1 Congruences

1.1 Introduction to Congruences

---

1. **Introduction:** Suppose you wished to find $x, y \in \mathbb{Z}$ satisfying $2x^2 - 8y = 11$. There is no solution because no matter what, $2x^2 - 8y$ is even and 11 is odd. What if even/odd does not work... what else might? $3x^2 - 15y = 8$, 3 divides the left side but not the right. If even/odd or divided by 3 works, there is no guarantee that it works $\underbrace{3x^2 - 15y = 9}_{\text{might work}}$. The idea of modular arithmetic formalizes all of this.

2. **Definition and Equivalencies:** For $a, b, m \in \mathbb{Z}$ with $m \geq 2$ we write $a \equiv b \bmod m$ which is read as "a and b are congruent modulo m." to mean that $m \mid (a - b)$. A few notes on this,

   - Equivalent to saying $m \mid (b - a)$.
   - Equivalent to saying $\exists c \in \mathbb{Z}$ such that $mc = a - b$ or $\exists x \in \mathbb{Z}$ such that $mc = b - a$ (definition of divisibility).
   - Equivalent to saying that if we divide a and b by m, the remainders are the same.

   Ex. $8 \equiv 18 \bmod 5$ in fact $8 \equiv 18 \equiv 3 \equiv -2 \equiv 23 \equiv \cdots \bmod 5$. Here with remainder 3. Also note $5 \mid (18 - 8)$ and $5 \mid (8 - 18)$.

   Even/odd is the same as $m = 2$.

   CS Note. In computer science we often define $\text{mod}(a, m) =$ remainder when $a/m = a\%m$. It is not uncommon to see $a = b \bmod m$ or $a \equiv_m b$ (strongly discouraged).

   Moving forward, please use $a \equiv b \bmod m$.

3. **Properties:**

   (a) **Theorem.** Congruence acts like an equals sign in the following sense:

   (i) $a \equiv a \bmod m$ (Reflexive).

   (ii) if $a \equiv b \bmod m$ then $b \equiv a \bmod m$ (Symmetric).

   (iii) If $a \equiv b \bmod m$ and $b \equiv c \bmod m$ then $a \equiv c \bmod m$ (Transitivity).

   Proof. $a \equiv b \bmod m \implies \exists x$ such that $a - b = mx$, $b \equiv c \bmod m \implies \exists y$ such that $b - c = my$. Then $a - c = (a - b) + (b - c) = mx + my = m(x + y)$ so $m \mid (a - c)$ so $a \equiv c \bmod m$. ☐

   (iv) If $a \equiv b \bmod m$ and $c \equiv \ \bmod m$ then $a \pm c \equiv b \pm d \bmod m$.

i.e. If we know $x \equiv y \bmod 5$ we can conclude $x+7 \equiv y+7 \bmod 5$ and also $x+7 \equiv y+12 \bmod 5$.

(v) If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then $ac \equiv bd \bmod m$

i.e. If we know $x \equiv y \bmod 5$ then we can conclude $17x \equiv 17y \bmod 5$ but we can also conclude $17x \equiv 12y \bmod 5$

(vi) If $a \equiv b \bmod m$ and $k \in \mathbb{Z}, k \geq 1$ then $a^k \equiv b^k \bmod m$. (Note: we can *not* use different powers!)

(b) **Division Issues.** First everything must be an integer, so does $2 \equiv 8 \bmod 6 \implies \frac{2}{3} \equiv \frac{8}{3} \bmod 6$ this is garbage because $\frac{2}{3}, \frac{8}{3} \notin \mathbb{Z}$. However, is $2 \equiv 8 \bmod 6 \implies \frac{2}{2} \equiv \frac{8}{2} \bmod 6$ true? No! because $1 \equiv 4 \bmod 6$ is not true. The point is even if division makes both sides integers there is no guarantee that the congruence is preserved!

Theorem. Suppose we have $ac \equiv bc \bmod m$ then $a \equiv b \bmod m/\gcd(m,c)$. In other words we may cancel an integer from both sides provided we divide the modulus by the gcd of the modulus and the integer we're canceling.

Proof. Suppose $ac \equiv bc \bmod m$, $\exists k \in \mathbb{Z}$ with $mk = ac - bc$. So $mk = c(b-a)$,

$$\frac{m}{\gcd(c,m)} k = \frac{c}{\gcd(c,m)} (a-b)$$

Note that from a previous theorem we know that:

$$\gcd\left(\frac{m}{\gcd(c,m)}, \frac{c}{\gcd(c,m)}\right) = 1$$

Then the above statement says that $\frac{m}{\gcd(c,m)} \Big| \frac{c}{\gcd(c,m)}(a-b)$ which implies $\frac{m}{\gcd(\mathrm{c,m})} \Big| a-b$. Therefore, $a \equiv b \bmod \frac{m}{\gcd(c,m)}$. ☐

Note. Don't think division, think cancelation when dealing with modulo.

