Introduction to Information Security

Lecture 5: Number Theory

2007. 6.

Prof. Byoungcheon Lee
sultan (at) joongbu . ac . kr

Information and Communications University

Contents

Divisibility

- Let Z denote the set of all integers. $Z=\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$
- Division Theorem ($a,b \in Z$)
  - For nonzero b, $\exists\ q,r \in Z$ s.t. $a=qb+r$, $0 \leq r < b$
  - q: quotient, r: remainder
- Divide
  - b divides a, or $b|a$ iff $\exists\ c \in Z$ s.t. $a=bc$ (i.e. $r=0$)
  - If $a|b$, then $a|bc$
  - If $a|b$ and $a|c$, then $a|(bx+cy)$
  - If $a|b$ and $b|a$ then $a=\pm b$ (antisymmetry)
  - If $a|b$ and $b|c$, then $a|c$ (transitivity)

$$b|a$$

b divides *a*

Prime Numbers

- Prime
  - An integer p is called prime if its divisors are ± 1 and $\pm p$
  - A number that is divisible only by 1 and itself
  - 2,3,5,7,11,13,17,19,23,29,31,…..
  - If a prime p divides ab, then $p|a$ or $p|b$

- Composite number
  - Any number that is not prime

Prime Number Theorem

❖ There are infinitely many prime numbers

❖ Prime number theorem

$$\pi(x) \approx \frac{x}{\ln x} : \text{number of primes less than } x$$

$$\lim_{n\to\infty} \frac{\pi(x)\ln(x)}{x} = 1$$

❖ Example: Estimate the number of 100-digit primes

$$\pi(10^{100}) - \pi(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9\times 10^{97}$$

Sieve of Eratosthenes

❖ **Sieve of Eratosthenes** : Determine all primes smaller than N

S1. Create an initial set of all numbers $N_N=\{2,3,4,\ldots,N\text{-}1\}$

S2. For all integers $n < sqrt(N)$, remove all multiples of n from the above N_N

S3. The final reduced set N_N contains all primes smaller than N

❖ **Exercise 1: Obtain all primes less than 200**

Factorization

- Factorization
  - Any positive integer can be uniquely factored into the product of primes

$$n = \prod_{p \in P} p^{e_P}$$

  - $504 = 2^3 3^2 7$, $1125 = 3^2 5^3$

lcm and gcd

- *lcm(a,b)* - least common multiple
  - lcm of *a* and *b* is the smallest integer which is divisible by both *a* and *b*

- *gcd(a,b)* - greatest common divisor
  - gcd of *a* and *b* is the largest integer which divides both *a* and *b*
  - Example: gcd(24,60)=12, gcd(5,7)=1
  - *a* and *b* are relatively prime if *gcd(a,b)=1*

- Finding *gcd(a,b)*
  - Using the factorization of *a* and *b*

    $576=2^6 3^2$, $135=3^3 5$, $gcd(576,135)=3^2$
  - Using the Euclidean algorithm

Euclidean Algorithm - find gcd using division and remainder

- Find $gcd(a,b)$
  - Initialize $r_0=a$, $r_1=b$
  - Computes the following sequence of equations

$$r_0=q_1r_1+r_2$$
$$r_1=q_2r_2+r_3$$
$$r_2=q_3r_3+r_4$$
$$\ldots\ldots$$
$$r_{n-2}=q_{n-1}r_{n-1}+r_n \quad \text{where } r_n=0$$

  - Then $gcd(a,b) = r_{n-1}$

$$r_0 = a = (?)\times r_{n-1}$$
$$r_1 = b = (??)\times r_{n-1}$$

Euclidean Algorithm - find gcd using division and remainder

❖Example : *gcd(3465,882)=63*

$3465 = 3 \times 882 + 819$

$882 = 1 \times 819 + 63$

$819 = 13 \times 63 + 0$

3	3465	882	1
	2646		
13	819	819	
	819	63	
	0		

Extended Euclidean Algorithm

- Extended Euclidean Algorithm
  - *Let d=gcd(a,b). Then there exist integers x, y such that* **ax+by=d**.
  - *If a and b are relatively prime, then there exist x, y such that ax+by=1*

$$a = q_1 b + r_2 \qquad\qquad r_2 = a - q_1 b$$

$$b = q_2 r_2 + r_3 \qquad\qquad r_3 = b - q_2 r_2 = -q_2 a + (1 + q_1 q_2) b$$

$$r_2 = q_3 r_3 + r_4 \quad \longrightarrow \quad r_4 = r_2 - q_3 r_3 = (?)a + (??)b$$

$$\cdots \qquad\qquad \cdots$$

$$r_{n-2} = q_{n-1} r_{n-1} \qquad\qquad r_{n-1} = (?)a + (??)b \longrightarrow ax+by=d$$

