RYERSON UNIVERSITY

DEPARTMENT
OF
MATHEMATICS

MTH 210	**Final Exam**	**April 20, 2009**
Total marks: 70		**Time allowed: 3 hrs.**

NAME (Print): ______________________ **STUDENT #:** ______________

SIGNATURE ______________________________

Circle your Lab Section:

011	021	031
VIC 200	VIC 205	VIC 608

Instructions:

- Verify that your paper contains 8 questions on 7 pages.
- You are allowed an $8\frac{1}{2} \times 11$ formula sheet written on both sides.
- No other aids allowed. Electronic devices such as calculators, cellphones, pagers and ipods must be turned off and kept inaccessible during the test.
- Please keep your Ryerson photo ID card displayed on your desk during the test.
- In every question show all your work. The correct answer alone may be worth nothing.
- Delete all irrelevant and incorrect work because marks may be deducted for work which is misleading, irrelevant or incorrect, even if steps for a correct solution are also shown.
- Please write only in this booklet. Use of scrap paper or additional enclosures is not allowed. If you need more space continue on the back of the page, directing marker where the answer continues with a bold sign.

8 Mk

1. Show that $2^x \geq x^2$ for every $x \geq 4,\ x \in \mathbb{N}$.
   (You may assume $r^2 \geq 2r + 1$ for every $r > 2$.)

2. Let $G = (V, E)$ be a graph of order n.

5 Mk

(a) Suppose that there is a vertex $x \in V$, where the degree of x is d and $d \geq n$, use the pigeonhole principle to show that G is not simple.

5 Mk

(b) Show that if G is simple and every vertex $x \in V$ has degree $n - 1$, then $G \cong K_n$

6 Mk

3. For this question L_1 and L_2 are regular languages, while the languages L_3 and L_4 are not regular. For each of the following indicate whether they are **Regular**, **Not Regular**, or **Unknown** by circling your answer. Here, **Unknown** means that there is not enough information to determine whether the language is regular or not.

(a) $L_1 \cup L_2$ **Regular** **Not Regular** **Unknown**

(b) $L_1 \cap L_2$ **Regular** **Not Regular** **Unknown**

(c) $L_1 \cup L_3$ **Regular** **Not Regular** **Unknown**

(d) $L_3 \cup L_4$ **Regular** **Not Regular** **Unknown**

(e) L_3^c **Regular** **Not Regular** **Unknown**

(f) L_1^c **Regular** **Not Regular** **Unknown**

4. For this question let

$$L = \{w \in \{a, b\}^* \mid w \text{ has no pair of consecutive } a\text{'s } \}$$

4 Mk

(a) Find a regular expression for L.

4 Mk

(b) Give the state diagram of an FSA that recognizes L.

8 Mk

5. Let L be the language over $\{a, b\}^*$, defined by having the same number of a's as b's. i.e.

$$L = \{w \in \{a, b\}^* \mid |w|_a = |w|_b\}$$

(Recall $|x|_a$ is the number of a's in the string x, and $|x|_b$ is the number of b's.)

Use the pumping Lemma to show that L is not regular.

6 Mk

6. Find x when $3x^2 + 1 \equiv 0 \pmod 7$. Your answer should be an integer between 0 and 6. (Be sure to show all your working.)

7. Suppose that we are using the RSA cipher with primes $p = 7$ and $q = 11$.
(In this question you **must** use the fastpower algorithm whenever you need to find powers and the gcd method to find multiplicative inverses mod n.)

4 Mk (a) Determine whether $e = 33$ is a valid key. (Be sure to show all your working.)

6 Mk (b) Given that our encryption key is $e = 43$, find the corresponding decryption key d. (Be sure to show all your working.)

6 Mk (c) Suppose that we have the decription key $d = 17$ and receive the ciphertext $C = 2$, find the original message x.

8 Mk 8. (a) How many four digit hexadecimal numbers can be formed using the hexadecimal digits 1, 5, 6, 9, A, C? (Note repetition is allowed, so 15AC, 1115, 15AA, etc. are all allowed.)

(b) How many four digit hexadecimal numbers with distinct digits can be formed using the hexadecimal digits 1, 5, 6, 9, A, C?

(c) What is the probability that a randomly chosen four digit hexadecimal numbers will have distinct digits?

(d) What is the probability a four digit hexadecimal number formed using the hex digits 1, 5, 6, 9, A, C chosen at random will be less than A15C? (Show your working.)