University of Birmingham
School of Mathematics

1AC Algebra: Feedback Sheet 2

Marking guidance

AQ2 and AQ4 are the questions to be marked using the guidance after those questions. There are a total of 20 marks for these algebra questions. The mark out of 20 for the algebra questions should be combined with the mark for the combinatorics questions, and then a total mark given as a percentage.

More importantly than giving the mark, you should provide detailed written feedback. There should be comments to explain where improvements can be made, even when it is just minor improvements. This could include: places where there are mathematical errors or inaccuracies; places where mathematics should be explained more clearly or in more detail; places where the mathematics should be set out better; or places where the solution is longer than necessary or overly verbose. You should ensure that feedback is given to explain reasons why marks have not been gained.

AQ1. Let $a, b, c \in \mathbb{Z}$.

(a) Suppose that a is coprime to b, and $a \mid bc$. Prove that $a \mid c$.

(b) Suppose that a is coprime to b, and that $a \mid c$ and $b \mid c$. Prove that $ab \mid c$.

(c) Suppose that a is coprime to c, and that b is coprime to c. Prove that ab is coprime to c.

You should use Bézout's lemma in your proofs, but you should **not** *use the Fundamental Theorem of Arithmetic.*

Solution

Let $a, b, c \in \mathbb{Z}$.

(a)

Claim. *Suppose that a is coprime to b and $a \mid bc$. Prove that $a \mid c$.*

Proof. Since a is coprime to b, there exist $x, y \in \mathbb{Z}$ such that

$$1 = xa + yb,$$

by Bézout's lemma. Multiplying by c gives

$$c = xac + ybc$$

Since $a \mid bc$, there exists $t \in \mathbb{Z}$ such that $at = bc$. Substituting this in to the equation above gives

$$c = xac + yat = a(xc + yt).$$

Therefore, $a \mid c$. □

(b)

Claim. *Suppose that a is coprime to b, and that $a \mid c$ and $b \mid c$. Then $ab \mid c$.*

Proof. Since $a \mid c$, there exists $x \in \mathbb{Z}$ such that $ax = c$, and since $b \mid c$, there exists $y \in \mathbb{Z}$ such that $by = c$.

Since a is coprime to b there exists $k, l \in \mathbb{Z}$ such that $ka + lb = 1$ by Bézout's lemma. Multiplying this equation by c and then substituting gives

$$\begin{aligned} c &= c(ka) + c(lb) \\ &= (by)(ka) + (ax)(lb) \\ &= (ab)(ky) + (ab)(lx) \\ &= ab(ky + lx). \end{aligned}$$

Hence, $ab \mid c$. □

(c)

Claim. *Suppose that a is coprime to c and b is coprime to c. Then ab is coprime to c.*

Proof. Since a is coprime to c there exists $k, l \in \mathbb{Z}$ such that $ka + lc = 1$ by Corollary 2.17. Multiply this equation by b to obtain

$$b = k(ab) + (lb)c.$$

Let $h = \text{hcf}(ab, c)$. Then $h \mid b$ by Lemma 2.3(a). Thus h is a common factor of b and c. Since b is coprime to c, we must have $h = 1$. Hence, ab is coprime to c. □

Feedback

The point of this question is to give you some more practice writing proofs well. The steps in the proofs are not obvious, so you may have to play around a bit before you see the trick required for the proof. Often the best method is to write down some equations that you can get from the hypothesis and then mess around with these and aim for an equation that implies the desired conclusion. The hints given on the canvas page should have helped too.

As always you should make sure that you give enough words and explanation in your proofs. Also you should remember to justify each of the steps.

There are alternative ways to do these proofs, and it is fine if you have done it another way (although it is not too good if the alternative is a lot longer). For example in (c) you can get equations $ka+lc = 1$ and $rb+sc = 1$ for some $k, l, r, s \in \mathbb{Z}$; then you could multiply these together to get $(kr)(ab) + (kas + lrb + lsc)c = 1$ and use that and Lemma 2.3(a) to show that $\mathrm{hcf}(ab, c) \mid 1$ and thus $\mathrm{hcf}(ab, c) \mid 1$.

