Polynomial factorization by root approximation

Arjen K. Lenstra
Centrum voor wiskunde en informatica
Kruislaan 413
1098 SJ Amsterdam
The Netherlands

Abstract

We show that a constructive version of the fundamental theorem of algebra [3], combined with the basis reduction algorithm from [1], yields a polynomial-time algorithm for factoring polynomials in one variable with rational coefficients.

Introduction

In 1982 the first polynomial-time algorithm for factoring polynomials in one variable with rational coefficients was published [1]. The most important part of this factoring algorithm is the so-called *basis reduction algorithm*. This basis reduction algorithm, when applied to an arbitrary basis for an integral lattice, computes in polynomial time a *reduced basis* for the lattice, which is, roughly speaking, a basis that is *nearly orthogonal*. Also, such a reduced basis yields approximations of the successive minima of the lattice, and the first vector in the reduced basis is a reasonable approximation of a shortest non-zero vector in the lattice.

For certain specially constructed lattices it can be shown that the basis reduction algorithm actually computes a shortest non-zero vector in the lattice. This happens for instance in the factoring algorithm from [1]. By means of a sufficiently precise, irreducible, p-adic factor of the polynomial $f \in \mathbf{Z}[X]$ to be factored, an integral lattice is defined that contains a factor of f as shortest non-zero vector. The basis reduction algorithm is then applied to this specially constructed lattice to compute this factor in polynomial time.

Here we show that the lattice for the factoring algorithm can also be constructed in another way. Instead of a p-adic factorization of f, we use approximations of the (real or complex) roots of f to define a lattice with similar properties as the lattice above: its shortest vector leads to a factorization of f, and this shortest vector can be found by means of the basis reduction algorithm. As a result we get a polynomial-time algorithm for factoring univariate rational polynomials, which does not apply the usual Berlekamp-Hensel techniques (to compute the p-adic factors), but which relies on (a constructive version of) the fundamental theorem of algebra.

An outline of our algorithm to factor f is as follows. First, we compute a sufficiently precise approximation $\tilde{\alpha}$ of a root α of f, by means of the algorithm from [3]. The minimal polynomial h of α, which clearly is an irreducible factor of f, can then be found by looking for a $\mathbf{Z}$-linear relation of minimal degree among the powers of $\tilde{\alpha}$. In Section 1 we show that the coefficients of this $\mathbf{Z}$-linear relation are given by the shortest vector in a certain lattice, and in Section 2 we present the factoring algorithm and we analyze its running time.

For a polynomial $f = \sum_i f_i X^i \in \mathbf{Z}[X]$ we denote by δf its *degree*, and by $|f| = (\sum_i f_i^2)^{1/2}$ its *length*. We say that f is *primitive* if the *gcd* of its coefficients equals one. By $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{C}$ we denote the set of the integers, the rational numbers, and the complex numbers respectively.

1. Approximated roots and lattices

Let $f \in \mathbf{Z}[X]$ be a primitive polynomial of degree n, and let $\alpha \in \mathbf{C}$ be a zero of f. Obviously, the minimal polynomial $h \in \mathbf{Z}[X]$ of α is an irreducible factor of f. We will show that a sufficiently precise complex rational approximation of α enables us to determine the factor h of f. First, we need the following proposition.

(1.1) **Proposition.** *For any $s \in \mathbf{Z}_{\geq 0}$ and for any $\tilde{\alpha} \in \mathbf{C}$ satisfying $|\alpha - \tilde{\alpha}| < 2^{-s}$, we have $|h(\tilde{\alpha})| < 2^{-s} \delta h \, |f| (2 + |f|)^{\delta h - 1}$.*

Proof. Because $h(\alpha) = 0$, and because the $(\delta h + 1)$-th derivative $h^{(\delta h + 1)}$ of h is zero, we derive from Taylor's formula and $|\alpha - \tilde{\alpha}| < 2^{-s}$, that

$$|h(\tilde{\alpha})| < \sum_{i=0}^{\delta h} \frac{2^{-si}}{i!} \, |h^{(i)}(\alpha)|. \tag{1.2}$$

