ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

ON POLYNOMIAL FACTORIZATION

HANS ZASSENHAUS

Dedicated to the memory of E.G. Straus

Introduction. This note originated in response to the paper [3] by A.K. Lenstra, H.W. Lenstra, Jr., and L. Lovász.

In that paper an earlier p-adic method of polynomial factorization over the rational integer ring $\mathbf{Z}$ which the author had communicated only orally is proven to be feasible in polynomial time in terms of the degree $n > 0$ of a given separable monic polynomial

$$f = t^n + a_1 t^{n-1} + \cdots + a_n \tag{1a}$$

with rational integer coefficients $a_1, \ldots, a_n$ and the positive definite quadratic form (1b)

$$|f|^2 = 1 + a_1^2 + \cdots + a_n^2. \tag{1b}$$

Moreover, the authors establish a new elegant and powerful method of polynomial factorization based on the reduction theory of positive definite quadratic forms.

1. Use of the maximal order. Some time ago the author of this note observed that the maximal $\mathbf{Z}$-order

$$\mathfrak{o}_{\max} = C\curlyvee(\mathbf{Z}[t]/f) \tag{2}$$

of the unital hypercomplex system

$$A = \mathbf{Q}[t]/f \tag{3}$$

determined by f as the algebra over the rational number field $\mathbf{Q}$ generated by an element

$$x = t/f \tag{4}$$

with defining relator

$$f(x) = 0 \tag{5}$$

Received by the editors May 28, 1983.

contains all the idempotents of A. In particular, if $e_1, \ldots, e_s$ are the primitive idempotents of A so that

$$A = \bigoplus_{i=1}^{s} A_i \tag{6}$$

is the algebraic sum of the finite extensions

$$A_i = e_i A \tag{7a}$$

of the fields $e_i\mathbf{Q}$ isomorphic to $\mathbf{Q}$, then

$$\mathfrak{o}_{\max} = \bigoplus_{i=1}^{s} e_i \mathfrak{o}_{\max} \tag{7b}$$

where the component rings

$$e_i \mathfrak{o}_{\max} = \mathfrak{o}_{\max} \cap A_i \tag{7c}$$

are the maximal $\mathbf{Z}$-orders of A_i.

Moreover, the author observed that the multiplicative semigroup A^* of A contains a unique maximal finite subsemigroup $\mathrm{MF}(A)$ of the form

$$\mathrm{MF}(A) = \bigoplus_{i=1}^{s} \mathrm{MF}(A_i) \tag{8a}$$

where the maximal finite subsemigroup $\mathrm{MF}(A_i)$ consists of 0 and the (cyclic) torsion subgroup $\mathrm{Tor}\, U(A_i)$ of the unit subgroup $U(A_i)$.

Using the positive definite quadratic form

$$Q\colon A \to R^{\geqq 0} \tag{9a}$$

defined on the n-dimensional $\mathbf{Q}$-linear space A by means of

$$Q(x) = \sum |\theta_i(x)|^2, \tag{9b}$$

where $\theta_1, \ldots, \theta_n$ are the distinct non zero $\mathbf{Q}$-homomorphisms of A into the complex numberfield $\mathbf{C}$, we characterize the elements of $\mathrm{MF}(A)$ as follows.

PROPOSITION 1. *The element x of A^* belongs to $\mathrm{MF}(A)$ if and only if*

$$x \in \mathfrak{o}_{\max} \tag{10a}$$

$$Q(x) = \dim_{\mathbf{Q}} xA. \tag{10b}$$

In fact for any element y of $\mathfrak{o}_{\max}$ not beinging to $\mathrm{MF}(A)$ we have

$$Q(y) > \dim_{\mathbf{Q}} yA. \tag{10c}$$

PROOF. Denoting by

$$n_i = \dim A_i \quad (1 \leqq i \leqq s) \tag{11a}$$

the degree of the finite extension A_i over $e_i\mathbf{Q}$, we may number $\theta_1, \ldots, \theta_n$ in such a way that

$$\theta_i(A_j) = 0 \quad (j \neq h) \tag{11b}$$

and

$$\theta_i | A_h \neq 0, \tag{11c}$$

where

$$m_h = \sum_{k<h} n_k < i \leqq \sum_{k \leqq h} n_k, \tag{11d}$$

and, hence, the restrictions

$$\theta_{m_h} + g | A_h \quad (1 \leqq g \leqq n_h) \tag{11e}$$

are the distinct monomorphisms of A_h in $\mathbf{C}$.

