to be prepared for 15.12.2022

Exercise 39. 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 $\overline{f} = \overline{g} \iff f = g$.

Exercise 40. Let $f, g \in \mathbb{Z}[x]$. Show that $||fg||_1 \leq ||f||_1 \cdot ||g||_1$.

Exercise 41. Given the polynomials

$$\begin{aligned} f(x) &= x^7 - 3x^5 - 2x^4 + 13x^3 - 15x^2 + 7x - 1, \\ g(x) &= x^6 - 9x^5 + 18x^4 - 13x^3 + 2x^2 + 2x - 1 \end{aligned}$$

compute their gcd $h \in \mathbb{Z}[x]$. Check whether the integer factors of the resultant of f/h and g/h are unlucky primes in the modular approach to gcd computation.

Exercise 42. Let $A = (a_{ij}) \in \mathbb{Z}^{n \times n}$ be a square matrix with integer entries. Set $||A||_\infty = \max_{1 \leq i,j \leq n} |a_{ij}|$. Prove that

$$|\det A| \leq n^{n/2} ||A||_\infty^n.$$

Hint: You may produce a matrix $B \in \mathbb{Q}^{n \times n}$ by applying Gram-Schmidt (without normalization) to the columns of A and prove that this process preserves determinants. Then express $\det B$ in terms of the length (2-norms) of its column vectors and compare with the length of A's columns.

Exercise 43. Let R be a Euclidean domain, $p \in R$ a prime and $f, g \in R[x] \setminus 0$ such that $p \nmid \gcd_R\big(\mathrm{lc}(f), \mathrm{lc}(g)\big)$. Let $\overline{f}$ denote the image of f in $\mathbb{F} = R/\langle p \rangle$ and assume hat $\gcd_{\mathbb{F}[x]}\big(\overline{f}, \overline{g}\big) = 1$. Prove that $\gcd_{R[x]}(f, g) = \gcd_R\big(\mathrm{cont}(f), \mathrm{cont}(g)\big)$.