Wilson's Theorem and Fermat's Theorem

Suppose p is prime. Wilson's theorem says $(p-1)! = -1 \pmod{p}$. Fermat's theorem says if $p \nmid a$, then $a^{p-1} = 1 \pmod{p}$. They are often used to reduce factorials and powers mod a prime.

I'll prove Wilson's theorem first, then use it to prove Fermat's theorem.

Lemma. Let p be a prime and let $0 < x < p$. Then $x^2 = 1 \pmod{p}$ if and only if $x = 1$ or $x = p - 1$.

Proof. If $x = 1$, then $x^2 = 1 \pmod{p}$. If $x = p - 1$, then

$$x^2 = p^2 - 2p + 1 = 1 \pmod{p}.$$

Conversely, suppose $x^2 = 1 \pmod{p}$. Then

$$p \mid x^2 - 1 = (x-1)(x+1).$$

Since p is prime, $p \mid x - 1$ or $p \mid x + 1$. The only number in $\{1, \ldots, p-1\}$ which satisfies $p \mid x - 1$ is 1, and the only number in $\{1, \ldots, p-1\}$ which satisfies $p \mid x + 1$ is $p - 1$. $\square$

$k^2 = 1 \pmod{p}$ means $k \cdot k = 1 \pmod{p}$ — that is, k is its own multiplicative inverse. So the result says that 1 and $p - 1 = -1$ are the only numbers which are their own multiplicative inverses mod p.

Theorem. (Wilson's theorem) Let $p > 1$. p is prime if and only if

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

Proof. Suppose p is prime. If $k \in \{1, \ldots, p-1\}$, then k is relatively prime to p. So there are integers a and b such that

$$ak + bp = 1, \quad \text{or} \quad ak = 1 \pmod{p}.$$

Reducing a mod p, I may assume $a \in \{1, \ldots, p-1\}$.

Thus, every element of $\{1, \ldots, p-1\}$ has a reciprocal mod p in this set. The preceding lemma shows that only 1 and $p - 1$ are their own reciprocals. Thus, the elements $2, \ldots, p-2$ must pair up into pairs $\{x, x^{-1}\}$. It follows that their product is 1. Hence,

$$(p-1)! = 1 \cdot 2 \cdots (p-2) \cdot (p-1) = 1 \cdot 1 \cdot (p-1) = p - 1 = -1 \pmod{p}.$$

Now suppose $(p-1)! = -1 \pmod{p}$. I want to show p is prime. Begin by rewriting the equation as $(p-1)! + 1 = kp$.

Suppose $p = ab$. I may take $1 \le a, b \le p$. If $a = p$, the factorization is trivial, so suppose $a < p$. Then $a \mid (p-1)!$ (since it's one of $\{1, \ldots, p-1\}$) and $a \mid p$, so $(p-1)! + 1 = kp$ shows $a \mid 1$. Therefore, $a = 1$.

This proves that the only factorization of p is the trivial one, so p is prime. $\square$

Let's see how this works in a particular case. Take $p = 11$. Then mod 11 I have

$$\begin{aligned} 10! &= 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \\ &= 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \\ &= 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) \\ &= -1 \end{aligned}$$

Notice how the numbers other than 1 and 10 paired up as a number and its multiplicative inverse, and how 1 and 10 are the only numbers which are their own multiplicative inverses.

Note that $(p-1)! = -1 \pmod{p}$ implies that p is prime — but this is not a very good way to test that a number is prime. The factorials grow too rapidly.

Theorem. (Fermat) Let p be prime, and suppose $p \not| a$. Then $a^{p-1} = 1 \pmod{p}$.

Proof. Consider the set of integers

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

I'll show that they reduce mod p to the standard system of residues $\{1, \ldots, p-1\}$, then apply Wilson's theorem.

