University of Birmingham
School of Mathematics

1AC Algebra: Feedback Sheet 3

Marking guidance

AQ1 and AQ3 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.
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. (SUM)

(a) Use the extended Euclidean algorithm to find $y, z \in \mathbb{Z}$ such that

$$41y + 32z = 1.$$

(b) Solve the linear congruence equation

$$32x \equiv 7 \bmod 41.$$

(c) Solve the following pair of simultaneous congruences.

$$x \equiv 18 \bmod 32$$
$$x \equiv 31 \bmod 41.$$

Solution

(a) We start by using the Euclidean algorithm to calculate $\mathrm{hcf}(41, 32)$; although we may be able to see in advance that this highest common factor is 1, we want to use the extended Euclidean algorithm, so that we can reverse this to calculate the required y and z.

First we write

$$41 = 32 + 9 \tag{1}$$

so that $\text{hcf}(41, 32) = \text{hcf}(32, 9)$.
Second we write

$$32 = 3 \cdot 9 + 5 \tag{2}$$

so that $\text{hcf}(32, 9) = \text{hcf}(9, 5)$.
Next we write

$$9 = 5 + 4 \tag{3}$$

so that $\text{hcf}(9, 5) = \text{hcf}(5, 4)$.
Next we write

$$5 = 4 + 1 \tag{4}$$

so that $\text{hcf}(5, 4) = \text{hcf}(4, 1) = 1$.
Thus $\text{hcf}(41, 32) = 1$.

Reversing our calculations we first rearrange (4) to get

$$1 = 5 - 4.$$

Then substituting for 4 from (3), we get

$$\begin{aligned} 1 &= 5 - (9 - 5)) \\ &= -9 + 2 \cdot 5. \end{aligned}$$

Then substituting for 5 from (2), we get

$$\begin{aligned} 1 &= -9 + 2(32 - 3 \cdot 9) \\ &= 2 \cdot 32 - 7 \cdot 9. \end{aligned}$$

Then substituting for 32 from (1), we get

$$\begin{aligned} 1 &= 2 \cdot 32 - 7(41 - 32) \\ &= -7 \cdot 41 + 9 \cdot 32. \end{aligned}$$

Therefore, $41y + 32z = 1$ for $y = -7$ and $z = 9$.

(b) To solve the linear congruence equation

$$32x \equiv 7 \bmod 41. \tag{5}$$

we look for $z \in \mathbb{Z}$ such that $32z \equiv 1 \bmod 41$. From (a) we know that we can take

$z = 9$. Thus multiplying (5) by 9 gives

$$\begin{aligned} 9 \cdot 32x &\equiv 9 \cdot 7 \bmod 41 \\ x &\equiv 63 \bmod 41 \\ x &\equiv 22 \bmod 41. \end{aligned}$$

In the above we get from the first line to the second by using that $9 \cdot 32 \equiv 1 \bmod 41$, and from the second to the third by using $63 \equiv 22 \bmod 41$.

Therefore, the solutions of (5) are given by $x \equiv 22 \bmod 41$.

(c) To solve the pair of simultaneous congruences

$$\begin{aligned} x &\equiv 18 \bmod 32 \\ x &\equiv 31 \bmod 41. \end{aligned} \tag{6}$$

we first use the first congruence to write $x = 18 + 32y$ for some $y \in \mathbb{Z}$. Then substituting into the second we obtain

$$\begin{aligned} 18 + 32y &\equiv 31 \bmod 41 \\ 32y &\equiv 13 \bmod 41. \end{aligned}$$

We solve this as in (b) to get

$$\begin{aligned} 9 \cdot 32y &\equiv 9 \cdot 13 \bmod 41 \\ y &\equiv 117 \bmod 41 \\ y &\equiv 35 \bmod 41. \end{aligned}$$

we then have $y \equiv 35 \bmod 41$, so $y = 35 + 41z$ for some $z \in \mathbb{Z}$. Hence,

$$x = 18 + 32(35 + 41z) = 1138 + 1312z.$$

Therefore, $x \equiv 1138 \bmod 1312$. Hence, we get that the solutions of (6) are given by $x \equiv 1138 \bmod 1312$.

Feedback

The first part gives you some more practice applying the extended Euclidean algorithm and you can find feedback on this from the first exercise sheet.

