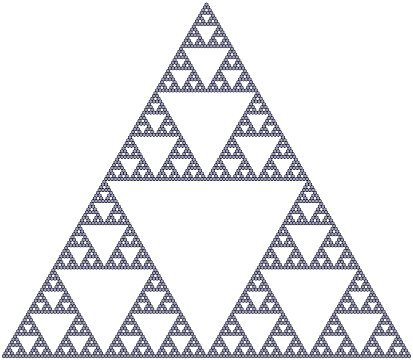
Lucas congruences modulo p^2

Eric Rowland
Hofstra University

Experimental Mathematics Seminar
Rutgers University, 2021–11–4

Pascal's triangle

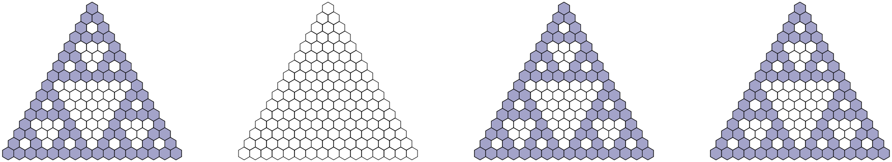
Which does Pascal's triangle look like modulo 2? First 128 rows:



Explored by many people, probably including Lucas in the 1870s.

4 subsequences:

$\binom{2n+0}{2m+0}$ $\binom{2n+0}{2m+1}$ $\binom{2n+1}{2m+0}$ $\binom{2n+1}{2m+1}$



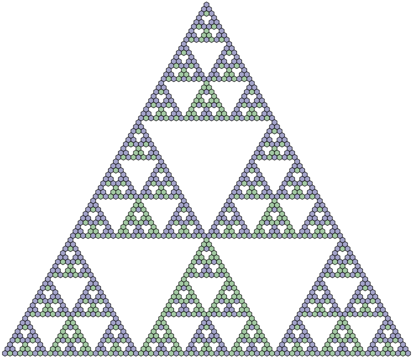
If $0 \leq r \leq 1$ and $0 \leq s \leq 1$, then

$$\binom{2n+r}{2m+s} \equiv \begin{cases} 0 \mod 2 & \text{if } r = 0 \text{ and } s = 1 \\ \binom{n}{m} \mod 2 & \text{otherwise.} \end{cases}$$

What's special about $r = 0, s = 1$?

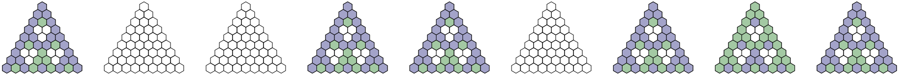
$\binom{0}{0} = 1$ $\binom{0}{1} = 0$ $\binom{1}{0} = 1$ $\binom{1}{1} = 1$

Modulo 3:

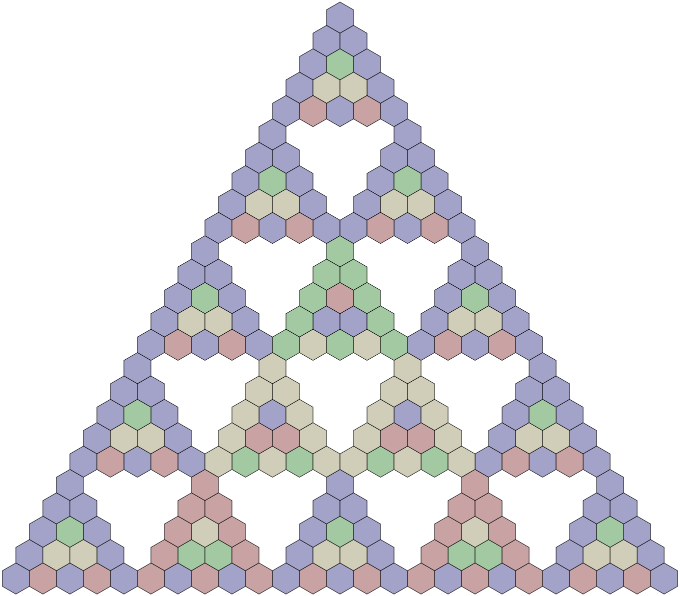


9 subsequences:

