MATHEMATICS OF COMPUTATION, VOLUME 32, NUMBER 141
JANUARY 1978, PAGES 287–292

A Remark on the Hensel Factorization Method

By Hans Zassenhaus

Abstract. In response to a remark of David Yun a new version of "On Hensel factorization I" (*J. Number Theory*, v. 1, 1969) is given which sets in evidence the quadratic convergence behavior of the method using a minimum of bookkeeping.

In 1974 it was shown by Miola and Yun (see also Yun (1975)) that a p-adic method of polynomial factorization which apparently was suggested in Zassenhaus (1969) usually is slower than a similar method suggested by K. Hensel (1913) even though the first method exhibits quadratic convergence while the second is a linearly convergent approximation method.

However, as in all numerical work in algebraic number theory, it is necessary to develop the underlying idea to its full range of application for the purpose of a fair comparison of effectivity. It is the purpose of this note to indicate in greater detail the algorithm recommended in accordance with Zassenhaus (1969) for the purpose of finding a congruence factorization

$$f(t) \equiv f_{1k} f_{2k}(t) \pmod{p^{2^k} \mathbb{Z}[t]}, \tag{1}$$

provided a congruence factorization

$$f(t) \equiv f_1(t) f_2(t) \pmod{p\mathbb{Z}[t]} \tag{2}$$

as well as a congruence

$$f_1(t)g_1(t) + f_2(t)g_2(t) \equiv 1 \pmod{p\mathbb{Z}[t] + f(t)\mathbb{Z}[t]} \tag{3}$$

are known already.

Here p is a prime number, and f, f_1, f_2, g_1, g_2, are members of the ring of polynomials $\mathbb{Z}[t]$ in the variable t over the rational integer ring $\mathbb{Z}$ with f, f_1, f_2 being monic nonconstant, k is a natural number and f_{1k}, f_{2k} are desired to be monic members of $\mathbb{Z}[t]$ satisfying the coherence condition

$$f_{jk}(t) \equiv f_j(t) \pmod{p\mathbb{Z}[t]} \ (j = 1, 2). \tag{4}$$

Before the method of approach is explained, let us agree on the following two reductions:

(1) By the common polynomial long division method we find for any member A of $\mathbb{Z}[t]$ and for any monic member B of $\mathbb{Z}[t]$ an equation

Received October 5, 1976.
AMS (MOS) subject classifications (1970). Primary 12–04.

Copyright © 1978, American Mathematical Society

(5) $$A = Q(A, B)B + R(A, B),$$

where $Q(A, B)$, $R(A, B)$ are members of $\mathbb{Z}[t]$ such that either $R(A, B) = 0$ or the degree of $R(A, B)$ is less than the degree of B.

It follows from (2) that the degrees $[f]$, $[f_1]$, $[f_2]$ of f, f_1, f_2 respectively satisfy the equation,

(6) $$[f] = [f_1] + [f_2].$$

In case the degree of g_1 should happen to be not less than the degree of f_2 replace g_1, g_2 by $\bar{g}_2 = g_2 - Q(g_2, f_1)f_1, \bar{g}_1 = g_1 - Q(g_1, f_2)f_2$.

It follows that $f_1\bar{g}_1 + f_2\bar{g}_2 \equiv 1 \pmod{p\mathbb{Z}[t]}$ and $[\bar{g}_1] < [f_2]$, $[\bar{g}_2] < [f_1]$.

Thus, without loss of generality (3) may be replaced by

(3)′ $$f_1g_1 + f_2g_2 \equiv 1 \pmod{p\mathbb{Z}[t]}, \quad [g_j] < [f_{3-j}] \quad (j = 1, 2).$$

(2) If A is a rational integer, B a nonzero rational integer then we find by long division an equation (5) with rational integers $Q(A, B)$, $R(A, B)$ subject to the inequalities

(6) $$-|B| < 2R(A, B) \leqslant |B|$$

characterizing $R(A, B)$ as absolutely least remainder modulo B.

