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

'Number Theory Down Under', Newcastle, Sept. 26, 2016

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: $m = 5, 6, \ldots, 11$.

1.1. Current Status (as of August 31, 2016)

- Completely factored: $m = 5, 6, \dots, 11$.

- Known to be composite, but no factor known: $m = 20, 24$.

1.1. Current Status (as of August 31, 2016)

- Completely factored: $m = 5, 6, \dots, 11$.
- Known to be composite, but no factor known: $m = 20, 24$.
- Nature unknown: $m = 33, 34, 35, 40, 41, 44, 45, 46, \dots$

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

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: $m = 5, 6, \dots, 11$.

- Known to be composite, but no factor known: $m = 20, 24$.

- Nature unknown: $m = 33, 34, 35, 40, 41, 44, 45, 46, \dots$

- 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)

(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 $p = k \cdot 2^{m+2} + 1$.

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:

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

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

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

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

• Having found such a prime p,
“sieve", using the recurrence $\pmod{p}$:

$$F_{n+1} = (F_n - 1)^2 + 1.$$

"Small" Fermat Numbers ($m \le 24$):
Primality testing:

"Small" Fermat Numbers ($m \leq 24$):
Primality testing:

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

1.2. Finding Factors (cont'd)

"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.

1.2. Finding Factors (cont'd)

"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):

1.2. Finding Factors (cont'd)

"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)

1.2. Finding Factors (cont'd)

"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).

Richard E. Crandall
1947–2012

According to Richard Crandall, the computer power that went into

- proving F_{22} composite, and
- producing “Toy Story"

(both in 1995) were roughly equivalent.

1.2. Finding Factors (cont'd)

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

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)

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).

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).

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.

2. Generalized Fermat Numbers

Define

$$F_m(a) = a^{2^m} + 1.$$

2. Generalized Fermat Numbers

Define

$$F_m(a) = a^{2^m} + 1.$$

Again, odd prime factors must be of the form

$$k \cdot 2^{m+1} + 1.$$

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.

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).

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).

A “typical" result:

Theorem. (Jiménez Calvo & KD, 1999)
$p = k \cdot 2^n + 1$ 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

$$F_{m-\ell}(k) = k^{2^{m-\ell}} + 1.$$

2. Generalized Fermat Numbers (cont'd)

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;

2. Generalized Fermat Numbers (cont'd)

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;

2. Generalized Fermat Numbers (cont'd)

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.

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

$$3^{2^{382428}} + (2^{141839})^{2^{382428}}.$$

3. Wilson's Theorem and Gauss Factorials

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

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

3. Wilson's Theorem and Gauss Factorials

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*

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

3. Wilson's Theorem and Gauss Factorials

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*

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

The Gauss-Wilson theorem: For any $n \geq 2$,

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

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

General long-term program: To study the Gauss factorials

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

General long-term program: To study the Gauss factorials

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

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

General long-term program: To study the Gauss factorials

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

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

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

General long-term program: To study the Gauss factorials

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

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

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

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

General long-term program: To study the Gauss factorials

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

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

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

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

General long-term program: To study the Gauss factorials

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

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

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

- $M = 1$: 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

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

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

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

- $M = 1$: 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

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

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

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

- 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 $(\frac{n-1}{M})_n! \pmod{n}$ is a divisor of M. In certain cases, solutions of (1) can be characterized.

Different point of view: Consider again

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

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

Different point of view: Consider again

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

– 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; 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

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

– 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 $(\frac{n-1}{M})_n! \pmod{n}$ 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;
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).

4. The case $M = 4$

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

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

Obviously, this holds for $n = 5$.

4. The case $M = 4$

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

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

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.

4. The case $M = 4$

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

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

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 $\equiv 1 \pmod 4$.

4. The case $M = 4$

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

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

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

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

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

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

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 $p \equiv 1 \pmod 4$.

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

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

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

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

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

How can we characterize such solutions?

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

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*.

n	n factored	p
205479813	$3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
1849318317	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 46817$	46817
233456083377	$3 \cdot 11 \cdot 19 \cdot 571 \cdot 652081$	652081

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*.

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

$$46817 - 1 = 2^5 \cdot \mathbf{7} \cdot \mathbf{11} \cdot \mathbf{19},$$

$$46817 + 1 = 2 \cdot \mathbf{3}^4 \cdot 17^2,$$

$$652081 - 1 = 2^4 \cdot \mathbf{3} \cdot 5 \cdot \mathbf{11} \cdot 13 \cdot \mathbf{19},$$

$$652081 + 1 = 2 \cdot \mathbf{571}^2.$$

Consider multiplicative orders:

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

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

Consider multiplicative orders:

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

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

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

Consider multiplicative orders:

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

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

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

we say that p is a *Gauss prime* of level ℓ.