$\binom{3n+0}{3m+0}$ $\binom{3n+0}{3m+1}$ $\binom{3n+0}{3m+2}$ $\binom{3n+1}{3m+0}$ $\binom{3n+1}{3m+1}$ $\binom{3n+1}{3m+2}$ $\binom{3n+2}{3m+0}$ $\binom{3n+2}{3m+1}$ $\binom{3n+2}{3m+2}$



Modulo 5:



Theorem (Édouard Lucas 1878)

Let p be a prime. If $n \geq 0$, $m \geq 0$, and $r, s \in \{0, 1, \ldots, p-1\}$, then

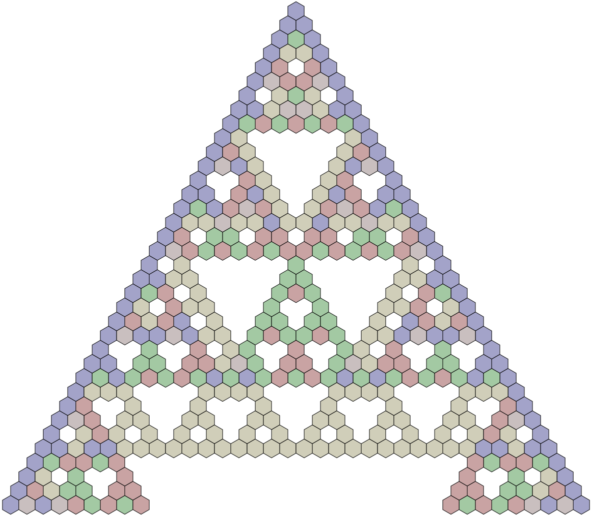
$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s} \mod p.$$

Iterate:
If $n_\ell, \ldots, n_1, n_0, m_\ell, \ldots, m_1, m_0$ are elements of $\{0, 1, \ldots, p-1\}$, then

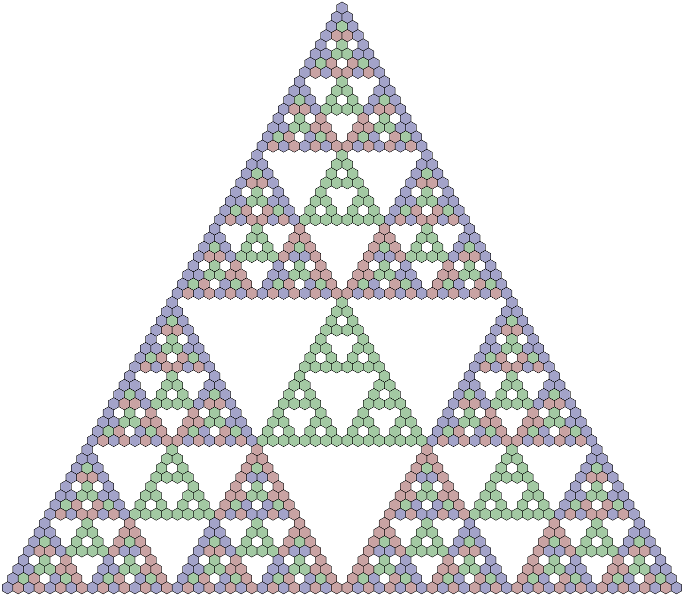
$$\binom{n_\ell p^\ell + \cdots + n_1 p + n_0}{m_\ell p^\ell + \cdots + m_1 p + m_0} \equiv \binom{n_\ell}{m_\ell} \cdots \binom{n_1}{m_1}\binom{n_0}{m_0} \mod p.$$

What about non-primes?

Modulo 6:



Modulo 4:



Does the Lucas congruence hold modulo p^2?

$$\binom{pn+r}{pm+s} \stackrel{?}{\equiv} \binom{n}{m}\binom{r}{s} \mod p^2$$

Counterexample

Let $p = 2$.

$$\binom{2\cdot 1+0}{2\cdot 0+1} = \binom{2}{1} = 2 \not\equiv 0 = \binom{1}{0}\binom{0}{1} \mod 4$$

However, $\binom{pn}{pm} \equiv \binom{n}{m} \mod p^2$.

