NAME: ____________________________

SPIRE ID: ____________________________

COMPSCI 250
Introduction to Computation
SOLUTIONS to First Midterm Fall 2025 – Version 2

D. A. M. Barrington and M. Golin 9 October 2025

DIRECTIONS:

- Answer the problems on the exam pages.
- There are 6 problems on pages 2-11, some with multiple parts, for 100 total points plus 5 extra credit. Final scale will be determined after the exam.
- Page 12 contains useful definitions and is given to you separately – do not put answers on it!
- But, if you do write on the back of a page, you must explicitly add a note on the front side stating that you are continuing on the back page. Otherwise, we might not see your solution on Gradescope.
- No books, notes, calculators, or collaboration.
- In case of a numerical answer, an arithmetic expression like "$2^{17} - 4$" need not be reduced to a single integer.
- Your answers must be LEGIBLE, and not cramped. Write only short paragraphs with space between paragraphs

1	/10
2	/10
3	/20
4	/20
5	/20+5
6	/20
Total	/100+5

Family Name: ______________________

Definitions for Questions 1-3: In this scenario, we have a set $D = \{b, c, i, k, r\}$ of exactly five dogs (Blaze, Clover, Indie, Kiké, and Rhonda), and a set $T = \{\text{Curly}, \text{Fluffy}, \text{None}, \text{Straight}\}$ of exactly four tail types.

The relation H from D to T, which is also a **function**, is defined by the predicate $H(d, t)$ meaning "dog d has tail type t". The binary relation Y on D is defined by the predicate $Y(d, e)$ meaning "dog d is younger than dog e". You are given that Y is a **strict partial order**, meaning that it is **antireflexive**, **antisymmetric**, and **transitive**.

Question 1 (10): (Translations)

- (a, to symbols, 2 points) **Statement I:** If Clover has a Fluffy tail, then either Indie has a Straight tail or Blaze has no tail, but not both.

  $H(c, F) \rightarrow (H(i, S) \oplus H(b, N))$. *(97% correct.)*

- (b, to English, 2 points) **Statement II:** $H(c, F) \vee \neg(H(i, S) \rightarrow H(b, N))$

  Either Clover has a Fluffy tail, or it is not the case that if Indy has a Straight tail, then Blaze has no tail. *(62% correct. Lots of people incorrectly negated the implication, and others got the parenthesization wrong. Also, if the first word of your answer was "if", it is wrong because of the scope of the implication.)*

- (c, to symbols, 2 points) **Statement III:** If it is not the case that both Indie has a Straight tail and Clover has a Fluffy tail, then Clover has a Fluffy tail and it is not the case that Blaze has no tail.

  $\neg(H(i, S) \wedge H(c, S)) \rightarrow (H(c, F) \wedge \neg H(b, N))$. *(95% correct.)*

- (d, to English, 2 points) **Statement IV:** $\forall d : ((d = r) \vee Y(r, d)) \wedge ((d = k) \vee Y(d, k))$

  Any dog is either has Rhonda equal to it or younger than it, and is either equal to or younger than Kiké. (*66% correct. The most common problem was to ignore case of equal elements, by saying something like "Every dog is older than Rhonda". "Every other dog is older than Rhonda", etc., was fine.)*

- (e, to symbols, 2 points) **Statement V:** Any dog has a Fluffy tail if and only if it is younger than Blaze, and any dog has a Straight tail if and only if Blaze is younger than it.

  $\forall d : (H(d, F) \leftrightarrow Y(d, b)) \wedge (H(d, S) \leftrightarrow Y(b, d))$. *(79% correct. It was fine to use either* *one or two quantifiers, and one or two free variables. I think the most common mistake was just getting the quantifier type wrong.)*

Family Name: ____________________

Question 2 (10): (Boolean Proof)

For this problem, please use the abbreviations $p = H(c, F)$, $q = H(i, S)$, and $r = H(b, N)$. Using **either** a truth table **or** a deductive sequence proof, **prove** that there is **exactly one setting** of these three variables that satisfies **Statements I, II, and III**.

Note that you must show both that your setting satisfies that statements, and that no other setting does so. If you construct a correct truth table, you will prove both. If you use a deductive sequence to that your setting is implied by the three statements, you must **also** verify that your setting in fact does satisfy the three statements.

So that you may have correct inputs to the following problem, we will tell you that the correct setting has p **true**, q **true**, and r **false**.

Here is a truth table – we would expect you to have some of the internal values along the values of the three statements on each line:

p	q	r	$I = p \rightarrow (q \oplus r)$	$II = p \vee \neg(q \rightarrow r)$	$III = \neg(q \wedge p) \rightarrow (\wedge \neg r)$
0	0	0	1	0	0
0	0	1	1	0	0
0	1	0	1	1	0
0	1	1	1	0	1
1	0	0	0	1	1
1	0	1	1	1	0
1	1	0	1	1	1
1	1	1	0	1	1

The translated statements are $p \rightarrow (q \oplus r)$, $p \vee \neg(q \rightarrow r)$, and $\neg(q \wedge p) \rightarrow (p \wedge \neg r)$.

