
STEM Class: Modular Arithmetic

Author

Justin STEVENS

Definition 1.0.1. We call two numbers *relatively prime* if they don't share any prime factors. We write the *greatest common divisor* of two numbers as the largest number that divides both of them. We write this as $\gcd(a, b)$ or sometimes shorthand to (a, b) .

IMPORTANT: For this whole text, p is assumed to be a prime.

Example 1.0.1. Are 2 and 3 relatively prime? What about 3 and 6? What about 8 and 2? Calculate the gcd's of all these pairs.

Solution. We prime factorize all the numbers.

- $2 = 2^1, 3 = 3^1$ so they are indeed relatively prime. $\gcd(2, 3) = 1$
- $3 = 3^1, 6 = 3^1 \cdot 2^1$ so they are not relatively prime. $\gcd(3, 6) = 3$
- $8 = 2^3, 2 = 2^1$ so they are not relatively prime. $\gcd(8, 2) = 2$

□

1.1 Linear Congruences

Motivation: We know the congruence $5 \equiv 2 \pmod{3}$ and equations such as $2x + 1 = 5$. Now, we combine the two concepts of modular arithmetic and equations to get **linear congruences**.

Definition 1.1.1. A linear congruence is an equation of the form

$$ax \equiv b \pmod{c} \quad (1.1)$$

Since this notation may be a bit intense, we look at several examples first.

Example 1.1.1. Solve the equation $2x \equiv 2 \pmod{3}$.

Solution.

$$\begin{cases} 2 \cdot 0 \equiv 0 \pmod{3} \\ 2 \cdot 1 \equiv 2 \pmod{3} \\ 2 \cdot 2 \equiv 4 \equiv 1 \pmod{3} \end{cases} \implies x \equiv 1 \pmod{3}$$

□

Example 1.1.2. Solve the equations $2x \equiv 5 \pmod{7}$, $3x \equiv 8 \pmod{11}$, $3x \equiv 1 \pmod{2}$, $9x \equiv 1 \pmod{11}$. What do you notice?

Solution. By trial and error we arrive at

- $2x \equiv 5 \pmod{7} \implies x \equiv 6 \pmod{7}$
- $3x \equiv 8 \pmod{11} \implies x \equiv 10 \pmod{11}$
- $3x \equiv 1 \pmod{2} \implies x \equiv 1 \pmod{2}$
- $9x \equiv 1 \pmod{11} \implies x \equiv 5 \pmod{11}$

We notice that in all cases there is only one solution for x . We also notice that looking back at the notation $ax \equiv b \pmod{c}$ we have $\gcd(a, c) = 1$. □

Example 1.1.3. Solve the equations $2x \equiv 1 \pmod{2}$, $3x \equiv 2 \pmod{6}$, $5x \equiv 19 \pmod{1000}$, $9x \equiv 10^{1000} \pmod{510}$. What do you notice?

Solution. We notice in the following examples, there are no solutions.

- $2x \equiv 0 \pmod{2}$ so there are no solutions.

- $3x \equiv 0, 3 \pmod{6}$ so there are no solutions.
- We must have $5x \equiv 19 \pmod{5} \implies 19 \equiv 0 \pmod{5}$ so there are no solutions.
- If $9x$ is divisible by 510, it must also be divisible by 3, so $9x \equiv 10^{1000} \pmod{3}$, therefore there are no solutions.

