CSIT 495/595 - Introduction to Cryptography

Overview of Number Theory

Bharath K. Samanthula
Department of Computer Science
Montclair State University

Outline

- Prime and Composites
- Modular Arithmetic
- Groups and Fermat's theorem
- Euler's Generalization
- Intractable Problems

Primes and Composites

- The set of integers is denoted by $\mathbb{Z}$
- For any $a, b \in \mathbb{Z}$, we say a divides b (denoted by $a|b$), if $ac = b$
- If a is positive, a is called a divisor of b
- Prime Number: any integer greater than 1 that has only two divisors, namely 1 and itself
  - Example: 2,3,5,7,11,...
- Composite Number: A positive integer greater than 1 and not a prime
  - Example: 4,6,8,9,10,...

Primes and Composites

- Every integer greater than 1 can be expressed uniquely as product of primes, each with positive exponent
- Fundamental Theorem of Arithmetic: any positive integer x can be written as

$$x = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

where p_i's are distinct primes for all $e_i \geq 1$

- Example: $84 = 2^2 \cdot 3 \cdot 7$

Greatest Common Divisor

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

Example: gcd(12, 18) = 6 $2 \times 12 + (-1) \times 18 = 6$

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**

some slides are adopted from *Intro. Number Theory* by Dan Boneh

Modular Arithmetic Notation

- Let $\mathbb{Z}_N$ denote the set $\{0,1,\ldots,N-1\}$, where N is a positive integer
- a mod N denote the remainder of a upon division by N
- If $a = qN + r$, then $r = a$ mod N (of course, $q = 0$ if $a \in \mathbb{Z}_N$)
- The process of mapping a to a mod N is called "reduction modulo N"
- Note that a mod $N \in \mathbb{Z}_N$

Modular Arithmetic Example

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 $\mathbb{Z}_N$

How to handle negative modulo reduction modulo *N*?

Modular Arithmetic Properties

1) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:

$a \pm c \equiv b \pm d \pmod{n}$ and

$ac \equiv bd \pmod{n}$

2) If $a \equiv b \pmod{n}$ and $d \mid n$ then:

$a \equiv b \pmod{d}$

Modular Inversion

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

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

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

The Group $\mathbb{Z}_N^*$

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

= { $x \in \mathbb{Z}_N$: 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: $O(\log^2 N)$

Fermat's Theorem (1640)

Thm: Let p be a prime

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

Example: $p=5$. $\quad 3^4 = 81 = 1$ 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}**

Cyclic Group and Generators

Thm (Euler): $(Z_p)^*$ is a **cyclic group**, that is

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

g is called a **generator** 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: $\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

Group Order

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

the **group generated by g**, denoted $\langle g \rangle$

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

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

Examples: $\text{ord}_7(3) = 6$; $\text{ord}_7(2) = 3$; $\text{ord}_7(1) = 1$

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

Euler's Generalization of Fermat

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

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

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

Intractable problems

- There many problems that are easy to solve
  - Given a composite N and $x \in \mathbb{Z}_N$ find x_N^{-1}
- There also exist several hard (intractable) problems

Discrete Log Problem (DLOG)

Fix a prime $p>2$ and g in $(Z_p)^*$ of order q.

Consider the function: $x \mapsto g^x$ in Z_p

Now, consider the inverse function:

$\text{Dlog}_g(g^x) = x$ where x in $\{0, \ldots, q-2\}$

Example:

in $\mathbb{Z}_{11}$:	1,	2,	3,	4,	5,	6,	7,	8,	9,	10
$\text{Dlog}_2(\cdot)$:	0,	1,	8,	2,	4,	9,	7,	3,	6,	5

Discrete Log Problem (DLOG)

Let **G** be a finite cyclic group and **g** a generator of G

$$G = \{ 1, g, g^2, g^3, \ldots, g^{q-1} \} \qquad (q \text{ is called the order of } G)$$

Def: We say that **DLOG is hard in G** if for all efficient alg. A:

$$\Pr_{g \leftarrow G,\, x \leftarrow Z_q} [\, A(G, q, g, g^x) = x \,] < \text{negligible}$$

Example candidates:

(1) $(Z_p)^*$ for large p, (2) Elliptic curve groups mod p

Intractable problems with Composites

Consider the set of integers: (e.g. for n=1024)

$$\mathbb{Z}_{(2)}(n) := \{ N = p \cdot q \text{ where } p,q \text{ are n-bit primes} \}$$

Problem 1: Factor a random N in $\mathbb{Z}_{(2)}(n)$ (e.g. for n=1024)

Problem 2: Given a polynomial **f(x)** where degree(f) > 1

and a random N in $\mathbb{Z}_{(2)}(n)$

find x in $\mathbb{Z}_N$ s.t. f(x) = 0 in $\mathbb{Z}_N$

Factorization Problem

Gauss (1805): *"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic."*

Best known alg. (NFS): run time exp($\tilde{O}(\sqrt[3]{n})$) for n-bit integer

Current world record: **RSA-768** (232 digits)

- Work: two years on hundreds of machines
- Factoring a 1024-bit integer: about 1000 times harder

$\Rightarrow$ likely possible this decade

Summary

- Prime and Composites
- Modular Arithmetic
- Groups and Fermat's theorem
- Euler's Generalization
- Intractable Problems

Useful References

- Chapter 8, Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell, 2nd Edition, CRC Press, 2015.
- `http://shoup.net/ntb/ntb-v2.pdf`
- `http://www.math.utk.edu/~finotti/papers/grad.pdf`