Gauss Factorials, Jacobi Primes, and Generalized Fermat Numbers

Karl Dilcher

Number Theory Seminar, September 28, 2018
Joint work with

John B. Cosgrave

Dublin, Ireland
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

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

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

\[
1 \cdot 2 \ldots \frac{p-1}{2} \frac{p+1}{2} \ldots (p-1) \equiv \left( \frac{p-1}{2} \right)! (-1)^{\frac{p-1}{2}} \left( \frac{p-1}{2} \right)! \pmod{p}.
\]
We begin with *Wilson’s Theorem*: \( p \) is a prime if and only if

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

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

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

Thus, with Wilson’s Theorem,

\[
\left( \frac{p-1}{2} \right)!^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.
\]
We begin with *Wilson’s Theorem*: \( p \) is a prime if and only if

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

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

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

Thus, with Wilson’s Theorem,

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

This was apparently first observed by Lagrange (1773).
John Wilson  
1741–1793

Joseph-Louis Lagrange  
1736–1813
This congruence,

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

has the following consequences:

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

\[
\text{ord}_p \left( \left( \frac{p-1}{2} \right)! \right) = 4 \quad \text{for} \quad p \equiv 1 \pmod{4}.
\]
This congruence,

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

has the following consequences:

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

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

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

\[
\left( \frac{p-1}{2} \right)! \equiv \pm 1 \pmod{p}.
\]
This congruence,

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

has the following consequences:

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

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

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

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

What is the sign on the right?
Theorem 1 (Mordell, 1961)

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

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

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


Discovered independently by Chowla.

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

Karl Dilcher

Gauss factorials
Theorem 1 (Mordell, 1961)

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

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

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


This completely determines the order mod $p$ of $\left(\frac{p-1}{2}\right)!$. 
Louis J. Mordell  
1888–1972

Sarvadaman Chowla  
1907–1995
Is there an analogue of Wilson’s Theorem for \textit{composite} integers?
Is there an analogue of Wilson’s Theorem for composite integers?

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

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

Theorem 2 (The Gauss-Wilson Theorem)

For any $n \geq 2$,

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

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

Karl Dilcher

Gauss factorials
Is there an analogue of Wilson’s Theorem for composite integers?

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

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

Theorem 2 (The Gauss-Wilson Theorem)

For any $n \geq 2$,

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

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

Karl Dilcher

Gauss factorials
General long-term program: To study the Gauss factorials

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

• \( M = 1 \): Gauss-Wilson theorem.
• \( M = 2 \): Completely determined (JBC & KD, 2008). Only possible orders are 1, 2, and 4.
• \( M \geq 3 \): Orders are generally unbounded. Various partial results; e.g.,
  – If \( n \) has at least 3 different prime factors \( \equiv 1 \pmod{M} \), then \( \left( \frac{n - 1}{M} \right)_n! \equiv 1 \pmod{n} \);
  – If \( n \) has two different prime factors \( \equiv 1 \pmod{M} \), then the order of \( \left( \frac{n - 1}{M} \right)_n! \) is a divisor of \( M \).
General long-term program: To study the Gauss factorials

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

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

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

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

- \( M = 1 \): Gauss-Wilson theorem.

- \( M = 2 \): Completely determined (JBC & KD, 2008).
  - Only possible orders are 1, 2, and 4.
- \( M \geq 3 \): Orders are generally unbounded.
  - Various partial results; e.g.,
    - If \( n \) has at least 3 different prime factors \( \equiv 1 \pmod{M} \),
      then \( \left( \frac{n - 1}{M} \right)_n ! \equiv 1 \pmod{n} \);
    - If \( n \) has two different prime factors \( \equiv 1 \pmod{M} \),
      then the order of \( \left( \frac{n - 1}{M} \right)_n ! \) is a divisor of \( M \).
General long-term program: To study the Gauss factorials

\[
\left( \frac{n - 1}{M} \right)_n!, \quad M \geq 1, \quad n \equiv 1 \pmod{M},
\]
in particular their multiplicative orders (mod \(n\)), but also, if possible, their values (mod \(n\)).

- \(M = 1\): Gauss-Wilson theorem.

- \(M = 2\): Completely determined (JBC & KD, 2008). Only possible orders are 1, 2, and 4.
General long-term program: To study the Gauss factorials

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

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

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

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

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

- **\( M = 1 \):** Gauss-Wilson theorem.

- **\( M = 2 \):** Completely determined (JBC & KD, 2008). Only possible orders are 1, 2, and 4.

- **\( M \geq 3 \):** Orders are generally unbounded. Various partial results; e.g.,
  - If \( n \) has **at least 3** different prime factors \( \equiv 1 \pmod{M} \), then \( \left( \frac{n-1}{M} \right)_n! \equiv 1 \pmod{n} \);
General long-term program: To study the Gauss factorials

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

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

- \( M = 1 \): Gauss-Wilson theorem.

