Chapter 7. Introduction to Number Theory

- 7.1 Prime and Relatively Prime Numbers
- 7.2 Modular Arithmetic
- 7.3 Fermat's and Euler's Theorems
- 7.4 Testing for Primality
- 7.5 Euclid's Algorithm
- 7.6 The Chinese Remainder Theorem
- 7.7 Discrete Logarithms

7.1 Prime and Relatively Prime (1)

- 1. Divisors
  - $b \mid a$: $b\,(\neq 0)$ divides a i.e. $a = mb$ for some m.
  - b is <u>divisor</u> of a.
  - Properties
    - ✓ $a \mid 1$ $a =$ 1
    - ✓ $a \mid b$ and $b \mid a$ $a =$ b
    - ✓ Any $b\,($ $0) \mid 0$
    - ✓ $b \mid g$ and $b \mid h$ $b \mid (mg + nh)$ for arbitrary m and n.

7.1 Prime and Relatively Prime (2)

- 2. Prime Numbers
  - p is prime number if its only divisors are ± 1 and $\pm p$.
  - a can be factored in a unique way

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

where p_i : distinct prime, $\alpha_i > 0$.

7.1 Prime and Relatively Prime (3)

- 3. Relatively Prime Numbers
  - Greatest Common Divisor
    - ✓ $c = \gcd(a, b)$ if $c \mid a$, $c \mid b$ and
      $d \mid a$, $d \mid b$ $d \mid c$.
    - ✓ $\gcd(a, b) = \gcd(|a|, |b|)$
  - a and b are relatively prime if $\gcd(a, b) = 1$.

7.2 Modular Arithmetic (1)

- 1. Remainder
  - Any integer *a* satisfy the following relationship
  - Quotient $a = qn + r$
  - Remainder $q = \lfloor a/n \rfloor$
  - The remainder *r* is often referred to as a <u>residue</u>. $0 \le r < n$
  - Examples

    $11 = 1 \times 7 + 4 \Rightarrow r = 4,\quad 11 \bmod 7 = 4$

    $-11 = (-2) \times 7 + 3 \Rightarrow r = 3,\quad -11 \bmod 7 = 3$

7.2 Modular Arithmetic (2)

- 2. Congruent modulo *n*
  - $a \equiv b \bmod n$ if $n \mid (a - b)$
  - $(a \bmod n) = (b \bmod n) \Leftrightarrow a \quad b \bmod n$
  - $a \quad b \bmod n \Leftrightarrow b \quad a \bmod n$
  - $a \quad b \bmod n$ and $b \quad c \bmod n \quad\quad a \quad c \bmod n$
  - Examples

    73 4 mod 23

    21 -9 mod 10

7.2 Modular Arithmetic (3)

- 3. Modular arithmetic operations
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
  - $(a + b) \equiv (a + c) \bmod n \Rightarrow b \equiv c \bmod n$
  - $(a \times b) \equiv (a \times c) \bmod n \Rightarrow b \equiv c \bmod n$

    if $\gcd(a, n) = 1$

7.2 Modular Arithmetic (4)

- Examples
  - ✓ [(11 mod 8) + (15 mod 8)] mod 8 = 2 = (11 + 15) mod n
  - ✓ [(11 mod 8) - (15 mod 8)] mod 8 = 4 = (11 - 15) mod n
  - ✓ [(11 mod 8) (15 mod 8)] mod 8 = 5 = (11 15) mod n
  - ✓ (5 + 23) (5 + 7) mod 8 23 7 mod 8
  - ✓ (5 23) (5 7) mod 8 23 7 mod 8 gcd(5, 8) = 1
  - ✓ (6 3) (6 7) mod 8 3 7 mod 8 gcd(6, 8) = 2

	0	1	2	3	4	5	6	7
5i mod 8	0	6	4	2	0	6	4	2
6i mod 8	0	5	2	7	4	1	6	3

7.2 Modular Arithmetic (5)

- Additive inverse
  - ✓ $(z + w) \equiv 0 \bmod n \Rightarrow z\ (= -w)$ is the additive inverse of w.
  - ✓ Addition Modulo 7

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

7.2 Modular Arithmetic (6)

- Multiplicative inverse
  - ✓ $(z \quad w) \equiv 0 \bmod n \quad z\ (= w^{-1})$ is the multiplicative inverse of w.
  - ✓ Multiplicative Modulo 7 (gcd(w,n)=1)

	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

7.3 Fermat's and Euler's Theorems (1)

- 1. Fermat's Theorem

  $a^{p-1} \equiv 1 \bmod p$

  where p is prime and a is a positive integer.