Example

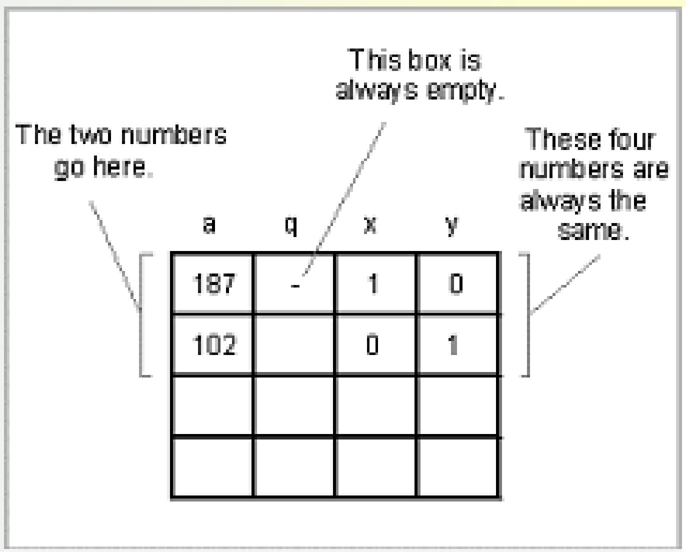
gcd(10,7) = 1 ⟶ 1 = (-2)(10) + (3)(7).

gcd(367,221) = 1 ⟶ 1 = (-56)(367) + (93)(221)

Extended Euclidean Algorithm

- Easier calculation algorithm by hand
  - http://marauder.millersville.edu/~bikenaga/absalg/exteuc/exteucex.html

- Example: for gcd(187,102) = 17



a	q	x	y
187	-	1	0
102	1	0	1
85	1	1	-1
17	5	-1	2

(next x) = (next-to-last x) - q (last x)
(next y) = (next-to-last y) - q (last y)

17 = (187,102) = (-1)(187) + (2)(102).

Extended Euclidean Algorithm

- Exercise 2: For the following pair of numbers

  1. Find gcd using Euclidean algorithm

  2. Solve $ax+by=d$ using Extended Euclidean algorithm

  1. *gcd(55,123)*
  2. *gcd(41,789)*
  3. *gcd(352,124)*
  4. *gcd(1124,368)*
  5. *gcd(2733,725)*

Congruence

- Definition) Congruence

  $a \equiv b \bmod n$ iff $n|(a-b)$

  $a = b+kn$ for some integer k

  $a\%n=b\%n$

  a is congruent to b modulo n

  $32 \equiv 2 \bmod 5$

  $-12 \equiv 37 \bmod 7$

  $a \equiv a$

  $a \equiv b$ iff $b \equiv a$

  If $a \equiv b$ and $b \equiv c$ then $a \equiv c$

- Residue Class Group: $Z_n=\{x \in Z \mid 0 \leq x < n\}$

  Addition: $a+b = (a+b \bmod n)$

  Multiplication: $ab = (ab \bmod n)$

  Closed under addition, subtraction, and multiplication

  Closed under division if n is prime

Modular Arithmetic

- Modular addition
- Modular subtraction

- Modular multiplication
  - Fill out the table

b

a

x	1	2	3	4	5	6	7	8	9	10
1	1	2								
2	2	4								
3			9	1	4	7				
4										
5										
6										
7										
8										
9										
10										

Modular multiplication in mod 11
Compute axb mod 11

Modular Arithmetic

- ❖ Modular exponentiation
  - ❖Fill out the table

b

a

^	1	2	3	4	5	6	7	8	9	10
1										
2										
3	3	9	5	4	1	3	9	5	4	1
4										
5										
6										
7										
8										
9										
10										

