FACTORING MODULAR POLYNOMIALS

JOACHIM VON ZUR GATHEN AND SILKE HARTLIEB
Fachbereich 17 Mathematik-Informatik, Universität-GH Paderborn
D-33095 Paderborn, Germany
{gathen,hartlieb}@uni-paderborn.de
May 13, 1996

Abstract. This paper gives an algorithm to factor a polynomial f (in one variable) over residue class rings of $\mathbb{Z}$ or $\mathbb{F}_q[y]$. The Chinese Remainder Theorem reduces our problem to the case where r is a prime power. Then factorization is not unique, but if r does not divide the discriminant of f, our (probabilistic) algorithm produces a description of all (possibly exponentially many) factorizations into irreducible factors in polynomial time. If r divides the discriminant, we only know how to factor by exhaustive search, in exponential time.

1. Introduction

Let $R = \mathbb{Z}$ or $R = \mathbb{F}_q[y]$ with a finite field $\mathbb{F}_q$ having q elements, and let $r \in R$. We consider polynomials in $R[x]$, and we aim to describe all possible factorizations into irreducibles over the ring $R/(r)$, where (r) denotes the ideal generated by r. Over such rings, factorization of polynomials into irreducible factors is not unique.

EXAMPLE 1.1. *Let $R = \mathbb{Z}$ and $r = 8$. Then*

$$x^2 + 7 \equiv (x+1)(x+7) \equiv (x+3)(x+5) \bmod 8,$$

and in fact all four linear factors are irreducible.

It is shown that the number of irreducible factors of a polynomial can be exponential in the length of the polynomial, defined in the natural way. A special case of our problem is to find square roots in $R/(r)$. A solution has been known for a long time; a good overview is given in Vahle (1993).

In Sections 2 and 3, the factorization problem is reduced with the Chinese Remainder Theorem and Hensel's Lemma to the case where $r \in R$ is a prime power and the polynomial is a power of an irreducible polynomial modulo the prime. In Section 4, the algorithm for the factorization problem if $r = p^k$ is a prime power is stated. It only works when the discriminant of the polynomial is not divisible by p^k. In particular, the polynomial is squarefree. There may exist exponentially many irreducible factors, but we provide in polynomial time a concise data structure that describes all of them in a transparent way. In the last section a generalization of Hensel's Lemma is given. It can speed up the algorithm of Section 4 in many cases, but it does not yield a smaller asymptotic running time of the algorithm.

Our goal is an algorithm that describes all factorizations into irreducible factors. Sometimes it may suffice to deal with a (possibly) simpler problem: finding one factorization into irreducible factors. This task is completely solved in the case that p^k does not divide the discriminant by Chistov's (1987, 1994) algorithm for factoring polynomials over the p-adic completion $R_{(p)}$. In the case that the discriminant vanishes, i.e., the polynomial is not squarefree, this may be reduced to the case where the discriminant is nonzero. But in the case where the discriminant is nonzero and p^k divides the discriminant, we even do not know how to solve this easier problem in polynomial time.

We need two properties of the ring R both satisfied by the two examples stated at the beginning. The first one is that polynomials over $R/(p)$ can be factored efficiently, i.e., there are polynomial time (probabilistic) algorithms for factoring polynomials over finite fields (Berlekamp 1970). The second one is that the completion of the field of fractions K of R with respect to the p-adic valuation on K is a local field in the sense of Chistov (1987, 1994). Hence we can use his fast algorithm for factoring polynomials over local fields. Our methods work for any R that satisfies these assumptions.

We also analyze the running time of our algorithm. This is presented for $R = \mathbb{Z}$ and for $R = \mathbb{F}_q[y]$ with $p = y$. In the former case, our algorithm produces on input $f \in \mathbb{Z}[x]$ of degree n and $k \in \mathbb{N}$ such that the discriminant is nonzero and not divisible by p^k all factorizations of f over $\mathbb{Z}/p^k$ in at most $\mathsf{C}_{\mathbb{Z}}(p,n,k) + O(n^7 k \log p (k \log p + \log n)^2)$ bit operations. Here $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ denotes the time such that the complete factorization over $\mathbb{Z}_{(p)}$ of a polynomial $f \in \mathbb{Z}[x]$ with $\deg f = n$ can be computed modulo p^k with $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ bit operations; Chistov's algorithm does this in polynomial time. In the latter case the factorizations of a polynomial $f \in \mathbb{F}_q[y][x]$ with $\deg_x f = n$ into irreducible factors over $\mathbb{F}_q[y]/(y^k)$ can be computed with $\mathsf{C}_q(y,n,k) + O(n^4 k^2 \mathsf{M}(\log nk) \log^2 nk + k^2 n^{\omega+2} \mathsf{M}(\log nk) + nSNF(n,k))$ operation in $\mathbb{F}_q$.

Here $\mathsf{C}_q(y,n,k)$ denotes the time such that the complete factorization over $\mathbb{F}_q[[y]]$ of a polynomial $f \in \mathbb{F}_q[y][x]$ with $\deg_x f = n$ can be computed modulo y^k with $\mathsf{C}_q(y,n,k)$ operations in $\mathbb{F}_q$. Chistov's algorithm yields again that $C_q(y,n,k)$ can be chosen polynomial. The estimate $SNF(n,k)$ describes the number of operations such that the Smith normal form of an $n \times n$-matrix over $\mathbb{F}_q[y]$ together with the transition matrices can be computed modulo y^k with $O(SNF(n,k))$ operations. By Kaltofen *et al.* (1990) this can be done in polynomial time. We have made no attempt to minimize these cost estimates.

2. The Chinese Remainder Theorem

Let $r \in R$ be a nonunit, and

$$r = u \prod_{1 \leq i \leq s} p_i^{k_i} \tag{2.1}$$

be a complete factorization of r, i.e., u is a unit in R, the elements $p_1, \ldots, p_s \in R$ are primes and pairwise relatively prime, and each integer k_i is at least 1. Then the Chinese Remainder Theorem provides an isomorphism

$$\begin{array}{rcl} R/(r)[x] & \simeq & R/(p_1^{k_1})[x] \times \ldots \times R/(p_s^{k_s})[x] \\ f \bmod r & \mapsto & (f \bmod p_1^{k_1}, \ldots, f \bmod p_s^{k_s}). \end{array}$$

Hence the irreducible factors of $f \in R[x]$ over $R/(r)$ are, up to multiplication by units, of the form

$$g = (1, \ldots, 1, g_i, 1, \ldots, 1), \tag{2.2}$$

where $1 \leq i \leq s$, all entries but the ith are 1, and $g_i \in R[x]$ is an irreducible factor of f over $R/(p_i^{k_i})$. Shamir (1993) made an interesting proposal for using families of multivariate modular polynomials in cryptography. He gave a wonderful example of how already the most innocuous of all polynomials has a surprising factorization.

EXAMPLE 2.1. *(Shamir) Let $r = pq$ for different primes $p, q \in \mathbb{Z}$. Then $p^2 + q^2$ is a unit in $\mathbb{Z}/(r)$, $px + q$ and $qx + p$ are irreducible over $\mathbb{Z}/(r)$, and*

$$x \equiv (p^2 + q^2)^{-1}(px + q)(qx + p) \bmod r.$$

In particular, nontrivial irreducible factors of f can have the same degree as f.

$\mathsf{M}(n)$ denotes a "multiplication time", so that integers of bit length at most n can be multiplied with $O(\mathsf{M}(n))$ bit operations and polnynomials of degree at most n in $\mathbb{F}_q[y]$ can be multiplied with $O(\mathsf{M}(n))$ operations in $\mathbb{F}_q$. By Schönhage & Strassen (1971) and Schönhage (1977), we may assume that

$$\mathsf{M}(n) = n \log n \operatorname{loglog} n.$$

REMARK 2.2. *Consider the case $R = \mathbb{Z}$. Assume that the complete factorization of r is $r = u \prod_{1 \le i \le s} p_i^{k_i}$ as in (2.1), and $k_i \log p_i < N$ for $1 \le i \le s$. Let $c_i \in R$ with $c_i < p_i^{k_i}$ for $1 \le i \le s$. It is well-known that one can compute an element $c \in R$ with $c \equiv c_i \bmod p^{k_i}$ for $1 \le i \le s$ with $O(\mathsf{M}(sN) \log s + s\mathsf{M}(N) \log N)$ bit operations (see Aho* et al. *1974, 8.11). Hence, let $f_i \in R[x]$ be such that the absolute value of each coefficient of f_i is less than $p_i^{k_i}$ and $\deg f_i \le n$ for $1 \le i \le s$. Then one can compute a polynomial $f \in R[x]$ such that $\deg f \le n$ and $f \equiv f_i \bmod p_i^{k_i}$ for $1 \le i \le s$ with $O(n\mathsf{M}(sN) \log s + ns\mathsf{M}(N) \log N)$ bit operations.*

For $R = \mathbb{F}_q[y]$ and $r = u \prod_{1 \le i \le s} p_i^{k_i}$ with $\deg_y r = N$ let $f_i \in R[x]$ such that the degree of each coefficient of f_i in y is less than $\deg p_i^{k_i}$ for $1 \le i \le s$. Then one can compute a polynomial $f \in R[x]$ such that $f \equiv f_i \bmod p_i^{k_i}$ for $1 \le i \le s$ with $O(n\mathsf{M}(N) \log N)$ operations in $\mathbb{F}_q$ (Aho et al. *1974).*

Assume that we are able to factor $f \in R[x]$ into irreducible factors over $R/(p^k)$ for any given prime p and $k \ge 1$. The Chinese Remainder Theorem shows that if we know the factorization of $r \in R$, then we are able to factor f over $R/(r)$ into irreducible factors. In the case where $R = \mathbb{F}_q[y]$, good algorithms for the factorization of polynomials over finite fields are known. The best (probabilistic) algorithms need $O((n^2 + n \log q)(\log n)^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$ (von zur Gathen & Shoup 1992) or $O(n^{1.815} \log q)$ operations in $\mathbb{F}_q$ (Kaltofen & Shoup 1995) for factoring a polynomial of degree n. Hence we obtain the following:

LEMMA 2.3. *Let $R = \mathbb{F}_q[y]$. There is a (probabilistic) polynomial time reduction from the problem of factoring polynomials over $R/(r)$ for some $r \in R$ to the problem of factoring polynomials over $R/(p^k)$ for a prime $p \in R$.*

According to current knowledge, factoring integers seems harder than factoring polynomials over finite fields; see Bach (1990) and Lenstra & Lenstra, Jr (1990, 1993) for fast integer factoring algorithms.

The following proposition is from Shamir (1993). We state it only for the case that $R = \mathbb{Z}$.

