Algorithmic Number Theory

Course 7

Jean-Sébastien Coron

University of Luxembourg

May 2, 2014

Summary

- Polynomial arithmetic and applications.
  - Basic arithmetic
  - Euclid's algorithm
  - Chinese remaindering and polynomial interpolation.
- Many similarities with operations in $\mathbb{Z}$.

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 $k < \ell$, 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
    - $q_i \leftarrow r_{i+\ell-1} \cdot b_{\ell-1}^{-1}$
    - $r \leftarrow r - q_i \cdot b \cdot X^i$
  - 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 $\deg r < \deg n = \ell$

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 $b := a \mod n$.

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.

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
      $r'' \leftarrow r \mod r'$
      $(r, r') \leftarrow (r', r'')$
    $d \leftarrow r/\mathrm{lc}(r)$ // lc=leading coefficient
    output d

Theorem

Let $a, b \in F[X]$, *with* $\deg a \geq \deg b$ *and* $a, b \neq 0$. *The previous algorithm outputs* $\gcd(a, b)$ *in at most* $\deg b + 1$ *steps.*

Proof.

Let $r_0 = a$, $r_1 = b$ and $r_i = r_{i+1} \cdot q_i + r_{i+2}$ for $0 \leq i \leq \ell - 1$, where $r_{\ell+1} = 0$. We have that $\deg r_i$ for $i \geq 1$ is strictly decreasing, therefore $\ell \leq \deg b + 1$. Moreover,

$$\gcd(a, b) = \gcd(r_0, r_1) = \cdots = \gcd(r_\ell, r_{\ell+1}) = \gcd(r_\ell, 0) = r_\ell / \mathrm{lc}(r_\ell)$$

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. Moreover:

$$z \equiv a_i \pmod{n_i} \Leftrightarrow z(b_i) = a_i$$

  - $n_i' = \prod_{j \neq i}(X - b_j)$ and $m_i = 1/\prod_{j \neq i}(b_i - b_j) \in F$.

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

Polynomial interpolation

- Theorem
  - Given $(a_0, b_0), \ldots (a_{k-1}, b_{k-1}) \in F^2$, where the b_i's are distincts, there is a unique $z \in F[X]$ such that $z(b_i) = a_i$ for all $i = 0, \ldots, k-1$ and $\deg z < k$.
  - $z = \sum_{i=0}^{k-1} a_i \frac{\prod_{j \neq i}(X - b_j)}{\prod_{j \neq i}(b_i - b_j)}$
- Write $z = \sum_{i=0}^{k-1} z_i \cdot X^i$.
  - This implies that $\sigma : F^k \to F^k, (z_0, \ldots, z_{k-1}) \to (a_0, \ldots, a_{k-1})$ such that $a_i = z(b_i)$ for $i = 0, \ldots, k-1$ is a bijection.

Secret sharing

- Assume that Alice has a secret value $s \in F$ that she wants to share among m parties $P_1, \ldots, P_m$ with $m > k$ so that:
  - Any subset of k parties can reconstruct the secret s.
  - Any subset of less than $k-1$ parties obtain no information about s.

Application of secret-sharing

- Application:
  - Alice wants to backup some secret data on file servers.
  - Even if some of the file servers crash, she can always reconstruct her secret data as long as at least k servers are available.
  - If an attacker takes control of less than $k-1$ servers, then he obtains no information about Alice's secret.

Procedure

- Sharing the secret $s \in F$:
  - Alice generates and publish distinct elements $b_0, \ldots, b_m$ in F, where $b_0 = 0$.
  - Alice let $z_0 := s$, then generates random $z_1, \ldots, z_{k-1} \in F$, and let $z = \sum_{i=0}^{k-1} z_i X^i$
  - For $i = 1, \ldots, m$, Alice gives party P_i its share $a_i := z(b_i)$.
- Reconstructing the share
  - For the polynomial interpolation theorem, any subset of k parties can find s by first interpolating z on the k points and then recovering $z(b_0) = z(0) = s$.

