

Solving discrete problems — Math 2020, Spring 2005

Hints for homework 4, and similar worked examples.

1. Multiplication and division tables for $\mathbf{Z}/13\mathbf{Z}$.

Note, in the book, the notation used is $\mathbf{Z}_{13} = \mathbf{Z}/13\mathbf{Z}$.

Note that $13 \equiv 0 \pmod{13}$, so we include a column and row for 0, but not for 13, which would be the same.

Note, you may find it helpful to write out a usual multiplication table first, to refer to:

a	b												
	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	27	30	33	36
4	0	4	8	12	16	20	24	28	32	36	40	44	48
5	0	5	10	15	20	25	30	35	40	45	50	55	60
6	0	6	12	18	24	30	36	42	48	54	60	66	72
7	0	7	14	21	28	35	42	49	56	63	70	77	84
8	0	8	16	24	32	40	48	56	64	72	80	88	96
9	0	9	18	27	36	45	54	63	72	81	90	99	108
10	0	10	20	30	40	50	60	70	80	90	100	110	120
11	0	11	22	33	44	55	66	77	88	99	110	121	132
12	0	12	24	36	48	60	72	84	96	108	120	132	144

Table for $a \times b$, usual integer multiplication

Use the above table to create the next table of multiplication modulo 13:

replace 42 with 3, because $42 = 39 + 3 = 13 \times 3 + 3 \equiv 3 \pmod{13}$

a	b												
	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	2	4	6	8	10	12	1	3	5	7	9	11
3	0	3	6	9	12	2	5	8	11	1	4	7	10
4	0	4	8	12	3	7	11	2	6	10	1	5	9
5	0	5	10	2	7	12	4	9	1	6	11	3	8
6	0	6	12	5	11	4	10	3	9	2	8	1	7
7	0	7	1	8	2	9	3	10	4	11	5	12	6
8	0	8	3	11	6	1	9	4	12	7	2	10	5
9	0	9	5	1	10	6	2	11	7	3	12	8	4
10	0	10	7	4	1	11	8	5	2	12	9	6	3
11	0	11	9	7	5	3	1	12	10	8	6	4	2
12	0	12	11	10	9	8	7	6	5	4	3	2	1

Table for $a \times b \pmod{13}$

Use the above multiplication table to find the mod 13 division table:

a	b												
	0	1	2	3	4	5	6	7	8	9	10	11	12
0	—	0	0	0	0	0	0	0	0	0	0	0	0
1	—	1	7	9	10	8	11	2	5	3	4	6	12
2	—	2	1	5	7	3	9	4	10	6	8	12	11
3	—	3	8	1	4	11	7	6	2	9	12	5	10
4	—	4	2	10	1	6	5	8	7	12	3	11	9
5	—	5	9	6	11	1	3	10	12	2	7	4	8
6	—	6	3	2	8	9	1	12	4	5	11	10	7
7	—	7	10	11	5	4	12	1	9	8	2	3	6
8	—	8	4	7	2	12	10	3	1	11	6	9	5
9	—	9	11	3	12	7	8	5	6	1	10	2	4
10	—	10	5	12	9	2	6	7	11	4	1	8	3
11	—	11	12	8	6	10	4	9	3	7	5	1	2
12	—	12	6	4	3	5	2	11	8	10	9	7	1

Table for $a/b \pmod{13}$, with “—” meaning “does not exist”

To find $x = 2/11 \pmod{13}$,

you need to solve

$11x \equiv 2 \pmod{13}$, so you just look for a 2 in the column under 11 in the previous table, and find that this is in row 12.

Filling in each column of this table comes from looking at the order of the entries in the same column of the previous table.

There are lots of interesting patterns in this table. Some of these are easier to see if you color in the numbers. E.g., color in all 11s blue — what pattern do you see? Why do you think this might be?

Notice that there are many patterns in the above two tables. Look for patterns you can see and relationships between the rows and columns.

Here are the tables for arithmetic modulo 12. Note that since 12 is not a prime, whereas 13 is, there are some important differences between these tables and the tables for arithmetic modulo 13.

a	b											
	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Table for $a \times b \pmod{12}$

a	b											
	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	-	1	-	-	-	5	-	7	-	-	-	11
2	-	2	1	-	-	10	-	2	-	-	5	10
3	-	3	-	1	-	3	-	9	-	3	-	9
4	-	4	2	-	1	8	-	4	2	-	4	8
5	-	5	-	-	-	1	-	11	-	-	-	7
6	-	6	3	2	-	6	1	6	-	2	3	6
7	-	7	-	-	-	11	-	1	-	-	-	5
8	-	8	4	-	2	4	-	8	1	-	2	4
9	-	9	-	3	-	9	-	3	-	1	-	3
10	-	10	5	-	-	2	-	10	-	-	1	2
11	-	11	-	-	-	7	-	5	-	-	-	1

Table for $a/b \pmod{12}$

We can write $2/10 \equiv 5 \pmod{12}$,

because $10 \times 5 \equiv 2 \pmod{12}$,

however, though the equation $10 \times x \equiv 2 \pmod{12}$ has a solution, which you can find in the table above, by looking at the 10 column, this equation has two solutions, since we also have $10 \times 11 \equiv 2 \pmod{12}$, since the 2 appears twice in this column.

So $2/10 \pmod{12}$ exists, but it's not unique.

The situation is even worse for trying to say what $6/6 \pmod{12}$ is — there are 6 possible values you could give this fraction.

