

MAT 535: HOMEWORK 9 - SOLUTION OF PROBLEM 3

3. Let η be a primitive p -th root of unity in \mathbb{C} . Show that if p is prime, $p > 2$, then the cyclotomic field $\mathbb{Q}(\eta)$ contains either \sqrt{p} or $\sqrt{-p}$. [Hint: take a be the generator of the cyclic group $(\mathbb{Z}_p)^*$; show that the elements

$$\varepsilon_1 = \eta^a + \eta^{a^3} + \cdots + \eta^{a^{p-2}}; \quad \varepsilon_2 = \eta^{a^2} + \eta^{a^4} + \cdots + \eta^{a^{p-1}}$$

satisfy a quadratic equation.]

Solution:

We will show that $\varepsilon_1, \varepsilon_2$ are roots of a quadratic polynomial with coefficients in \mathbb{Q} . To find these coefficients, note:

$$\varepsilon_1 + \varepsilon_2 = \sum_{i \in \mathbb{Z}_p^*} \eta^i = -1$$

because $\sum_{i \in \mathbb{Z}_p} \eta^i = 0$. Similarly,

$$\varepsilon_1 \varepsilon_2 = \sum_{i \in \mathbb{Z}_p} n_i \eta^i$$

where

$$n_i = \text{number of ways to write } i = a^e + a^o, \quad e \in E, o \in O$$

and E, O are sets of even (respectively, odd) elements in \mathbb{Z}_{p-1} .

Lemma. *If $p = 4k + 1$, then*

$$n_i = \frac{p-1}{4} = k \text{ for all } i \neq 0 \\ n_0 = 0$$

If $p = 4k + 3$, then

$$n_i = \frac{p-3}{4} = k \text{ for all } i \neq 0 \\ n_0 = \frac{p-1}{2} = 2k + 1$$

(the proof of the lemma is below).

From this lemma, it follows that if $p = 4k + 1$, then

$$\varepsilon_1 \varepsilon_2 = \sum_{i \in \mathbb{Z}_p} n_i \eta^i = k \left(\sum_{i \in \mathbb{Z}_p^*} \eta^i \right) = -k$$

and therefore, $\varepsilon_1, \varepsilon_2$ are roots of polynomial $x^2 + x - k = 0$, whose discriminant is $D = 1 - 4(-k) = 1 + 4k = p$, so $\varepsilon_{1,2} = \frac{-1 \pm \sqrt{p}}{2}$.

Similarly, that if $p = 4k + 3$, then

$$\varepsilon_1 \varepsilon_2 = \sum_{i \in \mathbb{Z}_p} n_i \eta^i = (2k + 1) + k \left(\sum_{i \in \mathbb{Z}_p^*} \eta^i \right) = k + 1$$

and therefore, $\varepsilon_1, \varepsilon_2$ are roots of polynomial $x^2 + x + (k + 1) = 0$, whose discriminant is $D = 1 - 4(k + 1) = -4k + 3 = -p$, so $\varepsilon_{1,2} = \frac{-1 \pm \sqrt{-p}}{2}$.

Proof of the lemma. First, it is easy to see that $n_{ai} = n_i$; thus, since every non-zero element in \mathbb{Z}_p can be written as $a^m \cdot 1$, we see that $n_i = n_1$ for all $i \neq 0$.

Next, n_0 = number of ways to write $-1 = a^{e-o}$; since it is well known that $-1 = a^{(p-1)/2}$, we see that

$$n_0 = \text{number of ways to write } (p-1)/2 = e - o \text{ in } \mathbb{Z}_{p-1}$$

which easily gives the formula for n_0 .

Finally, since $\sum_{i \in \mathbb{Z}_p} n_i = |E| \cdot |O| = \left(\frac{p-1}{2}\right)^2$, we get

$$n_i = \frac{\left(\frac{p-1}{2}\right)^2 - n_0}{p-1}$$

□