Chapter 15 Hensel lifting and factoring polynomials

15.1 Factoring in $\mathbb{Z}[x]$: the basic idea

If a squarefree f factors as $f = f_1 \cdots f_k$ in $\mathbb{Z}[x]$, then $\bar{f} = \bar{f}_1 \cdots \bar{f}_k$ in $\mathbb{Z}_p[x]$, but $\bar{f}_i$ need not be irreducible.

1. How large do we have to choose p to recover f_i from $\bar{f}_i$.
2. How about the probability of p so that $f \mod p$ is squarefree.
3. How can we find the modular factors of $f \mod p$ that correspond to a true irreducible factor of f in $\mathbb{Z}[x]$.

15.2 A factoring algorithm

Lemma 1. *Let* $f \in \mathbb{Z}[x]$ *be a nonzero squarefree polynomial,* $p \in \mathbb{N}$ *a prime not dividing* lc(f)*, and denoted by a bar the reduction modulo* p*. Then* $\bar{f}$ *is squarefree if and only if* $p \nmid \mathrm{disc}(f)$*,* $\mathrm{disc}(f) =$ *res*(f, f') *the discriminant of* f*.*

Let $f = f_1 \cdots f_k$ in $\mathbb{Z}[x]$ be the irreducible factorization of f, then

$$\bar{f} = \bar{f}_1 \cdots \bar{f}_k = \bar{\mathsf{lc}}(f) g_1 \cdots g_r \in \mathbb{F}_p[x]$$

where $g_1, \ldots, g_r$ are the monic irreducible factors of $\bar{f}$ in $\mathbb{F}_p[x]$.

Algorithm 15.2 Factorization in $\mathbb{Z}[x]$(big prime version)

Input: A squarefree primitive polynomial $f \in \mathbb{Z}[x]$ of degree $n > 0$ with $\mathrm{lc}(f) > 0$ and $\|f\|_\infty = A$.

Output: The irreducible factors $\{f_1, \ldots, f_k\} \subseteq \mathbb{Z}[x]$ of f.

1. if $n = 1$ then return $\{f\}$
   $b \longleftarrow \mathrm{lc}(f), B \longleftarrow (n+1)^{1/2} 2^n A b$

2. repeat
   choose a random odd prime p with $2B < p < 4B$
   $\bar{f} \longleftarrow f \mod p$
   until $\gcd(\bar{f}, \bar{f}') = 1$ in $\mathbb{F}_q[x]$

3. compute the irreducible factorization $f \equiv b g_1 \cdots g_r \mod p$.

4. $F \longleftarrow \{1, \ldots, r\}, s \longleftarrow 1, G \longleftarrow \varnothing, f^* \longleftarrow f$

5. while $2s \leq \sharp T$ do

   for all subsets $S \subseteq T$, $\sharp S = s$ do

   compute $g^*, h^* \in \mathbb{Z}[x]$, $\|g^*\|_\infty < p/2, \|h^*\|_\infty < p/2$ satifying

   $g^* \equiv b\Pi_{i \in S} g_i \mod p$ and $h^* \equiv b\Pi_{i \in T \setminus S} g_i \mod p$

   if $||g^*||_1, ||h^*||_1 \leq B$ then

   $T \longleftarrow T \setminus S, G \longleftarrow G \bigcup \{\text{pp}(g^*)\}$

   $f^* \longleftarrow \text{pp}(h^*), b \longleftarrow \text{lc}(f^*)$ go to 6

   $s \longleftarrow s + 1$

6. return $G \cup \{f^*\}$

Algorithm 15.5 Polynomial factorization in $\mathbb{Q}[x]$

Input: A polynomial $f \in \mathbb{Z}[x]$ of degree $n > 0$ and $\|f\|_\infty = A$.

Output: A constant $c \in \mathbb{Z}$ and a set of pairs $\{(f_1, e_1), \ldots, (f_k, e_k)\}$ such that $f = cf_1^{e_1} \ldots f_r^{e_r}$ is irreducible factorization of f.

