Due: Thursday, 29th February, 18:00 (AEDT)

Submission is through inspera. Your assignment will be automatically submitted at the above due date. If you manually submit before this time, you can reopen your submission and continue until the deadline.

If you need to make a submission after the deadline, please use this link to request an extension: https://www.cse.unsw.edu.au/ cs9020/extension_request.html. Unless you are granted Special Consideration, a lateness penalty of 5% of raw mark per 24 hours or part thereof for a maximum of 5 days will apply. You can request an extension up to 5 days after the deadline.

You may submit a pdf for each question in the final section (each question should be on its own pdf, and at most one pdf per question). Ideally this should be typeset for several reasons including legibility and plagiarism detection. The current policy is that handwritten submissions will still be marked.

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 (33 marks)

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

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

a) Prove that for all $m, n, x, y, z \in \mathbb{Z}$, if $z|x$ and $z|y$ then $z|(mx + ny)$. 4 marks

b) Prove that 2 is the smallest positive element of $S_{4,6}$.
Hint: To show that the element is the smallest, you will need to show that some values cannot be obtained. Use the fact proven in part (a) 4 marks

c) Find the smallest positive element of $S_{-6,15}$. 4 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 $S_{x,y}$.

d) Prove that $S_{x,y} \subseteq \{n \in \mathbb{Z} : d|n\}$. 4 marks

e) Prove that $d \leq z$. 3 marks

f) Prove that $z|x$ and $z|y$.
Hint: consider $(x\%z)$ and $(y\%z)$ 8 marks

g) Prove that $z \leq d$. 2 marks

h) Using the answers from (e) and (g), explain why $S_{x,y} \supseteq \{n \in \mathbb{Z} : d|n\}$ 4 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. Two useful consequences of Bézout's identity are:

- If $c|x$ and $c|y$ then $c|\gcd x, y$ (i.e. $\gcd(x, y)$ is a multiple of all common factors of x and y)
- If $\gcd(x, y) = 1$, then there is a unique $w \in [0, y)$ such that $xw =_{(y)} 1$ (i.e. multiplicative inverses exist in modulo y, if x is coprime with y)

Problem 2 (16 marks)

Proof Assistant: https://cgi.cse.unsw.edu.au/~cs9020/cgi-bin/proof_assistant?A1

Prove, using the laws of set operations (and any results proven in lectures), the following identities hold for all sets A, B, C.

a) (Annihilation) $A \cap \emptyset = \emptyset$ 4 marks

b) $(A \setminus C) \cup (B \setminus C) = (A \cup B) \setminus C$ 4 marks

c) $A \oplus \mathcal{U} = A^c$ 4 marks

d) (De Morgan's law) $(A \cap B)^c = A^c \cup B^c$ 4 marks

Problem 3 (26 marks)

Let $\Sigma = \{a, b\}$, and let

$$L_2 = (\Sigma^{=2})^* \qquad \text{and} \qquad L_3 = (\Sigma^{=3})^*.$$

a) Give a complete description of $\Sigma^{=2}$ and $\Sigma^{=3}$; and an informal description of L_2 and L_3. 4 marks

b) Prove that for all $w \in L_1$, $length(w) =_{(2)} 0$. 4 marks

c) Show that Σ^2 and Σ^3 give a counter-example to the proposition that for all sets $X, Y \subseteq \Sigma^*$, $(X \cap Y)^* = X^* \cap Y^*$. 4 marks

d) Prove that:

$$L_2 \cap L_3 = (\Sigma^{=6})^*$$

8 marks

e) Using the observation that every natural number $n \geq 2$ is either even or 3 more than a non-negative even number, prove that:

$$L_2 L_3 = \Sigma^* \setminus \{a, b\}$$

6 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:

  PASS CREDIT DISTINCTION HIGH DISTINCTION

  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.