Advanced Algorithms Analysis and Design

By

Nazir Ahmad Zafar

Lecture No 38

Number Theoretic Algorithms

(Definitions and Some Important Results)

Today Covered

- Applications of Number Theory
- Divisibility
- Numbers
- Prime Numbers
- Relatively Prime Numbers
- GCD
- Partitioning of Integers
- Congruency classes
- Proofs of some results

Applications of number theoretic algorithms

Electronic commerce

- Electronic commerce enables goods and services to be negotiated and exchanged electronically.
- The ability to keep information such as credit card numbers, passwords, bank statements private is essential if electronic commerce is used widely.
- Public-key cryptography and digital signatures are among the core technologies used and are based on numerical algorithms and number theory.

Applications of number theoretic algorithms

Congruency equations modulo n

- For example, if we are given an equation $ax \equiv b \pmod{n}$, where a, b, and n are integers, and we wish to find all the integers x, modulo n, that satisfy the equation.
- There may be zero, one, or more solution.
- Using brute force approach, we can simply try $x = 0, 1, ..., n - 1$ in order, and can find the solution
- But our objective is not to find a solution only, in fact we want an efficient, of course this problem can be solved using number theory.

Numbers

- Z = set of all integers = . . .,-3, -2, -1, 0, +1, +2 +3, . . .
- Set of all even integers = $\{ 2k \mid k \in Z \}$
- Set of all odd integers = $\{ 2k + 1 \mid k \in Z \}$
- Q = Set of all rational numbers
  - p/q
  - $p, q \in Z$
  - $q \neq 0$
- I = set of all irrational numbers: which are not irrationals i.e.
  - ~p/q OR
  - $\sim(p, q \in Z)$ OR
  - $\sim(q \neq 0)$

Definitions

Divisibility

Let a, $b \in \mathbf{Z}$ with $a \neq 0$ then we say that

$a|b \equiv a$ *divides* $b \Leftrightarrow \exists\, c \in \mathbf{Z} : b = ac$

It means that $a|b$ if and only if there exists an integer c such that c times a equals b.

Example 1:

3|(–12), because if we assume that a = 3, b = -12 then there exists c = -4 such that b = ac

Example 2:

3 does not divide 7, because if we assume that a = 3, b = 7 then there does not exists any integer c such that b = ac

Some Facts

Statement:

Prove that if $a|b$ then $a|(-b)$

Proof

Since a|b hence there exist an integer x such that b = ax,

Now -b = -ax = a(-x)

Since if $x \in Z$ then $(-x) \in Z$, Hence, $a|(-b)$

Note:

Because of the above lemma why not choose divisors as only positive.

- Hence if d is a divisor of b, then $1 \le d \le |b|$,

Example:

Only divisors of 24 are: 1, 2, 3, 4, 6, 8, 12,and 24.

Some Facts

Statement: Prove that $a|0 \ \forall \ a \in \mathbf{Z}$

Proof

- As we know that $a|b$ means there is an integer s such that $b = as$, and
- *Since 0 = a.0, where 0 is an integer, hence* $a|0$

Statement: *If* $a|b$, $a|c$ then $a \mid (b + c) \ \forall$ a, b, c $\in \mathbf{Z}$

Proof :

- As we know that $a|b$ means there is an integer s such that $b = as$, and
- $a|c$ means that there is a t such that $c = at$,
- Now $b + c = as + at = a(s + t)$, and hence $a|(b + c)$.

Some Facts

Statement:

If $a|b$, $a|c$ then $a \mid (b - c)\ \forall\ a, b, c \in \mathbf{Z}$

Proof :

- If $a|b$ means then there is an integer s such that $b = as$, and
- *If* $a|c$ then there is an integer t such that $c = at$,
- Now $b - c = as - at$

  $= a(s - t)$,
- Since if $s, t \in Z \Rightarrow s - t \in Z$
- Hence $a|(b - c)$.

