J. Symbolic Computation (1998) **26**, 583–606
Article No. sy980228

Factoring Modular Polynomials

JOACHIM VON ZUR GATHEN† AND SILKE HARTLIEB†

Fachbereich 17 Mathematik–Informatik,
Universität-GH Paderborn, 33095 Paderborn, Germany

This paper gives an algorithm to factor a polynomial f (in one variable) over rings like $\mathbb{Z}/r\mathbb{Z}$ for $r \in \mathbb{Z}$ or $\mathbb{F}_q[y]/r\mathbb{F}_q[y]$ for $r \in \mathbb{F}_q[y]$. 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 be either $\mathbb{Z}$ or $\mathbb{F}_q[y]$, where $\mathbb{F}_q$ is a finite field containing q elements, and let $r \in R$ be a non-zero non-unit. 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 known that the number of irreducible factors of a polynomial can be exponential in the length of the polynomial, defined in the natural way. An overview on the special case of finding square roots in $R/(r)$ is given in Vahle (1993).

In Sections 2 and 3, the factorization problem is reduced by the Chinese Remainder Theorem and a generalization of 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. Our main result is an algorithm in Section 4 for finding **all** irreducible factorizations if $r = p^k$ is a prime power. It only works when the discriminant of the polynomial is not divisible by p^k. In particular, the polynomial to be factored must be square-free. There may exist exponentially many irreducible factors, but we provide in polynomial time a

†E-mail: {gathen,hartlieb}@uni-paderborn.de

0747–7171/98/110583 + 24 $30.00/0

concise data structure that describes all of them in a simple way. Our description is a considerable generalization of the fact that

$$x^2 \equiv (x - \alpha p)(x + \alpha p) \bmod p^2 \tag{1.1}$$

for all $\alpha \in \{0, 1, \ldots, p-1\}$.

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 $R_{(p)}$. If the discriminant vanishes, i.e. the polynomial is not squarefree, this task 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 do not know how to solve this problem in polynomial time. This reduction to nonzero discriminant does not work for finding all factorizations (Example 4.13).

We need two properties of the unique factorization domain 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, that is, K is a field complete with respect to a discrete valuation such that the residue class field is finite (see, for example, Cassels (1986)). Then we can use Chistov's (1987, 1994) algorithm for factoring polynomials over local fields. This algorithm is quite complicated, but its running time is analysed (though not in detail). There is another algorithm by Ford–Zassenhaus for factoring polynomials over complete local Dedekind rings (see Ford (1987)). This algorithm is easier to understand, but as far as we know its running time has not been analysed yet. The algorithm is implemented for $R = \mathbb{Z}$ in the computer algebra system MAGMA and performs very well. We rely on Chistov's algorithm, but any algorithm which runs in (probabilistic) polynomial time works as well.

We did not analyse the running time of our algorithm in detail, because there is no detailed analysis of Chistov's algorithm. It is clear that all steps of the algorithm can be done in probabilistic polynomial time. In fact, our algorithm can be viewed as a probabilistic polynomial time reduction from factoring over $R/(p^k)$ to factoring over $R_{(p)}$.

2. The Chinese Remainder Theorem

Let $r \in R$ be a non-zero non-unit, and

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

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

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

Let $f \in R[x]$ correspond via the Chinese Remainder isomorphism to $(f_1, \ldots, f_s)$. If $i \neq j$ and f_i and f_j are non-units over $R/(p_i^{k_i})$ and $R/(p_j^{k_j})$, respectively, then we can write

$$(f_1, \ldots, f_s) = (1, \ldots, 1, f_i, 1, \ldots, 1) \cdot (f_1, \ldots, f_{i-1}, 1, f_{i+1}, \ldots, f_s),$$

and both factors are non-units over $R/(r)$. Hence f is reducible. It follows that if f is irreducible over $R/(r)$ (that is, its residue class modulo r is irreducible in $R/(r)[x]$), then there is at most one $i \leq s$ such that f_i is a non-unit over $R/(p_i^{k_i})$. In fact, f_i is irreducible in $R/(p_i^{k_i})[x]$. On the other hand, there is at least one such $i \leq s$, because otherwise f would be a unit over $R/(r)$. So the irreducible polynomials $f \in R[x]$ over $R/(r)$ are, up to multiplication by units, of the form

$$f = (1, \ldots, 1, f_i, 1, \ldots, 1), \tag{2.2}$$

where for some $1 \leq i \leq s$ all entries but the ith are 1, and $f_i \in R[x]$ is an irreducible polynomial 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, namely x, has a surprising factorization.

EXAMPLE 2.1. (SHAMIR, 1993) *Let $r = pq$ for different (non-associate) 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.

If $f \equiv 0 \bmod p_i^{k_i}$ for some $i \leq s$, then f is not irreducible, since $(f_1, \ldots, f_s) = (1, \ldots, 1, x, 1, \ldots, 1) \cdot (f_1, \ldots, f_s)$ is a factorization in which none of the two factors is invertible. In the presence of zerodivisors we sometimes have no factorization of f into irreducible factors at all, since in the example $R = \mathbb{Z}$, $f = 4x$, and $r = 6$. But we are not ready to give up at this point, as it seems that only the constants cause the difficulties. The subtleties of this question are illustrated by the fact that $2 \equiv 2 \cdot 4 \bmod 6$ is not irreducible modulo 6, but 2 is irreducible modulo 12, by (2.2) and its irreducibility modulo 4. We write $f = (\prod_{1 \leq i \leq s} p_i^{l_i}) \cdot g$ with $l_i = 0$ or $l_i \geq k_i$ and $g \not\equiv 0 \bmod p_i$ for all $i \leq s$ such that $l_i \geq k_i$. Now we factor g into irreducible factors modulo r, say $g \equiv g_1 \ldots g_t \bmod r$, where all $g_i \in R[x]$ are irreducible over $R/(r)$. Then the factorization of f is $f \equiv (\prod_{1 \leq i \leq s} p_i^{l_i}) g_1 \ldots g_t \bmod r$. In the example above, where $R = \mathbb{Z}$, $f = 4x$ and $r = 6$, this yields the factorization $f \equiv 2^2(4x + 3)(3x + 4) \bmod 6$, in which the constant 2 is not irreducible. But the only reducible factors that appear are constants, and in this case there is no factorization of these constants (or f) into irreducible factors. The example $R = \mathbb{Z}$, $f = 4x$, and $r = 12$, in which we have the factorization $f \equiv 2^2(4x + 9)(9x + 4) \bmod 12$, shows that sometimes we obtain in this way factorizations in which all factors are irreducible. Thus we will assume from now on that no $p_i^{k_i}$ divides f, and will extract powers $p_i^{l_i}$ with $l_i < k_i$ in Proposition 3.15.

By Corollary 3.17 below, we know that every polynomial $f \in R[x]$ with $f \not\equiv 0 \bmod p^k$ for a prime p and $k \in \mathbb{N}$ has a factorization into irreducible factors over $R/(p^k)$. The main purpose of this paper is to show how all factorizations of f over $R/(p^k)$ into irreducible factors can be computed. 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. Currently, the asymptotically fastest (probabilistic) algorithms use $O((n^2 + n \log q)(\log n)^2 \operatorname{loglog} n)$ operations in $\mathbb{F}_q$ (von zur Gathen and Shoup, 1992) or $O(n^{1.815} \log q)$ operations in $\mathbb{F}_q$ (Kaltofen and Shoup, 1995) for factoring a polynomial of degree n. Hence we obtain the following:

PROPOSITION 2.2. *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 $p \in R$ and $k \in \mathbb{N}$.*

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

The following proposition is from Shamir (1993) and shows that our assumption of knowing the factorization is indeed necessary. We state it only for the case that $R = \mathbb{Z}$.

PROPOSITION 2.3. (SHAMIR, 1993) *There is a polynomial-time reduction from the problem of factoring $r \in \mathbb{Z}$ to the problem of factoring polynomials over $\mathbb{Z}/r\mathbb{Z}$.*

Finally, we state a corollary of the Chinese Remainder Theorem which follows directly from (2.2). When we count irreducible factors, we really should count classes of associate factors that differ only by an invertible multiplier.

