Generalized Fermat Numbers: Some Results and Applications

John B. Cosgrave and Karl Dilcher

Dublin, Ireland and Halifax, Nova Scotia, Canada

In honour of Richard Brent
John B. Cosgrave
1. Fermat Numbers

\[ F_m = 2^{2^m} + 1 \]

has no "algebraic factors", and is prime for \( m = 0, 1, 2, 3, 4 \).
1. Fermat Numbers

\[ F_m = 2^{2^m} + 1 \]

has no "algebraic factors", and is prime for \( m = 0, 1, 2, 3, 4. \)

Fermat conjectured: All are prime.
1. Fermat Numbers

\[ F_m = 2^{2^m} + 1 \]

has no "algebraic factors", and is prime for \( m = 0, 1, 2, 3, 4 \).

Fermat conjectured: All are prime.

However, Euler showed: \( F_5 = 641 \cdot 6700417 \).
1. Fermat Numbers

\[ F_m = 2^{2^m} + 1 \]

has no "algebraic factors", and is prime for \( m = 0, 1, 2, 3, 4 \).

Fermat conjectured: All are prime.

However, Euler showed: \( F_5 = 641 \cdot 6700417 \).

Pierre de Fermat
1601–1665

Leonhard Euler
1707–1783
1.1. Current Status (as of August 31, 2016)

- Completely factored: $m = 5, 6, \ldots, 11.$
- Known to be composite, but no factor known: $m = 20, 24.$
- Nature unknown: $m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots$
- 288 FNs known to be composite.
- 331 prime factors known.
- Largest known composite: $m = 3329780$ (Ottusch et al., 2014)
- Latest factor found: 
  $24142479 \cdot 2^{14590} + 1 \mid F_{14587}$ (A. Nordin, May 25, 2016)
  (From Wilfrid Keller's list: http://www.prothsearch.net/fermat.html).
1.1. Current Status (as of August 31, 2016)

- Completely factored: \( m = 5, 6, \ldots, 11 \).
- Known to be composite, but no factor known: \( m = 20, 24 \).

- 288 FNs known to be composite.
- 331 prime factors known.
- Largest known composite: \( m = 3,329,780 \) (Ottusch et al., 2014)
- Latest factor found: \( 24,142,479 \cdot 2^{14590} + 1 \) | \( F_{14587} \) (A. Nordin, May 25, 2016)

(From Wilfrid Keller's list: http://www.prothsearch.net/fermat.html).
1.1. Current Status (as of August 31, 2016)

- Completely factored: $m = 5, 6, \ldots, 11$.
- Known to be composite, but no factor known: $m = 20, 24$.
- Nature unknown: $m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots$
1.1. Current Status (as of August 31, 2016)

- Completely factored: $m = 5, 6, \ldots, 11$.
- Known to be composite, but no factor known: $m = 20, 24$.
- Nature unknown: $m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots$
- 288 FNs known to be composite.
1.1. Current Status (as of August 31, 2016)

- Completely factored: \( m = 5, 6, \ldots, 11 \).
- Known to be composite, but no factor known: \( m = 20, 24 \).
- Nature unknown: \( m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots \).
- 288 FNs known to be composite.
- 331 prime factors known.

(Largest known composite: \( m = 3329780 \) (Ottusch et al., 2014).
Latest factor found: \( 24142479 \cdot 2^{14590} + 1 \mid F_{14587} \) (A. Nordin, May 25, 2016).
(From Wilfrid Keller's list: http://www.prothsearch.net/fermat.html).
1.1. Current Status (as of August 31, 2016)

- Completely factored: $m = 5, 6, \ldots, 11$.
- Known to be composite, but no factor known: $m = 20, 24$.
- Nature unknown: $m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots$
- 288 FNs known to be composite.
- 331 prime factors known.
- Largest known composite: $m = 3\,329\,780$ (Ottusch et al., 2014)
1.1. Current Status (as of August 31, 2016)

- Completely factored: \( m = 5, 6, \ldots, 11 \).
- Known to be composite, but no factor known: \( m = 20, 24 \).
- Nature unknown: \( m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots \).
- 288 FNs known to be composite.
- 331 prime factors known.
- Largest known composite:
  \( m = 3,329,780 \) (Ottusch et al., 2014)
- Latest factor found:
  \[ 24,142,479 \cdot 2^{14590} + 1 \mid F_{14587} \] (A. Nordin, May 25, 2016)
1.1. Current Status (as of August 31, 2016)

- Completely factored: \( m = 5, 6, \ldots, 11 \).
- Known to be composite, but no factor known: \( m = 20, 24 \).
- Nature unknown: \( m = 33, 34, 35, 40, 41, 44, 45, 46, \ldots \).
- 288 FNs known to be composite.
- 331 prime factors known.
- Largest known composite:
  \( m = 3329780 \) (Ottusch et al., 2014)
- Latest factor found:
  \( 24142479 \cdot 2^{14590} + 1 \mid F_{14587} \) (A. Nordin, May 25, 2016)

(From Wilfrid Keller’s list:
http://www.prothsearch.net/fermat.html).
1.2. Finding Factors

**Theorem:** (Euler 1747, Lucas 1879)
If a prime \( p \) divides \( F_m \), then \( p = k \cdot 2^{m+2} + 1 \).
Theorem: (Euler 1747, Lucas 1879)
If a prime $p$ divides $F_m$, then $p = k \cdot 2^{m+2} + 1$.

Large Fermat Numbers:
1.2. Finding Factors

**Theorem:** (Euler 1747, Lucas 1879)
If a prime $p$ divides $F_m$, then $p = k \cdot 2^{m+2} + 1$.

**Large Fermat Numbers:**

- Use “Proth’s Theorem” to find a prime

\[ p = k \cdot 2^n + 1, \quad 2^n > k. \]
1.2. Finding Factors

**Theorem:** (Euler 1747, Lucas 1879)
If a prime $p$ divides $F_m$, then $p = k \cdot 2^{m+2} + 1$.

Large Fermat Numbers:

- Use “Proth’s Theorem" to find a prime

  $$p = k \cdot 2^n + 1, \quad 2^n > k.$$

- Having found such a prime $p$,
  “sieve", using the recurrence (mod $p$):

  $$F_{n+1} = (F_n - 1)^2 + 1.$$
"Small" Fermat Numbers \((m \leq 24)\):
Primality testing:

\[
F_m \text{ is prime iff } 3^{(F_m - 1)/2} \equiv -1 \pmod{F_m}.
\]

In practice: repeated squaring of 3.
Currently best method: "Discrete Weighted Transform" (DWT) (Crandall & Fagin, 1994); a variant of the Discrete Fourier Transform.

Latest primality results (i.e., proven composite):
• \(F_{20}\): Young & Buell, 1988 ("direct" FFT)
• \(F_{22}\): Crandall, Doenias, Norrie & Young and (independently) Trevisan & Carvalho, 1995 (DWT)
• \(F_{24}\): Crandall, Mayer & Papadopoulos, Sept., 1999 (DWT).
“Small” Fermat Numbers \((m \leq 24)\):
Primality testing:

**Theorem:** (Pepin, 1877)
\(F_m\) is prime iff \(3^{(F_m - 1)/2} \equiv -1 \pmod{F_m}\).

In practice: repeated squaring of 3.
Currently best method:
“Discrete Weighted Transform” (DWT) (Crandall & Fagin, 1994); a variant of the Discrete Fourier Transform.
Latest primality results (i.e., proven composite):
• \(F_{20}\): Young & Buell, 1988 (“direct” FFT)
• \(F_{22}\): Crandall, Doenias, Norrie & Young and (independently) Trevisan & Carvalho, 1995 (DWT)
• \(F_{24}\): Crandall, Mayer & Papadopoulos, Sept., 1999 (DWT).
“Small” Fermat Numbers \((m \leq 24)\):

Primality testing:

**Theorem:** (Pepin, 1877)

\(F_m\) is prime iff \(3^{(F_m-1)/2} \equiv -1 \pmod{F_m}\).

In practice: repeated squaring of 3.
“Small” Fermat Numbers ($m \leq 24$):
Primality testing:

**Theorem:** (Pepin, 1877)

$F_m$ is prime iff $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.

In practice: repeated squaring of 3.

Currently best method:
“Discrete Weighted Transform” (DWT) (Crandall & Fagin, 1994); a variant of the Discrete Fourier Transform.
“Small” Fermat Numbers \((m \leq 24)\):
Primality testing:

**Theorem:** (Pepin, 1877)
\[ F_m \text{ is prime iff } 3^{(F_m-1)/2} \equiv -1 \pmod{F_m}. \]

In practice: repeated squaring of 3.

Currently best method:
“Discrete Weighted Transform” (DWT) (Crandall & Fagin, 1994);
a variant of the Discrete Fourier Transform.

Latest primality results (i.e., proven composite):
“Small" Fermat Numbers \((m \leq 24)\):

Primality testing:

**Theorem:** (Pepin, 1877)

\[ F_m \text{ is prime iff } 3^{(F_m-1)/2} \equiv -1 \pmod{F_m}. \]

In practice: repeated squaring of 3.

