

Midterm 1 Solutions

Note: These solutions are not necessarily model answers. Rather, they are designed to be tutorial in nature, and sometimes contain more explanation (occasionally much more) than an ideal solution. Also, bear in mind that there may be more than one correct solution. The maximum total number of points available is 60.

1. Quick Questions

(a) The truth tables are as follows:

6pts

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
true	true	true	true	true
true	false	false	true	false
false	true	true	false	false
false	false	true	true	true

Almost all people got this question right. The most common mistake was in the table for $P \Leftrightarrow Q$.

(b) (i) and (iii) are valid strategies. (ii) and (iv) are invalid strategies. Although they were not required, 8pts here are explanations for these answers:

The original statement is $(\exists x P(x)) \Rightarrow (\forall y Q(y))$.

(i): The *contrapositive* is $(\exists y \neg Q(y)) \Rightarrow (\forall x \neg P(x))$. The contrapositive is logically equivalent to the original statement. Thus, we can approach this problem by assuming the left-hand side is true and showing that this implies the right-hand side.

(ii): This would prove the statement $(\forall y Q(y)) \Rightarrow (\exists x P(x))$. This is the *converse* of the original statement which is not logically equivalent to the original statement.

(iii): This is a proof by *contradiction*. It approaches the proof by assuming that the negation of the statement is true. The negation of the statement is

$$\begin{aligned}
 \neg[(\exists x P(x)) \Rightarrow (\forall y Q(y))] &\equiv \neg[\neg(\exists x P(x)) \vee (\forall y Q(y))] \\
 &\equiv \neg[(\forall x \neg P(x)) \vee (\forall y Q(y))] \\
 &\equiv \neg(\forall x \neg P(x)) \wedge \neg(\forall y Q(y)) \\
 &\equiv (\exists x P(x)) \wedge (\exists y \neg Q(y))
 \end{aligned}$$

(iv): This would prove the statement

$$\begin{aligned}
 \neg[(\forall x P(x)) \wedge (\forall y \neg Q(y))] &\equiv \neg(\forall x P(x)) \vee \neg(\forall y \neg Q(y)) \\
 &\equiv \neg(\forall x P(x)) \vee (\exists y Q(y)) \\
 &\equiv (\exists x \neg P(x)) \vee (\exists y Q(y))
 \end{aligned}$$

which is not logically equivalent to the original statement.

A number of people had some trouble with one or more parts of this problem. Some people reduced incorrectly. It was not necessary to show your work for this part.

- (c) The stable marriage produced by the algorithm is (1,B), (2,C), (3,A), (4,D). 4pts

Almost all people got this question right.

- (d) We use the extended-gcd algorithm: 6pts

```
e-gcd(743,10)
  e-gcd(10,3)
    e-gcd(3,1)
      e-gcd(1,0)
        return (1,1,0)
      return (1,0,1)
    return (1,1,-3)
  return (1,-3,223)
```

Since the gcd of 743 and 10 is 1, we know that 10 has a multiplicative inverse modulo 743. We know from the return values that $1 = (-3)(743) + (223)(10)$. Modulo 743, this is equivalent to $1 = (223)(10)$, telling us that 223 is the multiplicative inverse of 10 modulo 743.

Most people got this question right. A few people had trouble with the calls or return values of extended-gcd. A few people had no problem with the calls but did not know how to use the results to find the inverse.

2. A Tiling Problem

- (a) Clearly there is only one way to tile a 2×1 board, namely with a single **B**-tile; hence $T_1 = 1$. A 2×2 board can be tiled in exactly three ways: with two **A**-tiles, two **B**-tiles, or two **C**-tiles. Hence $T_2 = 3$. 2pts

Virtually everybody got this right.

- (b) Consider any tiling configuration of a $2 \times n$ board for $n \geq 3$. We identify three cases, according to whether the last column of this tiling is covered by one **B**-tile, or by (part of) a **C**-tile or two **A**-tiles. If we remove the tile or tiles covering this last column, we are left with either a $2 \times (n-1)$ configuration (in the case of the **B**-tile), or a $2 \times (n-2)$ configuration (in the other two cases). Thus every $2 \times n$ configuration is uniquely obtained by adding a **B**-tile to a $2 \times (n-1)$ configuration, or by adding two **A**-tiles or one **C**-tile to a $2 \times (n-2)$ configuration. Thus we have $T_n = T_{n-1} + 2T_{n-2}$. 4pts

Many people got confused by this part; obviously, since the answer was given, it was possible to come up with a completely bogus explanation of it! The most common error was to try to extend a $2 \times (n-1)$ and/or a $2 \times (n-2)$ configuration to a $2 \times n$ configuration; the problem with this is that it is hard to convince the reader that you are really counting each $2 \times n$ configuration exactly once, though some students were able to argue this convincingly. (Notice how the above argument starts from the $2 \times n$ configuration, splits it into cases, and works back down to the smaller configurations, which is much easier.) There were many other arguments, based on sliding tiles around, adding tiles at the beginning and at the end (and even in the middle) etc., all of which missed the point.

- (c) Goal: Prove by induction on n that $T_n = \frac{2^{n+1} + (-1)^n}{3}$ 9pts

Base cases ($n = 1$ and $n = 2$): Setting $n = 1$ in the formula gives $\frac{2^{1+1} + (-1)^1}{3} = \frac{4-1}{3} = 1$, which is indeed equal to T_1 by part (a). Setting $n = 2$ gives $\frac{2^{2+1} + (-1)^2}{3} = \frac{8+1}{3} = 3$, which is indeed equal to T_2 by part (a).

Induction hypothesis: For an arbitrary $n \geq 3$, assume that $T_k = \frac{2^{k+1} + (-1)^k}{3}$ for $1 \leq k < n$.

