Chapter 4: Congruences

Greg Knapp

February 20, 2022

1 Introduction to Congruences

1.1 Definition and Perspective

- We're going learn about a system that seems unrelated to a lot of things we've talked about so far, but actually provides us with a lot of tools to analyze things.
- Remember linear Diophantine equations: $ax + by = c$
- We said initially that the equation $6x + 15y = 83$ doesn't have solutions because the LHS has to be a multiple of 3 and the RHS isn't.
- We're going to be able to apply similar reasoning to be able to show (easily) that no integer in the sequence
$$11, 111, 1111, 11111, \ldots$$
is a perfect square for instance
- **Def:** Let m be a positive integer. If $a, b \in \mathbb{Z}$, we say that <u>a is congruent to b modulo m</u> if $m \mid (a - b)$
  - In this case, we write $a \equiv b \mod m$
  - Otherwise, we write $a \not\equiv b \mod m$
- **Ex:** $22 \equiv 7 \mod 15$, $-3 \equiv 30 \mod 11$, $91 \equiv 0 \mod 13$
- Important: in other classes (maybe discrete, maybe CS), you may have seen the notation $\mod m$ to represent a function.
- I.e. for you, $a \mod m$ means "the least positive integer congruent to a modulo m."
- We are not going to use that notation here because it's not useful for what we're going to do with modular arithmetic.
- Here's a connection to something we've been looking at before: $a \equiv b \mod m$ if and only if a is of the form $b + km$
- E.g. $a \equiv 1 \mod 4$ if and only if a is of the form $1 + 4k$.
- This claim holds because $m \mid (a - b)$ if and only if there exists k so that $mk = a - b$, i.e. $a = b + mk$
- This ties congruences into arithmetic progressions. Every member of the arithmetic progression $\{b + mk : k \in \mathbb{Z}\}$ is congruent to b modulo m

1.2 Equivalence and Arithmetic

- Importantly, congruence modulo m is what's called an equivalence relation. This means that it satisfies three important properties:
- **Thm:** Let $m > 0$. Then for all $a, b, c \in \mathbb{Z}$:
  1. (Reflexive property): $a \equiv a \mod m$
  2. (Symmetric property): $a \equiv b \mod m$ if and only if $b \equiv a \mod m$
  3. (Transitive property): if $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$
- Proofs:
  - Note that $m \mid 0 = a - a$ so $a \equiv a \mod m$
  - Suppose $a \equiv b \mod m$. Then there exists $k \in \mathbb{Z}$ so that $mk = a - b$. But then $m(-k) = b - a$, so $b \equiv a \mod m$
  - Suppose $a \equiv b \mod m$ and $b \equiv c \mod m$. Then there exist $k, \ell \in \mathbb{Z}$ so that $a - b = km$ and $b - c = \ell m$. Then $a - c = a - b + b - c = km + \ell m = (k + \ell)m$ so $a \equiv c \mod m$
- In addition to $\equiv$ acting kind of like an equals sign when it comes to the essential properties, it also plays nicely with arithmetic
- **Thm:** Let $m > 0$, and let $a, b, c \in \mathbb{Z}$ with $a \equiv b \mod m$. Then
  - $a + c \equiv b + c \mod m$
  - $a - c \equiv b - c \mod m$
  - $ac = bc \mod m$
- Proofs left as exercise.
- The other thing that you maybe want to do is divide both sides by c.
- However, this is difficult because even if both sides are divisible by c, you may not be able to make the conclusion you want.
- **Ex:** $100 \equiv 20 \mod 10$ and 100 and 20 are both multiples of 5.
- I.e. $5 \cdot 20 \equiv 5 \cdot 4 \mod 10$
- But we can't divide both sides by 5 because $20 \not\equiv 4 \mod 10$
- What's happening here?
- We have $100 - 20 = 10k$ for some k
- To conclude that $100/5 \equiv 20/4 \mod 10$, we would need to have $\frac{100-20}{5} = 10\ell$ for some integer ℓ, i.e. we would need k to be a multiple of 5
- But of course $100 - 20 = 10 \cdot 8$ and 8 is not a multiple of 5
- When we divide by 5, we have to reduce the modulus too: $20 - 4 = 2 \cdot 8$, so $20 \equiv 4 \mod 2$
- More generally, if we have $ac \equiv bc \mod m$, then we can write $ac - bc = mk$ and so we know that the RHS is divisible by c
- Divide both sides by c to get $a - b = \frac{mk}{c}$.
- We don't know anything about how k and c interact; maybe we need part of the c to cancel out part of the m.