Modular exponentiation in mod 11
Compute $a^b \bmod 11$

Modular Arithmetic

b

a

a^b	1	2	3	4	5	6	7	8	9	10	11	12
1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1
3	3	9	1	3	9	1	3	9	1	3	9	1
4	4	3	12	9	10	1	4	3	12	9	10	1
5	5	12	8	1	5	12	8	1	5	12	8	1
6	6	10	8	9	2	12	7	3	5	4	11	1
7	7	10	5	9	11	12	6	3	8	4	2	1
8	8	12	5	1	8	12	5	1	8	12	5	1
9	9	3	1	9	3	1	9	3	1	9	3	1
10	10	9	12	3	4	1	10	9	12	3	4	1
11	11	4	5	3	7	12	2	9	8	10	6	1
12	12	1	12	1	12	1	12	1	12	1	12	1

Modular exponentiation in mod 13

Compute a^b *mod 13*

Modular Arithmetic

- ❖ Modular division
  - ❖ Solve: 2x+7=3 (mod 17) → 2x=-4 (mod 17) → x=-2 (mod 17)=15
- ❖ You can divide by a mod n only when gcd(a,n)=1
  - ❖ Find the multiplicative inverse of a mod n = a^{-1} and then multiply a^{-1}
  - ❖ b/a mod n = b*a^{-1} mod n
  - ❖ If ac=1 mod n, then c=a^{-1} mod n
  - ❖ Compute a^{-1} mod n using the extended Euclidean algorithm
  - ❖ For gcd(n,a)=1, solve ax+ny=1, then x=a^{-1} mod n

Efficient Modular Exponentiation

- How to compute $a^x \ (mod\ n)$ efficiently?
  - Multiply a x times? No good

2^{1234} mod 789 = $2^{1024+128+64+16+2}$ mod 789

= $2^{1024} * 2^{128} * 2^{64} * 2^{16} * 2^{2}$ mod 789

= 286 * 559 * 367 * 49 * 4 mod 789

= 481 mod 789

Square and Multiply Algorithm

❖ How to compute $y=a^x \pmod{n}$ efficiently?

1. binary representation of $x=x_r x_{r-1} \ldots x_1 x_0$
2. Let y=a
3. For i from r-1 to 0

   $y=y^2 \bmod n$

   If $x_i=1$, then $y=ya \bmod n$
4. Output y

Compute $7^{21} \bmod 11$, $21=10101_{(2)}$, r=4

i	bit	y^2	y*a	y
4	1			7
3	0	$7^2=5$	-	5
2	1	$5^2=3$	3*7=10	10
1	0	$10^2=1$	-	1
0	1	$1^2=1$	1*7=7	7

→ Output 7 as the result

$7^{21} \bmod 11$
$= 7^{16+4+1} \bmod 11$
$= (((7^2)^2 7)^2)^2 7 \bmod 11$

Chinese Remainder Theorem (CRT)

❖ Chinese Remainder Theorem

Suppose gcd(m,n)=1. Given integers a and b, there exists exactly one solution x (mod mn) to the simultaneous congruences

$x=a$ mod m, $x=b$ mod n

proof)

- ❖there exists s, t such that $ms+nt=1$
- ❖$ms=1 \bmod n$, $nt=1 \bmod m$
- ❖Let $x=ant+bms$, then
  - ❖$x=ant \bmod m=a \bmod m$
  - ❖$x=bms \bmod n=b \bmod n$

Chinese Remainder Theorem (CRT)

Find a number x which satisfies

$x=b_1 \bmod m_1$

$\cdots\cdots$

$x=b_n \bmod m_n$

Example: Find x such that

$x=4 \bmod 5$

$x=3 \bmod 7$

$x=6 \bmod 11$

❖ Efficient algorithm to compute x

1. $m=m_1m_2\ldots m_n = 5*7*11 = 385$
2. $M_1 = m/m_1 = 385/5 = 7*11 = 77$

   $M_2 = m/m_2 = 385/7 = 5*11 = 55$

   $M_3 = m/m_3 = 385/11 = 5*7 = 35$
3. $N_1=M_1^{-1} \bmod m_1=77^{-1} \bmod 5=3$ ← Use extended Euclidean algorithm

   $N_2=M_2^{-1} \bmod m_2=55^{-1} \bmod 7=6$

   $N_3=M_3^{-1} \bmod m_3=35^{-1} \bmod 11=6$
4. $T=b_1M_1N_1+b_2M_2N_2+b_3M_3N_3 \bmod m$

   $=4*77*3+3*55*6+6*35*6 \bmod 385=94$

Chinese Remainder Theorem (CRT)

