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 70. Comments in italics following the solutions highlight some common errors or give explanations.

1. [Multiple Choice/Short Answers]
For these questions, correct answers received positive scores, incorrect answers a score of -1 (except in parts (g), (h), (i), where incorrect answers were not penalized), and blank answers zero. No partial credit was given and no working was expected.

(a) **[True or false?]** *Mark each of the following "True" if it is a valid logical equivalence, and "False" otherwise.*

- $P \Rightarrow Q \equiv P \vee \neg Q$: **False** *1pt*
- $P \Rightarrow Q \equiv (\neg P \Rightarrow \neg Q)$: **False** *1pt*
- $P \Rightarrow Q \equiv (Q \wedge P) \vee \neg P$: **True** *1pt*

(b) **[True or false?]** *Let $P(x)$ be a proposition about an integer x, and suppose you want to prove the theorem $\forall x\,(P(x) \Rightarrow Q(x))$. Mark each of the following proof strategies "True" if it would be a valid way to proceed with such a proof, and "False" otherwise.*

- Find an x such that $Q(x)$ is true or $P(x)$ is false: **False** *1pt*
- Show that, for every x, if $Q(x)$ is false then $P(x)$ is false: **True**. *1pt*
- Assume that there exists an x such that $P(x)$ is false and $Q(x)$ is false and derive a contradiction: **False** *1pt*
- Assume that there exists an x such that $P(x)$ is true and $Q(x)$ is false and derive a contradiction: **True** *1pt*

(c) **[True or false?]** *Suppose you have a rectangular array of pebbles, where each pebble is either red or blue. Suppose that for every way of choosing one pebble from each column, there exists a red pebble among the chosen ones. Then there must exist an all-red column.* **True** *1pt*

(d) **[Multiple choice]** *Two of the following quantified propositions are equivalent to each other, while the other is not equivalent.* **Circle** *the one which is* **not** *equivalent to the other two.* *3pts*

- The correct answer is the **first** proposition: $(\exists a \in A)(\forall b \in B)(R(a) \vee \neg P(a,b))$.

(e) **[True or false?]** *Which of the following propositions also implies that $P(n)$ holds for all n? Mark each one "True" if so, and "False" if not.*

- $P(0) \wedge P(1) \wedge \forall n(P(n) \Rightarrow P(n+2))$: **True** *1pt*
- $P(0) \wedge P(1) \wedge (\forall n \geq 1)((P(n) \Rightarrow P(2n-1)) \wedge (P(n) \Rightarrow P(2n+1)))$: **False** *1pt*
- $P(0) \wedge P(1) \wedge \forall n_1 \forall n_2((P(n_1) \wedge P(n_2)) \Rightarrow P(n_1+n_2))$: **True** *1pt*

(f) **[True or false?]** *Mark each of the two statements below "True" or "False".*

- The set $\mathbb{R}$ of real numbers is well-ordered under the standard ordering: **False** *1pt*
- $\mathbb{N}$ is well-ordered under the even-odd ordering $\preceq$: **True** *1pt*

(g) **[Short answer]**

- What is the inverse of 8 mod 13? Answer: **5** *1pt*
- Solve the equation $8x = 5 \bmod 13$. Answer: $x =$ **12** *1pt*

(h) **[Short answer]** *Bob runs a small business selling widgets over the Internet. Alice wants to buy one of Bob's widgets but is worried about the security of her credit card information, so she and Bob agree to use RSA encryption. Bob generates $p = 7, q = 3$ and $e = 5$.*

- What does Bob need to send to Alice (i.e., what is Bob's public key)? Answer: (**21**, **5**) *1pt*
- What is Bob's private key? Answer: **5** *1pt*
- Suppose Alice's credit card number is $x = 4$. What is the encrypted message $E(x)$? Answer: **16** *1pt*