Ex. If we know that $4x \equiv 8y \bmod 50$ then we can conclude that $x \equiv 2y \bmod 50/\gcd(50,4)$ and so $x \equiv 2y \bmod 25$ (think *cancel* the 4).

Corollary. If $ac \equiv bc \bmod m$ and $\gcd(c,m) = 1$ then $a \equiv b \bmod m$.

Ex. $15x \equiv 20y \bmod 27$, note that $\gcd(5,27) = 1$ so we may cancel the 5. So $3x \equiv 4y \bmod 27$.

4. **Residue Classes:**

(a) **Introduction:** Suppose we are working $\bmod m = 5$. We know $0 \equiv 5 \equiv 10 \equiv -5 \equiv \cdots \bmod 5$, we also know $1 \equiv 6 \equiv 11 \equiv -4 \equiv \cdots \bmod 5$, all of $\mathbb{Z}$ fall into one out of $m = 5$ classes.

$$\{\cdots, -15, -10, -5, 0, 5, 10, 15, \cdots\}$$
$$\{\cdots, -16, -9, -4, 1, 6, 11, 16, \cdots\}$$
$$\{\cdots, -13, -8, -3, 2, 7, 12, 17, \cdots\}$$
$$\{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\}$$
$$\{\cdots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

(b) **Definition.** For a given $m \geq 2$ there are m congruence classes.

(c) **Definition.** From each we may pick a representative of the class so those would be m representatives.
Ex. $m = 5 : \{0, 1, 2, 3, 4\}$ (the obvious one) or you could use $m = 5 : \{0, 2, 4, 6, 8\}$ (all even) or $m = 5 : \{0, 2, 4, 8, 16\}$ (all powers of 2, except 0).
Ex. $m = 5 : \{0, 1, 2, 3, 4\}$ (the obvious one) or you could use $m = 5 : \{0, 2, 4, 6, 8\}$ (all even) or $m = 5 : \{0, 2, 4, 8, 16\}$ (all powers of 2, except 0).

(d) **Definition.** The set of representatives $\{0, \cdots, m-1\}$ = the complete set of least non-negative residues.

In $\mathbb{R}$, $17^x = 48246319 \implies x = \log_1 7(48246319)$. Now consider $\mathbb{Z}$ mod 100, $6^x \equiv 88 \bmod 100$ is *significantly* harder to solve (the discrete logarithm problem).

(e) **Definition.** A complete set of residues (CSOR) mod m is a set of m integers, no two of which are congruent mod m.
Ex. $m = 5$: here are 3 CSORs: $\{0, 1, 2, 3, 4\}$, $\{0, 2, 4, 6, 8\}$, $\{0, 2, 4, 8, 16\}$, and more!

(f) **Theorem.** A subset S of $\mathbb{Z}$ is a CSOR mod m if and only if every integer is congruent to exactly one element in S.
Ex. $m = 4$: $S = \{0, 9, 14, 3\}$ some observations:

- $m = 4$ of them.
- No two are congruent to each other.
- Any $a \in \mathbb{Z}$ is congruent to exactly one of these.

(g) **Theorem.** If $\{r_1, r_2, \cdots, r_m\}$ is a CSOR mod m and if $a, b \in \mathbb{Z}$ with $\gcd(a, m) = 1$ then $\{ar_1 + b, ar_2 + b, \cdots, ar_m + b\}$ if also a CSOR mod m.

Proof. We will show that no two are congruent mod m. Suppose $ar_i + b \equiv ar_j + b \bmod m$ with $i \neq j$. Then $ar_i \equiv ar_j \bmod m \implies r_i \equiv r_j \bmod m$ because $\gcd(a, m) = 1$. Contradiction because the r_i, r_j came from a CSOR mod m. $\square$

Ex. $\{0, 1, 2, 3, 4\}$ CSOR mod 5. Pick $a = 9, b = 42$, $\{0 \cdot 9 + 42, 1 \cdot 9 + 42, 2 \cdot 9 + 42, 3 \cdot 9 + 42, 4 \cdot 9 + 42\}$ is also a CSOR mod 5.

5. **Fast Arithmetic - Fast Exponentiation.** Suppose we wished to calculate $2^{503} \equiv a \bmod 5$, $a = 0, 1, 2, 3, 4$ but which one? Warning: Do not reduce exponent mod 5! $2^{503} \equiv 2^x \bmod 5$.

