Queen Mary University of London

MTH4104 Introduction to Algebra

Week 4 tutorial questions w/c 14 February 2022

This sheet contains questions for you to work through in your tutorial, singly or in a group.

It's important to work through lots of questions for practice. Remember that mathematics is not a spectator sport! If you want more questions, look at the "Extra questions" sheets on QMPlus.

Question 1

(a) The greatest common divisor of 61 and 18 is 1. Using the extended Euclidean algorithm, find a pair of integers (x,y) such that $61x+18y=1$.

(b) Find *all* pairs of integers (x,y) such that $61x+18y=0$.

[Hint: your previous experience with solving equations may be more useful than the Euclidean algorithm here.]

(c) Find all pairs of integers (x,y) such that $61x+18y=1$.

[Hint: combine the previous two parts.]

Solution (a) The Euclidean algorithm starts by dividing 61 with 18 obtaining a remainder r. Then divide 18 by r obtaining a new remainder, and continue. Explicitly:

$$\begin{aligned} 61 &= 3\cdot 18+7\\ 18 &= 2\cdot 7+4\\ 7 &= 1\cdot 4+3\\ 4 &= 1\cdot 3+1\\ 3 &= 3\cdot 1+0. \end{aligned}$$

This confirms that $\gcd(61,18)=1$, which was the last remainder before zero obtained by the algorithm.

The extended Euclidean algorithm works by back-substitution:

$$\begin{aligned} 1 &\\ &= 4-1\cdot 3\\ = 4-1(7-1\cdot 4) &= -1\cdot 7+2\cdot 4\\ = -1\cdot 7+2(18-2\cdot 7) &= 2\cdot 18-5\cdot 7\\ = 2\cdot 18-5(61-3\cdot 18) &= -5\cdot 61+17\cdot 18. \end{aligned}$$

Hence we can take $x = -5$ and $y = 17$.

(b) There are some "easy" solutions to this equation, namely $x = 18k$, $y = -61k$ for any integer k. These are solutions because

$$61(18k) + 18(-61k) = 0.$$

If you didn't see these right away, hopefully you found them after rearranging the equation to

$$\frac{y}{x} = \frac{-61}{18}$$

and realising that the fraction at left need not be in lowest terms.

In fact these are the only solutions. Because 61 divides $61x$, it must also divide $18y = -61x$; but it is a prime that does not divide 18, so in fact it must divide x. Therefore $x = 18k$ for some integer, which after substituting forces $y = -61k$.

(c) The key to this part is to notice that adding the two equations

$$61x + 18y = 1$$
$$61x' + 18y' = 0$$

gives the equation

$$61(x + x') + 18(y + y') = 1 + 0 = 1.$$

Therefore, by taking our single solution from part (a) and adding to it all the solutions from part (b), we will get more solutions to the equation with a 1 on the right hand side:

$$61(-5 + 18k) + 18(17 - 61k) = 1$$

for any integer k.

To prove that these are all of the solutions, we can use a similar trick and subtract equations. If

$$61x'' + 18y'' = 1$$

then

$$61(x'' - (-5)) + 18(y'' - 17) = 1 - 1 = 0$$

which implies, by the exhaustiveness of part (b), that $x'' + 5 = 18k$ and $y'' - 17 = -61k$ for some integer k.

Question 2 If you use the extended Euclidean algorithm with inputs 272 and 200, you will find that $\gcd(272, 200) = 8$, and that $272 \cdot (-11) + 200 \cdot 15 = 8$. You are welcome to do the computation yourself and double-check this, but for this question we will take it for granted.

(a) Find integers x and y such that $272x + 200y = 16$.

[Try to do this just using what I've told you, without running the algorithm.]

(b) Prove that there are no integers x and y such that $272x + 200y = 4$.

Solution (a) Because $16 = 8 \cdot 2$, we can produce a solution by doubling both sides of the equation that was given. That is,

$$272 \cdot (2 \cdot -11) + 200 \cdot (2 \cdot 15) = 2 \cdot (826 \cdot (-11) + 350 \cdot 15) = 2 \cdot 8 = 16.$$

So $x = 2 \cdot -11 = -22$ and $y = 2 \cdot 15 = 30$ will work.

(b) 8 is a common divisor of 272 and 200, that is, both of these numbers are divisible by 8. (Explicitly, $272 = 8 \cdot 34$ and $200 = 8 \cdot 25$.) So in the equation

$$272x + 200y = 4,$$

the left hand side is divisible by 8 (it equals $8(34x + 25y)$), while the right hand side is not. So they cannot be equal.

Question 3 Which elements $x \in \mathbb{Z}_{17}$ satisfy the equation

$$[9]_{17}x + [1]_{17} = [11]_{17} \cdot [9]_{17}^{-1} ?$$

Justify your answer.

Solution It is possible to do this by trial and error. After all, $\mathbb{Z}_{17}$ only has 17 elements. But it will be better preparation to solve the linear equation in the way you're used to doing, and then think about whether the with these unfamiliar congruence classes in place of numbers.

