Due: Monday, 17th July, 12:00 (AEDST)

Submission is through inspera. Prose should be typed, not handwritten.

Discussion of assignment material with others is permitted, but the work submitted *must* be your own in line with the University's plagiarism policy.

Problem 1 (16 marks)

For $x, y \in \mathbb{Z}$ we define the set:

$$S_{x,y} = \{mx + ny : m, n \in \mathbb{Z}\}.$$

(a) Give four elements of $S_{6,9}$.

(b) Give four elements of $S_{10,-16}$. 2 marks

For the following questions, let $d = \gcd(x, y)$ and z be the smallest positive number in $S_{x,y}$, or 0 if there are no positive numbers in $S_{x,y}$.

(c) (i) Show that $S_{x,y} \subseteq \{n : n \in \mathbb{Z} \text{ and } d|n\}$.

(ii) Show that $d \leq z$. 2 marks

(d) (i) Show that $z|x$ and $z|y$ (*Hint: consider* $(x \,\%\, z)$ *and* $(y \,\%\, z)$).

(ii) Show that $z \leq d$. 2 marks

Remark

The result that there exists $m, n \in \mathbb{Z}$ such that $mx + ny = \gcd(x, y)$ is known as Bézout's Identity.

Problem 2 (12 marks)

For all $x, y \in \mathbb{Z}$ with $y > 1$:

(a) Prove that if $\gcd(x, y) = 1$ then there is at least one $w \in [0, y) \cap \mathbb{N}$ such that $wx =_{(y)} 1$.
(*Hint: Use Bézout's identity*)

(b) Prove that if $\gcd(x, y) = 1$ and $y|kx$ then $y|k$.

(c) Prove that if $\gcd(x, y) = 1$ then there is at most one $w \in [0, y) \cap \mathbb{N}$ such that $wx =_{(y)} 1$.

Problem 3 (4 marks)

Prove that for all $m, n \in \mathbb{N}_{>0}$ with $n \leq m$:

$$\frac{3}{2}(n + (m \,\%\, n)) < m + n.$$ 4 marks

Problem 4 (12 marks)

Let $\Sigma = \{0,1\}$. For each of the following, prove that the result holds for all sets $X, Y, Z \subseteq \Sigma^*$, or provide a counterexample to disprove:

(a) $(X \cup Y)^* = X^* \cup Y^*$ 4 marks

(b) $(X \cap Y)^* = X^* \cap Y^*$ 4 marks

(c) $X(Y \cup Z) = (XY) \cup (XZ)$ 4 marks

Problem 5 (12 marks)

(a) List all possible functions $f : \{a,b,c\} \to \{0,1\}$, that is, all elements of $\{0,1\}^{\{a,b,c\}}$.

(b) Describe a connection between your answer for (a) and $\text{Pow}(\{a,b,c\})$. 4 marks

(c) Describe a connection between your answer for (a) and $\{w \in \{0,1\}^* : \text{length}(w) = 3\}$.

Problem 6 (4 marks)

Show that for any sets A, B, C there is a bijection between $A^{(B \times C)}$ and $(A^B)^C$. 4 marks

---

Problem 7 (12 marks)

Let S be a set.

(a) Show that for any set T and any function $f : S \to T$, the relation $R_f \subseteq S \times S$, defined as:

$$(s, s') \in R_f \text{ if and only if } f(s) = f(s')$$

is an equivalence relation. 6 marks

(b) Show that if $R \subseteq S \times S$ is an equivalence relation, then there exists a set T and a function $f_R : S \to T$ such that:

$$(s, s') \in R \text{ if and only if } f_R(s) = f_R(s')$$

6 marks

Problem 8 (16 marks)

Let $\mathbb{B} = \{0,1\}$ and consider the function $f : \mathbb{N} \to \mathbb{B}$ given by

$$f(n) = \begin{cases} 1 & \text{if } n > 0, \\ 0 & \text{otherwise.} \end{cases}$$

(a) Show that for all $a, b \in \mathbb{N}$:

(i) $f(a+b) = \max\{f(a), f(b)\}$

(ii) $f(ab) = \min\{f(a), f(b)\}$ 2 marks

From Problem 7, we know that $R_f \subseteq \mathbb{N} \times \mathbb{N}$, the relation given by:

$$(m, n) \in R_f \text{ if and only if } f(m) = f(n)$$

is an equivalence relation. Let $\mathbb{E} \subseteq \text{Pow}(\mathbb{N})$ be the set of equivalence classes of R_f, and for $n \in \mathbb{N}$, let $[n] \in \mathbb{E}$ denote the equivalence class of n.

