Fast norm computation in smooth-degree Abelian number fields

D. J. Bernstein

University of Illinois at Chicago;
Ruhr University Bochum;
Academia Sinica

Notation,
for α in number field K:
$\mathrm{tr}^K_{\mathbf{Q}}\,\alpha$, $\det^K_{\mathbf{Q}}\,\alpha$ mean tr, det of
$\beta \mapsto \alpha\beta$ as $\mathbf{Q}$-linear map $K \to K$.
More generally: $\mathrm{tr}^K_F\,\alpha$, $\det^K_F\,\alpha$ as
F-linear map for subfield F of K.

Often want to compute $\det^K_{\mathbf{Q}}$.

One of many examples: Define $\zeta_m = \exp(2\pi i/m)$ and $h^-_m = \#\mathrm{Cl}(\mathbf{Q}(\zeta_m))/\#\mathrm{Cl}(\mathbf{R} \cap \mathbf{Q}(\zeta_m))$.

e.g. $h^-_{64} = 17$; $h^-_{128} = 17 \cdot 21121$; $h^-_{256} = 17 \cdot 21121 \cdot 29102880226241$.

$17 = 2 \det^{\mathbf{Q}(\zeta_{16})}_{\mathbf{Q}}(B_{64}/2)$ where $B_{64} = \zeta_{16}^7 - \zeta_{16}^6 + \zeta_{16}^5 + \zeta_{16}^4 + \zeta_{16}^3 - \zeta_{16}^2 - \zeta_{16} - 1$.

$21121 = 2 \det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}}(B_{128}/2)$ where $B_{128} = -\zeta_{32}^{15} + \zeta_{32}^{14} - \zeta_{32}^{13} + \zeta_{32}^{12} + \zeta_{32}^{11} + \zeta_{32}^{10} + \zeta_{32}^9 + \zeta_{32}^8 - \zeta_{32}^7 - \zeta_{32}^6 - \zeta_{32}^5 + \zeta_{32}^4 + \zeta_{32}^3 - \zeta_{32}^2 - \zeta_{32} - 1$.

$29102880226241 = \cdots$

1851 Kummer, 1952 Hasse, 1964 Schrutka von Rechtenstamm, 1970 Newman, 1978 Lehmer–Masley, 1992 Fung–Granville–Williams, 1995 Jha, 1998 Louboutin, 1999 Shokrollahi: various algorithms to evaluate $m \mapsto h_m^-$, all using at least $m^{1.5+o(1)}$ bit operations (even with fast multiplication).

h_m^- has $m^{1+o(1)}$ bits.

1851 Kummer, 1952 Hasse, 1964 Schrutka von Rechtenstamm, 1970 Newman, 1978 Lehmer–Masley, 1992 Fung–Granville–Williams, 1995 Jha, 1998 Louboutin, 1999 Shokrollahi: various algorithms to evaluate $m \mapsto h_m^-$, all using at least $m^{1.5+o(1)}$ bit operations (even with fast multiplication).

h_m^- has $m^{1+o(1)}$ bits.

For many choices of m:
Fast $\det_{\mathbf{Q}}^{K}$ as in this talk gives h_m^- using $m^{1+o(1)}$ bit operations.

Main motivation

Core computation in algebraic number theory: filter all small elements of $\mathcal{O}_K$ to find S-units (elements with prime-ideal factorizations supported on S).

More generally, filter all small elements of an $\mathcal{O}_K$-ideal $I \neq 0$ to find S-generators of I.

Traditional application: Compute S-unit group; in particular, conjecturally obtain $\mathcal{O}_K^*$ and $\mathrm{Cl}(K)$ in subexponential time.

How to recognize S-units?

For some fields K (e.g., in NFS), find small elements of $\mathcal{O}_K$ in a low-dimensional lattice. Easily scan a sublattice for each factor.

How to recognize S-units?

For some fields K (e.g., in NFS), find small elements of $\mathcal{O}_K$ in a low-dimensional lattice. Easily scan a sublattice for each factor.

For balanced high-degree K (e.g., cyclotomics), lattice has high dimension; scanning sublattices seems hard. So, for each small α (modulo automorphisms etc.), compute $\det_{\mathbf{Q}}^{K} \alpha$, see whether $\det_{\mathbf{Q}}^{K} \alpha$ factors suitably.

How fast is $\alpha \mapsto \det_{\mathbf{Q}}^{K} \alpha$?