There are $p-1$ numbers in the set $\{a, 2a, \ldots, (p-1)a\}$. So all I need to do is show that they're distinct mod p. Suppose that $1 \le j, k \le p-1$, and

$$aj = ak \pmod{p}.$$

This means $p \mid aj - ak = a(j-k)$, so $p \mid a$ or $p \mid j-k$. Since the first case is ruled out by assumption, $p \mid j-k$. But since $1 \le j, k \le p-1$, this is only possible if $j = k$.

Thus, $\{a, 2a, \ldots, (p-1)a\}$ are $p-1$ distinct numbers mod p. So if I reduce mod p, I must get the numbers in $\{1, \ldots, p-1\}$. Hence,

$$a \cdot 2a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1) = (p-1)! = -1 \pmod{p}.$$

On the other hand, another application of Wilson's theorem shows that

$$a \cdot 2a \cdots (p-1)a = a^{p-1}(p-1)! = -a^{p-1} \pmod{p}.$$

So $-a^{p-1} = -1 \pmod{p}$, or $a^{p-1} = 1 \pmod{p}$. $\square$

Corollary. If p is prime, then $a^p = a \pmod{p}$ for all a.

Proof. If $p \mid a$, then $a^p = 0 \pmod{p}$ and $a = 0 \pmod{p}$, so $a^p = a \pmod{p}$.

If $p \not| a$, then $a^{p-1} = 1 \pmod{p}$. Multiplying by a, I get $a^p = a \pmod{p}$ again. $\square$

Example. Reduce $50^{250} \pmod{83}$ to a number in the range $\{0, 1, \ldots 82\}$. (Note: 83 is prime.)

If you multiply out 50^{250}, here's what you get:

52714787526044456024726519219225572551424023323922008641517022

09078987540239533171017648022226446499875026812553578470207 68

63325972445883937922417317167855799198150634765625000000000000

00000000000000000000000000000000000000000000000000000000000000

00000000000000000000000000000000000000000000000000000000000000

00000000000000000000000000000000000000000000000000000000000000

0000000000000000000000000000000000000000000000000000

Now just reduce mod 83. Heh.

If you don't have access to software that can do this, you can use Fermat's theorem. First, 83 is prime and $83 \not| 50$, so Fermat says $50^{82} = 1 \pmod{83}$.

Now

$$250 = 3 \cdot 82 + 4.$$

Hence,

$$50^{250} = 50^{246} \cdot 50^4 = (50^{82})^3 \cdot 6250000 = 1^3 \cdot 6250000 = 17 \pmod{83}.$$

In other words, if you're trying to reduce a^k mod p, where $p \not| a$, factor out as many a^{p-1}'s as possible, then reduce the rest "by hand". □

Example. Reduce $47^{222} \pmod{113}$ to a number in the range $\{0, 1, \ldots 112\}$. (Note that 113 is prime.)

Since 113 is prime and $113 \not| 47$, Fermat's theorem gives $47^{112} = 1 \pmod{113}$. So

$$47^{222} \pmod{113} = 47^{112} \cdot 47^{110} = 1 \cdot 47^{110} = 47^{110} \pmod{113}.$$

.

Next,

$$\begin{aligned} x &= 47^{110} \pmod{113} \\ 47^2 \cdot x &= 47^2 \cdot 47^{110} \pmod{113} \\ 2209x &= 47^{112} \pmod{113} \\ 62x &= 1 \pmod{113} \end{aligned}$$

I need to compute $62^{-1} \pmod{113}$.

113	-	31
62	1	17
51	1	14
11	4	3
7	1	2
4	1	1
3	1	1
1	3	0

$$\begin{aligned} (-17) \cdot 113 + 31 \cdot 62 &= 1 \\ 31 \cdot 62 &= 1 \pmod{113} \end{aligned}$$

Hence, $62^{-1} = 31 \pmod{113}$. So

$$\begin{aligned} 31 \cdot 62x &= 31 \cdot 1 \pmod{113} \\ x &= 31 \pmod{113} \end{aligned}$$ □

Example. Compute

$$12 \cdot 13 \cdots 20 \cdot 21 \pmod{11}.$$

The any ten consecutive numbers, none divisible by 11, reduce mod 11 to $\{1, 2, \ldots, 10\}$. Hence,

$$12 \cdot 13 \cdots 20 \cdot 21 = 10! = -1 = 10 \pmod{11}. \quad \square$$

Example. Simplify $\dfrac{130!}{87} \pmod{131}$ to a number in the range $\{0, 1, \ldots, 130\}$.

