LINEAR EQUATIONS WITH MODULO N

Link to: physicspages home page.

To leave a comment or report an error, please use the auxiliary blog and include the title or URL of this post in your comment.

Post date: 17 September 2025.

Reference: *A Gentle Introduction to Group Theory*, Bana Al Subaiei & Muneerah Al Nuwairan, Section 3.6.

The $\mod n$ relation is an equivalence relation. The set $\mathbb{Z}_n$ is defined as the set of equivalence classes for the integer n:

$$\mathbb{Z}_n = \left\{[0]_n, [1]_n, \ldots, [n-1]_n\right\} \tag{1}$$

Addition and multiplication can be defined on $\mathbb{Z}_n$. These create new relations defined as follows.

$$\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \text{ (addition)} \tag{2}$$

$$\otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \text{ (multiplication)} \tag{3}$$

Addition is defined as

$$[a] \oplus_n [b] = [a+b] \tag{4}$$

where the square brackets indicate equivalence classes.

Multiplication is defined as

$$[a] \otimes_n [b] = [ab] \tag{5}$$

A linear equation with mod n is defined as an equation with one variable, and is written in terms of the equivalence classes:

$$([a] \otimes_n [x]) \oplus_n [b] = [c] \tag{6}$$

where $[x]$ is the class to be determined.

We can write this equation in a simpler form as

$$ax + b \equiv c \mod n \tag{7}$$

where the $\equiv$ sign signifies equality modulo n.

Theorem 1. *(Existence of solutions) Let $n \in \mathbb{N}$and a, b and c be integers. The equation 7 has a solution (possibly more than one) if and only if* $\gcd(a,n) \mid (c-b)$.

Another useful theorem is:

Theorem 2. *Let $n \in \mathbb{N}$ and a, b and c be integers. If $[x_0]$ is a solution to 7, then the set*

$$\left\{\left[x_0 + \frac{n}{\gcd(a,n)}t\right] : t \in \mathbb{Z}\right\} \tag{8}$$

$[x]$	$12x-10 \mod 7$
$[0]$	$[-10]=[4]$
$[1]$	$[2]$
$[2]$	$[14]=[0]$
$[3]$	$[26]=[5]$
$[4]$	$[38]=[3]$
$[5]$	$[50]=[1]$
$[6]$	$[62]=[6]$

TABLE 1. Solving $12x-10=2 \mod 7$.

contains all possible solutions in $\mathbb{Z}_n$. All distinct *solutions are given by 8 with t restricted to* $0 \leq t < \gcd(a,n)$.

The proofs are rather long and can be found in Al Subaiei & Al Nuwairan, section 3.6.

The problem with this theorem is that we need to find the solution $[x_0]$ in order to generate the other solutions. For small values of n this can be done by trial and error.

Example 1. Given

$$3x+3 \equiv 1 \mod 9 \tag{9}$$

We apply theorem 1 with $a=3$, $b=3$, $c=1$ and $n=9$. By inspection (or using Euclid's algorithm) we see that $\gcd(3,9)=3$, and $c-b=-2$ since $3 \not| -2$, this equation has no solution.

Example 2. Given

$$12x-10 \equiv 2 \mod 7 \tag{10}$$

We have $a=12$, $b=-10$, $c=2$ and $n=7$. Thus $\gcd(12,7)=1$ and $c-b=12$. Since 1 divides everything, this equation does have solutions. We can find them by trying the integers from 0 up to 6. See Table 1

We see that $[x]=[1]$ provides the only distinct solution. From 8, other solutions are $[8]$, $[15]$ and so on, but these are all equivalent to $[1]$.

Example 3. Given

$$6x+10 \equiv 20 \mod 3 \tag{11}$$

We have $a=6$, $b=10$, $c=20$ and $n=3$. Thus $\gcd(6,3)=3$ and $c-b=10$. Since $3 \not| 10$, this has no solutions.

$[x]$	$[7x \mod 6]$
$[0]$	$[0]$
$[1]$	$[7] = [1]$
$[2]$	$[14] = [2]$
$[3]$	$[21] = [3]$
$[4]$	$[28] = [4]$
$[5]$	$[35] = [5]$

TABLE 2. Solving $7x = 3 \mod 6$.

Example 4. Given

$$7x \equiv 3 \mod 6 \tag{12}$$

we have $a = 7$, $b = 0$, $c = 3$ and $n = 6$. Thus $\gcd(7,6) = 1$ so there are solutions. This time, we can just try the integers from 0 to 5 to see if they are solutions. See Table 2.

The only distinct solution is $[x] = [3]$.

Example 5. Given

$$3x + 7 \equiv 1 \mod 15 \tag{13}$$

we have $a = 3$, $b = 7$, $c = 1$ and $n = 15$. Thus $\gcd(3,15) = 3$ and $3|(1-7)$ so there are solutions. We can find the first solution as follows. Subtract 7 from both sides to get

$$3x \equiv -6 \mod 15 \tag{14}$$

Now $-6 = -15 + 9$ so $[-6] = [9]$ and we have

$$3x \equiv 9 \mod 15 \tag{15}$$

$$x \equiv 3 \mod 15 \tag{16}$$

Thus $[x] = [3]$ is a solution. Applying 8 we can find other solutions. We have

$$\frac{n}{\gcd(a,n)} = \frac{15}{3} = 5 \tag{17}$$

Therefore, we can take $0 \leq t < \gcd(a,n)$ or $0 \leq t < 3$ to get the other solutions

$$[3+5] = [8] \tag{18}$$

$$[3+10] = [13] \tag{19}$$

We can verify these by checking in 13.

$$[3 \times 8 + 7] = [31] = [15 \times 2 + 1] \equiv [1] \tag{20}$$

$$[13 \times 3 + 7] = [46] = [15 \times 3 + 1] \equiv [1] \tag{21}$$