Security

- Consider a subset of $k-1$ parties, $P_1, \ldots, P_{k-1}$, with corresponding $b_1, \ldots, b_{k-1}$.
  - Let $z(X) = \sum_{j=0}^{k-1} z_j X^j$ and $a_i = z(b_i)$ for all $1 \leq i \leq k-1$.
  - Write $a_0 := z(b_0) = z_0 = s$.
  - We have a bijection:

$$\begin{array}{rcl} \Psi_{z_0} : F^{k-1} & \rightarrow & F^{k-1} \\ (z_1, \ldots, z_{k-1}) & \rightarrow & (a_1, \ldots, a_{k-1}) \end{array}$$

    where $a_i = z(b_i)$ for all $1 \leq i \leq k-1$.
  - Namely for any $a_1, \ldots, a_{k-1}$, given $a_0 = z(b_0) = z_0$ there is a unique $z_0, z_1, \ldots, z_{k-1}$ such that $a_i = z(b_i)$ for all $0 \leq i \leq k-1$.
  - Therefore for all $s = z_0 \in F$, the vector $(a_1, \ldots, a_{k-1})$ is uniformly distributed in F^{k-1}.
- Therefore the vector $(a_1, \ldots, a_{k-1})$ does not given any information about the secret s.

Finite fields

- Definition
  - A field is a commutative ring $(F, +, *)$ such that $0 \neq 1$ and all elements except 0 have a multiplicative inverse.
  - A finite field is a field that contains only finitely many elements.
- Example:
  - For any prime p, $\mathbb{Z}_p$ is a finite field

Finite fields

- Properties
  - The order or number of elements of a finite field is of the form p^n for prime p and $n \geq 1$.
  - For any prime p and integer $n \geq 1$, there exists a finite field of p^n elements.
  - Any two finite fields with same number of elements are isomorphic.
- Notation
  - $GF(p^n)$ or $\mathbb{F}_{p^n}$.

Construction

- Construction of $GF(p^n)$
  - Select an irreducible polynomial $f(X)$ of degree n with coefficients in $GF(p)$
  - Then the set of polynomials in $GF(p)[X]$ modulo $f(X)$ is a finite field of size p^n.
- Example
  - $F(X) = X^2 + X + 1$ is irreducible in $GF(2) = \{0, 1\}$.
  - Then $GF(2^2) = GF(2)[X]/ < X^2 + X + 1 >$
  - $GF(2^2) = \{0, 1, X, X + 1\}$
  - Addition: addition of polynomials
  - Multiplication: use $X^2 + X + 1 = 0$

Example

- $f(X) = X^4 + X^3 + 1$ is irreducible over over $GF(2)$.
  - $f(0) = 0 + 0 + 1 = 1$ and $f(1) = 1 + 1 + 1 = 1$ so no root =¿ no irreducible factor of degree 1.
  - Only irreducible polynomial of degree 2: $X^2 + X + 1$ and $(X^2+X+1)^2 = X^4+2X^3+3X^2+2X+1 = X^4+X^2+1 \neq f(X)$
- $GF(2^4) = GF(2)/ < X^4 + X^3 + 1 >$
  - Its elements can be written $a_3X^3 + a_2X^2 + a_1X + a_0$ where $a_0, \ldots, a_3 \in \{0, 1\}^4$.
  - Can be represented as 4-bit strings.

The field $GF(2)/(X^4 + X^3 + 1)$

- Addition in $GF(2^4)$: bitwise xor.
- Multiplication: multiply the polynomials modulo f.
  - $1010 \to (X^3 + X)$, $0101 \to (X^2 + 1)$
  - $(X^3 + X)(X^2 + 1) = X^5 + X$
  - $X^5 + X = X^3 + 1 \mod (X^4 + X^3 + 1)$
  - so $1010 \cdot 0101 = 1001$
- Inversion: use Euclid extended algorithm (or exhaustive search for small fields).
  - $(X^3+X)\cdot(X^3+X+1) = X^6+X^3+X^2+X = X^2\cdot(X^3+1)+$ $X^3+X^2+X = X^5+X^3+X = (X^4+X)+X^3+X = X^4+X^3 = 1$
  - so $1010^{-1} = 1011$