MACM 442/CMPT 881/MATH 800
Assignment 4, Fall 2006

Michael Monagan

This assignment is to be handed in on Thursday November 2nd at the beginning of class. Late penalty: 10% off for each day late.

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

For exercise 5.17 include 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. See `?sort`.
Note, Maple is using "mergesort" which does $O(n \log n)$ comparisons in the worst case.

For exercise 6.10, decrypting the first 6 lines (24 characters) of the ciphertext is enough.

For exercise 6.11 use the `Expand(...) mod p` and `Rem(...) mod p` commands to multiply and divide polynomials in $\mathbb{Z}_p[x]$ where needed. For part (b) first use the `Gcdex(...) mod p` command to compute the inverse then either program the extended Euclidean algorithm or execute the steps of the extended Euclidean algorithm in Maple to compute the inverse. For part (c) first use the `Powmod(...) mod p` command to compute x^{25} in the given field then program the square and multiply algorithm to compute x^{25}.

For exercise 6.12 use Maple to do to all arithmetic.

Additonal exercises on primitive elements and finite fields:

1: Using the `nextprime` and `isprime` commands in Maple, find the first prime $p > 10^{100}$ of the form $p = 2q + 1$ where q is also prime. Now show that 2 is a primitive element and 3 is NOT a primitive element in $\mathbb{Z}_p$.

2: Let GF(q) be a finite field with $q = p^k$ elements. For non-zero $\alpha \in GF(q)$, prove that $\alpha^{q-1} = 1$. Hint: adapt the proof of Euler's theorem for $\mathbb{Z}_n$ to $GF(q)$.

3: For the finite field $GF(16)$ constructed as $\mathbb{Z}_2[x]/(x^4+x+1)$ compute the order of each non-zero element and identify the primitive elements. There should be $\phi(16-1) = 8$ primitive elements.

4: (for graduate students)
Do exercise 5.34 and implement algorithm 5.13 on page 217. Test it on the authors' data (n=1457, b=779, $y = 772$) and generate the numbers in Figure 5.3 on page 218.