Gauss Factorials: Properties and Applications

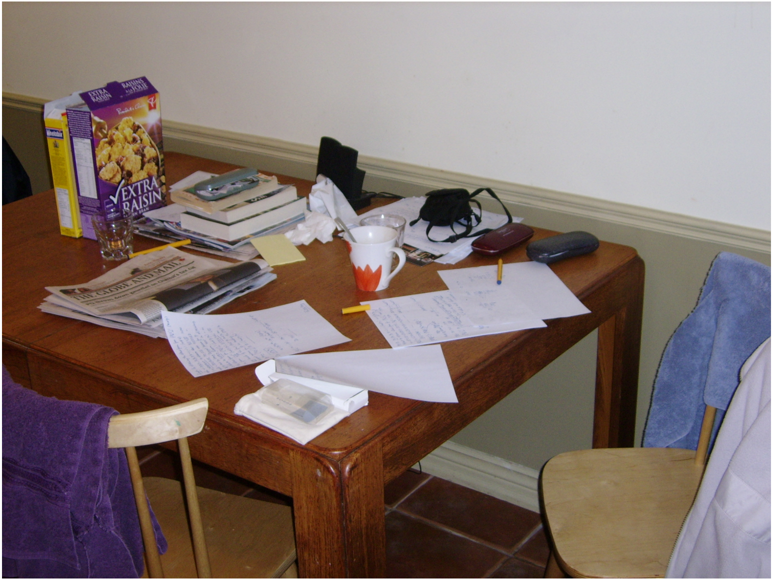
Karl Dilcher

Dalhousie University, Halifax, Nova Scotia

Joint work with

John B. Cosgrave

Dublin, Ireland


EXTRA RAISIN

1. Introduction

Recall Wilson's Theorem:

p is a prime if and only if

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

(Converse is due to Lagrange).

1. Introduction

Recall Wilson's Theorem:

p is a prime if and only if

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

(Converse is due to Lagrange). A proof depends on the fact that any integer a with $1 < a < p-1$ has its inverse $a^{-1} \not\equiv a \pmod{p}$.

If we write out the factorial $(p-1)!$ and exploit symmetry modulo p, we obtain

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

If we write out the factorial $(p-1)!$ and exploit symmetry modulo p, we obtain

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

and thus, with Wilson's Theorem,

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

If we write out the factorial $(p-1)!$ and exploit symmetry modulo p, we obtain

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

and thus, with Wilson's Theorem,

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

This was apparently first observed by Lagrange (1773).

If we write out the factorial $(p-1)!$ and exploit symmetry modulo p, we obtain

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

and thus, with Wilson's Theorem,

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

This was apparently first observed by Lagrange (1773).

For $p \equiv 1 \pmod 4$ the RHS is -1, so

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

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

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

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?

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 $p \equiv 3 \pmod 4$,

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

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

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 $p \equiv 3 \pmod 4$,

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

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

Discovered independently by Chowla.

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

Now consider the two halves of the product

$$1 \cdot 2 \cdots \frac{p-1}{2} \frac{p+1}{2} \cdots (p-1)$$

and denote them, respectively, by

$$\Pi_1^{(2)}, \qquad \Pi_2^{(2)}.$$

Now consider the two halves of the product

$$1 \cdot 2 \cdots \tfrac{p-1}{2}\,\tfrac{p+1}{2} \cdots (p-1)$$

and denote them, respectively, by

$$\Pi_1^{(2)}, \qquad \Pi_2^{(2)}.$$

By Wilson's theorem:

$$\Pi_1^{(2)}\Pi_2^{(2)} \equiv -1 \pmod{p},$$

Now consider the two halves of the product

$$1 \cdot 2 \cdots \frac{p-1}{2} \frac{p+1}{2} \cdots (p-1)$$

and denote them, respectively, by

$$\Pi_1^{(2)}, \qquad \Pi_2^{(2)}.$$

By Wilson's theorem:

$$\Pi_1^{(2)} \Pi_2^{(2)} \equiv -1 \pmod{p},$$

and by symmetry:

$$\Pi_2^{(2)} \equiv (-1)^{\frac{p-1}{2}} \Pi_1^{(2)} \pmod{p}.$$

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

Then

$$\Pi_1^{(3)} = 1{\cdot}2 \cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3} \cdots \tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3} \cdots (p-1).$$

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

Then

$$\Pi_1^{(3)} = 1{\cdot}2 \cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3} \cdots \tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3} \cdots (p-1).$$

Once again there is an obvious symmetry:

$$\Pi_3^{(3)} \equiv \Pi_1^{(3)} \pmod p,$$

(without a power of -1 since $\frac{p-1}{3}$ is always even.)

