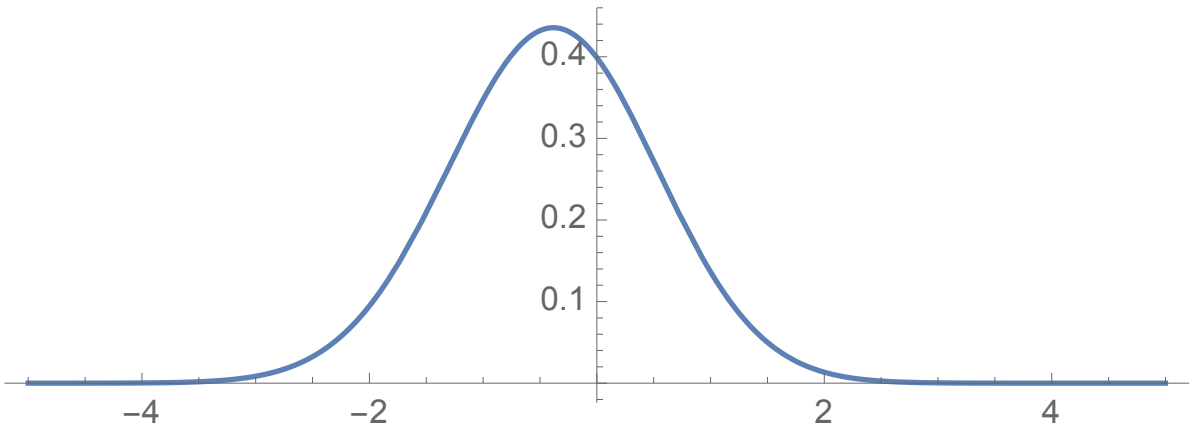
# Example invariant factor: 2 (the truth)

**Theorem (M.–Simpson, $> 2019$)**

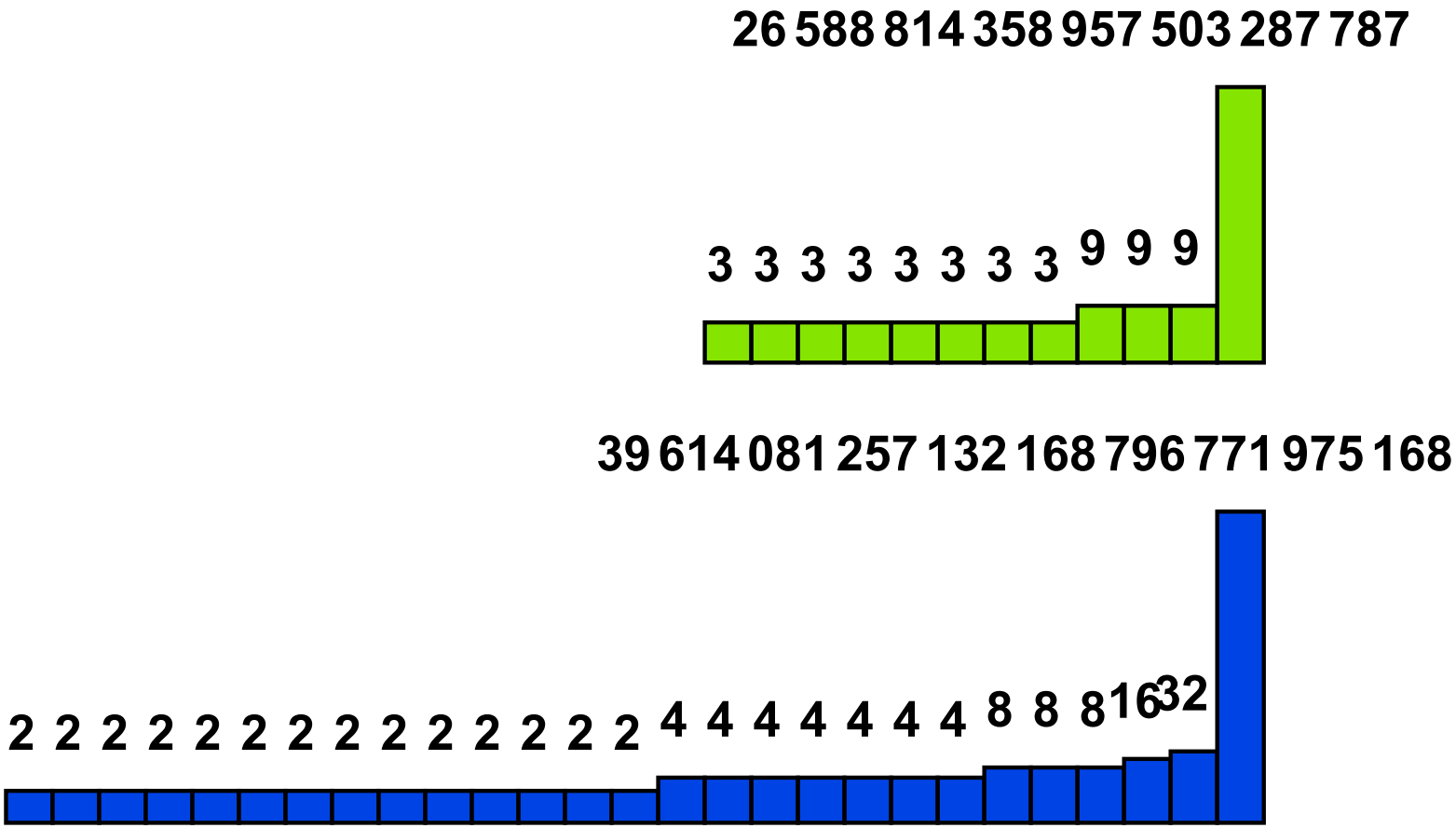
*The limiting distribution of the normalized count*

$$\frac{(\text{multiplicity of the invariant factor } 2) - \frac{1}{2}\log\log n}{(\frac{1}{2}\log\log n)^{1/2}}$$

*is a skew-normal random variable with "shape" parameter* $\frac{1}{\sqrt{3}}$.