Jacobsthal 1949: If $p \geq 5$, then $\binom{pn}{pm} \equiv \binom{n}{m} \mod p^3$.

Bailey 1990: If $p \geq 5$ and $r, s \in \{0, 1, \dots, p-1\}$, then

$$\binom{p^3 n+r}{p^3 m+s} \equiv \binom{n}{m}\binom{r}{s} \mod p^3.$$

Apéry numbers

$$A(n) := \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$$ arose in Apéry's proof that $\zeta(3)$ is irrational.

$A(n)_{n\geq 0}$: $1, 5, 73, 1445, 33001, 819005, 21460825, \dots$

Theorem (Gessel 1982)

Let p be a prime. The Apéry numbers satisfy the Lucas congruence

$$A(pn+d) \equiv A(n)A(d) \mod p$$

for all $n \geq 0$ and all $d \in \{0, 1, \dots, p-1\}$.

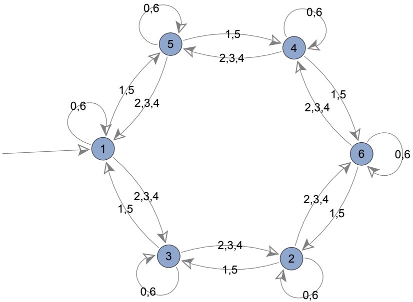
$A(n)$ modulo 7:

$1, 5, 3, 3, 3, 5, 1,\ \ 5, 4, 1, 1, 1, 4, 5,\ \ 3, 1, 2, 2, 2, 1, 3,\ \ \ldots$

Example

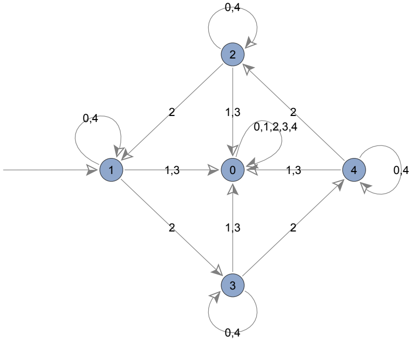
$$A(2039) = A(5642_7) \equiv A(5)A(6)A(4)A(2) \equiv 5 \cdot 1 \cdot 3 \cdot 3 \equiv 3 \mod 7.$$

Automaton:



$A(n)$ modulo 5:

$1, 0, 3, 0, 1,\ \ 0, 0, 0, 0, 0,\ \ 3, 0, 4, 0, 3,\ \ 0, 0, 0, 0, 0,\ \ \ldots$

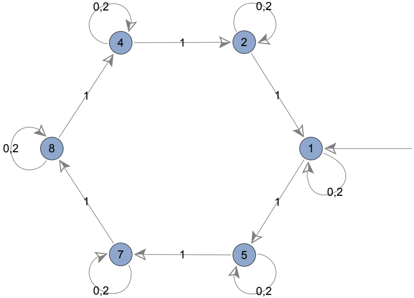


If the base-5 digits of n contain 1 or 3, then $A(n) \equiv 0 \mod 5$.

$A(n)$ modulo 9:

Theorem (Gessel)

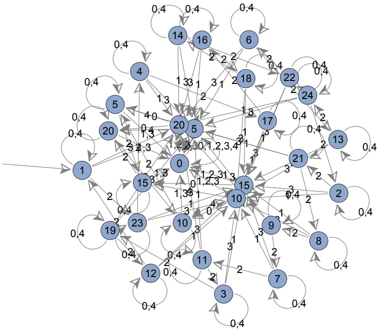
$A(3n + d) \equiv A(n)A(d) \mod 9$ *for all* $n \geq 0$ *and all* $d \in \{0, 1, 2\}$.

