Midterm 1

7:00-9:00pm, 1 March

Your Name: **Your Section:**

Person on Your Left: **Person on Your Right:**

Instructions:

(a) *There are* **five** *questions on this midterm.*

(b) **Question 1** *consists of several parts, each requiring true/false, multiple choice, or very short answers. Indicate your answers in the space provided for each part; you do* **not** *need to show your working for Question 1.*

(c) *For* **Questions 2–5***, you should write your answer to each part in the space below it, using the back of the sheet to continue your answer if necessary. If you need more space, use the blank sheet at the end. In both cases, be sure to clearly label your answers!*

(d) **None of the questions requires a very long answer, so avoid writing too much! Unclear or long-winded solutions may be penalized.**

(e) *The approximate credit for each question part is shown in the margin (total 70 points). Points are not necessarily an indication of difficulty!*

For official use; please do not write below this line!

Q1	
Q2	
Q3	
Q4	
Q5	
Total	

[exam starts on next page]

1. [Multiple Choice/Short Answers]

Each of the following questions requires a very short answer: either True/False, or Multiple Choice, or a single number or expression. Except where otherwise indicated, write your answer in the **box** *provided. You do* **not** *need to show your working. Incorrect answers may receive negative scores, so if you are unsure of your answer leave it blank;* **do not guess***.*

(a) **[True or false?]** Mark each of the following "True" if it is a valid logical equivalence, and "False" otherwise. *3pts*

□ $P \Rightarrow Q \ \equiv \ P \vee \neg Q$

□ $P \Rightarrow Q \ \equiv \ (\neg P \Rightarrow \neg Q)$

□ $P \Rightarrow Q \ \equiv \ (Q \wedge P) \vee \neg P$

(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. *4pts*

□ Find an x such that $Q(x)$ is true or $P(x)$ is false.

□ Show that, for every x, if $Q(x)$ is false then $P(x)$ is false.

□ Assume that there exists an x such that $P(x)$ is false and $Q(x)$ is false and derive a contradiction.

□ Assume that there exists an x such that $P(x)$ is true and $Q(x)$ is false and derive a contradiction.

(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. *1pt*

□

[continued on next page]

(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*

- $(\exists a \in A)(\forall b \in B)(R(a) \vee \neg P(a, b))$
- $\neg(\forall a \in A)(\exists b \in B)(R(a) \Rightarrow P(a, b))$
- $(\exists a \in A)\neg(\exists b \in B)(\neg R(a) \vee P(a, b))$

(e) **[True or false?]** Recall that the principle of mathematical induction (over the natural numbers) asserts that, if $P(n)$ is a proposition concerning a natural number n, then the proposition *3pts*

$$P(0) \wedge \forall n(P(n) \Rightarrow P(n+1))$$

implies that $P(n)$ holds for all n.

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

□ $P(0) \wedge P(1) \wedge \forall n(P(n) \Rightarrow P(n+2))$

□ $P(0) \wedge P(1) \wedge (\forall n \geq 1)((P(n) \Rightarrow P(2n-1)) \wedge (P(n) \Rightarrow P(2n+1)))$

□ $P(0) \wedge P(1) \wedge \forall n_1 \forall n_2((P(n_1) \wedge P(n_2)) \Rightarrow P(n_1 + n_2))$

(f) **[True or false?]** Mark each of the two statements below "True" or "False". *2pts*

□ The set $\mathbb{R}$ of real numbers is well-ordered under the standard ordering.

□ $\mathbb{N}$ is well-ordered under the *even-odd ordering* $\preceq$, defined by $a \preceq b$ if and only if either

- a is even and b is odd; or
- a and b are both even or both odd, and $a \leq b$.

(g) **[Short answer]** *2pts*

□ What is the inverse of 8 mod 13?

□ Solve the equation $8x = 5 \bmod 13$.

[continued on next page]

(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 $e = 5$. *3pts*

□ What does Bob need to send to Alice (i.e., what is Bob's public key)?

□ What is Bob's private key?

□ Suppose Alice's credit card number is $x = 4$. What is the encrypted message $E(x)$?

(i) **[Multiple choice]** *4pts*

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

  0 1 2 3 q not determined

- 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

  0 1 2 4 q not determined

- The number of distinct polynomials of degree at most 2 over $GF(q)$ that pass through one given point $(0, y_0)$ is

  0 1 q q^2 ∞ not determined

- 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

  0 1 2 3 q ∞

[continued on next page]

2. [Induction]

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

[NOTE: Points will be deducted for over-long or overly complicated solutions. Keep your solution clear and concise! Be sure to clearly show the structure of your proof.]

[continued on next page]

3. [Stable Marriage]

Consider the following set of marriage preferences for four men 1, 2, 3, 4 and four women A, B, C, D.

Man	Women			
1	A	C	B	D
2	C	D	A	B
3	C	D	B	A
4	A	B	C	D

Woman	Men			
A	3	4	2	1
B	2	1	3	4
C	4	1	2	3
D	4	2	1	3

(a) Use the Propose-Reject algorithm to find a male-optimal pairing. Show your work. *4pts*

(b) Find the best (according to B) man that woman B can be paired with in any stable pairing. *4pts*

(c) Find a rogue couple for the following pairing: $\{(1,A), (2,D), (3,C)\ (4,B)\}$. *2pts*

[continued on next page]

4. Modular Arithmetic

(a) Compute $11^{13} \pmod{100}$ using repeated squaring. Show your intermediate results and write your $\boxed{\text{final answer}}$ in a box. *5pts*

(b) State Fermat's Little Theorem, and then use it to give a careful proof of the following claim. *5pts*
Claim: If p is prime and b, c are positive integers such that $b = c \bmod (p-1)$, then $a^b = a^c \bmod p$ for any integer a.

(c) Find $8^{(321^{49})} \pmod{11}$. Show your working and write your $\boxed{\text{final answer}}$ in a box. *3pts*
NOTE*: You should use part (b). It is possible to figure out this question in two lines. If you are doing a lot of calculations, you are probably on the wrong track. Write no more than five lines.*

[continued on next page]

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. *5pts*

[continued on next page]

(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. *3pts*

(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. *4pts*

[The End!]