Number Theory

Lakshmy K V

March 30, 2022

Let n be a positive integer. Consider the following linear congruence

$$ax \equiv b \bmod n,$$

where a is an integer which is not divisible by n. We want to find all integers x which satisfy the above congruence. It is clear that if r is a solution, so is any $s \equiv r$ modulo n. So by a solution we mean a congruence class mod n whose members satisfy the equation.

we find that it is possible to have linear congruence which has *no solutions*, *only one solution* or *more than one solutions*. For example, the linear congruence

$$2x \equiv 5 \bmod 6$$

has no solution: if r is a solution, then 6 must divide $2r - 5$, which implies in particular that $2r - 5$ must be even. But that is not possible as $2r$ is even but 5 is odd. Now consider

$$2x \equiv 1 \bmod 3.$$

If we look at three congruence classes modulo 3, we find that [0] and [1] are not solutions, but [2] is a solution. Therefore, this congruence has a unique equivalence class of solutions. Now consider the congruence

$$4x \equiv 2 \bmod 6.$$

We can check the 6 elements of a complete residue system of 6, and observe that both [2] and [5] are solutions.

THEOREM 2.10. *The congruence*

$$ax \equiv b \ mod \ n$$

has a solution if and only if $gcd(a,n)$ divides b.

Proof: Let $gcd(a,n) = d$. First assume that the above congruence has a solution r. Then,

$$\begin{aligned} ar &\equiv b \bmod n \\ \implies n &\mid (b - ar) \\ \implies d &\mid (b - ar), \quad d \mid a \\ \implies d &\mid (b - ar + ar) \\ \implies d &\mid b. \end{aligned}$$

Conversely, suppose d divides b. We will now exhibit a solution for the above congruence. We can write $b = db_1$ for some integer b_1. By Euclid's algorithm, we can find integers r_1 and s_1 such that

$$\begin{aligned} ar_1 + ns_1 &= d \\ \implies b_1(ar_1 + ns_1) &= db_1 \\ \implies a(b_1r_1) + n(b_1s_1) &= b \\ \implies a(b_1r_1) &\equiv b \bmod n. \qquad \square \end{aligned}$$

The examples that we saw above are consistent with the theorem. The congruence $2x \equiv 5 \mod 6$ had no solution as the $gcd(2,6) = 2$ does not divide 5. But $2x \equiv 1 \mod 3$ has a solution as the gcd of 2 and 3 divides 1. In the third example too, the gcd of 4 and 6 divides 2, and we could find solutions.

THEOREM 2.11. *Consider the congruence*

$$ax \equiv b \ mod \ n,$$

where the $gcd(a, n) = d$ *divides* b. *Let* x_0 *be a solution. Then all the other solutions are precisely given by the following set:*

$$x_0, \;\; x_0 + \frac{n}{d}, \;\; x_0 + \frac{2n}{d}, \;\; \cdots, \;\; x_0 + \frac{(d-1)n}{d}.$$

Proof: It is a trivial exercise to verify that for all i with $0 \leq i \leq (d-1)$, $x_0 + \frac{in}{d}$ is a solution $ax \equiv b \bmod n$.

Next, we show that any two distinct elements in the above set are inequivalent modulo n. As d divides n, we can write $n = dk$ for some integer k. Consider i, j such that $0 \leq i, j \leq (d-1)$. Then ,

$$\begin{aligned}
x_0 + \frac{in}{d} &\equiv x_0 + \frac{jn}{d} \bmod n \\
\implies \frac{in}{d} &\equiv \frac{jn}{d} \bmod n \\
\implies ik &\equiv jk \bmod dk \qquad (n = dk) \\
\implies dk &\mid k(i-j) \\
\implies d &\mid (i-j).
\end{aligned}$$

But $-(d-1) \leq (i-j) \leq (d-1)$, hence $d \mid (i-j)$ implies $i = j$. Thus, two distinct elements in the above set can not be congruent modulo n.

We still have to show that any solution x_1 must be congruent to one of the d elements in the set modulo n. We have $n = dk$ and $a = da_1$, where $gcd(k, a_1) = 1$.

$$\begin{aligned} & ax_1 && \equiv b \equiv ax_0 \bmod n \\ \implies & dk && \mid da_1(x_1 - x_0) \\ \implies & k && \mid (x_1 - x_0) \quad \text{as } k \text{ and } a_1 \text{ are coprime} \\ \implies & x_1 && = x_0 + ik \qquad \text{for some integer } i \\ \implies & x_1 && = x_0 + i\frac{n}{d}. \end{aligned}$$

It is enough to consider the above integer i in the range $\{0,\ 1,\ ,(d-1)\}$, as

$$i \equiv i' \bmod d \implies x_0 + \frac{in}{d} \equiv x_0 + \frac{i'n}{d} \bmod n. \ \square$$

Corollary 2.12. *The congruence*

$$ax \equiv b \ mod \ n$$

has a unique solution if and only if a and n are coprime.