Currently best method:

“Discrete Weighted Transform" (DWT) (Crandall & Fagin, 1994); a variant of the Discrete Fourier Transform.

Latest primality results (i.e., proven composite):

- \(F_{20}\): Young & Buell, 1988 ("direct" FFT)
“Small” Fermat Numbers \((m \leq 24)\):
Primality testing:

**Theorem:** (Pepin, 1877)
\(F_m\) is prime iff \(3^{(F_{m-1})/2} \equiv -1 \pmod{F_m}\).

In practice: repeated squaring of 3.

Currently best method:
“Discrete Weighted Transform” (DWT) (Crandall & Fagin, 1994); a variant of the Discrete Fourier Transform.

Latest primality results (i.e., proven composite):
- \(F_{20}\): Young & Buell, 1988 (“direct” FFT)
- \(F_{22}\): Crandall, Doenias, Norrie & Young and (independently) Trevisan & Carvalho, 1995 (DWT)
“Small” Fermat Numbers \((m \leq 24)\):
Primality testing:

**Theorem:** (Pepin, 1877)
\(F_m\) is prime iff \(3^{(F_m-1)/2} \equiv -1 \pmod{F_m}\).

In practice: repeated squaring of 3.

Currently best method:
“Discrete Weighted Transform” (DWT) (Crandall & Fagin, 1994); a variant of the Discrete Fourier Transform.

Latest primality results (i.e., proven composite):

- \(F_{20}\): Young & Buell, 1988 (“direct” FFT)
- \(F_{22}\): Crandall, Doenias, Norrie & Young and (independently) Trevisan & Carvalho, 1995 (DWT)
- \(F_{24}\): Crandall, Mayer & Papadopoulos, Sept., 1999 (DWT).
According to Richard Crandall, the computer power that went into
• proving $F_{22}$ composite, and
• producing “Toy Story"
(both in 1995) were roughly equivalent.
State of the art in 1996/97: Factors of “small” Fermat numbers:

- 27-d factor of $F_{13}$ (2467 digits)
- 33-d factor of $F_{15}$ (9865 digits)
- 27-d factor of $F_{16}$ (19729 digits)

(Using the Elliptic Curve Method, with large-integer arithmetic based on the Discrete Weighted Transform).

This was published in 2000 in Math. Comp. (R. Brent, R. Crandall, KD, and C. Van Halewyn. KD’s contribution was restricted to providing computing power).

Note: Yesterday I found the first of these factors in 28 minutes on a single core, using GMP-ECM.
1.2. Finding Factors (cont’d)

State of the art in 1996/97: Factors of “small" Fermat numbers:

- 27-d factor of $F_{13}$ (2467 digits)
- 33-d factor of $F_{15}$ (9865 digits)
- 27-d factor of $F_{16}$ (19729 digits)

(Using the Elliptic Curve Method, with large-integer arithmetic based on the Discrete Weighted Transform).

This was published in 2000 in Math. Comp. (R. Brent, R. Crandall, KD, and C. Van Halewyn. KD’s contribution was restricted to providing computing power).

Note: Yesterday I found the first of these factors in 28 minutes on a single core, using GMP-ECM.)
State of the art in 1996/97: Factors of “small" Fermat numbers:

- 27-d factor of $F_{13}$ (2467 digits)
- 33-d factor of $F_{15}$ (9865 digits)
- 27-d factor of $F_{16}$ (19729 digits)

(Using the Elliptic Curve Method, with large-integer arithmetic based on the Discrete Weighted Transform).
State of the art in 1996/97: Factors of “small” Fermat numbers:

- 27-d factor of $F_{13}$ (2467 digits)
- 33-d factor of $F_{15}$ (9865 digits)
- 27-d factor of $F_{16}$ (19729 digits)

(Using the Elliptic Curve Method, with large-integer arithmetic based on the Discrete Weighted Transform).

This was published in 2000 in Math. Comp. (R. Brent, R. Crandall, KD, and C. Van Halewyn. KD’s contribution was restricted to providing computing power).
State of the art in 1996/97: Factors of “small” Fermat numbers:

- 27-d factor of $F_{13}$ (2467 digits)
- 33-d factor of $F_{15}$ (9865 digits)
- 27-d factor of $F_{16}$ (19729 digits)

(Using the Elliptic Curve Method, with large-integer arithmetic based on the Discrete Weighted Transform).

This was published in 2000 in Math. Comp. (R. Brent, R. Crandall, KD, and C. Van Halewyn. KD’s contribution was restricted to providing computing power).

Note: Yesterday I found the first of these factors in 28 minutes on a single core, using GMP-ECM.
Define

\[ F_m(a) = a^{2^m} + 1. \]
Define

\[ F_m(a) = a^{2^m} + 1. \]

Again, odd prime factors must be of the form

\[ k \cdot 2^{m+1} + 1. \]
Define

\[ F_m(a) = a^{2^m} + 1. \]

Again, odd prime factors must be of the form

\[ k \cdot 2^{m+1} + 1. \]

- Many factors have been found by computation.
2. Generalized Fermat Numbers

Define

\[ F_m(a) = a^{2^m} + 1. \]

Again, odd prime factors must be of the form

\[ k \cdot 2^{m+1} + 1. \]

- Many factors have been found by computation.
- Some theoretical results are known (Riesel, 1969; Dubner & Keller, 1995; Björn & Riesel, 1998).
Define

\[ F_m(a) = a^{2^m} + 1. \]

Again, odd prime factors must be of the form

\[ k \cdot 2^{m+1} + 1. \]

- Many factors have been found by computation.
- Some theoretical results are known (Riesel, 1969; Dubner & Keller, 1995; Björn & Riesel, 1998).

A “typical" result:

**Theorem.** (Jiménez Calvo & KD, 1999)

If \( p = k \cdot 2^n + 1 \) a prime, \( k \) odd, \( n = \nu 2^\ell, \nu \geq 3 \) odd. If \( p \) divides the Fermat number \( F_m = 2^{2^m} + 1 \), then it also divides the GFN

\[ F_{m-\ell}(k) = k^{2^{m-\ell}} + 1. \]
Further generalization:

\[ F_m(a, b) = a^{2^m} + b^{2^m}, \quad \gcd(a, b) = 1. \]
Further generalization:

\[ F_m(a, b) = a^{2^m} + b^{2^m}, \quad \gcd(a, b) = 1. \]

- Analogue of Euler-Lucas theorem is known;
Further generalization:

\[ F_m(a, b) = a^{2^m} + b^{2^m}, \quad \gcd(a, b) = 1. \]

- Analogue of Euler-Lucas theorem is known;
- numerous factors have been found;
Further generalization:

\[ F_m(a, b) = a^{2^m} + b^{2^m}, \quad \gcd(a, b) = 1. \]

- Analogue of Euler-Lucas theorem is known;
- numerous factors have been found;
- some divisibility results are known.

Example:

\[ p = 3 \cdot 2^{382449} + 1 \] divides

\[ 3^{2^{382428}} + (2^{141839})^{2^{382428}}. \]
Further generalization:

\[ F_m(a, b) = a^{2^m} + b^{2^m}, \quad \gcd(a, b) = 1. \]

- Analogue of Euler-Lucas theorem is known;
- numerous factors have been found;
- some divisibility results are known.

**Example:**

\[ p = 3 \cdot 2^{382449} + 1 \]

divides

\[ 3^{2^{382428}} + (2^{141839})^{2^{382428}}. \]
We begin with *Wilson’s Theorem*: $p$ is a prime if and only if

$$(p - 1)! \equiv -1 \pmod{p}.$$
We begin with *Wilson’s Theorem*: $p$ is a prime if and only if

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

For a composite analogue we define the *Gauss factorial*

$$N_n! = \prod_{1 \leq j \leq N, \gcd(j, n) = 1} j \quad (N, n \in \mathbb{N})$$
We begin with *Wilson’s Theorem*: $p$ is a prime if and only if

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

For a composite analogue we define the *Gauss factorial*

$$N_n! = \prod_{1 \leq j \leq N, \gcd(j, n) = 1} j \quad (N, n \in \mathbb{N})$$

**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 $\alpha \geq 1$. 

### John B. Cosgrave and Karl Dilcher

**Generalized Fermat Numbers**
General long-term program: To study the Gauss factorials
\[ \left\lfloor \frac{n-1}{M} \right\rfloor n!, \quad M \geq 1, \quad n \equiv \pm 1 \pmod{M}, \]

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

Here:
- Given a fixed $M \geq 1$, we consider the question:
  - Which integers $n$ satisfy \( \left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n} \), \( n \equiv \pm 1 \pmod{M} \)?
  - Determined by Gauss-Wilson theorem.
  - $M = 2$: Completely determined (JBC & KD, 2008).
  - $M = 3, 4, 6$: Most interesting cases.
  - This talk will be about some aspects of these.
General long-term program: To study the Gauss factorials

\[ \left\lfloor \frac{n-1}{M} \right\rfloor, \quad M \geq 1, \quad n \equiv \pm 1 \pmod{M}, \]

in particular their multiplicative orders (mod n), but also, if possible, their values (mod n).
General long-term program: To study the Gauss factorials
\[ \left\lfloor \frac{n-1}{M} \right\rfloor n!, \quad M \geq 1, \quad n \equiv \pm 1 \pmod{M}, \]
in particular their multiplicative orders (mod n), but also, if possible, their values (mod n).