Let $h = \sum_{j=0}^{\delta h} h_j X^j$, then

$$h^{(i)}(\alpha) = \sum_{j=i}^{\delta h} \left(\prod_{k=0}^{i-1} (j-k) \right) h_j \alpha^{j-i}, \text{ for } 1 \leq i \leq \delta h. \tag{1.3}$$

Because h is a factor of f in $\mathbf{Z}[X]$, we have from [2] that $|h_j| \leq \binom{\delta h}{j} |f|$, and because α is a zero of f we have from for instance [3] that $|\alpha| \leq |f|$. Combined with (1.3) this yields

$$|h^{(i)}(\alpha)| \leq |f| \sum_{j=i}^{\delta h} \left(\prod_{k=0}^{i-1} (j-k) \right) \binom{\delta h}{j} |f|^{j-i},$$

so that we get from (1.2) that

$$|h(\tilde{\alpha})| < |f| \sum_{j=1}^{\delta h} \binom{\delta h}{j} \sum_{i=1}^{j} \binom{j}{i} 2^{-si} |f|^{j-i}.$$

Because $\sum_{i=1}^{j} \binom{j}{i} 2^{-si} |f|^{j-i} = (2^{-s} + |f|)^j - |f|^j$, and because $\sum_{j=1}^{\delta h} \binom{\delta h}{j} (2^{-s} + |f|)^j - \sum_{j=1}^{\delta h} \binom{\delta h}{j} |f|^j = (2^{-s} + |f| + 1)^{\delta h} - (|f| + 1)^{\delta h}$, we find

$$|h(\tilde{\alpha})| < |f| ((2^{-s} + |f| + 1)^{\delta h} - (|f| + 1)^{\delta h}).$$

The proposition now follows from

$$(2^{-s} + |f| + 1)^{\delta h} - (|f| + 1)^{\delta h} < 2^{-s} \delta h (2^{-s} + |f| + 1)^{\delta h - 1}. \square$$

Suppose that we are given an $s \in \mathbf{Z}_{\geq 0}$ and an $\tilde{\alpha} \in \mathbf{Q}(i)$ such that

$$|\alpha - \tilde{\alpha}| < 2^{-s}, \text{ and } |\tilde{\alpha}| \leq |\alpha|. \tag{1.4}$$

In the sequel we will see how large s should be chosen, i.e. how well α should be approximated.

(1.5) Let m be a positive integer, and let $c \in \mathbf{Q}$ be a positive constant. Suppose that we have computed, for $0 \leq i \leq m$, approximations $\tilde{\alpha}_i \in \mathbf{Q}(i)$ of $\tilde{\alpha}^i$:

$$|\tilde{\alpha}^i - \tilde{\alpha}_i| < 2^{-s}, \text{ for } 0 \leq i \leq m. \tag{1.6}$$

We will identify a polynomial $g = \sum_{i=0}^{\delta g} g_i X^i \in \mathbf{Z}[X]$ of degree at most m with the $(m+1)$-dimensional integral vector $(g_0, g_1, \ldots, g_m) \in \mathbf{Z}^{m+1}$, where $g_{\delta g+1}, g_{\delta g+2}, \ldots, g_m$ are zero. By $\tilde{g}(\tilde{\alpha})$ we will denote $\sum_{i=0}^{\delta g} g_i \tilde{\alpha}_i \in \mathbf{Q}(i)$. For an $(m+1)$-dimensional integral vector $v = (v_0, v_1, \ldots, v_m) \in \mathbf{Z}^{m+1}$ we will denote by $\hat{v} \in \mathbf{Q}^{m+3}$ the $(m+3)$-dimensional rational vector $(v_0, v_1, \ldots, v_m, c(\mathrm{Re}(\sum_{i=0}^{m} v_i \tilde{\alpha}_i)), c(\mathrm{Im}(\sum_{i=0}^{m} v_i \tilde{\alpha}_i)))$. Notice that $|\hat{v}|^2 = |v|^2 + c^2 |\tilde{v}(\tilde{\alpha})|^2$. By L we will denote the lattice $\mathbf{Z}^{m+1}$ embedded in $\mathbf{Q}^{m+3}$ by

$$v \mapsto \hat{v}$$

for $v \in \mathbf{Z}^{m+1}$. The next proposition shows that s and c can be chosen in such a way that a short vector in L leads to an irreducible factor of f.

