Queen Mary University of London

MTH4104 **Introduction to Algebra**

Extra questions for chapter 2 **Spring 2021**

These questions are for you to practice with on your own schedule. You may e.g. want to try some each week as their topics come up in lectures, or use them in exam revision.

2 Modular arithmetic

2.1 Integer division

Question 2.1.1 A relation R on a set X is said to be *antisymmetric* if, for any elements $a, b \in X$, if aRb and bRa both hold then $a = b$.

(a) Prove that the divisibility relation $\mid$ on the set of positive integers is antisymmetric.

(b) Prove that $\mid$ is not antisymmetric on the set of all integers.

Solution (a) Let a and b be positive integers so that $a \mid b$ and $b \mid a$. By definition, this implies there are integers k and ℓ so that $b = ka$ and $a = \ell b$. Both of them must be positive. Substituting the second equation into the first shows $a = \ell(ka)$. Since $a \neq 0$, we may divide through by a. Then $1 = \ell k$, and the only way to factorise 1 as a product of two positive integers is $1 \cdot 1$. So $k = \ell = 1$, which implies that $a = b$.

(b) The divisibility relation on the integers is defined by the same rule as the relation on the naturals: if a and b are integers, then a divides b (written $a \mid b$) if and only if there is an integer q such that $b = qa$.

A counterexample to antisymmetry consists of two different integers each of which divides the other. For example, $a = 2$ and $b = -2$ provide such a counterexample: $2 \mid -2$ and $-2 \mid 2$ because $-2 = -1 \cdot 2$ and $2 = -1 \cdot -2$, but 2 and -2 are not equal.

2.2 Congruence mod m

Question 2.2.1 Let a be an integer. Suppose you don't know what a is; you only know what the congruence classes $[a]_4$ and $[a]_5$ are. From this information, is it possible to deduce the following congruence classes? Justify your answers.

(a) $[a]_2$

(b) $[a]_3$

(c) $[a]_{20}$

Solution (a) This question is asking: if you know the remainder of a on division by 4 and by 5, do you know its remainder on division by 2 (that is, whether it is even or odd)? The answer is yes, and it turns out only the remainder on division by 4 is important; the 5 is a red herring for the purposes of this part.

Looking at the congruence classes modulo 4 suggests this. Each congruence class in $\mathbb{Z}_4$ consists entirely of even or entirely of odd numbers:

$$\begin{aligned}
[0]_4 &= \{\ldots,-8,-4,0,4,8,12,\ldots\} : \text{even} \\
[1]_4 &= \{\ldots,-7,-3,1,5,9,13,\ldots\} : \text{odd} \\
[2]_4 &= \{\ldots,-6,-2,2,6,10,14,\ldots\} : \text{even} \\
[3]_4 &= \{\ldots,-5,-1,3,7,11,15,\ldots\} : \text{odd}
\end{aligned}$$

So if $[a]_4$ is $[0]_4$ or $[2]_4$ then $[a]_2 = [0]_2$ (a is even), whereas if $[a]_4$ is $[1]_4$ or $[3]_4$ then $[a]_2 = [1]_2$ (a is odd). In fact, what we have seen here can be put in set notation as

$$\begin{aligned}
[0]_4 \cup [2]_4 &= [0]_2, \\
[1]_4 \cup [3]_4 &= [1]_2.
\end{aligned}$$

We can prove this. Here is one of several possible proofs, using the *division algorithm*. If we write a in the form given by the division algorithm, $a = 4q + r$ where q is an integer and $r \in \{0,1,2,3\}$, the congruence class $[a]_4$ tells us what r is. Similarly, if $a = 2q' + r'$ where q is an integer and $r' \in \{0,1\}$, then knowing $[a]_2$ and knowing r' are the same thing.

Now, when we divide r itself by 2 with remainder, we get $r = 2s + t$, where s is 0 or 1 and t is 0 or 1. Substituting this in, we may write

$$a = 4q + (2s + t) = 2(2q + s) + t.$$

Since the quotient-remainder form is unique, $2q + s$ and t must be the quotient and remainder q' and r' from dividing a by 2. But t, and thus r', only depended on r (not on q); it can be computed from r alone. In other words, $[a]_2$ can be computed from $[a]_4$ alone.