**Here:** given a fixed \( M \geq 1 \), we consider the question: which integers \( n \) satisfy
\[ \left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M} \]
General long-term program: To study the Gauss factorials

\[ \left\lfloor \frac{n-1}{M} \right\rfloor !, \quad M \geq 1, \quad n \equiv \pm 1 \pmod{M}, \]

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

**Here:** given a fixed \( M \geq 1 \), we consider the question: which integers \( n \) satisfy

\[ \left\lfloor \frac{n-1}{M} \right\rfloor ! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M} \]

- \( M = 1 \): Determined by Gauss-Wilson theorem.
- \( M = 2 \): Completely determined (JBC & KD, 2008).
- \( M = 3, 4, 6 \): Most interesting cases. This talk will be about some aspects of these.
General long-term program: To study the Gauss factorials

$$\left\lfloor \frac{n-1}{M} \right\rfloor n!, \quad M \geq 1, \quad n \equiv \pm 1 \pmod{M},$$

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

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

$$\left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}$$

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

John B. Cosgrave and Karl Dilcher

Generalized Fermat Numbers
General long-term program: To study the Gauss factorials

\[ \left\lfloor \frac{n-1}{M} \right\rfloor n!, \quad M \geq 1, \quad n \equiv \pm 1 \pmod{M}, \]

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

**Here:** given a fixed \( M \geq 1 \), we consider the question: which integers \( n \) satisfy

\[ \left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M} \]

- \( M = 1 \): Determined by Gauss-Wilson theorem.
- \( M = 2 \): Completely determined (JBC & KD, 2008).
- \( M = 3, 4, 6 \): Most interesting cases.
General long-term program: To study the Gauss factorials

\[ \left\lfloor \frac{n-1}{M} \right\rfloor_n! , \quad M \geq 1 , \quad n \equiv \pm 1 \pmod{M}, \]

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

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

\[ \left\lfloor \frac{n-1}{M} \right\rfloor_n! \equiv 1 \pmod{n} , \quad n \equiv \pm 1 \pmod{M} \]

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
- $M = 3, 4, 6$: Most interesting cases.
  - This talk will be about some aspects of these.
Different point of view: Consider again

\[ \left( \frac{n-1}{M} \right) n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}. \quad (1) \]
Different point of view: Consider again

\[ \left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}. \quad (1) \]

– 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

$$\left\lfloor \frac{n-1}{M} \right\rfloor_n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}. \quad (1)$$

– 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 $\left( \frac{n-1}{M} \right)_n! \pmod{n}$ is a divisor of $M$.

• Other partial products of the “full” product $\left( \frac{n-1}{M} \right)_n! \pmod{n}$ have also been studied (JBC & KD, 2013).
Different point of view: Consider again

\[
\left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm1 \pmod{M}. \tag{1}
\]

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

– If \( n \) has \textbf{two} different prime factors \( \equiv 1 \pmod{M} \),
then the order of \( \left( \frac{n-1}{M} \right) n! \pmod{n} \) is a divisor of \( M \).
In certain cases, solutions of (1) can be characterized.
Different point of view: Consider again

\[
\left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}. \quad (1)
\]

– 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 \( \left( \frac{n-1}{M} \right)n! \pmod{n} \) 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;
this talk will be about some specific aspects of this as well.
Different point of view: Consider again

\[ \left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}. \quad (1) \]

– 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 \( \left( \frac{n-1}{M} \right) n! \pmod{n} \) 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;
  this talk will be about some specific aspects of this as well.

– If \( n \) has no prime factor \( \equiv 1 \pmod{M} \):
  Very little can be said.
Different point of view: Consider again

\[ \left\lfloor \frac{n-1}{M} \right\rfloor_n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}. \quad (1) \]

– 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 \( \left( \frac{n-1}{M} \right)_n! \pmod{n} \) 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;
  this talk will be about some specific aspects of this as well.

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

• Other partial products of the “full" product \((n-1)_n!\) have also been studied (JBC & KD, 2013).
For which integers $n \equiv 1 \pmod{4}$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod{n}? \quad (2)$$

Obviously, this holds for $n = 5$. 

The next solutions:

$n = 205, 725, 1025, \text{ and } 1105$, 

with a total of 37109 solutions up to $10^{20}$.

Common property (except $n = 5$):

At least two distinct prime factors $\equiv 1 \pmod{4}$.

One might therefore conjecture that this is true in general. 

However, (2) does have solutions with $n \equiv 1 \pmod{4}$, 

$n$ having only one prime factor $p \equiv 1 \pmod{4}$.

Such solutions are exceedingly rare; only three up to $10^{20}$:

$\text{John B. Cosgrave and Karl Dilcher}$

Generalized Fermat Numbers
4. The case \( M = 4 \)

For which integers \( n \equiv 1 \pmod{4} \) do we have

\[
\left( \frac{n-1}{4} \right)_n! \equiv 1 \pmod{n}
\] (2)

Obviously, this holds for \( n = 5 \).
The next solutions: \( n = 205, 725, 1025, \) and 1105, with a total of 37109 solutions up to \( 10^6 \).
For which integers $n \equiv 1 \pmod{4}$ do we have

$$
\left( \frac{n-1}{4} \right)_n! \equiv 1 \pmod{n}
$$

(2)

Obviously, this holds for $n = 5$.
The next solutions: $n = 205, 725, 1025, \text{and} 1105$, with a total of 37109 solutions up to $10^6$.

Common property (except $n = 5$):
At least two distinct prime factors $\equiv 1 \pmod{4}$. 
For which integers \( n \equiv 1 \pmod{4} \) do we have

\[
\left( \frac{n-1}{4} \right)_n! \equiv 1 \pmod{n}
\] (2)

Obviously, this holds for \( n = 5 \).

The next solutions: \( n = 205, 725, 1025, \) and \( 1105 \), with a total of 37109 solutions up to \( 10^6 \).

Common property (except \( n = 5 \)):
At least two distinct prime factors \( \equiv 1 \pmod{4} \).

One might therefore conjecture that this is true in general.
4. The case $M = 4$

For which integers $n \equiv 1 \pmod{4}$ do we have

$$\left(\frac{n-1}{4}\right)_n! \equiv 1 \pmod{n} \tag{2}$$

Obviously, this holds for $n = 5$.

The next solutions: $n = 205, 725, 1025,$ and $1105$, with a total of 37109 solutions up to $10^6$.

Common property (except $n = 5$):
At least two distinct prime factors $\equiv 1 \pmod{4}$.

One might therefore conjecture that this is true in general.

However, (2) does have solutions with $n \equiv 1 \pmod{4}$, $n$ having only one prime factor $p \equiv 1 \pmod{4}$.
4. The case $M = 4$

For which integers $n \equiv 1 \pmod{4}$ do we have

$\left( \frac{n-1}{4} \right)_n! \equiv 1 \pmod{n}$? \hspace{1cm} (2)

Obviously, this holds for $n = 5$.
The next solutions: $n = 205, 725, 1025, \text{ and } 1105$, with a total of 37109 solutions up to $10^6$.

Common property (except $n = 5$):
At least two distinct prime factors $\equiv 1 \pmod{4}$.

One might therefore conjecture that this is true in general.

However, (2) does have solutions with $n \equiv 1 \pmod{4}$, $n$ having only one prime factor $p \equiv 1 \pmod{4}$.

Such solutions are exceedingly rare; only three up to $10^{20}$:
Table 1: The 3 smallest solutions of (2), $p \equiv 1 \pmod{4}$.
<table>
<thead>
<tr>
<th>$n$</th>
<th>$n$ factored</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>205479813</td>
<td>$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$</td>
<td>46817</td>
</tr>
<tr>
<td>1849318317</td>
<td>$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$</td>
<td>46817</td>
</tr>
<tr>
<td>233456083377</td>
<td>$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$</td>
<td>652081</td>
</tr>
</tbody>
</table>

**Table 1**: The 3 smallest solutions of (2), $p \equiv 1 \pmod{4}$.

How can we characterize such solutions?
<table>
<thead>
<tr>
<th></th>
<th>( n )</th>
<th>( n \txt{ factored} )</th>
<th>( p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>205479813</td>
<td>( 3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817 )</td>
<td>46817</td>
</tr>
<tr>
<td>2</td>
<td>1849318317</td>
<td>( 3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817 )</td>
<td>46817</td>
</tr>
<tr>
<td>3</td>
<td>233456083377</td>
<td>( 3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081 )</td>
<td>652081</td>
</tr>
</tbody>
</table>

**Table 1:** The 3 smallest solutions of (2), \( p \equiv 1 \pmod{4} \).

How can we characterize such solutions?