For any element y of A we have

$$yA = \bigoplus_{j=1}^{k(y)} A_{i_j}, \tag{12a}$$

where

$$\begin{gathered} k(y) \in \mathbf{Z}^{\geqq 0} \\ 1 \leqq i_1 < \cdots < i_{k(y)} \leqq s \\ e_{i_j} y \neq 0 \quad (1 \leqq j \leqq k(y)) \end{gathered} \tag{12b}$$

but

$$e_i y = 0 \text{ if } i \neq i_1, \ldots, i_{k(y)}. \tag{12c}$$

Hence,

$$\dim_{\mathbf{Q}} yA = \sum_{j=1}^{k(y)} n_{i_j}, \tag{12d}$$

and y belongs to $\mathfrak{o}_{\max}$ if and only if

$$e_{i_j} y \in e_{i_j} \mathfrak{o}_{\max} \quad (1 \leqq j \leqq k(y)). \tag{12e}$$

But if (12e) is satisfied, then it follows that the product of the conjugates $\theta_{m_{i_j}+g}(y)$ $(1 \leqq g \leqq n_i)$ is equal to the norm of the non-zero algebraic integer e_{i_j} of A_{i_j} over $e_{i_j}\mathbf{Q}$, hence

$$\prod_{g=1}^{n_{ij}} |\theta_{m_{i_j}+g}(y)| \geqq 1 \tag{12f}$$

and by the arithmetic geometric mean inequality

$$\sum_{g=1}^{n_{ij}} |\theta_{m_{i_j}+g}(y)^2 \geqq m \tag{12g}$$

with equality if and only if

(12h) $\quad |\theta_{m_{i_j}+g}(y)| = 1 \quad (1 \leqq g \leqq n_{i_j})$, in other terms;

(12i) $\quad e_{i_j} y \in \operatorname{Tor} Ue_{i_j}\mathfrak{o}_{\max} = \operatorname{Tor} U(A_{i_j})$.

Hence (10c) follows unless (12i) holds for $j = 1, 2, \ldots, k(y)$, i.e., y belongs to $\mathrm{MF}(A)$.

As a consequence of Proposition 1, the minima μ_τ forming the chain

(13a) $$\mu_1 \leqq \mu_2 \leqq \cdots \leqq \mu_n$$

of $Q\,|\mathfrak{o}_{\max}$ in the sense of reduction theory for positive definite quadratic forms (see [1], p. 201) are assumed precisely by elements y of $\mathrm{MF}(A)$ subject to the condition

$$\dim_{\mathbf{Q}} yA = n^* = \min_{1 \leqq i \leqq s} n_i$$

in case the dimension τ satisfies

(13b) $$\tau \leqq (n_i = n^*)$$

In particular, the first minimum μ_1 is assumed only by non zero elements y of $\mathfrak{o}_{\max}$ which belong to $\mathrm{MF}(A) \cap A_i$ with minimum value of n_i.

Either

(14a) $$\begin{aligned} &\mu_1 = n \text{ and} \\ &f \text{ irreducible over } \mathbf{Q} \end{aligned}$$

or

(14b) $$\mu_1 < n,$$

and, for

(14c) $$\begin{aligned} &y \in \operatorname{Tor} U(A_{i_j}) \\ &n_i = \min_{1 \leqq k \leqq s} n_k, \end{aligned}$$

it follows that

(14d) $$\begin{aligned} Q(y) &= \mu_1, \\ y &= g_i(x), \\ g &\in \mathbf{Q}[t], \\ [g] &< n, \end{aligned}$$

f is reducible over $\mathbf{Q}$, and the quotient of f and $\gcd(g^{|\operatorname{Tor} U(A_i)|} - 1, f)$ is an irreducible divisor of f over $\mathbf{Q}$.

Thus, if the maximal order of A is known in terms of the equation order $\mathbf{Z}[t]/f$ of f, i.e., if a minimal basis of A, say

$$w_i = h_i(x) \quad (1 \leqq i \leqq n) \tag{15a}$$

with

$$h_i \in \mathbf{Q}[t] \quad (1 \leqq i \leqq n), \tag{15b}$$

$$\mathfrak{o}_{\max} = \sum_{i=1}^{n} \mathbf{Z} w_i, \tag{15c}$$

is known already, then the application of reduction theory to $\mathbf{Q}$ yields the first minimum μ_1 as well as the finite subset of $\mathrm{MF}(A)$ on which Q assumes μ_1; in this way an irreducible divisor of f is exhibited. But the available maximal order embeddings (e.g., [2]) hinge on the knowledge of the square prime factors of the discriminant $d(f)$ of f; it is not known yet whether this knowledge can be achieved in polynomial time depending on n and $\log |f|$ (as defined in [3]).

