Let $F$ be a field, $F[x] = \text{ring of polynomials with coefficients in } F$. Let's compare $F[x]$ with the ring $\mathbb{Z}$ of integers.

<table>
<thead>
<tr>
<th>Comparisons of $\mathbb{Z}$ vs $F[x]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Z}$</td>
</tr>
<tr>
<td>infinite? Yes</td>
</tr>
<tr>
<td>integral domain Yes</td>
</tr>
<tr>
<td>unit group ${\pm 1}$</td>
</tr>
<tr>
<td>division algorithm $n = mq + r$</td>
</tr>
<tr>
<td>$0 &lt; r &lt; m$</td>
</tr>
<tr>
<td>divisibility $m</td>
</tr>
<tr>
<td>prime $p &gt; 1, p = ab$ $(\Rightarrow)$</td>
</tr>
<tr>
<td>$a$ or $b = \text{unit}$</td>
</tr>
<tr>
<td>Unique Factorization into primes $n = \pm 1 \cdot p_1 \cdot p_2 \cdots p_r$ for primes $p_i$ not necessarily distinct (unique up to order)</td>
</tr>
<tr>
<td>$f(x)$ not necessarily distinct (unique up to order)</td>
</tr>
<tr>
<td>$f(x)$ is monic irreducible</td>
</tr>
<tr>
<td>Factorization $f(x)$ unique up to order</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>$I = \langle n \rangle$</td>
</tr>
<tr>
<td>every ideal</td>
</tr>
<tr>
<td>principal</td>
</tr>
<tr>
<td>maximal ideal</td>
</tr>
<tr>
<td>$\mathbb{Z}/I$</td>
</tr>
<tr>
<td>$=\text{field when}$</td>
</tr>
<tr>
<td>$I$ maximal</td>
</tr>
<tr>
<td>$\gcd(12, 8) = 4$</td>
</tr>
<tr>
<td>$= 12x + 8y$</td>
</tr>
<tr>
<td>$\gcd$ computable</td>
</tr>
<tr>
<td>Euclid's Lemma</td>
</tr>
<tr>
<td>$p \mid ab \iff p \mid a$ or $p \mid b$</td>
</tr>
<tr>
<td>$f(x) \mid a(x) b(x) \implies {f(x) \mid a(x) \text{ or } f(x) \mid b(x)}$</td>
</tr>
</tbody>
</table>

The proofs of these facts for $\mathbb{F}[x]$ are about the same as the proofs for $\mathbb{Z}$. 
**Facts about $F[x]$**

**Test for Irreducibility of** $f(x) \in F[x]$, $F$ = field

when degree $f = 2$ or $3$',

$f(x)$ has a non-trivial factorization $\iff$

$f(x) = g(x)h(x)$, deg $g +$ deg $h = \leq 3$

$\Rightarrow$ either $g$ or $h$ has degree $1$

$\Rightarrow (x-a)$ divides $f(x)$ for some $a \in F$, $a \neq 0$

$\Rightarrow (x-c)$ divides $f(x)$ for some $c \in F$, $c = b/a$

Here $f(c) = 0$

Conversely $f(c) = 0 \Rightarrow (x-c)$ divides $f(x)$

So the Irreducibility test says

$f(x) \in F[x]$, $F$ = field, degree $0 \leq 3$

is irreducible $\iff f(a) \neq 0 \forall a \in F$

This fails when $F = \mathbb{F}_6$

$f(x) = (2x+1)^2$ has no roots in $\mathbb{F}_6$

It works in $\mathbb{F}_3 [x]$ to find monic degree 2 polynomials $x^2+bx+c$, $b,c \in \mathbb{F}_3$

Irreducible ones have no roots: e.g.

$f(x) = x^2+1$, $f(0) = 1$, $f(1) = 2$, $f(-1) = 2$

$\mathbb{F}_p [x]/\langle f(x) \rangle$ is a field when

$f(x)$ irreducible by Cor. 1, p. 311

**Proof**

Uses Thm 14.4, p. 268 and fact that $\langle f(x) \rangle$ is a maximal ideal if $f(x)$ is irreducible.
To see this, note every ideal $I$ in $\mathbb{F}[x]$ is principal, $I = \langle h(x) \rangle$ some $h(x) \in \mathbb{F}[x]$ (of least degree).

