A mod p^3 analogue of a theorem of Gauss on binomial coefficients

Karl Dilcher

Dalhousie University, Halifax, Canada

ELAZ, Schloß Schney , August 16, 2012

Joint work with

John B. Cosgrave

Dublin, Ireland

We begin with a table:

We begin with a table:

We begin with a table:

p	$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$	(mod p)
5	2	2
13	20	7
17	70	2
29	3432	10
37	48620	2
41	184756	10
53	10400600	39
61		10
73		67
89		10
97		18

$p \equiv 1 \pmod 4$

Add in sums of squares:

p	$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$	$\pmod p$	a	b
5	2	2	1	2
13	20	7	3	2
17	70	2	1	4
29	3432	10	5	2
37	48620	2	1	6
41	184756	10	5	4
53	10400600	39	7	2
61		10	5	6
73		67	3	8
89		10	5	8
97		18	9	4

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

Reformulating the table:

p	$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$	$\pmod p$	$\lvert\cdots\rvert < \frac{p}{2}$	a	b
5	2	2	2	1	2
13	20	7	-6	3	2
17	70	2	2	1	4
29	3432	10	10	5	2
37	48620	2	2	1	6
41	184756	10	10	5	4
53	10400600	39	-14	7	2
61		10	10	5	6
73		67	-6	3	8
89		10	10	5	8
97		18	18	9	4

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

1. Introduction

The table is an illustration of the following celebrated result:

Theorem 1 (Gauss, 1828)

Let $p \equiv 1 \pmod 4$ *be a prime and write*

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

Then

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

1. Introduction

The table is an illustration of the following celebrated result:

Theorem 1 (Gauss, 1828)

Let $p \equiv 1 \pmod 4$ *be a prime and write*

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

Then

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

Several different proofs are known, some using “Jacobsthal sums".

Goal: Extend this to a congruence mod p^2.

Goal: Extend this to a congruence mod p^2.
Need *Fermat quotients*: For $m \in \mathbb{Z}$, $m \geq 2$, and $p \nmid m$, define

$$q_p(m) := \frac{m^{p-1} - 1}{p}.$$

Goal: Extend this to a congruence mod p^2.
Need *Fermat quotients*: For $m \in \mathbb{Z}$, $m \geq 2$, and $p \nmid m$, define

$$q_p(m) := \frac{m^{p-1} - 1}{p}.$$

Beukers (1984) conjectured, and Chowla, Dwork & Evans (1986) proved:

Theorem 2 (Chowla, Dwork, Evans)

Let p and a be as before. Then

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

Goal: Extend this to a congruence mod p^2.
Need *Fermat quotients*: For $m \in \mathbb{Z}$, $m \geq 2$, and $p \nmid m$, define

$$q_p(m) := \frac{m^{p-1} - 1}{p}.$$

Beukers (1984) conjectured, and Chowla, Dwork & Evans (1986) proved:

Theorem 2 (Chowla, Dwork, Evans)

Let p and a be as before. Then

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

Application: Search for Wilson primes.

2. Gauss Factorials

Recall *Wilson's Theorem*: p is a prime if and only if

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

2. Gauss Factorials

Recall *Wilson's Theorem*: p is a prime if and only if

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

Define the *Gauss factorial*

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

2. Gauss Factorials

Recall *Wilson's Theorem*: p is a prime if and only if

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

Define the *Gauss factorial*

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

Theorem 3 (Gauss)

For any integer $n \ge 2$,

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

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

Recall Gauss' Theorem:

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

Recall Gauss' Theorem:

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

Can we have something like this for p^2 in place of p, using Gauss factorials?

Recall Gauss' Theorem:

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

Can we have something like this for p^2 in place of p, using Gauss factorials?

Idea: Use the mod p^2 extension by Chowla et al.

Recall Gauss' Theorem:

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

Can we have something like this for p^2 in place of p, using Gauss factorials?

Idea: Use the mod p^2 extension by Chowla et al.

