Comments on the Euclidean Algorithm

I want to clarify and correct some comments I made about the Euclidean Algorithm and its extension to polynomials.

The Euclidean Algorithm for integers relies upon the following Division Algorithm for Integers: Given any nonnegative integer $a$ and positive integer $b$, there exist unique nonnegative integers $q$ and $r$ so that $a = qb + r$ and $r < b$.

The Euclidean Algorithm for positive integers $a_1, a_2$ proceeds by dividing $a_1$ by $a_2$ yielding remainder $a_3$, then dividing $a_2$ by $a_3$ yielding remainder $a_4$, etc., until a remainder $a_n = 0$ is reached. Then $a_{n-1}$ is the greatest common factor of $a_1$ and $a_2$.

Extending this idea to polynomials $\mathbb{R}[x]$ with real coefficients relies upon the following Division Algorithm for Polynomials: Given any polynomial $a(x)$ and nonzero polynomial $b(x)$, there exist unique polynomials $q(x)$ and $r(x)$ so that $a(x) = q(x)b(x) + r(x)$ and the degree of $r(x)$ is strictly less than the degree of $b(x)$.

The Euclidean Algorithm for nonzero polynomials $a_1, a_2$ proceeds by dividing $a_1$ by $a_2$ yielding remainder $a_3$, then dividing $a_2$ by $a_3$ yielding remainder $a_4$, etc., until a remainder $a_n = 0$ is reached. Then $a_{n-1}$ is the greatest common factor of $a_1$ and $a_2$. It is unique up to multiplication by a real number.

For example, if you wish to find the greatest common factor of $x^2 - 2x + 1$ and $x^2 - 1$, divide $a_1 = x^2 - 2x + 1$ by $a_2 = x^2 - 1$ to get quotient 1 and remainder $a_3 = -2x + 2$. Then divide $a_2$ by $a_3$ to get quotient $-\frac{1}{2}x - \frac{1}{2}$ and remainder $a_4 = 0$. Thus the greatest common factor (greatest in terms of degree) of $a_1$ and $a_2$ is $a_3 = -2x + 2$ (or we can multiply by the real number $-\frac{1}{2}$ to get $x - 1$). In this way we can find the greatest common factor without first factoring!