Algorithms – CS-27200/37000 Homework – February 14, 2005

Instructor: László Babai Ry-164 e-mail: laci@cs.uchicago.edu

TA SCHEDULE: TA sessions are held in Ryerson-255, Tuesday and Thursday 5–6pm, Saturday 11am–noon, and (this is new) **Wednesday after class** 12:30–1:20 or 1:30–2:20 depending on demand. Indicate your interest in the Wednesday session to the instructor immediately after class. (The Wednesday evening sessions are discontinued.)

ADVICE. Take advantage of the TA sessions.

Check the class website, http://www.classes.cs.uchicago.edu/current/27200-1.

HOMEWORK. Please **print your name on each sheet.** Print "U" next to your name if you seek 27200 credit and "G" if you seek 37000 credit. Undergraduates receive the stated number of points as *bonus points* for "G only" problems. – Please try to make your solutions readable. Unless expressly stated otherwise, all solutions are due at the **beginning of the next class.**

REVIEW: number theory: greatest common divisor, Euclid's algorithm, congruences, Fermat's Little Theorem, Chinese Remainder Theorem.

DATES TO REMEMBER: Mon Feb 21: Quiz 2, Mon Mar 7: Midterm 2, Fri Mar 11: Last class. ATTENDANCE REQUIRED. Fri Mar 18, 10:30–12:30: Final Exam

13.1 (3 points each) Recall that x is a multiplicative inverse of t mod m if $tx \equiv 1 \pmod{m}$. The notation $x = (t^{-1} \pmod{m})$ refers to the value of the multiplicative inverse between 0 and $m-1$. (m is a positive integer, t, x are integers.) Calculate the following multiplicative inverses (give the result as an integer between 0 and the modulus minus 1) or prove that they do not exist. Show all your work.

(a) $15^{-1} \pmod{70}$; (b) $15^{-1} \pmod{71}$; (c) $15^{-1} \pmod{72}$.

13.2 (8 points) Suppose we have n coins of k different weights. Sort the coins by weight using $O(n \log k)$ steps using pairwise comparisons. (Steps are comparisons, moving coins, bookkeeping). The value of k is *not* known in advance. *Hint.* Use a dynamic data structure. Elegance counts.

13.3 (3+8 points, due Friday) Two parties, Alice and Bob, use the following cryptosystem in their confidential communication over a public channel. They first agree on a large prime number p. The message (plaintext) Alice wants to send to Bob is an integer m, where $1 \le m \le p-1$. Next, Alice privately selects an integer x ($1 \le x \le p-1$) and keeps it secret. Similarly, Bob privately selects an integer y ($1 \le y \le p-1$) and keeps it secret. Now Alice sends the value $a := (mx \bmod p)$ to Bob; then Bob sends $b := (ay \bmod p)$ to Alice; finally, Alice sends

$c := (bx^{-1} \bmod p)$ to Bob. (a) Show how Bob can find out in polynomial time what the message m is. (b) Assume that Chuck, the eavesdropper, monitors the communication and gets each of the numbers p, a, b, c. Show how Chuck can compute the message m in polynomial time. (So this cryptosystem is not secure.) Perform Chuck's calculations with the following data: $p = 71$, $a = 29$, $b = 15$, $c = 61$. Show all your work.