2. Restriction to the equation order. In [3] it was pointed out that, for any monic polynomial f_1 in t over $\mathbf{Z}$ which enters a congruence factorization

$$f \equiv f_1 \hat{f}_1 \pmod{p\mathbf{Z}[t]} \tag{16a}$$

modulo the prime number p in such a way that $\hat{f}_1$ is monic in t over $\mathbf{Z}$ and f_1 is irreducible modulo p, there is precisely one irreducible monic polynomial h_0 in t over $\mathbf{Z}$ which divides f and which is divisible by f_1 modulo p:

$$f = h_0 h_1 \tag{16b}$$

$$\begin{aligned} &h \equiv f_1 X \pmod{p\mathbf{Z}[t]} \\ &(h_1,\ X \text{ monic in } t \text{ over } \mathbf{Z}). \end{aligned} \tag{16c}$$

An estimate for $Q(h_0(x))$ is obtained as follows.
Let

$$\begin{aligned} &f = \prod_{i=1}^{n} (t - \xi_i) \\ &\xi_i = \theta_i(x) \quad (1 \leqq i \leqq n) \end{aligned} \tag{16d}$$

be a factorization of f in linear factors in $\mathbf{C}$. The magnitude of the roots $\xi_1, \ldots, \xi_n$ is related to the computable quantity

$$\varphi(f) = \max_{1 \leqq i \leqq n} \left| \left(a_i \Big/ \binom{n}{i} \right)^{1/2} \right| \tag{16e}$$

by the inequalities

$$0 \leqq \min_{1\leqq k\leqq n} |\xi_k| \leqq \varphi(f) \leqq \max_{1\leqq k\leqq n} |\xi_k| \leqq \varphi(f)/(2^{1/n} - 1) \tag{16f}$$

as was shown in [6].

Assuming that

$$h_0 = \prod_{i=1}^{m} (t - \xi_i), \tag{16g}$$

we obtain the inequality

$$Q(h_0(x)) = \sum_{i=m+1}^{n} \prod_{j=1}^{m} |\xi_j - \xi_i|^2 \leqq (n - m)(2 \max |\xi_k|)^{2m} \tag{16h}$$

$$Q(h(x) < M_f = \max_{1\leqq k\leqq n} (n - k)\,(2\varphi(f)/(2^{1/n} - 1))^{2k} \tag{16i}$$

for any divisor h of f in $\mathbf{Z}[t]$.

The main result of [3] is summed up and extended by the following theorem.

THEOREM. *Let* (1) *be a monic separable polynomial of degree n over* $\mathbf{Z}$. *Let*

$$f \equiv f_1 \hat{f}_1 \pmod{p^k \mathbf{Z}[t]} \tag{17a}$$

be a congruence factorization of f modulo the k-th power of the prime number p satisfying the conditions

$$p^{2k} > n^n M_f^n \tag{17b}$$

and

$$p \nmid d(f) \tag{17c}$$

such that $f_1, \hat{f}_1$ *are monic polynomials in t over* $\mathbf{Z}$ *and* f_1 *is irreducible modulo p.*

a) *The ideal*

$$L = p^k \mathbf{Z}[t]/f + f_1 \mathbf{Z}[t]/f \tag{17d}$$

of the equation order of f,

$$\mathbf{Z}[t]/f = \mathbf{Z}[x], \tag{17e}$$

where

$$\begin{aligned} x &= t/f \\ f(x) &= 0 \end{aligned} \tag{17f}$$

is of rank n over $\mathbf{Z}$ *with* $\mathbf{Z}$*-basis*

$$1, x, \ldots, x^{[f_1]-1}, f_1(x), \ldots, f_1(x)x^{n-[f_1]-1} \tag{17g}$$

such that upon restriction of Q to L a positive definite quadratic form $Q|L$ on the n-lattice L arises.

b) *Either f is irreducible and the minimum μ of $Q|L$ satisfies the inequality*

$$\mu \geqq p^{2k}/n, \tag{17h}$$

or f is irreducible and

$$\mu < p^{2k}/n. \tag{17i}$$

In the second case μ is assumed for finitely many elements $g(x)$ of L, when g is a polynomial of t over $\mathbf{Z}$ and the greatest common divisor of each g and f is a proper monic divisor of f which is divisible by h_0.

c) *Upon restriction of Q to the d-sublattice L_d of L formed by the elements $P(x)$ of L with P a polynomial of t of degree $< d$ over $\mathbf{Z}$ or $P = 0$, it follows that the minimum of $Q|L_d$ equals p^k if $d \leqq [f_1]$, it is $\geqq p^{2k/n}/n$ if $[f_1] < d \leqq [h_0]$, but it is $< p^{2k/n}/n$ if $[h_0] < d \leqq n$.*

In particular, in case $[h_0] < n$, the minimum of Q on $L_{[h_0]+1}$ is assumed precisely at $\pm h_0(x)$.

