Basic Number theory

Prof. Ashok K Bhateja, IIT Delhi

Algorithms Complexity

- **Polynomial-time algorithm** is an algorithm whose worst-case running time function is of the form $O(n^k)$, where n is the input size and k is a constant.
- **Subexponential-time algorithm** is an algorithm whose worst-case running time function is of the form $e^{O(n)}$, where n is the input size.

  A subexponential-time algorithm is asymptotically faster than an algorithm whose running time is fully exponential in the input size, while it is asymptotically slower than a polynomial-time algorithm.
- Definition: **Decision problems**, i.e., problems which have either YES or NO as an answer.

Algorithms Complexity

- The **complexity class NP** is the class of problems that can be verified by a polynomial-time algorithm.
- Definition The **complexity class NP** is the set of all decision problems for which a YES answer can be verified in polynomial time using some extra information, called a certificate.
- Example: COMPOSITES belongs to NP because if an integer n is composite, then this fact can be verified in polynomial time if one is given a divisor a of n, where $1 < a < n$ (the certificate in this case consists of the divisor a).

NP Complete

- Definition Let L_1 and L_2 be two decision problems. **L_1 is said to polytime reduce to L_2**, written $L_1 \leq_p L_2$, if there exists a polynomial-time computable function *f* such that $f(L_1) = L_2$.

  This function *f* is called the **reduction function**, and a polynomial-time algorithm that computes *f* is a **reduction algorithm**.

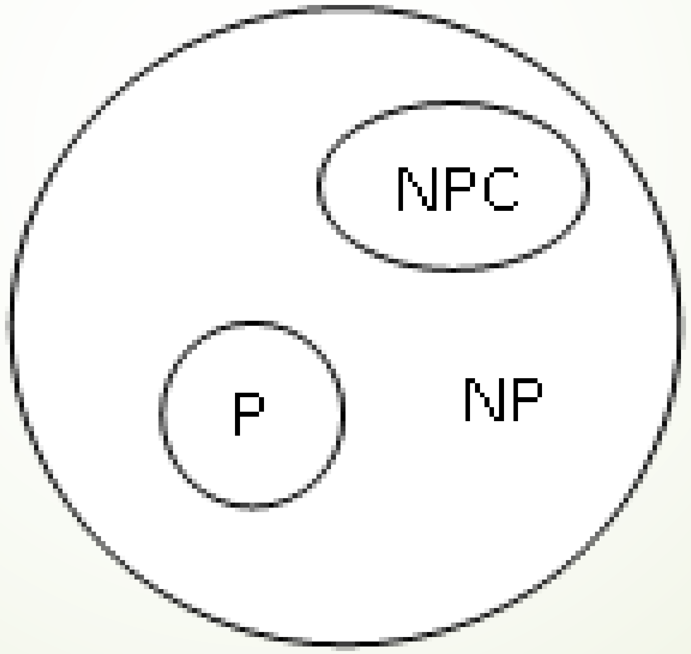
- Definition A decision problem L is said to be **NP-complete** if

  1. $L \in NP$ and
  2. $L_1 \leq_p L$ for every $L_1 \in NP$.

  Example: Subset sum problem, clique problem, vertex cover problem

- If a problem L satisfies property 2, but not necessarily property 1, we say that L is ***NP-hard***.

- Example (NP-hard problem): Given positive integers $a_1, a_2, \ldots, a_n$ and a positive integer s, finding a subset of the a_i which sums to s, provided that such a subset exists. This problem is NP-hard.



Greatest Common Divisor

- Definition: An integer c is a **common divisor** of a and b if c/a and c/b.
- Definition A non-negative integer d is the greatest common divisor of integers a and b, denoted $d = \gcd(a, b)$, if
  1. d is a common divisor of a and b; and
  2. whenever c/a and c/b, then c/d.
- Example: The common divisors of 12 and 18 are $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, and gcd (l2, 18) = 6.
- Fact: For any integer $k \neq 0$, $\gcd(ka, kb) = |k| \gcd(a, b)$.

