EXERCISES 7, QUESTION 1

1. Let $D$ denote the discriminant of

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Prove that

$$D \equiv 0 \text{ or } 1 \pmod 4.$$

Solution. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Let $\theta_1, \ldots, \theta_n$ be the $n$ complex roots of $f(x)$. The discriminant $D$ of $f$ is given by

$$\prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2.$$

Clearly $D$ is a symmetric polynomial in $\theta_1, \ldots, \theta_n$ so by the symmetric function theorem $D$ is a polynomial with rational coefficients in the elementary symmetric polynomials

$$\begin{aligned} \theta_1 + \cdots + \theta_n &= -a_{n-1} \in \mathbb{Z}, \\ \theta_1\theta_2 + \cdots + \theta_{n-1}\theta_n &= a_{n-2} \in \mathbb{Z}, \\ &\cdots \\ \theta_1\theta_2 \cdots \theta_n &= (-1)^n a_0 \in \mathbb{Z}, \end{aligned}$$

showing that $D \in \mathbb{Q}$. Each of $\theta_1, \ldots, \theta_n$, being a root of a monic polynomial with integer coefficients, is an algebraic integer, and so $D$ is an algebraic integer. Hence $D$ is both rational and an algebraic integer so $D \in \mathbb{Z}$.

Now we have the value of determinant

$$\begin{vmatrix} \theta_1^{n-1} & \theta_1^{n-2} & \cdots & \theta_1 & 1 \\ \theta_2^{n-1} & \theta_2^{n-2} & \cdots & \theta_2 & 1 \\ . & . & \cdots & . & . \\ \theta_n^{n-1} & \theta_n^{n-2} & \cdots & \theta_n & 1 \end{vmatrix} = \prod_{1 \le i < j \le n} (\theta_i - \theta_j).$$

In the expansion of the above determinant there are $n!$ terms, half with a plus sign and half with a minus sign. Let the sum of those with a plus sign be $\lambda$ and those with the minus sign $\mu$ so that

$$\prod_{1 \leq i < j \leq n} (\theta_i - \theta_j) = \lambda - \mu.$$

Set $A = \lambda + \mu$ and $B = \lambda\mu$ so that

$$D = (\lambda - \mu)^2 = (\lambda + \mu)^2 - 4\lambda\mu = A^2 - 4B.$$

As $\theta_1, \ldots, \theta_n$ are algebraic integers so are $\lambda$ and $\mu$. Thus $A$ and $B$ are algebraic integers. As $A$ is a symmetric function of $\theta_1, \ldots, \theta_n$ with rational coefficients arguing as before $A \in \mathbb{Q}$. Hence $A \in \mathbb{Z}$. Then

$$B = \frac{A^2 - D}{4} \in \mathbb{Q}.$$

But $B$ is an algebraic integer so $B \in \mathbb{Z}$. Hence

$$D \equiv A^2 \equiv 0, 1 \pmod{4}. \qquad \blacksquare$$

February 12, 2004