(b) No, knowing $[a]_4$ and $[a]_5$ tells you nothing about $[a]_3$. For example,

- when $a = 0$, $[a]_4 = [0]_4$ and $[a]_5 = [0]_5$ but $[a]_3 = [0]_3$;
- when $a = 20$, $[a]_4 = [0]_4$ and $[a]_5 = [0]_5$ but $[a]_3 = [2]_3$;
- when $a = 40$, $[a]_4 = [0]_4$ and $[a]_5 = [0]_5$ but $[a]_3 = [1]_3$.

In other words, even if $[a]_4$ and $[a]_5$ are both zero, $[a]_3$ can be anything at all. Any number of similar examples can be cooked up by considering $a = b$, $a = 20 + b$, and $a = 40 + b$ for any integer b.

(c) Yes, you can deduce $[a]_{20}$, again as experimentation might suggest. In fact it turns out there is a very crisp way to say what this congruence class is:

$$[a]_{20} = [a]_4 \cap [a]_5.$$

Indeed, we can prove the above statement. To show an equality of two sets we need to show containment of each set in the other. So let b be an element of $[a]_{20}$. Then $b-a$ is a multiple of 20, that is $b-a=20k$ for some integer k. But then *a fortiori* $b-a$ is a multiple of 4 and of 5: indeed, $b-a=4(5k)=5(4k)$. So $b\in[a]_4\cap[a]_5$.

Conversely, suppose $b\in[a]_4\cap[a]_5$. This implies $b-a$ is divisible, separately, by both 4 and 5. We can write, e.g. $b-a=4\ell=5m$, where ℓ and m are integers. Therefore $5m$ is a multiple of 4, and this implies that m itself is a multiple of 4: you could see this e.g. by a case analysis considering every possible residue modulo 4, or by considering prime factorisations. We may thus write $m=4n$ for some integer n, so that $b-a=20n$, which implies $b\in[a]_{20}$ as desired.

In fact, using a similar argument to part (a), we see that knowing $[a]_{20}$ gives you exactly the same information as knowing $[a]_4$ and $[a]_5$, nothing more and nothing less. This is a case of a theorem in number theory or ring theory known as the *Chinese remainder theorem*. The theorem is so called because the first recorded problem involving it appears in *Sūnzǐ Suànjīng* (Master Sūn's Mathematical Classic), probably written in the Wèi or Jìn dynasties (220–420 AD). The first algorithm for solving it was given by Āryabhaṭa in the 6th century.

Question 2.2.2 Let m and n be positive integers and a any integer.

(a) Prove that, as sets,
$$[a]_m\cap[a]_n=[a]_{\mathrm{lcm}(m,n)}.$$

(b) I have a secret integer a in mind. I don't tell you what a is, but I do tell you the remainders when a is divided by m and when a is divided by n. Explain why the equation in part (a) implies that you can work out what the remainder is[1] when a is divided by $\mathrm{lcm}(m,n)$.

Solution (a) I will give the name ℓ to $\mathrm{lcm}(m,n)$, because it's annoying to have a long formula in a subscript. So we wish to prove
$$[a]_\ell=[a]_m\cap[a]_n.$$
This is an equality of two sets, so we need to show containment of each set in the other.

So let b be an element of $[a]_\ell$. Then $b-a$ is a multiple of ℓ, that is $b-a=k\ell$ for some integer k. But then $b-a$ is a multiple of m and of n, because ℓ is a multiple of m and n, and divisibility is transitive. So $b\in[a]_m\cap[a]_n$.

Conversely, suppose $b\in[a]_m\cap[a]_n$. This implies $b-a$ is divisible, separately, by both m and n. in other words, $b-a$ is a common multiple of m and n. What we have to prove is that $b-a$ is a multiple of $\ell=\mathrm{lcm}(m,n)$. In other words, we must prove that any common multiple of m and n is a *multiple* of $\mathrm{lcm}(m,n)$.

Sometimes this fact is given as part of the definition of the least common multiple. But our definition (see Section 2.4 of the notes) only tells us that the other common multiples are *larger*. So the rest of this proof is to reconcile that difference. One approach goes by contradiction: if $b-a$ were not a multiple of ℓ, then the remainder

[1] This principle, the *Chinese Remainder Theorem*, is used by several old riddles: see for example `https://www.cut-the-knot.org/blue/chinese.shtml`.

$r = (b-a) \bmod \ell$ could not equal zero, so it would satisfy $0 < r < \ell$, and it would also be a multiple of m and n by Proposition 2.9 from the notes. This contradicts the fact that ℓ is the *least* common multiple, and the proof is complete.

2.3 Arithmetic with congruence classes

Question 2.3.1 Explain how you could work out the remainder of 2^{80} modulo 19 *without* using a calculator or a computer.