The key point in (b) is to realise that you have already found $z \in \mathbb{Z}$ such that $32z \equiv 1 \bmod 41$ in (a), so that you can use this to get a solution. This is much quicker than trying to find a solution by trial and error, so is the best way to proceed

here. You have to be careful with your calculations, and give some explanation of what you are doing.

For (c), you can proceed similarly to how we have done examples in the lectures. Then you should notice that you can solve the linear congruence equation similarly to how you did (b). Remember you have to explain your solution rather than just writing down a few calculations and stating the solution.

Marking guidance.

14 marks

(a) 4 marks. 1 mark for applying the Euclidean algorithm, 2 marks for correctly find y and z by reversing the Euclidean algorithm, 1 mark for the overall presentation and explanation.

(b) 5 marks. 1 mark for stating that the equation should be multiplied by the z found in (a), 3 marks for correctly carrying the calculations to obtain the solution, 1 mark for the overall presentation and explanation.

(c) 5 marks. 2 marks for making the substitution to obtain the linear congruence equation, 2 marks for solving this linear congruence equation and then deducing the solution of the simultaneous congruences. 1 mark for the overall presentation and explanation.

The marks for the presentation and explanation can be shared between the three parts, so that a mark out of 3 can be given for this over the three parts.

It is possible that a different method may be used in (b) and (c) in which case you should apply professional judgment to award partial credit. To be awarded a high mark there must be good explanation, and there should be some justification that all solutions are found.

AQ2. Prove Lemma 3.12

Lemma. *Let $a, b, x \in \mathbb{Z}$, let $n \in \mathbb{N}$ and let $h = \mathrm{hcf}(a, n)$.*

(a) *Suppose that $ax \equiv b \bmod n$. Then $h \mid b$.*

(b) *Suppose that $h \mid b$, let $a' = \frac{a}{h}$, $b' = \frac{b}{h}$ and $n' = \frac{n}{h}$.*

  (i) *$ax \equiv b \bmod n$ if and only if $a'x \equiv b' \bmod n'$; and*

  (ii) *a' is coprime to n'.*

Solution

Lemma. *Let $a, b, x \in \mathbb{Z}$, let $n \in \mathbb{N}$ and let $h = \mathrm{hcf}(a, n)$.*

(a) *Suppose that* $ax \equiv b \bmod n$. *Then* $h \mid b$.

(b) *Suppose that* $h \mid b$, *let* $a' = \frac{a}{h}$, $b' = \frac{b}{h}$ *and* $n' = \frac{n}{h}$.

(i) $ax \equiv b \bmod n$ *if and only if* $a'x \equiv b' \bmod n'$; *and*

(ii) a' *is coprime to* n'.

Proof. (a) Since $ax \equiv b \bmod n$, we have $ax = b + ny$ for some $y \in \mathbb{Z}$.

Also $h \mid a$ and $h \mid n$.

Hence, $h \mid b = ax - ny$.

(b) Suppose that $h \mid b$.
Let $h = \mathrm{hcf}(a, n)$, $a' = \frac{a}{h}$, $b' = \frac{b}{h}$ and $n' = \frac{n}{h}$.

(i) First suppose that $ax \equiv b \bmod n$. Then $ax = b + ny$ for some $y \in \mathbb{Z}$. Dividing by h, we obtain $a'x = b' + n'y$, so that $a'x \equiv b' \bmod n'$.

Now suppose that $a'x \equiv b' \bmod n'$. Then $a'x = b' + n'y$ for some $y \in \mathbb{Z}$. Multiplying by h, we obtain $ax = b + ny$, so that $ax \equiv b \bmod n$.

(ii) Let $h' = \mathrm{hcf}(a', n')$. Then there exist $u, v \in \mathbb{Z}$ such that $a' = h'u$ and $n' = h'v$. Multiplying by h gives that $a = ha' = hh'u$ and $n = hn' = hh'v$. Thus hh' is a common factor of a and n, so that $hh' \leq h$, and we deduce that $h' = 1$. Hence, a' is coprime to n'. □

Feedback

This question is a bit different from what we have seen in the lectures and it is important that you understand what you are being asked to prove before you start to write your proofs. Once you have understood the proofs, you'll hopefully see that the statements are reasonably clear, so it is just a matter of writing your proof well. Now that you have had some practice in constructing proofs, you hopefully have got used to writing down the equations that you can get from the hypothesis, and then trying to manipulate them to obtain an equation that implies the conclusion. Of course, after you have worked this out, you need to write out your proof properly and give good explanation in it.

