MATH 255: ELEMENTARY NUMBER THEORY
HOMEWORK #11

JOHN VOIGHT

11.1: Quadratic Residues and Nonresidues

Problem 11.1.2. Find all quadratic residues modulo of each of the following integers:

(a) 7 (b) 8 (c) 15

Problem 11.1.5. Evaluate the Legendre symbol $\left(\dfrac{7}{11}\right)$ using:

(a) Euler's criterion.
(b) Gauss' lemma.

Problem 11.1.6. Let a, b be integers not divisible by the prime p. Show that either one or all three of the integers a, b, ab are quadratic residues modulo p.

Problem 11.1.7. Show that if p is an odd prime, then

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1, 3 \pmod 8; \\ -1, & \text{if } p \equiv -1, -3 \pmod 8. \end{cases}$$

Problem 11.1.10. Show that if b is a positive integer not divisible by the prime p, then

$$\left(\frac{b}{p}\right) + \left(\frac{2b}{p}\right) + \left(\frac{3b}{p}\right) + \cdots + \left(\frac{(p-1)b}{p}\right) = 0.$$

Problem 11.1.12. Consider the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod p$, where p is prime and $a, b, c \in \mathbb{Z}$ are integers with $p \nmid a$.

(a) Let $p = 2$. Determine which quadratic congruences modulo 2 have solutions.
(b) Let p be an odd prime and let $d = b^2 - 4ac$. Show that the congruence $ax^2+bx+c \equiv 0 \pmod p$ is equivalent to the congruence $y^2 \equiv d \pmod p$, where $y = 2ax+b$. Conclude that if $d \equiv 0 \pmod p$, then there is exactly one solution x modulo p; if d is a quadratic residue of p, then there are two incongruent solutions; and if d is a quadratic nonresidue of p, then there are no solutions.

Problem 11.1.36*. Show that a prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$ must be of the form $2^{n+2}k + 1$. *[Hint: Show that 2 has order 2^{n+1} modulo p. Then show that $2^{(p-1)/2} \equiv 1 \pmod p$ using Theorem 11.6. Conclude that $2^{n+1} \mid (p-1)/2$.]*

Computation 11.1.6*. Use numerical evidence to determine for which odd primes p there are more quadratic residues a of p with $1 \le a \le (p-1)/2$ than there are with $(p+1)/2 \le a \le p-1$.

Date: Due Wednesday, 15 April 2009.

11.2: The Law of Quadratic Reciprocity

Problem 11.2.1. Evaluate each of the following Legendre symbols:

$$\text{(a)} \left(\frac{3}{53}\right) \qquad \text{(b)} \left(\frac{7}{79}\right)$$

Problem 11.2.3. Show that if p is an odd prime, then

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 6; \\ -1, & \text{if } p \equiv -1 \pmod 6. \end{cases}$$

Problem 11.2.4. Find a congruence describing all primes for which 5 is a quadratic residue.

Problem 11.2.15. The integer $p = 1 + 8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 = 892371481$ is prime. Show that for all primes q with $q \leq 23$, we have $\left(\frac{p}{q}\right) = 1$. Conclude that there is no quadratic nonresidue of p less than 29 and that p has no primitive root less than 29.