1. $c \longleftarrow \mathrm{cont}(f), g \longleftarrow$ pp(f), if lc$(f) < 0$ then $c \longleftarrow -c, g \longleftarrow -g$

2. call Yun's algorithm compute squarefree decomposition $g = \Pi_{1 \le i \le s} g_i^i$ of g

3. $G \longleftarrow \varnothing$, for $1 \le i \le s$ do
   compute the irreducible factors $h_1, \ldots, h_t \in \mathbb{Z}[x]$ of g_i
   $G \longleftarrow G \bigcup \{(h_1, i), \ldots, (h_t, i)\}$

4. return c and G.

15.3 Frobenius's and Chebotarev's density theorem

Let $f = f_1 \dots f_k$ be its factorization with $f_1, \dots, f_k \in \mathbb{Z}[x]$ irreducible. Then

$$f \mod p = (f_1 \mod p) \cdots (f_k \mod p)$$

$f_i \mod p$ may not be irreducible, the factor combination stage may try exponentially many combinations.

1. Swinnerton-Dyer polynomial

$$f = \Pi(x \pm \sqrt{2} \pm \sqrt{3} \pm \cdots \pm \sqrt{p_i}) \in \mathbb{Z}[x]$$

f is irreducible polynomial The irreducible factors of $f \mod p$ in $\mathbb{F}_p[x]$ are either all linear(or all quadratic.

$$\begin{aligned} f &= \Pi(x \pm \sqrt{2} \pm \sqrt{3}) = x^4 - 10x^2 + 1 \\ &\equiv (x+2)(x-2)(x+11)(x-11) \mod 23 \end{aligned}$$

2. nth cyclotomic polynomial

$$\Phi_n = \prod_{\substack{\omega \in \mathbb{C} \text{primitive} \\ nth \text{root of unity}}} (x - \omega) = \prod_{\substack{1 \le k < n \\ \gcd(k,n)=1}} (x - e^{2\pi i k/n}) \in \mathbb{C}[x]$$

Φ_n are irreducible over $\mathbb{Q}$ bit split modulo each prime for most n.

$$\Phi_5 = x^4 + x^3 + x^2 + x + 1 \equiv (x+2)(x+6)(x+7)(x+8) \mod 11$$

3. For a random polynomials of degree n, it remains irreducible modulo p for a fraction of only about $1/n$ for all primes.

15.4 Hensel lifting

Let R be a ring (commutative, with 1), for example $R = \mathbb{Z}, \mathbb{F}[y]$, $f, g, h \in R[x]$, and $m \in R$ such that $f \equiv gh \mod m$. We want to lift this to a factorization $f \equiv \hat{g}\hat{h} \mod m^2$. Assume we have $s, t \in R[x]$ with $sg + th \equiv 1 \mod m$. We now calculate

$$e = f - gh, \hat{g} = g + te, \hat{h} = h + se$$

and find

$$\begin{aligned} f - \hat{g}\hat{h} &= f - gh - gse - hte - ste^2 = f - gh - (sg + th)e - ste^2 \\ &= (1 - sg - th)e - ste^2 \equiv 0 \mod m^2 \end{aligned}$$

since $e \equiv 0 \mod m$ and $(1 - sg - th) \equiv 0 \mod m$.

Lemma 2. *Let* $f, g \in R[x]$ *with* g *nonzero and monic. Then there exist unique polynomials* $q, r \in R[x]$ *with* $f = qg + r$ *and* $\deg r \leq \deg g$. *If* $f \equiv 0 \mod m$, *then* $q \equiv r \equiv 0 \mod m$.

Algorithm 15.10 Hensel step

Input: An element m in a ring R, and polynomials $f, g, h, s, t \in R[x]$ such that

$$f \equiv gh \mod m, \;\; sg + th \equiv 1 \mod m$$

h is monic, $\deg f = \deg g + \deg h, \deg s < \deg h, \deg t < \deg g$.