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

- \( M \geq 3 \): Orders are generally unbounded. Various partial results; e.g.,
  - If \( n \) has at least 3 different prime factors \( \equiv 1 \pmod{M} \),
    then \( \left( \frac{n-1}{M} \right)_n! \equiv 1 \pmod{n} \);
  - If \( n \) has two different prime factors \( \equiv 1 \pmod{M} \),
    then the order of \( \left( \frac{n-1}{M} \right)_n! \) is a divisor of \( M \).
– If \( n \) has one prime factor \( \equiv 1 \pmod{M} \):
    Most interesting case;
    this talk will be about three different instances of this.
– If $n$ has **one** prime factor $\equiv 1 \pmod{M}$: 
  Most interesting case; 
  this talk will be about three different instances of this.

– If $n$ has **no** prime factor $\equiv 1 \pmod{M}$: 
  Next to nothing is known.
– If $n$ has **one** prime factor $\equiv 1 \pmod{M}$:
  Most interesting case;
  this talk will be about three different instances of this.

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

Some further aspects:

- Other partial products of the “full” product $(n - 1)_n!$
  have also been studied (JBC & KD, 2013).
  (Not in this talk).
– If \( n \) has **one** prime factor \( \equiv 1 \pmod{M} \):
  Most interesting case;
  this talk will be about three different instances of this.

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

Some further aspects:

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

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

In 1828, Gauss proved the following remarkable congruence.

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

First application of Gauss factorials:

In 1828, Gauss proved the following remarkable congruence.

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

**Theorem 3 (Gauss, 1828)**

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

\[
\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv 2a \pmod{p}.
\]
This can be extended:
This can be extended:

**Theorem 4**

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

\[
\left( \frac{p^\alpha - 1}{2} \right)_p \left( \frac{p^\alpha - 1}{4} \right)_p \equiv 2a - 1 \cdot \frac{p}{2a} - 1 \cdot \frac{p^2}{8a^3} - 2 \cdot \frac{p^3}{(2a)^5} - 5 \cdot \frac{p^4}{(2a)^7} - 14 \cdot \frac{p^5}{(2a)^9} - \ldots - C_{\alpha-2} \frac{p^{\alpha-1}}{(2a)^{2\alpha-1}} \pmod{p^\alpha}.
\]
This can be extended:

**Theorem 4**

*With* \( p \) and \( a \) as above and \( \alpha \geq 2 \), we have

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

\( C_n := \frac{1}{n+1} \binom{2n}{n} \in \mathbb{N} \) is the *n*th Catalan number.

**Karl Dilcher**

**Gauss factorials**
Jacobi proved a similar theorem to that of Gauss:

**Theorem 5 (Jacobi, 1837)**

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

\[
\left( \frac{2(p-1)}{3} \right) \left( \frac{p-1}{3} \right) \equiv -r \pmod{p}.
\]
Jacobi proved a similar theorem to that of Gauss:

**Theorem 5 (Jacobi, 1837)**

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

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

Yet another theorem of this type is due to Hudson and Williams (1984) (later).
Jacobi proved a similar theorem to that of Gauss:

**Theorem 5 (Jacobi, 1837)**

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

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

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

These and others also have “Catalan analogues” (JBC & KD, 2010; Al-Shaghay, 2014; JBC & KD, 2016).
C. F. Gauss  
1777–1855  

C. G. J. Jacobi  
1804–1851  

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

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

In what follows: Fix $M$ and $p$; let $\alpha$ vary.

What can we say about the sequence $\{ \gamma^M_{\alpha}(p) \}_{\alpha \geq 1}$?

Note: $(p^\alpha - 1)M \equiv (p^\alpha - 1)^M \pmod{M}$.

We can therefore replace the subscript $p^\alpha$ by $p^\alpha$.

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

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

$$\gamma^M_\alpha(p) := \text{ord}_p \left( \left( \frac{p^\alpha - 1}{M} \right) p^\alpha ! \right).$$

In what follows: Fix $M$ and $p$; let $\alpha$ vary.
For the second part of this talk, the main objects of study are:

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

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

In what follows: Fix $M$ and $p$; let $\alpha$ vary.

What can we say about the sequence

$$\{\gamma^M_\alpha(p)\}_{\alpha \geq 1}$$
For the second part of this talk, the main objects of study are:
For $M \geq 2$ and prime $p \equiv 1 \pmod{M}$, define

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

In what follows: Fix $M$ and $p$; let $\alpha$ vary.

What can we say about the sequence

$$\{ \gamma^M_\alpha(p) \}_{\alpha \geq 1}?$$

Note:

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

We can therefore replace the subscript $p^\alpha$ by $p$. 
For the second part of this talk, the main objects of study are:

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

$$\gamma^M_\alpha(p) := \text{ord}_p\left(\left(\frac{p^\alpha - 1}{M}\right) p^\alpha!\right).$$

In what follows: Fix $M$ and $p$; let $\alpha$ vary.