  - Example

    $7^2 \equiv 49 \equiv 11 \bmod 19$

    $7^4 \equiv 11^2 \equiv 121 \equiv 7 \bmod 19$

    $7^8 \equiv 7^2 \equiv 11 \bmod 19$

    $7^{16} \equiv 11^2 \equiv 7 \bmod 19$

    $7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \bmod 19$

7.3 Fermat's and Euler's Theorems (2)

- 2. Euler's Totient Function
  - $\phi(n)$: the number of positive integers less than n and relatively prime to n.

    $\phi(n) = \prod^{m} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$

    where $n = \prod^{m} p_i^{\alpha_i}$, p_i is prime and α_i is a positive integer.

7.3 Fermat's and Euler's Theorems (3)

- Examples

  ✓ $\phi(7) = 7 - 1 = 6$

  Above 6 integers are {1, 2, 3, 4, 5, 6}.

  ✓ $f(21) = f(3 \times 7)$

  $= (3-1)(7-1)$

  $= 12$

  Above 12 integers are {1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}.

7.3 Fermat's and Euler's Theorems (4)

❑ 3. Euler's Theorem

$$a^{\phi(n)} \equiv 1 \bmod n$$

where gcd(a, n) = 1.

- A useful alternative form

$^{\phi(n)+1}$,

where gcd(a, n) = 1 and gcd(a, n)≠1.

7.4 Testing for Primality (1)

- 1. Miller-Rabin Test
  - By Fermat's theorem,

$$
\begin{aligned}
0 &\equiv a^{n-1} - 1 \\
&\equiv a^{m2^k} - 1 \qquad \text{where } m \text{ is odd.} \\
&\equiv (a^{m2^{k-1}} + 1)(a^{m2^{k-1}} - 1) \\
&\equiv (a^{m2^{k-1}} + 1)(a^{m2^{k-2}} + 1)(a^{m2^{k-2}} - 1) \\
&\equiv (a^{m2^{k-1}} + 1)(a^{m2^{k-2}} + 1)\cdots(a^m + 1)(a^m - 1) \qquad (1)
\end{aligned}
$$

7.4 Testing for Primality (2)

- If n is prime, a satisfies (1).
- If a satisfies (1), n is pseudoprime.

- If n is an odd composite integer, then at most 1/4 of all the number a, $1 \le a \le n-1$, satisfy (1).
- If (1) is performed s times, the probability that n is prime is at least $1-(1/4)^s$.
- Usually, $s = 50$.

7.4 Testing for Primality (3)

- Algorithm

MillerRabin(a, n)

1. write n-1 = $m2^k$, where m is odd.
2. choose a random integer a, 1 $\leq a$ $\leq n$-1
3. compute $b = a^m \bmod n$
4. if $b \equiv 1 \pmod{n}$ then

    answer "n is pseudoprime" and quit

5. for i = 0 to k-1 do
6. if $b \equiv -1 \pmod{n}$ then

    answer "n is pseudoprime" and quit

    else

    b=b^2 mod n

7. answer "n is composite"

7.5 Euclid's Algorithm (1)

1. Euclid's Algorithm

- Finding the Greatest Common Divisor

$$a = qb + r \qquad 0 \leq r < b$$

$$\gcd(a,b) \mid a \;\&\; \gcd(a,b) \mid b \Rightarrow \gcd(a,b) \mid r$$

$$\therefore \gcd(a,b) = \gcd(b,r)$$

- More generally

$$\begin{array}{lll}
r_0 = q_1 r_1 + r_2 & 0 < r_2 < r_1 & \gcd(r_0, r_1) \\
r_1 = q_2 r_2 + r_3 & 0 < r_3 < r_2 & = \gcd(r_1, r_2) \\
\vdots & \vdots & \vdots \\
r_{m-2} = q_{m-1} r_{m-1} + r_m & 0 < r_m < r_{m-1} & = \gcd(r_{m-1}, r_m) \\
r_{m-1} = q_m r_m & & = r_m
\end{array}$$

7.5 Euclid's Algorithm (2)

- Algorithm

  Euclid(d, f)

  1. X $\leftarrow f$; Y $\leftarrow d$
  2. if Y = 0 return X = gcd(d, f)
  3. R = X mod Y
  4. X $\leftarrow$ Y
  5. Y $\leftarrow$ R
  6. goto 2

- Examples

  gcd(55,22) = gcd(22, 11) = 11

  gcd(11,10) = gcd(10, 1) = 1

7.5 Euclid's Algorithm (3)

- 2. Extended Euclid's Algorithm
  - Finding the Muliplicative Inverse
    - ✓ Applying Euclid's algorithm to X3 and Y3 holding with

      fT1 + dT2 = T3 fX1 + dX2 = X3 fY1 + dY2 = Y3.

