Modular Arithmetic, Chinese Remainder Theorem, Fermat's Little Theorem

1 Introduction to modular arithmetic

1. Are 22 and 11 congruent mod 2? mod 3? mod 5? mod 6? mod 7? mod 11?
2. Are -5 and 2 congruent mod 2? mod 3? mod 5? mod 6? mod 7? mod 11?
3. Can you find a strategy for finding all n so that 22 and 11 are congruent mod n?
4. Make a list of 10 numbers that are congruent to one another mod 10.
5. Make a list of 10 numbers that are congruent to one another mod 6.
6. Is 1+7 congruent to 6+(-3) mod 5?
7. Is 212+984 congruent to 563+(-319) mod 5?
8. Justify the following statement: If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a + b \equiv c + d \pmod{n}$.
9. Is the product $-2 \cdot 13$ congruent to $4 \cdot 16$ mod 3?
10. Is the product $6 \cdot 78$ congruent to $-8 \cdot 142$ mod 7? Can you find a strategy that will help answer this question without needing to find the products of these numbers?

2 Some leading questions

Next, we will look at a couple of families of questions and make some guesses about them. After thinking about them for awhile, we'll introduce some new tools that will help us draw further conclusions about them.

2.1 First set of questions

1. As we established at the end of the last section, multiplication works nicely with thinking "mod n". It's tempting to want to multiply our different moduli together, but notice that it doesn't work as nicely. What is 7 mod 3, mod 5 and mod 15?
2. Which numbers less than 20 are congruent to 1 mod 2 and congruent to 1 mod 3?
3. Can you find a number less than 100 that is congruent to 0 mod 3, congruent to 3 mod 5, and congruent to 1 mod 7?
4. How many numbers less than 24 are congruent to 1 mod 3 and 0 mod 2? How many numbers less than 24 are congruent to 1 mod 3 and 0 mod 4?
5. Consider the number 168. Suppose you want to tell someone you're thinking of the number 168, but you're only allowed to tell them that it's less than 200 and what it's congruent to modulo different numbers n. How many different congruences do you need to tell the person about so that they'll know your number is 168? How does this game change if you're only allowed to tell them about congruences modulo prime numbers? How does this game change if you're only allowed to tell them about congruences modulo powers of prime numbers (e.g. 2,4,8,3,9,27,etc.)? How does the game change if you're only allowed to tell the person the number is less than 500 rather than less than 200?

2.2 Second set of questions

1. Check that the set of numbers $\{0, 1, 2, 3, 4, 5\}$ a group under the operation addition mod 6? If so, what is the inverse of 2? The inverse of 3?

2. Is the group from the last question cyclic? Which elements of the group can generate it?

3. Consider the group generated by 1 under the operation addition mod 5. How many elements does it have? What is its identity? Which other elements of this group also generate it? Which elements of the group do not generate it?

2.3 Third set of questions

1. Check that the set of numbers $\{1, 2, \ldots, 6\}$ a group under the operation of multiplication mod 7? If so, what is the inverse of 2? The inverse of 5?

2. Is the set of numbers $\{1, 2, \ldots, 5\}$ a group under the operation of multiplication mod 6? If not, is there any way to salvage it by deleting some of the numbers in the set?

3. Consider the group generated by 2 under the operation multiplication mod 5. How many elements does it have? Which other elements of this group also generate it? Which elements of the group do not generate it?

4. Consider the group generated by 2 under the operation multiplication mod 12. How many elements does it have? Which other elements of this group also generate it? Which elements of the group do not generate it?

5. How many times did you have to take powers of 2 to get a number congruent to 2 mod 5 again?

6. How many times did you have to take powers of 2 to get a number congruent to 2 mod 12 again?

7. Do you think that there is any n out there where we can't ever find a power of 2 that's congruent to 2 mod n?

3 Some powerful tools: Bézout's lemma and the Euclidean algorithm

1. Can you find integers m and n that fill in the following equation:

$$3m + 5n = 1$$

   Can you find more than one pair of integers that works?

2. Can you find integers m and n that fill in the following equation:

$$4m + 6n = 1$$

   Can you find more than one pair of integers that works?

3. Why must any number of the form $4m + 6n$ be divisible by 2? Or more generally for any fixed a and b, why must any number of the form $am + bn$ be divisible by the gcd of a and b?

