Multiplicative inverses mod $M(x)$

A polynomial $i(x)$ is a **multiplicative inverse** of $f(x)$ modulo $M(x)$ if

$$[f(x) \cdot i(x)] \,\%\, M(x) = 1$$

or, equivalently, if

$$f(x) \cdot i(x) = 1 \bmod M(x)$$

As a corollary of the peculiar characterization of the *gcd*, for $\gcd(f(x), M(x)) = 1$, there are $r(x)$ and $s(x)$ such that

$$1 = \gcd(f(x), M(x)) = r(x) \cdot f(x) + s(x) \cdot M(x)$$

Considering the equation

$$r(x) \cdot f(x) + s(x) \cdot M(x) = 1$$

modulo $M(x)$, we have

$$r(x) \cdot f(x) = 1 \bmod M(x)$$

so $r(x)$ is a multiplicative inverse of $f(x)$ mod $M(x)$.

(And, symmetrically, $s(x)$ is a multiplicative inverse of $M(x)$ mod $f(x)$.)

As with ordinary integers, use the (extended) Euclidean algorithm to find polynomials $r(x)$ and $s(x)$ such that

$$\gcd(f, g) = r \cdot f + s \cdot g$$

Example: To find a multiplicative inverse of x mod $x^2 + x + 1$, use extended Euclid with inputs these two polynomials:

$$\begin{array}{ccc} x^2 + x + 1 - (x+1)(x) & = & 1 \\ x - (x)(1) & = & 0 \end{array}$$

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

Since in general

$$1 = r \cdot f + s \cdot g$$

implies that r is a multiplicative inverse of f mod g we see that $x + 1$ is a multiplicative inverse of x mod $x^2 + x + 1$.

Example: To find a multiplicative inverse of x^2+1 mod x^3+x^2+1, use extended Euclid with inputs these two polynomials:

$$\begin{array}{rcl} x^3 + x^2 + 1 - (x+1)(x^2+1) & = & x \\ x^2 + 1 - (x)(x) & = & 1 \\ x - (x)(1) & = & 0 \end{array}$$

$$\begin{array}{rcl} 1 & = & (1)(x^2+1) + (x)(x) \\ & = & (x^2+1)+(x)((x^3+x^2+1)+(x+1)(x^2+1)) \\ & = & (x)(x^3+x^2+1) + (x^2+x+1)(x^2+1) \end{array}$$

Since in general

$$1 = r \cdot f + s \cdot g$$

implies that r is a multiplicative inverse of f mod g, x^2+x+1 is a multiplicative inverse of x^2+1 mod x^3+x^2+1.