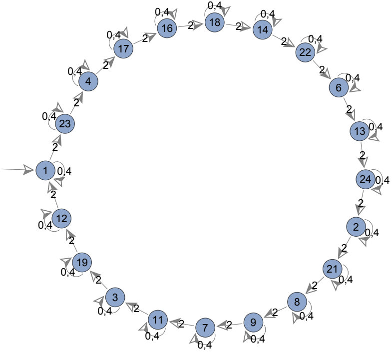


The Lucas congruence does not always hold modulo p^2:

$$\begin{aligned} A(5 \cdot 2 + 1) &= A(11) = 403676083788125 \\ &\not\equiv 365 = 73 \cdot 5 = A(2)A(1) \mod 25. \end{aligned}$$

$A(n)$ modulo 25:





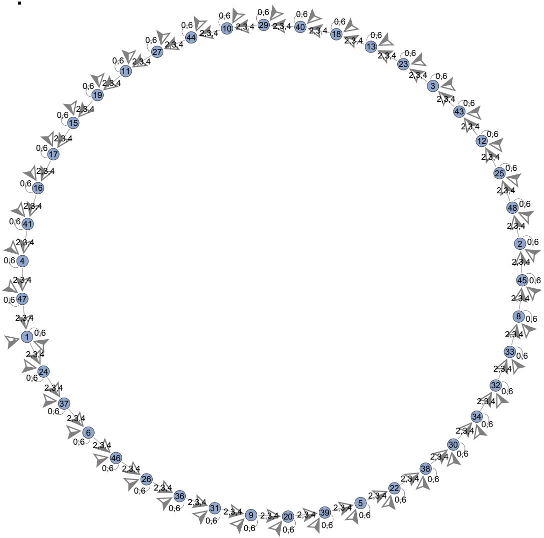
Restrict the digit set.

Theorem (Rowland–Yassawi 2015)

$A(5n + d) \equiv A(n)A(d) \mod 25$ *for all* $n \geq 0$ *and all* $d \in \{0, 2, 4\}$.

Which digits support a Lucas congruence for $A(n)$ modulo p^2?

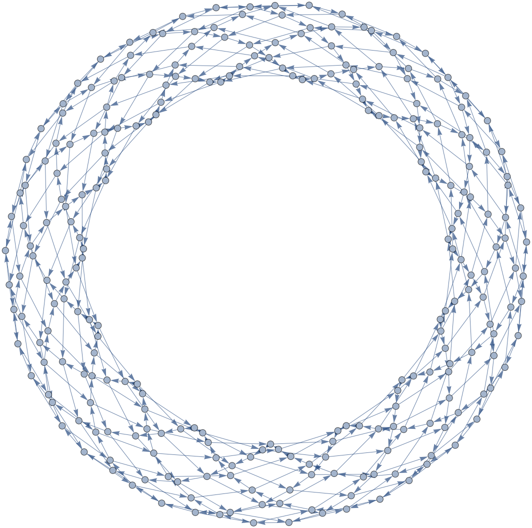
$A(n)$ modulo 7^2:



digit set: $\{0, 2, 3, 4, 6\}$

$$(A(0), A(2), A(3), A(4), A(6)) \equiv (1, 24, 24, 24, 1) \mod 7^2$$

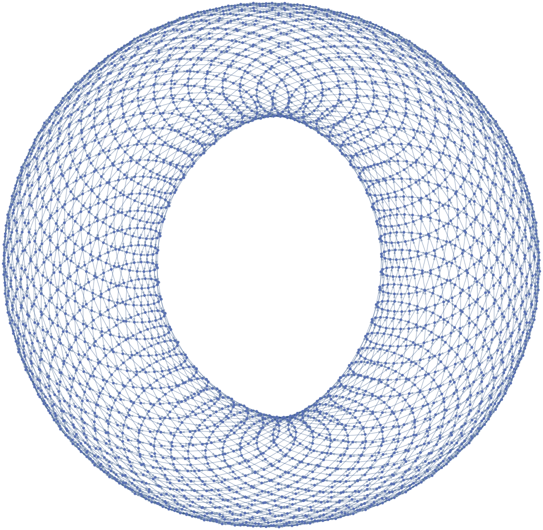
$A(n)$ modulo 23^2:



digit set: $\{0, 7, 11, 15, 22\}$

$$(A(0), A(7), A(11), A(15), A(22)) \equiv (1, 415, 473, 415, 1) \mod 23^2$$

$A(n)$ modulo 59^2:



digit set: $\{0, 6, 29, 52, 58\}$

$(A(0), A(6), A(29), A(52), A(58)) \equiv (1, 460, 2813, 460, 1) \mod 59^2$

Reflection symmetry:

