Gauss Factorials, Jacobi Primes, and Generalized Fermat Numbers

Karl Dilcher

Number Theory Seminar, September 28, 2018

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:

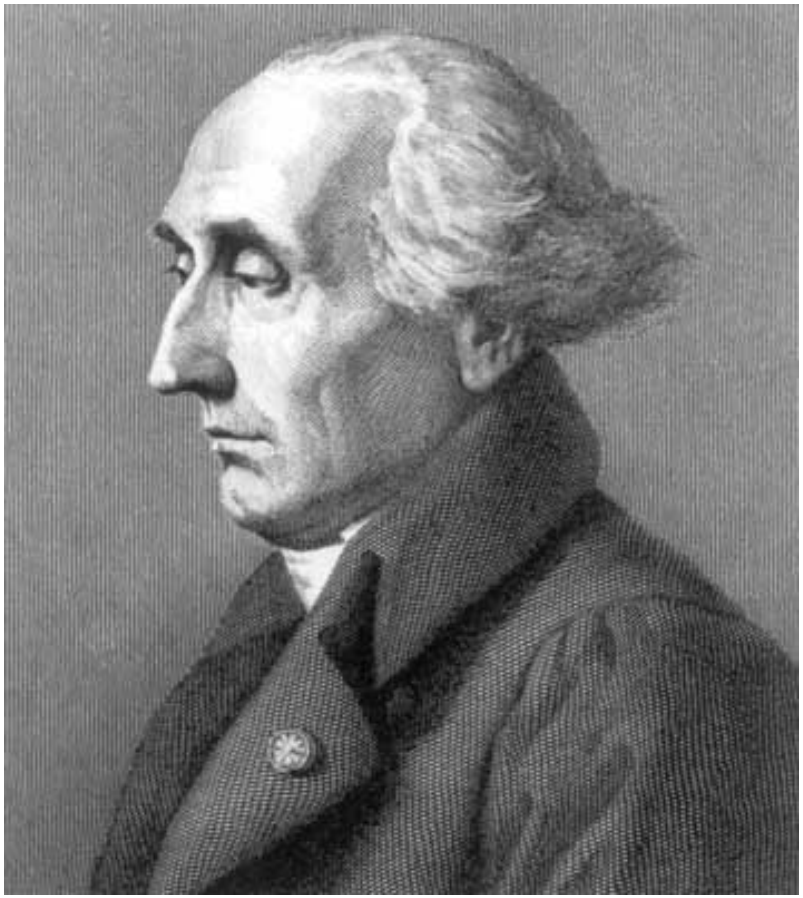
$$1 \cdot 2 \cdot \ldots \cdot \tfrac{p-1}{2} \, \tfrac{p+1}{2} \cdot \ldots \cdot (p-1) \equiv \left(\tfrac{p-1}{2}\right)! (-1)^{\frac{p-1}{2}} \left(\tfrac{p-1}{2}\right)! \pmod{p}.$$

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).

John Wilson
1741–1793



Joseph-Louis Lagrange
1736–1813

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

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

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

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

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

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

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

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

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)

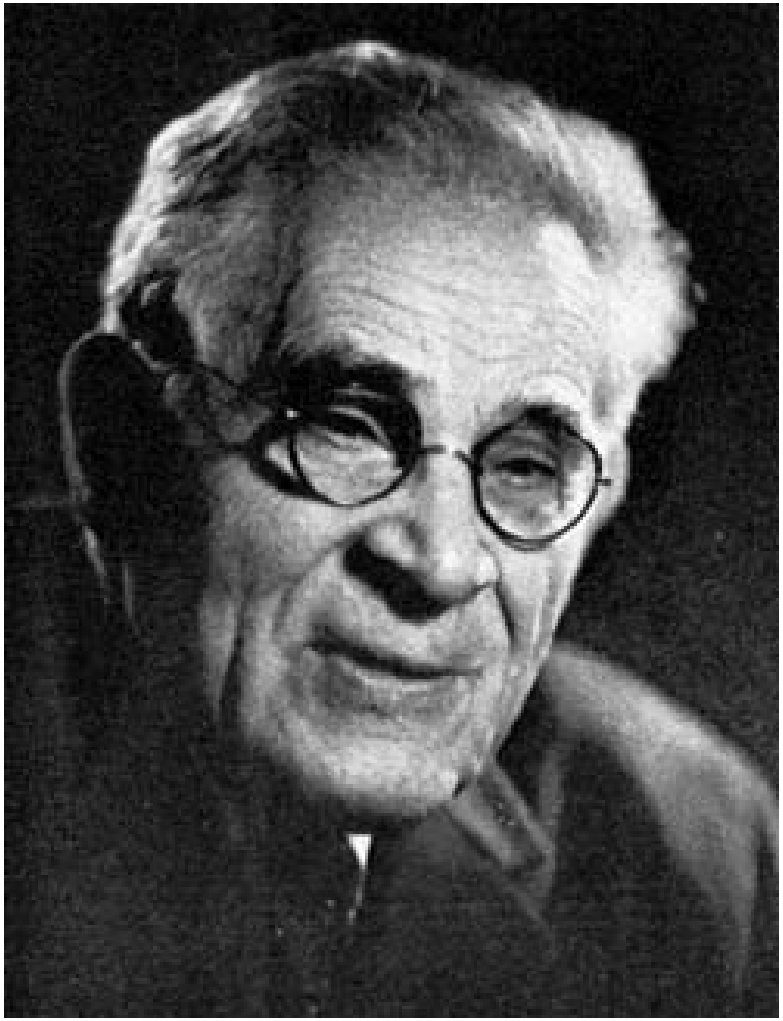
For a prime $p \equiv 3 \pmod 4$,

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

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

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

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



Louis J. Mordell
1888–1972

Sarvadaman Chowla
1907–1995

Is there an analogue of Wilson's Theorem for *composite* integers?

Is there an analogue of Wilson's Theorem for *composite* integers?

For integers $N, n \geq 1$ we define the *Gauss factorial*

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

Is there an analogue of Wilson's Theorem for *composite* integers?

For integers $N, n \geq 1$ we define the *Gauss factorial*

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

Theorem 2 (The Gauss-Wilson Theorem)

For any $n \geq 2$,

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

where p is an odd prime and $\alpha \geq 1$.

General long-term program: To study the Gauss factorials

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

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),

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).

