Rules for Factoring over $\mathbb{Q}$

1) Rational Root Test: If

$$f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$$

and $f(\frac{r}{s}) = 0$, where $r, s, \in \mathbb{Z}$ and $\gcd(r, s) = 1$, then $r|a_0$ and $s|a_n$.

2) Gauss's Lemma: If $f(x) \in \mathbb{Z}[x]$, then f is reducible in $\mathbb{Q}[x] \iff f$ has a proper factor in $\mathbb{Z}[x]$, i.e. a factor $g|_{\mathbb{Z}} f$ with $0 < \deg(g) < \deg(f)$.

Special Case: Method of comparing coefficients.

3) Modular Test: If $f = gh$ in $\mathbb{Z}[x]$ then

$$f \equiv g \cdot h \,(\mathrm{mod}\, p), \quad \text{for every prime } p.$$

Thus: if $\bar{f} \equiv f \,(\mathrm{mod}\, p)$ is irreducible in $\mathbb{F}_p[x]$ for one prime p such that $\deg(f) = \deg(\bar{f})$, then f is irreducible in $\mathbb{Z}[x]$.

Remark: To test for irreducibility in $\mathbb{F}_p[x]$, use:

Naive Method: Given f, calculate $\mathrm{rem}(f, g)$ for all (irreducible) polynomials $g \in \mathbb{F}_p[x]$ with $\deg(g) \leq \deg(f)/2$.

Example 1: Factor $f(x) = 2x^3 + 3x^2 + 2x + 3$.

Rational Root Test: $f(\frac{r}{s}) = 0 \Rightarrow r = \pm 1, \pm 3$, $s = 1, 2$.

Note: $r > 0 \Rightarrow f(\frac{r}{s}) > 0$, so we may assume $r < 0$.

Now $f(-1) = 2$, $f(-3) = -30$,

$f(-\frac{1}{2}) = 3$, $f(-\frac{3}{2}) = 0$.

Thus: $x = -\frac{3}{2}$ is a root of f, so $(x + \frac{3}{2}) | f(x)$

$\Rightarrow$ $(2x + 3) | f(x)$ (clear denominators)

$\Rightarrow$ $f(x) = (2x + 3)(x^2 + 1)$ (by long division)

Example 2: Factor $g(x) = x^4 + 5x^3 + 1$.

RRT fails for g, so try Modular Test with prime $p = 2$.

Write $\overline{g}(x) \equiv g(x) \pmod 2 \equiv x^4 + x^3 + 1$.

Now $\overline{g}(0) \equiv \overline{g}(1) \equiv 1 \pmod 2$, so x, $x + 1 \nmid \overline{g}$

$\Rightarrow$ $\overline{g}$ has no linear factors (in $\mathbb{F}_2[x]$).

Moreover, $\mathrm{rem}(\overline{g}, x^2 + x + 1) = x$ (by long division)

$\Rightarrow x^2 + x + 1 \nmid \overline{g}$

$\Rightarrow \overline{g}(x)$ is irreducible in $\mathbb{F}_2[x]$ (by "naive method")

$\Rightarrow g(x)$ is irreducible in $\mathbb{Z}[x]$ (Modular Test)

$\Rightarrow g(x)$ is irreducible in $\mathbb{Q}[x]$ (Gauss's Lemma)

4) Eisenstein's Criterion: Let

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

be an integer polynomial. If there exists a prime number p such that

(i) $p \nmid a_n$,

(ii) $p \mid a_i$, for $0 \leq i \leq n-1$,

(iii) $p^2 \nmid a_0$,

then $f(x)$ is irreducible over $\mathbb{Q}$.

Remark: This useful criterion was discovered by G. Eisenstein (1823–1852). It can be proven by using the modular test.

Example 3: If $a \in \mathbb{Z}$ and if there is a prime $p \mid a$ such that $p^2 \nmid a$, then $x^n - a$ is irreducible over $\mathbb{Q}$, for every $n \geq 1$. In particular, $\sqrt[n]{a}$ is irrational.