Division Algorithm

Monday, January 24, 2022 12:44 PM

Recall: FTA

1] exer on FTA:

n has exactly 10 divisors.

$60 = 2^2 \cdot 3^1 \cdot 5^1$ →  $2^i \cdot 3^j \cdot 5^k \,\big|\, 60$ for $i = 0,1$, $j = 0,1$, $k = 0,1,2$

$3 \cdot 2 \cdot 2 = 12$ divisors

Sol.

$n = 512 = 2^9 \implies 2^i \mid n$ for $i = 0, \dots, 9$

$\implies$ 10 divisors

by FTA, $10 = 2 \cdot 5$

$\implies n = p^i \cdot q^j$ $\quad i = 0, 1$

$j = 0, \dots, 4$

for $p = 2,\ q = 3$ $\quad$ p, q are small primes

$n = 2^1 \cdot 3^4 = 162$ has 10 divisors

or $n = 2^4 \cdot 3^1 = 48$ has 10 divisors

2] Exer. n has exactly 35 divisors

Sol. $n = 2^6 \cdot 3^4$

$2^j \cdot 3^i \,\big|\, n$

$i \downarrow$ \ $j \leftarrow$	0	1	2	3	4	5	6
0	1	2	4	8	16	32	64
1	3						
2	9	18					
3	27	54					
4	81						n

$2^j \cdot 3^i \mid n$

0	1	2	4	8	16	32	64
1	3						
2	9	18					
3	27	54					
4	81						n

3] Exer. n has exactly 18 divisors

$18 = 2^1 \cdot 3^2$

$n = p^i \cdot q^j \cdot r^k$

HW

4] Thrm: There are infinitely many primes.

Proof: assume there are finite primes

$p_1, p_2, \dots, p_n$

let $q = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

$\Rightarrow \forall i, \; p_i \nmid q$

$\therefore$ q is prime by FTA.

5] Mersenne Primes:

a prime of the form $2^p - 1$ (for prime p) is called a Mersenne Prime, otherwise it is a Mersenne Composite.

e.g. $2^2 - 1 = 3$ ✓

$2^3 - 1 = 7$ ✓

$2^5 - 1 = 31$ ✓

$2^5 - 1 = 31$ ✓

$2^7 - 1 = 127$ ✓

$2^{11} - 1 = 2047$ not prime (23×89)

6] Thm: Number of Primes

The number of primes $\leq n$ is $\pi(n)$

$$\boxed{\pi(x) \approx \frac{n}{\ln x}}$$ by Gauss

i.e. $\displaystyle \lim_{n \to \infty} \frac{\pi(n)}{n/\ln n} = 1$

$$\frac{n}{\ln n} < \pi(n) < \frac{n}{\ln(n) - 1.084}$$

by Gauss by Lagrange

7] Division Algorithm

let $a, b \in \mathbb{Z}^+$ then there are unique integers q, r such that:

$$a = q \cdot b + r \quad \text{with} \quad 0 \leq r < b$$

q is the quotient

r is the remainder

e.g. Find q and r when

① $a = 101$, $b = 11$

$101 = 9 \cdot 11 + 2$ $\therefore$ $q = 9$, $r = 2$

① $a = 101$, $b = 11$

$101 = \underline{9} \cdot 11 + \underline{2}$ $\quad \therefore \quad q = 9$, $r = 2$

or $101 = 8 \cdot 11 + 13$ ✗ $\quad \underline{13 > 11}$

② $a = -11$, $b = 3$

$-11 = -3(3) - 2$ ✗ $\quad q = -3$, $r = -2$ ✗

$0 \leq r < b$

$-11 = -4(3) + 1$ $\quad q = -4$, $r = 1$

8] The Greatest Common Divisor (gcd)

Def^n. $\gcd(a,b)$ is the largest integer d s.t. $d \mid a$ and $d \mid b$

e.g. $\gcd(24, 36) = 12$

$\gcd(17, 22) = 1$ relatively prime / co-prime

9] How to find the $\gcd(a,b)$

by the F.T.A. let $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots p_n^{a_n}$

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

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

e.g. $\gcd(120, 36)$

$120 = 2^3 \cdot 3^1 \cdot 5^1$

$36 = 2^2 \cdot 3^2 \cdot 5^0$

$\gcd(120, 36) = 2^2 \cdot 3^1 \cdot 5^0 = 12$

10) The least Common multiple (lcm)

Def^{n}. lcm (a,b) is the smallest positive integer m s.t. $a \mid m$ and $b \mid m$

e.g. $gcd(24, 36) = 72$
$gcd(17, 22) = 17 \cdot 22$

11) How to find the lcm (a,b)

by the F.T.A. let $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots p_n^{a_n}$

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

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

$lcm(a,b) \cdot gcd(a,b)$