FACTORIZATION OF POLYNOMIALS MODULO SMALL PRIME POWERS

JOACHIM VON ZUR GATHEN AND SILKE HARTLIEB
Fachbereich 17 Mathematik-Informatik, Universität-GH Paderborn
D-33095 Paderborn, Germany
{gathen,hartlieb}@uni-paderborn.de
July 16, 1996

Abstract. This paper describes an algorithm for factoring polynomials over residue class rings of $\mathbb{Z}$ or $\mathbb{F}_q[y]$, in the "difficult" case where we want to factor modulo a prime power which divides the discriminant of the polynomial, i.e., the discriminant of the polynomial is zero in the residue class ring. The method works in exponential time.

1. Introduction

Let $R = \mathbb{Z}$ or $R = \mathbb{F}_q[y]$ and let p be a prime in R. We aim to factor polynomials over rings of the form $R/(p^k)$ with $k \in \mathbb{N}$ such that p^k is a small prime power in the following sense:

DEFINITION 1.1. *Let $f \in R[x]$, $disc(f) \in R$ the discriminant of f, and $p \in R$ a prime. A prime power p^k is called* **small** *(with respect to f) if $k \geq 1$ and $p^k | disc(f)$.*

Factorization into irreducible factors over rings of the form $R/(p^k)$ is in general not unique, as illustrated in Section 2, and there are two different meanings of the task of factoring a polynomial. The first one is to find one factorization into irreducible factors. The second one is to produce, more generally, a list of all factorizations into irreducible factors. We will deal with both of these in the following.

In von zur Gathen & Hartlieb (1996), the problem of factoring polynomials over $R/(r)$, where $r \in R$ is not necessarily a prime power (but whose prime factors are given, if $R = \mathbb{Z}$) is reduced in probabilistic polynomial time to the problem of factoring polynomials over $R/(p^k)$, where p^k is a small prime power. In particular, the case where p^k is a prime power, but is not small, is solved in polynomial time. It is shown that if one could solve the problem of finding all factorizations into irreducible factors modulo small prime powers in (probabilistic) polynomial time, then the whole task of factoring over $R/(r)$ would be solvable in probabilistic polynomial time. Unfortunately, no such algorithm is known to us. In this paper, we illustrate the difficulties which arise when factoring modulo small primes, and we propose an algorithm for this task.

2. Examples and reductions

Let $p \in R$ be a prime and $k \geq 1$. The following example shows that factorization over the ring $R/(p^k)$ is in general not unique.

EXAMPLE 2.1. *Let $R = \mathbb{Z}$. Then*

$$x^2 \equiv x \cdot x \equiv (x+3)(x+6) \bmod 9,$$

and all three linear factors are irreducible by Corollary 2.4.

The following theorem is well-known as Hensel's Lemma. The proof can be found for example in Borevich & Shafarevich (1966), Chapter 4, §3.

THEOREM 2.2. *(Hensel's Lemma) Let p be a prime, $k \geq 1$, and $f, u_0, w_0 \in R[x]$ such that $f \equiv u_0 w_0 \not\equiv 0 \bmod p$ and $\gcd(u_0 \bmod p, w_0 \bmod p) = 1$ in $R/(p)[x]$.*

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

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

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

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

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

(iii) The polynomials u_{k-1} and w_{k-1} can be constructed in polynomial time.

The following corollary is from von zur Gathen & Hartlieb (1996).

COROLLARY 2.3. *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, i.e., there is a probabilistic polynomial time algorithm which computes the unique factorization $f \equiv eg \bmod p^k$ such that $g \in R[x]$ is monic, and $e \in R[x]$ is the product of a power of p and a unit in $R/(p^k)$.*

Now we have the following criterion for irreducibility in $R/(p^k)$.

