CSE 107: Introduction to Modern Cryptography

Nadia Heninger

UCSD

Winter 2025 Lecture 11

Last time: Midterm

This time: Number theory review

Fundamental theorem of arithmetic

Theorem

Every $n \in \mathbb{Z}$ $n \neq 0$ has unique factorization $n = \pm p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ with p_i distinct primes and e_i positive integers.

Division and remainder

Theorem

$a, b \in \mathbb{Z},\ b > 0,\ \exists$ *unique* $q, r \in \mathbb{Z}$ *s.t.* $a = bq + r,\ 0 \leq r < b.$

$r \equiv a \bmod b \qquad a \bmod b = a - b\lfloor \frac{a}{b} \rfloor$

Because we're in CS, we also write $r = a \bmod b$.

$b \mid a \iff a \bmod b = 0$

$a = b \bmod N$: $(a \bmod N) = (b \bmod N)$

$a = b \bmod N \iff N \mid (a - b)$

GCDs and Extended Euclidean Algorithm

$\gcd(a, b)$: greatest common divisor d s.t. $d \mid a$ and $d \mid b$

Theorem (Extended Euclidean Algorithm)

$a, b \in \mathbb{Z}$ (and positive) $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a, b)$

Euclidean Algorithm

Input: $a, b \in \mathbb{Z}$
Output: $d = \gcd(a, b)$

If $b = 0$:
    return a
else:
    return $\gcd(b, a \bmod b)$

Extended Euclidean Algorithm

Input: $a, b \in \mathbb{Z}$
Output: d, x, y with $d = \gcd(a, b)$, $ax + by = d$

If $b \mid a$:
  return $b, 0, 1$
else:
  compute $a = qb + r$
  $d, x, y = \text{egcd}(b, r)$ (xb + yr = d)
  return $(d, y, x - yq)$

Theorem
The Extended Euclidean Algorithm runs in time $O(\lg(a)\lg(b))$.

Theorem
If $c \mid ab$, $\gcd(a, c) = 1 \implies c \mid b$

Addition modulo N

The integers modulo $N \in \mathbb{Z}$ are *closed* under addition.

$$a + b \equiv c \bmod N \iff (a \bmod N) + (b \bmod N) = (c \bmod N)$$

There is an *identity element* 0 with the property that:

$$a + 0 \equiv 0 + a \equiv a \bmod N \qquad \forall a \in \mathbb{Z}$$

Any $a \in \mathbb{Z}$ has an *additive inverse* which is an integer "$-a$" such that

$$a + (-a) \equiv (-a) + a \equiv 0 \bmod N$$

For example, $3 + (-3) \equiv 3 + 2 \equiv 0 \bmod 5$.

Multiplication modulo N

Let's do the same thing with multiplication.

The integers modulo $N \in \mathbb{Z}$ are *closed* under multiplication.

$$a \cdot b \equiv c \bmod N \iff (a \bmod N) \cdot (b \bmod N) = (c \bmod N)$$

There is an *identity element* 1 with the property that:

$$a + 1 \equiv 1 + a \equiv a \bmod N \qquad \forall a \in \mathbb{Z}$$

We would like to define a "multiplicative inverse" analogously to the additive inverse we defined on the previous slide. For $a \in \mathbb{Z}$, we would like to find some "multiplicative inverse" element a^{-1} such that

$$a \cdot (a^{-1}) \equiv 1 \bmod N$$

Multiplicative inverses are not always well defined

For $a \in \mathbb{Z}$, we would like to find some "multiplicative inverse" element a^{-1} such that

$$a \cdot (a^{-1}) \equiv 1 \bmod N$$

However, we can't always do this.
For example:

- Set $a = 3$ and $N = 3$. Check that there is no integer we can multiply with a to get $1 \bmod N$.
- Set $a = 3$ and $N = 6$. $a \cdot b$ is always 0 or 3 mod6.
- Set $a = 6$ and $N = 9$. Same problem.

Multiplicative modular inverses

Inverse of b mod N: $b^{-1} \in \mathbb{Z}$, $0 < b^{-1} < N$, with

$$b \cdot b^{-1} \equiv 1 \bmod N$$

- Not defined if b not invertible modulo N.
- 0 has no inverse.

Theorem

a *invertible* $\bmod N \iff \gcd(a, N) = 1$

Multiplicative modular inverses

Inverse of b mod N: $b^{-1} \in \mathbb{Z}$, $0 < b^{-1} < N$, with

$$b \cdot b^{-1} \equiv 1 \bmod N$$

- Not defined if b not invertible modulo N.
- 0 has no inverse.

Theorem

a invertible mod $N \iff \gcd(a, N) = 1$

Proof.

$\Longrightarrow$

$$ab \equiv 1 \bmod N$$

$$ab = 1 + cN$$

$$ab - cN = 1 \quad \Longrightarrow \gcd(a, N) = 1$$

Multiplicative modular inverses

Inverse of b mod N: $b^{-1} \in \mathbb{Z}$, $0 < b^{-1} < N$, with

$$b \cdot b^{-1} \equiv 1 \bmod N$$

- Not defined if b not invertible modulo N.
- 0 has no inverse.

Theorem

a invertible mod $N \iff \gcd(a, N) = 1$

Proof.

$\Longrightarrow$

$$ab \equiv 1 \bmod N$$

$$ab = 1 + cN$$

$$ab - cN = 1 \quad \Longrightarrow \gcd(a, N) = 1$$

$\Longleftarrow \quad ax + Ny = 1 \quad \Longrightarrow x = a^{-1} \bmod N$

Explicitly computing multiplicative modular inverses

Implication of previous slide: Can compute modular inverses using extended GCD algorithm.