Introduction to Number Theory

Outline

- Division
- Prime
- GCD and LCM
- Modular Arithmetic
- Chinese Remainder Theorem
- Fermat’s little theorem

Division

Def: a,b $\in$ Z with a ≠ 0.

- We say a divides b (written a | b) if

  there exists, k $\in$ Z s.t. b = ka

  - a | b =>
    - a is a factor (or divisor) of b and
    - b is a multiple of a.
- Ex:
  - 3 | 12 (* 12 = 4 x 3, k=4)
  - -4 | 8,
  - 13 | 0 (0 = 0 x 13,k=0)
  - 3 !| 7(3 does not divide 7)

Properties of |

1. $a \mid b \wedge a \mid c \Rightarrow a \mid b + c$
2. $a \mid b \Rightarrow a \mid bc$ for all $c \in Z$
3. | is reflexive ($a \mid a$ for all $a \in Z$)
4. | is transitive ($a \mid b \wedge b \mid c$) $a \mid c$)
   - □ pf: $a \mid b \wedge b \mid c \Rightarrow$
   - □ $b = k_1 a$ and $c = k2\ b$ for some $k_1, k_2 \in Z$
   - □ $\Rightarrow c = k_2 (k_1 a) = (k_1 k_2) a$
5. | is antisymmetric ($a \mid b \wedge b \mid a \Rightarrow a = b$)

6. Any relation satisfying 3,4,5 is called a partial order

Primes

- An integer p > 1 is said to be prime if
  - $\forall$ n $\in$ N^+ (n | p $\Rightarrow$ n = 1 or n = p).
  - I.e., the only positive factors of p are 1 and p.
- p > 1 is not prime => P is composite.
- Examples:
  - 7 is prime
  - primes < 20 include :   2,3,5,7,11,13,17,19.

Fundamental Theorem of Arithmetic

- $\forall n \in N^{+} > 1$, there exists a unique increasing sequence of primes $p_1 \leq p_2 \leq \ldots \leq p_k$ ($k \geq 0$) s.t.

$$n = p_1 \text{ x } p_2 \ldots \text{ x } p_k.$$

- Ex:
  - 100 = 2 x 2 x 5 x 5
  - 99 = 3 x 3 x 3 x 37.

Proof:

- (Existence) by Mathematical Induction
  - Basis step: $n = 1, 2 : 1 = 1 \times 1, 2 = 1 \times 2$.
  - Inductive step: $n > 1$.
  - if n is prime, then $n = p_1 = 1 \times p_1$, where $p_1 = n$ and $k = 1$.
  - if n is not prime then $n = n_1 \times n_2$ with $n_1, n_2 < n$.
  - => by ind. hyp. $n_1 = q_1 \times q_2 \ldots \times q_t$
  - $n_2 = r_1 \times r_2 \ldots r_s$
  - => $n = n_1 \times n_2 = q_1 \times \ldots \times q_t \times r_1 \times \ldots \times r_s$.
  - => $n = p_1 \times \ldots \times p_{s+t}$. where $p_1,\ldots,p_{s+t}$ is an increasing reordering of $q_1,\ldots,q_t$ and $r_1,\ldots,r_t$.
- Uniqueness:
  - let $n = p_1 \times \ldots \times p_k \times q_1 \times \ldots \times q_s$
  - $= p_1 \times \ldots \times p_k \times r_1 \times \ldots \times r_t$ where $q_1 \neq r_1$
  - => $n - n = p_1 \times \ldots \times p_k \times (q_1 \times \ldots \times q_t - r_1 \times \ldots r_t)$
  - $\neq 0$ (a contradiction !!).

Division algorithm

- $a \in Z$, $d \in N^+$

  $\exists$i q,r such that $a = qd + r$ where $0 \leq r < d$.

Def: if $a = dq + r$ Then

- d is called the divisor
- a : dividend
- q: quotient
- r: remainder

- Examples:
  - $101 = 11 \cdot 9 + 2$
  - $-11 = -4 \cdot 3 + 1$
- Note: $d \mid a$ iff $r = 0$.

Proof of the division algorithm

Consider the sequence :

… a-3d, a-2d, a-d, a, a-(-d), a-(-2d), a-(-3d), …

- Let r = a – qd be the smallest nonnegative number in the sequence.

1. since the sequence is strictly increasing toward infinity such q (and r) must exist and unique.
2. if r ≥ d → r' =r-d =a – (q+1) d ≥ 0 is another nonnegative number in the sequence smaller than r. That's a contradiction.