Highlights of the 2022 paper

Section 2: For small α, how large is $\det_{\mathbf{Q}}^{K} \alpha$? Case study: $\mathbf{Q}(\zeta_m)$ where $m = 2n \in \{4, 8, 16, \ldots\}$. Trivially $O(n \log n)$ bits; more precise "circular approximation" to distribution; experiments.

Highlights of the 2022 paper

Section 2: For small α, how large is $\det_{\mathbf{Q}}^{K} \alpha$? Case study: $\mathbf{Q}(\zeta_m)$ where $m = 2n \in \{4, 8, 16, \ldots\}$. Trivially $O(n \log n)$ bits; more precise "circular approximation" to distribution; experiments.

Section 3: How fast are standard $\det_{\mathbf{Q}}^{K}$ algorithms? Modular resultants via continued fractions: usually $n^2(\log n)^{3+o(1)}$. $\prod_\sigma \sigma(\alpha)$ in $\mathbf{C}$: $n^2(\log n)^{3+o(1)}$; $n^2(\log n)^{2+o(1)}$ using a cyclotomic speedup from 1982 Schönhage.

Section 1: $\det_{\mathbf{Q}}^{K} \alpha = \det_{\mathbf{Q}}^{F} \det_{F}^{K} \alpha$
obviously reduces cost to $n^{1+o(1)}$
for the same $\mathbf{Q}(\zeta_m)$ case study.
See paper for credits + speedups.

Section 1: $\det_{\mathbf{Q}}^{K} \alpha = \det_{\mathbf{Q}}^{F} \det_{F}^{K} \alpha$ obviously reduces cost to $n^{1+o(1)}$ for the same $\mathbf{Q}(\zeta_m)$ case study. See paper for credits + speedups.

Section 4: How general is this? Want small-relative-degree tower. Also want small bases supporting fast multiplication and subfields. For Abelian fields: Gauss-period basis is small, supports subfields; generalizing Rader's FFT gives fast multiplication; total cost $n(\log n)^{3+o(1)}$ if reldeg $(\log n)^{o(1)}$.

Section 1: $\det_{\mathbf{Q}}^{K} \alpha = \det_{\mathbf{Q}}^{F} \det_{F}^{K} \alpha$ obviously reduces cost to $n^{1+o(1)}$ for the same $\mathbf{Q}(\zeta_m)$ case study. See paper for credits + speedups.

Section 4: How general is this? Want small-relative-degree tower. Also want small bases supporting fast multiplication and subfields. For Abelian fields: Gauss-period basis is small, supports subfields; generalizing Rader's FFT gives fast multiplication; total cost $n(\log n)^{3+o(1)}$ if reldeg $(\log n)^{o(1)}$.

Section 5: S-unit application.

Power-of-2 cyclotomics

Take, e.g., $B_{128} = -\zeta_{32}^{15} + \cdots$.

$$\det_{\mathbf{Q}(\zeta_{16})}^{\mathbf{Q}(\zeta_{32})} B_{128} = B_{128} \cdot \sigma(B_{128})$$
$$= -6\zeta_{16}^{7} - 2\zeta_{16}^{6} - 6\zeta_{16}^{5} - 6\zeta_{16}^{4} - 6\zeta_{16}^{3} + 6\zeta_{16}^{2} - 2\zeta_{16} - 2.$$

$$\det_{\mathbf{Q}(\zeta_{8})}^{\mathbf{Q}(\zeta_{32})} B_{128}$$
$$= -88\zeta_{8}^{3} + 104\zeta_{8}^{2} + 56\zeta_{8} + 88.$$

$$\det_{\mathbf{Q}(\zeta_{4})}^{\mathbf{Q}(\zeta_{32})} B_{128}$$
$$= 22912\zeta_{4} - 12928.$$

$$\det_{\mathbf{Q}}^{\mathbf{Q}(\zeta_{32})} B_{128}$$
$$= 692092928 = 21121 \cdot 2^{15}.$$

2010 Gentry–Halevi: This costs $n(\log n)^{O(1)}$ and "relies heavily on the special form of … $x^n + 1$, with n a power of two".

2010 Gentry–Halevi: This costs $n(\log n)^{O(1)}$ and "relies heavily on the special form of ... $x^n + 1$, with n a power of two".

In fact, also works for $\mathbf{Q}(\zeta_m)$ for any smooth positive integer m.

2010 Gentry–Halevi: This costs $n(\log n)^{O(1)}$ and "relies heavily on the special form of . . . $x^n + 1$, with n a power of two".