COROLLARY 2.4. *Let the complete factorization of $r \in R$ be $r = u \prod_{1 \le i \le s} p_i^{k_i}$ as in (2.1), and $f \in R[x]$ with $f \not\equiv 0 \bmod p_i^{k_i}$ for all i. An irreducible factor of f over $R/(r)$ corresponds to an irreducible factor of f modulo $p_i^{k_i}$ for some $i \le s$ as in (2.2). An irreducible factorization of f over $R/(r)$ corresponds to an irreducible factorization of f modulo each $p_i^{k_i}$. In particular, the number of classes of irreducible factors of f over $R/(r)$ is the sum over all i of the numbers of classes of irreducible factors of f over $R/(p_i^{k_i})$, and the number of irreducible factorizations of f over $R/(r)$ is the product over all i of the corresponding number over $R/(p_i^{k_i})$.*

3. A Generalization of Hensel's Lemma

From now on, we assume that $r = p^k$ for some prime $p \in R$ and $k \ge 1$ and that our polynomials in $R[x]$ are not divisible by p^k. Figure 1 shows the *Sylvester matrix* $S(g, h)$ of two polynomials $g, h \in R[x]$ with degrees n and m, and $g = \sum_{0 \le i \le n} g_i x^i$ and $h = \sum_{0 \le j \le m} h_j x^j$. (Sometimes the transpose of this matrix is called the Sylvester matrix.) By definition, the resultant of the two polynomials is $\operatorname{res}(g, h) = \det S(g, h)$.

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 $a, b \in R$ with $b \neq 0$. The p-adic valuation induces an absolute value $|.|_p$ on K by setting $|a|_p = p^{-v_p(a)}$ for $a \neq 0$, and $|0|_p = 0$. By $K_{(p)}$ we denote the completion of K with respect to this

$$S(g,h) = \begin{pmatrix} f_n & & & & g_m & & & \\ f_{n-1} & f_n & & & g_{m-1} & g_m & & \\ \vdots & \vdots & \ddots & & \vdots & \vdots & \ddots & \\ \vdots & \vdots & & f_n & g_1 & \vdots & & \ddots \\ \vdots & \vdots & & f_{n-1} & g_0 & \vdots & & \\ \vdots & \vdots & & \vdots & & g_0 & & g_m \\ f_0 & \vdots & & \vdots & & & \ddots & \vdots \\ & f_0 & & \vdots & & & & \vdots \\ & & \ddots & \vdots & & & & \vdots \\ & & & f_0 & & & & g_0 \end{pmatrix}$$

m n

Figure 1. The Sylvester matrix.

absolute value. 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 $K_{(p)} = \mathbb{F}_q((y))$ is the field of formal Laurent series in 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 $A = (a_{ij})_{i,j} \in K_{(p)}^{n \times m}$ as:

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

The p-adic value of a vector is defined in the same way. For more information about valuation theory, see e.g. Cohn (1977, Chapter 9).

Before discussing the factorization of polynomials over $R/(p^k)$, we describe the invertible elements in the ring $R/(p^k)[x]$. In contrast to polynomial rings over fields, our rings have invertible elements which are not constant.

LEMMA 3.1. *Let $f \in R[x]$. Then f is invertible over $R/(p^k)$ if and only if f is invertible over $R/(p)$.*

PROOF. Let f be invertible over $R/(p^k)$. Then clearly f is also invertible over $R/(p)$. Now let f be invertible over $R/(p)$, i.e. there exists a polynomial $g_1 \in R[x]$ such that $fg_1 \equiv 1 \bmod p$. Now Newton Iteration shows that for all $k \geq 1$ there exists $g_k \in R[x]$ such that $fg_k \equiv 1 \bmod p^k$. □

NOTATION 3.2. *Let $g, h \in R[x]$ be monic. Then $d(g) = v_p(\mathrm{disc}(g))$, where* $\mathrm{disc}(g) =$

$\operatorname{res}(g, g') \in R$ *is the discriminant of* g, $r(g,h) = v_p(\operatorname{res}(g,h))$, *and if* $\operatorname{res}(g,h) \neq 0$, *then* $s(g,h) = -v_p(S(g,h)^{-1})$.

LEMMA 3.3. *Let* $g, h \in R[x]$ *with* $\operatorname{res}(g,h) \neq 0$. *Then*

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

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

PROOF. Since $\operatorname{res}(g,h) = \det S(g,h)$, the adjoint $A = \operatorname{res}(g,h)S(g,h)^{-1}$ of $S(g,h)$ is a matrix over R and has nonnegative p-adic value. Hence, $r(g,h) - s(g,h) = v_p(A) \geq 0$. 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 $\operatorname{res}(g,h) \in R$.

If $s(g,h) = 0$, then $S(g,h)$ is invertible over $R_{(p)}$, and hence $\operatorname{res}(g,h)$ is invertible over $R_{(p)}$. It follows that $r(g,h) = 0$. □

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

EXAMPLE 3.4. *Let* $R = \mathbb{Z}$, $p = 3$, $g = x^2 + 3$, *and* $h = x^3 + 9x^2 + 12x + 27$. *Then*

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

Thus $\operatorname{res}(g,h) = 3^5$, $r(g,h) = 5$, *and* $s(g,h) = 3$.

REMARK 3.5. The running time of our method is proportional to $s(g,h)$. Our algorithm and all the following statements (except Theorem 4.2) also work when $s(g,h)$ is replaced by $r(g,h)$. We have no better general bounds on $s(g,h)$ than on $r(g,h)$ and thus our asymptotic time estimates would not be affected. But Lemma 3.3, Example 3.4, and Example 3.9 show that for individual polynomials the use of $s(g,h)$ may be advantageous.

The proof of the following proposition is analogous to the proof of the Lemma in Borevich and Shafarevich (1966, Chapter 4, Section 3). We substitute the value $r(g,h)$ in their version by the sometimes smaller value $s(g,h)$.

PROPOSITION 3.6. *Let* $g, h \in R[x]$ *have degrees* n, m, *respectively, and* $\operatorname{res}(g,h) \neq 0$. *Let* $l \in R_{(p)}[x]$ *with* $\deg l < n + m$. *Then there exist uniquely determined polynomials* $\varphi, \psi \in R_{(p)}[x]$ *with* $\deg \varphi < m$ *and* $\deg \psi < n$ *such that*

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

PROOF. Write $l = \sum_{0 \leq i < n+m} l_i x^i$ with all $l_i \in R_{(p)}$. 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 $R_{(p)}$

(namely, the coefficients of the two polynomials) such that

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

Since $\operatorname{res}(g,h) \neq 0$, the matrix $S(g,h)$ is invertible over the quotient field of $R_{(p)}$, and (3.2) is equivalent to

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

The entries of $p^{s(g,h)}S(g,h)^{-1}$ are in $R_{(p)}$, and so are 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). □

Often, it suffices to compute polynomials $\varphi, \psi \in R[x]$ with $\deg\varphi < m$ and $\deg\psi < n$ such that $p^{s(g,h)}l \equiv \varphi g + \psi h \bmod p^{s(g,h)+1}$. As in the proof of Proposition 3.6, the solutions correspond to the solutions of the congruence

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

REMARK 3.7. Let $g, h, l \in R[x]$ be as in Proposition 3.6. In order to compute $\varphi, \psi \in R[x]$ such that $\deg\varphi < m, \deg\psi < n$ and $p^{s(g,h)}l \equiv \varphi g + \psi h \bmod p^{s(g,h)+1}$, it suffices to determine $S(g,h) \bmod p^{s(g,h)+1}$.

Another description of $s(g,h)$ is given in the next lemma.

LEMMA 3.8. *Let $g, h \in R[x]$ with $\operatorname{res}(g,h) \neq 0$ and at least one of $lc(g), lc(h)$ not divisible by p. Then $s(g,h)$ is minimal with the property that there exist polynomials $a, b \in R_{(p)}[x]$ such that $ag + bh = p^{s(g,h)}$.*

PROOF. Proposition 3.6 shows that there exist polynomials $a, b \in R_{(p)}[x]$ such that $ag + bh = p^{s(g,h)}$. It remains to show that $s(g,h)$ is minimal with this property.