Main technical device: We can show that

$$\left(\frac{p^2-1}{2}\right)_p ! \equiv (p-1)!^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \left(1 + \frac{p-1}{2} p \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j}\right) \pmod{p^2}.$$

We can derive a similar congruence for

$$\left(\frac{p^2-1}{4}\right)_p! \pmod{p^2}.$$

We can derive a similar congruence for

$$\left(\frac{p^2-1}{4}\right)_p! \pmod{p^2}.$$

Also used is the congruence

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j} \equiv -2\,q_p(2) \pmod{p},$$

and other similar congruences due to Emma Lehmer (1938) and others before her.

We can derive a similar congruence for

$$\left(\frac{p^2-1}{4}\right)_p! \pmod{p^2}.$$

Also used is the congruence

$$\sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j} \equiv -2\,q_p(2) \pmod{p},$$

and other similar congruences due to Emma Lehmer (1938) and others before her.

Altogether we have, after simplifying,

$$\frac{\left(\frac{p^2-1}{2}\right)_p!}{\left(\left(\frac{p^2-1}{4}\right)_p!\right)^2} \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \frac{1}{1+\frac{1}{2}pq_p(2)} \pmod{p^2}.$$

Combining this with the theorem of Chowla, Dwork & Evans:

Theorem 4

Let p and a be as before. Then

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

Combining this with the theorem of Chowla, Dwork & Evans:

Theorem 4

Let p and a be as before. Then

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

- Hopeless to conjecture an extension of the theorem of Chowla et al.,

- but easily possible for the theorem above.

3. Extensions modulo p^3

By numerical experimentation we first conjectured

Theorem 5

Let p and a be as before. Then

$$\frac{\left(\frac{p^3-1}{2}\right)_p!}{\left(\left(\frac{p^3-1}{4}\right)_p!\right)^2} \equiv 2a - \frac{p}{2a} - \frac{p^2}{8a^3} \pmod{p^3}.$$

(Proof later).

3. Extensions modulo p^3

By numerical experimentation we first conjectured

Theorem 5

Let p and a be as before. Then

$$\frac{\left(\frac{p^3-1}{2}\right)_p!}{\left(\left(\frac{p^3-1}{4}\right)_p!\right)^2} \equiv 2a - \frac{p}{2a} - \frac{p^2}{8a^3} \pmod{p^3}.$$

(Proof later).

Using more complicated congruences than the ones leading to Theorem 4 (but the same ideas), and going *backwards*, we obtain

Theorem 6 (Main result)

Let p and a be as before. Then

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

Theorem 6 (Main result)

Let p and a be as before. Then

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

Here E_{p-3} is the Euler number defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n \qquad (|t| < \pi).$$

Theorem 6 (Main result)

Let p and a be as before. Then

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

Here E_{p-3} is the Euler number defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n \qquad (|t| < \pi).$$

How can we prove Theorem 5?

Theorem 6 (Main result)

Let p and a be as before. Then

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

Here E_{p-3} is the Euler number defined by

$$\frac{2}{e^t + e^{-t}} = \sum_{n=0}^{\infty} \frac{E_n}{n!} t^n \qquad (|t| < \pi).$$

How can we prove Theorem 5?
By further experimentation we first conjectured, and then proved the following generalization.

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

$$\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \equiv 2a-1\cdot\frac{p}{2a}-1\cdot\frac{p^2}{8a^3}$$

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

$$\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \equiv 2a - 1 \cdot \frac{p}{2a} - 1 \cdot \frac{p^2}{8a^3} - 2 \cdot \frac{p^3}{(2a)^5}$$

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

$$\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \equiv 2a - 1\cdot\frac{p}{2a} - 1\cdot\frac{p^2}{8a^3} - 2\cdot\frac{p^3}{(2a)^5} - 5\cdot\frac{p^4}{(2a)^7}$$

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

$$\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2} \equiv 2a - 1\cdot\frac{p}{2a} - 1\cdot\frac{p^2}{8a^3} - 2\cdot\frac{p^3}{(2a)^5} - 5\cdot\frac{p^4}{(2a)^7} - 14\cdot\frac{p^5}{(2a)^9}$$

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

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

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

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

Here $C_n := \frac{1}{n+1}\binom{2n}{n}$ is the nth Catalan number which is always an integer.

