Irreducibility in $\mathbb{Q}[x]$

Observation: Let $p(x) = \frac{b_3}{c_3}x^3 + \frac{b_2}{c_2}x^2 + \frac{b_1}{c_1}x + \frac{b_0}{c_0}$, where $\forall 1 \le i \le 3$, $b_i, c_i \in \mathbb{Z}$. Then

$$p(x) = \frac{1}{c_0c_1c_2c_3}\left[b_3c_0c_1c_2x^3 + b_2c_0c_1c_3x^2 + b_1c_0c_2c_3x + b_0c_1c_2c_3\right]$$

Let $d = \gcd(b_3c_0c_1c_2, b_2c_0c_1c_3, b_1c_0c_2c_3, b_0c_1c_2c_3)$ and let

$$a_3 = \frac{b_3c_0c_1c_2}{d},\ a_2 = \frac{b_2c_0c_1c_3}{d},\ a_1 = \frac{b_1c_0c_2c_3}{d},\ a_0 = \frac{b_0c_1c_2c_3}{d}.$$

Then $p(x) = \frac{d}{c_0c_1c_2c_3}\left[a_3x^3 + a_2x^2 + a_1x + a_0\right]$ and $\gcd(a_0, a_1, a_2, a_3) = 1$

$= \frac{r}{s}\left[a_3x^3 + a_2x^2 + a_1x + a_0\right]$ where $\frac{r}{s} = \frac{d}{c_0c_1c_2c_3}$ and $\gcd(r, s) \ge 1$.

Lemma: Let $p(x) \in \mathbb{Q}[x]$. Then

$$p(x) = \frac{r}{s}\left(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0\right)$$

where $r, s, a_0, \ldots, a_n \in \mathbb{Z}$, $\gcd(a_i, a_j) = 1\ \forall\ 1 \le i \ne j \le n$, and $\gcd(r, s) = 1$.

Theorem (Gauss's Lemma): Let $f(x)$ be a monic polynomial with integer coefficients. Then $f(x)$ factors into a product of polynomials of degrees m and n in $\mathbb{Q}[x]$ if and only if $f(x)$ factors as a product of monic polynomials of degrees m, n in $\mathbb{Z}[x]$.

Proof: ($\Leftarrow$) Immediate.

($\Rightarrow$) Suppose $f(x) = \alpha(x)\beta(x)$, where $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ and $\deg(\alpha(x)) = m$ and $\deg(\beta(x)) = n$. By the previous lemma, we can write

$$\alpha(x) = \frac{c_1}{d_1}\left(a_mx^m + \cdots + a_0\right) \qquad \beta(x) = \frac{c_2}{d_2}\left(b_nx^n + \cdots + b_0\right)$$

where $c_1, c_2, d_1, d_2 \in \mathbb{Z}$, $\gcd(c_i, d_i) = 1$ for $i = 1, 2$.

Let $\alpha_1(x) = a_m x^m + \cdots + a_0$ and $\beta_1(x) = b_n x^n + \cdots + b_0$. Now $f(x) = \frac{c_1 c_2}{d_1 d_2}\alpha_1(x)\beta_1(x) = \frac{c}{d}\alpha_1(x)\beta_1(x)$, where $\frac{c}{d} = \frac{c_1 c_2}{d_1 d_2}$ and $\gcd(c,d) = 1$. Bec. $f(x)$ is monic, then $\frac{c a_m b_n}{d} = 1$ implies that $c a_m b_n = 1$. Now we consider the following cases

Case 1: If $d = 1$, then $c a_m b_n = 1$, so

c	a_m	b_n	$a(x)$	$b(x)$
1	1	1	$\alpha_1(x)$	$\beta_1(x)$
1	−1	−1	$-\alpha_1(x)$	$-\beta_1(x)$
−1	1	−1	$\alpha_1(x)$	$-\beta_1(x)$
−1	−1	1	$-\alpha_1(x)$	$\beta_1(x)$.

Case 2: If $d > 1$, let p be a prime factor of d. Since $\gcd(c,d) = 1$ and $p \nmid c$. Then $df(x) = c\alpha_1(x)\beta_1(x) = 0$. Bec. $p \nmid c$, then $\alpha_1(x)\beta_1(x) = 0 \bmod p$. which is absurd, because neither $\alpha_1(x)$ nor $\beta_1(x)$ is the zero polynomial. and $\mathbb{Z}_p[x]$ is an integral domain.

Definition: A polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ is called a **primitive** if $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Remark: In Case 2, if $a(x)$ and $\beta(x)$ are primitive polynomials in $\mathbb{Z}[x]$. then so is $\alpha_1(x)$ and $\beta_1(x)$

Corollary: Let $p(x) = a_n x^n + \cdots + a_0$ be a polynomial in $\mathbb{Z}[x]$ with $a_0 \neq 0$. If $f(x)$ has a root in $\mathbb{Q}[x]$. then $p(x)$ has a root $\alpha \in \mathbb{Z}$ with $\alpha \mid a_0$.

Proof: Suppose $f(r) = 0$ for some $r \in \mathbb{Q}$. By a previous Corollary, $f(x) = (x - r)g(x)$ and so by the previous lemma,

$f(x) = a(x)b(x)$, where $a(x)$ and $b(x)$ are in $\mathbb{Z}[x]$ and are monic, and $\deg(a(x)) = 1$.

Let $a(x) = x - \alpha$ and $b(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0$

Then $f(x) = (x-\alpha)(x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_0)$. Then α is a root of $f(x)$ and $a_0 = -\alpha b_0 \Rightarrow \alpha \mid a_0$.