Let $\deg g = n$, $\deg h = m$, and $a', b' \in R_{(p)}[x]$ be such that $a'g + b'h = p^{\sigma}$ for some

$\sigma \geq 0$. We choose one of g, h with leading coefficient not divisible by p, say g. Then $\mathrm{lc}(g)$ is a unit in $R_{(p)}$, and we can divide b' by g with remainder: $b' = qg + b''$ with $q, b'' \in R_{(p)}[x]$ and $\deg b'' < n$. If we set $a'' = a' + qh$, then $a''g + b''h = p^\sigma$ and $\deg a'' < m$. In other words, we may assume that $\deg a' < m$ and $\deg b' < n$. Then there exists for all $l \in R[x]$ with $\deg l < n + m$ polynomials $a_l, b_l \in R_{(p)}[x]$ such that $a_l g + b_l h = p^\sigma l$, and again by division with remainder we may assume that $\deg a_l < m$, $\deg b_l < n$. Let $a_l = \sum_{0 \leq i < m} \alpha_i x^i$, $b_l = \sum_{0 \leq i < n} \beta_i x^i$, $l = \sum_{0 \leq i < n+m} l_i x^i$, where all $\alpha_i, \beta_i \in R_{(p)}$, and all $l_i \in R$. Then

$$S(g,h) \begin{pmatrix} \alpha_{m-1} \\ \vdots \\ \alpha_0 \\ \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix} = p^\sigma \begin{pmatrix} l_{n+m-1} \\ \vdots \\ \vdots \\ \vdots \\ l_0 \end{pmatrix},$$

and therefore

$$\begin{pmatrix} \alpha_{m-1} \\ \vdots \\ \alpha_0 \\ \beta_{n-1} \\ \vdots \\ \beta_0 \end{pmatrix} = p^\sigma S(g,h)^{-1} \begin{pmatrix} l_{n+m-1} \\ \vdots \\ \vdots \\ \vdots \\ l_0 \end{pmatrix}.$$

Using successively all monomials x^i with $i = 0, \ldots, n+m-1$ for l, we obtain that $p^\sigma S(g,h)^{-1}$ is a matrix over $R_{(p)}$, and hence $s(g,h) \leq \sigma$. □

Without the condition on the leading coefficients, $s(g,h)$ may fail to be minimal, as shown by the example $g = p^k x + 2$, $h = p^k x + 1$, where $g - h = 1$ and $s(g,h) = r(g,h) = k$.

EXAMPLE 3.9. *This example shows that the difference between $r(g,h)$ and $s(g,h)$ may become arbitrarily large. Let $R = \mathbb{Z}$, $n \geq 1$, $g = x^{2^n} + 1$, $h = x^{2^{n-1}} - 1$, and $p = 2$. Then $r(g,h) = 2^{n-1}$ (Apostol, 1970, Proof of Theorem 2). In particular, $r(g,h) \geq 1$, and hence $s(g,h) \geq 1$. On the other hand,*

$$(x^{2^n} + 1) - (x^{2^{n-1}} + 1)(x^{2^{n-1}} - 1) = 2,$$

and by Lemma 3.8 we have $s(g,h) \leq 1$. Thus $s(g,h) = 1$.

LEMMA 3.10. *Let $g, h, g', h' \in R[x]$ be such that $\mathrm{res}(g,h) \neq 0$, $g' \equiv g \bmod p^{s(g,h)+1}$, $h' \equiv h \bmod p^{s(g,h)+1}$, $\deg g = \deg g'$, $\deg h = \deg h'$, and at least one of $\mathrm{lc}(g')$, $\mathrm{lc}(h')$ is not divisible by p. Then $s(g',h') = s(g,h)$.*

PROOF. Let $\sigma = s(g,h)$, and assume first that $\mathrm{res}(g',h') = 0$. Then $S(g',h')$ is not invertible, and there is a vector $b \in R^{n+m}$ such that $S(g',h')b = 0$, and $b \not\equiv 0 \bmod p$. Hence there are polynomials $\varphi, \psi \in R[x]$ such that $\deg \varphi < m = \deg h$, $\deg \psi < n = \deg g$, and

$$\varphi g' + \psi h' = 0,$$

with $\varphi \not\equiv 0 \bmod p$ or $\psi \not\equiv 0 \bmod p$. But then $\varphi g + \psi h \equiv 0 \bmod p^{\sigma+1}$. Hence $\varphi g + \psi h = p^{\sigma+1} l$ for a polynomial $l \in R[x]$ with $\deg l < n+m$. By Proposition 3.6 there exist unique solutions φ', ψ' of the equation $\varphi' g + \psi' h = p^\sigma l$ with $\deg \varphi' < m$ and $\deg \psi' < n$. Then the unique solutions φ, ψ of $\varphi g + \psi h = p^{\sigma+1} l$ with $\deg \varphi < m$ and $\deg \psi < n$ are $\varphi = p\varphi'$ and $\psi = p\psi'$, a contradiction. Hence, $\operatorname{res}(g', h') \neq 0$, and $s(g', h')$ is defined.

By Proposition 3.6, there exist polynomials $\varphi, \psi \in R_{(p)}[x]$ with $\deg \varphi < m$ and $\deg \psi < n$ such that $\varphi g + \psi h = p^\sigma$. It follows that $\varphi g' + \psi h' \equiv p^\sigma \bmod p^{\sigma+1}$. Let $\varphi g' + \psi h' = p^\sigma + p^{\sigma+1} l'$ with $l' \in R_{(p)}[x]$. Then $\varphi g' + \psi h' = p^\sigma (1 + pl')$, and $(1 + pl')$ is invertible over $R/(p^k)$ for every $k \geq 1$. Hence there exist polynomials $a, b \in R[x]$ such that $ag' + bh' \equiv p^\sigma \bmod p^{s(g',h')+1}$. Now assume that $\sigma < s(g', h')$. Then $p^{s(g',h')-\sigma} ag' + p^{s(g',h')-\sigma} bh' \equiv p^{s(g',h')} \bmod p^{s(g',h')+1}$. Thus there exists an $l' \in R[x]$ such that

$$p^{s(g',h')-\sigma} ag' + p^{s(g',h')-\sigma} bh' = p^{s(g',h')}(1 + pl').$$

Let $a = \sum_{0 \leq i < m} a_i x^i$, $b = \sum_{0 \leq i < n} b_i x^i$, and $l' = \sum_{0 \leq i < n+m} l_i x^i$ with all $a_i, b_i, l_i \in R$. Then

$$S(g', h') \begin{pmatrix} p^{s(g',h')-\sigma} a_{m-1} \\ \vdots \\ p^{s(g',h')-\sigma} a_0 \\ p^{s(g',h')-\sigma} a_{m-1} b_{n-1} \\ \vdots \\ p^{s(g',h')-\sigma} b_0 \end{pmatrix} = p^{s(g',h')} \begin{pmatrix} pl_{n+m-1} \\ \vdots \\ \vdots \\ \vdots \\ pl_1 \\ 1 + pl_0 \end{pmatrix},$$

hence

$$p^{s(g',h')-\sigma} \begin{pmatrix} a_{m-1} \\ \vdots \\ a_0 \\ b_{n-1} \\ \vdots \\ b_0 \end{pmatrix} = p^{s(g',h')} S(g', h')^{-1} \begin{pmatrix} pl_{n+m-1} \\ \vdots \\ \vdots \\ pl_1 \\ 1 + pl_0 \end{pmatrix}. \tag{3.3}$$

We are done if we can show that the last column of $p^{s(g',h')} S(g', h')^{-1}$ is not divisible by p, because then the right-hand side of (3.3) is not divisible by p, whereas the left-hand side obviously is. This contradiction proves that $\sigma \geq s(g', h')$. In the same way we can then show that $\sigma \leq s(g', h')$.

So, assume that the last column of $p^{s(g',h')} S(g', h')^{-1}$ is divisible by p. Then

$$p^{s(g',h')-1} S(g', h')^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in R_{(p)}^{n+m},$$

say

$$p^{s(g',h')-1}S(g',h')^{-1}\begin{pmatrix}0\\ \vdots\\ \vdots\\ 0\\ 1\end{pmatrix}=\begin{pmatrix}a_{m-1}\\ \vdots\\ a_0\\ b_{n-1}\\ \vdots\\ b_0\end{pmatrix}.$$

With $a=\sum_{0\le i<m}a_ix^i\in R_{(p)}[x]$ and $b=\sum_{0\le i<n}b_ix^i\in R_{(p)}[x]$ we have that $ag'+bh'=p^{s(g',h')-1}$, a contradiction to Lemma 3.8. □

The basic tool for lifting factorizations modulo higher powers of p is Hensel's Lemma. It was invented by Gauß (published posthumously in 1863). Cauchy (1847) also states a correct version, but draws the incorrect conclusion that f cannot have more than $\deg f$ many roots modulo p^k (Théorème IX, p. 330). A simple counterexample is given in (1.1).