AQ3. (SUM) Let $a \in \mathbb{N}$ with digits $a_r a_{r-1} \ldots a_2 a_1 a_0$. So

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^{r-1} a_{r-1} + 10^r a_r.$$

(a) Prove that $9 \mid a$ if and only if $9 \mid a_0 + a_1 + a_2 + \cdots + a_{r-1} + a_r$.

(b) Prove that $11 \mid a$ if and only if $11 \mid a_0 - a_1 + a_2 - \cdots + (-1)^{r-1} a_{r-1} + (-1)^r a_r$.

Solution

Let $a \in \mathbb{N}$ with digits $a_r a_{r-1} \dots a_2 a_1 a_0$. So

$$a = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^{r-1} a_{r-1} + 10^r a_r.$$

(a)

Claim. $9 \mid a$ *if and only if*

$$9 \mid a_0 + a_1 + a_2 + \cdots + a_{r-1} + a_r.$$

Proof. First we see that $10 \equiv 1 \bmod 9$, so we have $10^s \equiv 1 \bmod 9$ for all $s \in \mathbb{N}$. Therefore, we get

$$a \equiv a_0 + a_1 + a_2 + \cdots + a_{r-1} + a_r \bmod 11.$$

We have $9 \mid a$ if and only if $a \equiv 0 \bmod 9$. Thus $9 \mid a$ if and only if

$$a_0 + a_1 + a_2 + \cdots + a_{r-1} + a_r \equiv 0 \bmod 9$$

if and only if

$$9 \mid a_0 + a_1 + a_2 + \cdots + a_{r-1} + a_r. \qquad \square$$

(b)

Claim. $11 \mid n$ *if and only if*

$$11 \mid a_0 - a_1 + a_2 - \cdots + (-1)^{r-1} a_{r-1} + (-1)^r a_r.$$

Proof. First we see that $10 \equiv -1 \bmod 11$, so we have $10^s \equiv (-1)^s \bmod 11$ for all $s \in \mathbb{N}$. Therefore, we get

$$a \equiv a_0 - a_1 + a_2 - \cdots + (-1)^{r-1} a_{r-1} + (-1)^r a_r \bmod 11.$$

We have $11 \mid a$ if and only if $a \equiv 0 \bmod 11$. Thus $11 \mid a$ if and only if

$$a_0 - a_1 + a_2 - \cdots + (-1)^{r-1} a_{r-1} + (-1)^r a_r \equiv 0 \bmod 11$$

if and only if

$$11 \mid a_0 - a_1 + a_2 - \cdots + (-1)^{r-1} a_{r-1} + (-1)^r a_r. \qquad \square$$

Feedback

You should be able to do this question by adapting the method we used in Examples 3.8(b). So if you understand that example that example this problem hopefully shouldn't have caused much trouble. A key step in that example and also in doing these problems is to use that, for $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, we have $n \mid a$ if and only if $a \equiv 0 \bmod n$.

For (a) you should see that you only really need to changes the 3s to 9s in what we did in Examples 3.8(b). So that example shoes how you can set this out and you can use that as a template.

For (b), the key thing to notice is that $10^s \equiv (-1)^s \bmod 11$. Then it is mainly a matter of writing out your proof well by adapting what was done in Examples 3.8(b) and including all the details.

Marking guidance.

6 marks

(a) 3 marks. Award 3 marks if proof is fully correct and explained fully. Award 2 marks if the structure of the prof is correct, it is explained fairly well and there are just minor errors. Award 1 mark in the general idea of the proof is correct and deserves some credit.

(b) 3 marks. Same guidance as (a).

AQ4. (a) Let A be a subset of $\mathbb{Z}$ with 5 elements. Show that there exists a subset $B = \{a, b, c\}$ of A with 3 elements such that $a + b + c$ is divisible by 3.

(b) Find a subset A of $\mathbb{Z}$ with 4 elements such that $a + b + c$ is not divisible by 3 for any subset $B = \{a, b, c\}$ of A with 3 elements.

Solution

(a) Let A be a subset of $\mathbb{Z}$ with 5 elements.