(46% of you got full marks with a truth table. This one above would actually not have gotten full marks because I wanted to see some of the reasoning behind the columns for the three statements.)

Deductive Sequence Argument:

Assume that p is false. By II, $q \rightarrow r$ is false, so q is true and r is false. But the premise of III is true, forcing p to be false, a contradiction.

So p must be true, and I forces $q \oplus r$ to be true. II is vacuously true, so we look at III. Substituting 1 for p, III becomes $\neg q \rightarrow \neg r$, which is $r \rightarrow q$ by contrapositive. Then r cannot be true, since it would force q to be true, violating $q \oplus r$. So r must be false, and q must be true for $q \oplus r$ to be true.

With this setting, I is satisfied trivially because $q \oplus r$ is true, II is satisfied because p is true, and III is satisfied trivially because p is true and r is false.

(Only 2% of you had full marks with a deductive sequence argument, as the vast majority used a truth table. Another 4% got 9/10 because they gave correct deductive sequence arguments but didn't check that their solution satisfied the three statements.)

(The overall mean score on the problem was 7.87/10.)

Family Name: ____________________

Question 3 (20) (Predicate Proof) :

For this proof, we ask you to determine two things:

- (a, 10) What is the age order of the five dogs?
- (b, 10) What is the tail type of each dog?

For part (a), number the dogs D_1, D_2, D_3, D_4, and D_5, with D_1 being the youngest dog and D_5 the oldest.

To show your results fill in the table below with, e.g., the entry below D_1 being the name of the youngest dog and the entry below D_5 the name of the oldest one.

D_1	D_2	D_3	D_4	D_5

D_1 is Rhonda, D_2 is Clover, D_3 is Blaze, D_4 is Indie, and D_5 is Kiké.

Using quantifier rules on Statements I-V, and the **given properties** of H and Y, justify the claims that $Y(D_1, D_2)$, $Y(D_2, D_3)$, $Y(D_3, D_4)$, and $Y(D_4, D_5)$.

- Justify your claim that $Y(D_1, D_2)$:

  By Specification on Statement IV to $d = b$, and Left Separation, we get $(b = r) \vee Y(r, b)$. Since $b = r$ is false, $Y(r, b)$ must be true.

- Justify your claim that $Y(D_2, D_3)$:

  By Statements I-III, Clover has a Fluffy tail. By Specification on Statement V to Clover, Clover has a Fluffy tail if and only if he is younger than Blaze, so $Y(c, b)$ must be true.

- Justify your claim that $Y(D_3, D_4)$:

  By Statements I-III, Indie has a a Straight tail. By Specification on Statement V to Indie, she has a Straight tail if and only if Blaze is younger than her, so $Y(b, i)$ is true.

- Justify your claim that $Y(D_4, D_5)$:

  By Specification on Statement IV to $d = i$, and Right Separation, we get $(i = k) \vee Y(i, k)$. Since $i = k$ is false, $Y(i, k)$ must be true.
  We have made no use of the properties of H and Y in this argument.

(There were 64% with full marks, and a mean of 8.75/10. It was sometimes a judgement call on my part as to whether your first and fourth parts fully explained how Rhonda had to be younger than Clover*, for example, rather than just saying that "Rhonda is the youngest".)*

For part (b), find the tail type of each of the five dogs, justifying each choice by quantifier rules. Indicate where, if anywhere, you use the given properties of H and Y.

The tail types you find should be shown in the following table, with entry (d, t) being the value **1** if $H(d, t)$ is true and **0** if $H(d, t)$ is false. We start you off by filling in the three values you already know from Question 2.

$D \backslash T$	C	F	N	S
b			**0**	
c		**1**		
i				**1**
k				
r				

Clover has a Fluffy tail from Statements I-III, and since H is a function he cannot have any other tail type as well.

Indy has a Straight tail from Statements I-III, and since H is a function she cannot have any other tail type as well.

Rhonda has a Fluffy tail, because we found in part (a) that she is younger than Blaze, and by Specification of Statement V to Rhonda, she has a Fluffy tail if and only if she is younger than Blaze.

Kiké has a Straight tail, because we found in part (a) that Blaze is younger than him, and by Specification of Statement V to Kiké, he has a Straight tail if and only if Blaze is younger than him.

Blaze has a Curly tail. We know from Statements I-III that she does not lack a tail entirely. By the antireflexivity of Y, we know that $Y(b, b)$ is false. By Specification of Statement V to Blaze, we know that Blaze cannot have a Fluffy tail or a Straight tail, since either option would imply $Y(b, b)$. Since H is a function, the remaining option for Blaze's tail type must be correct.

