Chapter 5 Modular algorithms and interpolation

$$
\begin{tikzcd}
\text{problem in } R \arrow[r, "\text{modular reduction}"] \arrow[d, "\text{direct computation}"'] & \text{problem in } R/<m> \arrow[d, "\text{modular computation}"] \\
\text{solution in } R & \text{solution in } R/<m> \arrow[l, "\text{reconstruction}"]
\end{tikzcd}
$$

Figure 5.1: General scheme for modular algorithms.

$$
\begin{tikzcd}
R \arrow[r, "\text{modular reduction}"] \arrow[d, "\text{direct computation}"'] & R/<m> \arrow[r, "\text{modular redcution}"] & \{R/<p_1>,\ldots,R/<p_r>\} \arrow[d, "\text{modular computation}"'] \\
R & R/<m> \arrow[l, "\text{reconstruction}"] & \{R/<p_1>,\ldots,R/<p_r>\} \arrow[l, "\text{reconstruction}"]
\end{tikzcd}
$$

Figure 5.2: General scheme for small primes modular algorithms.

$$
\begin{tikzcd}
R \arrow[r, "\text{modular reduction}"] \arrow[d, "\text{direct computation}"] & R/<p^l> \arrow[r, "\text{modular reduction}"] & R/<p> \arrow[d, "\text{modular computation}"] \\
R & R/<p^l> \arrow[l, "\text{reconstruction}"'] & R/<p> \arrow[l, "\text{lifing}"']
\end{tikzcd}
$$

Figure 5.3: General scheme for prime power modular algorithms.

5.1 Change of representation

1. Chooses a base and presents data in an expansion along powers of that base.

2. Represents a polynomial by it values at various points $u_0, \ldots, u_{n-1}$ or an integer modulo different primes $p_0, \ldots, p_{n-1}$.

Q1. In which representation is the problem easiest to solve?

Q2. How do we convert to and from that representation?

5.2 Evaluation and interpolation

Horner's rule: Evaluating a polynomial $f = \sum_{0 \le i < n} f_i x^i \in F[x]$ at $u \in F$

$$f(u) = (\cdots(f_{n-1}u + f_{n-2})u + \cdots + f_1)u + f_0$$

Given n points $u_0, \ldots, u_{n-1} \in F$, we define the evalution map $\chi : F^n \longrightarrow F^n$ by

$$\chi(f_0, \ldots, f_{n-1}) = \left(\sum_{0 \le j < n} f_j u_0^j, \ldots, \sum_{0 \le j < n} f_j u_{n-1}^j \right)$$

χ is represented by the Vandermonde matrix

$$V = VDM(u_0, \ldots, u_{n-1}) = \begin{pmatrix} 1 & u_0 & u_0^2 & \cdots & u_0^{n-1} \\ 1 & u_1 & u_1^2 & \cdots & u_1^{n-1} \\ 1 & u_2 & u_2^2 & \cdots & u_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & u_{n-1} & u_{n-1}^2 & \cdots & u_{n-1}^{n-1} \end{pmatrix} \in F^{n \times n}$$

V is nonsingular iff the u_i are distinct and V^{-1} is the matrix of the interpolation map.

Lagrange interpolant

$$l_i = \prod_{\substack{0 \le j < n \\ j \ne i}} \frac{x - u_j}{u_i - u_j} \in F[x]$$

$l_i(u_j) = \delta_{ij}$, i.e. 0 if $i \neq j$ or 1 if $i = j$.