COROLLARY 2.4. *Let $f \in R[x]$ be monic. If f is irreducible over the finite field $R/(p)$, then f is irreducible over $R/(p^k)$ for every $k \geq 1$. On the other hand, if f is irreducible over $R/(p^k)$ for some $k \geq 1$, then $f \equiv g^e \bmod p$ for some $e \geq 1$ and a polynomial $g \in R[x]$ which is irreducible over $R/(p)$.*

Hence, we may assume from now on that the polynomial which we aim to factor is monic and over $R/(p)$ is a power of a polynomial which is irreducible over $R/(p)$.

Let $g, h \in R[x]$ with degrees n and m, and $g = \sum_{0 \leq i \leq n} g_i x^i$ and $h = \sum_{0 \leq j \leq m} h_j x^j$. Then

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

is the **Sylvester matrix** of g and h (sometimes the transposed of this matrix is called the Sylvester matrix). If $f \in R[x]$ is monic, and $\deg(f) = n$, then $\mathrm{disc}(f) = (-1)^{n(n-1)/2} \det(S(f, f'))$ is the discriminant of f (see for example Cohn 1974, 7.4).

The idea when factoring modulo a prime power p^k which is not small is to compute the factorization over the p-adic completion $R_{(p)}$, and then all factorizations over $R/(p^k)$ are modifications of this (unique) factorization (see von zur Gathen & Hartlieb (1996) for details). In particular, if the polynomial is irreducible over $R_{(p)}$, then it is irreducible over $R/(p^k)$ for all prime powers which are not small. This fails to hold in the case where the prime power is small:

LEMMA 2.5. *Let $R = \mathbb{Z}$, $p = 3$, $k \geq 1$, and $f = x^2 + 3^k$. Then disc$(f) = 4 \cdot 3^k$, and f is irreducible over $\mathbb{Z}/(3^{k+1})$, hence over $\mathbb{Z}_{(3)}$, but it is of course reducible over $\mathbb{Z}/(3^k)$.*

PROOF. We have that

$$\operatorname{disc}(f_k) = -\det S(f_k, f_k') = -\det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 2 \\ 3^k & 0 & 0 \end{pmatrix} = 4 \cdot 3^k.$$

Now it remains to show that f is irreducible over $\mathbb{Z}/(3^{k+1})$. If it is reducible over $\mathbb{Z}/(3^{k+1})$, then there is an $a \in \mathbb{Z}$ such that $a^2 \equiv -3^k \equiv 2 \cdot 3^k \bmod 3^{k+1}$. If k is odd, then $a^2 = 2 \cdot 3^k + 3^{k+1}b = 3^k(2+3b)$ for some $b \in \mathbb{Z}$, a contradiction. If k is even, then $(a/3^{\frac{k}{2}})^2 \equiv 2 \bmod 3$. This is a contradiction, because 2 is a non-square in $\mathbb{Z}/(3)$. $\square$

This example shows that it is not possible to apply the methods of von zur Gathen & Hartlieb (1996) in our case. But the situation is even worse. One might hope that if we have a factorization $f = gh$ over $R_{(p)}$, then it is sufficient to factor g and h over $R/(p^k)$. The next example shows that this is not the case.

EXAMPLE 2.6. *Let $R = \mathbb{Z}$, $p = 3$, and $f = (x^2 + 243)(x^2 + 6) = x^4 + 249x^2 + 1458$. Then disc$(f) = 2^5 3^{10} 79^4$. The polynomial $x^2 + 6$ is an Eisenstein polynomial and hence irreducible over $\mathbb{Z}_{(3)}$. It is irreducible over $\mathbb{Z}/(3^6)$ by Corollary 3.2. The polynomial $x^2 + 243$ is the polynomial f of Lemma 2.5 with $k = 5$, and also irreducible over $\mathbb{Z}/(3^6)$. But we have*

$$f \equiv (x + 351)(x + 135)(x^2 + 243x + 249) \bmod 3^6,$$

where all factors are irreducible. (Note that $(x + 351)(x + 135) \equiv x^2 + 243$, and $x^2 + 243x + 249 \equiv x^2 + 6$ modulo 3^5, but not modulo 3^6.)

