Math 458
Homework Due Wednesday, May 8

1. From the text do 3.1ab, 3.4ab, 3.7, 3.8, 3.14a,b(i), 3.15bd (use Sage for this last problem, and read question #3 below first).

2. Find all the Miller-Rabin witnesses for the number 9. Do this by hand, so that you understand the algorithm.

3. In class (and in the text) it was stated that if n is an odd composite number then at least 75% of the numbers between 1 and $n-1$ are Miller-Rabin witnesses for n. In this problem you will investigate that claim. Recall that Sage has the built-in command `is_prime` which tells if a number is prime, e.g. `is_prime(10)` will tell if 10 is prime.

   On the course website is a Sage notebook that contains the function `miller_rabin_test(n,a)`, which outputs TRUE if a is a Miller-Rabin witness for n and FALSE otherwise.

   (a) Find a Miller-Rabin witness for the number 32573242343.

   (b) Write some Sage code that takes a number n, counts all the Miller-Rabin witnesses from 1 up through $n-1$, and returns the ratio

   $$\frac{\#\text{ of witnesses}}{n-1}$$

   Your code should return about 0.888 for $n = 10$. Pick five or six numbers between 10 and 10,000 and compute the corresponding ratios.

   (c) What do you think the average value of the ratio is (approximately), say for composite numbers up to 10,000? Take an educated guess. Compute it precisely if you know how to make Sage do that.

   (d) There are exactly 8 composite numbers below 2000 for which the ratio is under 0.85. Find them, and give their ratios.