We want to find a field with 4 element ($\mathbb{F}_4$)

$\mathbb{F}_4$ is not the same as $\mathbb{Z}_4$. This can be proven with addition and multiplication tables.
In this example $\mathbb{Z}_4 = (0, 1, 2, 3)$: Remember this is $\pmod 4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

X	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

While everything is OK with addition there are a few problems with multiplication. The row for 2 has no inverse and has repetition. This means that there is no way to undo multiplication by 2. This also means that $\mathbb{Z}_4$ cannot be a field.

We can use polynomials to find $\mathbb{F}_4$

Let $\mathbb{Z}_2[x]$ be a set of all polynomials with coefficients $\pmod 2$ (0 and 1) This is a ring so we can add, subtract, and multiply any two polynomials in the set.

In modulo 2 arithmetic addition and subtraction are the same operation and give the same result. Because the two operations are the same, there is no need to use a negative sign when in modulo 2. Multiplication still works identical to usual polynomial multiplication except you keep the coefficients in modulo 2.

Ex: Have $f(x) = x^3 + x^2 + 1$ and $g(x) = x^3 + 1$. Both f(x) and g(x) are in $\mathbb{Z}_2[x]$

$f(x) + g(x) \equiv (x^3 + x^2 + 1) + (x^3 + 1) \equiv \cancel{2(x^3)} + x^2 + \cancel{2(1)} \equiv x^2 \pmod 2$

$f(x) - g(x) \equiv (x^3 + x^2 + 1) - (x^3 + 1) \equiv x^2$

$f(x) * g(x) \equiv (x^3 + x^2 + 1) * (x^3 + 1) \equiv x^6 + x^5 + x^3 + x^3 + x^2 + 1 \equiv x^6 + x^5 + \cancel{2(x^3)} + x^2 + 1 \equiv x^6 + x^5 + x^2 + 1$

We can't do regular division in $\mathbb{Z}_2[x]$ but we can do division with remainder.

Find the remainder when $x^5 + x^4 + x^2 + 1$ is divided by $x^3 + x + 1$

$$
\begin{array}{r l}
 & x^2 + x - 1 \\
\cline{2-2}
x^3 + x + 1 \big) & x^5 + x^4 + x^2 + 1 \\
 & -x^5 - x^3 - x^2 \\
\cline{2-2}
 & x^4 - x^3 \\
 & - x^4 - x^2 - x \\
\cline{2-2}
 & - x^3 - x^2 - x + 1 \\
 & x^3 + x + 1 \\
\cline{2-2}
 & - x^2 + 2
\end{array}
$$

The long division gives us $R = -x^2 + 2$ but because we are in $\pmod 2$ the negative sign and the 2 are canceled out leaving $R = x^2$

We can use the rules of addition/subtraction, multiplication, and division with remainder to find any polynomial mod another polynomial

Find $(x^2 + 1) + (x + 1) \pmod{x^3 + x + 1}$ and $(x^2 + 1) * (x + 1) \pmod{x^3 + x + 1}$

$(x^2 + 1) + (x + 1) \equiv (x^2 + x + \cancel{2(x)}) \equiv (x^2 + x) \pmod{x^3 + x + 1}$
$x^2 + x$ has a lower leading degree than the modulus so it is less then the modulus.

$(x^2 + 1) * (x + 1) \equiv (x^3 + x^2 + x + 1)$

$(x^3 + x^2 + x + 1)$ has the same degree as the modulus so it needs to be divided with remainder

$$
\begin{array}{r l}
 & 1 \\
\cline{2-2}
x^3 + x + 1 \big) & x^3 + x^2 + x + 1 \\
 & -x^3 - x - 1 \\
\cline{2-2}
 & x^2
\end{array}
$$

R=x^2 so $(x^3 + x^2 + x + 1) \equiv (x^2) \pmod{x^3 + x + 1}$

By using Euclid's algorithm and Euclid's extended algorithm we can find the GCD and inverse of polynomials.

