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
$B_{128} = -\zeta_{32}^{15} + \zeta_{32}^{14} - \zeta_{32}^{13} + \zeta_{32}^{12} + \zeta_{32}^{11} + \zeta_{32}^{10} + \zeta_{32}^{9} + \zeta_{32}^{8} - \zeta_{32}^{7} - \zeta_{32}^{6} - \zeta_{32}^{5} + \zeta_{32}^{4} + \zeta_{32}^{3} - \zeta_{32}^{2} - \zeta_{32} - 1$.

$29102880226241 = \cdots$

m computation
th-degree
number fields

ernstein

ty of Illinois at Chicago;
iversity Bochum;
ia Sinica

---

n,

number field K:
$\mathrm{et}^K_{\mathbf{Q}}\,\alpha$ mean tr, det of
as $\mathbf{Q}$-linear map $K \to K$.
nerally: $\mathrm{tr}^K_F\,\alpha$, $\det^K_F\,\alpha$ as
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 Ku
Schrutka
1970 Ne
Masley,
Williams
Loubout
various a
$m \mapsto h^-_m$
$m^{1.5+o(1}$
(even wi

h^-_m has

tation

elds

is at Chicago;

ochum;

eld K:

an tr, det of

ar map $K \to K$.

$^{K}_{F}\,\alpha$, $\det^{K}_{F}\,\alpha$ as

ubfield 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 $B_{64} = \zeta^7_{16} - \zeta^6_{16} + \zeta^5_{16} + \zeta^4_{16} + \zeta^3_{16} - \zeta^2_{16} - \zeta_{16} - 1$.

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

$29102880226241 = \cdots$

1851 Kummer, 19

Schrutka von Rech

1970 Newman, 19

Masley, 1992 Fung

Williams, 1995 Jha

Louboutin, 1999 S

various algorithms

$m \mapsto h^-_m$, all using

$m^{1.5+o(1)}$ bit oper

(even with fast mu

h^-_m has $m^{1+o(1)}$ bi

ago;

of

$\to K$.

α as

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 $B_{64} = \zeta^7_{16} - \zeta^6_{16} + \zeta^5_{16} + \zeta^4_{16} + \zeta^3_{16} - \zeta^2_{16} - \zeta_{16} - 1$.

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

$29102880226241 = \cdots$

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

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

Often want to compute $\det_{\mathbf{Q}}^{K}$.
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. $h_{64}^- = 17$; $h_{128}^- = 17\cdot 21121$; $h_{256}^- = 17\cdot 21121\cdot 29102880226241$.

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

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

Often want to compute $\det_{\mathbf{Q}}^{K}$.
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. $h_{64}^- = 17$; $h_{128}^- = 17 \cdot 21121$; $h_{256}^- = 17 \cdot 21121 \cdot 29102880226241$.

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

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

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

ant to compute $\det^K_{\mathbf{Q}}$.
many examples: Define
p$(2\pi i/m)$ and $h^-_m =$
$\zeta_m))/\#\mathrm{Cl}(\mathbf{R} \cap \mathbf{Q}(\zeta_m))$.

$= 17$; $h^-_{128} = 17 \cdot 21121$;
$7 \cdot 21121 \cdot 29102880226241$.

let$^{\mathbf{Q}(\zeta_{16})}_{\mathbf{Q}}(B_{64}/2)$ where
$_{16} - \zeta^6_{16} + \zeta^5_{16} + \zeta^4_{16} + \zeta^3_{16} -$
$_6 - 1$.

$= 2 \det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}}(B_{128}/2)$ where
$-\zeta^{15}_{32} + \zeta^{14}_{32} - \zeta^{13}_{32} + \zeta^{12}_{32} +$
$_2 + \zeta^9_{32} + \zeta^8_{32} - \zeta^7_{32} - \zeta^6_{32} -$
$_2 + \zeta^3_{32} - \zeta^2_{32} - \zeta_{32} - 1$.

$0226241 = \cdots$

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.