PROPOSITION 2.4. *(Shamir) There is a polynomial-time reduction from the problem of factoring $r \in \mathbb{Z}$ to the problem of factoring polynomials over $\mathbb{Z}/r\mathbb{Z}$.*

PROOF. For given $r \in \mathbb{Z}$, take the polynomial $x \in \mathbb{Z}[x]$ and factor it into irreducible factors over $\mathbb{Z}/r\mathbb{Z}$. By Corollary 3.9 below the polynomial x is irreducible over $\mathbb{Z}/p^k\mathbb{Z}$ for all primes p and all $k \geq 1$. If the complete factorization of r is $r = (-1)^k p_1^{k_1} \dots p_s^{k_s}$ as in (2.1), then the irreducible factors of x over $\mathbb{Z}/r\mathbb{Z}$ are up to multiplication by units the $f_i = (1, \dots, 1, x, 1, \dots, 1)$, where x is in the ith component. Thus f_i has degree at most 1 over $\mathbb{Z}/r\mathbb{Z}$. If we write $f_i \equiv a_i x + b_i \bmod r$ with $a_i, b_i \in \mathbb{Z}$ then

$$b_i \equiv \begin{cases} 0 \bmod p_i^{k_i}, \\ 1 \bmod p_j^{k_j} \text{ for } i \neq j. \end{cases}$$

Thus $\gcd(r, b_i) = p_i^{k_i}$ for $1 \leq i \leq s$. Now for given $m_i = p_i^{k_i}$ it is easy to find p_i and k_i in polynomial time just by trying all possible exponents. □

Finally, we state a corollary of the Chinese Remainder Theorem which follows directly from (2.2):

COROLLARY 2.5. *Let the complete factorization of $r \in R$ be $r = u \prod_{1 \leq i \leq s} p_i^{k_i}$ as in (2.1). Then the number of irreducible factors of $f \in R[x]$ over $R/(r)$ is the sum over all $1 \leq i \leq s$ of the numbers of irreducible factors of f over $R/(p_i^{k_i})$.*

3. Hensel's Lemma

From now on, we assume that $r = p^k$ for some prime $p \in R$ and $k \geq 1$. The Sylvester matrix $S(g, h)$ of two polynomials $g, h \in R[x]$ with degrees n and m, and $g = \sum_{0 \leq i \leq n} g_i x^i$ and $h = \sum_{0 \leq j \leq m} h_j x^j$ is the following matrix:

$$S(g,h) = \left(\begin{array}{cccc|cccc} \underbrace{\begin{matrix} g_n & & \\ g_{n-1} & \ddots & \\ \vdots & \ddots & \\ g_0 & & g_n \\ & \ddots & g_{n-1} \\ & \ddots & \vdots \\ & & g_0 \end{matrix}}_{m} & \underbrace{\begin{matrix} h_m & & \\ h_{m-1} & \ddots & \\ \vdots & & h_m \\ \vdots & & h_{m-1} \\ h_0 & & \vdots \\ & \ddots & \vdots \\ & & h_0 \end{matrix}}_{n} \end{array} \right) \in R^{(n+m)\times(n+m)}.$$

(Sometimes the transposed of this matrix is called the Sylvester matrix.) By definition, the resultant of the two polynomials is $\mathrm{res}(g,h) = \det S(g,h)$.

Since R is a UFD, there is a p-adic (non-archimedean) valuation on the field of fractions K of R. For $a \in R$ it is defined as follows:

$$v_p(a) = \begin{cases} \nu & \text{if } a \neq 0 \text{ and } p^\nu || a, \\ \infty & \text{if } a = 0. \end{cases}$$

Here, $p^\nu || a$ means that p^ν is the exact power of p which divides a, i.e., $p^\nu | a$ and $p^{\nu+1} \nmid a$. This valuation extends to K in the natural way, via $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ for $a, b \in R$, $b \neq 0$. The p-adic valuation induces an absolute value on K by $|a|_p = p^{-v_p(a)}$, $|0|_p = 0$. By $K_{(p)}$ we denote the completion of K with respect to the absolute value $|.|_p$. In the case $R = \mathbb{Z}$ this procedure yields the well-known p-adic numbers $\mathbb{Q}_{(p)}$. If $R = \mathbb{F}_q[y]$ and $p = y$, then $K_{(p)} = \mathbb{F}_q((y))$. The ring R is contained in the ring $R_{(p)}$ of valuation integers of $K_{(p)}$ which are defined by the property that $v_p(a) \geq 0$. Any element a of $R_{(p)}$ can be written uniquely in the form

$$a = \sum_{i \geq 0} a_i p^i,$$

where $a_i \in R$ is an element of a fixed set of representatives in R of the finite field $R_{(p)}/(p)$ (e.g., $a_i \in \{0, 1, \ldots, p-1\}$ in the case where $R = \mathbb{Z}$). The ring $R_{(p)}$ is a local ring with precisely one prime, namely p, and hence a UFD. We define the p-adic value of a matrix $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in K^{n \times m}$ as:

$$v_p(A) = \min\{v_p(a_{ij}) : 1 \leq i \leq n, 1 \leq j \leq m\}.$$

For more information about valuation theory, see e.g. Cohn (1977), Chapter 9.

In the cost analysis of our algorithms, we use a matrix multiplication exponent $\omega \in \mathbb{R}$, such that multiplication of $n \times n$ matrices over a field F can be done with $O(n^\omega)$ operations in F. The ordinary school method yields $\omega = 3$, whereas the best known value is $\omega < 2.376$ (Coppersmith & Winograd 1990). Inversion of an (invertible) $n \times n$ matrix over F, computation of the determinant and solution of a system of linear equations can also be done with $O(n^\omega)$ operations in F. For further details see Bini & Pan (1994), 2.2.

LEMMA 3.1. *Let $R = \mathbb{F}_q[y]$, and assume that $g, h \in R[x]$ with $\deg_x g + \deg_x h = d$ and $\deg_y g, \deg_y h \leq N$.*

(a) *The resultant $\mathrm{res}_x(g,h) \in R$ can be computed with*

$$O(d^3 N \mathsf{M}(\log dN) \log^2 dN)$$

operations in $\mathbb{F}_q$.

(b) *If* $res(g,h) \neq 0$, *and* $l \in \mathbb{F}_q[y]^d$ *with* $\deg_y l_i \leq L$ *for* $1 \leq i \leq d$ *and* $L \geq N$, *then the system of linear equations* $S(g,h)a = l$ *can be solved with*

$$O(d^2 L\mathsf{M}(\log L)\log^2 L + Ld^\omega \mathsf{M}(\log L))$$

operations in $\mathbb{F}_q$.

PROOF.

(a) Since $\text{res}(g,h)$ is a polynomial of degree at most d in the coefficients of g and h, the degree of $\text{res}(g,h)$ is at most dN. Hence we evaluate $S(g,h)$ at $dN+1$ points. If $q < dN+1$ we have to extend the field $\mathbb{F}_q$. This yields an additional factor of $\mathsf{M}(\log dN)$ in our asymptotic running time. The evaluation can be done with $O(d^3 N\mathsf{M}(\log dN)\log^2 dN)$ operations by Aho *et al.* (1974), 8.5. Then for all the evaluated matrices the resultant can be computed with $O(d^2 N\mathsf{M}(\log dN)\log^2 d)$ operations (Bini & Pan 1994, 2.8). The asymptotic cost for the interpolation is the same as for the evaluation (Aho *et al.* 1974, 8.7), and hence we have a total cost of at most $O(d^3 N\mathsf{M}(\log dN)\log^2 dN)$ operations.

(b) We evaluate $S(g,h)$ and l at $L+1$ points. If $q < L+1$, we pass over to a field extension of an appropriate degree. Then the evaluation can be done with $O(d^2 L\mathsf{M}(\log L)\log^2 L)$ operations in $\mathbb{F}_q$. Then we solve the systems of linear equations with $O(Ld^\omega \mathsf{M}(\log L))$ operations, and interpolate within the same asymptotic running time as we have for the evaluation. Hence we obtain a bound of $O(d^2 L\mathsf{M}(\log L)\log^2 L + L\mathsf{M}(\log L)d^\omega)$ operations.

The following proposition and theorem are known (Borevich & Shafarevich (1966), Chapter 4, §3), but since we need some details later, we also give the proofs.

PROPOSITION 3.2. *Let* $g, h \in R[x]$ *of degrees* n, m, *respectively, such that* $res(g,h) \neq 0$. *Let* $l \in R[x]$ *with* $\deg l < n+m$. *Then there exist uniquely determined polynomials* $\varphi, \psi \in R[x]$ *with* $\deg\varphi < m$ *and* $\deg\psi < n$ *such that*

$$res(g,h)l = \varphi g + \psi h. \tag{3.1}$$

If $R = \mathbb{Z}$, *and the bit length of the coefficients of* g *and* h *is bounded by* N, *then* $O((n+m)^6(N+\log(n+m))^2)$ *operations suffice to compute* φ *and* ψ, *given* g, h, l. *If* $R = \mathbb{F}_q[y]$, *and* $\deg_y g, \deg_y h, \deg_y l \leq N$, *then* φ *and* ψ *can be computed with* $O((n+m)^3 N\mathsf{M}(\log(n+m)N)\log^2(n+m)N + N(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ *operations in* $\mathbb{F}_q$.

PROOF. Write $l = \sum_{i=0}^{n+m-1} l_i x^i$ with all $l_i \in R$. There exist polynomials φ and ψ satisfying (3.1) if and only if there exist elements $\varphi_0, \ldots, \varphi_{m-1}$ and $\psi_0, \ldots, \psi_{n-1}$ in R (namely, the coefficients of the two polynomials) such that

$$S(g,h)\begin{pmatrix} \varphi_{m-1} \\ \vdots \\ \varphi_0 \\ \psi_{n-1} \\ \vdots \\ \psi_0 \end{pmatrix} = \operatorname{res}(g,h)\begin{pmatrix} l_{n+m-1} \\ \vdots \\ l_0 \end{pmatrix}. \tag{3.2}$$

Since $\operatorname{res}(g,h) \neq 0$, the matrix $S(g,h)$ is invertible, and (3.2) is equivalent to

$$\begin{pmatrix} \varphi_{m-1} \\ \vdots \\ \varphi_0 \\ \psi_{n-1} \\ \vdots \\ \psi_0 \end{pmatrix} = \operatorname{res}(g,h)S(g,h)^{-1}\begin{pmatrix} l_{n+m-1} \\ \vdots \\ l_0 \end{pmatrix}.$$

The entries of $\operatorname{res}(g,h)S(g,h)^{-1}$ are in R, and thus also all φ_i and ψ_i. Then $\varphi = \sum_{i=0}^{m-1} \varphi_i x^i$ and $\psi = \sum_{i=0}^{n-1} \psi_i x^i$ form the unique solution of (3.1).

Now let $R = \mathbb{Z}$. The resultant $\operatorname{res}(g,h)$ can be computed with

$$O((n+m)^3 N + (n+m)^2 N^2)$$

bit operations by Collins (1971). Moreover, it follows from Hadamard's inequality that the bit length of $\operatorname{res}(g,h)$ is at most $\frac{(n+m)}{2}\log(n+m) + (n+m)N + 1$. Hence, the multiplication of $\operatorname{res}(g,h)$ with the vector of coefficients of l can be done with $O((n+m)\mathsf{M}((n+m)(\log(n+m)+N)))$ operations. Now the system of linear equations (3.2) has to be solved. It follows from Chou & Collins (1982) that the solution can be found with $O((n+m)^6(N+\log(n+m))^2)$ operations. Hence we have a total cost of $O((n+m)^6(N+\log(n+m))^2)$ operations. If $R = \mathbb{F}_q[y]$, then it follows from Lemma 3.1(a) that $\operatorname{res}(g,h)$ and hence r can be computed in $O((n+m)^3 N \mathsf{M}(\log(n+m)N)\log^2(n+m)N)$ operations in $\mathbb{F}_q$. Moreover, $\deg_y \operatorname{res}(g,h) \leq (n+m)N$. Hence, the multiplication of $\operatorname{res}(g,h)$ with the vector of the coefficients of l can be done with $O((n+m)\mathsf{M}((n+m)N))$ operations in $\mathbb{F}_q$ and yields a vector with coordinates of degree at most $(n+m+1)N$. By Lemma 3.1(b) the system of linear equations (3.2) can be solved with

$O((n+m)^3 N \mathsf{M}(\log(n+m)N)\log^2(n+m)N + N(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ operations in $\mathbb{F}_q$. Thus this is also the total asymptotic cost. □

Of course, the polynomials φ and ψ of Proposition 3.2 can also be computed via the Extended Euclidean Algorithm. This reduces the running time, but we did not find exact estimates for the running time of the Extended Euclidean Algorithm over $\mathbb{Z}[x]$ and $\mathbb{F}_q[y,x]$ in the literature. Since we assume that the running time of the final algorithm is dominated by the values $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ and $\mathsf{C}_q(y,n,k)$, respectively, we content ourselves with the computed asymptotic running times.

