ALGEBRA: HOMEWORK 2

Problem 1. *Let $p = 1$ (mod 4) be a prime number. Then*

$$\sum_{a=1}^{p-1} (\frac{a}{p}) a = 0$$

Proof. If $p = 1$ mod 4, $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = 1$ and $(\frac{-a}{p}) = (\frac{-1}{p})(\frac{a}{p}) = (\frac{a}{p})$. So

$$2\sum_{a=1}^{p-1} (\frac{a}{p}) a = \sum_{a=1}^{p-1} (\frac{a}{p}) a + \sum_{a=1}^{p-1} (\frac{p-a}{p})(p-a) = p\sum_{a=1}^{p-1} (\frac{a}{p}) = 0.$$

□

Problem 2. *Let $p > 5$ be prime. Show that*

$$\sum_{a=1}^{p-1} (\frac{a}{p}) a^2 = 0 \text{ (mod p)}$$

Proof.

$$\sum_{a=1}^{p-1} (\frac{a}{p}) a^2 = \sum_{a=1}^{p-1} a^{\frac{p-1}{2}} a^2 = \sum_{a=1}^{p-1} a^{\frac{p+3}{2}} \text{ (mod p)}$$

since $p > 5$, we have $p - 1 > \frac{p+3}{2}$, and therefore $p - 1 \nmid \frac{p+3}{2}$. Then we get

$$\sum_{a=1}^{p-1} (\frac{a}{p}) a^2 = \sum_{a=1}^{p-1} a^{\frac{p+3}{2}} = 0 \text{ (mod p)}.$$

□

Problem 3. *For prime $p \nmid b$*

$$\sum_{a=1}^{p-1} (\frac{a(a+b)}{p}) = -1.$$

Proof. It is easy to see in modulo p,

$$\{a^{-1}b : a = 1, ..., p-1\} = \{1, ..., p-1\}$$

and then

$$\sum_{a=1}^{p-1} (\frac{a(a+b)}{p}) = \sum_{a=1}^{p-1} (\frac{1+a^{-1}b}{p}) = \sum_{x=1}^{p-1} (\frac{1+x}{p}) = \sum_{x=1}^{p} (\frac{x}{p}) - (\frac{1}{p}) = -1.$$

□

Problem 4. Find the number of non-trivial solutions of

$$x^3 + y^3 + z^3 + t^3 = 0 \text{ (mod 5)}$$

Proof. (By Vladimir Kobzar) Each element of $\mathbb{Z}/5$ is a cube. Therefore, if for arbitrary x, y, z, there always exists unique t such that $t^3 = -(x^3 + y^3 + z^3)$. Therefore we have $5 \cdot 5 \cdot 5 = 125$ solutions, of which 124 are non-trivial. □

Problem 5. *Show that the congruence*

$$x^4 - 17y^4 \equiv 2z^2 \text{ (mod p)}$$

has nontrivial solutions for all primes p.

Proof. For $p = 2, 3, 5, 13, 19$, we can construct solutions directly.

Now we assume $p \neq 2, 3, 5, 13, 19$ and there is no nontrivial solutions (x, y, z) to this equation. Let QR be the set of quadratic residues of p.

Let $x = 1, y = 0$ and we have that $1 = 2z^2 \pmod{p}$ has no solutions and then $2 \notin QR$.

Let $y = 1$ and we have that $x^4 - 17 = 2z^2 \pmod{p}$ has no solutions. By adding some constant to both sides we have that

$$x^4 - 5^2 = 2(z^2 - 4) \tag{1}$$

$$x^4 - 3^2 = 2(z^2 + 4) \tag{2}$$

$$x^4 - 6^2 = 2(z^2 - 19/2) \tag{3}$$

$$x^4 - 13^2 = 2(z^2 - 76) \tag{4}$$

$$x^4 - 15^2 = 2(z^2 - 104) \tag{5}$$

all have no solutions modulo p. Now
In (1) let $z = 2$ and we know $5 \notin QR, -5 \notin QR$ and then $-1 \in QR$;
In (2) let $z^2 = -4 \in QR$, and we know $3 \notin QR$, and $6 = 2 \cdot 3 \in QR$;
In (3) let $x^2 = 6 \in QR$, and we know $19/2 \notin QR$, and $19 \in QR$;
In (4) let $z^2 = 2^2 \cdot 19 \in QR$, and then $13 \notin QR, 104 = 2^3 \cdot 13 \in QR$;
In (5) let $x^2 = 15 = 3 \cdot 5 \in QR$, and $z^2 = 104 \in QR$ and we find a solution. Contradictory! □