Joachim von zur Gathen & Silke Hartlieb (1996). Factoring Modular Polynomials. In *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation ISSAC '96, Zürich, Switzerland*, Y. N. Lakshman, editor, 10–17. ACM Press. ISBN 0-89791-796-0. URL http://dx.doi.org/10.1006/jsco.1998.0228. Final version in *Journal of Symbolic Computation* (1998).

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

September 5, 1996

Abstract. 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 $R = \mathbb{Z}$ 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 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. 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.

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 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 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 did not analyze the running time of the algorithm in detail, because it seems that the running time of Chistov's algorithm (which is not analyzed in detail) dominates the running time of ours. It is clear that all steps of the algorithm can be done in probabilistic polynomial time.

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.

Assume that we are able to factor $f \in R[x]$ into irreducible factors over $R/(p^k)$ for any given prime p and $k \geq 1$. 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 2.2. *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 $p \in R$.*

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) 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) 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):

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). Then the number of irreducible factors of $f \in R[x]$ over $R/(r)$ is the sum over all $1 \le i \le s$ of the numbers of irreducible factors of f 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 $k \ge 1$. 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 $h = \sum_{0 \le j \le m} h_j x^j$, is the following matrix:

$$S(g,h) = \left(\begin{array}{cccccc} g_n & & & h_m & & \\ g_{n-1} & \ddots & & h_{m-1} & \ddots & \\ \vdots & & \ddots & \vdots & & h_m \\ g_0 & & g_n & \vdots & & h_{m-1} \\ & \ddots & g_{n-1} & h_0 & & \vdots \\ & & \ddots \;\; \vdots & & \ddots & \vdots \\ & & g_0 & & & h_0 \\ \multicolumn{3}{c}{\underbrace{\hspace{5cm}}_{m}} & \multicolumn{3}{c}{\underbrace{\hspace{4.5cm}}_{n}} \end{array}\right) \in R^{(n+m)\times(n+m)}.$$

(Sometimes the transpose 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:

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

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 $a, b \in R$, $b \ne 0$. 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 this 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 $K_{(p)} = \mathbb{F}_q((y))$ 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 $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in K^{n \times m}$ 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.

Notation 3.1. *Let $g, h \in R[x]$ be monic. Then $d(g) = v_p(disc(g))$, where $disc(g) = res(g, g') \in R$ is the discriminant of g, $r(g, h) = v_p(res(g, h))$, and if $res(g, h) \neq 0$, then $s(g, h) = -v_p(S(g, h)^{-1})$.*

Lemma 3.2. *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 $r(g, h) = 0$. □

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

Example 3.3. *Let $R = \mathbb{Z}$, $p = 3$, $g = x^2 + 3$, and $h = x^3 + 9x^2 + 12x + 27$. Then*

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

Thus $res(g, h) = 3^5$, $r(g, h) = 5$, and $s(g, h) = 3$.

Remark 3.4. *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 asymtotic time estimates would not be affected. But Lemma 3.2 and Example 3.3 show that for individual polynomials, the use of $s(g,h)$ may be advantageous.*

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

Proposition 3.5. *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*

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

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

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

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

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

The entries of $p^{s(g,h)}bS(g,h)^{-1}$ 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). □

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 3.5, the solutions correspond to the solutions of the congruence

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

Corollary 3.6. *Let $g, h, l \in R[x]$ be as in Proposition 3.5. 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 $S(g,h) \bmod p^{s(g,h)+1}$.*

Lemma 3.7. *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 $\sigma = s(g,h)$, $u = g + p^{\sigma+1} g_0$ and $w = h + p^{\sigma+1} h_0$ with $g_0, h_0 \in R[x]$, and assume first that $\operatorname{res}(u,w) = 0$. 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

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

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 3.5, we obtain that $a \equiv 0 \bmod p$ and $b \equiv 0 \bmod p$, a contradiction. Hence, $\operatorname{res}(u,w) \neq 0$, and $s(u,w)$ is defined.

Let $n = \deg g$ and $m = \deg h$. By Proposition 3.5, 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

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

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 over R, each of whose columns has p-adic value 0. □

The next theorem is a more general version of Hensel's Lemma. The proof is analogous to the proof of Hensel's Lemma in Borevich & Shafarevich (1966).

THEOREM 3.8. *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) $k > 2s(u,w)$.

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

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

and the leading coefficient of g and h equals the leading coefficient of u and w, respectively.

