Spring 2021, Math 522: Problem Set 8
Due: Thursday, March 25th, 2021
Primitive Roots

(D1) *Counting primitive roots.* Fix $n \geq 2$.

(a) Find the number of primitive roots in $\mathbb{Z}_6$, $\mathbb{Z}_7$, and $\mathbb{Z}_9$.
Hint: divide and conquer within your group!

(b) In what follows, let $N = \phi(n)$, and let

$$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \gcd(a, n) = 1\}.$$

Verify that $\mathbb{Z}_n^*$ is closed under multiplication and that $|\mathbb{Z}_n^*| = N$.

(c) Let α denote a **fixed** primitive root modulo n. Consider the map

$$\begin{aligned} f : \mathbb{Z}_n^* &\longrightarrow \mathbb{Z}_N \\ [\alpha^b]_n &\longmapsto [b]_N \end{aligned}$$

Write explicitly where f sends every element of $\mathbb{Z}_n^*$ in the special case $n = 9$ and $\alpha = 2$. For example, $f([2]_9) = [1]_6$ and $f([4]_9) = f([2^2]_9) = [2]_6$.

(d) Verify that f is well-defined (that is, if $[\alpha^b]_n = [\alpha^c]_n$, then $b \equiv c \bmod N$).
Hint: use the lemma from the start of today's class.

(e) Prove that f is one-to-one and onto.
Hint: prove f is one-to-one, then argue $|\mathbb{Z}_n^*| = |\mathbb{Z}_N|$ to conclude f must also be onto.

(f) Prove that $f([\alpha^b][\alpha^c]) = f([\alpha^b]) + f([\alpha^c])$ for any $b, c \in \mathbb{Z}$.

(g) Prove that α^b is a primitive root modulo n if and only if $[b]_N$ has (additive) order N (that is, if and only if $\gcd(b, N) = 1$).

(h) Find a formula in terms of n for the number of primitive roots modulo n.

(D2) *Existence of primitive roots.* The goal of this problem is to prove parts of the following.

Theorem. *There exists a root modulo n if and only if $n = 2$, $n = 4$, $n = p^r$ for some odd prime p, or $n = 2p^r$ for some odd prime p.*

(a) Verify the theorem for $n = 2, 4, 8, 10, 15$.
Hint: divide and conquer within your group!

(b) Use induction on $k \geq 3$ to prove that if a is odd, then

$$a^{2^{k-2}} \equiv 1 \bmod 2^k.$$

(c) Use the previous part to prove if n is a power of 2, then the theorem holds.

(d) It turns out that if $\gcd(m, n) = 1$ and we have $a^k \equiv 1 \bmod n$ and $a^\ell \equiv 1 \bmod m$, then

$$a^{\operatorname{lcm}(k,j)} \equiv 1 \bmod nm,$$

(we will not be proving this today). Using this fact, if $\gcd(a, 91) = 1$, what is the largest possible multiplicative order of a modulo 91?

(e) Use the previous part to prove the theorem holds if n is divisible by 2 odd primes.

(f) Conclude the forward direction of the theorem.
Note: the remainder of the proof can be found in the exercises of Andrews 7.2.

Homework problems. You must submit *all* homework problems in order to receive full credit.

Unless otherwise stated, $a, b, c, n, p \in \mathbb{Z}$ are arbitrary with $p > 1$ prime and $n \geq 2$.

(H1) Find all primitive roots modulo 14.

(H2) Determine the number of integers $n \leq 1000$ that have a primitive element modulo n.

Hint: there are 168 primes less than 1000, of which 95 are less than 500.

(H3) Determine which integers n have a **unique** primitive root modulo n.

(H4) Suppose p is prime, a is a primitive root modulo p, and $k \mid (p-1)$. Find the number of incongruent solutions modulo p to

$$x^k \equiv a \bmod p.$$

(H5) (a) Locate 4 primes p for which

$$x^2 \equiv -1 \bmod p$$

has an integer solution, and 4 primes for which it has no solutions.

(b) Determine for which primes p the equation

$$x^2 \equiv -1 \bmod p$$

has an integer solution.

Note: your answer should be an "if and only if" characterization, with a proof!