to be prepared for 11.01.2024

Exercise 37. We consider the modular GCD-algorithm for $\mathbb{F}[x, y]$.

INPUT: $f, g \in \mathbb{F}[x, y]$ primitive as polynomials in $\mathbb{F}[y][x]$, with $\deg_x f \geq \deg_x g$;
$d \in \mathbb{N}$ with $d \geq \deg_y(f), \deg_y(g)$.
OUT: $h = \gcd(f, g)$.

Let $b = \gcd\big(\mathrm{lc}_x(f), \mathrm{lc}_x(g)\big)$. Choose a monic irreducible $g \in \mathbb{F}[y]$ with $\deg p = d+1+\deg b$ and Let $\overline{\varphi}$ denote the result of reducing mod p a polynomial $\varphi \in \mathbb{F}[x, y]$, i.e.,

$$\mathbb{F}[y][x] \to \mathbb{F}[y]/\langle p\rangle[x],\ \varphi = \sum_j \varphi_j(y)x^j \mapsto \sum_j \big(\varphi_j(y) + \langle p\rangle\big)x^j = \overline{\varphi}.$$

Compute $w \in \mathbb{F}[x, y]$, $\deg_y w < \deg p$ with $\overline{w} = \overline{b} \cdot \gcd\left(\overline{f}, \overline{g}\right)$.
Since $\overline{w} \mid \overline{fb}$, $\overline{w} \mid \overline{g}\overline{b}$, we may compute $f^\star, g^\star \in \mathbb{F}[x, y]$ with $\deg_y(f^\star), \deg_y(g^\star) < \deg p$ and $\overline{f^\star} = \frac{\overline{fb}}{\overline{w}}$ and $\overline{g^\star} = \frac{\overline{g}\overline{b}}{\overline{w}}$. Then the `halting condition` is

$$\deg_y(f^\star w) = \deg_y(fb) \text{ and } \deg_y(g^\star w) = \deg_y(gb). \tag{1}$$

Prove that the halting condition holds if and only if p does not divide the x-resultant of $\frac{f}{h}, \frac{g}{h}$, i.e.,

$$(1) \iff \neg\, p \,\Big|\, \mathrm{res}_x\left(\frac{f}{h}, \frac{g}{h}\right).$$

Exercise 38. In the situation of Exercise 37, although the degree of p is large enough to leave the coefficients of $\overline{f}, \overline{g}$ unaffected, create an example that demonstrates that the degree of $\gcd\left(\overline{f}, \overline{g}\right)$ may exceed $\deg p$.

Exercise 39. Again the situation of Exercise 37 prove that the number of unlucky primes is small, i.e., the cardinality of the set of all monic irreducibles $p \in \mathbb{F}[y]$ with a fixed degree $d + 1 + \deg b$ that divide $\mathrm{res}_x(f/h, g/h)$ is at most $2 \cdot \deg_x f$.

Exercise 40. Let $f, g, h \in \mathbb{Z}[x]$ with degrees
$n = \deg f \geq 1$, $m = \deg g$, $k = \deg h$, and assume that $gh|f$ in $\mathbb{Z}[x]$. Prove that

$$||g||_1||h||_1 \leq 2^{m+k}||f||_2 \leq (n + 1)^{1/2} \cdot 2^{m+k}||f||_\infty.$$

Derive from this that

$$||h||_\infty \leq ||h||_2 \leq 2^k||f||_2 \leq 2^k||f||_1 \text{ and } ||h||_\infty \leq ||h||_2 \leq (n + 1)^{1/2} \cdot 2^k||f||_\infty.$$

Exercise 41. Let $p \in \mathbb{N}$ be a prime number and consider the ring homomorphism

$$\mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x],\ f = \sum_k f_k x^k \mapsto \overline{f} = \sum_k \overline{f_k} x^k \text{ where } \overline{f_k} = f_k + \langle p\rangle.$$

Show the validity of the following statement:

If $f, g \in \mathbb{Z}[x]$ with $||f||_\infty, ||g||_\infty < \frac{p}{2}$ then $\overline{f} = \overline{g} \iff f = g$.