Algorithmic Number Theory

Course no. 13

Jean-Sébastien Coron

Université du Luxembourg

December 13, 2009

Summary

- Polynomial arithmetic
  - Polynomial congruence
  - Euclid's algorithm
  - Chinese remaindering and polynomial interpolation.

Basic arithmetic

- Let R be a ring. A polynomial $a \in R[X]$ is written

$$a(X) = \sum_{i=0}^{k-1} a_i \cdot X^i \text{ where } a_i \in R$$

  - Addition, substraction of polynomials.
  - Multiplication of polynomials.
- Division of polynomials.
  - Let $a, b \in R[X]$ such that the leading coefficient of b is invertible in R.
  - Compute $q, r \in R[X]$ such that $a = b \cdot q + r$ where $\deg r < \deg b$. We denote $r := a \mod b$.

Polynomial congruence

- Let F be a field. Let $n \in F[X]$.
  - For polynomials $a, b \in F[X]$, we say that a is congruent to b modulo n if $n | (a - b)$.
  - Notation: $a \equiv b \pmod{n}$.
- Using division with remainder:
  - For any $a \in F[X]$, there exists a unique $b \in F[X]$ such that $a \equiv b \pmod{n}$ and $\deg(b) < n$.
  - Take $b := a \mod n$.

Greatest Common Divisor

- Let F be a field. Let $a, b \in F[X]$.
  - $d \in F[X]$ is a *common divisor* of a and b if $d|a$ and $d|b$.
  - Such a d is a *greatest common divisor* of a and b if d is monic (leading coefficient equal to 1) or zero, and all other common divisors of a and b divide d.
  - We denote $d = \gcd(a, b)$.
- Theorem (proof: see Shoup's book).
  - For any $a, b \in F[X]$, there exists a unique greatest common divisor d of a and b.
  - Moreover, there exists $u, v \in F[X]$ such that $a \cdot u + b \cdot v = d$.

Euclid's algorithm

- Computes $\gcd(a, b)$ for $a, b \in F[X]$. Analogous to the integer case.
  - Input: $a, b \in F[X]$ with $\deg a \geq \deg b$ and $a \neq 0$.
  - Output $d = \gcd(a, b) \in F[X]$.
  - $r \leftarrow a,\ r' \leftarrow b$
    while $r' \neq 0$ do
    $\quad r'' \leftarrow r \mod r'$
    $\quad (r, r') \leftarrow (r', r'')$
    $d \leftarrow r/\mathrm{lc}(r)$ // lc=leading coefficient
    output d

Euclid's extended algorithm

- Input: $a, b \in F[X]$ with $\deg a \geq \deg b$ and $a \neq 0$.
- Output: $d, s, t \in F[X]$ such that $d = \gcd(a, b)$ and $as + bt = d$.

$r \leftarrow a,\ r' \leftarrow b$
$s \leftarrow 1, s' \leftarrow 0$
$t \leftarrow 0, t' \leftarrow 1$
while $r' \neq 0$ do
  Compute q, r'' such that $r = r'q + r''$, with
    $\deg(r'') < \deg(r')$
  $(r, s, t, r', s', t') \leftarrow (r', s', t', r'', s - s'q, t - t'q)$
$c \leftarrow \mathrm{lc}(r)$
$d \leftarrow r/c, s \leftarrow s/c, t \leftarrow t/c$
Output d, s, t.

Modular inverses

- Modular inverse
  - Let $n \in F[X]$, $n \neq 0$ and $a \in F[X]$. $a' \in F[X]$ is a *modular inverse of a modulo n* if $aa' \equiv 1 \pmod{n}$.
- Facts (analogous to the integer case)
  - Let $a, n \in F[X]$ with $n \neq 0$. Then a has a multiplicative inverse modulo n iff $\gcd(a, n) = 1$ (a and n are relatively prime).
  - If a has a multiplicative inverse, it is unique modulo n.
    - Denote by a^{-1} the unique mulitplicative inverse of a modulo n with $\deg(a) < \deg(n)$.

Computing modular inverses

- Let $n \in F[X]$ with $\ell := \deg n > 0$. Let $y \in F[X]$ with $\deg y < \ell$.
  - Using the Extended Euclidean Algorithm, find $d, s, t \in F[X]$ such that

$$s \cdot y + t \cdot n = d \quad \text{and } d = \gcd(y, n)$$

  - If $\gcd(y, n) = 1$, then s is a multiplicative inverse of y modulo n. Moreover, $\deg s < \ell$ so $s = y^{-1} \mod n$.
- Computation time:
  - $\mathcal{O}(\ell^2)$ operations in F.

The field $F[x]/(n)$

- If $n \in F[X]$ is irreducible, then $F[X]/(n)$ is a field.
  - Addition, substraction in $F[X]/(n)$ in $\mathcal{O}(\ell)$ operations.
  - Multiplication in $F[X]/(n)$ in $\mathcal{O}(\ell^2)$ operations.
  - Inverse in $F[X]/(n)$ in $\mathcal{O}(\ell^2)$ operations (using the Extended Euclidean algorithm).

Chinese remaindering

- Theorem (analogous to the integer case)
  - Let $n_1, \ldots, n_k \in F[X]$ such that $n_i \neq 0$ and $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Let $a_1, \ldots, a_k \in F[X]$. There exists a polynomial $z \in F[X]$ such that :

$$z \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k)$$

  - Moreover, the polynomial z is unique modulo $n := \prod_{i=1}^{k} n_i$.
  - $z := \sum_{i=1}^{k} \omega_i \cdot a_i$, where $\omega_i := n_i' \cdot m_i$, $n_i' := n/n_i$ and $m_i := (n_i')^{-1} \mod n_i$.

Polynomial interpolation

- Problem:
  - Given $(a_1, b_1), \ldots (a_k, b_k) \in F$, where the b_is are distinct, find $z \in F[X]$ such that $z(b_i) = a_i$ for all $i = 1, \ldots, k$ and $\deg z < k$.
- Can be viewed as a special case of Chinese remaindering.
  - Take $n_i = (X - b_i)$. The n_i are pairwise relatively prime since the b_i are distinct. $z \equiv a_i \mod n_i \Leftrightarrow z(b_i) = a_i$
  - $n'_i = \prod_{j \neq i}(X - b_j)$ and $m_i = 1/\prod_{j \neq i}(b_i - b_j) \in F$.

$$z = \sum_{i=1}^{k} a_i \frac{\prod_{j \neq i}(X - b_j)}{\prod_{j \neq i}(b_i - b_j)}$$