It was stated that you should not use the fundamental theorem of arithmetic for the questions, and in any case it is better not to, as it is quicker without.

AQ2. (SUM) Find all solutions $x, y \in \mathbb{Z}$ to the following Diophantine equations.

(a) $x^3 = 4y^2 + 4y - 3$

(b) $x^2 - 3x = 9y^2 - 6y + 1$

Solution

(a) We want to find all solutions $x, y \in \mathbb{Z}$ of

$$x^3 = 4y^2 + 4y - 3 \tag{1}$$

First we factorize to get

$$x^3 = (2y - 1)(2y + 3).$$

Let $h = \mathrm{hcf}(2y - 1, 2y + 3)$.
By Lemma 2.3(a), $h \mid 4 = 2y + 3 - (2y - 1)$.
Also h is odd, as $h \mid 2y - 1$ so we must have $h = 1$.
Therefore, $2y - 1$ is coprime to $2y + 3$.

Using Theorem 2.26, we deduce that if $y \geq 1$, so that $2y - 1, 2y + 3 \in \mathbb{N}$, then they are perfect cubes. Also if $y \leq -2$, so that $-(2y - 1), -(2y + 3) \in \mathbb{N}$, then we can apply Theorem 2.26 to say that both $-(2y-1)$ and $-(2y+3)$ are perfect cubes, so that $2y + 1, 2y - 3$ are cubes of negative integers. The remaining cases where $y = 0$ or $y = -1$, we have that $(2y - 1)(2y + 3) = -3$, which is not a cube.

Thus both $2y + 3$ and $2y - 1$ are cubes of integers. From the list of cubes

$$0, \pm 1, \pm 8, \pm 27, \pm 64, \pm 125, \ldots$$

we see that we see that there are no perfect cubes that differ by 4.
Therefore, there are no the solutions $x, y \in \mathbb{Z}$ of (1).

(b) We want to find all solutions $x, y \in \mathbb{Z}$ of

$$x^2 - 3x = 9y^2 - 6y + 1 \tag{2}$$

First we factorize to get

$$x(x-3) = (3y-1)^2.$$

Let $h = \text{hcf}(x, x-3)$.
By Lemma 2.3(a), h is a factor of $3 = x - (x-3)$.
We have $3 \nmid (3y-1)^2$ and $x \mid (3y-1)^2$, so that $3 \nmid x$ and thus $3 \nmid h$.
Therefore, we must have $\text{hcf}(x, x-3) = 1$, so x is coprime to $x-3$.

We now split in to 4 cases depending on x.

Case 1. $x \geq 4$. Then $x, x-3 \in \mathbb{N}$, and we may apply Theorem 2.26, to see that both x and $x-3$ are perfect squares. From the list of squares

$$1, 4, 9, 16, 25, \ldots$$

we see that the only square that differ by 3 are 4 and 1. Thus $x = 4$ (and $x-3 = 1$), and then we have $4 = (3y-1)^2$. Thus $3y - 1 = \pm 2$, so that $y = 1$ or $y = -\frac{1}{3}$. Since we are want solutions with $y \in \mathbb{Z}$, we just get the solution $x = 4$, $y = 1$.

Case 2. $x = 0$ or $x = 3$. Then we have $x(x-3) = 0 = (3y-1)^2$, so that $y = \frac{1}{3}$. So we get no solutions with $y \in \mathbb{Z}$.

Case 3. $x = 1$ or $x = 2$. Then we have $x(x-3) = -2 = (3y-1)^2$, which has no solutions with $y \in \mathbb{Z}$.

Case 4. $x \leq -1$. Then $-x, -(x-3) \in \mathbb{N}$, and we may apply Theorem 2.26, to see that both $-x$ and $-(x-3)$ are perfect squares. Now the same logic as in Case 1., shows thats $-x = 1$ (and $-(x-3) = 4$), and we then find that the only solution for $y \in \mathbb{Z}$ is $y = 1$.

