NAME: _____

SPIRE ID: _____

COMPSCI 250
Introduction to Computation
SOLUTIONS to First Midterm Spring 2025

D. A. M. Barrington and M. Golin 11 March 2025

DIRECTIONS:

- Answer the problems on the exam pages.
- There are problems on pages 2-10, some with multiple parts, for 100 total points plus 5 extra credit. Final scale will be determined after the exam.
- Page 11 contains useful definitions and is given to you separately – do not put answers on it!
- But, if you do write on the back, 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: While each of the dogs in Dave's neighborhood is perfect in their own way, some of them are given to certain undesirable activities.

Let D be the set of dogs $\{b, c, i, k, r\}$, containing the five dogs Blaze, Clover, Indie, Kiké, and Rhonda.

Let U be a set of behaviors, containing exactly $\{CR, GP, PB, WHO\}$, referring to "chewing rugs", "growling at pedestrians", "peremptory[1] barking", and 'waking humans overnight".

Let E be a binary predicate from D to U, so that $E(d, u)$ means "dog d exhibits behavior u". Your eventual goal is to determine all the 20 truth values of this relation, based on the following five statements in Question 1.

Question 1 (10): (Translations)

- (a, to symbols) **Statement I:** If Kiké chews rugs, then Clover peremptorily barks but Blaze does not wake humans overnight.

  Solution: $E(k, CR) \rightarrow (E(c, PB) \wedge \neg E(b, WHO))$ **Grading Notes:** *This was pretty basic, and 92% of you got it right. I was forgiving about dangling parens. Writing no parens was correct, but a few people put some incorrect ones in, some confused $\wedge$ and $\vee$, and some overlooked the negation.*

- (b, to English) **Statement II:** $(E(c, PB) \leftrightarrow E(b, WHO)) \wedge \neg(E(k, CR) \oplus E(c, PB))$

  Solution: Clover peremptorily barks if and only if Blaze wakes humans overnight, and it is not the case that Kiké chews rugs or Clover peremptorily barks, but not both.
  Equivalent form: The three propositions here are either all true or all false.

  Grading Notes: *Only 60% of you got it right, as many of you either neglected the exclusive or, or incorrectly computed its negation. Those who noted that the negation of $\oplus$ is $\leftrightarrow$ probably simplified their life later.*

- (c, to symbols) **Statement III:** Blaze growls at pedestrians, and no other dog does so.

  Solution: $\forall d : E(d, GP) \leftrightarrow (d = b)$**.**
  Equivalent form: $E(b, GP) \wedge \forall d : (d \neq b) \rightarrow \neg E(d, GP)$**. There were several correct versions of this.**
  Another correct form with no quantifiers: $E(b, GP) \wedge \neg E(c, GP) \wedge \neg E(i, GP) \wedge \neg E(k, GP) \wedge \neg E(r, GP)$**.**

  Grading Notes: *Only 51% of you got this right. You needed to first realize that you are talking about all dogs, and so need a $\forall$, and once you did that you needed to say one thing about Blaze and something else about the other dogs, requiring $\rightarrow$ or $\leftrightarrow$. Many people just connected the statements with $\wedge$, leading to unintended statements that all dogs were Blaze, or that none of them were, or that they all didn't growl. If you got this*

[1] **peremptory**: in a manner insisting on immediate obedience or attention

wrong, and even if you didn't, look again at how you restrict a statement in a $\forall$, using the general form $\forall x : P(x) \to Q(x)$.

- (d, to English) **Statement IV:** $(\exists u : E(i, u)) \to (\forall v : E(b, v) \leftrightarrow E(r, v))$

  Solution: If Indy has any of the behaviors, then Blaze and Rhonda exhibit exactly the same set of behaviors.

