CHAPTER 5, QUESTION 21

21. Let p be an odd prime. Let a and c be integers with

$$a \equiv 1 \pmod{2}, \quad \left(\frac{a^2-4c}{p}\right) = -1.$$

Prove that

$$x^4 + ax^2 + px + c$$

is irreducible in $\mathbb{Z}[x]$.

Solution. Suppose that $x^4 + ax^2 + px + c$ has a linear factor in $\mathbb{Z}[x]$. Then there exists $e \in \mathbb{Z}$ such that

$$e^4 + ae^2 + pe + c = 0.$$

Hence

$$e^4 + ae^2 + c \equiv 0 \pmod{p}.$$

Thus

$$(2e^2 + a)^2 = 4e^4 + 4ae^2 + a^2 \equiv a^2 - 4c \pmod{p}$$

so that

$$\left(\frac{a^2-4c}{p}\right) = 0 \text{ or } 1,$$

contradicting $\left(\frac{a^2-4c}{p}\right) = -1$. Hence x^4+ax^2+px+c has no linear factors in $\mathbb{Z}[x]$.

Next suppose that x^4+ax^2+px+c has a quadratic factor in $\mathbb{Z}[x]$. Then there exist $A, B, C, D \in \mathbb{Z}$ such that

$$x^4 + ax^2 + px + c = (x^2 + Ax + B)(x^2 + Cx + D).$$

Equating coefficients we obtain

$$\begin{aligned} A + C &= 0, & (1)\\ AC + B + D &= a, & (2)\\ AD + BC &= p, & (3)\\ BD &= c. & (4) \end{aligned}$$

From (1) we have $C = -A$. Then (2) and (3) give $A \mid p$ and

$$\begin{aligned} B + D &= a + A^2, \\ D - B &= p/A. \end{aligned}$$

Hence

$$2B = a + A^2 - \frac{p}{A},$$
$$2D = a + A^2 + \frac{p}{A}.$$

As $A \mid p$ and p is ann odd prime, we have $A \in \{\pm 1, \pm p\}$ so that A is odd. Thus, as a is odd, we see that $a + A^2 \pm \frac{p}{A}$ is odd, a contradiction.

This completes the proof that $x^4 + ax^2 + px + c$ is irreducible in $\mathbb{Z}[x]$.

■

June 23, 2004