Solution It's too troublesome and error-prone to work out 2^{80} (which is a twenty-five digit number), then divide by 19 and take the remainder.

The easiest way to turn that into a doable method is to "take remainders as you go along". That is, work out the powers of 2 in sequence by successive doubling, and take the remainder modulo 19 whenever doubling gives you a value greater than 19. This amounts working out the canonical representatives of $[2]_{19}, ([2]_{19})^2, ([2]_{19})^3$, etc. in sequence. This computation would begin thus:

$$\begin{aligned} &2^0 = 1, && 2^1 = 2, && 2^2 = 4, \\ &2^3 = 8, && 2^4 = 16, && 2^5 = 32 \equiv 32 - 19 = 13, \\ &2^6 \equiv 26 \equiv 26 - 19 = 7, && 2^7 \equiv 14, && \text{etc.} \end{aligned}$$

It's still tedious to do that 80 times. If you were dedicated and pressed ahead, though, you would soon notice that these values repeat, starting from $2^{18} \equiv_{19} 1$. So to compute 2^{80} mod 19 we only need to know what the 80th term of this sequence is, and for that we only need to know 80 mod 18, which is $80 - 72 = 8$. This is just one step beyond where I stopped in my table above: $2^8 \equiv 2 \cdot 14 \equiv 9$, so the answer is $[9]_{19}$.

In fact, this repetition is nothing but *Fermat's little theorem*, the fact that $a^{p-1} \equiv_p 1$ whenever p is a prime and a is not a multiple of p. So a good answer is "use Fermat's little theorem to factor $2^{80} = 2^{72} \cdot 2^8$ and ignore the first factor".

Another efficient approach you could have used is to factor the exponent 80 as $5 \cdot 2 \cdot 2 \cdot 2 \cdot 2$, which implies that $2^{80} = ((((2^5)^2)^2)^2)^2$. You can take the remainder mod 19 after each exponentiation. This plays out in the following way, where at intermediate stages I'm allowing myself negative numbers to make the squares smaller.

$$\begin{aligned} 2^5 &= 32 \equiv 13 \equiv -6, \\ 2^{10} &\equiv (-6)^2 = 36 \equiv 17 \equiv -2, \\ 2^{20} &\equiv (-2)^2 = 4, \\ 2^{40} &\equiv 4^2 = 16 \equiv -3, \\ 2^{80} &\equiv (-3)^2 = 9. \end{aligned}$$

Again we get the same answer $[9]_{19}$.

If you didn't know in advance when the sequence of powers would repeat (for instance if you couldn't factor the modulus m, which would stop you from using Fermat's little theorem), procedures of this general kind, based on repeated squaring, are the most efficient known. This works even when the given exponent doesn't have lots of factors of 2. For instance, if I had asked for 2^{81}, you could compute 2^{80} as above then multiply

by 2 at the end. By mixing multiplication by a and squaring in a suitable sequence, you can deal with any exponent — in fact, the sequence is derived from writing the exponent in binary.

2.4 gcd and Euclid's algorithm

Question 2.4.1

(a) Explain how to find the lcm of two positive integers using prime factorisations, similarly to how the gcd is found in the extra set of notes on QMplus "Greatest common divisors by prime factorisation".

(b) Prove that

$$\gcd(a,b)\cdot\operatorname{lcm}(a,b) = a\cdot b$$

for any two positive integers a and b.

(c) Describe an algorithm [i.e. a method] to compute the least common multiple of two positive integers which is efficient even when the integers are large.

You can use Euclid's algorithm, but not prime factorisations, as we have no efficient way to find the prime factorisation of a large number.

Solution (a) The formula for the lcm is: if $a = p_1^{e_1}\cdots p_k^{e_k}$ and $b = p_1^{f_1}\cdots p_k^{f_k}$ are prime factorisations, then

$$\operatorname{lcm}(a,b) = p_1^{\max(e_1,f_1)}\cdots p_k^{\max(e_k,f_k)}.$$

As in lecture, we let some of the e_i and/or f_j be zero so that we can use the same list of primes each time.

This works for a reason parallel to the proof of Proposition 1.3. If $m = p_1^{g_1}\cdots p_k^{g_k}$ is a common multiple of a and b, then by part (i) of the proposition, we have $g_i \geq e_i$ and $g_i \geq f_i$ for each i. Of these two lower bounds, the smaller one is redundant, so it is equivalent to require that $g_i \geq \max(e_i, f_i)$, which is the greater of the two bounds. The smallest m comes from minimising all of these exponents independently, i.e. $g_i = \max(e_i, f_i)$ for each i, giving the formula I presented above.

