Wilson's Theorem and Fermat's Little Theorem

Wilson'sTheorem

THEOREM 1 (Wilson's Theorem): $(p-1)! \equiv -1 \pmod{p}$ if and only if p is prime.

EXAMPLE: We have

$$\begin{aligned}
&(2-1)!+1=2\\
&(3-1)!+1=3\\
&(4-1)!+1=7\\
&(5-1)!+1=5^2\\
&(6-1)!+1=11^2\\
&(7-1)!+1=7\cdot 103\\
&(8-1)!+1=71^2\\
&(9-1)!+1=61\cdot 661\\
&(10-1)!+1=19\cdot 71\cdot 269\\
&(11-1)!+1=11\cdot 329891\\
&(12-1)!+1=39916801\\
&(13-1)!+1=13^2\cdot 2834329\\
&(14-1)!+1=83\cdot 75024347\\
&(15-1)!+1=23\cdot 3790360487\\
&(16-1)!+1=59\cdot 479\cdot 46271341\\
&(17-1)!+1=17\cdot 61\cdot 137\cdot 139\cdot 1059511
\end{aligned}$$

REMARK: The first proof of Wilson's Theorem was given by the French mathematician Joseph Lagrange in 1770. The mathematician after whom the theorem is named, John Wilson, conjectured, but did not prove it.

Proof: Suppose p is prime. When $p=2$ and $p=3$, the Theorem is true (see the Example above). Now let p be a prime greater than 3. By Theorem 1 from Section 4.2, for each integer a with $1 \leq a \leq p-1$ there is a unique (since $(a,p)=1$) inverse $\bar{a}$, $1 \leq \bar{a} \leq p-1$, with

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

By Theorem 2 from Section 4.2, the only positive integers less than p that are their own inverses are 1 and $p-1$. Therefore, we can group the integers from 2 to $p-2$ into $(p-3)/2$ pairs of integers, with the product of each pair congruent to 1 modulo p. Hence, we have

$$2\cdot 3\ldots(p-3)(p-2) \equiv 1 \pmod{p}$$

We multiply both sides of this congruence by 1 and $p-1$ to obtain

$$(p-1)! = 1\cdot 2\cdot 3\ldots(p-3)(p-2)(p-1) \equiv 1\cdot(p-1) \equiv -1 \pmod{p}$$

This completes the first part of the proof.

Now assume that p is a composite integer and that

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

Since p is composite, we have $p = ab$, where $1 < a < p$ and $1 < b < p$. Because $a < p$, we know that $a \mid (p-1)!$, since a is one of the $p-1$ numbers multiplied together to form $(p-1)!$. Because $(p-1)! \equiv -1 \pmod{p}$, it follows that $p \mid ((p-1)!+1)$. This means, by Theorem 1 from Section 1.5, that a also divides $(p-1)!+1$. By Theorem 2 from Section 1.5, since

$$a \mid (p-1)! \quad \text{and} \quad a \mid ((p-1)!+1)$$

we conclude that

$$a \mid [((p-1)!+1)-(p-1)!] = 1$$

This is a contradiction, since $a > 1$. ■

Fermat's Little Theorem

THEOREM 2 (Fermat's Little Theorem): If p is prime and a is an integer with

$$p \nmid a \tag{1}$$

then

$$p \mid a^{p-1}-1 \quad \text{or, equivalently,} \quad a^{p-1} \equiv 1 \pmod{p} \tag{2}$$

REMARK 1: If $p \mid a$, then $a^{p-1} \not\equiv 1 \pmod{p}$. Indeed, $p \mid a$ implies $a \equiv 0 \pmod{p}$, which gives $a^{p-1} \equiv 0 \pmod{p}$ by Theorem 5 from Section 4.1.

REMARK 2: The converse of Fermat's little theorem is not generally true. Indeed, if $a = 5$ and $p = 4$, then (2) becomes

$$5^{4-1} \equiv 1 \pmod{4}$$

It is much harder to find a similar example for $a = 2$. Indeed, the smallest composite integer $p > 1$ such that

$$2^{p-1} \equiv 1 \pmod{p}$$

is $p = 341 = 11 \cdot 31$.

