Fermat's Theorem.

1. Multiplicative Inverse: A multiplicative inverse modulo p for a natural number a is a natural number b s.t. $ab \equiv 1 \pmod{p}$.

2. Cancellation Law: If p is a prime number and a is no divisible by p. if $ab \equiv ac \pmod{p}$, then $b \equiv c \pmod{p}$

proof: Let p be a prime, $p \nmid a$.

Assume $ab \equiv ac \pmod{p}$. i.e. $p \mid ab - ac$ by definition.

WTS: $b \equiv c \pmod{p}$.

Since $p \mid ab - ac \Rightarrow p \mid a(b-c)$, also $p \nmid a$, gives $p \mid (a-c)$.

i.e. $a \equiv c \pmod{p}$. ∎

3. Fermat's Little Theorem: If p is a prime and a is a natural number that is not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

rewrite for contrad.

proof. Let p be a prime.

Let $a \in \mathbb{N}$. $p \nmid a$.

WTS: $a^{p-1} \equiv 1 \pmod{p}$.

Consider the set of numbers $\{a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)\}$

Since in set $\{1, 2, \dots, p-1\}$ no two of the numbers are congruent to each other (from theorem 3.1.4).

Since p is prime, $p \nmid a$. if $am \equiv an \pmod{p} \Rightarrow m \equiv n \pmod{p}$.

Thus. $\{a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)\}$ not congruent to each other.

Also, they congruent to one of the number in $\{1, 2, \dots, (p-1)\}$.

From multiplication, gives. $a^{p-1}(1 \cdot 2 \cdots (p-1)) \equiv (1 \cdot 2 \cdots (p-1)) \pmod{p}$.

Since $p \nmid 1 \cdot 2 \cdots (p-1)$. gives $a^{p-1} \equiv 1 \pmod{p}$.

$\longrightarrow$ If p is a prime and a is a natural num. then $a^p \equiv a \pmod{p}$

Case 1:

Case 2: $a | p \Rightarrow a^n | p \Rightarrow a^n \equiv a \pmod p$. (7.3.1.3).

$\longrightarrow$ If p is a prime and a is a natural number that's not divisible by p, then there exists a natural number x s.t. $ax \equiv 1 \pmod p$.

p is prime 2 $x = 1$ when $ax \equiv 1 \pmod 2$.

$p > 2$. $x = a^{p-2}$, $ax = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod p$

4. Theorem 5.1.6: If a and c have the same multiplicative inverse modulo p, then a is congruent to c modulo p.

proof: Let $ab \equiv 1 \pmod p$; $cb \equiv 1 \pmod p$. gives.

$cba \equiv a \pmod p$ (by multiplication $a \equiv a \pmod p$).

Since $ab \equiv 1 \pmod p$. gives. $c \equiv a \pmod p$.

(symmetry) $\Rightarrow a \equiv c \pmod p$.

5. Theorem 5.1.7. If p is a prime and x is an integer satisfying $x^2 \equiv 1 \pmod p$. then either $x \equiv 1 \pmod p$ or $x \equiv p-1 \pmod p$.

proof: Let $x^2 \equiv 1 \pmod p$. gives $p | x^2 - 1$, which $p | (x+1)(x-1)$.

Since p is prime and $p | (x+1)(x-1)$. by 4.1.3. gives.

$p | (x+1)$ or $p | (x-1)$.

① $p | (x+1)$. gives. $x \equiv -1 \pmod p \Rightarrow x \equiv p-1 \pmod p$.

② $p | (x-1)$, gives $x \equiv 1 \pmod p$.