It turns out: the primes 46817 and 65281 play a special role; we will call them *Gauss primes*. 
Table 1: The 3 smallest solutions of (2), \( p \equiv 1 \pmod{4} \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( n ) factored</th>
<th>( p )</th>
</tr>
</thead>
<tbody>
<tr>
<td>205479813</td>
<td>( 3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817 )</td>
<td>46817</td>
</tr>
<tr>
<td>1849318317</td>
<td>( 3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817 )</td>
<td>46817</td>
</tr>
<tr>
<td>233456083377</td>
<td>( 3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081 )</td>
<td>652081</td>
</tr>
</tbody>
</table>

How can we characterize such solutions?

It turns out: the primes 46817 and 65281 play a special role; we will call them *Gauss primes*.

Also note (with prime factors \( \equiv 3 \pmod{4} \) in bold):

\[
\begin{align*}
46817 - 1 &= 2^5 \cdot 7 \cdot 11 \cdot 19, \\
46817 + 1 &= 2 \cdot 3^4 \cdot 17^2, \\
652081 - 1 &= 2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19, \\
652081 + 1 &= 2 \cdot 571^2.
\end{align*}
\]
Consider multiplicative orders:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\frac{p-1}{4}!\pmod{(p)}$</th>
<th>order</th>
<th>$p$</th>
<th>$\frac{p-1}{4}!\pmod{(p)}$</th>
<th>order</th>
<th>$p$</th>
<th>$\frac{p-1}{4}!\pmod{(p)}$</th>
<th>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>97</td>
<td>20</td>
<td>32</td>
<td>197</td>
<td>92</td>
<td>98</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>12</td>
<td>101</td>
<td>46</td>
<td>100</td>
<td>229</td>
<td>168</td>
<td>38</td>
</tr>
<tr>
<td>17</td>
<td>7</td>
<td>16</td>
<td>109</td>
<td>7</td>
<td>27</td>
<td>233</td>
<td>36</td>
<td>116</td>
</tr>
<tr>
<td>29</td>
<td>23</td>
<td>7</td>
<td>113</td>
<td>32</td>
<td>28</td>
<td>241</td>
<td>130</td>
<td>16</td>
</tr>
<tr>
<td>37</td>
<td>21</td>
<td>18</td>
<td>137</td>
<td>90</td>
<td>136</td>
<td>257</td>
<td>120</td>
<td>32</td>
</tr>
<tr>
<td>41</td>
<td>13</td>
<td>40</td>
<td>149</td>
<td>23</td>
<td>148</td>
<td>269</td>
<td>258</td>
<td>67</td>
</tr>
<tr>
<td>53</td>
<td>26</td>
<td>52</td>
<td>157</td>
<td>145</td>
<td>6</td>
<td>277</td>
<td>221</td>
<td>276</td>
</tr>
<tr>
<td>61</td>
<td>19</td>
<td>30</td>
<td>173</td>
<td>40</td>
<td>86</td>
<td>281</td>
<td>157</td>
<td>28</td>
</tr>
<tr>
<td>73</td>
<td>18</td>
<td>18</td>
<td>181</td>
<td>3</td>
<td>45</td>
<td>293</td>
<td>69</td>
<td>73</td>
</tr>
<tr>
<td>89</td>
<td>22</td>
<td>22</td>
<td>193</td>
<td>89</td>
<td>64</td>
<td>313</td>
<td>109</td>
<td>312</td>
</tr>
</tbody>
</table>

Table 2: The first 30 primes $p \equiv 1 \pmod{4}$. 
Consider multiplicative orders:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\frac{p-1}{4} ! (p)$</th>
<th>order</th>
<th>$p$</th>
<th>$\frac{p-1}{4} ! (p)$</th>
<th>order</th>
<th>$p$</th>
<th>$\frac{p-1}{4} ! (p)$</th>
<th>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>97</td>
<td>20</td>
<td>32</td>
<td>197</td>
<td>92</td>
<td>98</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>12</td>
<td>101</td>
<td>46</td>
<td>100</td>
<td>229</td>
<td>168</td>
<td>38</td>
</tr>
<tr>
<td>17</td>
<td>7</td>
<td>16</td>
<td>109</td>
<td>7</td>
<td>27</td>
<td>233</td>
<td>36</td>
<td>116</td>
</tr>
<tr>
<td>29</td>
<td>23</td>
<td>7</td>
<td>113</td>
<td>32</td>
<td>28</td>
<td>241</td>
<td>130</td>
<td>16</td>
</tr>
<tr>
<td>37</td>
<td>21</td>
<td>18</td>
<td>137</td>
<td>90</td>
<td>136</td>
<td>257</td>
<td>120</td>
<td>32</td>
</tr>
<tr>
<td>41</td>
<td>13</td>
<td>40</td>
<td>149</td>
<td>23</td>
<td>148</td>
<td>269</td>
<td>258</td>
<td>67</td>
</tr>
<tr>
<td>53</td>
<td>26</td>
<td>52</td>
<td>157</td>
<td>145</td>
<td>6</td>
<td>277</td>
<td>221</td>
<td>276</td>
</tr>
<tr>
<td>61</td>
<td>19</td>
<td>30</td>
<td>173</td>
<td>40</td>
<td>86</td>
<td>281</td>
<td>157</td>
<td>28</td>
</tr>
<tr>
<td>73</td>
<td>18</td>
<td>18</td>
<td>181</td>
<td>3</td>
<td>45</td>
<td>293</td>
<td>69</td>
<td>73</td>
</tr>
<tr>
<td>89</td>
<td>22</td>
<td>22</td>
<td>193</td>
<td>89</td>
<td>64</td>
<td>313</td>
<td>109</td>
<td>312</td>
</tr>
</tbody>
</table>

**Table 2**: The first 30 primes $p \equiv 1 \pmod{4}$.

Note: Orders appear to be unbounded – many primitive roots.
Consider multiplicative orders:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\frac{p-1}{4}!(p)$</th>
<th>order</th>
<th>$p$</th>
<th>$\frac{p-1}{4}!(p)$</th>
<th>order</th>
<th>$p$</th>
<th>$\frac{p-1}{4}!(p)$</th>
<th>order</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1</td>
<td>1</td>
<td>97</td>
<td>20</td>
<td>32</td>
<td>197</td>
<td>92</td>
<td>98</td>
</tr>
<tr>
<td>13</td>
<td>6</td>
<td>12</td>
<td>101</td>
<td>46</td>
<td>100</td>
<td>229</td>
<td>168</td>
<td>38</td>
</tr>
<tr>
<td>17</td>
<td>7</td>
<td>16</td>
<td>109</td>
<td>7</td>
<td>27</td>
<td>233</td>
<td>36</td>
<td>116</td>
</tr>
<tr>
<td>29</td>
<td>23</td>
<td>7</td>
<td>113</td>
<td>32</td>
<td>28</td>
<td>241</td>
<td>130</td>
<td>16</td>
</tr>
<tr>
<td>37</td>
<td>21</td>
<td>18</td>
<td>137</td>
<td>90</td>
<td>136</td>
<td>257</td>
<td>120</td>
<td>32</td>
</tr>
<tr>
<td>41</td>
<td>13</td>
<td>40</td>
<td>149</td>
<td>23</td>
<td>148</td>
<td>269</td>
<td>258</td>
<td>67</td>
</tr>
<tr>
<td>53</td>
<td>26</td>
<td>52</td>
<td>157</td>
<td>145</td>
<td>6</td>
<td>277</td>
<td>221</td>
<td>276</td>
</tr>
<tr>
<td>61</td>
<td>19</td>
<td>30</td>
<td>173</td>
<td>40</td>
<td>86</td>
<td>281</td>
<td>157</td>
<td>28</td>
</tr>
<tr>
<td>73</td>
<td>18</td>
<td>18</td>
<td>181</td>
<td>3</td>
<td>45</td>
<td>293</td>
<td>69</td>
<td>73</td>
</tr>
<tr>
<td>89</td>
<td>22</td>
<td>22</td>
<td>193</td>
<td>89</td>
<td>64</td>
<td>313</td>
<td>109</td>
<td>312</td>
</tr>
</tbody>
</table>

**Table 2**: The first 30 primes $p \equiv 1 \pmod{4}$.

Note: Orders appear to be unbounded – many primitive roots.

Of particular interest here: Orders that are powers of 2 (in bold).
Definition

Let $p$ be a prime with $p \equiv 1 \pmod{4}$. If

$$\text{ord}_p \left( \frac{p-1}{4} ! \right) = 2^\ell$$

for some $\ell \geq 0$,

we say that $p$ is a Gauss prime of level $\ell$. 

