Intermediate Math Circles
March 20, 2013
Number Theory II

How many prime numbers are there?

Euclid's Theorem: "There are infinitely many prime numbers".

Why is this true?
Imagine that there are only 4 prime numbers, namely $2, 3, 5, 7$. The product of these numbers is $P = 2(3)(5)(7) = 210$. When we do the Sieve, 210 is crossed out by each of our 4 primes. What does this mean for 211? Since all of our 4 primes crosses out 210, when we continue the Sieve each of our primes would skip over 211. This means that 211 will never be crossed out. So, there must be more than 4 primes. In fact, this process would work for any finite number of primes.

Greatest Common Divisor

The greatest common divisor of two natural numbers a and b is the largest positive integer that is a divisor of both a and b. We denote the greatest common divisor of a and b by $\gcd(a, b)$.

For example, let's find the $\gcd(40, 32)$.
Divisors of $40 : 1, 2, 4, 5, 8, 10, 20, 40$
Divisors of $32 : 1, 2, 4, 8, 16, 32$
Thus, $\gcd(40, 32) = 8$.

The gcd is important when we are removing common factors to simplify expressions or solve equations.

Least Common Multiple

The least common multiple of a and b is the smallest positive integer that is a multiple of both a and b. We denote the least common multiple of a and b by $\mathrm{lcm(a, b)}$.

For example, let's find the $\mathrm{lcm}(40, 32)$.
Multiples of $40 : 40, 80, 120, 160, 200, 240, 280, 320, \cdots$
Multiples of $32 : 32, 64, 96, 128, 160, \cdots$
Thus, $\mathrm{lcm}(40, 32) = 160$.

We use the lcm when finding common denominators.

Exercise 1.

Determine the greatest common factor and least common multiple for each pair of values.
(a) $(18, 24)$ (b) $(72, 54)$

Using the Prime Factorization to Find the gcd and lcm

How would we find the gcd and lcm of $a = 12!$ and $b = 100^3$? Our method of listing the divisors and multiples of each number would be tedious and time consuming. Let's look at the $\gcd(18, 24)$ and $\text{lcm}(18, 24)$ again, to spot their relationship with 18 and 24.

The Prime Factorization of 18 is 2×3^2.
The Prime Factorization of 24 is $2^3 \times 3$.

The $\gcd(18, 24) = 6$.
The Prime Factorization of 6 is 2×3.
What is the link between the prime factorization of two values and their gcd? The gcd is the product of all common prime factors of the two numbers.

The $\text{lcm}(18, 24) = 72$.
The Prime Factorization of 72 is $2^3 \times 3^2$.

What is the link between the prime factorization of two values and their lcm? The lcm is the product of the highest power of every prime factor of the two numbers.

Example Find the $\gcd(756, 1386)$ and $\text{lcm}(756, 1386)$

The Prime Factorization of 756 is $2^2 \times 3^3 \times 7$.
The Prime Factorization of 1386 is $2 \times 3^2 \times 7 \times 11$.
The $\gcd(756, 1386) = 2 \times 3^2 \times 7 = 126$.

The $\text{lcm}(756, 1386) = 2^2 \times 3^3 \times 7 \times 11 = 8\,316$.

Exercise 2.

Determine the greatest common factor and least common multiple of each pair of values.
(a) $(784, 1400)$ (b) $(12!, 100^3)$

Using the gcd to find the lcm

The Prime Factorization of 784 is $2^4 \times 7^2$.
The Prime Factorization of 1400 is $2^3 \times 5^2 \times 7$.
The product of our two numbers is

$$(784)(1400) = (2^4 \times 7^2)(2^3 \times 5^2 \times 7) = 2^7 \times 5^2 \times 7^3$$

The $\gcd(784, 1400) = 2^3 \times 7$.
The $\text{lcm}(784, 1400) = 2^4 \times 5^2 \times 7^2$.
The product of the gcd and lcm is

$$\gcd(784, 1400) \times \text{lcm}(784, 1400) = (2^3 \times 7)(2^4 \times 5^2 \times 7^2) = 2^7 \times 5^2 \times 7^3$$

We see that,

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

Rearranging this formula we have,

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

This formula is very useful when finding the lcm of numbers whose prime factorization is difficult to determine. i.e. for integers whose prime factors are large numbers. But, how can we find the gcd without the prime factorizations?

Division Algorithm

Suppose a, b are integers and $0 < b < a$. When a is divided by b, there will exist a quotient, q, and a remainder, r, where $0 \leq r < b$. Another way of writing this is $a = qb+r$, where $0 \leq r < b$.

For example,
if $a = 15$ and $b = 6$, we can write a in terms of b as $15 = (2)(6) + 3$

Exercise 3.

Use the division algorithm to write the larger integer in terms of the smaller.
(a) $(90, 28)$ (b) $(137, 19)$

Euclidean Algorithm

If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$

What does this mean? Suppose we want to find the $\gcd(7429, 969)$

$$\begin{array}{rl|rl} 7429 &= 7(969) + 646, & & \gcd(7429, 969) \\ 969 &= 1(646) + 323, & = & \gcd(969, 646) \\ & & = & \gcd(646, 323) \end{array}$$

Since $2(323) = 646$, we know that $\gcd(646, 323) = 323$.
Therefore, $\gcd(7429, 969) = 323$

Exercise 4.

Use the Euclidian Algorithm to determine the $\gcd(a, b)$

(a) $(24, 210)$ (b) $(945, 399)$

Exercise 5.

Use the gcd and the formula $\text{lcm(a, b)} = \dfrac{\text{ab}}{\gcd(\text{a, b})}$ to determine,

(a) $\text{lcm}(24, 210)$ (b) $\text{lcm}(945, 399)$

Exercise 6.

Jupiter does one complete revolution around the Sun every 103 944 Earth hours. The Earth completes one revolution around the Sun every 8766 hours. How often does the Sun, Earth and Jupiter line up?