Module I : Number Theory (MATH 2201)

by

Dr. RITUPARNA GHOSH

Heritage Institute of Technology, Kolkata

1 Well-Ordering principle

Every non-empty subset S of set of positive integers has a least element.

Counter-Examples

Set of integers, or, set of positive real numbers does not satisfy well-ordering principle.

Problem : There are no positive integers strictly between 0 and 1.

Let S be the set of integers x such that $0 < x < 1$. Let n be its least element. Multiplying both sides of $n < 1$ by n gives, $n^2 < n$. Therefore, $0 < n^2 < n < 1$. This is a contradiction since n is least element. Hence S is empty.

2 Division Algorithm

Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying $a = bq + r$, $0 \leq r < b$. The integers q and r are respectively called, the quotient and remainder in division of a by b.

Proof. Let us consider the set $S = \{a - xb : x \in \mathbb{Z}, a - xb \geq 0\}$. We first show that S is non-empty. Since $b \geq 1$, $|a|b \geq |a|$, and so, $a - (-|a|)b \geq a + |a| \geq 0$. Thus, for the choice $x = -|a|$, S is non-empty. Hence by well-ordering principle, S contains a least element. say r. By the definition of S, there exists an integer q satisfying $r = a - bq, r \geq 0$.

We argue that $r < b$. Let us assume in the contrary, $r \geq b$ and $a - (q + 1)b = (a - bq) - b = r - b \geq 0$. This implies that it is a member of S. But $r - b < r$, leading to a contradiction of choice r as the least element. Hence, $r < b$.

Next we show the uniqueness of q and r. Suppose that a has two representations $a = bq + r = bq' + r', 0 \leq r < b, 0 \leq r' < b$. Then $r - r' = b(q' - q)$, which gives, $|r - r'| = b|q - q'|$. Upon adding two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we obtain, $-b < r' - r < b$, or, $|r' - r| < b$. Thus, $b|q - q'| < b$ yields $|q - q'| < 1$. The only possibility hence is that $|q - q'| < 0$, proving $q = q'$ and hence $r = r'$. $\square$

The Algorithm holds if $b < 0$, taking absolute value of b.

Divisibility

An integer a is said to be divisible by an integer $b \neq 0$ if there exists some ingeter c such that $a = bc$. We express it as "b divides a" or, $b|a$.

Some immediate observations are:

- $a|0, 1|a, a|a$.
- $a|b$, $c|d$ implies $ac|bd$.
- $a|b$ and $a|c$ implies $a|(bx + cy)$ for arbitrary integers x and y.

Greatest Common Divisor(gcd)

Definition: Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $gcd(a, b)$ or, (a, b) is the positive integer d satisfying the following :

(i) $d|a$ and $d|b$.

(ii) If $c|a$ and $c|b$, then $c \leq d$ and $c|d$.

Result: Given integers a and b, not both of which are zero, there exist integers x and y such that $gcd(a, b) = ax + by$.

Proof. Let $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. We show that S is non-empty and hence it must have a least element. We show that the least element in the set S is actually the gcd of a and b. $\square$

Definition: Two integers a and b, not both zero, are said to be **relatively prime** whenever $gcd(a, b) = 1$.

Least Common Multiple(lcm)

Definition: Let $a, b \in \mathbb{Z}$. m is called the lowest common multiple [lcm], written as $[a, b]$ if $a|m, b|m$ and if c be any number such that $a|c$ and $b|c$, $c > 0$ then $m|c$.

Result: Given integers a and b, not both of which are zero, $[a, b](a, b) = |ab|$.

3 Problems

1. Prove that if $gcd(a,b) = d$ then $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

   Proof. Since $gcd(a,b) = d$, $d|a$ and $d|b$. Then $a = dx, b = dy$. Now there exists integers u, v such that $au + bv = d$, i.e., $\frac{a}{d}u + \frac{b}{d}v = 1$. This implies the result. □

2. Prove the following:

(a) If $a|bc$ and $gcd(a,b) = 1$ then $a|c$.