$\langle \not f(x) \rangle < \langle h(x) \rangle$

$\Rightarrow h(x) \mid f(x)$; i.e. $f(x) = h(x) \cdot g(x)$

$h(x)$ irreducible $\Rightarrow \{\begin{cases} 
\text{either } h(x) = c \cdot f(x) \\
\text{or } h(x) = c \text{ some } c \in \mathbb{F}
\end{cases}$

$\Rightarrow \text{either } I = \langle f(x) \rangle \text{ or } I = \mathbb{F}[x]$

So $\langle f(x) \rangle$ maximal.

$\mathbb{Z}_p[x]/\langle f(x) \rangle$, $f(x) \in \mathbb{Z}_p[x]$ irreducible degree $n$

$\Rightarrow$ this field has $p^n$ elements.

**Proof**

Elements are remainders $r(x)$ of $h(x) \in \mathbb{Z}_p[x]$

upon division by $f(x)$;

$r(x) = a_{n-1}x^{n-1} + \ldots + a_1x + a_0$, $a_j \in \mathbb{Z}_p$

$\deg r < n$

How many remainders?

$\# \{ (a_{n-1}, \ldots, a_1, a_0) \mid a_j \in \mathbb{Z}_p \}$.
Example: $\mathbb{Z}_3 [x] / \langle x^2 + 1 \rangle \cong \{ a + bi \mid a, b \in \mathbb{Z}_3 \}$ isomorphic to a field with 9 elements.

Here left hand side consists of remainders $ax + b$, $a, b \in \mathbb{Z}_3$.

Map $x \mapsto i$

$ax + b \mapsto ai + b$

to identify both versions of the field.

Note: $x^2 + 1 = 0$ in our field.

Thus $x$ behaves like $i$.

For mod $\langle x^2 + 1 \rangle$ means "think $x^2 + 1 = 0$".

The quadratic formula works in $\mathbb{Z}_p$ as long as $p \neq 2$, $p$ = prime.

Given $ax^2 + bx + c = 0$, $a, b, c \in \mathbb{Z}_p$, $a \neq 0$.

Divide by $a$, (O.K. we're in a field)

$X^2 + \frac{b}{a}X = -\frac{c}{a}$

$p \neq 2 \Rightarrow X^2 + \frac{b}{a}X + \left(\frac{b}{2a}\right)^2 = -\frac{c}{a} + \left(\frac{b}{2a}\right)^2$

$\Rightarrow (X + \frac{b}{2a})^2 = \frac{-4ac + b^2}{4a^2}$
Set

\[ D = b^2 - 4ac = \text{discriminant} \]

**Case 1**

If \( D = r^2 \), some \( r \in \mathbb{Z}_p \)

\[
X = \frac{-b \pm r}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \in \mathbb{Z}_p
\]

**Case 2**

If \( D \neq r^2 \), \( \forall r \in \mathbb{Z}_p \),

\[
X = \frac{-b \pm \sqrt{D}}{2a} \in \mathbb{Z}_p
\]

*In some sense for \( p \neq 2 \) the quadratic formula works for all \( \mathbb{Z}_p \). But in case 2 the roots aren’t in \( \mathbb{Z}_p \).*

Here

\[
\sqrt{D} \in \mathbb{F}_p^2 = \mathbb{Z}_p[x]/\langle x^2 - r \rangle
\]

(field with \( p^2 \) elements, \( p \neq 2 \)).

When \( p \equiv 3 \pmod{4} \), we can introduce an analogue of \( i = \sqrt{-1} \), and do a similar thing to high school. Put \( x \in \mathbb{Z}_p[x] \).

But when \( p \equiv 1 \pmod{4} \), \(-1 \equiv r^2 \) some \( r \).

For example, \(-1 \equiv 2^2 \pmod{5} \). Later we’ll find there is only 1 field with \( p^2 \) elements (Gallian, p. 372).

**Notes**

1. When \( p = 2 \), the quadratic formula doesn’t make sense as \( \frac{1}{2} \) doesn’t make sense \( \pmod{2} \) as it is \( \frac{1}{0} \).

2. The situation is like the quadratic formula over \( \mathbb{R} \).
   - **Case 1**: \( b^2 - 4ac > 0 \Rightarrow \) roots real
   - **Case 2**: \( b^2 - 4ac < 0 \Rightarrow \) roots complex