UMASS AMHERST MATH 471 F. HAJIR

HOMEWORK 9: PRIMITIVE ROOTS

1. (a) Show that 2 is a primitive root modulo 29.
(b) Using (a) quickly find elements of order 2, 4, 7, and 14 in $(\mathbb{Z}/29\mathbb{Z})^\times$.

2. Find all the primitive roots modulo 17. Hint: by a theorem discussed in class, once you find one primitive root, g, then g^k for $k \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$ are all the primitive roots modulo p.

3. Suppose $m = p^n$ where p is a prime and $n \geq 1$. Suppose also that $\{g\}_m$ has order $\varphi(m)$, so g is a primitive root mod p^n. Show that g is a primitive root modulo p as well, i.e. $\{g\}_p$ has order $p-1$.

Hint: Suppose the order of g modulo p is $e = \text{order}(\{g\}_p)$. We want to show that $e = p-1$. If we could show that

$$(*) \qquad g^{ep^{n-1}} \equiv 1 \bmod p^n,$$

then we would be done because the order of g modulo p^n is $(p-1)p^{n-1}$. So how do we show (*)? Repeatedly use the fact that if $x \equiv 1 \bmod p^k$, then $x^p \equiv 1 \bmod p^{k+1}$. This fact is more or less the same as problem d from Exam 2.

4. Suppose $p = 2^n + 1$ is a prime number (such primes are called "Fermat primes," and not much is known about them). Show that 3 is a primitive root modulo p. *Hint: You may use the fact that if p is a prime, then the congruence $x^2 \equiv -3 \bmod p$ is solvable if and only if $p \equiv 1 \bmod 3$.*

Even More Hint: Let g be a primitive root mod p. Write $3 = g^r$. Now use the fact quoted above to show that r is odd. Conclude that $\gcd(r, p-1) = 1$. Now conclude that 3 is a primitive root mod p by a theorem we proved in class.

5. Let p be an odd prime, and suppose $1 < a < p$. Show that a is a primitive root modulo p if and only if for all primes q dividing $p-1$, $a^{(p-1)/q} \not\equiv 1 \bmod p$.

Hint: One direction is very easy. For the other direction, if a is not a primitive root, then $a^d \equiv 1 \bmod p$ for some proper divisor d of $p-1$; let q be a prime divisor of $(p-1)/d$.....

6. Suppose p is a prime with primitive root g and d is a divisor of $p-1$. We say that $\{a\}_p$ is a dth power if there exists an integer r such that $a \equiv r^d \bmod p$. Show that there are exactly $(p-1)/d$ non-zero dth powers in $\mathbb{Z}/p\mathbb{Z}$, namely

$$\{h^t\}_p, \text{ where } t = 1, 2, 3, \ldots, (p-1)/d \text{ and } h = g^d.$$

Note: it's easy to show these are distinct dth powers, but you also have to show that there aren't any others.

7. Use problems 1 and 6 to determine the squares modulo 29.

8. Show that for an odd prime p, $x^4 \equiv -1 \bmod p$ has as solution $x \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 8$.

Hint: you may wish to use problem 5 or something similar to it.

9. Show that if p is an odd prime and $1 \leq a \leq p-1$, then $a^{(p-1)/2} \equiv \pm 1 \bmod p$, and that a is a square mod p if and only if $a^{(p-1)/2} \equiv 1 \bmod p$.

10. Show that if $p \equiv 1 \bmod 3$ is a prime, then -3 is a square modulo p.

Hint: use the existence of a primitive root to find an element r of order 3. What cubic equation does this r satisfy? What quadratic equation does r satisfy? (Remeber, $r \neq 1$!) Now show that $u = 2r + 1$ is the square root you are looking for.