What can we say about the sequence

$$\{\gamma^M_\alpha(p)\}_{\alpha \geq 1}?$$

Note:

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

We can therefore replace the subscript $p^\alpha$ by $p$.

Let’s look at some examples with $M = 4$: 
<table>
<thead>
<tr>
<th>$\alpha/p$</th>
<th>5</th>
<th>13</th>
<th>17</th>
<th>29</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>12</td>
<td>16</td>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>156</td>
<td>272</td>
<td>406</td>
<td>333</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>2028</td>
<td>4624</td>
<td>5887</td>
<td>24642</td>
</tr>
<tr>
<td>4</td>
<td>250</td>
<td>26364</td>
<td>78608</td>
<td>341446</td>
<td>455877</td>
</tr>
<tr>
<td>5</td>
<td>625</td>
<td>342732</td>
<td>1336336</td>
<td>4950967</td>
<td>33734898</td>
</tr>
<tr>
<td>$\alpha/p$</td>
<td>5</td>
<td>13</td>
<td>17</td>
<td>29</td>
<td>37</td>
</tr>
<tr>
<td>-----------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>12</td>
<td>16</td>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>156</td>
<td>272</td>
<td>406</td>
<td>333</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>2028</td>
<td>4624</td>
<td>5887</td>
<td>24642</td>
</tr>
<tr>
<td>4</td>
<td>250</td>
<td>26364</td>
<td>78608</td>
<td>341446</td>
<td>455877</td>
</tr>
<tr>
<td>5</td>
<td>625</td>
<td>342732</td>
<td>1336336</td>
<td>4950967</td>
<td>33734898</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\gamma$</th>
<th>$2p\gamma$</th>
<th>$p^2\gamma$</th>
<th>$2p^3\gamma$</th>
<th>$p^4\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma$</td>
<td>$p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>$p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$2p^3\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
</tr>
<tr>
<td>$\gamma$</td>
<td>$2p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
</tbody>
</table>

Table 1: $\gamma := \gamma_1^4(p)$, $p \equiv 1 \pmod{4}$. 
<table>
<thead>
<tr>
<th>$\alpha/p$</th>
<th>5</th>
<th>13</th>
<th>17</th>
<th>29</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>12</td>
<td>16</td>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>156</td>
<td>272</td>
<td>406</td>
<td>333</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>2028</td>
<td>4624</td>
<td>5887</td>
<td>24642</td>
</tr>
<tr>
<td>4</td>
<td>250</td>
<td>26364</td>
<td>78608</td>
<td>341446</td>
<td>455877</td>
</tr>
<tr>
<td>5</td>
<td>625</td>
<td>342732</td>
<td>1336336</td>
<td>4950967</td>
<td>33734898</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\alpha$</th>
<th>$\gamma$</th>
<th>$2p\gamma$</th>
<th>$p^2\gamma$</th>
<th>$2p^3\gamma$</th>
<th>$p^4\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\gamma$</td>
<td>$\gamma$</td>
<td>$p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
<tr>
<td>$2\gamma$</td>
<td>$2p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$p^2\gamma$</td>
<td>$2p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
<tr>
<td>$p^2\gamma$</td>
<td>$p^2\gamma$</td>
<td>$p^3\gamma$</td>
<td>$p^3\gamma$</td>
<td>$2p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
<tr>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
</tbody>
</table>

**Table 1:** $\gamma := \gamma^4_1(p)$, $p \equiv 1$ (mod 4).

Note the 3 different patterns; otherwise regular.
<table>
<thead>
<tr>
<th>$\alpha/p$</th>
<th>5</th>
<th>13</th>
<th>17</th>
<th>29</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>12</td>
<td>16</td>
<td>7</td>
<td>18</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>156</td>
<td>272</td>
<td>406</td>
<td>333</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>2028</td>
<td>4624</td>
<td>5887</td>
<td>24642</td>
</tr>
<tr>
<td>4</td>
<td>250</td>
<td>26364</td>
<td>78608</td>
<td>341446</td>
<td>455877</td>
</tr>
<tr>
<td>5</td>
<td>625</td>
<td>342732</td>
<td>1336336</td>
<td>4950967</td>
<td>33734898</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\gamma$</th>
<th>$2p\gamma$</th>
<th>$p^2\gamma$</th>
<th>$2p^3\gamma$</th>
<th>$p^4\gamma$</th>
<th>$\frac{1}{2}p\gamma$</th>
<th>$p^2\gamma$</th>
<th>$\frac{1}{2}p^3\gamma$</th>
<th>$p^4\gamma$</th>
<th>$\frac{1}{2}p^3\gamma$</th>
<th>$p^4\gamma$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\gamma$</td>
<td>$\gamma$</td>
<td>$\gamma$</td>
<td>$\gamma$</td>
<td>$\gamma$</td>
<td>$\frac{1}{2}p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
</tr>
<tr>
<td>2</td>
<td>$2p\gamma$</td>
<td>$p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$2p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
</tr>
<tr>
<td>3</td>
<td>$p^2\gamma$</td>
<td>$p^3\gamma$</td>
<td>$p^3\gamma$</td>
<td>$2p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p\gamma$</td>
<td>$p^2\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
</tr>
<tr>
<td>4</td>
<td>$2p^3\gamma$</td>
<td>$p^3\gamma$</td>
<td>$2p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
<tr>
<td>5</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
<td>$\frac{1}{2}p^3\gamma$</td>
<td>$p^4\gamma$</td>
</tr>
</tbody>
</table>

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

Note the 3 different patterns; otherwise regular.