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).

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

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).

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

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).

- $M = 1$: Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
  Only possible orders are 1, 2, and 4.
- $M \geq 3$: Orders are generally unbounded.
  Various partial results; e.g.,

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).

- $M = 1$: Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
  Only possible orders are 1, 2, and 4.
- $M \geq 3$: Orders are generally unbounded.
  Various partial results; e.g.,
  - If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$,
    then $(\frac{n-1}{M})_n! \equiv 1 \pmod{n}$;

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).

- $M = 1$: Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
  Only possible orders are 1, 2, and 4.
- $M \geq 3$: Orders are generally 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;
this talk will be about three different instances of this.

– If n has **one** prime factor $\equiv 1 \pmod{M}$:
  Most interesting case;
  this talk will be about three different instances of this.

– If n has **no** prime factor $\equiv 1 \pmod{M}$:
  Next to nothing is known.

– If n has **one** prime factor $\equiv 1 \pmod{M}$:
Most interesting case;
this talk will be about three different instances of this.

– If n has **no** prime factor $\equiv 1 \pmod{M}$:
Next to nothing is known.

Some further aspects:

- Other partial products of the “full" product $(n-1)_n!$ have also been studied (JBC & KD, 2013).
(Not in this talk).

– If n has **one** prime factor $\equiv 1 \pmod{M}$:
Most interesting case;
this talk will be about three different instances of this.

– If n has **no** prime factor $\equiv 1 \pmod{M}$:
Next to nothing is known.

Some further aspects:

- Other partial products of the “full" product $(n-1)_n!$ have also been studied (JBC & KD, 2013).
(Not in this talk).

- Some meaningful results also when $n \not\equiv 1 \pmod{M}$;
in this case consider $\lfloor \frac{n-1}{M} \rfloor_n!$.
(Later in this talk).

2. Binomial Coefficient Congruences

First application of Gauss factorials:

2. Binomial Coefficient Congruences

First application of Gauss factorials:

In 1828, Gauss proved the following remarkable congruence.

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

2. Binomial Coefficient Congruences

First application of Gauss factorials:

In 1828, Gauss proved the following remarkable congruence.

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 3 (Gauss, 1828)

Let p and a be as above. Then

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

This can be extended:

This can be extended:

Theorem 4

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

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

This can be extended:

Theorem 4

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.

Jacobi proved a similar theorem to that of Gauss:

Theorem 5 (Jacobi, 1837)

Let $p \equiv 1 \pmod 3$, *and write* $4p = r^2 + 27t^2$, $r \equiv 1 \pmod 3$, *which uniquely determines the integer* r. *Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

Jacobi proved a similar theorem to that of Gauss:

Theorem 5 (Jacobi, 1837)

Let $p \equiv 1 \pmod 3$, *and write* $4p = r^2 + 27t^2$, $r \equiv 1 \pmod 3$, *which uniquely determines the integer* r. *Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

Yet another theorem of this type is due to Hudson and Williams (1984) (later).

Jacobi proved a similar theorem to that of Gauss:

Theorem 5 (Jacobi, 1837)

Let $p \equiv 1 \pmod 3$, *and write* $4p = r^2 + 27t^2$, $r \equiv 1 \pmod 3$, *which uniquely determines the integer* r. *Then*

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

Yet another theorem of this type is due to Hudson and Williams (1984) (later).

These and others also have “Catalan analogues" (JBC & KD, 2010; Al-Shaghay, 2014; JBC & KD, 2016).

C. F. Gauss
1777–1855

C. G. J. Jacobi
1804–1851

3. Sequences of Multiplicative Orders

For the second part of this talk, the main objects of study are:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

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

3. Sequences of Multiplicative Orders

For the second part of this talk, the main objects of study are:
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.

3. Sequences of Multiplicative Orders

For the second part of this talk, the main objects of study are:
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

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

3. Sequences of Multiplicative Orders

For the second part of this talk, the main objects of study are:
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

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

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.

3. Sequences of Multiplicative Orders

For the second part of this talk, the main objects of study are:
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

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

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

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

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

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

Computations seem to support this.

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

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

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 $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

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

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 $\gamma_1^4 \to \gamma_2^4$.

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

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

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 next part 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

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

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 next part 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

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

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 next part 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

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

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 next part 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 6

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

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

Theorem 6

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 6

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 $3 \leq M \leq 100$.

4. Exceptional Primes

The proof of Theorem 6 provides a first criterion;
all entries in the table were found with this criterion.

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

4. Exceptional Primes

The proof of Theorem 6 provides a first criterion;
all entries in the table were found with this 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.

4. Exceptional Primes

The proof of Theorem 6 provides a first criterion;
all entries in the table were found with this 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.

4. Exceptional Primes

The proof of Theorem 6 provides a first criterion;
all entries in the table were found with this 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.

5. 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 in a certain technical way.

5. 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 in a certain technical way.

With a and b as above, we obtain two closely related pairs r, s and u, v which also satisfy sums-of-squares identities:

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

5. 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 in a certain technical way.

With a and b as above, we obtain two closely related pairs r, s and u, v which 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 numbers u occur in the following analogue of the binomial coefficient theorems of Gauss and Jacobi:

Theorem 7 (Hudson and Williams, 1984)

Let $p \equiv 1 \pmod 6$ *be a prime and* u *as above. Then*

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1} u \pmod p.$$

Theorem 7 (Hudson and Williams, 1984)

Let $p \equiv 1 \pmod 6$ be a prime and u as above. Then

$$\binom{\frac{p-1}{3}}{\frac{p-1}{6}} \equiv (-1)^{\frac{p-1}{6}+1} u \pmod p.$$

This has the following “Catalan extension":

Theorem 8

Let p and u be as above. Then for $\alpha \geq 1$ we have

$$\frac{\left(\frac{p^{\alpha+1}-1}{3}\right)_p!}{\left(\left(\frac{p^{\alpha+1}-1}{6}\right)_p!\right)^2} \equiv (-1)^{\frac{p-1}{6}+1} \times \left(u - \frac{p}{u} - \frac{p^2}{u^3} - \cdots - C_{\alpha-1}\frac{p^\alpha}{u^{2\alpha-1}}\right) \pmod{p^{\alpha+1}}.$$

Kenneth S. Williams
b. 1940

Eugène Catalan
1814–1894

The next result will be the basis for all that follows.