Thus in order to find all factorizations of a polynomial into irreducibles modulo a small prime it is not sufficient to be able to factor polynomials which are irreducible over $R_{(p)}$ modulo small primes. This is only true when only one factorization into irreducible factors is required.

LEMMA 2.7. *In order to find a factorization of polynomials modulo a small prime power it suffices to be able to factor polynomials which are irreducible over $R_{(p)}$ modulo small prime powers.*

PROOF. The factorization over $R_{(p)}$ into irreducible factors can be computed in probabilistic polynomial time by Chistov (1987, 1994). Then, of course, it suffices to compute irreducible factors of the irreducible factors over $R_{(p)}$. □

Now we show that it can happen that there are exponentially many factorizations of f into irreducible factors.

EXAMPLE 2.8. *Let $f = x^2 \in \mathbb{Z}[x]$. Then disc$(f) = 0$, and hence every prime power p^k is small with respect to f. Let p be odd, k be even, $0 \le \varphi < \frac{p^{k/2}}{2}$, and $\psi = p^{k/2} - \varphi$. Then*

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

Hence, there are $(p^{k/2}-1)/2$ different factorizations of x^2 into irreducible factors over $R/(p^k)$.

3. An algorithm

In this section, we assume that monic polynomials $f, g \in R[x]$, a prime $p \in R$ and $e \in \mathbb{Z}$ are given, such that

$$f \equiv g^e \bmod p, \; g \text{ is irreducible over } R/(p), \text{ and } e \ge 2. \tag{3.1}$$

Over $R/(p)$ the factorization of f into irreducible factors can be computed in probabilistic polynomial time by Berlekamp (1970).

We have seen in the previous section that there may be proper irreducible factors modulo small prime powers, even in the case where f is irreducible over $R_{(p)}$. However, it turns out that lifting the factorization of f over $R/(p)$ to a factorization over $R/(p^k)$ is sufficient.

LEMMA 3.1. *Let f, p, g, e be as in (3.1) and $f \equiv uw \bmod p^k$ for some $k \ge 1$ with $u, w \in R[x]$ monic and $u \equiv g^l \bmod p$, $w \equiv g^{e-l} \bmod p$ for some $l \le \frac{e}{2}$. Then the following are equivalent:*

(i) $\frac{f-uw}{p^k} \in R[x]$ is over $R/(p)$ divisible by g^l.

(ii) For every $\varphi \in R[x]$ with $\deg \varphi < \deg u$ there exists a polynomial $\psi \in R[x]$ with $\deg \psi < \deg w$ such that $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$.

(iii) *There exist polynomials* $\varphi, \psi \in R[x]$ *with* $\deg \varphi < \deg u$ *and* $\deg \psi < \deg w$ *such that* $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$.

(iv) *There exist polynomials* $\varphi, \psi \in R[x]$ *with* $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$.

PROOF. "(i) $\Rightarrow$ (ii)": Let $\frac{f-uw}{p^k} \equiv g^l\alpha \bmod p$ with $\alpha \in R[x]$, and $\varphi, \psi \in R[x]$ with $\deg \varphi < \deg u$, and $\psi \equiv \alpha - g^{e-2l}\varphi \bmod p$. Then $\deg \psi < \deg w$, and

$$\begin{aligned} f - (u + p^k\varphi)(w + p^k\psi) &\equiv f - uw - p^k(\varphi w + \psi u) \\ &\equiv f - uw - p^k(\varphi g^{e-l} + (\alpha - g^{e-2l}\varphi)g^l) \\ &\equiv f - uw - p^k g^l \alpha \\ &\equiv 0 \bmod p^{k+1}. \end{aligned}$$

