MATH 350 ASSIGNMENT 6, FALL 2015

Due in class on Friday, October 16

Read Chapters 19 and chapter 28. (We have proved the existence of primitive $p-1^{\text{st}}$ root of 1 in $\mathbb{Z}/p\mathbb{Z}$ in class. Please compare the proof we give in class with the proof in the textbook.)

Part 1. From the textbook *A friendly introduction to number theory*.

- Exercises 19.1 and 19.2
- Exercises 28.6 (a) and 28.7.

Part 2. Extra credit problems:

1. Suppose that p is a prime number.
   (a) Does $(\mathbb{Z}/p\mathbb{Z})^{\times}$ contain a primitive 4-th root of 1?
   (b) How many elements of $\mathbb{Z}/p\mathbb{Z}$ are *cubes* (i.e. elements of the form $\bar{a}^3$ for some $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$)? [Your answer will depends on $p \bmod 3$.]
2. Let n be a positive odd integer. For any positive integer a which is *not* divisible by n, we say that a is a *witness* that n is a composite number according to the the Miller-Rabin test if both conditions (a), (b) in Theorem 19.3 hold.
   (a) Suppose that n is a composite number. Let S be the set of all positive integers a such that $1 \leq a \leq n-1$ and a is a witness that n is a composite number according to Miller-Rabin. Determine the cardinality of S.
   [Your answer will depend on the prime factorization of n.]
   (b)) Suppose we randomly draw an element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$, in such a way that all elements of $\mathbb{Z}/n\mathbb{Z}$ have equal chance of being drawn. What is the chance that $\bar{a}$ is a witness that n is composite?
   (c) Can you give a uniform lower bound for the chance in (b), assuming that n is a composite number?
   (d) If you repeat the random drawing as in (b) N times in such a way that each drawing is independent of what occurred before. Estimate the chance that these N drawings do not produce any witness that n is a composite number.