Theorem 9

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.

The next result will be the basis for all that follows.

Theorem 9

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;

The next result will be the basis for all that follows.

Theorem 9

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 9;

The next result will be the basis for all that follows.

Theorem 9

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 9;
- quotients of certain Gauss factorials are involved as intermediate steps.

Corollary 10

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 10

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 11

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 10

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 11

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 10

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

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

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

Corollary 11

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 12

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 12

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 13

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

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

It turns out: 1-exceptionality is the most important case:

Theorem 14

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).

It turns out: 1-exceptionality is the most important case:

Theorem 14

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.

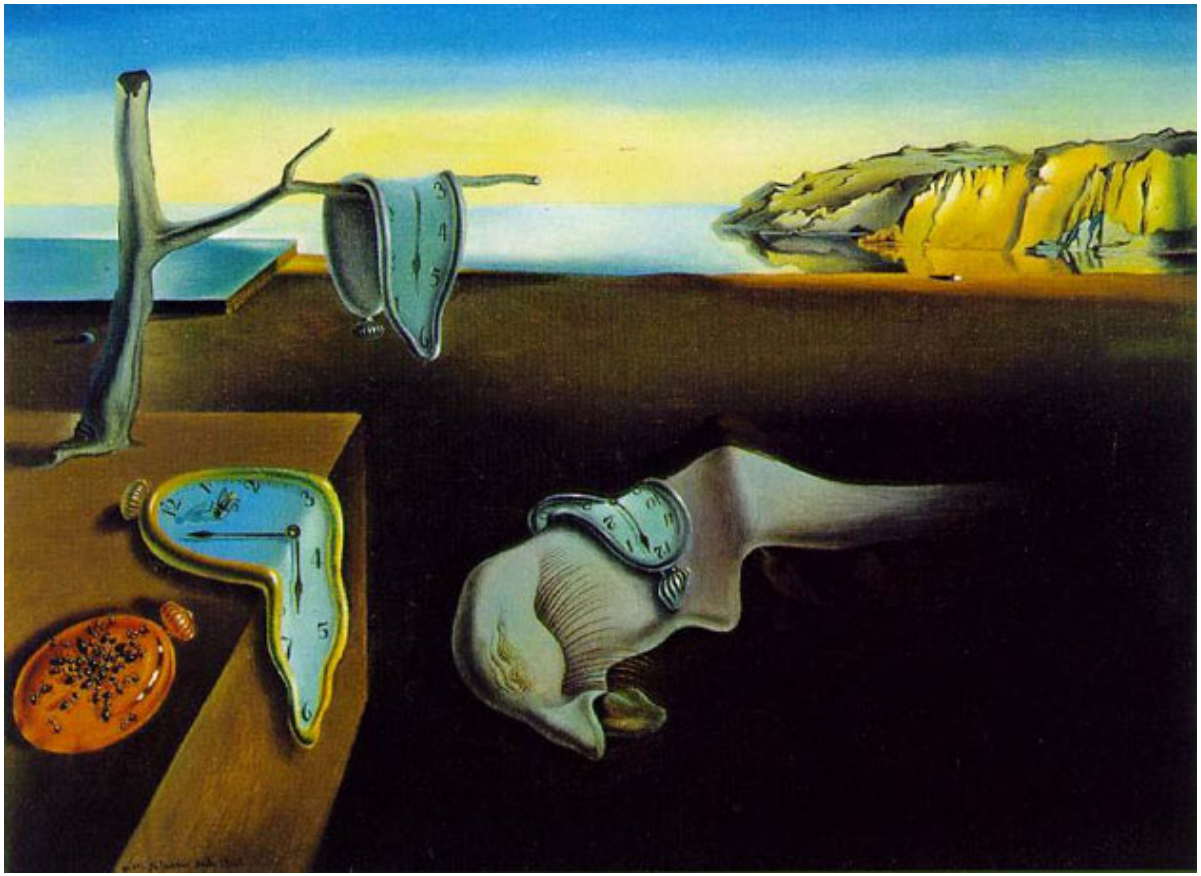
Results:

- $M = 3, 6$: 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.

How are we doing with time?



Salvador Dalí, *The Persistence of Memory*, 1931.

6. Gauss Factorials of Order 1

This is the third part of this talk.

Now: given a fixed $M \geq 1$, we consider the question: which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}$$

6. Gauss Factorials of Order 1

This is the third part of this talk.

Now: given a fixed $M \geq 1$, we consider the question: which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}$$

Recall:

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

6. Gauss Factorials of Order 1

This is the third part of this talk.

Now: given a fixed $M \geq 1$, we consider the question: which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}$$

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).

6. Gauss Factorials of Order 1

This is the third part of this talk.

Now: given a fixed $M \geq 1$, we consider the question: which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}$$

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
- $M = 3, 4, 6$: Most interesting cases.

6. Gauss Factorials of Order 1

This is the third part of this talk.

Now: given a fixed $M \geq 1$, we consider the question: which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}$$

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
- $M = 3, 4, 6$: Most interesting cases.
  - $M = 4$: Previously studied (JBC & KD, 2014).

6. Gauss Factorials of Order 1

This is the third part of this talk.

Now: given a fixed $M \geq 1$, we consider the question:
which integers n satisfy

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}$$

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
- $M = 3, 4, 6$: Most interesting cases.
  - $M = 4$: Previously studied (JBC & KD, 2014).
  - $M = 3, 6$: Similar to each other, but different from $M = 4$; topic of the remainder of this talk.

Different point of view: Consider again

$$\left\lfloor \frac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{1}$$

Different point of view: Consider again

$$\left\lfloor \frac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{1}$$

– If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then (1) always holds for $n \equiv 1 \pmod{M}$.

Different point of view: Consider again

$$\left\lfloor \frac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{1}$$

– If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then (1) always holds for $n \equiv 1 \pmod{M}$.

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

Different point of view: Consider again

$$\left\lfloor \tfrac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{1}$$

– If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then (1) always holds for $n \equiv 1 \pmod{M}$.

– If n has **two** different prime factors $\equiv 1 \pmod{M}$, then the order of $(\tfrac{n-1}{M})_n ! \pmod{n}$ is a divisor of M. In certain cases, solutions of (1) can be characterized.

Different point of view: Consider again

$$\left\lfloor \frac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{1}$$

– If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then (1) always holds for $n \equiv 1 \pmod{M}$.

