LATTICES AND FACTORIZATION OF POLYNOMIALS

A.K. Lenstra
Department of Computer Science
Mathematisch Centrum
Kruislaan 413
1098 SJ Amsterdam

A new algorithm to factorize univariate polynomials over an algebraic number field has been implemented in Algol-68 on a CDC-Cyber 170-750 computer. The algebraic number field is given as the field of rational numbers adjoined by a root of a prescribed minimal polynomial. Unlike other algorithms [1,2] the efficiency of our so-called lattice algorithm does not depend on the irreducibility of the minimal polynomial modulo some prime. The factorization of the polynomial to be factored is constructed from the factorization of that polynomial over a finite field determined by a prime p and an irreducible factor of the minimal polynomial modulo p. The algorithm is based on a theorem on integral lattices and a theorem giving a lower bound for the length of a shortest-length polynomial having modulo p^k a non-trivial common divisor with the minimal polynomial. These theorems also enable us to formulate a new algorithm for factoring polynomials over the integers. A technical report describing the algorithms will soon be available from the Mathematisch Centrum, Amsterdam.

To illustrate the lattice approach we factorize a polynomial from [2]. Let $F(T) = T^6+3T^5+6T^4+T^3-3T^2+12T+16$, and let $f(X) = X^3-3 \in (\mathbb{Q}(\alpha))[X]$, where α denotes a zero of F. The minimal polynomial F has an irreducible factor $T^3-1399040T^2-1399043T-4 = H(T)$ modulo $7^8 = 57604801$. The irreducible factorization of f modulo $H(\alpha)$ and 7^8 is

$$f \equiv (X-2387947\alpha-2387948)\cdot(X+2387948\alpha+1)\cdot(X-\alpha+2387947);$$

using 12 as the denominator of the factors of f over $\mathbb{Q}(\alpha)$ this becomes

$$f \equiv (X+(168641\alpha+168629)/12)\cdot(X-(168629\alpha-12)/12)\cdot(X-(12\alpha+168641)/12).$$

Consider the 6-dimensional lattice L generated by the following basis:

$$\begin{pmatrix} 57604801 & 0 & 0 & -4 & 0 & 0 \\ 0 & 57604801 & 0 & -1399043 & -4 & 0 \\ 0 & 0 & 57604801 & -1399040 & -1399043 & -4 \\ 0 & 0 & 0 & 1 & -1399040 & -1399043 \\ 0 & 0 & 0 & 0 & 1 & -1399040 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = M.$$

Clearly L equals the set of polynomials of degree ≤ 5 having H as a factor modulo 7^8. We denote by $\tilde{M}$ a reduced basis generating L, resulting from an orthogonalization of M:

$$\begin{pmatrix} 1265 & -1265 & -1059 & -1265 & 0 & -103 \\ 479 & -273 & -547 & 683 & 2530 & 34 \\ 547 & 547 & -137 & -34 & 752 & 1641 \\ -752 & -2017 & 2359 & -752 & 0 & -171 \\ -957 & -205 & -957 & -1231 & 1265 & 205 \\ -1299 & -1299 & -376 & 2051 & -752 & 376 \end{pmatrix} = \tilde{M}.$$

Let $\tilde{v}$ be an arbitrary coefficient of a factor of f modulo $H(\alpha)$ and 7^8 (without denominator). We can find the shortest vector v congruent to $\tilde{v}$ modulo L by putting $v = \tilde{v} - \tilde{M}[\tilde{M}^{-1}\tilde{v}]$, where $[\tilde{M}^{-1}\tilde{v}]$ denotes componentwise rounding of the real vector $\tilde{M}^{-1}\tilde{v}$. In the paper we prove that $v/12$ will be a coefficient of a factor of f over $\mathbb{Q}(\alpha)$ for a correct choice of $\tilde{v}$. Taking $\tilde{v} = 168641\alpha+168629$, we find $v = -\alpha^5-3\alpha^4-6\alpha^3-5\alpha^2+3\alpha-12$, and $X-(\alpha^5+3\alpha^4+6\alpha^3+5\alpha^2-3\alpha+12)/12$ is a factor of f over $\mathbb{Q}(\alpha)$. In the same way we construct the other factors of f over $\mathbb{Q}(\alpha)$:

$$f = (X-(\alpha^5+3\alpha^4+6\alpha^3+5\alpha^2-3\alpha+12)/12)\cdot(X+(\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)/6)\cdot(X-(\alpha^5+\alpha^4+2\alpha^3-7\alpha^2+11\alpha+16)/12).$$

Examples

We compared the lattice algorithm with a slightly modified version of the Weinberger-Rothschild algorithm. The new algorithm always looks for a prime p such that the minimal polynomial has a non-trivial small-degree factor modulo p, whereas the Weinberger-Rothschild algorithm tries to find a prime such that the minimal polynomial remains irreducible. In the examples below we denote by 'new time' and 'old time' the time taken by the lattice algorithm and the time taken by the Weinberger-Rothschild algorithm respectively.

