Cryptography and Network Security

Professor Dr. Rafiqul Islam

Number Theory Outline

- Basic Number theory
- Congruence
- Chinese Remainder Theorem
- Modular Exponentiation
- Fermat and Euler’s theorem
- Finite Fields

Basic Number Theory

- Division Algorithm

$$A = QN + R$$

$$11 = 1 \times 7 + 4$$

Q = quotient

R = Remainder

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
  - eg GCD(60,24) = 12
- define gcd(0, 0) = 0
- often want **no common factors** (except 1) define such numbers as **relatively prime**
  - eg 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)

Example GCD

To find $d =$ gcd $(a,b) =$ gcd $(1160718174, 316258250)$		
$a = q_1 b + r_1$	$1160718174 = 3 \times 316258250 + 211943424$	$d = \gcd(316258250, 211943424)$
$b = q_2 r_1 + r_2$	$316258250 = 1 \times 211943424 + 104314826$	$d = \gcd(211943424, 104314826)$
$r_1 = q_3 r_2 + r_3$	$211943424 = 2 \times 104314826 + 3313772$	$d = \gcd(104314826, 3313772)$
$r_2 = q_4 r_3 + r_4$	$104314826 = 31 \times 3313772 + 1587894$	$d = \gcd(3313772, 1587894)$
$r_3 = q_5 r_4 + r_5$	$3313772 = 2 \times 1587894 + 137984$	$d = \gcd(1587894, 137984)$
$r_4 = q_6 r_5 + r_6$	$1587894 = 11 \times 137984 + 70070$	$d = \gcd(137984, 70070)$
$r_5 = q_7 r_6 + r_7$	$137984 = 1 \times 70070 + 67914$	$d = \gcd(70070, 67914)$
$r_6 = q_8 r_7 + r_8$	$70070 = 1 \times 67914 + 2156$	$d = \gcd(67914, 2156)$
$r_7 = q_9 r_8 + r_9$	$67914 = 31 \times 2516 + 1078$	$d = \gcd(2156, 1078)$
$r_8 = q_{10} r_9 + r_{10}$	$2156 = 2 \times 1078 + 0$	$d = \gcd(1078, 0) = 1078$
Therefore, $d = \gcd(1160718174, 316258250) = 1078$		

Inverse Mod

26 = 1 * 23 + 3

23 = 7 * 3 + 2

3 = 1 * 2 + **1**

2 = 2 * 1 + 0.

Back-substitutions yield:

1 = 3 - 2

= 3 - (23 - 7*3)

= 8*3 - 23

= 8*(26-23) - 23

= 8*26 - 9*23

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
    - ie. 0 <= b <= n-1
  - process is known as **modulo reduction**
    - eg. -12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7

Modular Arithmetic

- *a* & *b* are **congruent** if: a mod n = b mod n
  - when divided by *n*, a & b have same remainder
  - eg. 100 mod 11 = 34 mod 11

    so 100 is congruent to 34 mod 11

Two integers *a* and *b* are said to be **congruent modulo** *n*, if $(a \bmod n) = (b \bmod n)$. This is written as $a \equiv b \pmod{n}$.[2]

$73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$

Modular Arithmetic

1. $a \equiv b \pmod{n}$ if $n|(a - b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

To demonstrate the first point, if $n|(a - b)$, then $(a - b) = kn$ for some k. So we can write $a = b + kn$. Therefore, $(a \bmod n)$ = (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = $(b \bmod n)$.

$23 \equiv 8 \pmod{5}$	because	$23 - 8 = 15 = 5 \times 3$
$-11 \equiv 5 \pmod{8}$	because	$-11 - 5 = -16 = 8 \times (-2)$
$81 \equiv 0 \pmod{27}$	because	$81 - 0 = 81 = 27 \times 3$

Modular Arithmetic Operations

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

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

- modular arithmetic is when do addition & multiplication and modulo reduce answer
- can do reduction at any point, ie
  - a+b mod n = [a mod n + b mod n] mod n

Modular Arithmetic Operations

1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
2. $[(a \bmod n) – (b \bmod n)] \bmod n = (a – b) \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

e.g.