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

$$f \equiv ab \bmod p^{k+i-1} \tag{3.3}$$

with $a, b \in R[x]$ such that $a \equiv u \bmod p^{k-\sigma}$ and $b \equiv w \bmod p^{k-\sigma}$, and $\mathrm{lc}(a) = \mathrm{lc}(u)$, $\mathrm{lc}(b) = \mathrm{lc}(w)$, 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 3.3 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 $a \equiv u \bmod p^{k-\sigma}$, $b \equiv w \bmod p^{k-\sigma}$, and $k - \sigma > \sigma$, we have by Lemma 3.7 that $\sigma = s(u, w) = s(a, b)$. By Proposition 3.5 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

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

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

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

A version of Theorem 3.8 is already proven in von zur Gathen (1984) in a different setting. In particular, no explicit formula for $s(u, w)$ is given.

COROLLARY 3.9. *Assume that conditions (a) and (b) of Theorem 3.8 hold. Then condition (c) is true if* $k > d(f)$.

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

$$\mathrm{disc}(f) = \mathrm{disc}(gh) = \mathrm{disc}(g)\mathrm{disc}(h)\mathrm{res}(g, h)^2 \tag{3.4}$$

(c.f. Borevich & Shafarevich 1966, Chapter 4, §3). Using Lemma 3.2, 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 3.10. *It follows from Corollary 3.6 that in order to apply Theorem 3.8 it suffices to know* $S(u,w) \bmod p^{s(u,w)+1}$.

The next corollary follows from Theorem 3.8 in the case $s(g,h) = 0$:

Corollary 3.11. *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 $f \equiv \nu g^e \bmod p$ with $e \geq 1$, $g \in R[x]$ irreducible over $R/(p)$, and $\nu \in R$ a unit modulo p.*

Corollary 3.12. *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 $f = p^l g$ with $\gcd(p,g) = 1$ and $l \in \mathbb{N}$. Then $g \not\equiv 0 \bmod p$, and $g \equiv \nu_0 m_0 \bmod p$, where $\nu_0 \in R[x]$ is a unit over $R/(p)$ and $m_0 \in R[x]$ is monic. Of course, ν_0 can be chosen such that $\mathrm{lc}(g) = \mathrm{lc}(\nu_0 m_0)$. Then $\mathrm{res}(\nu_0,m_0) = \nu_0^{\deg m_0} \neq 0$, and $s(\nu_0,m_0) = 0$. By Theorem 3.8 there exist $\nu, m \in R[x]$ such that $g \equiv \nu m \bmod p^{k-l}$ where $\nu \equiv \nu_0 \bmod p$, $m \equiv m_0 \bmod p$, and $\mathrm{lc}(m) = \mathrm{lc}(m_0)$. This means that ν is a unit over $R/(p^{k-l})$, m is monic and $f \equiv p^l \nu m \bmod p^k$. The irreducible factors of f are the irreducible factors of m and of p^l. □

Theorem 3.13. *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 $r = u \prod_{1 \leq i \leq s} p_i^{k_i}$ be the complete factorization of r as in (2.1). Theorem 3.8 for $s(g,h) = 0$ shows that f can be uniquely factored over $R/(p_i^{k_i})$ into factors which are relatively prime over $R/(p_i)$ for $1 \leq i \leq s$. This can be done in polynomial time (c.f. von zur Gathen 1984). Hence it remains to consider the case where $f \equiv \nu g^e \bmod p_i$ with $e \geq 2$, $g \in R[x]$ irreducible over $R/(p_i)$ and $v \in R[x]$ a unit over $R/(p_i)$ for some $1 \leq i \leq s$. By Corollary 3.12, we may assume that f is monic. □

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

It follows from Theorem 3.8 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 $g_k \equiv g \bmod p^{k-\sigma}$ and $h_k \equiv h \bmod p^{k-\sigma}$, where $\sigma = s(g,h) \leq \frac{d}{2}$. Hence, any two factorizations of f over $R/(p^k)$ which give rise to the same factorization over $R_{(p)}$ are equal over $R/(p^{k-\sigma})$. In particular, Theorem 3.8 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 $f = \prod_{1 \leq i \leq l} g_i$ over $R_{(p)}$ with disc$(f) \neq 0$, $l \geq 1$, and $g_i \in R_{(p)}[x]$ monic and irreducible for $1 \leq i \leq l$. 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 $g \equiv \prod_{i \in S} g_i \bmod p^{k-\sigma}$ 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 $1 \leq i \leq l$ 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 3.9 and Theorem 3.8. 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

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

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

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

by Lemma 3.7. □

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 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 3.5 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 polynomial $f \in R[x]$ with disc$(f) \neq 0$ over $R/(p^k)$ for $k > d(f) = v_p(\text{disc}(f))$. 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 4.3. *Let $R = \mathbb{Z}$, $p \in \mathbb{Z}$ an odd prime, $\sigma \in \mathbb{Z}$, $\sigma \geq 1$, and $f = x^2 - p^{2\sigma} \in \mathbb{Z}[x]$. Then $d(f) = 2\sigma$. Now let $k > 2\sigma$, $0 \leq \varphi < p^\sigma$, 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 3.11. 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, 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 $f \equiv \prod_{1 \leq i \leq l} g_i \bmod p^k$ 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 $1 \leq i \leq l$ 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 3.8.