Often, it suffices to compute polynomials $\varphi, \psi \in R[x]$ with $\deg\varphi < m$ and $\deg\psi < n$ such that $p^r l \equiv \varphi g + \psi h \bmod p^{r+1}$, where $r = v_p(\mathrm{res}(g,h))$. As in the proof of Proposition 3.2, the solutions correspond to the solutions of the congruence

$$S(g,h)\begin{pmatrix}\varphi_{m-1}\\ \vdots \\ \varphi_0 \\ \psi_{n-1} \\ \vdots \\ \psi_0\end{pmatrix} \equiv p^r \begin{pmatrix} l_{n+m-1} \\ \vdots \\ l_0\end{pmatrix} \bmod p^{r+1}.$$

Corollary 3.3. *Let $g,h,l,r \in R[x]$ be as in Proposition 3.2. In order to compute $\varphi, \psi \in R[x]$ such that $\deg\varphi < m, \deg\psi < n$ and $p^r l \equiv \varphi g + \psi h \bmod p^{r+1}$, it suffices to determine $S(g,h) \bmod p^{r+1}$.*

Notation 3.4. *Let $g,h \in R[x]$. Then $r(g,h) = v_p(res(g,h))$, and $d(g) = v_p(disc(g))$, where $disc(g)$ is the discriminant of g.*

Theorem 3.5. *(Hensel's Lemma) Let $p \in R$ be a prime, $k \in \mathbb{N}$ and $f,u,w \in R[x]$ be polynomials of degrees $n+m, n, m$, respectively, with the following properties:*

(a) $f \equiv uw \bmod p^k$, and the leading coefficients of f and uw are equal,

(b) the resultant $res(u,w)$ is nonzero,

(c) $k > 2r(u,w)$.

Then there are polynomials $g,h \in R_{(p)}[x]$ such that

$$f = gh \text{ in } R_{(p)}[x], g \equiv u \bmod p^{k-r(u,w)}, h \equiv w \bmod p^{k-r(u,w)},$$

and the leading coefficient of g and h equals the leading coefficient of u and w, respectively. For $N > k$ the polynomials $g \bmod p^N$ and $h \bmod p^N$ can be computed with $O((n+m)^6 N(N\log p + \log(n+m))^2)$ operations, if $R = \mathbb{Z}$ and we assume that the absolute values of the coefficients of f, u, w are bounded by p^N, and with $O((n+m)^3 N^2 \mathsf{M}(\log(n+m)N)\log^2(n+m)N + N^2(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ operations, if $R = \mathbb{F}_q[y]$ and $p = y$.

PROOF. Let $\rho = r(u, w)$. We construct inductively polynomials $\varphi_i, \psi_i \in R[x]$ for $i \geq 1$ with $\deg \varphi_i < m$, $\deg \psi_i < n$ such that if

$$f \equiv ab \bmod p^{k+i-1}$$

with $a, b \in R[x]$ such that $a \equiv u \bmod p^{k-\rho}$ and $b \equiv w \bmod p^{k-\rho}$, and $\mathrm{lc}(a) = \mathrm{lc}(u)$, $\mathrm{lc}(b) = \mathrm{lc}(w)$, then

$$f \equiv (a + p^{k-\rho+i-1}\psi_i)(b + p^{k-\rho+i-1}\varphi_i) \bmod p^{k+i}.$$

Here lc denotes the leading coefficient. We start with the factorization $f \equiv uw \bmod p^k$ and now assume that $i \geq 1$ and $a, b \in R[x]$ are already constructed such that $f \equiv ab \bmod p^{k+i-1}$. Then

$$f = ab + p^{k+i-1} l,$$

with $l \in R[x]$ and $\deg l < n + m$, because $\mathrm{lc}(ab) = \mathrm{lc}(f)$. Since $a \equiv u \bmod p^{k-\rho}$, $b \equiv w \bmod p^{k-\rho}$, and $k - \rho > \rho$, we have $\rho = r(u, w) = r(a, b)$. By Proposition 3.2 there exist polynomials $\varphi_i, \psi_i \in R[x]$ of degrees less than m, n, respectively, such that

$$p^\rho l \equiv a\varphi_i + b\psi_i \bmod p^{\rho+1}.$$

Then

$$\begin{aligned} f - (a + p^{k-\rho+i-1}\psi_i)(b + p^{k-\rho+i-1}\varphi_i) & \\ = \ & f - ab - p^{k-\rho+i-1}(a\varphi_i + b\psi_i) - p^{2k-2\rho+2i-2}\varphi_i\psi_i \\ \equiv \ & p^{k+i-1} l - p^{k-\rho+i-1} p^\rho l - p^{2k-2\rho+2i-2}\varphi_i\psi_i \\ \equiv \ & 0 \bmod p^{k+i}, \end{aligned}$$

because $i \geq 1$ and $k > 2\rho$.

Together we have for the polynomials $g = u + \sum_{i\geq 1} p^{k-\rho+i-1}\psi_i \in R_{(p)}[x]$ and $h = w + \sum_{i\geq 1} p^{k-\rho+i-1}\varphi_i \in R_{(p)}[x]$ that $f = gh$. Furthermore, $g \equiv u \bmod p^{k-\rho}$ and $h \equiv w \bmod p^{k-\rho}$.

Now let $R = \mathbb{Z}$ and $N > k$. In order to compute $r(u,w)$, we have to compute $\mathrm{res}(u,w)$ and then divide it by powers of p to compute $r(u,w)$. The first computation can be done with $O((n+m)^3 N \log p + (n+m)^2 N^2 \log^2 p)$ operations (Collins 1971). Then we compute all powers p^i of p for $1 \le i \le \lfloor \frac{k}{2} \rfloor$. This can be done with $O(N\mathsf{M}(N \log p))$ operations. With a binary search one can compute the exact power of p which divides $\mathrm{res}(u,w)$ with

$$O(\log N \mathsf{M}((n+m)\log(n+m) + (n+m)N \log p))$$

operations, since the binary length of $\mathrm{res}(u,w)$ is at most $\frac{(n+m)}{2}\log(n+m) + N(n+m)\log p + 1$ by Hadamard's inequality. For the construction of g and h, we first compute the cost for one step of the inductive procedure. So let $f \equiv ab \bmod p^{k+i-1}$ with $1 \le i \le N-k$. The cost for the computation of $l = \frac{f-ab}{p^{k+i-1}}$ is essentially the cost for the multiplication of the polynomials a and b. The multiplication can be done with $O((n+m)^2 N^2 \log^2 p)$ operations by the ordinary school method. After the computation of l, Proposition 3.2 has to be applied once. Hence the cost for one step is $O((n+m)^6 (N \log p + \log(n+m))^2)$ operations. Since there are less than N such steps we obtain $O((n+m)^6 N(N \log p + \log(n+m))^2)$ operations.

If $R = \mathbb{F}_q[y]$ and $p = y$, we may assume that $\deg_y f, \deg_y u, \deg_y w < N$. By Lemma 3.1(a) the computation of $\mathrm{res}(g,h)$ can be done with $O((n+m)^3 N \mathsf{M}(\log(n+m)N)\log^2(n+m)N)$ operations. The multiplication of the two multivariate polynomials in a step of the inductive procedure can be done with $O(\mathsf{M}(nN))$ operations by Bini & Pan (1994), 1.8. Then Proposition 3.2 has to be applied. This yields $O((n+m)^3 N \mathsf{M}(\log(n+m)N)\log^2(n+m)N + N(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ operations. Hence one step can be done with $O((n+m)^3 N \mathsf{M}(\log(n+m)N)\log^2(n+m)N + N(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ operations. Since there are less than N steps, we obtain $O((n+m)^3 N^2 \mathsf{M}(\log(n+m)N)\log^2(n+m)N + N^2(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ operations in $\mathbb{F}_q$. $\square$

COROLLARY 3.6. *Assume that conditions (a) and (b) of Theorem 3.5 hold. Then condition (c) is true if $k > d(f)$.*

PROOF. Let $f = gh$ with $g, h \in R_{(p)}[x]$. Then

$$\mathrm{disc}(f) = \mathrm{disc}(gh) = \mathrm{disc}(g)\mathrm{disc}(f)\mathrm{res}(g,h)^2 \tag{3.3}$$

(c.f. Borevich & Shafarevich 1966, Chapter 4, §3). Hence

$$d(f) = d(g) + d(h) + 2r(g,h) \ge 2r(g,h).$$

Since the discriminant and the resultant are polynomials in the coefficients of f, g, h, the same is true for factorizations over $R/(p^k)$. □

REMARK 3.7. *It follows from Corollary 3.3 that in order to apply Theorem 3.5 it suffices to know* $S(u,w) \bmod p^{r(u,w)+1}$.

The following special case of Theorem 3.5 is also often called Hensel's Lemma.

THEOREM 3.8. *Let p be a prime, $k \geq 1$, $f, u_0, w_0 \in R[x]$ be such that* $f \equiv u_0 w_0 \not\equiv 0 \bmod p$ *and* $\gcd(u_0 \bmod p, w_0 \bmod p) = 1$ *in $R/(p)[x]$.*

(a) *There exist polynomials u_{k-1} and w_{k-1} in $R[x]$ such that*

$$f \equiv u_{k-1} w_{k-1} \bmod p^k,$$

$$u_{k-1} \equiv u_0 \bmod p, w_{k-1} \equiv w_0 \bmod p,$$

and $\deg u_{k-1} = \deg(u_0 \bmod p)$.