It is clear that (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv). Hence, it remains to show that (i) follows from (iv). Let $\varphi, \psi \in R[x]$ with $f \equiv (u + p^k\varphi)(w + p^k\psi) \bmod p^{k+1}$. Then

$$\begin{aligned} \frac{f - uw}{p^k} &\equiv \varphi w + \psi u \\ &\equiv \varphi g^{e-l} + \psi g^l \equiv g^l(\varphi g^{e-2l} + \psi) \bmod p. \quad \square \end{aligned}$$

COROLLARY 3.2. *Let* $p \in R$ *be a prime and* $f \in R[x]$ *an Eisenstein polynomial, i.e.,* $f = \sum_{0 \le i \le n} a_i x^i$ *with* $a_n = 1$, $a_i \equiv 0 \bmod p$ *for* $0 \le i < n$, *and* $a_0 \not\equiv 0 \bmod p^2$. *Then* f *is irreducible over* $R/(p^k)$ *for every* $k \ge 2$.

PROOF. We have $f \equiv x^n \bmod p$, and hence $g = x$. Now let $1 \le l \le n/2$. Then

$$\frac{f - x^l \cdot x^{n-l}}{p} = \frac{f - x^n}{p} = \sum_{0 \le i < n} \frac{a_i}{p} x^i.$$

Since $\frac{a_0}{p} \not\equiv 0 \bmod p$, this is not divisible by x^l over $R/(p)$. Hence by Lemma 3.1 the factorization $f \equiv x^l \cdot x^{n-l} \bmod p$ cannot be lifted to a factorization over $R/(p^2)$ for all $1 \le l \le n/2$. Hence f is irreducible over $R/(p^2)$ and therefore irreducible over $R/(p^k)$ for all $k \ge 2$. $\square$

Now it is clear how an algorithm for factoring polynomials modulo small prime powers could look like. For $1 \le l \le e/2$ we have to start with the factorization $f \equiv g^l \cdot g^{e-l} \bmod p$ and then lift it to a factorization over $R/(p^k)$. Here, Lemma 3.1 can be used to decide whether a factorization can be lifted.

Of course, for every l there can be lots of factorizations. For every factorization which has been found, the factors have to be factored again with Lemma 3.1.

There is one possible improvement of the above algorithm. If the factorization $f \equiv uw \bmod p^k$ is already computed and it can be lifted (i.e., $\frac{f-uw}{p^k} \equiv g^l\alpha \bmod p$), then we have the factorization

$$f \equiv (u + p^k\varphi)(w + p^k(\alpha - g^{e-2l}\varphi)) \bmod p^{k+1}$$

for every $\varphi \in R[x]$ with $\deg \varphi < \deg u$ by Lemma 3.1. Now we can deal with φ in a symbolic way as a formal parameter. When computing

$$\frac{f - (u + p^k\varphi)(h + p^k(\alpha - g^{e-2l}\varphi))}{p^{k+1}} \bmod p$$

one obtains some relations which have to hold for φ such that this factorization can be lifted.

EXAMPLE 3.3. *Let $R = \mathbb{Z}, p = 3$, and $f = x^2+27x+162$. Then $f \equiv x^2 \bmod 3$, and $\frac{f-x^2}{3} \equiv 0 \bmod 3$. Hence we take $u = w = g = x$, $e = 2$, $l = 1$, $\alpha = 0$, and have*

$$f \equiv (x + 3\varphi)(x + 3(-\varphi)) \equiv (x + 3\varphi)(x + 6\varphi) \bmod 9, \qquad (3.2)$$

with $0 \leq \varphi \leq 2$. Then

$$\frac{f - (x + 3\varphi)(x + 6\varphi)}{9} \equiv 2(\varphi + \varphi^2) \bmod 3.$$

Hence a factorization of the form (3.2) can be lifted to a factorization over $\mathbb{Z}/(27)$ if and only if $\varphi = 0$ or $\varphi = 2$. These two possiblities have to be tested separately.

