Generalized Fermat numbers and congruences for Gauss factorials

Karl Dilcher

Dalhousie University, Halifax, Nova Scotia, Canada

CMS Winter Meeting 2015, Montréal

Joint work with

John B. Cosgrave

Dublin, Ireland

1. Introduction

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

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

1. Introduction

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

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

For a composite analogue we define the *Gauss factorial*

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

1. Introduction

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

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

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

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

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.

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).

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.
  - $M = 4$: Previously studied (JBC & KD, 2014).

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.
  - $M = 4$: Previously studied (JBC & KD, 2014).
  - $M = 3, 6$: Similar to each other, but different from $M = 4$; topic of this talk.

Different point of view: Consider again

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

Different point of view: Consider again

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

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

Different point of view: Consider again

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

– 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.

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.

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 a specific aspect.

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 a specific aspect.

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

Different point of view: Consider again

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

– 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 a specific aspect.

– 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).

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

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

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

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

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

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

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

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

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

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

Here: study integers of this type for which

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

or

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

First few solutions of

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

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

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

How can we characterize these solutions?

First few solutions of

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

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

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

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

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

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

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

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

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

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

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

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

Combination of theory and computation shows:

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

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

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

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

Combination of theory and computation shows:

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

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

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

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

with 30 and 36 decimal digits, respectively.

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

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

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

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

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

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

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

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \dots, 5$: 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 $s = 1, \dots, 5$: 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 $s = 1, \dots, 5$: 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?

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

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

- For $s = 0$: trivial solution $n = 7$.
- For $s = 1, \ldots, 5$: 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 $s = 1, \dots, 5$: no solutions.
- For $s = 6$: single 40-digit solution

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

Questions:

(i) What determines presence/absence of solutions?

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

(iii) For what p can solutions exist?

"You know, most people's favourite number is 7, but mine is 6273990103648829910048253048103855572229571004927401015482947738885917389."

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:

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

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

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

...

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

For $M = 6$**:**

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

Note:

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

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

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

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

...

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

For $M = 6$**:**

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

Note:

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

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

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

2. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

2. 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.

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

2. 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

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

2. Towards an explanation

We can find necessary and sufficient conditions for the solutions of

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

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

For simplicity, here: Restrict our attention to

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

Main approach: Find criteria for

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

then combine the two using the Chinese Remainder Theorem.

Congruences modulo w:

We define the partial totient function

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

3. 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

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

3. 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

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

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

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

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

This means:

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

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

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

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

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

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

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

We have therefore shown:

Proposition

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

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

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

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

Note: This is in fact true for

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

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma

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

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

4. Jacobi primes

Congruences modulo p^α:

The following is the second crucial ingredient.

Lemma

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

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

Once again:

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

4. Jacobi primes

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

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

Therefore the main conditions is

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

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

Using the notation

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

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

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

Therefore the main conditions is

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

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

Using the notation

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

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

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

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

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

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

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

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

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*

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

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.

5. Main results

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

Theorem

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

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

to hold is that all of the following be satisfied:

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

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

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

5. Main results

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

Theorem

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

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

to hold is that all of the following be satisfied:

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

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

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

What does "$(\alpha - 1)$-exceptional" mean?

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

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

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

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

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

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

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

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

What can we say about the sequence

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

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

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

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

What can we say about the sequence

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

Note:

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

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

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

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

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

What can we say about the sequence

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

Note:

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

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

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

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

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

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

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

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

Note the 3 different patterns; otherwise regular.

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

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

Note the 3 different patterns; otherwise regular.

- Are there more patterns?

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

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

Note the 3 different patterns; otherwise regular.

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

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

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

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

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

Computations seem to support this.

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

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

Computations seem to support this.

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

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

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

Computations seem to support this.

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

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

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

Computations seem to support this.

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

We call such primes “exceptional primes" for M.

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

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

Computations seem to support this.

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

We call such primes “exceptional primes" for M.
- They can be characterized and computed.

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

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

Computations seem to support this.

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

We call such primes "exceptional primes" for M.

- They can be characterized and computed.
- They are exceedingly rare:

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

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

No 2-exceptional primes are known.

Relevant here:

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

Relevant here:

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

Theorem

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

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

to hold is that all of the following be satisfied:

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

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

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

Thank you

Much more could be said ...

The paper itself (to be published in Math. Comp.):

`http://www.mathstat.dal.ca/~dilcher/jacobi.html`

For extensive computations and other related papers:

`http://www.johnbcosgrave.com/`