If instead

(7a) $$A = \sum_{i=0}^{n} A_i t^i \quad (n \in \mathbb{Z} \geqslant 0; A_i \in \mathbb{Z}, 0 \leqslant i \leqslant n),$$

then there obtains the equation (5) with

(7b) $$Q(A, B) = \sum_{i=0}^{n} Q(A_i, B)t^i, \qquad R(A, B) = \sum_{i=0}^{n} R(A_i, B)t^i.$$

Without loss of generality we may assume that the polynomials f_j satisfy the additional condition

(8) $$f_j = R(f_j, p) \qquad (j = 1, 2),$$

conferring the advantage of using polynomials all of whose coefficients are least absolute remainders to a certain module.

The algorithm is as follows: Let

(9a) $$E_{10} = f_1g_1, \qquad N_0 = R(E_{10}^2 - E_{10}, f).$$

If $N_0 = 0$, then let $E_{1j} = E_{10}$ $(0 < j \leqslant k)$, $\nu_k = 2^k$. Otherwise, there is an exponent $\nu_0 \geqslant 1$ for which

(9b) $$p^{\nu_0} \| N_0,$$

where the '$\|$' symbol indicates that precisely the ν_0th power of p divides N_0; in other words,

(9c) $$p^{\nu_0} | N_0, \qquad p^{\nu_0+1} \nmid N_0.$$

Suppose we defined already $E_{1,j-1}$ and $N_{j-1} = R(E_{1,j-1}^2 E_{1,j-1}, f)$ subject to the condition that

$$p^{\nu_{j-1}} \| N_{j-1} \tag{9d}$$

for some exponent ν_{j-1} satisfying the inequality

$$\nu_{j-1} \geqslant 2^{j-1}. \tag{9e}$$

Then let

$$E_{1j} = R(E_{1,j-1} + N_{j-1} - 2R(E_{1,j-1}N_{j-1}, f), p^{2\nu_{j-1}}), \tag{9f}$$

$$N_j = R(E_{1j}^2 - E_{1j}, f),$$

and here we have either $N_j = 0$ or there is an exponent ν_j satisfying the inequality

$$\nu_j \geqslant 2\nu_{j-1} \geqslant 2^j \tag{9g}$$

such that

$$p^{\nu_j} \| N_j. \tag{9h}$$

If $N_j = 0$, then let

$$E_{1h} = E_{1j}, \qquad \nu_h = 2^{h-j+1}\nu_{j-1} \qquad (j \leqslant h \leqslant k).$$

Otherwise, we continue with the algorithm.

Having obtained E_{1k}, we define f_{1k} by

$$f_{1k} \equiv \gcd(E_{1k}, f) \pmod{p^{\nu_k}\mathbb{Z}[t]}, \tag{10a}$$

$$f_{1k} = R(f_{1k}, f), \qquad f_{1k} \text{ monic}, f_{1k} = R(f_{1k}, p^{\nu_k}). \tag{10b}$$

Let us explain the items (9a), (9b) and (10). From (3) and (9a) we infer that

$$E_{10} \equiv f_1 g_1 \pmod{p\mathbb{Z}[t]},$$

$$1 - E_{10} \equiv f_2 g_2 \pmod{p\mathbb{Z}[t]},$$

$$E_{10} - E_{10}^2 = E_{10}(1 - E_{10}) \equiv f_1 f_2 g_1 g_2 \equiv f \pmod{p\mathbb{Z}[t]}.$$