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

– If n has **one** prime factor $\equiv 1 \pmod{M}$: Most interesting case.

Different point of view: Consider again

$$\left\lfloor \frac{n-1}{M} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad n \equiv \pm 1 \pmod{M}. \tag{1}$$

– If n has **at least 3** different prime factors $\equiv 1 \pmod{M}$, then (1) always holds for $n \equiv 1 \pmod{M}$.

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

– If n has **one** prime factor $\equiv 1 \pmod{M}$: Most interesting case.

– If n has **no** prime factor $\equiv 1 \pmod{M}$: Very little can be said.

Setting the stage: We'll consider integers of the form

$$n = p^{\alpha} w, \quad \text{with} \quad w = q_1^{\beta_1} \dots q_s^{\beta_s}$$

($s \geq 0, \alpha, \beta_1, \dots, \beta_s \in \mathbb{N}$), where

$$p \equiv 1 \pmod 3, \quad q_1 \equiv \cdots \equiv q_s \equiv -1 \pmod 3$$

are distinct primes (case $s = 0$ is interpreted as $w = 1$.)

Setting the stage: We'll consider integers of the form

$$n = p^{\alpha} w, \quad \text{with} \quad w = q_1^{\beta_1} \dots q_s^{\beta_s}$$

($s \geq 0, \alpha, \beta_1, \dots, \beta_s \in \mathbb{N}$), where

$$p \equiv 1 \pmod 3, \quad q_1 \equiv \cdots \equiv q_s \equiv -1 \pmod 3$$

are distinct primes (case $s = 0$ is interpreted as $w = 1$.)

Here: study integers of this type for which

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod n, \tag{2}$$

or

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod n. \tag{3}$$

First few solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}:$$

First few solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}, \qquad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}:$$

n	factored	n	factored
26	$2 \cdot \mathbf{13}$	1105	$5 \cdot \mathbf{13} \cdot 17$
244	$2^2 \cdot \mathbf{61}$	14365	$5 \cdot \mathbf{13^2} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13^2}$	303535	$5 \cdot 17 \cdot \mathbf{3571}$
9755	$5 \cdot \mathbf{1951}$	309485	$5 \cdot 11 \cdot 17 \cdot \mathbf{331}$
18205	$5 \cdot 11 \cdot \mathbf{331}$	353365	$5 \cdot 29 \cdot \mathbf{2437}$
33076	$2^2 \cdot \mathbf{8269}$	508255	$5 \cdot 11 \cdot \mathbf{9241}$
48775	$5^2 \cdot \mathbf{1951}$	510605	$5 \cdot \mathbf{102121}$
60707	$17 \cdot \mathbf{3571}$	527945	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

In bold: $p \equiv 1 \pmod{3}$.

First few solutions of

$$\left\lfloor \frac{n-1}{3} \right\rfloor_n! \equiv 1 \pmod{n}, \qquad \left\lfloor \frac{n-1}{6} \right\rfloor_n! \equiv 1 \pmod{n}:$$

n	factored	n	factored
26	$2 \cdot \mathbf{13}$	1105	$5 \cdot \mathbf{13} \cdot 17$
244	$2^2 \cdot \mathbf{61}$	14365	$5 \cdot \mathbf{13^2} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13^2}$	303535	$5 \cdot 17 \cdot \mathbf{3571}$
9755	$5 \cdot \mathbf{1951}$	309485	$5 \cdot 11 \cdot 17 \cdot \mathbf{331}$
18205	$5 \cdot 11 \cdot \mathbf{331}$	353365	$5 \cdot 29 \cdot \mathbf{2437}$
33076	$2^2 \cdot \mathbf{8269}$	508255	$5 \cdot 11 \cdot \mathbf{9241}$
48775	$5^2 \cdot \mathbf{1951}$	510605	$5 \cdot \mathbf{102121}$
60707	$17 \cdot \mathbf{3571}$	527945	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

In bold: $p \equiv 1 \pmod{3}$.

How can we characterize these solutions?

First few solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n! \equiv 1 \pmod{n}, \qquad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n! \equiv 1 \pmod{n}:$$

n	factored	n	factored
26	$2 \cdot \mathbf{13}$	1105	$5 \cdot \mathbf{13} \cdot 17$
244	$2^2 \cdot \mathbf{61}$	14365	$5 \cdot \mathbf{13^2} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13^2}$	303535	$5 \cdot 17 \cdot \mathbf{3571}$
9755	$5 \cdot \mathbf{1951}$	309485	$5 \cdot 11 \cdot 17 \cdot \mathbf{331}$
18205	$5 \cdot 11 \cdot \mathbf{331}$	353365	$5 \cdot 29 \cdot \mathbf{2437}$
33076	$2^2 \cdot \mathbf{8269}$	508255	$5 \cdot 11 \cdot \mathbf{9241}$
48775	$5^2 \cdot \mathbf{1951}$	510605	$5 \cdot \mathbf{102121}$
60707	$17 \cdot \mathbf{3571}$	527945	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

In bold: $p \equiv 1 \pmod{3}$.

How can we characterize these solutions?
Let's consider some specific $p \equiv 1 \pmod{3}$.

Example. Let $p = 7$, the smallest admissible p in

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

Example. Let $p = 7$, the smallest admissible p in

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(a) Solutions of $\left\lfloor \frac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}$:

Example. Let $p = 7$, the smallest admissible p in

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(a) Solutions of $\left\lfloor \frac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}$:

Combination of theory and computation shows:

- For $s = 0, 1, \dots, 6$: no solutions.

Example. Let $p = 7$, the smallest admissible p in

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(a) Solutions of $\left\lfloor \frac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}$:

Combination of theory and computation shows:

- For $s = 0, 1, \dots, 6$: no solutions.

- For $s = 7$: exactly 27 solutions, the smallest and largest of which are

$$n = \mathbf{7} \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833,$$

$$n = \mathbf{7} \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833,$$

with 30 and 36 decimal digits, respectively.

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

- For $s = 0$: trivial solution $n = 7$.

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \dots, 6$: no solutions.

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \dots, 6$: no solutions.
- For $s = 6$: single 40-digit solution

$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \dots, 6$: no solutions.
- For $s = 6$: single 40-digit solution

$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$

Questions:

(i) What determines presence/absence of solutions?

