The multiplicative orders of certain Gauss factorials

Karl Dilcher

Dalhousie University, Halifax, Nova Scotia, Canada

UIUC Number Theory Seminar, February 19, 2015

Joint work with

John B. Cosgrave

Dublin, Ireland

1. Introduction

We begin with *Wilson's Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

1. Introduction

We begin with *Wilson's Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Write out the factorial $(p-1)!$, exploit symmetry mod p:

$$1\cdot 2\cdot \ldots \cdot \tfrac{p-1}{2}\,\tfrac{p+1}{2}\cdot \ldots \cdot (p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

1. Introduction

We begin with *Wilson's Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Write out the factorial $(p-1)!$, exploit symmetry mod p:

$$1\cdot 2\cdot\ldots\cdot\tfrac{p-1}{2}\tfrac{p+1}{2}\cdot\ldots\cdot(p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

Thus, with Wilson's Theorem,

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

1. Introduction

We begin with *Wilson's Theorem*: p is a prime if and only if

$$(p-1)! \equiv -1 \pmod{p}.$$

Write out the factorial $(p-1)!$, exploit symmetry mod p:

$$1\cdot 2\cdot \ldots \cdot \tfrac{p-1}{2}\,\tfrac{p+1}{2}\cdot \ldots \cdot (p-1) \equiv \left(\tfrac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

Thus, with Wilson's Theorem,

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

This was apparently first observed by Lagrange (1773).

This congruence,

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

has the following consequences:

For $p \equiv 1 \pmod 4$ the RHS is -1, so

$$\mathrm{ord}_p\left(\left(\frac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod 4.$$

This congruence,

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

has the following consequences:

For $p \equiv 1 \pmod{4}$ the RHS is -1, so

$$\operatorname{ord}_p\left(\left(\frac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod{4}.$$

In the case $p \equiv 3 \pmod{4}$ we get

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

This congruence,

$$\left(\tfrac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p},$$

has the following consequences:

For $p \equiv 1 \pmod 4$ the RHS is -1, so

$$\mathrm{ord}_p\left(\left(\tfrac{p-1}{2}\right)!\right) = 4 \quad \text{for} \quad p \equiv 1 \pmod 4.$$

In the case $p \equiv 3 \pmod 4$ we get

$$\left(\tfrac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

What is the sign on the right?

Theorem 1 (Mordell, 1961)

For a prime $p \equiv 3 \pmod 4$,

$$\left(\tfrac{p-1}{2}\right)! \equiv -1 \pmod p \quad \Leftrightarrow \quad h(-p) \equiv 1 \pmod 4,$$

where $h(-p)$ *is the class number of* $\mathbb{Q}(\sqrt{-p})$.

Theorem 1 (Mordell, 1961)

For a prime $p \equiv 3 \pmod 4$*,*

$$\left(\frac{p-1}{2}\right)! \equiv -1 \pmod p \quad \Leftrightarrow \quad h(-p) \equiv 1 \pmod 4,$$

where $h(-p)$ *is the class number of* $\mathbb{Q}(\sqrt{-p})$*.*

First mentioned in a book by Venkov (1937, in Russian). Discovered independently by Chowla.

This completely determines the order mod p of $\left(\frac{p-1}{2}\right)!$.

Now consider the two halves of the product

$$1 \cdot 2 \cdots \frac{p-1}{2} \, \frac{p+1}{2} \cdots (p-1)$$

and denote them, respectively, by

$$\Pi_1^{(2)}, \qquad \Pi_2^{(2)}.$$

Now consider the two halves of the product

$$1 \cdot 2 \cdots \tfrac{p-1}{2} \, \tfrac{p+1}{2} \cdots (p-1)$$

and denote them, respectively, by

$$\Pi_1^{(2)}, \qquad \Pi_2^{(2)}.$$

By Wilson's theorem:

$$\Pi_1^{(2)} \Pi_2^{(2)} \equiv -1 \pmod{p},$$

Now consider the two halves of the product

$$1 \cdot 2 \cdots \tfrac{p-1}{2} \, \tfrac{p+1}{2} \cdots (p-1)$$

and denote them, respectively, by

$$\Pi_1^{(2)}, \qquad \Pi_2^{(2)}.$$

By Wilson's theorem:

$$\Pi_1^{(2)} \Pi_2^{(2)} \equiv -1 \pmod{p},$$

and by symmetry:

$$\Pi_2^{(2)} \equiv (-1)^{\frac{p-1}{2}} \Pi_1^{(2)} \pmod{p}.$$

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

Then

$$\Pi_1^{(3)} = 1{\cdot}2 \cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3} \cdots \tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3} \cdots (p-1).$$

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

Then

$$\Pi_1^{(3)} = 1\cdot 2 \cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3} \cdots \tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3} \cdots (p-1).$$

Once again there is an obvious symmetry:

$$\Pi_3^{(3)} \equiv \Pi_1^{(3)} \pmod p,$$

(without a power of -1 since $\frac{p-1}{3}$ is always even.)

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

Then

$$\Pi_1^{(3)} = 1\cdot 2\cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3}\cdots\tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3}\cdots(p-1).$$

Once again there is an obvious symmetry:

$$\Pi_3^{(3)} \equiv \Pi_1^{(3)} \pmod p,$$

(without a power of -1 since $\frac{p-1}{3}$ is always even.)

No obvious relation between $\Pi_1^{(3)}$ and the “middle third" $\Pi_2^{(3)}$.

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\frac{p-1}{M} + i\right), \qquad (j = 1, 2, \ldots, M).$$

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\tfrac{p-1}{M} + i \right), \qquad (j = 1, 2, \dots, M).$$

Once again, clear that

$$\Pi_{M-j}^{(M)} \equiv \pm \Pi_j^{(M)} \pmod{p}, \qquad j = 1, 2, \dots, \lfloor \tfrac{M-1}{2} \rfloor.$$

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\tfrac{p-1}{M} + i\right), \qquad (j = 1, 2, \ldots, M).$$

Once again, clear that

$$\Pi_{M-j}^{(M)} \equiv \pm \Pi_j^{(M)} \pmod{p}, \qquad j = 1, 2, \ldots, \lfloor \tfrac{M-1}{2} \rfloor.$$

Example:

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	**2**	**−2**	**2**	5	1	2	−2	−1
13	−2	3	−2	13	6	3	−3	−6
19	−2	−5	−2	17	7	−3	−3	7
31	2	−8	2	29	−6	−2	2	6
37	7	3	7	37	−16	5	−5	16
43	−3	19	−3	41	13	7	7	13
61	**−14**	**14**	**−14**	53	26	7	−7	−26
67	−20	−33	−20	61	19	7	−7	−19
73	33	−12	33	73	18	−35	−35	18
79	−37	3	−37	89	22	42	42	22
97	21	−11	21	97	20	−28	−28	20

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	**2**	$-$**2**	**2**	5	1	2	-2	-1
13	-2	3	-2	13	6	3	-3	-6
19	-2	-5	-2	17	7	-3	-3	7
31	2	-8	2	29	-6	-2	2	6
37	7	3	7	37	-16	5	-5	16
43	-3	19	-3	41	13	7	7	13
61	$-$**14**	**14**	$-$**14**	53	26	7	-7	-26
67	-20	-33	-20	61	19	7	-7	-19
73	33	-12	33	73	18	-35	-35	18
79	-37	3	-37	89	22	42	42	22
97	21	-11	21	97	20	-28	-28	20

We observe:

- The obvious symmetries.

