Extended Euclidean Algorithm for Polynomials

The following example was begun in class on Mon Feb 5, 2007 to compute the gcd of the polynomials $f(X) = 5X^3 + 2X^2 + 3X - 10$, $g(X) = X^3 + 2X^2 - 5X + 2 \in \mathbb{Q}[X]$. The steps are almost the same as when computing the gcd of two integers, but with a twist:

$$\begin{aligned} f(X) &= 5g(X) + (-8X^2 + 28X - 20) \\ g(X) &= \left(-\tfrac{1}{8}X - \tfrac{11}{16}\right)(-8X^2 + 28X - 20) + \left(\tfrac{47}{4}X - \tfrac{47}{4}\right) \\ -8X^2 + 28X - 20 &= \tfrac{4}{47}\left(-8X + 20\right)\left(\tfrac{47}{4}X - \tfrac{47}{4}\right) + 0 \end{aligned}$$

At this point we might want to say that $gcd(f(X), g(X)) = \frac{47}{4}X - \frac{47}{4} = \frac{47}{4}(X - 1)$. However observe that the much simpler polynomial $X - 1$ divides both $f(X)$ and $g(X)$. In order to have a unique answer when computing gcd's, we will insist that the gcd be a **monic** polynomial, i.e. that its leading coefficient be 1. Thus in this case $gcd(f(X), g(X)) = X - 1$ and the extended form of the algorithm allows us to write this as a polynomial-linear combination of $f(X)$ and $g(X)$:

$$\begin{aligned} \tfrac{47}{4}X - \tfrac{47}{4} &= g(X) - \left(-\tfrac{1}{8}X - \tfrac{11}{16}\right)(-8X^2 + 28X - 20); \\ X - 1 &= \tfrac{4}{47}g(X) + \left(\tfrac{1}{94}X + \tfrac{11}{188}\right)(-8X^2 + 28X - 20) \\ &= \tfrac{4}{47}g(X) + \left(\tfrac{1}{94}X + \tfrac{11}{188}\right)\left(f(X) - 5g(X)\right) \\ &= \left(\tfrac{1}{94}X + \tfrac{11}{188}\right)f(X) + \left(-\tfrac{5}{94}X - \tfrac{39}{188}\right)g(X). \end{aligned}$$