Algorithms – CS-37000 Homework 8 – Feb 19, 2006

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

ADVICE. Take advantage of the TA's problem sessions. This is the **principal venue to discuss past homework and test problems.** Note that such problems may prop up in future tests.

READING. Review from Discrete Math: number theory (congruences, Fermat's Little Theorem, Chinese Remainder Theorem). Markov Chains. Finite Probability Spaces. - Handout: The method of reverse inequalities.

Review all previous handouts and readings.

HOMEWORK. Please **print your name on each sheet.** Put each solution on a separate sheet. Please try to make your solutions easily readable.

This homework is due on **Tuesday, February 21** at the **beginning of the class**.

Change of schedule. There will be no quizzes on Feb 21 and 28; instead, there will be a 40-minute **midterm on Thursday, Feb 23.**

8.1 (7 points) (The RSA public key cryptosystem) Suppose Alice carelessly reveals the number M to Eve. Show that Eve can now factor N in polynomial time. (Recall: $N = pq$ and $M = (p-1)(q-1)$, where p and q are distinct n-digit primes.) Analyse the running time of your algorithm in terms of n.

8.2 (7 points) (Method of reverse inequalities.) An important "divide and conquer" algorithm leads to the recurrent inequality

$$T(n) \leq T(\lfloor n/5 \rfloor) + T(\lfloor 7n/10 \rfloor) + O(n).$$

Asymptotically evaluate $T(n)$. (Does it follow from this inequality that $T(n) = O(n)$? Or $T(n) = O(n \log n)$? Or $T(n) = O(n^\alpha)$ for some $\alpha > 1$? Find the strongest possible conclusion.)

8.3 (8 points) Given two n-digit integers k and m, compute ($F_k \pmod{m}$) (the k-th Fibonacci number modulo m) in polynomial time ($O(n^c)$). - *Hint.* Study the powers of the matrix $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$.