Putting together the four cases, we see that the solutions $x, y \in \mathbb{Z}$ of (2) are $x = 4$, $y = 1$, and $x = -1$, $y = 1$.

Feedback. You can use Example 2.27 to give a framework of how to solve these Diophantine equations, and how to set out your solutions. The first key step is to find the right factorization to use. The next key step is showing that h is equal to 1, which can be done similarly to the corresponding step in Example 2.27, but some thought is needed to work out how to do this. Once you have worked out how to do these steps you should ensure that it is explained clearly.

There is a bit of subtlety in the next step, where you want to apply Theorem 2.26 which we discuss here. This theorem is stated with the conditions that $a, b \in \mathbb{N}$, so we should only apply it with this hypothesis. This leads to some consideration of cases. We note that this subtlety should also be considered in Example 2.27, and an additional argument is explained in the typed notes. There is further discussion of this in the typed notes and there is an alternative theorem given in Theorem 2.27. As noted in the marking guidance below, you should not have been penalized much if you didn't get this quite right. Having applied Theorem 2.26 you should ensure that there is sufficient explanation of how you get to your solutions.

Marking guidance.

10 marks

(a) 5 marks. 1 mark for the factorization. 2 marks for the justification that $2y-1$ is coprime to $2y+3$. 1 mark for the deduction that $2y-1$ and $2y+3$ are perfect cubes (you can be lenient here if an application of Theorem 2.26 is made without considering the cases). 1 mark for the obtaining the solutions. Deduct a mark if there is not sufficient overall explanation and justification.

(b) 5 marks. The same guidance as for (a).

AQ3. (a) Prove Lemma 3.6(b):

> **Lemma.** *Let $n \in \mathbb{N}$ and $a, b, a', b' \in \mathbb{Z}$. Suppose that $a \equiv b \bmod n$ and $a' \equiv b' \bmod n$. Then $aa' \equiv bb' \bmod n$.*

(b) Find the remainder when $14^{43} - 12^{23}$ is divided by 13.

Solution

(a)

Lemma. *Let $n \in \mathbb{N}$ and $a, b, a', b' \in \mathbb{Z}$. Suppose that $a \equiv b \bmod n$ and $a' \equiv b' \bmod n$. Then $aa' \equiv bb' \bmod n$.*

Proof. Since $a \equiv b \bmod n$ and $a' \equiv b' \bmod n$, there exist $x, x' \in \mathbb{Z}$ such that

$$a = b + nx \tag{3}$$

and

$$a' = b' + nx'. \tag{4}$$

Multiplying (3) and (4) gives

$$aa' = bb' + n(xb' + bx' + nxx').$$

We have $xb' + bx' + nxx' \in \mathbb{Z}$, because $n, a, b, x, x' \in \mathbb{Z}$.
Therefore, $aa' \equiv bb' \bmod n$. □

(b) We are going to find the remainder when $14^{43} - 12^{23}$ is divided by 13. First we note that $14 \equiv 1 \bmod 13$, so

$$\begin{aligned} 14^{43} &\equiv 1^{43} \bmod 13 \\ &\equiv 1 \bmod 13. \end{aligned}$$

Next we note that $12 \equiv -1 \bmod 13$, so

$$\begin{aligned} 12^{23} &\equiv (-1)^{23} \bmod 13 \\ &\equiv -1 \bmod 13. \end{aligned}$$

Thus

$$\begin{aligned} 14^{43} - 12^{23} &\equiv 1 - (-1) \bmod 13 \\ &\equiv 2 \bmod 13. \end{aligned}$$

Hence, the remainder when $14^{43} - 12^{23}$ is divided by 13 is 2.

Feedback

There shouldn't be many problems the proof in (a), as you can use the proof of Lemma 3.6(a) as a template. In particular, this tells you the amount of explanation you should give in your proof. Then you just have to notice that you should multiply (3) and (4) (rather than adding them). You should explicitly say that $xb' + bx' + nxx' \in \mathbb{Z}$.

