CISC-203*
Test #3
November 1, 2018

Student Number (Required) _____

Name (Optional) _____

This is a closed book test. You may not refer to any resources.

This is a 50 minute test.

Please write your answers in ink. Pencil answers will be marked, but will not be reconsidered after the test papers have been returned.

The test will be marked out of 50.

Question 1	/10
Question 2	/10
Question 3	/10
Question 4	/15
Question 5	/5
TOTAL	/50

☐ By writing my initials in this box, I authorize Dr. Dawes to destroy this test paper if I have not picked it up by January 15, 2019.

Question 1 : (10 marks)

Find all integer solutions to the equivalence $(x+6)*4 \equiv 5 \quad (\%7)$

Show your work.

Solution:

Look for a solution in $\mathbb{Z}_7$

$$
\begin{aligned}
(x \oplus 6) \otimes 4 &= 5 \text{ in } \mathbb{Z}_7 \\
x \oplus 6 &= 5 \otimes 4^{-1} \\
x \oplus 6 &= 5 \otimes 2 \text{ since } 4^{-1} = 2 \text{ in } \mathbb{Z}_7 \\
x \oplus 6 &= 3 \\
x &= 3 \ominus 6 \\
x &= 4
\end{aligned}
$$

Now generalize

Solutions are of the form x = 4 + k*7 for all integers k

Marking:

There are other acceptable approaches to this problem. For example, a student could solve $y*4 \equiv 5(\%7)$ **and get** $y = 3 + k*7$**, then use** $y = x + 6$ **to get** $x + 6 = 3 + k*7$**, ie** $x = -3 + k*7 \quad \forall k$ **, which is another equally correct form of the same set of solutions.**

Please give full marks for any correct derivation of the correct answer.

For a solution that is correct except for an error of arithmetic 8/10 or 9/10

For a solution that is mostly correct but makes an error of logic 6/10 or 7/10

For a solution that shows understanding of the problem but weak understanding of how to solve it	**5/10**
For a solution that shows limited understanding of the problem	**3/10 or 4/10**
For a solution that shows little understanding of the problem	**1/10 or 2/10**
For a blank page or a solution that shows no understanding of the problem	**0/10**

Question 2 : (10 Marks)

Prove that if a has an inverse in $\mathbb{Z}_n$ and a also has an inverse in $\mathbb{Z}_m$, then a has an inverse in $\mathbb{Z}_{n*m}$

(Hint: what must be true about a and n, in order for a^{-1} to exist in $\mathbb{Z}_n$?)

Solution:

a^{-1} exists in $\mathbb{Z}_n$ if and only if $a \in \mathbb{Z}_n$, $a > 0$, and a and n are relatively prime

$\Rightarrow$ a and n have no prime factors in common

Similarly, a and m have no prime factors in common

The prime factors of $n * m$ can only come from n or from m, so none of them can be prime factors of a

Thus a and $n * m$ are relatively prime

Note that $a < n$ and $a < m$, so $a < n * m$, so $a \in \mathbb{Z}_{n*m}$

Thus a has an inverse in $\mathbb{Z}_{n*m}$

Marking:

Students may express "a and n are relatively prime" as "gcd(a,n) = 1"

Marking should be similar to Question 1, with the difference that there is no scope for arithmetic error in this question. In general if a student makes a small error but then proceeds logically from that point, they should get a mark that reflects the correctness of "most of" their thinking. As always, a student whose answer shows that they completely understand the question should get at least 5/10

Students may attempt a constructive solution – for example, they may let $a^{-1} = x$ **in** $\mathbb{Z}_n$ **and** $a^{-1} = y$ **in** Z_m **and then try to identify** a^{-1} **in** $\mathbb{Z}_{n*m}$ **This is non-trivial. For example,** $2^{-1} = 3$ **in** $\mathbb{Z}_5$ **and** $2^{-1} = 4$ **in** $\mathbb{Z}_7$**, but** $2^{-1} = 18$ **in** $\mathbb{Z}_{35}$**. I don't know of a method to derive the** 18 **from the** 3 **and** 4**. Students who attempt to answer this way may get lost in the weeds quite quickly. This falls under the category of "understanding the question but not answering it" - I would give 6/10 for such an answer.**

Question 3 : (10 Marks)

Show the steps of computing $187^{37}\%144$ using "repeated squaring". You are not required to work out the final value, just show the steps.