(b) *If f, u_0, w_0 are monic, then there are uniquely determined (over $R/(p^k)$) monic polynomials u_{k-1} and w_{k-1} which satisfy (a).*

COROLLARY 3.9. *Let $f \in R[x]$ be such that f is irreducible in $R/(p)[x]$. Then f is irreducible over $R/(p^k)$ for all $k \geq 1$. On the other hand, if f is irreducible over $R/(p^k)$ for some $k \geq 1$, then* $f \equiv g^e \bmod p^k$ *with $e \geq 1$ and $g \in R[x]$ irreducible over $R/(p)$.*

COROLLARY 3.10. *Let $f \in R[x]$ and $k \geq 1$. Then in order to find all irreducible factors of f over $R/(p^k)$, we may assume that f is monic.*

PROOF. We write $f = p^\nu g$ with $\gcd(p, g) = 1$ and $\nu \in \mathbb{N}$. Then $g \not\equiv 0 \bmod p$, and $g \equiv e_0 m_0 \bmod p$, where $e_0 \in R[x]$ is a unit over $R/(p)$ and $m_0 \in R[x]$ is monic. By Hensel's Lemma there exist $e, m \in R[x]$ such that $g \equiv em \bmod p^{k-\nu}$ where $e \equiv e_0 \bmod p$, $m \equiv m_0 \bmod p$, and $\deg m = \deg m_0$. This means that e is a unit over $R/(p^{k-\nu})$ and m is monic. The irreducible factors of f are the irreducible factors of m and p^ν. □

THEOREM 3.11. *Let $R = \mathbb{F}_q[y]$. There is a probabilistic polynomial-time reduction from the problem of factoring polynomials over $R/(r)$ for $r \in R$ to the problem of factoring monic polynomials over $R/(p^k)$ – for a prime $p \in R$ and $k \in \mathbb{N}$ – which are a power of an irreducible polynomial over $R/(p)$. If $R = \mathbb{Z}$, the same holds if we assume that a complete factorization of r is given.*

PROOF. Let $r \in \mathbb{F}_q[y]$ and $f \in \mathbb{F}_q[y][x]$. We can factor r in probabilistic polynomial time to apply the Chinese Remainder Theorem. Let $r = u\prod_{1\le i\le s} p_i^{k_i}$ be the complete factorization of r as in (2.1). Theorem 3.8 shows that f can be uniquely factored over $R/(p_i^{k_i})$ in polynomial time into factors which are relatively prime over $R/(p_i)$ for $1 \le i \le s$. Hence it remains to consider the case where $f \equiv g^e \bmod p_i$ with $e \ge 2$ and $g \in R[x]$ irreducible over $R/(p_i)$ for some $1 \le i \le s$. By Corollary 3.10, we may assume that f is monic. □

4. Factorization over $R/(p^k)$ for large k

It follows from Theorem 3.5 that if $f \equiv g_k h_k \bmod p^k$ for $k > d = v_p(\mathrm{disc}(f))$, then there exists a factorization $f = gh$ over $R_{(p)}$ such that $g_k \equiv g \bmod p^{k-r}$ and $h_k \equiv h \bmod p^{k-r}$, where $r = v_p(\mathrm{res}(g_k, h_k)) \le \frac{d}{2}$. Hence, any two factorizations of f over $R/(p^k)$ which give rise to the same factorization over $R_{(p)}$ are equal over $R/(p^{k-r})$. In particular, Theorem 3.5 shows that if $k > d(f)$, then every factorization of f into irreducible factors over $R/(p^k)$ is compatible with the unique factorization into irreducibles of f over $R_{(p)}$. The next lemma formalizes this statement, which is fundamental for our algorithm.

LEMMA 4.1. *Let $f = \prod_{1\le i\le l} g_i$ over $R_{(p)}$ with disc$(f) \neq 0$, $l \ge 1$, and $g_i \in R_{(p)}[x]$ monic and irreducible for $1 \le i \le l$. Let $f \equiv gh \bmod p^k$ with $g, h \in R[x]$ monic and $k > d(f)$. Then there exists a partition $\{1, \ldots, l\} = S \,\dot\cup\, S'$ such that $g \equiv \prod_{i\in S} g_i \bmod p^{k-\rho}$ and $h \equiv \prod_{j\in S'} g_j \bmod p^{k-\rho}$ with $\rho = r(\prod_{i\in S} g_i, \prod_{j\in S'} g_j)$. In particular, if g is irreducible over $R/(p^k)$, then there exists $1 \le i \le l$ such that $g \equiv g_i \bmod p^{k-r(g_i,\prod_{j\neq i} g_j)}$.*

PROOF. Since $k > d(f)$, we can lift the factorization $f \equiv gh \bmod p^k$ to a factorization $f = \tilde g \tilde h$ over $R_{(p)}$ such that $\tilde g \equiv g \bmod p^{k-r(g,h)}$ and $\tilde h \equiv h \bmod p^{k-r(g,h)}$ by Corollary 3.6 and Theorem 3.5. Since factorization over $R_{(p)}$ is unique, there exists a partition $\{1, \ldots, l\} = S \,\dot\cup\, S'$ such that $\tilde g = \prod_{i\in S} g_i$, and $\tilde h = \prod_{j\in S'} g_j$. Hence

$$
\begin{aligned}
g &\equiv \tilde g \equiv \prod_{i\in S} g_i \bmod p^{k-r(g,h)},\\
h &\equiv \tilde h \equiv \prod_{j\in S'} g_j \bmod p^{k-r(g,h)}.
\end{aligned}
$$

Since $k > d(f) \geq 2r(g,h)$, we have that

$$r(g,h) = r(\prod_{i \in S} g_i, \prod_{j \in S'} g_j). \quad \square$$

We show now how to compute all factorizations of a given polynomial $f \in R[x]$ with $\mathrm{disc}(f) \neq 0$ over $R/(p^k)$ for $k > d(f) = v_p(\mathrm{disc}(f))$. A first approach would be to compute one irreducible factor of f, divide by it, and factor the quotient recursively. This works, and provides an irreducible factorization of f. However, we have a more ambitious goal, namely, we want to find all factorizations of f into irreducibles. The following example shows that the number of different factorizations of a polynomial over $R/(p^k)$ can be exponentially large, but by keeping track of all previously found factorizations in a symbolic way, we achieve a description of all factorizations in polynomial time.

EXAMPLE 4.2. *Let $R = \mathbb{Z}$, $p \in \mathbb{Z}$ prime, $\rho \in \mathbb{Z}$, $\rho \geq 1$, and $f = x^2 - p^{2\rho} \in \mathbb{Z}[x]$. Then $f = (x+p^\rho)(x-p^\rho)$, and $res(x+p^\rho, x-p^\rho) = -2p^\rho$. Now let $k > 2\rho$, $0 \leq \varphi < p^\rho$, and $\psi = p^\rho - \varphi$, so that $\psi \equiv -\varphi \bmod p^\rho$. Then*

$$\begin{aligned}
(x+p^\rho+p^{k-\rho}\varphi)(x-p^\rho+p^{k-\rho}\psi) &\equiv (x+p^\rho+p^{k-\rho}\varphi)(x-p^\rho-p^{k-\rho}\varphi) \\
&\equiv x^2-(p^\rho+p^{k-\rho}\varphi)^2 \\
&\equiv x^2-p^{2\rho}-2p^k\varphi-p^{2k-2\rho}\varphi^2 \\
&\equiv f \bmod p^k,
\end{aligned}$$

and each of the factors in this factorization is irreducible by Corollary 3.9. Thus we have p^ρ essentially different irreducible factorizations.

We use Chistov's (1987, 1994) algorithm for factoring polynomials over local fields whose running time is polynomial in the length of the polynomial and the logarithm of the size of the residue class field $R/(p)$, if one uses a fast probabilistic factorization algorithm for factoring polynomials over finite fields. If one uses a deterministic factorization algorithm for factoring polynomials over finite fields, the algorithm is polynomial in the length of the polynomial and the size of the residue class field.

With Chistov's algorithm, one can compute one factorization of $f \in R[x]$ over $R/(p^k)$ for $k > d(f)$. Let $f = \prod_{1 \leq i \leq l} \tilde{g}_i$ over $R_{(p)}[x]$ with $\tilde{g}_i \in R_{(p)}[x]$ monic and irreducible for $1 \leq i \leq l$. Let $g_i \in R[x]$ with $g_i \equiv \tilde{g}_i \bmod p^k$ for $1 \leq i \leq l$. By Lemma 4.1, it remains to compute from the factorization $f \equiv$

$\prod_{1\le i\le l} g_i \bmod p^k$ all other factorizations of f into irreducible factors. We know for each irreducible factor u of f over $R/(p^k)$ that $u \equiv g_i \bmod p^{k-r(g_i,\prod_{j\ne i} g_j)}$ for some $1 \le i \le l$ from Lemma 4.1. Let $h = \prod_{j\ne i} g_j$. In order to determine all irreducible factors u of f such that $u \equiv g_i \bmod p^{k-r(g_i,h)}$ we have to determine all polynomials $\varphi, \psi \in R[x]$ such that $f \equiv (g_i + p^{k-r(g_i,h)}\varphi)(h + p^{k-r(g_i,h)}\psi) \bmod p^k$ by Theorem 3.5.

Let f, g, h be monic with $f \equiv gh \bmod p^k$, and $\deg g = m, \deg h = n$. Moreover, we may assume that $r(g,h) > 0$. Then

$$\begin{aligned} f &\equiv (g + p^{k-r(g,h)}\varphi)(h + p^{k-r(g,h)}\psi) \bmod p^k && (4.1)\\ &\Leftrightarrow p^{k-r(g,h)}(\varphi h + \psi g) - p^{2k-2r(g,h)}\varphi\psi \equiv 0 \bmod p^k \\ &\Leftrightarrow \varphi h + \psi g \equiv 0 \bmod p^{r(g,h)} \\ &\Leftrightarrow S(g,h)\begin{pmatrix} \psi_{n-1}\\ \vdots \\ \psi_0 \\ \varphi_{m-1} \\ \vdots \\ \varphi_0 \end{pmatrix} \equiv 0 \bmod p^{r(g,h)}, && (4.2) \end{aligned}$$

where $\varphi = \sum_{0\le i<m} \varphi_i x^i \in R[x]$, and $\psi = \sum_{0\le i<n} \psi_i x^i \in R[x]$. Hence, factorizations of the form (4.1) correspond to solutions of the system of linear equations (4.2). For $R = \mathbb{Z}$ and $R = \mathbb{F}_q[y]$ it has been shown in Iliopoulos (1989) and Kaltofen *et al.* (1990) that there exist polynomial-time algorithms to compute the Smith normal form of the matrix $S(g,h)$, i.e., unimodular matrices P, Q over R (i.e., whose determinant is a unit in R) such that

$$PS(g,h)Q = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & d_{n+m} \end{pmatrix} =: D,$$

where d_i divides d_{i+1} for $1 \le i < n+m$. Let $\omega_i = \min\{v_p(d_i), r(g,h)\}$ for $1 \le i \le n+m$. Then $0 \le \omega_i \le \omega_{i+1} \le r(g,h)$ for $1 \le i < n+m$. Since we assume that $r(g,h) > 0$, we know that $\omega_i > 0$ for at least one $i \in \mathbb{Z}$ with $1 \le i \le n+m$. Hence, let $1 \le s \le n+m$ be minimal such that $\omega_s > 0$, and let $t = n+m-s+1$. A basis over R of the set $\{a \in R^{n+m} : Da \equiv 0 \bmod p^{r(g,h)}\}$ is $a_1 = p^{r(g,h)-\omega_s} e_s, \ldots, a_t = p^{r(g,h)-\omega_{n+m}} e_{n+m}$, where e_i denotes the ith unit vector for $1 \le i \le n+m$. Let $\mu_i = r(g,h) - \omega_{i+s-1}$ and $a_i' = \frac{1}{p^{\mu_i}} a_i$ for $1 \le i \le t$, so that $v_p(a_i') = 0$. Furthermore, let $b_i = Qa_i'$ for $1 \leq i \leq t$. Now it is easy to see that $p^{\mu_1}b_1, \ldots, p^{\mu_t}b_t$ is a basis over R of the set $\{b \in R^{n+m} : S(g,h)b \equiv 0 \bmod p^{r(g,h)}\}$.

