§ 4.3 Primes & GCD

Jessica Wei

Prime

DEF | Prime
Let $p \in \mathbb{Z}^+$. We say p is a prime if it is only divisible by p (itself) and 1. i.e. 2, 3, 5, 7...
Note: If an integer is not prime, then it is called composite.

THM 4.3.1 |
Every composite integer has a prime factorization.

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot ...p_k^{a_k}$$

Example 1. Find the prime factorization of 100.

$$100 = 10 \cdot 10$$
$$10 = 2 \cdot 5$$
$$\therefore 100 = 2 \cdot 2 \cdot 5 \cdot 5$$
$$\textbf{Answer: } 100 = 2^2 \cdot 5^2$$

THM 4.3.2 |
If n is composite, then $\exists p \in \mathbb{Z}$such that p is prime, $p \leq \sqrt{n}$, and $p|n$.

PROOF: Since n is composite, there exists $a, b \in \mathbb{Z}$ such that $n = a \cdot b$ and $a \neq n \neq b$.

Case 1: $a > \sqrt{n}$ and $b > \sqrt{n}$

Then $a \cdot b > \sqrt{n}$, $\sqrt{n} = n$

$\therefore a \cdot b > n$

This contradicts $a \cdot b = n$

Hence, it must be true that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

Assume $a \leq \sqrt{n}$. If this is not true, the following argument can be made for b.

Possibility #1. a is prime. Then $a \leq n$ satisfies and $n = a \cdot b \Rightarrow a|n$ satisfies.

Possibility #2. a is composite. Then by THM 4.3.1, a has a prime factorization so that $n = a \cdot b = p_1^{a_1}....p_x^{a_x} \cdot b$. SO any prime p_i in this factorization divides n ($p_i|n$) and $p_i^{a_i}....p_x^{a_x} = a \leq \sqrt{n}$ which implies $p_i \leq \sqrt{n}$

Example 2. Show that 61 is prime.

Assume that 61 is composite. In such a case $\exists p \leq \sqrt{61}$ such that $p|61$.

$\sqrt{61} \approx 7...$, $p \leq \sqrt{61} \approx 7...$

Range of primes: 2, 3, 5, 7...

$2 \nmid 61$, $3 \nmid 61$, $5 \nmid 61$, $7 \nmid 61$

$\Rightarrow$ Contradiction hence 61 cannot be composite. 61 must be prime.

THM 4.3.3 |
There are infinitely many primes.

PROOF: Assume that there are only k-number primes $p_1, p_2....p_k$. Form the number

$$Q = p_1...p_x + 1$$

Assuming Q is composite, Q must have a prime factorization. Suppose p is a prime factor of Q ($p|Q$).

Notice then that $p|Q - p_1....p_k \Rightarrow p|1$, which is impossible. Hence, Q cannot be composite.

So Q is prime which is a contradiction to finite number k primes. There are indefinitely-many primes.

$$2016 : 2^{74207281} - 1$$

$$2017 : 2^{7712321917} - 1$$

GCD's & LCM's

DEF | GCD
Let $a, b \in \mathbb{Z}^+$, the largest integer $d \in \mathbb{Z}^+$ that divides a and b is the greatest common divider.

$$d|a \wedge d|b$$

DEF | Pairwise Relatively Prime
Two or more integers are called pairwise relatively prime if the GCD between any two such integers is 1.

$$a_1, a_2...a_k$$

$$gcd(a_i, a_j) = 1$$
$$1 < i, j < k$$
$$gcd(4, 3) = 1$$
$$i \neq j$$

Example 3. What is...

a) gcd(24, 36) = 12
Answer: 12|24 & 12|36

b) gcd(17, 22) = 1
Answer: Relatively Prime

Example 4. Determine if the integers in the list are pairwise relatively prime.

a) 10, 17, 21
gcd(10, 19) = 1, gcd(10, 24) = 1, gcd(17, 21) = 1
Answer: ∴ pairwise relatively prime

b) 10, 19, 24
gcd(10, 19) = 1, gcd(10, 24) = **2**, gcd (19, 24)
Answer: ∴ not pairwise relatively prime

NOTICE: In general, if we are trying to find the GCD of any two numbers and we consider their prime factorization, then..

$$a = p_1^{a_1} ... p_k^{a_k}, b = p_1^{b_1} ... p_k^{b_k}$$
$$24 = 2^3 \cdot 3, 10 = 2 \cdot 5$$
$$gcd(24, 10) = 2$$
$$24 = 2^3 \cdot 3^1, 36 = 2^2 \cdot 3^2$$
$$gcd = 2^2 \cdot 3^1 = 12$$
$$** gcd(a, b) = p_1^{min(a_1 b_1} .... p_k^{min(a_k b_k} **$$

DEF | LCM
The Least Common Multiple of $a, b \in \mathbb{Z}^+$ is the smallest integer m such that $a|m$ and $b|m$.

i.e. lcm(8, 10) = 40

8: 8, 16, 24, 32, **40**, 48...

