

We tested on several examples the efficiency of our algorithm, using Maple 10. We construct the examples in the following way.

We consider random polynomials  $g_1 \in \mathbb{Q}[x, y, z]$  monic in  $y$  and  $g_2 \in \mathbb{Q}[z]$  monic, of degrees  $d_1$  and  $d_2$  resp. We compute  $f = \text{Res}_z(g_1, g_2)$ . In this way we obtain an irreducible polynomial  $f \in \mathbb{Q}[x, y]$ , monic in  $y$ , of degree  $d_1 \cdot d_2$  with  $d_2$  absolute irreducible factors each of degree  $d_1$ .

The polynomials  $g_1$  and  $g_2$  used are listed in the file “ExamplesData.mws”.

Here we summarize the time needed to obtain  $q(Z)$ , the minimal rational polynomial of  $\alpha$ , such that the absolute factors of  $f$  are in  $\mathbb{K}[x, y]$ ,  $\mathbb{K} = \mathbb{Q}(\alpha) = \mathbb{Q}[Z]/q(Z)$ .

**Example 1.**  $f$  rational irreducible polynomial of degree 60 with 6 absolute factors of degree 10.

We choose  $p = 269$ .

- Time to factor  $f \bmod p$ : 0.210 sec.
- Time to lift the factorization  $f(0, Y) = g_1(0, Y)g_2(0, Y) \bmod p$  to a factorization  $\bmod p^{256}$ , using Quadratic Hensel Lifting: 4.020 sec.
- Time to find the minimal polynomial of  $\alpha$  through its approximation  $\bmod p^{256}$  using LLL: 0.981 sec.

**Example 2.**  $f$  rational irreducible polynomial of degree 120 with 6 absolute factors of degree 20.

We choose  $p = 65479$ .

- Time to factor  $f \bmod p$ : 15.260 sec.
- Time to lift the factorization  $f(0, Y) = g_1(0, Y)g_2(0, Y) \bmod p$  to a factorization  $\bmod p^{128}$ , using Quadratic Hensel Lifting: 31.919 sec.
- Time to find the minimal polynomial of  $\alpha$  through its approximation  $\bmod p^{128}$  using LLL: 0.960 sec.

**Example 3.**  $f$  rational irreducible polynomial of degree 200 with 10 absolute factors of degree 20.

We choose  $p = 103$ .

- Time to factor  $f \bmod p$ : 6.891 sec.
- Time to lift the factorization  $f(0, Y) = g_1(0, Y)g_2(0, Y) \bmod p$  to a factorization  $\bmod p^{256}$ , using Quadratic Hensel Lifting: 129.649 sec.
- Time to find the minimal polynomial of  $\alpha$  through its approximation  $\bmod p^{256}$  using LLL: 2.970 sec.

**Example 4.**  $f$  rational irreducible polynomial of degree 300 with 10 absolute factors of degree 30.

We choose  $p = 1201$ .

- Time to factor  $f \bmod p$ : 37.260 sec.

- Time to lift the factorization  $f(0, Y) = g_1(0, Y)g_2(0, Y) \bmod p$  to a factorization  $\bmod p^{256}$ , using Quadratic Hensel Lifting: 807.830 sec.
- Time to find the minimal polynomial of  $\alpha$  through its approximation  $\bmod p^{256}$  using LLL: 7.059 sec.

**Example 5.**  $f$  rational irreducible polynomial of degree 400 with 10 absolute factors of degree 40.

We choose  $p = 131$ .

- Time to factor  $f \bmod p$ : 84.621 sec.
- Time to lift the factorization  $f(0, Y) = g_1(0, Y)g_2(0, Y) \bmod p$  to a factorization  $\bmod p^{512}$ , using Quadratic Hensel Lifting: 3086.65 sec.
- Time to find the minimal polynomial of  $\alpha$  through its approximation  $\bmod p^{512}$  using LLL: 18.06 sec.

**Example 6.**  $f$  rational irreducible polynomial of degree 150 with 15 absolute factors of degree 10.

We choose  $p = 19$ .

- Time to factor  $f \bmod p$ : 2.140 sec.
- Time to lift the factorization  $f(0, Y) = g_1(0, Y)g_2(0, Y) \bmod p$  to a factorization  $\bmod p^{512}$ , using Quadratic Hensel Lifting: 73.521 sec.
- Time to find the minimal polynomial of  $\alpha$  through its approximation  $\bmod p^{512}$  using LLL: 9.739 sec.