1. Euclidean Algorithm: Given polynomials $f(x), g(x) \in F[x]$ for F a field, with $\deg f(x) \le \deg g(x)$, we perform repeated polynomial division to write:

$$\begin{aligned}
f(x) &= q_1(x)g(x) + r_1(x) \\
g(x) &= q_2(x)r_1(x) + r_2(x) \\
&\vdots \\
r_i(x) &= q_{i+2}(x)r_{i+1}(x) + r_{i+2}(x) \\
&\vdots \\
r_{k-2}(x) &= q_k(x)r_{k-1}(x) + r_k(x) \\
r_{k-1}(x) &= q_{k+1}(x)r_k(x) + 0.
\end{aligned}$$

For consistency, we may denote $f(x) = r_{-1}(x)$ and $g(x) = r_0(x)$.

a. PROPOSITION: $r_k(x)$ is a polynomial divisor of $f(x)$ and $g(x)$.

Proof: We show $r_k \,|\, r_i$ by induction on $i = k, k{-}1, \ldots, 1, 0, -1$, ending with $r_k \,|\, r_0 = g$ and $r_k \,|\, r_{-1} = f$. The base cases $r_k \,|\, r_k, r_{k-1}$ are clear. Now assume inductively that $r_k \,|\, r_{i+1}, r_{i+2}, \ldots, r_k$. Then $r_k \,|\, q_{i+2}r_{i+1} + r_{i+2} = r_i$, so the induction proceeds, and the Proposition holds.

b. PROPOSITION: $r_k(x) = a(x)f(x) + b(x)g(x)$ for some $a(x), b(x) \in F[x]$.

Proof: We show $r_k = a_{i-1}r_{i-1} + b_{i-1}r_i$ by induction on $i = k{-}2, k{-}3, \ldots, 0, -1$, ending with $r_k = a_{-1}f + b_{-1}g$. The base case is $r_k = r_{k-2} - q_k r_{k-1}$. Now assume inductively that $r_k = a_{i+1}r_{i+1} + b_{i+1}r_{i+2}$. By definition $r_i = q_{i+2}r_{i+1} + r_{i+2}$, so:

$$\begin{aligned}
r_k &= a_{i+1}r_{i+1} + b_{i+1}r_{i+2} \;=\; a_{i+1}r_{i+1} + b_{i+1}(r_i - q_{i+2}r_{i+1}) \\
&= b_{i+1}r_i + (a_{i+1} - b_{i+1}q_{i+2})r_{i+1} \;=\; a_i r_i + b_i r_{i+1}.
\end{aligned}$$

c. PROPOSITION: The polynomial $d(x) = r_k(x)$ has the defining properties of a greatest common divisor $\gcd(f(x), g(x))$: namely $d(x) \,|\, f(x), g(x)$, and for any common divisor $c(x) \,|\, f(x), g(x)$, we have $c(x) \,|\, d(x)$.

Proof: We know $d = r_k \,|\, f, g$ by #1(a). Now if $c \,|\, f, g$, then by #1(b) we have:

$$c \,|\, (af + bg) = r_k = d.$$

Note: A gcd is unique up to multiplication by units: if d, e both have the defining properties, then $d|e$ and $e|d$, meaning $d = ae$ and $e = bd$, so that $d = abd$ and $ab = 1$. That is, d and e are multiples of each other by units (here, constant polynomials).

d. PROPOSITION: Any ideal $I \subset F[x]$ must be a principal ideal comprising all multiples of some $f(x) \in F[x]$: that is, $I = (f(x)) = \{q(x)f(x) \text{ for } q(x) \in F[x]\}$.

Proof: Except when $I = \{0\} = (0)$, we can find a non-zero element $f(x) \in I$ having minimal degree. By definition of ideals, $q(x)f(x) \in I$ for any $q(x)$, so $(f(x)) \subset I$.

For the reverse inclusion, take any $g(x) \in I$. We can write $g(x) = q(x)f(x) + r(x)$, where the remainder satisfies $r(x) = g(x) - q(x)f(x) \in I$ by the closure properties of an ideal, but also $\deg r(x) < \deg f(x)$. Since $f(x)$ has the lowest degree of any non-zero polynomial in I, we can only have $r(x) = 0$. That is, $g(x) = q(x)f(x) \in (f(x))$, and hence $I \subset (f(x))$. We conclude $I = (f(x))$.

2. We construct the field of 8 elements as the quotient ring:

$$\mathbb{F}_8 \;=\; \mathbb{F}_2[x]/I \;=\; \{\,\overline{f(x)} = f(x) + I \text{ for } f(x) \in \mathbb{F}_2[x]\,\},$$

for the principal ideal $I = (x^3{+}x{+}1) \subset \mathbb{F}_2[x]$.

