A polynomial with Galois group M_{12}

Let

$$\begin{aligned} f &= 3x^{12} + 100x^{11} + 1350x^{10} + 9300x^9 + 32925x^8 + 45000x^7 - 43500x^6 \\ &\quad -147000x^5 + 46125x^4 + 172500x^3 + 22500x + 1875. \end{aligned}$$

Let F_k be the polynomial of minimal degree such that the product of every set of k roots of f is a root of F_k. The polynomials F_5 and F_6 are square-free and have degrees $12!/(5!7!) = 792$ and $12!/(6!6!) = 924$. It is well-known that f has Galois group M_{12} if and only if F_5 is irreducible and F_6 is reducible. However, until now it was not possible to use this criterion because F_5 and F_6 were too hard to factor due to the large number of modular factors: For F_5 there are at least $n = 792/11 = 72$ p-adic factors and for F_6 there are at least $n = 924/11 = 84$ p-adic factors, because M_{12} does not have elements of order > 11. This makes factorization of F_5 or F_6 far out of reach of previous factoring algorithms.

Due to the high degree and very large size of the coefficients of F_5 and F_6 the computation time is dominated by Hensel lifting, which takes 81% of the 15 hours to factor F_6 on a Sun workstation (corresponds to around 30 hours on a Pentium 266 laptop). Considerable time and memory usage could be saved, however, because F_5 can still be proven to be irreducible even if we use a smaller value for a than prescribed by the Landau-Mignotte bound. And the smallest of the two factors of F_6 could also be computed with smaller a.

Other examples: The polynomial P7 on Paul Zimmerman's web-site, which was apparently also out of reach for previous algorithms because the factorization was unknown, took less than one hour on a Pentium 266 laptop (about 10 minutes on a Pentium 733) and is irreducible. Another polynomial with $n = 128$, degree $N = 256$, and 2 irreducible factors of degree 128 (Swinnerton-Dyer polynomials) took about 7 hours on a Pentium 266, most of which was spent on lattice reductions. Memory usage was dominated by Hensel lifting in all examples we tried. An implementation of the knapsack factorization algorithm and additional examples can be found on

`http://www.math.fsu.edu/~hoeij/knapsack.html`

Remarks: There now exist implementations in other systems as well, such as Magma, NTL, and GP-PARI. These latter implementations run much faster; it is clear that compiled C-code runs many times faster than interpreted Maple code. With these implementations it is possible to factor in a short time even larger examples than the ones given above, which in turn were already too big for any previous algorithm implemented in any system.

At the MEGA'1996 conference in Eindhoven, Netherlands, the prize question was to find and prove the Galois group of a particular polynomial, which happened to be a polynomial with Galois group M_{12} (it was obtained by taking such polynomial from the literature and applying a transformation to it). Although four years too late, the prize question is now finally solved.