Fermat's Little Theorem

p prime, $a \in \mathbb{N}$ s.t. $p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$.

pf.: consider $a, 2a, 3a, \ldots, (p-1)a$.

There are all incongruent mod p: if $ma \equiv na \pmod{p}$,

then $m \equiv n \pmod{p}$, i.e., $m = n$ since $1 \le m, n \le p-1$.

multiply them:

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$$

$$\implies a^{p-1} \equiv 1 \pmod{p}. \quad \blacksquare$$

Corollary p prime, $a \in \mathbb{N} \implies a^p \equiv a \pmod{p}$.

__1__ $\quad 17 \mid 11^{104}+1$:

Fermat $\Longrightarrow 11^{16} \equiv 1 \pmod{17}$

$\Longrightarrow (11^{16})^6 \equiv 1 \pmod{17}$, i.e., $\underline{\underline{11^{96} \equiv 1 \pmod{17}}}$.

__Note:__ $11^2 \equiv 2 \pmod{17} \Longrightarrow 11^8 \equiv 16 \pmod{17}$

$\Longrightarrow 11^8 \equiv -1 \pmod{17}$.

Then $11^{104} \equiv -1$.

__Aside:__ $11^8 \equiv r \pmod{17} \Longrightarrow 11^{16} \equiv r^2 \pmod{17}$

and $r^2 \equiv 1 \pmod{17}$ (by Fermat)

$(r+1)(r-1) \equiv 0 \pmod{17}$

$\Longrightarrow r=1$ or $r=16$

$\Longrightarrow 11^8 \equiv 1$ __or__ $11^8 \equiv -1 \pmod{17}$

6(b) $a^5 \equiv a \pmod{10}$ for any $a \in \mathbb{N}$:

Know that $a^5 \equiv a \pmod{2}$ (parity)

and that $a^5 \equiv a \pmod{5}$ (Fermat)

$$\Longrightarrow \quad a^5 \equiv a \pmod{10}.$$

The converse of Fermat's Little Theorem is NOT true:

$2^{341} \equiv 2 \pmod{341}$, but 341 is NOT prime.

$\underline{2^{340} \equiv 1 \pmod{341}}$ $\quad (341 = 31 \cdot 33)$.

$1024 = \underline{2^{10} \equiv 1 \pmod{341}} \Longrightarrow 2^{340} \equiv 1 \pmod{341}$

$\Longrightarrow \quad \Longrightarrow 2^{341} \equiv 2 \pmod{341}$.

<u>related</u>: $\underline{2^n - 2 \text{ is prime for } 2 \le n \le 340}$.

Wilson's Theorem

p odd prime, then $(p-1)! \equiv -1 \pmod p$. And conversely!

pf.

consider $\underbrace{ax \equiv 1 \pmod p}$, where a, p are relatively prime.

has a unique solution, $a' \Longrightarrow aa' \equiv 1 \pmod p$

(a and a' are called inverses mod p).

Note: any a between 1 and $p-1$ (inclusive) has a unique inverse mod p.

If a is its own inverse, $a^2 \equiv 1 \pmod p$, then

$$a^2 - 1 \equiv 0 \pmod p$$

$$(a+1)(a-1) \equiv 0 \pmod p \Longrightarrow \underline{\underline{a \equiv 1}} \text{ or } a = \underline{\underline{p-1}}.$$

$$1, \underbrace{2, 3, \ldots, p-2}_{\frac{p-3}{2} \text{ pairs of inverses}}, p-1 \Longrightarrow \begin{array}{l} p-1 \equiv -1 \pmod p \\ (p-2)! \equiv 1 \pmod p \\ \hline (p-1)! \equiv -1 \pmod p. \end{array}$$

$\blacksquare$

<u>Converse</u>: if $\underline{\underline{(n-1)! \equiv -1 \pmod{n}}}$, then n is prime.

<u>pf.</u>: if n not prime, then n has a divisor d with $1 < d < n$.

$d \mid (n-1)!$ since d is one of the factors.

~~$d \nmid (n-1)! + 1$~~ Assuming that $n \mid (n-1)! + 1$

$$\Longrightarrow \quad d \mid (n-1)! + 1$$

$$\Longrightarrow \quad d \mid 1 \quad \times.$$

<u>Next</u> time: use these to prove that

$$x^2 + 1 \equiv 0 \pmod{p}, \quad p \text{ prime}$$

is solvable iff $p \equiv 1 \pmod{4}$, i.e., $p = 4k+1$.