Discrete Mathematics

Assignment 6

Date Due: 8:00 PM, Thursday, the 29th of June 2011

Office hours: Tuesdays, 1:00-3:00 PM, and Wednesdays, 12:00-1:00 PM

Exercise 1. The goal of this exercise is to prove the uniqueness of the solution in the Chinese Remainder Theorem. Consequently, you may not use the Chinese Remainder Theorem in the following parts.

i) Let $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0, 1\}$ be pairwise relatively prime and $a, b \in \mathbb{Z}$. Show that if $a \equiv b \mod m_i$ for $i = 1, \ldots, n$, then $a \equiv b \mod m$, where $m = \prod_{i=1}^{n} m_i$.

ii) Show that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime integers is unique modulo the product of these moduli. *Hint:* Let x, y be two simultaneous solutions. Show that $m_i \mid (x - y)$ for all i. Then apply i) above.

(3+2 Marks)

Exercise 2. Let $m_1, \ldots, m_n \in \mathbb{N} \setminus \{0, 1\}$ be pairwise relatively prime, $m = \prod_{i=1}^{n} m_i$ and $a \in \mathbb{Z}$ with $0 \leq a < m$. Use the Chinese Remainder Theorem to show that a is uniquely determined by the n-tuple $(a \bmod m_1, \ldots, a \bmod m_n)$.
(1 Mark)

Exercise 3. This exercise outlines a proof of Fermat's Little Theorem

i) Suppose that a is not divisible by the prime p. Show that no two of the integers $1 \cdot a$, $2 \cdot a, \ldots, (p-1)a$ are congruent modulo p.

ii) Conclude that the product of $1, 2, \ldots, p-1$ is congruent modulo p to the product of $a, 2a, \ldots, (p-1)a$. Use this to show that

$$(p-1)! \equiv a^{p-1}(p-1)! \mod p.$$

iii) Use Corollary 2.1.42 of the lecture to show from ii) that $a^{p-1} \equiv 1 \mod p$ if $p \nmid a$.

iv) Use iii) to show that $a^p \equiv a \mod p$ for all $a \in \mathbb{Z}$.

(2+2+2+1 Marks)

Exercise 4. Use Fermat's Little Theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$ and $5^{2003} \bmod 13$. Then use the Chinese Remainder Theorem to compute $5^{2003} \bmod 1001$ (note that $1001 = 7 \cdot 11 \cdot 13$).
(2 Marks)

Exercise 5. Let M, N be finite sets with $\operatorname{card} M = \operatorname{card} N$ and $M \subset N$. Prove that $M = N$.
(2 Marks)

Exercise 6. Use the Pigeonhole Principle or Theorem 2.2.16 of the lecture to prove the following theorem:

Let M, N be finite sets with $\operatorname{card} M > \operatorname{card} N$ and $f \colon M \to N$. Then f is not injective.

(2 Marks)

Exercise 7. In this exercise, $R(m, n)$ denotes the Ramsey number and we assume that in a group of people, any two people are either friends or enemies.

i) Show that in a group of five people there are not necessarily either three mutual enemies or three mutual friends.

ii) Show that in a group of 10 people there are either three mutual friends or four mutual enemies, and there are either three mutual enemies or four mutual friends.

iii) Use ii) to show that among any group of 20 people there are either four mutual friends or four mutual enemies.

iv) Show that $R(2, n) = n$ for $n \in \mathbb{N}$, $n \geq 2$.

v) Show that $R(m, n) = R(n, m)$ for $m, n \in \mathbb{N}$, $m, n \geq 2$.

(2+2+2+1+1 Marks)

Exercise 8. Prove that at a party where there are at least two people, there are two people who know the same number of other people there.
(3 Marks)