Wilson’s Theorem and Fermat’s Theorem

- **Wilson’s theorem** says that \( p \) is prime if and only if \((p - 1)! = -1 \pmod{p}\).
- **Fermat’s theorem** says that if \( p \) is prime and \( p \nmid a \), then \( a^{p-1} = 1 \pmod{p} \).
- Wilson’s theorem and Fermat’s theorem can be used to reduce large numbers with respect to a given modulus and to solve congruences. They are also used to prove other results in number theory — for example, those used in cryptographic applications.

**Lemma.** Let \( p \) be a prime and let \( 0 < k < p \). \( k^2 = 1 \pmod{p} \) if and only if \( k = 1 \) or \( k = p - 1 \).

**Proof.** If \( k = 1 \), then \( k^2 = 1 \pmod{p} \). If \( k = p - 1 \), then

\[ k^2 = p^2 - 2p + 1 = 1 \pmod{p}. \]

Conversely, suppose \( k^2 = 1 \pmod{p} \). Then

\[ p \mid k^2 - 1 = (k - 1)(k + 1), \]

and since \( p \) is prime, \( p \mid k - 1 \) or \( p \mid k + 1 \). The only number in \( \{1, \ldots, p - 1\} \) which satisfies \( p \mid k - 1 \) is 1, and the only number in \( \{1, \ldots, p - 1\} \) which satisfies \( p \mid k + 1 \) is \( p - 1 \). \( \square \)

**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,\n
\[(p - 1)! = 1 \cdot 2 \cdots (p - 2) \cdot (p - 1) = 1 \cdot 1 \cdot (p - 1) = p - 1 = -1 \pmod{p}. \]

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 \( 1 \leq a, b \leq p \). 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. \( \square \)

**Example.** Wilson’s theorem implies that the product of any ten consecutive numbers, none divisible by 11, equals \(-1 \pmod{11}\) (since any ten consecutive numbers reduce mod 11 to \( \{1, 2, \ldots, 10\} \)). For example,

\[ 12 \cdot 13 \cdots 20 \cdot 21 = -1 \pmod{11}. \]
Example. Find the least nonnegative residue of 70! (mod 5183).

Note that 5183 = 71 · 73. I'll start by finding the residues of 70! mod 71 and 73.
By Wilson’s theorem,

\[ 70! = -1 \pmod{71} . \]

Next, let \( k = 70! \pmod{73} \). Then

\[ 71 \cdot 72 \cdot k = 70! \cdot 71 \cdot 72 \pmod{73} , \]

\[ (-2)(-1)k = 72! \pmod{73} , \]

\[ 2k = -1 \pmod{73} . \]

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

\[ 37 \cdot 2k = 37 \cdot (-1) \pmod{73} , \]

\[ k = -37 = 36 \pmod{73} . \]

Thus,

\[ 70! = -1 \pmod{71} \quad \text{and} \quad 70! = 36 \pmod{73} . \]

I’ll the the iterative method of the Chinese Remainder Theorem to get a congruence mod 5183. First, \( 70! = -1 \pmod{71} \) means \( 70! = -1 + 71a \) for some \( a \in \mathbb{Z} \). Plugging this into the second congruence yields

\[ -1 + 71a = 36 \pmod{73} , \]

\[ 71a = 37 \pmod{73} , \]

\[ -2a = 37 \pmod{73} , \]

\[ (-37)(-2a) = (-37)(37) \pmod{73} , \]

\[ a = -1369 = 18 \pmod{73} . \]

The last congruence means that \( a = 18 + 73b \) for some \( b \in \mathbb{Z} \). Plugging this into \( 70! = -1 + 71a \) gives

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

Theorem. (Fermat) Let \( p \) be prime, and suppose \( p \nmid a \). Then \( a^{p-1} = 1 \pmod{p} \).

Proof. The idea is to show that the integers

\[ a, 2a, \ldots, (p-1)a \]

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 \( 1 \leq j, k \leq p-1 \), 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 \( 1 \leq j, k \leq p-1 \), 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 \(a^{p-1} = 1 \pmod{p}\).

**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 \(p \nmid a\), then \(a^{p-1} = 1 \pmod{p}\). Multiplying by \(a\), I get \(a^p = a \pmod{p}\) again.

**Example.** Compute \(50^{250} \pmod{83}\).

One way is to multiply out \(50^{250}\); Mathematica tells me it is

\[
52714787526044560247265192192255725514240233239220086415170222
09078987540239533171017648022226464649987502681255357847020768
63325972445883979224173171678557991981506347656250000000000000
00000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000

Now just reduce mod 83. Heh.

If you don’t have Mathematica, maybe you should use Fermat’s theorem. \(83 \nmid 50\), so Fermat says \(50^{82} = 1 \pmod{83}\). Now \(3 \cdot 82 = 246\), so

\[ 50^{250} = 50^{246} \cdot 50^4 = (50^{82})^3 \cdot 2500^2 = 1^3 \cdot 10^2 = 100 = 17 \pmod{83} . \]

In other words, if you’re trying to reduce \(a^k \pmod{p}\), where \(p \nmid a\), factor out as many \(a^{p-1}\)’s as possible, then reduce the rest “by hand”.

**Example.** Solve \(16x = 25 \pmod{41}\).

I’d like to multiply both sides by the reciprocal of 16 mod 41. What is it? Well, I could use the Euclidean algorithm on \((16, 41)\), or I could do a multiplication table mod 41. A simpler approach is to note that by Fermat, \(16^{40} = 1 \pmod{41}\). Hence,

\[ 16^{39} \cdot 16x = 16^{39} \cdot 25 \pmod{41} \quad \text{gives} \quad x = 16^{39} \cdot 25 \pmod{41}. \]

Now this is an answer, but a rather cheesy one. I ought to reduce the right side mod 41 to something a little smaller! I can’t use Fermat any more, so I just “divide and conquer”.

\[ 16^2 = 256 = 10 \pmod{41}, \quad \text{so} \quad 16^{39} \cdot 25 = (16^2)^{19} \cdot (16 \cdot 25) = 10^{19} \cdot 400 = 10^{19} \cdot 31 \pmod{41}. \]

Now \(10^2 = 100 = 18 \pmod{41}, \) so

\[ 10^{19} \cdot 31 = (10^2)^9 \cdot (10 \cdot 31) = 18^9 \cdot 310 = 18^9 \cdot 23 \pmod{41}. \]

\[ 18^2 = 324 = 37 \pmod{41}, \quad \text{so} \quad 18^9 \cdot 23 = (18^4)^2 \cdot (18 \cdot 23) = 37^4 \cdot 414 = 1874161 \cdot 414 = 10 \cdot 4 = 40 \pmod{41}. \]

(I reduce down to the point where the arithmetic can be handled by whatever computational tools I have available.)

©2008 by Bruce Ikenaga