The next theorem is a more general version of Hensel's Lemma. The usual version assumes $s(g_0,h_0)=0$ instead of (c), and the one in Borevich and Shafarevich (1966) replaces (d) by $k>2r(g_0,h_0)$.

THEOREM 3.11. *Let $p\in R$ be a prime, $k\in\mathbb{N}$ and $f,g_0,h_0\in R[x]$ be polynomials of degrees $n+m,n,m$, respectively, with the following properties:*

(a) $f\equiv g_0h_0 \bmod p^k$,
(b) the leading coefficients of f and g_0h_0 are equal, and at least one of $\mathrm{lc}(g_0)$, $\mathrm{lc}(h_0)$ *is not divisible by p,*
(c) the resultant $\mathrm{res}(g_0,h_0)$ *is nonzero,*
(d) $k>2s(g_0,h_0)$.

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

$$f=gh \text{ in } R_{(p)}[x],\quad g\equiv g_0 \bmod p^{k-s(g_0,h_0)},\quad h\equiv h_0 \bmod p^{k-s(g_0,h_0)},$$

and the leading coefficients of g and h equal those of g_0 and h_0, respectively.

PROOF. Let $\sigma=s(g_0,h_0)$. Using induction on i, it is sufficient to construct for $i\ge 1$ polynomials $\varphi_i,\psi_i\in R[x]$ with $\deg\varphi_i<m$, $\deg\psi_i<n$ such that if

$$f\equiv ab \bmod p^{k+i-1} \tag{3.4}$$

with $a,b\in R[x]$ such that $a\equiv g_0 \bmod p^{k-\sigma}$ and $b\equiv h_0 \bmod p^{k-\sigma}$, and $\mathrm{lc}(a)=\mathrm{lc}(g_0)$, $\mathrm{lc}(b)=\mathrm{lc}(h_0)$, then

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

Here lc denotes the leading coefficient. We rewrite (3.4) as

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

with $l\in R[x]$ and $\deg l<n+m$, because $\mathrm{lc}(ab)=\mathrm{lc}(f)$. Since $a\equiv g_0 \bmod p^{k-\sigma}$, $b\equiv h_0 \bmod p^{k-\sigma}$, and $k-\sigma>\sigma$, we have by Lemma 3.10 that $\sigma=s(g_0,h_0)=s(a,b)$.

By Proposition 3.6 there exist polynomials $\varphi_i, \psi_i \in R[x]$ of degrees less than m, n, respectively, such that

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

Then

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

where $2(k+i-1) - 2\sigma \geq k+i$.

Put together, we have for the polynomials $g = g_0 + \sum_{i\geq 1} p^{k-\sigma+i-1}\psi_i \in R_{(p)}[x]$ and $h = h_0 + \sum_{i\geq 1} p^{k-\sigma+i-1}\varphi_i \in R_{(p)}[x]$ that $f = gh$. Furthermore, $g \equiv g_0 \bmod p^{k-\sigma}$ and $h \equiv h_0 \bmod p^{k-\sigma}$.

Assume that $f = gh = g'h'$ in $R_{(p)}[x]$ with $g \equiv g' \equiv g_0 \bmod p^{k-s(g_0,h_0)}$ and $h \equiv h' \equiv h_0 \bmod p^{k-s(g_0,h_0)}$. Let $g' = g + p^{k-s(g_0,h_0)}a$ and $h' = h + p^{k-s(g_0,h_0)}b$ with $a, b \in R_{(p)}[x]$. Then

$$gh = g'h' = (g+p^{k-s(g_0,h_0)}a)(h+p^{k-s(g_0,h_0)}b) = gh+p^{k-s(g_0,h_0)}(bg+ah)+p^{2k-2s(g_0,h_0)}ab.$$

It follows that $bg + ah \equiv 0 \bmod p^{k-s(g_0,h_0)}$, and by Proposition 3.6 and Lemma 3.10 we have $a \equiv b \equiv 0 \bmod p^{k-2s(g_0,h_0)}$. Hence $g \equiv g' \bmod p^{2k-3s(g_0,h_0)}$ and $h \equiv h' \bmod p^{2k-3s(g_0,h_0)}$, where $2k - 3s(g_0,h_0) > k - s(g_0,h_0)$. Inductively, one can now show that $g = g'$, and $h = h'$. □

A version of Theorem 3.11 is already proven in von zur Gathen (1984) in a different setting. In particular, no explicit formula for $s(g,h)$ is given from which to compute $s(g,h)$ given g and h. In Böffgen and Reichert (1987) the "reduced resultant" of two polynomials $g, h \in \mathbb{Z}[x]$ is defined as the ideal $(g\mathbb{Z}[x] + h\mathbb{Z}[x]) \cap \mathbb{Z}$ in $\mathbb{Z}$. Let $s'(g,h)$ be the p-adic value of a generator of this ideal. Then Lemma 3.8 shows that $s'(g,h) = s(g,h)$. Theorem 3.11 was also proven in Böffgen and Reichert (1987) in this setting.

COROLLARY 3.12. *Assume that conditions (a), (b), and (c) of Theorem 3.11 hold. Then condition (d) is true if $k > d(f)$.*

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

$$\operatorname{disc}(f) = \operatorname{disc}(gh) = \operatorname{disc}(g)\operatorname{disc}(h)\operatorname{res}(g,h)^2 \tag{3.5}$$

(see Borevich and Shafarevich (1966, Chapter 4, Section 3)). Using Lemma 3.3, we have

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

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 3.13. It follows from Remark 3.7 that in order to apply Theorem 3.11 it suffices to know $S(g_0,h_0) \bmod p^{s(g_0,h_0)+1}$.

The following corollary describes the relation between irreducible polynomials over

$R/(p)$ and irreducible polynomials over $R/(p^k)$. When p does not divide f, this is Theorem XIII.7 of McDonald (1974).

COROLLARY 3.14. *Let $f \in R[x]$. If f is irreducible over $R/(p)$, then f is irreducible over $R/(p^k)$ for all $k \geq 1$. If f is irreducible over $R/(p^k)$ for some $k \geq 1$, then either $f \equiv \nu g^e \bmod p$ with $e \geq 1$, $g \in R[x]$ irreducible over $R/(p)$, and $\nu \in R$ a unit modulo p, or $k \geq 2$ and $f = \nu p$ with $\nu \in R[x]$ a unit modulo p.*

PROOF. The first part of the claim is clear. For the second part, let $f \not\equiv 0 \bmod p$. If $f \equiv gh \bmod p$, where $g, h \in R[x]$ are non-units over $R/(p)$ which are relatively prime over $R/(p)$ (i.e. $s(g,h) = 0$), then f is reducible by Theorem 3.11. Hence $f \equiv \nu g^e \bmod p$, where $\nu \in R$ is a unit modulo p, and $g \in R[x]$ is irreducible over $R/(p)$. It remains to show that if $f \equiv 0 \bmod p$, and f is irreducible, then $f = \nu p$ as in the claim of the corollary. First, we show that p is irreducible over $R/(p^k)$ for $k \geq 2$. Assume that $p = ab \bmod p^k$ with $a, b \in R[x]$. Then $p|ab$, and since p is a prime, we have $p|a$ or $p|b$. Let $a = pa'$ with $a' \in R[x]$. Then $p|(a'b - 1)$, and hence $a'b \equiv 1 \bmod p$ and a' and b are invertible over $R/(p^k)$. This shows that p is irreducible. On the other hand, if $f \equiv 0 \bmod p$, then $p|f$, so if f is irreducible, then $f = \nu p$ with ν invertible modulo p^k. □

May we assume, as is customary over a field, our polynomial to be monic? Examples like $3x^2 + x + 3 \in \mathbb{Z}/(27)[x]$ cast some doubt, but it is a pleasant fact that the assumption may indeed be made.