Why "Gauss prime"? Recall:

Theorem (Gauss, 1828)

Let the prime $p \equiv 1 \pmod{4}$ be written as $p = a^2 + b^2$, and choose the sign of $a$ such that $a \equiv 1 \pmod{4}$. Then

$$\left( \frac{p-1}{2p-1} \right)_p \equiv 2^\ell \pmod{p}.$$ 

This turns out to be essential in the study and applications of Gauss primes.
Definition

Let $p$ be a prime with $p \equiv 1 \pmod{4}$. If

$$\text{ord}_p\left(\frac{p-1}{4}!\right) = 2^\ell \quad \text{for some } \ell \geq 0,$$

we say that $p$ is a Gauss prime of level $\ell$.

Why “Gauss prime”? Recall:
Definition

Let $p$ be a prime with $p \equiv 1 \pmod{4}$. If

$$\text{ord}_p\left(\frac{p-1}{4}!\right) = 2^\ell$$

for some $\ell \geq 0$, we say that $p$ is a Gauss prime of level $\ell$.

Why “Gauss prime”? Recall:

Theorem (Gauss, 1828)

Let the prime $p \equiv 1 \pmod{4}$ be written as $p = a^2 + b^2$, and choose the sign of $a$ such that $a \equiv 1 \pmod{4}$. Then

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

Let $p$ be a prime with $p \equiv 1 \pmod{4}$. If

$$\text{ord}_p\left(\frac{p-1}{4}!ight) = 2^\ell \quad \text{for some } \ell \geq 0,$$

we say that $p$ is a Gauss prime of level $\ell$.

Why “Gauss prime”? Recall:

Theorem (Gauss, 1828)

Let the prime $p \equiv 1 \pmod{4}$ be written as $p = a^2 + b^2$, and choose the sign of $a$ such that $a \equiv 1 \pmod{4}$. Then

$$\left(\frac{p-1}{2} \mid \frac{p-1}{4}\right) \equiv 2a \pmod{p}.$$

This turns out to be essential in the study and applications of Gauss primes.
Theorem

Let \( p \equiv 1 \pmod{4} \) be a prime. Then the order of \( \frac{p-1}{4}! \mod p \)
(a) is 1 if and only if \( p = 5 \);
(b) cannot be 2, 4, or 8;
(b) is 16 if and only if \( p - 1 = 4ab \), where \( p = a^2 + b^2 \), \( a, b > 0 \).
Theorem

Let \( p \equiv 1 \pmod{4} \) be a prime. Then the order of \( \frac{p-1}{4}! \pmod{p} \)

(a) is 1 if and only if \( p = 5 \);
(b) cannot be 2, 4, or 8;
(b) is 16 if and only if \( p - 1 = 4ab \), where \( p = a^2 + b^2 \), \( a, b > 0 \).

More can be said about this last case:

Corollary

A prime \( p \equiv 1 \pmod{4} \) is a level-4 Gauss prime, i.e.,

\[
\left( \frac{p-1}{4}! \right)^8 \equiv -1 \pmod{p},
\]

if and only if \( p = p_k := a_{k+1}^2 + a_k^2 \) for some \( k \geq 1 \), where

\[
a_0 = 0, \quad a_1 = 1, \quad a_k = 4a_{k-1} - a_{k-2}.
\]
The first few values of $a_k$ and $p_k$:

<table>
<thead>
<tr>
<th>$k$</th>
<th>$a_k$</th>
<th>$p_k$</th>
<th>prime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>17</td>
<td>yes</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>241</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>3361</td>
<td>yes</td>
</tr>
<tr>
<td>4</td>
<td>56</td>
<td>46817</td>
<td>yes</td>
</tr>
<tr>
<td>5</td>
<td>209</td>
<td>652081</td>
<td>yes</td>
</tr>
<tr>
<td>6</td>
<td>780</td>
<td>9082321</td>
<td>no</td>
</tr>
</tbody>
</table>
The first few values of $a_k$ and $p_k$:

<table>
<thead>
<tr>
<th>$k$</th>
<th>$a_k$</th>
<th>$p_k$</th>
<th>prime</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>17</td>
<td>yes</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>241</td>
<td>yes</td>
</tr>
<tr>
<td>3</td>
<td>15</td>
<td>3361</td>
<td>yes</td>
</tr>
<tr>
<td>4</td>
<td>56</td>
<td>46817</td>
<td>yes</td>
</tr>
<tr>
<td>5</td>
<td>209</td>
<td>652081</td>
<td>yes</td>
</tr>
<tr>
<td>6</td>
<td>780</td>
<td>9082321</td>
<td>no</td>
</tr>
</tbody>
</table>

$p_k$ is composite for $6 \leq k \leq 100\,000$, with the exception of:

- $k = 131, 200, 296, 350, 519, 704, 950, 5\,598, 6\,683, 7\,445, 8\,775, 8\,786, 11\,565, 12\,483$;
  (all proven prime by F. Morain – elliptic curve primality test).

- $k = 13\,536, 18\,006, 18\,995, 48\,773,$ and $93\,344$.
  (PARI: probable primes).
There is no apparent structure for levels $\ell \geq 5$. 
There is no apparent structure for levels $\ell \geq 5$.

However, it is easy to show by way of Gauss’ Binomial Coefficient Theorem:

**Corollary**

If $F_n$ is a Fermat prime, then for $n \geq 2$ the multiplicative order of $((F_n - 1)/4)!$ modulo $F_n$ is $2^{n+2}$. 
There is no apparent structure for levels $\ell \geq 5$.

However, it is easy to show by way of Gauss’ Binomial Coefficient Theorem:

**Corollary**

If $F_n$ is a Fermat prime, then for $n \geq 2$ the multiplicative order of $((F_n - 1)/4)!$ modulo $F_n$ is $2^{n+2}$.

In other words, $F_n$ is a Gauss prime of level $n + 2$. 
There is no apparent structure for levels $\ell \geq 5$.

However, it is easy to show by way of Gauss’ Binomial Coefficient Theorem:

**Corollary**

If $F_n$ is a Fermat prime, then for $n \geq 2$ the multiplicative order of $\left( (F_n - 1)/4 \right)!$ modulo $F_n$ is $2^{n+2}$.

In other words, $F_n$ is a Gauss prime of level $n + 2$.

The following is the main result in the case $M = 4$: 
Suppose that
\[ n = p q_1^{\beta_1} \cdots q_r^{\beta_r} \]
with \( p \equiv 1 \pmod{4} \) and \( q_j \equiv -1 \pmod{4} \) distinct primes.
Theorem

Suppose that

\[ n = p q_1^{\beta_1} \cdots q_r^{\beta_r} \]

with \( p \equiv 1 \pmod{4} \) and \( q_j \equiv -1 \pmod{4} \) distinct primes. Then

\[ \left\lfloor \frac{n - 1}{4} \right\rfloor \frac{n!}{n} \equiv 1 \pmod{n} \]  \hspace{1cm} (3)

is impossible for \( r = 1, 2 \) or \( 3 \).
Theorem

Suppose that

\[ n = p q_1^{\beta_1} \cdots q_r^{\beta_r} \]

with \( p \equiv 1 \pmod{4} \) and \( q_j \equiv -1 \pmod{4} \) distinct primes. Then

\[ \left\lfloor \frac{n - 1}{4} \right\rfloor \quad \text{is impossible for } r = 1, 2 \text{ or } 3. \quad \text{Otherwise, (3) holds iff} \]

(i) \( \text{ord}_p \left( \frac{p - 1}{4} \right)! = 2^\ell \quad \text{for some } \ell \geq 4; \)

(ii) \( q_j^{\beta_j} \mid (p - 1) \text{ or } (p + 1); \)

(iii) \( r \geq \ell. \)

(Note: This is a somewhat simplified version).
● 26 Gauss primes with $5 \leq \ell \leq 18$ have been found. None of them satisfy $r \geq \ell$. 

When $\ell = 4$:

- $p_4 = 46817$ is the smallest with the necessary $r = 4$ primes $q_j | p \pm 1$.

- Another example: $p_{131} = 881218785186320224738518516256503796205310883044356986457857324150680203969199260511507595926468857084114007285544744995271784268717820573108544336161$ (150 digits) has 14 factors $q_j$, from 3 to 14036878282733744060263105174260179, two with multiplicity 2.

- The largest example we could write down has 14 412 digits.
• 26 Gauss primes with $5 \leq \ell \leq 18$ have been found. None of them satisfy $r \geq \ell$.

When $\ell = 4$:

• $p_4 = 46,817$ is the smallest with the necessary
  $r = 4$ primes $q_j \mid p \pm 1$. 
• 26 Gauss primes with $5 \leq \ell \leq 18$ have been found.
  None of them satisfy $r \geq \ell$.

When $\ell = 4$:

• $p_4 = 46,817$ is the smallest with the necessary $r = 4$ primes $q_j | p \pm 1$.

• Another example: $p_{131} =$
  88121878518632022473851851625650379620531088304435
  69864578573241506802039691992605115075959264688570
  84114007285544744995271784268717820573108544336161
  (150 digits)

  14 factors $q_j$,
  from 3 to 14036878282733744060263105174260179,
  two with multiplicity 2.
• 26 Gauss primes with $5 \leq \ell \leq 18$ have been found. None of them satisfy $r \geq \ell$.