(1.7) **Proposition.** *Let $g \in \mathbf{Z}[X]$ of degree at most m be such that $gcd(h, g)=1$. Suppose that $\delta h \leqslant m$, and that*

$$2^{\frac{m^2}{2}+\frac{m}{2}+4} B^{\frac{1}{2}+m} |f|^{m-1} \leqslant c \leqslant \frac{2^s}{4m|f|(2+|f|)^{m-1}}, \tag{1.8}$$

where $B=\binom{2m}{m}|f|^2+1$. Then $|\hat{h}|^2<B$, and $|\hat{g}|^2 \geqslant 2^m B$.

Proof. First we will show that $|\hat{h}|^2<B$. Because $|\hat{h}|^2=|h|^2+c^2|\tilde{h}(\tilde{\alpha})|^2$ and $|\tilde{h}(\tilde{\alpha})| \leqslant |h(\tilde{\alpha})| + |h(\tilde{\alpha})-\tilde{h}(\tilde{\alpha})|$, we find

$$|\hat{h}|^2 \leqslant |h|^2+c^2(|h(\tilde{\alpha})|^2 + 2|h(\tilde{\alpha})|\,|h(\tilde{\alpha})-\tilde{h}(\tilde{\alpha})| + |h(\tilde{\alpha})-\tilde{h}(\tilde{\alpha})|^2). \tag{1.9}$$

From Proposition (1.1) and $\delta h \leqslant m$ we know that $|h(\tilde{\alpha})|<2^{-s} m|f|(2+|f|)^{m-1}$, which yields, combined with (1.8)

$$|h(\tilde{\alpha})|<\frac{1}{2c}. \tag{1.10}$$

The polynomial $h=\sum_{j=0}^{\delta h} h_j X^j$ is a factor of f in $\mathbf{Z}[X]$, so that we get from [2] that $|h_j| \leqslant \binom{\delta h}{j}|f|$. With (1.6) and $\delta h \leqslant m$ this gives $|h(\tilde{\alpha})-\tilde{h}(\tilde{\alpha})|<2^{-s} \sum_{j=0}^{\delta h} \binom{\delta h}{j}|f| \leqslant 2^{-s+m}|f|$, and with (1.8)

$$|h(\tilde{\alpha})-\tilde{h}(\tilde{\alpha})|<\frac{1}{2c}. \tag{1.11}$$

From $|h_j| \leqslant \binom{\delta h}{j}|f|$ we also derive

$$|h|^2 \leqslant \binom{2\delta h}{\delta h}|f|^2, \tag{1.12}$$

so that we obtain by combining (1.9), (1.10), (1.11), (1.12), and $\delta h \leqslant m$

$$|\hat{h}|^2<\binom{2m}{m}|f|^2+c^2\left(\frac{1}{4c^2}+\frac{2}{4c^2}+\frac{1}{4c^2}\right)=B.$$

Now we will prove that $|\hat{g}|^2 \geqslant 2^m B$. If $|g|^2 \geqslant 2^m B$, then $|\hat{g}|^2 \geqslant 2^m B$, because $|\hat{g}|^2= |g|^2+c^2|\tilde{g}(\tilde{\alpha})|^2$. Therefore, we may assume that

$$|g|^2<2^m B; \tag{1.13}$$

we will prove that $c^2|\tilde{g}(\tilde{\alpha})|^2 \geqslant 2^m B$, so that $|\hat{g}|^2 \geqslant 2^m B$. From (1.13), (1.6), and $\delta g \leqslant m$ we derive

$$|g(\tilde{\alpha})-\tilde{g}(\tilde{\alpha})| \leqslant 2^{-s+\frac{m}{2}}(m+1)B^{\frac{1}{2}},$$

so that, with $2^{-s}(m+1) \leqslant \frac{1}{c}$ (cf. (1.8)), it suffices to prove that

