Institut für Mathematische Optimierung
TU Braunschweig

WS 2005/2006

Prof. Dr. Sándor Fekete
Nils Schweer

Discrete Mathematics I
Assignment 6 (December 07, 2005)

(This assignment is due on December 14, 2005, 1.00 p.m., by dropping it into the wooden box **in front of** F 310)

Exercise 1 (Modular arithmetic):

Show that if $n|m$, where n and m are positive integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$

(20 Points)

Exercise 2 (Pseudorandom numbers):

What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 1) \mod 7$ with seed $x_0 = 3$?

(20 Points)

Exercise 3 (Systems of linear congruences):

a) Find an $x \neq 8$ that satisfies $x \equiv 2 \pmod{3}$ AND $x \equiv 3 \pmod{5}$.

b) Find an x that satisfies $x \equiv 7 \pmod{4}$, $x \equiv 2 \pmod{3}$ AND $x \equiv 5 \pmod{11}$.

(8+12 Points)