Euclidean algorithm or Euclid's algorithm

- It is an efficient method for computing GCD of two numbers, the largest number that divides both without leaving a remainder.
- It is named after the ancient Greek mathematician Euclid.

For two given numbers a and b, such that $a \geq b$

if b / a, then gcd (a, b) = b,

otherwise gcd (a, b) = gcd (b, a mod b).

Euclidean algorithm (Example)

gcd (138, 105)

$138 = 1 \times 105 + 33$

$105 = 3 \times 33 + 6$

$33 = 5 \times 6 + 3$

$6 = 2 \times 3 + 0$

Therefore gcd (138, 105) = 3

- If gcd (a, b) = 1, then a and b are said to be coprime (or relatively prime) e.g., 6 and 35

Fact: If a and b are not both zero, then for any integers x and y

$$\gcd(a, b) \mid (ax + by).$$

(Bezout's Theorem): If a and b are integers, not both zero, then there are integers x and y such that $ax + by = \gcd(a, b)$.

Use the Euclidean Algorithm to determine the GCD, then work backwards using substitution.

gcd (138, 105) $138 = 1 \times 105 + 33$ $105 = 3 \times 33 + 6$ $33 = 5 \times 6 + 3$ $6 = 2 \times 3 + 0$	$3 = 33 - 5 \times 6$ $3 = 33 - 5 \times (105 - 3 \times 33)$ $3 = 16 \times 33 - 5 \times 105$ $3 = 16 \times (138 - 1 \times 105) - 5 \times 105$ $3 = 16 \times 138 - 21 \times 105$

Lemma: If a and b are integers such that there are integers x and y with $ax + by = 1$, then $\gcd(a, b) = 1$.

Congruences

- Given three integers a, b and n; a is congruent to b modulo n i.e., write $a \equiv b \bmod n$, if the difference $a - b$ is divisible by n.
- n is called the modulus of the congruence.
- Theorem: Let $a, a', b, b', n \in Z$ with $n > 0$. If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then

  $a + b \equiv a' + b' \pmod{n}$ and $a \cdot b \equiv a' \cdot b' \pmod{n}$.

Theorem: Let $a, x, y \in Z$ and $n \in N$. Then

$$a\,x \equiv a\,y \pmod{n} \Leftrightarrow x \equiv y \pmod{n/\gcd(a, n)}.$$

If $a\,x \equiv a\,y \pmod{n}$ and $\gcd(a, n) = 1$, then $x \equiv y \pmod{n}$

Proof. Observe first that when $\gcd(a, n) = 1$, then

$$n \mid a\,(x - y) \Leftrightarrow n \mid (x - y).$$

i.e. whenever $(a, n) = 1$,

$a\,x \equiv a\,y \pmod{n}$ implies $x \equiv y \pmod{n}$

When $\gcd(a, n) > 1$, on the other hand, one does at least have

$$\left(\frac{a}{\gcd(a,n)}, \frac{n}{\gcd(a,n)}\right) = 1, \text{ so that}$$

$$n \mid a(x-y) \;\Leftrightarrow \frac{n}{\gcd(a,n)} \,\Big|\, \frac{a}{\gcd(a,n)}(x-y) \Leftrightarrow \frac{n}{\gcd(a,n)} \,\Big|\, (x-y)$$

Multiplicative Inverse of *a* modulo *n*

Let $a \in Z_n$. The **multiplicative inverse of *a* modulo *n*** is an integer $x \in Z_n$, s.t., $ax \equiv 1 \pmod{n}$. If such an x exists, then it is unique, and a is said to be invertible, or a unit.

