

Hensel lifting

(Due date: May 28th)

1. Here are the irreducible factorizations of the monic polynomial $f \in \mathbb{Z}[x]$ of degree 8 modulo some small primes

$$\begin{aligned} f &= (x+1)^2(x^2+x+1)(x^4+x^3+x^2+x+1) \in \mathbb{F}_2[x] \\ f &= (x+3)(x^3+3)(x^4+4x^3+2x^2+x+4) \in \mathbb{F}_7[x] \\ f &= (x+9)(x^2+2x+4)(x^5+5) \in \mathbb{F}_{11}[x]. \end{aligned}$$

What can you say about the degrees of the irreducible factors of f in $\mathbb{Z}[x]$?

2. Let \mathbb{F}_q be a finite field with q elements, for an odd prime power q . Let x, y be indeterminates over \mathbb{F}_q , and

$$f = (x + \sqrt{y} + \sqrt{y+1})(x + \sqrt{y} - \sqrt{y+1})(x - \sqrt{y} + \sqrt{y+1})(x - \sqrt{y} - \sqrt{y+1}).$$

Show that $f \in \mathbb{F}_q[x, y]$ and that f is irreducible, but that $f(x, u) \in \mathbb{F}_q[x]$ splits into at least two factors for all $u \in \mathbb{F}_q$.

3. Let $f = x^3 - 292x^2 - 2170221x + 6656000 \in \mathbb{Z}[x]$. Find 13-adic linear factors $x - a_i$ with $f \bmod x - a_i \equiv 0 \bmod 13^{2^i}$ for $i = 0, 1, 2$, starting with $a_0 = 0$.
4. Suppose that the monic polynomial $f \in \mathbb{Z}[x]$ has degree 8, and p is prime so that $f \bmod p = g_1 g_2 g_3$ factors into three irreducible and pairwise coprime polynomials $g_1, g_2, g_3 \in \mathbb{F}_p[x]$, with $\deg(g_1) = 1$, $\deg(g_2) = 2$, $\deg(g_3) = 5$.
- What can you say about the possible factorizations of f modulo p^{100} ?
 - What can you say about the possible factorizations of f in $\mathbb{Q}[x]$?
 - Suppose q is another prime for which $f \bmod q = h_1 h_2$ with $h_1, h_2 \in \mathbb{F}_q[x]$ irreducible and $\deg(h_1) = \deg(h_2) = 4$. What can you say about the possible factorizations of f in $\mathbb{Q}[x]$ using all this information?

5. Let $f = x^{15} - 1 \in \mathbb{Z}[x]$. Take a nontrivial factorization $f \equiv gh \bmod 2$ with $g, h \in \mathbb{Z}[x]$ monic and of degree at least 2. Compute $g^*, h^* \in \mathbb{Z}[x]$ such that

$$f \equiv g^* h^* \bmod 16, \quad \deg(g^*) = \deg(g), \quad g^* \equiv g \bmod 2.$$

Show your intermediate results. Can you guess some factors of f in $\mathbb{Z}[x]$?

6. Let $f = 14x^4 + 15x^3 + 42x^2 + 3x + 1 \in \mathbb{Z}[x]$.
- Find a suitable prime $p \in \mathbb{N}$ such that $f \bmod p$ is squarefree and has degree 4.