  Grading Notes: *This was better, with 64% correct, but only because I was generous with the phrasing of the statement $\forall v : E(b, v) \leftrightarrow E(r, v)$. The most common phrasing I got was "Blaze exhibits all behaviors if and only if Rhonda exhibits all behaviors". This was totally wrong because it says $(\forall v : E(b, v)) \leftrightarrow (\forall v : E(r, v))$. What you meant, and what I interpreted it as, was "Blaze exhibits* each *behavior if and only if Rhonda exhibits* that *behavior." On the final, you will need to express yourself more clearly in such situations!*

  The mistake I did *punish was to say "There exists a behavior which if Indy exhibits, this happens." This is wrong because it means $\exists u : E(i, u) \to \ldots$, which ignores the parens around $\exists u : E(i, u)$ in the original. My note on Gradescope was "scope of $\to$". The problem with the incorrect version is that it is vacuously true if there is any behavior that Indy does not exhibit. If you took this version into Q2 and Q3, it will cost you.*

- (e, to symbols) **Statement V:** Each of the behaviors, except for growling at pedestrians, is exhibited by exactly three of the dogs. (**Note:** This statement does not say whether these three dogs are the same dogs or different ones.)

  Solution: $\forall u : (u \neq GP) \to \exists x : \exists y : \exists z : (x \neq y) \wedge (x \neq z) \wedge (y \neq z) \wedge (\forall d : E(d, u) \leftrightarrow ((d = x) \vee (d = y) \vee (d = z)))$

  Equivalent form, using the fact that this says that exactly two dogs do not have that behavior: $\forall u : (u \neq GP) \to \exists x : \exists y : (x \neq y) \wedge (\forall d : \neg E(d, u) \leftrightarrow ((d = x) \vee (d = y)))$

  Grading Notes: *Only 8% of you got this right, though probably at least half of you made reasonable attempts. (This was one in which a three-point scale might have been fairer.) The problem was that there are a number of things you have to all get right:*

  - *You need a $\forall$ quantifier for the behaviors, and it has to be at the beginning, because there could be different dogs satisfying the statement for each dog.*
  - *You have to exclude GP from the statement, most likely with a $\to$, but possibly with an $\vee$. If you just use $\wedge$, you will probably be claiming that none of the behaviors was GP, which was not true.*
  - *You need to use three $\exists$ quantifiers for the three dogs that exhibit the behavior. Most of you got this.*
  - *But those three dogs have to be* distinct*. The best way to say this is $(x \neq y) \wedge (x \neq z) \wedge (y \neq z)$. The phrasing $x \neq y \neq z$* might *do the right thing in Python, but doesn't work in general because it doesn't rule out $x = z$.*
  - *Finally, you need to make sure that there are* no more than three *dogs with that behavior. This means either a new $\forall$ quantifier, with an $\to$, to say that the other dogs don't exhibit, or use* five *$\exists$ quantifiers, make them all distinct (with ten $\neq$ statements), and say that three of them exhibit the behavior and the other two do not.*

The mean on the question was 7.67/10, but only 6% of you got 10/10.

Family Name: _____

Question 2 (10): (Boolean Proof)

Using Statements I and II *only*, determine the truth values of the three propositions $p = E(k, CR)$, $q = E(c, PB)$, and $r = E(b, WHO)$, using either a truth table or a deductive sequence proof. Note that (particularly with the deductive sequence approach) you are responsible for both showing that your solution agrees with the statements, and that no other solution does so.

Truth Table Solution, showing that the only solution is $p = q = r = 0$:

$(p$	$\rightarrow$	$(q$	$\wedge$	$\neg$	$r))$	$\wedge$	$((q$	$\leftrightarrow$	$r)$	$\wedge$	$\neg$	$(p$	$\oplus$	$q))$
0	1	0	0	1	0	**1**	0	1	0	1	1	0	0	0
0	1	0	0	0	1	**0**	0	0	1	0	1	0	0	0
0	1	1	1	1	0	**0**	1	0	0	0	0	0	1	1
0	1	1	0	0	1	**0**	1	1	1	0	0	0	1	1
1	0	0	0	1	0	**0**	0	1	0	0	0	1	1	0
1	0	0	0	0	1	**0**	0	0	1	0	0	1	1	0
1	1	1	1	1	0	**0**	1	0	0	0	1	1	0	1
1	0	1	0	0	1	**0**	1	1	1	1	1	1	0	1

Deductive Sequence Proof:

