Squarefree Factorization

The squarefree factorization of $a(x) \in \mathcal{Z}[x]$ consists of determining the squarefree pariwise relatively prime polynomials $b_1(x), \ldots, b_s(x)$ such that

$$a(x) = \prod_{i=1}^{s} b_i(x)^i.$$

Algorithm for Squarefree Factorization

Input: A primitive polynomial $a(x) \in \mathcal{Z}[x]$.

Output: $F = [b_1(x), \ldots, b_s(x)]$ is the list of squarefree factors of $a(x)$.

1. $F := [\ ]$;
   $a_1 := a$;
   $a_2 := \gcd(a_1, a_1')$;
   $c_1 := a_1/a_2$;
   $a_3 := \gcd(a_2, a_2')$;
   $c_2 := a_2/a_3$;
   $F := \mathrm{CONS}(c_1/c_2, F)$;

2. while $c_2 \neq 1$ do
   $a_2 := a_3$;
   $a_3 := \gcd(a_3, a_3')$;
   $c_1 := c_2$;
   $c_2 := a_2/a_3$;
   $F := \mathrm{CONS}(c_1/c_2, F)$;

3. $F := \mathrm{INV}(F)$; return.

Irreducible Factorization

The problem of factoring a primitive univariate polynomial $a(x) \in \mathcal{Z}[x]$ consists of finding the pariwise relatively prime irreducible polynomials $a_i(x)$ and positive integers m_i such that

$$a(x) = \prod_{i=1}^{r} a_i(x)^{m_i}.$$

Kronecker's Algorithm for Factorization

Input: A primitive squarefree polynomial $f(x) \in \mathcal{Z}[x]$, $\deg(f) = m$.

Output: Find polynomial $g(x)$ satisfies $g(x)|f(x)$.

For $k = 1, 2, \ldots, \lfloor m/2 \rfloor$ do

1. Choose $k+1$ distinct integers $x_0, x_1, \ldots, x_k$;
2. If there exists x_i such that $f(x_i) = 0$
   then return $g := x - x_i$ and stop
   else determine tge set E of $k+1$-tuples of integers
   $(d_0, d_1, \ldots, d_k) \in \mathcal{Z}^{k+1}$ such that each d_i runs over the set of the divisors of $f(x_i)$;
3. For all $d = (d_0, d_1, \ldots, d_k) \in E$ compute the polynomial $g_d \in \mathcal{Z}[x]$
   such that $g_d(x_i) = d_i$ for $i = 0, 1, \ldots, s$;
   if g_d divides $f($ in Q[x]) then return $g := g_d$ and stop.

Homework

1. Compute the squarefree factorization of
$$f(x) = 3x^6 - 2x^5 + 7x^4 - 4x^3 + 5x^2 - 2x + 1.$$
2. Prove $f(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible.(try expand $f(x+1)$ and prove $f(x+1)$ is irreducible)
3. By Kronecker's algorithm to factor
$$f(x) = x^4 + 3x^2 - 2x + 3.x$$

Berlekamp's Algorithm for Factoring in $Z_p[x]$.

Input: A squarefree polynomial $a(x) \in Z_p[x]$, p is a prime number.

Output: F is the list of prime factors of a.

1. Form the $(n \times n)$−matrix Q over Z_p, where the k-th line $(q_{k,0}, \ldots, q_{k,n-1})$ of Q satisfies:
rem$(x^{pk}, a(x)) = q_{k,n-1}x^{n-1} + \cdots + q_{k,0}$, for $0 \le k \le n-1$.

2. By column operations transform the matrix $Q - I$ into triangular form; read off the rank $n - r$ of the matrix $Q - I$ and independent solutions $v^{[1]}, \ldots, v^{[r]}$ of $v \cdot (Q - I) = 0$. Let $v^{[1]}$ be the trivial solution $(1, 0, \ldots, 0)$.

3. There are r irreducible factors of a. If $r = 1$, then set $F := [a(x)]$; otherwise, compute $\gcd(a(x), v^{[2]}(x) - s)$ for $s \in Z_p$ and put the factors of a found in this way into the list F; as long as F contains fewer than r factors, choose the next $v^{[k]}, k = 3, \ldots, r$, and compute the $\gcd(f(x), v^{[k]}(x) - s)$ for f in F and add the factors found in this way to F.

Hensel's Lifting Algorithm(linear version).

Input: $f(x), g_1(x), h_1(x)$, satisfy $f = g_1 h_1 \mod p$, p is a prime and k is a positive integer.

Output: $g_k(x)$ and $h_k(x)$ such that $f = g_k h_k \mod p^k$ and $g_k = g_1 \mod p, h_k = g_1 \mod p$.

1. Set $g(x) := g_1(x)$;
$h(x) := h_1(x)$;
apply Extend Euclidean alogorithm to obtain $u(x)$ and $v(x)$ satisfy $u(x)g_1(x) + v(x)h_1(x) = 1 \mod q$.

2. For $i := 2..k$ do

2.1. $r(x) := \frac{f(x) - g(x)h(x) \mod p^i}{p^{i-1}}$;

2.2. $u_1(x) := r(x) * u(x) \mod (p, h_1(x))$;
$v_1(x) := r(x) * v(x) \mod (p, g_1(x))$.