- We can always cancel out the greatest common divisor of m and c so that $a - b = \frac{m}{(c,m)} \cdot \frac{k(c,m)}{c}$ and a little rewriting gives
$$\frac{c}{(c,m)}(a-b) = \frac{m}{(c,m)} \cdot k$$
- Since $\frac{m}{(c,m)}$ is relatively prime to $\frac{c}{(c,m)}$, we know that $\frac{m}{(c,m)}$ must divide $a-b$, i.e. $a \equiv b \mod \frac{m}{(c,m)}$
- As a consequence, if you start with $ac \equiv bc \mod m$, the best you can do is conclude that $a \equiv b \mod \frac{m}{(c,m)}$
- Note the following special case: if m and c are relatively prime, you can divide by c mod m.

1.3 The Point

- One of the main purposes of modular arithmetic is to classify the integers into easier to understand pieces.
- E.g. we know that every integer can be divided by 4 to give some remainder: e.g. $n = 4q + r$ where $r = 0, 1, 2, 3$
- Note that this means that $n \equiv r \mod 4$: i.e. every integer is congruent to either $0, 1, 2$ or $3 \mod 4$.
- There are a few ways to visualize this:
$$\begin{aligned} \ldots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv \ldots &\quad \mod 4 \\ \ldots \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv \ldots &\quad \mod 4 \\ \ldots \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv \ldots &\quad \mod 4 \\ \ldots \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv \ldots &\quad \mod 4 \end{aligned}$$
or you could see the integers going 0,1,2,3,0,1,2,3, etc.
- Of course you could also say that every integer is congruent to either $0, 1, 2,$ or $7 \mod 4$.
- We want a phrase which describes a set of numbers with the above property.
- **Def:** A complete set of residues modulo m is a set S of integers for which every $n \in \mathbb{Z}$ has $n \equiv s \mod m$ for exactly one $s \in S$
- **Ex:** For any m, $\{0, 1, \ldots, m-1\}$ is a complete set of residues because any $n \in \mathbb{Z}$ can be written uniquely as $n = qm + r$ for $0 \leqslant r < m$, i.e. $r \in \{0, 1, \ldots, m-1\}$ and $n \equiv r \mod m$
- **Ex:** If m is odd, then $\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\}$ is a complete set of residues modulo m
- E.g. modulo 7, we have $\{-3, -2, -1, 0, 1, 2, 3\}$ is a complete set of residues.
- This comes from the fact that the "missing" positive integers $(4, 5, 6)$ have been replaced by themselves minus 7 $(-3, -2, -1)$
- Not every complete set of residues has to be consecutive, however.
- Any set of m incongruent integers modulo m forms a complete set of residues modulo m.
- **Thm:** If $r_1, \ldots, r_m$ is a complete set of residues modulo m and if a is relatively prime to m, then $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ is a complete set of residues modulo m.
- Proof
  - We have a set of m integers, so it suffices to show that they are incongruent
  - Suppose that $ar_j + b \equiv ar_k + b \mod m$

- We can subtract to get $ar_j \equiv ar_k \mod m$
- Then, we can divide by a because it is relatively prime to m, so $r_j \equiv r_k \mod m$
- This only happens if $j = k$, so $ar_j + b = ar_k + b$
- In other words, for $j \neq k$, $ar_j + b \not\equiv ar_k + b \mod m$

1.4 An Example

- **Ex:** Find the least positive residue of

$$1! + 2! + 3! + \cdots + 10!$$

modulo...3, 4, and 11

  - everything about the 3! is 0 mod 3, so just look at the lower terms
  - likewise with 4 so...
  - With 11, there's no trick. Reduce each one by 11 and add later to get 0.

- This is kind of cool though because we learn that $1! + 2! + \cdots + 10!$ is a multiple of 11 without having any clue how to factor the number.

2 Linear Congruences

2.1 Modular Equations

- Now that we know the basics of "mod m arithmetic," it's good for us to learn the basics of finding equations to solutions mod m
- Any integer equation that you could write previously can now be written as a congruence
- **Ex:** $6x + 3 = 7$ becomes $6x + 3 \equiv 7 \mod 4$ or mod 5 or whatever
- **Ex:** $x^2 + 2x + 1 = 0$ becomes $x^2 + 2x + 1 \equiv 0 \mod 2$ for instance.
- **Ex:** (non) $e^x = e^3$ cannot be translated into a modular equation because e^3 is not an integer
- Note that "having an integer solution" does not mean that an equation can become a modular equation: e.g. $e^x = e^3$
- Note also that "not having an integer solution" does not mean that an equation can't become a modular equation, e.g. $6x + 3 = 7$
- Additionally, "not having an integer solution" does not mean that an equation can't have solutions mod m. E.g. $6x + 3 \equiv 7 \mod 4$ has the solution $x = 2$. $6x + 3 \equiv 7 \mod 5$ has the solution $x = 4$. $6x + 3 \equiv 7 \mod 6$ has no solution.
- That said, "having an integer solution" always implies that an equation has a solution $\mod m$. E.g. $x^2 + 2x + 1 = 0$ always has the solution $x = -1$ no matter which modulus you take.

