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.

Answers are expected to be provided either:

- In the text box provided using plain text, including unicode characters and/or the built-in formula editor (diagrams can be drawn using the built-in drawing tool); or
- as a pdf (e.g. using LaTeX) – each question should be submitted on its own pdf, with at most one pdf per question.

Handwritten solutions will be accepted if unavoidable, but we don't recommend this approach as the assessments are designed to familiarise you with typesetting mathematics in preparation for the final exam and for future courses.

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

Objectives and Outcomes

The purpose of this assignment is to build your mathematical maturity in the areas of Number Theory and Sets and Languages. Most questions are presented at an abstract level so that the consequences are very general, and can be applied in a variety of situations: not just later on in the course, but also beyond. The specific motivation for each problem can be summarised as follows:

Problem 1: This question works through a proof of Bézout's Identity: the fact that the gcd of x and y can be written as an integer linear combination of x and y. To do this we work through an approach common throughout the course: Introducing a new definition based on known concepts; exploring that definition with some examples; and then proving results about the definition.

Problem 2: This question asks you to prove several set theory identities using the formality of the laws of set operations. Formal mathematical proofs are similar to programming because we are trying to reach an end goal by following very specific rules. We will see closely related proofs again when we cover Propositional Logic, and more generally, Boolean Algebras.

Problem 3: In this question we explore proofs involving formal languages. This question brings together the concepts of Sets, Languages and Number Theory and results from all areas will be needed to complete the proofs.

After completing this assignment, you will:

- Be able to make rigorous arguments about the foundational structures used in discrete mathematics [All problems]
- Understand several deeper connections between different topics of the course [Problems 1 and 3]

Advice on how to do assignments

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.
- In the assignment specification, 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.

Specific advice on how to do *this* assignment

Problem 1

The main purpose of any assignment is to assess your ability and understanding. A simple way to do this is to introduce you to a novel concept based on definitions you are familiar with; ask some exploratory questions to get you familiar with the concept; and then ask you to prove some results about the new concept. In this question we do this by defining a *family* of sets $S_{x,y}$ (i.e. one set for each pair of integers x, y); checking you are comfortable with the definition (parts (b) and (c)); and then proving results about the set which ultimately lead to Bézout's identity (parts (d) – (h)). The aim of the question is to show that the gcd of two numbers x and y is the smallest positive number that can be written in the form $mx + ny$ where m and n are integers (this is known as a *linear combination of x and y*). We do this by taking d to be the gcd and z to be the smallest positive linear combination of x and y and showing that $d = z$.

Important!

This question is asking you to prove Bézout's identity based on the principles from lectures. You should not make use of Bézout's identity in the process of the proof!

- Part (a) introduces a result that you will use throughout the problem (and the course), and it provides a gentle introduction to the process of providing rigorous proofs.

  Important!

  It is important that you prove this part (and parts (d) – (h)) in the abstract – that is, that you keep things general and use x, y, z, m, and n rather than proving the result for specific values. This will mean that the result can be applied in *any* situation.

  When working with proofs, a good first approach is to unravel definitions until you have something you can manipulate, and then reapply definitions until you reach the result. As an example, here is an HD-level solution for a related question:

  Prove that for all $x, m, z \in \mathbb{Z}$, if $x|z$ then $x|mz$.
  Suppose $x|z$.
  Then $z = kx$ for some $k \in \mathbb{Z}$ (by the definition of $|$).
  So for any $m \in \mathbb{Z}$: $mz = m(kx) = (mk)x$.
  As k and m are integers, (mk) is an integer, so $x|mz$ as required.

- Parts (b) and (c) are intended to get you familiar with the set $S_{x,y}$ for two pairs of x, y – namely $4, 6$ and $-6, 15$. The set $S_{4,6}$ is the set

  $$S_{4,6} = \{4m + 6n : m, n \in \mathbb{Z}\}$$

  so elements of this set are found by having m and n take various integer values. To show 2 is the smallest positive element of $S_{4,6}$ you need to show two things:

  – You need to show that $2 \in S_{4,6}$ – i.e. find integers m, n such that $2 = 4m + 6n$; and
  – You need to prove that $1 \notin S_{4,6}$. As this is fundamentally a "negated" statement, it could be useful to prove this by contradiction – that is, assume that $1 \in S_{4,6}$ and derive a contradiction. To use part (a), you need to find an integer z such that $z|4$ and $z|6$. This should tell you something useful about elements of $S_{4,6}$, in particular, why there is a problem if $1 \in S_{4,6}$.

- For part (c), it may be a good idea to try and find some elements of $S_{-6,15}$ and see if you notice a pattern. You do not need to include this experimentation in your final solution, unless you believe it adds to your demonstration of ability and understanding. To justify your answer, you should go through similar steps to part (b), but there may be additional steps required to exclude possible smaller values.
- For parts (d) –(h) you should be working in the abstract - that is, you should be keeping things general and using x, y, d and z rather than specific values – with the exception of the case when $z = 0$. It is easiest to consider this case separately, noting that $z = 0$ automatically places restrictions on x, y and d.
- To show a set A is a subset of B, you need to show that every element of A is also an element of B. In the case of part (d), the set A is the set $S_{x,y}$ and the set B is the set of integer multiples of d. So you need to prove that number that can be written in the form $mx + ny$ where $m, n \in \mathbb{Z}$ is multiple of d. Note that you have to prove this for all m and n, not specific values. Since we are working with arbitrary values for x, y, and d, the only way to prove this is to work from the definitions (just as with part (a)).
- To show that $d \leq z$, we note that, by definition, $z \in S_{x,y}$. So what does the previous result now tell us about z and d? Be careful – this doesn't immediately give the result, you need one more observation – namely that d and z are positive. You may use the result of (d), even if you haven't proven it, to answer this question.
- Once you have a proof that $z|x$, the proof that $z|y$ will likely follow in a similar way (because x and y are interchangeable in all definitions). It is acceptable to write "Similarly $z|y$".
- The hint says to show that $z|x$ you should conisder $x \,\%\, z$. If $z|x$, what does that mean for $x \,\%\, z$? Now consider the following two observations:
  - $0 \leq (x \,\%\, z) < z$ (from the lectures)
  - z is the smallest **positive** element of $S_{x,y}$

