MATH 465 NUMBER THEORY, SPRING 2025, SOLUTIONS 7

1. Prove that if p is an odd prime, then $\displaystyle\sum_{x=1}^{p}\sum_{y=1}^{p}\left(\frac{xy+1}{p}\right)_L = p.$

If $x \neq p$, then the inner sum is 0 by an example in the notes. If $x = p$ the inner sum is $\sum_{y=1}^{p}\left(\frac{1}{p}\right)_L = p$.

2. Suppose that p is an odd prime and $p \nmid a$. Show that the number of solutions to $ax^2+bx+c \equiv 0 \pmod{p}$ is $1+\left(\frac{b^2-4ac}{p}\right)_L$.

Since $p \nmid 2a$ we may multiply by $4a$ so that we are counting the number of solutions of $4a^2x^2+4abx+4ac \equiv 0 \pmod{p}$. That is, $(2ax+b)^2 \equiv (b^2-4ac) \pmod{p}$ and since $2ax+b$ runs over a complete set of residues as x does the number of solutions of this is the number of solutions of $y^2 \equiv b^2-4ac \pmod{p}$.

3. Let p be an odd prime and g be a primitive root modulo p. (i) Prove that the quadratic residues are precisely the residue classes g^{2k} with $0 \le k < \frac{1}{2}(p-1)$. (ii) Show that when $p > 3$ the sum of the quadratic residues modulo p is the 0 residue.

(i) The g^{2k} with $0 \le k < \frac{1}{2}(p-1)$ are distinct modulo p since g is a primitive root modulo p, and are clearly quadratic residues. Since there are exactly $\frac{1}{2}(p-1)$ such residues we have then all. (ii) By (i) the sum in question is $\equiv s = \sum_{k=0}^{\frac{p-3}{2}} g^{2k}$. Now $(g^2-1)s = \sum_{k=0}^{\frac{p-3}{2}}\left(g^{2k}-g^{2k+2}\right) = 1-g^{p-1} \equiv 0 \pmod{p}$. But $g^2 \not\equiv 1 \pmod{p}$.

4. Recall that for every reduced residue class r modulo p there is a unique reduced residue class s_r modulo p such that $1 \equiv rs_r \pmod{p}$, and that for every reduced residue class s modulo p there is a unique r such that $s_r \equiv s \pmod{p}$. Hence prove that if p is an odd prime, then

$$\sum_{r=1}^{p-1}\left(\frac{r(r+1)}{p}\right)_L = \sum_{r=1}^{p-1}\left(\frac{1+s_r}{p}\right)_L = \sum_{s=1}^{p-1}\left(\frac{1+s}{p}\right)_L = -1.$$

In the notation above thre sum in question is $\sum_{r=1}^{p-1}\left(\frac{r(r+rs_r)}{p}\right)_L$. The general term here is $\left(\frac{r^2(1+s_r)}{p}\right)_L = \left(\frac{1+s_r}{p}\right)_L$ using the multiplicative property of the Legendre symbol and the fact that $p \nmid r$ for each term. Now from $s_r \equiv s_{r'} \pmod{p}$ we would infer that $rs_r \equiv 1 \equiv r's_{r'} \equiv r's_r \pmod{p}$, whence $r \equiv r' \pmod{p}$. Thus the s_r are distinct modulo p and therefore range over a reduced set of residues as r does. Hence the sum $\sum_{r=1}^{p-1}\left(\frac{1+s_r}{p}\right)_L$ consists of the terms in the sum $\sum_{s=1}^{p-1}\left(\frac{1+s}{p}\right)_L$ in some order. Here the numbers $1+s$ run over the numbers from 2 to p. Thus $\displaystyle\sum_{s=1}^{p-1}\left(\frac{1+s}{p}\right)_L = -\left(\frac{1}{p}\right)_L + \sum_{t=1}^{p}\left(\frac{t}{p}\right)_L = -1$ since the sum is 0.