Math 11N
Homework 7
Due Saturday, February 26th, 2022

1. Do the following computations.

   (a) Reduce 8263^{12012} mod 7000.

   (b) Reduce $100^{101^{102}}$ mod 13.

   (c) Find all primes p such that $\text{ord}_p(2) = 24$.

   (d) Solve the equation $x^{13} \equiv 35 \bmod 360$.

2. This exercise is a primality test based on Fermat's little theorem. For any integer a and prime p with $p \nmid a$, Fermat's little theorem says $a^{p-1} \equiv 1 \bmod p$, so taking the contrapositive of this statement says that if $a^{p-1} \not\equiv 1 \bmod p$, then p is composite! This gives rise to an algorithm for testing if an integer n is prime or not:

   - Randomly pick an integer a with $n \nmid a$.
   - If $a^{n-1} \not\equiv 1 \bmod n$, then n is composite and we're done!
   - Otherwise, if $a^{n-1} \equiv 1 \bmod n$, pick a different integer a and repeat.

   If a is an integer such that $a^{n-1} \not\equiv 1 \bmod n$, we call a a *Fermat witness* for the compositeness of n.

   (a) Using WolframAlpha or any other computer algebra system, find the smallest Fermat witness for 2821.

   (b) Let $m = 56052361$. Using WolframAlpha or any other computer algebra system, determine if $2, 3, 5, 6, 7, 10$, or 11 are Fermat witnesses for m. What do you find? Is this enough information to tell you with certainty if m is prime or composite, and why?

   We call n a *Carmichael number* if $a^{n-1} \equiv 1 \bmod n$ for all integers a with $\gcd(a, n) = 1$. Carmichael numbers are the integers for which our primality test will never give us any information.

   (c) Prove that 561 is a Carmichael number. *(Hint:* $561 = 3 \cdot 11 \cdot 17$*. Euler's theorem might be useful.)*

3. Euler's theorem says for any integer a with $\gcd(a, n) = 1$, that $a^{\varphi(n)} \equiv 1 \bmod n$. However, $\varphi(n)$ is often times not the smallest exponent we can choose with this property. The *Carmichael function* $\lambda(n)$ is defined to be the smallest positive integer k such that $a^k \equiv 1 \bmod n$ for all integers a with $\gcd(a, n) = 1$. It turns out, for example, that $\lambda(1729) = 36$, and so every integer a with $\gcd(a, 1729) = 1$ satisfies $a^{36} \equiv 1 \bmod 1729$.

   (a) Prove that n is Carmichael number if and only if $\lambda(n) \mid n - 1$.

(b) Compute $\lambda(3), \lambda(11)$ and $\lambda(17)$.

(c) Compute $\lambda(561)$.

4. The goal of this problem is to give an alternate proof of Euler's theorem following the main philosophy of number theory.

   (a) Prove that for any integer k with $1 \leq k \leq p-1$, that $\binom{p}{k} \equiv 0 \bmod p$.

   (b) For any integer $a \geq 0$, prove by induction on a that $a^p \equiv a \bmod p$. Deduce that for $\gcd(a,p) = 1$, that $a^{\varphi(p)} \equiv 1 \bmod p$. (*You may assume the binomial theorem for this.*)

   (c) Prove that for any integers a, k with $k \geq 1$ and $\gcd(a,p) = 1$, that $a^{\varphi(p^k)} \equiv 1 \bmod p^k$. (*Again, you may assume the binomial theorem for this.*)

   (d) Prove that for integers a, n with $\gcd(a,n) = 1$ that $a^{\varphi(n)} \equiv 1 \bmod n$.

5. On homework 2, you proved the only integers of the form $2^n - 1$ that can be prime are *Mersenne primes*, primes of the form $2^p - 1$ for prime p, and that the only integers of the form $2^n + 1$ that can be prime are *Fermat numbers*, integers of the form $2^{2^n} + 1$.

   (a) Let p be an odd prime, and let q be a prime divisor of $2^p - 1$. Prove that $\mathrm{ord}_q(2) = p$. Similarly, for odd prime p prove that if $p \mid 2^{2^n}+1$ then $\mathrm{ord}_p(2) = 2^{n+1}$.

   (b) Deduce that if q is a prime divisor of $2^p - 1$, then $q = 2pk + 1$ for some integer k. Similarly, deduce that if p is a prime divisor of $2^{2^n} + 1$, that p must be of the form $2^{n+1}k + 1$ for some integer k.

   (c) On homework 2, you proved using a computer that $2^{32}+1 = 641 \cdot 6700417$. Use the previous part to explain how one could identify 641 as a possible factor, and prove by hand that $641 \mid 2^{32} + 1$ using modular arithmetic, so that 641 is the smallest prime divisor of $2^{32} + 1$. Similarly, find by hand the smallest prime divisor of $2^{29} - 1$.

6. On homework 4, you proved that there were infinitely many primes of the form $4k+3$. Now, you will prove that there are infinitely many primes of the form $4k + 1$.

   (a) Show that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k + 1$.

   (b) Prove there are infinitely many primes of the form $4k + 1$. (*Hint: consider* $(2p_1 \cdots p_k)^2 + 1$.)