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

Main mo

Core co
number
elements
(element
factoriza

More ge
elements
to find S

Traditio
S-unit g
conjectu
Cl(K) in

mpute $\det^K_{\mathbf{Q}}$.
nples: Define
and $h^-_m =$
$(\mathbf{R} \cap \mathbf{Q}(\zeta_m))$.

$_8 = 17 \cdot 21121$;
29102880226241.

$B_{64}/2)$ where
$\zeta_{16}^5 + \zeta_{16}^4 + \zeta_{16}^3 -$

$^{2)}(B_{128}/2)$ where
$^4_2 - \zeta_{32}^{13} + \zeta_{32}^{12} +$
$\zeta_{32}^8 - \zeta_{32}^7 - \zeta_{32}^6 -$
$\zeta_{32}^2 - \zeta_{32} - 1$.

$= \cdots$

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.

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

Main motivation

Core computation
number theory: fil
elements of $\mathcal{O}_K$ to
(elements with pri
factorizations supp

More generally, filt
elements of an $\mathcal{O}_K$
to find S-generato

Traditional applica
S-unit group; in p
conjecturally obtai
$\mathrm{Cl}(K)$ in subexpon

$^{K}_{\mathbf{Q}}$.
fine
=
$_n$)).
1121;
26241.

ere
$+\zeta_{16}^{3} -$

) where
$\zeta_{32}^{12} +$
$- \zeta_{32}^{6} -$
$- 1$.

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 algebra
number theory: filter all sma
elements of $\mathcal{O}_K$ to find S-un
(elements with prime-ideal
factorizations supported on

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

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

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.

ummer, 1952 Hasse, 1964
a von Rechtenstamm,
ewman, 1978 Lehmer–
1992 Fung–Granville–
s, 1995 Jha, 1998
in, 1999 Shokrollahi:
algorithms to evaluate
, all using at least
$^{1)}$ bit operations
th fast multiplication).

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

y choices of m:
$_{\mathbf{Q}}^{K}$ as in this talk gives h_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

For som
find sma
low-dim
scan a s

52 Hasse, 1964
ntenstamm,
78 Lehmer–
g–Granville–
a, 1998
Shokrollahi:
to evaluate
at least
ations
ultiplication).

its.

of m:
is talk gives h_m^-
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

For some fields K
find small element
low-dimensional la
scan a sublattice f

1964
n,
r–
e–
:
te
n).
es h_m^-
s.

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 N
find small elements of $\mathcal{O}_K$ i
low-dimensional lattice. Eas
scan a sublattice for each fa

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.

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.

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 $\det^K_{\mathbf{Q}} \alpha$, see whether $\det^K_{\mathbf{Q}} \alpha$ factors suitably.

How fast is $\alpha \mapsto \det^K_{\mathbf{Q}} \alpha$?

otivation

mputation in algebraic
theory: filter all small
s of $\mathcal{O}_K$ to find S-units
ts with prime-ideal
ntions supported on S).

nerally, filter all small
s of an $\mathcal{O}_K$-ideal $I \neq 0$
S-generators of I.

nal application: Compute
roup; in particular,
rally obtain $\mathcal{O}_K^*$ and
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.

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 $\det^K_{\mathbf{Q}} \alpha$, see whether $\det^K_{\mathbf{Q}} \alpha$ factors suitably.

How fast is $\alpha \mapsto \det^K_{\mathbf{Q}} \alpha$?

Highligh

Section
is $\det^K_{\mathbf{Q}}$ c
where m
Trivially
precise '
to distril

in algebraic
ter all small
find S-units
me-ideal
orted on S).

ter all small
-ideal $I \neq 0$
rs of I.

ation: Compute
articular,
in $\mathcal{O}_K^*$ and
ential 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.

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 2

Section 2: For sm
is $\det_{\mathbf{Q}}^K \alpha$? Case st
where $m = 2n \in \{$
Trivially $O(n \log n$
precise "circular ap
to distribution; exp

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 pape

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

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 $\det^K_{\mathbf{Q}} \alpha$, see whether $\det^K_{\mathbf{Q}} \alpha$ factors suitably.

How fast is $\alpha \mapsto \det^K_{\mathbf{Q}} \alpha$?