   (a) Look for patterns: $2^1 = 2 \bmod 5$, $2^2 \equiv 4 \bmod 5$, $2^3 \equiv 3 \bmod 5$, $2^4 \equiv 1 \bmod 5$, $2^5 \equiv 2 \bmod 5$. This last one is a repeat, so it repeats every 4. Note $503 = 4(125) + 1$ so

$$\begin{aligned} 2^{503} &\equiv (2^4)^{503} 2^3 \\ &\equiv (1)^{125} 2^3 \bmod 5 \\ &\equiv (1)8 \bmod 5 \\ &\equiv 3 \bmod 5 \end{aligned}$$

   (b) Use binary expansions. Suppose we want $3^{81} \equiv a \bmod 5$. $3^1 \equiv 3$, $3^2 \equiv 4$, $3^4 \equiv 1$, $3^8 \equiv 1$, $3^{16} \equiv 1$, $3^{32} \equiv 1$, $3^{64} \equiv 1$. Then $81 = 64 + 16 + 1$ so

$$\begin{aligned} 3^{81} &= 3^{64} 3^{16} 3^1 \\ &\equiv 1 \cdot 1 \cdot 3 \\ &\equiv 4 \bmod 5 \end{aligned}$$

1.2 Solving Linear Congruences

---

1. **Introduction:** The idea is that we would ideally like to solve "equations" like $3x^2 + x \equiv 5 \bmod 72$, $8^x \equiv 12 \bmod 5$, etc... So let's go back to basics.
   Definition: A linear congruence has the form $ax \equiv b \bmod m$. We would like to find all possible solutions, whatever that means.
   Process:

   (a) Do solutions exist?

   (b) If so, can we find just one?

   (c) Can we find more?

   (d) When are they "different"

2. **Do Solutions Exist:** To say that $ax \equiv b \bmod m$ has a solution means, $\exists x$ such that $ax \equiv b \bmod m$ which in turn means $\exists x, \exists y$ such that $ax + my = b$ ($ax \equiv b \bmod m \implies m \mid (ax - b) \implies my = ax - b \implies ax - my = b$). This means that b is a linear combination of a, m.
   Recall: {Linear combination of a, m} = { multiples of $\gcd(a, m)$}.
   Thus, b is a linear combination of a, m when b =multiple of $\gcd(a, m)$, so $ax \equiv b \bmod m$ has solution(s) if and only if $\gcd(a, m) \mid b$.
   Ex. $2x \equiv 8 \bmod 18$ has solutions, because gcd(2,18)=2 $\mid$ 8.
   $6x \equiv 8 \bmod 36$ does not, because gcd(6,36)=6 $\nmid$ 8.

3. **Finding One Solution:** We would like to solve $ax + my = b$, with b as a multiple of $\gcd(a, m)$. Well, we can solve $ax' + my' = \gcd(a, m)$! But how? With the Euclidean Algorithm. Use the Euclidean Algorithm to solve $ax' + my' = \gcd(a, m)$ then multiple both sides to get b on the right.
   Ex. Consider $4x \equiv 6 \bmod 50$. We have gcd(4,50)=2 | 6 so solutions exist. First we use the Euclidean Algorithm to solve:
   $$4x' + 50y' = 2$$
   This gives us $4\underbrace{(-12)}_{x'}+50\underbrace{(1)}_{y'} = 2$, we want to get a 6 on the right hand side so multiple by 3. So then we get $4\underbrace{(-36)}_{x}+50\underbrace{(3)}_{y} = 6$, so $4(-36) \equiv 6 \bmod 50$. Typically, we will use the least non-negative residue (add until you get a non-negative). So here the solution is $x_0 = (-36) + 50 = 14$.

4. **Finding All Solutions:** Suppose we have our one solution, $x_0 \implies ax_0 \equiv b \bmod m$. Suppose now x is another, this implies $ax \equiv b \bmod m$. So we subtract the second from the first
   $$\begin{aligned} a(x) - a(x_0) &\equiv b - b \bmod m \\ a(x - x_0) &\equiv 0 \bmod m \\ x - x_0 &\equiv 0 \bmod \frac{m}{\gcd(a, m)} \end{aligned}$$
   So,
   $$x = x_0 + k\left(\frac{m}{\gcd(a, m)}\right)$$
   Warning! Solutions must look like this but are all things which look like this actually solutions?

