Algorithmic Number Theory

Course 12

Jean-Sébastien Coron

Université du Luxembourg

December 5, 2009

Summary

- Algorithmic number theory.
  - Polynomial arithmetic

Basic arithmetic

- Let R be a ring. Let $k \geq 1$.
  - We represent a degree $k-1$ polynomial
  $$a(X) = \sum_{i=0}^{k-1} a_i \cdot X^i \in R[X]$$
  as a coefficient vector $(a_0, a_1, \ldots, a_{k-1})$.
  - When $a_{k-1} \neq 0$, we let $\deg a = k-1$.
  - Example: $R = \mathbb{Z}$ or $R = \mathbb{Z}_n$.
- Addition and substraction of polynomials.
  - Just add or substract coefficient vectors.

Multiplication of polynomials

- Let $a = \sum_{i=0}^{k-1} a_i X^i \in R[X]$ and $b = \sum_{i=0}^{\ell-1} b_i X^i \in R[X]$ where $k, \ell \geq 1$.
  - The product $c := a \cdot b$ is of the form $c = \sum_{i=0}^{k+\ell-2} c_i X^i$
  - Can be computed in $\mathcal{O}(k \cdot \ell)$ operations in R:

```
for i ← 0 to k + ℓ − 2 do c_i ← 0
for i ← 0 to k − 1 do
    for j ← 0 to ℓ − 1 do
        c_{i+j} ← c_{i+j} + a_i · b_j
```

Division of polynomials

- Let a, b two polynomials in $R[X]$, such that the leading coefficient of b is invertible in R.
  - We want to compute $q, r \in R[X]$ such that
$$a = b \cdot q + r$$
    where $\deg r < \deg b$.
  - We denote $r := a \mod b$.
- Let $\deg a = k - 1$ and $\deg b = \ell - 1$.
  - if $k < l$, then let $q \leftarrow 0$ and $r \leftarrow a$

Division of polynomials

- Let $b_{\ell-1}$ be the leading term of b and let $b_{\ell-1}^{-1}$ be its inverse
  - 1) Let $r \leftarrow a$
  - 2) For $i \leftarrow k - \ell$ down to 0 do
    - $q_i \leftarrow a_{i+\ell-1} \cdot b_{\ell-1}^{-1}$
    - $r \leftarrow r - q_i \cdot b \cdot X^i$
  - 3) $q \leftarrow \sum_{i=0}^{k-\ell} q_i X^i$
- Complexity: $\mathcal{O}(\ell(k - \ell + 1))$.

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

- As for modular integer arithmetic, we can do arithmetic in $R[X]/(n)$.
  - Where $n \in R[X]$ is a polynomial of degree $\ell > 0$ whose leading coefficient is in R^* (most of the time, 1).
- Let $\alpha \in R[X]/(n)$. There exists $a \in R[X]$ such that $\alpha = \{a' \in R[X] : a' = a + p \cdot n, p \in R[X]\} = [a]_n$
  - One can take the *canonical representative* of α by taking the unique polynomial r such that $\deg r < \ell$ and $\alpha = [r]_n$
  - Select any polynomial $a' \in \alpha$, and compute $a = q \cdot n + r$ where $\deg r < \deg n = \ell$

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

- Addition, substraction
  - Compute $c := a + b$ or $c := a - b$.
  - Complexity: $\mathcal{O}(\ell)$ operations in R.
- Multiplication
  - Compute $c := a \cdot b$.
  - Compute $c' := c \mod n$.
  - Complexity: $\mathcal{O}(\ell^2)$ operations in R.