For $l \geq 1$ let $R_l \subseteq R$ be a set of representatives of the finite set $R/(p^l)$. Then the set of solutions of (4.2) can be written as

$$\left\{ \sum_{1 \leq i \leq t} p^{\mu_i}\alpha_i b_i : \alpha_i \in R_{r(g,h)-\mu_i} \text{ for } 1 \leq i \leq t \right\}.$$

Let $1 \leq i \leq t$ and $b_i = (\psi_{i,n-1}, \ldots, \psi_{i,0}, \varphi_{i,m-1}, \ldots, \varphi_{i,0})^t$. The set of all factorizations (4.1) equals the set of factorizations $f \equiv g^{(\alpha_1,\ldots,\alpha_t)}h^{(\alpha_1,\ldots,\alpha_t)} \bmod p^k$ with

$$\begin{aligned} g^{(\alpha_1,\ldots,\alpha_t)} &= g + p^{k-r(g,h)}\Big(\sum_{0\leq i<n}\sum_{1\leq j\leq t} p^{\mu_j}\alpha_j\psi_{j,i}x^i\Big), \\ h^{(\alpha_1,\ldots,\alpha_t)} &= h + p^{k-r(g,h)}\Big(\sum_{0\leq i<m}\sum_{1\leq j\leq t} p^{\mu_j}\alpha_j\psi_{j,i}x^i\Big), \end{aligned}$$

where $\alpha_i \in R_{r(g,h)-\mu_i}$ for $1 \leq i \leq t$ are arbitrary. This data structure allows to represent the possibly exponentially many factorizations with data of only polynomial size.

The following lemma estimates the running time of the described procedure. Unfortunately, we did not find an exact estimate for the running time for computing the Smith normal form together with the transition matrices P and Q in the case that $R = \mathbb{F}_q[y]$. Hence, we define $SNF(n,k)$ to be the number of operations in $\mathbb{F}_q$ such that there is a (probabilistic) algorithm which computes the Smith normal form of an $n\times n$-Matrix over $\mathbb{F}_q[y]$ together with the transition matrices modulo y^k with $O(SNF(n,k))$ operations in $\mathbb{F}_q$. By Kaltofen *et al.* (1990) we may assume that $SNF(n,k)$ is polynomial in nk.

LEMMA 4.3. *Assume that $f, g, h \in R[x]$ are monic with $f \equiv gh \bmod p^k$ for some $k > 2r(g,h)$. Then the following holds:*

(a) If $R = \mathbb{Z}$, then the set set of all factorizations of the form (4.1) can be computed with

$$O(n^{\omega+2}(\log n + k\log p)\log(n\log n + nk\log p)\mathsf{M}(n\log n + nk\log p))$$

operations, if $\deg f = n$ and the coefficients of f, g, h are bounded by p^k.

(b) If $R = \mathbb{F}_q[y]$ and $p = y$, then the set of all facorizations of the form (4.1) can be computed with $O(SNF(n,k))$ operations in $\mathbb{F}_q$.

PROOF. In order to compute the set of factorizations, first the Smith normal form of $S(g,h) \bmod p^{r(g,h)}$ together with the transition matrices have to be computed. All other computations are just some multiplications and divisions by p. Note that the multiplication $b_i = Qa_i'$ is just a multiplication of a column of Q with a power of p. By Iliopoulos (1989), these computations can be done with

$$O(n^{\omega+2}(\log n + k\log p)\log(n\log n + nk\log p)\mathsf{M}(n\log n + nk\log p))$$

operations if $R = \mathbb{Z}$. If $R = \mathbb{F}_q[y]$ and $p = y$, then $O(SNF(n,k))$ operations suffice by definition. $\square$

EXAMPLE 4.4. *We consider* $f = (x^2+3)(x^3+9x^2+12x+27) = x^5+9x^4+15x^3+54x^2+36x+81 \in \mathbb{Z}[x]$ *and* $p = 3$. *We have* $disc(f) = 3^{14}\cdot 6100$, $d(f) = 14$, *and* $r(x^2+3, x^3+9x^2+12x+27) = 5$. *The factor* x^2+3 *is an Eisenstein polynomial and hence irreducible. We want to describe all factorizations* $f \equiv uw \bmod 3^{15}$ *such that* $u \in \mathbb{Z}[x]$ *is irreducible over* $\mathbb{Z}/(3^{15})$ *with* $u \equiv x^2+3 \bmod 3^{10}$. *We have to solve the system of equations*

$$S(x^2+3, x^3+9x^2+12x+27)\begin{pmatrix}\psi_2\\ \psi_1\\ \psi_0\\ \varphi_1\\ \varphi_0\end{pmatrix}$$
$$= \begin{pmatrix}1&0&0&1&0\\ 0&1&0&9&1\\ 3&0&1&12&9\\ 0&3&0&27&12\\ 0&0&3&0&27\end{pmatrix}\begin{pmatrix}\psi_2\\ \psi_1\\ \psi_0\\ \varphi_1\\ \varphi_0\end{pmatrix} \equiv 0 \bmod 3^5.$$

We compute the Smith normal form as

$$\begin{pmatrix}1&0&0&0&0\\ 0&1&0&0&0\\ -3&0&1&0&0\\ 0&-3&0&1&0\\ 9&-9&-3&3&1\end{pmatrix}\begin{pmatrix}1&0&0&1&0\\ 0&1&0&9&1\\ 3&0&1&12&9\\ 0&3&0&27&12\\ 0&0&3&0&27\end{pmatrix}\begin{pmatrix}1&0&0&-1&1\\ 0&1&0&-10&9\\ 0&0&1&-18&9\\ 0&0&0&1&-1\\ 0&0&0&1&0\end{pmatrix}$$
$$= \begin{pmatrix}1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&9&0\\ 0&0&0&0&27\end{pmatrix}.$$

Thus $\omega_1 = \omega_2 = \omega_3 = 0, \omega_4 = 2, \omega_5 = 3, s = 4, t = 2$. *Hence*

$$b_1 = \begin{pmatrix} 1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -10 & 9 \\ 0 & 0 & 1 & -18 & 9 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -10 \\ -18 \\ 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 8 \\ 0 \\ 1 \\ 1 \end{pmatrix} \bmod 9,$$

$$b_2 = \begin{pmatrix} 1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -10 & 9 \\ 0 & 0 & 1 & -18 & 9 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 9 \\ 9 \\ -1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 9 \\ 9 \\ 26 \\ 0 \end{pmatrix} \bmod 27,$$

and the set of solutions can be written as

$$\left\{ 27\alpha_1 \begin{pmatrix} 8 \\ 8 \\ 0 \\ 1 \\ 1 \end{pmatrix} + 9\alpha_2 \begin{pmatrix} 1 \\ 9 \\ 9 \\ 26 \\ 0 \end{pmatrix} : 0 \le \alpha_1 \le 8, 0 \le \alpha_2 \le 26 \right\}.$$

Hence the factorizations are $f \equiv u^{(\alpha_1,\alpha_2)} w^{(\alpha_1,\alpha_2)} \bmod 3^{15}$ *with*

$$\begin{aligned} u^{(\alpha_1,\alpha_2)} &= g + (3^{13}\alpha_1 + 26 \cdot 3^{12}\alpha_2)x + 3^{13}\alpha_1, \\ w^{(\alpha_1,\alpha_2)} &= h + (8 \cdot 3^{13}\alpha_1 + 3^{12}\alpha_2)x^2 + (8 \cdot 3^{13}\alpha_1 + 3^{14}\alpha_2)x + 3^{14}\alpha_2, \end{aligned}$$

where $g = x^2 + 3$, $h = x^3 + 9x^2 + 12x + 27$, $0 \le \alpha_1 \le 8$, *and* $0 \le \alpha_2 \le 26$. *We see that there exist* 243 *different factorizations which can be represented concisely via* α_1 *and* α_2.

The idea of the algorithm now is as follows: From Chistov's algorithm we obtain one factorization $f \equiv \prod_{1\le i\le l} g_i \bmod p^k$ with $g_i \in R[x]$ monic and irreducible over $R/(p^k)$ for $1 \le i \le l$. If $l > 1$, we inductively compute all irreducible factors of f in the following way. Let $\rho_j = \sum_{1\le i<j} r(g_i, \prod_{t>i} g_t)$ for $1 \le j \le l$. We assume that $1 \le i < l$ and all factorizations $f \equiv (\prod_{1\le j<i} u_j)w \bmod p^k$ such that $u_j \in R[x]$ is irreducible over $R/(p^k)$, $u_j \equiv g_j \bmod p^{k-\rho_j}$ for $1 \le j < i$ and $w \equiv \prod_{j\ge i} g_j \bmod p^{k-\rho_i}$ have already been computed. This means that we have a set of parameters such that the $u_j, 1 \le j < i$, and w depend linearly on them. Now we lift each factorization $w \equiv g_i \prod_{j>i} g_j \bmod p^{k-\rho_i}$ to a factorization over $R/(p^k)$ and compute all factorizations $w \equiv ab \bmod p^k$ such that $a \equiv g_i \bmod p^{k-\rho_i}$ and $b \equiv \prod_{j>i} g_j \bmod p^{k-\rho_i}$.

It is shown in Lemma 4.8 and Theorem 4.9 that these two steps can be done simultaneously for all parameters. The last step yields some new parameters which are added to the set of the previously computed ones. Theorem 4.9 shows that one obtains in this way all factorizations.

NOTATION 4.5. *Let $l \geq 2$ and $f, g_1, \ldots, g_l \in R[x]$ be monic such that $f \equiv \prod_{1\leq i\leq l} g_i \bmod p^k$. Then we define $r_i = r(g_i, \prod_{i<j\leq l} g_j)$ for $1 \leq i < l$.*

ALGORITHM 4.6.
Input: *A monic polynomial $f \in R[x]$ with $d(f) = v_p(disc(f)) < \infty$, a prime $p \in R$, and $k \geq 1$ such that $k > d(f)$.*
Output: *All factorizations of f over $R/(p^k)$ into irreducible monic factors.*

1. *Use Chistov's algorithm to find the factorization $f = \prod_{1\leq i\leq l} g_i$ into irreducible monic factors of f over $R_{(p)}$, i.e., for $1 \leq i \leq l$ compute $g_i \bmod p^k$. If $l = 1$, then output "f is irreducible" and stop. If $d(f) = 0$, then output "$f \equiv \prod_{1\leq i\leq l} g_i \bmod p^k$" and stop.*
2. *Set $w_1 = f$ and $j_0 = 0$. For $1 \leq m < l$ do Steps 3 and 4.*
3. *Lift the factorization*
$$w_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv g_m \prod_{m<i\leq l} g_i \bmod p^{k-\sum_{1\leq j<m} r_j}$$
depending on the parameters $\alpha_1, \ldots, \alpha_{j_{m-1}}$ to a factorization
$$w_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv a_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} b_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \bmod p^k, \text{ where}$$
$$a_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv g_m \bmod p^{k-\sum_{1\leq j\leq m} r_j}, \text{ and}$$
$$b_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv \prod_{m<i\leq l} g_i \bmod p^{k-\sum_{1\leq j\leq m} r_j}$$
for all parameters $\alpha_1, \ldots, \alpha_{j_{m-1}}$.
4. *Compute all solutions of Equation (4.2) with $g = g_m$ and $h = \prod_{m<i\leq l} g_i$ in order to obtain all factorizations*
$$w_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv u_m^{(\alpha_1,\ldots,\alpha_{j_m})} w_{m+1}^{(\alpha_1,\ldots,\alpha_{j_m})} \bmod p^k$$
such that
$$u_m^{(\alpha_1,\ldots,\alpha_{j_m})} \equiv a_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \bmod p^{k-r_m},$$
$$w_{m+1}^{(\alpha_1,\ldots,\alpha_{j_m})} \equiv b_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \bmod p^{k-r_m},$$
and $j_m \geq j_{m-1}$ together with the feasible values for $\alpha_{j_{m-1}+1}, \ldots, \alpha_{j_m}$.