Output: Polynomials $g^*, h^*, s^*, t^* \in R[x]$ such that

$$f \equiv g^* h^* \mod m^2, \;\; s^* g^* + t^* h^* \equiv 1 \mod m^2$$

h^* is monic,

$$\begin{array}{l} g^* \equiv g \mod m, h^* \equiv h \mod m, \\ s^* \equiv s \mod m, t^* \equiv t \mod m, \end{array}$$

$\deg g^* = \deg g, \deg h^* = \deg h, \deg s^* < \deg h^*$, and $\deg t^* < \deg g^*$.

1. compute $e, q, r, g^*, h^* \in R[x]$ such that $\deg r < \deg h$ and

$$\begin{aligned} e &\equiv f - gh \mod m^2,\ se \equiv qh + r \mod m^2 \\ g^* &\equiv g + te + qg \mod m^2,\ h^* \equiv h + r \mod m^2 \end{aligned}$$

2. compute $b, c, d, s^*, t^* \in R[x]$ such that $\deg d < \deg h^*$ and

$$\begin{aligned} b &\equiv sg^* + th^* - 1 \mod m^2,\ sb \equiv ch^* + d \mod m^2 \\ s^* &\equiv s - d \mod m^2,\ t^* \equiv t - tb - cg^* \mod m^2 \end{aligned}$$

3. return g^*, h^*, s^*, t^*.

Theorem 1. *Algorithm 15.10 works correctly as specified. It uses $O(M(n)M(\log m))$ word operations if $R = \mathbb{Z}, m > 1$, and all inputs have max-norm less than m^2, and $O(M(n)M(\deg_y m))$ operations in the field if $R = F[y]$ and the degree in y of all inputs is less than $2\deg_y m$.*

Proof:

$$\begin{aligned} f - g^*h^* &\equiv f - (g + te + qg)(h + se - qh) \\ &= f - gh - (sg + th)e - ste^2 - (sg - th)qe + ghq^2 \\ &= (1 - sg - th)e - ste^2 - (sg - th)qe + ghq^2 \equiv 0 \mod m^2 \end{aligned}$$

Theorem 2. *Hensel's lemma Given $l \in \mathbb{N}_{>0}$ and assuming the input specification of Algorithm 15.10, we can compute polynomials as in the output specification, but with m^2 replaced by m^l.*

Theorem 3. *Uniqueness of Hensel lifting Let R be a ring(commutative, with 1), $m \in R$ not a zero divisor, $l \in \mathbb{N}_{\geq 1}$, and $g, h, g^*, h^*, s, t \in R[x]$ nonzero such that $sg + th \equiv 1 \mod m$, the leading coefficients lc(g), lc(h) are not zero divisors modulo m, the polynomials g and g^* have the same leading coefficient and the same degree, and coincide modulo m, and similarly for h and h^*. If $gh \equiv g^*h^* \mod m^l$, then $g \equiv g^* \mod m^l$, and $h \equiv h^* \mod m^l$.*

15.5 Multifactor Hensel lifting

Let R be a ring, $m \in R$ and $f, f_1, \ldots, f_r \in R[x]$ such that $\mathrm{lc}(f)$ is a unit modulo m, $f_1, \ldots, f_r$ are monic, and $f \equiv \mathrm{lc}(f) f_1 \cdots f_r \mod m^i$. We arrange the monic factors v of $f \mod m$ as aa binary tree τ of depth $d = \lceil \log_2 r \rceil$ with leaves $f_1, \ldots, f_r$, root af, and such that each internal node is the product of its two children modulo m. Furthermore, at each internal node $v \in R[x]$ with children $g_v, h_v \in R[x]$, we need $s_v, t_v \in R[x]$ such that $\deg s_v < \deg h_v, \deg t_v < \deg g_v$, and $s_v g_v + t_v h_v \equiv 1 \mod m$. We call such a tree τ, including the s_v, t_v a factor tree of $f \mod m$.

Algorithm 15.17 Multifactor Hensel lifting

Input: An element m in a ring R, $f \in R[x]$ of degree $n, a_0 \in R$ such that $a_0 \mathrm{lc}(f) \equiv 1 \mod m, l \in \mathbb{N}$, and a factor tree τ of f modulo m, with root $a_0 f$ and r leaves.