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	**2**	**−2**	**2**	5	1	2	−2	−1
13	−2	3	−2	13	6	3	−3	−6
19	−2	−5	−2	17	7	−3	−3	7
31	2	−8	2	29	−6	−2	2	6
37	7	3	7	37	−16	5	−5	16
43	−3	19	−3	41	13	7	7	13
61	**−14**	**14**	**−14**	53	26	7	−7	−26
67	−20	−33	−20	61	19	7	−7	−19
73	33	−12	33	73	18	−35	−35	18
79	−37	3	−37	89	22	42	42	22
97	21	−11	21	97	20	−28	−28	20

We observe:

- The obvious symmetries.
- $\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ for $p = 7$ and $p = 61$.

Are these last cases just coincidences?

Are these last cases just coincidences?

It turns out:

$\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ also for $p = 331$, $p = 547$, $p = 1951$, and further relatively rare primes (explained later).

Are these last cases just coincidences?

It turns out:

$\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ also for $p = 331$, $p = 547$, $p = 1951$, and further relatively rare primes (explained later).

In contrast: No primes p for which

$\Pi_1^{(3)} \equiv \Pi_2^{(3)} \pmod{p}, \qquad p \equiv 1 \pmod{6}$, or

$\Pi_1^{(4)} \equiv \pm\Pi_2^{(4)} \pmod{p}, \qquad p \equiv 1 \pmod{4}$.

Are these last cases just coincidences?

It turns out:

$\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ also for $p = 331$, $p = 547$, $p = 1951$, and further relatively rare primes (explained later).

In contrast: No primes p for which

$$\Pi_1^{(3)} \equiv \Pi_2^{(3)} \pmod{p}, \qquad p \equiv 1 \pmod{6}, \text{ or}$$

$$\Pi_1^{(4)} \equiv \pm\Pi_2^{(4)} \pmod{p}, \qquad p \equiv 1 \pmod{4}.$$

This will be explained later.

2. Composite Moduli

Define the *Gauss factorial* by

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

2. Composite Moduli

Define the *Gauss factorial* by

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

Analogue of Wilson's theorem for composite moduli:

Theorem 2 (Gauss)

For any integer $n \geq 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \textit{for} \quad n = 2, 4, p^\alpha, \textit{ or } 2p^\alpha, \\ 1 \pmod{n} & \textit{otherwise}, \end{cases}$$

where p is an odd prime and α is a positive integer.

2. Composite Moduli

Define the *Gauss factorial* by

$$N_n! = \prod_{\substack{1 \le j \le N \\ \gcd(j,n)=1}} j.$$

Analogue of Wilson's theorem for composite moduli:

Theorem 2 (Gauss)

For any integer $n \geq 2$ we have

$$(n-1)_n! \equiv \begin{cases} -1 \pmod{n} & \textit{for} \quad n = 2, 4, p^\alpha, \textit{ or } 2p^\alpha, \\ 1 \pmod{n} & \textit{otherwise}, \end{cases}$$

where p is an odd prime and α is a positive integer.

The first case indicates exactly those n that have primitive roots.

Everything we did before can be extended to composite moduli.

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products:

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products: For $n \equiv 1 \pmod{M}$, set

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \qquad (j = 1, 2, \ldots, M),$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\tfrac{n-1}{M} + 1 \leq i \leq j\tfrac{n-1}{M},\ \gcd(i, n) = 1 \right\}.$$

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products: For $n \equiv 1 \pmod{M}$, set

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \qquad (j = 1, 2, \ldots, M),$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\frac{n-1}{M} + 1 \leq i \leq j\frac{n-1}{M},\ \gcd(i, n) = 1 \right\}.$$

- Dependence on n is implied in the notation;

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products: For $n \equiv 1 \pmod{M}$, set

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \qquad (j = 1, 2, \ldots, M),$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\tfrac{n-1}{M} + 1 \leq i \leq j\tfrac{n-1}{M},\ \gcd(i, n) = 1 \right\}.$$

- Dependence on n is implied in the notation;
- When $n = p$: reduces to previous case.

Example:

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	−7	−19
73	33	−12	33	65	**8**	**8**	**8**	**8**
76	−29	−15	−29	69	31	−26	−26	31
79	−37	3	−37	73	18	−35	−35	18
82	−33	−25	−33	77	16	31	31	16
85	−28	9	−28	81	2	40	−40	2
88	5	−7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	−23	43	−23	93	34	−10	−10	34
97	21	−11	21	97	20	−28	−28	20

Example:

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	-7	-19
73	33	-12	33	65	**8**	**8**	**8**	**8**
76	-29	-15	-29	69	31	-26	-26	31
79	-37	3	-37	73	18	-35	-35	18
82	-33	-25	-33	77	16	31	31	16
85	-28	9	-28	81	2	40	-40	2
88	5	-7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	-23	43	-23	93	34	-10	-10	34
97	21	-11	21	97	20	-28	-28	20

We see: In contrast to prime case, it *can* happen that all partial products are congruent to each other.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \#I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \#I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \#I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.
- When $M = 2$, then $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.
- When $M = 2$, then $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

In general, the situation is less straightforward.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.
- When $M = 2$, then $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

In general, the situation is less straightforward.
E.g., for $n = 4$:
$\phi_{3,1}(n) = \phi_{3,3}(n) = 1$, but $\phi_{3,2}(n) = 0$.

When do we have equal distribution?

When do we have equal distribution?

Theorem 3 (Lehmer, 1955)

Let $M \geq 2$ *and* $n \equiv 1 \pmod{M}$.
If n *has at least one prime factor* $p \equiv 1 \pmod{M}$, *then*

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \qquad (j = 1, 2, \ldots, M).$$

When do we have equal distribution?

Theorem 3 (Lehmer, 1955)

Let $M \geq 2$ *and* $n \equiv 1 \pmod{M}$.
If n *has at least one prime factor* $p \equiv 1 \pmod{M}$, *then*

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \qquad (j = 1, 2, \ldots, M).$$

Note: Condition is sufficient, but not necessary.

When do we have equal distribution?

Theorem 3 (Lehmer, 1955)

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least one prime factor $p \equiv 1 \pmod{M}$, then

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \qquad (j = 1, 2, \ldots, M).$$

Note: Condition is sufficient, but not necessary.