2.2 Linear Equations

- Let's explore how to solve linear equations.
- If we have something like $ax + b \equiv c \mod m$, then we can always write $ax \equiv c - b \mod m$ first, so there's no point in considering the $+b$
- We might as well just consider equations of the form $ax \equiv b \mod m$

- To solve this equation in $\mathbb{Q}$, we would want to divide by a, but we know that we can't really do that here, so let's do a little further exploration.
- Consider $6x \equiv 9 \mod 15$.
- We could do this by inspection: $6 \cdot 4 \equiv 9 \mod 15$, $6 \cdot 9 \equiv 9 \mod 15$, $6 \cdot 14 \equiv 9 \mod 15$
- Of course, this also means that $6 \cdot (4 + 15k) \equiv 9 \mod 15$, $6 \cdot (9 + 15k) \equiv 9 \mod 15$, etc.
- In fact, we've found all the solutions: we only have to check the numbers 0 through 14 and then we know all the solutions
- Of course, note that we could write the solutions more simply as $4 + 5k$. Hmm...
- $6x \equiv 9 \mod 15$ is equivalent to saying that there exists y with $6x - 9 = 15y$, i.e. $6x - 15y = 9$
- But we know how to do this because $(6, 15) = 3 \mid 9$
- Find a particular solution, say $x = 4$ and $y = 1$ and then the general solution looks like $x = 4 + \frac{15}{(6,15)}k$ and $y = 1 - \frac{6}{(6,15)}k$
- We don't really care about y, but note that we get the same solution description.
- Lesson: linear congruences are equivalent to two-variable linear diophantine equations.
- **Thm:** Let $a, b, m \in \mathbb{Z}$, $m > 0$. If $(a, m) \nmid b$, then $ax \equiv b \mod m$ has no solutions. If $(a, m) \mid b$, then $ax \equiv b \mod m$ has (a, m) incongruent solutions.
  - Proof: Exactly what we just did, but with letters instead of numbers
  - $ax \equiv b \mod m$ if and only if there exists $y \in \mathbb{Z}$ so that $ax + my = b$
  - This only occurs if $(a, m) \mid b$
  - If it does occur, then there exists a solution $ax_0 \equiv b \mod m$ and every other solution looks like $x = x_0 + \frac{m}{(a,m)}k$
  - For $0 \leqslant k < (a, m)$, these solutions are incongruent mod m:
  - Suppose $x_0 + \frac{m}{(a,m)}k \equiv x_0 + \frac{m}{(a,m)}j \mod m$
  - Then $\frac{m}{(a,m)}k \equiv \frac{m}{(a,m)}j \mod m$ which gives $k \equiv j \mod (a, m)$
  - But $0 \leqslant k, j < (a, m)$, so $k = j$
  - Therefore, there are (a, m) non congruent solutions

2.3 Special Case: Inverses

- By the theorem, $(a, m) = 1$ if and only if there is a solution to $ax \equiv 1 \mod m$.
- This is saying that there exists a multiplicative inverse to a modulo m.
- E.g. $7 \cdot 5 \equiv 1 \mod 34$, so 5 is an inverse of 7 and vice versa mod 34.
- Note that we can use this fact to easily solve $7x \equiv 12 \mod 34$
- Multiply both sides by 5 to give $x \equiv 60 \equiv 26 \mod 34$
- That's the only solution since $(7, 34) = 1$
- More generally, there's a unique solution to $ax \equiv b \mod m$ when $(a, m) = 1$
- Additionally, consider the case when p is prime
- Then $(a, p) = 1$ for all $0 < a < p$ and so a is always invertible mod p.
- Hence, you can solve every linear equation mod p.

