$\binom{p}{m} = \frac{p!}{m!(p-m)!}$ is a positive integer

A little arithmetic

Lemma 26 *For all natural numbers* p *and* m, *if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$.

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

PROOF: Let p and m be natural numbers. Assume $m=0$ or $m=p$. We need show $\binom{p}{m} \equiv 1 \pmod{p}$

Case 1 Assume $m=0$. Then

$$\binom{p}{m} = 1 \equiv 1 \pmod{p}$$

Case 2 Assume $m=p$. Then

$$\binom{p}{m} = 1 \equiv 1 \pmod{p}.$$

$\square$

Lemma 27 *For all integers* p *and* m, *if* p *is prime and* $0 < m < p$ *then* $\binom{p}{m} \equiv 0 \pmod{p}$.

$\binom{p}{m}$ is a multiple of p.

PROOF:

Let p and m be arbitrary integers. Assume p prime and assume $0 < m < p$.

$$\underbrace{\binom{p}{m}}_{\text{an integer}} = \frac{p!}{m!\,(p-m)!} = p \cdot \underbrace{\left[\frac{(p-1)!}{m!\,(p-m)!}\right]}_{\text{Argue it is an integer.}}$$

$\boxed{?}$ Is $\dfrac{(p-1)!}{m!\,(p-m)!}$ an integer? p prime, $0 < m < p$

$$p \cdot \frac{(p-1)!}{m!\,(p-m)!} = l \text{ is an integer.}$$

$$p \cdot (p-1)! = l \cdot m!\,(p-m)!$$

$\Longrightarrow$ by $\boxed{\text{a factorisation argument}}$ that

Fundamental Theorem of Arithmetic.

$l = p \cdot k$ for some integer k

$$\Longrightarrow \cancel{p}\,(p-1)! = \cancel{p} \cdot k \cdot m!\,(p-m)!$$

Proposition 28 *For all prime numbers* p *and integers* $0 \leq m \leq p$, *either* $\binom{p}{m} \equiv 0 \pmod{p}$ *or* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let p be an arbitrary prime and let m be an arbitrary integer. Assume $0 \leq m \leq p$.

Consider 3 cases:

Case 1: $m = 0$

Case 2: $0 < m < p$

Case 3: $m = p$

$\square$

A little more arithmetic

Corollary 29 (The Freshman's Dream) *For all natural numbers* m*,* n *and primes* p*,*

$$(m+n)^p \equiv m^p + n^p \pmod{p} \; .$$

PROOF: Let m and n be integers and p be a prime.
We need show

$$\underbrace{(m+n)^p}_{\|} - (m^p + n^p) \text{ is a multiple of } p.$$

$$\sum_{i=0}^{p} \binom{p}{i} m^i n^{p-i} - m^p - n^p = \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i}$$

$$= p \cdot \left[\sum_{i=1}^{p-1} \underbrace{\left[\frac{(p-1)!}{i!\,(p-i)!} \right]}_{\text{is an int}} m^i \, n^{p-i} \right]$$

and we are done $\square$

$\forall m\, n\; (m+n)^p \equiv m^p + n^p \pmod p$

Corollary 30 (The Dropout Lemma) *For all natural numbers* m *and primes* p,

specialising to the case $n=1$

$$(m+1)^p \equiv m^p + 1 \pmod p \ .$$

Proposition 31 (The Many Dropout Lemma) *For all natural numbers* m *and* i, *and primes* p,

$$(m+i)^p \equiv m^p + i \pmod p \ .$$

PROOF: $\underline{i=0}$: $m^p \equiv m^p \pmod p$ ✓

$\underline{i=1}$: $\forall m\; (m+1)^p \equiv m^p + 1 \pmod p$; i.e. the dropout lemma

$\underline{i=2}$: $\forall k\; (k+2)^p \equiv k^p + 2 \pmod p$

by one dropout lemma

Want to show

$$(k+2)^p \equiv k^p + 2 \pmod{p}$$

$$(k+2)^p = ((k+1)+1)^p \equiv (k+1)^p + 1 \pmod{p}$$

$$\equiv (k^p+1) + 1 \pmod{p}$$

$$= k^p + 2$$

More generally

$$(k+i)^p = ((k+i-1)+1)^p \equiv (k+i-1)^p + 1$$

$$= ((k+i-2)+1)^p + 1 \equiv (k+i-2)^p + 2 = \ldots$$

and iterating i times we get what we want.

$$\forall m\ i \quad (m+i)^p \equiv m^p + i \pmod p$$

In particular, specialising this for $m=0$ we get

$$\boxed{\forall\ i. \quad i^p \equiv i \pmod p}$$

(First part of) Fermat's little Theorem.

$a \quad i \cdot (i^{p-2}) \equiv 1 \pmod{p}$

The Many Dropout Lemma (Proposition 31) gives the fist part of the following very important theorem as a corollary.

Theorem 32 (Fermat's Little Theorem) *For all natural numbers* i *and primes* p,

1. $i^p \equiv i \pmod{p}$, *and*
2. $i^{p-1} \equiv 1 \pmod{p}$ *whenever* i *is not a multiple of* p.

The fact that the first part of Fermat's Little Theorem implies the second one will be proved later on .

Btw

1. Fermat's Little Theorem has applications to:
   (a) primality testing[a],
   (b) the verification of floating-point algorithms, and
   (c) cryptographic security.

[a] For instance, to establish that a positive integer m is not prime one may proceed to find an integer i such that $i^m \not\equiv i \pmod{m}$.