$D \backslash T$	C	F	N	S
b	1	0	**0**	0
c	0	**1**	0	0
i	0	0	0	**1**
k	0	0	0	1
r	0	1	0	0

(Here there were 40% with full marks, and a mean of 7.29/10. I insisted that the entire table be filled out, and most of you noted that we used functionality for the negative results. If you explicitly noted antireflexevity (or just the fact that Y is a strict partial order) for $\neg Y(b, b)$, you were fine. In other cases I had to decide whether your argument for that point was convincing.)

Family Name: ____________________

Question 4 (20): (Binary Relations on a Set) Parts (a) and (b) deal with two binary relations P and Q, each from a set to itself. Part (a) is on this page, part (b) on the next.

(a, 10) Let $A = \{a, b, c, d\}$. The relation $P \subseteq A \times A$ is a **partial order**. It is known that $(a, b) \in P$, $(a, d) \in P$, $(b, c) \in P$ and $(d, c) \notin P$.

(i) In the table given below, label all pairs that must be in P with a "✓" and all pairs that cannot be in P with a "×." For pairs that are neither, leave their entry blank. We start you off by labeling the four known pairs with the appropriate "✓" or ×.

Justify your answers. That is, you must provide a brief explanation as to why each of the pairs you marked "✓" are in P and those you marked "×" are not in P. Each pair that you justify must be explicitly named as being justified.

Your explanations must reference the properties of P that are being used. They must also be consistent. That is, if you somewhere use the fact that $(x, y) \notin P$ where $(x, y) \neq (d, c)$, then you must have already previously proven that $(x, y) \notin P$.

(ii) How many partial orders P' exist that satisfy $(a, b) \in P$, $(a, d) \in P$, $(b, c) \in P$ and $(d, c) \notin P$? Briefly explain how you know this. Draw a Hasse diagram illustrating each such P' that could exist.

(a,a)	(a,b)	(a,c)	(a,d)	(b,a)	(b,b)	(b,c)	(b,d)	(c,a)	(c,b)	(c,c)	(c,d)	(d,a)	(d,b)	(d,c)	(d,d)
	✓		✓			✓								×	

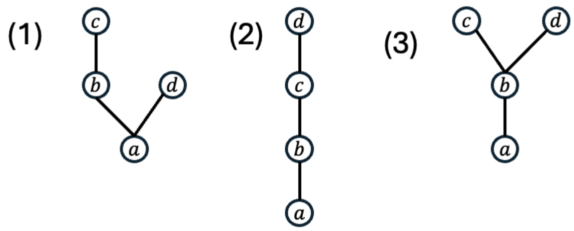
Solution: 3rd table row references justification line. A "–"'s denotes fact from problem statement.

(a,a)	(a,b)	(a,c)	(a,d)	(b,a)	(b,b)	(b,c)	(b,d)	(c,a)	(c,b)	(c,c)	(c,d)	(d,a)	(d,b)	(d,c)	(d,d)
✓	✓	✓	✓	×	✓	✓		×	×	✓		×	×	×	✓
1	–	2	–	3	1	–		3	3	1		3	4	–	1

1. By reflexivity, $(a, a), (b, b), (c, c), (d, d) \in P$.
2. By transitivity, since $(a, b) \in P$, $(b, c) \in P$, we have $(a, c) \in P$.
3. By antisymmetry with $(a, b) \in P$, $(a, d) \in P$, $(b, c) \in P$ and from (2), $(a, c) \in P$, we have $(b, a) \notin P$, $(d, a) \notin P$, $(c, b) \notin P$ and $(c, a) \notin P$.
4. If $(d, b) \in P$, then by transitivity with $(b, c) \in P$, we would get $(d, c) \in P$, contradicting known fact. So $(d, b) \notin P$.

(ii) There are three possible partial orders. They cover all of the possible ways of filling in the two empty entries (b, d) and (c, d).
Note that the case $(b, d) \notin P'$, $(c, d) \in P'$ is not possible.

(1) $(b, d), (c, d) \notin P'$.
(2) $(b, d), (c, d) \in P'$.
(3) $(b, d) \in P'$, $(c, d) \notin P'$.



Marking Notes.

Caveat: The rubrics were subtractive, i.e., points were deducted for every rubric checked. Because many errors were dependent upon each other we often did not deduct for every rubric associated with every existing error. If we had, many solutions would have received a zero rather than some partial credit.

One consequence of this is that if regrades are requested, even if a marking error is found, the grade might not increase, simply because there are many other errors remaining.

