Integers & Division - 1

Monday, November 2, 2020 10:51 AM

(i) If $a|b$ and $a|c$, then $a | b+c$.

Suppose $a|b$ and $a|c$. Then from the defn. of divisibility it follows that there are integers s & t with $b = a.s$ and $c = a.t$.

Hence, $b+c = a.s + a.t = a(\underline{s+t})$

This is also an integer.

Therefore, $a | b+c$. This establishes part (i) of the theorem.

(ii) if $a|b$, then $a | bc$ for all integers c.

As $b = a.s$, we have $b.c = acs$.

Therefore, a divides bc. This establishes part (ii) of the theorem.

(iii) if $a|b$ and $b|c$, then $a|c$.

Suppose $a|b$ and $b|c$. Therefore, using the definition of divisibility it follows that $b = a.s$ and $c = \underline{b}.t$ for some integers s & t.

Hence, $c = (as).t = a(st)$. Therefore, $a|c$.

This establishes part (iii) of the theorem.

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

→ If n is composite, by the defn. of composite number, it has a factor a with $1 < a < n$. Hence, by the definition of a factor of a positive integer, we have $\underline{n = a.b}$, where b is a positive integer greater than 1. We will show $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

If $a > \sqrt{n}$ and $b > \sqrt{n}$ then $\underline{ab > \sqrt{n}.\sqrt{n} > n}$, which is a contradiction. Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Because a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

Ex: Show that $\underline{101}$ is prime.

→ The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because, 101 is not divisible by 2, 3, 5, and 7, it follows that 101 is prime.

n $\quad$ $n-1$ $\quad$ $\sqrt{n}$

Theorem: There are infinitely many primes.

Proof: Suppose there are finitely many primes, let's say n. We denote them as $p_1, p_2, \ldots, p_n$

Now, we construct a new number:

$p = p_1 \times p_2 \times p_3 \times \ldots \times p_n + 1.$

Clearly, p is larger than any of the primes. So it doesn't equal to one of them. Since, $p_1, p_2, \ldots, p_n$ constitute all the primes, p can't be prime.

Thus, p must be divisible by at least one of our finitely many primes. But when we divide p by p_n, we get a remainder 1. That's a contradiction, So our original assumption that there are finitely many primes must be false.

Thus, there are infinitely many primes.

Theorem: Let a and b be positive integers. Then,

$ab = \gcd(a, b) . \operatorname{lcm}(a, b).$

$\rightarrow$ Let a and b can be factorized as:

$$a = p_1^{a_1} \cdot p_2^{a_2}, \cdots p_n^{a_n}$$

$$b = p_1^{b_1} \cdot p_2^{b_2}, \cdots p_n^{b_n}.$$

Product of the integers:

$$a.b = p_1^{(a_1+b_1)} \cdot p_2^{(a_2+b_2)} \cdots p_n^{(a_n+b_n)}$$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

$\therefore$ Multiplying gcd(a, b) and lcm(a, b) it follows:

$$\gcd(a,b).\operatorname{lcm}(a,b) = p_1^{\min(a_1,b_1)+\max(a_1,b_1)} + p_2^{\min(a_2,b_2)+\max(a_2,b_2)} + \cdots p_n^{\min(a_n,b_n)+\max(a_n,b_n)}$$

$$= p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdots p_n^{a_n+b_n}.$$

$$= \underline{ab}.$$

<u>Prob.</u> The given integers are 414 and 662.

Successive use of the division algorithm are:

$$\overset{x}{662} = 1.\overset{y}{414} + \overset{r}{248}.$$

$$414 = 1.248 + 166$$
$$248 = 1.166 + 82$$
$$166 = 2.82 + 2$$
$$82 = 41.\underline{\underline{2}} + \underline{0}$$

x y

$x = 2 \Rightarrow \gcd(414, 662)$ (last non-zero remainder)

Lemma: Let $a = bq + r$, where a, b, q, and r are all integers. Then $\gcd(a, b) = \gcd(b, r)$

Proof: If we can show that the common divisor of a & b are the same as the common divisor of b & r, then we will show $\gcd(a, b) = \gcd(b, r)$.

Let d divides both a and b. Then it follows that d divides $a - bq$ which is equal to r. Hence, any common divisor of a & b is also a common divisor of b & r. Likewise, suppose d divides both b and r. Then d divides $bq + r$ which is equal to a.

Hence, any common divisor of b and r is also a common divisor of a and b. Consequently. $\gcd(a,b) = \gcd(b,r)$.

Prob. Euclidean Algorithm.

$$
\begin{array}{lllll}
 & x & & y & r \\
1. & 252 & = & 1.198 & + 54 \\
2. & 198 & = & 3.54 & + 36 \\
3. & 54 & = & 1.36 & + 18 \\
4. & 36 & = & 2.18 & + 0
\end{array}
$$

Bezout's identity:

$$\boxed{18 = s \times 252 + t \times 198}$$

Using step-3 we get,

$$18 = 54 - 1.36 \quad \text{--- (1)}$$

Using step-2 we get,

$$36 = 198 - 3.54 \quad \text{--- (2)}$$

Substituting (2) in (1),

$$18 = 54 - 1.(198 - 3.54)$$

$$18 = 4.\underline{\underline{54}} - 1.198 \quad \text{--- (3)}$$

Using step-1 we get,

$$54 = 252 - 1.198, \quad \text{--- (4)}$$

$$54 = \underbrace{252 - 1 \cdot 198}_{} \longrightarrow (4)$$

Substituting (4) in (3) we get,

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198$$

$$\therefore \boxed{18 = 4 \cdot 252 - 5 \cdot 198}$$

↳ completes the solution.

with $s = 4$ and $t = -5$