Proof of the Theorem: Consider the following numbers:

$$a,\ 2a,\ 3a, \ldots, (p-1)a$$

By the Division Algorithm we have

$$\begin{aligned} a &= pk_1 + r_1 \\ 2a &= pk_2 + r_2 \\ 3a &= pk_3 + r_3 \\ &\cdots \\ (p-1)a &= pk_{p-1} + r_{p-1} \end{aligned} \quad \Longrightarrow \quad \begin{aligned} a &\equiv r_1 \pmod{p} \\ 2a &\equiv r_2 \pmod{p} \\ 3a &\equiv r_3 \pmod{p} \\ &\cdots \\ (p-1)a &\equiv r_{p-1} \pmod{p} \end{aligned} \tag{3}$$

where $0 \le r_i \le p-1$. Moreover, $r_i \ne 0$, since otherwise $p \mid ia$, and therefore by Theorem 2 from Section 3.5, $p \mid i$ or $p \mid a$. But this is impossible, since $p > i$ and $p \not| \, a$ by (1). So,

$$1 \le r_i \le p-1 \tag{4}$$

From (3) by part (iii) of Theorem 4 (Section 4.1) it follows that

$$(p-1)!a^{p-1} \equiv r_1 r_2 \dots r_{p-1} \pmod{p} \tag{5}$$

LEMMA: We have

$$r_1 r_2 \dots r_{p-1} = (p-1)! \tag{6}$$

Proof: We first show that

$$r_1, r_2, \dots, r_{p-1} \quad \text{are all distinct.} \tag{7}$$

In fact, assume to the contrary that $r_i = r_j$ for some $i \ne j$. Then by (3) we have

$$ia - pk_i = ja - pk_j$$

hence

$$(i-j)a = p(k_i - k_j)$$

This means that p divides $(i-j)a$. From this by Theorem 2 (Section 3.5) it follows that $p \mid (i-j)$ or $p \mid a$. But this is impossible, since $p > i - j$ by (4) and $p \not| \, a$ by (1). This contradiction proves (7).

So, we have $p-1$ distinct numbers between 1 and $p-1$. This means that

$$\{r_1, r_2, \dots, r_{p-1}\} = \{1, 2, \dots, p-1\}$$

which gives (6). ■

By (5) and (6) we obtain

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

$$(p-1)!a^{p-1} - (p-1)! \equiv 0 \pmod{p}$$

$$(p-1)!(a^{p-1} - 1) \equiv 0 \pmod{p}$$

so

$$p \mid 1 \cdot 2 \dots (p-1)(a^{p-1} - 1)$$

Since p divides the product, by Theorem 2 from Section 3.5, it follows that p divides at least one of its terms. Note that

$$p \not| \, 1, \quad p \not| \, 2, \dots, p \not| \, (p-1)$$

Therefore

$$p \mid a^{p-1} - 1 \quad \text{or, equivalently,} \quad a^{p-1} \equiv 1 \pmod{p} \ ■$$

COROLLARY: If p is prime and a is a positive integer, then

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

Proof: If $p \not| a$, by Fermat's little theorem, we know that

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

Multiplying both sides of this congruence by a, we find that

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

If $p \mid a$, then $p \mid a^p$ as well, so that

$$a^p \equiv a \equiv 0 \pmod{p}$$

This finishes the proof, since $a^p \equiv a \pmod{p}$ if $p \not| a$ and if $p \mid a$. ■

EXAMPLE: Prove that $17 \mid a^{80} - 1$ for any positive integer a with $(a, 17) = 1$.

Solution: By Fermat's Little theorem we have

$$a^{16} \equiv 1 \pmod{17}$$

therefore by Theorem 5 from Section 4.1, we get

$$a^{16 \cdot 5} \equiv 1^5 \equiv 1 \pmod{17}$$

and the result follows.

EXAMPLE: Prove that $23 \mid a^{154} - 1$ for any for any positive integer a with $(a, 23) = 1$.

