**ICS 161 — Algorithms — Winter 2005 — First Midterm**

Please answer the following six questions on the answer sheets provided. Answers written on other pages or on the wrong sheet will not be scored. Be sure to write your name and student ID on all three answer sheets. You may continue your answers on the back of the same answer sheet. No books, notes, or calculators may be used during the exam.

1. (15 points) Define what it means for a sorting algorithm to be stable.

2. (30 points) Suppose you wish to sort a sequence of 1000 numbers, each of which is an RSA encryption key with 300 decimal digits. How many rounds would be needed to sort them using radix sort, if each round involves bucket sorting with 1000 buckets? Would radix sorting be a better choice for this application than a general purpose comparison sorting routine? Why or why not?

3. (15 points) Use the master method to solve the recurrence $X(n) = 9X(n/3) + n^2 \log n$. Use $O$-notation, and explain which case of the master method this recurrence falls into.

4. (20 points) Draw a decision tree that finds the median of three numbers $p$, $q$, and $r$. What is the worst-case number of comparisons performed by your tree?

5. (30 points) Consider the following algorithm for printing out the *n*-digit decimal representation of an integer *x*:

```
void decimal(x,n)
{
    if (n > 1) decimal(x/10, n-1);
    putchar('0' + x%10);
}
```

(a) Analyze the running time of this algorithm, as a function of *n*, using *O*-notation. You may assume that *x* has at most *n* digits, and that each division and modulus by 10 operation may be performed in time $O(n)$, faster than general-purpose division and modulus operations. Do not assume that division and modulus are constant-time operations.

(b) Design a more efficient divide-and-conquer algorithm for the same problem. (Hint: start by division and modulus with a higher power of ten.)

(c) Write down a recurrence describing the running time of the algorithm for your answer to part (b), assuming that any multiplication, division, and modulus steps it performs are done using the Karatsuba multiplication algorithm.

6. (10 points, multiple choice) Which one of the following problems was recently shown to be solvable in polynomial time by a team of Indian undergraduates?

- Finding the prime factors of a composite number
- Testing whether a number is prime
- Multiplying two large prime numbers
- Exponentiation modulo a prime number
- Computing discrete logarithms modulo a composite number
- Breaking the RSA cryptosystem

**ICS 161 W05 — Answer Sheet 1**

Name:

Student ID:

Please answer question 1 in the space below.

Please answer question 2 in the space below.

1: 2: 3: 4: 5: 6: total:

**ICS 161 W05 — Answer Sheet 2**

Name:

Student ID:

Please answer question 3 in the space below.

Please answer question 4 in the space below.

**ICS 161 W05 — Answer Sheet 3**

Name:

Student ID:

Please answer question 5 in the space below.

Please answer question 6 in the space below.