Intro. Number Theory

Notation

Background

We will use a bit of number theory to construct:

- Key exchange protocols
- Digital signatures
- Public-key encryption

This module: crash course on relevant concepts

More info: read parts of Shoup's book referenced
at end of module

Notation

From here on:

- N denotes a positive integer.
- p denote a prime.

Notation: $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$

Can do addition and multiplication modulo N

Modular arithmetic

Examples: let $N = 12$

$$9 + 8 = 5 \quad \text{in } \mathbb{Z}_{12}$$

$$5 \times 7 = 11 \quad \text{in } \mathbb{Z}_{12}$$

$$5 - 7 = 10 \quad \text{in } \mathbb{Z}_{12}$$

Arithmetic in $\mathbb{Z}_N$ works as you expect, e.g $x \cdot (y+z) = x \cdot y + x \cdot z$ in $\mathbb{Z}_N$

Greatest common divisor

Def: For ints. x,y: **gcd(x, y)** is the greatest common divisor of x,y

Example: gcd(12, 18) = 6

$\boxed{2} \times 12 + \boxed{-1} \times 18 = 6$

Fact: for all ints. x,y there exist ints. a,b such that

$$a \cdot x + b \cdot y = \mathrm{gcd}(x,y)$$

a,b can be found efficiently using the extended Euclid alg.

If gcd(x,y)=1 we say that x and y are **relatively prime**

Modular inversion

Over the rationals, inverse of 2 is ½ . What about $\mathbb{Z}_N$?

<u>Def</u>: The **inverse** of x in $\mathbb{Z}_N$ is an element y in $\mathbb{Z}_N$ s.t. $x \cdot y = 1$ in $\mathbb{Z}_N$

y is denoted x^{-1} .

Example: let N be an odd integer. The inverse of 2 in $\mathbb{Z}_N$ is $\frac{N+1}{2}$

$$2 \cdot \left(\frac{N+1}{2}\right) = N+1 = 1 \text{ in } \mathbb{Z}_N$$

Modular inversion

Which elements have an inverse in $\mathbb{Z}_N$?

Lemma: x in $\mathbb{Z}_N$ has an inverse if and only if gcd(x,N) = 1

Proof:

gcd(x,N)=1 $\Rightarrow$ $\exists$ a,b: $a \cdot x + b \cdot N = 1$ $\Longrightarrow$ $a \cdot x = 1$ in $\mathbb{Z}_N$

$\Longrightarrow$ $x^{-1} = a$ in $\mathbb{Z}_N$

gcd(x,N) > 1 $\Rightarrow$ $\forall$a: gcd($a \cdot x$, N) > 1 $\Rightarrow$ $a \cdot x \neq 1$ in $\mathbb{Z}_N$

gcd(x,N) = 2 $\Longrightarrow$ $\forall a$: $a \cdot x$ is even $\Longrightarrow$ $\underbrace{a \cdot x}_{\text{even}} \neq \overbrace{b \cdot N + 1}^{\text{odd}}$

More notation

<u>Def:</u> $\mathbb{Z}_N^*$ = (set of invertible elements in $\mathbb{Z}_N$) =

= { x∈ $\mathbb{Z}_N$: gcd(x,N) = 1 }

Examples:

1. for prime p, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$

2. $\mathbb{Z}_{12}^*$ = { 1, 5, 7, 11}

For x in $\mathbb{Z}_N^*$, can find x^{-1} using extended Euclid algorithm.

Solving modular linear equations

Solve: $a \cdot x + b = 0$ in $\mathbb{Z}_N$

Solution: $x = -b \cdot a^{-1}$ in $\mathbb{Z}_N$

Find a^{-1} in $\mathbb{Z}_N$ using extended Euclid. Run time: $O(\log^2 N)$

What about modular quadratic equations?

next segments

End of Segment