5. *Set* $j_l = j_{l-1}$ *and* $u_l^{(\alpha_1,\ldots,\alpha_{j_l})} = w_l^{(\alpha_1,\ldots,\alpha_{j_{l-1}})}$, *and output*

$$\text{“}f \equiv \prod_{1\leq i\leq l} u_i^{(\alpha_1,\ldots,\alpha_{j_i})} \bmod p^k\text{”}$$

together with the ranges of $\alpha_1, \ldots, \alpha_{j_l}$.

EXAMPLE 4.7. *We take the polynomial* $f = x^5+9x^4+15x^3+54x^2+36x+81 \in \mathbb{Z}[x]$ *of Example 4.4 and* $k = 15$ *as input of Algorithm 4.6. Since* $d(f) = 14$, *we have* $d(f) < k$. *In Step 1 of the algorithm the factorization* $f \equiv g_1g_2g_3 \bmod 3^{15}$ *with*

$$\begin{aligned} g_1 &= x^2+3, \\ g_2 &= x+9+2\cdot 3^3+2\cdot 3^5+3^6+3^7+2\cdot 3^9+2\cdot 3^{10}+2\cdot 3^{12}+3^{14}, \\ g_3 &= x^2+(3^3+2\cdot 3^4+3^6+3^7+2\cdot 3^8+2\cdot 3^{11}+2\cdot 3^{13}+3^{14})x \\ &\quad +3+9+2\cdot 3^5+3^6+3^8+2\cdot 3^9+3^{10}+3^{13}+3^{14} \end{aligned}$$

is computed. The polynomial g_2 *is linear,* g_1 *and* g_3 *are Eisenstein polynomials, and hence all three factors of* f *are irreducible. Since* $g_2g_3 \equiv x^3+9x^2+12x+27 \bmod 3^{15}$, *Step 2 for* $m = 1$ *has been done in Example 4.4. It yields the factorizations* $f \equiv u_1^{(\alpha_1,\alpha_2)}w_2^{(\alpha_1,\alpha_2)} \bmod 3^{15}$ *with*

$$\begin{aligned} u_1^{(\alpha_1,\alpha_2)} &= x^2+3+(3^{13}\alpha_1+26\cdot 3^{12}\alpha_2)x+3^{13}\alpha_1, \\ w_2^{(\alpha_1,\alpha_2)} &= x^3+9x^3+12x^2+27+(8\cdot 3^{13}\alpha_1+3^{12}\alpha_2)x^2+(8\cdot 3^{13}\alpha_1+3^{14}\alpha_2)x \\ &\quad +3^{14}\alpha_2, \end{aligned}$$

and $0 \leq \alpha_1 \leq 8$, $0 \leq \alpha_2 \leq 26$. *In Step 3 for* $m = 2$, *one has to lift the factorization* $w_2^{(\alpha_1,\alpha_2)} \equiv g_2g_3 \bmod 3^{12}$ *to a factorization modulo* 3^{15}. *Since* $s(g_2, g_3) = 1$, *this can be done as in Theorem 3.5 and yields the factorizations* $w_2^{(\alpha_1,\alpha_2)} \equiv a^{(\alpha_1,\alpha_2)}b^{(\alpha_1,\alpha_2)} \bmod 3^{15}$, *where*

$$\begin{aligned} a^{(\alpha_1,\alpha_2)} &= g_2+3^{14}\alpha_1+7\cdot 3^{13}\alpha_2, \\ b^{(\alpha_1,\alpha_2)} &= g_3+(5\cdot 3^{13}\alpha_1+7\cdot 3^{12}\alpha_2)x+8\cdot 3^{13}\alpha_1. \end{aligned}$$

In Step 4, we have to find all factorizations $w_2^{(\alpha_1,\alpha_2)} \equiv u_2u_3 \bmod 3^{15}$ *such that* $u_2 \equiv a^{(\alpha_1,\alpha_2)} \bmod 3^{14}$ *and* $u_3 \equiv b^{(\alpha_1,\alpha_2)} \bmod 3^{14}$. *In the same way as in Example 4.4 one has to solve the system of linear equations*

$$S(a^{(\alpha_1,\alpha_2)}, b^{(\alpha_1,\alpha_2)}) \begin{pmatrix} \psi_1 \\ \psi_0 \\ \varphi_0 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \psi_1 \\ \psi_0 \\ \varphi_0 \end{pmatrix} \equiv 0 \bmod 3$$

and obtains the factorizations

$$w_2^{(\alpha_1,\alpha_2)} \equiv u_2^{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)} u_3^{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)} \bmod 3^{15},$$

where

$$\begin{aligned} u_2^{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)} &= g_2 + 3^{14}\alpha_1 + 7\cdot 3^{13}\alpha_2 + 3^{14}\alpha_3, \\ u_3^{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)} &= g_3 + (5\cdot 3^{13}\alpha_1 + 7\cdot 3^{12}\alpha_2 + 2\cdot 3^{14}\alpha_3)x + 8\cdot 3^{13}\alpha_1, \end{aligned}$$

and $0 \le \alpha_3 \le 2$. *Hence, the* 3^6 *factorizations of* f *into irreducible factors are*

$$\begin{aligned} f \equiv{}& (g_1 + (3^{13}\alpha_1 + 26\cdot 3^{12}\alpha_2)x + 3^{13}\alpha_1)\cdot(g_2 + 3^{14}\alpha_1 + 7\cdot 3^{13}\alpha_2 + 3^{14}\alpha_3)\cdot \\ & (g_3 + (5\cdot 3^{13}\alpha_1 + 7\cdot 3^{12}\alpha_2 + 2\cdot 3^{14}\alpha_3)x + 8\cdot 3^{13}\alpha_1) \bmod 3^{15}, \end{aligned}$$

where $0 \le \alpha_1 \le 8, 0 \le \alpha_2 \le 26, 0 \le \alpha_3 \le 2$.

Before we can show that the algorithm works correctly, we have to prove the following technical lemma.

LEMMA 4.8. *Let* $f \in R[x]$, $d(f) < \infty$, $k > d(f)$ *and* $g_i \in R[x]$ *be irreducible over* $R/(p^k)$ *for* $1 \le i \le l$ *with* $f \equiv \prod_{1\le i\le l} g_i \bmod p^k$. *Then the following relations hold:*

(a) *Let* $u, w \in R[x]$ *with* $u \equiv \prod_{1\le i\le m} g_i \bmod p^{k-r(u,w)}$, *and* $w \equiv \prod_{m<i\le l} g_i \bmod p^{k-r(u,w)}$ *for some* $m \le l$ *such that* $f \equiv uw \bmod p^k$. *Then* $r(u,w) = r(\prod_{1\le i\le m} g_i, \prod_{m<i\le l} g_i)$.

(b) *We have* $k - \sum_{1\le i\le m} r_i > 2r_{m+1}$ *for every* $m < l$.

(c) *Let* $a, b \in R[x]$ *such that*

$$a \equiv g_{m+1} \bmod p^{k-\sum_{1\le j\le m} r_j}, \text{ and } b \equiv \prod_{m+2\le i\le l} g_i \bmod p^{k-\sum_{1\le j\le m} r_j}$$

for some $m \le l-2$. *Then*

$$S(a,b) \equiv S(g_{m+1}, \prod_{m+2\le i\le l} g_i) \bmod p^{r(a,b)+1}.$$

(d) $r(g_i, \prod_{j\ne i} g_j) \le \sum_{1\le j\le i} r_j$ *for every* $1 \le i \le l$.

PROOF. Recall from (3.3) that for $f \equiv gh \bmod p^k$ we have

$$\operatorname{disc}(f) \equiv \operatorname{disc}(g)\operatorname{disc}(h)\operatorname{res}(g,h)^2 \bmod p^k,$$

hence $d(f) = d(g) + d(h) + 2r(g,h)$, since $k > d(f)$.

(a) We have

$$k - r(u,w) > d(f) - r(u,w) = d(u) + d(w) + 2r(u,w) - r(u,w) \geq r(u,w).$$

Now the claim follows.

(b) We have

$$\begin{aligned} k - \sum_{1\leq i\leq m} r_i &> d(f) - \sum_{1\leq i\leq m} r_i \\ &\geq \sum_{1\leq i\leq m} d(g_i) + d(\prod_{m<i\leq l} g_i) + 2\sum_{1\leq i\leq m} r_i - \sum_{1\leq i\leq m} r_i \\ &\geq d(\prod_{m<i\leq l} g_i) \\ &\geq d(g_{m+1}) + d(\prod_{m+2\leq i\leq l} g_i) + 2r_{m+1} \\ &\geq 2r_{m+1}. \end{aligned}$$

(c) Since

$$k - \sum_{1\leq i\leq m} r_i > 2r_{m+1} \geq r_{m+1} = r(a,b),$$

by (b), it follows that

$$a \equiv g_{m+1} \bmod p^{r(a,b)+1}, \text{ and } b \equiv \prod_{m+2\leq i\leq l} g_i \bmod p^{r(a,b)+1}.$$

Hence, $S(a,b) \equiv S(g_{m+1}, \prod_{m+2\leq i\leq l} g_i) \bmod p^{r(a,b)+1}$.

(d) Let $1 \leq i \leq l$. Recall that for polynomials $f,g,h \in R[x]$ we have $\operatorname{res}(f,gh) = \operatorname{res}(f,g)\operatorname{res}(f,h)$ (Cohn 1977, 7.4, Theorem 2). Hence

$$r(f,gh) = r(f,g) + r(f,h).$$

Now

$$\begin{aligned} r(g_i, \prod_{j\neq i} g_j) &= r_i + \sum_{1\leq j<i} r(g_i,g_j) \\ &\leq r_i + \sum_{1\leq j<i} r_j + r_i = \sum_{1\leq j\leq i} r_j. \quad \square \end{aligned}$$

Besides the correctness of our algorithm, we also prove a bound for the running time of the algorithm. Since no explicit running time bound for Chistov's algorithm for factoring polynomials over $R_{(p)}$ is known to us, we define $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ (resp. $\mathsf{C}_q(y,n,k)$) to be a function depending on p, n and k such that Chistov's algorithm with input a polynomial $f \in \mathbb{Z}[x]$ (resp. $f \in \mathbb{F}_q[y][x]$) of degree n and a positive integer k computes the factorization into irreducible factors over $\mathbb{Z}_{(p)}$ (resp. $\mathbb{F}_q((y))$) modulo p^k (resp. y^k) with $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ (resp. $\mathsf{C}_q(y,n,k)$) operations. $\mathsf{C}_{\mathbb{Z}}(n,p,k)$ and $\mathsf{C}_q(y,n,k)$ can be chosen polynomial in n, k and $\log p$ (resp. $\log q$)(Chistov 1994, Basic Theorem).

THEOREM 4.9. *Algorithm 4.6 works correctly, i.e. each irreducible factor of f over $R/(p^k)$ is of the form $u_i^{(\alpha_1,\ldots,\alpha_{j_i})}$ for some $1 \le i \le l$ and feasible values for $\alpha_1,\ldots,\alpha_{j_i}$ as computed in the algorithm. It works in polynomial time for $R = \mathbb{Z}$ and $R = \mathbb{F}_q[y]$. In particular, if $R = \mathbb{Z}$ and $\deg f = n$, then the set of all factorizations of f into irreducible factors can be computed with*

$$\mathsf{C}_{\mathbb{Z}}(p,n,k) + O(n^7 k \log p (k \log p + \log n)^2)$$

bit operations, if the coefficients of f are bounded by p^k. Let $R = \mathbb{F}_q[y]$ and $p = y$. Then the set of all factorizations of $f \in \mathbb{F}_q[y][x]$ into irreducible factors can be computed with

$$\mathsf{C}_q(y,n,k) + O(n^4 k^2 \mathsf{M}(\log nk) \log^2 nk + k^2 n^{\omega+2} \mathsf{M}(\log nk) + nSNF(n,k))$$

operations in $\mathbb{F}_q$.