What can we say about the three partial products

$$\Pi_1^{(3)}, \quad \Pi_2^{(3)}, \quad \Pi_3^{(3)}$$

obtained by dividing the entire product $(p-1)!$ into *three* equal parts?

We require $p \equiv 1 \pmod 3$; in fact, $p \equiv 1 \pmod 6$.

Then

$$\Pi_1^{(3)} = 1{\cdot}2 \cdots \tfrac{p-1}{3}, \quad \Pi_2^{(3)} = \tfrac{p+2}{3} \cdots \tfrac{2p-2}{3}, \quad \Pi_3^{(3)} = \tfrac{2p+1}{3} \cdots (p-1).$$

Once again there is an obvious symmetry:

$$\Pi_3^{(3)} \equiv \Pi_1^{(3)} \pmod p,$$

(without a power of -1 since $\frac{p-1}{3}$ is always even.)

No obvious relation between $\Pi_1^{(3)}$ and the "middle third" $\Pi_2^{(3)}$.

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\frac{p-1}{M} + i \right), \qquad (j = 1, 2, \ldots, M).$$

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\frac{p-1}{M} + i \right), \qquad (j = 1, 2, \ldots, M).$$

Once again, clear that

$$\Pi_{M-j}^{(M)} \equiv \pm \Pi_j^{(M)} \pmod{p}, \qquad j = 1, 2, \ldots, \lfloor \tfrac{M-1}{2} \rfloor.$$

Natural extension:

For any $M \geq 2$ and for a prime $p \equiv 1 \pmod{M}$, divide $(p-1)!$ into the products

$$\Pi_j^{(M)} = \prod_{i=1}^{\frac{p-1}{M}} \left((j-1)\frac{p-1}{M} + i\right), \qquad (j = 1, 2, \ldots, M).$$

Once again, clear that

$$\Pi_{M-j}^{(M)} \equiv \pm \Pi_j^{(M)} \pmod{p}, \qquad j = 1, 2, \ldots, \lfloor \tfrac{M-1}{2} \rfloor.$$

Example:

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	**2**	$-$**2**	**2**	5	1	2	-2	-1
13	-2	3	-2	13	6	3	-3	-6
19	-2	-5	-2	17	7	-3	-3	7
31	2	-8	2	29	-6	-2	2	6
37	7	3	7	37	-16	5	-5	16
43	-3	19	-3	41	13	7	7	13
61	$-$**14**	**14**	$-$**14**	53	26	7	-7	-26
67	-20	-33	-20	61	19	7	-7	-19
73	33	-12	33	73	18	-35	-35	18
79	-37	3	-37	89	22	42	42	22
97	21	-11	21	97	20	-28	-28	20

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	$\mathbf{2}$	$-\mathbf{2}$	$\mathbf{2}$	5	1	2	-2	-1
13	-2	3	-2	13	6	3	-3	-6
19	-2	-5	-2	17	7	-3	-3	7
31	2	-8	2	29	-6	-2	2	6
37	7	3	7	37	-16	5	-5	16
43	-3	19	-3	41	13	7	7	13
61	$-\mathbf{14}$	$\mathbf{14}$	$-\mathbf{14}$	53	26	7	-7	-26
67	-20	-33	-20	61	19	7	-7	-19
73	33	-12	33	73	18	-35	-35	18
79	-37	3	-37	89	22	42	42	22
97	21	-11	21	97	20	-28	-28	20

We observe:

- The obvious symmetries.

p	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	p	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
7	$\mathbf{2}$	$-\mathbf{2}$	$\mathbf{2}$	5	1	2	-2	-1
13	-2	3	-2	13	6	3	-3	-6
19	-2	-5	-2	17	7	-3	-3	7
31	2	-8	2	29	-6	-2	2	6
37	7	3	7	37	-16	5	-5	16
43	-3	19	-3	41	13	7	7	13
61	$-\mathbf{14}$	$\mathbf{14}$	$-\mathbf{14}$	53	26	7	-7	-26
67	-20	-33	-20	61	19	7	-7	-19
73	33	-12	33	73	18	-35	-35	18
79	-37	3	-37	89	22	42	42	22
97	21	-11	21	97	20	-28	-28	20

We observe:

- The obvious symmetries.
- $\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ for $p = 7$ and $p = 61$.