This method works as long as the relations which hold for the parameters are not too complicated. But the following examples show that the number of parameters and equations can be quite large.

EXAMPLE 3.4. *We take $R = \mathbb{Z}$, $f = x^{10}$, and $p = 3$. Then with $l = 4$ we obtain after three lifting steps the following 3^{10} factorizations:*

$$f \equiv uw \bmod 81$$

with

$$\begin{aligned} u &= x^4 + 3\varphi_3x^3 + 3\varphi_2x^2 + 9\varphi_1x + 9\varphi_0 \\ w &= x^6 + 78\varphi_3x^5 + (78\varphi_2 + 9\varphi_3^2)x^4 + (72\varphi_1 + 18\varphi_2\varphi_3 + 54\varphi_3^3)x^3 \\ &\quad +(72\varphi_0 + 9\varphi_2^2 + 54\varphi_1\varphi_3)x^2 + (54\varphi_0\varphi_3 + 54\varphi_1\varphi_2)x + 54\varphi_0\varphi_2 + 54\varphi_2^3, \end{aligned}$$

and $0 \le \varphi_i < 27$ *for* $i \in \{2,3\}$, *and* $0 \le \varphi_i < 9$ *for* $i \in \{0,1\}$. *Then*

$$\begin{aligned}\frac{f-uw}{81} \equiv\ & 2\varphi_3x^9 + 2\varphi_2x^8 + (2\varphi_3^3+2\varphi_1)x^7 + (2\varphi_3^2\varphi_2+2\varphi_0+\varphi_3^4)x^6 \\ & +(2\varphi_2^2\varphi_3+\varphi_2\varphi_3^3)x^5 + (2\varphi_2^3+\varphi_1^2)x^4 \\ & +(2\varphi_0\varphi_1+\varphi_1\varphi_2^3)x^3 + (\varphi_0^2+\varphi_2^4)x^2 \bmod 3.\end{aligned}$$

By Lemma 3.1, the factorization can be lifted to a factorization over $\mathbb{Z}/(243)$ *if and only if*

$$\begin{aligned}2\varphi_0\varphi_1+\varphi_1\varphi_2^3 &\equiv 0 \bmod 3, \\ \varphi_0^2+\varphi_2^2 &\equiv 0 \bmod 3.\end{aligned}$$

Since the sum of two nonzero squares is not 0 *over* $\mathbb{Z}/(3)$, *this implies* $\varphi_0 \equiv \varphi_2 \equiv 0 \bmod 3$, *and hence the factorization can be lifted if and only if* $\varphi_0 \equiv \varphi_2 \equiv 0 \bmod 3$. *This yields* 3^8 *different factorizations which can be lifted to a factorization over* $\mathbb{Z}/(243)$.

In the next example we see that things become more complicated if the degree of f becomes larger:

EXAMPLE 3.5. *We take* $R = \mathbb{Z}$, $p = 3$, $f = x^{20}$, *and* $l = 10$. *Then after two lifting steps we obtain the* 3^{15} *factorizations*

$$f \equiv uw \bmod 27$$

with

$$\begin{aligned}u =\ & x^{10}+3\varphi_1x^9+3\varphi_2x^8+3\varphi_3x^7+3\varphi_4x^6+3\varphi_5x^5+9\varphi_6x^4+9\varphi_7x^3 \\ & +9\varphi_8x^2+9\varphi_9x+9\varphi_{10}, \\ w =\ & x^{10}+24\varphi_1x^9+(24\varphi_2+9\varphi_1^2)x^8+(24\varphi_3+18\varphi_1\varphi_2)x^7 \\ & +(24\varphi_4+9\varphi_2^2+18\varphi_1\varphi_3)x^6+(24\varphi_5+18\varphi_2\varphi_3+18\varphi_1\varphi_4)x^5 \\ & +(18\varphi_1\varphi_5+9\varphi_3^2+18\varphi_6+18\varphi_2\varphi_4)x^4+(18\varphi_7+18\varphi_2\varphi_5+18\varphi_3\varphi_4)x^3 \\ & +(9\varphi_4^2+18\varphi_8+18\varphi_3\varphi_5)x^2+(18\varphi_9+18\varphi_4\varphi_5)x \\ & +9\varphi_5^2+18\varphi_{10},\end{aligned}$$