E.g., $M = 8$ and $n = 105 = 3 \cdot 5 \cdot 7$.
None of the prime factors are $\equiv 1 \pmod{8}$, but
$\phi_{M,j}(n) = \frac{1}{8}\phi(105) = 6$ for $j = 1, \ldots, 8$.

4. When Are the Partial Products Congruent?

Return to our table:

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	-7	-19
73	33	-12	33	65	**8**	**8**	**8**	**8**
76	-29	-15	-29	69	31	-26	-26	31
79	-37	3	-37	73	18	-35	-35	18
82	-33	-25	-33	77	16	31	31	16
85	-28	9	-28	81	2	40	-40	2
88	5	-7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	-23	43	-23	93	34	-10	-10	34
97	21	-11	21	97	20	-28	-28	20

Note:

$91 = 7 \cdot 13, \quad 65 = 5 \cdot 13, \quad 85 = 5 \cdot 17.$

This observation holds in general:

This observation holds in general:

Theorem 4

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv \left(\tfrac{n-1}{M}\right)_n! \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

This observation holds in general:

Theorem 4

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv \left(\tfrac{n-1}{M}\right)_n! \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

Result is best possible:
E.g., $M = 3$ and $n = 70 = 2 \cdot 5 \cdot 7$.
• Only one factor $\equiv 1 \pmod{3}$,
• $\Pi_1^{(3)} \equiv 29 \pmod{70}, \Pi_2^{(3)} \equiv 1 \pmod{70}$.

This observation holds in general:

Theorem 4

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv \left(\tfrac{n-1}{M}\right)_n! \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

Result is best possible:
E.g., $M = 3$ and $n = 70 = 2 \cdot 5 \cdot 7$.
- Only one factor $\equiv 1 \pmod{3}$,
- $\Pi_1^{(3)} \equiv 29 \pmod{70}, \Pi_2^{(3)} \equiv 1 \pmod{70}$.

On the other hand, condition is sufficient but not necessary.
E.g., $M = 3$ and $n = 2^2 \cdot 61$; statement still holds.

Proof is based on an observation:

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \qquad j = 1, 2, \ldots, M,$$

Proof is based on an observation:

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \qquad j = 1, 2, \ldots, M,$$

and a lemma:

Lemma 5

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$, $n = p^\alpha q^\beta w$ for distinct prime $p, q \equiv 1 \pmod{M}$, $\alpha, \beta \geq 1$, and $\gcd(pq, w) = 1$. Then for $j = 1, 2, \ldots, M$,

$$\left(j\frac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^{j\frac{p-1}{M}}}{p^{jA}} \pmod{q^\beta w}, \qquad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w),$$

where $\varepsilon = -1$ if $w = 1$, and $\varepsilon = 1$ if $w > 1$.

Proof is based on an observation:

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \qquad j = 1, 2, \ldots, M,$$

and a lemma:

Lemma 5

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$, $n = p^\alpha q^\beta w$ for distinct prime $p, q \equiv 1 \pmod{M}$, $\alpha, \beta \geq 1$, and $\gcd(pq, w) = 1$. Then for $j = 1, 2, \ldots, M$,

$$\left(j\frac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^{j\frac{p-1}{M}}}{p^{jA}} \pmod{q^\beta w}, \qquad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w),$$

where $\varepsilon = -1$ if $w = 1$, and $\varepsilon = 1$ if $w > 1$.

To prove the Theorem, use this and the Chinese Remainder Theorem; dependence on j disappears.

Idea of proof:

Idea of proof:

Break the range of the product in $\left(j\frac{n-1}{M}\right)_n!$ into
• a number of products of approximately equal length,
• a shorter “tail."

Idea of proof:

Break the range of the product in $\left(j\frac{n-1}{M}\right)_n!$ into
- a number of products of approximately equal length,
- a shorter “tail."

Then evaluate the products of the first type using the Gauss-Wilson theorem $\pmod{q^\beta w}$.

Idea of proof:

Break the range of the product in $\left(j\frac{n-1}{M}\right)_n!$ into
• a number of products of approximately equal length,
• a shorter “tail."

Then evaluate the products of the first type using the Gauss-Wilson theorem $\pmod{q^\beta w}$.

Carefully count which elements to include/exclude.

5. Some Consequences

1. We saw:
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the $\Pi_j^{(M)}$ are congruent to each other.

5. Some Consequences

1. We saw:
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the $\Pi_j^{(M)}$ are congruent to each other.

Since their product is $(n-1)_n!$, we have by Gauss-Wilson,

$$\left(\tfrac{n-1}{M}\right)_n!^M \equiv 1 \pmod{n}.$$

5. Some Consequences

1. We saw:
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the $\Pi_j^{(M)}$ are congruent to each other.

Since their product is $(n-1)_n!$, we have by Gauss-Wilson,

$$\left(\tfrac{n-1}{M}\right)_n!^M \equiv 1 \pmod{n}.$$

This implies:

Corollary 6

*Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the multiplicative order of $(\frac{n-1}{M})_n!$ modulo n is a divisor of M.*

2. In the case of at least *three* distinct prime factors $\equiv 1 \pmod{M}$ we can say more:

2. In the case of at least *three* distinct prime factors $\equiv 1 \pmod{M}$ we can say more:

Theorem 7

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least three distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv 1 \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

2. In the case of at least *three* distinct prime factors $\equiv 1 \pmod{M}$ we can say more:

Theorem 7

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least three distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv 1 \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

Method of proof is similar to that of the previous lemma.

Summary:

# of prime factors $\equiv 1 \pmod{M}$	All $\Pi_1^{(M)}, \ldots, \Pi_M^{(M)}$:
1	have the same number of factors
2	are congruent to each other $\pmod{M}$
3	are congruent to $1 \pmod{M}$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod{4}$.

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}}$$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2}$$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2}$$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod{4}$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}.$$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}.$$

There exists a celebrated congruence for this binomial coefficient:

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Theorem 8 (Gauss, 1828)

Let p and a be as above. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Theorem 8 (Gauss, 1828)

Let p and a be as above. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

As an easy application we get

$$\Pi_2^{(4)} \not\equiv \pm\Pi_1^{(4)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 4.$$

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Theorem 8 (Gauss, 1828)

Let p and a be as above. Then

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod p.$$

As an easy application we get

$$\Pi_2^{(4)} \not\equiv \pm\Pi_1^{(4)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 4.$$

A similar theorem, due to Jacobi (1837), implies that

$$\Pi_2^{(3)} \not\equiv \Pi_1^{(3)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 6.$$

A number of further consequences can be derived from these classical theorems.

A number of further consequences can be derived from these classical theorems. Two samples:

Corollary 9

For a prime $p \equiv 1 \pmod{6}$ *we have*

$$\Pi_2^{(3)} \equiv -\Pi_1^{(3)} \pmod{p} \quad \Leftrightarrow \quad p = 27x^2 + 27x + 7, x \in \mathbb{Z}.$$

A number of further consequences can be derived from these classical theorems. Two samples:

Corollary 9

For a prime $p \equiv 1 \pmod{6}$ *we have*

$$\Pi_2^{(3)} \equiv -\Pi_1^{(3)} \pmod{p} \quad \Leftrightarrow \quad p = 27x^2 + 27x + 7, x \in \mathbb{Z}.$$

The first such primes are 7, 61 (seen earlier), 331, 547, 1951.