(b) What we just showed is that

$$\gcd(a,b) = 2^{\min\{e_2,f_2\}}\cdot 3^{\min\{e_3,f_3\}}\cdot 5^{\min\{e_5,f_5\}}\cdots$$

and

$$\operatorname{lcm}(a,b) = 2^{\max\{e_2,f_2\}}\cdot 3^{\max\{e_3,f_3\}}\cdot 5^{\max\{e_5,f_5\}}\cdots.$$

Taking the product, we have

$$\gcd(a,b)\operatorname{lcm}(a,b) = 2^{\min\{e_2,f_2\}+\max\{e_2,f_2\}}\cdot 3^{\min\{e_3,f_3\}+\max\{e_3,f_3\}}\cdots$$

But $\min\{e,f\}+\max\{e,f\} = e+f$, because the two summands $\min\{e,f\}$ and $\max\{e,f\}$ are just e and f in increasing order. So the product above is

$$2^{e_2+f_2}\cdot 3^{e_3+f_3}\cdot 5^{e_5+f_5}\cdots = ab.$$

(c) Here is a suitable algorithm for computing the lcm. The ingredients are the Euclidean algorithm, which is efficient (this is the point of Question 6), and the equation in part (b), which can be solved for the lcm.

Input. Two positive integers a and b.

Output. $\mathrm{lcm}(a,b)$.

Steps.

(1) Use the Euclidean algorithm to compute $d = \gcd(a,b)$.

(2) Output ab/d.

That's it.

Question 2.4.2 Prove that

$$a\gcd(b,c) = \gcd(ab,ac)$$

for all positive integers a,b,c.

Solution I'll give two proofs of this.

Proof 1: using the definition, mostly. Since a is a common divisor of ab and ac, it must be a divisor of $\gcd(ab,ac)$. Why is this? According to our definition, all we can conclude is that $a \leq \gcd(ab,ac)$. However, this is easy to see by thinking about the gcd in terms of prime factorisations: if the putative "greatest" common divisor of ab and ac was not a multiple of a, we could get a greater common divisor yet by multiplying in whichever factors of a we didn't account for yet. A formal version of this argument is Proposition 7.4 in the notes.

Now, if ae is a common divisor of ab and ac, so that $kae = ab$ and $\ell ae = ac$ for some integers k and ℓ, then dividing out by a (which is nonzero) shows that $ke = b$ and $\ell e = c$, that is e is a common divisor of b and c. The converse is true for essentially the same reason: if e is a common divisor of b and c, then ae is a common divisor of ab and ac. Therefore if d is the greatest common divisor of b and c, it follows that ad is the greatest common divisor of ab and ac (because this gcd must be a multiple of a, and our argument works for any multiple of a). So $\gcd(ab,ac) = ad$, which is what was to be shown.

Proof 2: algorithmically-minded. Consider running the Euclidean algorithm on the inputs b and c, and compare it to what happens if the inputs are ab and ac.

In the first step, if the inputs are b and c, they will be replaced with c and the remainder $b \bmod c$. To be precise, that remainder is the quantity r if we write out $b = qc + r$ in the form guaranteed by the division rule (q and r integers, $0 \leq r < c$). If the inputs were ab and ac, they will instead be replaced by ac and $ab \bmod ac$. But multiplying through the equation $b = qc + r$ by a gives

$$ab = q(ac) + ar$$

where $0 \leq ar < ac$, so that the remainder $ab \bmod ac$ is ar; that is to say,

$$ab \bmod ac = a(b \bmod c).$$

Therefore, after one step of the algorithm with ab and ac, the numbers we're working with are still a times those we'd be working with if we had started with b and c.

Iterating this argument for every step, we see that over the whole course of the Euclidean algorithm, the only difference it makes to replace b and c by ab and ac is that all the intermediate remainders get multiplied by a. In particular it multiplies the last remainder before the zero by a. This last remainder is the gcd, so we have proved $\gcd(ab,ac) = a\gcd(b,c)$.

If this isn't formal enough a proof for you, transform it into an induction!

Commentary. The reason an algebraist might be interested in the equation

$$a\gcd(b,c) = \gcd(ab,ac)$$

is because it has the same structure as the familiar rule for expanding parentheses,

$$a(b+c) = ab+ac.$$

When we study fields and rings later this semester, we will call the latter rule the *distributive* law. So a brief way of putting the former equation into words would be "multiplication *distributes* over gcd".

