A Variation on Euclid's Method (HW 6 due Thursday, October 16)

Let $f(x), g(x) \in F[x]$ where F is a field. For any $a \in F$ and $k \geq 0$, the set of common divisors of $f(x)$ and $g(x)$ is the same as the set of common divisors of $f(x) - ax^k g(x)$ and $g(x)$ and is the same as the set of common divisors of $f(x)$ and $g(x) - ax^k f(x)$. To find the greatest common divisor, keep revising the pair $(f(x), g(x))$ until arriving at either $(\delta(x), 0)$ or $(0, \delta(x))$. This can be done in a finite number of steps if we always reduce the degree of one of the polynomials, but the ability to do this depends on the ability to find the multiplicative inverse of a non-zero coefficient, hence the need for field coefficients. Since the divisors of $f(x)$ and $g(x)$ are the same as the divisors of $\delta(x)$, $\delta(x)$ is a greatest common divisor of $f(x)$ and $g(x)$.

Example: Assume the polynomial ring is $\mathbb{Q}[x]$.

$(f_1, g_1) = (18 + 57x + 68x^2 + 38x^3 + 10x^4 + x^5, 12 + 28x + 23x^2 + 8x^3 + x^4)$

$(f_2, g_2) = (f_1 - xg_1, g_1) = (18 + 45x + 40x^2 + 15x^3 + 2x^4, 12 + 28x + 23x^2 + 8x^3 + x^4)$

$(f_3, g_3) = (f_2 - 2g_2, g_2) = (-6 - 11x - 6x^2 - x^3, 12 + 28x + 23x^2 + 8x^3 + x^4)$

$(f_4, g_4) = (f_3, g_3 + xf_3) = (-6 - 11x - 6x^2 - x^3, 12 + 22x + 12x^2 + 2x^3)$

$(f_5, g_5) = (f_4, g_4 + 2f_4) = (-6 - 11x - 6x^2 - x^3, 0)$

$\gcd(f_1, g_1) = -6 - 11x - 6x^2 - x^3 = -(1 + x)(2 + x)(3 + x)$.

Check:

$\frac{18+57x+68x^2+38x^3+10x^4+x^5}{-6-11x-6x^2-x^3} = -3 - 4x - x^2 = -(1 + x)(3 + x)$

$\frac{12+28x+23x^2+8x^3+x^4}{-6-11x-6x^2-x^3} = -2 - x = -(2 + x)$

Note that the algorithm yields polynomials $a(x)$ and $b(x)$ such that $\gcd(f(x), g(x)) = a(x)f(x) + b(x)g(x)$: Consider the evolution of the pairs (f, g) above. We have

$$(f, g)$$

$$(f - xg, g)$$

$$(f - xg - 2g, g)$$

$$(f - xg - 2g, g + xf - x^2 g - 2xg)$$

$$(f - xg - 2g, g + xf - x^2 g - 2xg + 2f - 2xg - 4g)$$

Therefore

$$(1)(f(x)) + (-x-2)(g(x)) = -6 - 11x - 6x^2 - x^3.$$

Check:

$$(1)(18+57x+68x^2+38x^3+10x^4+x^5)+(-x-2)(12+28x+23x^2+8x^3+x^4) = -6-11x-6x^2-x^3.$$

In particular, when $f(x)$ and $g(x)$ have greatest common divisor 1 there are polynomials $a(x)$ and $b(x)$ such that $a(x)f(x) + b(x)g(x) = 1$.

Exercises:

(1) In the ring of polynomials $\mathbb{Z}_{11}[x]$, find a greatest common divisor of $f(x) = 4+3x+6x^2+2x^3+5x^4+x^7$ and $g(x) = 4+6x+8x^2+5x^3+10x^5+7x^6+x^8$.

(2) Let $\delta(x)$ be the greatest common divisor found in (1). Check your work by showing that $\frac{f(x)}{\delta(x)} \in \mathbb{Z}_{11}[x]$ and $\frac{g(x)}{\delta(x)} \in \mathbb{Z}_{11}[x]$. Use long division.

(3) Find $a(x)$ and $b(x)$ in $\mathbb{Z}_{11}[x]$ such that $a(x)f(x) + b(x)g(x) = \delta(x)$.

(4) Factor $\delta(x)$ into $\mu(x)\nu(x)$ where $\mu(x)$ and $\nu(x)$ are monic (leading coefficient is 1) and $\deg \mu(x) = 2$ and $\deg \nu(x) = 3$. The factorization must take place in $\mathbb{Z}_{11}[x]$.

(5) To demonstrate why field coefficients are necessary, try finding a greatest common divisor of $2x^3$ and $3x^4$ in $\mathbb{Z}_6[x]$ using this method and repeat, if possible, the steps in problems 1–4.

NOTE: I have designed problems 1–4 so that so that $f(x)$ and $g(x)$ are irreducible in $\mathbb{Q}[x]$ and have no roots in $\mathbb{Z}_{11}$, yet they are factorable in $\mathbb{Z}_{11}[x]$. The point is that Euclid's algorithm does not depend on factoring or root extraction.