Lagrange interpolation For arbitrary $v_0, \ldots v_{n-1} \in F$,

$$f = \sum_{0 \le i < n} v_i l_i = \sum_{0 \le i < n} v_i \prod_{\substack{0 \le j < n \\ j \ne i}} \frac{x - u_j}{u_i - u_j}$$

f is a polynomial of degree less than n such that $f(u_i) = v_i$ for all i:

Assume that V is nonsingular and let $V^{-1} = W = (w_{ij})_{i,j=0}^{n-1}$,

$$\sum_{j=0}^{n-1} w_{ij} u_k^j = \delta_{ik},\ k = 0 : n-1.$$

It can be solved by the Langrange interpolant:

$$\sum_{j=0}^{n-1} w_{ij} x^j = \prod_{\substack{0 \le j < n \\ j \ne i}} \frac{x - u_j}{u_i - u_j} = l_i$$

Theorem 1. *Evaluating a polynomial $f \in F[x]$ of degree less than n at n distinct points $u_0, \ldots, u_{n-1} \in F$ or computing an interpolating polynomial at these points can be performed with $O(n^2)$ operations in F. More precisely, evaluation takes $2n^2 - 2n$ operations, and Langrange interpolation uses $7n^2 - 8n + 1$ operations.*

5.3 Application: Secret sharing

5.4 The Chinese Remainder Algorithm

R is a Euclidean domain, $m_0, \ldots, m_{r-1} \in R$ are pairwise coprime, $m = lcm(m_0, \ldots, m_{r-1}) = m_0 \cdots m_{r-1}$. For $0 \leq i < r$, we have the canonical ring homomorphism

$$\begin{array}{rcl} \pi_i : R & \longrightarrow & R/ < m_i > \\ f & \longmapsto & f \mod m_i \end{array}$$

Combining these for all i, we get the ring homomorphism

$$\begin{array}{rcl} \chi = \pi_0 \times \cdots \times \pi_{r-1} : R & \longrightarrow & R/ < m_0 > \times \cdots \times R/ < m_{r-1} > \\ f & \longmapsto & (f \mod m_0, \ldots, f \mod m_{r-1}) \end{array}$$

Theorem 2. χ *i s surjective with kernel* $< m >$.

Corollary 1. *Chinese Remainder Theorem(CRT) We have the ring isomorphism*

$$R/ < m > \cong R/ < m_0 > \times \cdots \times R/ < m_{r-1} >$$

and the group isomorphism of the multiplicative groups

$$(R/ < m >)^\times \cong (R/ < m_0 >)^\times \times \cdots \times (R/ < m_{r-1} >)^\times >$$

Algorithm 5.4 Chinese Remainder Algorithm(CRA)

Input: $m_0, \ldots, m_{r-1} \in R$ pariwise coprime, $v_0, \ldots, v_{r-1} \in R$.

Output: $f \in R$ such that $f \equiv v_i \mod m_i$ for $0 \leq i < r$.

1. $m \longleftarrow m_0 \cdots m_{r-1}$
2. for $0 \leq i < r$ do
   compute m/m_i
   call the EEA to compute $s_i, t_i \in R$ with
   $s_i \frac{m}{m_i} + t_i m_i = 1$, $c_i \longleftarrow v_i s_i \operatorname{rem} m_i$
3. return $\sum_{0 \leq i < r} c_i \frac{m}{m_i}$

Theorem 3. *Let $R = F[x]$ for a field F, $m_0, \ldots, m_{r-1}, m \in R$, $d_i = \deg m_i \geq 1$ for $0 \leq i < r$, $n = \deg m = \sum_{0 \leq i < r} d_i$ and $v_i \in R$ with $\deg v_i < d_i$. Then the unique solution $f \in F[x]$ with $\deg f < n$ of the Chinese Remainder Problem*

$$f \equiv v_i \mod m_i \text{ for} 0 \leq i < r (*)$$

for polynomials can be computed using $O(n^2)$ operations in F.

