Week 2

Last week, we started looking at arithmetic through the lens of "remainders when divided by q". As a reminder:

- Numbers a and b are "congruent modulo q", or "$a \equiv b \pmod{q}$", if a and b have the same remainder when divided by q.
- If a and b have remainders r and s when divided by q, then $(a+b)$ and $(r+s)$ are congruent modulo q. The same works for $(a \times b)$ and $(r \times s)$ (but not a^b and r^s).

Let's warm up with some modular arithmetic practice.

Question 1. Fill in the blanks:

(a) $3 + 5 \equiv$ ____ (mod 6)

(b) $8 + 11 \equiv$ ____ (mod 3)

(c) $407 + 806 \equiv$ ____ (mod 4)

(d) $33 + 47 \equiv$ ____ (mod 20)

(e) $399 + 798 \equiv$ ____ (mod 100)

(f) $3 \times 5 \equiv$ ____ (mod 6)

(g) $2 \times 6 \equiv$ ____ (mod 3)

(h) $26 \times 26 \equiv$ ____ (mod 5)

(i) $47 \times 63 \equiv$ ____ (mod 10)

(j) $399 \times 798 \equiv$ ____ (mod 100)

(k) $84 - 18 \equiv$ ____ (mod 8)

(l) $32 - 9 \equiv$ ____ (mod 6)

(m) $248 - 181 \equiv$ ____ (mod 5)

(n) $25 - 43 \equiv$ ____ (mod 7)

Let's look at some addition tables modulo q. Here's an addition table for remainders modulo 6:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Notice that (for example) the entry for $3 + 5$ is 2, not 8: since we're working modulo 6, the numbers 2 and 8 are the same thing. The only possible remainders when something is divided by 6 are 0, 1, 2, 3, 4 and 5, so we don't need to include any other numbers — anything else will be congruent to one of these numbers modulo 6.

Question 2. Make some more tables! Try remainders modulo 3, or 7, or 10, or whatever other numbers you want.

+	

Question 3. Here are some slightly silly questions — please bear with us.

(a) If you draw a diagonal line from the top left of the table to the bottom right, you get a line of symmetry. Why does this happen?

(b) Some rows of the tables contain every possible remainder. Which rows are these?

(c) Which rows contain a 0? What can you say about the positions of the 0s?

Question 4. When two numbers add to give a remainder of 0 modulo q, these numbers get a special name: we say that they're *additive inverses* of each other modulo q. Which numbers have an additive inverse?

Question 5. Forget modular arithmetic for a moment — do additive inverses make sense in normal, everyday arithmetic?

That was addition, now let's try multiplication! Here's a multiplication table for remainders modulo 6:

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Question 6. Make some more tables! Try remainders modulo 3, or 7, or 10, or whatever other numbers you want.

×	

Question 7. (a) If you draw a diagonal line from the top left of the table to the bottom right, you get a line of symmetry. Why does this happen?

(b) Some rows of the tables contain all possible remainders. Which rows are these?

(c) Which rows contain a 1? What can you say about the positions of the 1s?

Question 8. Do you notice a connection between questions (b) and (c) above...?

When two numbers multiply to give a remainder of 1 modulo q, these numbers are called *multiplicative inverses* of each other modulo q.

Question 9. Do multiplicative inverses exist for regular, non-modular arithmetic?

I want to be able to answer the question "which rows of the multiplication table modulo q have a 1?", for arbitrary choices of q. Let's investigate!

Question 10. Answer these questions for each multiplication table you made on the previous page.

(a) The number that you divide by is called the *modulus* — for example, the modulus for the tables I gave you above is 6. For each table you made, write the list of factors of the modulus. (For example, when the modulus is 6, its factors are 1, 2, 3 and 6.)

(b) For each row containing a 1 in the multiplication table, write the list of factors of the row number. (For example, in the modulo 6 multiplication table above, the rows for 1 and 5 contain a 1: the factors of 1 are just 1, and the factors of 5 are 1 and 5.)

(c) What do the lists of factors for the remainders have in common with the list for the corresponding modulus?

What if you do the same for the numbers of the rows that *don't* contain a 1 — what do their lists of factors have in common with the modulus?

Question 11. Can you come up with a hypothesis for which numbers have a multiplicative inverse modulo n?

If the pattern is hard to spot, try making more multiplication tables. I particularly recommend multiplication modulo 10.

Question 12. Based on your hypothesis, what multiplication tables will have the most 1s?

Question 13. Suppose p and q are two different prime numbers. How many 1s will there be in the multiplication table modulo pq? How about modulo p^2?