❖ Exercise 3: find a number which satisfies

1. $x = 3 \bmod 11 = 6 \bmod 7 = 8 \bmod 13$

2. $x = 5 \bmod 31 = 6 \bmod 17 = 8 \bmod 29$

Euler phi function: $\phi(n)$

- Euler phi function (or Euler totient function): $\phi(n)$
  - The number of integers in [1, n], which are relatively prime to n
  - If p is prime, $\phi(p) = p-1$
  - $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$ for prime $p > 2$
  - if $\gcd(n, m) = 1$, $\phi(nm) = \phi(n) . \phi(m)$ (multiplicative property)
  - So, for primes p & q, $\phi(pq) = \phi(p) . \phi(q) = (p-1)(q-1)$

Fermat's Theorem and Euler's Theorem

- Fermat's Theorem: Let p be a prime
  - If $\gcd(x, p) = 1$, then $x^{p-1} = 1 \bmod p$
  - If $a = b \bmod p-1$, then $x^a = x^b \bmod p$ for all integers x
  - $x^p = x \bmod p$ for all integers x

- Euler's Theorem: Let n be an integer
  - If $\gcd(x, n) = 1$, then $x^{\phi(n)} = 1 \bmod n$
  - If n is a product of distinct primes and $a = b \bmod \phi(n)$, then $x^a = x^b \bmod n$ for all integers x
  - $x^n = x \bmod n$ for all integers x

Legendre Symbol

❖ Quadratic congruence for a prime modulus p

$x^2 = a \pmod{p}$ where p is a prime

It will have

1. one solution if a=0 (mod p)
2. two solutions if a is a quadratic residue modulo p
3. no solution if a is a quadratic non-residue modulo p

❖ Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{If a = 0} \\ 1 & \text{If a is a QR} \\ -1 & \text{If a is a QNR} \end{cases}$$

It is computed by

$$\left(\frac{a}{p}\right) = a^{\frac{1}{2}(p-1)} \bmod p$$

Quadratic Residue

❖ **Example in Z_{13}***

$1^2 \equiv 1$	mod 13	$7^2 \equiv 10$	mod 13
$2^2 \equiv 4$	mod 13	$8^2 \equiv 12$	mod 13
$3^2 \equiv 9$	mod 13	$9^2 \equiv 3$	mod 13
$4^2 \equiv 3$	mod 13	$10^2 \equiv 9$	mod 13
$5^2 \equiv 12$	mod 13	$11^2 \equiv 4$	mod 13
$6^2 \equiv 10$	mod 13	$12^2 \equiv 1$	mod 13

❖ QR = {1, 3, 4, 9, 10, 12}

$$\left(\frac{3}{13}\right) = 3^{\frac{1}{2}(13-1)} \bmod 13 = 3^6 \bmod 13 = 1$$

❖ QNR={2, 5, 6, 7, 8, 11}

$$\left(\frac{2}{13}\right) = 2^{\frac{1}{2}(13-1)} \bmod 13 = 2^6 \bmod 13 = -1$$

Jacobi Symbol

- ❖ **Generalization of Legendre symbol**
- ❖ **Quadratic congruence for an arbitrary modulus n**

  $x^2 = a \pmod{n}$ where $n=p_1 \ldots p_r$

It is computed by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

Group

Definition) A group $(G,*)$ consists of a set G with a binary operation * on G satisfying the following three axioms.

1. $a*(b*c)=(a*b)*c$ for all $a,b,c \in G$: associative
2. There is an element $1 \in G$ called the identity element s.t. $a*1=1*a=a$
3. For each $a \in G$ there exists an element a^{-1} (inverse) s.t. $a*a^{-1}=a^{-1}*a=1$

A group G is abelian (or commutative) if, furthermore,

4. $a*b=b*a$ for all $a,b \in G$

Ring

Definition) A ring (R,+,x) consists of a set R with two binary operations arbitrarily denoted + (addition) and x (multiplication) on R satisfying the following axioms.

1. **(R,+) is an abelian group with identity denoted 0.**
2. **The operation x is associative. That is ax(bxc)=(axb)xc for all a,b,c $\in$ R.**
3. **There is a multiplicative identity denoted 1, s.t. 1xa=ax1=a for all a $\in$ R.**
4. **The operation x is distributive over +. ax(b+c)=(axb)+(axc) for all a,b,c $\in$ R.**

The ring R is a commutative ring if axb=bxa for all a,b $\in$ R.