In the examples that we have discussed in this lecture, we saw that $2x \equiv 1 \mod 3$ has a unique solution, namely [2], as 2 and 3 are coprime. On the other hand, $4x \equiv 2 \mod 6$ has more than one solution, as 4 and 6 are not coprime.

Simultaneous Linear Congruences

Consider the congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 2 \bmod 8.$$

Clearly, there is no common solution to both. The first one indicates that a solution x_0 must be an odd integer, as $x_0 - 3$ is divisible by 2, whereas the second one can have only even integers as solutions. On the other hand, the congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 2 \bmod 7$$

have a common solutions 23. We will now determine a sufficient condition for such congruences to have common solutions. We will also see when such a solution is unique. Note that in the second set of congruences, the moduli 10 and 7 are coprime. We will first show that when we have coprime moduli the simultaneous congruences will always have a solution.

Chinese Remainder Theorem

THEOREM 2.13. *Consider the linear congruences*

$$\begin{aligned} x &\equiv a_1 \; mod \; m_1, \\ x &\equiv a_2 \; mod \; m_2, \\ \vdots & \quad \vdots \\ x &\equiv a_n \; mod \; m_n. \end{aligned}$$

If the m_i are pairwise coprime, then these congruences have a common solution. Further, such a common solution is unique modulo $M = m_1 \cdot \cdots \cdot m_n$.

Proof: Let us define n integers

$$M_i = \frac{M}{m_i} = m_1 \cdot \cdots \cdot m_{i-1} \cdot m_{i+1} \cdot \cdots \cdot m_n, \qquad 1 \leq i \leq n.$$

As m_i's are pairwise coprime, each M_i is coprime to the corresponding m_i. For each i $(1 \leq i \leq n)$, consider the linear congruence

$$M_i x \equiv 1 \bmod m_i.$$

As M_i and m_i are coprime, the above congruence has a solution. So there is an integer $\tilde{m}_i$ such that

$$M_i \tilde{m}_i \equiv 1 \bmod m_i.$$

We claim that

$$x_0 = a_1 M_1 \tilde{m}_1 + \cdots + a_i M_i \tilde{m}_i + \cdots + a_n M_n \tilde{m}_n$$

satisfies all the given congruences in the theorem. Observe that

$$\begin{aligned} x_0 &= a_1 M_1 \tilde{m}_1 + \cdots + a_i M_i \tilde{m}_i + \cdots + a_n M_n \tilde{m}_n \\ &\equiv a_i M_i \tilde{m}_i \bmod m_i \\ &\equiv a_i \bmod m_i. \end{aligned}$$

As for the uniqueness of common solutions, let x_1 be another common solution to the above system of linear congruences. Then, for each i, we have

$$x_1 \equiv a_i \equiv x_0 \bmod m_i \quad \Longrightarrow \quad m_i | (x_1 - x_0).$$

As the m_i's are coprime, we have

$$(m_1 \cdot \cdots \cdot m_n) | (x_1 - x_0) \implies x_1 \equiv x_0 \bmod M. \qquad \square$$

Exercise: Solve the following system of linear congruences

$$x \equiv 2 \bmod 6, \quad x \equiv 1 \bmod 5, \quad x \equiv 3 \bmod 7.$$

Solution: Observe that the moduli are pairwise coprime. Here,

$$M = 6.5.7 = 210, \qquad M_1 = 5 \cdot 7 = 35, \qquad M_2 = 6 \cdot 7 = 42, \qquad M_3 = 6 \cdot 5 = 30.$$

Now,

$$\begin{aligned}
35\tilde{m}_1 \equiv 1 \bmod 6 &\implies -\tilde{m}_1 \equiv 1 \bmod 6 \implies \tilde{m}_1 \equiv 5 \bmod 6\\
42\tilde{m}_2 \equiv 1 \bmod 5 &\implies 2\tilde{m}_2 \equiv 1 \bmod 5 \implies \tilde{m}_2 \equiv 3 \bmod 5\\
30\tilde{m}_3 \equiv 1 \bmod 7 &\implies 2\tilde{m}_3 \equiv 1 \bmod 7 \implies \tilde{m}_3 \equiv -3 \bmod 7
\end{aligned}$$

Hence, by , we have a solution

$$x_0 = 2 \cdot 35 \cdot 5 + 1 \cdot 42 \cdot 3 + 3 \cdot 30 \cdot (-3) = 350 + 126 - 270 = 206.$$

