Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients

John B. Cosgrave[1], Karl Dilcher[2]

[1]Dublin, Ireland
[2]Dalhousie University, Halifax, Canada

The Fields Institute, September 22, 2009

We begin with a table:

p	$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$	(mod 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	$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$	(mod 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".

To extend this to a congruence $\mod p^2$, we need the concept of a *Fermat quotient*: For $m \in \mathbb{Z}$, $m \geq 2$, and $p \nmid m$, define

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

To extend this to a congruence $\pmod{p^2}$, we need the concept of a *Fermat quotient*: 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

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

To extend this to a congruence $\pmod{p^2}$, we need the concept of a *Fermat quotient*: 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

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

Application: Search for Wilson primes, $(p-1)! \equiv -1 \pmod{p^2}$.

To extend this to a congruence $\pmod{p^2}$, we need the concept of a *Fermat quotient*: 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

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

Application: Search for Wilson primes, $(p-1)! \equiv -1 \pmod{p^2}$. Can this be extended further?

2. Interlude: Gauss Factorials

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

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

2. Interlude: 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. Interlude: 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 $n \ge 2$,

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

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

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

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

While it would be quite hopeless to conjecture an extension of the theorem of Chowla et al., this is 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

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

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 ($k = 0, 1, \dots, n-1$)

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

- 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.

Thank you