If we define $\alpha = \overline{x} \in \mathbb{F}_8$, so that $f(\alpha) = \overline{f(x)}$, we can rewrite the definition:

$$\mathbb{F}_8 \;=\; \mathbb{F}_2[\alpha] = \{f(\alpha) \text{ for } f(x) \in \mathbb{F}_2[x]\}, \text{ where } \alpha^3{+}\alpha{+}1 = 0.$$

We proceed to prove the main properties of $\mathbb{F}_8$ from the definition.

a. CLAIM: $p(x) = x^3{+}x{+}1$ is an irreducible polynomial in $\mathbb{F}_2[x]$.
If the cubic $p(x)$ had a non-trivial factorization, at least one of the factors would have to be a linear polynomial $ax + b \in \mathbb{F}_2[x]$, meaning $p(x)$ would have a root $x = -\frac{b}{a} \in \mathbb{F}_2$. But $p(0) = p(1) = 1 \neq 0 \in \mathbb{F}_2$, so there can be no such factorization.
Note: Since $p(x)$ is irreducible, we can compute reciprocals in $\mathbb{F}_2[x]/(p(x))$ using the Euclidean Algorithm, so the quotient ring is in fact a field.

b. CLAIM: The set $\{1, \alpha, \alpha^2\}$ is a basis of $\mathbb{F}_8$ as a vector space over $\mathbb{F}_2$, and $\#\mathbb{F}_8 = 8$.
Proof: The set spans $\mathbb{F}_8$, since any element is of the form $f(\alpha)$ for a polynomial $f(x) = q(x)p(x) + r(x) \in \mathbb{F}_2[x]$ with $\deg r(x) < \deg p(x) = 3$. That is, $r(x) = a_0 + a_1 x + a_2 x^2$ for $a_i \in \mathbb{F}_2$, and:

$$f(\alpha) \;=\; q(\alpha)p(\alpha) + r(\alpha) \;=\; r(\alpha) \;=\; a_0 + a_1\alpha + a_2\alpha^2.$$

The set is linearly independent, since any linear relation $r(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 = 0 \in \mathbb{F}_8 = \mathbb{F}_2[x]/I$ must have $r(x) \in I = (p(x))$. That is, $p(x)$ of degree 3 divides $r(x)$ of degree ≤ 2, which can only mean $r(x) = 0$ and $a_0 = a_1 = a_2 = 0$, allowing only the trivial linear relation.

Thus, any element of $\mathbb{F}_8$ can be written as $a_0 + a_1\alpha + a_2\alpha^2$ for unique coordinates $a_0, a_1, a_2 \in \mathbb{F}_2$. Independently choosing each $a_i = 0$ or 1 gives $\#\mathbb{F}_8 = 2^3 = 8$.

c. Find reciprocals in $\mathbb{F}_8$
Method 1: To find α^{-1}, take $0 = p(\alpha) = (\alpha^2{+}1)\alpha + 1$, giving a pair of reciprocals $(\alpha^2{+}1)\alpha = -1 = 1$.

To find $(\alpha{+}1)^{-1}$, use the Euclidean Algorithm on $p(x)$ and $x{+}1$ to get:

$$p(x) = x^3{+}x{+}1 = (x^2{+}x)(x{+}1) + 1 \quad\Rightarrow\quad p(x) + (x^2{+}x)(x{+}1) = 1.$$

Substituting $x = \alpha$ gives the pair of reciprocals $(\alpha^2{+}\alpha)(\alpha{+}1) = 1$.

To find $(\alpha^2{+}\alpha{+}1)^{-1}$, use the Euclidean Algorithm on $p(x)$ and $x^2{+}x{+}1$ to get:

$$\left\{\begin{array}{r} p(x) = (x{+}1)(x^2{+}x{+}1) + x \\ x^2{+}x{+}1 = (x{+}1)x + 1 \end{array}\right. \quad\Rightarrow\quad (x{+}1)p(x) + x^2(x^2{+}x{+}1) = 1.$$

Substituting $x = \alpha$ gives the pair of reciprocals $\alpha^2(\alpha^2{+}\alpha{+}1) = 1$.

Together with $1 \cdot 1 = 1$, this accounts for all the reciprocal pairs in $\mathbb{F}_8$.

