natural $\leadsto$ $\binom{a}{b} = \frac{a!}{b!\,(a-b)!}$

A little arithmetic

Lemma 27 *For all positive integers* p *and natural numbers* m*, if* $m = 0$ *or* $m = p$ *then* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: $\forall$ pos. int. p. $\forall$ nat m.

$$(m = 0 \lor m = p) \implies \binom{p}{m} \equiv 1 \pmod{p}$$

Let p be a pos. int and m a natural.

Assume $m = 0 \lor m = p$

RTP: $\binom{p}{m} \equiv 1 \pmod{p}$

Case 1 $m = 0$

Then $\binom{p}{m} = \binom{p}{0} = 1 \equiv 1 \pmod{p}$

Case 2 : $m = p$

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

$\square$

Lemma 28 *For all integers* p *and* m, *if* p *is prime and* $0 < m < p$ *then* $\binom{p}{m} \equiv 0 \pmod{p}$.

PROOF: $\forall$ int p. $\forall$ int m.

$$\underbrace{(p \text{ prime} \wedge 0 < m < p) \Rightarrow \binom{p}{m} \equiv 0 \pmod{p}}_{\binom{p}{m} \text{ is a multiple of } p}$$

Let p be an int. and m be an int.

~~Assume~~ that p is prime and $0 < m < p$

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

Recall $\binom{p}{m} = \frac{p!}{m!\,(p-m)!} = p \cdot \left[\frac{(p-1)!}{m!\,(p-m)!}\right]$

~~Hence $\binom{p}{m}$ is a multiple of p~~

To exhibit $\binom{p}{m}$ as a multiple of p, it will be enough to show that the fraction

$$\frac{(p-1)!}{m!\,(p-m)!}$$

is in fact an integer.

<u>Exercise</u> Find p NOT prime and m s.t. $\frac{(p-1)!}{m!\,(p-m)!}$ is not an integer.

Know $p \cdot \left[\dfrac{(p-1)!}{m!(p-m)!}\right] = \binom{p}{m}$ is an integer

$\| \quad m$ Fundamental Theorem of Arithmetic

$p_0 \cdot p_1 \cdot \dots \cdot p_k$

p_i primes.

Some p_i should be p

w.l.o.g. say $p_0 = p$

Then $\left[\dfrac{(p-1)!}{m!\,(p-m)!}\right] = p_1 \cdots p_k$

So it is an integer.

$\square$

Proposition 29 *For all prime numbers* p *and integers* $0 \le m \le p$, *either* $\binom{p}{m} \equiv 0 \pmod{p}$ *or* $\binom{p}{m} \equiv 1 \pmod{p}$.

PROOF: Let p be a prime, and let m be an integer $0 \le m \le p$

RTP: $\binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p}$

By cases:

① $m = 0$: $\binom{p}{m} = 1 \equiv 1 \pmod{p}$

② $m = p$: $\binom{p}{m} = 1 \equiv 1 \pmod{p}$

③ $0 < m < p$: By Lemma 28, $\binom{p}{m} \equiv 0 \pmod{p}$. $\square$

$(m+n)^p = \sum_{i=0}^{p} \binom{p}{i} m^i . n^{p-i} = m^p + n^p + \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i}$

A little more arithmetic

Corollary 33 (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, n and p be natural numbers with p prime.

RTP: $(m+n)^p \equiv m^p + n^p \pmod{p}$

i.e. $(m+n)^p - (m^p + n^p)$ is a multiple of p

Note $(m+n)^p - (m^p + n^p) = \sum_{i=1}^{p-1} \binom{p}{i} m^i . n^{p-i}$

$$(m+n)^p - (m^p + n^p) \qquad (*)$$

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

Since $\binom{p}{i}$ for $i=1,\dots,p-1$ are multiples of p we have $\binom{p}{i} = p \cdot k_i$ for integers k_i.

Hence

$$(*) = \sum_{i=1}^{p-1} p \cdot k_i \, m^i n^{p-i}$$

$$= p \cdot \left[\sum_{i=1}^{p-1} k_i \cdot m^i n^{p-i} \right].$$

and since

$$\sum_{i=1}^{p-1} k_i \, m^i \, n^{p-i}$$

is an integer, we are done. $\square$

$a \equiv b \pmod{m}$ ~ predicate: so it is either true or false depending on the values of a, b, and m.

<u>In ML</u>,

3 <u>mod</u> 2 ~ This is <u>not</u> a predicate but an <u>operation</u> on numbers.

We won't use this notation!

instantiating $m=0$ we get $\boxed{i^p \equiv i \pmod p}$

Corollary 34 (The Dropout Lemma) *For all natural numbers* m *and primes* p,

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

Proposition 35 (The Many Dropout Lemma) *For all natural numbers* m *and* i, *and primes* p,

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

PROOF: Let m, i, p be nat. with p prime.

$$(m+i)^p = ([m+(i-1)]+1)^p \equiv (m+(i-1))^p + 1 \pmod p$$

$$= ([m+(i-2)]+1)^p + 1 \equiv (m+(i-2))^p + 2 \pmod p$$

$$\equiv (m+(i-j))^p + j \pmod p$$

Hence

$$\equiv (m+(i-i))^p + i = m^p + i \pmod p$$

as required. $\square$

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

The Many Dropout Lemma (Proposition 35) gives the fist part of the following very important theorem as a corollary.

Theorem 36 (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 .