$$c\,|g(\tilde{\alpha})| \geqslant 2(2^m B)^{\frac{1}{2}}. \tag{1.14}$$

Because $gcd(h, g)=1$, there exist polynomials $a, b \in \mathbf{Z}[X]$ satisfying $\delta a<\delta g$ and $\delta b<\delta h$, such that $ah+bg=R$, where $R \in \mathbf{Z}_{\neq 0}$ denotes the resultant of h and g. Because δh and δg are both at most m, it follows from the definition of the resultant and Hadamard's inequality, that the coefficients of a and b are bounded by $|h|^{m-1}|g|^m$ in absolute value, and therefore by $2^{\frac{m^2}{2}} B^m$ (cf. (1.12), (1.13)). From $|\alpha| \leqslant |f|$ (cf. [3]), $\delta a<m$, $\delta b<m$, and (1.4), we now obtain

(1.15) $$\max(|a(\tilde{\alpha})|, |b(\tilde{\alpha})|) \leq 2^{\frac{m^2}{2}} B^m \sum_{i=0}^{m-1} |\alpha|^i$$
$$\leq 2^{\frac{m^2}{2}} B^m \frac{|f|^m - 1}{|f| - 1}$$
$$< 2^{2+\frac{m^2}{2}} B^m |f|^{m-1},$$

where we use that $|f|-1 \geq \frac{|f|}{4}$. From (1.15), Proposition (1.1) and $\delta h \leq m$, it follows that

$$|a(\tilde{\alpha})h(\tilde{\alpha})| < 2^{2-s} m |f|^m (2+|f|)^{m-1} 2^{\frac{m^2}{2}} B^m,$$

which gives with (1.8)

(1.16) $$|a(\tilde{\alpha})h(\tilde{\alpha})| < ½.$$

Because $R \in \mathbf{Z}_{\neq 0}$ and $a(\tilde{\alpha})h(\tilde{\alpha}) + b(\tilde{\alpha})g(\tilde{\alpha}) = R$, it follows from (1.16) that $b(\tilde{\alpha}) \neq 0$, and that

$$|g(\tilde{\alpha})| \geq \frac{1}{2|b(\tilde{\alpha})|}.$$

Combining this with (1.8) and (1.15), we see that (1.14) holds. □

(1.17) **Corollary.** *Let c and s be such that (1.8) holds, and suppose that $\delta h \leq m$. Then for any non-zero polynomial $g \in \mathbf{Z}[X]$ satisfying $\delta g < \delta h$ we have $|\hat{g}|^2 \geq 2^m B$, where B is as in (1.7).*

Proof. The proof follows from the fact that h is irreducible, so that $gcd(h, g) = 1$, combined with (1.7). □

(1.18) **Corollary.** *Let c and s be such that (1.8) holds, and let $\hat{b}_1, \hat{b}_2, ..., \hat{b}_{m+1} \in \mathbf{Q}^{m+3}$ be a reduced basis for the lattice L as defined in (1.5) (cf. [1: (1.4), (1.5)]). If $\delta h = m$, then $|\hat{b}_1|^2 < 2^m B$ and $h = \pm b_1$, where $b_1 \in \mathbf{Z}^{m+1}$ is the $(m+1)$-dimensional vector consisting of the first $m+1$ coordinates of $\hat{b}_1$ (cf. (1.5)), and B is as in (1.7).*

Proof. From (1.7) it follows that $|\hat{h}|^2 < B$. Because $\delta h = m$ we have that $\hat{h} \in L$, so that L contains a non-zero vector of length smaller than $B^{½}$. From [1: (1.11)] we derive that $|\hat{b}_1|^2 < 2^m B$, so that, again with (1.7), we conclude that $gcd(h, b_1) \neq 1$. Because $\delta b_1 \leq m$, and because h is irreducible we find that $h = t b_1$ for some $t \in \mathbf{Z}_{\neq 0}$, so that $h = \pm b_1$, because $\hat{b}_1$ belongs to a basis for L. □

2. Description of the algorithm

(2.1) Let $f \in \mathbf{Z}[X]$ be a primitive polynomial of degree n. We describe an algorithm to compute the irreducible factorization of f in $\mathbf{Z}[X]$.