Corollary 10

Let $p \equiv 1 \pmod{4}$*. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod{p}$ *only if* $p = 5$*.*

Corollary 10

Let $p \equiv 1 \pmod 4$*. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$*.*

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$*.*

Corollary 10

Let $p \equiv 1 \pmod 4$. *Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *holds for* $p = 17, 241, 3361, 46817, 652081, \ldots$

Corollary 10

Let $p \equiv 1 \pmod 4$*. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$*.*

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$*.*

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *holds for* $p = 17, 241, 3361, 46817, 652081, \ldots$

Part (c) is related to the solution of a certain Pell equation.

7. Brief Pause: Summary and Outlook

General long-term program: To study the Gauss factorials

$$\left(\frac{n-1}{M}\right)_n!, \quad M \geq 1, \quad n \equiv 1 \pmod{M},$$

7. Brief Pause: Summary and Outlook

General long-term program: To study the Gauss factorials

$$\left(\frac{n-1}{M}\right)_n!, \quad M \geq 1, \quad n \equiv 1 \pmod{M},$$

in particular their multiplicative orders (mod n),

7. Brief Pause: Summary and Outlook

General long-term program: To study the Gauss factorials

$$\left(\frac{n-1}{M}\right)_n!, \quad M \geq 1, \quad n \equiv 1 \pmod{M},$$

in particular their multiplicative orders (mod n),
but also, if possible, their values (mod n).

7. Brief Pause: Summary and Outlook

General long-term program: To study the Gauss factorials

$$\left(\frac{n-1}{M}\right)_n!, \quad M \geq 1, \quad n \equiv 1 \pmod{M},$$

in particular their multiplicative orders (mod n),
but also, if possible, their values (mod n).

We saw in the first half of this talk:

- $M = 1$: Gauss-Wilson theorem.

7. Brief Pause: Summary and Outlook

General long-term program: To study the Gauss factorials

$$\left(\frac{n-1}{M}\right)_n!, \quad M \geq 1, \quad n \equiv 1 \pmod{M},$$

in particular their multiplicative orders (mod n),
but also, if possible, their values (mod n).

We saw in the first half of this talk:

- $M = 1$: Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
  Only possible orders are 1, 2, and 4.

- $M \geq 3$: Orders are unbounded.
  Various partial results; e.g.,

- $M \geq 3$: Orders are unbounded.
  Various partial results; e.g.,
  - If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then $(\frac{n-1}{M})_n! \equiv 1 \pmod{n}$;

- $M \geq 3$: Orders are unbounded.
  Various partial results; e.g.,

  – If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$,
    then $(\frac{n-1}{M})_n! \equiv 1 \pmod{n}$;

  – If n has **two** different prime factors $\equiv 1 \pmod{M}$,
    then the order of $(\frac{n-1}{M})_n!$ is a divisor of M.

- $M \geq 3$: Orders are unbounded.
  Various partial results; e.g.,

  – If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then $(\frac{n-1}{M})_n! \equiv 1 \pmod{n}$;

  – If n has **two** different prime factors $\equiv 1 \pmod{M}$, then the order of $(\frac{n-1}{M})_n!$ is a divisor of M.

  – If n has **one** prime factor $\equiv 1 \pmod{M}$:
  Most interesting case.
  Remainder of this talk will be about a specific aspect.

- $M \geq 3$: Orders are unbounded.
  Various partial results; e.g.,
  - If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then $(\frac{n-1}{M})_n! \equiv 1 \pmod{n}$;
  - If n has **two** different prime factors $\equiv 1 \pmod{M}$, then the order of $(\frac{n-1}{M})_n!$ is a divisor of M.
  - If n has **one** prime factor $\equiv 1 \pmod{M}$:
    Most interesting case.
    Remainder of this talk will be about a specific aspect.
  - If n has **no** prime factor $\equiv 1 \pmod{M}$:
    Next to nothing is known.

8. The case $n = p^\alpha$, $p \equiv 1 \pmod{M}$

This case is of particular interest, one reason being:

Let $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ with $a \equiv 1 \pmod 4$. (a is then uniquely determined).

8. The case $n = p^\alpha$, $p \equiv 1 \pmod{M}$

This case is of particular interest, one reason being:

Let $p \equiv 1 \pmod 4$, and write $p = a^2 + b^2$ with $a \equiv 1 \pmod 4$. (a is then uniquely determined).

Theorem 11 (JBC & KD, 2010)

With p and a as above and $\alpha \geq 2$, we have

$$\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \equiv 2a - 1\cdot\frac{p}{2a} - 1\cdot\frac{p^2}{8a^3} - 2\cdot\frac{p^3}{(2a)^5} - 5\cdot\frac{p^4}{(2a)^7}$$
$$-14\cdot\frac{p^5}{(2a)^9} - \ldots - C_{\alpha-2}\frac{p^{\alpha-1}}{(2a)^{2\alpha-1}} \pmod{p^\alpha}.$$

$C_n := \frac{1}{n+1}\binom{2n}{n} \in \mathbb{N}$ is the nth Catalan number.

This extends Gauss's binomial coefficient theorem:
With p and a as above,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.$$

This extends Gauss's binomial coefficient theorem:
With p and a as above,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.$$

There are similar theorems, due to Jacobi (1837), Hudson and Williams (1984), and others.

This extends Gauss's binomial coefficient theorem:
With p and a as above,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.$$

There are similar theorems, due to Jacobi (1837), Hudson and Williams (1984), and others.

These too have "Catalan analogues" (JBC & KD, 2010; JBC & KD (preprint); Al-Shaghay, 2014).

Our main objects of study here:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

$$\gamma_\alpha^M(p) := \mathrm{ord}_{p^\alpha}\left(\left(\frac{p^\alpha - 1}{M}\right)_{p^\alpha}!\right).$$

Our main objects of study here:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

$$\gamma_\alpha^M(p) := \operatorname{ord}_{p^\alpha}\left(\left(\frac{p^\alpha-1}{M}\right)_{p^\alpha}!\right).$$

In what follows: Fix M and p; let α vary.

Our main objects of study here:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

$$\gamma_\alpha^M(p) := \mathrm{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}!\right).$$

In what follows: Fix M and p; let α vary.

What can we say about the sequence

$$\{\gamma_\alpha^M(p)\}_{\alpha\geq 1}?$$

Our main objects of study here:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

$$\gamma_\alpha^M(p) := \mathrm{ord}_{p^\alpha}\left(\left(\frac{p^\alpha-1}{M}\right)_{p^\alpha}!\right).$$

In what follows: Fix M and p; let α vary.