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \dots, 6$: no solutions.
- For $s = 6$: single 40-digit solution

$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$

Questions:

(i) What determines presence/absence of solutions?

(ii) What are the factors q_j when solutions exist?

$$n = p^{\alpha} q_1^{\beta_1} \dots q_s^{\beta_s}.$$

(b) Solutions of $\left\lfloor \frac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$:

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \dots, 6$: no solutions.
- For $s = 6$: single 40-digit solution

$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$

Questions:

(i) What determines presence/absence of solutions?

(ii) What are the factors q_j when solutions exist?

(iii) For what p can solutions exist?

"You know, most people's favourite number is 7, but mine is 627399010364832991004825304810385572229571004927401015482947738885917389."

The solutions, again: **For $M = 3$:**

$$n = \mathbf{7} \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833,$$

$$\ldots$$

$$n = \mathbf{7} \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

For $M = 6$:

$$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

The solutions, again: **For $M = 3$:**

$$n = \mathbf{7} \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833,$$

$$\ldots$$

$$n = \mathbf{7} \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

For $M = 6$:

$$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

Note:

$$\begin{aligned} 5 &\mid 7^2 + 1, \\ 17 &\mid 7^{2^3} + 1 \quad \text{and} \quad 169\,553 \mid 7^{2^3} + 1, \\ 353 &\mid 7^{2^4} + 1 \quad \text{and} \quad 47\,072\,139\,617 \mid 7^{2^4} + 1, \\ 7\,699\,649 &\mid 7^{2^5} + 1 \quad \text{and} \quad 531\,968\,664\,833 \mid 7^{2^5} + 1. \end{aligned}$$

The solutions, again: **For $M = 3$:**

$$n = \mathbf{7} \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833,$$

$$\ldots$$

$$n = \mathbf{7} \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

For $M = 6$:

$$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

Note:

$$\begin{aligned} 5 &\mid 7^2 + 1, \\ 17 \mid 7^{2^3} + 1 \quad &\text{and} \quad 169\,553 \mid 7^{2^3} + 1, \\ 353 \mid 7^{2^4} + 1 \quad &\text{and} \quad 47\,072\,139\,617 \mid 7^{2^4} + 1, \\ 7\,699\,649 \mid 7^{2^5} + 1 \quad &\text{and} \quad 531\,968\,664\,833 \mid 7^{2^5} + 1. \end{aligned}$$

Also: $7^{2^2} + 1$ has no prime factor $q \equiv -1 \pmod 3$;

The solutions, again: **For $M = 3$:**

$$n = \mathbf{7} \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833,$$

$$\dots$$

$$n = \mathbf{7} \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

For $M = 6$:

$$n = \mathbf{7} \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$$

Note:

$$\begin{aligned} 5 &\mid 7^2 + 1, \\ 17 \mid 7^{2^3} + 1 \quad &\text{and} \quad 169\,553 \mid 7^{2^3} + 1, \\ 353 \mid 7^{2^4} + 1 \quad &\text{and} \quad 47\,072\,139\,617 \mid 7^{2^4} + 1, \\ 7\,699\,649 \mid 7^{2^5} + 1 \quad &\text{and} \quad 531\,968\,664\,833 \mid 7^{2^5} + 1. \end{aligned}$$

Also: $7^{2^2} + 1$ has no prime factor $q \equiv -1 \pmod 3$;
2^9 is the exact power of 2 that divides

$$(7-1)(7+1)(7^{2^1}+1)\dots(7^{2^5}+1).$$

7. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

$$\left\lfloor \frac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \quad \text{and} \quad \left\lfloor \frac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n},$$

7. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \quad \text{and} \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n},$$

i.e., necessary conditions for the original congruences.

7. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \quad \text{and} \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n},$$

i.e., necessary conditions for the original congruences.

For simplicity, here: Restrict our attention to

- denominator $M = 3$;
- the case $s \geq 2$, where $n = p^\alpha w$, $w = q_1^{\beta_1} \dots q_s^{\beta_s}$,
- $w \equiv 1 \pmod 3$, i.e., $n \equiv 1 \pmod 3$.

7. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \quad \text{and} \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n},$$

i.e., necessary conditions for the original congruences.

For simplicity, here: Restrict our attention to

- denominator $M = 3$;
- the case $s \geq 2$, where $n = p^\alpha w$, $w = q_1^{\beta_1} \dots q_s^{\beta_s}$,
- $w \equiv 1 \pmod 3$, i.e., $n \equiv 1 \pmod 3$.

Main approach: Find criteria for

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{w} \quad \text{and}$$
$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{p^\alpha};$$

7. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{n} \quad \text{and} \quad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n !^3 \equiv 1 \pmod{n},$$

i.e., necessary conditions for the original congruences.

For simplicity, here: Restrict our attention to

- denominator $M = 3$;
- the case $s \geq 2$, where $n = p^\alpha w$, $w = q_1^{\beta_1} \dots q_s^{\beta_s}$,
- $w \equiv 1 \pmod 3$, i.e., $n \equiv 1 \pmod 3$.

Main approach: Find criteria for

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{w} \quad \text{and}$$
$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod{p^\alpha};$$

then combine the two using the Chinese Remainder Theorem.

8. Generalized Fermat numbers

Congruences modulo w:

We define the partial totient function

$$\varphi(M, w) = \#\{\tau \mid 1 \le \tau \le \tfrac{w-1}{M}, \gcd(\tau, w) = 1\}.$$

8. Generalized Fermat numbers

Congruences modulo w:

We define the partial totient function

$$\varphi(M, w) = \#\{\tau \mid 1 \le \tau \le \tfrac{w-1}{M}, \gcd(\tau, w) = 1\}.$$

Lemma 15

With n as before, we have

$$\left(\tfrac{n-1}{3}\right)_n! \equiv \frac{1}{p^{\varphi(3,w)}} \pmod{w}, \qquad \varphi(3, w) = \tfrac{1}{3}(\varphi(w) + 2^{s-1}).$$

8. Generalized Fermat numbers

Congruences modulo w:

We define the partial totient function

$$\varphi(M, w) = \#\{\tau \mid 1 \le \tau \le \tfrac{w-1}{M}, \gcd(\tau, w) = 1\}.$$