First, we choose $s, c \in \mathbf{Z}$ minimal such that (1.8) holds with m replaced by $n-1$:

(2.2) $$2^{\frac{n^2}{2} - \frac{n}{2} + 4} \left(\binom{2(n-1)}{n-1} |f|^2 + 1\right)^{n-½} |f|^{n-2} \leq c$$

and

(2.3) $$4(n-1)|f|(2+|f|)^{n-2} c \leq 2^s.$$

Next, we apply the algorithm from [3] to compute an approximation $\tilde{\alpha} \in \mathbf{Q}(i)$ of an arbitrary root $\alpha \in \mathbf{C}$ of f, such that (1.4) holds.

Finally, we apply the results from the previous section to determine the minimal polynomial $h \in \mathbf{Z}[X]$ of α. For the values of $m = 1, 2, ..., n-1$ in succession we compute a reduced basis $\hat{b}_1, \hat{b}_2, ..., \hat{b}_{m+1}$ of the lattice L as defined in (1.5) (this can be done by means of the basis reduction algorithm from [1]). But we stop as soon as we find a vector $\hat{b}_1$ of length less than $2^{\frac{m}{2}}(\binom{2m}{m}|f|^2+1)^{½}$.

It follows from the choice of s and c that, if we find such a vector $\hat{b}_1$, then $m \geqslant \delta h$ according to (1.17); furthermore, because we try the values for m in succession, we find from (1.18) that $h = \pm b_1$ (where b_1 is defined as in (1.18)). If, on the other hand, we do not find such a vector $\hat{b}_1$, then $\delta h > n-1$ according to (1.18), so that $h = f$.

The polynomial h that we find in this way is an irreducible factor of f; the complete factorization of f can be found by applying Algorithm (2.1) to $\frac{f}{h}$.

(2.4) **Theorem.** *Algorithm (2.1) computes the irreducible factorization of any primitive polynomial $f \in \mathbb{Z}[X]$ of degree n in $O(n^6 + n^5 \log|f|)$ additions, subtractions, multiplications, or divisions of numbers which can be represented by $O(n^3 + n^2 \log|f|)$ binary bits.*

Proof. The correctness of Algorithm (2.1) follows from its description. We now analyze its running time. From the fact that c and s are chosen minimal such that (2.2) and (2.3) hold, we find

(2.5) $$\log c = O(n^2 + n \log|f|), \text{ and } s = O(n^2 + n \log|f|).$$

According to [3] and (2.5), the computation of approximations of the n roots of f such that (1.4) holds, satisfies the estimates in (2.4). Obviously, the same is true for the computation of the approximated powers $\tilde{\alpha}_i$ of an approximated root $\tilde{\alpha}$ as in (1.6); these powers have to be computed for the initial basis for L.

The entries of the initial basis for L can be represented by $\lceil \log c + s + \log|\tilde{\alpha}_i| \rceil = O(n^2 + n \log|f|)$ bits (cf. (2.5), (1.6); remember from Section 1 that $|\tilde{\alpha}| \leqslant |f|$). The applications of the basis reduction algorithm for the computation of one irreducible factor h of f can therefore be done in $O(\delta h^4 (n^2 + n \log|f|))$ operations on $O(n^3 + n^2 \log|f|)$-bit numbers (cf. [1: (1.26), (1.37), (1.38)], (1.5)).

It follows that the computation of the complete factorization of f satisfies the estimates in (2.4), where we apply that $|\frac{f}{h}| = O(n + \log|f|)$ (cf. (1.12) with h replaced by $\frac{f}{h}$). □

(2.6) **Remark** In [4] A. Schönhage noticed that for the lattice that we use in Algorithm (2.1), a better running time can be proved for the basis reduction algorithm. His observation leads to $O(n^5 + n^4 \log|f|)$ arithmetic operations on $O(n^2 + n \log|f|)$-bit numbers. Furthermore he wins another factor of $O(n)$ by an improved version of the basis reduction algorithm.

References

1. A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. **261** (1972), 515-534.

2. M. Mignotte, An inequality about factors of polynomials, Math. Comp. **28** (1974), 1153-1157.

3. A. Schönhage, The fundamental theorem of algebra in terms of computational complexity, manuscript, 1982.

4. A. Schönhage, Factorization of univariate integer polynomials by diophantine approximation and by an improved basis reduction algorithm, manuscript, 1983.