Math 465 Number Theory, Spring 2025, Problems 9

Return by Monday 24th March

1. (i) Let $S(p,a,b,c) = \sum_{x=1}^{p} \left(\frac{ax^2+bx+c}{p}\right)_L$. Show that if $p \nmid a$, then $S(p,a,b,c) = \left(\frac{4a}{p}\right)_L S(p,1,0,4ac-b^2)$.

(ii) Show that $S(p,1,0,c) = \sum_{y=1}^{p} \left(\frac{y+c}{p}\right)_L \left(1 + \left(\frac{y}{p}\right)_L\right)$. (Hint: Note that for each y with $1 \le y \le p$ the number of solutions in x to $x^2 \equiv y \pmod p$ is $1 + \left(\frac{y}{p}\right)_L$)

(iii) Deduce that $S(p,a,b,c) = p\left(\frac{c}{p}\right)_L$ when $p|a$ and $p|b$, is 0 when $p|a$ and $p \nmid b$, and satisfies

$$S(p,a,b,c) = \begin{cases} \left(\frac{a}{p}\right)_L (p-1) & \text{when } p \nmid a \text{ and } p | b^2 - 4ac, \\ -\left(\frac{a}{p}\right)_L & \text{when } p \nmid a(b^2-4ac). \end{cases}$$

2. Suppose that p is an odd prime and define $S(a) = \displaystyle\sum_{x=1}^{p} \left(\frac{x^3+ax}{p}\right)_L$.

(i) Show that if $p \nmid r$ and $a \equiv r^2 b \pmod p$, then $S(a) = \left(\frac{r}{p}\right)_L S(b)$.

(ii) Show that for any quadratic non-residue n modulo p we have

$$\sum_{a=1}^{p} |S(a)|^2 = \frac{p-1}{2}|S(1)|^2 + \frac{p-1}{2}|S(n)|^2.$$

(iii) Show that $\displaystyle\sum_{a=1}^{p} |S(a)|^2 = p(p-1)\left(1 + (-1)^{(p-1)/2}\right)$. (Question 1 is useful.)

(iv) Show that for any a, $S(a)$ is an even integer.

(v) Show that if $p \equiv 1 \pmod 4$, then for any quadratic non-residue n modulo p,

$$|S(1)/2|^2 + |S(n)/2|^2 = p,$$

giving an explicit representation of p as the sum of two squares.

(vi) Show that if $p \equiv 3 \pmod 4$, then, for any integer a, $S(a) = 0$.

3. Find all solutions to the diophantine equation $x^2 + y^2 = 3z^2 + 3t^2$.

4. Show that every positive integer n can be written in the form

$$n = x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2.$$

Hint: Consider separately, (a) n even, (b) n is odd and the sum of three odd squares and an even square, (c) n is odd and the sum of an odd square and three even squares. It is also useful to know that $2y_1^2 + 2y_2^2$ is the sum of two squares, and that when $z_1 z_2$ is odd $z_1^2 + z_2^2 = 2\left(\frac{z_1+z_2}{2}\right)^2 + 2\left(\frac{z_1-z_2}{2}\right)^2$.