Theorem 4. *Let $R = \mathbb{Z}, m_0, \ldots, m_{r-1}, m \in \mathbb{N}$, $n = \lfloor \log_2 m/64 + 1 \rfloor$ the word length of m, and $v_i \in \mathbb{Z}$ such that $0 \leq v_i < m_i$ for $0 \leq i < r$. Then the unique solution $f \in \mathbb{Z}$ with $0 \leq f < m$ of the Chinese Remainder Problem (*) for integers can be computed using $O(n^2)$ word operation.*

5.5 Modular determinant computation

Hadamard's inequality Given an $n \times n$ matrix $A = (a_{ij})_{1 \leq i,j \leq n} \in Z^{n \times n}$, $|\det A| \leq n^{n/2} B^n$, where $B = \max_{1 \leq i,j \leq n} |a_{ij}| \in \mathbb{N}$ is the maximal absolute value of an entry of A.

Theorem 5. *The cost of algorithm for calculating* $\det(A \mod p)$ *is* $O(n^3)$ *operations modulo* p *and* $O(n^3 \cdot n^2 (\log n + \log B)^2)$ *or* $O\left(n^5 \log^2 B\right)$ *word operations.*

Algorithm 5.10 Small primes modular determinant computation

Input: $A = (a_{ij})_{1\le i,j\le n} \in \mathbb{Z}^{n\times n}$, with $|a_{ij}| \le B$ for all i, j.

Output: $\det A \in \mathbb{Z}$.

1. $C \longleftarrow n^{n/2}B^n$, $r \longleftarrow \lceil \log_2(2C+1) \rceil$
   choose r distinct prime numbers $m_0, \ldots, m_{r-1} \in \mathbb{N}$

2. for $0 \le i < r$ do
   compute $d_i \in \{0, \ldots, m_i - 1\}$ such that $d_i \equiv \det A \mod m_i$ using Gaussian elimination over Z_{m_i}

3. call the CRA to determine a least absolute value $d \in \mathbb{Z}$ such that $d \equiv d_i \mod m_i$ for $0 \le i < r$, return d

Theorem 6. *The determinant of a matrix $A \in \mathbb{Z}^{n\times n}$ with all entries less than B in absolute value can be computed deterministically with*

$$O(n^4 \log^2(nB)(\log^2 n + (\log\log B)^2)) \,\mathrm{or}\, O\ (n^4 \log^2 B)$$

word operations

5.6 Hermite interpolation

If R is an arbitrary ring, $f \in R[x]$ has degree at most n, and $u \in R$, then the Taylor expansion of f around u is

$$f = f_n \cdot (x-u)^n + \cdots + f_1 \cdot (x-u) + f_0$$

$f_n, \ldots, f_0 \in R$ are the Taylor coefficients. The Taylor expansion of f around u of order e is

$$f \equiv f_{e-1} \cdot (x-u)^{e-1} + \cdots + f_1 \cdot (x-u) + f_0 \mod (x-u)^e.$$

A familiar form of Taylor expansion:

$$f = \frac{f^{(n)}}{n!} \cdot (x-u)^n + \cdots + \frac{f''(u)}{2} \cdot (x-u)^2 + f'(u) \cdot (x-u) + f(u).$$

The Hermite interpolation problem is to compute a polynomial $f \in F[x]$ of degree less than $n = e_0 + \cdots + e_{r-1}$ such that for all i, v_i is the Taylor expansion of f around u_i of order e_i, $u_i \in F$ are distinct:

$$f \equiv v_i \mod (x-u_i)^{e_i} \text{ for } 0 \le i < r.$$

5.7 Rational function reconstruction

Let F be a field, $m \in F[x]$ of degree $n > 0$, and $f \in F[x]$ of degree less than n. For a given $k \in \{0, \ldots, n\}$, find a rational function $r/t \in F[x]$ satisfying

$$\gcd(t, m) = 1 \text{ and } rt^{-1} \equiv f \mod m, \deg r < k, \deg t \leq n - k \ (**)$$

If we drop the gcd requirement, we obtain

$$r \equiv tf \mod m, \ \deg r < k, \deg t \leq n - k \ (***)$$

We say a rational function $r/t \in F(x)$ is in canonical form if t is monic and $\gcd(r, t) = 1$.