Theorem (Malik–Straub 2016)

$A(d) \equiv A(p-1-d) \mod p$ *for each* $d \in \{0, 1, \ldots, p-1\}$.

Let $D_A(p) := \left\{ d \in \{0, 1, \ldots, p-1\} : A(d) \equiv A(p-1-d) \mod p^2 \right\}$.

In particular, $\{0, \frac{p-1}{2}, p-1\} \subseteq D_A(p)$. $\{0, 2, 4\} \subseteq D_A(5)$

Theorem (Rowland–Yassawi 2021)

Let p be a prime and $d \in \{0, 1, \ldots, p-1\}$. The congruence

$$A(pn + d) \equiv A(n)A(d) \mod p^2$$

holds for all $n \geq 0$ if and only if $d \in D_A(p)$.

Size of $D_A(p)$ for the nth prime:

$$2, 3, 3, 5, 3, 3, 3, 3, 5, 3, 3, 3, 3, 7, 3, 3, 5, \dots \quad \text{[A348883]}$$

Primes p with $|D_A(p)| \geq 4$:

p	$D_A(p)$
7	$\{0, 2, 3, 4, 6\}$
23	$\{0, 7, 11, 15, 22\}$
43	$\{0, 5, 18, 21, 24, 37, 42\}$
59	$\{0, 6, 29, 52, 58\}$
79	$\{0, 18, 39, 60, 78\}$
103	$\{0, 17, 51, 85, 102\}$
107	$\{0, 14, 21, 47, 53, 59, 85, 92, 106\}$
127	$\{0, 17, 63, 109, 126\}$
131	$\{0, 62, 65, 68, 130\}$
139	$\{0, 68, 69, 70, 138\}$
151	$\{0, 19, 75, 131, 150\}$
167	$\{0, 35, 64, 83, 102, 131, 166\}$

How does $\sum_{p \leq x} |D_A(p)|$ grow?

Binomial coefficients

Let $D(p)$ be the set of pairs (r, s) such that

$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s} \mod p^2$$

for all $n \geq 0$ and $m \geq 0$.

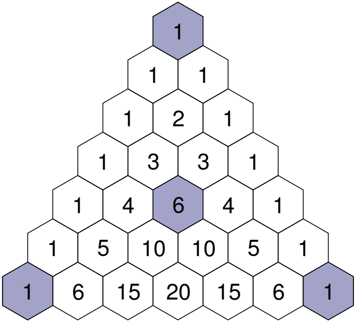
Which pairs belong to $D(p)$?

Experimentally...
$D(2) = \{(0,0)\}$
$D(3) = \{(0,0), (2,0), (2,2)\}$
$D(5) = \{(0,0), (4,0), (4,4)\}$

Since $\binom{pn}{pm} \equiv \binom{n}{m} \mod p^2$, $D(p)$ contains the pair $(0,0)$.

$p = 7$:

