MACM 442/CMPT 881/MATH 800
Assignment 3, Fall 2006

Michael Monagan

This assignment is to be handed in on Thursday October 19th at the beginning of class. Late penalty: 10% off for each day late.

Chapter 5 exercises 5.14, 5.18, 5.20, 5.21, 5.25, 5.26, 5.30.

Additional question. 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? Show your working.

MATH 800 and CMPT 881 students should also do exercise 5.22.

MACM 442 students may do 5.22 as a bonus (+2% of grade).

Notes: Problem 5.18 illustrates another potential disaster for RSA. Check that the statement is true for $n = 35$ with $b = 11$ and with $b = 13$. Notice what happens for $b = 13$. What is special about $b = 13$? To do the proof use the same argument that is used to count the number of solutions to the congruence $w^r \equiv 1 \bmod p$ on page 204.

For problem 5.21 compute also f_n, the number of bases $0 < a < n$ for which n is a pseudo-prime to the base a, and s_n, the number of bases $0 < a < n$ for which n is a strong pseudo-prime to the base a. Use `a &^ b mod n` in Maple to compute $a^b \bmod n$ (this uses the square-and-multiply algorithm) and use `numtheory[jacobi](a,n)` to compute the Jacobi symbol.