Highlights of the 2022 paper

Section 2: For small α, how large is $\det^K_{\mathbf{Q}} \alpha$? 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.

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 $\det^K_{\mathbf{Q}} \alpha$, see whether $\det^K_{\mathbf{Q}} \alpha$ factors suitably.

How fast is $\alpha \mapsto \det^K_{\mathbf{Q}} \alpha$?

Highlights of the 2022 paper

Section 2: For small α, how large is $\det^K_{\mathbf{Q}} \alpha$? 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 $\det^K_{\mathbf{Q}}$ 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.

recognize S-units?

e fields K (e.g., in NFS),
ll elements of $\mathcal{O}_K$ in a
ensional lattice. Easily
ublattice for each factor.

nced high-degree K (e.g.,
nics), lattice has high
on; scanning sublattices
ard. So, for each small α
automorphisms etc.),
e $\det^K_{\mathbf{Q}} \alpha$, see whether
factors suitably.

t is $\alpha \mapsto \det^K_{\mathbf{Q}} \alpha$?

Highlights of the 2022 paper

Section 2: For small α, how large is $\det^K_{\mathbf{Q}} \alpha$? 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 $\det^K_{\mathbf{Q}}$ 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
obviousl
for the s
See pape

S-units?

(e.g., in NFS),
s of $\mathcal{O}_K$ in a
ttice. Easily
or each factor.

-degree K (e.g.,
ce has high
ng sublattices
or each small α
phisms etc.),
see whether
tably.

det$^K_{\mathbf{Q}}\,\alpha$?

Highlights of the 2022 paper

Section 2: For small α, how large is $\det^K_{\mathbf{Q}}\alpha$? 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 $\det^K_{\mathbf{Q}}$ 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: $\det^K_{\mathbf{Q}}\,\alpha$
obviously reduces
for the same $\mathbf{Q}(\zeta_n$
See paper for cred

NFS),
n a
ily
ctor.
(e.g.,
h
ces
nall α
.),
er

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: $\det_{\mathbf{Q}}^{K} \alpha = \det_{\mathbf{Q}}^{F}$ d
obviously reduces cost to n^1
for the same $\mathbf{Q}(\zeta_m)$ case stu
See paper for credits + spee

Highlights of the 2022 paper

Section 2: For small α, how large is $\det^K_{\mathbf{Q}} \alpha$? 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 $\det^K_{\mathbf{Q}}$ 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: $\det^K_{\mathbf{Q}} \alpha = \det^F_{\mathbf{Q}} \det^K_F \alpha$ obviously reduces cost to $n^{1+o(1)}$ for the same $\mathbf{Q}(\zeta_m)$ case study. See paper for credits + speedups.

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 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 $(\log n)^{o(1)}$.

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 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.

ts of the 2022 paper

2: For small α, how large
α? Case study: $\mathbf{Q}(\zeta_m)$
$= 2n \in \{4, 8, 16, \ldots\}$.
$O(n \log n)$ bits; more
"circular approximation"
bution; experiments.

3: How fast are
l $\det^K_{\mathbf{Q}}$ algorithms?
r resultants via continued
s: usually $n^2(\log n)^{3+o(1)}$.
) in $\mathbf{C}$: $n^2(\log n)^{3+o(1)}$;
$)^{2+o(1)}$ using a cyclotomic
from 1982 Schönhage.

Section 1: $\det^K_{\mathbf{Q}} \alpha = \det^F_{\mathbf{Q}} \det^K_F \alpha$
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-o

Take, e.g

$\det^{\mathbf{Q}(\zeta_{32}}_{\mathbf{Q}(\zeta_{16}}$
$= -6\zeta^7_{16}$
$- 6\zeta^3_{1}$

$\det^{\mathbf{Q}(\zeta_{32}}_{\mathbf{Q}(\zeta_8)}$
$= -88\zeta$

$\det^{\mathbf{Q}(\zeta_{32}}_{\mathbf{Q}(\zeta_4)}$
$= 22912$

$\det^{\mathbf{Q}(\zeta_{32}}_{\mathbf{Q}}$
$= 69209$

2022 paper

all α, how large
tudy: $\mathbf{Q}(\zeta_m)$
{4, 8, 16, . . .}.
) bits; more
pproximation"
periments.

st are
orithms?
s via continued
$n^2(\log n)^{3+o(1)}$.
$(\log n)^{3+o(1)}$;
ing a cyclotomic
2 Schönhage.