Suppose

$$N_{j-1} \equiv E_{1,j-1}^2 - E_{1,j-1} \pmod{f\mathbb{Z}[t]},$$

$$E_{1,j} \equiv E_{1,j-1} + N_{j-1} - 2E_{1,j-1}N_{j-1} \pmod{f\mathbb{Z}[t] + p^{2\nu_{j-1}}\mathbf{Z}[t]},$$

then we have

$$\begin{aligned} E_{1j}^2 - E_{1j} &\equiv E_{1,j-1}^2 + N_{j-1}^2 + 4E_{1,j-1}^2 N_{j-1}^2 \\ &\quad + 2E_{1,j-1}N_{j-1} - 4E_{1,j-1}^2 N_{j-1} - 4E_{1,j-1}N_{j-1}^2 \\ &\quad - E_{1,j-1} - N_{j-1} + 4E_{1,j-1}N_{j-1} \\ &\equiv N_{j-1}^2 \pmod{f\mathbb{Z}[t] + p^{2\nu_{j-1}}\mathbf{Z}[t]}. \end{aligned}$$

Thus, we obtain either $N_j = 0$ or (9h), (9g).

In general, the factor ring $R = \mathbb{Z}[t]/p^\nu\mathbb{Z}[t]$ (p a prime number, ν a natural number) need not be a unique factorization ring nor is there always a greatest common divisor ($\gcd(u, v)$) of two given elements u, v. E.g., $(t+2)^2 \equiv (t-2)^2 \pmod{2^3\mathbb{Z}[t]}$, and $\gcd((t+2)^2/2^3\mathbb{Z}[t], (t^2-4)/2^3\mathbb{Z}[t])$ does not exist. But if $uR + vR = wR$, then $w = \gcd(u, v)$. We have the following algorithm to decide whether the ideal $uR + vR$ is principal and to exhibit a generator w in case there is one.

(1) If $\nu = 1$, then there always is a $\gcd(u, v)$ generating $uR + vR$ which is obtained by the standard Euclidean division algorithm for polynomials over the field of p elements.

(2) The $\gcd(u, v)$ exists if and only if $\gcd(v, u)$ exists and both are equal. We have $uR + vR = wR$ if and only if $vR + uR = wR$.

(3) The $\gcd(0, v) = v = 0.0 + 1.v$ generates $uR + vR = vR$.

(4) If $\nu > \mu > 0$ and $p^\mu \| u$, $p^\mu | v$ so that $u \equiv p^\mu v_1$, $v \equiv p^\mu v_1 \pmod{p^\nu\mathbb{Z}[t]}$ with u_1, v_1 in $\mathbb{Z}[t]$ and $p \nmid u_1$, then $\gcd(u, v)$ exists if and only if $\gcd(u_1 \mid \mathbb{Z}^{\nu-\mu}[t], v_1/\mathbb{Z}^{\nu-\mu}[t]) = w_1/\mathbb{Z}^{\nu-\mu}[t]$ exists with w_1 some polynomial of $\mathbb{Z}[t]$ that is not divisible by p. Moreover, $w = \gcd(u, v) = p^\mu w_1/\mathbb{Z}^\nu[t]$ and w generates $uR + vR$ if and only if $u_1\mathbb{Z}^{\nu-\mu}[t] + v_1\mathbb{Z}^{\nu-\mu}[t] = w_1\mathbb{Z}^{\nu-\mu}[t]$. Indeed, a presentation $u_1 a + v_1 b = w_1$ with a, b in $\mathbb{Z}[t]$ implies the presentation $w = ua/p^\nu\mathbb{Z}[t] + vb/p^\nu\mathbb{Z}[t]$.

(5) If $v > 1$ and $u \equiv p^{\mu+1}u_0 t^{\kappa+1} + u_1 p^\mu u_2 \pmod{p^\nu\mathbb{Z}[t]}$, $(0 \leqslant \mu < \nu; u_0, u_2 \in \mathbb{Z}[t]; [u_2] < \kappa; p \nmid u_1 \in \mathbb{Z})$, then determine a rational integer u_1 satisfying the congruence condition $u_1 u_1' \equiv 1 \pmod{p^{\nu-\mu}}$ and set

$$u' \equiv p^{\mu+1}u_0 u_1' t^{\kappa+1} + p^\mu t^\kappa + p^\mu u_2 u_1 \pmod{p^\nu\mathbb{Z}[t]}.$$

It follows that $\gcd(u, v)$ exists if and only if $\gcd(u', v)$ exists. Moreover, $uR + vR = u'R + vR$. If $u'a' + vb = w$, $wR = uR + vR$, then $u(u_1'a') + vb = w$.

