

Q) Which numbers have precisely 1 non-trivial (positive) divisors?

A) The squares of primes.

It is easy to "read off" the gcd of two numbers if we have them in factored form.

$$\gcd(2^{11} \cdot 3^2 \cdot 5 \cdot 7^3, 2^2 \cdot 3 \cdot 7^{13}) = 2^2 \cdot 3 \cdot 7^3$$

In general, with p_j running through all the primes and $a_j, b_j \geq 0$ (only finitely many non-zero)

$$\gcd\left(\prod_j p_j^{a_j}, \prod_j p_j^{b_j}\right) = \prod_j p_j^{\min(a_j, b_j)}$$

Q2) (prob sheet 2)

$a, b, c \geq 1$

a) If $ab|ac$ then $b|c$

Suppose $ab|ac$ and $b \nmid c$. Then we use division with remainder to get $c = qb + r$, $q \in \mathbb{Z}$, $0 < r < b$

Hence (mult. by a) we get $ac = qab + ar$

By ass., ab divides LHS, hence also ar , in particular $ab \leq ar$

Contradiction of $a0 < ar < ab$

2(b) If $b^2|c^3$ then $b|c$

Not true... by counter example ($b=8, c=4$)

c) $\gcd(a, b)^2 = \gcd(a^2, b^2)$

First Proof (using Q6a) $\gcd(an, bn) = n \gcd(a, b)$

Put $d = \gcd(a, b)$

Since $d|a$ and $d|b$, the integers $\frac{a}{d}$ and $\frac{b}{d}$ satisfy $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

From Q1b deduce $\gcd\left(\left(\frac{a}{d}\right)^2, \left(\frac{b}{d}\right)^2\right) = 1$

Applying Q6a again, we get $\gcd(a^2, b^2) = d^2$

Second proof using the above products...

6a)

Proof 1: use Q5a

for $a, b \geq 1$ set $S(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\}$ then $\gcd(a, b)$ is the smallest positive element in $S(a, b)$

$$= \min\{ax + by > 0 \mid x, y \in \mathbb{Z}\}$$

Now $\gcd(an, bn) = \min\{anx + bny > 0 \mid x, y \in \mathbb{Z}\}$

$$= n \cdot \min\{ax + by > 0 \mid x, y \in \mathbb{Z}\} = n \cdot \gcd(a, b)$$

b) if $m|a$ and $m|b$ then $m|\gcd(a, b)$

write $a = mr$, $b = ms$

then $\gcd(a, b) = ax + by$ for some $x, y \in \mathbb{Z}$

$$= mrx + msy$$

$$= m(rx + sy)$$

"Complementing" Notion

Definition:

The least common multiple of $a, b \in \mathbb{Z}$ is the smallest positive integer l for which $a|l$ and $b|l$

In factored form

$$\text{lcm}(a,b) = \prod_j p_j^{\max(\alpha_j, \beta_j)}$$

Important Property

$$\text{lcm}(a,b) \cdot \text{gcd}(a,b) = ab$$

Proof

$d = \text{gcd}(a,b)$ divides a, b hence $l = \frac{ab}{d}$ is an integer.

l is a multiple of both a and b

Consider any c s.t. $a|c$ and $b|c$

$$c = ar = bs$$

$$\text{Then } \frac{c}{l} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{cx}{b} + \frac{cy}{a} = sx + ry \in \mathbb{Z}$$

Primes of the form $6n-1$: \exists infinitely many

-only one type of $6n-3$: equal to 3.

-multiply primes of the type $6n+1$ together and you get the same type.

Now...