Number Theory 1 to 7 Revision

05 October 2023 17:56

$m|n \iff \frac{n}{m} \in \mathbb{Z}$

$x|y\ ,\ y|z \Rightarrow x|z$

$\frac{z}{x} = \frac{y}{x}\ \frac{z}{y} \in \mathbb{Z}$

$x|x\ ,\ 1|x,\ x|0$

$x|y \Rightarrow y = 0$ or $|x| \leq |y|$

$y = kx \Rightarrow$ if $k = 0$ then $y = 0$. If $k \neq 0$ then $k \geq 1,\ k \leq -1$

$|kx| \geq |x|$ $\qquad |k| \geq 1$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$N = \{ \underbrace{p_1, p_1, \ldots, p_1}_{\alpha_1}, \ldots, \underbrace{p_n, p_n, \ldots, p_n}_{\alpha_n} \}$

If $z|x,y$ then $z|ax+by$ for any $a, b \in \mathbb{Z}$

$x|y$ iff $xz|yz$ for some non-zero integer z

$x|y \Rightarrow x|yz$ for any $z \in \mathbb{Z}$

<u>Fundamental Theorem of Arithmatic</u>

Any natural number greater than 1 has a unique prime factorization upto order

$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_n^{\alpha_n}$ → p_i's are primes

If ($n = q_1^{\beta_1} q_2^{\beta_2} q_3^{\beta_3} \cdots q_n^{\beta_n}$ → q_i's are primes) exists

then $p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_n = q_n$

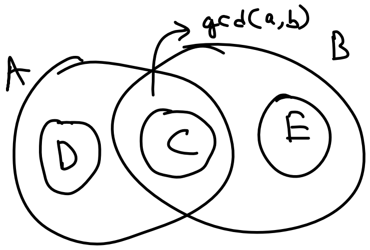
$\alpha_1 = \beta_1,\ \alpha_2 = \beta_2,\ \ldots\ldots,\ \alpha_n = \beta_n$

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ $\quad A = \{ p_1, p_1, \cdots p_1, \cdots, p_n, p_n, \cdots p_n \}$

$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}$ $\quad B = \{ q_1, q_2, \cdots q_1, \cdots, q_n, q_n, \cdots, q_n \}$

$GCD(a,b) = A \cap B$

$LCM(a,b) = A \cup B$



$c \mid a$ and $c \mid b \Rightarrow c \mid gcd(a,b)$ then C

$d \mid a$ but $gcd(d,b) = 1$ then D

$e \mid b$ but $gcd(e,a) = 1$ then E

$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$

$$gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \, p_2^{\min(\alpha_2,\beta_2)} \cdots p_n^{\min(\alpha_n,\beta_n)}$$

$$lcm(a,b) = p_1^{\max(\alpha_1,\beta_1)} \, p_2^{\max(\alpha_2,\beta_2)} \cdots p_n^{\max(\alpha_n,\beta_n)}$$

(Euclid) Prove that there are infinitely many primes

$\Rightarrow$ Suppose there are finitely many primes and those are $\{p_1, p_2, \cdots, p_k\}$

Let us define a number $N = p_1 p_2 p_3 \cdots p_k + 1$

Any number which not divisible by any prime less that itself is a prime number. $N > 1$ and by Fundamental Theorem of Arithmetic it must be divided by a prime

$p_1 \nmid N$ as $p_1 \mid (N-1)$

$p_2 \nmid N$ as $p_2 \mid (N-1)$

$\vdots$

$p_k \nmid N$ as $p_k \mid (N-1)$

Thus N has a divisor as prime $\neq p_1$ or p_2 or $\cdots$ or p_k

$\Rightarrow\Leftarrow$ Contradiction

Thus ...

$\Rightarrow\Leftarrow$ Contradiction

Thus our assumption is false

Hence there are infinitely many primes

Q Prove that $\sqrt{2}$ is irrational

Ans:— Suppose $\sqrt{2} = \frac{p}{q}$ $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$

$$2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2 \Rightarrow 2 \mid p^2 \Rightarrow 2 \mid p \Rightarrow 4 \mid p^2$$

$$4 \mid 2q^2 \Rightarrow 2 \mid q^2 \Rightarrow 2 \mid q \longrightarrow \gcd(p, q) \neq 1 \Rightarrow\Leftarrow$$

Hence $\sqrt{2} \neq \frac{p}{q}$ form for any $p, q \in \mathbb{Z}$.

Q) Find integers x, y such that $1110x + 1011y = 3$ (HomeWork)

(HomeWork) $\rightarrow$ Read

Euclid's Extended Algorithm :—

We have, a, b and we need x and y such that $ax + by = 1$

$$\gcd(b \pmod a, a, x, y)$$

Each step we need to calculate

If $a = 0$,
$x = 0$
$y = 1$

Otherwise, $x = y - \left\lfloor \frac{b}{a} \right\rfloor \times x$
$y = x$

$\lfloor x \rfloor \Rightarrow$ floor of x

$\Rightarrow$ largest integer $\leq x$

$\lfloor 2.5 \rfloor = 2$

$\lfloor 2 \rfloor = 2$ $\lfloor 2.999 \rfloor = 2$

$\lfloor 3.1 \rfloor = 3$

$\lfloor 0.00 \rfloor = 0$

$\lfloor -1.00 \rfloor = -1$

$\lfloor 0.00 \rfloor = 0$

$\lfloor -1.00 \rfloor = -1$

$\lfloor -1.1 \rfloor = -2$

Q) $21x + 13y = 1$ Find x, y.

Ans:-

r_i	x_i	y_i	q_i
21	1	0	
13	0	1	1
8	1	-1	1
5	-1	2	1
3	2	-3	1
2	-3	5	1
1	5	-8	