(6) If $\nu > 1$ and

$$u \equiv p^{\mu+\lambda}u_0 t^{\kappa+1} + p^\mu t^\kappa + p^\mu u_2 \pmod{p^\nu\mathbb{Z}[t]}$$

$$(0 \leqslant \mu < \mu + \lambda < \nu; u_0, u_2 \in \mathbb{Z}[t]; [u_2] < \kappa),$$

then let

$$u_1' \equiv 1 - p^\lambda u_0 + p^{2\lambda}u_0^2 - \cdots + (-1)^\alpha p^{\alpha\lambda}u_0^\alpha \pmod{p^{\nu-\mu}\mathbb{Z}[t]}$$

$$(\alpha = [(\mu - \nu)/\lambda])$$

and set $u \equiv u_1' u \pmod{p^\nu\mathbb{Z}[t]}$ so that $u' \equiv p^\mu(t^\kappa + u_2') \pmod{p^\nu\mathbb{Z}[t]}$ $u_2' \in \mathbb{Z}[t]$, $[u_2'] < \kappa$.

It follows that $\gcd(u, v)$ exists if and only if $\gcd(u', v)$ exists. Moreover, $uR + vR = uR + vR$. If $u'a' + vb = w$, $wR = uR + vR$, then $u(u'a') + vb = w$.

(7) If $v > 1$ and

$$u \equiv t^\kappa + u_2, \quad v \equiv v_1 t^\lambda + v_2 \pmod{p^\nu\mathbb{Z}[t]}$$

$$(0 \leqslant \kappa \leqslant \lambda; u_2, v_2 \in \mathbb{Z}[t]; [u_2] < \kappa, [v_2] < \lambda; v_1 \in \mathbb{Z}),$$

then let $v' \equiv v - t^{\lambda-\kappa}v_1 u$ so that $\gcd(u, v)$ exists if and only if $\gcd(u, v')$ exists and

$uR + vR = uR + wR$. If $ua' + vb = w$ generates $uR + vR$, then $w = ua + vb$ with $a = a' - t^{\lambda-\kappa}bv_1$. By a finite number of applications of (1)–(7) either we find a presentation $ua + vb = \gcd(u, v)$ or else we find that $uR + vR = p^{\mu}(u'R + p^{\lambda}v'R)$ where $0 \leqslant \mu < \mu + \lambda < \nu$ and u', v' are congruent to monic polynomials P, Q of $\mathbb{Z}[t]$ modulo $p^{\nu-\mu}\mathbb{Z}[t]$ with $[P] > [Q]$. In this case $uR + vR$ is not principal.

In the situation of (9f) it was shown in Zassenhaus (1969) that $\gcd(E_{1k}/p^{\nu k}\mathbb{Z}[t], f/p^{\nu k}\mathbb{Z}[t])$ exists and is representable by a monic polynomial f_{1k} of $\mathbb{Z}[t]$. In fact, by carrying out (10a) we obtain a polynomial f_{1k} with highest coefficient λ not divisible by p. Now solve the congruence $\lambda\lambda' \equiv 1 \pmod{p^{\nu k}}$ so as to satisfy both (10a) and (10b).

Let us point out that the Berlekamp algorithm directly for $p = 2$ and by an easy computation for $p > 2$ provides a system of f, p-reduced polynomials $e_{01}, \ldots, e_{0r}$ representing modulo $f(t)\mathbb{Z}[t] + p\mathbb{Z}[t]$.

By the method given above we obtain for any given natural number ν polynomials $e_1, \ldots, e_r$ that are f, p^{ν}-reduced and represent the primitive idempotents modulo $f(t)\mathbb{Z}[t] + p^{\nu}\mathbb{Z}[t]$.