Some Facts

Statement:

If $a|b$ and $b|a$ then prove that $a = \pm b$

Proof :

- Since $a|b$ hence there is an integer x such that

  $b = ax$, (1)

- *Since we are given that b*|a therefore there is an integer *t* such that

  $a = bt$, (2)

- From (1) and (2), $a = axt \Rightarrow xt = 1$
- Since x and t are both integers hence $x = t = \pm 1$
- Hence $a = \pm b$

Generalized Result

Statement: Prove that if $a|b$ then $a|bc$ $\forall$ a, b, c $\in$ **Z**

Proof :

- As we know that $a|b$ means there is an integer s such that $b = as$, and
- Now bc = asc = a(sc) and hence $a|bc$

Statement: Prove that if $a|b$, $b|c$ then $a|c$, $\forall$ a, b, c $\in$ **Z**

Proof :

- Since $a|b$, it means $\exists$ s $\in$ **Z** such that $b = as$, *and*
- Since $b|c$, it means $\exists$ t $\in$ **Z** such that $c = bt$
- Now c = bt = ast = a(st) and hence $a|c$

Generalized Result

Statement:

$\forall$ a, b, c $\in$ Z, *if a*|*b and a*|*c* then

a | (*bx* + *cy*), $\forall$ x, y $\in$ Z

Proof :

- As we know that *a*|*b* means there is an integer *s* such that *b* = *as* $\Rightarrow$ *bx* = *asx*, and
- *And if a*|c means that there is a *t* such that

  c = *at* $\Rightarrow$ *cy* = *aty*
- Now bx + *cy* = *asx* + *aty* = *a*(*sx* + *ty*), and hence *a*|(*bx* + *cy*), this is because (*sx* + *ty*) $\in$ Z

Generalized Result

Statement:

$\forall$ a, b, c $\in$ Z, *if a|b and a|c* then

$a \mid (bx - cy)$, $\forall$ x, y $\in$ Z

Proof :

- As we know that *a|b* therefore there is an integer *s* such that $b = as \Rightarrow bx = asx$, and
- *Since* a|c therefore there is an integer *t* such that

  $c = at \Rightarrow cy = aty$
- Now bx - $cy = asx - aty = a(sx - ty)$, and hence $a|(bx - cy)$, this is because $(sx - ty) \in Z$

Prime Numbers

Definition:

- A number p is prime if and only if it is divisible 1 and itself. OR
- A number p is prime if it can not be written as $p = x.y$ where $x, y \in Z$ and $x, y > 1$.

Note:

1 is prime, but is generally not of interest so we do not include it in set of primes

Examples

- 2, 3, 5,7 etc. are all prime

Examples

- 4, 6, 8, 9, 10 are not primes

Prime Numbers

- Prime numbers are central to number theory
- We will study some algorithms on prime numbers
- List of prime number less than 200

  2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199

- There are infinitely many primes.
- Any positive integer that is not prime is composite.
- 1 is the “unit” for multiplication and we assume that it is neither prime nor composite.

The Division Algorithm

Statement:

- For any integer *dividend* a and *divisor* $d \neq 0$, there is a unique *quotient* q and *remainder* $r \in \mathbf{N}$ such that

  $a = dq + r$, where $0 \leq r < |d|$

- In other way: $\forall\ a, d \in \mathbf{Z}, d > 0, \exists\ q, r \in \mathbf{Z}$ such that $0 \leq r < |d|$, and $a = d.q + r$
- We can find q by: $q = \lfloor a/d \rfloor$, and
- We can find r by: r = (a mod d) = a – dq

Example:

- a = 21; d = 4 then

  q = $\lfloor a/d \rfloor = \lfloor 21/4 \rfloor$ = 5, and r = a - dq = 21 - 4.5 = 1

Classification of Integers

When an integer is divided by 2 remainder is 0 or 1

1. $C_1 = \{ 2k \mid k \in Z \}$ and
2. $C_2 = \{ 2k + 1 \mid k \in Z \}$

When an integer is divided by 3 remainder is 0, 1 or 2

1. $C_1 = \{ 2k \mid k \in Z \}$,
2. $C_2 = \{ 2k + 1 \mid k \in Z \}$ and
3. $C_3 = \{ 2k + 2 \mid k \in Z \}$

When an integer divided by 4 remainder, 0, 1, 2 or 3

1. $C_1 = \{ 2k \mid k \in Z \}$,
2. $C_2 = \{ 2k + 1 \mid k \in Z \}$
3. $C_3 = \{ 2k + 2 \mid k \in Z \}$
4. $C_4 = \{ 2k + 3 \mid k \in Z \}$ . . .