PROPOSITION 3.15. *Let $f \in R[x]$, and $k \geq 1$. Then there exist $l \in \mathbb{N}$ and $\nu, m \in R[x]$ such that ν is a unit over $R/(p^k)$, m is monic and $f \equiv p^l \nu m \bmod p^k$. The irreducible factors of f are p (if $l \geq 1$) plus the irreducible factors of m over $R/(p^{k-l})$.*

PROOF. We write $f \equiv p^l g \bmod p^k$ with $g \not\equiv 0 \bmod p$, and may assume that $l < k$. We let $n = \deg g$ and $m = \deg(g \bmod p)$. If $n = m$, we set $\nu_0 = \mathrm{lc}(g)$, and if $m < n$, we set $\nu_0 = \mathrm{lc}(g)x^{n-m} + g_m$, where $g_m \in R$ is the coefficient of x^m in g. Then $g_m \not\equiv 0 \bmod p$. In either case, ν_0 is a unit modulo p, and there is a monic polynomial $m_0 \in R[x]$ such that $g \equiv \nu_0 m_0 \bmod p$, $\mathrm{lc}(g) = \mathrm{lc}(\nu_0 m_0)$ and $\deg g = \deg \nu_0 + \deg m_0$. As ν_0 is a unit over $R/(p)$, we have $s(\nu_0, m_0) = 0$. By Theorem 3.11 there exist $\nu, m \in R[x]$ such that $g \equiv \nu m \bmod p^{k-l}$, $\nu \equiv \nu_0 \bmod p$, $m \equiv m_0 \bmod p$, and $\mathrm{lc}(m) = \mathrm{lc}(m_0)$. This means that ν is a unit over $R/(p^k)$, and m is monic. □

EXAMPLE 3.16. *Let $R = \mathbb{Z}$, $f = 3x^2 + x + 3$, $p = 3$, and $k = 3$. We have*

$$f \equiv x \equiv (3x + 1)x \bmod 3.$$

So we take $l = 0$, $\nu_0 = 3x + 1$, and $m_0 = x$. The application of Theorem 3.11 yields the factorization

$$f \equiv (3x + 19)(x + 3) \bmod 27,$$

where $3x + 19$ is a unit over $\mathbb{Z}/(27)$ (we have $(3x + 1)(9x^2 - 3x + 10) \equiv 1 \bmod 27$), and $x + 3$ is monic.

COROLLARY 3.17. *Let $f \in R[x]$, $p \in R$ a prime and $k \in \mathbb{N}$ such that $f \not\equiv 0 \bmod p^k$. Then there exists always a factorization of f into irreducible factors over $R/(p^k)$.*

PROOF. By Proposition 3.15, we may assume that f is monic. If f is reducible, there exist polynomials $g, h \in R[x]$ such that $f \equiv gh \bmod p^k$, and g and h are non-units over $R/(p^k)$. Then we may again by Proposition 3.15 assume that g and h are monic. But $\deg g, \deg h < \deg f$, and we can recursively factor g and h. This process stops because the degrees of the factors are strictly decreasing and at least one. □

Given $f \in R[x]$ with $f \not\equiv 0 \bmod p^k$, we do the following in order to find the factorizations of f into irreducible factors: we write $f \equiv p^l \nu m \bmod p^k$ with $l < k$, $\nu \in R[x]$ invertible over $R/(p^k)$, and $m \in R[x]$ monic, as in Proposition 3.15. For each irreducible factorization $f \equiv f_1 \ldots f_s \bmod p^k$ of f there exists an irreducible factorization $m \equiv m_1 \ldots m_t \bmod p^{k-l}$ of m such that each f_i is, after multiplication by a unit in $R/(p^k)[x]$, either p or some m_j. Thus we are left with the task to find all factorizations of m into irreducible factors over $R/(p^{k-l})$. In other words, we consider two problems. We call the first one GENERALFACT. The input to this problem consists of a polynomial $f \in R[x]$ and a non-zero non-unit $r \in R$. If $R = \mathbb{Z}$, we require a third input, namely the complete factorization of r into prime power factors. Output are all factorizations of f over $R/(r)$ into irreducible factors. The second problem is SPECIALFACT which has as input a monic polynomial $f \in R[x]$, a prime $p \in R$ and an integer $k \geq 1$. Furthermore, the polynomial f when reduced modulo p is a power of an irreducible plynomial. The output are all factorizations of f over $R/(p^k)$ into irreducible monic factors. Now we have the following reduction:

THEOREM 3.18. *Let $R = \mathbb{F}_q[y]$ or $R = \mathbb{Z}$. There is a probabilistic polynomial-time reduction from* GENERALFACT *over R to* SPECIALFACT *over R.*

PROOF. Let $R = \mathbb{F}_q[x]$ or $R = \mathbb{Z}$. Let $f \in R[x]$ and $r \in R$ be the inputs of GENERALFACT. If $R = \mathbb{Z}$, a complete factorization $r = u \prod_{1 \leq i \leq s} p_i^{k_i}$ as in (2.1) is given as a third input. If $R = \mathbb{F}_q[x]$, such a complete factorization can be computed in probabilistic polynomial time. Hence in both cases the Chinese Remainder Theorem can be applied. For every $i \leq s$ we write $f \equiv p_i^{l_i} \nu_i g_i$ with $l_i \geq 0$, ν_i invertible modulo $p_i^{k_i}$ and $g_i \in R[x]$ monic. We now factor in probabilistic polynomial time g_i over $R/(p_i)$ into monic factors which are relatively prime powers of irreducible polynomials, and Theorem 3.11 then shows that such a factorization can be uniquely lifted to a factorization over $R/(p_i^{k_i})$. Furthermore, this can be done in polynomial time (see Zassenhaus (1969)). It is then sufficient to call SPECIALFACT to factor each lifted factor and apply Corollary 2.4. □

Thus in the sequel we can concentrate on SPECIALFACT.

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

It follows from Theorem 3.11 that if $f \equiv g_k h_k \bmod p^k$ for $k > d(f) = v_p(\mathrm{disc}(f))$, then there exists a factorization $f = gh$ over $R_{(p)}$ such that $g_k \equiv g \bmod p^{k-\sigma}$ and $h_k \equiv h \bmod p^{k-\sigma}$, where $\sigma = s(g, h) \leq d(f)/2$. Hence, any two factorizations of f over $R/(p^k)$ which give rise to the same factorization over $R_{(p)}$ are equal over $R/(p^{k-\sigma})$. In particular, Theorem 3.11 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* $f = \prod_{1 \le i \le l} g_i \in R_{(p)}[x]$ *be monic with* $\operatorname{disc}(f) \neq 0$, $l \geq 1$, *and* $g_1, \ldots, g_l \in R_{(p)}[x]$ *monic and irreducible. 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* $g \equiv \prod_{i \in S} g_i \bmod p^{k-\sigma}$ *and* $h \equiv \prod_{j \in S'} g_j \bmod p^{k-\sigma}$ *with* $\sigma = s(\prod_{i \in S} g_i, \prod_{j \in S'} g_j)$. *In particular, if* g *is irreducible over* $R/(p^k)$, *then there exists* $1 \le i \le l$ *such that* $g \equiv g_i \bmod p^{k - s(g_i, \prod_{j \neq i} g_j)}$.

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 $\tilde g \equiv g \bmod p^{k-s(g,h)}$ and $\tilde h \equiv h \bmod p^{k-s(g,h)}$ by Corollary 3.12 and Theorem 3.11. 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

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

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

$$s(g,h) = s\Big(\prod_{i \in S} g_i, \prod_{j \in S'} g_j\Big)$$

by Lemma 3.10. □

On the other hand, the next theorem shows that $s(g,h)$ is optimal in the sense that if $f \equiv gh \bmod p^k$ is a factorization, then there is always another factor g' of f over $R/(p^k)$ such that $g \equiv g' \bmod p^{k-s(g,h)}$ and $g \not\equiv g' \bmod p^{k-s(g,h)+1}$.

THEOREM 4.2. *Let* $f, g, h \in R[x]$ *be monic with degrees* $n+m, n, m$, *respectively, with* $f \equiv gh \bmod p^k$, $\operatorname{res}(g,h) \neq 0$ *and* $\sigma = s(g,h) > 0$. *If* $k > 2\sigma$, *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 $u = \sum_{0 \le i < n} u_i x^i$ and $w = \sum_{0 \le j < m} w_j x^j$ 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 the index of such a column. Then $1 \le i \le n+m$, and by Lemma 3.6 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 $\psi_k = w$. □

We show now how to compute all factorizations of a given monic polynomial $f \in R[x]$ with $\operatorname{disc}(f) \neq 0$ over $R/(p^k)$ for $k > d(f) = v_p(\operatorname{disc}(f))$. 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, as already did (1.1), that the number of different factorizations of a polynomial over $R/(p^k)$ can be exponentially large in the input size, which is about $\deg f \cdot k \log_2 p$ bits. But by keeping track of all previously found factorizations in a symbolic way, we achieve a description of all factorizations in polynomial time.