Part (b) just gives you a chance to practice doing calculations with congruences. A couple of points to make are that you should reduce your numbers modulo n after each calculation, and that it is sometimes easier to use negative numbers. As always you should provide explanation of what you're doing.

AQ4. (SUM) Determine whether each of the following statements is true and justify your answer.

(a) Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Suppose that $ab \equiv b^2 \bmod n$. Then $a \equiv b \bmod n$ or $b \equiv 0 \bmod n$.

(b) Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Suppose that there exists $z \in \mathbb{Z}$ such that $az \equiv 1 \bmod n$. Then a is coprime to n.

(c) Let $n \in \mathbb{N}$ with n odd. Then $8^{n-1} \equiv 1 \bmod n$.

When you are asked to justify your answer it means you have to prove it if it is true and give a counterexample if it is not true.

Solution

For the parts of this question we proceed by giving some rough working before presenting our solution.

(a) Consider the statement:

Rough working

Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Suppose that $ab \equiv b^2 \bmod n$. Then $a \equiv b \bmod n$ or $b \equiv 0 \bmod n$.

We start with some rough working, as we want to determine whether $a \equiv b \bmod n$ or $b \equiv 0 \bmod n$ can be deduced from $ab \equiv b^2 \bmod n$. Well supposing that $ab \equiv b^2 \bmod n$, we have that $n \mid ab - b^2 = (a-b)b$. Also $a \equiv b \bmod n$ means that $n \mid a - b$, and $b \equiv 0 \bmod n$ means that $n \mid b$. So we are trying to determined whether $n \mid (a-b)b$ implies that $n \mid a - b$ or $n \mid b$.

By now we should hopefully see that this is of statement is not true so we can aim to find a counterexample. Using Theorem 2.19 we can see that there won't be a counterexample with n prime. So we may first want to look for a counterexample with $n = 4$. Then some thought leads us to consider $a = 0$ and $b = 2$.

Now we have to write up our counterexample and ensure that we justify it is indeed a counterexample.

Statement. *Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. Suppose that $ab \equiv b^2 \bmod n$. Then $a \equiv b \bmod n$ or $b \equiv 0 \bmod n$.*

Counterexample. Let $n = 4$, $a = 0$, $b = 2$. Then $ab = 0$ and $b^2 = 4$, and $0 \equiv 4 \bmod 4$, so $ab \equiv b^2 \bmod n$. However, $0 \not\equiv 2 \bmod 4$ and $2 \not\equiv 0 \bmod 4$, so $a \not\equiv b \bmod n$ and $b \not\equiv 0 \bmod n$. Therefore, $n = 4$, $a = 0$, $b = 2$. is a counterexample to the statement.

(b) Consider the following statement.

Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Suppose that there exists $z \in \mathbb{Z}$ such that $az \equiv 1 \bmod n$. Then a is coprime to n.

Rough working

We aim to unpack the statement here to try to work out whether it is true. The hypothesis is equivalent to say that there exist $z, y \in \mathbb{Z}$ such that $az = 1 + ny$. We are then aiming to determine whether a is coprime to n, so we want to consider $h = \mathrm{hcf}(a, n)$ and try to show that it is equal to 1. To investigate this we can rearrange the equation above to get that $1 = az - ny$, and if we think about this equation we see that we can deduce that $h \mid 1$ by using Lemma 2.3, as we know that $h \mid a$ and $h \mid n$. Now we hopefully have the right idea of how to prove the statement and we can go ahead to give a proof.

Claim. *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Suppose that there exists $z \in \mathbb{Z}$ such that $az \equiv 1 \bmod n$. Then a is coprime to n.*

Proof. Since $az \equiv 1 \bmod n$, there exists $y \in \mathbb{Z}$ such that $az = 1 + ny$, and thus $1 = az - ny$. Let $h = \mathrm{hcf}(a, n)$. By Lemma 2.3(a) we have that $h \mid az - ny = 1$, and thus $h = 1$. Hence, a is coprime to n. □

(c) Consider the statement

Let $n \in \mathbb{N}$ with n odd. Then $8^{n-1} \equiv 1 \bmod n$.