$D(7) = \{(0,0), (4,2), (6,0), (6,6)\}$

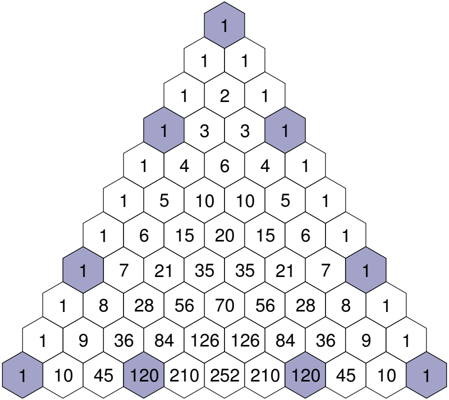


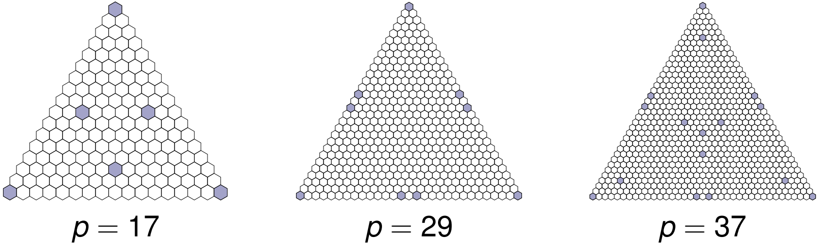
Example

$\binom{12002}{7156} \equiv \binom{4}{2}\binom{6}{6}\binom{6}{6}\binom{6}{0}\binom{4}{2} \equiv 6 \cdot 1 \cdot 1 \cdot 1 \cdot 6 = 36 \mod 7^2.$

$p = 11$:

$D(11) = \{(0,0),(3,0),(3,3),(7,0),(7,7),(10,0),(10,3),(10,7),(10,10)\}$

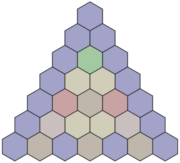




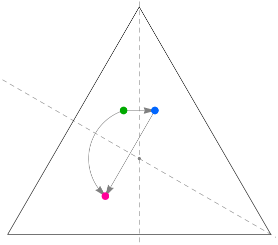
$D(p)$ seems to possess the symmetries of the equilateral triangle!

Reflection symmetry through the vertical axis follows (after some work) from reflection symmetry in Pascal's triangle.

But the first p rows modulo p are not invariant under rotation.



Where does rotation by 120° take a point (r, s)?



First reflection: $(r, s) \mapsto (r, r - s)$
Second reflection: $(r, s) \mapsto (p - 1 - r + s, s)$
Rotation: $(r, s) \mapsto (p - 1 - s, r - s)$

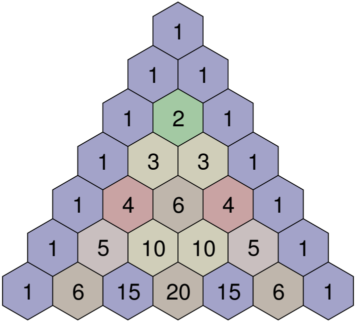
The three binomial coefficients visited by the orbit of (r, s) are

$$\binom{r}{s}, \binom{p-1-s}{r-s}, \binom{p-1-r+s}{s}.$$

If $0 \leq s \leq r \leq p-1$, then

$$\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \mod p.$$

$p = 7$:



$$\binom{1}{0} = 1 \equiv -6 = (-1)^{1-0}\binom{7-1-0}{1-0} \mod 7$$
$$\binom{2}{1} = 2 \equiv -5 = (-1)^{2-1}\binom{7-1-1}{2-1} \mod 7$$
$$\binom{4}{1} = 4 \equiv -10 = (-1)^{4-1}\binom{7-1-1}{4-1} \mod 7$$

Theorem (Rowland)

Let p be a prime and $0 \le s \le r \le p-1$. The following are equivalent.

- $(r,s) \in D(p)$; *that is, the congruence* $\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s} \mod p^2$ *holds for all* $n \ge 0$ *and* $m \ge 0$.
- $\binom{r}{s} \equiv (-1)^{r-s}\binom{p-1-s}{r-s} \equiv (-1)^{s}\binom{p-1-r+s}{s} \mod p^2$.
- $H_r \equiv H_{r-s} \equiv H_s \mod p$.

$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is the nth harmonic number.
$(H_n)_{n \ge 0}$: $0, 1, \frac{3}{2}, \frac{11}{6}, \frac{25}{12}, \frac{137}{60}, \frac{49}{20}, \frac{363}{140}, \dots$
When $n \le p-1$, we interpret $H_n \bmod p$ by inverting the denominator.

