05 Elementary Number Theory

05_03 GCD and LCM

The Fundamental Theorem of Arithmetic. Every positive integer that is at least 2 can be written uniquely as a prime or as the product of a collection of primes, where the primes are arranged in order of nondecreasing size.

Examples.

$7 = 7.$
$87 = 3*29.$
$111 = 3*37.$
$1400 = 2*2*2*5*5*7 = 2^3*5^2*7^1.$
$1024 = 2*2*2*2*2*2*2*2*2*2 = 2^{10}.$

Greatest Common Divisor. Suppose a and b are integers such that that $a \neq 0$ or $b \neq 0$. The greatest common divisor of two integers a and b, denoted GCD(a, b), is the largest positive integer that divides a and b.
If GCD(a, b) = 1, then we say a and b are relatively prime.
If |a| and |b| are small, we can find GCD(a, b) manually.

Example. Find GCD(12, 18) = GCD(18, 12).
The positive factors of 12 are 1, 2, 3, 4, 6, and 12.
The positive factors of 18 are 1, 2, 3, 6, 9, and 18.
Thus GCD(12, 18) = GCD(18, 12) = 6.

Example. Find GCD(57, 20) = GCD(20, 57).

The positive factors of 57 are 1, 3, 19, and 57.

The positive factors of 20 are 1, 2, 4, 5, 10, and 20.

Thus GCD(57, 20) = GCD(20, 57) = 1 and 57 and 20 are relatively prime.

The GCD for two integers can be found via prime factorizations of them.

Suppose a and b are integers such that $a \neq 0$ or $b \neq 0$. If a and b have the following prime factorizations,

$$a = p_1\text{^}(s_1)\ p_2\text{^}(s_2)\ \ldots\ p_k\text{^}(s_k),$$

$$b = p_1\text{^}(t_1)\ p_2\text{^}(t_2)\ \ldots\ p_k\text{^}(t_k),$$

where s_i is a nonnegative integer, $1 \leq i \leq k$, and

t_j is a nonnegative integer, $1 \leq j \leq k$. Then

Then GCD(a, b) is

$p_1\text{^}(\min\{s_1, t_1\})\ p_2\text{^}(\min\{s_2, t_2\})\ \ldots\ p_k\text{^}(\min\{s_k, t_k\})$,

where $\min\{s_i, t_i\}$ denotes the smaller one between s_i and t_i, for each i with $1 \leq i \leq k$.

Example. $\mathrm{GCD}(2^3\ 3^5\ 7^2,\ \ 2^2\ 3^4\ 7^3) = 2^2\ 3^4\ 7^2$.

Example. $\mathrm{GCD}(2^3\ 3^5\ 11^2,\ \ 2^2\ 3^4\ 7^3)$

$= \mathrm{GCD}(2^3\ 3^5\ 7^0\ 11^2,\ \ 2^2\ 3^4\ 7^3 11^0)$

$= 2^2\ 3^4\ 7^0\ 11^0 = 2^2\ 3^4 = 4*81 = 324$.

Example. Find GCD(1740, 666).

$1740 = 2*5*2*3*29 = 2^2\ 3^1\ 5^1\ 29^1$,

$666 = 2*3*3*37 = 2^1\ 3^2\ 37^1$.

Thus GCD(1740, 666)

$= \mathrm{GCD}(2^2\ 3^1\ 5^1\ 29^1\ 37^0, 2^1\ 3^2\ 5^0\ 29^0\ 37^1)$

$= 2^1\ 3^1\ 5^0\ 29^0\ 37^0 = 6$.

The <u>Least Common Multiple</u> of the positive integers a and b, denoted LCM(a, b), is the smallest positive integer that is divisible by both a and b. If a and b are small, we can find LCM(a, b) manually.

<u>Example.</u> Find LCM(6, 8) = LCM(8, 6).

The positive multiples of 6 are 6, 12, 18, 24, 30, 36, …

The positive multiples of 8 are 8, 16, 24, 32, 40, 48, …

Thus LCM(6, 8) = LCM(8, 6) = 24.

The LCM for two integers can be found via prime factorizations of them.

Suppose a and b are two positive integers. If a and b have the following prime factorizations,

$$a = p_1\text{^}(s_1)\ p_2\text{^}(s_2) \ldots p_k\text{^}(s_k),$$

$$b = p_1\text{^}(t_1)\ p_2\text{^}(t_2) \ldots p_k\text{^}(t_k),$$

where s_i is a nonnegative integer, $1 \le i \le k$, and

t_j is a nonnegative integer, $1 \le j \le k$. Then

Then LCM(a, b) is

$p_1\text{^}(\max\{s_1, t_1\})\ p_2\text{^}(\max\{s_2, t_2\}) \ldots p_k\text{^}(\max\{s_k, t_k\})$,

where $\max\{s_i, t_i\}$ denotes the larger one between s_i and t_i, for each i with $1 \le i \le k$.

Example. $LCM(2^3\ 3^5\ 7^2,\ 2^2\ 3^4\ 7^3) = 2^3\ 3^5\ 7^3$.

Example. $LCM(2^3\ 3^5\ 11^2,\ 2^2\ 3^4\ 7^3)$

$= LCM(2^3\ 3^5\ 7^0\ 11^2,\ 2^2\ 3^4\ 7^3 11^0)$

$= 2^3\ 3^5\ 7^3\ 11^2$.

Example. Find LCM(1740, 666).

$1740 = 2*5*2*3*29 = 2^2\ 3^1\ 5^1\ 29^1$,

$666 = 2*3*3*37 = 2^1\ 3^2\ 37^1$.

Thus LCM(1740, 666)

$= LCM(2^2\ 3^1\ 5^1\ 29^1\ 37^0,\ 2^1\ 3^2\ 5^0\ 29^0\ 37^1)$

$= 2^2\ 3^2\ 5^1\ 29^1\ 37^1$.

Theorem. Let a and b be positive integers. Then

$$a*b = GCD(a, b)*LCM(a, b).$$