Math 465 Number Theory, Spring Term 2025, Solutions 9

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 $S(p,1,0,c) = \sum_{y=1}^p \left(\frac{y+c}{p}\right)_L \left(1+\left(\frac{y}{p}\right)_L\right)$. (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

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

(i) By completing the square, $S(p,a,b,c) =$

$$\left(\frac{4a}{p}\right)_L \sum_{x=1}^p \left(\frac{(2ax+b)^2+4ac-b^2}{p}\right)_L = \left(\frac{4a}{p}\right)_L S(p,1,0,4ac-b^2).$$

(ii) $\sum_{x=1}^p \left(\frac{x^2+c}{p}\right)_L =$

$$\sum_{y=1}^p \left(\frac{y+c}{p}\right)_L \sum_{\substack{x=1 \\ x^2\equiv y \mod p}}^p 1 = \sum_{y=1}^p \left(\frac{y+c}{p}\right)_L \left(1+\left(\frac{y}{p}\right)_L\right).$$

(iii) When $p|(a,b)$ we have $S(p,a,b,c) = p\left(\frac{c}{p}\right)_L$. When $p|a$ and $p \nmid b$ $S(p,a,b,c) = 0$ from class. When $p \nmid a$, by (i) and (ii) and the fact $\left(\frac{4}{p}\right)_L = 1$, we have $S(p,a,b,c) = \left(\frac{a}{p}\right)_L \sum_{y=1}^p \left(\frac{y+4ac-b^2}{p}\right)_L \left(1+\left(\frac{y}{p}\right)_L\right)$. The total contribution from the "1" here is 0 and the remainder is $\left(\frac{a}{p}\right)_L \sum_{y=1}^p \left(\frac{y^2+(4ac-b^2)y}{p}\right)_L$. Using the same idea as in question 4 of homework 7 this is $\left(\frac{a}{p}\right)_L \sum_{z=1}^{p-1} \left(\frac{1+(4ac-b^2)z}{p}\right)_L$ and the sum here is -1 when $p \nmid 4ac-b^2$ and $p-1$ otherwise.

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

(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 $\sum_{a=1}^{p} |S(a)|^2 = p(p-1)\left(1+(-1)^{(p-1)/2}\right)$. (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, $S(a) = 0$.

(i) When $p \nmid r$ replace x by xr and the sum becomes $\left(\frac{r^3}{p}\right)_L S(b)$. (ii) By (i) when a is a QR we have $a \equiv r^2.1$ for some r and when a is a QNR, then $a \equiv r^2 n$ for some r. Note also that $S(0) = 0$. (iii) Squaring out and changeing the summation order gives

$$\sum_{x=1}^{p}\sum_{y=1}^{p}\sum_{a=1}^{p}\left(\frac{xya^2 + (x^3y + y^3x)a + x^3y^3}{p}\right)_L.$$

If $x = 0$ or $y = 0$, then the inner sum is 0. Thus we may suppose $1 \le x \le p-1$, $1 \le y \le p-1$. Now "$4ac - b^2$" $= (x^3y + y^3x)^2 - 4x^4y^4 = (x^3y - y^2x)^2$ and this is divisible by p if and only if $x^2 \equiv y^2$, i.e. $x \equiv \pm y$. Thus the sum is $\sum_{x=1}^{p-1} \sum^{p-1}{}_{\substack{y=1 \\ y\equiv\pm x \mod p}} p\left(\frac{xy}{p}\right)_L - \sum_{x=1}^{p-1}\sum_{y=1}^{p-1} 1\left(\frac{xy}{p}\right)_L$. The second mutliple sum is 0 and in the first the contribution from $y \equiv x$ is $p(p-1)$ and the contribution from the $y \equiv -x$ is $p(p-1)\left(\frac{-1}{p}\right)_L$. (iv) Each term contributes ±1 unless $p | x^3 + xa$ and the number of such terms is 1 or 3, depending on whether $-a$ ia a QNR or QR. The total number of terms is p, which is odd. (v) Combining (ii) and (iii) $p = |S(1)|^2/4 + |S(n)|^2/4$. (vi) In (iii) the RHS is 0, but the terms on the left are all non-negative, so have to be 0.

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

This cannot be positive, because if it were the LHS would have an even power of 3 in its canonical decomposition whereas the RHS would have an odd power. Thus the only solution is $x = y = z = t = 0$.

4. Show that every positive integer n can be written in the form $n = x_1^2 + x_2^2 + 2x_3^2 + 2x_4^2$.

(a) If n is even, then $n/2 = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and so $n = (x_1 - x_2)^2 + (x_1 + x_2)^2 + 2x_3^2 + 2x_4^2$. If n is odd then in it is either the sum of an odd square and three even ones, or three odd squares and one even one. In the former case (b) we have, when x_3 and x_4 are even, $n = x_1^2 + x_2^2 + 4y_3^2 + 4y_4^2 = x_1^2 + x_2^2 + 2(y_3 - y_4)^2 + 2(y_3 + y_4)^2$ and in the latter case (c), when x_1 and x_2 are odd we have $n = 2((x_1 - x_2)/2)^2 + 2((x_1 + x_2)/2)^2 + x_3^2 + x_4^2$.