Exercises: Week 4

Computation in Algebra and Arithmetic

David Loeffler & Tim Gehrunger

18.3.2022

Sage provides standard constructions for polynomials. A brief introduction on how they are implemented can be found here: `https://doc.sagemath.org/html/en/tutorial/tour_polynomial.html`.

1 Mignotte's factor bound

Consider the polynomial $x^4 + x + 1 \in \mathbf{Z}[x]$.

(1) Use Mignotte's factor bound to find out whether f has factors over $\mathbf{Z}$.
Hint: *First show by hand that f has no rational roots and then search for quadratic factors.*

(2) Compute the Mahler measure $M(f)$ of f.

(3) Verify that

$$||f||_\infty \leq \binom{d}{\lfloor \frac{d}{2} \rfloor} M(f)$$

and

$$M(f) \leq ||f||_2.$$

(4) Can you find a polynomial for which the last two bounds are equalities?

(5) In the lecture we defined the Mahler measure of monic polynomials. For a general $f \in \mathbf{C}[X]$, we define the Mahler measure by

$$M(f) := |c| \prod_i \max(1, |\alpha_i|),$$

where $f = c \prod_i (X - \alpha_i)$. Prove that the Mahler measure is multiplicative, i.e. that for $f, g \in \mathbf{C}[X]$, we have $M(f)M(g) = M(fg)$.

2 Hensel's Lemma

(1) Maybe some of you have seen the following, slightly less general version of Hensel's Lemma.

Theorem. Let $f \in \mathbf{Z}$ and let p be any prime number. If $\alpha \in \mathbf{Z}$ is such that $f(a) \equiv 0 \bmod p$ and $f'(a) \not\equiv 0 \bmod p$, then α can be uniquely lifted to a root α_n of $f \bmod p^n$ for all $n \geq 1$.

Show how this can be deduced from the theorem presented in the lecture.

(2) Use Hensel's Lemma to find all solutions of $x^4 + x^3 + 2x^2 + x = 13 \bmod 7^3$.
Hint: *In the less general setting of Hensel's Lemma presented in (1), we can give an explicit formula for the lift of a root. More precicely, in the notation of the theorem, we have for $k \geq 1$*

$$\alpha_{k+1} \equiv \alpha_k - f(\alpha_k)[f'(a))]^{-1} \bmod p^{k+1},$$

where $[f'(a))]^{-1}$ is the inverse of $f'(a)$ in $\mathbf{F}_{p^{k+1}}$.

Challenge: Intersecting curves in the plane

Let F be a field. Consider the plane curve $\mathcal{C}$ over K defined by

$$X(X+Y)(X+1) + Y(X+Y)(Y+1) + (X+1)(Y+1) = 4(X+Y)(X+1)(Y+1).$$

Find coordinates of intersection of $\mathcal{C}$ and the unit circle given by $X^2 + Y^2 + 1$.

Note: *We will learn how to efficiently compute such intersections later.*