Discrete Mathematics – CMSC-37110-1 Homework 6 – October 13, 2005

Instructor: László Babai Ry-164 e-mail: laci[at]cs[dot]uchicago[dot]edu

HOMEWORK. Please print your name on each sheet. Please try to make your solutions readable. Unless expressly stated otherwise, all solutions are due at the **beginning of the next class.** Please write solutions to challenge problems on a separate sheet.

READ: mathematical induction.

Recall the definition of divisibility: a divides b (notation: $a \mid b$) if $(\exists x)(ax = b)$. (All variables are integers.)

DO6.1 Prove: If $t \mid a$ and $t \mid b$, then $t \mid$ all linear combinations of a and b. (In our context, a linear combination of a and b is a number of the form $au + bv$ where u, v are integers.)

DO6.2 *(Transitivity of divisibility)* Prove: If $a \mid b$ and $b \mid c$ then $a \mid c$.

DO6.3 Prove: If $a \mid b$ and $b \mid a$ then $a = \pm b$.

Notation. $\text{Div}(a)$ denotes the set of divisors of the integer a. For instance, $\text{Div}(-6) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Note that $\text{Div}(0) = \mathbb{Z}$.

Recall the two definitions of g.c.d.:

Definition 1. $\gcd(a, b) = c$ if $\text{Div}(a) \cap \text{Div}(b) = \text{Div}(c)$.

Definition 2. $\gcd(a, b) = c$ if

1. $c \mid a$ and $c \mid b$ (c is a common divisor of a and b);
2. $(\forall x)($ if $x \mid a$ and $x \mid b$ then $x \mid c)$. (c is a multiple of all common divisors.)

DO6.4 Prove that the two definitions are equivalent.

DO6.5 (a) Prove that the ratio of a diagonal to a side of a regular pentagon is the golden ratio, $(1 + \sqrt{5})/2 \approx 1.618$. (b) Prove that two diagonals of a regular pentagon divide each other in proportion of the golden ratio.

Homework (due at the beginning of the next class):

HW6.1 (8 points) Let $d(n)$ denote the number of positive divisors of the positive integer n. Prove: $d(n) < 2\sqrt{n}$. (The proof should be very simple; requires one idea.)

HW6.2 (4 points) Prove that if $x \equiv y \pmod{m}$, then $x^2 \equiv y^2 \pmod{m}$.

HW6.3 (5 points) Prove: $\gcd(F_n, F_{n+1}) = 1$ (consecutive Fibonacci numbers are relatively prime.) (Hint: induction.)

HW6.4 (6 points) Determine the quantity $F_n^2 - F_{n+1}F_{n-1}$. Experiment. Conjecture. Prove.

HW6.5 (8 points) Prove: If a, b are $\leq n$-bit integers in binary, then Euclid's Algorithm takes $\leq 2n$ rounds to compute $\gcd(a, b)$.

HW6.6 (4 points) Recall **Fermat's little Theorem:** If p is a prime number and p does not divide the integer a then $a^{p-1} \equiv 1 \pmod{p}$. Calculate $2^{1000} \pmod{7}$. Your answer should be an integer x such that $2^{1000} \equiv x \pmod{7}$ and $0 \leq x \leq 6$.