By Wilson's theorem, $130! = -1 \pmod{131}$. So

$$x = \frac{130!}{87} \pmod{131}$$
$$87x = 130! = -1 \pmod{131}$$

131	-	3
87	1	2
44	1	1
43	1	1
1	43	0

$$1 = (87, 131) = (-3) \cdot 87 + 2 \cdot 131.$$

It follows that $87^{-1} = 128 \pmod{131}$, so

$$128 \cdot 87x = 128 \cdot (-1) \pmod{131}$$
$$x = -128 = 3 \pmod{131} \quad \square$$

Example. Simplify $146! \pmod{149}$ to a number in the range $\{0, 1, \ldots 148\}$.

Note: 149 is prime.

By Wilson's theorem, $148! = -1 \pmod{149}$.

$$x = 146! \pmod{149}$$
$$147 \cdot 148x = 147 \cdot 148 \cdot 146! \pmod{149}$$
$$147 \cdot 148x = 148! \pmod{149}$$
$$(-2) \cdot (-1)x = -1 \pmod{149}$$
$$-2x = 1 \pmod{149}$$

Now $-2^{-1} = 74 \pmod{149}$, so

$$74 \cdot -2x = 74 \cdot 1 \pmod{149}$$
$$x = 74 \pmod{149} \quad \square$$

The next problem shows how you can often deal with composite moduli: Factor the modulus into a product of (powers of) primes, solve the problem relative to the prime (power) moduli, then combine the results using the Chinese Remainder Theorem to answer the original question.

Example. Find the least nonnegative residue of $70! \pmod{5183}$.

Note: $5183 = 71 \cdot 73$.

I'll start by finding the residues of $x = 70!$ mod 71 and 73.
By Wilson's theorem,

$$x = 70! = -1 \pmod{71}.$$

Next, let $x = 70! \pmod{73}$. Then

$$\begin{aligned} x &= 70! \pmod{73} \\ 71 \cdot 72 \cdot x &= 70! \cdot 71 \cdot 72 \pmod{73} \\ (-2)(-1)x &= 72! \pmod{73} \\ 2x &= -1 \pmod{73} \end{aligned}$$

Note that $2 \cdot 37 = 74 = 1 \pmod{73}$. So

$$\begin{aligned} 37 \cdot 2x &= 37 \cdot (-1) \pmod{73} \\ x &= -37 = 36 \pmod{73} \end{aligned}$$

Thus,

$$x = -1 \pmod{71} \quad \text{and} \quad x = 36 \pmod{73}.$$

I'll the the iterative method of the Chinese Remainder Theorem to get a congruence mod 5183. First, $x = -1 \pmod{71}$ means $x = -1 + 71a$ for some $a \in \mathbb{Z}$. Plugging this into the second congruence yields

$$\begin{aligned} -1 + 71a &= 36 \pmod{73} \\ 71a &= 37 \pmod{73} \\ -2a &= 37 \pmod{73} \\ (-37)(-2a) &= (-37)(37) \pmod{73} \\ a &= -1369 = 18 \pmod{73} \end{aligned}$$

The last congruence means that $a = 18 + 73b$ for some $b \in \mathbb{Z}$. Plugging this into $x = -1 + 71a$ gives

$$x = -1 + 71(18 + 73b) = 1277 + 5183b, \quad \text{or} \quad x = 70! = 1277 \pmod{5183}. \quad \square$$