- *Not every box in the table was worth the same amount. Getting the entries (b, d) and (c, d) (to be left blank) and (d, b) ($\notin P$) correct were considered the most important part of the problem and worth quite a lot. The other entries were worth much less*
- *A common error was not deriving that $(d, b) \notin P$, and leaving its entry blank.* *This was considered a major error because it was the only derivation that required an indirect argument.*
- *Another common error was not leaving one of (b, d) and (c, d) blank.*
- *A less common error was misunderstanding antisymmetry, and claiming that $(d, c) \notin P$ implies $(c, d) \in P$.*
- *Some issues with the Hasse diagrams in (ii):*
  1. *Some solutions drew horizontal edges, e.g., a horizontal edge between a and b denoting (a, b). That was an error, since Hasse diagrams must represent (a, b) with an edge going* **up** *from a to b. Without that orientation, it's impossible to determine if the edge represents (a, b) or (b, a).*
     Some solutions drew edges in the wrong orientation.
  2. *Some solutions drew diagrams that did not remove transitivity implied edges, i.e., they drew edges for all of (a, b), (b, c) and (a, c). A correct Hasse diagram would NOT draw (a, c). Because of this, they sometimes drew two Hasse diagrams that actually represented the same partial order but counted them as two different partial orders.*
  3. *Some solutions drew Hasse diagram edges going down instead of up. We did not deduct for this error if everything else was correct.*

(32% got full marks, and the mean was 7.42/10.)

(b, 10) Let $B = \{a, b, c, d, e\}$. The relation $Q \subseteq B \times B$ is an **equivalence relation**.
It is known that $(a, b) \in Q$, $(a, c) \in Q$, $(b, e) \notin Q$ and $(e, d) \notin Q$.

(i) In the table given below, label all pairs that must be in Q with a "✓" and all pairs that cannot be in Q with a "×." For pairs that are neither, leave their entry blank. We start you off by labeling the four known pairs with the appropriate "✓" or ×.

Justify your answers following the same rules that were given in part (a).

(ii) How many Equivalence Relations Q' exist that satisfy $(a, b) \in Q$, $(a, c) \in Q$, $(b, e) \notin Q$ and $(e, d) \notin Q$? Briefly explain how you know this. Write down the possible equivalence relation(s) in partition form, that is, as a set of sets of items in B.

(a, a)	(a, b)	(a, c)	(a, d)	(a, e)		(b, a)	(b, b)	(b, c)	(b, d)	(b, e)
	✓	✓								×
(c, a)	(c, b)	(c, c)	(c, d)	(c, e)		(d, a)	(d, b)	(d, c)	(d, d)	(d, e)
(e, a)	(e, b)	(e, c)	(e, d)	(e, e)						
			×							

Solution:

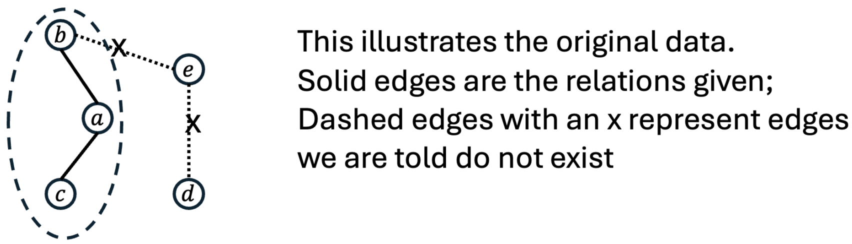
(a, a)	(a, b)	(a, c)	(a, d)	(a, e)		(b, a)	(b, b)	(b, c)	(b, d)	(b, e)
✓1	✓	✓		×7		✓2	✓1	✓4		×
(c, a)	(c, b)	(c, c)	(c, d)	(c, e)		(d, a)	(d, b)	(d, c)	(d, d)	(d, e)
✓2	✓5	✓1		×7					✓1	×3
(e, a)	(e, b)	(e, c)	(e, d)	(e, e)						
×6	×3	×6	×	✓1						

1. By reflexivity, $(a, a), (b, b), (c, c), (d, d), (e, e) \in Q$.
2. By symmetry on all pairs given to be in Q,
   $(b, a) \in Q$ and $(c, a) \in Q$.
3. By symmetry on all pairs given to not be in Q,
   $(e, b) \notin Q$ and $(d, e) \notin Q$.
4. By transitivity on $(b, a), (a, c) \in Q$, we have $(b, c) \in Q$.
5. By symmetry on $(b, c) \in Q$, $(c, b) \in Q$.
6. If $(e, a) \in Q$ or $(e, c) \in Q$, then, by transitivity with $(a, b) \in Q$, and $(c, b) \in Q$, we would get $(e, b) \in Q$, causing a contradiction. So, $(e, a) \notin Q$ and $(e, c) \notin Q$.
7. By symmetry on $(e, a) \notin Q$ and $(e, c) \notin Q$,
   $(a, e) \notin Q$ and $(c, e) \notin Q$.

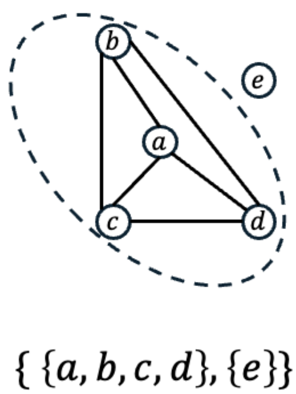
(ii) There are two possible equivalence relations. We know that e is an isolated element in an equivalence class by itself and a, b, c are in the same equivalence class. The only unknown is whether d is in the same equivalence class as $a, b.c$ or if d is also an isolated element.

