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: Let p be a positive integer and m natural.

Assume $m=0$ or $m=p$.

We proceed by cases:

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

and we are done

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

and we are done $\boxtimes$

Notation: Choose number

$\binom{p}{m}$, C^p_m, ${}^pC_m$

$= \dfrac{p!}{m!(p-m)!}$

it is a nat. number

= the number of m-element subsets of a set with p-elem.

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

PROOF: Let p and m be integers.

Assume: p is prime and $0 < m < p$.

RTP: $\binom{p}{m} \equiv 0 \pmod{p}$; that is,

$\binom{p}{m} = k\,p$ for some integer k.

idea

find such a k

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

To have a proof we need show that

$$\frac{(p-1)!}{m!\,(p-m)!}$$ is a natural number.

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

So

$$p\cdot(p-1)! = \binom{p}{m}\, m!\,(p-m)!$$

The prime factorisation of $m!(p-m)!$ is included in the prime factorisation of $(p-1)!$

Therefore $m!(p-m)!$ divides $(p-1)!$

and so $\dfrac{(p-1)!}{m!(p-m)!}$ is a natural number

$\blacksquare$

Exercise: Write the proof nicely.

Find p (necessarily not prime) and m such that

$\dfrac{(p-1)!}{m!(p-m)!}$ is not a natural number.

Proposition 29 *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 prime, m an integer.

assume $0 \leq m \leq p$.

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

We proceed by cases:

- Case 1: $m = 0$ ...
- Case 2: $m = p$ ...
- Case 3: $0 < m < p$ ...

use previous Lemmas...

A little more arithmetic

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

Corollary 33 (The Freshman's Dream) *For all natural numbers* m, n *and primes* p,

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

Lemma: $a \equiv x \pmod{q}$, $b \equiv y \pmod{q}$
$\Downarrow$
$a+b \equiv x+y \pmod{q}$
$a \cdot b \equiv x \cdot y \pmod{q}$

PROOF: Idea:

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

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

$$(*)$$

$$\equiv m^p + n^p + 0 \pmod{p}$$

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

$$\underbrace{\binom{p}{i} \equiv 0 \pmod p}_{\text{Lemma}} \qquad i = 1, \dots, p-1$$

$$\Rightarrow \binom{p}{i} m^i n^{p-i} \equiv 0 \pmod p$$

$$\Rightarrow \sum_{i=1}^{p-1} \binom{p}{i} m^i n^{p-i} \equiv 0 \pmod p.$$

$\boxtimes$

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

instantiating for $n=1$

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,

$m=0$ gives FLT

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

PROOF: $(m+i)^p = (m + \underbrace{1+1+\cdots+1}_{i \text{ ones}})^p$

$$\equiv (m + \underbrace{1+\cdots+1}_{i-1 \text{ ones}})^p + 1$$

$$\equiv (m + \underbrace{1+\cdots+1}_{i-2 \text{ ones}})^p + 1 + 1$$

$$\equiv (m + \underbrace{1 + \cdots + 1}_{i-3 \text{ ones}})^p + \underbrace{1 + 1 + 1}_{3 \text{ ones}}$$

$$\vdots$$

$$\equiv m^p + \underbrace{1 + \cdots + 1}_{i \text{ ones}} = m^p + i$$

<u>proof idea</u>

formalised by induction.

$\boxtimes$

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

the reciprocal.

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 .

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 $i^m \not\equiv i \pmod{m}$.

Negation

Negations are statements of the form

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

or, in symbols,

$$\boxed{\neg P}$$

Contrapositive: $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$$
\begin{array}{rcl}
\neg(P \Longrightarrow Q) & \Longleftrightarrow & P \wedge \neg Q \\
\neg(P \Longleftrightarrow Q) & \Longleftrightarrow & P \Longleftrightarrow \neg Q \\
\neg(\forall x.\, P(x)) & \Longleftrightarrow & \exists x.\, \neg P(x) \\
\neg(P \wedge Q) & \Longleftrightarrow & (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) & \Longleftrightarrow & \forall x.\, \neg P(x) \\
\neg(P \vee Q) & \Longleftrightarrow & (\neg P) \wedge (\neg Q) \\
\neg(\neg P) & \Longleftrightarrow & P \\
\neg P & \Longleftrightarrow & (P \Rightarrow \mathbf{false})
\end{array}
$$