Are these last cases just coincidences?

Are these last cases just coincidences?

It turns out:

$\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ also for $p = 331$, $p = 547$, $p = 1951$, and further relatively rare primes (explained later).

Are these last cases just coincidences?

It turns out:

$\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod{p}$ also for $p = 331$, $p = 547$, $p = 1951$, and further relatively rare primes (explained later).

In contrast: No primes p for which

$\Pi_1^{(3)} \equiv \Pi_2^{(3)} \pmod{p}, \qquad p \equiv 1 \pmod{6}$, or

$\Pi_1^{(4)} \equiv \pm\Pi_2^{(4)} \pmod{p}, \qquad p \equiv 1 \pmod{4}$.

Are these last cases just coincidences?

It turns out:

$\Pi_1^{(3)} \equiv -\Pi_2^{(3)} \pmod p$ also for $p = 331$, $p = 547$, $p = 1951$, and further relatively rare primes (explained later).

In contrast: No primes p for which

$$\Pi_1^{(3)} \equiv \Pi_2^{(3)} \pmod p, \qquad p \equiv 1 \pmod 6, \text{ or}$$

$$\Pi_1^{(4)} \equiv \pm\Pi_2^{(4)} \pmod p, \qquad p \equiv 1 \pmod 4.$$

This will be explained later.

2. Composite Moduli

Define the *Gauss factorial* by

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

2. Composite Moduli

Define the *Gauss factorial* by

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

Analogue of Wilson's theorem for composite moduli:

Theorem 2 (Gauss)

For any integer $n \geq 2$ we have

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

where p is an odd prime and α is a positive integer.

2. Composite Moduli

Define the *Gauss factorial* by

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

Analogue of Wilson's theorem for composite moduli:

Theorem 2 (Gauss)

For any integer $n \ge 2$ we have

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

where p is an odd prime and α is a positive integer.

The first case indicates exactly those n that have primitive roots.

Everything we did before can be extended to composite moduli.

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n
were completely determined; only orders 1, 2, 4 occur.
(JBC & KD, 2008).

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n
were completely determined; only orders 1, 2, 4 occur.
(JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products:

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products: For $n \equiv 1 \pmod{M}$, set

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \qquad (j = 1, 2, \ldots, M),$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\tfrac{n-1}{M} + 1 \leq i \leq j\tfrac{n-1}{M},\ \gcd(i, n) = 1 \right\}.$$

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products: For $n \equiv 1 \pmod{M}$, set

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \qquad (j = 1, 2, \ldots, M),$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\tfrac{n-1}{M} + 1 \leq i \leq j\tfrac{n-1}{M},\ \gcd(i, n) = 1 \right\}.$$

- Dependence on n is implied in the notation;

Everything we did before can be extended to composite moduli.

E.g., the multiplicative orders of $(\frac{n-1}{2})_n!$ modulo n were completely determined; only orders 1, 2, 4 occur. (JBC & KD, 2008).

Next, divide the product $(n-1)_n!$ into $M \geq 2$ partial products: For $n \equiv 1 \pmod{M}$, set

$$\Pi_j^{(M)} := \prod_{i \in I_j^{(M)}} i, \qquad (j = 1, 2, \ldots, M),$$

where, for $j = 1, 2, \ldots, M$,

$$I_j^{(M)} := \left\{ i \mid (j-1)\tfrac{n-1}{M} + 1 \leq i \leq j\tfrac{n-1}{M},\ \gcd(i, n) = 1 \right\}.$$

- Dependence on n is implied in the notation;
- When $n = p$: reduces to previous case.

Example:

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	−7	−19
73	33	−12	33	65	**8**	**8**	**8**	**8**
76	−29	−15	−29	69	31	−26	−26	31
79	−37	3	−37	73	18	−35	−35	18
82	−33	−25	−33	77	16	31	31	16
85	−28	9	−28	81	2	40	−40	2
88	5	−7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	−23	43	−23	93	34	−10	−10	34
97	21	−11	21	97	20	−28	−28	20

Example:

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	-7	-19
73	33	-12	33	65	**8**	**8**	**8**	**8**
76	-29	-15	-29	69	31	-26	-26	31
79	-37	3	-37	73	18	-35	-35	18
82	-33	-25	-33	77	16	31	31	16
85	-28	9	-28	81	2	40	-40	2
88	5	-7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	-23	43	-23	93	34	-10	-10	34
97	21	-11	21	97	20	-28	-28	20

We see: In contrast to prime case, it *can* happen that all partial products are congruent to each other.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \#I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.
- When $M = 2$, then $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.
- When $M = 2$, then $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

In general, the situation is less straightforward.