1. **Statement II, left separation:** $q \leftrightarrow r$
2. **Statement II, right separation:** $\neg(p \oplus q)$
3. **Definitions of Equivalence and Exclusive OR:** $p \leftrightarrow q$
4. **Transitivity of Equivalence, lines 1 and 3:** $p \leftrightarrow r$
5. **Assume p for a contradiction.**
6. **By Modus Ponens on Statement I, $q \wedge \neg r$.**
7. **This contradicts line 1, so by contradiction, we know $\neg p$.**
8. **By line 3, we have $\neg q$.**
9. **By lines 4 and 7, we have $\neg r$.**
10. **Check: Statement I is true vacuously since p is false.**
11. **Check: Statement II is true because q and r are both false, and it is not true that p and q have different values.**

Grading Notes: *So there were 41% of you with correct truth tables, 14% with fully correct deductive sequences, and another 14% with correct deductive sequences but no check. (Remember that a truth table verifies both that your solution is a valid one and that there is no other. A deductive sequence by itself proves only that there is no other solution, so you have to add a check that your solution is one. Many people included checks with their truth tables, which was redundant but ok.) So 69% of you got 9/10 or better, and the mean was* 8.54/10. *In fact 90% of you got 6/10 or better and 98% got 4/10 or better. As you should know, there will be a similar problem on the final exam, so if you did badly here you know what to do.*

A surprising number of people put their truth table rows in a non-standard order, which incurs no penalty but makes the grading more annoying.

If you had incorrect versions of Statements I and II due to mistakes on Q1 or during this problem, I usually gave full credit for a correct solution to the new problem. But since we gave you the correct solution, if you get a different one, you should note that in your solution, and go back to try and fix it if you have time.

Family Name: _____

Question 3 (20) (Predicate Proof) :

Using Statements I-V, fill in the table below to show all 20 truth values of the propositions in the relation E. Justify your conclusion, making clear where you are using quantifier rules. (One way to do this is to number the lines of your argument, and indicate in your table which entry is determined by which line.)

Hint: It follows from Statements I and II that *all three* of the propositions p, q, and r are *false*. (We've thus filled in those three entries of the table for you already.) You still need to prove this fact on Question 2, but *here* you may assume that without further proof.

Solution:

$E(b, CR) = 1$ (line 6)	$E(b, GP) = 1$ (line 1)	$E(b, PB) = 1$ (line 7)	$E(b, WHO) =$ **0**
$E(c, CR) = 1$ (line 6)	$E(c, GP) = 0$ (line 8)	$E(c, PB) =$ **0**	$E(c, WHO) = 1$ (line 7)
$E(i, CR) = 0$ (line 5)	$E(i, GP) = 0$ (line 5)	$E(i, PB) = 0$ (line 5)	$E(i, WHO) = 0$ (line 5)
$E(k, CR) =$ **0**	$E(k, GP) = 0$ (line 8)	$E(k, PB) = 1$ (line 7)	$E(k, WHO) = 1$ (line 7)
$E(r, CR) = 1$ (line 6)	$E(r, GP) = 0$ (line 2)	$E(r, PB) = 1$ (line 7)	$E(r, WHO) = 1$ (line 7)

1. **By Specification of IV to b, $E(b, GP) \leftrightarrow (b = b)$, which simplifies to $E(b, GP)$.**
2. **By Specification of IV to r, $E(r, GP) \leftrightarrow (r = b)$, which simplifies to $\neg E(r, GP)$.**
3. **By Definition of Equivalence, $\neg(E(b, GP) \leftrightarrow E(r, GP))$.**
4. **By Existence, $\exists v : \neg(E(b, v) \leftrightarrow E(r, v))$.**
5. **Line 4 is the negation of the conclusion of the implication in Statement III. By Modus Tollens, then, its premise is false, that is, $\neg\exists u : E(i, u)$, or equivalently (by Quantifier DeMorgan), $\forall u : \neg E(i, u)$. (Indy has none of the behaviors in question.)**
6. **By Specification of V to CR, using the variant form of V in the solution to Question 1, there are exactly two dogs x and y such that $\neg E(x, CR)$ and $\neg E(y, CR)$. We know that i is one of these dogs by Specification of line 5 to CR. We are given $\neg E(k, CR)$ from Statements I and II, making k the other dog here. We can conclude, then, that $E(b, CR)$, $E(c, CR)$, and $E(r, CR)$.**
7. **By exactly the same arguments for PB and WHO, there are exactly two dogs who do not exhibit that property. One is i, and the other is given by Statements I and II, so the other three do exhibit those properties.**
8. **Finally, we can find all the values for $E(x, GP)$, because IV tells us that $E(b, GP)$ is true and the other four values $E(x, GP)$ with $x \neq b$ are false.**