(i) **[Multiple choice]** *This question concerns polynomials over $GF(q)$, where $q \geq 5$ is a prime.* **Circle** *the correct answer in each case. (The response "not determined" means that you do not have enough information to give a precise answer.)*

- The number of distinct polynomials of degree at most 2 over $GF(q)$ that pass through three given points $(0, y_0)$, $(1, y_1)$, $(2, y_2)$ is: **1** *1pt*
- The number of distinct polynomials of degree at most 2 over $GF(q)$ that pass through four given points $(0, y_0)$, $(1, y_1)$, $(2, y_2)$, $(3, y_3)$ is: **not determined** *1pt*
- The number of distinct polynomials of degree at most 2 over $GF(q)$ that pass through one given point $(0, y_0)$ is: $\mathbf{q}^2$ *1pt*
- Let $P_1(x)$, $P_2(x)$ be two distinct polynomials of degree 2 over $GF(q)$. The maximum possible number of points at which P_1 and P_2 intersect (i.e., the maximum possible number of values of x for which $P_1(x) = P_2(x)$) is: **2** *1pt*

Part (i) gave the most problems of all parts in Q1. Here are brief explanations of the solutions. The first one uses the standard fact that a polynomial of degree at most d is uniquely specified by $d + 1$ points. For the second one, note that any three of the points uniquely specify a polynomial, and the fourth point either lies on this polynomial or does not; so the number of polynomials through the four points is either one or zero. For the third one, since only one point $(0, y_0)$ is given, we are free to specify the values of the polynomial at any two additional points (say, $(1, y_1)$ and $(2, y_2)$); there are exactly q^2 choices for the values y_1 and y_2, and each choice gives a unique polynomial (obviously all the polynomials are distinct), so there are q^2 polynomials in total. For the fourth and final one, note that any point x at which $P_1(x) = P_2(x)$ is a zero of the polynomial $Q(x) = P_1(x) - P_2(x)$, which has degree at most 2; hence the number of such points x is equal to the number of zeros of Q, which is at most 2.

---

2. [Induction]

Prove by induction that, for all natural numbers $n \geq 1$, the number $n(n^2 + 5)$ is divisible by 6. *10pts*

Let $P(n)$ denote the proposition "$n(n^2 + 5)$ is divisible by 6". We prove $(\forall n \geq 1)P(n)$ by induction on n.

Base case: $n = 1$. Note that $1(1^2 + 5) = 6$, which is clearly divisible by 6. Hence $P(1)$ holds.

Induction hypothesis: For an arbitrary $n \geq 1$, we assume $P(n)$, i.e., that $n(n^2 + 5)$ is divisible by 6.

Induction step: Using the induction hypothesis, we need to deduce that $P(n + 1)$ holds, i.e., that $(n + 1)((n + 1)^2 + 5)$ is divisible by 6. To do this, we proceed as follows:

$$\begin{aligned}(n+1)((n+1)^2+5) &= (n+1)(n^2+2n+6)\\ &= n^3+3n^2+8n+6\\ &= (n^3+5n)+(3n^2+3n+6)\\ &= n(n^2+5)+3(n^2+n)+6. \qquad (1)\end{aligned}$$

Now the first term in line (1) is divisible by 6 by the induction hypothesis $P(n)$, and the last term is obviously divisible by 6. So it remains only to show that the middle term, $3(n^2 + n)$, is divisible by 6.

But note that $3(n^2 + n) = 3n(n + 1)$, and that for any n either n or $n + 1$ must be even. Hence $n(n + 1)$ is divisible by 2, and hence $3n(n + 1)$ is divisible by 6.

This completes the verification that $P(n + 1)$ holds, and hence the induction proof.

Most students did well on this problem. The most common error was to get as far as equation (1) above, and then fail to argue correctly that the middle term, $3(n^2 + n)$, is divisible by 6. Many people wrote $3(n^2 + n) = 6(\frac{n^2}{2} + \frac{n}{2})$ and claimed that this is divisible by 6; but to claim this you have to show that $(\frac{n^2}{2} + \frac{n}{2})$ is an integer, which is essentially equivalent to the original claim.

