# Midterm 1 Solutions

*Note: These solutions are not necessarily model answers. They are designed to be tutorial in nature, and sometimes contain a little more explanation than an ideal solution. Also, bear in mind that there may be more than one correct solution. The maximum number of points is 60. Comments in italics following the solutions highlight some common errors or give explanations.*

**1. [Logic]** [10 pts; $+1$ for each correct answer; $-1$ for each incorrect answer]

(a) *5pts*

- $\forall n(Q(n) \Rightarrow P(n))$ **No**
- $\forall n(P(n) \vee \neg Q(n))$ **No**
- $\neg\exists n(P(n) \wedge \neg Q(n))$ **Yes** [*Equivalent to* $\forall n(\neg P(n) \vee Q(n))$.]
- $\forall n(\neg P(n) \Rightarrow \neg Q(n))$ **No**
- $Q(0) \wedge \neg P(1) \wedge \forall n(Q(n) \Rightarrow Q(n+2)) \wedge \forall n(P(n+2) \Rightarrow P(n))$ **No**
  [*This proposition says that, for all even $n$, $Q(n)$ is true, and for all odd $n$, $P(n)$ is false, which implies $\forall n(P(n) \Rightarrow Q(n))$. However, the reverse implication is not true, because, for example, the original proposition does not imply that $Q(0)$ is true.*]

(b) *5pts*

- $\exists m \forall n R(m,n)$ **No**
- $\forall m \exists n R(n,m)$ **Yes** [*interchanges roles of $m$ and $n$*]
- $\forall m \exists n R(m,n)$ **No**
- $\neg\exists n \forall m(\neg R(m,n))$ **Yes**
- $\forall n \exists m(R(n+m,n) \vee R(n-m,n))$ **Yes**
  [*As $m$ varies, the sets of values $\{n+m\}$ and $\{n-m\}$ cover all natural numbers.*]

**2. [Induction]** [10 pts]

Base case: $\sum_{i=1}^{1}(3i)^2 = 9 = \frac{3}{2}(1)(1+1)(2*1+1)$. *10pts*
Induction hypothesis: For some $k \geq 1$, assume $\sum_{i=1}^{k}(3i)^2 = \frac{3}{2}k(k+1)(2k+1)$.
Induction step:

$$\begin{aligned}
\sum_{i=1}^{k+1}(3i)^2 &= 9(k+1)^2 + \sum_{i=1}^{k}(3i)^2 \\
&= 9(k+1)^2 + \frac{3}{2}k(k+1)(2k+1) \qquad \text{by the induction hypothesis} \\
&= \frac{3}{2}(k+1)\left(6(k+1) + k(2k+1)\right) \\
&= \frac{3}{2}(k+1)(2k^2+7k+6) \\
&= \frac{3}{2}(k+1)(k+2)(2k+3) \\
&= \frac{3}{2}(k+1)(k+2)(2(k+1)+1).
\end{aligned}$$

Thus, assuming the statement holds for some value $k$, we have shown it is also holds for the value $k+1$. This completes the induction step and hence the proof by induction.

*Comments:*

- *Most students did well on this problem. The most common error was in the Induction Step; rather than proving that* $P(k) \implies P(k+1)$ *(which is what you need to do), some students assumed that* $P(k+1)$ *was true and derived* $P(k)$ *from that, but did not describe why their argument could be reversed to show that* $P(k+1)$ *could also be derived from* $P(k)$*. To clarify: If you start by assuming* $\sum_{i=1}^{k+1}(3i)^2 = \frac{3}{2}(k+1)(k+2)(2(k+1)+1)$*, and then rewrite the left-hand side, using your induction hypothesis, and simplify both sides to yield* $0 = 0$*, then your proof would be correct* provided you state that ”because each step can be inverted, each implication goes in both directions.” *If you did not state that your proof that* $P(k+1) \implies P(k)$ *could be inverted to show that* $P(k) \implies P(k+1)$*, you automatically lost (at least) three points.*
- *Quite a few students gave the Induction Hypothesis “*$\forall k, \sum_{i=1}^{k}(3i)^2 = \frac{3}{2}k(k+1)(2k+1)$*.” This is a very serious error, and invalidates the entire induction argument. (If this is your induction hypothesis, there is nothing to prove for the induction step!!!!) Partial credit was given if the rest of the proof was alright.*
- *Students who structured their proof correctly, but then got into trouble in the algebraic manipulation got few points taken off: 1 point if the student wrote something like ”I can’t get the algebra to work out, but this expression should be equivalent to* $(k+1)(k+2)(2(k+1)+1)$*. Students who got really bogged down in the manipulation, and then just crossed stuff out, and wrote* $= (k+1)(k+2)(2(k+1)+1)$*, were also penalized minimally. Students who clearly realized that they had made algebraic errors, but then tried to cover them up and ended up writing obviously false statements,such as* $n + (n+1) = (n+1)(n+2)(2(n+1)+1)$*, were deducted more heavily. (In life, as in academia, being open about one’s past mistakes is wonderful, making honest mistakes is perfectly fine, but actively trying to hide one’s mistakes is a pain for everyone.)*

**3. [Stable marriages]** [10 pts]

(a) The execution of the (traditional) Propose-and-Reject Algorithm is as follows:

| Day 1 | | Day 2 | | Day 3 | | Day 4 | |
|---|---|---|---|---|---|---|---|
| Women | Proposals | Women | Proposals | Women | Proposals | Women | Proposals |
| A | ① | A | ① | A | ④ 1 | A | ④ |
| B | | B | | B | | B | ① |
| C | ② 3 | C | ② | C | ② | C | ② |
| D | ④ | D | ③ 4 | D | ③ | D | ③ |

The final pairing is $\{(1,B),(2,C),(3,D),(4,A)\}$.