By the way, the result is still true if a, b or c are allowed to be 0. I just didn't want to make you have to bother with that case.

Question 2.4.3 This question explores how quickly the remainders in Euclid's algorithm decrease in size.

(a) Let $b_0, b_1, b_2, \ldots$ be the successive remainders computed in the course of Euclid's algorithm. Prove that $b_{i+2} < b_i/2$ for any $i \geq 1$.

[Hint: consider two cases, $b_{i+1} \leq b_i/2$ and $b_{i+1} > b_i/2$.]

(b) Let N be a natural number. Use part (a) to fill in the blank to make the following assertion true (your answer should have an N in it somewhere). Explain why your answer is correct.

> Let a and b be two natural numbers, both less than 2^N. If the Euclidean algorithm is used to compute $\gcd(a,b)$, it will take at most _____ steps to finish.

Solution (a) We consider two cases, as suggested. If $b_{i+1} \leq b_i/2$, then we need only observe that $b_{i+2} < b_{i+1}$, because b_{i+2} is a remainder obtained on division by b_{i+1}, and this implies

$$b_{i+2} < b_{i+1} \leq \frac{b_i}{2}.$$

So suppose that $b_{i+1} > b_i/2$, or equivalently, $2b_{i+1} > b_i$. Because $i+1$ is greater than 1, we know that b_{i+1} is genuinely the remainder of some number divided by b_i, as opposed to just being one of the inputs to the algorithm. Therefore $b_{i+1} < b_i$, which implies that b_{i+1} itself is the largest multiple of b_{i+1} not exceeding b_i, since $2b_{i+1}$ was too big. That is, $b_i \operatorname{div} b_{i+1} = 1$. This implies that the next remainder b_{i+2} equals

$$b_{i+2} = b_i - (b_i \operatorname{div} b_{i+1}) \cdot b_{i+1} = b_i - b_{i+1}.$$

By the assumption that $b_{i+1} > b_i/2$, we conclude

$$b_{i+2} < b_i - \frac{b_i}{2} = \frac{b_i}{2}.$$

(b) Part (a) says that, after every two steps of the Euclidean algorithm, the latest remainder is decreased to strictly less than half of its earlier value. Thus, starting with $b_1 = b$, we see that b_3 is less than $b/2$; that b_5 is less than $b_3/2$ which in turn is less than $b/4$; and so on. In general, if there is a b_{2k+1}, i.e. the algorithm didn't stop before that point, then b_{2k+1} is less than $b/2^k$. Since b itself is less than 2^N, setting $k = N$ tells us that if the algorithm didn't stop before getting to b_{2N+1}, then b_{2N+1} is less than $b/2^N < 2^N/2^N = 1$. The only natural number less than 1 is 0, so b_{2N+1} must equal zero, which means the algorithm stops upon computing b_{2N+1}. Therefore $\underline{2N+1}$ is a correct way to fill in the blank.

Actually, I suppose we should count b_2 as being the first step of the algorithm, b_3 as the second, and so on, because b_0 and b_1 are just the inputs, not a result of any step of computation. Then b_{2N+1} is computed on step number $\underline{2N}$, and you could fill the blank in that way.

Commentary. To give an example, let's take $N = 100$ and suppose that a and b are close to the upper limit of 2^{100}. Because

$$2^{100} = 10^{100 \cdot \log_{10} 2} = 10^{30.102999\ldots},$$

this means that a and b are 30- or 31-digit numbers. Even so, the Euclidean algorithm will finish in at most 200 steps! That would be painful to do by hand, but if you were locked in a cell with paper and pencil and not to be let out until you finished, you could do it in a day or two. Trying to do it by prime factorisation could be a life sentence...

As for modern computers, which do billions of operations a second, they would finish in the blink of an eye even for numbers much larger than this.

2.5 Euclid's algorithm extended

Question 2.5.1 Using the extended Euclidean algorithm[2], find $\gcd(186, 132)$, and find a pair of integers (x, y) such that

$$186x + 132y = \gcd(186, 132).$$

Solution (a) We run the algorithm. I will present it The forward phase goes:

$$\begin{aligned} 186 &= 1 \cdot 132 + 54 \\ 132 &= 2 \cdot 54 + 24 \\ 54 &= 2 \cdot 24 + 6 \\ 24 &= 4 \cdot 6 + 0. \end{aligned}$$

[2]If you want more questions to practice the extended Euclidean algorithm, see `http://www.maths.qmul.ac.uk/~fink/ExtendedEuclid.html`.