Hence r must < d. QED

GCD and LCM

- $a,b \in Z$, $ab \neq 0$.

  if $d \mid a$ and $d \mid b$ → d is a common divisor of a and b.
- $\gcd(a,b) =_{def}$ the greatest common divisor of a and b.

Note: The set $cd = \{x > 0 : x \mid a \text{ and } x \mid b\}$ is a finite subset of N^+ ($\because$ $\{1\} \subseteq cd \subseteq \{1,\dots \min(a,b)\}$ $\therefore$ $\gcd(a,b)$ must exist.

- Example:
  - $\gcd(24,36) = ?$
  - factors of 24 : 1,2,3,4,6,12,24
  - factors of 36: 1,2,3,4,6,9,12,18,36
  - $\therefore$ $cd(24,36) = \{1,2,3,4,6,12\}$
  - $\therefore$ $\gcd(24,36) = 12$.

Relatively prime

- If gcd(a,b) = 1 we say a and b are relatively prime(r.p.).
  - Ex: gcd(17,22) = 1.
- $a_1, a_2, \ldots a_n$ are pairwise r.p. if

  $\gcd(a_i, a_j) = 1$ for all $1 \leq i < j \leq n$.
  - Ex:
  - 10,17,21 are p.r.p.
  - 10,19,24 are not p.r.p since gcd(10,24) = 2.

Proposition 1:

If $a = p_1^{x_1}\, p_2^{x_2} \ldots p_n^{x_n}$

and $b = p_1^{y_1}\, p_2^{y_2} \ldots p_n^{y_n}$,

where

$p_1 < p_2 \ldots < p_n$ are primes and all x_i, $y_j \geq 0$,

then

$$\gcd(a,b) = s =_{\text{def}} p_1^{z_1}\, p_2^{z_2} \ldots p_n^{z_n}$$

where $z_i = \min(x_i,y_i)$ for all $0 \leq i \leq n$.

Proof:

1. $s \in cd(a,b)$.
   - what are the quotients of a and b when divided by s ?
2. $t \mid a = p_1^{x_1} p_2^{x_2} \ldots p_n^{x_n} \Rightarrow t = p_1^{d_1} p_2^{d_2} \ldots p_n^{d_n}$ for some $d_1,\ldots d_n$ with $d_i \le x_i$ for $1 \le i \le n$.

pf: $t \mid a \Rightarrow a = tk$ for some integer k. let p be any prime factor of k.

Then $p \mid k \Rightarrow p \mid tk = a \Rightarrow p = p_j$ for some $1 \le j \le n$.

O/W by FTA: $a = \ldots.\ p \ldots \ne p_1^{x_1} p_2^{x_2} \ldots p_n^{x_n}$.

$\Rightarrow k = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ for some $r_1 \le x_1,\ldots,r_n \le x_n$.

and $t = a/k = p_1^{x_1 - r_1} \ldots p_m^{x_n - r_n}$ with all $x_i - r_i \ge 0$.

3.Corollary: $\forall t\ \ t \in cd(a,b) \Rightarrow\ t = p_1^{d_1} p_2^{d_2} \ldots p_n^{d_n}$

for some $d_1,\ldots d_n$ with $d_i \le x_i$, $d_i \le y_i$,and $d_i \le z_i$.

- Ex:
  - $120 = 2^3 \cdot 3^1 \cdot 5^1$
  - $500 = 2^2 \cdot 5^3$
  - $\therefore$ gcd(120,500) $= 2^2 \cdot 3^0 \cdot 5^1 = 20$

LCM

- $a,b \in Z \quad c \in N^+$

if $a|c$ and $b|c \Rightarrow d$ is a common multiplier of a and b.

- $\mathrm{lcm}(a,b) =_{\mathrm{def}}$ the least common multiplier of a and b.

Note: The set $cm = \{x > 0 \mid, a|x \text{ and } b|x\} \neq \emptyset$ ($\because \{ a \cdot b\} \subseteq cm$ $\therefore$. lcm(a,b) must exist.