We would like to define binary operations, $\boxplus$ and $\boxdot$, on $\mathbb{E}$ as follows:

$$[x] \boxplus [y] := [x + y]$$
$$[x] \boxdot [y] := [xy].$$

The difficulty is that the operands $[x]$ and $[y]$ can have multiple representations (e.g. if $z \in [x]$ then $[x] = [z]$), and so it is not clear that such a definition makes sense: if we take a different representation of the operands, do we still end up with the same result? For example, suppose $[1] = [2]$. Then we would want $[1] \boxplus [1] = [2] \boxplus [2]$, but with the proposed definition above, we would have $[1] \boxplus [1] = [2]$, and $[2] \boxplus [2] = [4]$, and it is by no means clear that $[2] = [4]$.

Our next step is to show that such a definition makes sense.

(b) Define relations $\boxplus, \boxdot \subseteq \mathbb{E}^2 \times \mathbb{E}$ as follows:

$((X, Y), Z) \in \boxplus$ if and only if there is $x, y \in \mathbb{N}$ such that $X = [x]$, $Y = [y]$ and $Z = [x + y]$
$((X, Y), Z) \in \boxdot$ if and only if there is $x, y \in \mathbb{N}$ such that $X = [x]$, $Y = [y]$ and $Z = [xy]$

(i) Show that $\boxplus$ is a function. 3 marks

(ii) Show that $\boxdot$ is a function. 3 marks

Part (b) shows that the informal definition of $\boxplus$ and $\boxdot$ given earlier is *well-defined*, so from now we will view $\boxplus$ and $\boxdot$ as **binary operations** on $\mathbb{E}$, that is $\boxplus, \boxdot : \mathbb{E} \times \mathbb{E} \to \mathbb{E}$.

(c) Show that for all $A, B, C \in \mathbb{E}$:

(i) $A \boxdot [1] = A$ 2 marks

(ii) $A \boxplus B = B \boxplus A$ 2 marks

(iii) $A \boxdot (B \boxplus C) = (A \boxdot B) \boxplus (A \boxdot C)$

Remark

Objects that have a concept of "addition" ($\boxplus$) and "multiplication" ($\boxdot$) where:

- addition and multiplication are associative,
- both operations have identities (see (c)(i)),
- addition is commutative (see (c)(ii)), and
- multiplication distributes over addition (see (c)(iii))

are known as semirings. We have already seen a number of semirings in this course:

- The natural numbers with usual addition and multiplication,
- Integers modulo n with addition and multiplication modulo n,
- Subsets of a set X with union and intersection,
- Languages with union and concatenation,
- Binary relations with union and relational composition (see Assignment 1),
- Matrices with matrix addition and matrix multiplication.

Problem 9 (12 marks)

Eight houses are lined up on a street, with four on each side of the road as shown:

Each house wants to set up its own wi-fi network, but the wireless networks of neighbouring houses – that is, houses that are either next to each other (ignoring trees) or over the road from one another (directly opposite) – can interfere, and must therefore be on different channels. Houses that are sufficiently far away may use the same wi-fi channel. Your goal is to find the minimum number of different channels the neighbourhood requires.

(a) Model this as a graph problem. Remember to:

  (i) Clearly define the vertices and edges of your graph.

  (ii) State the associated graph problem that you need to solve. 2 marks

(b) Give the solution to the graph problem corresponding to this scenario; and determine the minimum number of wi-fi channels required for the neighbourhood? 2 marks

(c) How do your answers to (a) and (b) change if a house's wireless network can also interfere with those of the houses to the left and right of the house over the road? 4 marks

Advice on how to do the assignment

Collaboration is encouraged, but all submitted work must be done individually without consulting someone else's solutions in accordance with the University's "Academic Dishonesty and Plagiarism" policies.

- Assignments are to be submitted in inspera.
- When giving answers to questions, we always would like you to prove/explain/motivate your answers. You are being assessed on your understanding and ability.
- Be careful with giving multiple or alternative answers. If you give multiple answers, then we will give you marks only for your worst answer, as this indicates how well you understood the question.
- Some of the questions are very easy (with the help of external resources). You may make use of external material provided it is properly referenced[1] – however, answers that depend too heavily on external resources may not receive full marks if you have not adequately demonstrated ability/understanding.
- Questions have been given an indicative difficulty level:

  

  This should be taken as a *guide* only. Partial marks are available in all questions, and achievable by students of all abilities.

[1] Proper referencing means sufficient information for a marker to access the material. Results from the lectures or textbook can be used without proof, but should still be referenced.