Definition

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

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

we say that p is a *Gauss prime* of level ℓ.

Why “Gauss prime"? Recall:

Definition

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

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

we say that p is a *Gauss prime* of level ℓ.

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

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

Definition

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

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

we say that p is a *Gauss prime* of level ℓ.

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

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

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 $\frac{p-1}{4}!$ 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 $p = a^2 + b^2$, $a, b > 0$.*

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:

k	a_k	p_k	prime
1	1	17	yes
2	4	241	yes
3	15	3 361	yes
4	56	46 817	yes
5	209	652 081	yes
6	780	9 082 321	no

The first few values of a_k and p_k:

k	a_k	p_k	prime
1	1	17	yes
2	4	241	yes
3	15	3 361	yes
4	56	46 817	yes
5	209	652 081	yes
6	780	9 082 321	no

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 $\big((F_n - 1)/4\big)!$ 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 $\big((F_n - 1)/4\big)!$ 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 $\big((F_n - 1)/4\big)!$ 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 $M = 4$:

Theorem

Suppose that

$$n = p\, q_1^{\beta_1} \dots q_r^{\beta_r}$$

with $p \equiv 1 \pmod 4$ *and* $q_j \equiv -1 \pmod 4$ *distinct primes.*

Theorem

Suppose that

$$n = p\, q_1^{\beta_1} \dots q_r^{\beta_r}$$

with $p \equiv 1 \pmod 4$ *and* $q_j \equiv -1 \pmod 4$ *distinct primes. Then*

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv 1 \pmod n \tag{3}$$

is impossible for $r = 1, 2$ *or 3.*

Theorem

Suppose that

$$n = p\, q_1^{\beta_1} \dots q_r^{\beta_r}$$

with $p \equiv 1 \pmod 4$ *and* $q_j \equiv -1 \pmod 4$ *distinct primes. Then*

$$\left\lfloor \frac{n-1}{4} \right\rfloor_n ! \equiv 1 \pmod n \tag{3}$$

is impossible for $r = 1, 2$ *or 3. Otherwise,* (3) *holds iff*

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

(ii) $q_j^{\beta_j} \mid (p-1)$ *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 $r \geq \ell$.

- 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 $q_j \mid p \pm 1$.

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

14 factors q_j,
from 3 to 1403687828273374406026310517426O179,
two with multiplicity 2.

- 26 Gauss primes with $5 \le \ell \le 18$ have been found. None of them satisfy $r \ge \ell$.

When $\ell = 4$:

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

- Another example: $p_{131} =$
881218785186320224738518516256503796205310883044356986457857324150680203969199260511507595926468857084114007285544744995271784268717820573108544336161
(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 62739901036488299100482530481038557222957100492740101548294773888591 7389."

5. The cases $M = 3$ and $M = 6$

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 $w = 1$.)

5. The cases $M = 3$ and $M = 6$

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

$$\left\lfloor \tfrac{n-1}{3} \right\rfloor_n ! \equiv 1 \pmod{n}, \tag{4}$$

or

$$\left\lfloor \tfrac{n-1}{6} \right\rfloor_n ! \equiv 1 \pmod{n}. \tag{5}$$

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

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

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

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	$5 \cdot \mathbf{13}^{\mathbf{2}} \cdot 17$
305	$5 \cdot \mathbf{61}$	34765	$5 \cdot 17 \cdot \mathbf{409}$
338	$2 \cdot \mathbf{13}^{\mathbf{2}}$	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

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

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?
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

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

(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?

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

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

...

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

For $M = 6$**:**

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

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

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

...

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

For $M = 6$:

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

Note:

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

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

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

...

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

For $M = 6$**:**

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

Note:

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

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

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

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

...

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

For $M = 6$**:**

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

Note:

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

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

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

6. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

6. 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.

6. 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., $n \equiv 1 \pmod{3}$.

6. 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

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

6. 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 $n = p^\alpha w$, $w = q_1^{\beta_1} \ldots q_s^{\beta_s}$,
- $w \equiv 1 \pmod{3}$, i.e., $n \equiv 1 \pmod{3}$.

Main approach: Find criteria for

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

then combine the two using the Chinese Remainder Theorem.