Proposition 2:

If $a = p_1^{x_1} p_2^{x_2} \ldots p_n^{x_n}$, $b = p_1^{y_1} p_2^{y_2} \ldots p_n^{y_n}$, where

$p_1 < p_2 \ldots < p_n$ are primes and all $x_i, y_j \geq 0$,

then $\mathrm{lcm}(a,b) = t =_{\mathrm{def}} p_1^{z_1} p_2^{z_2} \ldots p_n^{z_n}$

where $z_i = \max(x_i,y_i)$ for all $0 \leq i \leq n$.

pf: $p_i^{x_i} \mid a \mid cm$ and $p_i^{y_i} \mid b \mid cm \Rightarrow p_i^{\max(x_i,y_i)} \mid cm \Rightarrow t \mid cm$.

Theorem 5: $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = a\,b$.

Modular Arithmetic

Def 8: $m \in N^+$, $a \in Z$.

a mod m $=_{def}$ the remainder of a when divided by m.

- Ex:
  - 17 mod 5 = 2
  - -133 mod 9 = 2.

Def 9: $a,b \in Z$, $m \in N^+$.

a ≡ b (mod m) means *m | (a-b)*.

- i.e., a and b have the same remainder when divided by m.
- i.e., a mod m = b mod m
- we say a is congruent to b (module m).

- Ex:
  - 17 ≡ 5 (mod 6) ?
  - 24 ≡ 14 (mod 6) ?

Properties of congruence

Theorem 6: $a \equiv b \pmod{m}$ iff

$a = km + b$ for some $k \in Z$.

pf: $a \equiv b \pmod{m} \Rightarrow (a-b) = km \Rightarrow a = km + b$.

Theorem 7: If $m > 0$, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

(1) $a + c \equiv b + d \pmod{m}$

(2) $ac \equiv bd \pmod{m}$.

pf: By the premise, $a = km + b$ and $c = sm + d$ for some k,s.

$\therefore$ $a + c = (b + d) + (k + s) m$ and

$ac = bd + (kd + sb + skm) m$

$\therefore$ (1) and (2) hold.

Ex: $7 \equiv 2 \pmod{5}$, $11 \equiv 1 \pmod{5}$ $\therefore$

$18 \equiv 3$ and $77 \equiv 2$.

Euclidean Algorithm

Lemma 1: $a = bq + r \Rightarrow \gcd(a,b) = \gcd(b,r)$.

pf: it suffices to show that cd(a,b) = cd(b,r). But

- $d|a \wedge d \mid b \Rightarrow d \mid (a-bq) = r$, and
- $d \mid b \wedge d \mid r \Rightarrow d \mid bq + r = a$. Hence cd(a,b) = cd(b,r).

Note: if $a = bq + 0 \Rightarrow \gcd(a,b) = \gcd(b,0) = b$.

- A simple algorithm:

```
gcd(a,b)  // $a \geq b \geq 0$.
  if (b == 0)
      return a;
    else
      return gcd(b, a mod b);
```

Note: this algorithm is very efficient.

Example: gcd(662, 414) = ?

a	b	a = qb+ r	q	r
662	414	662=1x414+248	1	248
414	248	414= 1x 248 + 166	1	166
248	166	248= 1 x 166 + 82	1	82
166	82	166= 2 x 82 + 2	2	2
82	2	82=42 x 2 + 0	42	0
2	0			

∴ gcd(662,414) = gcd(414,248) = …

= gcd(2,0) = 2.

Theorem

- $a > b \geq 0 \Rightarrow \gcd(a,b) = sa + tb$ for some s,t in Z.
  - i.e., gcd(a,b) is a linear combination of a and b.

Pf: By induction on b.

Basis: $b = 0. \Rightarrow \gcd(a,b) = a = 1 \cdot a + 0 \cdot b.$

Inductive case: $b > 0$.

case1: $b \mid a \Rightarrow \gcd(a,b) = b = 0\,a + 1\,b.$

case2: $b \nmid a \Rightarrow \gcd(a,b) = \gcd(b,r)$ where

$0 \leq r = a \bmod b < b.$

By I.H. $\gcd(b,r) = sb + t\,r.$ But $r = a - bq$

$$\therefore \gcd(a,b) = \gcd(b,r) = sb + tr$$

$$= sb + t(a - bq) = t\,a + (s - qt)\,b.$$ QED

Example

- gcd(252, 198) = 18 = ___· 252 + ___ · 198.

Sol:

Exercise: Let L(a,b) = {sa + tb | s,t ∈ Z } is the set of all linear combinations of a and b. Show that gcd(a,b) = the smallest positive number of L(a,b).

pf: let m = st + tb be any positive member of L(a,b) with m ≤ gcd(a,b) = g.

Since g | a and g | b , we have g | sa+tb => g ≥ m

Hence g = m.

