Number Theory

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

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

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

$5 - 7 = 10$ 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

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

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 $\frac{N+1}{2}$

$2 \cdot \left(\frac{N+1}{2}\right) = N+1 = 1$ 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 $\Longrightarrow$ $\overset{\text{even}}{\overline{a \cdot x}} \neq \overset{\text{odd}}{\overline{b \cdot N + 1}}$

More notation

Def: $\mathbb{Z}_N^*$ = (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

Intro. Number Theory

Fermat and Euler

Review

N denotes an n-bit positive integer. p denotes a prime.

- Z_N = { 0, 1, …, N-1 }

- $(Z_N)^*$ = (set of invertible elements in Z_N) =
  = $\{\ x \in Z_N\ :\ \gcd(x,N) = 1\ \}$

Can find inverses efficiently using Euclid alg.: time = $O(n^2)$

Fermat's theorem (1640)

<u>Thm</u>: Let p be a prime

$$\forall\, x \in (Z_p)^* : \quad x^{p-1} = 1 \text{ in } Z_p$$

Example: p=5. $3^4 = 81 = 1$ in Z_5

So: $x \in (Z_p)^* \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2}$ in Z_p

another way to compute inverses, but less efficient than Euclid

Application: generating random primes

Suppose we want to generate a large random prime

say, prime p of length 1024 bits (i.e. $p \approx 2^{1024}$)

Step 1: choose a random integer $p \in [\ 2^{1024}\ ,\ 2^{1025}-1\ ]$

Step 2: test if $2^{p-1} = 1$ in Z_p

If so, output p and stop. If not, goto step 1 .

Simple algorithm (not the best). **Pr[p not prime] < 2^{-60}**

The structure of $(Z_p)^*$

<u>**Thm**</u> (Euler): $(Z_p)^*$ is a **cyclic group**, that is

$$\exists\ g \in (Z_p)^* \quad \text{such that} \quad \{1, g, g^2, g^3, \ldots, g^{p-2}\} = (Z_p)^*$$

g is called a <u>**generator**</u> of $(Z_p)^*$

Example: $p=7$. $\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (Z_7)^*$

Not every elem. is a generator: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

Order

For $g \in (Z_p)^*$ the set $\{1, g, g^2, g^3, \dots\}$ is called

the **group generated by g**, denoted <g>

Def: the **order** of $g \in (Z_p)^*$ is the size of <g>

$$\mathbf{ord_p(g) \quad = \quad |\langle g \rangle| \quad = \quad (\text{smallest } a>0 \text{ s.t. } g^a = 1 \text{ in } Z_p)}$$

Examples: $ord_7(3) = 6$; $ord_7(2) = 3$; $ord_7(1) = 1$

Thm (Lagrange): $\forall g \in (Z_p)^*$: $\mathbf{ord_p(g)}$ divides $p-1$

Euler's generalization of Fermat (1736)

Def: For an integer N define $\varphi(N) = |(Z_N)^*|$ (Euler's φ func.)

Examples: $\varphi(12) = |\{1,5,7,11\}| = 4$; $\varphi(p) = p-1$

For $N=p\cdot q$: $\varphi(N) = N-p-q+1 = (p-1)(q-1)$

Thm (Euler): $\forall\, x \in (Z_N)^*$: $x^{\varphi(N)} = 1$ in Z_N

Example: $5^{\varphi(12)} = 5^4 = 625 = 1$ in Z_{12}

Generalization of Fermat. Basis of the RSA cryptosystem

End of Segment