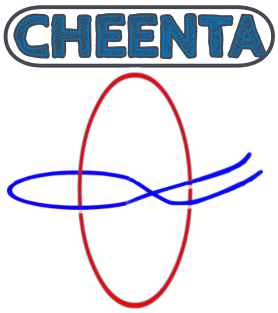

Divisibility

Dr. Sankhadip Chakraborty

0.1 Lesson Overview

We use this lesson to revisit some basic concepts of number theory, like digits of numbers, division, and primes.

0.2 Decimal digits

Every natural number can be expressed uniquely in the form

$$10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 = \sum_{i=0}^{n} 10^i a_i.$$

This is known as the *decimal representation* of n and the a_is are called the *digits* of n. The digit a_0 is known as the unit digit and a_1 is known as the tens digit.

Think! Can you prove that this representation is unique?

0.2.1 Divisibility by 2, 4, 5 and 10

The decimal representation lets us immediately observe some basic rules about divisibility. Note that

$$10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 = \boxed{10 \cdot (10^{n-1} a_n + 10^{n-2} a_{n-1} + \cdots + a_1)} + a_0.$$

The boxed part is divisible by 2, 5 and 10. Thus, the number is divisible by 2, 5 or 10 when the unit digit is divisible by 2, 5, or 10 respectively.

The conclusions are as follows :

- An integer is divisible by 2 if and only if the unit digit is 0, 2, 4, 6 or 8.
- An integer is divisible by 5 if and only if the unit digit is 0 or 5.
- An integer is divisible by 10 if and only if the unit digit is 0.

To check divisibility by 4, it suffices to write

$$10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 = \boxed{100 \cdot (10^{n-2} a_n + 10^{n-3} a_{n-1} + \cdots + a_2)} + (10a_1 + a_0)$$

and observe that the boxed part is divisible by 4.

An integer is divisible by 4 if and only if the integer formed by its last two digits is divisible by 4.

0.3 Divisibility by 3 and 9

We may rewrite $10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0$ as

$$\boxed{(10^n - 1)a_n + (10^{n-1} - 1)a_{n-1} + \cdots + (10 - 1)a_1} + (a_n + a_{n-1} + \cdots + a_0).$$

Note that, for every k, $10^k - 1$ is a number formed entirely by 9s, so it is divisible by 9 (and hence by 3). Thus the boxed part is divisible by both 3 and 9.

An integer is divisible by 3 (or 9) if and only if the sum of its digits is divisible by 3 (or 9).

Challenge Find (with explanation/proof) divisibility rules for 7, 11 and 13.

0.4 The division algorithm

This algorithm is the foundation upon which the whole edifice of divisibility theory rests. Though the idea is familiar to everyone who has been to primary school, here we state it in rigourous language.

Theorem 0.4.1 (The division algorithm)**.** *Given an integer a and a non-zero integer b, there exist unique integers q and r satisfying*

$$a = qb + r, \qquad 0 \leq r < |b|.$$

*The integers q and r are known respectively as the **quotient** and the **remainder** of the division of a by b.*

Think! Why does this theorem require a proof? Why can it not be considered "obvious"?

Definition 0.1. An integer a is said to be **divisible** by $b \neq 0$ (in symbols, $b \mid a$) if the remainder obtained upon division of a by b is zero. We write $b \nmid a$ to mean that b does not divide a.

Definition 0.2. An integer p is said to be a **prime** if its only divisors are $\{-1, 1, -p, p\}$. In other words, if $a \mid p$ then $|a| = 1$ or $|a| = p$.

0.5 The greatest common divisor

Definition 0.3. Consider two integers a and b, not both of which are equal to zero. The **greatest common divisor** of a and b (denoted by $\gcd(a, b)$) is the unique positive integer d that satisfies the following

- $d \mid a$ and $d \mid b$.
- If $c \mid a$ and $c \mid b$ then $c \leq d$.

We state the next result without a proof (and the reader is encouraged to find one).

Euclid's lemma If $a \mid bc$ and $\gcd(a,b)=1$, then $a \mid c$.

Think! Let a and b be two integers. If p is a prime, and $p \mid ab$, then prove that p divides at least one of a, b.

0.6 The Fundamental Theorem of Arithmetic

Theorem 0.4. *Every positive integer $n > 1$ can be represented uniquely as a product of prime powers:*

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and the n_i are positive integers.

Challenge Using Euclid's lemma, prove the fundamental theorem of Arithmetic.