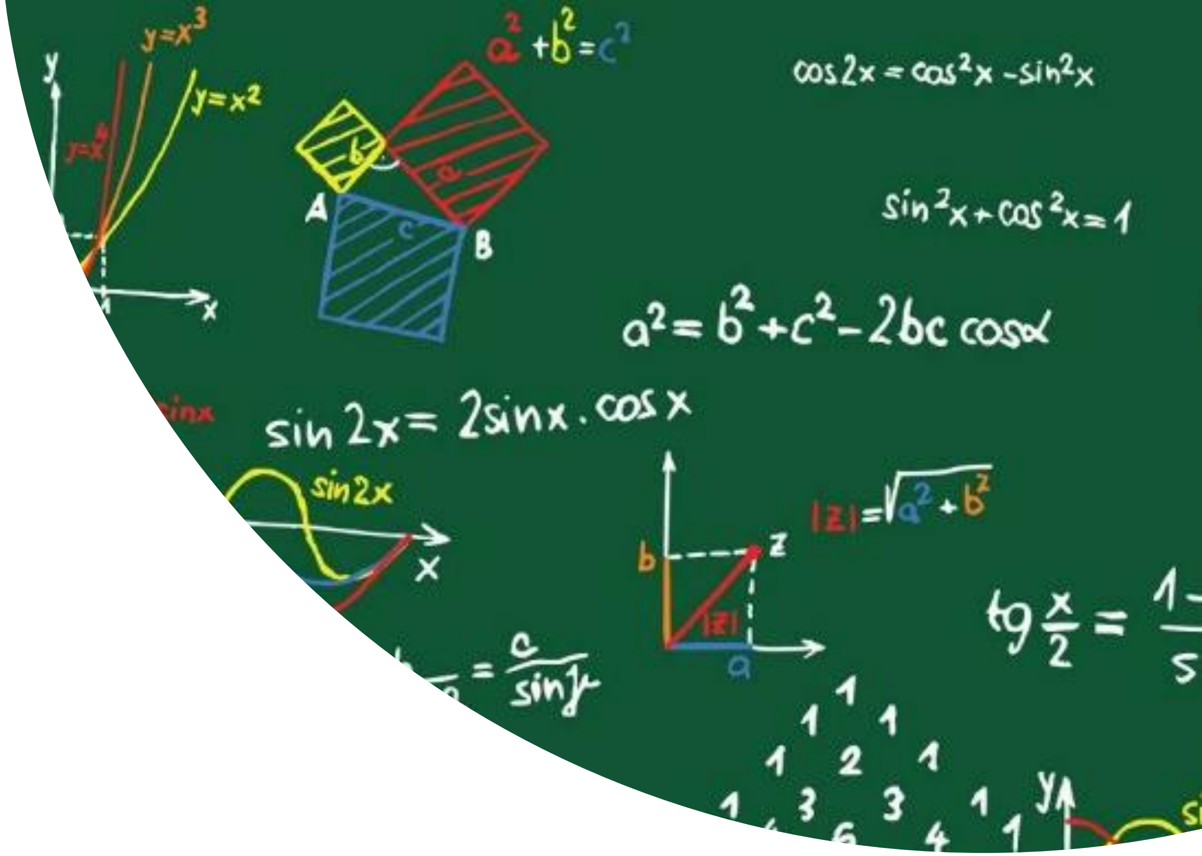

Number Theory

Ashish Nanda
Ashish.Nanda@uts.edu.au

Number Theory and Cryptography

Number theory is the basic of a lot of public-key crypto.

- Diffie-Hellman is “secure” because the discrete log problem is “hard”
- RSA is “secure” because integer factorisation is “hard”.

Key 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.

Let’s start with: Divisors

Say a non-zero number **b** divides **a** for some remainder **m**

- That is: **a = mb** where **a b** and **m** are all integers

If **b** divides **a** with no remainder, it is represented using ‘|’

- That is: **b | a**

- Example: All of **1,2,3,4,6,8,12,24** divide **24**
- Example: **13 | 182 –5 | 30 17 | 289 –3 | 33 17 | 0**

Properties of Divisibility

- If $a \mid 1$, then $a = \pm 1$.
- If $a \mid b$ and $b \mid a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $a \mid b$ and $b \mid c$, then $a \mid c$
  - Example: $11 \mid 66$ and $66 \mid 198$ so $11 \mid 198$

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$
  - Example: for arbitrary integers $b = 7$, $g = 14$, $h = 63$, $m = 3$, $n = 2$
  - $7 \mid 14$ and $7 \mid 63$ hence $7 \mid (42+126) = 7 \mid 168$

Greatest Common Divisor (GCD)

GCD (a, b) of **a** and **b** is the largest integer that divides both **a** and **b**

- Example: **GCD(60, 24) = 12** **GCD(0, 0) = 0**

If two numbers have no common factors (except 1) they can be defined as relatively prime

- Example: **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)

Euclidean Algorithm

An efficient way to find the **GCD(a, b)** is using the theorem that:

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

Euclidean Algorithm used to compute **GCD(a, b)** is:

Euclid(a, b)

If **(b=0)** then return **a;**

Else return **Euclid(b, a mod b);**

Modular Arithmetic

A modulo operator can be defined as **a mod n** to give the remainder **b**

- **a** is our divided
- **n** is called the modulus
- **b** is called a **residue** of **a mod n**

The same can represented as: **a = qn + b**

- We usually chose the smallest positive remainder as residue
  - **0 <= b <= n-1**
- The process is known as modulo reduction
  - **-12 mod 7 = -5 mod 7 = 2**

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** for the operation **mod 11**

Modular Arithmetic Operations

$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

$(a – b) \bmod n = [(a \bmod n) – (b \bmod n)] \bmod n$

$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Examples:

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$; $(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) – (15 \bmod 8)] \bmod 8 = –4 \bmod 8 = 4$; $(11 – 15) \bmod 8 = –4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$; $(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

Modular Arithmetic Properties

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

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

Integers modulo n: Z_n

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

Some examples of modulus division:

- **6 (mod 12) = 0**
- **–4 (mod 12) = 8**
- **55 (mod 12) = 7**

This system of numbers is called $\mathbf{Z_n}$.

(The example above is $\mathbf{Z_{12}}$).

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

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

The multiplicative group of $Z_n^{\times}$

A multiplicative group $\mathbf{Z_n^{\times}}$ can be defined as:

- $\mathbf{Z_n^{\times}} = \{\mathbf{a} \in \mathbf{Z_n} \mid \mathbf{gcd}(\mathbf{a}, \mathbf{n}) = \mathbf{1}\}$
- $\mathbf{Z_n^{\times}}$ is all elements $\mathbf{a} \in \mathbf{Z_n}$ such that the $\mathbf{gcd}(\mathbf{a}, \mathbf{n}) = \mathbf{1}$

For Example:

$$\mathbf{Z_{21}} = [\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \mathbf{7}, \mathbf{8}, \mathbf{9}, \mathbf{10}, \mathbf{11}, \mathbf{12}, \mathbf{13}, \mathbf{14}, \mathbf{15}, \mathbf{16}, \mathbf{17}, \mathbf{18}, \mathbf{19}, \mathbf{20}]$$

$$\mathbf{Z_{21}^{\times}} = \{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{5}, \mathbf{8}, \mathbf{10}, \mathbf{11}, \mathbf{13}, \mathbf{16}, \mathbf{17}, \mathbf{19}, \mathbf{20}\}$$

This removes **0** and any elements that share a divisor with **21**.

- Addition and subtraction can no longer be done in $\mathbf{Z_n^{\times}}$.
- Multiplication **and division** work: every number has an inverse!.
- The size of $\mathbf{Z_n^{\times}}$ is **ϕ(n)**, the number of positive integers less than **n** coprime to **n**.

Properties of $Z_n^\times$

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

- If $\mathbf{p}, \mathbf{q}$ are distinct primes, then $\boldsymbol{\phi}(\mathbf{pq}) = \boldsymbol{\phi}(\mathbf{p})\boldsymbol{\phi}(\mathbf{q}) = (\mathbf{p} - \mathbf{1})(\mathbf{q} - \mathbf{1})$
- For any $\mathbf{x} \in \mathbf{Z_n^\times}$, $\mathbf{x}^{\boldsymbol{\phi}(\mathbf{n})} = \mathbf{1}$.

Generator: There is sometimes an element $\mathbf{g} \in \mathbf{Z_n^\times}$ which "hits all of $\mathbf{Z_n^\times}$",

- i.e. $\{\mathbf{x}^0, \mathbf{x}^1, \mathbf{x}^2, \ldots, \mathbf{x}^{\mathbf{n}-1}\} = \mathbf{Z_n^\times}$.
- This is always the case if n is prime.

Inverses: Every element $\mathbf{a} \in \mathbf{Z_n^\times}$ has an inverse: $\mathbf{b} \in \mathbf{Z_n^\times}$ such that $\mathbf{ab} = \mathbf{1}$.

- Since $\mathbf{a}^{\boldsymbol{\phi}(\mathbf{n})} = \mathbf{1}$, this makes $\mathbf{a}^{\boldsymbol{\phi}(\mathbf{n})-\mathbf{1}}$ the inverse of $\mathbf{a}$: $\mathbf{a}^{\boldsymbol{\phi}(\mathbf{n})-\mathbf{1}}\mathbf{a} = \mathbf{1}$.
- Inverses are usually found using Bézout's identity, rather than computing $\phi(n)$.