When $\ell = 4$:

• $p_4 = 46\,817$ is the smallest with the necessary $r = 4$ primes $q_j | p \pm 1$.

• Another example: $p_{131} =$
88121878518632022473851851625650379620531088304435
69864578573241506802039691992605115075959264688570
84114007285544744995271784268717820573108544336161
(150 digits)

14 factors $q_j$, from 3 to 14036878282733744060263105174260179, two with multiplicity 2.

• The largest example we could write down has 14 412 digits.
"You know, most people's favourite number is 7, but mine is 627399010364332991004825304810385572229571004927401015482947738885917389."
Setting the stage: We’ll consider integers of the form

\[ n = p^\alpha w, \quad \text{with} \quad w = q_1^{\beta_1} \cdots q_s^{\beta_s} \]

\((s \geq 0, \alpha, \beta_1, \ldots, \beta_s \in \mathbb{N})\), 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

\[ n = p^{\alpha}w, \quad \text{with} \quad w = q_1^{\beta_1} \cdots q_s^{\beta_s} \]

\((s \geq 0, \alpha, \beta_1, \ldots, \beta_s \in \mathbb{N})\), 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

\[ \left\lfloor \frac{n-1}{3} \right\rfloor n! \equiv 1 \pmod{n}, \quad (4) \]

or

\[ \left\lfloor \frac{n-1}{6} \right\rfloor n! \equiv 1 \pmod{n}. \quad (5) \]
First few solutions of
\[ \left\lfloor \frac{n-1}{3} \right\rfloor n! \equiv 1 \pmod{n}, \quad \left\lfloor \frac{n-1}{6} \right\rfloor n! \equiv 1 \pmod{n}: \]

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

How can we characterize these solutions?

Let's consider some specific \( p \equiv 1 \pmod{3}. \)
First few solutions of \( \left\lfloor \frac{n-1}{3} \right\rfloor \cdot n! \equiv 1 \pmod{n}, \quad \left\lfloor \frac{n-1}{6} \right\rfloor \cdot n! \equiv 1 \pmod{n}: \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>factored</th>
<th>( n )</th>
<th>factored</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>2 \cdot 13</td>
<td>1105</td>
<td>5 \cdot 13 \cdot 17</td>
</tr>
<tr>
<td>244</td>
<td>2^2 \cdot 61</td>
<td>14365</td>
<td>5 \cdot 13^2 \cdot 17</td>
</tr>
<tr>
<td>305</td>
<td>5 \cdot 61</td>
<td>34765</td>
<td>5 \cdot 17 \cdot 409</td>
</tr>
<tr>
<td>338</td>
<td>2 \cdot 13^2</td>
<td>303535</td>
<td>5 \cdot 17 \cdot 3571</td>
</tr>
<tr>
<td>9755</td>
<td>5 \cdot 1951</td>
<td>309485</td>
<td>5 \cdot 11 \cdot 17 \cdot 331</td>
</tr>
<tr>
<td>18205</td>
<td>5 \cdot 11 \cdot 331</td>
<td>353365</td>
<td>5 \cdot 29 \cdot 2437</td>
</tr>
<tr>
<td>33076</td>
<td>2^2 \cdot 8269</td>
<td>508255</td>
<td>5 \cdot 11 \cdot 9241</td>
</tr>
<tr>
<td>48775</td>
<td>5^2 \cdot 1951</td>
<td>510605</td>
<td>5 \cdot 102121</td>
</tr>
<tr>
<td>60707</td>
<td>17 \cdot 3571</td>
<td>527945</td>
<td>5 \cdot 11 \cdot 29 \cdot 331</td>
</tr>
</tbody>
</table>

In bold: \( p \equiv 1 \pmod{3} \).
First few solutions of
\[
\left\lfloor \frac{n-1}{3} \right\rfloor n! \equiv 1 \pmod{n}, \quad \left\lfloor \frac{n-1}{6} \right\rfloor n! \equiv 1 \pmod{n}:
\]

<table>
<thead>
<tr>
<th>(n)</th>
<th>factored</th>
<th>(n)</th>
<th>factored</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>2 \cdot 13</td>
<td>1105</td>
<td>5 \cdot 13 \cdot 17</td>
</tr>
<tr>
<td>244</td>
<td>2^2 \cdot 61</td>
<td>14365</td>
<td>5 \cdot 13^2 \cdot 17</td>
</tr>
<tr>
<td>305</td>
<td>5 \cdot 61</td>
<td>34765</td>
<td>5 \cdot 17 \cdot 409</td>
</tr>
<tr>
<td>338</td>
<td>2 \cdot 13^2</td>
<td>303535</td>
<td>5 \cdot 17 \cdot 3571</td>
</tr>
<tr>
<td>9755</td>
<td>5 \cdot 1951</td>
<td>309485</td>
<td>5 \cdot 11 \cdot 17 \cdot 331</td>
</tr>
<tr>
<td>18205</td>
<td>5 \cdot 11 \cdot 331</td>
<td>353365</td>
<td>5 \cdot 29 \cdot 2437</td>
</tr>
<tr>
<td>33076</td>
<td>2^2 \cdot 8269</td>
<td>508255</td>
<td>5 \cdot 11 \cdot 9241</td>
</tr>
<tr>
<td>48775</td>
<td>5^2 \cdot 1951</td>
<td>510605</td>
<td>5 \cdot 102121</td>
</tr>
<tr>
<td>60707</td>
<td>17 \cdot 3571</td>
<td>527945</td>
<td>5 \cdot 11 \cdot 29 \cdot 331</td>
</tr>
</tbody>
</table>

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

How can we characterize these solutions?
First few solutions of

\[
\left\lfloor \frac{n-1}{3} \right\rfloor n! \equiv 1 \pmod{n}, \quad \left\lfloor \frac{n-1}{6} \right\rfloor n! \equiv 1 \pmod{n}:
\]

<table>
<thead>
<tr>
<th>n</th>
<th>factored</th>
<th>n</th>
<th>factored</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>2 \cdot 13</td>
<td>1105</td>
<td>5 \cdot 13 \cdot 17</td>
</tr>
<tr>
<td>244</td>
<td>2^2 \cdot 61</td>
<td>14365</td>
<td>5 \cdot 13^2 \cdot 17</td>
</tr>
<tr>
<td>305</td>
<td>5 \cdot 61</td>
<td>34765</td>
<td>5 \cdot 17 \cdot 409</td>
</tr>
<tr>
<td>338</td>
<td>2 \cdot 13^2</td>
<td>303535</td>
<td>5 \cdot 17 \cdot 3571</td>
</tr>
<tr>
<td>9755</td>
<td>5 \cdot 1951</td>
<td>309485</td>
<td>5 \cdot 11 \cdot 17 \cdot 331</td>
</tr>
<tr>
<td>18205</td>
<td>5 \cdot 11 \cdot 331</td>
<td>353365</td>
<td>5 \cdot 29 \cdot 2437</td>
</tr>
<tr>
<td>33076</td>
<td>2^2 \cdot 8269</td>
<td>508255</td>
<td>5 \cdot 11 \cdot 9241</td>
</tr>
<tr>
<td>48775</td>
<td>5^2 \cdot 1951</td>
<td>510605</td>
<td>5 \cdot 102121</td>
</tr>
<tr>
<td>60707</td>
<td>17 \cdot 3571</td>
<td>527945</td>
<td>5 \cdot 11 \cdot 29 \cdot 331</td>
</tr>
</tbody>
</table>

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

$$n = p^\alpha q_1^{\beta_1} \ldots q_s^{\beta_s}.$$
Example. Let \( p = 7 \), the smallest admissible \( p \) in

\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

(a) Solutions of \( \left\lfloor \frac{n-1}{3} \right\rfloor \equiv 1 \pmod{n} \):
Example. Let $p = 7$, the smallest admissible $p$ in

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

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

Combination of theory and computation shows:

- For $s = 0, 1, \ldots, 6$: no solutions.
Example. Let $p = 7$, the smallest admissible $p$ in

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

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

Combination of theory and computation shows:

- For $s = 0, 1, \ldots, 6$: no solutions.
- For $s = 7$: exactly 27 solutions, the smallest and largest of which are

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

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

with 30 and 36 decimal digits, respectively.
\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.
- For \( s = 6 \): single 40-digit solution
  \[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]

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?
\[ n = p^\alpha q_1^{\beta_1} \ldots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.
- For \( s = 6 \): single 40-digit solution
  \[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]
\[ n = p^{\alpha} q_1^{\beta_1} \ldots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.

For \( s = 6 \): single 40-digit solution
\[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]
\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.
- For \( s = 6 \): single 40-digit solution
  \[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]
\[ n = p^\alpha q_1^{\beta_1} \ldots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.
- For \( s = 6 \): single 40-digit solution
  \[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]

Questions:

(i) What determines presence/absence of solutions?
\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.
- For \( s = 6 \): single 40-digit solution \( n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833 \).

Questions:

(i) What determines presence/absence of solutions?

