Basics of Numbers, ~~Matrices, and Algorithms~~

Md. Shahriar Karim
Assistant Professor
Department of Electrical and Computer engineering
North South University, Bangladesh
Email: shahriar.karim@northsouth.edu

1 Number Theory [1]

In mathematics, we always need numbers to count and quantify to model systems of our interests. Number Theory is a branch of mathematics dedicated explicitly to studying integers and their properties. To facilitate our mathematical analysis, all the numbers are often subdivided into overlapping sets with specific names attached to them. A few such number sets that we use frequently are:

$$\begin{aligned}
&\mathbb{R} = \{-\infty \ldots -3, \ldots, -2.5 \ldots, -2 \ldots, \ldots 0 \ldots 0.5, \ldots 1, \ldots 1.5, \ldots 2, \ldots \ldots \infty\} \\
&\mathbb{Z} = \{-\infty \ldots -300, \ldots -1 \ldots \ldots 0 \ldots \ldots 200, \ldots \ldots + \infty\} \\
&\mathbb{Q} = \{-\infty \ldots -3, \ldots, -2.5 \ldots, -2 \ldots, \ldots 0 \ldots 0.5, \ldots 1, \ldots 1.5, \ldots 2, \ldots \ldots \infty\} \\
&\mathbb{N} = \{1, 2, 3, 4, \ldots \ldots \infty\}
\end{aligned}$$

Unless specified otherwise, all the variables in this chapter will be from $\mathbb{Z}$.
Question: Why are these topics necessary? Where do we use them in computer science? A quick, familiar, and relevant answer would be assigning computer memory locations to files handled by the computer to complete the desired tasks. In short, our goal is to review the earlier topics and touch upon a few simple application examples in computer arithmetic and cryptography [1].

2 Integers and its divisibility

Mathematics of integers is necessary for different computer science applications. For instance, integers-based mathematics such as divisibility, modulator arithmetic, Least Common Multiplier (LCM), Greatest Common Divisor (GCM), Prime numbers, etc., and their different applications are important for cryptography.

2.1 Definition

Consider two integers $a, b \in \mathbf{Z}$, where $\mathbf{Z}$ is the set of all integers. Assuming the division of the form a/b, the outcome (or the quotient) may be an integer or a fraction. For instance, $5/2 = 2.5$ is a fraction, whereas $4/2 = 2$ generates an integer as the quotient. As the norm suggests, divisibility goes along with an integer quotient, and the precise definition of divisibility is:

Divisibility

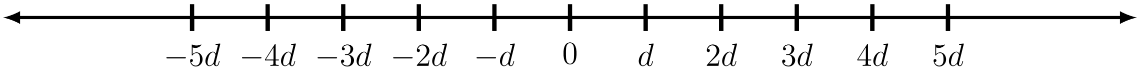
- If a and b are two integers with a be the nonzero integer $(a \neq 0)$, then the term a *divides* b means that there is an integer c available for which $a = bc$.

- a divides b is **denoted as** $a|b$, where a is the factor and b is the multiple of a.

Example: Assume that n and d positive integers ($n, d \in \mathbf{Z}^+$), how many positive integers less than or equal to n are divisible by d

Solution: All the positive integers divisible by d are of the form dk, where k is a positive integer. As observed from the number line drawn below, if n resides between kd and $(k+1)d$, the largest integer divisible by d becomes kd. So, a generalized representation of total numbers using the concept of floor function:

$$\lfloor n/d \rfloor$$



Facts on Divisibility

1. If $a|b$, then $a|bc$, $\forall a, b, c \in \mathbb{Z}$

2. If $a|b$ and $b|c$, then $a|c$, $\forall c \in \mathbb{Z}$

3. If $a|b$ and $a|c$, then $a|b + c$

4. If $a|b$ and $a|c$, then $a|mb + nc$ for any $m, n \in \mathbb{Z}$

Proof.
1: $a|b$ suggests that $b = ma$, $\forall a, b, m \in \mathbb{Z}$. Multiplying both sides by $n\mathbb{Z}$, we obtain $bc = mac = (mc)a = ka$, where $k \in \mathbb{Z}$. So, $bc = ka$ suggests that a divides bc; that is, $a|bc$ QED

