05 Elementary Number Theory

05_02 Prime Numbers

A positive integer p is prime if $p \geq 2$ and the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is composite.

Small prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23.
Each prime number is a positive odd integer except for 2.
57 is composite since 57 = 3*19.

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.

Theorem 1. There are infinitely many prime numbers.
[Proof] We can prove Theorem 1 by a proof by contradiction. We assume this assertion is false. Then there are finitely many prime numbers. We use $p_1, p_2, \ldots, p_k$ to denote all the prime numbers. Construct an integer

$$n = p_1 * p_2 * \ldots * p_k + 1.$$

Since n is not equal to any of $p_1, p_2, \ldots, p_k$ and $p_1, p_2, \ldots, p_k$ represent all the prime numbers, n is not a prime number.
By the Fundamental Theorem of Arithmetic, we have a prime number, say p_i, where $1 \leq i \leq k$, such that $n = s * p_i$, where s is

an integer. Thus $s*p_i = p_1*p_2* \ldots *p_k + 1$. Namely,

$$p_i\,(s - p_1*p_2* \ldots p_{i-1}*p_{i+1}*p_k) = 1.$$

Since p_i is an integer which is greater than ≥ 2 and $(s - p_1*p_2* \ldots p_{i-1}*p_{i+1}*p_k)$ is an integer, The equality

$$p_i\,(s - p_1*p_2* \ldots p_{i-1}*p_{i+1}*p_k) = 1$$

cannot be true, a contradiction. Thus, we complete the proof of Theorem 1.

<u>**Theorem 2**</u>**.** If m is a composite, then m must have a prime a factor less than or equal to $\sqrt{m}$.

[Proof]. Since m is a composite, there exists an integer s such that $m = s*t$, where $1 < s < m$, t is an integer. Then either $s \leq \sqrt{m}$ or $t \leq \sqrt{m}$, otherwise $m = s*t > m$. Thus m has a factor is less than or equal to $\sqrt{m}$. If this factor is a prime, the proof is finished. Otherwise, the Fundamental Theorem of Arithmetic ensures that the factor has a prime factor which is less than itself. This in turn guarantees m has a prime factor less than $\sqrt{m}$. Therefore the proof is complete.

<u>Example 1.</u> Show that 97 is a prime.

[Solution] Notice that the prime numbers which are less than or equal to $\sqrt{97}$ are 2, 3, 5, and 7. None of 2, 3, 5, and 7 is a factor of 97. Thus Theorem 2 implies that 97 is a prime.

<u>Exercise 1.</u> Show that 107 is a prime.

In Number Theory, there are conjectures involving primes. Below are two examples.

The Twin Prime Conjecture. There are infinitely many pairs of primes such that their difference is 2.
https://en.wikipedia.org/wiki/Twin_prime

Goldbach's Conjecture. Every even integer greater than two is the sum of two primes.
https://en.wikipedia.org/wiki/Goldbach's_conjecture