MACM 442/MATH 742/MATH 800
Assignment 3, Fall 2008

Michael Monagan

This assignment is to be handed in on Tuesday October 14th at the beginning of class.
Late penalty: 20% off for up to 24 hours late, zero after that.

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

MATH 742 and 800 students should also do exercise 5.22.
MACM 442 students may do 5.22 as a bonus (+1% 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.

Additional question.

Implement the square and multiply algorithm. Use either Algorithm 5.5 or the algorithm I gave in class. Show that it is working by computing $2^{43} \bmod 35$.

Conventional wisdom says that the primes used for the RSA cryptosystem should be 512 bits (154 decimal digits) long. Use Maple to create two random 154 digit primes p and q (using the `rand` and `nextprime` commands) and compute $n = pq$. Choose a suitable encryption exponent b (do this with care) then compute the decryption exponent a. Choose an integer x at random from $\mathbb{Z}_n$ for the plaintext. Use your square and multiply algorithm to compute $y = x^b \bmod n$ and verify that $y^a \bmod n = x$. Use the `time` command to time how long it takes to compute $y^a \bmod n$.