Lemma 1. *Let F be a field, $f, g, r, s, t \in F[x]$ with $\deg f = n, r = sf + tg$ and $t \neq 0$ and suppose that*

$$\deg r + \deg t < n = \deg f.$$

Moreover, let r_i, s_i, t_i for $0 \leq i \leq l + 1$ be the rows of the EEA for the pair (f, g). If we define $j \in \{1, \ldots, l + 1\}$ by

$$\deg r_j \leq \deg r < \deg r_{j-1}$$

then there exists a nonzero $\alpha \in F[x]$ such that

$$r = \alpha r_j, s = \alpha s_j, t = \alpha t_j.$$

Theorem 7. *Let $m \in F[x]$ of degree $n > 0$ and $f \in F[x]$ of degree less than n. Furthermore, let $r_j, s_j, t_j \in F[x]$ be the j-th row in the EEA for m, f where j is minimal such that $\deg r_j < k$.*

1. *There exist polynomials $r, t \in F[x]$ satisfying (***) namely $r = r_j$ and $t = t_j$. If in addition $\gcd(r_j, t_j) = 1$, then r and t also solve (**).*

2. *If $r/t \in F(x)$ is a canonical form solution to (**), then $r = \tau^{-1} r_j$ and $t = \tau^{-1} t_j$, where $\tau =$ lc$(t_j) \in F \backslash \{0\}$. In particular, (**) is solvable if and only if $\gcd(r_j, t_j) = 1$.*

Corollary 2. *There is an algorithm which decides whether (**) is solvable, and if so, computes its unique solution using $O(n^2)$ operations in F.*

input	moduli	polynomial output	rational function output
several values	$m_i = x - u_i$, u_i distinct	polynomial interpolation	Cauchy interpolation
Taylor expansion around 0	$m = x^n$		Padé approximation
Taylor expansions around several u_i	$m_i = (x - u_i)^{e_i}$, u_i distinct	Hermite interpolation	rational Hermit interpolation
remainder $\mod m$	m arbitrary		rational function reconstruction
reminders modulo several m_i	m_i arbitrary pairwise coprime	CRA	rational CRA

Various interpolation problems

5.8 Cauchy interpolation

Let F be a field, $u_0, \ldots, u_{n-1} \in F$ be distinct, $v_0, \ldots, v_{n-1} \in F$, $k \in \{0, \ldots, n\}$, Cauchy interpolation looks for a rational function $r/t \in F(x)$, with $r, t \in F[x]$, such that

$$t(u_i) \neq 0 \text{ and } \frac{r(u_i)}{t(u_i)} = v_i, \text{ for } 0 \leq i < n, \deg r < k, \deg t \leq n - k \;\; (**)$$

Dropping the requirement that it be nonzero, we obtain the weaker condition

$$r(u_i) = t(u_i)v_i \text{ for } 0 \leq i < n, \deg r < k, \deg t \leq n - k \;\; (***)$$

Corollary 3. *Let F be a field, $u_0, \ldots, u_{n-1} \in F$ be distinct, $v_0, \ldots, v_{n-1} \in F$, $f \in F[x]$ of degree less than n with $f(u_i) = v_i$ for all i, and $k \in \{0, \ldots, n\}$. Furthermore, let $r_j, s_j, t_j \in F[x]$ be the jth row in the EEA for the polynomials $m = (x - u_0) \cdots (x - u_{n-1})$ and f, where j is minimal such that $\deg r_j < k$.*

1. *There exist polynomials $r, t \in F[x]$ satisfying (***), namely $r = r_j$ and $t = t_j$. If in addition $\gcd(r_j.t_j) = 1$, then r and t also solve (**).*

2. *If $r/t \in F(x)$ is a canonical form solution to (**), then $r = \tau^{-1} r_j$ and $t = \tau^{-1} t_j$, where $\tau =$ lc$(t_j) \in F \setminus \{0\}$. In particular, (**) is solvable if and only if $\gcd(r_j, t_j) = 1$.*