Lemma 15

With n as before, we have

$$\left(\tfrac{n-1}{3}\right)_n! \equiv \frac{1}{p^{\varphi(3,w)}} \pmod{w}, \qquad \varphi(3, w) = \tfrac{1}{3}(\varphi(w) + 2^{s-1}).$$

Proof is very technical. Basic idea: Write

$$\tfrac{n-1}{3} = \tfrac{p^\alpha - 1}{3} w + \tfrac{w-1}{3} \qquad (n \equiv 1 \pmod 3).$$

(slightly different when $n \equiv -1 \pmod 3$).

$$\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.$$

This means:

$\lfloor \frac{n-1}{3} \rfloor_n!$ is a product of

$$\begin{cases} \frac{p^\alpha - 1}{3} \text{ “main terms", and} \\ \text{one “remainder term".} \end{cases}$$

$$\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.$$

This means:

$\lfloor \frac{n-1}{3} \rfloor_n!$ is a product of

$$\begin{cases} \frac{p^\alpha - 1}{3} \text{ “main terms", and} \\ \text{one “remainder term".} \end{cases}$$

- Main terms mostly evaluate to 1 (mod w), by Gauss-Wilson.

$$\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.$$

This means:

$\lfloor \frac{n-1}{3} \rfloor_n!$ is a product of

$$\begin{cases} \frac{p^\alpha - 1}{3} \text{ “main terms", and} \\ \text{one “remainder term".} \end{cases}$$

- Main terms mostly evaluate to 1 (mod w), by Gauss-Wilson.

- Remainder term is more subtle, but can also be evaluated by Gauss-Wilson and Euler-Fermat theorems.

$$\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.$$

This means:

$\lfloor \frac{n-1}{3} \rfloor_n!$ is a product of

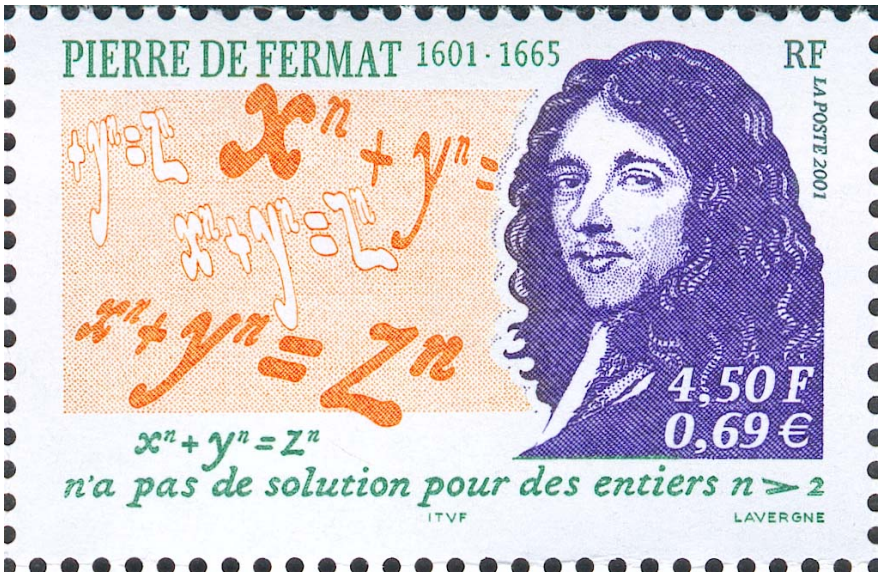
$$\begin{cases} \frac{p^\alpha - 1}{3} \text{ “main terms", and} \\ \text{one “remainder term".} \end{cases}$$

- Main terms mostly evaluate to 1 (mod w), by Gauss-Wilson.

- Remainder term is more subtle, but can also be evaluated by Gauss-Wilson and Euler-Fermat theorems.

- Similar result also for arbitrary denominators $M \geq 2$.


PRO JUVENTUTE 1957
LEONHARD EULER 1707-1783
$e^{i\varphi} = \cos\varphi + i\sin\varphi$
5
+5 HELVETIA


PIERRE DE FERMAT 1601 - 1665
RF
LA POSTE 2001
4,50 F
0,69 €
$x^n + y^n = z^n$
n'a pas de solution pour des entiers $n > 2$
ITVF
LAVERGNE

Now we can see how generalized Fermat numbers enter:

Raise both sides of Lemma to 3rd power.

Then

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv p^{-\varphi(w)-2^{s-1}} \equiv p^{-2^{s-1}} \pmod{w}, \qquad \delta = \pm 1.$$

Now we can see how generalized Fermat numbers enter:

Raise both sides of Lemma to 3rd power.

Then

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv p^{-\varphi(w)-2^{s-1}} \equiv p^{-2^{s-1}} \pmod{w}, \qquad \delta = \pm 1.$$

Therefore

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv 1 \pmod{w}$$

if and only if

$$p^{2^{s-1}} - 1 \equiv 0 \pmod{w}.$$

Now we can see how generalized Fermat numbers enter:

Raise both sides of Lemma to 3rd power.

Then

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv p^{-\varphi(w)-2^{s-1}} \equiv p^{-2^{s-1}} \pmod{w}, \qquad \delta = \pm 1.$$

Therefore

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv 1 \pmod{w}$$

if and only if

$$p^{2^{s-1}} - 1 \equiv 0 \pmod{w}.$$

This factors:

$$p^{2^{s-1}} - 1 = (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1).$$

We have therefore shown:

Theorem 16

Let n be as before, with $s \geq 1$. Then

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv 1 \pmod{w}$$

iff every $q_i^{\beta_i}$ is a divisor of $p^{2^{s-1}} - 1$; i.e., iff every

$$q_i^{\beta_i} \text{ divides } \begin{cases} p-1, & \text{for } s = 1, \\ (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1), & \text{for } s \geq 2. \end{cases}$$

We have therefore shown:

Theorem 16

Let n be as before, with $s \geq 1$. Then

$$\left(\tfrac{n-1}{3}\right)_n!^3 \equiv 1 \pmod{w}$$

iff every $q_i^{\beta_i}$ is a divisor of $p^{2^{s-1}} - 1$; i.e., iff every

$$q_i^{\beta_i} \text{ divides } \begin{cases} p-1, & \text{for } s = 1, \\ (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1), & \text{for } s \geq 2. \end{cases}$$

Note: This is in fact true for

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n! \equiv 1 \pmod{w}.$$

9. Jacobi primes

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma 17

Let $n \equiv 1 \pmod 3$ be as before. Then for $s \geq 2$,

$$\left(\frac{n-1}{3}\right)_n ! \equiv (q_1 \dots q_s)^{(-1)^{s-1}\frac{\varphi(p^\alpha)}{3}} \left(\left(\frac{p^\alpha - 1}{3}\right)_p !\right)^{2^s} \pmod{p^\alpha}.$$

9. Jacobi primes

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma 17

Let $n \equiv 1 \pmod 3$ be as before. Then for $s \geq 2$,

$$\left(\frac{n-1}{3}\right)_n ! \equiv (q_1 \dots q_s)^{(-1)^{s-1}\frac{\varphi(p^\alpha)}{3}} \left(\left(\frac{p^\alpha - 1}{3}\right)_p !\right)^{2^s} \pmod{p^\alpha}.$$

Once again:

- Lemma holds in greater generality;
- proof is very technical.