In all cases here there are no solutions to the linear congruences. We notice that $\gcd(a, c) \neq 1$ and $\gcd(a, c)$ doesn't divide b . \square

Example 1.1.4. *Conjecture whether or not there exists solutions to the following linear congruences: Again by trial and error we notice*

- $2x \equiv 9 \pmod{500}$
- $3x \equiv 5 \pmod{7}$
- $9x \equiv 2 \pmod{15}$
- $19x \equiv 1 \pmod{21}$
- $3x \equiv 6 \pmod{9}$
- $2x \equiv 4 \pmod{8}$

Solution. Again by trial and error we notice

We must have $9 \equiv 0 \pmod{2}$ contradiction. Notice that $\gcd(2, 500) = 2 \nmid 9$

- $x \equiv 4 \pmod{7}$. Notice that $\gcd(3, 7) = 1$.
- Taking the equation mod 3 we arrive at $2 \equiv 0 \pmod{3}$. Notice that $\gcd(9, 15) = 3 \nmid 2$.
- $x \equiv 10 \pmod{21}$. Notice that $\gcd(19, 21) = 1$.
- $x \equiv 2 \pmod{3}$ which gives three solutions mod 9: $x \equiv 2, 5, 8 \pmod{9}$. Notice that $\gcd(3, 9) = 3 \mid 6$.
- $x \equiv 2 \pmod{4}$. Notice that $\gcd(2, 8) = 2 \mid 4$.

\square

Example 1.1.5. *Take a conjecture as to how many solutions $ax \equiv b \pmod{c}$ can have as long as a and c are relatively prime. Then prove your conjecture.*

Solution. We predict that the equation has at most 1 solution mod c . \square

Proof. Assume that there exist two distinct solutions $a \equiv x_1, x_2 \pmod{c}$. Then we have

$$\begin{aligned} ax_1 &\equiv ax_2 \equiv b \pmod{c} \\ a(x_1 - x_2) &\equiv 0 \pmod{c} \end{aligned}$$

a and c share no common factors, so therefore we must have $x_1 - x_2 \equiv 0 \pmod{c}$ contradicting there being two distinct solutions. \square

1.2 A useful lemma

Example 1.2.1. *Reduce the set $\{2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4\} \pmod{5}$. What do you notice?*

Solution. We arrive at $\{2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4\} \equiv \{2, 4, 1, 3\} \pmod{5}$. This is the set of all natural numbers less than 5. \square

Example 1.2.2. *Reduce the sets below:*

- $\{3 \times 1, 3 \times 2, 3 \times 3, 3 \times 4, 3 \times 5, 3 \times 6\} \pmod{7}$
- $\{2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4, 2 \times 5, 2 \times 6\} \pmod{7}$
- $\{5 \times 1, 5 \times 2, 5 \times 3, \dots, 5 \times 9, 5 \times 10\} \pmod{11}$

What do you notice?

Solution. By reducing,

- $\{3 \times 1, 3 \times 2, 3 \times 3, 3 \times 4, 3 \times 5, 3 \times 6\} \equiv \{3, 6, 2, 5, 1, 4\} \pmod{7}$
- $\{2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4, 2 \times 5, 2 \times 6\} \pmod{7} \equiv \{2, 4, 6, 1, 3, 5\} \pmod{7}$

- $\{5 \times 1, 5 \times 2, 5 \times 3, 5 \times 4, 5 \times 5, 5 \times 6, 5 \times 7, 5 \times 8, 5 \times 9, 5 \times 10\} \pmod{11} \equiv \{5, 10, 4, 9, 3, 8, 2, 7, 1, 6\}$

We notice that again multiplying a set by a and reducing mod p results in the same set. \square

WARNING: $\{6 \times 1, 6 \times 2\} \equiv \{0, 0\} \pmod{3}$ **not** $\{1, 2\} \pmod{3}$.

Example 1.2.3. Complete the table:	$x \pmod{7}$	$2x \pmod{7}$
	1	?
	2	?
	3	?
	4	?
	5	?
	6	?

<i>Solution.</i>	$x \pmod{7}$	$2x \pmod{7}$	\square
	1	2	
	2	4	
	3	6	
	4	1	
	5	3	
	6	5	

Theorem 1.2.1. If $\gcd(a, p) = 1$ prove that

$$S = \{a \times 1, a \times 2, a \times 3, \dots, a \times (p-1)\} \equiv \{1, 2, 3, \dots, p-1\} = Q \pmod{p}$$

Proof. There are three conditions we need to prove that the two sets are the same.