- Are there more patterns?
Note the 3 different patterns; otherwise regular.

- Are there more patterns?
- Do we always have $1, p, p^2, p^3, \ldots$?
One might conjecture:
the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

\[
\begin{cases}
\gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod{8} \\
or p \equiv 5 \pmod{8} \text{ and } 4|\gamma, \\
\gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod{8} \text{ and } \gamma \equiv 2 \pmod{4}, \\
\gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod{8} \text{ and } \gamma \text{ is odd.}
\end{cases}
\]
One might conjecture: the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

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

Computations seem to support this.
One might conjecture:
the sequence of orders \( \gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots \) is

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

Computations seem to support this.

**However**, for \( p = 29789 \):
\( \gamma_1^4 = 14,894 \), \textbf{but} \( \gamma_2^4 = 7,447 \).
One might conjecture:
the sequence of orders \( \gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots \) is

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

Computations seem to support this.

**However**, for \( p = 29789 \):

\( \gamma_1^4 = 14894 \), \( \text{but } \gamma_2^4 = 7447 \).

The sequence “forgot” the factor \( p \) in the step \( \gamma_1^4 \to \gamma_2^4 \).
One might conjecture: the sequence of orders $\gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots$ is

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

Computations seem to support this.

**However**, for $p = 29789$: $\gamma_1^4 = 14894$, **but** $\gamma_2^4 = 7447$. The sequence “forgot" the factor $p$ in the step $\gamma_1^4 \to \gamma_2^4$.

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

Karl Dilcher

Gauss factorials
One might conjecture: the sequence of orders \( \gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots \) is

\[
\begin{cases}
\gamma, p\gamma, p^2\gamma, p^3\gamma, \ldots & \text{when } p \equiv 1 \pmod{8} \\
\gamma, \frac{1}{2}p\gamma, p^2\gamma, \frac{1}{2}p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod{8} \text{ and } 4 \mid \gamma,
\end{cases}
\]

or \( p \equiv 5 \pmod{8} \) and \( 4 \mid \gamma, \)

\[
\begin{cases}
\gamma, 2p\gamma, p^2\gamma, 2p^3\gamma, \ldots & \text{when } p \equiv 5 \pmod{8} \text{ and } \gamma \text{ is odd}.
\end{cases}
\]

Computations seem to support this.

**However**, for \( p = 29\,789: \quad \gamma_1^4 = 14\,894, \quad \text{but} \quad \gamma_2^4 = 7\,447. \)

The sequence “forgot” the factor \( p \) in the step \( \gamma_1^4 \to \gamma_2^4. \)

The next part of this talk will be about such “exceptional primes”:

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

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

Computations seem to support this.

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

The next part of this talk will be about such “exceptional primes”:

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

Karl Dilcher

Gauss factorials
One might conjecture: the sequence of orders \( \gamma_1^4 = \gamma, \gamma_2^4, \gamma_3^4, \ldots \) is

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

Computations seem to support this.

However, for \( p = 29789: \gamma_1^4 = 14894, \text{ but } \gamma_2^4 = 7447. \) The sequence “forgot” the factor \( p \) in the step \( \gamma_1^4 \rightarrow \gamma_2^4. \)

The next part of this talk will be about such “exceptional primes”:

- Are there more?
- Can we characterize them? Compute them?
- Can the “skipped \( p \)” occur elsewhere in the sequence?
Theorem 6

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

$$\gamma_{\alpha+1}^M(p) = p\gamma_{\alpha}^M(p) \quad \text{or} \quad \gamma_{\alpha+1}^M(p) = \gamma_{\alpha}^M(p).$$
Theorem 6

Let $M \geq 2$, $p \equiv 1 \pmod{M}$ and $\gamma^M_\alpha(p)$ as above.

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

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

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

$$\gamma^M_{\alpha+1}(p) = \begin{cases} 
p\gamma^M_\alpha(p) \quad \text{or} \quad \gamma^M_\alpha(p) & \text{if} \quad \gamma^M_\alpha(p) \equiv 0 \pmod{4}, \\
\frac{1}{2}p\gamma^M_\alpha(p) \quad \text{or} \quad \frac{1}{2}\gamma^M_\alpha(p) & \text{if} \quad \gamma^M_\alpha(p) \equiv 2 \pmod{4}, \\
2p\gamma^M_\alpha(p) \quad \text{or} \quad 2\gamma^M_\alpha(p) & \text{if} \quad \gamma^M_\alpha(p) \equiv 1 \pmod{2}. \end{cases}$$
Theorem 6

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

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

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

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

When the second alternative holds in one of the cases, we call $p$ an $\alpha$-exceptional prime for $M$. 
How often does this happen?
How often does this happen?

