Math 40520 Theory of Number
Homework 7

Due Friday, 11/2

Do 5 of the following problems.

1. Let $p, q \equiv 3 \pmod 4$ be two distinct primes and $n = pq$. Suppose a is a perfect square modulo n and $y = a^2 \mod n$. Show that a is the only one of the four solutions to the equation $x^2 \equiv y \pmod n$ which is a perfect square mod n.

2. Let $p > 5$ be a prime number and write $P = \{1, 2, \ldots, (p-1)/2\}$. Show that $x \in P$ is such that
$$5x \in 5P \cap (-P)$$
if and only if
$$\left\lceil \frac{p+1}{10} \right\rceil \leq x \leq \left\lfloor \frac{p-1}{5} \right\rfloor \quad \text{or} \quad \left\lceil \frac{3p+1}{10} \right\rceil \leq x \leq \left\lfloor \frac{2p-1}{5} \right\rfloor$$
and conclude that for $p > 5$,
$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 9 \pmod{20} \\ -1 & \text{if } p \equiv \pm 3, \pm 7 \pmod{20} \end{cases}$$
and remark that this is equivalent to the simpler statement
$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5 \\ -1 & \text{if } p \equiv \pm 2 \pmod 5 \end{cases}$$

3. Let p be an odd prime. Suppose that $a \neq 0$ is a square mod p. Show that a is a square mod p^n for every $n \geq 1$.

4. Let a be an odd integer and $n \geq 3$ be an integer. Show that a is a square modulo 2^n if and only if $a \equiv 1 \pmod 8$. [Hint: In class we showed that 17 is a square mod 2^n and indeed $17 \equiv 1 \pmod 8$.]

5. Let $p > 3$ be a prime. What is the sum modulo p of all the quadratic residues mod p?

6. Show that $(x^2 - 13)(x^2 - 17)(x^2 - 13 \cdot 17) = 0$ has no rational solutions but has solutions modulo n for every positive integer n.

7. Exercise 4.4 on page 90 in the textbook.

8. Exercise 4.7 on page 90 in the textbook.