Discrete Structures

Day 2

Primes and Greatest Common Divisors

- **Primes**
  - An integer *p* greater than 1 is called *prime* if the only positive factors of *p* are 1 and *p*. A positive integer that is greater than 1 and is not prime is called *composite*.
- **THE FUNDAMENTAL THEOREM OF ARITHMETIC:** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.
- Eg: $100 = 2 \times 2 \times 5 \times 5 = 2^2 5^2$

  $999 = 3^3 37$

- **THEOREM**

If *n* is a composite integer, then *n* has a prime divisor less than or equal to $\sqrt{n}$.

Eg: Check 71 is prime or not? Floor($\sqrt{71}$) = 8

THEOREM

There are infinitely many primes.

(both the above theorem can be proved using Proofs by contradiction. Proof will be shown when we study "Introduction to Proofs")

Greatest Common Divisors

- Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.
- The integers a and b are *relatively prime* if their greatest common divisor is 1.
- The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Q. Determine whether the integers are pairwise relatively prime

i. 10, 17, and 21

ii. 10, 19, and 24

GDCs as Linear Combinations

- **BÉZOUT'S THEOREM:** If *a* and *b* are positive integers, then there exist integers *s* and *t* such that gcd*(a, b)* = *sa* + *tb (called Bézout's identity*).

- The value of s and t can be computed either using Euclidean Algorithm or Extended Euclidean Algorithm.
- Euclidean Algorithm is based on two facts
  - $\gcd(a, 0) = a$
  - $\gcd(a, b) = \gcd(b, r)$, where r is the remainder of dividing a by b.

  Eg: $\gcd(6, 4) = \gcd(4, 2) = \gcd(2, 0) = 2$

Q. Given $a = 252, b = 198$. Find 's' and 't' such that $\gcd(a, b) = s \times a + t \times b$ using Euclidean Algorithm

$252 = 1 \times 198 + 54$

$198 = 3 \times 54 + 36$

$54 = 1 \times 36 + 18$

$36 = 2 \times 18 + 0$

Using the next-to-last division, we can express gcd(252, 198) = 18 as a linear combination of 54 and 36.

$18 = 54 - 1 \times 36$ ---(i)

$36 = 198 - 3 \times 54$ ---(ii)

$54 = 252 - 1 \times 198$ ---(iii)

$18 = 54 - 1 \times (198 - 3 \times 54) = 4 \times 54 - 1 \times 198$

$= 4 \times (252 - 1 \times 198)$ -$1 \times 198 = 4 \times 252 - 5 \times 198$

$18 = 4 \times 252 + (-5) \times 198$

Q. Given $a = 252, b = 198$. Find 's' and 't' such that $\gcd(a, b) = s \times a + t \times b$ using extended Euclidean Algorithm

q	r_1	r_2	r	s_1	s_2	$s = s_1 - q \times s_2$	t_1	$t_2 = t_1 - q \times t_2$	$r = r_1 - q \times r_2$
1	252	198	54	1	0	1	0	1	-1
3	198	54	36	0	1	-3	1	-1	4
1	54	36	18	1	-3	4	-1	4	-5
2	36	18	0	-3	4	-11	4	-5	14
	18	0		4	-11		-5	14	

Q. Given a=161 and b=28, find $\gcd(a, b)$ and the value of s and t such that $\gcd(a, b) = s \times a + t \times b$

Linear Diophantine Equations

- Find integer values of x and y that satisfy $ax + by = c$.
- This type of equation has either no solution or an infinite number of solutions.
- Let $d = \gcd(a, b)$.
  - If $d \nmid c$, then the equations has no solution.
  - If $d|c$, then the equations have an infinite number of solutions. One of them is called particular solutions and the rest general.
- Particular Solution
  - If $d|c$:
    - Reduce the equations to $a_1x + b_1y = c_1$ by dividing both sides by d.
    - Solve for s and t in the relations $a_1s + b_1t = 1$ using extended Euclidian algorithm.
    - Particular solutions: $x_0 = c_1s$ and $y_0 = c_1t$
    - General solutions: $x = x_0 + kb_1$ and $y = y_0 - ka_1$, where k is an integer

Q. Find the particular and general solutions to the equations $21x + 14y = 35$

$d = \gcd(21,14) = 7.$

Since $7|35$, the equations has infinite solutions

$3x + 2y = 5$

Use extended Euclidean algorithm and find s and t such that $3s + 2t = 1$

1	3	2	1	1	0	1	0	1	-1
2	2	1	0	0	1	-2	1	-1	3
	1	0		1	-2		-1	3	

$s = 1$ and $t = -1$

Particular: $x_0 = 5 \times 1 = 5$ and $y_0 = 5 \times (-1) = -5$

General: $x = 5 + k \times 2$ and $y = -5 - k \times 3$, where k is an integer

THE CHINESE REMAINDER THEOREM

- Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_k$ arbitrary integers. Then the system

$$x \equiv a_1 mod\, m_1$$
$$x \equiv a_2 mod\, m_2$$
$$.$$
$$x \equiv a_k mod\, m_k$$

has a unique solution

Steps.

1. Common modulus $M = m_1 \times m_2 \ldots \times m_k$.
2. $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, ..., $M_k = \frac{M}{m_k}$.
3. Find multiplicative inverse of $M_1, M_2, \ldots, M_k$ using the corresponding moduli $(m_1, m_2, \ldots, m_k)$ named as M_1^{-1}, $M_2^{-1}, \ldots, M_k^{-1}$.
4. The solution is $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots + a_k \times M_k \times M_k^{-1})$ mod M

Q. Solve x,

$x \equiv 2 \; mod \; 3$

$x \equiv 3 \; mod \; 5$

$x \equiv 2 \; mod \; 7$

1. $M = 3 \times 5 \times 7 = 105.$
2. $M_1 = \frac{105}{3} = 35, M_2 = \frac{105}{5} = 21, M_3 = \frac{105}{7} = 15.$
3. $M_1^{-1} = \frac{1}{35} mod 3 = 2, M_2^{-1} = \frac{1}{21} mod 5 = 1, M_3^{-1} = \frac{1}{15} mod 7 = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) mod \; 105 = 23$

Q. Solve x,

$x \equiv 1 \, mod \, 3$

$x \equiv 3 \, mod \, 11$

$x \equiv 6 \, mod \, 17$

Ans is 91

- Thank you.