<table>
<thead>
<tr>
<th>$M$</th>
<th>$p$</th>
<th>up to</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>13, 181, 2521, 76543, 489061</td>
<td>$10^{12}$</td>
</tr>
<tr>
<td>4</td>
<td>29789</td>
<td>$10^{11}$</td>
</tr>
<tr>
<td>5</td>
<td>71</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>6</td>
<td>13, 181, 2521, 76543, 489061</td>
<td>$10^{12}$</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>18</td>
<td>1090891</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>21</td>
<td>211, 15583</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>23</td>
<td>3037</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>24</td>
<td>73</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>29</td>
<td>59</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>35</td>
<td>1471</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>44</td>
<td>617</td>
<td>$2 \cdot 10^6$</td>
</tr>
<tr>
<td>48</td>
<td>97</td>
<td>$2 \cdot 10^6$</td>
</tr>
</tbody>
</table>

**Table 2**: 1-exceptional primes $p$ for $3 \leq M \leq 100$. 
The proof of Theorem 6 provides a first criterion; all entries in the table were found with this criterion.

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

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

Here: Consider $M = 3, 6$; $M = 4$ is similar. But also, as we saw: $M = 3, 6$ are connected in some special ways.
The proof of Theorem 6 provides a first criterion; all entries in the table were found with this criterion.

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

In the cases $M = 3, 4$ and $6$ we can use the theory of Jacobi sums to obtain some strong criteria, in addition to further insight.
The proof of Theorem 6 provides a first criterion; all entries in the table were found with this criterion.

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

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

Here: Consider $M = 3, 6$; $M = 4$ is similar.
The proof of Theorem 6 provides a first criterion; all entries in the table were found with this criterion.

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

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

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

But also, as we saw: $M = 3, 6$ are connected in some special ways.
Let $p \equiv 1 \pmod{6}$ be a prime.

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

We fix them in a certain technical way.
Let \( p \equiv 1 \pmod{6} \) be a prime.

Known: The representation \( p = a^2 + 3b^2 \) is unique up to sign, but the signs are crucial here.

We fix them in a certain technical way.

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

\[
4p = r^2 + 3s^2, \quad 4p = u^2 + 3v^2, \quad r \equiv u \equiv 1 \pmod{3}
\]
Let $p \equiv 1 \pmod{6}$ be a prime.

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

We fix them in a certain technical way.

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

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

The numbers $u$ occur in the following analogue of the binomial coefficient theorems of Gauss and Jacobi:
Theorem 7 (Hudson and Williams, 1984)

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

$$\left(\frac{p-1}{3}, \frac{p-1}{6}\right) \equiv (-1)^{\frac{p-1}{6}+1} u \pmod{p}.$$
Theorem 7 (Hudson and Williams, 1984)

Let \( p \equiv 1 \pmod{6} \) be a prime and \( u \) as above. Then

\[
\left( \frac{p-1}{3} \right) \equiv (-1)^{p-1/6+1} u \pmod{p}.
\]

This has the following "Catalan extension":

Theorem 8

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

\[
\left( \frac{p^{\alpha+1}-1}{3} \right) \equiv (-1)^{p-1/6+1} \left( \frac{p-1}{6} \right)^p \left( \left( \frac{p^{\alpha+1}-1}{6} \right)_p \right)^2 \equiv (-1)^{p-1/6+1}
\]

\[
\times \left( u - \frac{p}{u} - \frac{p^2}{u^3} - \cdots - C_{\alpha-1} \frac{p^\alpha}{u^{2\alpha-1}} \right) \pmod{p^{\alpha+1}}.
\]
Kenneth S. Williams  
b. 1940

Eugène Catalan  
1814–1894
The next result will be the basis for all that follows.

**Theorem 9**

Let \( p \equiv 1 \pmod{6} \) and \( r, u \) as above. Then for all \( \alpha \geq 1 \) we have

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

where \( C_n \) is the \( n \)th Catalan number.
The next result will be the basis for all that follows.

**Theorem 9**

Let \( p \equiv 1 \pmod{6} \) and \( r, u \) as above.

Then for all \( \alpha \geq 1 \) we have

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

where \( C_n \) is the \( n \)th Catalan number.

Main ingredients in proof:
- An identity between the third powers of certain Jacobi sums;
- Congruences \( \pmod{p^{\alpha+1}} \) between these Jacobi sums and both sides in Theorem 9;
- Quotients of certain Gauss factorials are involved as intermediate steps.
The next result will be the basis for all that follows.

