Université de Bordeaux **Computational Number Theory – N1MA9W11**
Master 2 MATH Année 2013–2014

EXERCISES, SESSION n° 1

Exercise 1 – Let R be a commutative ring containing a root of unity ω of order n such that $(1-\omega^\ell)$ is invertible for all ℓ not divisible by n. Prove that for all $T \in R[X]$, $\deg T < n$, we have

$$\mathcal{F}(\mathcal{F}(T,\omega),\omega^{-1}) = nT.$$

Exercise 2 – For $k \in \mathbb{Z}_{>0}$, write Φ_k for the k-th cyclotomic polynomial. Let R be a commutative ring, $n = p^k$ a power of a prime p. Let further $\omega \in R^*$ be of order n, such that $\Phi_n(\omega) = 0$. (This is automatic if R is a domain, but need not be true in general.) Using the factorization

$$\sum_{i<n} X^i = \prod_{j=1}^{k} \Phi_{p^j}(X) = \prod_{j=1}^{k} \Phi_p(X^{p^{j-1}}),$$

show that we still have

$$\sum_{i<n} \omega^{i\ell} = 0 \quad \text{when } \ell \not\equiv 0 \pmod{n},$$

so the conclusion of Exercise 1 still holds for $T \in R[X]$.

Exercise 3 – Representing polynomials in $\mathbb{Z}[X]$ by the vector of their coefficients, implement both the naive and Karatsuba multiplication algorithms in $\mathbb{Z}[X]$.

Exercise 4 – Let R be a commutative ring, m be an integer and $T \in R[X]$.

- let $T^\# \in R[X,Y]$ be the unique bivariate polynomial such that $T^\#(X, X^m) = T(X)$, $\deg_X T^\# < m$. Note that $\deg_Y T^\# = \lfloor \deg T/m \rfloor$.
- let $D = R[X]/(X^{2m}+1)$, in which $\omega = X$ is a primitive $4m$-th root of 1. We let $T^*(Y) = T^\#(X,Y) \mod X^{2m}+1 \in D[Y]$.

Study Algorithm 2 below and prove that its algebraic complexity $C(n)$ satisfies

$$C(n) \leqslant tC(2m) + O(n \log n).$$

Algorithm 1. Fast multiplication in $D[Y]$, $D = R[X]/(X^{2m}+1)$, $m = 2^k$

Input: $S, T \in D[Y]$, where $\deg S, \deg T < t$, where $t = m$ or $2m$.

Output: $t \times S \times T \pmod{Y^t - 1}$.

1: Let ω be the class of X^2 $(t = 2m)$, resp. the class of X^4 $(t = m)$; then ω is a primitive t-th root of 1 in D.

2: Compute $\omega^2, \dots, \omega^{t-1}$.

3: Compute $\mathcal{F}(S, \omega) = (a_0, \dots, a_{t-1})$.

4: Compute $\mathcal{F}(T, \omega) = (b_0, \dots, b_{t-1})$.

5: Return $\mathcal{F}\big((a_0 b_0, \dots, a_{t-1} b_{t-1}), \omega^{-1}\big)$.

Algorithm 2. Fast multiplication in $R[X]$, $\mathrm{Char} R \neq 2$ (Schönhage-Strassen)

Input: $f, g \in R[X]$ of degree $< n = 2^k$.

Output: $2^{e(n)} fg \mod X^n + 1$ for some $e(n) \in \mathbb{Z}_{\geqslant 0}$.

1: If $k \leqslant 2$, return $f \times g \mod X^n + 1$ using a naïve algorithm. In particular, $e(1) = e(2) = e(4) = 0$.

2: Let $m = 2^{\lfloor k/2 \rfloor}$ and $t = n/m = m$ or $2m$. Let $D = R[X]/(X^{2m}+1)$, and $f^*, g^* \in D[Y]$ be as above, with degree $< t$. Let η be a root of order $2t$ in D, namely $\eta = \omega$ $(t = 2m)$ or ω^2 $(t = m)$.

3: Compute $\mathcal{F}(f^*(\eta Y), \eta^2) = (a_0, \dots, a_{t-1}) \in D^t$, using Algorithm 1.

4: Compute $\mathcal{F}(g^*(\eta Y), \eta^2) = (b_0, \dots, b_{t-1}) \in D^t$.

5: Compute $\mathcal{F}\big((2^{e(2m)} a_0 b_0, \dots, 2^{e(2m)} a_{t-1} b_{t-1}), \eta^{-2}\big) = 2^{e(2m)+t} h^*(\eta Y)$ in $D[Y]$, $\deg h^* < t$. We call ourselves recursively for the t multiplications $a_i b_i$ in D, where we perform the multiplication on representatives of degree $< 2m$ in $R[X]$, yielding $2^{e(2m)} a_i b_i$ in $R[X]/(X^{2m}+1)$.

6: Recover $h^*(Y)$ from $h^*(\eta Y)$, then $h^\# \in R[X, Y]$ from h^* (lift all coefficients in D to their representative of minimal X-degree). Finally use $h^\#(X, X^m) = (fg)(X)$ to recover $2^{e(n)} fg \in R[X]$, with $e(n) = e(2m) + t$.

Exercise 5 – Let $B, C_0, C_1, \dots \in R[X]$ such that $B(0) = 1$ (so that B is invertible in $R[[X]]$), $C_0 = 1$ and $C_{i+1} \equiv 2C_i - BC_i^2 \pmod{X^{2^{i+1}}}$.

1) Prove that $BC_i \equiv 1 \pmod{X^{2^i}}$, for all $i \geqslant 0$.

2) Let $\mathsf{M}(n) := \mathsf{M}_{R[X]}(n)$. Assume that $2\mathsf{M}(n) \leqslant \mathsf{M}(2n)$ and that M is increasing. Prove that the above allows to compute $1/B \mod X^\ell$ in time $O(\mathsf{M}(\ell))$.