Induction step: We need to prove that $T_n = \frac{2^{n+1} + (-1)^n}{3}$. We have:

$$\begin{aligned}
 T_n &= T_{n-1} + 2T_{n-2} && \text{[by part (b)]} \\
 &= \frac{2^n + (-1)^{n-1}}{3} + 2 \cdot \frac{2^{n-1} + (-1)^{n-2}}{3} && \text{[by induction hypothesis for } k = n-1 \text{ and } k = n-2\text{]} \\
 &= \frac{1}{3} (2^n + 2^n + (-1)^{n-1} + 2(-1)^{n-2}) \\
 &= \frac{1}{3} (2^{n+1} + (-1)^n (-1 + 2)) \\
 &= \frac{1}{3} (2^{n+1} + (-1)^n).
 \end{aligned}$$

This completes the proof by (strong) induction.

Most people got this part more or less right, but few people got it completely right. Common errors were the following:

- *Many people forgot the second base case ($n = 2$); note that this is essential because we can only start using the relation in part (b) once $n \geq 3$. So, to prove the formula for T_3 , we need both T_1 and T_2 .*
- *Even more people did not write down the induction hypothesis correctly. Note that we must use strong induction here, since to prove the formula for T_n we need not only T_{n-1} but also T_{n-2} . So it is not enough just to assume the formula for $T_{n=1}$. [Many people said that their induction hypothesis is that the formula is true “for all $n \geq 1$ ”; this is nonsense as it is exactly what we are trying to prove. What those people presumably meant was that the formula is true “for some n ”, which is really just like assuming it for one value of n .] Many people also seemed to think that $T_n = T_{n-1} + 2T_{n-2}$ is part of the induction hypothesis; it is not – it is a fact that you proved in part (b) and that you use in order to prove the induction step, assuming the induction hypothesis.*
- *When proving the induction step, many people did not clearly state where they were using the induction hypothesis (see the second line of the derivation above). This should always be stated in any induction proof.*

3. Modular Arithmetic

(i) **True.** $((a + b)^3 = a^3 + b^3 \pmod{3})$

3pts

To prove this, first notice that $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$. Also we have that $3a^2b + 3ab^2 = 0 \pmod{3}$ because each term is a multiple of 3. Hence, taking the remainder of the division by 3 on both sides of $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$, we obtain

$$(a + b)^3 = a^3 + 0 + b^3 \pmod{3} = a^3 + b^3 \pmod{3}.$$

(ii) **False.** $((a + b)^4 \neq a^4 + b^4 \pmod{4} \text{ in general})$

3pts

A counterexample is obtained by setting $a = 1, b = 1$. In this case $a^4 + b^4 = 1^4 + 1^4 = 1 + 1 = 2 \pmod{4}$. On the other hand, $(a + b)^4 = (1 + 1)^4 = 2^4 = 16 = 0 \pmod{4}$.

*Some people took the **incomplete** approach that consists of first noticing that $(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$. Then using the same idea as in part (b), one can get rid of the terms $4a^3b$ and $4ab^3$, since they are $0 \pmod{4}$. These people then said that the remaining factor $6a^2b^2$ does not disappear. However, to complete the argument one needs to give a specific counterexample (i.e., values for a, b so that $6a^2b^2 \neq 0 \pmod{4}$.) An example of such values is $a = 1, b = -1$, as above. Many other examples are possible.*

(iii) **True.** $((a + b)^5 = a^5 + b^5 \pmod{5})$

3pts

This can be shown using the same argument as in part (a). First notice that $5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 = 0 \pmod{5}$ because each term is a multiple of 5. Now using the formula for $(a + b)^5$, we have

$$(a + b)^5 = a^5 + 0 + b^5 \pmod{5} = a^5 + b^5 \pmod{5}.$$

4. Stable Marriage

- (a) **True.** If we run the traditional propose and reject algorithm, on the first day, M will propose to W (since W is at the top of M 's preference list) and W will say "maybe" since M is at the top her preference list. In the subsequent days, M will keep proposing to W and W will keep saying "maybe" to M and rejecting offers from other men since she prefers M to all other men. Thus M and W will eventually be paired up upon termination of the algorithm. Since we know that the algorithm always terminates with a *stable* pairing, we know there must exist a stable pairing in which M is paired with W . 4pts

The most common mistake was to prove by contradiction that any stable pairing, if it exists, must have M paired with W . The missing point here is to say that a stable pairing always exists!

- (b) **False.** This is proved by giving a counter example. The common example given by many students was the following stable marriage instance with two men and women: 4pts

Man	Women	
1	A	B
2	A	B

Woman	Men	
A	1	2
B	1	2

The pairing $\{(A, 1)(B, 2)\}$ is stable, and has man 2 and woman B both at the bottom of their corresponding preference lists.

Almost everybody got this part right.

- (c) **True.** Since this is an *existential* statement, to prove it it is sufficient to give an example that satisfies it. 4pts

Consider the following example with two men and two women:

Man	Women	
1	A	B
2	B	A

Woman	Men	
A	1	2
B	2	1

For this example, the pairing $\{(A, 2), (B, 1)\}$ is unstable, and every unmatched pair (which in this example means $(A, 1)$ and $(B, 2)$) is a rogue couple.

More generally, we could take an example for any n in which man 1 and woman A put each other at the bottom of each other's preference lists, similarly for man 2 and woman B , for man 3 and woman C , and so on. Then in the unstable pairing $(1, A), (2, B), (3, C), \dots$ everybody is paired with their least-favorite person, so every unmatched pair (e.g., $(1, B), (2, C)$ etc.) is a rogue couple.

Some students apparently misunderstood this question, so they ended up trying to show the wrong property.