Math 55 Lecture 9 §4.4, 4.6

Recall Def: If $ax \equiv 1 \pmod{m}$ then x is an

Thm: If $\gcd(a,m)=1$,

Goal: Want to solve linear congruences $ax \equiv b \pmod{m}$ where

Earlier: If $a \equiv b \pmod{m}$ and $c \in \mathbb{Z}$, then

∴ can

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

Ex:

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

Pf:

To solve $ax \equiv b \pmod{m}$, first

Ex 1: Solve ①

First solve ②

Can check: every

Ex 2: Can we find x s.t.

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

To find x:

Let $M_k =$

Note:

Let $x =$

Exercise: Check that

Back to Ex 2:

Then $x =$

$=$

$\therefore x \equiv$

Fermat's Little Thm: If p prime, $a \in \mathbb{Z}$, $p \nmid a$, then

Further, $\forall\, a \in \mathbb{Z}$

§4.6 Cryptography

Public Key Cryptography: telling someone how to encode a message does not tell them how to

RSA Cryptosystem:

To produce key for RSA, need to find 2 large primes p and q, s.t. $n = pq$ has

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

Algo: Choose $n = pq$, where $p \neq q$ prime, and another integer e, such that

Step 1: Translate message into sequences of integers (e.g.
Then group these into blocks of larger integers M.

Step 2: Encrypt integer M by replacing with:
$f(M) =$

Example: Let $p =$ so $n =$
Use $e =$
Encrypt message using RSA, by translating letters to numbers & grouping them into 4-digit blocks.

$f(\quad) =$
$f(\quad) =$
So encrypted message is

How do we decrypt message?
Need to know

Claim: To decrypt a message C, compute d

That is,
Prop: If M is orig message and
$C = M^e \bmod n$ is the encrypted message, then

Lemma: If $n = pq$ and $a \equiv b \bmod n$, then

Pf:

Proof of Prop: $C^d \equiv$

Ex: Let $p =$

Decrypt

First need to compute inverse d of $e \bmod n$.

$d =$

Now compute

This gives

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

Computation tip:

To compute