

Write \equiv_k for equivalence modulo p^k , where p is prime.

The claim is that $\binom{pa}{pb} \equiv_2 \binom{a}{b}$ for $a, b \in \mathbb{Z}_{\geq 0}$, $0 \leq b \leq a$.

It suffices to show that the coefficients of powers of x^p in $(1+x)^{pa}$ and $(1+x^p)^a$ are congruent modulo p^2 .

Let $u = 1 + x^p$, and let $v = \frac{(1+x)^p - u}{p} \in \mathbb{Z}[x]$. Then

$$(1+x)^{pa} - (1+x^p)^a = (u+pv)^a - u^a \equiv_2 pau^{a-1}v,$$

and note that the result has no powers of x^p , since v only involves x, x^2, \dots, x^{p-1} .

To prove $\binom{pa}{pb} \equiv_3 \binom{a}{b}$, we need to go one step further and consider the term

$$\binom{a}{2} u^{a-2} p^2 v^2 = \binom{a}{2} (1+x^p)^{a-2} \left(\sum_{k=1}^{p-1} \binom{p}{k} x^k \right)^2$$

The only power of x^p that will appear in v^2 is x^p , so it suffices to prove that

$$\sum_{k=1}^{p-1} \binom{p}{k} \binom{p}{p-k} = \binom{2p}{p} - 2 \equiv_3 0,$$

which is equivalent to showing that

$$\binom{2p}{p} = \frac{(2p)(2p-1)\dots(p+2)(p+1)}{p(p-1)\dots(2)(1)} = 2 \frac{f(1)}{f(0)} \equiv_3 2,$$

where $f(n) = \prod_{i=1}^{p-1} (pn+i)$. Thus it suffices to show that $f(1) \equiv_3 f(0)$.

$$f(1) = \prod_{i=1}^{p-1} (i+p) = f(0) + p \sum_{i=1}^{p-1} \frac{f(1)}{i+p} + p^2 \sum_{i < j} \frac{f(1)}{(i+p)(j+p)} + \dots$$

We need to show that the second and third terms on the right hand side vanish modulo p^3 .

But note that

$$\begin{aligned} 2 \sum_{i=1}^{p-1} \frac{1}{p+i} &= \sum_{i=1}^{p-1} \left(\frac{1}{p+i} + \frac{1}{2p-i} \right) \\ &= \sum_{i=1}^{p-1} \frac{3p}{(p+i)(2p-i)} \\ &\equiv_2 3p \sum_{i=1}^{p-1} \frac{1}{-i^2} \equiv_2 -3p \sum_{i^{-1}=1}^{p-1} i^2 \\ &\equiv_2 -3p \frac{2(p-1)p(2p-1)}{6} \equiv_2 0, \end{aligned}$$

when $p > 3$, and further,

$$2 \sum_{i < j} \frac{1}{ij} = \left(\sum_i \frac{1}{i} \right)^2 - \sum_i \frac{1}{i^2} \equiv_1 0.$$