Many people used $P(n)$ interchangeably to denote both a proposition ($P(n)$ = "$n(n^2 + 5)$ is divisible by 6") and a formula ($P(n) = n(n^2 + 5)$). This is sloppy but did not lose points if the proof was otherwise correct. Some students mis-stated the inductive hypothesis, assuming "$P(n)$ for all n" rather than for some arbitrary n; this is also incorrect but did not generally lose points if the proof was otherwise correct. However, **in future you may lose points for either of these errors!**

A few students tried to prove the inductive step without the inductive hypothesis, using arguments involving Fermat's Little Theorem or factoring polynomials. Even when correct these answers did not receive many points, since the problem statement asks for a proof by induction.

Several people proved $P(n) \Rightarrow P(n + 2)$ as their inductive step (or equivalently, $P(n - 1) \Rightarrow P(n + 1)$). They received full credit as long as they realized that this approach requires two base cases, $P(1)$ and $P(2)$, since it is essentially two separate inductions on $n = 1, 3, 5, \ldots$ and $n = 2, 4, 6, \ldots$.

---

3. [Stable Marriage]

(a) The execution of the (traditional) Propose-and-Reject Algorithm on the given instance is as follows: *4pts*

	Day 1	Day 2	Day 3	Day 4
A	~~1~~ 4	4	4	4
B				3
C	2 ~~3~~	1 ~~2~~	1	1
D		3	2 ~~3~~	2

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

(b) The only reliable way to determine the best possible man for woman B is to construct a female-optimal stable pairing using the Female-Propose-Male-Reject algorithm as follows: *4pts*

	Day 1	Day 2	Day 3
1			B
2	B	~~B~~ D	D
3	A	A	A
4	C ~~D~~	C	C

The female-optimal pairing is $\{(1,B),(2,D),(3,A),(4,C)\}$. This shows that man 1 is the best possible man for B in any stable pairing.

(c) A rogue couple is a man and woman **who are not currently paired** such that each prefers the other to their current partner. Thus in the given pairing the only rogue couples are (2, C) and (4,A). *2pts*

---

4. [Modular Arithmetic]

(a) *Compute* $11^{13} \pmod{100}$ *using repeated squaring. Show your intermediate results and write your* $\boxed{\textit{final answer}}$ *in a box.*

By repeated squaring we compute: *5pts*

$$\begin{aligned} 11^2 &= 121 = 21 \pmod{100} \\ 11^4 &= 21^2 = 41 \pmod{100} \\ 11^8 &= 41^2 = 81 \pmod{100} \end{aligned}$$

$$\begin{aligned} 11^{13} &= 11^{1+4+8} = 11^1 \times 11^4 \times 11^8 \\ &= 11 \times 41 \times 81 = 51 \times 81 \\ &= \boxed{31} \pmod{100} \end{aligned}$$

- *At most one point was given if the successive powers* 11^2, 11^3, 11^4, 11^5, ... *were computed, as this approach does not use repeated squaring.*
- *Points were taken off if the structure of the repeated squaring was not clearly expressed, e.g., if* 11^{13} *was broken up into* $11^1 \times 11^2 \times 11^4 \times 11^6$ *where not all exponents were powers of two, or if* 11^8 *was not computed using* $(11^4)^2$ *in a clear way.*
- *A common mistake made by some students was to write* 11^{13} *in such a way that the exponents did not add up to* 13*, e.g.,* $11^{13} = 11^1 \times 11^2 \times 11^8$.
- *Partial credit was deducted for arithmetic errors or messy calculation, e.g., not reducing intermediate results* $\bmod 100$.

(b) *State Fermat's Little Theorem, and then use it to give a careful proof of the following claim.*
Claim: *If* p *is prime and* b, c *are positive integers such that* $b = c \pmod{p-1}$*, then* $a^b = a^c \pmod{p}$ *for any integer* a.

