Recap

Rec Yesterday, we defined, for $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$,

$a \equiv b \pmod{m}$ to mean

$a \bmod m$ to mean

and showed

$a \equiv b \pmod{m}$ iff

iff

Ex Note that $38 - 16 =$ Then

①

②

③

Rec By the Division Algorithm, . Since $a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$,

Ex Consider the integers mod 3.

When working with respect to a modulus

Rec As a result of what we proved, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

Ex Note that $154324 \equiv \quad \pmod{5}$ and $-76938 \equiv \quad \pmod{5}$.

$154324 - 76938 \equiv$

$154324 \cdot (-76938) \equiv$

Exponentiation

<u>Rec</u> For $a \in \mathbb{Z}$, $n \in \mathbb{N}$, a^n denotes

<u>Alg</u> We want to compute $a^n \bmod m$.
Observe: if $n = 2k$,
if $n = 2k+1$,

(Repeat Squares)

```
mod-exp(a, n, m):
  if n=0, return
  if n is even,
    a_k =
    return
  if n is odd,
    a_k =
    return
```

<u>Ex</u> Calculate $10^{20} \bmod 7$.

Linear Congruences

<u>Rec</u> A linear congruence is of the form

for $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, and y a variable

If $ax \equiv 1 \pmod{m}$, we say

The inverse of a exists and is unique iff

The inverse can be found using

<u>Ex</u> Find all solutions, if any exist, to $31x \equiv 33 \pmod{225}$

① Check for solutions

② Find the inverse

$$225 = 7 \times 31 + 8$$
$$31 = 3 \times 8 + 7$$
$$8 = 1 \times 7 + 1$$

③ Use inverse to isolate x.

Chinese Remainder Theorem

Our goal is to solve systems of linear congruences.

<u>Ex</u>

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

<u>Note</u> The existence of a solution to a general system of linear congruences is not guaranteed

$x \equiv 1 \pmod{2}$

$x \equiv 0 \pmod{4}$

<u>Def</u> $a, b \in \mathbb{Z}$ are or if

<u>Thm</u> (Chinese Remainder Theorem)

Let $1 < m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$ be pairwise coprime.

Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a solution, and that solution is unique mod $m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

<u>Pf</u> (Existence)

(Uniqueness) In discussion

Using Chinese Remainder Theorem

<u>Ex</u> Consider $n=3$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

<u>Ex</u> Find the smallest positive integer solution to the system

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

① Compute the M_i

② Compute the y_i

③ Construct a solution x