Algebraic Algorithms

mykyta.narusevych@matfyz.cuni.cz

January 2023

1 Theoretical part

1. Let $\mathbf{T}$ be $\mathbb{Z}_3$, $f \in \mathbf{T}[x]$ be x^2+2x+2 and g_1, $g_2, g_3 \in \mathbf{T}[x]$ be $(2x+1)$, $(x+1)$ and x, respectively. Find u_1, u_2 and u_3 such that $f = u_1\tilde{g_1} + u_2\tilde{g_2} + u_3\tilde{g_3}$ and $\deg u_i < \deg g_i$ for all i.

2. Let f be $5x^3 + 9x^2 - 146x - 120$ and p be 3. Consider the following decompostion:

$$f \equiv (2x+1)(x+1)x \mod 3.$$

   Apply Hensel's lifting algorithm to find a decomposition of f modulo $3^2 = 9$.

3. Let f be $6x^7+7x^6+4x^5+x^4+6x^3+7x^2+4x+1$. Consider its decomposition in $\mathbb{Z}_{25}[x]$:

$$f \mod 25 = (6x+3)(x^2-7)(x^2+7)(x^2+9x-8).$$

   Apply Zassenhaus's combination method to find a decomposition of f inside $\mathbb{Z}[x]$. Does 25 satisfy bounds from the algorithm's specification?

4. Show that the polynomial x^4+1 is irreducible in $\mathbb{Z}[x]$ but is decomposable in $\mathbb{Z}_p[x]$ for all prime p.

2 Computational part

1. Verify 1 using sage.
2. Verify 2 using sage.
3. Verify 3 using sage.