Overview of Number Theory Basics

Murat Kantarcioglu

Based on Prof. Ninghui Li's Slides

Divisibility

Definition

Given integers a and b, b ≠ 0, b divides a (denoted b|a) if ∃ integer c, s.t. a = c*b.*

b is called a **divisor** of a.

Theorem (Transitivity)

Given integers a, b, c, all > 1, with a|b and b|c, then a|c.

Proof:

a | b => ∃ m s.t. ma = b

b | c => ∃ n s.t. nb = c, nma = c,

We obtain that ∃ q = mn, s.t c = aq, so a | c

Divisibility (cont.)

Theorem

Given integers a, b, c, x, y all > 1, with a|b and a|c, then a | bx + cy.

Proof:

a | b => ∃ m s.t. ma = b
a | c => ∃ n s.t. na = c
bx + cy = a(mx + ny), therefore a| bx +cy

Divisibility (cont.)

Theorem (Division algorithm)

Given integers a,b such that a>0, a<b then there exist two unique integers q and r, $0 \le r < a$ s.t. $b = aq + r$.

Proof:

Uniqueness of q and r:
assume ∃ q' and r' s.t $b = aq' + r'$, $0 \le r' < a$, q' integer
then $aq + r = aq' + r' \Rightarrow a(q-q') = r'-r \Rightarrow q-q' = (r'-r)/a$
as $0 \le r, r' < a \Rightarrow -a < (r'-r) < a \Rightarrow -1 < (r'-r)/a < 1$
So $-1 < q-q' < 1$, but q-q' is integer, therefore
$q = q'$ and $r = r'$

Prime and Composite Numbers

Definition
An integer n > 1 is called a prime number if its positive divisors are 1 and n.

Definition
Any integer number n > 1 that is not prime, is called a composite number.

Example
Prime numbers: 2, 3, 5, 7, 11, 13,17 …
Composite numbers: 4, 6, 25, 900, 17778, …

Decomposition in Product of Primes

Theorem (Fundamental Theorem of Arithmetic)
Any integer number n > 1 can be written as a product of prime numbers (>1), and the product is unique if the numbers are written in increasing order.

$$n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$$

Example: 84 = 2^2•3•7

Greatest Common Divisor (GCD)

Definition
Given integers a > 0 and b > 0, we define gcd(a, b) = c, the greatest common divisor (GCD), as the greatest number that divides both a and b.

Example
gcd(256, 100)=4

Definition
Two integers a > 0 and b > 0 are relatively prime if gcd(a, b) = 1.

Example
25 and 128 are relatively prime.

GCD using Prime Decomposition

Theorem
Given $n = p_1^{e_1} p_2^{e2} \dots p_k^{ek}$ and

$m = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ then

where p_i are prime numbers
then

$$\gcd(n,m) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \dots p_k^{\min(e_k,f_k)}$$

Example: $84=2^2 \bullet 3 \bullet 7$ $90=2 \bullet 3^2 \bullet 5$

$\gcd(84,90)=2^1 \bullet 3^1 \bullet 5^0 \bullet 7^0$

GCD as a Linear Combination

Theorem
Given integers a, b > 0 and a > b, then d = gcd(a,b) is the least positive integer that can be represented as ax + by, x, y integer numbers.

Proof: Let t be the smallest integer, t = ax + by
$d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$, so $d \le t$.
We now show $t \le d$.
First $t \mid a$; otherwise, a = tu + r, 0 < r < t;
r = a - ut = a - u(ax+by) = a(1-ux) + b(-uy), so we found another linear combination and r < t. Contradiction.
Similarly $t \mid b$, so t is a common divisor of a and b, thus
$t \le$ gcd (a, b) = d. So t = d.

Example
gcd(100, 36) = 4 **=** $4 \times 100 – 11 \times 36$ = 400 - 396

GCD and Multiplication

Theorem
Given integers a, b, m >1. If
gcd(a, m) = gcd(b, m) = 1,
then gcd(ab, m) = 1

Proof idea:
ax + ym = 1 = bz + tm
Find u and v such that (ab)u + mv = 1

GCD and Division

Theorem

If g = gcd(a, b), where a > b, then gcd (a/g, b/g) = 1
(a/g and b/g are relatively prime).

Proof:
Assume gcd(a/g, b/g) = d, then a/g = md and b/g = nd.
a = gmd and b = gnd, therefore gd | a and gd | b
Therefore gd ≤ g, d ≤ 1, so d =1.

Example

gcd(100, 36) = 4
gcd (100/4, 36/4) = gcd(25, 9) = 1

GCD and Division

Theorem

Given integers a>0, b, q, r, such that b = aq + r,
then gcd(b, a) = gcd(a, r).