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma 17

Let $n \equiv 1 \pmod 3$ be as before. Then for $s \geq 2$,

$$\left(\frac{n-1}{3}\right)_n ! \equiv (q_1 \dots q_s)^{(-1)^{s-1}\frac{\varphi(p^\alpha)}{3}} \left(\left(\frac{p^\alpha - 1}{3}\right)_p !\right)^{2^s} \pmod{p^\alpha}.$$

Once again:
- Lemma holds in greater generality;
- proof is very technical.

To apply this lemma, first observe:
By cubing both sides, the $(q_1 \dots q_s)$ term becomes 1 (mod p^α).

Therefore the main conditions is

$$\left(\frac{p^\alpha-1}{3}\right)_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{4}$$

Therefore the main conditions is

$$\left(\frac{p^\alpha-1}{3}\right)_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{4}$$

We'll see: primes p that satisfy this are rather special.

Therefore the main conditions is

$$\left(\tfrac{p^\alpha-1}{3}\right)_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{4}$$

We'll see: primes p that satisfy this are rather special.

Using the notation

$$\gamma_\alpha(p) := \operatorname{ord}_{p^\alpha}\left(\left(\tfrac{p^\alpha-1}{3}\right)_p!\right) \qquad p \equiv 1 \pmod 3),$$

for the multiplicative order modulo p^α,

Therefore the main conditions is

$$(\tfrac{p^\alpha-1}{3})_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{4}$$

We'll see: primes p that satisfy this are rather special.

Using the notation

$$\gamma_\alpha(p) := \operatorname{ord}_{p^\alpha}((\tfrac{p^\alpha-1}{3})_p!) \qquad p \equiv 1 \pmod 3),$$

for the multiplicative order modulo p^α,(4) implies

$$\gamma_\alpha(p) = 2^\ell \quad \text{or} \quad 3\cdot 2^\ell \qquad (0 \le \ell \le s). \tag{5}$$

Therefore the main conditions is

$$(\tfrac{p^\alpha-1}{3})_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{4}$$

We'll see: primes p that satisfy this are rather special.

Using the notation

$$\gamma_\alpha(p) := \operatorname{ord}_{p^\alpha}((\tfrac{p^\alpha-1}{3})_p!) \qquad p \equiv 1 \pmod 3),$$

for the multiplicative order modulo p^α,(4) implies

$$\gamma_\alpha(p) = 2^\ell \quad \text{or} \quad 3\cdot 2^\ell \qquad (0 \le \ell \le s). \tag{5}$$

We saw earlier:
Sequence $\gamma_1(p), \gamma_2(p), \ldots$ behaves in a very specific way;
this means that (5) implies

$$\gamma_1(p) = 2^\ell \quad \text{or} \quad 3\cdot 2^\ell.$$

This gives rise to the following definition:

Definition 18

A prime $p \equiv 1 \pmod 3$ is called a *Jacobi prime of level* ℓ if

$$\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 2^\ell \quad \text{or} \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3\cdot 2^\ell.$$

This gives rise to the following definition:

Definition 18

A prime $p \equiv 1 \pmod 3$ is called a *Jacobi prime of level* ℓ if

$$\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 2^\ell \quad \text{or} \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3\cdot 2^\ell.$$

Examples: We consider the first three primes $p \equiv 1 \pmod 6$ and compute:

$$p = 7: \quad \tfrac{p-1}{3}! = 2, \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3 = 3\cdot 2^0;$$

$$p = 13: \quad \tfrac{p-1}{3}! = 24, \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 12 = 3\cdot 2^2;$$

$$p = 19: \quad \tfrac{p-1}{3}! = 720, \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 9.$$

This gives rise to the following definition:

Definition 18

A prime $p \equiv 1 \pmod 3$ is called a *Jacobi prime of level* ℓ if

$$\operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 2^\ell \quad \text{or} \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3\cdot 2^\ell.$$

Examples: We consider the first three primes $p \equiv 1 \pmod 6$ and compute:

$$p = 7: \quad \tfrac{p-1}{3}! = 2, \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 3 = 3\cdot 2^0;$$

$$p = 13: \quad \tfrac{p-1}{3}! = 24, \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 12 = 3\cdot 2^2;$$

$$p = 19: \quad \tfrac{p-1}{3}! = 720, \quad \operatorname{ord}_p\left(\tfrac{p-1}{3}!\right) = 9.$$

Thus, 7 and 13 are Jacobi primes of levels 0, resp. 2;
19 is not a Jacobi prime.

Why “Jacobi prime"? Recall:

Theorem 19 (Jacobi, 1837)

Let $p \equiv 1 \pmod 3$, and write $4p = r^2 + 27t^2$, $r \equiv 1 \pmod 3$, which uniquely determines the integer r. Then

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

Why “Jacobi prime"? Recall:

Theorem 19 (Jacobi, 1837)

Let $p \equiv 1 \pmod 3$, and write $4p = r^2 + 27t^2$, $r \equiv 1 \pmod 3$, which uniquely determines the integer r. Then

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv -r \pmod p.$$

An easy consequence:

Corollary 20

Let p and r be as above. Then

$$(\tfrac{p-1}{3})!^3 \equiv \frac{1}{r} \pmod p. \tag{6}$$

This leads to equivalent definition:

Corollary 21

A prime $p \equiv 1 \pmod 3$ *is a Jacobi prime of level* ℓ *iff*

$$\operatorname{ord}_p(r) = 2^\ell.$$

This leads to equivalent definition:

Corollary 21

A prime $p \equiv 1 \pmod 3$ is a Jacobi prime of level ℓ iff

$$\operatorname{ord}_p(r) = 2^\ell.$$

Examples:

$$\begin{aligned}
p = 7: &\quad 4p = 1^2 + 27 \cdot 1^2, &&\operatorname{ord}_p(1) = 2^0;\\
p = 13: &\quad 4p = (-5)^2 + 27 \cdot 1^2, &&\operatorname{ord}_p(-5) = 2^2;\\
p = 19: &\quad 4p = 7^2 + 27 \cdot 1^2, &&\operatorname{ord}_p(7) = 3.
\end{aligned}$$

Consistent with previous examples.