Fermat's Little Theorem states that for any prime p, for any $a \in \{1, 2, \ldots, p-1\}$, $a^{p-1} = 1 \pmod{p}$. *5pts*

Case 1: $a = 0 \pmod{p}$. Then $a^b = 0 = a^c \pmod{p}$ for any positive integers b and c.

Case 2: $a \neq 0 \pmod{p}$. Since $b = c \pmod{p-1}$, we have $b = c + k(p-1)$ for some integer k, so

$$a^b = a^{c+k(p-1)} = a^c \times (a^{p-1})^k \overset{(*)}{=} a^c \times 1^k = a^c \pmod{p} \ ,$$

where the equality $(*)$ comes from Fermat's Little Theorem.

- *Many students stated Fermat's Little Theorem incorrectly, claiming that* $a^{p-1} = 1 \pmod{p}$ *even when* $a = 0 \pmod{p}$.
- *Almost all students did not realize that equality* $(*)$ *does not directly follow from Fermat's Little Theorem when* $a = 0 \pmod{p}$*, and got points deducted for not properly handling that case (even though many of them stated Fermat's Little Theorem correctly, noting that* $a \neq 0 \pmod{p}$*).*

- *Points were deducted for ambiguous arguments (e.g., "keep subtracting $p-1$ from b until it equals c") or convoluted arguments.*

(c) *Find* $8^{(321^{49})} \pmod{11}$. *Show your working and write your* $\boxed{\textit{final answer}}$ *in a box.*

Using part (b) with $p = 11$, the first step is to calculate $321^{49} = 1^{49} = \boxed{1} \pmod{10}$. *3pts*
Then by part (b) we have $8^{(321^{49})} = 8^1 = 8 \pmod{11}$.

- *Some students jumped from* $8^{(321^{49})}$ *to* $(8^{321})^{49}$*, not realizing that* $x^{(y^z)} \neq (x^y)^z$ *in general.*
- *Points were deducted for computing* $49 \pmod 9$*, apparently trying to argue that*

$$321^{49} = 321^{49 \bmod 9} \pmod{10},$$

not realizing that 10 *is not prime and part (b) does not apply here. Even though it may give the right answer, this is not a valid reason.*

- *Points were deducted for overly complicated arguments.*

---

5. [Secret Sharing]

D'Artagnan wants to share a secret with the three Musketeers (Athos, Aramis, and Porthos) about the location of a valuable piece of jewelry. The secret s *is an integer in the range* $0 \leq s \leq 10$*, and D'Artagnan secretly generates a polynomial* p *of degree* ≤ 2 *over* $\mathrm{GF}(11)$*. He gives* $p(0) = 8$ *to Athos,* $p(1) = 4$ *to Aramis, and* $p(2) = 6$ *to Porthos, and tells them that the secret is* $s = p(3)$*.*

(a) *If the three Musketeers share their information with each other, show how they can recover the secret* s *using Lagrange interpolation. Show your working.*

The three points $(x_0, y_0) = (0, 8)$, $(x_1, y_1) = (1, 4)$, $(x_2, y_2) = (2, 6)$ specify a unique polynomial p of degree ≤ 2 over $\mathrm{GF}(11)$. Using Lagrange interpolation we may write *5pts*

$$p(x) = y_0\Delta_0(x) + y_1\Delta_1(x) + y_2\Delta_2(x)$$

where

$$\begin{aligned}
\Delta_0(x) &= (-1 \cdot -2)^{-1}(x-1)(x-2) = 2^{-1}(x^2 - 3x + 2) = 6x^2 + 4x + 1 \pmod{11} \\
\Delta_1(x) &= (1 \cdot -1)^{-1}(x)(x-2) = -1^{-1}(x^2 - 2x) = -x^2 + 2x \pmod{11} \\
\Delta_2(x) &= (2 \cdot 1)^{-1}(x)(x-1) = 2^{-1}(x^2 - x) = 6x^2 - 6x \pmod{11}
\end{aligned}$$

(Note that $2^{-1} = 6 \pmod{11}$ and $-1^{-1} = -1 \pmod{11}$.) Plugging in we get:

$$p(x) = 8(6x^2 + 4x + 1) + 4(-x^2 + 2x) + 6(6x^2 - 6x) = 3x^2 + 4x + 8 \pmod{11}$$

We can now compute the secret as $s = p(3) = 3 \pmod{11}$.

