Math 565, Problem Set 5: *due Friday, February 9*

1. This problem is about Carmichael numbers.

   a) The number 561 factors as $3 \cdot 11 \cdot 17$. Use Fermat's little theorem to prove that

   $$a^{561} \equiv a \pmod 3, \qquad a^{561} \equiv a \pmod{11}, \qquad a^{561} \equiv a \pmod{17}.$$

   Explain why these three congruences imply that $a^{561} \equiv a \pmod{561}$ for every value of a.

   b) Mimic the idea used in (a) to prove that each of the following numbers is a Carmichael number:

      i) $1729 = 7 \cdot 13 \cdot 19$

      ii) $1024651 = 19 \cdot 199 \cdot 271$

   c) Prove that every Carmichael number is odd.

2. Use the Miller-Rabin test on each of the following numbers. In each case, either provide a Miller-Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 10 numbers that are not Miller-Rabin witnesses for n.

   a) $n = 294409$

   b) $n = 118901521$

   c) $n = 118901509$

   d) $n = 118915387$

3. Use Pollard's $p - 1$ method to factor each of the following numbers:

   a) $n = 1739$

   b) $n = 220459$

   c) $n = 48356747$

   Be sure to show your work and indicate which prime factor p of n has the property that $p - 1$ is a product of small primes.

4. A prime of the form $2^n - 1$ is called a *Mersenne prime*.

   a) Factor each of the numbers $2^n - 1$ for $n = 2, 3, \ldots, 10$. Which ones are Mersenne primes?

   b) Use Sage to find the first seven Mersenne primes.

   c) If n is even and $n > 2$, prove that $2^n - 1$ is not prime.

   d) If $3|n$ and $n > 3$, prove that $2^n - 1$ is not prime.

   e) More generally, prove that if n is a composite number, then $2^n - 1$ is not prime. Thus all Mersenne primes have the form $2^p - 1$ with p a prime number.

   f) What is the largest known Mersenne prime? Are there any larger primes known? [Hint: google the phrase "Great Internet Mersenne Prime Search"]

5. Let p be an odd prime and let a be an integer not divisible by p.

   a) Prove that $a^{(p-1)/2}$ is congruent to ± 1 modulo p.

   b) Prove that $a^{(p-1)/2}$ is congruent to 1 modulo p if and only if a is a quadratic residue modulo p. [Hint: use the primitive root theorem]

   c) Prove that $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

   d) Use (c) to prove that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$