Some further properties:

Theorem 22

(*a*) *A prime p is a level-0 Jacobi prime if and only if*

$$p = 27X^2 + 27X + 7 \qquad (X \in \mathbb{Z}).$$

(*b*) *There is no level-1 Jacobi prime.*
(*c*) *The only level-2 Jacobi prime is $p = 13$.*

Some further properties:

Theorem 22

(*a*) *A prime p is a level-0 Jacobi prime if and only if*

$$p = 27X^2 + 27X + 7 \qquad (X \in \mathbb{Z}).$$

(*b*) *There is no level-1 Jacobi prime.*
(*c*) *The only level-2 Jacobi prime is $p = 13$.*

Remarks: (1) As expected, level-0 Jacobi primes are quite abundant; the first few (up to 1000) are 7, 61, 331 and 547; a total of 215 105 up to 10^{14}.

Some further properties:

Theorem 22

(*a*) *A prime p is a level-0 Jacobi prime if and only if*

$$p = 27X^2 + 27X + 7 \qquad (X \in \mathbb{Z}).$$

(*b*) *There is no level-1 Jacobi prime.*
(*c*) *The only level-2 Jacobi prime is $p = 13$.*

Remarks: (1) As expected, level-0 Jacobi primes are quite abundant; the first few (up to 1000) are 7, 61, 331 and 547; a total of 215 105 up to 10^{14}.

(2) On the other hand, Jacobi primes of levels $\ell \geq 3$ are very rare, with only 44 up to 10^{14}.
The first few are 13, 97, 193, 409, 769.

Using a slightly more general setting again, with $n \equiv w \equiv \pm 1 \pmod 3$, we have

Theorem 23

Let n be as above, with $\alpha \geq 1$ and $s \geq 2$. Then a necessary and sufficient condition for

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod n$$

to hold is that all of the following be satisfied:

(a) *p is $(\alpha - 1)$-exceptional if $\alpha > 1$;*

(b) *p is a level-ℓ Jacobi prime for some $0 \leq \ell \leq s$;*

(c) *$q_i^{\beta_i} \mid (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1)$ for all $1 \leq i \leq s$.*

Using a slightly more general setting again, with $n \equiv w \equiv \pm 1 \pmod 3$, we have

Theorem 23

Let n be as above, with $\alpha \geq 1$ and $s \geq 2$. Then a necessary and sufficient condition for

$$\left\lfloor \frac{n-1}{3} \right\rfloor_n !^3 \equiv 1 \pmod n$$

to hold is that all of the following be satisfied:

(a) p is $(\alpha - 1)$-exceptional if $\alpha > 1$;

(b) p is a level-ℓ Jacobi prime for some $0 \leq \ell \leq s$;

(c) $q_i^{\beta_i} \mid (p-1)(p+1)(p^2+1)\dots(p^{2^{s-2}}+1)$ for all $1 \leq i \leq s$.

Relevant here:

$p = 13$ is **the only** Jacobi prime $< 10^{12}$
that is also 1-exceptional.

Let’s return to our original table:

Let's return to our original table:

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n} \qquad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}$$

n	factored	n	factored
26	$2 \cdot \mathbf{13}$	1105	$5 \cdot \mathbf{13} \cdot 17$
244	$2^2 \cdot \mathbf{61}$	14365	$5 \cdot \mathbf{13^2} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13^2}$	303535	$5 \cdot 17 \cdot \mathbf{3571}$
9755	$5 \cdot \mathbf{1951}$	309485	$5 \cdot 11 \cdot 17 \cdot \mathbf{331}$
18205	$5 \cdot 11 \cdot \mathbf{331}$	353365	$5 \cdot 29 \cdot \mathbf{2437}$
33076	$2^2 \cdot \mathbf{8269}$	508255	$5 \cdot 11 \cdot \mathbf{9241}$
48775	$5^2 \cdot \mathbf{1951}$	510605	$5 \cdot \mathbf{102121}$
60707	$17 \cdot \mathbf{3571}$	527945	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

In bold: $p \equiv 1 \pmod{3}$.

Let's return to our original table:

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n! \equiv 1 \pmod{n} \qquad \left\lfloor \tfrac{n-1}{6} \right\rfloor_n! \equiv 1 \pmod{n}$$

n	factored	n	factored
26	$2 \cdot \mathbf{13}$	1105	$5 \cdot \mathbf{13} \cdot 17$
244	$2^2 \cdot \mathbf{61}$	14365	$5 \cdot \mathbf{13^2} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13^2}$	303535	$5 \cdot 17 \cdot \mathbf{3571}$
9755	$5 \cdot \mathbf{1951}$	309485	$5 \cdot 11 \cdot 17 \cdot \mathbf{331}$
18205	$5 \cdot 11 \cdot \mathbf{331}$	353365	$5 \cdot 29 \cdot \mathbf{2437}$
33076	$2^2 \cdot \mathbf{8269}$	508255	$5 \cdot 11 \cdot \mathbf{9241}$
48775	$5^2 \cdot \mathbf{1951}$	510605	$5 \cdot \mathbf{102121}$
60707	$17 \cdot \mathbf{3571}$	527945	$5 \cdot 11 \cdot 29 \cdot \mathbf{331}$

In bold: $p \equiv 1 \pmod{3}$.

We have seen: *Only* $p = 13$ can possibly appear to a higher power, for $p < 10^{12}$.

Thank you


1 2 3
I JUST INVENTED NUMBERS!
NEAT! HOW MANY?
12-15
THAVES
E-mail:BobThaves@aol.com
©2004 Thaves / Dist. by NEA, Inc.
www.frankandernest.com