2.

$$\mathbf{Z}/n\mathbf{Z}^\times = \{x : x \in \mathbf{Z}/n\mathbf{Z} \text{ and } \gcd(x, n) = 1\}.$$

Examples (this is for part B):

$$\mathbf{Z}/12\mathbf{Z}^\times = \{1, 5, 7, 11\}$$

$$\mathbf{Z}/13\mathbf{Z}^\times = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\mathbf{Z}/14\mathbf{Z}^\times = \{1, 3, 5, 9, 11, 13\}$$

$$\mathbf{Z}/15\mathbf{Z}^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

So, these sets have sizes: $\#(\mathbf{Z}/12\mathbf{Z}^\times) = 4$, $\#(\mathbf{Z}/13\mathbf{Z}^\times) = 12$, $\#(\mathbf{Z}/14\mathbf{Z}^\times) = 6$, $\#(\mathbf{Z}/15\mathbf{Z}^\times) = 8$.

(# means “size of” or “number of elements in” a set.)

A. Prove the following result:

If n, a and b are integers, and if $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

Hint 1: Before trying to prove something, you should make sure you understand what it means. A good way to do this is to compute examples.

E.g., let $n = 12$ and $a = 18$ and $b = 30$.

Then $a - b = 18 - 30 = 12 \times (-1)$, so $a \equiv b \pmod{12}$, so the hypothesis hold.

Now $\gcd(18, 12) = 6$ and $\gcd(30, 12) = 6$, so the conclusion is also true.

This only checks the result in one case, but if you can't do this you won't be able to prove it more generally, and examples are a good place to start to understand a theorem. You should try this out for other values of n, a, b .

Once you understand the result, you can try and prove it. The most important thing is to understand the definitions of the concepts used in the statement.

The following similar example should help you to see how to prove the result about the gcd:

Theorem: If n and a_1, b_1, a_2, b_2 are integers, then
if $a_1 \equiv a_2 \pmod n$ and if $a_2 \equiv b_2 \pmod n$ then $a_1 \times b_1 \equiv a_2 \times b_2 \pmod n$

proof: [first write the meaning of the hypothesis]

$a_1 \equiv a_2 \pmod n$ means that $a_1 - a_2$ is divisible by n , which means that there is some integer r and $a_1 - a_2 = n \times r$.

$b_1 \equiv b_2 \pmod n$ means that $b_1 - b_2$ is divisible by n , which means that there is some integer s and $b_1 - b_2 = n \times s$.

[Now what is the meaning of the conclusion, i.e., what do we want to show?

We want to show that $a_1 \times b_1 - a_2 \times b_2$ is divisible by n . So, in terms of the notation we've set up, involving r and s , we should try and compute this quantity. (We might not yet know how the hypothesis are going to get used, but we know they will get used somewhere.)]

We can rewrite the hypothesis as $a_1 = a_2 + nr$ and $b_1 = b_2 + ns$.

Now we have:

$$a_1 \times b_1 - a_2 \times b_2 = (a_2 + nr)(b_2 + ns) - a_2 b_2 = a_2 b_2 + nr b_2 + n s a_2 + a_2 b_2 n^2 r s - a_2 b_2 = nr b_2 + n s a_2 + a_2 b_2 n^2 r s = n(r b_2 + s a_2 + a_2 b_2 n r s). \text{ This is a multiple of } n.$$

So, $a_1 \times b_1 - a_2 \times b_2$ is a multiple of n , and so by definition $a_1 \times b_1 \equiv a_2 \times b_2 \pmod n$.

Q.E.D.

Note, the thinking behind the steps in this proof is given in square brackets. These parts are often not written in the final proof in text books. If you write the meaning of the hypothesis and conclusion for the result about the gcd, and follow similar steps, including remembering what the gcd actually means, you will get a proof of the result about the gcd.

Note, if you want more practice, you can see if you can prove results like:

If $a_1 \equiv a_2 \pmod n$ and $b_1 \equiv b_2 \pmod n$ then $a_1 + b_1 \equiv a_2 + b_2 \pmod n$. Try for $/$ and $-$ too. What kinds of results are true for powers?

C. Prove that if p is prime, then $\mathbf{Z}/p\mathbf{Z}^\times$ has $p - 1$ elements.

From some examples, you should be able to write a list of the elements of $\mathbf{Z}/p\mathbf{Z}^\times$, and once you have this it should not be too hard to see why they are in this set. See working for last week homework question about $n!$ for some useful comments relevant here also. (You can download this from the web page).

For parts D., E., F., Any kind of observations are OK. Don't have to be deep, or have a proof. Just compute examples and see if you see any patterns.

G. For integers n, a , find a condition on a so that $1/a \pmod n$ exists.

To do this, you need to go back to the definition — what does it mean for $x = 1/a \pmod n$? You will get an equation, and need to see if there is any way to tell whether this can have a solution or not. Before doing the general case, you should see what you can say in examples. E.g., does $1/3 \pmod 9$ exist? If not, why not? Looking at the tables of examples should also help. E.g., For the table for division mod 12 on the previous page, what is special about the entries in the first row, when they exist? You should use the other examples you should have computed also.

3. Can you find an example of a number m , which is not prime, and another number a so that $a^{m-1} \equiv 1 \pmod m$? Is so, give an example, if not, why not?

If $a^{m-1} \equiv 1 \pmod m$ for all a with $1 \leq a \leq m - 1$, can we conclude that m is prime? If so, prove this, if it's not true, give an example.

For this question, you need to refer to Fermat's little theorem, which we'll cover on Thursday (17 February). Computing several examples should give you enough to answer this.