   We would like $ax \equiv b \bmod m$.
   $$\begin{aligned} ax &\equiv a\left(x_0 + k\left(\frac{m}{\gcd(a, m)}\right)\right) \bmod m \\ ax &\equiv \underbrace{ax_0}_{b} + \underbrace{k\left(\frac{m}{\gcd(a, m)}\right)}_{\text{lcm}} \bmod m \\ ax &\equiv b + k\mathrm{lcm}(a, m) \bmod m \\ ax &\equiv b \bmod m \end{aligned}$$
   Therefore all solutons can be gained by doing, $x = x_0 + k\left(\frac{m}{\gcd(a,m)}\right), \forall k \in \mathbb{Z}$.

   Lastly, when are they unique mod m?

Consider that two of them with k_1 and k_2 are identical mod m when:

$$\begin{aligned} x_0 + k_1\left(\frac{m}{\gcd(a,m)}\right) &\equiv x_0 + k_2\left(\frac{m}{\gcd(a,m)}\right) \mod m \\ k_1\left(\frac{m}{\gcd(a,m)}\right) &\equiv k_2\left(\frac{m}{\gcd(a,m)}\right) \mod m \\ k_1 &\equiv k_2 \mod \frac{m}{m/\gcd(a,m)} \\ k_1 &\equiv k_2 \mod \gcd(a,m) \end{aligned}$$

Therefore, it follows that solutions will be congruent mod m when k-values are congruent mod $\gcd(a,m)$. So solutions are not congruent mod m by ensuring that the k-values are not congruent mod $\gcd(a,m)$. This can be done using $k = 0, 1, 2, \cdots, \gcd(a,m) - 1$.

5. **Summary Theorem:** The linear congruence $ax \equiv b \mod m$ has solutions if and only if $\gcd(a,m) \mid b$. If it has solutions then it has $\gcd(a,m)$ unique solutions mod m. If x_0 is one of those then all are

$$x = x_0 + k \cdot \frac{m}{\gcd(a,m)}, \text{ for } k = 0, 1, 2, \cdots, \gcd(a,m) - 1$$

Ex. $20x \equiv 15 \mod 65$, gcd(20,65)=5 | 15 so $\exists 5$ incongruent solutions mod 65. The Euclidean Algorithm gives us a solution $x_0 \equiv 56 \mod 65$. So all solutions are then

$$x \equiv 56 + k \cdot \frac{65}{\gcd(20,65)} \mod m, \text{ for } k = 0, 1, 2, 3, 4$$

$$x \equiv 56 + 13k \mod 65, k = 0, 1, 2, 3, 4$$

That is $x \equiv 56, 4, 17, 30, 43 \mod 65$.

Note: If $\gcd(a,m) = 1$ there exists only one solution mod m.

1.3 The Chinese Remainder Theorem

---

1. **Introduction:**
2. **Lemma:**
3. **The Chinese Remainder Theorem:**

1.4 Factoring Using Pollard's Rho Method

1.5 Problems

---

1. Calculate the least positive residues modulo 47 of each of the following with justification:

   (a) 2^{543}

   (b) 32^{932}

   (c) $46^{327349287323}$

2. Exhibit a complete set of residues mod 17 composed entirely of multiples of 3.

3. Show that if $a, b, m \in \mathbb{Z}$ with $m > 0$ and if $a \equiv b \mod m$ then $\gcd(a, m) = \gcd(b, m)$.

4. Suppose p is prime and $x \in \mathbb{Z}$ satisfies $x^2 \equiv x \mod p$. Prove that $x \equiv 0 \mod p$ or $x \equiv 1 \mod p$. Show with a counterexample that this fails if p is not prime.

5. Show that if n is an odd positive integer or if n is a positive integer divisible by 4 that:
$$1^3 + 2^3 + ... + (n-1)^3 \equiv 0 \mod n$$

6. Find all solutions (mod the given value) to each of the following.

   (a) $10x \equiv 25 \mod 75$

   (b) $9x \equiv 8 \mod 12$

7. Solve each of the following linear congruences using inverses.

   (a) $3x \equiv 5 \mod 17$

   (b) $10x \equiv 3 \mod 11$

8. What could the prime factorization of m look like so that $6x \equiv 10 \mod m$ has at least one solution? Explain.

9. Use the Chinese Remainder Theorem to solve:
   A troop of monkeys has a store of bananas. When they arrange them into 7 piles, none remain. When they arrange them into 10 piles there are 3 left over. When they arrange them into 11 piles there are 2 left over. What is the smallest positive number of bananas they can have? What is the second smallest positive number?

10. Solve the system of linear congruences:
$$\begin{aligned} 2x + 1 &\equiv 3 \mod 10 \\ x + 2 &\equiv 7 \mod 9 \\ 4x &\equiv 1 \mod 7 \end{aligned}$$