Discrete Mathematics

Assignment 5

Date Due: 8:00 PM, Thursday, the 23rd of June 2011

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

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

Exercise 2. Find the following using the algorithm for modular exponentiation given in the lecture. Show all the steps in the algorithm.

$$11^{644} \bmod 645, \qquad 123^{1001} \bmod 101, \qquad 3^{2003} \bmod 99$$

(1+1+1 Marks)

Exercise 3. Find the following using the Euclidean Algorithm. Show all the steps in the algorithm.

$$\gcd(1529, 14039), \qquad \gcd(1111, 11111), \qquad \gcd(9888, 6060)$$

(1+1+1 Marks)

Exercise 4. All books are identified by an *International Standard Book Number* (ISBN), a 10-digit code $x_1x_2\dots x_{10}$ assigned by the publisher. (The 10-digit code was used until 2007, when it was replaced by a 13-digit code.) These 10 digits consist of blocks identifying the language, the pub;isher, the number assigned to the book by the publishing company and, finally, a 1-digit check digit that is either a digit or the letter X (used to represent 10). This check digit is selected so that $\sum_{i=1}^{10} ix_i \equiv 0 \mod 11$ and is used to detect errors in individual digits and transposition of digits.

i) The first nine digits of the ISBN of the european version of the fifth edition of Rosen's book are 0-07-119881. What is the check digit for this book?

ii) The ISBN of the fifth edition of *Elementary Number Theory and its Applications* is 0-32-123Q072, where Q is a digit. Find the value of Q.

iii) Check whether the check digit in the ISBN-10 number for the edition of Rosen's book that you are using is correct.

(1+1+1 Marks)

Exercise 5. Adapt the proof that there are infinitely many primes to show that there are infinitely many primes of the form $4k + 3$, where k is an integer. *Hint*: suppose that there are only finitely many such primes, $q_1, \dots, q_n$ and consider $4q_1q_2\dots q_n - 1$.
(3 Marks)

Exercise 6. We call a positive integer *perfect* if it equals the sum of its positive divisors other than itself.

i) Show that 6 and 28 are perfect.

ii) Show that $2^{p-1}(2^p - 1)$ is perfect when $2^p - 1$ is prime.

iii) *Mersenne primes* are prime number of the form $2^p - 1$. Which of the following are Mersenne primes?

$$2^7 - 1, \qquad 2^9 - 1, \qquad 2^{11} - 1, \qquad 2^{13} - 1.$$

(1+3+2 Marks)

Exercise 7. The sums of the digits of numbers can be used to obtain a variety of results about the numbers:

i) Show that a positive integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3.

ii) Show that a positive integer is divisible by 11 if and only if the difference of the sum of its decimal digits in even-numbered positions and and the sum of its decimal digits in odd-numbered positions is divisible by 11.

iii) Show that a positive integer is divisible by 3 if and only if the difference of the sum of its binary digits in even-numbered positions and and the sum of its binary digits in odd-numbered positions is divisible by 3.

(2+2+2 Marks)

Exercise 8. The well-ordering property can be used to show that there is a unique greatest common divisor of two positive integers. Let $a, b \in \mathbb{Z}_+$ and efine $S := \{n \in \mathbb{N}\colon \underset{s,t\in\mathbb{Z}}{\exists}\ n = sa + tb\}$.

i) Show that $S \neq \emptyset$ and conclude that there exists a least element $c \in S$.

ii) Show that if $d \in \mathbb{Z}_+$ is a common divisor of a and b, then d is a commonsivisor of c.

iii) Show that $c \mid a$ and $c \mid b$. *Hint:* First, assume that $c \nmid a$. Then $a = qc + r$, $0 < r < c$. Show that $r \in S$, contradicting the choice of c.

iv) Conclude that $\gcd(a, b)$ exists and has the form $\gcd(a, b) = sa + tb$ for some $s, t \in \mathbb{Z}$.

(1+2+2+2 Marks)

Exercise 9. Let $p \in \mathbb{N} \setminus \{0, 1\}$ be a prime number and $a_1, \dots, a_n \in \mathbb{Z}$. Use mathematical induction to prove that if $p \mid a_1 a_2 \dots a_n$ then $p \mid a_i$ for some a_i.
(3 Marks)

Exercise 10. Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.
(3 Marks)