(b) If $a|c$ and $b|c$ with $gcd(a,b) = 1$, then $ab|c$.

(c) If a is prime to b and a is prime to c then a is prime to bc.

(d) If a is prime to b then $a + b$ is prime to ab.

(e) If a is prime to b then a^2 is prime to b^2.

3. Prove that the product of any three consecutive integers is divisible by 6.

4. Show that $(a, a+2)$ is either 1 or, 2 for any integer a.

5. If $k > 0$ then prove that $gcd(ka, kb) = k.gcd(a,b)$.

   Proof. Let $d = gcd(a,b)$. Then there exist integers u and v such that $d = au+bv$. Also $d|a, d|b \Rightarrow kd|ka, kd|kb$. Thus, kd is a common divisor of ka and kb. Let c be a common divisor of ka and kb. Then $c|ka, c|kb$ and $ka = cx, kb = cy$, for some integers x, y. Now $kd = k(au + bv) = cxu + cyv = c(xu + yv)$ implies $c|kd$. Hence kd is the gcd. □

6. If a, b are positive integers such that $gcd(a,b) = 1$, then show that $gcd(a+b, a-b) = 1$ or, 2.

   Proof. Let $gcd(a+b, a-b) = d$. Then $d|a+b$ and $d|a-b$. Hence $d|2a$ and $d|2b$. Hence d is a common divisor of $2a$ and $2b$. Now, $gcd(2a, 2b) = 2gcd(a,b) = 2$. Therefore, $d|2$. This implies $d = 1$ or, 2. □

   All unsolved problems are done in class

4 Euclidean Algorithm

It is an efficient method of finding the greatest common divisor of two given integers by repeated application of division algorithm. Let a and b be two integres whose gcd has to be calculated. Since $gcd(a, b) = gcd(|a|, |b|)$, it is enough to assume a, b as positive. By division algorithm, $a = bq_1 + r_1$, $0 \leq r_1 < b$. If it happens that $r_1 = 0$, then $gcd = b$. If not, by division algorithm, $b = r_1q_2 + r_2$, $0 \leq r_2 < r_1$. If $r_2 = 0$, process stops. Otherwise, division algorithm is repeated. Like this, if we continue, we reach $r_{n-1} = q_nr_n + 0$. We apply an important result here that, if $a = bq + r$, then $gcd(a, b) = gcd(b, r)$. Using this result, we get $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = ... = gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$.

5 Problems

1. Calculate $gcd(12378, 3054)$ and express it as $12378u + 3054v$, where u, v are integers.

   $12378 = 4 \cdot 3054 + 162$, $3054 = 18 \cdot 162 + 138$, $162 = 1 \cdot 138 + 24$, $138 = 5 \cdot 24 + 18$, $24 = 1 \cdot 18 + 6$, $18 = 3 \cdot 6 + 0$. Hence $gcd(12378, 3054) = 6$. Again,
   6=24-18

   =24-(138-5 ·24)

   $= 6.24 - 138$

   $= 6(162 - 138) - 138$

   $= 6 \cdot 162 - 7 \cdot 138$

   $= 6 \cdot 162 - 7(3054 - 18 \cdot 162)$

   $= 132 \cdot 162 - 7 \cdot 3054$

   $= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054$

   $= 132 \cdot 12378 + (-535)3054.$

   Hence, $u = 132$ and $v = -535$.

2. Find two integers u, v satisfying $54u + 24v = 30$.

3. Use Euclidean Algorithm to calculate $gcd(a, b)$ and hence express it as $au + bv$ for some $u, v \in \mathbb{Z}$ for the following a, b :

(a) $gcd(42823, 6409)$

(b) $gcd(1819, 3587)$

6 Linear Diophantine Equations

An equation in one or more unknowns which is to be solved in integers is said to be a Diophantine equation, named after a Greek mathematician Diophantus. A given linear Diophantine equation of the form $ax + by = c$ may have many solutions in integers or may not have even a single solution. For example, $2x + 4y = 6$ has many solutions in integers, say $x = 1, y = 1$, $x = 5, y = -1$,.... Whereas, $2x + 4y = 3$ cannot have a solution in integers.

