Number Theory

Notation: $\mathbb{N} = \{0, 1, 2, \ldots\}$; the natural numbers

$a \mid b$ denotes "a divides b"

Def: A number $p > 1$ is called **prime** if the only numbers that divide p are p and 1.

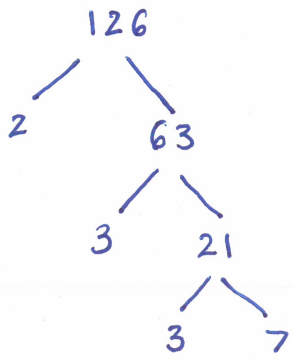
A number $n > 1$ is called **composite** if it is not prime.

Fundamental Theorem of Arithmetic:

Every natural number greater than 1 is either prime or representable as a **unique** product of prime numbers.

Note: unique up to the order of the factors.

Ex// 2 is prime

Ex// 

$126 = 2 \cdot 3^2 \cdot 7$

the above is called a factor tree

Finding Primes - The Sieve of Eratosthenes

To find all primes less than or equal to a number n:

1) List 2 through n.
2) Starting with 2, cross out all multiples of 2.
3) Find the next number that is not crossed out, this number is prime. Cross out all multiples of this number.
4) Repeat Step 3 until the list is exhausted.

Ex// Find all primes for $n \leq 22$.

(2), (3), ~~4~~, (5), ~~6~~, (7), ~~8~~

~~9~~, ~~10~~, (11), ~~12~~, (13), ~~14~~, ~~15~~

~~16~~, (17), ~~18~~, (19), ~~20~~, ~~21~~, ~~22~~

Def: Let a, b, c be natural numbers. The number c is called a common divisor of a and b if $c \mid a$ and $c \mid b$. The number c is called the greatest common divisor of a and b, denoted $\gcd(a,b)$, if c is the largest common divisor of a and b.

Def Let a, b, c be natural numbers. The number c is a common multiple of a and b if $c = q_1 a$ and $c = q_2 b$ for some q_1, q_2 natural numbers.

c is called the least common multiple if c is the smallest common multiple of a and b. Denote this by $c = \text{lcm}(a,b)$.

Finding the gcd(a,b) and lcm(a,b)

Method 1: Use the prime factorizations of a and b.

$\gcd(a,b) \Rightarrow$ 1) Write factorizations
2) Take the smallest Exponents

$\text{lcm}(a,b) \Rightarrow$ 1) Write factorizations
2) Take the largest Exponents.

Ex// $54 = 2^1 \cdot 3^2 = 2^1 \cdot 3^2 \cdot 7^0$
$126 = 2^1 \cdot 3^2 \cdot 7^1 = 2^1 \cdot 3^2 \cdot 7^1$

$\gcd(54,126) = 2^1 \cdot 3^2 \cdot 7^0 = 54$

$\text{lcm}(54,126) = 2^1 \cdot 3^2 \cdot 7^1 = 126$

Ex// $133 = 7^1 \cdot 19^1 = 3^0 \cdot 7^1 \cdot 19^1$
$147 = 3^1 \cdot 7^2 = 3^1 \cdot 7^2 \cdot 19^0$

$\gcd(133,147) = 3^0 \cdot 7^1 \cdot 19^0 = 7$

$\text{lcm}(133,147) = 3^1 \cdot 7^2 \cdot 19^1 = 2793$

Note $54 \mid 126$

Method 2: Use the Euclidean Algorithm

Fact: Given two natural numbers a and b w/ $b \geq a$ then $b = aq + r$ for some q and r in $\mathbb{N}$. Call r the remainder.

Ex// $b = 18$, $a = 7$

$18 = 2(7) + 4$

Euclidean Algorithm:

$b = q_0 a + r_0$

$a = q_1 r_0 + r_1$

$r_0 = q_2 r_1 + r_2$

$\vdots$

$r_{k-2} = q_k r_{k-1} + r_k$

Stop when $r_k = 0$

then $r_{k-1} = \gcd(a,b)$

Ex// $\gcd(123, 54)$

$123 = 2(54) + 15$

$54 = 3(15) + 9$

$15 = 1(9) + 6$

$9 = 1(6) + 3$ ← gcd

$6 = 2(3) + 0$ ← stop

$\gcd(123, 54) = 3$

Formula: For $a, b > 0$

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

Diophantine Equations

A two variable linear Diophantine Equation is an equation of the form $ax + by = c$.

We seek only integer solutions. ie. x and y in $\mathbb{Z} = \{\ldots -1, 0, 1, 2, \ldots\}$

GCD Characterization: Let a, b, c be natural numbers then $c = \gcd(a,b)$ if and only if $c = ax + by$ for some integers x and y.

Solving Diophantine Equations:

1) The equation $ax + by = c$ has a solution if and only if $c \mid \gcd(a,b)$.

2) If $d = \gcd(a,b)$ and $x = x_0$, $y = y_0$ are one solution to $ax + by = c$ then the complete solution set is given by

$$x = x_0 + n\,b/d \qquad y = y_0 - n\,a/d \qquad (n \text{ is an integer})$$

Ex// $62x + 24y = 4$

Step 1: Calculate $\gcd(62,24)$

$62 = 2(24) + 14$

$24 = 1(14) + 10$

$14 = 1(10) + 4$

$10 = 2(4) + 2$

$4 = 2(2) + 0$

$\gcd(62,24) = 2$

$62x + 24y = 4$ has solutions!

Step 2: Back substitute

$2 = 10 - 2(4)$

$2 = 10 - 2(14-10) = 3(10) - 2(14)$

$2 = 3(10) - 2(14) = 3(24-14) - 2(14) = 3(24) - 5(14)$

$2 = 3(24) - 5(14) = 3(24) - 5(62 - 2(24))$

$2 = 13(24) - 5(62)$

For $62x + 24y = 2$

$x = -5$ $y = 13$ is a solution.

So For $62x + 24y = 4$

$x = -10$ $y = 26$ is a solution.

Step 3: Use formulas!

$ax + by = c$; $d = \gcd(a,b)$

$x = x_0 + n\,b/d$; $y = y_0 - n\,a/d$

$$x = -10 + n\left(\frac{24}{2}\right)$$

$$y = 26 - n\left(\frac{62}{2}\right)$$