3. The Distribution of Totatives

We pause to consider the *number* of elements in our subintervals:

$$\phi_{M,j}(n) := \# I_j^{(M)}.$$

(Called *totatives* by J. J. Sylvester and later D. H. Lehmer).

- When $n = p$ is a prime, then $\phi_{M,j}(n) = \frac{p-1}{M}$ for all j.
- When $M = 1$, then $\phi_{1,1}(n) = \phi(n)$.
- When $M = 2$, then $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

In general, the situation is less straightforward.
E.g., for $n = 4$:
$\phi_{3,1}(n) = \phi_{3,3}(n) = 1$, but $\phi_{3,2}(n) = 0$.

When do we have equal distribution?

When do we have equal distribution?

Theorem 3 (Lehmer, 1955)

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least one prime factor $p \equiv 1 \pmod{M}$, then

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \qquad (j = 1, 2, \ldots, M).$$

When do we have equal distribution?

Theorem 3 (Lehmer, 1955)

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least one prime factor $p \equiv 1 \pmod{M}$, then

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \qquad (j = 1, 2, \ldots, M).$$

Note: Condition is sufficient, but not necessary.

When do we have equal distribution?

Theorem 3 (Lehmer, 1955)

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least one prime factor $p \equiv 1 \pmod{M}$, then

$$\phi_{M,j}(n) = \frac{1}{M}\phi(n), \qquad (j = 1, 2, \ldots, M).$$

Note: Condition is sufficient, but not necessary.

E.g., $M = 8$ and $n = 105 = 3 \cdot 5 \cdot 7$.
None of the prime factors are $\equiv 1 \pmod{8}$, but
$\phi_{M,j}(n) = \frac{1}{8}\phi(105) = 6$ for $j = 1, \ldots, 8$.

4. When Are the Partial Products Congruent?

Return to our table:

n	$\Pi_1^{(3)}$	$\Pi_2^{(3)}$	$\Pi_3^{(3)}$	n	$\Pi_1^{(4)}$	$\Pi_2^{(4)}$	$\Pi_3^{(4)}$	$\Pi_4^{(4)}$
70	29	1	29	61	19	7	-7	-19
73	33	-12	33	65	**8**	**8**	**8**	**8**
76	-29	-15	-29	69	31	-26	-26	31
79	-37	3	-37	73	18	-35	-35	18
82	-33	-25	-33	77	16	31	31	16
85	-28	9	-28	81	2	40	-40	2
88	5	-7	5	85	**13**	**13**	**13**	**13**
91	**29**	**29**	**29**	89	22	42	42	22
94	-23	43	-23	93	34	-10	-10	34
97	21	-11	21	97	20	-28	-28	20

Note:

$91 = 7 \cdot 13, \quad 65 = 5 \cdot 13, \quad 85 = 5 \cdot 17.$

This observation holds in general:

This observation holds in general:

Theorem 4

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv \left(\tfrac{n-1}{M}\right)_n! \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

This observation holds in general:

Theorem 4

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv \left(\tfrac{n-1}{M}\right)_n! \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

Result is best possible:
E.g., $M = 3$ and $n = 70 = 2 \cdot 5 \cdot 7$.
- Only one factor $\equiv 1 \pmod{3}$,
- $\Pi_1^{(3)} \equiv 29 \pmod{70}, \Pi_2^{(3)} \equiv 1 \pmod{70}$.

This observation holds in general:

Theorem 4

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv \left(\tfrac{n-1}{M}\right)_n! \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

Result is best possible:
E.g., $M = 3$ and $n = 70 = 2 \cdot 5 \cdot 7$.
• Only one factor $\equiv 1 \pmod{3}$,
• $\Pi_1^{(3)} \equiv 29 \pmod{70}, \Pi_2^{(3)} \equiv 1 \pmod{70}$.

On the other hand, condition is sufficient but not necessary.
E.g., $M = 3$ and $n = 2^2 \cdot 61$; statement still holds.