Use Euclid's extended algorithm to find the GCD of $x^5 + x^4 + x^2 + 1$ and $x^3 + x + 1$

Step 1)

$$
\begin{array}{r|l}
 & \quad x^2 + x - 1 \\
\hline
x^3 + x + 1 & x^5 + x^4 \quad + x^2 \quad + 1 \\
 & -x^5 \quad - x^3 - x^2 \\
\cline{2-2}
 & \quad x^4 - x^3 \\
 & \quad -x^4 \quad - x^2 - x \\
\cline{2-2}
 & \qquad -x^3 - x^2 - x + 1 \\
 & \qquad x^3 \quad + x + 1 \\
\cline{2-2}
 & \qquad\quad -x^2 \quad + 2
\end{array}
$$

Like said earlier because this is modulus 2 any minus/negative and any 2s are canceled out giving $R = x^2$

Step 2)

$$
\begin{array}{r|l}
 & \quad x \\
\hline
x^2 & x^3 + x + 1 \\
 & -x^3 \\
\cline{2-2}
 & \quad x + 1
\end{array}
$$

$R = x + 1$

Step 3)

$$
\begin{array}{r|l}
 & \quad x - 1 \\
\hline
x + 1 & x^2 \\
 & -x^2 - x \\
\cline{2-2}
 & \quad -x \\
 & \quad x + 1 \\
\cline{2-2}
 & \qquad 1
\end{array}
$$

$R = 1$

Step 4)

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
1 & x + 1 \\
 & -x \\
\cline{2-2}
 & \quad 1 \\
 & \quad -1 \\
\cline{2-2}
 & \quad 0
\end{array}
$$

$R = 0$ meaning that the previous remainder of 1 is the GCD
$x^5 + x^4 + x^2 + 1 = (x^2 + x + 1)(x^3 + x + 1) + (x^2)$
$x^3 + x + 1 = x(x^2) + (x + 1)$
$x^2 = (x + 1)(x + 1) + 1$

If $f(x)$ and $g(x)$ are polynomials and the GCD of (f,g) is 1, then f has an inverse (mod $g(x)$) which can be found using euclid's extended algorithm and the linear combination of f and g. The linear combination of f and g is $c(x)f(x) + d(x)g(x) = 1$

Use Eucid's extended algorithm to find the liner combination for $x^5 + x^4 + x^2 + 1$ and $x^3 + x + 1$ and the inverse of $(x^3 + x + 1) \pmod{x^5 + x^4 + x^2 + 1}$

Using the equations from the previous question we have,
$1 = 1(x^2) + (x + 1)(x + 1)$
$(x + 1) = 1(x^3 + x + 1) + x(x^2)$
$(x^2) = 1(x^5 + x^4 + x^2 + 1) + (x^2 + x + 1)(x^3 + x + 1)$

Then using the 3 steps of Eucid's extended algorithm which are,
1) Substitute
2) Distribute
3) Combine like terms
We get,

$1 \equiv (x^2) + (x + 1)(x^3 + x + 1 + x(x^2)) \equiv (x^2) + (1 + x)(x^3 + x + 1) + (x^2 + x)(x^2) \equiv (x^2 + x + 1)(x^2) + (x + 1)(x^3 + x + 1)$
$\equiv (x^2 + x)((x^5 + x^4 + x^2 + 1) + (x^2 + x + 1)(x^3 + x + 1)) + (x + 1)(x^3 + x + 1) \equiv (x^2 + x)(x^5 + x^4 + x^2 + 1) + (x^4 + x^2 + x)(x^3 + x + 1)$

$(x^2 + x)(x^5 + x^4 + x^2 + 1) + (x^4 + x^2 + x)(x^3 + x + 1) \equiv 1$
$f(x) = (x^5 + x^4 + x^2 + 1)$
$g(x) = (x^3 + x + 1)$
$c(x) = (x^2 + x)$
$d(x) = (x^4 + x^2 + x)$

$x^4 + x^2 + 1$ is the inverse of $(x^3 + x + 1) \pmod{x^5 + x^4 + x^2 + 1}$