Lemma 1 and Lemma 2

Lemma 1:$\gcd(a,b) = 1 \wedge a \mid bc \Rightarrow a \mid c$.

pf: $\gcd(a,b) = 1 \Rightarrow 1 = sa + tb$ for some $s,t \in Z$

$\Rightarrow c = sac + tbc = sac + tka \quad \because a \mid bc$

$= (sc + tk) \cdot a \therefore a \mid c$.

Lemma 2’: p : prime $\wedge\ p \nmid a \Rightarrow \gcd(p,a) = 1$.

Pf: $cd(p,a) \subseteq$ factors of $p = \{1,p\}$. but p is not a factor of a.

Hence $\gcd(p,a) = 1$.

Lemma 2: p : prime $\wedge\ p \mid a_1 a_2 \dots a_n \Rightarrow p \mid a_i$ for some i.

Pf: By ind. on n. Basis: $n = 1$. trivial.

Ind. case: $n = k + 1$. $p \mid a_1 a_2 \dots a_k a_{k+1}$.

If $p \mid a_1$ we are done.

O/W $p \nmid a_1$ and $\gcd(p, a_1) = 1$ by lem2’.

By Lem 1 : $p \mid (a_2 \dots a_{k+1}) \Rightarrow p \mid a_i$ for some $2 \leq i \leq k+1$ by IH.

Uniqueness of FTA

Pf: Suppose ∃ two distinct sequences

p_1 , … , p_s and q_1 , … , q_t with

$n = p_1$ x … x $p_s = q_1$ x … x q_t ⇒

Removing all common primes on both sides :

$m =_{def} p_{i1}$ x … $p_{iu} = q_{j1}$x … x q_{jv}

where $p_i \neq q_j$ for all p_i and q_j.

⇒ $p_{i1} \mid m = q_{j1}$x … x q_{jv}

⇒ $p_{i1} \mid q_j$ for some j (a contradiction!!).

Theorem 2

$m > 0 \;\wedge\; ac \equiv bc \pmod{m} \;\wedge\; \gcd(m,c) = 1 \Rightarrow$

$a \equiv b \pmod{m}$.

Pf: $ac \equiv bc \pmod{m}$

$\Rightarrow m \mid (ac - bc) = (a - b)\,c$.

$\because \gcd(m,c) = 1 \;\therefore\; m \mid (a - b)$

$\therefore a \equiv b \pmod{m}$.

Linear Congruence

Ex: Find all x such that 7 x ≡ 2 (mod 5).

Def: Equations of the form ax ≡ b (mod m) are called linear congruence equations.

Def: Given (a,m), any integer a’ satisfying the condition:

a a’ ≡ 1 (mod m)

is called the inverse of a (mod m).

Proposition: a a’ ≡ 1 (mod m) ⇒

x = a’ b + km is the general solution of the congruence equation ax ≡ b (mod m)

Pf: 1. a’b + km is a solution for any k ∈ Z.

2. y is a solution ⇒ ay ≡ b (mod m) => y ≡ a’b (mod m) => m | (y – a’b) ⇒ y = a’b + k’ m for some k.

Theorem:

- m > 0, gcd(a,m) = 1. Then ∃ b∈ Z s.t.
  - 1. ab ≡ 1 (mod m)
  - 2. if ab ≡ ac [≡ 1] ⇒ b ≡ c (mod m).

Pf: 1. gcd(a,m) = 1. Then ∃ b,t with ba + tm =1.

since m | ba –1 and hence ab ≡ 1 (mod m).

2. Direct from Theorem 2.

Note: Theorem 3 means That the inverse of a mod m uniquely exists (and hence is well defined) if a and m are relatively prime.

Examples

Ex: Find a s.t. $3a \equiv 1 \pmod{7}$.

Sol: since $\gcd(3,7) = 1$. the inverse of 3 (mod 7) exists and can be computed by the Euclidean algorithm:

$7 = 3 \times 2 + 1 \Rightarrow 1 = 7 + 3(-2)$. $\therefore$ $3(-2) \equiv 1 \pmod{7}$

$\Rightarrow a = -2 + 7k$ for all $k \in Z$.

EX: Find all solutions of $3x \equiv 4 \pmod{7}$.

Sol: -2 is an inverse of 3 (mod 7). Hence

$x = 4(-2) + 7k$ where $k \in Z$ are all solutions of x.