Proof is based on an observation:

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \qquad j = 1, 2, \ldots, M,$$

Proof is based on an observation:

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \qquad j = 1, 2, \ldots, M,$$

and a lemma:

Lemma 5

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$, $n = p^\alpha q^\beta w$ for distinct prime $p, q \equiv 1 \pmod{M}$, $\alpha, \beta \geq 1$, and $\gcd(pq, w) = 1$. Then for $j = 1, 2, \ldots, M$,

$$\left(j\frac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^{j\frac{p-1}{M}}}{p^{jA}} \pmod{q^\beta w}, \qquad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w),$$

where $\varepsilon = -1$ if $w = 1$, and $\varepsilon = 1$ if $w > 1$.

Proof is based on an observation:

$$\Pi_j^{(M)} = \frac{\left(j\frac{n-1}{M}\right)_n!}{\left((j-1)\frac{n-1}{M}\right)_n!}, \qquad j = 1, 2, \ldots, M,$$

and a lemma:

Lemma 5

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$, $n = p^\alpha q^\beta w$ for distinct prime $p, q \equiv 1 \pmod{M}$, $\alpha, \beta \geq 1$, and $\gcd(pq, w) = 1$. Then for $j = 1, 2, \ldots, M$,

$$\left(j\frac{n-1}{M}\right)_n! \equiv \frac{\varepsilon^{j\frac{p-1}{M}}}{p^{jA}} \pmod{q^\beta w}, \qquad A = \frac{p^{\alpha-1}}{M}\phi(q^\beta w),$$

where $\varepsilon = -1$ if $w = 1$, and $\varepsilon = 1$ if $w > 1$.

To prove the Theorem, use this and the Chinese Remainder Theorem; dependence on j disappears.

Idea of proof:

Idea of proof:

Break the range of the product in $\left(j\frac{n-1}{M}\right)_n!$ into
• a number of products of approximately equal length,
• a shorter “tail."

Idea of proof:

Break the range of the product in $\left(j\frac{n-1}{M}\right)_n!$ into
- a number of products of approximately equal length,
- a shorter “tail."

Then evaluate the products of the first type using the Gauss-Wilson theorem $\pmod{q^\beta w}$.

Idea of proof:

Break the range of the product in $\left(j\frac{n-1}{M}\right)_n!$ into
- a number of products of approximately equal length,
- a shorter "tail."

Then evaluate the products of the first type using the Gauss-Wilson theorem $\pmod{q^\beta w}$.

Carefully count which elements to include/exclude.

5. Some Consequences

1. We saw:
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the $\Pi_j^{(M)}$ are congruent to each other.

5. Some Consequences

1. We saw:
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the $\Pi_j^{(M)}$ are congruent to each other.

Since their product is $(n-1)_n!$, we have by Gauss-Wilson,

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

5. Some Consequences

1. We saw:
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the $\Pi_j^{(M)}$ are congruent to each other.

Since their product is $(n-1)_n!$, we have by Gauss-Wilson,

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

This implies:

Corollary 6

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least two distinct prime factors $\equiv 1 \pmod{M}$, then the multiplicative order of $(\frac{n-1}{M})_n!$ modulo n is a divisor of M.

2. In the case of at least *three* distinct prime factors $\equiv 1 \pmod{M}$ we can say more:

2. In the case of at least *three* distinct prime factors $\equiv 1 \pmod{M}$ we can say more:

Theorem 7

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least three distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv 1 \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

2. In the case of at least *three* distinct prime factors $\equiv 1 \pmod{M}$ we can say more:

Theorem 7

Let $M \geq 2$ and $n \equiv 1 \pmod{M}$.
If n has at least three distinct prime factors $\equiv 1 \pmod{M}$, then

$$\Pi_j^{(M)} \equiv 1 \pmod{n}, \qquad j = 1, 2, \ldots, M.$$

Method of proof is similar to that of the previous lemma.

Summary:

# of prime factors $\equiv 1 \pmod{M}$	All $\Pi_1^{(M)}, \ldots, \Pi_M^{(M)}$:
1	have the same number of factors
2	are congruent to each other $\pmod{M}$
3	are congruent to $1 \pmod{M}$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}}$$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2}$$

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2}$$

6. The Gauss and Jacobi Theorems

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}.$$

Return to the question of how $\Pi_1^{(4)}$ and $\Pi_2^{(4)}$ are related, for prime moduli $p \equiv 1 \pmod 4$.

