MACM 498/CMPT 881/MATH 800
Assignment 3, Fall 2004

Michael Monagan

This assignment is to be handed in on Thursday October 21st at the beginning of class. Late penalty: 10% off for each day late.

Chapter 5 exercises 5.14, 5.15, 5.18, 5.21, 5.25, 5.26, 5.30.

Computing 881 students should also do exercise 5.20.

Math 800 students should also do exercise 5.22.

Notes: Problem 5.18 illustrates another potential disaster for RSA. Check that the statement is true for $n = 35$ with $b = 11$ then with $b = 13$, i.e. compute $x^b \bmod n$ for $0 \leq x < 35$ with $\gcd(x, 35) = 1$. 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 198.

For problem 5.21 compute also f_n, the number of pseudo-primes and also s_n, the number of strong pseudo-primes to the base $0 < a < n$. Use the function `numtheory[jacobi]` from the Maple library to compute the Jacobi symbol $(\frac{a}{n})$. Use the command command `a &^ b mod n` to compute $a^b \bmod n$ (which uses the square-and-multiply algorithm).

For problem 5.25, don't use various choices for B as suggested by the author. Modify the algorithm to test if $d = \gcd(a - 1, n)$ each time round the loop.