Bézout's lemma says that given any fixed a and b, it's always possible to find integers m and n (they won't necessarily be unique) such that $am + bn = gcd(a, b)$.

4. Let's do another example of Bézout's lemma: Find m and n such that $24m + 9n = 3$.

There's a method for finding m and n that satisfy Bézout's lemma, called the Euclidean algorithm, which is performed by doing division with remainder repeatedly. In the following example, we carry out the Euclidean algorithm to find solutions to the following equation: $24m + 9n = 3$.

- First, let's divide (with remainder) 24 by 9: the quotient is 2 and the remainder is 6. Notice that we can write the following equation:

$$24 - 9 \cdot 2 = 6$$

  It looks a bit like the statement from Bézout's lemma, but not quite. It's got the remainder of the division where we want the gcd of 9 and 24.

- The next step is to divide the remainder we got in the last step by 9, which we can write like:

$$9 - 6 = 3$$

- We already know how to write 6 in terms of 9 and 24 from the first step, so we can substitute in:

$$\begin{aligned} 9 - (24 - 9 \cdot 2) &= 3 \\ -24 - 9 \cdot 3 &= 3 \end{aligned}$$

- For each step now, we divide the remainder we got two steps ago by the one in the previous step. 3 divides evenly into 6 with no remainder. If we try to do again what we just did, we get

$$\begin{aligned} 6 - 3 \cdot 2 &= 0 \\ (24 - 9 \cdot 2) - (-24 - 9 \cdot 3) \cdot 2 &= 0 \end{aligned}$$

  But if we go ahead and simplify this, we just get that $0 = 0$ and we don't have any new or interesting information. We know that where we wanted to stop was the step before this one. Intriguingly, the last nonzero remainder we computed happened to be the gcd of 9 and 24.

5. Carry out the Euclidean algorithm for 240 and 46. Is the last nonzero reaminder we get from performing the algorithm the gcd of 240 and 46?

A few comments on what's going on here: We know that the Euclidean algorithm has to give us 0 eventually because the remainders we're figuring up are non-negative but get strictly smaller with each step. We've also shown that if we're performing the Euclidean algorithm on a and b, then each remainder we get can be written in the form $ma + nb$ for some integers m and n. So, we know from problem 3 that each remainder we get is divisible by $gcd(a, b)$. But why does this gcd actually appear as one of the remainders? Why don't we sometimes end up skipping over it?

5. The answer to the question I just posed is that each successive pair of numbers in the Eucliean algorithm has the same gcd. So, going back to our first example, $\gcd(24, 9) = \gcd(9, 6) = \gcd(6, 3) = \gcd(3, 0)$. First, verify that all these gcd's are the same. Why do these equalities tell us that the last nonzero number we get has to be the gcd of the numbers we started with?

6. Check that the same thing happened when you performed the Euclidean algorithm for 240 and 46.

7. Given two whole numbers a and b, if we perform division wtih remainder, we get an equation $a = bq+r$. Why does this equation show us that a and b have to have the same gcd as b and r?

4 The Chinese remainder theorem

Bézout's lemma gives us a very powerful tool. We'll talk about the statement of the Chinese remainder theorem in class. Go back to the questions in section 2 in the "first set of questions". How does Bézout's lemma help you with them?

5 Another application of Bézout's lemma: Generators of $\mathbb{Z}/(n)$

Take another look at the "second set of questions" in Section 2. Does Bézout's lemma help you with these problems? In general, which elements of $\mathbb{Z}/(n)$ are generators of it?

6 $U(n)$ and Fermat's Little Theorem

1. Take another look at the third set of questions. Does Bezout's lemma help decide how we might construct a group under the operation of multiplication modulo n?
2. Suppose p is a prime. Does the set $\{1, 2, \ldots, p-1\}$ form a group under the operation of multiplication mod p?
3. Consider an element $a \in \{1, 2, \ldots, p-1\}$. Thinking back to our work with groups the other day, what order could the cyclic group generated by a possibly have?
4. Use the last question to decide why a^{p-1} must be congruent to 1 mod p.
5. Fermat's Little Theorem says that for any integer a and any prime p, a^p is congruent to a mod p. Why have we proven it?