What can we say about the sequence

$$\{\gamma_\alpha^M(p)\}_{\alpha\geq 1}?$$

Note:

$$\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}! = \left(\tfrac{p^\alpha-1}{M}\right)_p!;$$

We can therefore replace the subscript p^α by p.

Our main objects of study here:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

$$\gamma_\alpha^M(p) := \operatorname{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}!\right).$$

In what follows: Fix M and p; let α vary.

What can we say about the sequence

$$\{\gamma_\alpha^M(p)\}_{\alpha\geq 1}?$$

Note:

$$\left(\tfrac{p^\alpha-1}{M}\right)_{p^\alpha}! = \left(\tfrac{p^\alpha-1}{M}\right)_p!;$$

We can therefore replace the subscript p^α by p.

Let's look at some examples with $M = 4$:

α/p	5	13	17	29	37
1	1	12	16	7	18
2	10	156	272	406	333
3	25	2 028	4 624	5 887	24 642
4	250	26 364	78 608	341 446	455 877
5	625	342 732	1 336 336	4 950 967	33 734 898

α/p	5	13	17	29	37
1	1	12	16	7	18
2	10	156	272	406	333
3	25	2 028	4 624	5 887	24 642
4	250	26 364	78 608	341 446	455 877
5	625	342 732	1 336 336	4 950 967	33 734 898
1	γ	γ	γ	γ	γ
2	$2p\gamma$	$p\gamma$	$p\gamma$	$2p\gamma$	$\frac{1}{2}p\gamma$
3	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$
4	$2p^3\gamma$	$p^3\gamma$	$p^3\gamma$	$2p^3\gamma$	$\frac{1}{2}p^3\gamma$
5	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$

Table 1: $\gamma := \gamma_1^4(p), \; p \equiv 1 \pmod 4$.

α/p	5	13	17	29	37
1	1	12	16	7	18
2	10	156	272	406	333
3	25	2 028	4 624	5 887	24 642
4	250	26 364	78 608	341 446	455 877
5	625	342 732	1 336 336	4 950 967	33 734 898
1	γ	γ	γ	γ	γ
2	$2p\gamma$	$p\gamma$	$p\gamma$	$2p\gamma$	$\frac{1}{2}p\gamma$
3	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$
4	$2p^3\gamma$	$p^3\gamma$	$p^3\gamma$	$2p^3\gamma$	$\frac{1}{2}p^3\gamma$
5	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$

Table 1: $\gamma := \gamma_1^4(p),\ p \equiv 1 \pmod 4$.

Note the 3 different patterns; otherwise regular.

α/p	5	13	17	29	37
1	1	12	16	7	18
2	10	156	272	406	333
3	25	2 028	4 624	5 887	24 642
4	250	26 364	78 608	341 446	455 877
5	625	342 732	1 336 336	4 950 967	33 734 898
1	γ	γ	γ	γ	γ
2	$2p\gamma$	$p\gamma$	$p\gamma$	$2p\gamma$	$\frac{1}{2}p\gamma$
3	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$
4	$2p^3\gamma$	$p^3\gamma$	$p^3\gamma$	$2p^3\gamma$	$\frac{1}{2}p^3\gamma$
5	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$

Table 1: $\gamma := \gamma_1^4(p),\ p \equiv 1 \pmod 4$.

Note the 3 different patterns; otherwise regular.

- Are there more patterns?

α/p	5	13	17	29	37
1	1	12	16	7	18
2	10	156	272	406	333
3	25	2 028	4 624	5 887	24 642
4	250	26 364	78 608	341 446	455 877
5	625	342 732	1 336 336	4 950 967	33 734 898
1	γ	γ	γ	γ	γ
2	$2p\gamma$	$p\gamma$	$p\gamma$	$2p\gamma$	$\frac{1}{2}p\gamma$
3	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$	$p^2\gamma$
4	$2p^3\gamma$	$p^3\gamma$	$p^3\gamma$	$2p^3\gamma$	$\frac{1}{2}p^3\gamma$
5	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$	$p^4\gamma$

Table 1: $\gamma := \gamma_1^4(p)$, $p \equiv 1 \pmod 4$.

Note the 3 different patterns; otherwise regular.

- Are there more patterns?
- Do we always have $1, p, p^2, p^3, \ldots$?

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \dots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \dots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

However, for $p = 29\,789$: $\gamma_1^4 = 14\,894$, **but** $\gamma_2^4 = 7\,447$.

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \dots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \dots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \dots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

However, for $p = 29\,789$: $\gamma_1^4 = 14\,894$, **but** $\gamma_2^4 = 7\,447$.
The sequence “forgot" the factor p in the step $\gamma_1^4 \to \gamma_2^4$.

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

However, for $p = 29\,789$: $\gamma_1^4 = 14\,894$, **but** $\gamma_2^4 = 7\,447$.
The sequence “forgot" the factor p in the step $\gamma_1^4 \to \gamma_2^4$.

The rest of this talk will be about such “exceptional primes":

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

However, for $p = 29\,789$: $\gamma_1^4 = 14\,894$, **but** $\gamma_2^4 = 7\,447$.
The sequence “forgot" the factor p in the step $\gamma_1^4 \to \gamma_2^4$.

The rest of this talk will be about such “exceptional primes":

- Are there more?

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

However, for $p = 29\,789$: $\gamma_1^4 = 14\,894$, **but** $\gamma_2^4 = 7\,447$.
The sequence “forgot" the factor p in the step $\gamma_1^4 \to \gamma_2^4$.

The rest of this talk will be about such “exceptional primes":

- Are there more?
- Can we characterize them? Compute them?

One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

$$\begin{cases} \gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod 8 \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } 4|\gamma, \\ \gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \equiv 2 \pmod 4, \\ \gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod 8 \text{ and } \gamma \text{ is odd.} \end{cases}$$

Computations seem to support this.

However, for $p = 29\,789$: $\gamma_1^4 = 14\,894$, **but** $\gamma_2^4 = 7\,447$.
The sequence "forgot" the factor p in the step $\gamma_1^4 \to \gamma_2^4$.

The rest of this talk will be about such "exceptional primes":

- Are there more?
- Can we characterize them? Compute them?
- Can the "skipped p" occur elsewhere in the sequence?

