*CS70 Discrete Mathematics and Probability Theory, Spring 2010*

# Midterm 1

6:00-8:00pm, 4 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]**

(a) Consider the proposition *5pts*

$$\forall n(P(n) \Rightarrow Q(n)),$$

where $P$ and $Q$ are propositions indexed by the natural number $n$. Next to each of the following propositions, write "yes" if the proposition is equivalent to the above proposition, and "no" if it is not equivalent. (There is no need to justify your answers. **Warning:** Do not guess! Incorrect answers may receive negative scores.)

- $\forall n(Q(n) \Rightarrow P(n))$
- $\forall n(P(n) \vee \neg Q(n))$
- $\neg\exists n(P(n) \wedge \neg Q(n))$
- $\forall n(\neg P(n) \Rightarrow \neg Q(n))$
- $Q(0) \wedge \neg P(1) \wedge \forall n(Q(n) \Rightarrow Q(n+2)) \wedge \forall n(P(n+2) \Rightarrow P(n))$

---

(b) Consider the proposition *5pts*

$$\forall n \exists m R(m, n),$$

where $R$ is a proposition indexed by natural numbers $m, n$. Next to each of the following propositions, write "yes" if the proposition is equivalent to the above proposition, and "no" if it is not equivalent. (There is no need to justify your answers. **Warning:** Do not guess! Incorrect answers may receive negative scores.)

- $\exists m \forall n R(m, n)$
- $\forall m \exists n R(n, m)$
- $\forall m \exists n R(m, n)$
- $\neg\exists n \forall m(\neg R(m, n))$
- $\forall n \exists m(R(n+m, n) \vee R(n-m, n))$

---

**[continued on next page]**

**2. [Induction]**

Prove by induction that, for every natural number $n \geq 1$, *10pts*

$$\sum_{i=1}^{n} (3i)^2 = \frac{3}{2} n(n+1)(2n+1).$$

[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 marriages]**

Consider an instance of the Stable Marriage Problem in which the men are $\{1, 2, 3, 4\}$, the women are $\{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}\}$, and the preference lists are:

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

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

Answer the following questions about the above instance.

(a) Run the Propose-and-Reject Algorithm to find a stable pairing. Clearly show the steps performed by the algorithm, as well as the final pairing. *6pts*

(b) Using your solution to part (a) and results from class, give a one-sentence proof that there is no stable pairing in which Man $4$ is matched with Woman D. *2pts*

(c) Using your solution to part (a) and results from class, give a one-sentence proof that there is no stable pairing in which Man $3$ is matched with Woman B. *2pts*

**[continued on next page]**

**4. [Modular arithmetic]**

In the 1960's, three mathematicians showed that there was a positive integer $n$ satisfying

$$133^5 + 110^5 + 84^5 + 27^5 = n^5,$$

disproving a longstanding conjecture (originally due to Euler). In this problem we will find such an integer $n$.

(a) What is $n \bmod 2$? Give a one-sentence justification. *2pts*

---

(b) What is $n \bmod 3$? Show your working. Do **not** use a calculator. *4pts*

---

(c) What is $n \bmod 5$? Show your working. Do **not** use a calculator. [HINT: It may be helpful to use Fermat's Little Theorem.] *4pts*

---

(d) It is easy to show that $n < 170$. Given this information, find $n$. *3pts*

---

**[continued on next page]**

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

Given a prime $p$ and an integer $a \neq 0 \bmod p$, the *order* of $a$ modulo $p$, written $\mathrm{ord}_p(a)$, is defined as the least $i \geq 1$ such that

$$a^i = 1 \bmod p.$$

(a) Use Fermat's Little Theorem to deduce that $\mathrm{ord}_p(a) \leq p - 1$ for all $a \neq 0$. *2pts*

---

(b) Prove that, for all $a \neq 0$, $ord_p(a)$ divides $p-1$. [HINT: You may want to try a proof by contradiction.] *5pts*

---

**[continued on next page]**

**6. [Secret Sharing]**

After a long and illustrious career as a buccaneer, Captain Flint passed away in the year 1754. He had split the gold accumulated over years of terrorizing ships into two batches, and just before his death he told his five faithful pirates the locations of the the two batches using a secret sharing scheme.

The captain chose polynomials $P(x)$ and $Q(x)$ over $GF(7)$, of degrees 1 and 2 respectively, with the secrets being the values $P(0)$ and $Q(0)$. For $1 \leq i \leq 5$, Pirate $i$ received the two numbers $P(i)$ and $Q(i)$, but was not told which was which. The pirates cursed the Captain as they could not figure out how to recover the secrets, and the treasure lay undiscovered for many years.

On the eve of the 10th anniversary of the Captain's demise, the pirates captured a small vessel and encountered Monsieur Lagrange (who, having forsaken the ennui of land-life in favor of the vicissitudes of the life on the high seas, was himself an aspiring pirate). Lagrange offered his mathematical prowess in solving the pirates' problems, in exchange for a share of the treasure.

The secret shares received by the five pirates were $\{0, 5\}, \{1, 4\}, \{3, 4\}, \{0, 4\}$ and $\{0, 3\}$ respectively. (So, for example, Pirate 2's share was $\{1, 4\}$, meaning that either $P(2) = 1$ and $Q(2) = 4$, or $P(2) = 4$ and $Q(4) = 1$.) Trace the following steps to see how M. Lagrange helped the pirates to solve the mystery.

(a) Find $P(0) + Q(0)$. *4pts*

**[continued on next page]**

(b) Find $P(0)Q(0)$. *4pts*

(c) Using parts (a) and (b), find the two secrets $P(0)$ and $Q(0)$ that were hidden by Captain Flint, assuming that $P(0) < Q(0)$. *2pts*

**[The End!]**