EXAMPLE 4.3. *Let $R = \mathbb{Z}$, $p \in \mathbb{Z}$ an odd prime, $\sigma \in \mathbb{Z}$, $\sigma \ge 1$, and $f = x^2 - p^{2\sigma} \in \mathbb{Z}[x]$. Then $d(f) = 2\sigma$. Now let $k > 2\sigma$, $0 \le \varphi < p^\sigma$, and $\psi = p^\sigma - \varphi$, so that $\psi \equiv -\varphi \bmod p^\sigma$. Then*

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

and each of the factors in this factorization is irreducible by Corollary 3.14. Thus we have p^σ 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, we can easily compute one factorization of $f \in R[x]$ over $R/(p^k)$ for $k > d(f)$. Let $f = \prod_{1 \le i \le l} \tilde{g}_i$ over $R_{(p)}[x]$ with $\tilde{g}_i \in R_{(p)}[x]$ monic and irreducible for $i = 1, \ldots, l$. Let $g_i \in R[x]$ with $g_i \equiv \tilde{g}_i \bmod p^k$ for $i = 1, \ldots, l$. 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 $u \equiv g_i \bmod p^{k-s(g_i,\prod_{j\neq i} g_j)}$ for some $1 \le i \le l$ from Lemma 4.1. Let $h = \prod_{j\neq i} g_j$. In order to determine all irreducible factors u of f such that $u \equiv g_i \bmod p^{k-s(g_i,h)}$ we have to determine all polynomials $\varphi, \psi \in R[x]$ such that $f \equiv (g_i + p^{k-s(g_i,h)}\varphi)(h + p^{k-s(g_i,h)}\psi) \bmod p^k$ by Theorem 3.11.

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

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

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 Villard (1995) 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 such that

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

where d_i divides d_{i+1} for $i = 1, \ldots, n+m-1$. (A matrix is unimodular if its determinant is a unit.) Let $\omega_i = \min\{v_p(d_i), s(g,h)\}$ for $i \le n+m$. Then $0 \le \omega_i \le \omega_{i+1} \le s(g,h)$ for $i < n+m$. Since we assume that $s(g,h) > 0$, we know that $\sum_{1\le i\le n+m} v_p(d_i) = r(g,h) > 0$, and hence $\omega_i > 0$ for at least one $i \le n+m$. Now let $1 \le r \le n+m$ be minimal such that $\omega_r > 0$, and let $t = n+m-r+1$.

We are interested in the set $\{a \in R^{n+m} : Da \equiv 0 \bmod p^{s(g,h)}\}$. This set is an R-module generated by $a_1 = p^{s(g,h)}e_1, \ldots, a_{r-1} = p^{s(g,h)}e_{r-1}, a_r = p^{s(g,h)-\omega_r}e_r, \ldots, a_{n+m} = p^{s(g,h)-\omega_{n+m}}e_{n+m}$, where e_i denotes the ith unit vector for $i \le n+m$. Then the R-module $M = \{b \in R^{n+m} : S(g,h)b \equiv 0 \bmod p^{s(g,h)}\}$ is generated by $\{Qa_i : 1 \le i \le n+m\}$. But every element $m \in M$ with $m \equiv 0 \bmod p^{s(g,h)}$ gives us a trivial solution of our original problem (4.1), namely a solution which is congruent to g and h modulo p^k. Hence we are only interested in the elements $m \in M$ such that $m \not\equiv 0 \bmod p^{s(g,h)}$, and we also allow the zero solution. So let $M' = \{b \in R^{n+m} : S(g,h) \equiv 0 \bmod p^{s(g,h)}, b = 0 \text{ or } b \not\equiv 0 \bmod p^{s(g,h)}\}$. This is no longer an R-module or has any algebraic structure, but it precisely describes the structure of the set of solutions we are interested in. For $l \ge 1$, let $R_l \subseteq R$ be a set of representatives of the finite set $R/(p^l)$, and let $b_i = Qa_{r+i-1}$ for

$1 \le i \le t$. Then

$$M' = \left\{ \sum_{1 \le i \le t} \alpha_i b_i : \alpha_i \in R_{s(g,h)-\mu_i} \text{ for } 1 \le i \le t \right\},$$

where $\mu_i = v_p(b_i)$ for $i \le t$. We put $(\psi_{i,n-1}, \ldots, \psi_{i,0}, \varphi_{i,m-1}, \ldots, \varphi_{i,0})^t = b_i$ for each $i = 1, \ldots, t$. The set of all factorizations as in (4.1) is equal to the set of factorizations $f \equiv g^{(\alpha_1,\ldots,\alpha_t)} h^{(\alpha_1,\ldots,\alpha_t)} \bmod p^k$ with

$$g^{(\alpha_1,\ldots,\alpha_t)} = g + p^{k-s(g,h)} \cdot \left(\sum_{0 \le i < n} \sum_{1 \le j \le t} \alpha_j \psi_{j,i} x^i \right),$$

$$h^{(\alpha_1,\ldots,\alpha_t)} = h + p^{k-s(g,h)} \cdot \left(\sum_{0 \le i < m} \sum_{1 \le j \le t} \alpha_j \varphi_{j,i} x^i \right),$$

where $\alpha_j \in R_{s(g,h)-\mu_j}$ for $i = 1, \ldots, t$ are arbitrary. This data structure allows one to represent the possibly exponentially many factorizations with data of only polynomial size.

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* $\operatorname{disc}(f) = 3^{14} \cdot 6100$, $d(f) = 14$, *and* $s(x^2+3, x^3+9x^2+12x+27) = 3$ *by Example 3.4. 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* $u \equiv x^2+3 \bmod 3^{12}$. *We have to solve the system of equations*

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

The Smith normal form provides unimodular matrices P *and* Q *such that*

$$P \cdot S(x^2+3, x^3+9x^2+12x+27) \cdot Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 27 \end{pmatrix}.$$

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

$$b_1 = Q \begin{pmatrix} 0 \\ 0 \\ 0 \\ 3 \\ 0 \end{pmatrix} = 3 \cdot \begin{pmatrix} -1 \\ -10 \\ -18 \\ 1 \\ 1 \end{pmatrix} \equiv 3 \cdot \begin{pmatrix} 8 \\ 8 \\ 0 \\ 1 \\ 1 \end{pmatrix} \bmod 27,$$

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

and the set of solutions can be written as

$$\left\{3\alpha_1\begin{pmatrix}8\\8\\0\\1\\1\end{pmatrix} + \alpha_2\begin{pmatrix}1\\9\\9\\26\\0\end{pmatrix} : 0 \le \alpha_1 < 9, 0 \le \alpha_2 < 27\right\}.$$

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

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

where $g = x^2 + 3$, $h = x^3 + 9x^2 + 12x + 27$, $0 \le \alpha_1 < 9$, *and* $0 \le \alpha_2 < 27$. *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: let $f \in R[x]$ be monic and $k > d(f)$. 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 $i = 1,\dots,l$. If $l > 1$, we inductively compute all irreducible factors of f in the following way. Let $\sigma_j = \sum_{1\le i<j} s(g_i, \prod_{i<t\le l} g_t)$ for $j = 1,\dots,l$. We take some $i < l$ and assume that 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 $R/(p^k)$, $u_j \equiv g_j \bmod p^{k-\sigma_j}$ for $j = 1,\dots,i-1$ and $w \equiv \prod_{i\le j\le l} g_j \bmod p^{k-\sigma_i}$ have already been computed. This means that we have a set of parameters such that the $u_j, j = 1,\dots,i-1$, and w depend linearly on them. Now we lift each factorization $w \equiv g_i \prod_{i<j\le l} g_j \bmod p^{k-\sigma_i}$ to a factorization over $R/(p^k)$ and compute all factorizations $w \equiv !ab \bmod p^k$ such that $a \equiv g_i \bmod p^{k-\sigma_{i+1}}$ and $b \equiv \prod_{i<j\le l} g_j \bmod p^{k-\sigma_{i+1}}$. 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. In the sequel, we will use the following abbreviations.