*Almost all people got this right. Partial credit was given to solutions showing an understanding of the algorithm, which however did not get the correct pairing due to careless mistakes.*

(b) Since the pairing in part (a) is male optimal, Man 4 can at best be paired with Woman $A$ under any stable pairing, so there is no stable pairing in which Man 4 is paired with Woman $D$.

*Less than half of the people got this right. A symmetric argument using female pessimality was also accepted. However, complicated arguments using three to four deductions to show a rogue pair received at most one point. Any argument about the execution of the Propose-and-Reject algorithm (e.g. Improvement Lemma or rejection on Day 2) received no points, because the algorithm finds only male optimal or female optimal pairings and so says nothing about other possible stable pairings.*

(c) Since the pairing in part (a) is female pessimal, Woman $B$ can at worst be paired with Man 1 under any stable pairing, so there is no stable pairing in which Woman $B$ is paired with Man 3.

*Similar remarks to those for part (b) also apply here. A few people computed as well the female optimal (male pessimal) pairing, and argued that Man 1 must be paired with Woman B in any stable pairing. This argument using the lattice of stable pairings was also accepted.*

**4. [Modular arithmetic]** [13 pts]

(a) For any integers $k, m$, since an odd number raised to any positive integer power is odd, and an even number raised to any positive integer power is even (or by Fermat's Little Theorem), $m^k = m \bmod 2$. Hence $n = n^5 = 133^5 + 110^5 + 84^5 + 27^5 = 133 + 110 + 84 + 27 = 1 + 0 + 0 + 1 = 0 \bmod 2$. *2pts*

(b) By Fermat's Little Theorem, $k^m = k^{m \bmod 2} \bmod 3$, and thus $n = n^5 = 133 + 110 + 84 + 27 = 1 + 2 + 0 + 0 = 0 \bmod 3$. *4pts*

(c) By Fermat's Little Theorem, $k^m = k^{m \bmod 4} \bmod 5$, and thus $n = n^5 = 133 + 110 + 84 + 27 = 3 + 0 + 4 + 2 = 4 \bmod 5$. *4pts*

(d) $n = 144$. To see this, note from parts (a), (b) and (c) that $n = 0 \bmod 2$, $n = 0 \bmod 3$, and $n = 4 \bmod 5$. This uniquely determines $n \bmod (2 * 3 * 5)$, i.e., we know that $n = 24 \bmod 30$ (the unique value mod 30 satisfying all three properties). Additionally, we are told that $n < 170$, and since $n^5 > 133^5$ we also know that $n > 133$. But there is just one value of $n$ in this range that is equal to 24 mod 30, namely $n = 144$. *3pts*

*Comments:*

- *In parts (b) and (c), several people correctly computed* $133^5 + 110^5 + 84^5 + 27^5 \bmod 3, 5$*, but then didn't see why* $n = n^5 \bmod 3, 5$*. Two points were taken off for this.*
- *Several people got incorrect answers for parts (a), (b) or (c), and then mysteriously gave the correct answer* $n = 144$ *for part (d). This received 0 points for part (d): if, for example, you said that* $n = 1 \bmod 2$ *for part (a), and then* $n = 144$ *for part (d), you should at least have noticed that these two answers are conflicting.*
- *People who gave incorrect answers for parts (a), (b) or (c), but gave an answer for part (d) that was consistent with their answers for these parts received full credit for part (d).*
- *Quite a few students gave the answer* $n = 24$*, which agrees with the correct answers for parts (a), (b) and (c). This received partial credit (for understanding the modular arithmetic component, but failing to observe that* $n > 133$*).*

**5. [Fermat's Little Theorem]** [7 pts]

(a) Fermat's Little Theorem says that, for any prime $p$ and integer $a \in \{1, 2, \ldots, p-1\}$, we have $a^{p-1} = 1 \bmod p$. Since $\mathrm{ord}_p(a)$ is defined as the *least* $i$ such that $a^i = 1 \bmod p$, and since $i = p - 1$ satisfies this condition, we must have $\mathrm{ord}_p(a) \le p - 1$. *2pts*

*Most people got this right, though many overlooked the very simple argument above. One point was awarded just for stating Fermat's Little Theorem.*

(b) Suppose for the sake of contradiction that $\mathrm{ord}_p(a)$ does not divide $p - 1$. Then, writing $i = \mathrm{ord}_p(a)$, we have $p - 1 = ki + \ell$, where $0 < \ell < i$. (Here $\ell$ is the remainder; it must be non-zero since $i$ does not divide $p - 1$.) *5pts*

By Fermat's Little Theorem we have $a^{p-1} = 1 \bmod p$, and hence (with all arithmetic mod $p$)

$$1 = a^{p-1} = a^{ki+\ell} = a^{ki}a^{\ell} = a^{\ell} \bmod p.$$

(In the last step here we used the fact that $a^i = 1 \bmod p$ since $i = \mathrm{ord}_p(a)$.)

