1. Parity, Divisibility, Multiples, and Divisors

In this chapter of the course notes we will explore introductory definitions in number theory that we will find useful in our study of cryptography. We will begin as many courses do with a mathematical definition of even and odd, properties called the *parity* of a number.

Definition 1.0.1

Even and odd

A number $n \in \mathbb{Z}$ is said to be *even* if there exists $k \in \mathbb{Z}$ such that

$$n = 2k.$$

Similarly, a number $n \in \mathbb{Z}$ is said to be *odd* if there exists $k \in \mathbb{Z}$ such that

$$n = 2k + 1.$$

Which of the two categories an integer belongs to is called its *parity*.

When we learn the definition of divisibility, we will recognize that the mathematical definition of an even number above coincides with the mathematical definition of "divisible by 2."

Example 1.0.1

Proving a quantity is even

In order to prove that a number n is even, we must show that it can be written as twice some integer. The work to be done goes into *finding* that integer, which may be written in terms of n or some other variables. To see an example of this, we will solve the following problem:

> Show that if n is an even integer, then $n^2 + 3n + 6$ is also an even integer.

In order to show this claim is true, we will start from what we are told: that n is an even integer. By the definition of even, we know that $n = 2k$ for some unknown integer k. Substituting this into the expression $n^2 + 3n + 6$ shows us that

$$\begin{aligned} n^2 + 3n + 6 &= (2k)^2 + 3(2k) + 6, && \text{(using } n = 2k\text{)} \\ &= 4k^2 + 6k + 6, \\ &= 2(2k^2 + 3k + 3). \end{aligned}$$

We now observe the following: because k was an integer, $2k^2 + 3k + 3$ is *also* an integer! We have now shown that $n^2 + 3n + 6$ can be written as twice some integer, and thus it is even. In summary, we first used the fact that we knew n was even to rewrite it as a multiple of 2. Then we performed some algebra to show that the final quantity is still *also* a multiple of two.

Luckily the format of a proof that a quantity is odd follows a similar structure. If you can show a quantity is even, there is a good chance you can construct a similar proof showing another is odd.

Example 1.0.2

Proving a quantity is odd

When showing that a quantity is *odd* our goal is to execute a similar process to that as when we showed a quantity is even. However, we will hope to keep a *remainder* of 1 outside our multiple of 2.

Show that if n is any integer, then $(2n+1)^2$ is always odd.

This problem is slightly different than the one before in that it asks us to show that *any* integer n we use results in an odd number. We will prove this by handling *both cases*. That is to say, we will write a proof where we suppose that n is odd, and another where we suppose that n is even.
If n is even, then as before $n = 2k$ for some integer k. Doing the same work as before,

$$\begin{aligned}(2n+1)^2 &= (2(2k)+1)^2,\\ &= (4k+1)^2,\\ &= 16k^2 + 8k + 1,\\ &= 2(8k^2 + 4k) + 1.\end{aligned}$$

Notice that we have written $(2n+1)^2$ as twice some integer plus a remainder of 1! We conclude that when n is even, the result is true.
Suppose instead that n is odd. Then $n = 2k + 1$ for some integer k. Let us try similar algebra and see what happens.

$$\begin{aligned}(2n+1)^2 &= (2(2k+1)+1)^2,\\ &= (4k+3)^2,\\ &= 16k^2 + 24k + 9,\\ &= (16k^2 + 24k + 8) + 1. && \text{(Borrowing 1 from 9.)}\\ &= 2(8k^2 + 12k + 4) + 1.\end{aligned}$$

Conclude that in either case, we still get an odd number!

The idea of even and oddness is actually related quite closely to the idea of divisibility and remainders.

Definition 1.0.2

Divisor, multiple, and divides

Given two integers $a, b \neq 0$, we say that a divides b (alt. b is divisible by a) if there exists a value $k \in \mathbb{Z}$ such that $b = ka$. If b is divisible by a, then we say that b is a *multiple* of a, and a is a *divisor* of b. If a divides b, it is common to write $a|b$ as shorthand.

Example 1.0.3

Proving one quantity divides another

In order to show that one quantity divides another, we will use the same philosophy as in showing a number was even. Our goal is to show or rewrite some quantity as a *multiple* of the other using the information we are given. Often by trying to factor out an integer from all terms.

Show that if $3|a$, then $9|(a^2 + 15a + 45)$.

As always, we start with what we are told: that 3 divides a. That implies there is an integer k for which $a = 3k$. Substituting this into the expression shows us that

$$\begin{aligned} a^2 + 15a + 45 &= (3k)^2 + 15(3k) + 45, \\ &= 9k^2 + 45k + 45, \\ &= 9(k^2 + 5k + 5). \end{aligned}$$

By showing that $a^2 + 15a + 45$ can be written as a multiple of 9, we have shown that $9|(a^2 + 15a + 45)$.

With this idea, we may define the common and frequently used concept of a prime number.

Definition 1.0.3

Prime and composite

An integer $n \geq 2$ is called prime if it has *no* integer divisors other than 1 and itself. In the event that an integer is not prime, it is called composite.

What is up with the naming convention here? Why are numbers that are not prime called 'composite'? Why do we care about primes? We care about prime numbers because in reality, all integers are 'built' from primes. Composite numbers are named so because they are *composed* of said primes. This result is known as the fundamental theorem of arithmetic and is given below.

Theorem 1.0.1

Fundamental theorem of arithmetic

Every positive integer $n \geq 2$ can be written as a *unique* product of primes.