Number Theory

Munir Uz Zaman

Date: December 22, 2021

Contents

1 Divisibility

§1.1 Divisibility Properties

Theorem 1.1.1 (Division Algorithm)
For any integers a, b, with $b > 0$, there exists **unique** integers q and r such that,

$$a = qb + r, \quad 0 \leq r < b$$

The integers r and q are called the *remainder* and *quotient* upon dividing a by b, respectively.

Proof: Suppose $\mathcal{S} = \{a - qb \mid q \in \mathbb{Z}, a - qb \geq 0\}$. We want to show that r is the least element of the set $\mathcal{S}$. But first we have to show that $\mathcal{S}$ is a non-empty set. Notice,

$$\left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b} \implies \left\lfloor \frac{a}{b} \right\rfloor \times b \leq a \implies 0 \leq a - \left\lfloor \frac{a}{b} \right\rfloor b$$

Therefore for the choice $q = \left\lfloor \frac{a}{b} \right\rfloor$, $a - \left\lfloor \frac{a}{b} \right\rfloor b \in \mathcal{S}$. Thus $\mathcal{S}$ is a non-empty set of non-negative integers.

Theorem (Well Ordering Principle)
Every non-empty set of non-negative integers contains a least element. That is if $\mathcal{S}$ is a non-empty set of non-negative integers then there exists a non-negative integer $n \in \mathcal{S}$ such that $n \leq x$ for every $x \in \mathcal{S}$.

Now from the Well Ordering Principle we know that $\mathcal{S}$ contains a least element. Let r be the least element of $\mathcal{S}$. Assume $r \geq b$ and let $r' = r - b$. Since $r \geq b$ we have,

$$r' = r - b \geq 0 \implies r' = a - qb - b = a - (q+1)b \geq 0 \implies r' \in \mathcal{S}$$

But this contradicts our assumption that r is the least element of $\mathcal{S}$. Thus r must be less than b. Now we will prove the uniqueness of the integers r and q. Suppose there exists integers q' and r', with $0 \leq r' < b$, such that $a = q'b + r'$. Now,

$$q'b + r' = qb + r \implies (q' - q)b = r - r' \implies \left|q' - q\right| b = \left|r - r'\right|$$

Adding the two inequalities, $0 \leq r < b$ and $-b < -r' \leq 0$, we get $-b < r - r' < b \implies 0 \leq |r - r'| < b$. Therefore,

$$0 \leq \left|r - r'\right| < b \implies 0 \leq \left|q' - q\right| b < b \implies 0 \leq \left|q' - q\right| < 1$$

Since $|q' - q|$ is a non-negative integer we must have $q' - q = 0 \implies q = q'$ and which in turn implies $r = r'$.

♣

Corollary 1.1.1.1

If a and b are integers, with $b \neq 0$, then there exists unique integers q and r such that,

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

Definition 1.1.1. An integer n is said to be divisible by m if and only if there exists an integer k such that $n = km$. If n is divisible by m then we symbolically write this as, $m \mid n$. This is read as "m divides n".

For example, the number 35 is divisible by 7 as $35 = 5 \times 7$. Therefore we can write $7 \mid 35$. From the definition it is clear that

$$m \mid n \iff \frac{n}{m} \in \mathbb{Z}$$

Here are some basic properties of divisibility.

Theorem 1.1.2

If $n \mid a$ and $n \mid b$, and $x, y \in \mathbb{Z}$ then, $n \mid a$ and $n \mid b \implies m \mid ax \pm by$.

The proof is very simple and so it is left as an exercise to the reader.

Theorem 1.1.3

If $m \mid n$ then either $n = 0$ or $|m| \leq |n|$.

Proof: We know that there exists an integer k such that $n = km$. Now if $k \neq 0$ then $|k| \geq 1$,

$$n = km \implies |n| = |k| \cdot |m| \geq |m| \implies |n| \geq |m|$$

If $k = 0$ then $n = 0$. And we are done!

♣

Theorem 1.1.4

If x, y are two distinct integers and n is a natural number then,

$$x^n - y^n = (x - y)\left(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\right)$$

Proof: We will first prove that if r is a real number then,

$$\left(1 + r + \cdots + r^{n-1}\right)(r - 1) = r^n - 1$$

Assume $S = 1 + r + \cdots + r^{n-1}$. Now,

$$\begin{aligned} rS &= r + r^2 + \cdots + r^{n-1} + r^n \\ S &= 1 + r + r^2 + \cdots + r^{n-1} \\ (r-1)S &= r^n - 1 \implies \left(1 + r + \cdots + r^{n-1}\right)(r - 1) = r^n - 1 \end{aligned}$$

♣

2 Modular Arithmetic

§2.1 Basics

§2.2 Linear Congruences

Theorem 2.2.1

The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$ where $d = \gcd(a, n)$. Moreover the equation will have d incongruent solutions modulo n.

Proof: $ax \equiv b \pmod{n}$ implies that there exists an integer y such that $ax - b = ny \implies ax - ny = b$. We already know that the equation $ax - ny = b$ will have a solution if and only if $\gcd(a, n) \mid b$.
Now let us show that the equation will have d incongruent solutions modulo n. We know that if (x_0, y_0) is a solution of $ax - ny = b$ then every other solution of the equation will be of the form

$$x = x_0 + \frac{n}{d}t \quad y = y_0 + \frac{a}{d}t$$

where t is some integer. Now let us consider the solutions when $0 \leq t \leq d - 1$. We claim that these are all of the incongruent solutions modulo n.
We will first show that if $0 \leq t_1 < t_2 \leq n - 1$ are two distinct integers then the two solutions $x_0 + \frac{n}{d}t_1$ and $x_0 + \frac{n}{d}t_2$ must be incongruent modulo n. Suppose that the two solutions are congruent then

$$\begin{aligned} x_0 + \frac{n}{d}t_1 &\equiv x_0 + \frac{n}{d}t_2 \pmod{n} \\ \implies \frac{n}{d}t_1 &\equiv \frac{n}{d}t_2 \pmod{n} \end{aligned}$$

Now since $\gcd(n/d, n) = n/d$ we get

$$t_1 \equiv t_2 \pmod{d} \implies d \mid t_2 - t_1$$

But $d \mid t_2 - t_1 \implies d \leq t_2 - t_1$ which is impossible because $t_2 - t_1 < d$. Therefore the solutions for which $0 \leq t \leq d - 1$ must be incongruent modulo n.
Now it remains to show that any other solution $x_0 + \frac{n}{d}t$ is congruent to one of the d solutions for which $0 \leq t \leq d - 1$. From the division algorithm we know that there exists integers q and t' where $0 \leq t' \leq d - 1$ such that $t = dq + t'$. Now,

$$\begin{aligned} x_0 + \frac{n}{d}t &\equiv x_0 + \frac{n}{d}(dq + t') \pmod{n} \\ &\equiv x_0 + \frac{n}{d} \times dq + \frac{n}{d} \times t' \pmod{n} \\ &\equiv x_0 + \frac{n}{d}t' \pmod{n} \end{aligned}$$

We are done!

♣

Corollary 2.2.1.1

If a and n are coprime integers, that is $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ where b is some integer has a unique solution modulo n.

Example 2.2.1

Find all incongruent solutions of the linear congruence $36x \equiv 8 \pmod{102}$

Solution: Since $\gcd(36, 102) = 6$ and $6 \nmid 8$, there does not exist any solution to this linear congruence.

♣