Proof. a) was shown in [3].

b) That $h_0(x)$ belongs to L is implied by (16c). Note that

$$Q(h_0(x) < p^{2k/n}/n \tag{18a}$$

because of (17b), (16i).

The norm $N_{A/\mathbf{Q}}(y)$ from A over $\mathbf{Q}$ of any element y of L equals the determinant of the regular representation of L applied to y. Modulo p^k the application of y produces linear combinations of the last n-$[f_1]$ basis elements. Hence, $p^k | N_{A/\mathbf{Q}}(y)$ ($y \in L$). In case $N_{A/\mathbf{Q}}(y) \neq 0$, there holds the inequality

$$\prod_{i=1} |\theta_i(y)| \geqq p^k$$

which implies the inequality

$$\mathbf{Q}(y) = \sum_{i=1}^{n} |\theta_i(y)|^2 \geqq p^{2k/n}/n$$

according to the arithmetic geometric mean inequality.

But if $N_{A/\mathbf{Q}}(y) = 0$, $y = P(x)$, $P \in \mathbf{Z}[t]$, $[P] < n$, then

$$\begin{aligned} &0 \subset yA \subset A \\ &h = \gcd(P, f) \text{ is monic constant in } \mathbf{Q}[t] \\ &P = P_1 h, f = P_2 h, P_1 \in \mathbf{Z}[t], P_2 \in \mathbf{Z}[t], \\ &N_{A/\mathbf{Q}}(P(x) \neq 0. \end{aligned} \tag{18b}$$

The equation $f = h_0 h_1$ with irreducible monic h_0 implies that $A = h_0 A \oplus h_1 A$, $h_1 A = e_1 A$ with primitive idempotent e_1 such that $h_0(e_1 x) = 0$ and $h_0 A = (1 - e_1)A$.

If f_1 does not divide h modulo p, then f_1 divides P_1 modulo p^k and

$$p^k | N_{e_1 A/e_1 \mathbf{Q}}(e_1 P).$$

Also, by construction,

$$N_{e_1 A/e_1 \mathbf{Q}}(e_1 P) \neq 0.$$

Hence, as above,

$$Q(e_1 P(x)) \geqq \frac{p^{2k/\lceil h_0 \rceil}}{[h_0]}$$

$$Q(P(x)) = Q(e_1 P(x)) + Q((1 - e_1)P) \geqq \frac{p^{2k/\lceil h_0 \rceil}}{[h_0]} \geqq \frac{p^{2k/n}}{n}.$$

Finally, if f_1 divides h modulo p, then h_0 divides h as was pointed out above. Hence,

$$h_0 | P, \tag{18c}$$

$$P = h_0 P_3,$$

$$P_3 \in \mathbf{Z}[t],\ [P_3] < n - [h_0] \tag{18d}$$

$$y = h_0(x) P_3(x).$$

Because of (18a), (17b), we have shown b). From (18c) and (18d), we derive c).

3. Concluding remarks. The reduction algorithm given in [**3**] also is applicable to the positive definite quadratic form (9a) using floating point instead of integer programming. However, the methods contained in [**4**], [**5**], [**6**] appear to the author of this note as fast and efficient as the algorithm given in [**3**] and have the advantage of giving precise minima.

One could also form the $\mathbf{Z}[t]/f$-invariant module

$$M = f_1 \mathbf{Z}[t]/f + p^k \{ y \in A \ \& \ \forall i (0 \leqq i < n \Rightarrow \operatorname{tr} y x^i \in \mathbf{Z}) \}$$

with exponent k sufficiently large so that the minimum of Q on M is assumed by the idemptotent e_1 corresponding to f_1.

References

1. J.W.S. Cassels, *An Introduction to the Geometry of Numbers*, Springer Band **99** (1959).

2. David James Ford, *On the Computation of the Maximal Order in a Dedekind Domain*, Dissertation, Ohio State University, 1978.

3. A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534.

4. Hermann Minkowski, *Diskontinuitätsbereich für Arithmetische Äquivalenz*, Werke II, S.53–100.

5. Michael Pohst, Peter Weiler, and Hans Zassenhaus, *On Effective Computation of Fundamental Units*. II, Math. of Comp. **38** (1982), 293–329.

6. Hans Zassenhaus, *Gauss' theory of Ternary Quadratic Forms*, Ternary Quadratic Forms and Norms, edited by Olga Taussky, Marcel Dekker 1982, 75–135.

MATHEMATICS DEPARTMENT, OHIO STATE UNIVERSITY, COLUMBUS, OH 43210