Proof:
Let gcd(b, a) = d and gcd(a, r) = e, this means

d | b and d | a, so d | b - aq , so d | r
Since gcd(a, r) = e, we obtain d ≤ e.

e | a and e | r, so e | aq + r , so e | b,
Since gcd(b, a) = d, we obtain e ≤ d.

Therefore d = e

Finding GCD

Using the Theorem: Given integers a>0, b, q, r, such that b = aq + r, then gcd(b, a) = gcd(a, r).

Euclidian Algorithm

Find gcd (b, a)

```
while a ≠0 do
    r ← b mod a
    b ← a
    a ← r
return a
```

Euclidian Algorithm Example

Find gcd(143, 110)

$$143 = 1 \times 110 + 33$$
$$110 = 3 \times 33 + 11$$
$$33 = 3 \times 11 + 0$$

gcd (143, 110) = 11

Towards Extended Euclidian Algorithm

- **Theorem:** Given integers a, b > 0 and a > b, then d = gcd(a,b) is the least positive integer that can be represented as ax + by, x, y integer numbers.
- How to find such x and y?

- If a and b are relative prime, then there exist x and y such that ax + by = 1.
  - In other words, ax mod b = 1.

Euclidian Algorithm Example

Find gcd(143, 111)

$143 = 1 \times 111 + 32$
$111 = 3 \times 32 + 15$
$32 = 2 \times 15 + 2$
$15 = 7 \times 2 + 1$

gcd (143, 111) = 1

$32 = 143 - 1 \times 111$
$15 = 111 - 3 \times 32$
$\quad = 4 \times 111 - 3 \times 143$
$2 = 32 - 2 \times 15$
$\quad = 7 \times 143 - 9 \times 111$
$1 = 15 - 7 \times 2$
$\quad = 67 \times 111 - 52 \times 143$

Extended Euclidian Algorithm

```
x=1;  y=0;  d=a;  r=0;  s=1;  t=b;
while (t>0) {
        q = $\lfloor d/t \rfloor$
        u=x-qr;  v=y-qs;  w=d-qt
        x=r;     y=s;     d=t
        r=u;     s=v;     t=w
}
return (d, x, y)
```

Invariants:

$ax + by = d$

$ar + bs = t$

Equivalence Relation

Definition
A relation is defined as any subset of a cartesian product. We denote a relation (a,b) ∈ R as aRb, a ∈ A and b ∈ B.

Definition
A relation is an equivalence relation on a set S, if R is

Reflexive: aRa for all a ∈ R
Symmetric: for all a, b ∈ R, aRb ⇒ bRa .
Transitive: for all a,b,c ∈ R, aRb and bRc ⇒ aRc

Example
“=“ is an equivalence relation on N

Modulo Operation

Definition:

$$a \bmod n = r \Leftrightarrow \exists q, \text{s.t. } a = q \times n + r$$
$$\text{where } 0 \le r \le n-1$$

Example:

7 mod 3 = 1
-7 mod 3 = 2

Definition (Congruence):

$$a \equiv b \bmod n \Leftrightarrow a \bmod n = b \bmod n$$

Congruence Relation

Theorem

Congruence mod n is an equivalence relation:

Reflexive: $a \equiv a$ (mod n)
Symmetric: $a \equiv b$(mod n) iff $b \equiv a$ mod n .
Transitive: $a \equiv b$(mod n) and $b \equiv c$(mod n) $\Rightarrow$
$a \equiv c$(mod n)

Congruence Relation Properties

Theorem

1) If a ≡ b (mod n) and c ≡ d (mod n), then:
   a ± c ≡ b ± d (mod n) and
   ac ≡ bd (mod n)

2) If a ≡ b (mod n) and d | n then:
   a ≡ b (mod d)

Reduced Set of Residues

Definition: A reduced set of residues (RSR) modulo m is a set of integers R each relatively prime to m, so that every integer relatively prime to m is congruent to exactly one integer in R.

The group (Z_n^*, ×)

- Z_n^* consists of all integers in [1..n-1] that are relative prime to n
  - $Z_n^* = \{ a \mid 1 \le a \le n \text{ and } \gcd(a,n)=1 \}$
  - is a reduced set of residues modulo n
  - (Z_n^*, ×) is a group
    - gcd(a,n)=1 and gcd(b,n)=1 $\Rightarrow$ gcd(ab, n)=1
  - given $a \in Z_n^*$, how to compute a^{-1}?

Linear Equation Modulo

Theorem

If gcd(a, n) = 1, the equation $ax \equiv 1 \bmod n$ has a unique solution, $0 < x < n$

Proof Idea:

if $ax_1 \equiv 1 \pmod{n}$ and $ax_2 \equiv 1 \pmod{n}$, then $a(x_1-x_2) \equiv 0 \pmod{n}$, then $n \mid a(x_1-x_2)$, then $n \mid (x_1-x_2)$, then $x_1-x_2=0$

Linear Equation Modulo (cont.)