The condition for solvability is stated as : the linear Diophantine equation $ax+by = c$ admits a solution if and only if $d|c$, where $d = gcd(a, b)$. We know that there are integers r and s for which $a = dr$ and $b = ds$. If a solution of $ax + by = c$ exists, so that $ax_0+by_0 = c$ for suitable x_0 and y_0, then $c = ax_0+by_0 = drx_0+dsy_0 = d(rx_0+sy_0)$ which implies that $d|c$. Conversely, assume that $d|c$, say $c = dt$. Using result from gcd, we have $d = au + bv$. This implies, $c = dt = atu + btv$. Thus, tu and tv are solutions to the equation. If x_0, y_0 is any particular solution of this equation then all other solutions are given by $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$, where t is an arbitrary integer.

7 Prime Numbers

Definition: An integer $p > 1$ is called a prime number, if its only positive divisors are 1 and p.

A composite number has at least one prime divisor. (*Proof done in class*)

Fundamental Theorem of Arithmetic: Every positive integer $n > 1$ is either prime or a product of primes; this representation is unique.

Canonical form: Any positive integer $n > 1$ can be written as $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, where p_i's are primes, α_i's are positive integers.

Example: $4725 = 3^3.5^2.7$, $7460 = 2^3.3^2.5.7^2$.

Euclid Theorem: The number of primes is infinite.

Proof. Let us suppose that the number of primes is finite and let p be the greatest prime. We write the primes $2, 3, 5, 7, ...p$ in succession and p is the last in the enumeration. The product $2.3.5.7...p$ in which every prime appears only once is divisible by each prime and therefore, the number $(2.3.5.7...p) + 1$ is not divisible by any of the primes $2, 3, 5, 7, ...p$. Hence the number $(2.3.5.7...p) + 1$ is either itself a prime or being a composite number, is divisible by a prime number greater than p. In both the cases p fails to be the greatest prime and thus,primes are infinite. □

Test for primality: If a positive integer a be composite, then $a = bc$ for integers b, c satisfying $1 < b < a$, $1 < c < a$. Then $b^2 \leq bc = a$ and this implies $b \leq \sqrt{a}$. Since $b > 1$, b has at least one prime divisor p and $p \leq b \leq \sqrt{a}$. In testing primality of a positive integer n, it is sufficient to divide n by primes not exceeding $\sqrt{n}$. In order to determine all primes ≤ 30, the method is to strike all multiples of $2, 3, 5$ from the table of integers 2 to 30, since 5 is the largest prime $\leq \sqrt{30}$.

The number of positive divisors of a positive integer: Let n be a positive integer greater than 1. Then n can be expressed as $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ where prime p_i are distinct with $p_1 < p_2 < ... < p_r$ and α_i's are positive integers. Then total number of positive divisors of a positive integer is denoted by $\tau(n)$ and

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_r + 1).$$

Result: The total number of positive divisors of a positive integer n is odd if and only if n is a perfect square.

The sum of all positive divisors of a positive integer: Let n be a positive integer greater than 1. Then n can be expressed as $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ where prime p_i are distinct with $p_1 < p_2 < ... < p_r$ and α_i's are positive integers. Then total number of positive divisors of a positive integer is denoted by $\sigma(n)$ and

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}.\frac{p_2^{\alpha_2+1}-1}{p_2-1}...\frac{p_r^{\alpha_r+1}-1}{p_r-1}.$$

Proof. Each term of the product $(1+p_1+{p_1}^2+...+{p_1}^{\alpha_1})(1+p_2+{p_2}^2+...+{p_2}^{\alpha_2})...(1+p_r+{p_r}^2+...+{p_r}^{\alpha_r})$ is a positive divisor of n and conversely. Hence we get $\tau(n)$ and $\sigma(n)$. □

