Recall: Def:

Thm: If \( \gcd(a,m) = 1 \), an inverse of \( a \) mod \( m \) exists.

Goal: want to solve linear congruences
\[ ax \equiv b \pmod{m} \]

Earlier:

Caution: Can't divide both sides by an integer.

Ex:

Thm: Let \( a, b, c \in \mathbb{Z} \), \( m \in \mathbb{Z}^+ \). If
\[ ac \equiv bc \pmod{m} \text{ and } \gcd(c, m) = 1, \]
then \( a \equiv b \pmod{m} \).

Pf:
To solve $ax \equiv b \pmod{m}$, it's useful to first solve $ay \equiv 1 \pmod{m}$.

**Ex:**

Can check:

**Ex:** Can we find $x$ s.t. $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{5}$ and $x \equiv 2 \pmod{7}$?

When does such $x$ exist? How find it?

**Chinese Remainder Theorem:** Let $m_1, \ldots, m_n$ be pairwise relatively prime positive integers and $a_1, \ldots, a_n \in \mathbb{Z}$. Then the system

\[
\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
& \vdots \\
x &\equiv a_n \pmod{m_n}
\end{align*}
\]

has a unique solution modulo $m = m_1 m_2 \ldots m_n$ (i.e., there is a solution $x$ with $0 \leq x < m$, and the set of all solutions is the set of numbers congruent to $x$ mod $m$).
Pf: We'll describe how to find $x$.

Hw: showing uniqueness.

---

Fermat's Little Thm: If $p$ prime, $a \in \mathbb{Z}$, $\not\mid p$, then $a^{p-1} \equiv 1 \pmod{p}$.

Further,

Pf:
§4.6 Cryptography

Public Key Cryptography:

RSA Cryptosystem:

To produce key for RSA, need to find 2 large primes \( p \) and \( q \), s.t.

Security of RSA based on fact that it's hard to

Algorithm: Choose \( n = pq \), where \( p \neq q \) prime, and another integer \( e \), such that

Step 1: Translate message into sequences of integers

Step 2: Encrypt integer \( M \) by replacing with:
Example:

How do we decrypt message?

Claim: To decrypt a message $C$

That is,

Prop: If $M$ is orig message and $C = M^e \mod n$ is the encrypted message, then
Lemma: If \( n = pq \) and \( a \equiv b \mod n \), then

Proof of Prop:

Ex:
Rk: Giving someone the algorithm to encrypt a message does not allow them.