TP 12: arithmetic with polynomials

Jean-Sébastien Coron

Université du Luxembourg

1 Arithmetic with polynomials

Implement the addition, substraction, multiplication and division of polynomials algorithm over the ring $\mathbb{Z}_p$, for a given integer $p > 1$.

2 Arithmetic in $R[X]/(n)$

Using the previous routines, implement the addition, substraction and multiplication of polynomials over $R[X]/(n)$, where $R = \mathbb{Z}_p$ for some given integer $p > 1$ and $n \in R[X]$ is a polynomial of degree $\ell > 0$ with leading coefficient 1_R.

3 Horner's rule

Let $g \in R[X]$ and let $a \in R$. Horner's rule is an efficient algorithm to compute $g(a) \in R$.

Let $g = \sum_{i=0}^{k-1} g_i \cdot X^i$, where $k \geq 0$ and $g_i \in R$.

$\beta \leftarrow 0$
for $i \leftarrow k-1$ downto 0 do
  $\beta \leftarrow \beta \cdot \alpha + g_i$
output β.

1) Show that this algorithm correctly computes $g(\alpha)$.
2) Implement this algorithm with $R = \mathbb{Z}_n$ for some integer $n > 1$.