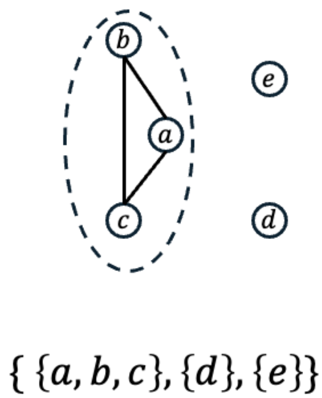
The two partitions associated with those equivalence relations are $\Big\{\{a, b, c, d\}, \{e\}\Big\}$ and $\Big\{\{a, b, c\}, \{d\}, \{e\}\Big\}$

To illustrate. The figure below describes the original data



The only available unknown is whether d gets added to the component containing a, b, c or stays alone in an isolated component. After making that decision, we need to add all remaining edges in the large component.





Marking note: Caveat: The rubrics were subtractive, i.e., points were deducted for every rubric checked. Because many errors were dependent upon each other we often did not deduct for every rubrics associated with every existing error. If we had, many solutions would have received a zero rather than some partial credit.

One consequence of this is that if regrades are requested, even if a marking error is found, the grade might not increase simply because there are many other errors remaining.

1. *Not every box in the table was worth the same amount.*
2. *A major issue was not filling in many of the $\times$'s.*
   (a) *In some cases this was because the solver didn't understand that those pairs could not occur. That was considered a major error*
   (b) *In some cases the solver noted in part (ii) that those pairs could not occur but just didn't seem to understand that they should fill in the boxes with a $\times$". That was still considered an error (since this same formulation was used in both the homework and the study guide, so this should not have been misunderstood) but had fewer points deducted.*
3. *A few students thought that transitivity also implied that: if $(x, y) \notin Q$ and $(y, z) \notin Q$ then $(x, z) \notin Q$. This is not correct and was considered a major error.*
4. *In part (ii) some solutions understood there were two partitions but either did not write down what those partition were or wrote them down in an incorrect format. That was marked as a minor error.*

(33% got full marks, and the mean was 6.83/10.)

Question 5 (20+5): (Number Theory)

- (a, 4) For each of (i) and (ii) below say whether m has a multiplicative inverse modulo n. In each one, if the inverse exists, write down what it is. You do not need to show your work. The number you write down should be between 0 and $n-1$. If the inverse does not exist, prove that it does not exist.

  (i) $m = 5$, $n = 34$.
  Solution: $x = 7$
  [Justification. Not needed: $5 \cdot 7 = 35$ and $35 \equiv 1 \pmod{34}$]

  (ii) $m = 333$, $n = 336$
  Solution: No inverse exists.
  3 divides both 333 and 336 so $gcd(333, 336) \neq 1$. Thus, by the inverse theorem taught in class, 333 does *not* have a multiplicative inverse modulo 336.

  Marking note: The problem required a **proof** *that the inverse does not exist. The proof needed to contain two steps.*
  Step (a) to show that $gcd(336, 333) > 1$.
  Step (b) to note that we have a theorem that states that "m has an inverse modulo m if and only if $gcd(m, n) \neq 1$*".*

  What was being marked was not only whether you knew the answer, but whether you could write a correct proof.
  For full credit for (a) it was necessary to show why $gcd(333, 336) > 1$, *e.g., running the EA or, more simply, just noting that both numbers are divisible by 3. But, just stating that* $gcd(333, 336) \neq 1$ *without any justification wasn't enough.*

  For (b) it was not enough to say that "the inverse does not exist because $gcd(333, 336) \neq 1$*". For a correct answer, it was necessary to explain WHY that implies the nonexistence of the inverse. That is, to explicitly state that you are using a known theorem/lemma/fact (the inverse theorem) and state what that theorem says. We did not deduct points for this omission, though.*

  (81% got full marks, but only 5% had full justifications, see above. The mean score was 3.49/4.)

- (b, 8) The naturals 67 and 30 are relatively prime.
  Use the Extended GCD algorithm as taught in class to find integers a and b satisfying the equation $a \cdot 67 + b \cdot 30 = 1$. Show all of your work.

  After solving the problem, write your final solution here
  $a = \underline{\mathbf{13}}$. $b = \underline{\mathbf{-29}}$.

  Solution:

$$\begin{array}{rcl} 67 &=& 2 \cdot 30 + 7 \\ 30 &=& 4 \cdot 7 + 2 \\ 7 &=& 3 \cdot 2 + 1 \end{array} \qquad \begin{array}{rcl} 7 &=& 67 - 2 \cdot 30 \\ 2 &=& 30 - 4 \cdot 7 = 30 - 4(67 - 2 \cdot 30) = -4 \cdot 67 + 9 \cdot 30 \\ 1 &=& 7 - 3 \cdot 2 = (67 - 2 \cdot 30) - 3(4 \cdot 67 + 9 \cdot 30) = 13 \cdot 67 - 29 \cdot 30. \end{array}$$

  So $a = 13$ and $b = -29$.

