# Math 40520 Theory of Number
# Homework 6

Due Wednesday, 2015-10-14, in class

**Do 5 of the following 8 problems. Please only attempt 5 because I will only grade 5.**

1. Let $p > 3$ be a prime number and write $P = \{1, 2, \ldots, (p-1)/2\}$. Show that $x \in P$ is such that

$$3x \in 3P \cap (-P)$$

if and only if

$$\left\lceil \frac{p+1}{6} \right\rceil \leq x \leq \left\lfloor \frac{p-1}{3} \right\rfloor$$

and conclude that for $p > 3$,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12} \\ -1 & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$$

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 $p > 3$ be a prime number $\equiv 2 \pmod{3}$. Show that $p \mid x^2 + 3y^2$ for integers $x$ and $y$ if and only if $p \mid x$ and $p \mid y$. [Hint: Use Problem 1. Similar to Exercise 7.10 on page 129.]

4. 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 $n \geq 1$.

5. 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 $17 \equiv 1 \pmod{8}$.]

6. Let $p > 2$ be a prime and $k, n \geq 1$ be two integers. Show that there are $\dfrac{\varphi(p^n)}{(k, \varphi(p^n))}$ residues in $\mathbb{Z}_{p^n}^{\times}$ which are $k$-th powers.

7. Exercise 7.27 on page 141.

8. (A simplification of Exercise 7.22 to not necessitate quadratic reciprocity) Suppose $q$ and $r$ are distinct primes such that $q \equiv r \equiv 1 \pmod 4$ and $\left(\dfrac{q}{r}\right) = \left(\dfrac{r}{q}\right) = 1$. Show that $(x^2 - q)(x^2 - r)(x^2 - qr) = 0$ has no rational solutions but has solutions modulo $n$ for every positive integer $n$. [Hint: You might find Problem 5 useful.]