PROOF. If f is irreducible over $R_{(p)}$, it is irreducible over $R/(p^k)$ for all $k > d(f)$ by Theorem 3.5. Also, if $d(f) = 0$, the factorization of f into irreducible factors is unique over $R/(p^k)$ for every $k \ge 1$ by Theorem 3.8(b). Hence, from now on we assume that $d(f) > 0$ and f is reducible over $R_{(p)}$.

From Corollary 3.3 and Lemma 4.8(d), we obtain that only the matrix

$$S(g_m, \prod_{m<i\le l} g_i)$$

is needed in order to lift the factorizations of Step 3. Besides, Lemma 4.8(c) also shows that in order to compute the solutions in Step 4, only this matrix is necessary. Hence, both steps can be done for all parameters at once.

Now, we prove by induction on $m < l$ the claim that after the execution of Steps 3 and 4 for m all factorizations $f \equiv (\prod_{1\le i\le m} u_i)w \bmod p^k$ such that for all $1 \le i \le m$ one has $u_i \equiv g_i \bmod p^{k-\sum_{1\le j\le i} r_j}$ have been computed.

If $m = 1$, then $w_0 = f$, and in Step 3 there is nothing to do. In Step 4, all factorizations $f \equiv uw \bmod p^k$ such that $u \equiv g_1 \bmod p^{k-r_1}$, and $w \equiv \prod_{1<i\leq l} g_i \bmod p^{k-r_1}$ are computed.

Now let $1 < m \leq l-1$, and assume the induction hypothesis holds for $m-1$. Then by induction hypothesis we have have found every factor w_{m-1} such that

$$w_{m-1} \equiv g_{m-1} \prod_{m\leq i\leq l} g_i \bmod p^{k-\sum_{1\leq j<m} r_j}. \tag{4.3}$$

By Lemma 4.8(b) and Theorem 3.5 we can lift the factorization in (4.3) as is claimed in Step 3. On the other hand, if there is a factorization $w_{m-1} \equiv ab \bmod p^k$ such that $a \equiv g_m \bmod p^{k-\sum_{1\leq j} r_j}$, and $b \equiv \prod_{m<i\leq l} g_i \bmod p^{k-\sum_{1\leq j<m} r_j}$, then again by Lemma 4.8(b) and Theorem 3.5 this factorization is found in Step 4. Hence, the claim is proven.

Now assume that $f \equiv uw \bmod p^k$ such that u is irreducible. Since $k > d(f)$, it follows from Lemma 4.1 that $u \equiv g_i \bmod p^{k-r(u,w)}$ and $w \equiv \prod_{j\neq i} g_j \bmod p^{k-r(u,w)}$ for some $1 \leq j \leq l$. Moreover, $r(u,w) = r(g_j, \prod_{i\neq j} g_i)$ by Lemma 4.8(a). By Lemma 4.8(d), we have $r(g_i, \prod_{j\neq i} g_j) \leq \sum_{1\leq j\leq i} r_j$. Hence

$$\begin{aligned} u &\equiv g_i \bmod p^{k-\sum_{1\leq j\leq i} r_j}, \text{ and} \\ w &\equiv \prod_{j\neq i} g_i \bmod p^{k-\sum_{1\leq j\leq i} r_j}. \end{aligned}$$

Therefore, this factorization will be computed by Algorithm 4.6.

For the running time analysis, assume that $R = \mathbb{Z}$ and $\deg f = n$. By definition, $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ operations suffice to compute the factorization of Step 1. Furthermore, $d(f)$ has to be computed. This can be done by Collins (1971), since $d(f) = r(f, f')$, with $O(n^3(\log n + k\log p) + n^2(\log n + k\log p)^2)$ operations. Step 3 is one application of Theorem 3.5, hence it can be done with $O(n^6 k\log p(\log n + k\log p)^2)$ operations. In Step 4,

$$O(n^{\omega+2}(\log n + k\log p)\log(n\log n + nk\log p)\mathsf{M}(n\log n + nk\log p))$$

operations suffice by Lemma 4.3(a). Since $l \leq n$ we obtain

$$O(n^7 k\log p(\log n + k\log p)^2)$$

bit operations for Steps 2-5.

Now let $R = \mathbb{F}_q[y]$, $p = y$, and $\deg_x f = n$. Step 1 of the algorithm can be done with $\mathsf{C}_q(y,n,k)$ operations by definition. From Theorem 3.5 follows that Step 3 can be done with $O(n^3k^2\mathsf{M}(\log nk)\log^2 nk + k^2n^{\omega+1}\mathsf{M}(\log nk))$ operations. Now for Step 4, $O(SNF(n,k))$ operations suffice by Lemma 4.3(b). Hence, Steps 2-5 can be done with

$$O(n^4k^2\mathsf{M}(\log nk)\log^2 nk + k^2n^{\omega+2}\mathsf{M}(\log nk) + nSNF(n,k))$$

operations in $\mathbb{F}_q$. □

REMARK 4.10. *The case $k \le d(f)$ seems more difficult to handle. We have not been able to make the methods introduced here work for this case. Of course, the factorization of f in $R_{(p)}[x]$ provides a factorization modulo each p^k, but we have no efficient way of factoring a polynomial over $R/(p^k)$ which is irreducible in $R_{(p)}[x]$. At this point, the only way we know to obtain all or even just one irreducible factorization is to try all possibilities (of which there may be exponentially many). In von zur Gathen & Hartlieb (1996) we show how this can be done.*

REMARK 4.11. *In the case that disc$(f) = 0$ our method does not work. It is not difficult to compute a factorization of f over R by a squarefree factorization. In the case where $k > d(f)$ this would mean that all factorizations of f over $R/(p^k)$ are compatible with this factorization, as Lemma 4.1 shows; in particular, all factorizations of f into irreducible factors have the same degrees as the factorization of f over R into irreducible factors. Even this is not guaranteed in the case disc$(f) = 0$, as is shown in the next example. Thus, one can reduce the problem of finding a single factorization into irreducibles over $R/(p^k)$ to the case where disc$(f) \neq 0$, but apparently not the problem of finding all factorizations into irreducibles.*

EXAMPLE 4.12. *Let $R = \mathbb{Z}$, $p = 3$, and $f = x^3(x+12)^2 = x^5 + 24x^4 + 144x^3$. Then*

$$f \equiv (x+60)(x^4 + 207x^3 + 117x^2 + 27x + 81) \bmod 3^5,$$

where both factors are irreducible over $\mathbb{Z}/3^5\mathbb{Z}$.

5. A generalization of Hensel's Lemma

Our algorithm of the previous section is mainly based on the fact that if a given polynomial $f \in R[x]$ has a factorization into irreducibles $f = \prod_{1\le i\le l} g_i$ over $R_{(p)}$ then every irreducible factor u of f over $R/(p^k)$ is of the form $u \equiv$

$g_i \bmod p^{k-r(g_i,\prod_{j\neq i} g_j)}$ for some $1 \leq i \leq l$, if $k > d(f)$. Example 4.4 shows that it may happen that for some i there is no irreducible factor u of f such that $u \equiv g_i \bmod p^{k-r(g_i,\prod_{j\neq i} g_j)}$ but $u \not\equiv g_i \bmod p^{k-r(g_i,\prod_{j\neq i} g_j)+1}$. In this section we improve Hensel's Lemma in exchanging $r(g,h)$ with a sometimes smaller value $s(g,h)$ such that the same statements as for $r(g,h)$ hold and in addition this value is always optimal. This means that whenever $f \equiv gh \bmod p^k$ with $k > 2s(g,h)$ holds, then there exists a factorization $f \equiv uw \bmod p^k$ such that $u \equiv g \bmod p^{k-s(g,h)}$ and $w \equiv h \bmod p^{k-s(g,h)}$, but $u \not\equiv g \bmod p^{k-s(g,h)+1}$ or $w \not\equiv h \bmod p^{k-s(g,h)+1}$.

DEFINITION 5.1. *Let $g, h \in R[x]$ such that $res(g,h) \neq 0$. Then we define $s(g,h) = -v_p(S(g,h)^{-1})$.*

LEMMA 5.2. *Let $g, h \in R[x]$ with $res(g,h) \neq 0$. Then*

$$0 \leq s(g,h) \leq r(g,h).$$

Moreover, if $s(g,h) = 0$, then $r(g,h) = 0$.

PROOF. Since $\mathrm{res}(g,h) = \det S(g,h)$, the matrix $\mathrm{res}(g,h)S(g,h)^{-1}$ is a matrix over R and has nonnegative p-adic value. Hence, $r(g,h) \geq s(g,h)$. Now assume that $v_p(S(g,h)^{-1}) > 0$. Then $v_p(\det S(g,h)^{-1}) > 0$, hence $r(g,h) < 0$. This is a contradiction, because $\mathrm{res}(g,h) \in R$.

Now assume that $s(g,h) = 0$. Then $S(g,h)$ is invertible over $R_{(p)}$, and hence $\mathrm{res}(g,h)$ is invertible over $R_{(p)}$. It follows that $r(g,h) = 0$. □

Now it is easy to see that Proposition 3.2 also holds in the following version:

PROPOSITION 5.3. *Let $g, h \in R[x]$ of degrees n, m, respectively, such that $res(g,h) \neq 0$. Let $res(g,h) = p^{r(g,h)}b$ with $b \in R$, and $l \in R[x]$ with $\deg l < n + m$. Then there exist uniquely determined polynomials $\varphi, \psi \in R[x]$ with $\deg \varphi < m$ and $\deg \psi < n$ such that*

$$p^{s(g,h)}bl = \varphi g + \psi h.$$

If $R = \mathbb{Z}$, and the bit length of the coefficients of g and h is bounded by N, then $O((n+m)^6(N + \log(n+m))^2)$ operations suffice to compute φ and ψ, given g, h, l. If $R = \mathbb{F}_q[y]$, $\deg_y g, \deg_y h, \deg_y l \leq N$, and $p = y$, then $O((n+m)^3 N \mathsf{M}(\log(n+m)N)\log^2(n+m)N + N(n+m)^{\omega+1}\mathsf{M}(\log(n+m)N))$ operations in $\mathbb{F}_q$ suffice to compute φ and ψ.

PROOF. The proof works analogously to the proof of Proposition 3.2. We only have to remark that the entries of the matrix $bp^{s(g,h)}S(g,h)^{-1}$ are in R by the definition of $s(g,h)$. For the running time analysis, it suffices to observe that the computation of $s(g,h)$ can be done within the stated running time bound. $\square$

We have seen in the previous section that if $u, w, g, h \in R[x]$ are given such that $u \equiv g \bmod p^{r(g,h)+1}$ and $w \equiv h \bmod p^{r(g,h)+1}$, then $r(u,w) = r(g,h)$. The next lemma shows that the same is true for $s(g,h)$.