Solution:

We can start by reducing 187 ***to*** $187\%144 = 43$***, but this is optional***

The important part is working out the pattern for squaring. Students can take the direct approach of translating 37 into binary 100101 or they can reason out that 37 = 2*18 + 1

18 = 2*9 + 0
9 = 2*4 + 1
4 = 2*2 + 0
2 = 2*1 + 0
1 = 1

Either way we end up with 100101 as the pattern for squaring, and the steps look like this

x = 187 % 144	***# 1***
x = x^2 % 144	***# 0***
x = x^2 % 144	***# 0***
x = (x^2 * 187) % 144	***# 1***
x = x^2 % 144	***# 0***
x = (x^2 * 187) % 144	***# 1***

This can also be expressed as

$$(((((187^2)^2)^2 * 187)^2)^2 * 187)\%144$$

Marking:

For a solution that shows the steps that build up to the final answer 10/10

Marking for incorrect or partially correct solutions should follow the guidelines for Question 1

Question 4 : (15 Marks)

(a) [5 marks] Let n be any odd number > 1.

If $a^{-1} = b$ in $\mathbb{Z}_n$, does $(2 \otimes a)^{-1} = b \oslash 2$ in $\mathbb{Z}_n$?

Show your work.

Solution: *First we must observe that 2^{-1} exists in $\mathbb{Z}_n$ because 2 is relatively prime with all odd numbers.*

Therefore $b \oslash 2$ is defined in $\mathbb{Z}_n$

$$\begin{aligned}(b \oslash 2) \otimes (2 \otimes a) &= (b \otimes 2^{-1}) \otimes (2 \otimes a) \\ &= b \otimes (2^{-1} \otimes 2) \otimes a \\ &= b \otimes a \\ &= 1\end{aligned}$$

Therefore $(b \oslash 2) = (2 \otimes a)^{-1}$ in $\mathbb{Z}_n$

Marking: The existence of 2^{-1} is an important point. Please give at most 4/5 if the student does not establish that modular division by 2 is always possible in this scenario.

There are other valid manipulations that establish $b \oslash 2$ as the inverse of $2 \otimes a$ Anything that is mathematically sound and reaches the correct conclusion is acceptable.

As always, give part marks to reflect the level of demonstration of understanding of the question and how to solve it.

(b) [5 marks] **Show that in $\mathbb{Z}_n$ where $n \geq 2$,** $(n-1) \otimes (n-1) = 1$

Solution:

$$\begin{aligned}(n-1) \otimes (n-1) &= ((n-1) * (n-1))\%n \\ &= (n^2 - 2n + 1)\%n \\ &= (1)\%n \\ &= 1 \text{ in } \mathbb{Z}_n\end{aligned}$$

Marking :

Students may conclude with just "$\ldots = 1$" rather than "$\ldots = 1$ in $\mathbb{Z}_n$" without penalty.

As usual, please give part marks for incomplete or partially correct answers.

(c) [5 marks]

Let n be a prime number. Let a, b and c be non-zero elements of $\mathbb{Z}_n$

Prove or disprove: $(a \otimes b) \oslash c = a \otimes (b \oslash c)$ in $\mathbb{Z}_n$

Solution: Since n is prime, all non-zero elements of $\mathbb{Z}_n$ have inverses in $\mathbb{Z}_n$

Thus

$$\begin{aligned}(a \otimes b) \oslash c &= (a \otimes b) \otimes c^{-1} \\ &= a \otimes (b \otimes c^{-1}) \qquad \text{because we know multiplication is associative} \\ &= a \otimes (b \oslash c)\end{aligned}$$

Students may choose to provide more detail, for example

$$\begin{aligned}(a \otimes b) \oslash c &= (a \otimes b) \otimes c^{-1} \\ &= ((a * b)\%n * c^{-1})\%n \\ &= ((a * b) * c^{-1})\%n \\ &= (a * (b * c^{-1}))\%n \qquad \text{because we know multiplication is associative} \\ &= (a * (b * c^{-1})\%n)\%n \\ &= a \otimes (b \otimes c^{-1}) \\ &= a \otimes (b \oslash c)\end{aligned}$$

Students may also try to argue that we can go directly from $(a \otimes b) \oslash c$ to $a \otimes (b \oslash c)$ because this is true in "normal" math, but it is not really obvious that it is also true in modular math, where division is not really the same as "normal" division.

Marking:

Please give full marks for any sequence of manipulations that establishes equality between the two expressions. Reducing everything to simple multiplication is the best method (I think). Students who do not replace "$b \oslash c$" by "$b \otimes c^{-1}$" need to provide some clear justification for re-arranging the parentheses.

As usual, please give part marks for incomplete or partially correct solutions.