(ii) What are the factors \( q_j \) when solutions exist?
\[ n = p^\alpha q_1^{\beta_1} \ldots q_s^{\beta_s}. \]

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

- For \( s = 0 \): trivial solution \( n = 7 \).
- For \( s = 1, \ldots, 6 \): no solutions.
- For \( s = 6 \): single 40-digit solution
  \[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]

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

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

\[
\ldots
\]

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

**For** $M = 6$:

$n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833.$
The solutions, again: For $M = 3$:

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

$\ldots$

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

For $M = 6$:

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

Note:

$5 \mid 7^2 + 1,$

$17 \mid 7^3 + 1$ and $169553 \mid 7^3 + 1,$

$353 \mid 7^4 + 1$ and $47072139617 \mid 7^4 + 1,$

$7699649 \mid 7^5 + 1$ and $531968664833 \mid 7^5 + 1.$
The solutions, again: For $M = 3$:

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

$$\ldots$$

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

For $M = 6$:

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

Note:

$$5 \mid 7^2 + 1,$$

$$17 \mid 7^3 + 1 \quad \text{and} \quad 169553 \mid 7^3 + 1,$$

$$353 \mid 7^4 + 1 \quad \text{and} \quad 47072139617 \mid 7^4 + 1,$$

$$7699649 \mid 7^5 + 1 \quad \text{and} \quad 531968664833 \mid 7^5 + 1.$$

Also: $7^{2^2} + 1$ has no prime factor $q \equiv -1 \pmod{3}$;
The solutions, again: For $M = 3$:

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

\[ \ldots \]

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

For $M = 6$:

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

Note:

\[
\begin{align*}
5 & \mid 7^2 + 1, \\
17 & \mid 7^3 + 1 \quad \text{and} \quad 169553 \mid 7^3 + 1, \\
353 & \mid 7^4 + 1 \quad \text{and} \quad 47072139617 \mid 7^4 + 1, \\
7699649 & \mid 7^5 + 1 \quad \text{and} \quad 531968664833 \mid 7^5 + 1.
\end{align*}
\]

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

\[
(7 - 1)(7 + 1)(7^{2^1} + 1) \ldots (7^{2^5} + 1).
\]
6. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

i.e., necessary conditions for the original congruences. For simplicity, here:

- Denominator \(M = 3\);
- The case \(s \geq 2\), where \(n = p^\alpha w\), \(w = q^\beta_1 \ldots q^\beta_s\);
- \(w \equiv 1 \pmod 3\), i.e., \(n \equiv 1 \pmod 3\).

Main approach: Find criteria for

\[
\left\lfloor \frac{n-1}{3} \right\rfloor n!^3 \equiv 1 \pmod w \quad \text{and} \quad \left\lfloor \frac{n-1}{6} \right\rfloor n!^3 \equiv 1 \pmod p^\alpha;
\]

then combine the two using the Chinese Remainder Theorem.
6. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

i.e., necessary conditions for the original congruences.
6. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

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

For simplicity, here: Restrict our attention to

- denominator \(M = 3\);
- the case \(s \geq 2\), where \(n = p^\alpha w, \ w = q_1^{\beta_1} \cdots q_s^{\beta_s}\),
- \(w \equiv 1 \pmod{3}\), i.e., \(n \equiv 1 \pmod{3}\).
6. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

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

For simplicity, here: Restrict our attention to

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

**Main approach:** Find criteria for

\[ \left\lfloor \frac{n-1}{3} \right\rfloor n!^3 \equiv 1 \pmod{w} \quad \text{and} \quad \left\lfloor \frac{n-1}{3} \right\rfloor n!^3 \equiv 1 \pmod{p^\alpha}; \]
6. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

\[ \left\lfloor \frac{n-1}{3} \right\rfloor n!^3 \equiv 1 \pmod{n} \] and \[ \left\lfloor \frac{n-1}{6} \right\rfloor n!^3 \equiv 1 \pmod{n}, \]

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

For simplicity, here: Restrict our attention to

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

**Main approach:** Find criteria for

\[ \left\lfloor \frac{n-1}{3} \right\rfloor n!^3 \equiv 1 \pmod{w} \] and \[ \left\lfloor \frac{n-1}{3} \right\rfloor n!^3 \equiv 1 \pmod{p^\alpha}; \]

then combine the two using the Chinese Remainder Theorem.
7. Generalized Fermat numbers

Congruences modulo \( w \):

We define the partial totient function

\[
\varphi(M, w) = \#\{\tau | 1 \leq \tau \leq \frac{w-1}{M}, \gcd(\tau, w) = 1\}.
\]
7. Generalized Fermat numbers

**Congruences modulo** $w$:

We define the partial totient function

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

**Lemma**

*With $n$ as before, we have*

$$\left( \frac{n-1}{3} \right)_n ! \equiv \frac{1}{p^{\varphi(3,w)}} \pmod{w}, \quad \varphi(3, w) = \frac{1}{3}(\varphi(w) + 2^{s-1}).$$
7. Generalized Fermat numbers

Congruences modulo $w$:

We define the partial totient function

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

Lemma

With $n$ as before, we have

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

Proof is very technical. Basic idea: Write

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

(slightly different when $n \equiv -1 \pmod{3}$).
\[
\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.
\]

This means:

\[
\left\lfloor \frac{n-1}{3} \right\rfloor_n! \text{ is a product of}
\]

\[
\begin{cases}
\frac{p^\alpha - 1}{3} \text{ "main terms"}, \text{ and} \\
\text{one "remainder term".}
\end{cases}
\]
\[
\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.
\]

This means:

\[
\left\lfloor \frac{n-1}{3} \right\rfloor n! \text{ is a product of }
\]

\[
\left\{ \begin{array}{l}
\frac{p^\alpha - 1}{3} \text{ "main terms", and } \\
\text{one "remainder term".}
\end{array} \right.
\]

- 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:

\[
\lfloor \frac{n-1}{3} \rfloor n! \text{ is a product of }
\]

\[
\left\{ \begin{array}{l}
p^\alpha - 1 \text{ "main terms"}, \\
\text{and}
\end{array} \right.
\]

\[
\left\{ \begin{array}{l}
\frac{w - 1}{3} \text{ one "remainder term"}. \\
\end{array} \right.
\]

- 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:

\[ \left\lfloor \frac{n-1}{3} \right\rfloor n! \] is a product of

\[ \left\{ \frac{p^\alpha - 1}{3} \right\} \text{ "main terms", and} \]
\[ \text{one "remainder term".} \]

- 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 \( M \geq 2 \).
Now we can see how generalized Fermat numbers enter:

Raise both sides of Lemma to 3rd power.

Then

\[
\left(\frac{n-1}{3}\right)_n!^3 \equiv p^{-\varphi(w)-2^{s-1}} \equiv p^{-2^{s-1}} \pmod{w}, \quad \delta = \pm 1.
\]
Now we can see how generalized Fermat numbers enter:

Raise both sides of Lemma to 3rd power.

Then

\[
\left( \frac{n-1}{3} \right)_n!^3 \equiv p^{-\varphi(w)-2s-1} \equiv p^{-2s-1} \pmod{w}, \quad \delta = \pm 1.
\]

Therefore

\[
\left( \frac{n-1}{3} \right)_n!^3 \equiv 1 \pmod{w}
\]

if and only if

\[
p^{2s-1} - 1 \equiv 0 \pmod{w}.
\]
Now we can see how generalized Fermat numbers enter:

Raise both sides of Lemma to 3rd power.

Then

\[
\left( \frac{n-1}{3} \right)_n!^3 \equiv p^{-\varphi(w) - 2^{s-1}} \equiv p^{-2^{s-1}} \quad (\text{mod } w), \quad \delta = \pm 1.
\]

Therefore

\[
\left( \frac{n-1}{3} \right)_n!^3 \equiv 1 \quad (\text{mod } w)
\]

if and only if

\[
p^{2^{s-1}} - 1 \equiv 0 \quad (\text{mod } w).
\]

This factors:

\[
p^{2^{s-1}} - 1 = (p - 1)(p + 1)(p^2 + 1) \ldots (p^{2^{s-2}} + 1).
\]
We have therefore shown:

**Proposition**

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

\[
\left( \frac{n-1}{3} \right)^3 !^3 \equiv 1 \quad \text{(mod } w)\]

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

$q_i^{\beta_i}$ divides \[\begin{cases} p - 1, & \text{for } s = 1, \\ (p - 1)(p + 1)(p^2 + 1) \ldots (p^{2^{s-2}} + 1), & \text{for } s \geq 2. \end{cases}\]
We have therefore shown:

**Proposition**

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

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

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

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

**Note:** This is in fact true for

$$\left\lfloor \frac{n-1}{3} \right\rfloor n! \equiv 1 \pmod{w}.$$
8. Jacobi primes

Congruences modulo $p^\alpha$:

The following is the second crucial ingredient.

**Lemma**

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

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

Congruences modulo $p^\alpha$:

The following is the second crucial ingredient.

**Lemma**

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

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

Once again:

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

Congruences modulo $p^\alpha$:

The following is the second crucial ingredient.

