Polynomial Toolkit

① Divide $x^3 + 3x^2 + 3x + 5$ by $x+2$ and find out the rest.

② Factorize $x^3 + x^2 + x + 1$ in $GF(2)[x]$ into irreducible polynomials.

③ Find the inverse of $x+1$ in $GF(2)[x]_{x^2+x+1}$.

④ Show that $x^4 + x^2 + 1$ in $GF(2)[x]$ has no factors of degree 1.
There is $f(x)$ with $(f(x))^2 = x^4 + x^2 + 1$. What is $f(x)$?

Solutions

① $x^3 + 3x^2 + 3x + 5 : x + 2 = x^2 + x + 1$

$$
\begin{array}{l}
x^3 + 3x^2 + 3x + 5 \\
-(x^3 + 2x^2) \\
\quad x^2 + 3x + 5 \\
\quad -(x^2 + 2x) \\
\qquad x + 5 \\
\qquad -(x+2) \\
\qquad\quad 3 = \text{rest}
\end{array}
$$

② $x^3 + x^2 + x + 1$ has the root 1.
So it is divisible by $(x-1) = (x+1)$
We divide:

$$
\begin{array}{l}
x^3 + x^2 + x + 1 : x + 1 = x^2 + 1 \\
-(x^3 + x^2) \\
\qquad x + 1 \\
\qquad -(x+1) \\
\qquad\quad 0
\end{array}
$$

$x^2 + 1$ again has the root 1. We find that
$(x+1)(x+1) = x^2+1$ and so the factorization is $(x+1)^3$.

③ We want to find $g(x)$ such that

$$(x+1)\, g(x) \equiv_{x^2+x+1} 1$$

Let's try if we can find $g(x)$ with

$$(x+1)\, g(x) = (x^2+x+1) + 1 = x^2 + x.$$

We find $(x+1)x = x^2 + x$. So x is the inverse.

(4) It has no roots. So no factors of degree 1.
Since it has no factors of degree 1, the polynomial f must be irreducible.
The only such polynomial (we know from the script) is x^2+x+1.

Poly. Div. Example

$$
\begin{array}{l}
x^3 + 2x^2 + 2x + 2 : (x+1) = x^2 + x + 1 \\
-(x^3 + x^2) \\
\qquad x^2 + 2x + 2 \\
\qquad -(x^2 + x) \\
\qquad\qquad x + 2 \\
\qquad\qquad -(x + 1) \\
\qquad\qquad\quad 1 \text{ rest}
\end{array}
$$