Field and Finite Field

Definition) A field is a commutative ring in which all non-zero elements have multiplicative inverses.

Definition) A finite field (Galois Field) is a field F which contains a finite number of elements.

Galois Field $GF(p)=Z_p$ with prime p

addition, subtraction, multiplication, and division by non-zero elements are all well-defined.

arithmetic modulo p.

Galois Field $GF(q^n)$ with prime q and degree n

arithmetic modulo irreducible polynomials of degree n whose coefficients are integers modulo q.

Order of Group

- Order of group in modular arithmetic
  - $x = y \bmod n$: x is congruent to y modulo n; n divides (x-y)
  - $Z_n = \{0, 1, 2, . . ., n-1\}$
  - $Z_n^* = \{ x \in Z_n \mid \gcd(x, n) = 1\}$: multiplicative group of Z_n
  - Order of Z_n^* = the number of elements in $Z_n^* = | Z_n^* | = \phi(n)$
  - Order of $x \in Z_n^*$ = smallest integer r such that $x^r = 1 \bmod n$
  - Ord(x) for any $x \in Z_n^*$ = a divisor of $\phi(n)$

Cyclic Group

- Let p be a prime
  - $Z_p = \{0, 1, 2, \ldots, p-1\}$
  - $Z_p^* = \{ x \in Z_p \mid \gcd(x, p) = 1\} = \{1, 2, \ldots, p-1\} = Z_p - \{0\}$
  - Order of $Z_p = | Z_p^* | = \phi(p) = p-1$
  - Order of an element $\alpha \in Z_p^* = \mathrm{Ord}(\alpha)$ = a divisor of p-1
  - α is a generator / primitive element of Z_p^* if $\mathrm{Ord}(\alpha) = \phi(p) = p-1$
    - ✓ Then $Z_p^* = \{\alpha^i \mid i = 0, 1, \ldots, p-2\}$: cyclic group
    - ✓ For any $y \in Z_p^*$, there exists an integer $x \in [0, p-2]$ such that $y = \alpha^x \bmod p$
- Let p be a prime and q be a prime divisor of p-1, I.e., p-1= kq
  - Let g be an element of order q, I.e., $g \neq 1$and $g^q = 1 \bmod p$
  - $\langle g \rangle = \{g^i \mid i = 0, 1, \ldots, q-1\} \subset Z_p^*$: a multiplicative subgroup of Z_p^*
  - That is, for any $y \in \langle g \rangle$, there exists an integer $x \in [0, q-1]$ such that $y = g^x \bmod p$

Cyclic Group

- Example: $p = 13$
  - $Z_{13} = \{0, 1, 2, \ldots, 12\}$
  - $Z_{13}^* = \{1, 2, \ldots, 12\}$; $| Z_p^* | = 12$
  - $\alpha = 6$: a generator of Z_{13}^*

i	0	1	2	3	4	5	6	7	8	9	10	11
α^i mod 13	1	6	10	8	9	2	12	7	3	5	4	11

  - Order of $x \in Z_{13}^*$: a divisor of 12 = 2.2.3

x	1	2	3	4	5	6	7	8	9	10	11	12
Ord(x)	1	12	3	6	4	12	12	4	3	6	12	2

- **Exercise 4. Find the order of $x \in Z_{31}^*$**

Z_{13}^*

b

a

a^b	1	2	3	4	5	6	7	8	9	10	11	12	Ord(a)
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	3	6	12	11	9	5	10	7	1	12
3	3	9	1	3	9	1	3	9	1	3	9	1	3
4	4	3	12	9	10	1	4	3	12	9	10	1	6
5	5	12	8	1	5	12	8	1	5	12	8	1	4
6	6	10	8	9	2	12	7	3	5	4	11	1	12
7	7	10	5	9	11	12	6	3	8	4	2	1	12
8	8	12	5	1	8	12	5	1	8	12	5	1	4
9	9	3	1	9	3	1	9	3	1	9	3	1	3
10	10	9	12	3	4	1	10	9	12	3	4	1	6
11	11	4	5	3	7	12	2	9	8	10	6	1	12
12	12	1	12	1	12	1	12	1	12	1	12	1	2

Homework #5

Solve the exercises appeared in this lecture.

1. **Exercise 1 on finding prime numbers**
2. **Exercise 2 on Euclidean / Extended Euclidean algorithm**
3. **Exercise 3 on Chinese Remainder Theorem**
4. **Exercise 4 on Order in cyclic group**