So $\gcd(186,132) = 6$.
(b) Now

$$\begin{aligned} 6 &= 54 - 2 \cdot 24 \\ &= 54 - 2(132 - 2 \cdot 54) = -2 \cdot 132 + 5 \cdot 54 \\ &= -2 \cdot 132 + 5(186 - 1 \cdot 132) = 5 \cdot 186 - 7 \cdot 132. \end{aligned}$$

Hence we can take $x = 5$ and $y = -7$.

Question 2.5.2

(a) Use the extended Euclidean algorithm to compute the greatest common divisor d of 206 and 64, and to find integers x and y such that $206x + 64y = d$.

(b) Write down another pair of integers (x', y') such that $206x' + 64y' = d$, different from the pair (x, y) you found in part (b).

Solution (a) We run the algorithm. The forward phase goes

$$\begin{aligned} 206 &= 3 \cdot 64 + 14 \\ 64 &= 4 \cdot 14 + 8 \\ 14 &= 1 \cdot 8 + 6 \\ 8 &= 1 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

So $d = \gcd(206, 64) = 2$.

Now for the extended phase:

$$\begin{aligned} 2 &= 8 - 1 \cdot 6 \\ &= 8 - 1(14 - 1 \cdot 8) = -1 \cdot 14 + 2 \cdot 8 \\ &= -1 \cdot 14 + 2(64 - 4 \cdot 14) = 2 \cdot 64 - 9 \cdot 14 \\ &= 2 \cdot 64 - 9(206 - 3 \cdot 64) = -9 \cdot 206 + 29 \cdot 64. \end{aligned}$$

Hence we can take $x = -9$ and $y = 29$.

(b) If (x, y) is a particular integer solution to $xa + yb = c$, then the general solution is

$$(x', y') = (x + kb/\gcd(a,b),\ y - ka/\gcd(a,b))$$

for $k \in \mathbb{Z}$. This is proved in Question 2.5.3 below. But for the present question we don't need to prove it, only to show off one more example. so we'll just use the formula. Here, taking $(x, y) = (-9, 29)$ and for example $k = 1$ yields $(x', y') = (23, -74)$.

How could you see this if you hadn't known the general formula? The insight is to think of a nonzero integer solution to $206X + 64Y = 0$, which is easy, and then put $x' = x + X$ and $y' = y + Y$.

Question 2.5.3 Let a and b be positive integers, and $d = \gcd(a,b)$.

(a) Prove that all solutions to the equation

$$ax + by = 0$$

with x and y integers are given by $x = kb/d$ and $y = -ka/d$, where k is an arbitrary integer.

(b) Suppose that x_0 and y_0 are the integers output by the extended Euclidean algorithm such that

$$ax_0 + by_0 = d.$$

Prove that all solutions to the equation

$$ax + by = d$$

are given by $x = x_0 + kb/d$ and $y = y_0 - ka/d$, where k is an arbitrary integer.

Solution (a) You will know how to solve this equation over the real numbers, and it may help to think about that first. You'd solve this equation by isolating one variable: it is equivalent to $by = -ax$, or $y = -ax/b$. So if x is any real number, then $y = -ax/b$ provides a real solution. Once you know this, all that is left to do is to figure out which integer values for x make y come out to be an integer as well.

Suppose x and y are integers solving the equation. We must have $b \mid ax$, in order for y to come out to an integer; formally speaking, $b \mid (-y)b = ax$. Since x is an integer we also have $b \mid bx$: that is, b is a common divisor of ax and bx. By Proposition 4.4 in the notes, b divides the greatest common divisor of these two, in symbols $b \mid \gcd(ax, bx)$, and by Question D, this can be recast as $b \mid \gcd(a,b) \cdot x$, that is, $\gcd(a,b) \cdot x = kb$ for some integer k. Dividing through by $\gcd(a,b)$, and remembering that we have given it the name d, yields $x = kb/d$. Substituting this into our real solution for y above produces $y = -ka/d$.