  So if we could show that $(x \,\%\, z) \in S_{x,y}$ what does that mean? How might we show $(x \,\%\, z) \in S_{x,y}$? Well, as we are working in the abstract, we cannot do much with $x \,\%\, z$ other than rewrite it according to its definition.
- To show $z \leq d$ recall the definition of d and consider what we have shown about z in the previous question. You may use the result of (e), even if you haven't proven it, to answer this question.
- For part (h) we now have to show every multiple of d is an element of $S_{x,y}$. The hint tells us to us (e) and (g) – this should give you one multiple of d in $S_{x,y}$. How might we be able to extend that to show that *every* multiple of d is in $S_{x,y}$?

Problem 2

For this problem you are asked to prove the identities using the Laws of Set Operations (and any derived laws proven in lectures).

Important

Full marks for these questions will only be awarded to proofs using the Laws of Set Operations. Partial marks are available for proofs that do not use the laws.

Formal proofs, as we require here, are much stricter than other types of proofs encountered in this course (or even this assignment!). There are two main reasons why we require formal proofs for these questions:

– Formal proofs highlight the close connection between mathematical reasoning and programming in Computer Science. When programming, you have to be precise with your instructions because computers are very strict with their execution. If we can write mathematical arguments with the same level of strictness, then this gives us a basis for having computers "reason".

– We will see the same set of laws twice more in the course when we cover Propositional Logic and Boolean Algebras. This means that proofs built solely from the Laws of Set Operations will translate directly to those other topics – giving us multiple results for free.

Here is an example of a formal proof using the Laws of Set Operations:

Prove that $\emptyset^c = \mathcal{U}$:

$$\begin{aligned} \emptyset^c &= \emptyset^c \cup \emptyset && \text{(Identity of } \cup\text{)} \\ &= \emptyset \cup \emptyset^c && \text{(Commutativity)} \\ &= \mathcal{U} && \text{(Complementation)} \end{aligned}$$

- To ensure full marks, each step should be justified with a single rule. That rule may apply in multiple, non-overlapping, places (not currently implemented in the Proof Assistant).
- You may use Uniqueness of Complement and/or Principle of Duality, and these may be useful for part (d). These are not currently implemented in the Proof Assistant either.
- You may prove and use your own intermediate results if it helps (also not implemented in the Proof Assistant).

Problem 3

This question brings together the topics of Sets, Languages and Number Theory. You are asked to prove and disprove set-based identities, but because the constructed sets are based around formal languages, the Laws of Set Operations do not apply. Instead, we will need to prove these results from first principles, together with results from Number Theory.

- Part (a) is intended to familiarise you with the languages L_2 and L_3. The languages $\Sigma^{=2}$ and $\Sigma^{=3}$ have only finitely many words in them, so can be explicitly listed out. L_2 and L_3, on the other hand, have infinitely many words so cannot be completely listed. Instead you should provide a description of these languages, **based on their construction** rather than on properties such as the one used in part (b). A good description makes it easy to check if a given word belongs to the language or not. A few examples following the description can be helpful. As an example, here is a reasonable informal description of the language XY where $X = \{a\}^*$ and $Y = \{a\}^*$:

  > XY consists of words of the form xy where x is a word of 0 or more a's and y is a word of 0 or more a's. That is, $XY = \{\lambda, a, aa, aaa, \ldots\}$.

  Note that the observation that $XY = \{a\}^*$ was not part of the description, as this is something that should be proven (see below)

- A counterexample to a "for all" type of proposition, is a single example which shows that the proposition is false. In part (c) we want to show that

  $$(\Sigma^{=2} \cap \Sigma^{=3})^* \neq (\Sigma^{=2})^* \cap (\Sigma^{=3})^*.$$

  To show two sets are unequal it is sufficient to find an element of one which is not an element of the other (note that λ is an element of both sides!). You may use part (d) (if proven) if it helps.

- The only approach to proving set equality (covered in lectures) that applies in parts (d) and (e) is to show $A \subseteq B$ and $B \subseteq A$. Here is an example of such a proof, using the sets X and Y defined earlier:

  Prove that $XY = \{a\}^*$:
  We first show that $XY \subseteq \{a\}^*$.
  If $w \in XY$ then $w = xy$ where $x \in X$ and $y \in Y$. As $X = Y = \{a\}^*$, we have x and y are a sequence of 0 or more a's. Therefore xy is a sequence of 0 or more a's, and hence $xy \in \{a\}^*$.

  We now show that $\{a\}^* \in XY$.
  Let $w \in \{a\}^*$. Then $w = w\lambda$. As $w \in \{a\}^* = X$ and $\lambda \in Y$ we have that $w \in XY$.

  We have shown that $XY \subseteq \{a\}^*$ and $\{a\}^* \in XY$, therefore $XY = \{a\}^*$.

- For part (d) it may help to review the definition of the least common multiple from the Number Theory content.

- For part (e), another way of describing $\Sigma^* \setminus \{a, b\}$ which may be helpful is:

$$\Sigma^* \setminus \{a, b\} = \{\lambda\} \cup \Sigma^{\geq 2}.$$