Chinese Remainder Theorem

- EX: Find all integer x satisfying the equations simultaneously:
  - $x \equiv 2 \pmod{3}$
  - $x \equiv 3 \pmod{5}$
  - $x \equiv 2 \pmod{7}$
- Theorem 4: $m_1, m_2, \ldots, m_n$: pairwise relatively prime. The system of congruence equations:
  - $x \equiv a_1 \pmod{m_1}$
  - $x \equiv a_2 \pmod{m_2}$
  - …
  - $x \equiv a_n \pmod{m_n}$
  - has a unique solution modulo $m = m_1\, m_2 \ldots m_n$.

Proof of the Chinese remainder theorem

Pf: Let $M_k = m / m_k$ for $1 \le k \le n$.

Note:

1. $\gcd(m_k, M_k) = 1$ and
2. $m_i \mid M_k$ if $i \neq k$. Hence

$\exists\ s_k, y_k$ s.t. $s_k m_k + y_k M_k = 1$. Hence

y_k is an inverse of M_k mod m_k. Now

$M_k y_k \equiv 1 \pmod{m_k}$ and

$M_k y_k \equiv 0 \pmod{m_j}$ for all $j \neq k$. Let

$x = a_1 M_1 y_1 + \ldots + a_n M_n y_n$ then

$x \equiv a_1 M_1 y_1 + \ldots + a_n M_n y_n \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$ for all $1 \le k \le n$.

Proof of the uniqueness part

If x and y satisfying the equations, then

$x\text{-}y \equiv 0 \pmod{m_k}$ for all k = 1..n. =>

$\exists\ s_1,\ldots,s_n$ with $x\text{-}y = s_1\ m_1 = \ldots = s_n\ m_n$.

since $\gcd(m_i, m_k) = 1$ for all $i \neq k$ and

$m_k \mid s_1\ m_1$, we have $m_k \mid s_1$ for all $k \neq 1$.

Hence s_1 is a multiple of $m_2\ m_3 \ldots m_n$ and

$x\text{-}y = s_1\ m_1$ is a multiple of $m = m_1\ m_2 \ldots m_k$.

Hence $x \equiv y \pmod{m}$. QED

Example

- Find x ≡ (2,3,2) (mod (3,5,7)) respectively.
- Sol:

i	m_i	a_i	M_i	$y_i = M_i^{-1}$ (mod m_i)	$a_i\ M_i\ y_i$
1	3	2	m/3=35	$35\ y_1 \equiv\ 1$ (mod 3) $\Rightarrow$ -1	2 x 35 x -1
2	5	3	m/5=21	$21\ y_2 \equiv 1$ (mod 5) $\Rightarrow$ 1	3 x 21 x 1
3	7	2	m/7=15	$15\ y_3 \equiv 1$ (mod 7) $\Rightarrow$ 1	2 x 15 x 1
	m = 105				x = -70 + 63 + 30 = 23.

Fermat’s little theorem

- p: prime, $a \in N$. Then

  1. if (p - a) then $a^{p-1} \equiv 1 \pmod p$. Moreover,

  2. for all a, $a^p \equiv a \pmod p$.

Ex:

1. $p = 17$, $a = 2 \Rightarrow 2^{16} = 65536 = 3855 \times 17 + 1$

   $\Rightarrow 2^{16} \equiv 1 \pmod{17}$.

2. $p = 3$, $a = 20 \Rightarrow 20^3 – 20 = 8000 –20 = 7980$ is a multiple of 3. Hence $20^3 \equiv 20 \pmod 3$.

Proof of Fermat's little theorem

Lemma: $\forall 1 \leq i < j \leq p-1$, $ia \not\equiv ja \pmod{p}$ and $ia \not\equiv 0 \pmod{p}$.

Pf: $ia \equiv ja \pmod{p} \Rightarrow p \mid (j-i)\, a$. Since $p - a$, $p \mid (j-i)$.

But $0 < j-i < p$, $p - (j-i)$, a contradiction.

1. Note the above lemma means ia and ja have different remainders when divided by p. Hence

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

   $\Rightarrow (p-1)!\, a^{p-1} \equiv (p-1)\,! \pmod{p}$. Then

   $p \mid (p-1)!\, (a^{p-1} - 1)$. $\because p - (p-1)!$, $p \mid a^{p-1} - 1$, and

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

2. if $p \mid a \Rightarrow p \mid a\,(a^{p-1} - 1) = a^p - a \Rightarrow a^p \equiv a \pmod{p}$.

   if $p - a \Rightarrow a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$.