Theorem 7

Let p and a be as before and let $\alpha \geq 2$ be an integer. Then

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

Here $C_n := \frac{1}{n+1}\binom{2n}{n}$ is the nth Catalan number which is always an integer.

Theorem 5 is obviously a special case of Theorem 7.

4. Main Ingredients in the Proof

- The Jacobi sum

$$J(\chi,\psi)=\sum_{j \bmod p}\chi(j)\psi(1-j),$$

where χ and ψ are characters modulo p.

4. Main Ingredients in the Proof

- The Jacobi sum

$$J(\chi,\psi)=\sum_{j \bmod p}\chi(j)\psi(1-j),$$

where χ and ψ are characters modulo p.

- Fix a primitive root g mod p;
let χ be a character of order 4 such that $\chi(g)=i$.

4. Main Ingredients in the Proof

- The Jacobi sum

$$J(\chi,\psi)=\sum_{j \bmod p}\chi(j)\psi(1-j),$$

where χ and ψ are characters modulo p.

- Fix a primitive root g mod p;
let χ be a character of order 4 such that $\chi(g)=i$.
Define integers a', b' by

$$p=a'^2+b'^2,\quad a'\equiv\left(\frac{2}{p}\right)\pmod 4,\quad b'\equiv a'g^{(p-1)/4}\pmod p.$$

4. Main Ingredients in the Proof

- The Jacobi sum

$$J(\chi,\psi)=\sum_{j \bmod p}\chi(j)\psi(1-j),$$

where χ and ψ are characters modulo p.

- Fix a primitive root g mod p;
let χ be a character of order 4 such that $\chi(g)=i$.
Define integers a', b' by

$$p=a'^2+b'^2,\quad a'\equiv\left(\frac{2}{p}\right)\pmod 4,\quad b'\equiv a'g^{(p-1)/4}\pmod p.$$

These are uniquely defined, differ from a and b of Gauss' theorem only (possibly) in sign.

- Then

$$J(\chi,\chi) = (-1)^{\frac{p-1}{4}}(a' + ib'),$$
$$J(\chi^3,\chi^3) = (-1)^{\frac{p-1}{4}}(a' - ib'),$$

- Then

$$J(\chi,\chi) = (-1)^{\frac{p-1}{4}}(a' + ib'),$$
$$J(\chi^3,\chi^3) = (-1)^{\frac{p-1}{4}}(a' - ib'),$$

- On the other hand,

$$J(\chi,\chi) \equiv 0 \pmod{p},$$
$$J(\chi^3,\chi^3) = \frac{\Gamma_p(1-\frac{1}{2})}{\Gamma_p(1-\frac{1}{4})^2}.$$

These are deep results, related to the “Gross-Koblitz formula" (see, e.g., *Gauss and Jacobi Sums* by B. Berndt, R. Evans and K. Williams).

- $\Gamma_p(z)$ is the p-adic gamma function defined by

$$F(n) := (-1)^n \prod_{\substack{0<j<n \\ p\nmid j}} j,$$

$$\Gamma_p(z) = \lim_{n\to z} F(n) \qquad (z \in \mathbb{Z}_p),$$

where n runs through any sequence of positive integers p-adically approaching z.

- In particular,

$$
\begin{aligned}
(-1)^{\frac{p-1}{4}}(a' - ib') = J(\chi^3, \chi^3) &= \frac{\Gamma_p(1-\frac{1}{2})}{\Gamma_p(1-\frac{1}{4})^2} \\
&\equiv \frac{\Gamma_p(1+\frac{p^\alpha-1}{2})}{\Gamma_p(1+\frac{p^\alpha-1}{4})^2} \pmod{p^\alpha} \\
&= \frac{F(1+\frac{p^\alpha-1}{2})}{F(1+\frac{p^\alpha-1}{4})^2} \\
&= -\frac{\left(\frac{p^\alpha-1}{2}\right)_p!}{\left(\left(\frac{p^\alpha-1}{4}\right)_p!\right)^2}.
\end{aligned}
$$

