Number Theory

Deepak Puthal

Email: Deepak.Puthal@uts.edu.au

41900 – Fundamentals of Security

Overview

- Motivation
- Introduction
- Divisors
- Greatest Common Divisor (GCD)
- Modular Arithmetic
- Euclidean Algorithm
- Group
- Ring
- Field

Motivation

- Number theory is the basic of a lot of public-key crypto.
- RSA is “secure” because factoring large numbers is hard.

Core Concept

Find a number theoretic problem that’s incredibly difficult to solve if you don’t have a key piece of information.

- For example:
  - Multiplying two large primes p, q is easy. Splitting a number $n = pq$ into its factors is hard.
  - Raising a number g to the power a is easy. Finding a given only g^a is hard.

Introduction

- Will now introduce finite fields
- Increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- Concern operations on “numbers”
  - Where what constitutes a “number” and the type of operations varies considerably
- Start with basic number theory concepts

Divisors

- Say a non-zero number `b` divides `a` if for some `m` have `a=mb`

  (`a,b,m` all integers)
- That is `b` divides into `a` with no remainder
- denote this `b|a`
- and say that `b` is a divisor of `a`
- eg. all of 1,2,3,4,6,8,12,24 divide 24
- eg. 13 | 182; –5 | 30; 17 | 289; –3 | 33; 17 | 0

Properties of Divisibility

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $a|b$ and $b|c$, then $a|c$

  e.g. $11|66$ and $66|198$ so $11|198$
- If $b|g$ and $b|h$, then $b|(mg + nh)$

for arbitrary integers m and n

e.g. b = 7; g = 14; h = 63; m = 3; n = 2

7|14 and 7|63 hence 7 | 42+126 = 168

Division Algorithm

- if divide a by n get integer quotient q and integer remainder r such that:

  $a = qn + r$ where $0 \leq r < n$; $q = floor(a/n)$

- Remainder r often referred to as a **residue**

Greatest Common Divisor (GCD)

- A common problem in number theory
- `GCD (a, b)` of `a` and `b` is the largest integer that divides evenly into both `a` and `b`

  e.g. `GCD(60, 24) = 12`

- define `gcd(0, 0) = 0`
- often want no common factors (except 1) define such numbers as relatively prime

  e.g. `GCD(8, 15) = 1`

  hence `8` & `15` are relatively prime

Example GCD(1970,1066)

```
1970 = 1 x 1066 + 904   gcd(1066, 904)
1066 = 1 x 904 + 162    gcd(904, 162)
904 = 5 x 162 + 94      gcd(162, 94)
162 = 1 x 94 + 68       gcd(94, 68)
94 = 1 x 68 + 26        gcd(68, 26)
68 = 2 x 26 + 16        gcd(26, 16)
26 = 1 x 16 + 10        gcd(16, 10)
16 = 1 x 10 + 6         gcd(10, 6)
10 = 1 x 6 + 4          gcd(6, 4)
6 = 1 x 4 + 2           gcd(4, 2)
4 = 2 x 2 + 0           gcd(2, 0)
```

Integers modulo n: $Z_n^\times$

Fix a number $n \in Z$, and do arithmetic modulo n : keep only the remainder after dividing by n.

`6+6=12=0 (mod 12)`

`5−9=−4=8 (mod 12)`

`5×11=55=7(mod 12)`

This system of numbers is called Z_n. (The example above is Z_{12}).

It is finite: each number is uniquely represented as one of

$$Z_n = \{0, 1, 2, 3, \ldots, n-1\}$$

If $a, b \in Z_n$ a, write simply `a + b` instead of `a+b(mod n)`.

Properties of $Z_n^\times$

Group Size The size of the group $Z_n^\times$ is denoted $\phi(n)$, called Euler's phi function or Euler's totient function.

If p, q are distinct primes, then $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$

Important For any $x \in Z_n^\times$, $x^{\phi(n)}$ = 1.

Generators There is sometimes an element $g \in Z_n^\times$ which "hits all of $Z_n^\times$", i.e. $\{x^0, x^1, x^2, \ldots, x^{n-1}\}$ = $Z_n^\times$.

This is always the case if n is prime.

Inverses Every element $a \in Z_n^\times$ has an inverse: some $b \in Z_n^\times$ such that $ab = 1$. Since $a^{\phi(n)} = 1$, this makes $a^{\phi(n)-1}$ the inverse of a: $a^{\phi(n)-1}a = 1$.

- Inverses are usually found using Bézout's identity, rather than computing $\phi(n)$.

Generated Sequences in $Z_n^{\times}$

If all elements in $Z_n^{\times}$ can be obtained via g using:

$$g^x mod\ n$$

Where $x \in Z$ (i.e. any integer)

Then we state that:

$$g \text{ is a generator for } Z_n^{\times}$$

$$Z_n^{\times} = [1, g, g^2, g^3, \cdots, g^{\phi(n)-1}]$$

The length of the maximum sequence for $Z_n^{\times}$ is given by $\phi(n)$.

- If Z_p^*, where p is prime, then $\phi(p) = p - 1$
- If $Z_n^{\times}$, where $n = pq$ (a composite prime), then:

$$\phi(n) = \phi(p)\phi(q) = (p - 1)(q - 1)$$

Note: the length of the sequence is maximal for Z_p^*

Inverses in $Z_n^\times$

Each element $a \in Z_n^\times$ has an inverse a^{-1} such that

$$a \times a^{-1} = 1 \; mod \; n.$$

Each element $a \in Z_n^\times$, except for 0, is invertible.