10: 10, 20, 30, **40**, 50...

$8 = 2^3$, $10 = 2^3 \cdot 5^1$

The powers of the prime factors of the least common multiple have to be the highest power present in the prime factors for $a\&b$.

$$LCM(a,b) = p_1^{max(a_1,b_1}...p_k^{max(a_k,b_k}$$

NOTE: Finding the GCD by trail & error of prime factorization is very costly and slow when trying to program it.

Euclidean Algorithm

THM 4.3.4 |
Let $a, b \in \mathbb{Z}^+$ such that $a = b \cdot q + r$, $r > 0$. Then the $gcd(a,b) = gcd(b,r)$

PROOF: Idea - show that all divisors of a & b are divisors of b and r because this includes the GCD.
i.e. Show $d|a \wedge d|b$

(i) $d|a \Rightarrow a = d \cdot s + a_0$

(ii) $b|d \Rightarrow b = d \cdot k + b_0$

To show $d|r$: $a = b \cdot q + r$

$d_s = d \cdot k \cdot q + r$

$\Rightarrow r = d \cdot s - d \cdot k \cdot q$

$\Rightarrow r = d \cdot s - d \cdot k \cdot q$

$\Rightarrow r = d(s - k \cdot q)$ where $s - k \cdot q \in \mathbb{Z}$

$\Rightarrow d|r$

$\Rightarrow d|b$ and $d|r$

Now assume $d|b$ and $d|r$ so that $b = d \cdot k$ & $r = d \cdot s$

Since $a = b \cdot q + r$

$a = d \cdot k \cdot q + d \cdot s = d(k \cdot q + s) \Rightarrow d|a$ where $k \cdot q + s \in \mathbb{Z}$

$\therefore d|a$ & $d|b$

Hence all divisors of a & b are divisors of b & r including GCD.

Example 5. Find the GCD(a, b) where $a = b \cdot q + r$, then we can successfully reduce the problem of finding GCD(a, b) by dividing the large number by the smaller number, then the smaller number by the remainder until $r = 0$.

a) Find gcd(120, 500)
$500 = 4 \cdot 120 + 20 \Rightarrow$ gcd(120, 20)
$120 = 6 \cdot 20 + 0 \Rightarrow 20$
Answer: gcd(20, 500) = 20

b) Find gcd(414,662)
$662 = 1 \cdot 414 + 248 \Rightarrow$ gcd(414, 248)
$414 = 1 \cdot 248 + 166 \Rightarrow$ gcd(248, 166)
$248 = 1 \cdot 166 + 82 \Rightarrow$ gcd(166, 82)
$166 = 2 \cdot 82 + 2 \Rightarrow$ gcd(82, 2)
$82 = 41 \cdot 2 + 0 \Rightarrow 2$
Answer: gcd(414, 662) = 2

THM 4.3.5 |
Let $a, b \in \mathbb{Z}^+$. Then $\exists s, t \in \mathbb{Z}$ such that $a \cdot s + b \cdot t = \gcd(a,\ b) \Rightarrow$ (Bezout Identity) where s and t are Bezout coefficients.

Example 6. Find the Bezout Coefficient for.

a) gcd(120, 500) = 20
$500 = 4 \cdot 120 + 20 \Rightarrow 20 = 500 - 4 \cdot 20$
$120 = 6 \cdot 20 + 0 \Rightarrow$ (1, -4)
Answer: (-4, 1)

b) Find gcd(414,662)
$662 = 1 \cdot 414 + 248 \Rightarrow 248 = 662 - 1 \cdot 414$
$414 = 1 \cdot 248 + 166 \Rightarrow 166 = 414 - 1 \cdot 248$
$248 = 1 \cdot 166 + 82 \Rightarrow 82 = 2 \cdot 48 - 1 \cdot 116$
$166 = 2 \cdot 82 + 2 \Rightarrow 2 = 166 - 2 \cdot 82$
$82 = 41 \cdot 2 + 0$

$2 = 166 - 2 \cdot 82$
$= 166 - 2 \cdot (248 - 166) = 3 \cdot 166 - 2 \cdot 248$
$= 3(414 - 248) - 2 \cdot 248 = 3 \cdot 414 - 5 \cdot 248$
$= 3 \cdot 414 - 5 \cdot 248 = 3 \cdot 414 - 5(662 - 1 \cdot 414)$
$8 \cdot 414 - 5 \cdot 662 \Rightarrow (-5, 8)$
Answer: (-5, 8)