2.3. $g(x) := g(x) + p^{i-1}v_1(x)$;
$h(x) := h(x) + p^{i-1}u_1(x)$.

3. Return g and h.

Hensel's Lifting Algorithm(quadritic version).

Input: $f(x), g_1(x), h_1(x)$, satisfy $f = g_1 h_1 \mod p$, p is a prime and k is a positive integer.

Output: $g_k(x)$ and $h_k(x)$ such that $f = g_k h_k \mod p^k$ and $g_k = g_1 \mod p, h_k = g_1 \mod p$.

1. Set $g(x) := g_1(x)$;
$h(x) := h_1(x)$;
$q := p$.

2. For $i := 2..\lceil \log_2 k \rceil$ do

2.1. $r(x) := \frac{f(x)-g(x)h(x) \mod q^2}{q}$;

2.2. Apply Extend Euclidean alogorithm to obtain $u(x)$ and $v(x)$ satisfy $u(x)g(x) + v(x)h(x) = 1 \mod q$;

2.3. $u_1(x) := r(x) * u(x) \mod (q, h(x))$;
$v_1(x) := r(x) * v(x) \mod (q, g(x))$;

2.4. $g(x) := g(x) + q * v_1(x)$;
$h(x) := h(x) + q * u_1(x)$;
$q := q^2$.

3. Return g and h.

Algorithm for Factoring Univariate Polynomials over the Integers

Input: A primitive squarefree polynomial $a(x)$ in $Z[x]$.

Output: $F = [a_1, \ldots, a_r]$ such that a_i are all primitive irreducible factors of a.

1. Choose a prime number p that can not be divided by $\mathrm{lc}(a)$ and a is squarefree modulo p.

2. Apply Berlekamp algorithm to factor

$$a(x) = u_1(x) \cdots u_s(x) \mod p$$

normalize the $u_i's$ such that $\mathrm{lc}(u_1) = \mathrm{lc}(a) \mod p$ and $\mathrm{lc}(u_2) = \cdots = \mathrm{lc}(u_s) = 1$.

3. Determine a natural number B which bounds the absolute value of any coefficient in the factor of a over the integers. (Laudau-Mignotte bound or other optimal bound.)

$$K := min\{k \in \mathcal{N} : \quad p^k \geq 2|\mathrm{lc}(a)|B \quad \}.$$

4. Lift the factors to

$$a = v_1 \cdots v_s \mod p^K.$$

5. Combine factors $v_1, v_2, \ldots, v_s$ to find the ture factors $a_1, \ldots, a_r$.

6. Return $F := [a_1, \ldots, a_r]$.

Kronecker's Algorithm for Factoring Multivariate Polynomials over the Integers

Input: A multivariate polynomial $f \in Z[x_1, \ldots, Z_n]$.

Output: $F = [f_1, \ldots, f_s]$ such that f_i are all irreducible factors of f.

1. Compute degree bound

$$d := (\max_{1 \leq i \leq n} \deg_{x_i}(f)) + 1.$$

2. Reduce f to univariate case and factor it into

$$S_d(f) = g_1 \dots g_s \quad \text{in} \quad Z[t].$$

3. Recover multivariate factors by combinations

$F := [\ ]; C := \{1, \dots, s\}; i := 0;$
while $C \neq \emptyset$ do

$i := i + 1;$
for all $g_{j_1}, \dots, g_{j_i}$ such that $j_k \in C$ do
$g := {S_d}^{-1}(g_{j_1} \cdots g_{j_i});$
if $g|f$ then
$F := CONS(g, F); C := C \setminus \{j_1, \dots, j_i\};\ f := f/g.$

4. Return F.

Algorithm for Factoring Multivariate Polynomials over the Integers

Input: A multivariate polynomial $f \in Z[x_1, \dots, x_n]$.

Output: $F = [f_1, \dots, f_s]$ such that f_i are all irreducible factors of f.

1. Choose an evaluation point $(c_1, c_2, \dots, c_{n-1})$ such that $f(c_1, \dots, c_{n-1}, x_n)$ preserves the degree and squarefreeness and as many c_i be zero as possible.

2. By the change of variables $x_1 = x_1 - c_1, \dots, x_{n-1} = x_{n-1} - c_{n-1}$ we move the evaluation point to the origin: $\overline{f}(x_1, \dots, x_{n-1}, x_n) = f(x_1 - c_1, \dots, x_{n-1} - c_{n-1}, x_n)$ and $\overline{f}(0, \dots, 0, x_n) = f(c_1, \dots, c_{n-1}, x_n)$.

3. By the univariate factorization algorithm we get

$$\overline{f}(x_1, \dots, x_{n-1}, x_n) = u_1(x_n)u_2(x_n) \cdots u_s(x_n) \mod S.$$

Where $S = (x_1, x_2, \dots, x_{n-1})$.

4. By Henel lifting algorithm, the factors are lift to:

$$\overline{f}(x_1, \dots, x_{n-1}, x_n) = v_1 v_2 \cdots v_s \mod S^k.$$

5. When k is bigger than total degree of f, combine factors $v_1, v_2, \ldots, v_s$ to find the ture factors $\overline{a_1}, \ldots, \overline{a_r}$.

6. Let $a_i = \overline{a_i}(x_1 + c_1, \ldots, x_{n-1} + c_{n-1}, x_n)$, return $F := [a_1, \ldots, a_r]$.