Finally, we should check that these are indeed integer solutions, to make sure we haven't introduced any spurious solutions. Indeed, $x = kb/d$ is an integer because $d \mid b$, and $y = -ka/d$ is because $d \mid a$, and moreover

$$a \cdot \frac{kb}{d} + b \cdot \frac{-ka}{d} = \frac{kab}{d} - \frac{kab}{d} = 0.$$

(b) I mentioned the trick to this in lecture, namely, adding and subtracting the equations with different solutions. Suppose that

$$ax + by = d$$

for some integers x and y. Subtracting this equation from

$$ax_0 + by_0 = d,$$

we get

$$a(x - x_0) + b(y - y_0) = 0.$$

Now by part (a), we know $x - x_0 = kb/d$ and $y - y_0 = -ka/d$ for some integer k, and moving x_0 and y_0 to the right hand side gives the statement sought.

Question 2.5.4 Let a, b, and c be fixed integers. Prove that there is an integer solution to $ax+by=c$ if and only if $\gcd(a,b)$ divides c.

Solution Let $d=\gcd(a,b)$, and let x_0 and y_0 be the integers provided by the extended Euclidean algorithm that make $ax_0+by_0=d$. Now if d divides c, we may write $c=kd$ for some integer k, and then

$$a(kx_0)+b(ky_0)=kd=c,$$

so that $(x,y)=(kx_0,ky_0)$ is a solution.

Conversely, suppose $ax+by=c$ where x and y are any integers. We know by the definition of the gcd that d divides each of a and b. Suppose $a=\ell d$ and $b=md$. Then

$$c=ax+by=a\ell d+bmd=(a\ell+bm)d,$$

so that d divides c.

Question 2.5.5 Let a and b be nonnegative integers.

(a) If a and b are not both zero, prove that the greatest common divisor of a and b is the unique nonnegative integer $d\geq 0$ with the properties

(i) $d \mid a$ and $d \mid b$;

(ii) if e is a nonnegative integer satisfying $e \mid a$ and $e \mid b$, then $e \mid d$.

(b) If $a=b=0$, prove that $d=0$ is the unique non-negative integer that satisfies conditions (i) and (ii).

The reason the statement in (a) is interesting is that, if we had used it as the *definition* of "greatest common divisor", then $\gcd(0,0)=0$ would be true by definition (this is what you showed in part (b)) and we would not have had to tack this on as a special case.

Solution (a) Let $d=\gcd(a,b)$. Condition (i) holds by the definition of common divisor. Now suppose that e is a nonnegative integer satisfying $e \mid a$ and $e \mid b$. Euclid's algorithm gives us integers x and y such that $d=xa+yb$. Now $e \mid xa$ and $e \mid yb$. So $e \mid xa+yb=d$, which is condition (ii).

We also have to prove that $d=\gcd(a,b)$ is the unique integer satisfying (i) and (ii). Any integer d satisfying (i) is a common divisor of a and b. And if d is not the greatest common divisor, then there is a greater common divisor e, so e cannot divide d.

(b) Every integer divides 0, so condition (i) is no restriction on d. For the same reason, condition (ii) amounts to

> if e is any nonnegative integer, then $e \mid d$.

Since every integer divides 0, the last sentence is true when $d=0$, but not when $d>0$ (for instance take $e=d+1$).

2.6 Modular inverses

Question 2.6.1

(a) Explain why $[59]_{84}$ has a multiplicative inverse in $\mathbb{Z}_{84}$.

(b) Find a non-negative integer $b < 84$ such that $[59]_{84}^{-1} = [b]_{84}$.

Solution (a) 84 and 59 have no common factors, that is, the gcd of these integers is 1. This can be justified by the Euclidean algorithm computations in part (b), but you can come to the answer more quickly if you can see it through the prime factorisations. 59 is a prime number, and so the only way it could have a common factor with 84 is if 59 were a factor of 84, but it is not (instead $84 = 2^2 \cdot 3 \cdot 7$).

By the extended Euclidean algorithm, there are integers x, y such that $84x + 59y = 1$. Hence $59y \equiv_{84} 1$, which implies that $[59]_{84}[y]_{84} = [1]_{84}$. So this $[y]_{84}$ is the multiplicative inverse for $[59]_{84}$ sought.

