An appendix for a recent paper of Kim [Kim15]

Razvan Barbulescu

CNRS,Univ Paris 6, Univ Paris 7

Abstract. This note can be seen as an appendix of a recent paper of Kim [Kim15]. We show that the discrete logarithm problem in fields $\mathbb{F}_Q$ where $Q = p^n$ with p of medium size and n having a factor of the good size (specified in the article) has a complexity of $L_Q(1/3, \sqrt[3]{48/9})$.

We propose here a variant of NFS which combines exTNFS with the Conjugation method of polynomial selection. Let $Q = p^n$ where $n = \eta k$ for some integers k and η with $k = (12^{-1/3} + o(1))(\frac{\log Q}{\log\log Q})^{1/3}$. Then we select a field $\mathbb{Q}(\iota)$ of degree η where p is inert; call h the minimal polynomial of ι over $\mathbb{Q}$. Next we use the Conjugation method to construct two polynomials f and g in $\mathbb{Z}[x]$, irreducible, with a common irreducible factor of degree k modulo p such that:

- $\deg(f) = 2k$ and $\|f\|_\infty = O(\log k)$;
- $\deg(g) = k$ and $\|g\|_\infty = p^{1/2} = Q^{1/(2\eta k)}$.

We sieve on pairs $(a(\iota), b(\iota))$ where $a(t), b(t) \in \mathbb{Z}[t]$ are such that $\|a\|_\infty, \|b\|_\infty \leq A$ for a parameter A to be chosen. Then we continue the algorithm as in Kim's exTNFS.

Fact 1 *If $Q = p^n$ is a prime power so that*

- *$p = L_Q(\alpha, c)$ with $1/3 < \alpha < 2/3$ or $\alpha = 2/3$ and $c \leq 12^{-1/3}$;*
- *n has a divisor $k = (12^{-1/3} + o(1))(\frac{\log Q}{\log\log Q})^{1/3}$.*

Then the discrete logarithm in $\mathbb{F}_Q$ has

$$\text{complexity} = L_Q(1/3, \sqrt[3]{48/9})$$

In the following $K_f = \mathbb{Q}(\alpha_f)$ and respectively $K_g = \mathbb{Q}(\alpha_g)$ are the extensions of $\mathbb{Q}(\iota)$ by f and respectively g.
Let E be a parameter to be chosen and put $A = E^{1/\eta}$. By Theorem 3 in [BGK15], we have

$$|N_{K_f/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_f)| < A^{2k\eta} O(\log k)^\eta O(\log \eta)^{2k(\eta-1)} C(\eta, 2k),$$

$$|N_{K_g/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_g)| < A^{k\eta} (Q^{1/(2k\eta)})^\eta O(\log \eta)^{k(\eta-1)} C(\eta, k),$$

and then

$$|N_{K_f/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_f)| \cdot |N_{K_g/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_g)| < E^{3k} Q^{1/(2k)} C(\eta, 2k)^{2+o(1)}. \quad (1)$$

Next we have

$$C(\eta, 2k) = \exp(O(1)2k\eta \log(k\eta)) = \exp(O(1)n \log n).$$

Since $n = \frac{\log Q}{\log p} = (\frac{\log Q}{\log \log Q})^{1-\alpha}$, $n \log n = o((\log Q)^{2/3}(\log \log Q)^{1/3})$ and then

$$C(\eta, 2k) = L_Q(2/3, 1)^{o(1)}. \tag{2}$$

When we combine Equations (1) and (2) we obtain

$$|N_{K_f/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_f)| \cdot |N_{K_g/\mathbb{Q}}(a(\iota) - b(\iota)\alpha_g)| < E^{3k}Q^{(1+o(1))/(2k)}.$$

But this is Equation (5) in [BGGM15] when $t = 2$. The rest of the computations are identical as in point 3. of Theorem 1 in [BGGM15].

References

[BGGM15] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 129–155. Springer, 2015.

[BGK15] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The tower number field sieve. Cryptology ePrint Archive, Report 2015/505, 2015. `http://eprint.iacr.org/`.

[Kim15] Taechan Kim. Extended tower number field sieve: A new complexity for medium prime case. Cryptology ePrint Archive, Report 2015/1027, 2015. `http://eprint.iacr.org/`.