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 $s(g,h) > 0$. 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 (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 $\omega_i = \min\{v_p(d_i), s(g,h)\}$ for $1 \le i \le n+m$. Then $0 \le \omega_i \le \omega_{i+1} \le s(g,h)$ for $1 \le i < n+m$. Since we assume that $s(g,h) > 0$, we know that $\omega_i > 0$ for at least one $i \in \mathbb{Z}$ with $1 \le i \le n+m$. Hence, let $1 \le r \le n+m$ be minimal such that $\omega_r > 0$, and let $t = n+m-r+1$. A basis over R of the set $\{a \in R^{n+m} : Da \equiv 0 \bmod p^{s(g,h)}\}$ is $a_1 = p^{s(g,h)-\omega_r} e_r, \ldots, a_t = p^{s(g,h)-\omega_{n+m}} e_{n+m}$, where e_i denotes the ith unit vector for $1 \le i \le n+m$. Let $\mu_i = s(g,h) - \omega_{i+r-1}$ 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 $1 \le i \le t$. 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 $\{b \in R^{n+m} : S(g,h)b \equiv 0 \bmod p^{s(g,h)}\}$.

For $l \ge 1$ 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

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

Let $1 \le i \le t$ 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

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

where $\alpha_i \in R_{s(g,h)-\mu_i}$ for $1 \le i \le t$ are arbitrary. This data structure allows 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 disc*$(f) = 3^{14} \cdot 6100$, $d(f) = 14$, *and* $s(x^2+3, x^3+9x^2+12x+27) = 3$. *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*

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

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

$$\begin{aligned} b_1 &= \begin{pmatrix} 1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -10 & 9 \\ 0 & 0 & 1 & -18 & 9 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ -10 \\ -18 \\ 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 8 \\ 8 \\ 0 \\ 1 \\ 1 \end{pmatrix} \bmod 9, \\ b_2 &= \begin{pmatrix} 1 & 0 & 0 & -1 & 1 \\ 0 & 1 & 0 & -10 & 9 \\ 0 & 0 & 1 & -18 & 9 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 9 \\ 9 \\ -1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 9 \\ 9 \\ 26 \\ 0 \end{pmatrix} \bmod 27, \end{aligned}$$

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*

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

where $g = x^2 + 3$, $h = x^3 + 9x^2 + 12x + 27$, $0 \le \alpha_1 < 9$, *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: 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 $\sigma_j = \sum_{1 \le i < j} s(g_i, \prod_{t > i} g_t)$ 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 $R/(p^k)$, $u_j \equiv g_j \bmod p^{k-\sigma_j}$ for $1 \le j < i$ and $w \equiv \prod_{j\ge i} g_j \bmod p^{k-\sigma_i}$ have already been computed. This means that we have a set of parameters such that the $u_j, 1 \le j < i$, and w depend linearly on them. Now we lift each factorization $w \equiv g_i \prod_{j>i} g_j \bmod p^{k-\sigma_i}$ to a factorization over $R/(p^k)$ and compute all factorizations $w \equiv ab \bmod p^k$ such that $a \equiv g_i \bmod p^{k-\sigma_i}$ and $b \equiv \prod_{j>i} g_j \bmod p^{k-\sigma_i}$. 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 $l \ge 2$ and $f, g_1, \dots, g_l \in R[x]$ be monic such that $d(f) \ne 0$ and $f \equiv \prod_{1\le i\le l} g_i \bmod p^k$. Then we define $s_i = s(g_i, \prod_{i<j\le l} g_j)$ and $r_i = r(g_i, \prod_{i<j\le l} g_j)$ for $1 \le i < l$.*

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 $k \ge 1$ 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 $1 \le i \le l$ 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 $1 \le m < l$ do Steps 3 and 4.*