Theorem 12 (JBC & KD, 2011)

Let $M \geq 2$, $p \equiv 1 \pmod{M}$ *and* $\gamma_\alpha^M(p)$ *as above.*
When $p \equiv 1 \pmod{2M}$, *then*

$$\gamma_{\alpha+1}^M(p) = p\gamma_\alpha^M(p) \quad \textit{or} \quad \gamma_{\alpha+1}^M(p) = \gamma_\alpha^M(p).$$

Theorem 12 (JBC & KD, 2011)

Let $M \geq 2$, $p \equiv 1 \pmod{M}$ *and* $\gamma_\alpha^M(p)$ *as above.*
When $p \equiv 1 \pmod{2M}$, *then*

$$\gamma_{\alpha+1}^M(p) = p\gamma_\alpha^M(p) \quad \text{or} \quad \gamma_{\alpha+1}^M(p) = \gamma_\alpha^M(p).$$

When $p \equiv M+1 \pmod{2M}$, *then*

$$\gamma_{\alpha+1}^M(p) = \begin{cases} p\gamma_\alpha^M(p) \quad \text{or} \quad \gamma_\alpha^M(p) & \text{if} \quad \gamma_\alpha^M(p) \equiv 0 \pmod{4}, \\ \frac{1}{2}p\gamma_\alpha^M(p) \quad \text{or} \quad \frac{1}{2}\gamma_\alpha^M(p) & \text{if} \quad \gamma_\alpha^M(p) \equiv 2 \pmod{4}, \\ 2p\gamma_\alpha^M(p) \quad \text{or} \quad 2\gamma_\alpha^M(p) & \text{if} \quad \gamma_\alpha^M(p) \equiv 1 \pmod{2}. \end{cases}$$

Theorem 12 (JBC & KD, 2011)

Let $M \geq 2$, $p \equiv 1 \pmod{M}$ *and* $\gamma_\alpha^M(p)$ *as above.*
When $p \equiv 1 \pmod{2M}$, *then*

$$\gamma_{\alpha+1}^M(p) = p\gamma_\alpha^M(p) \quad \text{or} \quad \gamma_{\alpha+1}^M(p) = \gamma_\alpha^M(p).$$

When $p \equiv M+1 \pmod{2M}$, *then*

$$\gamma_{\alpha+1}^M(p) = \begin{cases} p\gamma_\alpha^M(p) \quad \text{or} \quad \gamma_\alpha^M(p) & \text{if} \quad \gamma_\alpha^M(p) \equiv 0 \pmod{4}, \\ \frac{1}{2}p\gamma_\alpha^M(p) \quad \text{or} \quad \frac{1}{2}\gamma_\alpha^M(p) & \text{if} \quad \gamma_\alpha^M(p) \equiv 2 \pmod{4}, \\ 2p\gamma_\alpha^M(p) \quad \text{or} \quad 2\gamma_\alpha^M(p) & \text{if} \quad \gamma_\alpha^M(p) \equiv 1 \pmod{2}. \end{cases}$$

When the second alternative holds in one of the cases, we call p an α-**exceptional prime** for M.

How often does this happen?

How often does this happen?

M	p	up to
3	13, 181, 2 521, 76 543, 489 061	10^{12}
4	29 789	10^{11}
5	71	$2 \cdot 10^6$
6	13, 181, 2 521, 76 543, 489 061	10^{12}
10	11	$2 \cdot 10^6$
18	1 090 891	$2 \cdot 10^6$
21	211, 15 583	$2 \cdot 10^6$
23	3 037	$2 \cdot 10^6$
24	73	$2 \cdot 10^6$
29	59	$2 \cdot 10^6$
35	1 471	$2 \cdot 10^6$
44	617	$2 \cdot 10^6$
48	97	$2 \cdot 10^6$

Table 2: 1-exceptional primes p for $3 \leq M \leq 100$.

9. Exceptional Primes

For a first criterion for exceptionality, we need some definitions:

9. Exceptional Primes

For a first criterion for exceptionality, we need some definitions:

1. For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)! + 1}{p}.$$

9. Exceptional Primes

For a first criterion for exceptionality, we need some definitions:

1. For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)! + 1}{p}.$$

Always an integer (by Wilson's theorem).

9. Exceptional Primes

For a first criterion for exceptionality, we need some definitions:

1. For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)!+1}{p}.$$

Always an integer (by Wilson's theorem).

2. For $M \geq 2$ and $p \equiv 1 \pmod{M}$, define

$$S^M(p) := \sum_{j=1}^{\frac{p-1}{M}} \frac{1}{j}.$$

9. Exceptional Primes

For a first criterion for exceptionality, we need some definitions:

1. For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)!+1}{p}.$$

Always an integer (by Wilson's theorem).

2. For $M \geq 2$ and $p \equiv 1 \pmod{M}$, define

$$S^M(p) := \sum_{j=1}^{\frac{p-1}{M}} \frac{1}{j}.$$

For $M = 2, 3, 4$ and 6 there are well-known evaluations in terms of the Fermat quotient $q_p(a) := (a^{p-1}-1)/p$;

9. Exceptional Primes

For a first criterion for exceptionality, we need some definitions:

1. For any prime p, the *Wilson quotient* is defined by

$$w(p) := \frac{(p-1)!+1}{p}.$$

Always an integer (by Wilson's theorem).

2. For $M \geq 2$ and $p \equiv 1 \pmod{M}$, define

$$S^M(p) := \sum_{j=1}^{\frac{p-1}{M}} \frac{1}{j}.$$

For $M = 2, 3, 4$ and 6 there are well-known evaluations in terms of the Fermat quotient $q_p(a) := (a^{p-1}-1)/p$; e.g.,

$$\sum_{j=1}^{\frac{p-1}{4}} \frac{1}{j} \equiv -3q_p(2) \pmod{p}, \qquad \sum_{j=1}^{\frac{p-1}{3}} \frac{1}{j} \equiv -\tfrac{3}{2}q_p(3) \pmod{p}.$$

3. For $\alpha \geq 1$, $M \geq 2$ and $p \equiv 1 \pmod{M}$ we define $V_\alpha^M(p)$ by

$$\left(\left(\frac{p^\alpha - 1}{M}\right)_p!\right)^{\gamma_\alpha^M(p)} \equiv 1 + V_\alpha^M(p)p^\alpha \pmod{p^{\alpha+1}}.$$

3. For $\alpha \geq 1$, $M \geq 2$ and $p \equiv 1 \pmod{M}$ we define $V_\alpha^M(p)$ by

$$\left(\left(\frac{p^\alpha - 1}{M}\right)_p !\right)^{\gamma_\alpha^M(p)} \equiv 1 + V_\alpha^M(p) p^\alpha \pmod{p^{\alpha+1}}.$$

Theorem 13 (JBC & KD, 2011)

The first alternative in each case of Theorem 4 holds iff

$$V_\alpha^M(p) + \tfrac{1}{M}\gamma_\alpha^M(p)\left(w(p) - S^M(p)\right) \not\equiv 0 \pmod{p}.$$

3. For $\alpha \geq 1$, $M \geq 2$ and $p \equiv 1 \pmod{M}$ we define $V_\alpha^M(p)$ by

$$\left(\left(\frac{p^\alpha-1}{M}\right)_p!\right)^{\gamma_\alpha^M(p)} \equiv 1 + V_\alpha^M(p)p^\alpha \pmod{p^{\alpha+1}}.$$

Theorem 13 (JBC & KD, 2011)

The first alternative in each case of Theorem 4 holds iff

$$V_\alpha^M(p) + \tfrac{1}{M}\gamma_\alpha^M(p)\left(w(p) - S^M(p)\right) \not\equiv 0 \pmod{p}.$$

Idea of proof of Theorems 4 and 5:

- Establish a congruence connecting

$$\left(\frac{p^{\alpha+1}-1}{M}\right)_p! \quad \text{and} \left(\frac{p^\alpha-1}{M}\right)_p! \pmod{p^{\alpha+1}}.$$

- Raise both sides to an appropriate power.
- Use definition of order.