- (b) Compute the irreducible factorization of $f \bmod p$ in $\mathbb{F}_p[x]$. Choose two factors $g, h \in \mathbb{Z}[x]$ that are coprime modulo p such that h is monic and irreducible modulo p , and $f \equiv gh \bmod p$. Determine $s, t \in \mathbb{Z}[x]$ with $sg + th \equiv 1 \bmod p$.
- (c) Execute two successive Hensel steps to obtain a factorization $f \equiv g^* h^* \bmod p^4$ with $g \equiv g^*$ and $h \equiv h^*$ modulo p . Can you derive a factorization of f in $\mathbb{Q}[x]$ from it?
7. Let $N = pq$ be the product of two distinct primes p, q .
- (a) Show that $u = p^2 + q^2$ is a unit in \mathbb{Z}_N^\times .
- (b) Verify the factorization $x \equiv u^{-1}(px + q)(qx + p) \bmod N$.
- (c) Prove that the two linear factors in (b) are irreducible in $\mathbb{Z}_N[x]$.
8. Let $N = p_1 \dots p_s$ be a product of s distinct primes, and $f \in \mathbb{Z}_N[x]$ be monic and squarefree.
- (a) Let $g_1 \in \mathbb{Z}_{p_1}[x]$ be irreducible and $g \in \mathbb{Z}_N[x]$ with $g \equiv g_1 \bmod p_1$ and $g \equiv 1 \bmod p_i$ for $i \geq 2$. Prove that g is irreducible in $\mathbb{Z}_N[x]$.
- (b) Assume that we have factored f modulo each p_i . Determine the factorization of f into irreducible polynomials in $\mathbb{Z}_N[x]$. How many irreducible factors are there, in terms of the numbers of irreducible factors modulo each p_i ?
- (c) How many irreducible factors does $x^3 - x$ have modulo 105? Find four or them.
9. Let R be a commutative ring, and $f, g \in R[x]$, with g nonzero and monic.
- (a) Show that exist unique polynomials $q, r \in R[x]$ with $f = qg + r$ and either $r = 0$ or $\deg r < \deg g$.
- (b) If $f \equiv 0 \pmod{m}$ for some $m \in R$, then show that $q \equiv r \equiv 0 \pmod{m}$.
10. Let $f = 6x^5 + 23x^4 + 51x^3 + 65x^2 + 65x + 42 \in \mathbb{Z}[x]$ and $p = 11$.
- (a) Compute the irreducible factorization of f modulo p .
- (b) Use the Multifactor Hensel Lifting Algorithm to lift the factorization above to a factorization of f modulo p^4 .
- (c) Try to find nontrivial factors of f in $\mathbb{Z}[x]$ via factor combination.
11. Let R be a ring, $1 \leq k < r$, $f_1, \dots, f_r \in R[x]$ monic, nonconstant, and pairwise Bézout-coprime, b a unit in R^\times , $g = bf_1 \dots f_k$, and $h = f_{k+1} \dots f_r$. Show that g and h are Bézout-coprime. Moreover, prove that there exist polynomials $s, t \in R[x]$ such that $sg + th = 1$ with $\deg(s) < \deg(h)$ and $\deg(t) < \deg(g)$.

12. The aim of this exercise is to shave off the factor $\log r$ in the complexity analysis of the Multifactor Hensel Lifting Algorithm when using classical arithmetic. In addition to the input specifications of this algorithm, we assume that the f_i are sorted by degree, so that $n_1 = \deg(f_1) \leq n_2 = \deg(f_2) \leq \dots \leq n_r = \deg(f_r)$. Let $\ell_i = \lfloor \log n_i \rfloor$ for all i and $e = e(n_1, \dots, n_r) = \lceil \log \sum_{i=1}^r 2^{\ell_i} \rceil$.
- (a) Assume $r \geq 2$ and let $1 \leq k < r$ be maximal such that $\sum_{k < i \leq r} 2^{\ell_i} < 2^{e-1}$. Prove that such a k exists, that actually equality holds, and conclude that $e(n_1, \dots, n_k) \leq e - 1$ and $e(n_{k+1}, \dots, n_r) \leq e - 1$.
- (b) We replace the definition of k in step 2 of the Multifactor Hensel Lifting Algorithm by the definition as in (a) and denote by $T(n_1, \dots, n_r)$ the cost of the algorithm with classical arithmetic. Prove that there is a positive constant c such that

$$T(n) \leq c 2^3 \ell^2 \mu^2, \quad T(n_1, \dots, n_r) \leq T(n_1, \dots, n_k) + T(n_{k+1}, \dots, n_r) + c 2^{2e} + \ell^2 \mu^2,$$

with both μ being the constant and ℓ the exponent appearing in the complexity analysis of the algorithm, $n = n_1 + \dots, n_r$, and $e = e(n_1, \dots, n_r)$. Conclude that $T(n_1, \dots, n_r) \leq \frac{4}{3} c 2^{2e} \ell^2 \mu^2 \in \mathcal{O}(n^2 \ell^2 \mu^2)$.