Congruencies and Remainder

Remainder

- When a is divided by n then we can write (a mod n) as remainder of this division.
- If, remainder when a is divisible by n = remainder when b is divisible by n then

  (a mod n) = (b mod n) e.g. (8 mod 3) = (11 mod 3)

Congruency

- If (a mod n) = (b mod n) we write it as $a \equiv b \pmod{n}$

  "a is equivalent to b modulo n."
- Thus, a and b have same remainder, w.r.t. n then

  $a = q_a n + r$, for some $q_a \in Z$

  $b = q_b n + r$, for some $q_b \in Z$

Congruencies and Remainder

Lemma

If $a \equiv b \pmod{n}$ then prove that $n|(b - a)$

Proof:

Since $a \equiv b \pmod{n}$ *hence* $(a \bmod n) = (b \bmod n)$

Let $(a \bmod n) = (b \bmod n) = r$

By division theorem, $\exists\ q_1, q_2 \in Z$ such that

$$a = q_1 n + r, \qquad 0 \leqslant r < n$$

$$b = q_2 n + r, \qquad 0 \leqslant r < n$$

Now, $b - a = (q_2 - q_1)n + r - r = (q_2 - q_1)n$

Hence, $n|(b - a)$ because $(q_2 - q_1) \in Z$

Congruencies and Remainder

- The equivalence of b class modulo *n*:

$$[b]_n = \{b + kn : k \in Z\}, e.g.$$

$$[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$$

$$[-4]_7 = \ldots$$

$$[17]_7 = \ldots$$

- $Z_n = \{[a]_n : 0 \leq a \leq n - 1\}$ and we often write

Example

$Z_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

Usually we write $Z_4 = \{0, 1, 2, 3\}$

$Z_n = \{0, 1, 2, 3, \ldots, n - 1\}$, we associate a with $[a]_n$.

Prime Factorization

- By **factorization** of a number n, we mean that n = a × b × c, where a, *b, c* ∈ **Z**
- By a **prime factorization** of a number n, we mean that n = a × b × c, where a, *b, c* ∈ **Z**

  and all factors are prime number

Example:

- 3600 = 24 × 32 × 52 factorization
- 3600 = $2^{10} \times 3^{1} \times 13^{1}$ prime factorization
- 91 = 7×13 prime factorization

$$n = p_1^{m_1}.p_2^{m_2}\ldots p_k^{m_k} = \prod_{i=1}^{k} p_i^{m_i}$$

Relatively Prime Numbers

Definition

- Two numbers a, b are **relatively prime** if they have **no common divisors** except 1

Example

15, 23 are relatively prime, this is because

- Factors of 15 are 1, 3, 5, 15 and
- Factors of 23 are 1, 23 and
- Common factor is only 1
- Hence 15 and 23 are relatively prime

Some More Results

Definition: The greatest common divisor of a and b, not both zero, is the largest common divisor of a and b

Some elementary gcd properties

gcd(a, b) = gcd(b, a), gcd(a, b) = gcd(-a, b)

gcd(a, b) = gcd(|a|, |b|), gcd(a, 0) = |a|

Examples

gcd(24, 30) = 6, gcd(5, 7) = 1

gcd(0, 9) = 9, gcd(0, 0) = 0 by definition

$\gcd(a, ka) = |a| \text{ for any } k \in Z.$

Note: $1 \leq \gcd(a, b) \leq \min(|a|, |b|)$

Example: Greatest Common Divisor

- GCD of two integers can be obtained by comparing their prime factorizations and using least powers

Example

- 600 = 2 x 2 × 2 x 3 × 5 x 5 = 2^3 x 3^1 x 5^2
- 36 = 2 x 2 × 3 x 3 = 2^2 x 3^2
- Rearrange the factorization of 600 and 36
- 600 = 2 x 2 × 2 x 3 × 5 x 5 = 2^3 x 3^1 x 5^2
- 36 = 2 x 2 × 3 x 3 = 2^2 x 3^2 x 5^0
- GCD(36, 600) = $2^{\min(3,2)}$ x $3^{\min(1,2)}$ x $5^{\min(2,0)}$

