Number Theory

Munir Uz Zaman

Date: December 17, 2021

Contents

1 Modular Arithmetic

§1.1 Basics

§1.2 Linear Congruences

Theorem 1.2.1

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 1.2.1.1

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 1.2.1

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.

♣