8 Problems

1. Find the general solution in integers of the equation $7x + 11y = 1$.
2. Find the general solution in integers of the equation $5x + 12y = 80$.
3. Find the general solution in integers of the equation $172x + 20y = 1000$.
4. Find the general solution in integers of the equation $56x + 72y = 40$.
5. Find the general solution in integers of the equation $24x + 138y = 18$.
6. Find the general solution in integers of the equation $221x + 35y = 11$.
7. Find $\tau(360)$, $\sigma(360)$, $\tau(1482)$, $\sigma(1225)$, $\tau(1932)$, $\sigma(7007)$.

9 Congruence

Definition: Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m if $a-b$ is divisible by m. Symbolically this is expressed as $a \equiv b(\mod m)$. For example let $m = 7$. Then $3 \equiv 24(\mod 7)$, $-31 \equiv 11(\mod 7)$, etc.

Given an integer a, let q and r be its quotient and remainder upon division by m, such that $a = qm + r$, $0 \le r < m$. Then by definition of congruence, $a \equiv r(\mod m)$. Because there are m choices of r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, ..., m-1$; the set of these integers is called the set of *least nonnegative residues modulo m*. The whole set of integers is divided into m distinct and disjoint subsets, called the *residue classes modulo m*, denoted by, $\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}$.

Properties: Let $m > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

1. $a \equiv a(\mod m)$.

2. If $a \equiv b(\mod m)$ then $b \equiv a(\mod m)$.

3. If $a \equiv b(\mod m)$ and $b \equiv c(\mod m)$ then $a \equiv c(\mod m)$.

4. If $a \equiv b(\mod m)$ then $a + c \equiv (b + c)(\mod m)$ and $ac \equiv bc(\mod m)$.

5. If $a \equiv b(\mod m)$ and $c \equiv d(\mod m)$, then $a+c \equiv (b+d)(\mod m)$ and $ac \equiv bd(\mod m)$.

6. If $a \equiv b(\mod m)$ then $a^k \equiv b^k(\mod m)$ for any positive integer k.(Proof by principle of mathematical induction)

Problem: If $ax \equiv ay(\mod m)$ and a is prime to m then $x \equiv y(\mod m)$.

Proof. $ax - ay = km$ implies $x - y = \frac{km}{a}$. Now, since $x - y$ is an integer, $a|km$. Since $a \nmid m$ hence $a|k$ and $k = ar$. Thus, $x - y = rm$. □

Result: If $d = gcd(a, m)$, then $ax \equiv ay(\mod m) \Leftrightarrow x \equiv y(\mod \frac{m}{d})$.
Result: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ be a polynomial with integer coefficients a_i. If $a \equiv b(\mod m)$ then $f(a) \equiv f(b)(\mod m)$.

10 Linear Congruence

An equation of the form $ax \equiv b(\mod m)$ is called a linear congruence and by a solution of such equation we mean an integer c such that $ac \equiv b(\mod m)$.
Result: The linear congruence $ax \equiv b(\mod m)$ has a solution if and only if $d|b$, where $d = gcd(a, m)$. If $d|b$ then it has d mutually incongruent solutions modulo m.

The above result can be expressed from the concept of linear diophantine equations. $ax \equiv b(\mod m) \Rightarrow m|(ax - b) \Rightarrow ax - b = mr, r \in \mathbb{Z} \Rightarrow ax + my = b$(taking $y = -r$). Thus, the result follows. Moreover, if x_0, y_0 is a particular solution of the equation then general solution is $x = x_0 + \frac{m}{d}t$, $y = y_0 - \frac{a}{d}t$. Taking $t = 0, 1, 2, ..., d-1$ will give the solutions that are incongruent modulo m. Since, $x = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(dq + r) \equiv (x_0 + \frac{m}{d}r)(\mod m)$, $0 \leq r \leq (d-1)$.