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

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

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

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

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);
```

Euclidean Algorithm

Table 4.1 Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943434	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

Finite (Galois) Fields

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime p^n
- known as Galois fields
- denoted $GF(p^n)$
- in particular often use the fields:
  - $GF(p)$
  - $GF(2^n)$

Galois Fields GF(p)

- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field
  - since have multiplicative inverses
  - find inverse with Extended Euclidean algorithm
- hence arithmetic is "well-behaved" and can do addition, subtraction, multiplication, and division without leaving the field GF(p)

GF(7) Multiplication Example

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

Relatively Prime Numbers & GCD

- two numbers `a, b` are **relatively prime** if have **no common divisors** apart from 1
  - eg. 8 & 15 are relatively prime since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor
- conversely can determine the greatest common divisor by comparing their prime factorizations and using least powers
  - eg. $300=2^1 \times 3^1 \times 5^2$ $18=2^1 \times 3^2$ hence $GCD(18,300)=2^1 \times 3^1 \times 5^0=6$

Fermat's Theorem

- $a^{p-1} = 1 \pmod{p}$
  - where p is prime and $\gcd(a,p)=1$
- also known as Fermat's Little Theorem
- also have: $a^p = a \pmod{p}$
- useful in public key and primality testing

Fermat's Theorem

$$a = 7, p = 19$$
$$7^2 = 49 \equiv 11 \pmod{19}$$
$$7^4 \equiv 121 \equiv 7 \pmod{19}$$
$$7^8 \equiv 49 \equiv 11 \pmod{19}$$
$$7^{16} \equiv 121 \equiv 7 \pmod{19}$$
$$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$$

An alternative form of Fermat's theorem is also useful: If p is prime and a is a positive integer, then

$$a^p \equiv a \pmod{p} \tag{8.3}$$

Euler Totient Function $\varnothing(\mathtt{n})$

- when doing arithmetic modulo n
- **complete set of residues** is: `0..n-1`
- **reduced set of residues** is those numbers (residues) which are relatively prime to n
  - eg for n=10,
  - complete set of residues is {0,1,2,3,4,5,6,7,8,9}
  - reduced set of residues is {1,3,7,9}
- number of elements in reduced set of residues is called the **Euler Totient Function ø(n)**

Euler Totient Function $\varnothing(n)$

- to compute ø(n) need to count number of residues to be excluded
- in general need prime factorization, but
  - for p (p prime) $\varnothing(p)=p-1$
  - for p.q (p,q prime) $\varnothing(p.q)=(p-1)x(q-1)$
- eg.

$\varnothing(37) = 36$

$\varnothing(21) = (3-1)x(7-1) = 2x6 = 12$

Euler's Theorem

- a generalisation of Fermat's Theorem
- $a^{\varnothing(n)} = 1 \pmod{n}$
  - for any a,n where $\gcd(a,n)=1$
- eg.

  $a=3; n=10; \varnothing(10)=4;$

  hence $3^4 = 81 = 1 \bmod 10$

  $a=2; n=11; \varnothing(11)=10;$

  hence $2^{10} = 1024 = 1 \bmod 11$
- also have: $a^{\varnothing(n)+1} = a \pmod{n}$

Chinese Remainder Theorem

- used to speed up modulo computations
- if working modulo a product of numbers
  - eg. `mod M = ` $m_1 m_2 \ldots m_k$
- Chinese Remainder theorem lets us work in each moduli m_i separately
- since computational cost is proportional to size, this is faster than working in the full modulus M

Chinese Remainder Theorem

- can implement CRT in several ways
- to compute `A (mod M)`
  - first compute all $a_i = A \bmod m_i$ separately
  - determine constants c_i below, where $M_i = M/m_i$
  - then combine results to get answer using:

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) \pmod{M}$$

$$c_i = M_i \times \left(M_i^{-1} \bmod m_i\right) \quad \text{for } 1 \leq i \leq k$$

Chinese Remainder Theorem

- Let p and q be co-prime. Then the system of equations:

$$x = a \pmod{p}$$

$$x = b \pmod{q}$$

- Has a unique solution for **x (modulo pq)**

Chinese Remainder Theorem

Problem: Find x

$$x = 2\ (mod\ 3)$$

$$x = 3\ \left(mod\ 5\right)$$

$$x = 2\ (mod\ 7)$$

Solution:

M =

$$3 \times 5 \times 7 = 105;\ M1 = \frac{105}{3} = 35;\ M2 = \frac{105}{5} = 21;\ M3 = \frac{105}{7} = 15;$$

Chinese Remainder Theorem

- $M1^{-1}\ (mod\ 3) = 35^{-1}(mod\ 3) = 35^{3-2}(mod\ 3) = 2$
- $M2^{-1}\ \left(mod\ 5\right) = 21^{-1}\left(mod\ 5\right) = 21^{5-3}\left(mod\ 5\right) = 1$
- $M3^{-1}\ (mod\ 7) = 15^{-1}(mod\ 7) = 15^{7-2}(mod\ 7) = 1$
- $x = \left[2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1\right]\left(mod\ 105\right) = 233\ \left(mod\ 105\right) = 23$