All entries in Table 2 were found with this last criterion.

M	p	up to
3	13, 181, 2 521, 76 543, 489 061	10^{12}
4	29 789	10^{11}
5	71	$2 \cdot 10^6$
6	13, 181, 2 521, 76 543, 489 061	10^{12}
10	11	$2 \cdot 10^6$
18	1 090 891	$2 \cdot 10^6$
21	211, 15 583	$2 \cdot 10^6$
23	3 037	$2 \cdot 10^6$
24	73	$2 \cdot 10^6$
29	59	$2 \cdot 10^6$
35	1 471	$2 \cdot 10^6$
44	617	$2 \cdot 10^6$
48	97	$2 \cdot 10^6$

Table 2: 1-exceptional primes p for $3 \leq M \leq 100$.

All entries in Table 2 were found with this last criterion.

However, it is awkward and computationally expensive.
Can we do better?

All entries in Table 2 were found with this last criterion.

However, it is awkward and computationally expensive.
Can we do better?

In the cases $M = 3, 4$ and 6 we can use the theory of Jacobi sums to obtain some strong criteria, in addition to further insight.

All entries in Table 2 were found with this last criterion.

However, it is awkward and computationally expensive.
Can we do better?

In the cases $M = 3, 4$ and 6 we can use the theory of Jacobi sums to obtain some strong criteria, in addition to further insight.

Here: Consider $M = 3, 6$; $M = 4$ is similar.

All entries in Table 2 were found with this last criterion.

However, it is awkward and computationally expensive.
Can we do better?

In the cases $M = 3, 4$ and 6 we can use the theory of Jacobi sums to obtain some strong criteria, in addition to further insight.

Here: Consider $M = 3, 6$; $M = 4$ is similar.

But also, as we saw: $M = 3, 6$ are connected in some special ways.

10. Some Fundamental Congruences for $M = 3, 6$

Let $p \equiv 1 \pmod 6$ be a prime.

Known: The representation $p = a^2 + 3b^2$ is unique up to sign,

10. Some Fundamental Congruences for $M = 3, 6$

Let $p \equiv 1 \pmod{6}$ be a prime.

Known: The representation $p = a^2 + 3b^2$ is unique up to sign, but the signs are crucial here. We fix them as follows:

10. Some Fundamental Congruences for $M = 3, 6$

Let $p \equiv 1 \pmod 6$ be a prime.

Known: The representation $p = a^2 + 3b^2$ is unique up to sign, but the signs are crucial here. We fix them as follows:

Let

- g be a primitive root modulo p,

10. Some Fundamental Congruences for $M = 3, 6$

Let $p \equiv 1 \pmod{6}$ be a prime.

Known: The representation $p = a^2 + 3b^2$ is unique up to sign, but the signs are crucial here. We fix them as follows:

Let

- g be a primitive root modulo p,
- χ_6 a character modulo p of order 6 with $\chi_6(g) = e^{2\pi i/6} = (1 + i\sqrt{3})/2$.

10. Some Fundamental Congruences for $M = 3, 6$

Let $p \equiv 1 \pmod 6$ be a prime.

Known: The representation $p = a^2 + 3b^2$ is unique up to sign, but the signs are crucial here. We fix them as follows:

Let

- g be a primitive root modulo p,
- χ_6 a character modulo p of order 6 with $\chi_6(g) = e^{2\pi i/6} = (1 + i\sqrt{3})/2$.

Then we fix the signs of a and b by the congruences

$$a \equiv -1 \pmod 3 \qquad \text{and} \qquad 3b \equiv (2g^{(p-1)/3} + 1)a \pmod p.$$

With a and b as above, we define two closely related pairs r, s and u, v (in this talk only r and u):

With a and b as above, we define two closely related pairs r, s and u, v (in this talk only r and u):

Let $Z = \text{ind}_g 2$, the index of $2 \pmod{p}$ with respect to g.

With a and b as above, we define two closely related pairs r, s and u, v (in this talk only r and u):

Let $Z = \mathrm{ind}_g 2$, the index of $2 \pmod{p}$ with respect to g. Then

$$\begin{aligned} r &= 2a, & u &= 2a & (Z &\equiv 0 \pmod{3}), \\ r &= -a - 3b, & u &= -a + 3b & (Z &\equiv 1 \pmod{3}), \\ r &= -a + 3b, & u &= -a - 3b & (Z &\equiv 2 \pmod{3}). \end{aligned}$$

With a and b as above, we define two closely related pairs r, s and u, v (in this talk only r and u):

Let $Z = \text{ind}_g 2$, the index of $2 \pmod p$ with respect to g. Then

$$\begin{aligned} r &= 2a, & u &= 2a & (Z &\equiv 0 \pmod 3), \\ r &= -a-3b, & u &= -a+3b & (Z &\equiv 1 \pmod 3), \\ r &= -a+3b, & u &= -a-3b & (Z &\equiv 2 \pmod 3). \end{aligned}$$

They also satisfy sums-of-squares identities:

$$4p = r^2 + 3s^2, \qquad 4p = u^2 + 3v^2, \qquad r \equiv u \equiv 1 \pmod 3$$

With a and b as above, we define two closely related pairs r, s and u, v (in this talk only r and u):

Let $Z = \text{ind}_g 2$, the index of $2 \pmod{p}$ with respect to g. Then

$$\begin{array}{lll} r = 2a, & u = 2a & (Z \equiv 0 \pmod{3}), \\ r = -a - 3b, & u = -a + 3b & (Z \equiv 1 \pmod{3}), \\ r = -a + 3b, & u = -a - 3b & (Z \equiv 2 \pmod{3}). \end{array}$$

They also satisfy sums-of-squares identities:

$$4p = r^2 + 3s^2, \qquad 4p = u^2 + 3v^2, \qquad r \equiv u \equiv 1 \pmod{3}$$

The following fundamental result will be the basis for all that follows.