# Sylow-2 and -3 subgroups for $M_{101!}$



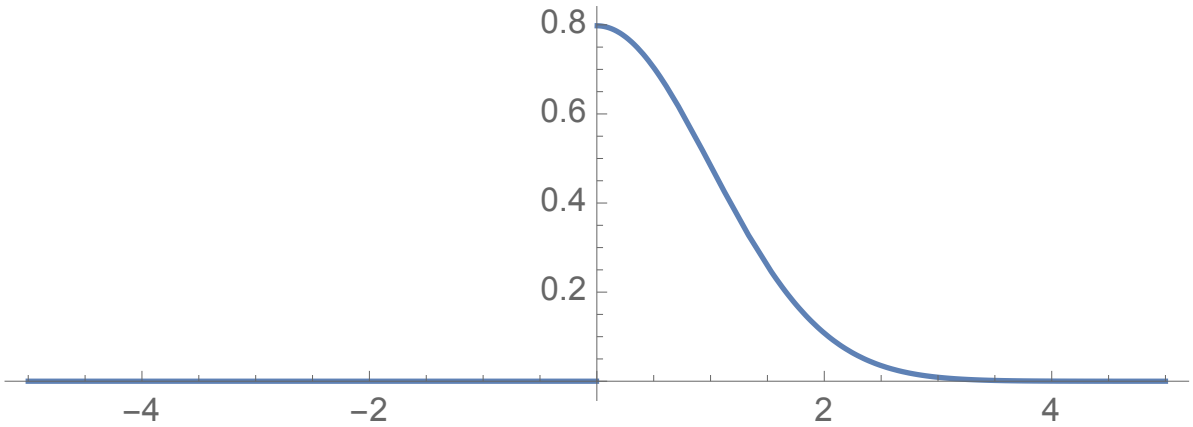

**101! has 26 prime factors . . .**

12 of them are $\equiv 1 \pmod 4$, and 11 of them are $\equiv 1 \pmod 3$

# Invariant factors between 2 and 12

Let $X$ be a standard normal random variable; then $|X|$ has a half-normal distribution.

- For asymptotically $50\%$ of integers $n$, the distribution of $(\text{multiplicity of the invariant factor } 4)/(\frac{1}{2}\log\log n)^{1/2}$ is a standard half-normal variable.
- For asymptotically $50\%$ of integers $n$, the distribution of $(\text{multiplicity of the invariant factor } 6)/(\frac{1}{2}\log\log n)^{1/2}$ is a standard half-normal variable.



# Types of prime power totient pairs

## Fun fact

Every integer is the totient of at most one prime and at most one proper prime power.

| totient | 1 | 2 | 4 | 6 | 8 | 10 | 12 | 16 | 18 | 20 | ⋯ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| prime | 2 | 3 | 5 | 7 | | 11 | 13 | 17 | 19 | | ⋯ |
| prime power | | 4 | 8 | 9 | 16 | | | 32 | 27 | 25 | ⋯ |

A pair $ppt_k, ppt_{k+1}$ of consecutive prime-power totients is called type $(i,j)$ if $ppt_k$ has $i \in \{1,2\}$ prime-power preimages and $ppt_{k+1}$ has $j \in \{1,2\}$ prime-power preimages.

## Examples

- $10, 12$ is type $(1,1)$
- $1, 2$ is type $(1,2)$ and $18, 20$ is type $(2,1)$
- $4, 6$ is type $(2,2)$

# Several different distributions in one theorem

## Theorem (M.–Simpson, $> 2019$)

*For consecutive prime-power totients $ppt_k, ppt_{k+1}$, set $\lambda_k = \operatorname{lcm}[p^r : \phi(p^r) \le ppt_k]$ and $\delta_k = \frac{1}{ppt_k} - \frac{1}{ppt_{k+1}}$. There exists a constant $\sigma_k^2$ such that the limiting distribution of*

$$\frac{(\text{multiplicity of the invariant factor } \lambda_k) - \delta_k \log\log n}{(\sigma_k^2 \log\log n)^{1/2}}$$

*is ...*

- *if $ppt_k, ppt_{k+1}$ is type $(1,1)$: standard normal*
- *if $ppt_k, ppt_{k+1}$ is type $(1,2)$ or type $(2,1)$: skew-normal*
- *if $ppt_k, ppt_{k+1}$ is type $(2,2)$: something (explicit but) peculiar involving a Kampé de Feriét function*
- *when $ppt_2 = 2$ and $ppt_3 = 4$ (so $\lambda_2 = 12$): something aggressively peculiar ...*

# The end

## These slides

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

## The paper with Ben Chang (smallest invariant factor)

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

## The paper with Lee Troupe (number of subgroups)

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

## Papers with Jenna Downey (Sylow subgroups) and Reginald M. Simpson (universal invariant profile)

Coming soon!