Math 567, Assignment #7

(due March 23)

This assignment covers material up through section 7.5. You may use a hand-calculator, but you may not use a multiple precision package on a computer.

1. Use Möbius inversion to count the rotationally distinct 4-bead necklaces, when each bead can be any of 3 colors.

2. Compute $2^{100000} \pmod{77}$ in two ways: first, using Euler's theorem, and second, using Fermat's theorem and the Chinese remainder theorem.

3. Find the last two digits of the number 9^{9^9} $(= 9^{(9^{(9^9)})})$.

4. Do there exist infinitely many integers n for which $\phi(n) = n/2$? $n/3$? $n/4$? (Hint: See problems 4(e), 15(a), and 15(b) in section 7.2 of Burton.)

5. x is a 6-digit number which when multiplied by 853 gives a number whose last 6 digits are 135813. What is x? (Hint: 3,000,001 is a multiple of 853.)

6. y is a 3-digit number which when raised to the 89th power gives a number whose last 3 digits are 247. What is y? (Note: solution by exhaustive search is not allowed for problems 5 and 6!)

7. (a) Use the RSA encryption algorithm with key $(n, k) = (3233, 1063)$ to encipher the (single-block) plain-text message 560. Note that 3233 factors as 53 times 61.

(b) What is the recovery exponent for this cryptosystem?

(c) Apply the recovery exponent you calculated in part (b) to decipher the encrypted message you calculated in part (a).

8. If $n = pq = 243449$ and $\phi(n) = 241536$, find the primes p and q. (Hint: See problem 4 in section 7.5 of Burton.)