and $0 \le \varphi_i < 9$ *for* $1 \le i \le 5$, *and* $0 \le \varphi_i < 3$ *for* $6 \le i \le 10$. *Since for every factorization of the above form such that there exists an* i *with* $\varphi_i \ne 0$ *there is another in which* u *and* w *are interchanged, there are* $\frac{3^{15}+1}{2}$ *different* *factorizations. By Lemma 3.1, the factorization can be lifted if and only if* $\frac{f-uw}{27}$ *is divisible by* x^{10} *over* $\mathbb{Z}/(3)$*, and this holds if and only if*

$$\begin{aligned}
\varphi_5\varphi_6 + \varphi_2\varphi_9 + \varphi_4\varphi_7 + \varphi_3\varphi_8 + \varphi_1\varphi_{10} &\equiv 0 \bmod 3\\
\varphi_3\varphi_9 + \varphi_5\varphi_7 + \varphi_2\varphi_{10} + \varphi_4\varphi_8 + \varphi_4 &\equiv 0 \bmod 3\\
\varphi_3\varphi_{10} + \varphi_5\varphi_8 + \varphi_4\varphi_9 &\equiv 0 \bmod 3\\
\varphi_5\varphi_9 + \varphi_4\varphi_{10} &\equiv 0 \bmod 3\\
\varphi_5 + \varphi_5\varphi_{10} &\equiv 0 \bmod 3.
\end{aligned}$$

If one solves the system of polynomial equations (e.g., by hand), one obtains the following solutions:

$$(0,0,0,0,0,\varphi_6,\varphi_7,\varphi_8,\varphi_9,\varphi_{10}),(\varphi_1,0,0,0,0,\varphi_6,\varphi_7,\varphi_8,\varphi_9,0)$$

$$(\varphi_1,\varphi_2,\varphi_3,0,0,\varphi_6,\varphi_7,0,0,0),(\varphi_1,\varphi_2,0,0,0,\varphi_6,\varphi_7,\varphi_8,0,0),$$
$$(\varphi_1,\varphi_2,0,0,0,\varphi_6,\varphi_7,\varphi_8,0,0),(\varphi_1,\varphi_2,\varphi_4\varphi_7,\varphi_4,0,\varphi_6,\varphi_7,2,0,0),$$
$$(\varphi_5(\varphi_6+2\varphi_7\varphi_9+2\varphi_9^2+\varphi_8^2),\varphi_5(\varphi_7+2\varphi_8\varphi_9+2\varphi_9),\varphi_5(\varphi_8+\varphi_9^2),\varphi_5\varphi_9,\varphi_5,$$
$$\varphi_6,\varphi_7,\varphi_8,\varphi_9,2),$$

where φ_i *for* $1 \le i \le 10$ *is arbitrary.*

In general, it is not clear how to solve the resulting system of polynomial equations symbolically; we can, of course, always substitute individual values for the parameters.

A different version of Lemma 3.1 can be used to formulate an algorithm which uses a quadratic lifting procedure.