**Theorem 9**

Let \( p \equiv 1 \pmod{6} \) and \( r, u \) as above.

Then for all \( \alpha \geq 1 \) we have

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

where \( C_n \) is the \( n \)th Catalan number.

Main ingredients in proof:

- An identity between the third powers of certain Jacobi sums;
- congruences \( \pmod{p^{\alpha+1}} \) between these Jacobi sums and both sides in Theorem 9;
The next result will be the basis for all that follows.

**Theorem 9**

Let \( p \equiv 1 \pmod{6} \) and \( r, u \) as above.

Then for all \( \alpha \geq 1 \) we have

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

where \( C_n \) is the \( n \)th Catalan number.

Main ingredients in proof:

- An identity between the third powers of certain Jacobi sums;
- congruences \((\mathrm{mod} \ p^{\alpha+1})\) between these Jacobi sums and both sides in Theorem 9;
- quotients of certain Gauss factorials are involved as intermediate steps.
Corollary 10

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

$$\left( \left( \frac{p^\alpha - 1}{3} \right)_p ! \right)^{24} \equiv \left( \left( \frac{p^\alpha - 1}{6} \right)_p ! \right)^{12} \pmod{p^\alpha}.$$
Corollary 10

For any \( p \equiv 1 \pmod{6} \) and \( \alpha \geq 1 \) we have

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

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

Corollary 11

Let \( p \equiv 1 \pmod{6} \) and \( \alpha \geq 1 \). Then \( p \) is \( \alpha \)-exceptional for \( M = 3 \) iff it's \( \alpha \)-exceptional for \( M = 6 \).
Corollary 10

For any \( p \equiv 1 \pmod{6} \) and \( \alpha \geq 1 \) we have

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

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

Corollary 11

Let \( p \equiv 1 \pmod{6} \) and \( \alpha \geq 1 \). Then

\( p \) is \( \alpha \)-exceptional for \( M = 3 \) iff it's \( \alpha \)-exceptional for \( M = 6 \).

This confirms our observation from Table 1.
Corollary 10

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

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

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

Corollary 11

Let $p \equiv 1 \pmod{6}$ and $\alpha \geq 1$. Then

$p$ is $\alpha$-exceptional for $M = 3$ iff it's $\alpha$-exceptional for $M = 6$.

This confirms our observation from Table 1.

Another consequence is the desired exceptionality criterion:
Theorem 12

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

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

where \( C_n \) is the \( n \)th Catalan number.
Theorem 12

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

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

where \( C_n \) is the \( n \)th Catalan number.

Special case:

Corollary 13

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

\[
(u - \frac{p}{u})^{p-1} \equiv 1 \pmod{p^2}.
\]
It turns out: 1-exceptionality is the most important case:

**Theorem 14**

Let $M \geq 2$, $p \equiv 1 \pmod{M}$, and $\alpha \geq 2$. If $p$ is $\alpha$-exceptional, then it's also $(\alpha - 1)$-exceptional (for $M$).
It turns out: 1-exceptionality is the most important case:

**Theorem 14**

Let \( M \geq 2 \), \( p \equiv 1 \pmod{M} \), and \( \alpha \geq 2 \).

If \( p \) is \( \alpha \)-exceptional, then it’s also \( (\alpha - 1) \)-exceptional (for \( M \)).

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

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

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

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

Karl Dilcher

Gauss factorials
Results:

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

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

- All $M \leq 100$:
  None of the known 1-exceptional primes are 2-exceptional.
How are we doing with time?

This is the third part of this talk.

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

$$\left\lfloor \frac{n-1}{M} \right\rfloor n! \equiv 1 \pmod{n}, \quad n \equiv \pm 1 \pmod{M}$$
This is the third part of this talk.

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

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

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
This is the third part of this talk.

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

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

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
This is the third part of this talk.

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

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

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
- $M = 3, 4, 6$: Most interesting cases.
This is the third part of this talk.

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

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

Recall:

- $M = 1$: Determined by Gauss-Wilson theorem.
- $M = 2$: Completely determined (JBC & KD, 2008).
- $M = 3, 4, 6$: Most interesting cases.
  - $M = 4$: Previously studied (JBC & KD, 2014).
This is the third part of this talk.

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

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

Recall:

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

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

– If \( n \) has \textbf{one} prime factor \( \equiv 1 \pmod{M} \):
Most interesting case.
Different point of view: Consider again

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

– 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.

– If \( n \) has \textbf{one} prime factor \( \equiv 1 \pmod{M} \): Most interesting case.

– If \( n \) has \textbf{no} prime factor \( \equiv 1 \pmod{M} \): Very little can be said.
**Setting the stage:** We’ll consider integers of the form

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

(s ≥ 0, α, β₁, ..., βₛ ∈ 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

\[ \left\lfloor \frac{n-1}{3} \right\rfloor n! \equiv 1 \pmod{n}, \quad (2) \]

or

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

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 17 \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

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

(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

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

(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.