Grading Notes: *Essentially, success or failure depended on whether you had a correct notion of Statement IV and used it to determine that Indie had no bad behaviors. From that point, most of the rest follows quickly from Statement V. Fortunately, while hardly anyone was able to correctly translate V, most of you were able to work with the English version.*

I gave 0/20 for no answer at all, 4/20 that I couldn't connect to any of the statements, and 7/20 for implementing Statement III and nothing else. The largest category (about 40%) got 9/20 because they got Statement III and then did something fatally wrong with Statement IV, or apparently never used it at all.

There were 39% with 20/20 answers, which required (in either English or symbols) explaining why Indie had no bad behaviors because Statement III, specialized to GP, contradicts the conclusion of Statement IV. I usually gave 15/20 for the right table but insufficient justification.

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 $(b, c) \in P$, $(c, a) \in P$, $(d, a) \in P$ 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.

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

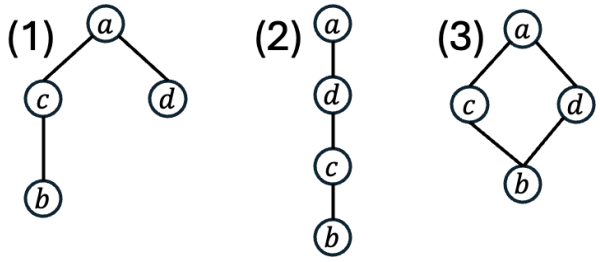
(a,a)	(a,b)	(a,c)	(a,d)	(b,a)	(b,b)	(b,c)	(b,d)	(c,a)	(c,b)	(c,c)	(c,d)	(d,a)	(d,b)	(d,c)	(d,d)
						✓		✓				✓		×	

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	3	3	3	2	1	−		−	3	1		−	4	−	1

1. By reflexivity, $(a, a), (b, b), (c, c), (d, d) \in P$.
2. By transitivity, since $(b, c) \in P$, $(c, a) \in P$, we have $(b, a) \in P$.
3. By antisymmetry with $(b, c) \in P$, $(c, a) \in P$, $(d, a) \in P$ and from (2), $(b, a) \in P$, we have $(c, b) \notin P$, $(a, c) \notin P$, $(a, d) \notin P$ and $(a, b) \notin P$.
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
(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 check 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.*
- *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, its impossible to determine if it 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.*

Family Name: _____

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

1. By reflexivity, $(a, a), (b, b), (c, c), (d, d), (e, e) \in Q$.
2. By transitivity on $(a, b), (b, c) \in Q$, $(a, c) \in Q$.
   By transitivity on $(a, b), (a, c) \in Q$ and $(d, a) \in Q$, $(d, b), (d, c) \in Q$.
3. By symmetry on all pairs known to be in Q,
   $(b, a), (c, a), (c, b), (a, d), (b, d), (c, d), (d, e) \in Q$.
4. If $(e, a) \in Q$, $(e, b) \in Q$, or $(e, c) \in Q$ then, by transitivity with $(a, d) \in Q$, $(b, d) \in Q$ and $(c, d) \in Q$, we would get $(e, d) \in Q$, causing a contradiction. So, $(e, a) \notin Q$, $(e, b) \notin Q$, and $(e, c) \notin Q$
5. By symmetry, $(a, e) \notin Q$, $(b, e) \notin Q$, and $(c, e) \notin Q$.

(ii) There is only one equivalence relation. This is because all of the 25 possible pairs are forced to either exist or not exist in Q.

The partition is $\Big\{\{a, b, c, d\}, \{e\}\Big\}$.

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 check the 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.

