MATH 255: ELEMENTARY NUMBER THEORY
HOMEWORK #10

JOHN VOIGHT

9.1: The Order of an Integer and Primitive Roots

Problem 9.1.A. Determine the order of 10 modulo 13 and the order of 9 modulo 25.

Problem 9.1.5. Show that the integer 12 has no primitive roots.

Problem 9.1.9. Show that if a^{-1} is an inverse of $a \in (\mathbb{Z}/n\mathbb{Z})^*$, then $o(a^{-1}) = o(a)$, that is to say, the order of a^{-1} modulo n is equal to the order of a modulo n.

Problem 9.1.10. Show that if $a, b \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $\gcd(o(a), o(b)) = 1$, then $o(ab) = o(a)o(b)$.

Problem 9.1.14. Show that if $m \in \mathbb{Z}_{>0}$ and $a \in (\mathbb{Z}/m\mathbb{Z})^*$ with $o(a) = m - 1$, then m is prime.

Problem 9.1.18*. Let p be a prime divisor of the Fermat number $F_n = 2^{2^n} + 1$.

(a) Show that $o(2) = 2^{n+1}$ modulo p.
(b) Conclude that $2^{n+1} \mid (p-1)$, so that p must be of the form $2^{n+1}k + 1$ for some $k \in \mathbb{Z}$.

Computation 9.1.B*. Let $\pi^{(2)}(x)$ denote the set of primes $p \leq x$ such that 2 is a primitive root modulo p. Compute $\pi^{(2)}(x)/\pi(x)$ for a large $x \in \mathbb{R}_{>0}$. Use this to estimate the probability that 2 is a primitive root modulo p for p a large prime.

9.2: Primitive Roots for Primes

Problem 9.2.1(a)–(b). Find the number of incongruent roots modulo 11 of each of the following polynomials:

(a) $x^2 + 2$.
(b) $x^2 + 10$.

Problem 9.2.5. Find a complete set of incongruent primitive roots of 13.

Problem 9.2.8. Let r be a primitive root for the prime p with $p \equiv 1 \pmod 4$. Show that $-r$ is also a primitive root.

Problem 9.2.9. Show that if p is a prime with $p \equiv 1 \pmod 4$, then there is an integer x such that $x^2 \equiv -1 \pmod p$. *[Hint: Use Theorem 9.8 to show that there is an integer x of order 4 modulo p.]*

Problem 9.2.10.

(a) Find the number of incongruent roots modulo 6 of the polynomial $x^2 - x$.
(b) Explain why the answer to part (a) does not contradict Lagrange's theorem.

Date: Due Wednesday, 8 April 2009.