Resultants & gcd computation

`(Due date: Sunday April 10th)`

1. Let $a = qb+r$ be a division with remainder, with $a, b, c, r, \in \mathbb{Q}[x]$, $-1+\deg(a) = \deg(b) > \deg(r)$, and $\lambda(a)$, $\lambda(b) \leq l \in \mathbb{N}$. Give estimates for $\lambda(q)$ and $\lambda(r)$ in terms of l (a and b need not be monic).

2. Let R be a Unique Factorization Domain, and $f \in R[x]$. Show that $f = \mathrm{pp}(f)$ if and only if f is primitive.

3. Let $p \in \mathbb{Z}$ be a prime, and $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ be defined by taking coefficients modulo p. Show that when $f \in \mathbb{Z}[x]$, p does not divide $lc(f)$, and $\varphi(f)$ is irreducible in $\mathbb{Z}_p[x]$, then f is irreducible in $\mathbb{Q}[x]$.

4. Show that the probability for two random polynomials in $\mathbb{Z}[x]$ of degree at most n and max-norm at most A to be coprime in $\mathbb{Q}[x]$ is at least $1 - 1/(2A+1)$.

5. Consider the ring $R = \mathbb{Z}[1/2] = \{a/2^n,\ a \in \mathbb{Z},\ n \in \mathbb{N}\}$ of binary rationals.
   (a) Prove that R is the smallest subring of $\mathbb{Q}$ containing $\mathbb{Z}$ and $1/2$.
   (b) What are the units of R?
   (c) You may use the fact that R is a UFD and that any two elements of R have a gcd which is unique up to associates. Find a normal form on R and use this to define a gcd function on R.
   (d) Determine the content and primitive part of the polynomial $f = 2x^2 + 6x - 4$ with respect to the three rings $\mathbb{Z}$, R, and $\mathbb{Q}$. Is f primitive with respect to R?

6. Let $f, g \in \mathbb{Z}[x]$, $r = \mathrm{res}(f, g) \in \mathbb{Z}$, and $u \in \mathbb{Z}$. Prove that $\gcd(f(u), g(u))$ divides r.

7. Let F be a field, and $f = \sum_{i=0}^{n} f_i x^i$, $g = \sum_{i=0}^{m} g_i x^i \in \mathbb{F}[x, y]$ having total degrees n and m respectively (so that $\deg_y(f_i) \leq n - i$, $\deg_y(g_i) \leq m - i$, $i = 0, \ldots$. Let $r = \mathrm{res}_x(f, g) \in F[x]$. Show that each of the $(n + m)!$ summands contributing to r has degree at most nm, and hence $\deg_y(r) \leq nm$.

8. For each $n \in \mathbb{N}$, find polynomials $f_1, \ldots, f_n \in \mathbb{Q}[x]$ such that $\gcd(f_1, \ldots, f_n) = 1$, and any proper subset of them has a nonconstant gcd .

9. Let R be a Unique Factorization Domain, $f_1, \ldots, f_n \in R$, $m = f_1 \ldots f_n$, and $g_i = m/f_i\, 1 \leq i \leq n$. Show that $\mathrm{lcm}(f_1, \ldots, f_n) = m/\gcd(g_1, \ldots, g_n)$. Derive an algorithm for computing $\mathrm{lcm}(f_1, \ldots, f_n)$ if $R = F[x]$ for a field F, and analyze its complexity.

10. Let $\alpha \in \mathbb{C}$, and $f,\, g \in \mathbb{Q}[x]$ of degrees $n, m \in \mathbb{Z}_{>0}$ such that f is the minimal polynomial of α. We want to compute the minimal polynomial of $g(\alpha)$, so we may assume $n > m$.
    (a) Let $r = \mathrm{res}_y(f(y), x - g(y)) \in \mathbb{Q}[x]$. Show that $\deg_x(r) = n$, and that the minimal polynomial of $g(\alpha)$ divides r.
    (b) Compute the minimal polynomials of $\sqrt{3}+1$, and $\sqrt[3]{4}+\sqrt[3]{2}+1$ over $\mathbb{Q}$.

11. Let $\alpha, \beta \in \mathbb{C} \setminus \{0\}$, with (monic) minimal polynomials $f,\, g \in \mathbb{Q}[x]$ of degrees n and m respectively.
    (a) Prove that the reversal $\mathrm{rev}(f) := x^n f(x^{-1})$ of f is the minimal polynomial of α^{-1}.
    (b) Let $r = \mathrm{res}_y(\mathrm{rev}(f)(y), g(xy)) \in \mathbb{Q}[x]$. Show that $\deg_x(r) = nm$, and $r(\alpha\beta) = 0$.
    (c) Find multiples of degree nm of the minimal polynomial $a\alpha + b\beta$, where $a, b \in \mathbb{Q} \setminus \{0\}$ are arbitrary, and also of $\frac{\alpha}{\beta}$.

12. Compute the minimal polynomial $f \in \mathbb{Q}[x]$ of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$. Let $\mathbb{F}_{19^2} = \mathbb{F}_{19}[z]/\langle z^2 - 2\rangle$, and $\alpha = z \bmod z^2 - 2 \in \mathbb{F}_{19^2}$ a square root of 2. Check that 7α is a square root of 3, and compute the minimal polynomial of $\alpha + 7\alpha$ over $\mathbb{F}_{19}$. How is this related to f?

13. Compute (with explanation) the gcd over $\mathbb{Z}[x]$ of the polynomials $36x^4+72x^3+68x^2+104x+60$ and $36x^5+24x^4+116x^3+126x^2+150x+150$ with the small primes modular algorithm.

14. Compute the gcd of $x^4 - 3ax^3 - 8a^2x^2 + 18a^3x - 8a^4$ and $x^3 - ax^2 - 8a^2x + 6a^3$ in $\mathbb{Q}[a, x]$ using the small primes modular algorithm.

15. Let F be a field, $f,\, g \in F[x, y]$ nonzero with $\deg_x(f)$, $\deg_x(g) \le n$, $\deg_y(f)$, $\deg_y(g) \le d$, and $\mathrm{lc}_x(f) = \mathrm{lc}_x(g) = 1$. Suppose that $\gcd(f(x, u), g(x, u)) \neq 1$ for at least $2nd + 1$ values $u \in F$. Show that $\deg_x(\gcd(f, g)) > 0$.

16. Let $\alpha \in \mathbb{R}$ be a parameter, and $f,\, g_\alpha \in \mathbb{R}[x]$ monic polynomials with $\mathrm{res}(f, g_\alpha) = \alpha^3 + \alpha^2 + \alpha + 1$. Determine all values of α for which $\gcd(f, g_\alpha) \neq 1$.

17. Let $f = x^4 - 13x^3 - 62x^2 - 78x - 408$, $g = x^3 + 6x^2 - x - 30 \in \mathbb{Z}[x]$.
    (a) Write down the Sylvester matrix of f and g and compute $\mathrm{res}(f, g)$.
    (b) Let $p_1 = 5$, $p_2 = 7$, $p_3 = 11$, and $p_4 = 13$. Compute $h = \gcd(f, g)$ in $\mathbb{Q}[x]$. for which of the primes is the modular image of h equal to the gcd modulo that prime, and why?

18. Why do the `Mathematica` commands `PolynomialGCD[`$x^2+1, x+1$`, Modulus -> 2]` and `PolynomialMod[PolynomialGCD[`$x^2+1, x+1$`], 2]` compute different things?