- *Some students missed points due to arithmetic errors, mostly due to not reducing intermediate results* $\bmod 11$.

(b) *Suppose that the three Musketeers are too busy fighting for their country, and they hire their compatriot René Descartes to find the secret for them. Knowing how smart the mathematician is, and afraid he would steal their treasure, they decide to modify the values they give Descartes as follows: they tell him that* $p(0) = 7$*,* $p(1) = 3$*, and* $p(2) = 5$*. After a few minutes, Descartes gives back* $p(3) = 2$*.*

Explain how the Three Musketeers can recover the original secret s easily, without solving a system or doing Lagrange interpolation, and justify your answer.

If we define the polynomial $q(x) = p(x) - 1$, then $q(0) = 7$, $q(1) = 3$, and $q(2) = 5$. Thus, the three Musketeers actually gave Descartes three points on the polynomial $q(x)$ instead of on $p(x)$. So the value returned by Descartes will be exactly $q(3) = p(3) - 1$. To recover the secret, they therefore just need to add 1 to the value that Descartes gives back: $s = p(3) = q(3) + 1 = 3 \pmod{11}$. *3pts*

- *Many students used the $\Delta_i(x)$ values from the previous part, which violates the instructions in the question (because the Musketeers are not supposed to do interpolation). However, such solutions were given partial credit if the justifications and answer were correct.*
- *Some students provided a "graphic" interpretation for what the Musketeers did to the polynomial, i.e., shifting it down by 1. We gave full credit if the explanation was correct.*

(c) *A few years later, D'Artagnan has a new secret s' which is an integer in the range $0 \leq s' \leq 4$. Bored of hiding secrets in the usual way, he decides to hide it as the root of a polynomial q of degree 2 over $\mathrm{GF}(5)$. He then tells his men that q has only one root (so there is no confusion about the value of s', which is the only value that satisfies $q(s') = 0$). Suppose that $q = 4x^2 + x + 1$, and that he gives to Athos the coefficient of x^2 (which is 4), to Aramis the coefficient of x (which is 1), and to Porthos the constant term (which is 1). Athos and Aramis get together and decide to find s without Porthos. Can they succeed in this particular case? Justify your answer.*

Athos and Aramis know that $q(x) = 4x^2 + x + a$ for some a in the range $0 \leq a \leq 4$. Recall that, for every root r of $q(x)$, $(x - r)$ must divide $q(x)$. Thus, since $q(x)$ has degree 2 and only one root r, we must have $q(x) = c(x - r)^2$ for constants c and r. Comparing coefficients, we see that *4pts*

$$c = 4; \qquad -2rc = 1; \qquad cr^2 = a.$$

The first equation gives $c = 4$. Plugging this into the second equation gives $-8r = 1$, which solves to $r = (-8)^{-1} = 2^{-1} = 3 \pmod{5}$.

- *Many people who solved this part did so by "brute force". They enumerated all the possibilities for a, and found that only if $a = 1$ does $q(x)$ have a single root. They were then able to find this root easily. We subtracted a point for this as such an approach is inefficient (e.g., if the field were larger, this approach would require a lot of time).*
- *Some people plotted $q(x)$ and noted that the constant term was the "shift", and that only for one value of a did the polynomial cross the x-axis at exactly one point. Again, because this is also a brute force approach, we subtracted a point for this.*