Theorem 14

Let $p \equiv 1 \pmod 6$ *and* r, u *as above.*
Then for all $\alpha \geq 1$ *we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^{\alpha}}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^{\alpha}}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}},$$

where C_n *is the nth Catalan number.*

Theorem 14

Let $p \equiv 1 \pmod 6$ *and* r, u *as above.*
Then for all $\alpha \geq 1$ *we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^\alpha}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^\alpha}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}},$$

where C_n *is the nth Catalan number.*

Main ingredients in proof:

- An identity between the third powers of certain Jacobi sums;

Theorem 14

Let $p \equiv 1 \pmod 6$ *and* r, u *as above.*
Then for all $\alpha \geq 1$ *we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^{\alpha}}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^{\alpha}}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}},$$

where C_n *is the nth Catalan number.*

Main ingredients in proof:

- An identity between the third powers of certain Jacobi sums;
- congruences $(\bmod\ p^{\alpha+1})$ between these Jacobi sums and both sides in Theorem 6;

Theorem 14

Let $p \equiv 1 \pmod 6$ *and* r, u *as above.*
Then for all $\alpha \geq 1$ *we have*

$$\left(r - \frac{p}{r} - \cdots - \frac{C_{\alpha-1}p^{\alpha}}{r^{2\alpha-1}}\right)^3 \equiv \left(u - \frac{p}{u} - \cdots - \frac{C_{\alpha-1}p^{\alpha}}{u^{2\alpha-1}}\right)^3 \pmod{p^{\alpha+1}},$$

where C_n *is the nth Catalan number.*

Main ingredients in proof:

- An identity between the third powers of certain Jacobi sums;
- congruences (mod $p^{\alpha+1}$) between these Jacobi sums and both sides in Theorem 6;
- quotients of certain Gauss factorials are involved as intermediate steps.

Corollary 15

For any $p \equiv 1 \pmod{6}$ *and* $\alpha \geq 1$ *we have*

$$\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\frac{p^\alpha-1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}.$$

Corollary 15

For any $p \equiv 1 \pmod 6$ *and* $\alpha \geq 1$ *we have*

$$\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\frac{p^\alpha-1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}.$$

This, in turn, implies (after some work):

Corollary 16

Let $p \equiv 1 \pmod 6$ *and* $\alpha \geq 1$*. Then*
p *is* α*-exceptional for* $M = 3$ *iff it's* α*-exceptional for* $M = 6$*.*

Corollary 15

For any $p \equiv 1 \pmod 6$ *and* $\alpha \geq 1$ *we have*

$$\left(\left(\frac{p^\alpha - 1}{3}\right)_p!\right)^{24} \equiv \left(\left(\frac{p^\alpha - 1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}.$$

This, in turn, implies (after some work):

Corollary 16

Let $p \equiv 1 \pmod 6$ *and* $\alpha \geq 1$*. Then*
p *is* α*-exceptional for* $M = 3$ *iff it's* α*-exceptional for* $M = 6$*.*

This confirms our observation from Table 1.

Corollary 15

For any $p \equiv 1 \pmod 6$ *and* $\alpha \geq 1$ *we have*

$$\left(\left(\frac{p^\alpha-1}{3}\right)_p!\right)^{24} \equiv \left(\left(\frac{p^\alpha-1}{6}\right)_p!\right)^{12} \pmod{p^\alpha}.$$

This, in turn, implies (after some work):

Corollary 16

Let $p \equiv 1 \pmod 6$ *and* $\alpha \geq 1$*. Then*
p *is* α*-exceptional for* $M = 3$ *iff it's* α*-exceptional for* $M = 6$*.*

This confirms our observation from Table 1.

Another consequence is the desired exceptionality criterion:

Theorem 17

Let $p \equiv 1 \pmod 6$ *and u as before. Then for a fixed* $\alpha \geq 1$, *p is* α*-exceptional for* $M = 3$ *(and* $M = 6$*) iff*

$$\left(u - \frac{p}{u} - \frac{p^2}{u^3} - 2\frac{p^3}{u^5} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}},$$

where C_n *is the nth Catalan number.*

Theorem 17

Let $p \equiv 1 \pmod 6$ *and* u *as before. Then for a fixed* $\alpha \geq 1$*,* p *is* α*-exceptional for* $M = 3$ *(and* $M = 6$*) iff*

$$\left(u - \frac{p}{u} - \frac{p^2}{u^3} - 2\frac{p^3}{u^5} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}}\right)^{p-1} \equiv 1 \pmod{p^{\alpha+1}},$$

where C_n *is the nth Catalan number.*

Special case:

Corollary 18

Let $p \equiv 1 \pmod 6$ *and* u *as before. Then* p *is* 1*-exceptional for* $M = 3$ *(and* $M = 6$*) iff*

$$\left(u - \tfrac{p}{u}\right)^{p-1} \equiv 1 \pmod{p^2}.$$

Some final remarks:

1. For 1-exceptionality, u can be replaced by $2a$, to give:

Corollary 19

Let $p \equiv 1 \pmod 6$, $p = a^2 + 3b^2$ with $a \equiv -1 \pmod 3$. Then p is 1-exceptional for $M = 3$ (and $M = 6$) iff

$$(2a)^{p-3}\left((2a)^2 + p\right) \equiv 1 \pmod{p^2}.$$

Some final remarks:

1. For 1-exceptionality, u can be replaced by $2a$, to give:

Corollary 19

Let $p \equiv 1 \pmod 6$, $p = a^2 + 3b^2$ with $a \equiv -1 \pmod 3$. Then p is 1-exceptional for $M = 3$ (and $M = 6$) iff

$$(2a)^{p-3}\left((2a)^2 + p\right) \equiv 1 \pmod{p^2}.$$

2. 1-exceptionality is the most important case:

Theorem 20

Let $M \geq 2$, $p \equiv 1 \pmod M$, and $\alpha \geq 2$. If p is α-exceptional, then it's also $(\alpha - 1)$-exceptional (for M).

Some final remarks:

1. For 1-exceptionality, u can be replaced by $2a$, to give:

Corollary 19

Let $p \equiv 1 \pmod{6}$, $p = a^2 + 3b^2$ with $a \equiv -1 \pmod{3}$. Then p is 1-exceptional for $M = 3$ (and $M = 6$) iff

$$(2a)^{p-3}\left((2a)^2 + p\right) \equiv 1 \pmod{p^2}.$$

2. 1-exceptionality is the most important case:

Theorem 20

Let $M \geq 2$, $p \equiv 1 \pmod{M}$, and $\alpha \geq 2$. If p is α-exceptional, then it's also $(\alpha - 1)$-exceptional (for M).

This means that only 1-exceptional primes need to be checked for 2-exceptionality.

Results:

- $M = 3, 6$: Searched up to 10^{12}.
  No new 1-exceptional primes found.

Results:

- $M = 3, 6$: Searched up to 10^{12}.
  No new 1-exceptional primes found.

- $M = 4$: A similar new criterion.
  Searched up to 10^{11}.
  No new 1-exceptional primes found.

Results:

- $M = 3, 6$: Searched up to 10^{12}.
  No new 1-exceptional primes found.

- $M = 4$: A similar new criterion.
  Searched up to 10^{11}.
  No new 1-exceptional primes found.

- All $M \leq 100$:
  None of the known 1-exceptional primes are 2-exceptional.

And now for something completely different:

And now for something completely different:

At Peggy's Cove, Nova Scotia, $\sim$1988

Thank you