1st lecture

Note Title 21-01-2022

we are working only with set of integers

$$\mathbb{Z} = \{ \cdots -2, -1, 0, 1, 2, \cdots \}.$$

a $\quad b = aq.$ $\quad$ $a \mid b$

a divides b $\quad a \mid b.$

a does not divide b $\quad a \nmid b.$

Thm: For all $a, b, c \in \mathbb{Z}$ we have

1. $a \mid a$, $1 \mid a$, & $a \mid 0$.
2. $0 \mid a$ iff $a = 0$
3. $a \mid b$ iff $-a \mid b$ iff $a \mid (-b)$.
4. $a \mid b$ & $a \mid c$ $\Rightarrow$ $a \mid (b + c)$
5. $a \mid b$ & $b \mid c$ $\Rightarrow$ $a \mid c$

Rmk: If $a \mid b$ then $-a \mid b$ it is enough to consider +ve divisors.

simple properties

(1) $\forall\ a, b \in \mathbb{Z}$ $\quad a \mid b \ \& \ b \mid a \iff a = \pm b$

$a \mid b \Rightarrow b = aq \qquad q \in \mathbb{Z}$

$b \mid a \Rightarrow a = br \qquad r \in \mathbb{Z}$

$b = brq = b(rq)$ now as $q \& r \in \mathbb{Z}$

$\Rightarrow rq = 1 \quad \Rightarrow r = \pm 1 \ , \ q = \pm 1$

$\therefore \quad b = aq \Rightarrow b = \pm a.$

gcd = 1

$a \mid 1 \Rightarrow a = \pm 1$

(2) If $a|b$ then every divisor of a divides b.
i.e. $a|b$ & $c|a \Rightarrow c|b$

(3) $a|b_1$ & $a|b_2$ then $a|b_1+b_2$

$a|b_1, a|b_2 \text{ --- } a|b_n \Rightarrow a|b_1+b_2+\text{---}+b_n$.

$a|c_1b_1+c_2b_2+\text{---}+c_nb_n$.

Primes & composite numbers

let $n \in \mathbb{Z}$ $\quad 1/n$ & n/n.

If no other tre integer divides 'n' then n is called Prime.

If $n > 1$ & n is not Prime then n is called composite number.

Rmk: 0 & 1 are not consider prime or composites.

Composite number means $n = a \cdot b$ $\quad 1 < a < n$, $1 < b < n$.

2, 3, 5, ~~7, 11, 13~~, 17, 19, 23, 29.

notation. p q

p_n – n^{th} prime

$p_1 = 2$

$p_2 = 3$

$p_3 = 5$

⋮

Fundamental thm of Arithmetic:

Thm: Every integer $n > 1$ can be expressed as a product of Primes.

Pf: we can give straightforward proof.

Let $n \in \mathbb{Z}$ +ve integer > 1.

If n is prime then we are done. $n = p$

If n is not a prime then $n = n_1 \cdot n_2$. $1 < n_1 < n$. $1 < n_2 < n$.

If n_1 is prime then ignore n_1 & look at n_2.

If n_1 is not prime then $n_1 = n_3 \cdot n_4$. $1 < n_3 < n_1$, $1 < n_4 < n_1$

again consider n_3. If n_3 is prime then look at n_4 & ignore n_3 - -
continue this process.
notice that this process should terminate because the factors are becoming smaller & smaller than n.
& each factor is >1
$\therefore$ we can write $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$.
they need not be distinct primes

$$\therefore n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}.$$

$2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 2 \cdot 3 \cdot$
$n = 2^2 3^2 5^1 7^1 - -$

Rmk: This is called canonical factoring of n. This repn is unique in the sense that if we write another repn of n as product of primes.

// for $\mathbb{Z}$ unique factorization looks trivial but when you start studying alg integers or algebraic numbers this becomes nontrivial.

alg number α is called alg number if α satisfies some poly $p(x)$ over $\mathbb{Q}$.

$\alpha = \sqrt{2}$ $\quad x^2 - 2 = 0$ $\quad \sqrt{2}$ is alg number.

alg integer means that poly has integer coeffs.

$\frac{1+\sqrt{7}}{2}$ is also alg number.

$x^n + y^n = z^n$ Fermats last thm.

// simple example of

class $C = \{$ ~~set of~~ all the even integers $\}$.

$C = \{2, 4, 6, 8, 10, 12, 14, 16 - - - - \}$

Note that C is closed under multiplication

That means $a \in C$ $b \in C$ then $a \cdot b \in C$.

Just concentrate on C & forget about all other numbers.

look at $24 = 4 \cdot 6$ $\therefore$ 24 is composite number in C.

What about 10? 10 is actually prime in C since 10 can not be written as product of two elents of C.

4, 8, 12, 16, --- are composite numbers in C

2, 6, 10, 14, 18 --- are prime numbers in C.

Now look at $60 = 6 \times 10 = 30 \times 2$.

60 has two different reprs as product of primes

$\therefore$ C does not have unique factorization.

Ex: consider class $C = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$

$1 + 2\sqrt{-6}$, $100 + 3\sqrt{-6}$, $-5 + 7\sqrt{-6} \in C$

in fact C is also closed under multiplication.

$$(a + b\sqrt{-6})(c + d\sqrt{-6}) = (ac - 6bd) + \sqrt{-6}(ad + bc)$$
$$= R + S\sqrt{-6} \in C.$$

closed under addition. $(a + b\sqrt{-6}) + (c + d\sqrt{-6})$

$$= (a + c) + (b + d)\sqrt{-6} = R + S\sqrt{-6}$$

$\mathbb{Z} \subset C$

$a + b\sqrt{-6}$ $b = 0$ $a \in \mathbb{Z}$

$10 = 2 \cdot 5 = (2+\sqrt{-6})(2-\sqrt{-6})$

in fact 2, 5, $2+\sqrt{-6}$, $2-\sqrt{-6}$ all are primes in $\mathbb{C}$.

