CMPUT 272 Fall 2007 Prof. Hayward Final Exam VERSION B

6 pages 3 hours 40 marks

no electronic devices write answers in the space provided

1. [2 marks]

   (i) Give the base 9 representation of 21011201_3.

   (ii) Give the base 11 representation of 1000_{10}; show your work.

2. [5 marks] Consider a 9-bit two's complement register.

   (i) What is the greatest integer that can be stored? Give both the decimal and two's complement representations.

   (ii) What is the least integer that can be stored? Give both representations.

   (iii) Give the decimal representation of the number x represented by 1 0 0 0 0 1 0 1 1.

   (iv) Give the two's complement representation of decimal 93.

   (v) Show the register contents after the operation "x - 93", where x is from (iii).

   (vi) Is the result of this operation valid? Explain briefly.

3. [2 marks] $P(\ )$ is a predicate defined on integers. N is the set of nonnegative integers. R is the statement $\forall n \in N, \exists m \geq n, P(m)$.

   (i) In a form ending in $\sim P(m)$, give the negation of R.

   (ii) Does R imply that $P(\ )$ is satisfied by an infinite number of integers? Explain carefully.

4. [5 marks] Recall the algebraic rules for sets: (C) commutative, (As) associative, (D) distributive, (I) idempotent, (NN) double negation, (DeM) DeMorgan, (Ab) absorption.

   (i) For sets A, B, C, give a simplified expression for $(A - B) - (B - C)$.

   (ii) Give an algebraic proof that your answer to (i) is correct. For each step, give the rule being used. (**If you cannot give an algebraic proof**: for part marks, give some other proof.)

5. [3 marks] Let $g = \gcd(13,20)$.

   (i) Use Euclid's algorithm to find g.

   (ii) Find integers x, y such that $13x + 20y = g$.

   (iii) Find an integer t in $\{0, 1, \ldots 19\}$ such that $13t = g \bmod 20$.

6. [4 marks] Alice uses the RSA protocol. She publishes $n = 33$ and $e = 13$.

   (i) Can Bob send Alice the message 15? Explain (and if yes, give an arithmetic expression describing the ciphertext number Bob sends).

   (ii) Can Bob send Alice the message 26? Explain (and if yes, give an arithmetic expression describing the ciphertext number Bob sends).

   (iii) An eavesdropper observes Kim sending Alice the ciphertext number 2. Find the exact plaintext message (as an integer) Kim sent; show your work.

7. [3 marks] S is the set of subsets of $\{a, b, c, d\}$. R is the subset relation on S.

   (i) Is R an equivalence relation? If no, explain; if yes, group the elements of S into equivalence classes.

   (ii) Is R an order relation? If no, explain; if yes, draw the Hasse diagram.

8. [4 marks] Prove by induction: for all non-negative integers j, $10^j = 1 \bmod 3$.

   (i) Base case.

   (ii) Inductive hypothesis.

   (iii) Rest of proof.

9. [3 marks] $S(n,k)$ is the number of k-partitions of an n-set.

   (i) List all 3-partitions of $\{p,q,r,s\}$.

   (ii) Explain why $S(n,k) = S(n-1,k-1) + kS(n-1,k)$.

10. [4 marks] A set of integers is 3-*sum* if it has 3 different subsets whose entries have the same respective sum. For example, $\{1,2,3,4,5,6\}$ is 3-sum, since the 3 subsets $\{1,5\}$, $\{2,4\}$, $\{6\}$ each have sum 6.

    Prove or disprove: each 8-subset of $\{1,2,\ldots,10\}$ is 3-sum.

11. [5 marks] For the Sudoku puzzle below, (i) write in the value of each dotted cell, and then (ii) write in the possible values of the other empty cells. (iii) Can cell [9,7] be 9? Justify carefully.

1	6			3		8	5	
4	3	9	.	.	8	6	.	7
5	8					1	3	
3	2	1	5		6		7	8
.	.	8		1		3		5
9	4	.	3	8	7	2	1	6
8	9	3			.	7		1
7	1		.		3	5		2
2	5			7	1		8	3

(iv) Complete the puzzle.

1	6			3		8	5	
4	3	9			8	6		7
5	8					1	3	
3	2	1	5		6		7	8
		8		1		3		5
9	4		3	8	7	2	1	6
8	9	3				7		1
7	1				3	5		2
2	5			7	1		8	3

END OF EXAM