- *Not every box in the table was worth the same amount.*
- *A major issue was not filling in many of the $\times$'s.*
  1. *In some cases this was because the solver didn't understand that those pairs could not occur. That was considered a major error*
  2. *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.*
- *In part (ii) some solutions understood there was only one partition but either did not write down what the partition was or wrote it in an incorrect format. That was marked as a minor error.*

Family Name: _____

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) $m = 3$, $n = 14$.
  Solution: $x = 5$
  [Justification. Not needed: $3 \cdot 5 = 15$ and $15 \equiv 1 \pmod{14}$]

  (ii) $m = 422$, $n = 446$
  Solution: No inverse exists.
  2 divides both 422 and 426 so $gcd(422, 446) \neq 1$. Thus, by the inverse theorem taught in class, 422 does *not* have a multiplicative inverse modulo 446.

- (b, 8) The naturals 87 and 38 are relatively prime.
  Use the Extended GCD algorithm as taught in class to find integers a and b satisfying the equation $a \cdot 87 + b \cdot 38 = 1$. Show all of your work.
  After solving the problem, write your final solution here
  $a =$ **7**. $b =$ **−16**.

  Solution:

$$\begin{array}{lcllcl} 87 & = & 2 \cdot 38 + 11 & 11 & = & 87 - 2 \cdot 38 \\ 38 & = & 3 \cdot 11 + 5 & 5 & = & 38 - 3 \cdot 11 = 38 - 3(87 - 2 \cdot 38) = -3 \cdot 87 + 7 \cdot 38 \\ 11 & = & 2 \cdot 5 + 1 & 1 & = & 11 - 2 \cdot 5 = (87 - 2 \cdot 38) - 2(-3 \cdot 87 + 7 \cdot 38) = 7 \cdot 87 - 16 \cdot 38. \end{array}$$

  So $a = 7$ and $b = -16$.

  Marking Note: "Showing your work" here meant (i) showing the running of the Euclidean algorithm AND (ii) showing the work of the extended Euclidean algorithm.
  The factors $2, 3, 2$ *from the lines of the Euclidean algorithm were needed to construct the coefficients of* 38 *and* 87 *in the running of the extended Euclidean algorithm.*
  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.

- (c, 4) Using the results from the previous part, determine both an inverse of 38 modulo 87 and an inverse of 87 modulo 38.
  For full credit, your answers should each be the smallest natural numbers that are inverses.

  After solving the problem, write your final solutions here:

  7 is an inverse of 87 modulo 38.
  71 is an inverse of 38 modulo 87.

  Solution: 7 is an inverse of 87 modulo 38.
  $-16 + 87 = 71$ is an inverse of 38 modulo 87.

  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* 38 *is* $38 - 16$ *and not* $87 - 16$. *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

- (d, 4) You are now given that $9 \cdot 45 - 4 \cdot 101 = 1$.
  Using the technique taught in class, determine the smallest natural x that solves both the congruences

  $$x \equiv 3 \pmod{45} \quad \text{and} \quad x \equiv 4 \pmod{101}.$$

  Show all of your your work.
  After solving the problem, write your final solution below:
  The smallest natural satisfying both congruences is $x =$ **408**.

  Solution: Set

  $$c = 4 \cdot 9 \cdot 45 - 3 \cdot 4 \cdot 101 = 1620 - 1212 = 408.$$

  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.*

- (e, 5 extra credit) You are now given that $7 \cdot 23 - 8 \cdot 20 = 1$.
  Find the smallest natural x that satisfies

$$x \equiv 2 \pmod{20} \quad \text{and} \quad x \equiv 1 \pmod{23} \quad \text{and} \quad x \equiv 0 \pmod{14}.$$

  It is not necessary to show your work but, if you do not, and get the answer wrong, we cannot give partial credit for a correct technique.
  After solving the problem, write your final solution below:
  The smallest natural satisfying all three congruences is $x = \underline{\mathbf{2002}}$.

  Solution: Note that the Chinese remainder theorem can NOT be used here because $gcd(20, 14) = 2 \neq 1$.