5.9 Padé approximation

Let F be a field and $f = \sum_{i \geq 0} f_i x^i \in F[[x]]$ with all $f_i \in F$ be a formal power series. A Padé approximant to f is a rational function $\rho = r/t \in F(x)$, with $r, t \in F[x]$ and $x \nmid t$, that "approximates" f to a sufficiently high power of x. More precisely, r/t is a $(k, n-k)$-Padé approximant to f if

$$x \nmid t, \ \mathit{and} \ \frac{r}{t} \equiv f \mod x^n, \deg r < k, \deg t \leq n-k (****)$$

Corollary 4. *Let $f \in F[x]$ have degree less than $n \in N$, $k \in \{0, \ldots, n\}$, and $r_j, s_j, t_j \in F[x]$ be the jth row in the EEA for the polynomials $m = x^n$ and f, where j is minimal such that $\deg r_j < k$.*

1. *There exist polynomials* $r, t \in F[x]$ *satisfying*

$$r \equiv tf \mod x^n, \deg r < k, \deg t \leq n-k,$$

namely $r = r_j$ *and* $t = t_j$. *If in addition* $\gcd(r_j, t_j) = 1$, *then* r *and* t *also solve (**).*

2. *If* $r/t \in F(x)$ *is a canonical form solution to (****), then* $r = \tau^{-1} r_j$ *and* $t = \tau^{-1} t_j$, *where* $\tau =$ *lc*$(t_j) \in F \backslash \{0\}$. *In particular, (****) is solvable if and only if* $\gcd(r_j, t_j) = 1$.

5.10 Rational number reconstruction

Given integers $m > f \geq 0$ and $k \in \{1, \ldots, m\}$, to compute a rational number $r/t \in \mathbb{Q}$, with $r, t \in \mathbb{Z}$, such that

$$\gcd(t, m) = 1 \text{ and } rt^{-1} \equiv f \mod m,\ |r| < k, 0 \leq t \leq \frac{m}{k},$$

where t^{-1} is the inverse of t modulo m.

5.11 Partial fraction decomposition

Let F be a field, $f_1, \dots f_r \in F[x]$ nonconstant monic and pairwise coprime polynomials, $e_1, \dots, e_r \in \mathbb{N}$ positive integers, and $f = f_1^{e_1} \cdots f_r^{e_r}$. For another polynomial $g \in F[x]$ of degree less than $n = \deg f$, the partial fraction decomposition of the rational function $g/f \in F(x)$ is

$$\frac{g}{f} = \frac{g_{1,1}}{f_1} + \cdots + \frac{g_{1,e_1}}{f_1^{e_1}} + \cdots + \frac{g_{r,1}}{f_r} + \cdots + \frac{g_{r,e_r}}{f_r^{e_r}},$$

with $g_{ij} \in F[x]$ of smaller degree than f_i for all i, j.

Lemma 2. *There exist unique polynomials $c_i \in F[x]$ with $\deg c_i < e_i \deg f_i$ for all i such that*

$$\frac{g}{f} = \frac{c_1}{f_1^{e_1}} + \cdots + \frac{c_r}{f_r^{e_r}}.$$

Let R be a ring and $a, p \in R[x]$ with p monic of degree $m > 0$ and a of degree less than km, for some $k, m \in \mathbb{N}$. The p-adic expansion of a is

$$a = a_{k-1}p^{k-1} + \cdots + a_1 p + a_0,$$

where $a_0, \ldots, a_{k-1} \in R[x]$ have degree less than m.

Lemma 3. *The p-adic expansion exists uniquely, and it can be computed using at most $(km)^2 - km^2$ operations in R.*

Theorem 8. *The partial fraction decomposition exists uniquely, and it can be computed using $O(n^2)$ operations in F.*