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

\[ n = 7 \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833, \]
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.
- 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?
\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

(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
  \[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]
\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

(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.

\[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]
$$n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}.$$ 

(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

\[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]
\[ n = p^\alpha q_1^{\beta_1} \cdots q_s^{\beta_s}. \]

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

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

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

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

- 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?
"You know, most people's favourite number is 7, but mine is 627399010364832991004825304810385572229571004927401015482947738885917389."
The solutions, again: \textbf{For} $M = 3$:

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

\[ \ldots \]

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

\textbf{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:

\[
\begin{align*}
5 & \mid 7^2 + 1, \\
17 & \mid 7^3 + 1 \quad \text{and} \quad 169553 \mid 7^3 + 1, \\
353 & \mid 7^4 + 1 \quad \text{and} \quad 47072139617 \mid 7^4 + 1, \\
7699649 & \mid 7^5 + 1 \quad \text{and} \quad 531968664833 \mid 7^5 + 1.
\end{align*}
\]
The solutions, again: \textbf{For } M = 3:
\[ n = 7 \cdot 2 \cdot 5 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 531968664833, \]
\[ \ldots \]
\[ n = 7 \cdot 2^9 \cdot 5 \cdot 17 \cdot 353 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]

\textbf{For } M = 6:
\[ n = 7 \cdot 17 \cdot 353 \cdot 169553 \cdot 7699649 \cdot 47072139617 \cdot 531968664833. \]

\textbf{Note:}
\[ 5 \mid 7^2 + 1, \]
\[ 17 \mid 7^3 + 1 \quad \text{and} \quad 169 \, 553 \mid 7^3 + 1, \]
\[ 353 \mid 7^4 + 1 \quad \text{and} \quad 47 \, 072 \, 139 \, 617 \mid 7^4 + 1, \]
\[ 7 \, 699 \, 649 \mid 7^5 + 1 \quad \text{and} \quad 53 \, 196 \, 866 \, 483 \, 33 \mid 7^5 + 1. \]

\textbf{Also: } 7^2 + 1 \text{ 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:

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

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

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

We can find necessary and sufficient conditions for the solutions of

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

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., \( n \equiv 1 \pmod{3} \).
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

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

We can find necessary and sufficient conditions for the solutions of

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

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., \( n \equiv 1 \pmod{3} \).

**Main approach:** Find criteria for

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

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

Congruences modulo \( w \):

We define the partial totient function

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

Congruences modulo $w$:

We define the partial totient function

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

Lemma 15

*With $n$ as before, we have*

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

Proof is very technical. Basic idea: Write $n-1 = p^{\alpha} + w - 1$ for $n \equiv 1 \pmod{3}$ or $n \equiv -1 \pmod{3}$.
8. 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 15

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:

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

\[
\left\{ \frac{p_\alpha - 1}{3} \text{ “main terms”, and} \right. \\
\left. \frac{w-1}{3} \text{ “remainder term”} \right\}
\]
\[
\frac{n-1}{3} = \frac{p^\alpha - 1}{3} w + \frac{w-1}{3}.
\]

This means:

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

\[\left\{ \frac{p^\alpha - 1}{3} \right\}
\]

“main terms", and

one “remainder term".

- 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:

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

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

- 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

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

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

Raise both sides of Lemma to 3rd power.

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

Therefore
\[
\left( \frac{n-1}{3} \right)_n!^3 \equiv 1 \pmod{w}
\]
if and only if
\[
p^{2^{s-1}} - 1 \equiv 0 \pmod{w}.
\]

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

**Theorem 16**

*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*

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

**Theorem 16**

*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 \( q_i^{\beta_i} \) 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

\[
\left\lfloor \frac{n-1}{3} \right\rfloor_n! \equiv 1 \pmod{w}.
\]
9. Jacobi primes

Congruences modulo $p^\alpha$: The following is the second crucial ingredient.

**Lemma 17**

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

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

Congruences modulo $p^\alpha$:

The following is the second crucial ingredient.

Lemma 17

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

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

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

Congruences modulo $p^\alpha$:

The following is the second crucial ingredient.

**Lemma 17**

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

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

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 $1 \pmod{p^\alpha}$. 
Therefore the main conditions is

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

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

Using the notation \(\gamma_\alpha(p) := \text{ord}_p \left( \left( \frac{p^\alpha - 1}{3} \right)p! \right) \equiv 1 \pmod{3}\), for the multiplicative order modulo \(p^\alpha\), (4) implies \(\gamma_\alpha(p) = 2\ell\) or \(3 \cdot 2\ell\) \((0 \leq \ell \leq s)\). (5)

We saw earlier: Sequence \(\gamma_1(p), \gamma_2(p), \ldots\) behaves in a very specific way; this means that (5) implies \(\gamma_1(p) = 2\ell\) or \(3 \cdot 2\ell\).
Therefore the main conditions is

\[
\left(\frac{p^\alpha - 1}{3}\right)p!3^s2^s \equiv 1 \pmod{p^\alpha}.
\] (4)