Solution: By Fermat's Little theorem we have

$$a^{22} \equiv 1 \pmod{23}$$

therefore by Theorem 5 from Section 4.1, we get

$$a^{22 \cdot 7} \equiv 1^7 \equiv 1 \pmod{23}$$

and the result follows.

EXAMPLE: Prove that $300 \mid 11^{10} - 1$.

Solution: We have

$$11^{10} - 1 = (11^5 + 1)(11^5 - 1) = (11^5 + 1)(11 - 1)(11^4 + 11^3 + 11^2 + 11 + 1) \tag{8}$$

Since $11 \equiv 1 \bmod 10$, by Theorem 5 from Section 4.1, we get $11^n \equiv 1 \bmod 10$. Therefore by Theorem 4 from Section 4.1, we obtain

$$11^4 + 11^3 + 11^2 + 11 + 1 \equiv 5 \pmod{10}$$

hence $11^4 + 11^3 + 11^2 + 11 + 1$ is divisible by 5. We also note that $11^5 + 1$ is divisible by 2 and $11 - 1$ is divisible by 10. Therefore the right-hand side of (8) is divisible by $2 \cdot 10 \cdot 5 = 100$. On the other hand, by Fermat's Little Theorem, $11^{10} - 1$ is divisible by 3. Since $(3, 100) = 1$, the whole expression is divisible by 300.

EXAMPLE: What is the remainder after dividing 3^{50} by 7?

Solution: By Fermat's Little theorem we have

$$3^6 \equiv 1 \pmod{7}$$

therefore by Theorem 5 from Section 4.1, we get

$$3^{6\cdot 8} \equiv 1^{48} \equiv 1 \pmod{7}$$

therefore

$$3^{50} \equiv 9 \equiv 2 \pmod{7}$$

EXAMPLE: Prove that

$$3 \mid n^3 - n \tag{9}$$

for any integer $n \geq 0$.

Solution 1:

STEP 1: For $n = 0$ (9) is true, since $3 \mid 0^3 - 0$.

STEP 2: Suppose (9) is true for some $n = k \geq 0$, that is $3 \mid k^3 - k$.

STEP 3: Prove that (9) is true for $n = k + 1$, that is $3 \mid (k + 1)^3 - (k + 1)$. We have

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 = \underbrace{k^3 - k}_{\substack{\text{St. 2}\\ \text{div. by 3}}} + \underbrace{3k^2 + 3k}_{\text{div. by 3}}.$$

Solution 2: $3 \mid n^3 - n$ by the Corollary above with $p = 3$.

THEOREM 3: If p is prime and a is an integer such that $p \not\mid a$, then a^{p-2} is an inverse of a modulo p.

Proof: If $p \not\mid a$, then by Fermat's little theorem we have

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

Hence, a^{p-2} is an inverse of a modulo p. ■

COROLLARY: If a and b are positive integers and p is prime with $p \not\mid a$, then the solutions of the linear congruence

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

are the integers x such that

$$x \equiv a^{p-2} b \pmod{p}$$

Proof: Suppose that $ax \equiv b \pmod{p}$. Since $p \not\mid a$, we know from the Theorem above that a^{p-2} is an inverse of a modulo p. Multiplying both sides of the original congruence by a^{p-2}, we have

$$a^{p-2} ax \equiv a^{p-2} b \pmod{p}$$

Hence,

$$x \equiv a^{p-2} b \pmod{p} \ ■$$

EXAMPLE: Find all solutions of the following congruence

$$2x \equiv 5 \pmod{7}$$

Solution 1: We first note that $(2,7)=1$. Therefore we can apply the Corollary from Section 4.2. Since $s=4$ is a particular solution of $2s \equiv 1 \pmod{7}$, we get

$$x \equiv bs \equiv 5 \cdot 4 \equiv 6 \pmod{7}$$

Solution 2: Since $p=7$ is a prime number and $7 \not| \, 2$, we can apply the Corollary above. We have

$$x \equiv a^{p-2}b = 2^{7-2} \cdot 5 = 160 \equiv 6 \pmod{7}$$