Example: Construct a finite field of order $q\ (=3^2)$. We use the following characterizations proven previously.

Theorem: $f(x) \in F[x]$ is irreducible over F if and only if $\langle f(x)\rangle$ is a maximal ideal.

Theorem: $F[x]/\langle f(x)\rangle$ is a field if and only if $\langle f(x)\rangle$ is a maximal ideal of $F[x]$.

Let $h(x) \in F[x]$. Then by the division algorithm, $\exists g(x), r(x)$ s.t. $h(x) = g(x)f(x) + r(x)$. where $0 < \deg[r(x)) < \deg[f(x))$ or $r(x) = 0$.

$\langle f(x)\rangle$ is an ideal, so for $g(x) \in F[x]$, $g(x)f(x) \in \langle f(x)\rangle$. Thus, $h(x) + \langle f(x)\rangle = r(x) + \langle f(x)\rangle$. Then

$$F[x]/\langle f(x)\rangle = \{r(x) + \langle f(x)\rangle : r(x) = 0 \text{ or } 0 < \deg(r(x)) < \deg(f(x))\}.$$

Now take $F = \mathbb{Z}_3$. We seek an irreducible polynomial $f(x)$ of degree 2 over $\mathbb{Z}_3$. A polynomial $f(x) = x^2+1$ is irreducible since $f(0) = 1 \neq 0$, $f(1) = 1+1 = 2 \neq 0$, and $f(2) = 2^2+1 = 2 \neq 0$. Therefore, $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a finite field of order 9.

Observation: If $I = \langle x^2+1\rangle$, then the quotient ring

$$\mathbb{Z}_3[x]/\langle x^2+1\rangle = \{0+I,\ 1+I,\ 2+I,\ x+I,\ (x+1)+I,\ (x+2)+I,\ 2x+I,\ (2x+1)+I,\ (2x+2)+I\}.$$

Question: What is $[(2x+1)+I][(x+2)+I]$ over $\mathbb{Z}_3$?

$$[(2x+1)+I][(x+2)+I] = (2x+1)(x+2) + I$$

$$= 2x^2 + 4x + x + 2 + I = 2x^2 + 2x + 2 + I = 2(x^2+1) + 2x + I$$

$$= 2x + I.$$

Note: When $I = \langle x^2+1 \rangle$, then $x^2+1+I = 0+I \Rightarrow x^2+I = -1+I$

$\Rightarrow 2x^2+I = -2+I$. Using Long Division,

$$\begin{array}{r} 2 \\ x^2+1 \;\overline{)\; 2x^2+2x+2} \\ -(2x^2 \quad +2) \\ \hline -2x \end{array}$$

Therefore, $2x^2+2x+2 = 2(x^2+1) - 2x$

$\Rightarrow 2x^2+2x+2+I = -2x+I$

Example: Compute the multiplicative inverse in $\mathbb{Z}_n[x]/\langle f(x) \rangle$ in general.

If $r(x)+\langle f(x)\rangle = b+\langle f(x)\rangle$ for some $b \neq 0 \in F$, then

$(b+\langle f(x)\rangle)^{-1} = b^{-1} + \langle f(x)\rangle$. Let $(b+\langle f(x)\rangle)^{-1} = c+\langle f(x)\rangle$.

Then $(b+\langle f(x)\rangle)(c+\langle f(x)\rangle) = 1+\langle f(x)\rangle$.

$$bc + \langle f(x)\rangle = 1 + \langle f(x)\rangle$$

$$c + \langle f(x)\rangle = b^{-1} + \langle f(x)\rangle$$

Let $1 \leq \deg(r(x)) < \deg(f(x))$ and $f(x)$ be irreducible. Then $\gcd(r(x), f(x)) = 1$, so by Bezout's Theorem, $\exists\, s(x), t(x) \in F[x]$ such that $s(x)r(x) + t(x)f(x) = 1$. Since $\langle f(x)\rangle$ is an ideal, then $t(x)f(x) \in \langle f(x)\rangle$, and so

$$s(x)r(x) + \langle f(x)\rangle = 1 + \langle f(x)\rangle$$

$$(s(x)+\langle f(x)\rangle)(r(x)+\langle f(x)\rangle) = 1+\langle f(x)\rangle.$$

$$(r(x)+\langle f(x)\rangle)^{-1} = s(x)+\langle f(x)\rangle.$$

Example: Find $((2x+1)+\langle x^2+1\rangle)^{-1}$ in $\mathbb{Z}_3[x]/\langle x^2+1\rangle$.

By the division algorithm,

$x^2+1 = (2x+2)(2x+1)+2$ (1) and $2x+1 = 2(x)+1$. (2)

Then $\gcd(x^2+1, 2x+1) = 1$. Then doing the reverse Euclidean algorithm, by ② $1 = (2x+1) - 2x$ and because by ①

$2 = (x^2+1) - (2x+2)(2x+1)$, then

$$1 = (2x+1) - x((x^2+1) - (2x+2)(2x+1))$$

$$= (2x+1) - x(x^2+1) + x(2x+2)(2x+1)$$

$$= (2x+1)[1 - x(x^2+1) + x(2x+2)] \quad ③$$

$$= (2x+1)(2x^2+2x+2) + \langle x^2+1 \rangle$$

Hence $((2x+1) + \langle x^2+1 \rangle)^{-1} = 3x^2 + 2x + 1 + \langle x^2+1 \rangle$

$$= -2 + 2x + 1 + \langle x^2+1 \rangle$$

$$= 2x + 2 + \langle x^2+1 \rangle.$$