In fact, also works for $\mathbf{Q}(\zeta_m)$ for any smooth positive integer m.

What about further fields?
Main challenge: fast multiplication.

2010 Gentry–Halevi: This costs $n(\log n)^{O(1)}$ and "relies heavily on the special form of . . . $x^n + 1$, with n a power of two".

In fact, also works for $\mathbf{Q}(\zeta_m)$ for any smooth positive integer m.

What about further fields?
Main challenge: fast multiplication.

2017 Bauch–Bernstein–de Valence–Lange–van Vredendaal includes analogous det evaluation for multiquadratic fields, built from a fast-multiplication algorithm for those fields.

Prime-conductor cyclotomics

For prime p with smooth $p-1$: use long tower $\mathbf{Q} \subset \cdots \subset \mathbf{Q}(\zeta_p)$.

Use Gauss periods as a basis for each subfield $F \subseteq \mathbf{Q}(\zeta_p)$: e.g., for degree-4 subfield F of $K = \mathbf{Q}(\zeta_{17})$, use the basis

$$\mathrm{tr}_F^K \zeta_{17}^1 = \zeta_{17}^1 + \zeta_{17}^4 + \zeta_{17}^{-4} + \zeta_{17}^{-1},$$
$$\mathrm{tr}_F^K \zeta_{17}^3 = \zeta_{17}^3 + \zeta_{17}^{-5} + \zeta_{17}^{5} + \zeta_{17}^{-3},$$
$$\mathrm{tr}_F^K \zeta_{17}^2 = \zeta_{17}^2 + \zeta_{17}^{8} + \zeta_{17}^{-8} + \zeta_{17}^{-2},$$
$$\mathrm{tr}_F^K \zeta_{17}^6 = \zeta_{17}^6 + \zeta_{17}^{7} + \zeta_{17}^{-7} + \zeta_{17}^{-6}.$$

(Care is required for general conductor. Use 1997 Breuer; Breuer credits Hiss and Lenstra.)

Multiply in $\mathbf{Q}(\zeta_p)$ using FFT.

1968 Rader FFT: To evaluate
$g = g_1 x^1 + g_2 x^2 + \cdots + g_{16} x^{16}$
at $\zeta_{17}^1, \ldots, \zeta_{17}^{16}$, notice that
$g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g_{3^{-a}} \zeta_{17}^{3^{b-a}}$.

Multiply in $\mathbf{Q}(\zeta_p)$ using FFT.

1968 Rader FFT: To evaluate
$g = g_1 x^1 + g_2 x^2 + \cdots + g_{16} x^{16}$
at $\zeta_{17}^1, \ldots, \zeta_{17}^{16}$, notice that
$g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g_{3^{-a}} \zeta_{17}^{3^{b-a}}$.
Length-16 cyclic convolution of
$g_1, g_6, \ldots, g_9, g_3$ and
$\zeta_{17}^1, \zeta_{17}^3, \zeta_{17}^9, \ldots, \zeta_{17}^6$ is
$g(\zeta_{17}^1), g(\zeta_{17}^3), g(\zeta_{17}^9), \ldots, g(\zeta_{17}^6)$.

Multiply in $\mathbf{Q}(\zeta_p)$ using FFT.

1968 Rader FFT: To evaluate
$g = g_1x^1 + g_2x^2 + \cdots + g_{16}x^{16}$
at $\zeta_{17}^1, \ldots, \zeta_{17}^{16}$, notice that
$g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g_{3^{-a}} \zeta_{17}^{3^{b-a}}$.
Length-16 cyclic convolution of
$g_1, g_6, \ldots, g_9, g_3$ and
$\zeta_{17}^1, \zeta_{17}^3, \zeta_{17}^9, \ldots, \zeta_{17}^6$ is
$g(\zeta_{17}^1), g(\zeta_{17}^3), g(\zeta_{17}^9), \ldots, g(\zeta_{17}^6)$.

Folding the Rader FFT:
g represents elt of deg-4 subfield
$\Leftrightarrow$ $g_1, g_6, \ldots$ is 4-periodic.
Use length-4 cyclic convolution
with the Gauss periods.

2017 Arita–Handa: folded Rader FFT for prime conductor. (No mention of Gauss periods, Rader.)

2022 paper: Application to det. Application of segmentation. Analysis and comparison.

And beyond prime conductor: Generalization to arbitrary conductor (Section 4.12; one part is 1978 Winograd FFT). Sage scripts for arbitrary conductor (Appendix A). Fast C software (Appendix C) for the power-of-2 case study.