Quantitative Reasoning **28**:
The Magic of Numbers

Homework **29**

Assigned on Monday December 8th
Due at 12 noon **Friday** December 12th

Please submit problem sets at the end of the relevant lecture, or leave in the box labeled QR28 outside the Math Department's main office, on the third floor of the Science Center (Room 325).

Reading:

Gross-Harris, Chapter 24

Problems:

Please explain your reasoning and show your work.

1. We've seen that we can use Fermat's Theorem to test if a number is composite. If a number is prime, then it will alway's pass this "Fermat test." What if the number n is composite? What fraction of a that are relatively prime to n satisfy $a^{n-1} \equiv 1 \pmod{n}$? It turns out that there are some n so that *all* a have this property, yet n is composite! Such numbers are called *Carmichael numbers.*

   The smallest Carmichael number is 561. In this problem we'll take a look at why 561 has no witnesses for the Fermat test.

   (a) Find the factorization of 561.

   (b) Find the factorization of 560.

   (c) Now suppose that a is relatively prime to 561. Use the Chinese Remainder Theorem, and Fermat's Theorem to explain why $a^{560} \equiv 1 \pmod{561}$ (see Homework 24 for an example)

   (d) (**Optional challenge**; you will not be graded on this part) Find the next Carmichael number.

2. In this problem, we explore a way to defeat Carmichael numbers: the Miller-Rabin primality test.

    (a) We've seen that 5 is not a Fermat witness for 561, because 561 is a Carmichael number. So $5^{560} \equiv 1 \pmod{561}$, but we can consider smaller powers of 5. In particular, we factor $560 = 2^4 \cdot 35$.
    Compute 5^{35}, then $5^{70}, 5^{140}, 5^{280}$, and $5^{560} \pmod{561}$

    (b) Find the last one in this sequence that is not 1. If 561 were prime, there would be only two numbers that squared to 1: 1 and -1. Why is this?

    (c) Can one conclude from this information that 561 is composite? If so, how?

    (d) Use this test again with $3 \pmod{91}$ to check if 91 is composite.