Theorem: If $ax + by = 1$ then $x^{-1} \bmod y \equiv a$

Proof: $ax + by = 1$

Taking mod y both sides

$ax \bmod y + by \bmod y \equiv 1 \bmod y$

$\Rightarrow ax \bmod y \equiv 1 \Rightarrow x^{-1} \bmod y \equiv a$

Multiplicative Inverse : Example

Find $35^{-1} \bmod 51$

$51 = 1 \times 35 + 16$

$35 = 2 \times 16 + 3$

$16 = 5 \times 3 + 1$

$16 = 5 \times 3 + 1 \Rightarrow 1 = 16 - 5 \times 3$

$\Rightarrow 1 = 16 - 5 \times (35 - 2 \times 16)$ because $3 = 35 - 2 \times 16$

$\Rightarrow 1 = 11 \times 16 + (-5) \times 35$

$\Rightarrow 1 = 11 \times (51 - 1 \times 35) + (-5) \times 35$

$\Rightarrow 1 = 11 \times 51 + (-16) \times 35$

Taking mod 51 both side $(-16) \times 35 \equiv 1 \bmod 51 \Rightarrow 35^{-1} \bmod 51 \equiv -16$

or $35^{-1} \bmod 51 \equiv 35$

Theorem: If a and b are integers, m is a positive integer. Given the congruence $ax \equiv b \pmod{m}$.

1. If $\gcd(a, m) = 1$, then the congruence has a unique solution.
2. If $\gcd(a, m) = d$ and $d \mid b$, then the congruence has d solutions.
3. If $\gcd(a, m) = d$ and $d \nmid b$, then the congruence has no solution.

Proof : Case 1: Let y be another solution to $ax \equiv b \pmod{m}$

$ax \equiv ay \equiv b \pmod{m} \Rightarrow a(x - y) \equiv 0 \pmod{m}$

then m divides $a(x - y)$ and as m and a are relatively prime and have no factors in common, m divides $x - y$.

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

As $\gcd(a, m) = 1$, $\exists$ integers x and y s.t. $ax + my \equiv 1 \pmod{m}$

i.e., $ax \equiv 1 \pmod{m}$. Hence x is a unique solution to $ax \equiv b \pmod{m}$.

Theorem: If a and b are integers, m is a positive integer. Given the congruence $ax \equiv b \pmod{m}$.

1. If gcd $(a, m) = 1$, then the congruence has a unique solution.
2. If gcd $(a, m) = d$ and $d \mid b$, then the congruence has d solutions.
3. If gcd $(a, m) = d$ and $d \nmid b$, then the congruence has no solution.

Case 2: gcd $(a, m) = d$ and $d \mid b$.

Let $m' = m/d$ and $a' = a/d$; gcd $(a', m') = 1$

Then $ax \equiv b \pmod{m} \Longrightarrow ax - b$ is divisible by m

$\Longrightarrow a'd\,x - dk$ is divisible by $m'd$. So, $a'x - k$ is divisible by m'

or $a'x \equiv k \pmod{m'}$ which has exactly one solution.

Let that solution be g. Any solution x must be so that $x \equiv \text{g} \pmod{m'}$

$\Longrightarrow$ there are d such x, where $x = g + jm'$; $0 \le j < d$

Theorem: If a and b are integers, m is a positive integer. Given the congruence $ax \equiv b \pmod{m}$.

1. If gcd $(a, m) = 1$, then the congruence has a unique solution.
2. If gcd $(a, m) = d$ and $d \mid b$, then the congruence has d solutions.
3. If gcd $(a, m) = d$ and $d \nmid b$, then the congruence has no solution.

Proof : Case 3: Suppose that x_0 is a solution of $ax \equiv b \pmod{m}$.

$\therefore\ ax_0 \equiv b \pmod{m}$, hence, $ax_0 - b = km$ for some integer k.

Since $d \mid a$ and $d \mid m$ it follows that $d \mid b$.

By contraposition, if $d \nmid b$, then no solution exists to $ax \equiv b \pmod{m}$.

Prime Number

An integer $p \geq 2$ is said to be **prime** if its only positive divisors are 1 and p. Otherwise, p is called composite.

Prime Number Theorem: Let $\pi(x)$ denotes the number of prime numbers $\leq x$. Then

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

i.e., for large values of x, $\pi(x)$ is closely approximated by the expression $x/\ln(x)$. e.g. for $x = 10^{10}$, $\pi(x) = 455{,}052{,}511$.