Output: An inverse $a^* \in R$ of $\mathrm{lc}(f) \mod m^l$ and a factor tree τ^* of $f \mod m^l$ with root $a^* f$ such that each node $v^* \in R[x]$ of τ^* is congruent modulo m to the corresponding node $v \in R[x]$ of τ.

1. $d \longleftarrow \lfloor \log_2 k \rfloor$, $\tau_0 \longleftarrow \tau$

2. for $j = 1, \ldots, d$ do
   compute $a_j \in R$ such that $a_j \equiv 2a_{j-1} - \mathrm{lc}(f) a_{j-1}^2 \mod m^{2^j}$
   $\tau_j \longleftarrow \tau_{j-1}$
   replace the root of τ_j by $a_j f$.

for each internal node $v \in R[x]$ of τ_j, from the root to the leaves do

lift the congruences $v \equiv g_v h_v$ and $s_v g_v + t_v h_v \equiv 1 \mod m^{2^{j-1}}$ to congruences modulo m^{2^j}.

3. return a_d and τ_d.

15.6 Factoring using Hensel lifting: Zassenhaus's algorithm

Algorithm 15.19 Factorization in $Z[x]$ (prime power version)

Input: A squarefree primitive polynomial $f \in \mathbb{Z}[x]$ of degree $n \geq 1$ with $\mathrm{lc}(f) > 0$ and $||f||_\infty = A$.

Output: The irreducible factors $\{f_1, \ldots, f_k\} \subseteq \mathbb{Z}[x]$ of f.

1. if $n = 1$ then return $\{f\}$
   $b \longleftarrow \mathrm{lc}(f), B \longleftarrow (n+1)^{1/2} 2^n A b,$
   $C \longleftarrow (n+1)^{2n} A^{2n-1}, \gamma \longleftarrow \lceil 2 \log_2 C \rceil$

2. repeat choose a prime $p \leq 2\gamma \mathrm{ln}\gamma, \bar{f} \longleftarrow f \mod p$

until $p \nmid b$ and $\gcd(\bar{f}, \bar{f}') = 1$ in $\mathbb{F}_p[x]$
$l \longleftarrow \lceil \log_p(2B+1) \rceil$

3. compute irreducible factor of f modulo p: $f \equiv bh_1 \cdots h_r \mod p$.

4. $a \longleftarrow b^{-1} \mod p$
   use EEA set up a factor tree of $f \mod p$ with leaves $h_1, \ldots, h_r$
   lift the factorization to $f \equiv bg_1 \cdots g_r \mod p^l$ with monic polynomials $g_1, \ldots, g_r \in \mathbb{Z}[x]$ of max-norm at most $p^l/2$ such that $g_i \equiv h_i \mod p$ for $1 \leq i \leq r$

5. $T \longleftarrow \{1, \ldots, r\}, s \longleftarrow 1, G \longleftarrow \varnothing, f^* \longleftarrow f$

6. while $2s \leq \sharp T$ do
   for all subsets $S \subseteq T$ of cardinality $\sharp S = s$ do

compute $g^*, h^* \in \mathbb{Z}[x]$, $\|g^*\|_\infty < p/2, \|h^*\|_\infty < p/2$ satifying
$g^* \equiv b\Pi_{i\in S} g_i \mod p^l$ and $h^* \equiv b\Pi_{i\in T\setminus S} g_i \mod p^l$
if $||g^*||_1||h^*||_1 \leq B$ then
$T \longleftarrow T\setminus S, G \longleftarrow G \bigcup \{\text{pp}(g^*)\}$
$f^* \longleftarrow$ pp$(h^*), b \longleftarrow$ lc(f^*) go to 6

7. $s \longleftarrow s + 1$

8. return $G \cup \{f^*\}$

Algorithm 15.20 Bivariate Factorization in (prime power version)

Input: A primitive polynomial $f \in R[x] = F[x, y]$, where $R = F[y]$ for a field F with at least $4nd$ elements and effective univariate factorization, such that $\deg_x f = n \geq 1, \deg_y f = d$, and $\gcd(f, \partial f/\partial x) = 1$ in $F(y)[x]$.