Theorem

If gcd(a, n) = 1, the equation

$$ax \equiv b \bmod n$$

has a solution.

Proof Idea:
$x = a^{-1}$ b mod n

Chinese Reminder Theorem (CRT)

Theorem

Let n_1, n_2, ,,, n_k be integers s.t. gcd(n_i, n_j) = 1, i ≠ j.

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\ldots$$

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo
$n = n_1 n_2 \ldots n_k$

Proof of CMT

- Consider the function χ: $Z_n \rightarrow Z_{n1} \times Z_{n2} \times \ldots \times Z_{nk}$ $\chi(x) = (x \bmod n_1, \ldots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \le i \le k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i) = 1$
- For $1 \le i \le k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a1,a2,\ldots,ak) = \Sigma\ a_i m_i y_i \bmod n$
  - $a_i m_i y_i \equiv a_i \pmod{n_i}$
  - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

Proof of CMT

- Example of the mappings: $n_1=3$, $n_2=5$, $n=15$

χ: ρ: $m_1=5$, $y_1=2$, $m_1 y_1=10$, $m_2 y_2=6$,

1	(1,1)	(1,1)	10+6	1
2	(2,2)	(1,2)	10+12	7
4	(1,4)	(1,3)	10+18	13
7	(1,2)	(1,4)	10+24	4
8	(2,3)	(2,1)	20+6	11
11	(2,1)	(2,2)	20+12	2
13	(1,3)	(2,3)	20+18	8
14	(2,4)	(2,4)	20+24	14

Example of CMT:

$x \equiv 5 \pmod{7}$
$x \equiv 3 \pmod{11}$
$x \equiv 10 \pmod{13}$

- n_1=7, n_2=11, n_3=13, n=1001
- m_1=143, m_2=91, m_3=77
- $y_1=143^{-1}$ mod 7 = 3^{-1} mod 7 = 5
- $y_2=91^{-1}$ mod 11 = 3^{-1} mod 11 = 4
- $y_3=77^{-1}$ mod 13 = 12^{-1} mod 13 = 12
- x=(5×143×5 + 3×91×4 + 10×77×12) mod 1001 = 13907 mod 1001 = 894

The Euler Phi Function

Definition

Given an integer n, $\Phi(n) = |Z_n^*|$ is the number of all numbers a such that 0 < a < n and a is relatively prime to n (i.e., gcd(a, n)=1).

Theorem:

If gcd(m,n) = 1, $\Phi(mn) = \Phi(m)\,\Phi(n)$

The Euler Phi Function

Theorem: Formula for $\Phi(n)$

Let p be prime, e, m, n be positive integers

1) $\Phi(p) = p-1$
2) $\Phi(p^e) = p^e - p^{e-1}$
3) If $n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$ then

$$\Phi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\ldots(1-\frac{1}{p_k})$$

Fermat's Little Theorem

Fermat's Little Theorem

If *p* is a prime number and *a* is a natural number that is not a multiple of p, then

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

Proof idea:

gcd(a, p) = 1, then the set { i*a mod p} 0< i < p is a permutation of the set {1, …, p-1}.(otherwise we have 0<n<m<p s.t. ma mod p = na mod p

$p \mid (ma - na) \Rightarrow p \mid (m-n)$, where $0<m-n < p$)

$a * 2a * \ldots *(p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$

Since gcd((p-1)!, p) = 1, we obtain $a^{p-1} \equiv 1 \pmod{p}$

Consequence of Fermat's Theorem

Theorem

- p is a prime number and
- a, e and f are positive numbers
- $e \equiv f \bmod p\text{-}1$ and
- p does not divide a, then

$$a^e \equiv a^f \pmod{p}$$

Proof idea:

$a^e = a^{q(p-1)+f} = a^f (a^{(p-1)})^q$

by applying Fermat's theorem we obtain

$a^e \equiv a^f \pmod{p}$

Euler's Theorem

Euler's Theorem

Given integer n > 1, such that gcd(a, n) = 1 then

$$a^{\Phi(n)} \equiv 1 \pmod{n}$$

Corollary

Given integer n > 1, such that gcd(a, n) = 1 then $a^{\Phi(n)-1} \bmod n$ is a multiplicative inverse of a mod n.

Corollary

Given integer n > 1, x, y, and a positive integers with gcd(a, n) = 1. If $x \equiv y \pmod{\Phi(n)}$, then

$$a^x \equiv a^y \pmod{n}.$$

Next …

- Prime number distribution and testing
- RSA
- Efficiency of modular arithmetic