The solution is unique modulo $M = 6 \cdot 5 \cdot 7 = 210.$ $\square$

Exercise: Solve the system of linear congruences

$$5x \equiv 1 \text{ mod } 6, \quad 3x \equiv 2 \text{ mod } 5, \quad 4x \equiv 5 \text{ mod } 7.$$

Solution: Observe that each of the above congruences is solvable, for example, in the first one, 5 is coprime to 6. We have $5.5 \equiv 1$ mod 6, so we can multiply the first congruence by 5 to obtain $x \equiv 5$ mod 6. Similarly, we multiply the second congruence by 2 (as $3 \cdot 2 \equiv 1$ mod 5) to obtain $x \equiv 4$ mod 5. We multiply the the congruence above by 2 to obtain $x \equiv 10 \equiv 3$ mod 7. Thus, the given system is reduced to

$$x \equiv 5 \text{ mod } 6, \quad x \equiv 4 \text{ mod } 5, \quad x \equiv 3 \text{ mod } 7.$$

Proceeding as in the previous example, we have

$$M = 6 \cdot 5 \cdot 7 = 210, \qquad M_1 = 5 \cdot 7 = 35, \qquad M_2 = 6 \cdot 7 = 42, \qquad M_3 = 6 \cdot 5 = 30.$$

and

$$\begin{aligned} 35\tilde{m}_1 &\equiv 1 \bmod 6 &\implies& \quad \tilde{m}_1 \equiv 5 \bmod 6 \\ 42\tilde{m}_2 &\equiv 1 \bmod 5 &\implies& \quad \tilde{m}_2 \equiv 3 \bmod 5 \\ 30\tilde{m}_3 &\equiv 1 \bmod 7 &\implies& \quad \tilde{m}_3 \equiv -3 \bmod 7 \end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 5 \cdot 35 \cdot 5 + 4 \cdot 42 \cdot 3 + 3 \cdot 30 \cdot (-3) = 875 + 504 - 270 = 1109 \equiv 59 \bmod 210.$$

The solution is unique modulo 210. $\square$

THEOREM 2.14. *Consider the linear congruences*

$$\begin{aligned} x &\equiv a_1 \ mod \ m_1, \\ x &\equiv a_2 \ mod \ m_2, \\ \vdots & \quad \vdots \\ x &\equiv a_n \ mod \ m_n, \end{aligned}$$

where the moduli m_i's are not necessarily pairwise coprime. Let $d_{i,j} = gcd(m_i, m_j)$ for $i \neq j$. Then the above system has a simultaneous solution if and only if $d_{i,j}$ divides $(a_i - a_j)$ for all $i \neq j$. Further, such a solution is unique modulo $lcm(m_1, \cdots, m_n) = l$.

Exercise: Solve the system of linear congruences

$$x \equiv 2 \text{ mod } 12, \quad x \equiv 6 \text{ mod } 10, \quad x \equiv 11 \text{ mod } 45.$$

Solution: Observe that

$$gcd(12,10)|(6-2), \quad gcd(10,45)|(11-6), \quad gcd(12,45)|(11-2).$$

By the above theorem, the given system will have a solution. Here, the lcm of 12, 10, 45 is $2^2 \cdot 3^2 \cdot 5 = 180$. Hence, the given system reduces to

$$x \equiv 2 \text{ mod } 2^2, \quad x \equiv 6 \text{ mod } 5, \quad x \equiv 11 \text{ mod } 3^2.$$

For the above system with prime-power moduli which are pairwise coprime, we can apply Chinese Remainder Theorem with

$$M = 2^2 \cdot 3^2 \cdot 5 = 180 = l, \qquad M_1 = 5 \cdot 9, \qquad M_2 = 4 \cdot 9, \qquad M_3 = 4 \cdot 5.$$

Now,

$$\begin{aligned}
5\cdot 9\cdot \tilde{m}_1 \equiv 1 \bmod 4 \quad &\implies \quad \tilde{m}_1 \equiv 1 \bmod 4\\
4\cdot 9\cdot \tilde{m}_2 \equiv 1 \bmod 5 \quad &\implies \quad \tilde{m}_2 \equiv 1 \bmod 5\\
4\cdot 5\cdot \tilde{m}_3 \equiv 1 \bmod 9 \quad &\implies \quad 2\tilde{m}_3 \equiv 1 \bmod 9 \implies \quad \tilde{m}_3 \equiv -4 \bmod 9
\end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 2\cdot(5\cdot 9)\cdot 1 + 6\cdot(4\cdot 9)\cdot 1 + 11\cdot(4\cdot 5)\cdot(-4) = -574 \equiv 146 \bmod 180.$$

The solution is unique modulo 180. $\square$