Math 573 Problem Set 5

1. List the primitive roots modulo 14.

2. **(a)** Prove that for $n > 1$, the sum of the positive integers less then n and relatively prime to n is $\frac{1}{2}n\phi(n)$.

(b) Let p be a prime. Show that the product of the $\phi(p-1)$ primitive roots modulo p is congruent modulo p to $(-1)^{\phi(p-1)}$.

3. Prove that $\mathrm{ord}_n(ab) = \mathrm{ord}_n(a)\,\mathrm{ord}_n(b)$ if $\gcd(\mathrm{ord}_n(a), \mathrm{ord}_n(b)) = 1$.

4. Let $a, n \in \mathbb{Z}_{>1}$ and let p be a prime. If $p \mid a^{2^n} + 1$, prove that $p = 2$ or $p \equiv 1 (\mathrm{mod}\, 2^{n+1})$.

5. **(a)** Let p and q be odd primes. If $q \mid a^p - 1$, then either $q \mid (a-1)$ or $q = 2kp + 1$ for some $k \in \mathbb{Z}$.

(b) Prove that if p is an odd prime, then the prime divisors of $2^p - 1$ are of the form $2kp + 1$.

(c) Find the smallest prime divisor of $2^{29} - 1$.

6. Let p be a prime and $a \in \mathbb{Z}$ so that $\gcd(a, p) = 1$. Show that the congruence

$$x^n \equiv a (\mathrm{mod}\, p)$$

has $\gcd(n, p-1)$ solutions if

$$a^{(p-1)/\gcd(n,p-1)} \equiv 1 (\mathrm{mod}\, p)$$

and no solutions otherwise. (Hint: Think primitive roots! Write $a = r^j$ for some j with r a primitive root.)

7. Prove that $1^k, 2^k, \ldots, (p-1)^k$ form a reduced residue system modulo p if and only if $\gcd(k, p-1) = 1$.

8. **(a)** Let r be a primitive root modulo p. Express $-r$ as a power of r.

(b) If $p \equiv 3 (\mathrm{mod}\, 4)$, prove that $-r$ is not a primitive root modulo p.

(c) If $p \equiv 1 (\bmod 4)$, prove that $-r$ is a primitive root modulo p.

9. Use Euler's criterion to prove that if 2^k+1 is a prime, then all quadratic nonresidues are primitive roots modulo 2^k+1.

10. **(a)** Consider the polynomial $f(x) = x^{2^m n}+1$ for $m \geq 1$, $n > 1$ with n odd. Prove that the polynomial is not irreducible. In other words, show that the polynomial factors into two polynomials each of degree greater then or equal to 1.

(b) Let $a \in \mathbb{Z}_{>1}$, $k \in \mathbb{Z}_{>0}$ and suppose $p = a^k+1$ is a prime. Prove that $\operatorname{ord}_p(a)$ must be a power of 2.