$f = X^2+X-1,\quad \alpha^2-5 = 0.$

$\alpha-4 = 0$ modulo 11: new time 50 msec,

irreducible modulo 3: old time 124 msec.

factors over $\mathbb{Q}(\alpha)$:

$$\frac{(2X+\alpha+1)\cdot(2X-\alpha+1)}{4}.$$

$f = \dfrac{47X^6+21X^5+598X^4+1561X^3+1198X^2+261X+47}{47}$,

$\alpha^2-\alpha+3 = 0.$

$\alpha-1 = 0$ modulo 3: new time 143 msec,

irreducible modulo 7: old time 676 msec.

factors over $\mathbb{Q}(\alpha)$:

$$(47X^3-(121\alpha-71)X^2-(121\alpha+70)X-47)\cdot(47X^3+(121\alpha-50)X^2+(121\alpha-191)X-47)/2209.$$

$f = X^6-2X^5+2X^3-X-1,\quad \alpha^3+\alpha^2-2\alpha-1 = 0.$

$\alpha+3 = 0$ modulo 13: new time 183 msec,

irreducible modulo 2: old time 844 msec.

factors over $\mathbb{Q}(\alpha)$:

$$(X^2-(\alpha+1)X+\alpha^2+\alpha-1)\cdot(X^2+(\alpha^2+\alpha-2)X-\alpha^2+2)\cdot(X^2-(\alpha^2-1)X-\alpha).$$

$f = \dfrac{16X^6-1}{16},\quad \alpha^3+2 = 0.$

$\alpha^2+2\alpha-1 = 0$ modulo 5: new time 431 msec,

irreducible modulo 7: old time 511 msec.

factors over $\mathbb{Q}(\alpha)$:

$$\frac{(4X^2+2\alpha X+\alpha^2)\cdot(4X^2-2\alpha X+\alpha^2)\cdot(2X-\alpha)\cdot(2X+\alpha)}{64}.$$

$f = X^8-X^7-X^6+X^4-X^2+X+1,\quad \alpha^4-\alpha+1 = 0.$

$\alpha^3-\alpha^2+\alpha+1 = 0$ modulo 3: new time 1347 msec,

$\alpha+1 = 0$ modulo 3: new time 235 msec,

irreducible modulo 7: old time 2038 msec.

factors over $\mathbb{Q}(\alpha)$:

$$(X^6-(\alpha^3+\alpha^2+\alpha)X^5+(2\alpha^3+\alpha^2-3)X^4+(\alpha^3+2\alpha^2+2\alpha)X^3-(2\alpha^3+\alpha^2-3)X^2-(\alpha^3+\alpha^2+\alpha)X-1)\cdot(X^2+(\alpha^3+\alpha^2+\alpha-1)X-1).$$

$f = X^5-X^4-3X^3+X^2+2X-1,\quad \alpha^5+\alpha^3-\alpha^2+\alpha-1 = 0.$

$\alpha^2+\alpha-1 = 0$ modulo 3: new time 352 msec,

$\alpha+1 = 0$ modulo 5: new time 292 msec,

irreducible modulo 2: old time 1152 msec.

factors over $\mathbb{Q}(\alpha)$:

$$(X^4+(\alpha^4+\alpha^2)X^3+(\alpha^3+\alpha^2-2)X^2-(\alpha^4-\alpha^3+\alpha^2-\alpha+1)X-\alpha^3+1)\cdot(X-\alpha^4-\alpha^2-1).$$

$f = X^3-3,\quad \alpha^6+3\alpha^5+6\alpha^4+\alpha^3-3\alpha^2+12\alpha+16 = 0.$

$\alpha^2-2\alpha-1 = 0$ modulo 5: new time 564 msec,

two factors modulo 7: old time 814 msec.

factors over $\mathbb{Q}(\alpha)$:

$$(12X-\alpha^5-3\alpha^4-6\alpha^3-5\alpha^2+3\alpha-12)\cdot(6X+\alpha^5+2\alpha^4+4\alpha^3-\alpha^2+4\alpha+14)\cdot(12X-\alpha^5-\alpha^4-2\alpha^3+7\alpha^2-11\alpha-16)/864.$$

$f = X^6+X^5-3X^4-4X^3+2X^2+3X+1,$

$\alpha^6-\alpha^5-2\alpha^4+2\alpha^3+2\alpha^2-2\alpha-1 = 0.$

$\alpha^2+2\alpha-2 = 0$ modulo 7: new time 700 msec,

irreducible modulo 2: old time 2094 msec.

factors over $\mathbb{Q}(\alpha)$:

$$(X^3-(\alpha^5-\alpha^4-\alpha^3+2\alpha^2-2)X^2-X+\alpha^5-\alpha^4-\alpha^3+2\alpha^2-3)\cdot(X^2+(\alpha^4-\alpha^2+1)X+\alpha^4-2\alpha^2+\alpha+1)\cdot(X+\alpha^5-2\alpha^4-\alpha^3+3\alpha^2-2).$$

References

1. P.S. Wang, Factoring multivariate polynomials over algebraic number fields, Math. Comp. 30 (1976), 324-336.

2. P.J. Weinberger, L.P. Rothschild, Factoring polynomials over algebraic number fields, ACM Transactions on Mathematical Software 2 (1976), 335-350.

3. A.K. Lenstra, Lattices and factorization of polynomials, Mathematisch Centrum Amsterdam, to appear.