Rough working
To determine whether we think this statement is true, we first we look at small values of odd n. We can calculate up to $n = 19$ and we get

$$\begin{aligned}
8^{1-1} &= 8^0 = 1 \equiv 1 \bmod 1\\
8^{3-1} &= 8^2 = 64 \equiv 1 \bmod 3\\
8^{5-1} &= 8^4 = 4096 \equiv 1 \bmod 5\\
8^{7-1} &= 8^6 = 262144 \equiv 1 \bmod 7\\
8^{9-1} &= 8^8 = 16777216 \equiv 1 \bmod 9\\
8^{11-1} &= 8^{10} = 1073741824 \equiv 1 \bmod 11\\
8^{13-1} &= 8^{12} = 68719476736 \equiv 1 \bmod 13\\
8^{15-1} &= 8^{14} = 4398046511104 \equiv 4 \bmod 15
\end{aligned}$$

Actually we stopped at $n = 15$ as we got a counterexample there. Note that these calculations could have been carried out electronically using an online modular arithmetic calculator, and if you did try to do them by hand then you should remember to reduce modulo n after each step, similarly to what we did in Examples 3.7

Now we just have to write this out and ensure that it is justified.

Statement. *Let $n \in \mathbb{N}$ with n odd. Then $8^{n-1} \equiv 1 \bmod n$.*

Counterexample. Let $n = 15$. We have $8^{15-1} = 8^{14} = 4398046511104 \equiv 4 \bmod 15$, and $4 \not\equiv 1 \bmod 15$, so $8^{15-1} \not\equiv 1 \bmod 15$. Therefore, $n = 15$ is a counterexample to the statement.

Feedback

In the rough working above there is guidance on how you may come to determining whether the statement is true or false. You do not have to include rough working in your submission, though there is no harm if there is some of this. It is really important in these sorts of questions to make sure you really understand the statement before you try to determine whether it is true or false, and doing some rough work will help with this. Remember though that the part of the solution that counts is the proof or counterexample. As stated on the problem sheet you should always give a proof to show that a statement is true, and provide a counterexample if the statement is not true.

When you are giving a proof, then you should ensure that it is explained sufficiently, and need to think through the steps. A common error in the proof for (b) can be to try to apply Bézout's lemma, but you are not in a position to apply this. If you're not sure why, then you should think through why it is not suitable to apply Bézout's lemma in this question, so that we should proceed in the proof as above.

Hopefully, for (a) once you think through what the statement says and have understood it, then you should be able to predict that it is false. You may also find that trying some small values for a, b and n may help with this. Then you should be able come up with your counterexample, and must ensure that you justify it. A comment here that may be helpful more generally is that we may be considering a statement that is similar to something we have seen before, for this case we note that the hypothesis translates to $n \mid b(a-b)$, which is a bit similar to hypothesis in Theorem 2.19, and so this may give a hint on how to come up with a counterexample.

We'll see Fermat's little theorem later in the module, and this will tell us that for a prime $p \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $p \nmid a$, we have $a^{p-1} \equiv 1 \bmod p$. This explains why it may take a while to get a counterexample to the statement in (c), as we need n to be composite, and as the statement is true for $n = 9$, the first time we can get a counterexample is for $n = 15$, and indeed we do. If you did have a go at proving this statement, then you may well have found that you weren't able to make any progress, which may make you think that it may not be true, so it is worth trying some more values of n to look for a counterexample. Then you should think that you may want to use some sort of online calculator to do this.

Marking guidance.

10 marks.

(a) 3 marks. 1 mark for stating that the statement is not true. 1 mark for the counterexample. 1 mark for the justification that it is a counterexample.

(b) 4 marks. 1 mark for stating the statement is true and 3 marks for the proof. The marks for the proof can be split as 1 mark for getting an equation of the form $az = 1+ny$, then 1 mark for saying $h \mid az-ny$ and 1 mark for deducing that $h = 1$.

(c) 3 marks. Same as for (a).