Claim. *There exists a subset $B = \{a, b, c\}$ of A with 3 elements such that $a + b + c$ is divisible by* 3.

Proof. For $i = 0, 1, 2$, we let $n_i = |\{x \in A : x \equiv i \bmod 3\}|$, so n_i is the number of elements of A that are congruent to i modulo 3. We consider two cases for the values of n_0, n_1, n_2.

Case 1. $n_0, n_1, n_2 \geq 1$. Then there exist $a, b, c \in A$ such that $a \equiv 0 \mod 3$, $b \equiv 1 \mod 3$ and $c \equiv 2 \mod 3$. Then we have

$$\begin{aligned} a+b+c &\equiv 0+1+2 \mod 3 \\ &\equiv 3 \mod 3 \\ &\equiv 0 \mod 3. \end{aligned}$$

Case 2. There is some $i \in \{0,1,2\}$ such that $n_i = 0$. Let j and k be the elements of $\{0,1,2\}$ different from i. Then $5 = n_j + n_k$ and therefore either $n_j \geq 3$ or $n_k \geq 3$. Without loss of generality we may assume that $n_j \geq 3$, and then we can take distinct $a, b, c \in A$ such that $a \equiv j \mod 3$, $b \equiv j \mod 3$ and $c \equiv j \mod 3$. Then we have

$$\begin{aligned} a+b+c &\equiv 3j \mod 3 \\ &\equiv 0 \mod 3. \end{aligned}$$

In both cases we have that $a+b+c$ is divisible by 3, so we can take $B = \{1,2,3\}$. □

(b) Let $A = \{0,1,3,4\}$. We have $0 \equiv 0 \mod 3$, $1 \equiv 1 \mod 3$, $3 \equiv 0 \mod 3$ and $4 \equiv 1 \mod 3$. As in (a) we define $n_i = |\{x \in A : x \equiv i \mod 3\}|$, for $i = 0, 1, 2$. Then we have $n_0 = 2$, $n_1 = 2$ and $n_2 = 0$.

Now let $B = \{a, b, c\}$ be a subset of A with 3 elements and define $m_i = |\{x \in B : x \equiv i \mod 3\}|$ for $i = 0, 1, 2$. Since $n_2 = 0$, we have $m_2 = 0$ and we have the following two possibilities for m_0 and m_1.

(i) $m_0 = 2$, $m_1 = 1$; or

(ii) $m_0 = 1$, $m_1 = 2$.

Also we note that $a + b + c \equiv m_1 \mod 3$, and therefore $a + b + c \not\equiv 0 \mod 3$.

Hence, for any subset $\{a, b, c\}$ of A with three elements, we have that $a + b + c$ is not divisible by 3.

Feedback

This question was intended to be quite challenging and to make you think about how we can use congruences in this situation. You may have found it difficult to know where to start, but hopefully the hints on Canvas helped you to get started. It is important to realise that we want to consider congruences modulo 3, and what the elements of B are congruent to modulo 3.

For (a) it may have helped for you to think about different possibilities, for what the elements of B are congruent modulo 3, and then you may manage to spot a

pattern. Defining n_i as in the solution above is useful for being able to write out the proof nicely, as writing out the proof clearly is quite tricky. There are many other ways that you may have written out the proof, and there is not really a best way to do this.

To do (b) you should use what you have seen in (a). So that you want a set B which does not have 3 elements a, b and c that are all to each other congruent modulo 3, or such that $a \equiv 0 \bmod 3$, $b \equiv 1 \bmod 3$ and $c \equiv 2 \bmod 3$. One possible way to do this is to have two elements of B that are congruent to 0 modulo 3 and two elements of B that are congruent to 1 modulo 3. The example given above is the simplest way to get this configuration of congruences modulo 3. Remember that you do need to justify that your example does really satisfy the required condition. This can be done with a short proof as above, or you could do it by considering all 4 subsets of A of size 3.

Part (a) of this question deals with the case $n = 3$ of a much more general theorem known as the Erdös–Ginburg–Ziv theorem. This theorem says that in any set of $2n - 1$ integers, there is a subset of size of n whose sum is divisible by n. If you're interested, then you could find out more about that theorem on wikipedia at:
https://en.wikipedia.org/wiki/Zero-sum_problem
Actually it is stated differently there, though it is equivalent to what I have written above.