- Raise

$$(-1)^{\frac{p-1}{4}}(a' + ib') = J(\chi, \chi) \equiv 0 \pmod{p}$$

to the power α:

- Raise

$$(-1)^{\frac{p-1}{4}}(a' + ib') = J(\chi, \chi) \equiv 0 \pmod{p}$$

to the power α:

$$(a' + ib')^{\alpha} \equiv 0 \pmod{p^{\alpha}}.$$

- Raise

$$(-1)^{\frac{p-1}{4}}(a' + ib') = J(\chi, \chi) \equiv 0 \pmod{p}$$

to the power α:

$$(a' + ib')^{\alpha} \equiv 0 \pmod{p^{\alpha}}.$$

- Expand the left-hand side; get binomial coefficients;

- Raise

$$(-1)^{\frac{p-1}{4}}(a' + ib') = J(\chi, \chi) \equiv 0 \pmod{p}$$

to the power α:

$$(a' + ib')^{\alpha} \equiv 0 \pmod{p^{\alpha}}.$$

- Expand the left-hand side; get binomial coefficients;
- separate real and imaginary parts;

- Raise

$$(-1)^{\frac{p-1}{4}}(a' + ib') = J(\chi, \chi) \equiv 0 \pmod{p}$$

to the power α:

$$(a' + ib')^{\alpha} \equiv 0 \pmod{p^{\alpha}}.$$

- Expand the left-hand side; get binomial coefficients;
- separate real and imaginary parts;
- use the combinatorial identity ($k = 0, 1, \ldots, n-1$)

$$\sum_{j=0}^{k} \frac{(-1)^j}{j+1} \binom{2j}{j} \binom{n+j-k}{k-j} = \binom{n-1-k}{k};$$

- Raise

$$(-1)^{\frac{p-1}{4}}(a' + ib') = J(\chi, \chi) \equiv 0 \pmod{p}$$

to the power α:

$$(a' + ib')^{\alpha} \equiv 0 \pmod{p^{\alpha}}.$$

- Expand the left-hand side; get binomial coefficients;
- separate real and imaginary parts;
- use the combinatorial identity ($k = 0, 1, \ldots, n-1$)

$$\sum_{j=0}^{k} \frac{(-1)^j}{j+1} \binom{2j}{j} \binom{n+j-k}{k-j} = \binom{n-1-k}{k};$$

- putting everything together, we obtain Theorem 7.

5. A Jacobi Analogue

Let $p \equiv 1 \pmod 6$. Then we can write

$$4p = r^2 + 3s^2, \qquad r \equiv 1 \pmod 3, \qquad 3 \mid s,$$

which determines r uniquely.

5. A Jacobi Analogue

Let $p \equiv 1 \pmod 6$. Then we can write

$$4p = r^2 + 3s^2, \qquad r \equiv 1 \pmod 3, \qquad 3 \mid s,$$

which determines r uniquely.

In analogy to Gauss' Theorem 1 we have

Theorem 8 (Jacobi, 1837)

Let p and r be as above. Then

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

5. A Jacobi Analogue

Let $p \equiv 1 \pmod 6$. Then we can write

$$4p = r^2 + 3s^2, \qquad r \equiv 1 \pmod 3, \qquad 3 \mid s,$$

which determines r uniquely.

In analogy to Gauss' Theorem 1 we have

Theorem 8 (Jacobi, 1837)

Let p and r be as above. Then

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

This was generalized to mod p^2 independently by Evans (unpublished, 1985) and Yeung (1989):

Theorem 9 (Evans; Yeung)

Let p and r be as above. Then

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

Theorem 9 (Evans; Yeung)

Let p and r be as above. Then

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

With methods similar to those in the first part of this talk, we proved

Theorem 10

Let p and r be as above. Then

$$\binom{\frac{2(p-1)}{3}}{\frac{p-1}{3}} \equiv \left(-r + \frac{p}{r} + \frac{p^2}{r^3}\right)\left(1 + \frac{1}{6}p^2 B_{p-2}(\tfrac{1}{3})\right) \pmod{p^3}.$$

Here $B_n(x)$ is the nth Bernoulli polynomial.