NOTATION 4.5. *Let* $l \ge 2$ *and* $f, g_1, \dots, g_l \in R[x]$ *be monic such that* $\mathrm{disc}(f) \ne 0$ *and* $f \equiv \prod_{1\le i\le l} g_i \bmod p^k$. *Then we define* $s_i = s(g_i, \prod_{i<j\le l} g_j)$, $r_i = r(g_i, \prod_{i<j\le l} g_j)$ *for* $i = 1,\dots,l-1$, *and* $\sigma_j = \sum_{1\le i<j} s_i$ *for* $j = 2,\dots,l$.

ALGORITHM 4.6. *Input: A monic polynomial* $f \in R[x]$ *with* $d(f) = v_p(\mathrm{disc}(f)) < \infty$, *a prime* $p \in R$, *and* $k \ge 1$ *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* $f = \prod_{1\le i\le l} g_i$ *into irreducible monic factors of* f *over* $R_{(p)}$, *i.e. for* $i = 1,\dots,l$ *compute* $g_i \bmod p^k$. *If* $l = 1$, *then output "*f *is irreducible" and stop. If* $d(f) = 0$, *then output "*$f \equiv \prod_{1\le i\le l} g_i \bmod p^k$*" and stop.*
2 *Set* $w_1 = f$ *and* $j_0 = 0$. *For* $m = 1\dots,l-1$ *do Steps (a) and (b).*

(a) *Lift the factorization*

$$w_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv g_m \prod_{m<i\le l} g_i \bmod p^{k-\sigma_m}$$

depending on the parameters $\alpha_1,\ldots,\alpha_{j_{m-1}}$ *to a factorization*

$$w_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv a_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} b_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \bmod p^k, \text{ where}$$

$$a_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv g_m \bmod p^{k-\sigma_{m+1}}, \text{ and}$$

$$b_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \equiv \prod_{m<i\le l} g_i \bmod p^{k-\sigma_{m+1}}$$

for all parameters $\alpha_1,\ldots,\alpha_{j_{m-1}}$.

(b) *Compute all solutions of Equation (4.2) with* $g = g_m$ *and* $h = \prod_{m<i\le l} g_i$ *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

$$u_m^{(\alpha_1,\ldots,\alpha_{j_m})} \equiv a_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \bmod p^{k-s_m},$$

$$w_{m+1}^{(\alpha_1,\ldots,\alpha_{j_m})} \equiv b_m^{(\alpha_1,\ldots,\alpha_{j_{m-1}})} \bmod p^{k-s_m},$$

and $j_m \ge j_{m-1}$ *together with the feasible values for* $\alpha_{j_{m-1}+1},\ldots,\alpha_{j_m}$.

3 *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*

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

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* $f \equiv g_1 g_2 g_3 \bmod 3^{15}$ *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* $g_2 g_3 \equiv x^3 + 9x^2 + 12x + 27 \bmod 3^{15}$, *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 $0 \le \alpha_1 < 9$, $0 \le \alpha_2 < 27$. *In Step 2(a) for* $m = 2$, *one has to lift the factorization*

$w_2^{(\alpha_1,\alpha_2)} \equiv g_2 g_3 \bmod 3^{12}$ *to a factorization modulo* 3^{15}. *Since* $s(g_2, g_3) = 1$, *this can be done as in Theorem 3.11 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 2(b), we have to find all factorizations $w_2^{(\alpha_1,\alpha_2)} \equiv u_2 u_3 \bmod 3^{15}$ *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 obtain the factorizations

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

where

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

and $0 \le \alpha_3 < 3$. *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 $0 \le \alpha_1 < 9, 0 \le \alpha_2 < 27, 0 \le \alpha_3 < 3$.

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

LEMMA 4.8. *Let* $f, g_1, \ldots, g_l \in R[x]$ *be monic,* $d(f) < k \in \mathbb{N}$ *with* $f \equiv \prod_{1 \le i \le l} g_i \bmod p^k$ *and* $g_i \in R[x]$ *irreducible over* $R/(p^k)$ *for all* i. *Using Notation 4.5, the following relations hold:*

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

$$s(u, w) = s\Big(\prod_{1 \le i \le m} g_i, \prod_{m < i \le l} g_i \Big).$$

(b) We have

$$k - \sigma_{m+1} \quad = \quad k - \sum_{1 \le j \le m} s_j \quad \ge \quad k - \sum_{1 \le j \le m} r_j \quad > \quad 2s_{m+1}$$

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 $1 \le m \le l-2$. *Then* $s(a,b) = s_{m+1}$.

(d) *Let* $a, b \in R[x]$ *as in (c). Then*

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

(e) $s(g_m, \prod_{i\neq m} g_i) \le \sum_{1\le j\le m} r_j$ *for every* $m = 1, \ldots, l$.

PROOF. Recall from (3.5) 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 $d(f) = d(g) + d(h) + 2r(g,h)$, because $k > d(f)$.

(a) We have

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

Now the claim follows from Lemma 3.10.

(b) Since $s(g,h) \le r(g,h)$ for $g, h \in R[x]$ by Lemma 3.3, we only have to prove the second inequality. Let $1 \le m < l$. We use that

$$\begin{aligned} d(f) &= d(g_1) + d\Big(\prod_{2\le i\le l} g_i\Big) + 2r_1 \\ &= d(g_1) + d(g_2) + d\Big(\prod_{3\le i\le l} g_i\Big) + 2r_1 + 2r_2 \\ &\vdots \\ &= \sum_{1\le i\le m} d(g_i) + d\Big(\prod_{m<i\le l} g_i\Big) + 2\sum_{1\le i\le m} r_i, \end{aligned}$$

and obtain

$$\begin{aligned} k - \sum_{1\le j\le m} r_j &> d(f) - \sum_{1\le j\le m} r_j \\ &= \sum_{1\le i\le m} d(g_i) + d\Big(\prod_{m<i\le l} g_i\Big) + 2\sum_{1\le j\le m} r_j - \sum_{1\le j\le m} r_j \\ &\ge d\Big(\prod_{m<i\le l} g_i\Big) \quad \ge \quad d(g_{m+1}) + d\Big(\prod_{m+2\le i\le l} g_i\Big) + 2r_{m+1} \\ &\ge 2s_{m+1}. \end{aligned}$$

(c) The claim follows by applying Part (b) and Lemma 3.10.

(d) Since

$$k - \sum_{1\le j\le m} s_j > 2s_{m+1} \ge s_{m+1} = s(a,b),$$

by (b) and (c), it follows that

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

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

(e) Let $1 \le j \le l$. Recall that for polynomials $f, g, h \in R[x]$ we have $\operatorname{res}(f, gh) = \operatorname{res}(f, g)\operatorname{res}(f, h)$ (see, for example, Cohn (1977, Section 7.4, Theorem 2)). Hence

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

Now

$$s\Big(g_m, \prod_{i \ne m} g_i\Big) \le r\Big(g_m, \prod_{i \ne m} g_i\Big) = \sum_{1 \le j < m} r(g_m, g_j) + r\Big(g_m, \prod_{m < i \le l} g_i\Big)$$
$$\le \sum_{1 \le j < m} r\Big(g_j, \prod_{j < i \le l} g_i\Big) + r_m = \sum_{1 \le j \le m} r_j. \quad \square$$

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 probabilistic polynomial time for $R = \mathbb{Z}$ and $R = \mathbb{F}_q[y]$.*

PROOF. If f is irreducible over $R_{(p)}$, it is irreducible over $R/(p^k)$ for all $k > d(f)$ by Theorem 3.11. 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 3.11. Hence, from now on we assume that $d(f) > 0$ and f is reducible over $R_{(p)}$.

From Remark 3.7 and Lemma 4.8(d) we find that only the matrix

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

is needed in order to lift the factorizations of Step 2(a). Besides, Lemma 4.8(d) also shows that in order to compute the solutions in Step 2(b), only this matrix is necessary. Hence, both steps can be done for all parameters at once.

Now we prove by induction the following claim: after the execution of Steps 2(a) and 2(b) for m all factorizations $f \equiv (\prod_{1 \le i \le m} u_i) w \bmod p^k$ with $u_i \equiv g_i \bmod p^{k - \sum_{1 \le j \le i} s_j}$ for all $i \le m$ have been computed. Furthermore, these are also all factorizations such that $u_i \equiv g_i \bmod p^{k - \sum_{1 \le j \le i} r_j}$ for every $i = 1, \ldots, m$.