Method 2. The non-zero elements of $\mathbb{F}_8$ form a cyclic group under multiplication:

$$\alpha, \quad \alpha^2, \quad \alpha^3 = \alpha{+}1, \quad \alpha^4 = \alpha^2{+}\alpha, \quad \alpha^5 = \alpha^2{+}\alpha{+}1, \quad \alpha^6 = \alpha^2{+}1, \quad \alpha^7 = 1.$$

This gives the reciprocal pairs $\alpha^i \alpha^{7-i} = 1$ for $i = 1, 2, 3$:

$$\alpha(\alpha^2{+}1) = \alpha^2(\alpha^2{+}\alpha{+}1) = (\alpha{+}1)(\alpha^2{+}\alpha) = 1.$$

Note: This works for any finite field $\mathbb{F}_q$: the non-zero elements under multiplication always form a cyclic group of order $q{-}1$, as we shall prove later.

d. Find the minimal polynomial of every element $\beta \in \mathbb{F}_8$.

Method 1. The minimal polynomial has degree at most 3, since the 4 elements $1, \beta, \beta^2, \beta^3$ must be linearly dependent over $\mathbb{F}_2$. If we define an $\mathbb{F}_2$-linear operator $L_\beta : \mathbb{F}_2^4 \to \mathbb{F}_8$ by $L_\beta(a_0, a_1, a_2, a_3) = a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3$, and we write L_β in terms of the standard basis of $\mathbb{F}_2^4$ and the basis $\{1, \alpha, \alpha^2\}$ of $\mathbb{F}_8$, we get a 3×4 matrix. Any kernel vector (a_0, a_1, a_2, a_3) gives a polynomial $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$ with $f(\beta) = 0$. Taking such $f(x)$ of smallest degree gives the minimal polynomial.

Method 2. The minimal polynomial of $\beta \in \mathbb{F}_8$ must divide any $f(x) \in \mathbb{F}_2[x]$ with $f(\beta) = 0$, so an irreducible $f(x)$ with $f(\beta) = 0$ must be the minimal polynomial.

The minimal polynomial of $a = 0, 1 \in \mathbb{F}_2$ is obviously $x{-}a$. It is easy to see that the only irreducible cubic polynomials in $\mathbb{F}_2[x]$ are:

$$p(x) = x^3{+}x{+}1 \text{ with roots } \alpha\,, \alpha^2\,, \alpha^2{+}\alpha,$$
$$q(x) = x^3{+}x^2{+}1 \text{ with roots } \alpha{+}1\,, \alpha^2{+}1\,, \alpha^2{+}\alpha{+}1.$$

Note: If β is a root of $f(x) \in \mathbb{F}_2[x]$, then β^2 is also a root. To see this, define the Frobenius automorphism $\Phi : \mathbb{F}_8 \to \mathbb{F}_8$ by $\Phi(\beta) = \beta^2$, satisfying $\Phi(\beta{+}\gamma) = \Phi(\beta) + \Phi(\gamma)$, $\Phi(\beta\gamma) = \Phi(\beta)\,\Phi(\gamma)$, and $\Phi(a) = a$ for $a \in \mathbb{F}_2$. If $f(\beta) = 0$, then $0 = \Phi(f(\beta)) = f(\Phi(\beta)) = f(\beta^2)$.

Thus $p(x) = (x{-}\alpha)(x{-}\alpha^2)(x{-}\alpha^4)$, and:

$$q(x) \;=\; (x{-}\alpha^3)(x{-}\alpha^6)(x{-}\alpha^{12}) \;=\; (x{-}\alpha^3)(x{-}\alpha^6)(x{-}\alpha^5).$$

e. CLAIM: $\mathbb{F}_8$ does not contain a field with 4 elements.

Proof 1. Recall from #2(b) that $[\mathbb{F}_8 : \mathbb{F}_2] = \dim_{\mathbb{F}_2}(\mathbb{F}_8) = 3$, and similarly $[\mathbb{F}_4 : \mathbb{F}_2] = 2$. If we had $\mathbb{F}_4 \subset \mathbb{F}_8$, we would have the prime field $\{0, 1\} = \mathbb{F}_2 \subset \mathbb{F}_4$, and the degree-multiplication formula would give:

$$3 = [\mathbb{F}_8 : \mathbb{F}_2] = [\mathbb{F}_8 : \mathbb{F}_4]\,[\mathbb{F}_4 : \mathbb{F}_2] = (k)(2)$$

for a whole number k, which is impossible. Thus there is no such $\mathbb{F}_4 \subset \mathbb{F}_8$.

Proof 2. If $\mathbb{F}_4 \subset \mathbb{F}_8$, then the 7-element multiplicative group $\mathbb{F}_8^\times = \mathbb{F}_8 - \{0\}$ would contain the 3-element group $\mathbb{F}_4^\times = \mathbb{F}_4 - \{0\}$, which is impossible since $3 \nmid 7$.