CZ3106 Symbolic Computing, Lab 5

Dr. Wang Jian-Sheng For the week 17-22 March 03, due 5 Apr 03

This is the last set of lab problems worth 15 marks

1. Based on your program for testing group, write a program for testing a finite field. The field testing program will accept two tables, one for $+$ and one for $*$, and testing that addition is an Abelian group and $F - \{0\}$ is an Abelian group with respect to multiplication. Additionally, testing that multiplication is distributive over addition. Use $(Z_4; +, *)$ and $(Z_5; +, *)$ as input examples.

2. Consider the set of all polynomials with coefficients in Z_3 modulo $1+x^2$. Addition and multiplication are defined in the usual way but modulo $1+x^2$. The arithmetic of the coefficients are in Z_3. Work out the rules for addition and multiplications.

(a) Generate the addition and multiplication tables, and verify by your above program that it is a field. This is an example of a Galois field GF(3,2) with 9 elements.

(b) Compute the multiplicative inverse by extended Euclidean algorithm for all the nonzero elements, and show that it is the same as given in (read from) the table. Use built-in function `PolynomialExtendedGCD[]`, or other built-ins for your computation.

3. Implement the Gardner's algorithm for the Chinese remainder problem. See page 174 to 180 of "Algorithm for Computer Algebra," Geddes et al, for more details. Please do read these pages before attempting the lab.

The Chinese remainder problem is the following: given a set of pairwise relative primes, $m_i \in$ Z, with GCD$(m_i, m_j) = 1$ for $i \neq j$, find u such that $u_i = u \bmod m_i$, for $i = 0$ to n, for a given set of u_i. The Garner's algorithm relies on the representation

$$u = \nu_0 + \nu_1(m_0) + \nu_2(m_0 m_1) + \cdots + \nu_n(\prod_{i=0}^{n-1} m_i).$$

We determine ν_0 first, then ν_1, and so on. u is unique modulo $\prod_{i=0}^{n} m_i$. Program in Mathematica. Here is an example, $u \bmod 7 = 2$, $u \bmod 11 = -5$, $u \bmod 13 = -2$, $u \bmod 17 = 5$, $u \bmod 19 = 9$, then it is found by the Gardner algorithm $u = -44280$.