If $m = 1$, then $w_0 = f$, and in Step 2(a) there is nothing to do. In Step 2(b), all factorizations $f \equiv uw \bmod p^k$ such that $u \equiv g_1 \bmod p^{k - s_1}$ and $w \equiv \prod_{1 < i \le l} g_i \bmod p^{k - s_1}$ are computed. Then by Theorem 3.11 and since $r(g, h) \ge s(g, h)$ for all $g, h \in R[x]$, these are also all factorizations $f \equiv uw \bmod p^k$ such that $u \equiv g_1 \bmod p^{k - r_1}$ and $w \equiv \prod_{1 < i \le l} g_i \bmod p^{k - r_1}$.

Now we let $1 < m < l$. Then by the induction hypothesis we have found every factor w_{m-1} such that

$$w_{m-1} \equiv g_{m-1} \prod_{m \le i \le l} g_i \bmod p^{k - \sigma_m}. \tag{4.3}$$

By Lemma 4.8(b) and Theorem 3.11 we can lift the factorization in (4.3) as is claimed in Step 2(a). On the other hand, if there is a factorization $w_{m-1} \equiv ab \bmod p^k$ such that $a \equiv g_m \bmod p^{k - \sum_{1 \le j < m} r_j}$, and $b \equiv \prod_{m < i \le l} g_i \bmod p^{k - \sum_{1 \le j < m} r_j}$, then again by Lemma 4.8(b) and Theorem 3.11 this factorization is found in Step 2(b). Hence, the claim is proven.

Now assume that $f \equiv uw \bmod p^k$ with u irreducible. As $k > d(f)$, it follows that $u \equiv g_m \bmod p^{k-s(u,w)}$ and $w \equiv \prod_{i \neq m} g_i \bmod p^{k-s(u,w)}$ for some $1 \leq m \leq l$. Moreover, $s(u,w) = s(g_m, \prod_{i \neq m} g_i)$. By Lemma 4.8(c) we have $s(g_m, \prod_{i \neq m} g_i) \leq \sum_{1 \leq j \leq m} r_j$. Hence

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

Therefore, this factorization will be computed by Algorithm 4.6. □

REMARK 4.10. (a) Let $R = \mathbb{Z}$, and let $\mathsf{C}_{\mathbb{Z}}(p,n,k)$ denote the number of bit operations for computing the complete factorization over $\mathbb{Z}_{(p)}$ of a polynomial $f \in \mathbb{Z}[x]$ with $\deg f = n$ modulo p^k; Chistov's (1987, 1994) algorithm does this in polynomial time. Then a more detailed analysis shows that 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 (von zur Gathen and Hartlieb, 1996a).

(b) Let $R = \mathbb{F}_q[y]$ and $p = y$. In this 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 $\mathsf{C}_q(n,k) + O(n^4 k^2 \log^4 nk + k^2 n^{\omega+2} \log^2 nk + n\mathsf{SNF}(n,k))$ operations in $\mathbb{F}_q$. Here $\mathsf{C}_q(n,k)$ denotes a time bound 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 $\mathsf{C}_q(n,k)$ operations in $\mathbb{F}_q$. Chistov's algorithm yields again that $\mathsf{C}_q(n,k)$ can be chosen polynomial in n and $\log q$. $\mathsf{SNF}(n,k)$ is 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 $O(\mathsf{SNF}(n,k))$ operations. By Villard (1995) this can be done in polynomial time. For the analysis of the running time, see von zur Gathen and Hartlieb (1996a).

REMARK 4.11. The case $k \leq d(f)$ 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 and Hartlieb (1996b) we show how this can be done.

REMARK 4.12. In the case that $\mathrm{disc}(f) = 0$ our method does not work. It is not difficult to compute some factorization of f over R by a square-free 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 $\mathrm{disc}(f) = 0$, 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 $\mathrm{disc}(f) \neq 0$, but apparently not the problem of finding all factorizations into irreducibles.

EXAMPLE 4.13. *Let* $R = \mathbb{Z}$, $p = 3$, *and* $f = x^3(x+12)^2 = x^5 + 24x^4 + 144x^3$. *Then*

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

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

Acknowledgements

We thank Mark Giesbrecht for conversations about matrix normal forms and the anonymous referees, one of which provided an especially careful report with many helpful suggestions. An extended abstract of this paper appeared in *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation*, Zürich, Switzerland, ACM Press, pp. 10–17.

References

Apostol, T.M. (1970). Resultants of cyclotomic polynomials. *Proc. AMS*, **24**, 457–462.
Bach, E. (1990). Number-theoretic algorithms. *Ann. Rev. Comput. Sci.*, **4**, 119–172.
Berlekamp, E.R. (1970). Factoring polynomials over large finite fields. *Math. Comp.*, **24**, 713–735.
Böffgen, R., Reichert, M.A. (1987). Computing the decomposition of primes p and p-adic absolute values in semi-simple algebras over $\mathbb{Q}$. *J. Symb. Comput.*, **4**, 3–10.
Borevich, Z.I., Shafarevich, I.R. (1966). *Number Theory*. Academic Press.
Cassels, J. W. S. (1986). *Local Fields*. Cambridge University Press.
Cauchy, A. (1847). Mémoire sur les racines des équivalences correspondantes à des modules quelconques premiers ou non premiers, et sur les avantages que présente l'emploi de ces racines dans la théorie des nombres. *Comptes Rendus de l'Académie*, **25**, 37 ff. Œuvres Complètes, I^re série, tome 10, Gauthier-Villars, Paris, 1897, pp. 324–333.
Chistov, A.L. (1987). Efficient factorization of polynomials over local fields. *Soviet Math. Dokl.*, **35**, 430–433.
Chistov, A.L. (1994). Algorithm of polynomial complexity for factoring polynomials over local fields. *J. Math. Sciences*, **70**, 1912–1933.
Cohn, P. (1977). *Algebra*, Vol. 2. John Wiley & Sons.
Ford, D.J. (1987). The construction of maximal orders over a Dedekind domain. *J. Symb. Comput.*, **4**, 69–75.
von zur Gathen, J. (1984). Hensel and Newton methods in valuation rings. *Math. Comp.*, **42**, 637–661.
von zur Gathen, J., Hartlieb, S. (1996a). Factoring modular polynomials. *Technical Report tr-ri-96-176*, Universität-GH Paderborn. `ftp://ftp.uni-paderborn.de/doc/techreports/Informatik/`.
von zur Gathen, J., Hartlieb, S. (1996b). Factorization of polynomials modulo small prime powers. *Technical Report tr-ri-96-180, Universität-GH Paderborn.* `ftp://ftp.uni-paderborn.de/doc/techreports/Informatik/`.
von zur Gathen, J., Shoup, V. (1992). Computing Frobenius maps and factoring polynomials. *Computational Complexity*, **2**, 187–224.
Gauß, C. F. (1863). Theoria residuorum biquadraticorum, Commentatio secunda. *Werke*, **2**.
Iliopoulos, C.S. (1989). 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**, 658–669.
Kaltofen, E., Shoup, V. (1995). Subquadratic-time factoring of polynomials over finite fields. *Math Comp.*, **67**, 1179–1197.
Lenstra, A.K., Lenstra, Jr., H.W. (1990). Algorithms in number theory. In van Leeuwen, J., ed., *Handbook of Theoretical Computer Science*, Vol. A, pp. 673–715. Amsterdam, Elsevier.
Lenstra, A.K., Lenstra, Jr., H.W., eds. (1993). *The Development of the Number Field Sieve*, LNCS 1554. Springer.
McDonald, B.R. (1974). *Finite Rings with Identity*. New York, Marcel Dekker.
Shamir, A. (1993). On the generation of polynomials which are hard to factor. In *Proceedings of the 25th Annual ACM Symposium on the Theory of Computing*, pp. 796–804.
Vahle, M.O. (1993). Solving the congruence $x^2 \equiv a \bmod n$. *MapleTech*, **9**, 69–76.
Villard, G. (1995). Generalized subresultants for computing the Smith normal form of polynomial matrices. *J. Symb. Comput.*, **20**, 269–286.
Zassenhaus, H. (1969). On Hensel factorization, I. *J. Number Theory*, **1**, 291–311.

Originally received 11 September 1996
Accepted 19 June 1998