Generated Sequences in $\mathrm{Z}_{\mathbf{n}}^{\times}$

If all elements in $\mathbf{Z}_{\mathbf{n}}^{\times}$ can be obtained via $\mathbf{g}$ using:

$$\mathbf{g}^{\mathbf{x}} \ \mathbf{mod} \ \mathbf{n}$$

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

Then we state that:

$$\mathbf{g} \text{ is a generator for } \mathbf{Z}_{\mathbf{n}}^{\times}$$

$$\mathbf{Z}_{\mathbf{n}}^{\times} = [\mathbf{g}^{\mathbf{0}}, \mathbf{g}^{\mathbf{1}}, \mathbf{g2}\ , \mathbf{g3}\ , \cdot\cdot\cdot , \mathbf{g}^{\boldsymbol{\phi}(\mathbf{n})-\mathbf{1}}]$$

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

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

$$\boldsymbol{\phi}(\mathbf{n}) = \boldsymbol{\phi}(\mathbf{p})\boldsymbol{\phi}(\mathbf{q}) = (\mathbf{p} - \mathbf{1})(\mathbf{q} - \mathbf{1})$$

Note: the length of the sequence is maximal for $\mathbf{Z}_{\mathbf{p}}^{*}$

Example: Generated Sequences in $Z_n^{\times}$

Is g = 2 a generator for Z_7^* ?	Is g = 2 a generator for Z_5^* ?	Is g = 4 a generator for Z_5^* ?
$2^1 = 2 \bmod 7 = 2$	$2^1 = 2 \bmod 5 = 2$	$4^1 = 4 \bmod 5 = 4$
$2^2 = 4 \bmod 7 = 4$	$2^2 = 4 \bmod 5 = 4$	$4^2 = 16 \bmod 5 = 1$
$2^3 = 8 \bmod 7 = 1$	$2^3 = 8 \bmod 5 = 3$	$4^3 = 64 \bmod 5 = 4$
$2^4 = 16 \bmod 7 = 2$	$2^4 = 16 \bmod 5 = 1$	$4^4 = 256 \bmod 5 = 1$
$2^5 = 32 \bmod 7 = 4$	$2^5 = 32 \bmod 5 = 2$	$4^5 = 1024 \bmod 5 = 4$
$2^6 = 64 \bmod 7 = 1$	$2^6 = 64 \bmod 5 = 4$	$4^6 = 4096 \bmod 5 = 1$
$2^7 = 256 \bmod 7 = 2$	$2^7 = 256 \bmod 5 = 3$	$4^7 = 16384 \bmod 5 = 4$
$Z_7^* \neq$ [1, 2, 4] Nope	$Z_5^* =$ [1, 2, 3, 4] Yes!	$Z_5^* \neq$ [1, 4] Nope

Inverses in $\mathbf{Z_n^\times}$

Each element $\mathbf{a} \in \mathbf{Z_n^\times}$ has an inverse $\mathbf{a^{-1}}$ such that $\mathbf{a \times a^{-1} = 1 \bmod n}$.

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

Simple inversion algorithm

For $\mathbf{Z_p^*}$, where $\mathbf{p}$ is prime:

- $\mathbf{x^{-1} = x^{\phi(n)-1} = x^{(p-1)-1} = x^{p-2} \bmod p}$

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

- $\mathbf{x^{-1} = x^{\phi(n)-1} = x^{\phi(p)\phi(q)-1} = x^{(p-1)(q-1)-1} \bmod p}$

Example: inverses in $\mathrm{Z}_{\mathrm{n}}^{\times}$

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

We select **x = 11** out of $\mathbf{Z}_{21}^{*}$ and want to invert it.

$$\begin{aligned}\mathbf{x^{-1}} &= \mathbf{x^{(p-1)(q-1)-1} \bmod n} \\ &= \mathbf{x^{(6\times 2)-1} \bmod 21} \\ &= \mathbf{11^{11} \bmod 21} \\ &= \mathbf{2}\end{aligned}$$

Check that $\mathbf{x} \cdot \mathbf{x^{-1} \bmod n}$ **= 1**

$$\mathbf{11 \times 2 \bmod 21 = 22 \bmod 21 = 1}$$

What is a Group

It is a set **S** of elements or numbers that:

- may be finite or infinite
- Consist of some operation '**.**' so **G=(S,.)**

They have to Obeys CAIN:

- Closure: **a**,**b** in **S**, then **a.b** in **S**
- Associative: $(a.b).c = a.(b.c)$
- Identity **e**: $e.a = a.e = a$
- Inverse a^{-1}: $a.a^{-1} = e$

If it is also commutative, that is: $a.b = b.a$

Then the group forms an 'Abelian Group'

Cyclic Group

If we defined the exponentiation as repeated application of an operator

- Example: $\mathbf{a^3 = a.a.a}$

And let identity be: $\mathbf{e = a^0}$

A group is cyclic if every element is a power of some fixed element **a**

- i.e., $\mathbf{b = a^k}$ for some **a** and every **b** in group

Here **a** is said to be a **generator** of the group.

Ring

A set of numbers with two operations (addition and multiplication) which have the following properties:

- It forms an abelian group with addition and multiplication operation
- It has closure
- It is associative
- It is 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

It is a set of numbers with two operations which form:

- An abelian group for addition
- An abelian group for multiplication (ignoring 0)
- A ring

The relation can be stated as:

Group -> Ring -> Field