Proof.
2: $a|b$ suggests that $b = ma$. Similarly, $b|c$ suggests that $c = nb$. Here, both m, n are integers. So, $c = nb = n(ma) = (mn)a = Ka$, where integer $K = mn$. Therefore, $a|c$ QED

Proof.
3: Let $b = ma$ as a divides b. Similarly, $c = na$ for $a|c$. By adding both, we obtain $b + c = a(m + n)$, where m and n are integers. So, $a|(b + c)$. QED

Proof.
4: From the definition of divisibility, that is, if $a|b$ then $a|bm$, $\forall a, b, m \in \mathbb{Z}$. Similarly, for

$a|c$ we obtain $a|nc$. From Part 3: if $a|b$ and $a|c$ then $a|(b+c)$. By plugging in the values of b, c finally we obtain $a|(bm+nc)$ QED

2.2 Division Algorithm

Every time we divide an integer a by a positive integer, the outcomes include two different quantities: quotient (q) and the remainder (r). Interestingly, the integer can be expressed using the quotient and remainder obtained in the division process.

Division Theorem

Theorem 1. *Let* $\boldsymbol{a}$ *be the integer divided by another positive integer* $\mathbf{d}$*. Then, there are **unique** integers* q *and* r $(0 \leq r < d)$ *such that* $\boldsymbol{a = qd + r}$*.*

Here, a *is the dividend,* d *is the divisor,* q *is the quotient, and* r *is the remainder. The notations used for* q *and* r *are: the quotient* $q = a$ **div** d *and the remainder* $r = a$ **mod** d*.*

The condition r $(0 \leq r < d)$ is crucial, which suggests that the **remainder r is always positive** as per the division theorem.

Example: What are the quotient and remainder when 51 is divided by 11, 17?
Solution: 101 could be written as $101 = 11 \times 9 + 2 = \lfloor 101/11 \rfloor + 2$. So, quotient here is $q = 9 = 101$ **div** 11 and remainder $r = 2 = 101$ **mod** 11. Similarly, for 17, we can write $q = 5 = 101$ **div** 17 and remainder $r = 16 = 101$ **mod** 17.

Example: What are the quotient and remainder when -11 is divided by 3?
Solution: We can write: $-11 = 3(-4) + 1$ or $-11 = 3(-3) - 2$. However, as the division theorem states $a = q + r$, and r is always positive, $-11 = 3(-4) + 1$ is the acceptable representation. Hence, quotient $q = -11$ **div** $3 = -4$ and remainder $r = 1 = 11$ **mod** 3. Here, the other option $r = -2$ violates the condition $0 \leq r < d$.

2.3 Modular Arithmetic

In many calculations, we are often interested in the remainder. For instance, if the current time is 7:00 AM, what time is it after 10 hours? As the clock cycle is 12 hours and transforms from AM to PM, the time would be $7 + 10 = 17$ hours divided by the 12 hours clock cycle. The remainder would provide us with the time after the 10 hours. In many problems, we are primarily interested in the remainder, and modular Arithmetic accommodates such calculations with integers. The greatest mathematician Karl Fredrich Gauss laid the foundation for modern number theory and developed the current approaches for modulator arithmetic.

Concept of Congruence

Theorem 2. *Let $\boldsymbol{a}$ be the integer divided by another positive integer* **d**. *Then, there are **unique** integers q and r $(0 \leq r < d)$ such that $\boldsymbol{a = qd + r}$.*

*Here, a is the dividend, d is the divisor, q is the quotient, and r is the remainder. The notations used for q and r are: the quotient $q = a$ **div** d and the remainder $r = a$ **mod** d.*

The condition r $(0 \leq r < d)$ is crucial, which suggests that the **remainder r is always positive** as per the division theorem.

2.3.1 Definition: Congruence

If $a,\ b \in \mathbb{Z}$ and $m \in \mathbb{Z}^{+}$, then a is congruent to b **modulo** m.

References

[1] Kenneth H Rosen. *Discrete mathematics and its applications.* The McGraw Hill Companies,, 2007.