**Proof:** \((p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)\), every element, \(a\), this product has a unique inverse, \(a' \equiv (\text{mod}\ p)\) also on that list. If \(a \neq a'\), they cancel out \((\text{mod}\ p)\). Otherwise, \(a^2 \equiv 1 \pmod p\) \(\Rightarrow a^2 - 1 \equiv 0 \pmod p\) \(\Rightarrow (a-1)(a+1) \equiv 0 \pmod p\) so \(a \equiv \pm 1 \pmod p\) so \(a \equiv 1 \pmod p\) or \((p-1) \pmod p\). So \((p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod p\).

**Wilson's Theorem**

**Converse:** For \(n \in \mathbb{N}\), \((n-1)! \equiv -1 \pmod n\) IFF \(n\) is prime.

**Proof:** If \(n\) is not prime then \(n = ab\) for \(a, b > 2\), indeed \(a \leq \left\lfloor \frac{n}{2} \right\rfloor < n - 1\). So \(a \mid (n-1)\). If \((n-1)! \equiv -1 \pmod a\) then \((n-1)! \equiv -1 \pmod a\), but \((n-1)! \equiv 0 \pmod a\) so \((n-1)! \not\equiv -1 \pmod n\).

**Proposition:** If \(p\) is an odd prime, \(x^2 \equiv -1 \pmod p\) has a solution in \(x \in \mathbb{Z}\) IFF \(p \equiv 1 \pmod 4\).

**Proof:** If \(p \equiv 1 \pmod 4\), let \(x = \pm (r!)\) where \(r = \frac{1}{2}(p-1)\). Indeed, consider

\[
(p-1)! = 1 \cdot 2 \cdots (r-1)(r+1)(r+2) \cdots (p-1) \pmod p
\]

\[
\equiv 1 \cdot 2 \cdots (r-1)(-1)(1-r)(2-r) \cdots (-1) \pmod p
\]

\[
\equiv (-1)^{(p-1)/2} \equiv -1 \pmod p
\]

By Wilson's Theorem.
Since \( p - 1 \equiv 0 \pmod{4} \), \( r \equiv 0 \pmod{2} \), so \((-1)^r = 1\).

And we have \((r!)^2 \equiv -1 \pmod{p}\).

If \( p \equiv 3 \pmod{4} \), then if \( x^2 \equiv -1 \pmod{p} \)
then \((x^2)^{r/2} \equiv (-1)^{r/2} \pmod{p}\) and \(r = \frac{1}{2}(p - 1)\) is odd so
\(x^{p-1} = x^{2r} \equiv -1 \pmod{p}\) would contradict Fermat's Little Theorem.

### §3.5 Lagrange's Theorem

**Lagrange's Theorem:** If \( f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_0 \)
with \( c_i \in \mathbb{Z} \) and \( p \nmid c_n \) then \( f(x) \equiv 0 \pmod{p} \)
has at most \( n \) solutions \( \pmod{p} \).

**Proof:** Obviously true if \( n = 1 \), since \( c_1 x \equiv -c_0 \)
has a unique solution \( x \equiv -(c_1)^{-1}c_0 \pmod{p} \) since
\((c_1, p) = 1\).

We proceed by induction.

Assume it is true for all degree \((n-1)\) polynomials.

Note that if \( h(x) = f(x) - f(a) \) then \( h(a) = 0 \) so
\( h(x) = (x-a) g(x) \) where \( g(x) \) is a degree \((n-1)\)
polynomial with same leading coefficient (from the division algorithm on
polynomials, which you know). Let \( x = a \) be a
solution to \( f(x) \equiv 0 \pmod{p} \), then \( f(x) \equiv h(x) \equiv (x-a)g(x) \pmod{p} \).
\( g(x) \) has at most \((n-1)\) solutions and we're
done.
Remark: This is the same argument to show \( f(x) = 0 \) has at most \( n \) solutions in \( \mathbb{Z}/p\mathbb{Z} \), the base case is just different \((\mod p)\).

For \( f(x), g(x) \in \mathbb{Z}[x] \), we say \( f(x) \equiv g(x) \pmod{p} \) if all the coefficients are equivalent \((\mod p)\).

If \( f(x) \in \mathbb{Z}[x] \) has degree \( n \) with \( (c_n, p) = 1 \) and \( f(x) \equiv 0 \pmod{p} \) has \( n \) solutions \((\mod p)\), which are \( a_1, a_2, \ldots, a_n \) then following a similar inductive argument as above we have \( f(x) \equiv c_n(x - a_1) \cdots (x - a_n) \pmod{p} \).

Thus, by Fermat's Little Theorem:

\[ x^{p-1} - 1 = (x-1)(x-2) \cdots (x-(p-1)) \pmod{p} \]

and by comparing coefficients we get an alternate proof of Wilson's Theorem.

Alternative formulation of Lagrange's Theorem: Any polynomial \( f(x) \in \mathbb{Z}/p\mathbb{Z}[x] \) of degree \( n \) has at most \( n \) roots in \( \mathbb{Z}/p\mathbb{Z} \).

Lagrange's Theorem:

Corollary of Fermat's Little Thm: If \( d \mid (p-1) \) then \( x^d - 1 \) has exactly \( d \) zeros \((\mod p)\).
**Proof:** \( x^{p-1} - 1 = (x^d - 1) \left( 1 + x^d + x^{2d} + \cdots + x^{(p-1)d} \right) \frac{g(x)}{9(x)} \)

And \( g(x) \) has at most \( p-1-d \) roots, and \( x^d - 1 \) has at most \( d \) roots, but \( x^{p-1} - 1 \) has exactly \( p-1 \) roots and \( (p-1-d) + d = p-1 \) so \( x^d - 1 \) and \( g(x) \) both have the maximum # of roots.

Lagrange's Thm doesn't hold modulo \( n \) for composite \( n \). Indeed if for \( m_1, m_2, \ldots, m_k \) distinct we had \( s_1, s_2, \ldots, s_k \) solutions to \( f(x) \equiv 0 \pmod{m_i} \), then the CRT would give \( s_1, s_2, \ldots, s_k \) distinct solutions mod \( m_1, m_2, \ldots, m_k \).

It does work for prime powers, \( p^j \), unless \( p \) divides the discriminant of \( f(x) \). [See book].

§ 3.6 PRIMITIVE ROOTS

For \( (a, n) = 1 \), the least \( d \in \mathbb{N} \) such that \( a^d \equiv 1 \pmod{n} \) is the 'order of \( a \) mod \( n \)' and \( a \) is said to 'belong to \( d \) mod \( n \)'.

Claim: Such \( d \) exists for all such \( a, n \) and \( d \mid k \) if \( a^k \equiv 1 \pmod{p} \).