7. Generalized Fermat numbers

Congruences modulo w:

We define the partial totient function

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

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

With n as before, we have

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

7. 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

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

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

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

• 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 $M \geq 2$.

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:

Proposition

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

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

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

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

Note: This is in fact true for

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

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma

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

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

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma

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

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

Once again:

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

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma

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 $1 \pmod{p^\alpha}$.

Therefore the main conditions is

$$\left(\frac{p^\alpha-1}{3}\right)_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{6}$$

Therefore the main conditions is

$$(\tfrac{p^\alpha-1}{3})_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{6}$$

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

Using the notation

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

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

$$\gamma_\alpha(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell \qquad (0 \le \ell \le s). \tag{7}$$

Therefore the main conditions is

$$\left(\tfrac{p^\alpha-1}{3}\right)_p!^{3\cdot 2^s} \equiv 1 \pmod{p^\alpha}. \tag{6}$$

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

Using the notation

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

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

$$\gamma_\alpha(p) = 2^\ell \quad \text{or} \quad 3\cdot 2^\ell \qquad (0 \le \ell \le s). \tag{7}$$

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

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

This gives rise to the following definition:

Definition

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

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

This gives rise to the following definition:

Definition

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

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

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

$$\begin{aligned}
p = 7: &\quad \tfrac{p-1}{3}! = 2, &\quad \mathrm{ord}_p\left(\tfrac{p-1}{3}!\right) &= 3 = 3\cdot 2^0;\\
p = 13: &\quad \tfrac{p-1}{3}! = 24, &\quad \mathrm{ord}_p\left(\tfrac{p-1}{3}!\right) &= 12 = 3\cdot 2^2;\\
p = 19: &\quad \tfrac{p-1}{3}! = 720, &\quad \mathrm{ord}_p\left(\tfrac{p-1}{3}!\right) &= 9.
\end{aligned}$$

This gives rise to the following definition:

Definition

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

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

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

$$\begin{aligned}
p = 7: &\quad \tfrac{p-1}{3}! = 2, &\quad \mathrm{ord}_p\left(\tfrac{p-1}{3}!\right) = 3 = 3 \cdot 2^0;\\
p = 13: &\quad \tfrac{p-1}{3}! = 24, &\quad \mathrm{ord}_p\left(\tfrac{p-1}{3}!\right) = 12 = 3 \cdot 2^2;\\
p = 19: &\quad \tfrac{p-1}{3}! = 720, &\quad \mathrm{ord}_p\left(\tfrac{p-1}{3}!\right) = 9.
\end{aligned}$$

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*

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

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*

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

An easy consequence:

Corollary

Let p *and* r *be as above. Then*

$$(\tfrac{p-1}{3})!^3 \equiv \frac{1}{r} \pmod p. \tag{8}$$

This leads to equivalent definition:

Corollary

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

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

This leads to equivalent definition:

Corollary

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

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

Examples:

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

Consistent with previous examples.

Some further properties:

Proposition

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

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

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

Some further properties:

Proposition

(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:

Proposition

(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.

9. Main results

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

Theorem

Let $n = p \cdot q_1^{\beta_1} \dots q_s^{\beta_s}$ *where* $p \equiv 1 \pmod 3$, $q_1 \equiv \dots \equiv q_s \equiv -1 \pmod 3$, $s \geq 2$.
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 $n \equiv w \equiv \pm 1 \pmod 3$, we have

Theorem

Let $n = p \cdot q_1^{\beta_1} \dots q_s^{\beta_s}$ *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

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

to hold is that the following be satisfied:

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

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

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:

$$\tfrac{1}{2}\left(331^{2^8}+1\right),\quad \tfrac{1}{2}\left(2\,752\,513^{2^4}+1\right),\quad \tfrac{1}{2}\left(6\,684\,673^{2^5}+1\right)$$

are all primes, with 648, 103 and 219 digits.
(None of them are support primes)

p	j	comp. cofactor	prime fact.	Method
1 951	6	157	**72**, 85	N
2 437	6	166	67, **99**	N
4 219	6	156	**77**, **80**	N
25 117	6	197	**43**, **154**	E
55 681	6	293	**44**, **249**	E
331 777	5	170	**51**, **119**	E
737 281	7	702	**43**, **660**	E
75 079 681	5	197	**43**, 155	E
460 794 822 529	4	151	75, 77	N
1 136 051 159 041	4	154	**76**, 78	N

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

N: cado-nfs
E: GMP-ECM

Factors

$$13^{2^8} + 1$$

- Has 4 small odd prime factors;
- composite cofactor has 184 digits.

Thank you