  Marking Note: "Showing your work" here meant
  (i) showing the running of the Euclidean algorithm AND
  (ii) showing the work of the version of the extended Euclidean algorithm taught in class. and illustrated in every example provided.
  In particular, a correct solution REQUIRED showing the two intermediate solutions:
  $7 = 67 - 2 \cdot 30$
  and
  $2 = -4 \cdot 67 + 9 \cdot 30$.
  Note that the problem instructions explicitly required **both showing your work and using the method taught in class.** *That method was chosen because it explicitly shows that every intermediate remainder in the EA can be written as a linear combination of the original two items, which is what helped prove the correctness of the EEA. We therefore wanted to see those intermediate results and explicitly requested them.*

  - *Some solutions were correct and showed their work but did NOT use the method taught in class, instead using a variation. They were given a minor deduction for ignoring explicit instructions.*
  - *Solutions that used the method taught in class and made one small arithmetic error in an early stage, resulting in an incorrect solution, usually received full credit. That's because we were easily able to identify that the error was a trivial one and that they otherwise perfectly understood the concept.*
  - *Solutions that were incorrect and did NOT use the technique taught in class had many more points deducted. This was because their method hid where the error occurred and we could not quickly distinguish between trivial and substantial errors.*

  Solutions that **correctly** *showed the working of the EEA without showing the EA received full credit.*
  Solutions whose EEA calculations contained errors and did NOT show their EA calculations also had points deducted for not showing their work, since that work would be needed to verify where the errors in the EEA calculation came from, i.e., whether they were just simple calculation errors or conceptual errors.
  (54% got full marks, and the mean score was 6.66/8.)

- (c, 4) Using the results from the previous part, determine both an inverse of 30 modulo 67 and an inverse of 67 modulo 30.
  For full credit, your answers should each be the smallest natural numbers that are inverses.
  After solving the problem, write your final solutions here:
  13 is an inverse of 67 modulo 30.
  38 is an inverse of 30 modulo 67.

  Solution: 13 is an inverse of 67 modulo 30.
  $-29 + 67 = 38$ is an inverse of 30 modulo 67.

  Marking note:

  1. *This was marked based on the solution to (b). So, if (b) was wrong but the answer to (c) would be correct if the written answer for (b) was correct, than no points were deducted.*
  2. *A negative number would not be accepted as a fully correct answer.*
  3. *A common error would be to write that the inverse of* 30 *is* $30 - 29$ *and not* $67 - 29$. *This was treated as a conceptual error and not a typographical one.*
     More explicitly, for any $am + bn = 1$, *you were expected to understand from first principles that*
     a is a multiplicative inverse of m modulo n and
     b is a multiplicative inverse of n modulo m
     so flipping a and b to be the inverses of n and m respectively was considered a conceptual error.

  (70% got full marks and the mean was 3.34/4.)

- (d, 4) You are now given that $2 \cdot 101 - 3 \cdot 67 = 1$.
  Using the technique taught in class, determine the smallest natural x that solves both the congruences

  $$x \equiv 3 \pmod{67} \quad \text{and} \quad x \equiv 2 \pmod{101}.$$

  Show all of your your work.
  After solving the problem, write your final solution below:

  The smallest natural satisfying both congruences is $x =$ **204**.
  Solution: Set

  $$c = 3 \cdot 2 \cdot 101 - 2 \cdot 3 \cdot 67 = 606 - 402 = 204.$$

  Marking note: Similar as in the answer of part (c), you were expected to understand that if $am + bn = 1$, *then* $c = amu + bnv$ *is a solution to*

  $$x \equiv v \pmod{m} \quad \textit{and} \quad x \equiv u \pmod{n}.$$

  Flipping locations for the variables, e.g., writing $c = amv + bnu$, *was marked as a conceptual error.*
  (*66% got full marks, and the mean was 3.05/4.*)

Family Name: ________________

- (e, 5 extra credit)

  There are a number of classic puzzles involving pirates on an island (usually also with a monkey) that need to divide a hoard of coconuts. In this case, three pirates A, B, and C, have n coconuts and have agreed to divide them equally in the morning. During the night, each pirate secretly takes away what they think to be their share. Specifically,

  - A first visits the hoard of n coconuts. She divides them into three equal piles of size a, except there is one left over which she gives to the monkey. She hides a coconuts, leaves $2a$ remaining, and gives one to the monkey, so $n = 3a + 1$.
  - B now visits, and divides the remaining $2a$ coconuts into three equal piles of size b, giving one left over to the monkey. He hides b coconuts, and leaves $2b$, so that $2a = 3b + 1$.
  - C finds the remaining $2b$ coconuts, divides them into three piles of size c, giving one to the monkey, and leaves $2c$, so that $2b = 3c + 1$.
  - In the morning, the remaining $2c$ coconuts are divided equally into three piles, *without* one for the monkey.

