Wilson's Theorem and Fermat's Little Theorem

Theorem 6.1: Wilson's Theorem

Let p be prime. Then,

$$(p-1)! \equiv -1 \pmod{p}.$$

In other words, Wilson's theorem says that

$$p \mid ((p-1)!+1)$$

for any prime p.

ex: $(7-1)!+1 = 6!+1 = 721$

Note that $7 \mid 721$. $\left(\frac{721}{7} = 108\right)$.

Let's see why this theorem is true with the above example.

Note that

$$6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$$

Let's find the inverse of each of $1, 2, \ldots, 6$ modulo 7.

$\bar{1} = 1$ $\quad$ $\bar{3} = 5$ $\quad$ $\bar{5} = 3$

$\bar{2} = \bar{4}$ $\quad$ $\bar{4} = 2$ $\quad$ $\bar{6} = 6$

Let's group the pairs of inverses.

$$
\begin{aligned}
1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 &= 1\cdot(2\cdot 4)\cdot(3\cdot 5)\cdot 6\\
&\equiv 1\cdot 6\\
&\equiv 6\\
&\equiv -1 \pmod{7}
\end{aligned}
$$

Now we prove Wilson's theorem.

Proof (of Wilson's theorem):

When $p=2$, $(p-1)! = 1! \equiv -1 \pmod{2}$.

Hence, the theorem is true for $p=2$.
Let p be a prime > 2.

Let $1 \leq a \leq p-1$.
By Theorem 4.11, a has an inverse $\bar{a}$ such that

$$a\bar{a} \equiv 1 \pmod{p}.$$

We also proved in Theorem 4.12 that the only own inverses modulo a prime p are 1 and $p-1$.

As seen in the example, when we group the pairs of inverses, and replace each pair by 1 modulo p, we get

$$1\cdot 2\cdot 3\cdot \cdots \cdot (p-1) \equiv 1\,(p-1)$$
$$\equiv -1 \pmod p$$

and the theorem follows.

The converse of Wilson's theorem is also true.

<u>Theorem 6.2:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.

If $(n-1)! \equiv -1 \pmod n$ then n is prime.

Proof: We use the method of contradiction.

Suppose $(n-1)! \equiv -1 \pmod n$ — (1)

and n is composite.

Then, $n = ab$ with $1 < a, b < n$.

Since $a < n$, we have $a \mid (n-1)!$. — (2)

(1) $\Rightarrow$ $n \mid ((n-1)!+1)$. Also, $a \mid n$.

$\therefore a \mid ((n-1)!+1)$ — (3) (Theorem 1.8)

$\therefore a \mid ((n-1)!+1 - (n-1)!)$ (by (2) and (3))

$\Rightarrow a \mid 1$, a contradiction as $a > 1$.

ex: $(6-1)! = 5! = 120 \equiv 0 \pmod 6$

$\therefore$ 6 is not prime (as we obviously know)

Following theorem is due to Fermat.

Theorem 6.3: Fermat's Little Theorem.

Let p be a prime and $a \in \mathbb{Z}$ be s.t. $p \nmid a$.
Then,
$$a^{p-1} \equiv 1 \pmod{p}$$

Proof: Exercise.

ex: Let's illustrate the proof with an example.
Let $p=7$ and $a=3$

Then,
$$\begin{aligned}
1\cdot 3 &\equiv 3 \pmod{7}\\
2\cdot 3 &\equiv 6 \pmod{7}\\
3\cdot 3 &\equiv 2 \pmod{7}\\
4\cdot 3 &\equiv 5 \pmod{7}\\
5\cdot 3 &\equiv 1 \pmod{7}\\
6\cdot 3 &\equiv 4 \pmod{7}
\end{aligned}$$

$\therefore (1\cdot 3)(2\cdot 3)(3\cdot 3)(4\cdot 3)(5\cdot 3)(6\cdot 3) \equiv 1\cdot 2\cdot 3 \cdots 6 \pmod{7}$

$\therefore \quad 3^6 (1\cdot 2\cdot 3 \cdots 6) \equiv 1\cdot 2\cdot 3 \cdots 6 \pmod{7}$

$\therefore \quad 3^6 \equiv 1 \pmod{7} \quad (\because \gcd(1\cdot 2 \cdots 6, 7) = 1)$

In fact $3^6 - 1 = 728$ and

$$\frac{728}{7} = 104.$$

<u>Theorem 6.4</u>: Let p be a prime and $a \in \mathbb{Z}$. Then,

$$a^p \equiv a \pmod{p}.$$

Proof: If $p \nmid a$, then

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

Multiply by a to get

$$a^p \equiv a \pmod{p}.$$

If $p \mid a$, then $p \mid a(a^{p-1}-1)$.

$$\Rightarrow p \mid (a^p - a)$$

$$\Rightarrow a^p \equiv a \pmod{p}$$

Fermat's little theorem can be used to find the least positive residue of powers of integers modulo a prime.

<u>ex</u>: Let's find the least positive residue of 3^{201} modulo 11.

By Fermat's little theorem (with $p=11$ and $a=3$), we've

$$3^{10} \equiv 1 \pmod{11}$$

$$\therefore (3^{10})^{20} \equiv 1^{20} \pmod{11}$$

$\therefore\ 3^{200} \equiv 1 \pmod{11}$

$\therefore\ 3^{201} \equiv 3^{200} \cdot 3 \equiv 1 \cdot 3 \equiv 3 \pmod{11}$

Theorem 6.5: Let p be a prime and $a \in \mathbb{Z}$ be s.t. $p \nmid a$. Then, a^{p-2} is an inverse of a modulo p.

Proof: We've

$$a \cdot a^{p-2} = a^{p-1}$$
$$\equiv 1 \pmod{p}$$

ex: Let's find the inverse of 2 modulo 11.

We know, $2^9 = 512 \equiv 6 \pmod{11}$

$9 = 11 - 2$.

$\therefore$ 6 is an inverse of 2 modulo 11.

Following corollary can be used to solve linear congruences of the form

$$ax \equiv b \pmod{p}$$

where p is a prime.

Corollary 6.5.1: Let $a, b \in \mathbb{Z}^+$, p = a prime and $p \nmid a$. Then, the solutions of $ax \equiv b \pmod{p}$ are given by $x \equiv a^{p-2} b \pmod{p}$.

Proof: Exercise

ex: Show that, for a prime $p > 2$,

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$