(b) To actually *compute* the inverse, we have to find integer solutions to $84x + 59y = 1$. This is done by applying the Euclidean algorithm, as follows:

$$\begin{array}{rcl} 84 = 1 \cdot 59 + 25 & \Rightarrow & 25 = 84 - 59 \\ 59 = 2 \cdot 25 + 9 & \Rightarrow & 9 = 59 - 2 \cdot 25 \\ 25 = 2 \cdot 9 + 7 & \Rightarrow & 7 = 25 - 2 \cdot 9 \\ 9 = 1 \cdot 7 + 2 & \Rightarrow & 2 = 9 - 1 \cdot 7 \\ 7 = 3 \cdot 2 + 1 & \Rightarrow & 1 = 7 - 3 \cdot 2 \\ 2 = 2 \cdot 1 + 0. & & \end{array}$$

Now we back-substitute starting from $1 = 7 - 3 \cdot 2$, remembering to open up brackets and to simplify before re-substituting:

$$\begin{array}{ll} & 1 \\ & = 7 - 3 \cdot 2 \\ = 7 - 3 \cdot (9 - 1 \cdot 7) & = -3 \cdot 9 + 4 \cdot 7 \\ = -3 \cdot 9 + 4 \cdot (25 - 2 \cdot 9) & = 4 \cdot 25 - 11 \cdot 9 \\ = 4 \cdot 25 - 11 \cdot (59 - 2 \cdot 25) & = -11 \cdot 59 + 26 \cdot 25 \\ = -11 \cdot 59 + 26 \cdot (84 - 59) & = 26 \cdot 84 + -37 \cdot 59. \end{array}$$

Hence $1 = 26(84) + (-37)(59)$ gives the solution $x = 26$ and $y = -37$. However the question asks for y in the range $0 \leq y < 169$! To arrange this, we simply add 84 to -37 to get another solution, representing the same congruence class,

$$y = 47.$$

It is always a good idea to check that you haven't made a mistake by calculating that the answer ($y = 47$) really does what it should do, namely satisfy the congruence

$$59 \cdot 47 \equiv_{84} 1.$$

This is true if and only if $59 \cdot 47 - 1$ is an integer multiple of 84. But $59 \cdot 47 - 1 = 2772$ and $2772/84 = 33$ is an integer.

Question 2.6.2 Find all solutions $x \in \mathbb{Z}_{31}$ to the equation

$$[16]_{31}\,x + [26]_{31} = [2]_{31}\,x + [3]_{31}.$$

Show your working. You are given that $[14]_{31}^{-1} = [20]_{31}$.

Solution The solution is presented in Antonino's first video, `https://qmplus.qmul.ac.uk/pluginfile.php/2506513/mod_folder/content/0/1.mov?forcedownload=1`, from 10:42 on. The solution in the video assumes knowledge that $\mathbb{Z}_{31}$ is a field.

Question 2.6.3 Find all $X, Y \in \mathbb{Z}_{11}$ that satisfy the simultaneous system of linear equations

$$\begin{aligned} [5]_{11}\,X + [2]_{11}\,Y &= [6]_{11} \\ [4]_{11}\,X + \qquad Y &= [2]_{11}. \end{aligned}$$

Solution This system of equations can be solved by any of the methods you know from school. There are, roughly, two ways to justify why. One way is to prove that each step in the manipulations below (or in your preferred method) is valid in modular arithmetic, by using the definitions of the operations in $\mathbb{Z}_{11}$. The other way is to use a fact from Chapter 3: since 11 is a prime number, $\mathbb{Z}_{11}$ is a *field*. So the "usual manipulations" work, and moreover we can divide freely by any element other than $[0]_{11}$, by multiplying by its multiplicative inverse.

For example, the second equation implies that

$$Y = [2]_{11} - [4]_{11}X$$

which we can substitute into the first equation to give

$$[5]_{11}\,X + [2]_{11}\,([2]_{11} - [4]_{11}X) = [6]_{11}.$$

Expanding the brackets and rearranging gives

$$([5]_{11} - [8]_{11})X = [6]_{11} - [4]_{11}$$

that is to say

$$[-3]_{11}X = [2]_{11}$$

or

$$[8]_{11}X = [2]_{11}.$$

So we must find $([8]_{11})^{-1}$, and multiply through by it. You could always use the extended Euclidean algorithm, but since the numbers here are small, it might honestly be faster to go through your 8 times table until you find a multiple of 8 which exceeds a multiple of 11 by one. Aha, $8 \cdot 7 = 56 = 5 \cdot 11 + 1$, so $([8]_{11})^{-1} = [7]_{11}$. So

$$X = [2]_{11}[7]_{11} = [14]_{11} = [3]_{11}.$$

Back-substituting into $Y = [2]_{11} - [4]_{11}X$ gives

$$Y = [2]_{11} - [4]_{11}[3]_{11} = [2]_{11} - [12]_{11} = [-10]_{11} = [1]_{11}.$$

So $X = [3]_{11}$ and $Y = [1]_{11}$ is the solution. Check this by substituting in again, if you need practice!