Midterm 1

6:00-8:00pm, 5 March

Notes: There are **six** *questions on this midterm. Answer each question 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!* **None of the questions requires a very long answer, so avoid writing too much! Unclear or long-winded solutions may be penalized.** *The approximate credit for each question part is shown in the margin (total 60 points). Points are not necessarily an indication of difficulty!*

Your Name: **Your Section:**

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

Q1	
Q2	
Q3	
Q4	
Q5	
Q6	
Total	

[exam starts on next page]

1. Logic

In the following, $P(n)$ and $Q(n)$ denote propositions concerning the natural number n, and $R(m, n)$ denotes a proposition concerning natural numbers m and n. Each part asserts a logical equivalence $\mathcal{A} \equiv \mathcal{B}$. For each part, say whether the equivalence is valid or invalid. You do **not** need to justify your answers. **Note: Do not guess: incorrect answers will receive negative credit!**

(a) $\forall n(\neg Q(n) \Rightarrow P(n)) \equiv \neg[\exists n(\neg P(n) \wedge \neg Q(n))]$ *2pts*

(b) $\forall n(P(n) \Leftrightarrow Q(n)) \equiv \forall n[(P(n) \vee \neg P(n)) \wedge (Q(n) \vee \neg Q(n))]$ *2pts*

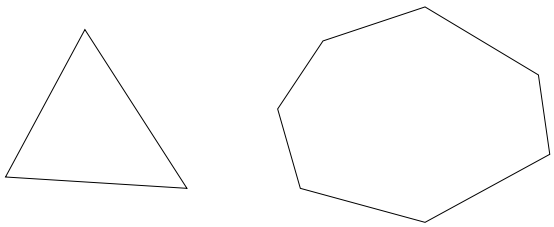
(c) $\forall m \forall n\ [R(m, n) \Rightarrow \neg(\forall l[R(m + l, n) \vee R(n, m + l)])] \equiv$
$\forall m \forall n\ [\neg R(m, n) \vee \exists l\ (\neg R(m + l, n) \wedge \neg R(n, m + l))]$ *2pts*

(d) $\forall n \exists m\ R(m, n) \equiv \exists m \forall n\ R(n, m)$ *2pts*

[continued on next page]

2. Induction

A *convex polygon* with n vertices is a closed shape defined by n non-intersecting line segments in the plane, such that any diagonal of the polygon (i.e., any line connecting two of its vertices, or corners) lies entirely inside the polygon. Below are examples of convex polygons for $n = 3$ and $n = 7$.



In this problem, you are asked to prove by induction that the sum of the interior angles of a convex polygon with n vertices is exactly $(n - 2)\pi$.

(a) State and prove the base case for the induction. *3pts*

(b) State and prove the inductive step, and thus complete the proof. *7pts*

[continued on next page]

3. [Stable Marriage]

Consider an input to the stable marriage problem consisting of four men A, B, C, D and four women a, b, c, d, with the following preference lists:

Men	Women			
A	a	d	b	c
B	b	d	c	a
C	d	c	a	b
D	d	a	b	c

Women	Men			
a	D	B	C	A
b	D	C	A	B
c	A	D	B	C
d	D	B	A	C

(a) Find a male-optimal stable pairing and a female-optimal stable pairing. *4pts*

(b) Does a stable pairing which is neither male optimal nor female optimal exist? If so, find one. *4pts*

[continued on next page]

4. [Modular Arithmetic]

1. Use the extended gcd algorithm to compute the inverse of 5 mod 48. Show your working clearly. *4pts*

---

2. Using part (a), solve the equation $5x + 7 = 20 \bmod 48$. Again, show your working. *4pts*

---

3. Does the equation $6x + 7 = 20 \bmod 48$ have a solution? Justify your answer.

4pts

[continued on next page]

5. [Divisibility Tests]

(a) Let n be any natural number and let s denote the sum of its digits. Prove that $n = s \bmod 3$. *5pts*

(b) Deduce from part (a) the following well-known test for divisibility by 3: *2pts*
"n is divisible by 3 if and only if the sum of its digits is divisible by 3".

(c) Can you give a test for divisibility by 9? Briefly justify your answer. *3pts*

[continued on next page]

6. [Secret sharing]

Suppose we wish to share a secret among five people, and we decide to work modulo 11. We construct a degree-two polynomial $p(x) = ax^2 + bx + s$ by picking the coefficients a and b at random (mod 11); the constant term is the secret s (also a number mod 11). We give shares $p(1), \ldots, p(5)$ to each of the five people (all operations being done mod 11). *7pts*

(a) Suppose that three of the people arrange a meeting and share the information that $p(1) = 9$, $p(2) = 5$ and $p(4) = 1$. What is the secret s? Use Lagrange interpolation and show your working; also be sure to check your answer!

(b) Suppose now that the first of these three people (the one holding the value of $p(1)$) wants to discover the secret herself but deceive the others into thinking that the value of the secret is larger by 1 than the true value s. Explain clearly how she can do this, assuming that the other two are honest. [HINT: You should not need to repeat the entire calculation from part (a).] *5pts*

[The end]