3. *Lift the factorization*

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

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

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

   $$a_m^{(\alpha_1,\dots,\alpha_{j_{m-1}})} \equiv g_m \bmod p^{k-\sum_{1\le j\le m} s_j}, \text{ and}$$
   $$b_m^{(\alpha_1,\dots,\alpha_{j_{m-1}})} \equiv \prod_{m<i\le l} g_i \bmod p^{k-\sum_{1\le j\le m} s_j}$$

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

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

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

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

   and $j_m \geq j_{m-1}$ *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 $0 \leq \alpha_1 < 9$, $0 \leq \alpha_2 < 27$. *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 3.8 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 $w_2^{(\alpha_1,\alpha_2)} \equiv u_2 u_3 \bmod 3^{15}$ 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 obtains 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 $f \in R[x]$, $d(f) < \infty$, $k > d(f)$ 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 $f \equiv uw \bmod p^k$ 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 $s(u,w) = s(\prod_{1 \le i \le m} g_i, \prod_{m < i \le l} g_i)$.

(b) *We have*

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

for every $1 \le m \le l-1$.

(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*

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

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

Proof. Recall from (3.4) 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

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

Now the claim follows from Lemma 3.7.

(b) Since $s(g, h) \le r(g, h)$ for $g, h \in R[x]$ by Lemma 3.2, we only have to prove the second inequality. Let $1 \le m < l$. We have

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

(c) The claim follows by applying Part (b) and Lemma 3.7.

(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 $\text{res}(f, gh) = \text{res}(f,g)\text{res}(f,h)$ (Cohn 1977, 7.4, Theorem 2). Hence

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

Now

$$\begin{aligned} s(g_m, \prod_{i \ne m} g_i) &\le r(g_m, \prod_{i \ne m} g_i) = \sum_{1 \le j < m} r(g_m, g_j) + r(g_m, \prod_{m < i \le l} g_i) \\ &\le \sum_{1 \le j < m} r(g_j, \prod_{j < i \le l} g_i) + r_m = \sum_{1 \le j \le m} r_j. \end{aligned}$$

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 3.8. 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. Hence, from now on we assume that $d(f) > 0$ and f is reducible over $R_{(p)}$.

By Corollary 3.6 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(d) 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 $u_i \equiv g_i \bmod p^{k-\sum_{1\le j\le i} s_j}$ have been computed. Furthermore, we show that 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 $1 \le i \le m$.

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 $u \equiv g_1 \bmod p^{k-s_1}$, and $w \equiv \prod_{1<i\le l} g_i \bmod p^{k-s_1}$ are computed. Then by Theorem 3.8 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 let $1 < m \le l - 1$, and assume the induction hypothesis holds for $m - 1$. Then by induction hypothesis we have found every factor w_{m-1} such that

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

By Lemma 4.8(b) and Theorem 3.8 we can lift the factorization in (4.3) as is claimed in Step 3. On the other hand, if there is a factorization $w_{m-1} \equiv ab$ mod 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 3.8 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 that $u \equiv g_m \bmod p^{k-s(u,w)}$ and $w \equiv \prod_{i\ne m} g_i \bmod p^{k-s(u,w)}$ for some $1 \le m \le l$. Moreover, $s(u,w) = s(g_m, \prod_{i\ne m} g_i)$. By Lemma 4.8(e) we have $s(g_m, \prod_{i\ne m} g_i) \le \sum_{1\le j\le m} r_j$. Hence

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

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 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 (1987, 1994) algorithm does this in polynomial time. Then 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 (see von zur Gathen & Hartlieb 1996b).*

(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 $\mathsf{C}_q(y,n,k)+O(n^4k^2\log^4 nk+k^2n^{\omega+2}\log^2 nk+nSNF(n,k))$ operations 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 Villard (1995) this can be done in polynomial time. For the analysis of the running time see von zur Gathen & Hartlieb (1996b).*

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 & Hartlieb (1996a) we show how this can be done.*

REMARK 4.12. *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 4.13. *Let $R = \mathbb{Z}$, $p = 3$, and $f = x^3(x+12)^2 = x^5 + 24x^4 + 144x^3$. Then*

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

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

Acknowledgements

We thank Mark Giesbrecht for conversations about matrix normal forms. An Extended Abstract of this paper appears in *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation, Zürich, Switzerland.*

References

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.

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.

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

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, 1996a. To appear.

J. von zur Gathen and S. Hartlieb, Factoring modular polynomials. Technical Report tr-ri-96-176, Universität-GH Paderborn, 1996b.

J. von zur Gathen and V. Shoup, Computing Frobenius maps and factoring polynomials. *Computational 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.

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. 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.

G. Villard, Generalized subresultants for computing the Smith normal form of polynomial matrices. *J. Symbolic Computation* **20** (1995), 269–286.