Euler phi-function

Let n be a positive integer. The Euler phi-function $\varphi(n)$ is defined as $\varphi(n)$ = number of nonnegative integers less than n which are co-prime to n.

Properties of Euler phi-function:

1. $\varphi(1) = 1$
2. If p is a prime, then $\varphi(p) = p - 1$
3. If gcd $(m, n) = 1$, then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$
   i.e., Euler phi function is multiplicative.
4. If $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot (p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

$$= n\,(1 - 1/\,p_1).\,(1 - 1/\,p_2) \ldots (1 - 1/\,p_k).$$

Chinese Remainder Theorem (CRT)

Let $m_1, m_2 \ldots m_r$ be relatively coprime. Then the system of equations

$$x \equiv a_1 \bmod m_1,$$
$$x \equiv a_2 \bmod m_2,$$
$$\ldots \quad \ldots$$
$$x \equiv a_r \bmod m_r$$

has a unique solution $x \equiv \sum_{i=1}^{r} a_i N_i z_i \bmod N$

where $N = m_1 . m_2 \ldots m_r$, $N_i = \frac{N}{m_i}$ and $z_i = N_i^{-1} \bmod m_i$

CRT: Example

Example: Solve the system of congruences

$x \equiv 1 \bmod 3$

$x \equiv 4 \bmod 5$

$x \equiv 6 \bmod 7$

Solution: Here $N = 105$, $N_1 = 35$, $N_2 = 21$, $N_3 = 15$

$$x \equiv \{(1 \cdot 35 \cdot 35^{-1} mod\ 3) + (4 \cdot 21 \cdot 21^{-1} mod\ 5) + (6 \cdot 15 \cdot 15^{-1} mod\ 7)\}\ mod\ 105$$

$$x \equiv \{(1 \cdot 35 \cdot 2) + (4 \cdot 21 \cdot 1) + (6 \cdot 15 \cdot 1)\}\ mod\ 105$$

$$\equiv 244\ mod\ 105 \equiv 34\ mod\ 105$$

Fact: If $\gcd(n_1, n_2) = 1$, then the pair of congruences $x \equiv a \pmod{n_1}$, $x \equiv a \pmod{n_2}$, has a unique solution $x \equiv a \pmod{n_1 n_2}$.

Solution of linear congruences when moduli are not relatively prime

- CRT works only if pair of moduli are coprime.
- If a pair of congruences are not coprime, then we can split each of the congruences into two congruences so that the new moduli are relatively prime.
- If both m_1 and m_2 are divisible by prime p, then split each of the congruences into two congruences where one of the new moduli is the factor having highest power of p.

Splitting a single congruence

- A single congruence

  $x \equiv a \bmod (m_1 m_2)$ can be written as

  $x \equiv a \bmod m_1$ and $x \equiv a \bmod m_2$

  Example: $x \equiv 3 \bmod 63$ is equivalent to

  $x \equiv 3 \bmod 7$ and $x \equiv 3 \bmod 9$

Splitting of two congruences both divisible by a prime

Example: $x \equiv 3 \bmod 63$ and $x \equiv 5 \bmod 108$

Here 3 is a prime, both 63 (= $3^2 \times 7$) and 108 (= $3^3 \times 4$) are divisible by 3.

Split into four congruences:

$$x \equiv 3 \pmod 9$$

$$x \equiv 5 \pmod{27}$$

$$x \equiv 3 \pmod 7$$

$$x \equiv 5 \pmod 4$$

- If both the congruences involve powers of a same prime p, then one of following will be true
  - The congruences are contradictory and so there are no solutions.

  Example: $x \equiv 3 \pmod 9$

  $$x \equiv 5 \pmod{27};\ x = 5, 32, 59, \ldots \not\equiv 3 \pmod 9$$

  - Both congruences for powers of p are implied by the congruence with the higher power. So, the other congruence (with lower power of p) may be ignored.

  Example: $x \equiv 5 \pmod 9$

  $$x \equiv 23 \pmod{27};\ x = 23, 50, \ldots \equiv 5 \pmod 9$$