In Chap 2, we studied solving linear diophantine eqn

$$ax + by = c$$

The problem can be restated as

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

or

$$by \equiv c \pmod{a}$$

§ 5.1 Linear congruences

$a, b, c$ integers. Want to solve

$$ax \equiv b \pmod{2} \quad \text{(1)}$$

for integer $x$.

If $x = n$ is a solution of (1), then $x + k2$ is also a solution for any integer $k$.

We may rewrite (1) as a linear diophantine eqn

$$ax - 2b = c \quad \text{(2)}$$

Let $d = \gcd(a, b)$, we know that (2) has solution if and only if $d \mid b$. 

Ex.1 \[ 5x \equiv 3 \quad (\text{mod } 8) \]
\[ 5 \times 5 = 25 \equiv 1 \quad (\text{mod } 8) \]
So \[ 2 \times 25 \equiv 15 \quad (\text{mod } 8) \]
\[ x \equiv 7 \quad (\text{mod } 8) \]

Ex.2 \[ 2x \equiv 11 \quad (\text{mod } 6) \]
no solution

Ex.3 \[ 15x \equiv 9 \quad (\text{mod } 12) \]
may divide by 3
\[ 5x \equiv 3 \quad (\text{mod } 4) \]
\[ x \equiv 3 \quad (\text{mod } 4) \]

Def. We say that a solution \( n \) of a congruence \( ax \equiv b \quad (\text{mod } \phi) \) is \underline{unique} modulo \( \phi \) if any solution \( n' \) of it is congruent to \( n \) modulo \( \phi \).

Def. If \( a \equiv 1 \quad (\text{mod } \phi) \) then we say that \( a \) is the inverse of \( a \) modulo \( \phi \).

Thm 5.1 If \((a, \phi) = 1\) then \( a \) has an inverse, and
\( a^{-1} \) is unique modulo \( \phi \).
Ex 4. \( \phi = 15 \)

reduced residue system

\[ 1, 2, 4, 7, 8, 11, 13, 14 \]

According to Thm 5.1, every number above has a unique inverse modulo 15.

\[ 1 \cdot 1 \equiv 1 \pmod{15} \]
\[ 2 \cdot 8 \equiv 1 \pmod{15} \]
\[ 4 \cdot 4 \equiv 1 \pmod{15} \]
\[ 7 \cdot 13 \equiv 1 \pmod{15} \]
\[ 11 \cdot 11 \equiv 1 \pmod{15} \]
\[ 14 \cdot 14 \equiv 1 \pmod{15} \]

§ 5.2. Theorems of Euler, Fermat and Wilson

In Ex 4, we may multiply the reduced residue system modulo 15 by a constant,

\[ x_2: 2, 4, 8, 14, 1, 7, 11, 13 \quad \text{also a reduced residue system} \]
\[ x_3: 3, 6, 12, 6, 9, 3, 9, 12 \quad \text{(not a reduced residue system)} \]
\[ x_4: 4, 8, 1, 13, 2, 14, 7, 11 \quad \text{(also a reduced residue system)} \]
\begin{align*}
\Phi(n) \cdot (g, m) = 1
\end{align*}

If \( r_1, r_2, \ldots, r_s \) is a reduced residue system modulo \( m \), then \( a r_1, a r_2, \ldots, a r_s \) is also a reduced residue system modulo \( m \). (Because if \( a r_i \equiv a r_j \pmod{m} \), then \( r_i \equiv r_j \pmod{m} \), contradiction.)

So

\begin{align*}
r_1 \cdot r_2 \cdots r_s &\equiv a r_1 \cdots a r_s \pmod{m} \\
&\equiv \Phi(m) r_1 r_2 \cdots r_s
\end{align*}

So

\begin{align*}
\Phi(m) &\equiv 1 \pmod{m}
\end{align*}

**Thm 5.2 (Euler's theorem)**

If \( (a, m) = 1 \), then \( a^{\Phi(m)} \equiv 1 \pmod{m} \)

**Thm 5.3 (Fermat's little theorem)**

If \( p \) is a prime and \( p \neq a \), then

\begin{align*}
a^{p-1} &\equiv 1 \pmod{p} \quad \text{(by \( a^p \equiv a \pmod{p} \))}
\end{align*}

**Ex.** What is the remainder when \( 41^{75} \) is divided by 7?
Thm 5.4. The congruence \((m-1)! \equiv -1 \pmod{m}\) if and only if \(m\) is a prime.

Proof. If \(m\) is a prime, then we consider

1, 2, 3, \ldots, m-1 as a reduced residue system \(\pmod{m}\).

We pair each number \(a\) above with its inverse, so that

\[a \cdot a^{-1} \equiv 1 \pmod{m}\].

But it may happen that a \(a\) may be its own inverse; in other words, that

\[a^2 \equiv 1 \pmod{m}\].

If that case, \(m \mid (a-1)(a+1)\); since \(m\) is a prime, we see that either \(m \mid a-1\) or \(m \mid a+1\); therefore \(a \equiv \pm 1 \pmod{m}\). Since our \(a\) lies in the range \(1 \leq a \leq m-1\), such an \(a\) can only be 1 or \(m-1\). So

\[(m-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (m-2) \cdot (m-1)
\underbrace{\text{pair each number}}_{\text{with its inverse}}
\equiv 1 \cdot 1 \cdots 1 \cdot (m-1).
\equiv -1 \pmod{m}\)
Conversely, suppose \((m-1)! \equiv -1 \pmod{m}\), then \(\gcd(m, (m-1)!) = 1\). So \(m\) must be a prime.

Though Wilson's theorem is really cute, but it is not really a good way to detect primes. (why?)

**Example.** \(p\) is a prime and \(p \nmid a\); we may use Fermat's Little Theorem to solve \(ax \equiv b \pmod{p}\). Indeed:

\[ a \cdot a^{p-2} \equiv a^{p-1} \equiv 1 \pmod{p} \]

This means that \(a^{p-2}\) is the inverse of \(a\) mod \(p\). So

\[ a^{p-1} x \equiv b \cdot a^{p-2} \pmod{p} \]

\[ x \equiv a^{p-2} \cdot b \pmod{p}. \]

**Example.** The converse of Fermat's Little Theorem is not true. We may find a counter example as follows:

(i) \(341 = 11 \times 31\) not a prime

(ii) \(2^{10} = 1024 \equiv 1 \pmod{341}\)

(iii) \(2^{340} \equiv (2^{10})^{34} \equiv 1 \pmod{341}\)