Computing roots in number fields

Andrea Lesavourey

Computing roots of elements is an important step when solving various tasks in computational number theory. It arises for example during the final step of the General Number Field Sieve [3]. This problem also intervenes during saturation processes while computing the class group or S-units of a number field [2].

I will describe methods to compute a e-th root x of a number field element $y \in K$, with a particular interest for potentially large e and dimension n.

— When K and e are such that there are infinitely many prime integers p such that $\forall \mathfrak{p} \mid p, p^{f(\mathfrak{p}|p)} \not\equiv 1 \bmod e$, we reconstruct x from $x \pmod{p_1}, \dots, x \pmod{p_r}$ using a generalisation of Thomé's work on square-roots in the context of the NFS [6].

— When this good condition on K and e is not satisfied, one can adapt Couveignes' approach for square roots [4] to relative extensions of number fields K/k provided $[K : k]$ is coprime to e and infinitely many prime integers p are such that each prime ideal $\mathfrak{p}$ of $\mathcal{O}_k$ above p is inert in K. All these conditions allows us to take advantage of the commutativity of the norm maps with respect to fields extensions K/k and $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ where $\mathfrak{P}$ is above $\mathfrak{p}$ and $\mathbb{F}_{\mathfrak{P}}$ (resp. $\mathbb{F}_{\mathfrak{p}}$) is the corresponding residue field. Then one can fix a eth root $\mathrm{N}_{K/k}(y)^{1/e} \in k$ of $\mathrm{N}_{K/k}(y)$ so that we can eliminate any enumeration when computing the roots in the residue fields ; more precisely we choose the eth root $x \bmod \mathfrak{P}$ of $(y \bmod \mathfrak{P})$ such that $\mathrm{N}_{\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}}(x \bmod \mathfrak{P}) = \mathrm{N}_{K/k}(y)^{1/e} \bmod \mathfrak{p}$. We recover x from these chosen embeddings again through a CRT procedure.

We ran experiments to evaluate the performances of our algorithms when compared to standard methods and implementations, especially Pari/Gp nfroots. We focused on cyclotomic fields, as they are the main fields used in our application domain, i.e. lattice-based cryptography, but our algorithms extend to other number fields in most cases. All of our implementations are done using SageMath with few optimisations. Meanwhile, we compare with Pari/Gp, and still achieve several orders of performance (between 10 to 10000+ when n and e increase). Thus, our timings could be further improved if we have C implementations.

Over "good" cases, our CRT ; generalisation algorithm seems to be clearly more efficient than Pari/Gp nfroots, and the gap seems to widen when the exponent e increases. We have graphs up to $e = 2^{16}$ but our algorithms scale well and we can use without any problems for e with 60-bit prime, which would be completely out of scope for Pari/Gp.

Over "bad" cases, experiments show that our generalization of Couveignes' algorithm is more efficient than Pari/Gp nfroots [5]. Our algorithms are always faster, and the gap with nfroots becomes larger when e and n increase.

Finally, we tested our algorithms in concrete experiments for the saturation using the code of [1].

Références

[1] O. Bernard et al. "Twisted-PHS : Using the Product Formula to Solve Approx-SVP in Ideal Lattices". In : *Advances in Cryptology – ASIACRYPT 2020*. Sous la dir. de S. Moriai et al. Cham : Springer International Publishing, 2020, p. 349-380. isbn : 978-3-030-64834-3.

[2] J.-F. Biasse et al. "Improved techniques for computing the ideal class group and a system of fundamental units in number fields." In : *Algorithmic Number Theory, 10th International Symposium, ANTS-IX, San Diego CA, USA, July 9-13, 2012. Proceedings*. T. 1. Open Book Series. Mathematical Science Publishers, 2012, p. 113-133.

[3] J. P. Buhler et al. "Factoring integers with the number field sieve". In : *The development of the number field sieve*. Sous la dir. d'A. K. Lenstra et al. Berlin, Heidelberg : Springer Berlin Heidelberg, 1993, p. 50-94. isbn : 978-3-540-47892-8.

[4] J.-M. Couveignes. "Computing A Square Root For The Number Field Sieve". In : 1554 (juin 1997).

[5] *PARI/GP version `2.11.2`*. available from `http://pari.math.u-bordeaux.fr/`. Univ. Bordeaux : The PARI Group, 2019.

[6] E. Thomé. "Square Root Algorithms for the Number Field Sieve". In : *Arithmetic of Finite Fields*. Sous la dir. de F. Özbudak et al. Berlin, Heidelberg : Springer Berlin Heidelberg, 2012, p. 208-224. isbn : 978-3-642-31662-3.