LEMMA 3.6. *Let* f,p,g,e *as in (3.1),* $\deg g = n$*,* $1 \le l \le e/2$*, and* $u,w \in R[x]$ *monic with* $u \equiv g^l \bmod p$*,* $w \equiv g^{e-l} \bmod p$ *such that* $f \equiv uw \bmod p^k$*. Let* $\varphi = \sum_{0\le i<nl} \varphi_i x^i \in R[x]$*,* $\psi = \sum_{0\le i<(e-l)n} \psi_i x^i \in R[x]$*, and write* $\frac{f-uw}{p^k} = \sum_{0\le i<ne} a_i x^i$ *with* $a_i \in R$ *for* $0 \le i < ne$*. Then* $f \equiv (u+p^k\varphi)(w+p^k\psi) \bmod p^{2k}$ *if and only if*

$$S(u,w)\begin{pmatrix}\psi_{(e-l)n-1}\\ \vdots\\ \psi_0\\ \varphi_{ln-1}\\ \vdots\\ \varphi_0\end{pmatrix} \equiv \begin{pmatrix}a_{en-1}\\ a_{en-2}\\ \vdots\\ a_0\end{pmatrix} \bmod p^k.$$

PROOF. We have

$$
\begin{aligned}
f \equiv (u+p^k\varphi)(w+p^k\psi) \bmod p^{2k} &\Leftrightarrow f-uw \equiv p^k(\psi u+\varphi w) \bmod p^{2k}\\
\Leftrightarrow \quad \frac{f-uw}{p^k} &\equiv \psi u+\varphi w \bmod p^k\\
\Leftrightarrow \quad S(u,w)\begin{pmatrix} \psi_{(e-l)n-1}\\ \vdots \\ \psi_0 \\ \varphi_{ln-1} \\ \vdots \\ \varphi_0 \end{pmatrix} &\equiv \begin{pmatrix} a_{en-1}\\ a_{en-2} \\ \vdots \\ a_0 \end{pmatrix} \bmod p^k. \quad \square
\end{aligned}
$$

The last congruence is a system of linear equations which has to be solved over $R/(p^k)$. This can be done in polynomial time by Iliopoulos (1989) and Kaltofen *et al.* (1990). In von zur Gathen & Hartlieb (1996) the solution of a system of linear equations is represented by a basis and a number of parameters togehter with their feasible ranges. These parameters are used in a symbolic way to represent all solutions concisely. We do not see how we can do this here, because in dealing with the solutions we have to solve the next system of linear equations, where the parameters are involved. Since the shape of the Smith Normal Form may be different for different values of the parameters, we do not see how this can be done for all parameters at once. Hence we have to proceed for each solution separately.

Thus we obtain the following algorithm for factoring modulo small prime powers. With the notation of (3.1) we first choose an $1 \leq l \leq e/2$ and start with the factorization $f \equiv g^l \cdot g^{e-l} \bmod p$. Then this is lifted by solving a system of linear equations to a set of factorizations over $R/(p^2)$. All these factorizations are then lifted, if possible, to factorizations over $R/(p^4)$, then to factorizations over $R/(p^8)$, and so on. Hence, if there is an addition chain (see Knuth (1981) for the definition) for k of length $l(k)$, after $l(k)$ steps all factorization $f \equiv uw \bmod p^k$ with $u, w \in R[x]$ monic, $u \equiv g^l \bmod p$, and $w \equiv g^{e-l} \bmod p$ are computed. By Brauer (1939), we may assume that $l(k) \leq \log k + o(\log k)$. Of course, this version needs fewer lifting steps than the linear algorithm but the bound on the number of factorizations which can occur is the same. Hence in the worst case the number of computations which have to be made are the same. Since we do linear algebra here instead of polynomial computations, one computation is more costly than in the linear version. But the practical advantage is that sometimes factorizations which cannot be lifted to a factorization over $R/(p^k)$ are detected earlier and no longer dealt with.

References

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. Brauer, On addition chains. *Bull. Amer. Math. Soc.* **45** (1939), 736–739.

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. 1. John Wiley & Sons, 1974.

J. von zur Gathen and S. Hartlieb, Factoring modular polynomials. In *Proc. ISSAC '96*, 1996. To appear.

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

D. E. Knuth, *The Art of Computer Programming, Vol.2, Seminumerical Algorithms*. Addison-Wesley, Reading MA, 2 edition, 1981.