

Solving $ax \equiv b \pmod{n}$.

When $\gcd(a, n) = d > 1$.

$$\text{Example: } \underline{3x \equiv 2 \pmod{6}} \Rightarrow \underline{3x \equiv 2 \pmod{3}} \quad \times$$

$$\text{No solution!} \quad y \equiv 2 \pmod{6} \Rightarrow y \equiv 2 \pmod{3}.$$

$$\text{Example: } 12x \equiv 21 \pmod{39}.$$

iff $4x \equiv 7 \pmod{13}$. → reduces to Case 1.

In HW/exam,
both are correct
answers.

$$[x \equiv 5 \pmod{13}] \Leftrightarrow x = 13k + 5 \quad \text{where } \gcd(a, n) = 1.$$

$$x = 5, 18, 31 \pmod{39} \quad x = 5, 18, 31, 44 \dots$$

solution = d.

$$x = x_0 + i \cdot \frac{n}{d} \pmod{n} \quad \text{for } i = 0 \dots (d-1).$$

$$k = 3k' \text{ or } 3k'+1 \text{ or } 3k'+2$$

Chinese Remainder Theorem (CRT)

$$\text{Example: } x \equiv 25 \pmod{42} \Rightarrow \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 1 \pmod{6} \end{cases}$$

$$\Downarrow$$

$$x = 42k + 25 \Rightarrow x = 7 \cdot (6k) + (7 \cdot 3 + 4)$$

$$x = 6 \cdot (7k) + (6 \cdot 4 + 1)$$

(CRT can be generalized to more than two congruence equations, under the condition that the divisors are pairwise coprime.)

Theorem: Suppose $\gcd(m, n) = 1$. There exists a unique solution $x \pmod{mn}$ to the following congruences:

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Proof (uniqueness): Suppose there are two solutions x and x' where $x \neq x' \pmod{mn}$.

$$(x - x') \equiv 0 \pmod{m}$$

$$(x - x') \equiv 0 \pmod{n} \quad \xrightarrow{\text{Lemma 1}} \quad mn \mid (x - x')$$

Lemma 1: If $\gcd(m, n) = 1$, and C is a multiple of both m and n , then C is a multiple of mn .

$$\begin{aligned} \text{Proof: } \gcd(m, n) = 1 &\Rightarrow m \cdot s + n \cdot t = 1 \Rightarrow C = \underline{Cms} + \underline{Cnt} \\ C = \underline{mk} = \underline{nl} &= ntms + mknt \\ &= mn(ls + kt). \end{aligned}$$

Algorithms for CRT:

1. Use the extend Euclidean algorithm to compute (s, t)
 $ms + nt = 1$.

2. Return $x = ant + bms \pmod{mn}$.

$$\begin{aligned} \text{Correctness: } nt &\equiv 1 \pmod{m} \\ ms &\equiv 1 \pmod{n} \end{aligned}$$

$$\text{We can verify } x \equiv \underline{ant} + \underline{bms} \equiv a \pmod{m}$$

$$\text{Similarly } x \equiv \underline{-} \dots \equiv b \pmod{n}$$

$$\text{Alternative algorithm: } x \equiv a \pmod{m} \Leftrightarrow nx \equiv na \pmod{mn}$$

$$x \equiv b \pmod{n} \Leftrightarrow mx \equiv mb \pmod{mn}$$

$$(m+n)x \equiv ant + bm \Leftrightarrow x \equiv \underline{(m+n)^{-1}}(ant + bm) \pmod{mn}$$

$$\gcd(m, n) \Rightarrow \gcd(m+n, mn) = 1 \Rightarrow \underline{(m+n)^{-1}} \pmod{mn} \text{ exists.}$$

Modular Exponentiation.

What is $x^a \bmod n$?

Example: $2^{1234} \bmod 789$.

Last 3 digits of 3^{101}

Attempt 1: Compute x^a and then mod n.

Too slow! Need to work with very large numbers.

Attempt 2: $\underbrace{((x \cdot x \bmod n) \cdot x \bmod n) \cdot x \bmod n \dots}_{\text{repeat } a \text{ times}}$

This is better. We work with only numbers $< n^2$

Still slow. Need $(a-1)$ modular multiplication.

Repeated squaring.

We can compute $(x^a \bmod n)$ using at most

$2 \cdot \log_2(a)$ multiplications mod n.