  The smallest natural satisfying

$$x \equiv 2 \pmod{20} \quad \text{and} \quad x \equiv 1 \pmod{23}.$$

  is

$$x = 2 \cdot 7 \cdot 23 - 8 \cdot 20 = 322 - 160 = 162.$$

  We know that it is the smallest because it is less than $20 \cdot 23 = 460$.
  Every natural y satisfying

$$y \equiv 2 \pmod{20} \quad \text{and} \quad y \equiv 1 \pmod{23}.$$

  must be of the form

$$y = 162 + k \cdot 20 \cdot 23 = 162 + k \cdot 460$$

  where k is a natural.
  We can find the smallest by just plugging in values $k = 0, 1, 2, 3 \ldots$ until we get a number that satisfies all the congruences. This will be $162 + 4 \cdot 460 = 2002$.

  An alternative way of finding $k = 4$ is to first calculate $162 \bmod 14 = 8$ and $460 \bmod 14 = 12$
  The problem is now to find the smallest natural k satisfying $(8 + k \cdot 12) \bmod 14 = 0$ which is much easier to solve for $k = 4$.

  Marking note: Solutions that realized that 162 *was a solution to (just) the first two congruences received some partial credit.*

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.

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

- (a) There exists a non-empty subset S of the naturals such that if x is any element of S, x's predecessor is also in S.

  FALSE (70% correct). By the Least Number Axiom, S must have a least element and thus its predecessor cannot be in S.

- (b) Let R be a partial order on a set A. Then if x and y are different elements of A, we know that $((x, y) \in R) \oplus ((y, x) \in R)$.

  FALSE (49% correct). By antisymmetry, these two statments cannot be both true, but there is no reason why they can't both be false.

- (c) Let $a > 1$ be a natural, and let $z = a! - 1$. Then for any natural b such that $1 < b \leq a$, z is not divisible by b.

  TRUE (74% correct). Since $a!$ is divisible by b, z must be congruent to -1 modulo b, and since $b > 1$, it cannot also be congruent to 0.

- (d) Consider a truth table using two boolean variables a and b. We know that $a \rightarrow (a \vee b)$. Then in the truth table the column for the term a has two 1's, and the column for the term $a \vee b$ has three.

  TRUE (82% correct). This is correct since a has two settings making it true, TF and TT, while $a \vee b$ has three, FT, TF, and TT.

- (e) Let a be any natural such that $a \equiv 2 \pmod 5$. Then there exists some natural n such that $a^n \equiv 0 \pmod 5$.

  FALSE (78% correct). Any such number a^0 is congruent to 1. Since a^4 is congruent to 1 as well, any number a^n is congruent to $a^0 \equiv 1$, $a^1 \equiv 2$, $a^2 \equiv 4$, or $a^3 \equiv 3$, mod 5.

- (f) Hasse Diagrams may be used to represent equivalence relations as well as to represent partial orders.

  FALSE (71% correct). The assumptions for a Hasse Diagram makes its relation antisymmetric.

- (g) Let X be the set of all even naturals, and let Y be the set of all odd naturals. Then there does not exist a set Z such that $Z \subseteq X$ and $Z \subseteq Y$.

  FALSE (59% correct). $Z = \emptyset$ makes $Z \subseteq X$ and $Z \subseteq Y$ both true.

- (h) A function $f : X \rightarrow Y$ is one-to-one if and only if for every element x of X, there is exactly one element y of Y such that $f(x) = y$.

  FALSE (47% correct). This is the definition for any function, not for one-to-one.

- (i) Let x, y, and z be three naturals such that $xyz = 4200$. Then one of these three numbers is divisible by 7, and the other two are not.

TRUE (83% correct). This follows from Unique Factorization. Since there is exactly one 7 in the factorization of $4200 = 2^2 3^3 5^2 7^1$, there must be exactly one 7 between the three factors.

- (j) The statement $X \Delta Y = (X \cup Y) \setminus (X \cap Y)$ is a set identity.
  TRUE (78% correct). This translates to the boolean tautology $(x \oplus y) \leftrightarrow (x \vee y) \wedge \neg(x \vee y)$.

Grading Notes: *There were 9% of you with perfect 20/20 scores, and six people (2%) who gave no answers at all. The mean score was 13.8/20, 69% correct.*