LEMMA 5.4. *Let $g, h, u, w \in R[x]$ be monic such that res$(g,h) \neq 0$, $g \equiv u \bmod p^{s(g,h)+1}$, and $w \equiv h \bmod p^{s(g,h)+1}$. Then $s(u,w) = s(g,h)$.*

PROOF. Let $s(g,h) = \sigma$, $u = g + p^{\sigma+1}g_0$ and $w = h + p^{\sigma+1}h_0$ with $g_0, h_0 \in R[x]$, and assume that $\mathrm{res}(u,w) = 0$. Then $S(u,w)$ is not invertible, and there are polynomials $a, b \in R[x]$ such that $\deg a < \deg w$, $\deg b < \deg u$, and

$$au + bw = 0,$$

with $a \not\equiv 0 \bmod p$ or $b \not\equiv 0 \bmod p$. But then

$$\begin{aligned} 0 &= au + bw = a(g + p^{\sigma+1}g_0) + b(h + p^{\sigma+1}h_0) \\ &= ag + bh + p^{\sigma+1}(g_0 a + h_0 b) + p^{2\sigma+2}g_0 h_0. \end{aligned}$$

It follows that $ag + bh \equiv 0 \bmod p^{\sigma+1}$. Hence $ag + bh = p^{\sigma+1}l$ for a polynomial $l \in R[x]$ with $\deg l < \deg g + \deg h$. If we compute the unique solutions a, b of this equation by Proposition 5.3, we obtain that $a \equiv 0 \bmod p$ and $b \equiv 0 \bmod p$, a contradiction. Hence, $\mathrm{res}(u,w) \neq 0$, and $s(u,w)$ is defined.

Let $\deg g = n$ and $\deg h = m$. By Proposition 5.3, there exist for each $l \in R[x]$ with $\deg l < n + m$ polynomials $a, b \in R[x]$ with $\deg a < m$ and $\deg b < n$ such that $ag + bh \equiv p^\sigma l \bmod p^{\sigma+1}$. It follows that $au + bw \equiv p^\sigma l \bmod p^{\sigma+1}$. Let $au + bw = p^\sigma l + p^{\sigma+1}l'$ with

$$a = \sum_{0 \le i < m} a_i x^i, b = \sum_{0 \le i < n} b_i x^i,$$

$$l = \sum_{0 \le i < n+m} l_i x^i, \text{ and } l' = \sum_{0 \le i < n+m} l'_i x^i.$$

Then

$$au + bw = p^\sigma l + p^{\sigma+1}l'$$

$$\Leftrightarrow \quad S(u,w)\begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = p^\sigma \begin{pmatrix} l_{n+m-1} \\ \vdots \\ l_0 \end{pmatrix} + p^{\sigma+1} \begin{pmatrix} l'_{n+m-1} \\ \vdots \\ l'_0 \end{pmatrix}$$

$$\Leftrightarrow \quad \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = p^\sigma S(u,w)^{-1} \begin{pmatrix} l_{n+m-1} \\ \vdots \\ l_0 \end{pmatrix} + p^{\sigma+1} S(u,w)^{-1} \begin{pmatrix} l'_{n+m-1} \\ \vdots \\ l'_0 \end{pmatrix}.$$

Using all monomials $x^{n+m-1}, x^{n+m-2}, \ldots, x^0$ for l, we find that $p^\sigma S(u,w)^{-1}$ is a matrix in R, each of whose columns has p-adic value 0. □

With Proposition 5.3 and Lemma 5.4, the proof of the next theorem is analogue to the proof of Theorem 3.5.

THEOREM 5.5. *Let $f, u, w \in R[x]$ be monic such that $\mathrm{res}(u,w) \neq 0$, and $f \equiv uw \bmod p^k$ with $k > 2s(u,w)$. Then there exist monic polynomials $g, h \in R_{(p)}[x]$ such that $f = gh$, $g \equiv u \bmod p^{k-s(u,w)}$ and $h \equiv w \bmod p^{k-s(u,w)}$. For $R = \mathbb{Z}$, and $N > k$ the polynomials $g \bmod p^N$ and $h \bmod p^N$ can be computed in $O((n+m)^6 N (N \log p + \log(n+m))^2)$ operations, if we assume that $R = \mathbb{Z}$ and the absolute values of the coefficients of f, u, w are bounded by p^N, and with $O((n+m)^3 N^2 \mathsf{M}(\log(n+m)N) \log^2(n+m)N + N^2 (n+m)^{\omega+1} \mathsf{M}(\log(n+m)N))$ operations, if $R = \mathbb{F}_q[y]$ and $p = y$.*

A version of Theorem 5.5 is already proven in von zur Gathen (1984) in a different setting. In particular, no explicit formula for $s(u,w)$ is given.

The next example shows that sometimes $s(g,h) < r(g,h)$:

EXAMPLE 5.6. *Let $R = \mathbb{Z}$, $p = 3$, $g = x^2 + 3$, and $h = x^3 + 9x^2 + 12x + 27$. Then*

$$S(g,h) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 9 & 1 \\ 3 & 0 & 1 & 12 & 9 \\ 0 & 3 & 0 & 27 & 12 \\ 0 & 0 & 3 & 0 & 27 \end{pmatrix}, S(g,h)^{-1} = \begin{pmatrix} \frac{4}{3} & 0 & -\frac{1}{9} & 0 & \frac{1}{27} \\ 3 & \frac{4}{3} & -1 & -\frac{1}{9} & \frac{1}{3} \\ 0 & 3 & 0 & -1 & \frac{1}{3} \\ -\frac{1}{3} & 0 & \frac{1}{9} & 0 & -\frac{1}{27} \\ 0 & -\frac{1}{3} & 0 & \frac{1}{9} & 0 \end{pmatrix}.$$

It follows that $\mathrm{res}(g,h) = 3^5$, $r(g,h) = 5$, and $s(g,h) = 3$.

THEOREM 5.7. *Let $f, g, h \in R[x]$ be monic of degrees $n+m, n, m$, respectively, with $f \equiv gh \bmod p^k$, $res(g,h) \neq 0$ and $\sigma = s(g,h)$. If $k > 2\sigma$, then there exist polynomials $\varphi_k, \psi_k \in R[x]$ of degrees less than n, m, respectively, such that $\varphi_k \not\equiv 0 \bmod p$ or $\psi_k \not\equiv 0 \bmod p$ and $f \equiv (g + p^{k-\sigma}\varphi_k)(h + p^{k-\sigma}\psi_k) \bmod p^k$.*

PROOF. Let $u, w \in R[x]$ with $\deg u < n$ and $\deg w < m$ such that $u = \sum_{0 \le i < n-1} u_i x^i$ and $w = \sum_{0 \le j < m-1} w_j x^j$ and all $u_i, w_j \in R$. Then

$$\begin{aligned} f &\equiv (g + p^{k-\sigma}u)(h + p^{k-\sigma}w) \bmod p^k \\ &\Leftrightarrow p^{k-\sigma}(uh + wg) - p^{2k-2\sigma}uw \equiv 0 \bmod p^k \\ &\Leftrightarrow uh + wg \equiv 0 \bmod p^\sigma \\ &\Leftrightarrow S(g,h)\begin{pmatrix} w_{m-1} \\ \vdots \\ w_0 \\ u_{n-1} \\ \vdots \\ u_0 \end{pmatrix} \equiv 0 \bmod p^\sigma. \end{aligned}$$

Since $\sigma = -v_p(S(g,h)^{-1})$, there is a column in the matrix $p^\sigma S(g,h)^{-1} \in R^{(n+m)\times(n+m)}$ with an entry not divisible by p. Let i be a number of such a column. Then $1 \le i \le n+m$, and by Lemma 5.3 there exists a solution of the equation

$$uh + wg \equiv p^\sigma x^{i-1} \bmod p^{\sigma+1}$$

with $\deg u < n$ and $\deg w < m$. This means that

$$\begin{pmatrix} w_{m-1} \\ \vdots \\ w_0 \\ u_{n-1} \\ \vdots \\ u_0 \end{pmatrix} \equiv p^\sigma S(g,h)^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \bmod p^{\sigma+1}.$$

By assumption the ith column of $p^\sigma S(g,h)^{-1}$ is not divisible by p, so the vector of the coefficients of u and w is not divisible by p. Hence we can take $\varphi_k = u$ and $\psi_k = w$. □

The improvement of Theorem 3.5 by Theorem 5.5 also yields an improvement of Algorithm 4.6. We can substitute r by s whenever it occurs and thus reduce the running time in cases like that of Example 5.6. But since we have no general upper bound for $s(g,h)$ other than $\frac{d(f)}{2}$ (if $f \equiv gh \bmod p^k$), which is the same as for $r(g,h)$, this does not yield an improvement for the asymptotic running time of the algorithm.

References

A. V. Aho, J. E. Hopcroft, and J. D. Ullman, *The Design and Analysis of Computer Algorithms.* Addison-Wesley, Reading MA, 1974.

E. Bach, Number-theoretic algorithms. *Ann. Rev. Comput. Sci.* **4** (1990), 119–172.

E. R. Berlekamp, Factoring polynomials over large finite fields. *Math. Comp.* **24** (1970), 713–735.

D. Bini and V. Pan, *Polynomial and matrix computations*, vol. 1. Birkhäuser, 1994.

Z. I. Borevich and I. R. Shafarevich, *Number Theory.* Academic Press, 1966.

A. L. Chistov, Efficient factorization of polynomials over local fields. *Soviet Math. Dokl.* **35**(2) (1987), 430–433.

A. L. Chistov, Algorithm of polynomial complexity for factoring polynomials over local fields. *J. Math. Sciences* **70**(4) (1994), 1912–1933.

T. J. Chou and G. E. Collins, Algorithms for the solution of systems of linear Diophantine equations. *SIAM J. Comput.* **11**(4) (1982), 687–708.

P.M. Cohn, *Algebra*, vol. 2. John Wiley & Sons, 1977.

G. E. Collins, The calculation of multivariate polynomial resultants. *J. Assoc. Comput. Mach.* **18** (1971), 515–532.

D. Coppersmith and S. Winograd, Matrix multiplication via arithmetic progressions. *J. Symb. Comp.* **9** (1990), 251–280.

J. von zur Gathen, Hensel and Newton methods in valuation rings. *Math. Comp.* **42** (1984), 637–661.

J. von zur Gathen and S. Hartlieb, Factorization of polynomials modulo small prime powers. Technical report, Universität-GH Paderborn, 1996. To appear.

J. von zur Gathen and V. Shoup, Computing Frobenius maps and factoring polynomials. *Comput complexity* **2** (1992), 187–224.

C. S. Iliopoulos, Worst-case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the Hermite and Smith normal forms of an integer matrix. *SIAM J. Comput.* **18**(4) (1989), 658–669.

E. Kaltofen and V. Shoup, Subquadratic-time factoring of polynomials over finite fields. In *Proc. 27th Annual ACM Symp. Theory of Computing*. ACM Press, 1995, 398–406.

E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders, Parallel algorithms for matrix normal forms. *Linear Algebra and Appl.* **136** (1990), 189–208.

A. K. Lenstra and H. W. Lenstra, Jr., ed., *The development of the number field sieve*, Lecture Notes in Mathematics **1554**. Springer, 1993.

A. K. Lenstra and H. W. Lenstra, Jr, Algorithms in number theory. In *Handbook of Theoretical Computer Science*, ed. J. van Leeuwen, vol. A, 673–715. Elsevier, Amsterdam, 1990.

A. Schönhage, Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf.* **7** (1977), 395–398.

A. Schönhage and V. Strassen, Schnelle Multiplikation großer Zahlen. *Computing* **7** (1971), 281–292.

A. Shamir, On the generation of polynomials which are hard to factor. In *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing*, 1993, 796–804.

M. O. Vahle, Solving the congruence $x^2 \equiv a \bmod n$. *MapleTech* **9** (1993), 69–76.