  In fact, there are an infinite number of possible sizes n that fit this scenario. Your job is to **find one** (write it below) and then **prove** that your solution for n is the smallest one possible. (**Hint:** Modular arithmetic definitely comes into play, but there is no obvious way to use the Chinese Remainder Theorem.)

Solution:

The smallest natural satisfying the conditions is $n = \underline{\mathbf{25}}$.
Full credit required not just getting the value of n, but *proving* that 25 is the smallest possible value.

The problem is to find the smallest natural n satisfying that a, b, c are naturals where
(I) $n = 3a + 1$.
(II) $2a = 3b + 1$.
(III) $2b = 3c + 1$.
(IV) $2c$ is divisible by 3.

It's not difficult to show that $n = 25$ is a feasible solution value with naturals $c = 3$, $b = 5$ and $a = 8$. Just plug those values into (I)-(IV).
The "hard" part is showing that 25 is the *smallest* feasible value.

There are two very different approaches to showing this. The first is to show that none of $n = 0, \ldots 24$ are feasible solutions. The second is to show that n is an increasing (linear) function of c and that $c = 0, 1, 2,$ cannot lead to feasible solutions (while $c = 3$ leads to feasible solution $n = 25$).

(I) First approach: To show that $0, 1, \ldots, 24$ are not feasible solutions.
From (I), $n \pmod 3 = 1$, so we only need to check $n = 1, 4, 7, 10, 13, 16, 19, 22$.
$n = 1 :$ (I) forces $a = 0$. From (II), $b = -1/3$, contradicting b being a natural.
$n = 4 :$ (I) forces $a = 1$. From (II), $b = 1/3$, contradicting b being a natural.
$n = 7 :$ (I) forces $a = 2$. From (II), $b = 1$. From (III), $c = 1/3$ contradicting c being a natural.
$n = 10 :$ (I) forces $a = 3$. From (II), $b = 5/3$. contradicting b being a natural.

$n = 13$: (I) forces $a = 4$. From (II), $b = 7/3$, contradicting b being a natural.
$n = 16$: (I) forces $a = 5$. From (II), $b = 3$. From (III), $c = 5/3$ contradicting c being a natural.
$n = 19$: (I) forces $a = 6$. From (II), $b = 11/3$, contradicting b being a natural.
$n = 22$: (I) forces $a = 7$. From (II), $b = 13/3$, contradicting b being a natural.

(I) Second approach: To show that n is an increasing (linear) function on c and show that $c = 0, 1, 2$, cannot lead to feasible solutions (while $c = 3$ does).
Expanding the equations gives

$$\begin{aligned} n &= 3a + 1 \\ &= 3\left(\frac{3b+1}{2}\right) + 1 = \frac{9}{2}b + \frac{5}{2} \\ &= \frac{9}{2}\left(\frac{3c+1}{2}\right) + \frac{5}{2} = \frac{27}{4}c + \frac{19}{4} \end{aligned}$$

- $c = 0$ gives $n = 19/4$, contradicting that n is a natural.
- From (IV), $2c$ is divisible by 3, so c must be divisible by 3, so $c \neq 1, 2$.
- As shown at the start, $c = 3$ gives a feasible solution, with $n = 25$ so 25 is the smallest feasible value of n.

Marking Note: Some students showed that $c = 3$ was the first c that could lead to a feasible solution and calculated the resulting value $n = 25$.
Showing that $c = 3$ was the smallest value of c was not enough to get a fully complete solution. That would also require showing that a larger value of c could not lead to a smaller value of n, i.e., that n is a non-decreasing (or increasing) function in c. A small penalty number was deducted for omitting this fact.

(Only 3% got full marks, and another 9% got 4.75/5 by not showing that n was a monotone function of c. The overall mean was 0/91/5, as 66% got no credit at all.)

Family Name: ____________________

Question 6 (20): The following are ten true/false questions, with no explanation needed or wanted, no partial credit for wrong answers, and no penalty for guessing.

After reading the questions, write the correct answer, either T (for true) or F (for false), in the corresponding column.

Only one student got a perfect score – the average was 12.35/20.

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)
T	F	T	F	T	T	T	F	F	F

- (a) Given the three premises $(p \wedge \neg x) \rightarrow c$, $(p \wedge \neg(x \rightarrow y)) \rightarrow c$, and $(p \wedge x \wedge y) \rightarrow c$, we can conclude that $p \rightarrow c$ is true.

  TRUE: All cases are covered. *(71% correct.)*

- (b) Let u and v be two non-empty strings over the alphabet $\{a, b\}$. If u is both a prefix of v and a suffix of v, then u and v must be the same string, that is, $u = v$.

  FALSE: $u = a$ and $v = aa$ are a counterexample. *(75% correct.)*

- (c) Let A, B, C, and D each be finite non-empty sets. Then the statement $A \times B \subseteq C \times D$ is logically equivalent to the statement $(A \subseteq C) \wedge (B \subseteq D)$.

