CMSC 250: Parity, Primes, Divisibility, Modular Arithmetic

Justin Wyss-Gallifent

April 20, 2023

1 Introduction

The idea of this section is to introduct four concepts formally:

- Parity (even and odd)
- Prime and composite numbers
- Divisibility
- Modular arithmetic in computer science
- Modular arithmetic in mathematics

Having formal definitions will allow us to have an easy sandbox to play in when we start learning how to formally prove things.

In each of the following sections we also give a really light and informal proof just to see that we have an intuitive understanding of what a proof is.

2 Parity

Even and odd numbers are something we are all generally familiar with but that makes them a great place to introduce some formal definitions because we have the intuition to complement those definitions.

Definition 2.0.1. Given an integer x we say that:

1. x is *even* if there is some integer y such that $x = 2y$.
2. x is *odd* if there is some integer y such that $x = 2y + 1$.

> **Example 2.1.** The integer 10 is even because there is $y = 5$ with $10 = 2(5)$.

> **Example 2.2.** The integer 17 is odd because there is $y = 8$ with $10 = 2(8) + 1$.

Here is a light and informal proof:

> **Example 2.3.** The number 17 is not even. If it were, then there would be some integer y with $17 = 2y$ but then $y = 17/2$ which is not an integer at all!

3 Primes and Composites

Intuitively we know what a prime is. Here's the formal definition:

Definition 3.0.1. Given an integer $x > 1$ we say that:

1. x is *prime* if the only positive divisors of x are 1 and x.
2. x is *composite* if there are positive integers $y, z > 1$ with $x = yz$.

Note 3.0.1. The number 1 and in fact every $x \leq 1$ are neither prime nor composite.

Note 3.0.2. In a more abstract sense (in abstract algebra, for example) there is a different definition of prime.

> **Example 3.1.** The integer 17 is prime because the only positive divisors of 17 are 1 and 17.

> **Example 3.2.** The integer 10 is composite because $10 = 2 \cdot 5$.

Here is a light and informal proof:

> **Example 3.3.** The integer 2 is the only positive even integer which is prime since ever other even positive integer looks like $2x$ with $x > 1$ and is therefore divisible by both 2 and x, making it compositie.

4 Divisibility

We generally intuitively understand what it means for one number to divide another.

Definition 4.0.1. Given a integer $x \neq 0$ and an integer 0 we say that x *divides* y if there is some (unique!) integer z with $xz = y$. In this case we write:

$$x \mid y$$

If no such z exists then we say that x *does not divide* y and we write:

$$x \nmid y$$

> **Example 4.1.** Observe that $6 \mid 24$ because $6(4) = 24$.

> **Example 4.2.** Observe that $6 \mid 6$ because $6(1) = 6$.

> **Example 4.3.** Observe that $-5 \mid 10$ because $-5(-2) = 10$.

> **Example 4.4.** Observe that $6 \nmid 25$ because there is no integer z with $6z = 25$.

Note 4.0.1. Observe that $x \mid 0$ for any $x \neq 0$ because $x(0) = 0$.

Note 4.0.2. Observe that we don't talk about 0 dividing things. For example we don't write $0 \mid 5$ nor do we write $0 \nmid 5$. The reason for this is twofold. First, it would require that many theorems related to divisibility have special cases. Second, there are complications because $0x = 0$ has infinitely many solutions and we like divisibility to have just one.

Here is a light and informal proof:

> **Example 4.5.** Knowing that $5 \mid 10$ and $10 \mid 40$ allows us to conclude that $5 \mid 40$ because $5(2) = 10$ and $10(4) = 40$ and so $5(2)(4) = 40$, thus $5(8) = 40$.

5 Modular Arithmetic in Computer Science

Traditionally in computer science "mod" is defined as a function in the following way:

Definition 5.0.1. Given an integer x and another integer $m \geq 2$, called the *modulus*, we define:

$$a \mod m \text{ equals the remainder when } a \text{ is divided by } m.$$

Note 5.0.1. It's important to keep in mind that when we divide a by m we are doing $a = qm + r$ with $0 \leq r < m$.

> **Example 5.1.** We have $42 \mod 8 = 2$ because $42 = 5(8) + 2$.

> **Example 5.2.** We have $3 \mod 10 = 3$ because $3 = 0(10) + 3$.

When working with negative integers we must be careful.

> **Example 5.3.** We have $-38 \mod 7 = 4$ because $-38 = -6(7) + 4$.

Here is a light and informal proof:

> **Example 5.4.** It's always true that $x \mod x = 0$ since $x = 1(x) + 0$.

6 Modular Arithmetic in Mathematics

Traditionally in mathematics "mod" is defined in the following way:

Definition 6.0.1. Given two integers x, y and another integer $m \geq 2$, called the *modulus* we say that x is *equivalent*, or *congruent*, *to* y, *mod* m, written

$$x \equiv y \mod m$$

ff $m \mid (x - y)$.

Note 6.0.1. Since $y - x = -(x - y)$ it's fairly clear that it doesn't matter which way we subtract.

Example 6.1. We have $50 \equiv 34 \mod 8$ because $8 \mid (50-34)$ since $50-34 = 16$. Or if we prefer, because $8 \mid (34-50)$ because $34-40 = -16$.

Note 6.0.2. There other ways to think of this definition. One way is to recognize that $x \equiv y \mod m$ if we can add or subtract some multiple of m to x to obtain y.

Example 6.2. We have $10 \equiv 45 \mod 7$ because $10 + 5(7) = 45$.

Here is a light and informal proof:

Example 6.3. If we can add a multiple of m to x to obtain y an if we can add a multiple of m to y to obtain z then we can certainly add a multiple of m to x to obtain z. In other words if $x \equiv y \mod m$ and $y \equiv z \mod m$ then $x \equiv z \mod m$.