Fermat's Little Theorem

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:

If $a_i \equiv b_i \pmod{m}$ $i = 1, \ldots, n$

Then $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod{m}$

and $\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod{m}$.

Let m and n be natural numbers and let p be a prime.

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

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

$$= \underbrace{\sum_{i=1}^{p-1} \underbrace{\binom{p}{i}}_{\equiv 0 \pmod p} m^i n^{p-i}}_{\equiv 0 \pmod p} + m^p + n^p$$

$\boxtimes$

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:

$$i^p \equiv i \pmod{p}$$

Let m and i be natural numbers and p a prime.

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

- for $i=0$: $(m+i)^p = m^p = m^p + i$ ✓
- for $i \geq 1$: $(m+i)^p = (m+(i-1)+1)^p$

$$\equiv (m+(i-1))^p + 1 \overset{i=1}{\equiv} m^p + 1$$

- for $i \geq 2$:

$$\equiv (m+(i-2)+1)^p + 1$$

$$\equiv (m+(i-2))^p + 1 + 1$$

$$= (m+(i-2))^p + 2 \overset{i=2}{\equiv} m^p + 2$$

- for $i \geq 3$: ...

- <u>for $i \geq k$</u> : ... iterating the previous procedure

$$(m+i)^p \equiv (m+(i-k))^p + k$$

<u>for $i = k$</u>

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

$\boxtimes$

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 .

FERMAT'S LITTLE THEOREM

$$i \not\equiv 0 \pmod p \Rightarrow i^{p-1} \equiv 1 \pmod p$$

every $i \not\equiv 0 \pmod p$ has a reciprocal modulo p; namely i^{p-2}, since

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

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