3 Sun-Tsu's Theorem

3.1 Intro

- In the previous section, we discussed solving a single equation modulo m
- Maybe the next step is to solve a system of equations mod m
- Systems of linear equations can be manageable
- The next thing that we'll consider is a single equation with multiple moduli.
- It's kind of hard to motivate this actually.
- This is really useful though.
- Are there any integers x satisfying $x \equiv 1 \mod 5$ and $x \equiv 3 \mod 7$?
- Neither 1 nor 3 fits the bill, so we have to dig a little deeper.
- Let's add multiples of 7 to 3 to see what we find.
- Letting $a_n = 3 + 7n$, we have $a_0 = 3$ (3 mod 5), $a_1 = 10$ (0 mod 5), $a_2 = 17$ (2 mod 5), $a_3 = 24$ (4 mod 5), $a_5 = 31$ (finally 1 mod 5)
- Hence, $x = 31$ works
- Notice that we cycled through all of the congruence classes mod 5 when we took a number and added multiples of 7 to it.
- This is because 7 is invertible mod 5: if $3 + 7n \equiv 3 + 7m \mod 5$, then we'd have $n \equiv m \mod 5$, so $3, 3 + 7, 3 + 14, 3 + 21, 3 + 28$ must be distinct mod 5
- Are there any other solutions? (warm-up exercise)
- Yes: anything of the form $31 + 35k$ is a solution!

3.2 The Theorem

- We're going to call this theorem Sun-Tsu's Theorem since Sun-Tsu gave the earliest known statement of the theorem
- It's commonly called the Chinese Remainder Theorem
- Why is that a problematic name?
- (Because there are no other theorems named after entire groups of people)
- Ch'in Chiu-Shao published the first known proof of this fact
- **Thm:** Let $m_1, \ldots, m_r$ be pairwise relatively prime positive integers. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_r \mod m_r \end{aligned}$$

  has a unique solution modulo $M = m_1 \ldots m_r$
- Proof

- Define $L_k = \frac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$
- Note that $(L_k, m_k) = 1$ since the m_j are pairwise relatively prime
- Hence for each $1 \leqslant i \leqslant r$, there exists $y_k \in \mathbb{Z}$ so that $M_k y_k \equiv 1 \mod m_k$
- Hence, $a_k M_k y_k \equiv a_k \mod m_k$
- Now define $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$
- Observe that $x \equiv a_1 \mod m_1$ etc.
- Hence, we've solved the system of congruences
- Now we want to show that our solution is unique mod M
- Suppose that y also has $y \equiv a_k \mod m_k$ for all $1 \leqslant k \leqslant r$
- Then $y \equiv x \mod m_k$ implying $m_k \mid y - x$ for all k
- But then $m_1 \cdots m_r \mid y - x$ since the m_k are relatively prime
- Therefore, $y \equiv x \mod M$

3.3 Examples

- **Ex:** Solve $x \equiv 1 \mod 2$, $x \equiv 2 \mod 3$, $x \equiv 3 \mod 5$
  * $M = 30$, $L_1 = 15$, $L_2 = 10$, $L_3 = 6$
  * Want to solve $15y_1 \equiv 1 \mod 2$, $10y_2 \equiv 1 \mod 3$, and $6y_3 \equiv 1 \mod 5$
  * This gives $y_1 = 1$, $y_2 = 1$, and $y_3 = 1$
  * We can then take $x = 15 \cdot 1 + 10 \cdot 2 + 6 \cdot 3 = 53$. Could also have taken 23 or anything else $\equiv 23 \mod 30$.
- **Ex:** Find all solutions to

$$\begin{aligned} x &\equiv a_3 \mod 3 \\ x &\equiv a_5 \mod 5 \\ x &\equiv a_{11} \mod 11 \\ x &\equiv a_{13} \mod 13 \end{aligned}$$

  * Note $M = 2145$ and we have $L_3 = 715$, $L_5 = 429$, $L_{11} = 195$, and $L_{13} = 165$
  * Solving $715y_3 \equiv 1 \mod 3$ gives $y_3 = 1$
  * Solving $429y_5 \equiv 1 \mod 5$ gives $y_5 = 4$
  * Solving $195y_{11} \equiv 1 \mod 11$ gives $y_{11} = 7$
  * Solving $165y_{13} \equiv 1 \mod 13$ gives $y_{13} = 3$
  * Then the solution looks like $715a_3 + 4 \cdot 429a_5 + 7 \cdot 195a_{11} + 3 \cdot 165a_{13} \mod 2145$

- **Ex:** Solve

$$\begin{aligned} 2x &\equiv 1 \mod 5 \\ 3x &\equiv 9 \mod 6 \\ 4x &\equiv 1 \mod 7 \\ 5x &\equiv 9 \mod 11 \end{aligned}$$