According to Zassenhaus (1969), their existence is tantamount to the existence of a congruence factorization

$$f \equiv f_1 f_2 \cdots f_r \pmod{p^{\nu}\mathbb{Z}[t]}$$

with monic polynomials $f_1, \ldots, f_r$ of $\mathbb{Z}[t]$ that are mutually prime modulo p; and each of them is congruent to a power of some monic polynomial mod p which stays irreducible modulo p. The numbering can be done in such a way that $f_i e_i \equiv 0 \pmod{f\mathbb{Z}[t] + p^{\nu}\mathbb{Z}[t]}$, and we obtain the monic polynomials $f_1, \ldots, f_r$ in the form

$$\begin{aligned}
f_1 &= R(\gcd(f/p^{\nu}\mathbb{Z}[t], (e_2 + \cdots + e_r)/p^{\nu}\mathbb{Z}[t]), p^{\nu}),\\
\hat{f}_1 &= R(Q(f/p^{\nu}\mathbb{Z}[t], f_1/p^{\nu}\mathbb{Z}[t]), p^{\nu}),\\
f_2 &= R(\gcd(\hat{f}_1/p^{\nu}\mathbb{Z}[t], (e_3 + \cdots + e_r)/p^{\nu}\mathbb{Z}[t]), p^{\nu}),\\
&\cdots\\
f_r &= R(Q(\hat{f}_{r-1}/p^{\nu}\mathbb{Z}[t], f_{r-1}/p^{\nu}\mathbb{Z}[t]), p^{\nu}).
\end{aligned}$$

Example.

$$\begin{aligned}
f(t) &= t^3 - 5t^2 - 7t + 6,\\
\varphi(f) &= \max(f/3, \sqrt{7/3}, \sqrt[3]{6} < 8(\sqrt[3]{2} - 1).
\end{aligned}$$

If $f = f_1 f_2$ with monic rational polynomials f_1, f_2 of degrees 1, 2, then $\varphi(f_1) < 8(\sqrt[3]{2} - 1)/(\sqrt[3]{2} - 1) = 8$. Let $p = 2$. Hence $\nu = 4$. By Berlekamp $1^2 \equiv 1, (t)^2 \equiv t^2, (t^2)^2 \equiv t \pmod{f\mathbb{Z}[t] + 2\mathbb{Z}[t]}$, basic idempotents $1, t^2 + t$. Set $E_{10} = t^2 + t$, $N_0 = R(E_{10}^2 - E_{10}, f) = 42t^2 + 42t - 42$, $\nu_0 = 1$, $E_{11} = -t^2 - t + 2$, $N_1 = 40t^2 + 40t - 40$, $\nu = 3$. $E_{12} \equiv E_{11} + N_1 \equiv 7t^2 + 7t - 6 \pmod{16\mathbb{Z}[t]}$ $\gcd(f/16\mathbb{Z}[t], (7t^2 + 7t - 6)/(6\mathbb{Z}[t])) = (t - 6)/16\mathbb{Z}[t], f(t) = (t - 6)(t^2 + t - 1)$.

Obviously three linear Hensel approximations would be slower.

Department of Mathematics
The Ohio State University
Columbus, Ohio 43210

1. A. MIOLA & D. Y. Y. YUN, *The Computational Aspects of Hensel-Type Univariate Polynomial Greatest Common Divisor Algorithms,* Proc. Eurosam 1974 (ACM SIGSAM Bull. No. 31), Stockholm, Sweden, August 1974, pp. 46–54.

2. DAVID Y. Y. YUN, *Hensel Meets Newton–Algebraic Constructions in an Analytic Setting,* RC 5538 IBM Research, July 1975, 11pp.

3. HANS ZASSENHAUS, "On Hensel factorization. I," *J. Number Theory,* v. 1, 1969, pp. 291–311.