Define \( a \mod m = r \) at some \( q \) and \( a = qm + r \)

Function \( \mathbb{Z} : \{0 \ldots m-1\} \)

Define \( a \equiv b \pmod{m} \) \( \text{relation} \)

\( m \mid (a-b) \)

\( a = b + km \) for some \( k \)

Then \( a \equiv b \pmod{m} \) \& \( c \equiv d \pmod{m} \)

Then \( a + c \equiv b + d \pmod{m} \)

\( ac \equiv bd \pmod{m} \)

\( m \mid a-b \)

\( m \mid c-d \)

\[ \therefore m \mid (a-b)+(c-d) \]

\( a+c \equiv b+d \pmod{m} \)

\( \therefore a+c \equiv b+d \pmod{m} \)
if \( ac \equiv bc \pmod{m} \)

is \( a \equiv b \pmod{m} \)?

\[ \begin{align*}
14 & \equiv 8 \pmod{6} \\
7 & \not\equiv 4 \pmod{6}
\end{align*} \]

but always true if \( \gcd(m,c) = 1 \)

\[ \text{PT} \]

\[ \begin{align*}
m & \mid ac - bc \\
m & \mid c(a - b) \\
since \gcd(m,c) = 1 \\
\therefore m & \mid a - b \\
\therefore \ & a \equiv b \pmod{m}
\end{align*} \]
when/how solve

\[ a \times b \equiv b \pmod{m} \]

if \[ \text{I had } a \cdot x \equiv a \cdot a \equiv 1 \pmod{m} \]

Thus if \( \gcd(a, m) = 1 \)

Then \( \exists \bar{a}: a \cdot \bar{a} \equiv 1 \pmod{m} \)

\text{Multiplicative inverse of } a \]

Furthermore \( \bar{a} \) is unique up to \( \pmod{m} \)

\text{proof (existence only)}

\[ \exists x, \text{ s.t. } a \cdot x + t \cdot m = 1 \]

\[ t \cdot m \equiv 0 \pmod{m} \]
\[ -t \cdot m \equiv 0 \pmod{m} \]

\[ a \cdot t \equiv 1 \pmod{m} \]
\[ -t \cdot m \equiv 0 \pmod{m} \]

\[ a \cdot a \equiv 1 \pmod{m} \]

(can find \( \bar{a} = s \) via Euclid)
Chinese Remainder Theorem (CRT)

\[ x \equiv a_i \pmod{m_i} \text{ for } i = 1, 2, \ldots, n \]
\[ \gcd(m_i, m_j) = 1 \text{ for } i \neq j \]

\exists \text{ unique } 0 \leq x < M = \prod m_i \text{ satisfying these equations.}

**Proof**

let \( M_k = \frac{M}{m_k} \)

\[ y_k \cdot M_k \equiv 1 \pmod{m_k} \]
\[ \exists \text{ since } \gcd(M_k, m_k) = 1 \]

\[ x = \sum_i a_i \frac{M_i}{m_i} y_i \pmod{m_j} \]
\[ \equiv a_j \cdot M_j y_j \pmod{m_j} \]
\[ \equiv a_j \pmod{m_j} \]
**Fermat's Little Theorem**

If \( p \) is prime and \( a \) is not divisible by \( p \), then

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

For all \( a \) not divisible by \( p \),

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

- Example:
  - \( a = 5, \ n = 10 \)
  - \( 5^9 \equiv 5 \pmod{10} \)
  - \( 5^3 = 125 \equiv 5 \pmod{10} \)

**Fact:** \( 2^{n-1} \equiv 1 \pmod{n} \)

For all but 22 composite numbers \( n \) less than 10,000.
Fermat's Little Theorem

If $p$ is prime and $p \nmid a$, then

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

And for all $a$

\[ a^p \equiv a \pmod{p} \]

**Proof**

\[ \gcd(a, p) = 1 \]

\[ f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p f(i) = ai \pmod{p} \text{ is bijection} \]

\[ \prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} f(i) \]

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

\[ \gcd((p-1)!, p) = 1 \]

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

See also Rosen 3.7 #19
RSA - A Public Key Cryptosystem

Alice:
1. Privately chooses two primes $p, q$ of, say, 500 bits each, and an $e$ rel. prime to $(p-1)(q-1)$.
2. Privately computes $n = p \cdot q$
   and $d$ such that $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$
3. Publishes $n$ and $e$, in the phonebook
   (Keep $p, q, d$ private.)

Bob (or anyone else):

Sends her an message $M$ by looking up her $n, e$ and sending $C = M^e \mod n$

Alice decrypts by computing $C^d \mod n = M$.

Issues:
- do $d$ always exist?
- how hard to compute?
- why $(M^e)^d \mod n = M$?
- how to compute $d$?