  TRUE. Any pair $\langle a, b\rangle$ in $A \times B$ must be in $C \times D$ if $A \subseteq C$ and $B \subseteq D$. And if there existed an element in $x \in A \setminus C$ or $y \in B \setminus D$, we could make a pair in $A \times B$ with the bad element of one set and a good element of the other set, and this pair would not be in $C \times D$. *(55% correct.)*

- (d) Let $X = \{0, 1\}$ and $Y = \{a, b\}$. Then $\langle b, 0\rangle \in X \times Y$.

  FALSE. The order in an ordered pair matters. In such a pair, the first element must be from X and the second element must be from Y. *(79% correct.)*

- (e) Let P be a unary predicate on the set A, and assume the premise $\forall x : P(x)$. It may be possible that the statement $\exists y : P(y)$ is false.

  TRUE. If A were an empty set, the premise would be true and the conclusion false. *(53% correct.)*

- (f) Let R be a binary predicate on $\mathbb{N}$, defined as $\{\langle a, b\rangle : a^2 = b\}$. Then R is a function from $\mathbb{N}$ to $\mathbb{N}$, and is an injection (1-1 function), but it is not a surjection (onto function).

  TRUE. It is a function because for every a, there is exactly one natural b such that $\langle a, b\rangle \in R$. It is an injection because the b values for different a's are different. But if $b = 2$, for example, there is no a such that $a^2 = b$ within $\mathbb{N}$. *(56% correct.)*

- (g) Let a, b, and c be distinct odd naturals, each greater than 1. Then the number $n = abc + 4$ is not divisible by a, not divisible by b, and not divisible by c.

  TRUE. Modulo any of a, b, and c, we have $n \equiv 4$, and since 4 does not divide any odd prime number, n cannot divide any of those odd primes. *(69% correct.)*

- (h) A relation $R \subseteq A \times B$ is an injection (a one-to-one function) if and only if for every $x \in A$, there is exactly one element $y \in B$ such that $\langle x, y \rangle \in R$.

  FALSE. That is the definition for *any* function. An injection is when you never have two different $x_1 \in A$ and $x_2 \in A$, and a $y \in B$, such that both $\langle x_1, y \rangle$ and $\langle x_2, y \rangle$ are both in R. *(50% correct. You've seen this problem before, and unless people start answering it correctly, you'll likely see it again.)*

- (i) For all naturals x, y, and z, $x\%(y\%z) = (x\%y)\%z$, where "%" is the modular division operation, as in Java or Python.

  FALSE, for example $4\%(3\%2) = 4\%1 = 0$ but $(4\%3)\%2 = 1\%2 = 1$. *(69% correct.)*

- (j) Let $p_1, p_2, \ldots, p_k$ and $q_1, \ldots, q_m$ each be prime numbers, not necessarily distinct. If the two products $p_1 p_2 \ldots p_k$ and $q_1 \ldots q_m$ are equal, then we know both that $k = m$ and that for each i with $1 \leq i \leq k$, $p_i = q_1$.

  FALSE. We know that $k = m$, and that each prime occurs the same number of times in the list, but they could occur in a different order in the two lists. *(39% correct. This, I think, was the only really nasty question on the true/false, using my common strategy of stating a standard result that you should have studied, and taking out one clause that might or might not make it false.)*

COMPSCI 250 First Midterm Exam Supplementary Handout: 9 October 2025

Definitions for Questions 1-3:

In this scenario, we have a set $D = \{b, c, i, k, r\}$ of exactly five dogs (Blaze, Clover, Indie, Kiké, and Rhonda), and a set $T = \{\text{Curly}, \text{Fluffy}, \text{None}, \text{Straight}\}$ of exactly four tail types.

The relation H from D to T, which is also a **function**, is defined by the predicate $H(d, t)$ meaning "dog d has tail type t". The binary relation Y on D is defined by the predicate $Y(d, e)$ meaning "dog d is younger than dog e". You are given that Y is a **strict partial order**, meaning that it is **antireflexive**, **antisymmetric**, and **transitive**.

Here are the five statements for Question 1:

- (a, to symbols, 2 points) **Statement I:** If Clover has a Fluffy tail, then either Indie has a Straight tail or Blaze has no tail, but not both.
- (b, to English, 2 points) **Statement II:** $H(c, F) \vee \neg(H(i, S) \rightarrow H(b, N))$
- (c, to symbols, 2 points) **Statement III:** If it is not the case that both Indie has a Straight tail and Clover has a Fluffy tail, then Clover has a Fluffy tail and it is not the case that Blaze has no tail.
- (d, to English, 2 points) **Statement IV:** $\forall d : ((d = r) \vee Y(r, d)) \wedge ((d = k) \vee Y(d, k))$
- (e, to symbols, 2 points) **Statement V:** Any dog has a Fluffy tail if and only if it is younger than Blaze, and any dog has a Straight tail if and only if Blaze is younger than it.