$N(a+b\sqrt{-6}) = (a+b\sqrt{-6})(a-b\sqrt{-6})$

$= a^2 + 6b^2$.

$N(5) = 5^2 = 25$.

$a \mid b$

$N(a) \mid N(b)$.

$\alpha = \beta\gamma$

$N(\alpha) = N(\beta) \cdot N(\gamma)$

of $5 = (a+b\sqrt{-6})(c+d\sqrt{-6})$

$N(5) = N(\ )\ N(\ )$

$25 = (a^2+6b^2)(c^2+6d^2)$

$\geq 6 \cdot 6$

$25 > 36$ contradiction $\Rightarrow$ 5 is prime.

$\therefore$ in $\mathbb{C}$, 10 has two presentations as product of primes

∴ unique factorization fails in $C = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\}$.

we will prove uniqueness of fund thm of arithmetic later.

division algorithm:

$77 = 12 \times 6 + 5 \qquad 0 < 5 < 12.$

Thm (division algorithm)

Let a & b be any two integers with $b > 0$ then

$\exists$ unique integers q & r s.t. $a = bq + r \quad 0 \leq r < b$.

Pf: Consider infinite sequence of multiples of b

$$\cdots -3b, -2b, -b, 0, b, 2b, 3b, 4b \cdots$$

obviously $a = bq$ for some $q \in \mathbb{Z}$ or

a must be in between two consecutive multiples of b. i.e. $bq < a < b(q+1)$

$$0 < a - bq < b.$$

write $a - bq = r$. then $a = bq + r$ & $0 < r < b$.

$\therefore$ existence is done.

Now uniqueness: suppose they are not unique.

$a = bq + r \quad 0 \le r < b$

$a = bq_1 + r_1 \quad 0 \le r_1 < b$

for some integers q, r, q_1 & r_1

$\therefore bq + r = bq_1 + r_1$

$b(q - q_1) = r_1 - r$. $\Rightarrow$ b divides $(r_1 - r)$

ie. $b \mid (r_1 - r)$

only possibility is $r_1 - r$ is smaller than b.

$r_1 - r = 0 \Rightarrow r_1 = r$.

this also gives us $q = q_1$

$\therefore$ r & q are unique.

Rmk: In this division algorithm remainder is always +ve & strictly less than b.
but one can write another kind of division algorithm where $r < \frac{b}{2}$.

Ex $a = 37$ $b = 8$. $q = 4$, $r = 5$.

$37 = 8 \times 4 + 5$ $0 < 5 < 8$ $r > \frac{b}{2}$ $\frac{b}{2} = 4$.

what we can do is take $q = q + 1$. i.e. $q = 5$

$37 = 8 \times 5 + (-3)$ $\quad |-3| < \frac{8}{2}$.

Division algorithm for minimal remainder

Thm: a, b are any two integers with $b > 0$

then $\exists\ q, R$ s.t. $a = bq + eR$ $\quad 0 < R < \frac{b}{2}$

$e = +1$ or -1

Proof H.W.

Applications:

(1) Every integer is ~~of the form~~

(1) $3q$ or $3q+1$ or $3q+2$.

② $4q$, or $4q \pm 1$ or $4q \pm 2$.

③ $5q$ or $5q \pm 1$ or $5q \pm 2$.

Pf: ① $b = 3$ here. then for any $a \in \mathbb{Z}$

by minimal division algorithm

$a = 3q + eR$ $\quad 0 < R < \frac{b}{2}$ $\quad b = 3$

$0 < R < \frac{3}{2}$ $\quad e = +1$ or -1.

$0 < R < 1$

$R = 0$ or 1

$\therefore a = 3q$.

or $a = 3q + 1$

or $a = 3q - 1$.

$3q - 1 = 3(q-1) + 3 - 1$

$= 3t + 2$ //

any integer can be written as $3q$, or $3q+1$ or $3q+2$.

Similarly we can show any int looks like $2q$ or $2q+1$

$\therefore$ we can use normal division algorithm & show

$=$ every square of an integer is either $4q$ or $4q+1$

Pf: ~~every~~ $a \in \mathbb{Z}$ then $a = 2q$ or $a = 2q+1$

$a^2 = 4q^2$ or $a^2 = 4q^2 + 4q + 1$

$= 4Q$ $= 4Q + 1$

Ex: one of every 3 consecutive integers is divisible by 3.

Pf: any 3 consecutive integers can be written as a, $a+1$ & $a+2$.

now as we have seen a will look like $3q$, $3q+1$, $3q+2$

if $a = 3q$ then $3 \mid a$. done

if $a = 3q+1$, $a+1 = 3q+2$, $a+2 = 3q+3 \Rightarrow 3 \mid a+2$. done

if $a = 3q+2$ then $a+1 = 3q+3 \Rightarrow 3 \mid a+1$. done.

Thm

· Product of any 3 consecutive integers is divisible by 3!

pf: $a(a+1)(a+2)$

// Product of n consecutive integers is divisible by $n!$

---

gcd [greatest common divisor]

$a_1, a_2, \ldots a_n$ & gf $d|a_1$ $d|a_2$ $\ldots$ $d|a_n$

d is common divisor.

$d_1, d_2, d_3 \ldots$ common divisors of $a_1, a_2 \ldots a_n$.

(b, c) = gcd of b & c.

Thm: If $g = (b, c)$ then $\exists$ integers x_0 & y_0 s.t.

$$g = bx_0 + cy_0$$