We’ll see: primes \( p \) that satisfy this are rather special.
Therefore the main conditions is

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

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 \( p^\alpha \),
Therefore the main conditions is

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

(4)

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 \( p^\alpha \), (4) implies

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

(5)
Therefore the main conditions is
\[
\left( \frac{p^\alpha - 1}{3} \right)_p! 3 \cdot 2^s \equiv 1 \pmod{p^\alpha}.
\] (4)

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 \( p^\alpha \), (4) implies
\[
\gamma_\alpha(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell \quad (0 \leq \ell \leq s).
\] (5)

We saw earlier:
Sequence \( \gamma_1(p), \gamma_2(p), \ldots \) behaves in a very specific way;
this means that (5) implies
\[
\gamma_1(p) = 2^\ell \quad \text{or} \quad 3 \cdot 2^\ell.
\]
This gives rise to the following definition:

**Definition 18**

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

- \( p = 7 \):
  \[
  p-1 \equiv 6 \pmod{3} \\
  \text{ord}_p \left( \frac{p-1}{3}! \right) = 3 = 3 \cdot 2^0.
  \]
  Thus, 7 is a Jacobi prime of level 0.

- \( p = 13 \):
  \[
  p-1 \equiv 12 \pmod{3} \\
  \text{ord}_p \left( \frac{p-1}{3}! \right) = 12 = 3 \cdot 2^2.
  \]
  Thus, 13 is a Jacobi prime of level 2.

- \( p = 19 \):
  \[
  p-1 \equiv 18 \pmod{3} \\
  \text{ord}_p \left( \frac{p-1}{3}! \right) = 9.
  \]
  Thus, 19 is not a Jacobi prime.
This gives rise to the following definition:

**Definition 18**

A prime $p \equiv 1 \pmod{3}$ is called 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:

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

**Definition 18**

A prime $p \equiv 1 \pmod{3}$ is called 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 19 (Jacobi, 1837)**

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

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

**Theorem 19 (Jacobi, 1837)**

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

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

An easy consequence:

**Corollary 20**

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

$$\left( \frac{p-1}{3} \right)!^3 \equiv \frac{1}{r} \pmod{p}. \quad (6)$$
This leads to equivalent definition:

**Corollary 21**

*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 21**

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

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

**Examples:**

- $p = 7 : \quad 4p = 1^2 + 27 \cdot 1^2, \quad \text{ord}_p(1) = 2^0$
- $p = 13 : \quad 4p = (-5)^2 + 27 \cdot 1^2, \quad \text{ord}_p(-5) = 2^2$
- $p = 19 : \quad 4p = 7^2 + 27 \cdot 1^2, \quad \text{ord}_p(7) = 3$

Consistent with previous examples.
Some further properties:

**Theorem 22**

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

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

(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.
Theorem 22

(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:

**Theorem 22**

(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 $10^{14}$.

(2) On the other hand, Jacobi primes of levels $\ell \geq 3$ are very rare, with only 44 up to $10^{14}$. The first few are 13, 97, 193, 409, 769.
Using a slightly more general setting again, with \( n \equiv w \equiv \pm 1 \pmod{3} \), we have

**Theorem 23**

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

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

to hold is that all of the following be satisfied:

(a) \( p \) is \((\alpha - 1)\)-exceptional if \( \alpha > 1 \);
(b) \( p \) is a level-\( \ell \) Jacobi prime for some \( 0 \leq \ell \leq s \);
(c) \( q_i^{\beta_i} \mid (p - 1)(p + 1)(p^2 + 1) \ldots (p^{2s-2} + 1) \) for all \( 1 \leq i \leq s \).
Using a slightly more general setting again, with $n \equiv w \equiv \pm 1 \pmod{3}$, we have

**Theorem 23**

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

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

to hold is that all of the following be satisfied:

(a) $p$ is $(\alpha - 1)$-exceptional if $\alpha > 1$;
(b) $p$ is a level-$\ell$ Jacobi prime for some $0 \leq \ell \leq s$;
(c) $q_i^{\beta_i} | (p - 1)(p + 1)(p^2 + 1) \ldots (p^{2s-2} + 1)$ for all $1 \leq i \leq s$.

Relevant here:

$p = 13$ is the only Jacobi prime $< 10^{12}$ that is also 1-exceptional.
Let's return to our original table:

$$\left\lfloor \frac{n - 1}{3} \right\rfloor \cdot n! \equiv 1 \pmod{n}$$

$$\left\lfloor \frac{n - 1}{6} \right\rfloor \cdot n! \equiv 1 \pmod{n}$$

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

We have seen: Only $p = 13$ can possibly appear to a higher power, for $p < 10^{12}$. 
Let’s return to our original table:

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

<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>355365</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: \( p \equiv 1 \pmod{3} \).
Let's return to our original table:

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

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

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