**Lemma**

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

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

Once again:

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

To apply this lemma, first observe:

By cubing both sides, the $(q_1 \ldots q_s)$ term becomes $1 \pmod{p^\alpha}$. 

John B. Cosgrave and Karl Dilcher

Generalized Fermat Numbers
Therefore the main conditions is

\[ \left( \frac{p^{\alpha} - 1}{3} \right) p!^{3 \cdot 2^s} \equiv 1 \pmod{p^{\alpha}}. \]  

(6)
Therefore the main conditions is
\[
\left( \frac{p^\alpha - 1}{3} \right)_p!^{3 \cdot 2^s} \equiv 1 \pmod{p^\alpha}.
\] (6)

We’ll see: primes \( p \) that satisfy this are rather special.

Using the notation
\[
\gamma_\alpha(p) := \text{ord}_{p^\alpha} \left( \left( \frac{p^\alpha - 1}{3} \right)_p! \right) \quad p \equiv 1 \pmod{3},
\]
for the multiplicative order modulo \( p^\alpha \), (6) implies
\[
\gamma_\alpha(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell \quad (0 \leq \ell \leq s).
\] (7)
Therefore the main conditions is

\[(\frac{p^\alpha - 1}{3} p!)^{3 \cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{6}\]

We’ll see: primes \( p \) that satisfy this are rather special.

Using the notation

\[\gamma_\alpha(p) := \text{ord}_{p^\alpha}(\frac{p^\alpha - 1}{3} p!) \quad p \equiv 1 \pmod{3},\]

for the multiplicative order modulo \( p^\alpha \), (6) implies

\[\gamma_\alpha(p) = 2^\ell \text{ or } 3 \cdot 2^\ell \quad (0 \leq \ell \leq s). \tag{7}\]

We showed earlier (IJNT, 2011, in greater generality): sequence \( \gamma_1(p), \gamma_2(p), \ldots \) behaves in a very specific way; means that (7) implies

\[\gamma_1(p) = 2^\ell \text{ or } 3 \cdot 2^\ell.\]
This gives rise to the following definition:

**Definition**

A prime $p \equiv 1 \pmod{3}$ is a Jacobi prime of level $\ell$ if

$$\text{ord}_p \left( \frac{p-1}{3} ! \right) = 2^{\ell} \quad \text{or} \quad \text{ord}_p \left( \frac{p-1}{3} ! \right) = 3 \cdot 2^{\ell}.$$
This gives rise to the following definition:

**Definition**

A prime \( p \equiv 1 \pmod{3} \) is a Jacobi prime of level \( \ell \) if

\[
\text{ord}_p \left( \frac{p-1}{3}! \right) = 2^\ell \quad \text{or} \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 3 \cdot 2^\ell.
\]

**Examples:** We consider the first three primes \( p \equiv 1 \pmod{6} \) and compute:

\[
\begin{align*}
p = 7: \quad & \frac{p-1}{3}! = 2, \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 3 = 3 \cdot 2^0; \\
p = 13: \quad & \frac{p-1}{3}! = 24, \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 12 = 3 \cdot 2^2; \\
p = 19: \quad & \frac{p-1}{3}! = 720, \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 9.
\end{align*}
\]
This gives rise to the following definition:

**Definition**

A prime \( p \equiv 1 \pmod{3} \) is a Jacobi prime of level \( \ell \) if

\[
\text{ord}_p \left( \frac{p-1}{3}! \right) = 2 \ell \quad \text{or} \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 3 \cdot 2^\ell.
\]

**Examples:** We consider the first three primes \( p \equiv 1 \pmod{6} \) and compute:

- \( p = 7 : \quad \frac{p-1}{3}! = 2, \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 3 = 3 \cdot 2^0 \);
- \( p = 13 : \quad \frac{p-1}{3}! = 24, \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 12 = 3 \cdot 2^2 \);
- \( p = 19 : \quad \frac{p-1}{3}! = 720, \quad \text{ord}_p \left( \frac{p-1}{3}! \right) = 9. \)

Thus, 7 and 13 are Jacobi primes of levels 0, resp. 2; 19 is not a Jacobi prime.
Why “Jacobi prime”? Recall:

**Theorem (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

\[
\left( \frac{2(p-1)}{3} \right)_{p-1} \equiv -r \pmod{p}.
\]
Why “Jacobi prime”? Recall:

**Theorem (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

\[
\left( \frac{2(p-1)}{3} \right) \equiv -r \pmod{p}.
\]

An easy consequence:

**Corollary**

Let \( p \) and \( r \) be as above. Then

\[
\left( \frac{p-1}{3} \right)!^3 \equiv \frac{1}{r} \pmod{p}. \tag{8}
\]
This leads to equivalent definition:

**Corollary**

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

$$\text{ord}_p(r) = 2^\ell.$$
This leads to equivalent definition:

**Corollary**

> A prime \( p \equiv 1 \pmod{3} \) is a Jacobi prime of level \( \ell \) iff

\[
\text{ord}_p(r) = 2^\ell.
\]

**Examples:**

\[
\begin{align*}
p = 7 : & \quad 4p = 1^2 + 27 \cdot 1^2, \quad \text{ord}_p(1) = 2^0; \\
p = 13 : & \quad 4p = (-5)^2 + 27 \cdot 1^2, \quad \text{ord}_p(-5) = 2^2; \\
p = 19 : & \quad 4p = 7^2 + 27 \cdot 1^2, \quad \text{ord}_p(7) = 3.
\end{align*}
\]

Consistent with previous examples.
Some further properties:

**Proposition**

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

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

(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 215105 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.
Some further properties:

Proposition

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

\[ p = 27X^2 + 27X + 7 \quad (X \in \mathbb{Z}). \]

(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:

**Proposition**

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

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

(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 215105 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.
9. Main results

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

**Theorem**

Let $n = p \cdot q_1^{\beta_1} \ldots q_s^{\beta_s}$ where $p \equiv 1 \pmod{3}$, $q_1 \equiv \cdots \equiv q_s \equiv -1 \pmod{3}$, $s \geq 2$.

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 the following be satisfied:

...
9. Main results

Using a slightly more general setting again, with \( n \equiv w \equiv \pm1 \pmod{3} \), we have

Theorem

Let \( n = p \cdot q_1^{\beta_1} \cdots q_s^{\beta_s} \) where \( p \equiv 1 \pmod{3}, \)
\( q_1 \equiv \cdots \equiv q_s \equiv -1 \pmod{3}, \ s \geq 2. \)
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 the following be satisfied:
(a) \( p \) is a level-\( \ell \) Jacobi prime for some \( 0 \leq \ell \leq s \);
(b) \( q_i^{\beta_i} \mid (p - 1)(p + 1)(p^2 + 1) \ldots (p^{2^{s-2}} + 1) \) for all \( 1 \leq i \leq s. \)

This is again a simplified version of a more general result.
A large amount of computation was required,

- to compute Jacobi primes, and
- to factor generalized Fermat numbers.
A large amount of computation was required,
• to compute Jacobi primes, and
• to factor generalized Fermat numbers.

Some noteworthy results:

$$\frac{1}{2} (331^{2^8} + 1), \quad \frac{1}{2} (2752513^{2^4} + 1), \quad \frac{1}{2} (6684673^{2^5} + 1)$$

are all primes, with 648, 103 and 219 digits.
( None of them are support primes )
<table>
<thead>
<tr>
<th>$p$</th>
<th>$j$</th>
<th>comp. cofactor</th>
<th>prime fact.</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>1951</td>
<td>6</td>
<td>157</td>
<td>72, 85</td>
<td>N</td>
</tr>
<tr>
<td>2437</td>
<td>6</td>
<td>166</td>
<td>67, 99</td>
<td>N</td>
</tr>
<tr>
<td>4219</td>
<td>6</td>
<td>156</td>
<td>77, 80</td>
<td>N</td>
</tr>
<tr>
<td>25117</td>
<td>6</td>
<td>197</td>
<td>43, 154</td>
<td>E</td>
</tr>
<tr>
<td>55681</td>
<td>6</td>
<td>293</td>
<td>44, 249</td>
<td>E</td>
</tr>
<tr>
<td>331777</td>
<td>5</td>
<td>170</td>
<td>51, 119</td>
<td>E</td>
</tr>
<tr>
<td>737281</td>
<td>7</td>
<td>702</td>
<td>43, 660</td>
<td>E</td>
</tr>
<tr>
<td>75079681</td>
<td>5</td>
<td>197</td>
<td>43, 155</td>
<td>E</td>
</tr>
<tr>
<td>460794822529</td>
<td>4</td>
<td>151</td>
<td>75, 77</td>
<td>N</td>
</tr>
<tr>
<td>1136051159041</td>
<td>4</td>
<td>154</td>
<td>76, 78</td>
<td>N</td>
</tr>
</tbody>
</table>

**Table 3**: Numbers of digits of factors of some $p^{2j} + 1$.  

N: cado-nfs  
E: GMP-ECM
Factors

$13^{28} + 1$

• Has 4 small odd prime factors;
• composite cofactor has 184 digits.
Thank you