But this is a contradiction since $1 \le \ell < i$ and $i$ is the least value $\ge 1$ for which $a^i = 1 \bmod p$.

Hence our original assumption that $\mathrm{ord}_p(a)$ does not divide $p - 1$ must be false.

*The overwhelming majority of students missed this part entirely. The typical errors were: (1) Not realizing that, if you want to prove by contradiction that* $x$ *divides* $y$*, you need to start by assuming (for contradiction) that* $y = kx + \ell$ *for a non-zero remainder* $\ell$ *with* $\ell < x$*. (2) Claiming that if* $a^i = a^j \bmod p$ *then* $i = j \bmod p$ *(or the contrapositive: that if* $i \ne j \bmod p$ *then* $a^i \ne a^j \bmod p$*); this implication is patently false (check this!).*

**6. [Secret sharing]** [10 pts]

Summary: The sum $P(0)+Q(0)$ and the product $P(0)\cdot Q(0)$ of the secrets are recovered using Lagrange interpolation to find the polynomials $P(x)+Q(x)$ and $P(x)\cdot Q(x)$ from the given data. The secrets are obtained from the sum and product by solving a quadratic equation.

(a) $P(x)+Q(x)$ is a polynomial of degree 2 and passes through the points $(i, P(i)+Q(i))$. *(Note that we know all of these points exactly from the given data, because to compute $P(i)+Q(i)$ we don't need to know which value is $P(i)$ and which is $Q(i)$.)* We use the three points $(1,5),(2,5),(3,0)$ and write the Lagrange interpolation formula:

$$P(x)+Q(x) = 5\cdot\Delta_1(x) + 5\cdot\Delta_2(x) + 0\cdot\Delta_3(x) \tag{1}$$

The polynomials $\Delta_i$ are given by:

$$\begin{aligned}\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = 4(x^2-5x+6)\\ \Delta_2(x) &= \frac{(x-1)(x-3)}{(2-1)(2-3)} = 6(x^2-4x+3)\end{aligned}$$

We compute $P(x)+Q(x)$ by substituting the expressions for $\Delta_i$ in the Lagrange interpolation formula (1):

$$\begin{aligned}P(x)+Q(x) &= 5\cdot\Delta_1(x)+5\cdot\Delta_2(x)\\ &= -1(x^2-5x+6)+2(x^2-4x+3) = x^2-3x\end{aligned}$$

The sum of the secrets $P(0)+Q(0)$ is therefore equal to $0$.

(b) $P(x)\cdot Q(x)$ is a polynomial of degree 3 and passes through the points $(i, P(i)\cdot Q(i))$. We use the four points $(1,0),(2,4),(4,0),(5,0)$ and write the Lagrange interpolation formula:

$$P(x)\cdot Q(x) = 0\cdot\Delta_1(x) + 4\cdot\Delta_2(x) + 0\cdot\Delta_4(x) + 0\cdot\Delta_5(x) \tag{2}$$

Since three of these coefficients are zero, it is sufficient to compute the polynomial $\Delta_2$:

$$\Delta_2(x) = \frac{(x-1)(x-4)(x-5)}{(2-1)(2-4)(2-5)} = 6(x^3-3x^2+x+1)$$

We compute $P(x)\cdot Q(x)$ by substituting the expression for $\Delta_2$ in the Lagrange interpolation formula (2):

$$\begin{aligned}P(x)\cdot Q(x) &= 4\cdot\Delta_2(x)\\ &= 3x^3+5x^2+3x+3\end{aligned}$$

The product of the secrets $P(0)\cdot Q(0)$ is therefore equal to 3.

(c) The square of the difference of the secrets is given by $(Q(0)-P(0))^2 = (P(0)+Q(0))^2 - 4\cdot P(0)\cdot Q(0) = 2$. We observe that the two solutions to $x^2 = 2 \mod 7$ are $\pm 3$ hence $Q(0)-P(0) = \pm 3 \mod 7$. Given that $Q(0) > P(0)$ we find that the secrets are $P(0)=2$ and $Q(0)=5$.

*Many students tried a pattern matching approach to this question, trying to guess the linear polynomial $P(x)$; once $P(x)$ is known, the rest of the problem of course becomes trivial. While full credit was awarded to such solutions if the secrets were found correctly, this method would not be feasible for larger fields or higher degree polynomials. (E.g., suppose $P(x)$ and $Q(x)$ had degrees 5 and 7 over $GF(107)$). The key idea that $P(i)+Q(i)$ and $P(i).Q(i)$ can be computed given $(P(i),Q(i))$ OR $(Q(i),P(i))$ as they are symmetric functions (do not depend on order) was missed by many students.*