Before we get to that, let's work out $[9]_{17}^{-1}$. This inverse exists because 17 is prime so $\gcd(9, 17) = 1$. We could use Euclid's algorithm, but you might also just spot the fact that

$$[2]_{17} \cdot [9]_{17} = [18]_{17} = [1]_{17}$$

so that "by inspection" $[2]_{17}$ is the multiplicative inverse of $[9]_{17}$. Thus the right hand side of the equation is

$$[11]_{17} \cdot [9]_{17}^{-1} = [11]_{17} \cdot [2]_{17} = [22]_{17} = [5]_{17}.$$

Now, the first step of solving the linear equation

$$[9]_{17}x + [1]_{17} = [5]_{17}$$

would ordinarily be subtracting 1 from both sides. Doing that, and inserting some parentheses to be sure we don't make any undue assumptions about how $+$ works in modular arithmetic, yields

$$([9]_{17}x + [1]_{17}) - [1]_{17} = [5]_{17} - [1]_{17}.$$

The right hand side is simply $[4]_{17}$. To prove that we can simplify the left hand side, let's write $x = [a]_{17}$ and use this to work out the class in terms of a:

$$\begin{aligned} ([9]_{17}x + [1]_{17}) - [1]_{17} &= ([9]_{17}[a]_{17} + [1]_{17}) - [1]_{17} \\ &= [(9a + 1) - 1]_{17} \\ &= [9a]_{17} = [9]_{17}[a]_{17} = [9]_{17}x. \end{aligned}$$

Therefore

$$[9]_{17}x = [4]_{17}.$$

The next step would ordinarily be dividing through by $[9]_{17}$. Since we don't have division in $\mathbb{Z}_m$, let's multiply through by the inverse instead:

$$[9]_{17}^{-1}([9]_{17}x) = [9]_{17}^{-1}[4]_{17}.$$

For the right hand side we reuse our computation that the inverse of $[9]_{17}$ is $[2]_{17}$, giving

$$[4]_{17} \cdot [2]_{17} = [8]_{17}.$$

For the left hand side, again putting $x = [a]_{17}$, we have

$$[9]_{17}^{-1}([9]_{17}x) = [2]_{17}([9]_{17}[a]_{17}) = [18a]_{17} = [a]_{17} = x$$

because $18a - a = 17a$ is a multiple of 17.

Since all of the above steps were implications, $x = [8]_{17}$ is the only possible solution. Let's check that it really is a solution: $9 \cdot 8 + 1 = 73$ which *is* congruent to 5 modulo 17.

Alternatively, if you don't like finding modular inverses, you could have "cleared denominators first" by multiplying the whole equation by $[9]_{17}$. I leave as an exercise to you to check that that is also valid in $\mathbb{Z}_m$.

Question 4 How many of the elements of $\mathbb{Z}_{19}$ have multiplicative inverses? What about $\mathbb{Z}_{20}$? What about $\mathbb{Z}_{66}$?

Is there a way to calculate how many elements of $\mathbb{Z}_m$ have multiplicative inverses, without having to list and count them all? Hint: think about one prime factor of m at a time and which elements this factor "rules out".

Solution Recall that $[a]_m$ has a multiplicative inverse in $\mathbb{Z}_m$ if and only if a and m have no common factor. The first value of m is easy: since 19 is prime, none of the integers $1, 2, \ldots, 18$ have a common factor with 19, so all 18 nonzero elements

$$[1]_{19}, [2]_{19}, \ldots, [18]_{19}$$

have multiplicative inverses. (The zero element $[0]_{19}$ never does.)

Let's move on to $\mathbb{Z}_{20}$. 20 is not prime, but with just 20 elements

$$[0]_{20}, [1]_{20}, \ldots, [19]_{20}$$

of $\mathbb{Z}_{20}$, it is not a large ordeal to go through the whole list and check each a for common factors. Doing this shows that

$$a = 1, 3, 7, 9, 11, 13, 17, 19$$

is the complete list of a such that $[a]_{20}$ has a multiplicative inverse. All the other values of a either have a factor of 2 or 5 in common with 20. So the final answer is: 8 elements of $\mathbb{Z}_{20}$.

As m gets larger, writing down every element of $\mathbb{Z}_m$ starts to become a more arduous and error-prone task, and we should look for a systematic way to do it. Here is a more

systematic approach illustrated for $\mathbb{Z}_{66}$. We note that the prime factorisation of 66 is $2 \cdot 3 \cdot 11$. So these primes are the ones whose multiples we have to avoid when looking for numbers a for which $[a]_{66}$ is invertible. Multiples of 2 are the same as even numbers, so right away we can discard them and focus on the odd numbers only. 33 out of the 66 congruence classes are odd. Next we wish to get rid of the multiples of 3. In each group of three odd numbers, one is a multiple of 3, so this gets rid of one third of the remaining elements, and 22 are left. Finally, we have to get rid of the multiples of 11 that are still on the list, i.e. odd and not multiples of 3. The only such numbers less than $m = 66$ are

$$11 = 11 \cdot 1 \text{ and } 55 = 11 \cdot 5$$

so we remove these two more elements from the list of 22, leaving 20. These 20 elements have no common factors with 66, i.e. they are the elements with multiplicative inverses in $\mathbb{Z}_{66}$.

This answer can be generalised to any value of m, using the *Euler totient function*. If $p_1, \ldots, p_k$ are the distinct primes dividing m, then the number of invertible elements in $\mathbb{Z}_m$ is

$$\phi(m) := m \cdot (1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_n}).$$

Though this is not a proof, the formula should seem plausible in light of the above analysis. Starting with the m elements of $\mathbb{Z}_m$, we remove as non-invertible those that are multiples of p_1, that is one p_1-th of them; then of the remainder we remove those that are multiples of p_2, that is one p_2-th of what's left; etc.

Note that when we did $m = 20$, there was a prime that divided m "more than once", namely, 2^2 divides 20. But we still only have to remove the multiples of this prime once. This is why the word "distinct" appears in the previous paragraph.