More about polynomials.

- Let $p(x) \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field. Then if $\deg(p(x)) = 2$ or 3, then $p(x)$ is reducible $\iff$ $p(x)$ has a zero in $\mathbb{F}$ $\iff$ $p(x)$ has a linear factor.

Pf. The only possible factorization is
$p(x) = p_1(x) \cdot p_2(x)$ with $p_1(x)$ degree 1, $p_2(x)$ degree 1 or 2.
$\iff p_1(x) = ax + b$ with $a, b \in \mathbb{F}$, $a \neq 0$.
$\iff x = -ba^{-1}$ is a root of $p(x)$. ☑

- Integer coefficient polynomials $p(x) \in \mathbb{Z}[x]$.

The content of a polynomial $p(x) \in \mathbb{Z}[x]$ is the |GCD| of the coefficients. If the content of $p(x)$ is 1, we say $p(x)$ is primitive.

Thm (Gauss Lemma) The product of two primitive polynomials in $\mathbb{Z}[x]$ is primitive.

Pf: Suppose that $f(x)$ & $g(x)$ are primitive polynomials in $\mathbb{Z}[x]$. Let $p(x) = f(x)g(x)$ — suppose content of $p(x) \neq 1$. Let q be a prime factor of this content, and now reduce all the coefficients mod q.

$p(x) \longrightarrow \overline{p(x)}$ (means $p(x)$ mod q)

$\Rightarrow 0 = \overline{p(x)} = \overline{f(x)}\,\overline{g(x)}$, $\overline{f(x)}, \overline{g(x)} \in \mathbb{Z}_q[x]$.

$\mathbb{Z}_q$ is a field $\Rightarrow$ $\mathbb{Z}_q[x]$ an integral domain

$\Rightarrow \overline{f(x)}$ or $\overline{g(x)} = 0$. WLOG, suppose $\overline{f(x)} = 0$.

Then q is a factor of all the coefficients of f

$\Rightarrow$ content of $f(x) \neq 1$. Contradiction.

$\therefore$ content of $p(x) = 1$.

Cor. If $f(x) \in \mathbb{Z}[x]$ factors in $\mathbb{Q}[x]$ into irreducibles, it also factors in $\mathbb{Z}[x]$ into irreducibles, where each factor in the $\mathbb{Q}[x]$ factorization is an associate of one of the ones in the $\mathbb{Z}[x]$ factorization.

Example $4x^2 - 1 = (2x-1)(2x+1) = (x-\frac{1}{2})(4x+2)$

Proof of Cor:

If $f(x) \in \mathbb{Z}[x]$, and $f(x)$ factors as

$f(x) = g_1(x) \cdots g_k(x)$, $g_j(x) \in \mathbb{Q}[x]$ $\forall j$,

then we can multiply each factor by an integer to make it in $\mathbb{Z}[x]$, ie $n_j g_j(x) \in \mathbb{Z}[x]$ for some $n_j \in \mathbb{Z} \setminus \{0\}$.

$\Rightarrow f(x) \cdot n_1 n_2 \cdots n_k = (n_1 g_1(x))(n_2 g_2(x)) \cdots (n_k g_k(x))$

$\in \mathbb{Z}[x]$

Let c be the content of f, so $f(x) = c\,\tilde{f}(x)$, where $\tilde{f}(x)$ is primitive

$\Rightarrow \quad c n_1 n_2 \cdots n_k f(x) = \underbrace{(n_1 g_1(x)) \cdots (n_k g_k(x))}_{\text{Content}} = \#$

$= c n_1 n_2 \cdots n_k$

$\Rightarrow \quad \tilde{f}(x) = \dfrac{(n_1 g_1(x)) \cdots (n_k g_k(x))}{c n_1 n_2 \cdots n_k}$

(content g_1 = a_1, content g_k = a_k, $a_1 a_2 \cdots a_k$)

$\tilde{f}(x) = \dfrac{n_1 g_1(x)}{a_1} \tilde{g_1}(x) \cdots \dfrac{n_k g_k(x)}{a_k} \tilde{g_k}(x) \in \mathbb{Z}[x]$

$\tilde{f}(x)$: content 1. $\tilde{g_1}(x) \cdots \tilde{g_k}(x)$: rearrange the factors

$\Rightarrow \quad c\tilde{f}(x) = f(x) = c\, \tilde{g_1}(x) \cdots \tilde{g_k}(x)\, c(n_1) \cdots (n_k)$

Other useful facts.

- If $p(x) \in \mathbb{F}[x]$,
  $p(x)$ is irreducible $\Leftrightarrow$ $\langle p(x) \rangle$ is maximal
  $\Leftrightarrow$ $\mathbb{F}[x] / \langle p(x) \rangle$ is a field.

- If R is a UFD, then $R[x]$ is a UFD.

Cor: $\mathbb{F}[x_1, x_2, x_3]$ is a UFD for any field $\mathbb{F}$.

Proof: $\mathbb{F}$ is a field $\Rightarrow$ $\mathbb{F}$ is a UFD

$\Rightarrow \mathbb{F}[x_1]$ is a UFD.

$\Rightarrow \mathbb{F}[x_1][x_2] = \mathbb{F}[x_1, x_2]$ is a UFD.

$\Rightarrow \mathbb{F}[x_1, x_2, x_3]$ is a UFD. ☑

Fact: If p is a prime, then

$$\frac{x^p-1}{x-1} \text{ is irreducible in } \mathbb{Z}[x].$$

Pf: $\frac{x^p-1}{x-1} = 1+x+x^2+\cdots+x^{p-1}$