    - ✓ If gcd(d, f) = 1,Y3 of the final step is 0 and Y3 of the preceding step is 1.

    - ✓ Therefore,

      fY1 + dY2 = 1 $\Rightarrow$ dY2 $\equiv$ 1 mod f

      Y2 is the multiplicative inverse of d, modulo f.

7.5 Euclid's Algorithm (4)

- Algorithm

  ExtendedEuclid(d, f)

  1. (X1, X2, X3) ←(1, 0, f); (Y1, Y2, Y3)←(0, 1, d)
  2. if Y3 = 0 return X3 = gcd(d, f); no inverse
  3. if Y3 = 1 return Y3 = gcd(d, f); Y2 = d^{-1} mod f
  4. Q = $\lfloor X3/Y3 \rfloor$
  5. (T1, T2, T3) ←(X1-QY1, X2-QY2, X3-QY3)
  6. (X1, X2, X3)← (Y1, Y2, Y3)
  7. (Y1, Y2, Y3)← (T1, T2, T3)
  8. goto 2

7.5 Euclid's Algorithm (5)

- Example : 550^{-1} mod 1769 = 550

Q	X1	X2	X3	Y1	Y2	Y3
-	1	0	1769	0	1	550
3	0	1	550	1	-3	119
4	1	-3	119	-4	13	74
1	-4	13	74	5	-16	45
1	5	-16	45	-9	29	29
1	-9	29	29	14	-45	16
1	14	-45	16	-23	74	13
1	-23	74	13	37	-119	3
4	37	-119	3	-171	550	1

7.6 The Chinese Remainder Theorem (1)

- 1. CRT
  - $M = \prod_{i=1}^{k} m_i$ where m_i are pairwise relatively prime.

    $A \in Z_M \Rightarrow A \leftrightarrow (a_1, a_2, \cdots, a_k)$ where $a_i = A \bmod m_i$.
  - $Z_M \xleftrightarrow{1-to-1} Z_{m_1} \times Z_{m_2} \times \cdots \times Z_{m_k} \qquad 1 \le i \le k$
    - ✓ $A \rightarrow (a_1, a_2, \cdots, a_k)$ is obviously unique.

7.6 The Chinese Remainder Theorem (2)

✓ $(a_1, a_2, \cdots, a_k) \rightarrow A$

$M_i = M / m_i \qquad for\ 1 \le i \le k$

$c_i = M_i \times (M_i^{-1} \bmod m_i)$

$A = (\sum_{i=1}^{k} a_i c_i) \bmod M$

$\Rightarrow$satisfy $a_i = A \bmod m_i$, because $c_i \bmod m_i = 1$.

- Operations of Z_M $\xleftrightarrow{equivalent}$ Operations of $Z_1 \times Z_2 \times \cdots \times Z_k$

7.6 The Chinese Remainder Theorem (3)

- Example
  - ✓ 1813 = 37 × 49

973 mod 1813	(973 mod 37, 973 mod 49)
	= (11 mod 37, 42 mod 49)
+	+
678 mod 1813	(678 mod 37, 678 mod 49)
	= (12 mod 37, 41 mod 49)
⇓	⇓
(973 + 678) mod 1813	(11 + 12 mod 37, 42 + 41 mod 49)
= 1651 mod 1813	= (23 mod 37, 34 mod 49)

$$A = a_1 M_1 (M_1^{-1} \bmod m_1) + a_2 M_2 (M_2^{-1} \bmod m_2)$$
$$= [(23)(49)(34) + (34)(37)(4)] \bmod 1813 = 1651$$

7.7 Discrete Logarithms (1)

- 1. The order of a (mod n)
  - The least positive exponent m satisfying equation

$$a^m \equiv 1 \bmod n \quad .$$

- 2. A primitive root of n
  - If $m = \phi(n)$, a is a primitive root of n.

7.7 Discrete Logarithms (2)

❑3. Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}	order	pri.
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	13	1	18	*
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1	18	*
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1	9	
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1	9	
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1	9	
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	3	
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1	6	
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1	9	
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1	18	*
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	3	
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1	6	
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1	18	*
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1	18	*
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1	18	*
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1	9	
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1	9	
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	2	