Computational Number Theory - Notes

Philip Warton

January 6, 2021

1 Introduction and Divisibility

The first important set we look at is the set of integers

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

Definition 1.1. If $a, b \in \mathbb{Z}$, we say that a divides b, denote $a|b$ if there exists some $n \in \mathbb{Z}$ such that $b = na$.

If no such n exists we say that a does not divide b.

$\boxed{\text{The Division Algorithm}}$ Let $a, b \in \mathbb{Z}$ with $b \geqslant 1$. Then there exists unique integers q and r such that

$$a = qb + r$$

Where $q \in \mathbb{Z}$ and $r \in \{0, 1, \cdots b\}$.

Proof. Let $S = \{a + bx | x \in \mathbb{Z}\}$. It follows that the subset of nonnegative values in S is bounded below, and contains some smallest nonnegative element. Call this r. Then if $r = a + bx_0$, let $q = -x_0$. Then of course $a = qb + r$. To show that $0 \leqslant r < b$, first note that by construction r must be non-negative. Then if $r \geqslant b$, it follows that we can replace bx_0 with $b(x_0 - 1)$ resulting in a smaller non-negative element of S. Thuse $0 \leqslant r < b$.

Then show uniqueness, please. □

Theorem 1.1 (Euclid)**.** *There are infinitely many prime numbers.*

Lemma 1.1. *Every integer $n \geqslant 2$ is divisible by some prime.*

Proof. If this lemma is false, let n be the smallest integer which is not divisible by any prime. We know that n cannot be prime, since we would have $n|n$. So n can be factored as $n = ab$ where $a, b \in \{1, 2, 3, \cdots, n\}$. Then a is smaller than the smallest integer that has no prime factor, thus it has a prime factor. Then it follows that the prime factor of a must be a prime factor of n. □

Now that this lemma has been proven, we can move on to prove the theorem at hand.

Proof. Assume that there are finitely many primes. Let

$$N = p_1 p_2, \cdots p_k + 1$$

Then N is divisible by a some prime p_i. It follows that $N = p_i(m) + 1$ which means that $r \neq 0$ and p_i does not divide N. □

If $n \geqslant 2$ is composite then n is divisible by some prime $p \leqslant \sqrt{n}$.

Proof. If $x > \sqrt{n}$ and $y > \sqrt{n}$ then $n = xy > \sqrt{n}\sqrt{n} = n$ which is false. So either x or y is less than or equal to $\sqrt{n}$. Take p to be a prime factor of either x or y, depending on which is not larger than $\sqrt{n}$. □

Siene of Eratosthenes: A method to find all primes p up to some bound N.

$\boxed{1.}$ Write the numbers from 2 to N.

$\boxed{2.}$ Starting with the smallest element n still on the list. Eliminate all multiples of this number up to N.

$\boxed{3.}$ Let p be the next smallest element remaining, and remove the previous p. $\boxed{4.}$ Repeat steps 2 and 3 up to $\sqrt{N}$.