Homework 7
Math 329: Number Theory

March 25, 2018

1 Easy

Problem 1. Find all primitive roots modulo 13.

Problem 2. For the following n, state how many primitive roots mod$n$ exist:

(a) $n = 2018$

(b) $n = 97$.

Problem 3. What is the order of 3 modulo 29?

Problem 4. Show 3 is a primitive root modulo 17^2.

Problem 5. Suppose $n > 1$ and that p is a prime number dividing $2^{2^n} + 1$. Prove that the order of 2 modulo p is 2^{n+1}.

2 Medium

Problem 6. Let p be prime. Prove $p \equiv 1 \bmod 8$ if and only if there exists an integer x such that $x^4 \equiv -1 \bmod p$.

Problem 7. Prove that if $n = 2p^k$ for a positive integer k and p an odd prime number, then n has a primitive root.

Problem 8. Let Q be a polynomial of degree n with integer coefficients. Suppose p is a prime number greater than $n + 1$. Prove that

$$Q(0) + Q(1) + \cdots + Q(p - 1) \equiv 0 \bmod p.$$

Problem 9. Let p be a prime number greater than 5. We say that a is a cubic residue modulo p if $a \not\equiv 0 \bmod p$ and there exists an integer x such that $x^3 \equiv a \bmod p$. For example 4 is a cubic residue modulo 23 because $3^3 = 27 \equiv 4 \bmod 23$.

(a) Prove that if $p \equiv 1 \bmod 3$, then there are $(p - 1)/3$ cubic residues.

(b) Prove that if $p \equiv 2 \bmod 3$, then there are $p - 1$ cubic residues.

3 Hard

Problem 10. Let $n \geq 2$ be a positive integer. Prove that the following assertions are equivalent:

(a) for all integer x coprime with n, the congruence $x^6 \equiv 1 \bmod n$ holds;

(b) n divides 504.