MACM 498/CMPT 881/MATH 800
Assignment 4, Fall 2004

Michael Monagan

This assignment is to be handed in on Tuesday November 9th at the beginning of class.
Late penalty: 10% off for each day late.

Chapter 5 exercises 5.17, 5.29.
Chapter 6 exercises 6.1, 6.3, 6.6, 6.9, 6.11, 6.12.

For exercise 5.17 give an example to illustrate how you compute x from y_1, y_2 and y_3.

For exercise 6.1 use the `sort` command in Maple.
Maple is using mergesort which is $O(n \log n)$ in the worst case.

For exercise 6.12 you may use Maple do to all arithmetic.

For exercise 6.11 part (b) first use the `Gcdex(...) mod p` command in Maple to compute the inverse then program the half-extended Euclidean algorithm in Maple to compute the inverse. Note: Algorithm 5.3: Multiplicative Inverse on page 161 has a mistake in it; it is returning the wrong t value. For part (c) use the `Powmod(...) mod p` command to compute x^{25} then program the square and multiply algorithm to compute x^{25}. For both parts use the `Expand(...) mod p`, `Rem(...) mod p` and `Quo(...) mod p` commands to multiply and divide in $\mathbb{Z}_p[x]$.

Additonal exercises:

1: Suppose Bob is using the Rabin cryptosystem with $p = 103$, $q = 107$ hence $n = 11021$. Suppose Alice computes $y = x^2 \bmod n$ and sends y to Bob. If $y = 10990$ what are the four possible values x can be?

2: CMPT 881 and MATH 800 students should also do exercise 5.34. Also implement algorithm 5.13 on page 210 and test it on the authors' data and generate the numbers in Figure 5.2 on page 211.