Number Theory Basics

19CSE311 Computer Security

Jevitha KP
Department of CSE

Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message or encrypted message
- **cipher** - algorithm for transforming plaintext to ciphertext
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to ciphertext
- **decipher (decrypt)** - recovering ciphertext from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (codebreaking)** - the study of principles/ methods of deciphering ciphertext *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Basic Terminology

- **algorithm** - Series of steps / mathematical formula / function which takes plain text as input and returns encrypted text / vice-versa.
- **cryptosystem -** Implementation of cryptographic techniques and accompanying infrastructure
- **Components of crypto system**
  - Plaintext
  - Encryption algorithm
  - Decryption algorithm
  - Cipher text
  - Keys - single (symmetric) or multiple (asymmetric)

Basic Terminology

- **Cryptography process**
  - **Sender** selects the algorithm, message and key
  - **Key** is shared with the receiver
  - **Key and message** are fed to the encryption algorithm
  - **Ciphertext** is sent over the public network to the receiver
  - **Receiver** uses the key and cipher text as input to the decryption algorithm and receives the plain text
  - Attacker - Since the cipher text is shared in public, the attackers will try to get the key

Math behind cryptography

- **Number Theory**
- Linear Algebra
- Algebraic structures

Integer Arithmetic

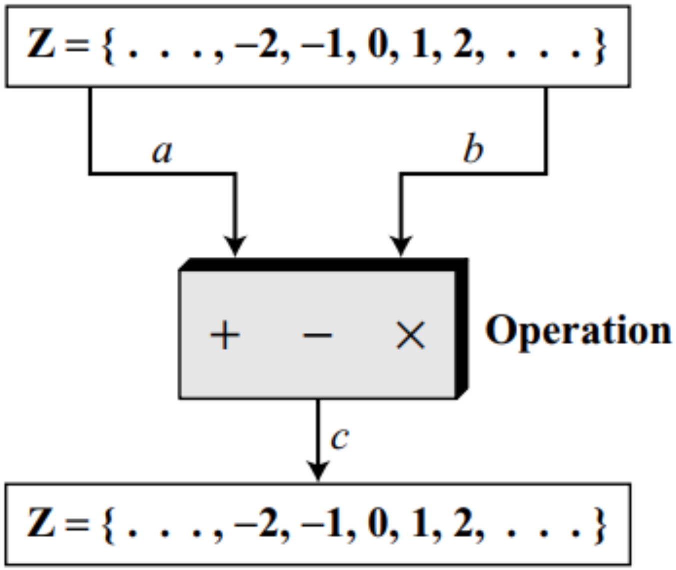
- In integer arithmetic, we use a set and a few operations.
- Set of Integers - The set of integers, denoted by Z, contains all integral numbers (with no fraction) from negative infinity to positive infinity

$$\boxed{\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}}$$

Binary Operations

- In cryptography, we are interested in three binary operations applied to the set of integers.
- A binary operation takes two inputs and creates one output.
- Three common binary operations defined for integers are **addition, subtraction, and multiplication**.
- Each of these operations takes two inputs (a and b) and creates one output (c)

Binary Operations



Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

Integer Division

» In integer arithmetic, if we divide a by n, we can get q and r.

» The relationship between these four integers can be shown as

» **$a = q \times n + r$**

» In this relation,

» a is called the dividend;

» q, the quotient;

» n, the divisor; and

» r, the

» remainder.

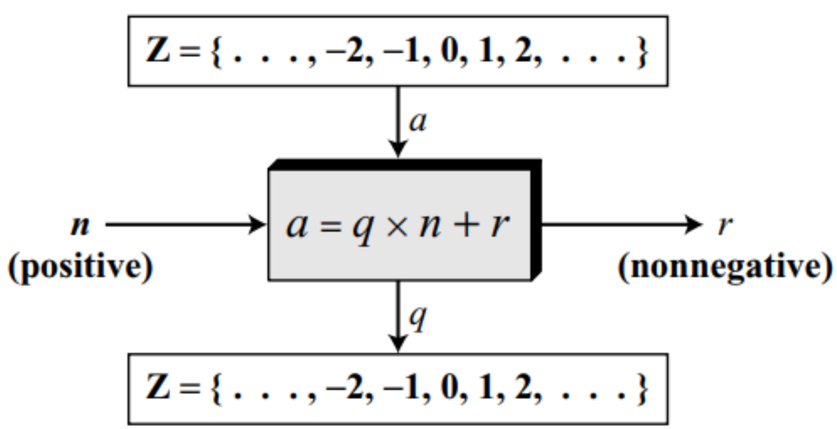
» Note that this is not an operation, because the result of dividing **a by n is two integers, q and r**.

» We call it **division relation**

Two Restrictions

» First, we require that the divisor be a positive integer (n > 0).

» Second, we require that the remainder be a nonnegative integer (r ≥ 0)



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

Properties of Divisibility

Property 1: if $a|1$, then $a = \pm 1$.
Property 2: if $a|b$ and $b|a$, then $a = \pm b$.
Property 3: if $a|b$ and $b|c$, then $a|c$.
Property 4: if $a|b$ and $a|c$, then $a|(m \times b + n \times c)$, where m and n are arbitrary integers.

Greatest Common Divisor (GCD)

- a common problem in number theory
- GCD (a,b) of a and b is the largest number that divides evenly into both a and b
  - eg GCD(60,24) = 12
- often want **no common factors** (except 1) and hence numbers are **relatively prime**
  - eg GCD(8,15) = 1
  - hence 8 & 15 are relatively prime

Euclid's GCD Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - `GCD(a,b) = GCD(b, a mod b)`
- **Euclid's Algorithm** to compute GCD(a,b):
  - `A=a, B=b`
  - `while B>0`
    - `R = A mod B`
    - `A = B, B = R`
  - `return A`

GCD(80808, 31863)

Q	N1	N2	R
2	80808	31863	17082
1	31863	17082	14781
1	17082	14781	2301
6	14781	2301	975
2	2301	975	351
2	975	351	273
1	351	273	78
3	273	78	39
2	78	**39**	0

GCD(42823, 6409)

Q	N1	N2	R
6	42823	6409	4369
1	6409	4369	2040
2	4369	2040	289
7	2040	289	17
17	289	17	0
	GCD = 17		

GCD(1160718174, 316258250)

Q	N1	N2	R
3	1160718174	316258250	211943424
1	316258250	211943424	104314826
2	211943424	104314826	3313772
31	104314826	3313772	1587894
2	3313772	1587894	137984
11	1587894	137984	70070
1	137984	70070	67914
1	70070	67914	2156
31	67914	2156	1078
2	2156	1078	0
	GCD = 1078		

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)