6. More on Gauss Factorials

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

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

6. More on Gauss Factorials

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

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

Thus, with Wilson's Theorem,

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

6. More on Gauss Factorials

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

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

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).

6. More on Gauss Factorials

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

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

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

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

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

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

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

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

What is the sign on the right?

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

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

What is the sign on the right?

Theorem 11 (Mordell, 1961)

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

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

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

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

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

What is the sign on the right?

Theorem 11 (Mordell, 1961)

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

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

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

Discovered independently by Chowla.

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

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

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

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

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

and denote them, respectively, by

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

By Wilson's theorem:

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

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

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

Natural extension:

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

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

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

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

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	**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

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	**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

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 below).

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 below).

In contrast: No primes p for which

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

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

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 below).

In contrast: No primes p for which

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

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

The theorems of Gauss and Jacobi can be used to explain this:

Consider the quotient

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

Consider the quotient

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

Consider the quotient

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

Consider the quotient

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

Consider the quotient

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

Recall Gauss' theorem:

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

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

Consider the quotient

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

Recall Gauss' theorem:

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

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

It follows easily that

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

Consider the quotient

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

Recall Gauss' theorem:

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

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

It follows easily that

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

Similarly, Jacobi's theorem 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 12

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 12

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 13

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

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

Corollary 13

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 13

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 13

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

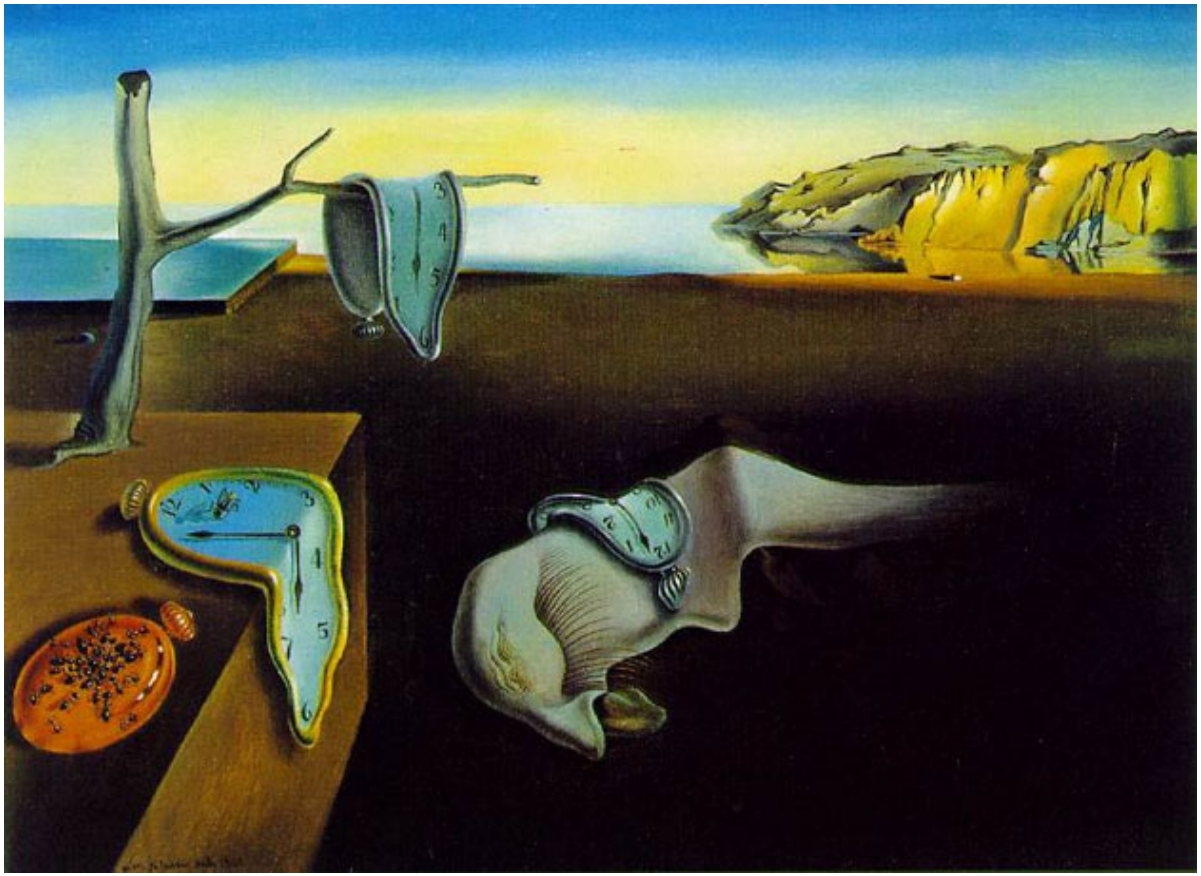
(a) $\frac{p-1}{4}! \equiv 1 \pmod p$ *only if* $p = 5$.