  = 2^2 x 3^1 x 5^0

  = 4 x 3

  = 12

Brute Force Approach Finding GCD

Statement:

- Given two integers a and b. Find their greatest common divisor

Method:

- Compute prime factorization of a

$$a = p_1^{m_1} . p_2^{m_2} \ldots p_k^{m_k} = \prod_{i=1}^{k} p_i^{m_i}$$

- Compute prime factorization of b

$$b = p_1^{n_1} . p_2^{n_2} \ldots p_l^{n_l} = \prod_{i=1}^{l} p_i^{n_i}$$

- Let p_1, p_2, . . ., p_t be the set of all prime numbers both in the factorization of a and b

Brute Force Approach Finding GCD

- Now the prime factorization of a is rearranged as

$$a = p_1^{m_1}.p_2^{m_2}\ldots p_t^{m_t} = \prod_{i=1}^{t} p_i^{m_i}, where\ p_1 < p_2 < \ldots < p_t$$

- Similarly the prime factorization of b is rearranged as

$$b = p_1^{n_1}.p_2^{n_2}\ldots p_t^{n_t} = \prod_{i=1}^{t} p_i^{n_i}, \text{where p}_1 < p_2 < \ldots < p_t$$

- Finally GCD of a and b can be computed as

$$\gcd(a,b) = p_1^{\min(m_1,n_1)}.p_2^{\min(m_2,n_2)}\ldots.p_t^{\min(m_t,n_t)}$$

$$\gcd(a,b) = \prod_{i=1}^{t} p_i^{\min(m_i,n_i)}.$$

Methods of Proof

Direct Method:

- Express the statement to be proved in the form: $\forall\ x \in D,\ P(x) \Rightarrow Q(x)$
- Suppose that P(x) is true for an arbitrary element x of D
- Prove that Q(x) is true for the supposed above value x of D.

Parity:

Two integers have same parity if both are either odd or even, otherwise opposite parity.

Direct Proof

Lemma:

- Prove that m + n and m – n have same parity, for all m, n $\in$ Z

Proof:

There are three cases

Case 1:

Both m, n are even i.e.,

m = $2k_1$ and n = $2k_2$ for some k_1, $k_2 \in$ Z

Now, m + n = $2k_1 + 2k_2 = 2(k_1 + k_2)$ an even

And, m - n = $2k_1 - 2k_2 = 2(k_1 - k_2)$ an even

Direct Proof

Case 2:

Both m, n are odd i.e.,

$m = 2k_1 + 1$ and $n = 2k_2 + 1$ for some $k_1, k_2 \in Z$

Now, $m + n = 2k_1 + 1 + 2k_2 + 1 = 2(k_1 + k_2 + 1) = 2k'$

And, $m - n = 2k_1 + 1 - 2k_2 – 1 = 2(k_1 - k_2) = 2k''$

Hence m + n and m - n both are even

Case 3:

m is even and n is odd i.e.,

$m = 2k_1$ and $n = 2k_2 + 1$ for some $k_1, k_2 \in Z$

Now, $m + n = 2k_1 + 2k_2 + 1 = 2(k_1 + k_2) + 1 = 2k' + 1$, odd

And, $m - n = 2k_1 - 2k_2 – 1 = 2(k_1 - k_2 – 1) +1 = 2k'' + 1$, odd

Hence m + n and m - n both have the same parity.