Size of $D(p)$ for the nth prime:

$$1, 3, 3, 4, 9, 4, 6, 4, 3, 9, 4, 16, 6, 10, 3, 9, 3, 10, \dots \quad \text{[A348884]}$$

In general:

Theorem

Let p be a prime. If $n \geq 0$, $m \geq 0$, and $r, s \in \{0, 1, \ldots, p-1\}$, then

$$\binom{pn+r}{pm+s} \equiv \binom{n}{m}\binom{r}{s}\left(1 + pn\left(H_r - H_{r-s}\right) + pm\left(H_{r-s} - H_s\right)\right) \mod p^2.$$

When

$$H_r - H_{r-s} \equiv 0 \mod p \quad \text{and} \quad H_{r-s} - H_s \equiv 0 \mod p,$$

we obtain a Lucas congruence.

Center of the triangle:

Corollary

If $p \equiv 1 \mod 3$, *$n \geq 0$, and $m \geq 0$, then*

$$\binom{pn + \frac{2}{3}(p-1)}{pm + \frac{1}{3}(p-1)} \equiv \binom{n}{m}\binom{\frac{2}{3}(p-1)}{\frac{1}{3}(p-1)} \mod p^2.$$

Jacobi studied $\binom{2(p-1)/3}{(p-1)/3}$ modulo p.

Yeung 1989: $\binom{2(p-1)/3}{(p-1)/3} \equiv -a + \frac{p}{a} \mod p^2$, where $4p = a^2 + 27b^2$ and the sign of a is chosen so that $a \equiv 1 \mod 3$.

Edge midpoints:

$\{(\frac{p-1}{2}, 0), (\frac{p-1}{2}, \frac{p-1}{2}), (p-1, \frac{p-1}{2})\} \subseteq D(p) \iff 2^{p-1} \equiv 1 \mod p^2$.

These are Wieferich primes. Only two are known: 1093, 3511.

$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} \mod p^2$

Why do harmonic numbers arise?

Lemma

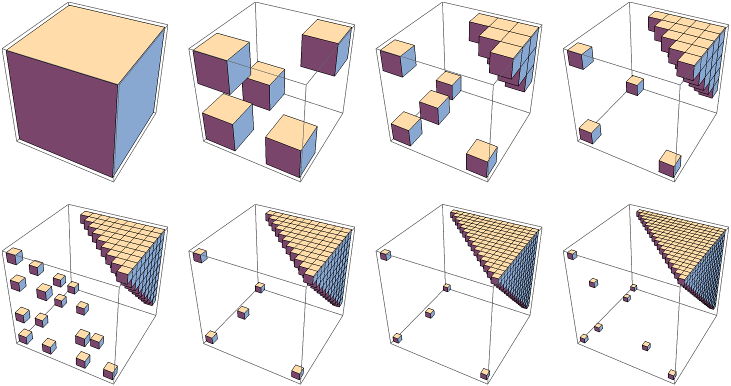
If $0 \leq s \leq r \leq p-1$, then $H_r \equiv H_s \mod p$ if and only if

$$\binom{r}{s} \equiv (-1)^{r-s} \binom{p-1-s}{r-s} \mod p^2.$$

$$\begin{aligned}(p-1-s)! &= \prod_{i=s+1}^{p-1} (p-i) \\ &\equiv \prod_{i=s+1}^{p-1} (-i) + p\,(-1)^{p-1-s} \frac{(p-1)!}{s!} \sum_{i=s+1}^{p-1} \frac{1}{-i} \mod p^2 \\ &= (-1)^{p-1-s} \frac{(p-1)!}{s!} \left(1 - p\,(H_{p-1} - H_s)\right).\end{aligned}$$

Multinomial coefficients

Joshua Crisafi is currently looking at generalizations.



2-argument multinomial $\frac{(m+n)!}{m!n!}$ seems to be more natural than $\frac{n!}{m!(n-m)!}$:
The orbit of (r, s) contains $(p - 1 - r - s, r)$ and $(s, p - 1 - r - s)$.