Result: If $gcd(a, m) = 1$, then the linear congruence $ax \equiv b(\mod m)$ has a unique solution modulo m.

11 Chinese Remainder Theorem

Let $n_1, n_2, ..., n_r$ be positive integers such that $gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1(\text{mod } n_1)$$
$$x \equiv a_2(\text{mod } n_2)$$
$$.$$
$$.$$
$$.$$
$$x \equiv a_r(\text{mod } n_r)$$

has a simultaneous solution, which is unique modulo the integer $n_1, n_2, ..., n_r$.

Problem: Solve the system of linear congruences $x \equiv 1(\mod 3)$, $x \equiv 2(\mod 5)$,$x \equiv 3(\mod 7)$.

3, 5, 7 are pairwise prime to each other. Let $N = 3.5.7 = 105$. Let $N_1 = \frac{N}{3} = 35$, $N_2 = \frac{N}{5} = 21$, $N_3 = \frac{N}{7} = 15$. Then $gcd(N_1, 3) = gcd(N_2, 5) = gcd(N_3, 7) = 1$. This implies the linear congruence $35x \equiv 1(\mod 3)$ has a unique solution. The solution is $x \equiv 2(\mod 3)$. Similarly, $21x \equiv 1(\mod 5)$ has a unique solution $x \equiv 1(\mod 5)$. And also, $15x \equiv 1(\mod 7)$ has a unique solution $x \equiv 1(\mod 7)$.

$\bar{x} = 1(35.2) + 2(21.1) + 3(15.1) = 157$. The solution of the given system is $x \equiv 157(\mod 105)$, which is $x \equiv 52(\mod 105)$.

12 Phi function

The function $\phi(n)$ is defined for all positive integers as the number of positive integers less than n and prime to n, and $\phi(1) = 1$.

If p is prime then $\phi(p) = p - 1$.

If p be prime and $k \in \mathbb{Z}^+$, $\phi(p^k) = p^k(1 - \frac{1}{p})$.

If $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, then $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_r})$

13 Fermat's Theorem

If p be a prime and p is not a divisor of a, then $a^{p-1} \equiv 1(\mod p)$.

Proof. Let us consider the integers $a, 2a, 3a, ..., (p-1)a$. None of these are divisible by p. No two of these are congruent modulo p. Hence the integers $a, 2a, 3a, ..., (p-1)a$ are congruent to $1, 2, 3, ..., p-1$ modulo p, not taken in the same order. Taking product, $a.2a.3a...(p-1)a \equiv 1.2.3...(p-1)(\mathrm{mod}\ p)$. This proves the result. □

14 Euler's Theorem

If n be a prime and a is prime to n, then $a^{\phi(n)} \equiv 1(\mod n)$.

15 Wilson's Theorem

If p be a prime then $(p-1)! + 1 \equiv 0(\mod p)$.

16 Problems

1. Find the least positive residues in $3^{36}(\mod 77)$.

2. Use the theory of congruences to prove that $7|2^{5n+3} + 5^{2n+3}$ for all $n \geq 1$.

3. Prove that $19^{20} \equiv 1(\mod 181)$.

4. Find the remainder when $1! + 2! + 3! + ... + 50!$ is divided by 15.

5. Solve the linear congruence $15x \equiv 9(\mod 18)$.

6. Find the number of integers less than n and prime to n, when $n = 256, 324, 900$.

7. Find the least positive residue in $2^{41}(\mod 23)$.

8. If p be a prime > 2, prove that $1^p + 2^p + ... + (p-1)^p \equiv 0(\mod p)$.

9. Prove that the eighth power of any integer is of the form $17k$ or $17k \pm 1$.

10. Show that $a^{12} - b^{12}$ is divisible by 91 if a and b are both prime to 91.

11. If n is a prime > 7 prove that $n^6 - n$ is divisible by 504.

12. Show that $4(29)! + 5!$ is divisible by 31.

13. Find the units digits of 7^{7^7}.

14. Prove that every year, including any leap year, has at least one Friday 13th.