Problem Set 6

Due: March 13th, 5pm

1 Formal proofs

For each problem in this section, you must give a complete and rigorous proof. Your arguments should be clear, logically ordered, and written in full sentences.

In particular, state all assumptions explicitly and define all notation. Justify every nontrivial step.

1. (1 point) Prove that if n is a Carmichael number and p is a prime divisor of n, then $p-1$ divides $n-1$.
2. (1 point) Let n be an odd composite number that is a strong pseudoprime to base a (i.e., n passes the Miller-Rabin test for base a). Prove that if n is also a strong pseudoprime to base b, then n is a strong pseudoprime to base ab mod n.

   Hint: Write $n-1 = 2^s \cdot d$ where d is odd. Consider the two cases in the Miller-Rabin test separately.
3. (1 point) Prove that if $n = pq$ where p and q are distinct prime numbers, then n is not a Carmichael number.
4. (1 point) Prove that if a, n are positive integers and $\gcd(a, n) = 1$ then there is some coefficient of the polynomial $(x-a)^n$ that is not congruent to zero modulo n.

2 Demonstrations

For problems in this section, you still need to give complete mathematical reasoning to support your answers. I should be able to follow and understand your work, but it doesn't have to be organized into a formal proof.

5. (1 point) Perform the Miller-Rabin primality test on the following numbers to determine whether they are probable primes. Show all your work, including the decomposition $n-1 = 2^s \cdot d$ and all relevant calculations.
   (a) Test $n = 25$ with base $a = 7$. Does 25 pass the test for this base?
   (b) Test $n = 45$ with base $a = 2$. Does 45 pass the test for this base?

(c) Test $n = 97$ with base $a = 5$. Does 97 pass the test for this base?

3 Explorations

In this section, I'm looking for answers that are supported by evidence, but you don't have to prove your answers. Please **include all code snippets** used for these problems, failure to do so may result in loss of points.

6. (1 point) For each composite number n between 120 and 130, determine how many bases $a \in \mathbb{Z}_n^\times$ pass the Miller-Rabin primality test for your chosen n. Give your final answer in the form of a table.

7. (1 point) For composite numbers up to 100:

   (a) How many numbers are Fermat pseudoprimes to base 2 (i.e., pass the Fermat primality test $2^{n-1} \equiv 1 \pmod{n}$ but are composite)? List them all.

   (b) How many numbers are strong pseudoprimes to base 2 (i.e., pass the Miller-Rabin test for base 2 but are composite)? List them all.

   (c) What do you notice when comparing these two lists?

8. (1 point) Let n be a positive integer. An integer a is a *square modulo* n (or *quadratic residue modulo* n) if the congruence $x^2 \equiv a \pmod{n}$ has a solution.

   (a) Which numbers are squares modulo 3? Modulo 5? Modulo 7? Give a complete list for each modulus by checking all possible values.

   (b) For which prime numbers $p \leq 100$ is 3 a square modulo p? What about 5? Give a conjecture about when 3 is a square modulo a prime p based on your data. Do the same for 5.