

**MATH 4450/6450**  
**HOMEWORK 5**  
**DUE 2/16/07**

Do the following book problems:

**7.6:** 3, 4, 7, 9, 11.

**7.7:** 4.

Your instructions for the extra problems this week are: 4450 students should do Extra Problem 1, 3(a), and 4(a) and (b). As usual, 6450 students have to do everything (except Extra Problem 4(c), which is optional).

**Extra Problem 1:** Let  $n = 925501069$ . I find the following relations (which you can check for yourself, if you don't believe me):

$$340181^2 \equiv 2^5 \cdot 7^2 \cdot 11^3 \cdot 17 \pmod{n}$$

$$384953^2 \equiv 3^5 \cdot 7 \cdot 13 \cdot 17^3 \pmod{n}$$

$$409287^2 \equiv 2^8 \cdot 5 \cdot 11^2 \pmod{n}$$

$$506327^2 \equiv 2^{10} \cdot 3^5 \cdot 13 \pmod{n}$$

$$527863^2 \equiv 2^3 \cdot 3 \cdot 5^5 \cdot 7 \cdot 11^2 \pmod{n}$$

$$534889^2 \equiv 2^5 \cdot 5^3 \cdot 11 \cdot 13^2 \cdot 17 \pmod{n}$$

$$597803^2 \equiv 5^2 \cdot 11^3 \cdot 13 \cdot 17^2 \pmod{n}$$

Factor  $n$ . (Unless you enjoy staring intently at numbers on a piece of paper, you might want to try to get Maple to do some of the adding for you. But probably you won't need to give me a printout of your Maple work.)

**Extra Problem 2:** Let  $\alpha = 301$ ,  $\beta = 350483$ ,  $p = 580787$ . I find the following relations (again, check them for yourself):

$$\alpha^{543} \equiv 2^9 \cdot 3^3 \cdot 5^2 \pmod{p}$$

$$\alpha^{1064} \equiv 2^3 \cdot 3 \cdot 7^3 \pmod{p}$$

$$\alpha^{1739} \equiv 2^7 \cdot 7^2 \pmod{p}$$

$$\alpha^{2512} \equiv 2^3 \cdot 3^7 \cdot 5 \pmod{p}$$

$$\beta\alpha^{41} \equiv 5^3 \cdot 7^4 \pmod{p}$$

Find  $L_\alpha(\beta)$ . (You'll probably want to work with matrices in Maple. This one will certainly require a printout.)

**Extra Problem 3:** Let  $p$  be a prime of the form  $2^k + 1$ .

(a) Show that  $k$  must be a power of 2. (Hint: Write  $k = 2^a m$  where  $m$  is odd, and look at  $p \bmod 2^{2^a} + 1$ .)

(b) Let  $A_n = 2^{2^n} + 1$ . Show that  $A_n$  is prime if and only if

$$3^{\frac{A_n-1}{2}} \equiv -1 \pmod{A_n}$$

(Hint: You've already done the work for one direction in Exercise 3.13.32. To show the "if" direction, let  $p$  be a prime dividing  $A_n$  and consider the order of 3 mod  $p$ .)

**Extra Problem 4:** Let  $q = 2^p - 1$ , and suppose that  $q$  is prime.

(a) Show that  $p$  must be prime. (Alas, the converse is false:  $2^{11} - 1 = 23 \cdot 89$ .)

(b) Show that if  $p$  is odd, then  $\left(\frac{3}{q}\right) = -1$ .

(c) (Extra credit) Prove the following beautiful theorem due to Lucas and Lehmer:

Let  $p$  be a prime number. Let  $S_n$  be defined by the formulas  $S_1 = 4$ ,  $S_{n+1} = S_n^2 - 2$ . Then  $q = 2^p - 1$  is prime if and only if  $q | S_{p-1}$ .