Primes and Greatest Common Divisors

- Primes
- Gcd, lcm
- Euclid's algorithm

Def An integer greater than 1 is called $\boxed{\text{prime}}$ if it is only divisible by 1 and itself.

A positive integer that is greater than 1 and not a prime is called $\boxed{\text{composite}}$

prime numbers $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$

THE FUNDAMENTAL THEOREM OF ARITHMETIC: Every integer gerater than 1 can be written uniquely as a prime or product of primes in a non-increasing order.

"prime factorization"

$$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$$
$$25 = 5 \cdot 5$$
$$26 = 2 \cdot 13$$

Thm: If $n > 1$ is not a prime, then it has a prime divisor less than or equal to $\sqrt{n}$.

Proof: $n = a \cdot b$

if $a > \sqrt{n}$ and $b > \sqrt{n}$ then $a \cdot b > n$ $\perp$

Thus $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

n has a divisor that does not exceed $\sqrt{n}$

(By FTA) It is either prime or it has a prime divisor less than itself

In either case n has a prime divisor $\leq \sqrt{n}$.

Ex Show that 103 is prime

check $2, 3, 5, 7,$ $\quad (11 > \sqrt{103})$

$2 \nmid 103, \quad 3 \nmid 103, \quad 5 \nmid 103, \quad 7 \nmid 103$

$\rightarrow$ thus 103 is prime

Ex Factorize 1023

$2, 3, 5, 7, 11.$

$(\sqrt{341} < 19)$

$1023 = 3 \cdot 341$

$= 3 \cdot 11 \cdot 31$

Euclid's theorem: There are infinitely many primes.

proof: Assume by the way of contradiction there are finitely many prime numbers.

$p_1, p_2, \ldots, p_n$

Let $Q = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$

By FTA either

1) Q is a prime or

2) Q can be written as a product of 2 or more prime numbers.

we reached a contradiction $\rightarrow$ Q is prime, Q is not on the list

$\Rightarrow$ There are inf. many prime numbers.

Dirchlet's thm: Every arithmetic progression $ak+b$, $k=1,2,\ldots$ where a and b are co-prime, $a>1$, $b>1$ contains infinitely many primes.

relatively prime

have no common divisor

$a=3 \quad b=5$

$3k+5 \quad k=1,2,\ldots$

$8, 11, 14, \ldots$

Goldbach's conjecture: Every even integer >2 is the sum of two primes.

Twin prime conjecture: $p, p+2$: twin primes, $5,7$ $3,5$

There are infinitely many twin primes.

Greatest Common Divisors & Least Common Multipliers

$a, b \in \mathbb{Z}_+$.

$\gcd(a,b)$ — The largest integer d s.t. $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b.

$\operatorname{lcm}(a,b)$ — The least common multiple of a, b is the smallest positive integer that is divisible by a and b.

ex $\gcd(12,8)=4$

$\gcd(3,2)=1$

if $\gcd(n,m)=1$ then n and m are relatively prime or co-prime

$25, 32$

$\operatorname{lcm}(12,8)=24$

$\operatorname{lcm}(3,2)=6$

$$a = p_1^{a_1}\, p_2^{a_2} \cdots p_n^{a_n}$$
$$b = p_1^{b_1}\, p_2^{b_2} \cdots p_n^{b_n}$$

prime factorizations

$a_i \geq 0 \quad b_i \geq 0$

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

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

45, 48

$$45 = 2^0 \cdot 3^2 \cdot 5^1$$
$$48 = 2^4 \cdot 3^1 \cdot 5^0$$

$\gcd(45,48) = 3.$

$\operatorname{lcm}(45,48) = 2^4 \cdot 3^2 \cdot 5^1 = 720$

Thm: Let a and b be positive numbers

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

proof idea $\quad x + y = \min(x,y) + \max(x,y)$