Consider their quotient:

$$Q_4(p) := \frac{\Pi_2^{(4)}}{\Pi_1^{(4)}} = \frac{\Pi_1^{(4)}\Pi_2^{(4)}}{\left(\Pi_1^{(4)}\right)^2} = \frac{\frac{p-1}{2}!}{\left(\frac{p-1}{4}!\right)^2} = \binom{\frac{p-1}{2}}{\frac{p-1}{4}}.$$

There exists a celebrated congruence for this binomial coefficient:

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Theorem 8 (Gauss, 1828)

Let p and a be as above. Then

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

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Theorem 8 (Gauss, 1828)

Let p and a be as above. Then

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

As an easy application we get

$$\Pi_2^{(4)} \not\equiv \pm\Pi_1^{(4)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 4.$$

Fix p, a, and b such that

$$p \equiv 1 \pmod 4, \qquad p = a^2 + b^2, \qquad a \equiv 1 \pmod 4.$$

Theorem 8 (Gauss, 1828)

Let p and a be as above. Then

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

As an easy application we get

$$\Pi_2^{(4)} \not\equiv \pm\Pi_1^{(4)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 4.$$

A similar theorem, due to Jacobi (1837), implies that

$$\Pi_2^{(3)} \not\equiv \Pi_1^{(3)} \pmod p \quad \text{for all} \quad p \equiv 1 \pmod 6.$$

A number of further consequences can be derived from these classical theorems.

A number of further consequences can be derived from these classical theorems. Two samples:

Corollary 9

For a prime $p \equiv 1 \pmod 6$ we have

$$\Pi_2^{(3)} \equiv -\Pi_1^{(3)} \pmod p \quad \Leftrightarrow \quad p = 27x^2 + 27x + 7, x \in \mathbb{Z}.$$

A number of further consequences can be derived from these classical theorems. Two samples:

Corollary 9

For a prime $p \equiv 1 \pmod 6$ *we have*

$$\Pi_2^{(3)} \equiv -\Pi_1^{(3)} \pmod p \quad \Leftrightarrow \quad p = 27x^2 + 27x + 7, x \in \mathbb{Z}.$$

The first such primes are 7, 61 (seen earlier), 331, 547, 1951.

Corollary 10

Let $p \equiv 1 \pmod 4$*. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

Corollary 10

Let $p \equiv 1 \pmod 4$*. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

Corollary 10

Let $p \equiv 1 \pmod 4$*. Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$*.*

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$*.*

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *holds for* $p = 17, 241, 3361, 46817, 652081, \ldots$

Corollary 10

Let $p \equiv 1 \pmod 4$. *Then*

(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(b) $\left(\frac{p-1}{4}!\right)^k \not\equiv -1 \pmod p$ *for* $k = 1, 2, 4$.

(c) $\left(\frac{p-1}{4}!\right)^8 \equiv -1 \pmod p$ *holds for* $p = 17, 241, 3361, 46817, 652081, \ldots$

Part (c) is related to the solution of a certain Pell equation.

7. Extensions of Gauss' Theorem

Recall:

Theorem 11 (Gauss, 1828)

If p and a are such that $p = a^2 + b^2,\ a \equiv 1 \pmod 4$, then

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

7. Extensions of Gauss' Theorem

Recall:

Theorem 11 (Gauss, 1828)

If p and a are such that $p = a^2 + b^2,\ a \equiv 1 \pmod 4$, then

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

Theorem 12 (Chowla, Dwork, Evans, 1986)

With p and a as above,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(1 + \frac{1}{2} p q_p(2)\right)\left(2a - \frac{p}{2a}\right) \pmod{p^2},$$

where $q_p(2) := (2^{p-1} - 1)/p$ is the Fermat quotient to base 2.

The concept of Gauss factorial was essential in the proof of the following further extension:

Theorem 13

With p and a as above,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right) \times \left(1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right) \pmod{p^3},$$

where E_n is the nth Euler number.

The concept of Gauss factorial was essential in the proof of the following further extension:

Theorem 13

With p and a as above,

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv \left(2a - \frac{p}{2a} - \frac{p^2}{8a^3}\right) \times \left(1 + \tfrac{1}{2}pq_p(2) + \tfrac{1}{8}p^2\left(2E_{p-3} - q_p(2)^2\right)\right) \pmod{p^3},$$

where E_n is the nth Euler number.

Similar extensions were also obtained for Jacobi's theorem, concerning the binomial coefficient

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \qquad (p \equiv 1 \pmod 6).)$$

Thank you


Welcome to
The IRMACS Centre
Friday, September 21
9:30 am - Presentation Studio
9:30 am - ASB 10908
10:00 am - ASB 10940
10:45 am - ASB 10908
FAB Research Project
11:30 am - Presentation Studio
IRMACS: The Interdisciplinary Colloquium