An Alternate Method of Direct Proof

We can formulate the same problem as

Notations

- Let S-EVEN (m, n) $\equiv$ m + n is even
- Let S-ODD (m, n) $\equiv$ m + n is odd
- Let D-EVEN (m, n) $\equiv$ m - n is even
- Let D-ODD (m, n) $\equiv$ m - n is odd

Mathematical Statement of the problem

- S-EVEN (m, n) $\Leftrightarrow$ D-EVEN (m, n), $\forall$ m, n $\in$ Z
- S-ODD (m, n) $\Leftrightarrow$ D-ODD (m, n), $\forall$ m, n $\in$ Z

An Alternate Method of Direct Proof

Proof

Case 1

- Suppose that S-EVEN (m, n), ∀ m, n ∈ Z
- Now, m – n = m + n – 2n = even - even = even integer
- Hence D-EVEN (m, n), ∀ m, n ∈ Z

Case 2

- Suppose that D-EVEN (m, n), ∀ m, n ∈ Z
- Now, m + n = m - n + 2n = even + even = an even integer, ∀ m, n ∈ Z
- Hence S-EVEN (m, n), ∀ m, n ∈ Z

An Alternate Method of Direct Proof

Case 3

- Suppose that S-ODD (m, n), $\forall$ m, n $\in$ Z
- Now, m – n = m + n – 2n = odd – even = odd
- D-ODD (m, n), $\forall$ m, n $\in$ Z

Case 4

- Suppose that D-ODD (m, n), $\forall$ m, n $\in$ Z
- Now, m + n = m - n + 2n = odd + even = odd
- S-ODD (m, n), $\forall$ m, n $\in$ Z

Hence

- S-EVEN (m, n) $\Leftrightarrow$ D-EVEN (m, n), $\forall$ m, n $\in$ Z
- S-ODD (m, n) $\Leftrightarrow$ D-ODD (m, n), $\forall$ m, n $\in$ Z

Disproof by Counter Example

To disprove a statement of the form:

$\forall\ x \in D, P(x) \Rightarrow Q(x)$

- Find a value of x in D for which P(x) is true and Q(x) is false.
- Such an example is called counter example.

Example : Prove or disprove

$$\forall\ a, b \in Z, a^2 = b^2 \Rightarrow a = b$$

Disproof:

Let $P(a, b) \equiv a^2 = b^2$, $Q(a, b) \equiv a = b$,

Now $P(1, -1) \equiv (1)^2 = (-1)^2$ true but $Q(1, -1) \equiv 1 \neq -1$

Method of Proof by Contradiction

Steps in proving by contradiction

- Suppose the statement to be proved is false
- Show that this supposition leads logically to a contradiction
- Conclude that the statement to be proved is true

Example:

- Prove that sum of an irrational and a rational number is irrational

Proof

- Suppose a is a rational, b is an irrational number and their sum is also rational

Example (Contd..)

- Since a is rational, $a = p/q$, $p, q \in Z$ and $q \neq 0$
- Now according to our supposition $a + b$ is rational and hence it can be written as

  $a + b = m/n$, where $m, n \in Z$ and $n \neq 0$
- Now consider

  $a + b = m/n$

$\Rightarrow$ $b = m/n – a = m/n – p/q = (mp – nq)/nq = r/s$,

where $r, s \in Z$ and $s \neq 0$

$\Rightarrow$ b is a rational number, which is contradiction.

$\Rightarrow$ Hence sum of an irrational and a rational number is always irrational.

Proof by Contradiction

Lemma

- For any integer n and any prime number p, if p divides n then p does not divide n + 1

Proof

- Express the statement in the form:

  $\forall\ x \in D, P(x) \Rightarrow Q(x)$

- Let, Z = set of all integers, and
- P = set of all primes
- $D(p, n) \equiv$ p divides n
- $DN(p, n) \equiv$ p does not divide n
- Now our problem becomes

  $\forall\ n \in Z, p \in P, D(p, n) \Rightarrow DN(p, n + 1)$

Proof by Contradiction

- Suppose that for some integer n and prime p, p divides n ≡ D(p, n)
- Now we have to prove that p does not divide n + 1
- On contrary we suppose that p divide n + 1
- It means that there exists an integer q_1 such that $n + 1 = pq_1$
- Since p divides n. Hence there exists an integer q_2 such that $n = pq_2$
- Now, $n + 1 – n = pq_1 – pq_2$

  $1 = pq_1–pq_2 = p(q_1– q_2) \Rightarrow p = 1$ or -1 contradiction
- Hence p does not divide n + 1 ≡ DN(p, n)