- No element in S is divisible by p .
- No two elements of p are the same.
- $p - 1$ elements

The reason behind this is that no element in S is divisible by p , the elements are all distinct, and it has $p - 1$ elements, it forces these $p - 1$ elements to be $\{1, 2, 3, \dots, p - 1\}$.

We verify that indeed:

- $\gcd(ar, p) = 1$ when $\gcd(a, p) = 1$ and $\gcd(r, p) = 1$.
- Proven earlier.
- They both have $p - 1$ elements.

□

1.3 First Proof of Fermat's Little Theorem

One immediate application of the lemma is in solving modular congruences, as illustrated below.

Problem 1.3.1. Consider the set $\{2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4\} \pmod{5}$. Use the above result to prove that there exists a solution to the equation $2x \equiv 1 \pmod{5}$.

Theorem 1.3.1. *The equation $ax \equiv b \pmod{p}$ has a solution in x as long as $\gcd(a, p) = 1$.*

Proof. If $b \equiv 0 \pmod{p}$ then set $x \equiv 0 \pmod{p}$. Else, we have $b \in Q$ so therefore $b \in S$ using our above lemma. □

This leads to Fermat's Little Theorem:

Example 1.3.1. *Consider the congruence*

$$\{2 \times 1, 2 \times 2, 2 \times 3, 2 \times 4\} \equiv \{1, 2, 3, 4\} \pmod{5}$$

Make a second conclusion based on this fact.

Solution. The product of the two sets must be the same. Therefore we must have

$$2^4 \cdot 4! \equiv 4! \pmod{5} \implies 4!(2^4 - 1) \equiv 0 \pmod{5}$$

Since $\gcd(4!, 5) = 1$ we have $2^4 \equiv 1 \pmod{5}$. □

Theorem 1.3.2. *As long as $\gcd(a, p) = 1$ we have*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. By our above theorem we have:

$$\begin{aligned} \{a \times 1, a \times 2, a \times 3, \dots, a \times (p-1)\} &\equiv \{1, 2, 3, \dots, p-1\} \pmod{p} \\ a^{p-1} \cdot (p-1)! &\equiv (p-1)! \pmod{p} \\ (p-1)! (a^{p-1} - 1) &\equiv 0 \pmod{p} \\ a^{p-1} &\equiv 1 \pmod{p} \end{aligned}$$

□

1.4 Second proof of Fermat's little theorem

This proof relies on using the binomial theorem.

Theorem 1.4.1. *We have $a^p \equiv a \pmod{p}$*

Proof. We use induction. We only account for $a \in \{0, 1, 2, \dots, p-1\}$ because this is the residue set mod p .

Base Case: For $a = 0$ we arrive at $0 \equiv 0 \pmod{p}$. For $a = 1$ we get $1^{p-1} \equiv 1 \pmod{p}$.

Inductive hypothesis: Assume the statement holds for $a = n$. We prove it holds for $a = n + 1$. We have

$$\begin{aligned} (n+1)^p &\equiv n^p + \binom{p}{1}n^{p-1} + \dots + \binom{p}{p-1}n^1 + \binom{p}{p} \pmod{p} \\ &\equiv n + 1 \pmod{p} \end{aligned}$$

The reason behind the last step is that $p \mid \binom{p}{i} = \frac{p!}{(p-i)!i!}$.

□

1.5 Problems for the reader

Problem 1.5.1. Calculate $19^{30} \pmod{31}$.

Problem 1.5.2. Calculate $8^{7^2} \pmod{5}$

Problem 1.5.3. Calculate $9^{10^2+1} \pmod{101}$

Problem 1.5.4. (Brilliant.org) If $29^p + 1$ is divisible by a prime p find all possible positive values of p .

Problem 1.5.5. Calculate $2^{10} + 5^{10} \pmod{10}$

Problem 1.5.6. Calculate $2^{3^{4^5}} \pmod{19}$