(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.

How are we doing with time?



Salvador Dalí, *The Persistence of Memory*, 1931.

7. Composite Moduli

Recall Gauss' generalization of Wilson's theorem,
the prototype of all composite modulus extensions:

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

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

7. Composite Moduli

Recall Gauss' generalization of Wilson's theorem,
the prototype of all composite modulus extensions:

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

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

Everything we did before can be extended to composite moduli.

7. Composite Moduli

Recall Gauss' generalization of Wilson's theorem,
the prototype of all composite modulus extensions:

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

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

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:

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

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

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;

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

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.

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).

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.

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 $\phi_{1,1}(n) = \phi(n)$.

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 $\phi_{2,1}(n) = \phi_{2,2}(n) = \frac{1}{2}\phi(n)$.

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.

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 14 (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 14 (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 Are the Partial Products Congruent to each other?

When Are the Partial Products Congruent to each other?

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

When Are the Partial Products Congruent to each other?

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 15

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 15

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.

This observation holds in general:

Theorem 15

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.

On the other hand, condition is sufficient but not necessary.

Idea of proof:

1. Observe that

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

Idea of proof:

1. Observe that

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

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

Idea of proof:

1. Observe that

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

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

3. 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:

1. Observe that

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

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

3. 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."

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

Idea of proof:

1. Observe that

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

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

3. 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."

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

5. Carefully count which elements to include/exclude.

Idea of proof:

1. Observe that

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

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

3. 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."

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

5. Carefully count which elements to include/exclude.

6. Use Chinese Remainder Theorem modulo $q^\beta w$ and $q^\alpha w$.

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

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

Theorem 16

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

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

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

Theorem 16

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 previous result.

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 $\pmod{M}$

Outlook

Main task: Understand the multiplicative orders of

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

Outlook

Main task: Understand the multiplicative orders of

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

When $M = 2$: Completely determined.

Outlook

Main task: Understand the multiplicative orders of

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

When $M = 2$: Completely determined.

Let $M \geq 3$ and $n \equiv 1 \pmod{M}$.

Outlook

Main task: Understand the multiplicative orders of

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

When $M = 2$: Completely determined.

Let $M \geq 3$ and $n \equiv 1 \pmod{M}$. Then, when

- n has ≥ 3 prime factors $\equiv 1 \pmod{M}$: order is always 1.

Outlook

Main task: Understand the multiplicative orders of

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

When $M = 2$: Completely determined.

Let $M \geq 3$ and $n \equiv 1 \pmod{M}$. Then, when

- n has ≥ 3 prime factors $\equiv 1 \pmod{M}$: order is always 1.
- n has 2 prime factors $\equiv 1 \pmod{M}$: order is a divisor of M.

Outlook

Main task: Understand the multiplicative orders of

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

When $M = 2$: Completely determined.

Let $M \geq 3$ and $n \equiv 1 \pmod{M}$. Then, when

- n has ≥ 3 prime factors $\equiv 1 \pmod{M}$:
  order is always 1.

- n has 2 prime factors $\equiv 1 \pmod{M}$:
  order is a divisor of M.

- n has 0 or 1 prime factor $\equiv 1 \pmod{M}$:
  – The most interesting and difficult case.
  – Several results already published.
  – Further work in progress.

Thank you – Danke