

**MATH 13150: Freshman Seminar**

**Homework #9** Due *Wednesday, April 11 2012*

- Using the mod 11 power table on page 197 of your textbook, say whether or not the following roots exist in mod 11 arithmetic, and if they exist, find them all.
  - $\sqrt[5]{3} \pmod{11}$ .
  - $\sqrt[7]{4} \pmod{11}$ .
  - $\sqrt[8]{2} \pmod{11}$ .
  - $\sqrt[8]{7} \pmod{11}$ .
- For which of the following  $k$ th root problems, does the 5 step method for computing  $\sqrt[k]{b} \pmod{p}$  described in section 3 work? You do not have to compute the  $k$ th root.
  - $\sqrt[5]{22} \pmod{23}$ .
  - $\sqrt[7]{13} \pmod{17}$ .
  - $\sqrt[13]{5} \pmod{53}$ .
  - $\sqrt[5]{3} \pmod{31}$ .
- Compute  $\sqrt[3]{0} \pmod{41}$  (hint: the method of this unit does not work, but you can do the computation anyway).
- Compute  $\sqrt[11]{3} \pmod{19}$ .
- Compute  $\sqrt[11]{5} \pmod{19}$ .
- Compute  $\sqrt[7]{3} \pmod{17}$ .
- Compute  $\sqrt[7]{2} \pmod{53}$ .
- Compute  $\sqrt[7]{5} \pmod{61}$ .

ESSAY ASSIGNMENT: Including earlier reading, read chapters 1-4 and chapter 6 of the CodeBook. Write a history of cryptography. Your essay should explain how cryptography worked before the RSA algorithm, and how the RSA algorithm changed cryptography. Feel free to write about aspects of the CodeBook that you found especially intriguing. Two pages would be an appropriate length for this essay.