Output: The irreducible factors $\{f_1, \ldots, f_k\} \subseteq F[x, y]$ of f.

1. if $n = 1$ then return f
   $b \longleftarrow \mathrm{lc}_x(f)$
   choose $U \subseteq F$ of cardinality $\sharp U = 4nd$

2. repeat randomly choose an element $u \in U, \bar{f} \longleftarrow f(x, u)$
   until $b(u) \neq 0$ and $\gcd(\bar{f}, \bar{f}') = 1$ in $F[x]$
   $l \longleftarrow d + 1 + \deg b$

3. compute a univariate irreducible factorization $f \equiv bh_1 \cdots h_r \mod (y-u)$.

4. $a \longleftarrow b(u)^{-1}$
   set up a factor tree of $f \mod y-u$ with leaves $h_1, \ldots, h_r$
   lift the factorization to $f \equiv bg_1 \cdots g_r \mod (y-u)^k$, $\deg_y g_i < l$ and $g_i(x,u) = h_i$ for $1 \leq i \leq r$

5. $T \longleftarrow \{1, \ldots, r\}, s \longleftarrow 1, G \longleftarrow \varnothing, f^* \longleftarrow f$

6. while $2s \leq \sharp T$ do
   for all subsets $S \subseteq T$ of cardinality $\sharp S = s$ do
   compute $g^*, h^* \in \mathbb{F}[x,y]$ of degree less than l in y satisfying,
   $g^* \equiv b\Pi_{i \in S} g_i \mod (y-u)^l$ and $h^* \equiv b\Pi_{i \in T \setminus S} g_i \mod (y-u)^l$
   if $\deg(g^* h^*) = \deg(bf^*)$ then
   $T \longleftarrow T \setminus S, G \longleftarrow G \bigcup \{\mathrm{pp}_x(g^*)\}$

$$f^* \longleftarrow \mathsf{pp}_x(h^*), b \longleftarrow \mathsf{lc}_x(f^*) \text{ go to 6}$$

7. $s \longleftarrow s+1$

8. return $G \cup \{f^*\}$

Algorithm 15.24 Bivariate Polynomial factorization

Input: A polynomial $f \in \mathbb{F}[x, y]$ with $\deg_x f = n$ and $\deg_y f = d$ where $\mathbb{F}$ is field with effective univariate factorization.

Output: A constant $a \in \mathbb{F}$ and a set of pairs $\{(f_1, e_1), \ldots, (f_k, e_k)\}$ such that $f = cf_1^{e_1} \ldots f_r^{e_r}$ is irreducible factorization of f.

1. $G \longleftarrow \varnothing$, $c_x \longleftarrow \mathrm{cont}_x(f), g \longleftarrow \frac{f}{c_x c_y}$

2. compute the irreducible factorization of c_x, c_y in $F[y]$ and $F[x]$ and add them to G

3. $g_x = \partial g/\partial x, u \longleftarrow \frac{g}{\gcd(g, g_x)}$
   $g_y = \partial g/\partial y, v \longleftarrow \frac{g}{\gcd(g, g_y)}$, $w \longleftarrow \frac{u}{\gcd(u, v)}$

4. compute the set $V \subseteq \mathbb{F}[x, y]$ of all irreducible factors of v and the set $W \subseteq \mathbb{F}[x, y]$ of all irreducible factors of w

5. for all $v \in V \cup W$ do
   determine the multiplicity e of v in g by trial division
   $G \longleftarrow \{(v, e)\}$, $g \longleftarrow \frac{g}{v^e}$

6. if F is finite of characteristic p and $g \notin \mathbb{F}$ then
   call the algorithm recursively with input $g^{1/p}$ yielding a, H
   $a \longleftarrow a^p$
   for each pair $(g, e) \in H$ do $G \longleftarrow G \cup \{(g, ep)\}$
   else $a \longleftarrow g$

7. return a and G.