Simple inversion algorithm

For Z_p^*, where p is prime:

$$x^{-1} = x^{\phi(n)-1} = x^{(p-1)-1} = x^{p-2} \; mod \; p$$

For $Z_n^\times$, where $n = pq$:

$$x^{-1} = x^{\phi(n)-1} = x^{\phi(p)\phi(q)-1} = x^{(p-1)(q-1)-1} \; mod \; p$$

Example inverses in $Z_n^{\times}$

Example:

Given p = 7, q = 3, and n = pq = 7 × 3 = 21

We select x = 11 out of Z_{21}^{*} and want to invert it.

$$x^{-1} = x^{(p-1)(q-1)-1} \; mod \; n$$

$$= x^{(6\times 2)-1} \; mod \; 21$$

$$= 11^{11} \; mod \; 21$$

$$= 2$$

check that $x \cdot x^{-1} \; mod \; n$ = 1

$$11 \times 2 \; mod \; 21 = 22 \; mod \; 21 = 1$$

Modular Arithmetic

- Define modulo operator "`a mod n`" to be remainder when `a` is divided by `n`
  - Where integer `n` is called the modulus
- `b` is called a residue of `a` mod `n`
  - Since with integers can always write: `a = qn + b`
  - Usually chose smallest positive remainder as residue

    i.e. `0 <= b <= n-1`
  - process is known as modulo reduction

    e.g. `-12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7`
- a & b are congruent if: `a mod n = b mod n`
  - when divided by `n`, `a` & `b` have same remainder

    e.g. 100 mod 11 = 34 mod 11

    so 100 is congruent to 34 mod 11

Modular Arithmetic Operations

- can perform arithmetic with residues
- uses a finite number of values, and loops back from either end

  $Z_n=\{0, 1, . . . , (n - 1)\}$

- modular arithmetic is when do addition & multiplication and modulo reduce answer
- can do reduction at any point,

  i.e. `a+b mod n = [a mod n + b mod n] mod n`

Modular Arithmetic Operations

- [(a mod n) + (b mod n)] mod n = (a + b) mod n
- [(a mod n) – (b mod n)] mod n = (a – b) mod n
- [(a mod n) x (b mod n)] mod n = (a x b) mod n

e.g.

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2 (11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) – (15 mod 8)] mod 8 = –4 mod 8 = 4 (11 – 15) mod 8 = –4 mod 8 = 4

[(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8 = 165 mod 8 = 5

Modulo 8 Addition Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Modulo 8 Multiplication

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Modular Arithmetic Properties

Property	Expression
Commutative laws	$(w + x) mod\ n = (x + w) mod\ n$ $(w \times x) mod\ n = (x \times w) mod\ n$
Associative laws	$[(w \times x) \times y] mod\ n = [w \times (x \times y)] mod\ n$ $[(w \times x) \times y] mod\ n = [w \times (x \times y)] mod\ n$
Distributive laws	$[w \times (x + y)] mod\ n = [(w \times x) + (w \times y)] mod\ n$
Identities	$(w + 0) mod\ n = w\ mod\ n$ $(w \times 1) mod\ n = w\ mod\ n$
Additive inverse (-w)	For each $w \in Z_n$, there exist a z such that $w + z = 0\ mod\ n$

Euclidean Algorithm

- an efficient way to find the `GCD(a, b)`
- uses theorem that:

```
GCD(a, b) = GCD(b, a mod b)
```

- Euclidean Algorithm to compute `GCD(a, b)` is:

```
Euclid(a, b)
    if (b=0) then return a;
    else return Euclid(b, a mod b);
```

Extended Euclidean Algorithm

- calculates not only GCD but x & y:

  `ax + by = d = gcd(a, b)`

- useful for crypto computations
- follow sequence of divisions for GCD but assume at each step `i`, can find `x & y`:

  `r = ax + by`

- at end find GCD value and also `x & y`
- if `GCD(a,b)=1` these values are inverses

Finding Inverses

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3)=(1, 0, m);
   (B1, B2, B3)=(0, 1, b)
2. if B3 = 0
   return A3 = gcd(m, b); no inverse
3. if B3 = 1
   return B3 = gcd(m, b); B2 = b–1 mod m
4. Q = A3 div B3
5. (T1, T2, T3)=(A1 – Q B1, A2 – Q B2, A3 – Q B3)
6. (A1, A2, A3)=(B1, B2, B3)
7. (B1, B2, B3)=(T1, T2, T3)
8. goto 2
```

Group

- a set S of elements or “numbers”
  - may be finite or infinite
- with some operation '.' so $G=(S,.)$
- Obeys CAIN:
  - Closure: a,b in S, then $a.b$ in S
  - Associative law: $(a.b).c = a.(b.c)$
  - has Identity e: $e.a = a.e = a$
  - has iNverses a^{-1}: $a.a^{-1} = e$
- if commutative $a.b = b.a$
  - then forms an abelian group

Cyclic Group

- define exponentiation as repeated application of operator

  example: $a^3 = a.a.a$
- and let identity be: $e=a^0$
- a group is cyclic if every element is a power of some fixed element a

  i.e., $b = a^k$ for some a and every b in group
- a is said to be a **generator** of the group

Ring

- a set of “numbers”
- with two operations (addition and multiplication) which form:
- an abelian group with addition operation
- and multiplication:
  - has closure
  - is associative
  - distributive over addition: $a(b+c) = ab + ac$
- if multiplication operation is commutative, it forms a **commutative ring**
- if multiplication operation has an identity and no zero divisors, it forms an **integral domain**

Field

- a set of numbers
- with two operations which form:
  - abelian group for addition
  - abelian group for multiplication (ignoring 0)
  - ring
- have hierarchy with more axioms/laws
- group -> ring -> field

Using a Generator

- equivalent definition of a finite field
- a generator g is an element whose powers generate all non-zero elements

    in F have $0, g^0, g^1, \dots, g^{q-1}$
- can create generator from root of the irreducible polynomial
- then implement multiplication by adding exponents of generator