Section 1: $\det^K_{\mathbf{Q}} \alpha = \det^F_{\mathbf{Q}} \det^K_F \alpha$ 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 cycloto

Take, e.g., $B_{128} =$

$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{16})} B_{128} = B$
$= -6\zeta_{16}^7 - 2\zeta_{16}^6 -$
$- 6\zeta_{16}^3 + 6\zeta_{16}^2 -$

$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_8)} B_{128}$
$= -88\zeta_8^3 + 104\zeta_8^2$

$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_4)} B_{128}$
$= 22912\zeta_4 - 1292$

$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}} B_{128}$
$= 692092928 = 2$

r

large

$m)$

$.\}.$

re

ion"

nued

$+o(1)$.

(1);

otomic

ge.

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., $B_{128} = -\zeta_{32}^{15} + \cdot$

$\det_{\mathbf{Q}(\zeta_{16})}^{\mathbf{Q}(\zeta_{32})} B_{128} = B_{128} \cdot \sigma(B$

$= -6\zeta_{16}^{7} - 2\zeta_{16}^{6} - 6\zeta_{16}^{5} - 6\zeta$

$- 6\zeta_{16}^{3} + 6\zeta_{16}^{2} - 2\zeta_{16} - 2$

$\det_{\mathbf{Q}(\zeta_{8})}^{\mathbf{Q}(\zeta_{32})} B_{128}$

$= -88\zeta_{8}^{3} + 104\zeta_{8}^{2} + 56\zeta_{8} +$

$\det_{\mathbf{Q}(\zeta_{4})}^{\mathbf{Q}(\zeta_{32})} B_{128}$

$= 22912\zeta_4 - 12928.$

$\det_{\mathbf{Q}}^{\mathbf{Q}(\zeta_{32})} B_{128}$

$= 692092928 = 21121 \cdot 2^{15}.$

Section 1: $\det^K_{\mathbf{Q}} \alpha = \det^F_{\mathbf{Q}} \det^K_F \alpha$ 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., $B_{128} = -\zeta_{32}^{15} + \cdots$.

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

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{8})} B_{128}$$
$$= -88\zeta_8^3 + 104\zeta_8^2 + 56\zeta_8 + 88.$$

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{4})} B_{128}$$
$$= 22912\zeta_4 - 12928.$$

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

1: $\det^K_{\mathbf{Q}} \alpha = \det^F_{\mathbf{Q}} \det^K_F \alpha$

y reduces cost to $n^{1+o(1)}$

ame $\mathbf{Q}(\zeta_m)$ case study.

er for credits + speedups.

4: How general is this?

nall-relative-degree tower.

nt small bases supporting

tiplication and subfields.

lian fields: Gauss-period

small, supports subfields;

zing Rader's FFT gives

tiplication; total cost

$^{3+o(1)}$ if reldeg $(\log n)^{o(1)}$.

5: S-unit application.

Power-of-2 cyclotomics

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

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

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_8)} B_{128}$$
$$= -88\zeta_8^3 + 104\zeta_8^2 + 56\zeta_8 + 88.$$

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_4)} B_{128}$$
$$= 22912\zeta_4 - 12928.$$

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

2010 Ge

$n(\log n)^{0}$

the spec

with n a

$= \det_{\mathbf{Q}}^{F} \det_{F}^{K} \alpha$

cost to $n^{1+o(1)}$

$_n$) case study.

its + speedups.

eneral is this?

e-degree tower.

ases supporting

and subfields.

Gauss-period

ports subfields;

's FFT gives

; total cost

eldeg $(\log n)^{o(1)}$.

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–Hale

$n(\log n)^{O(1)}$ and "

the special form o

with n a power of

$\det^K_F \alpha$
$+o(1)$
udy.
edups.
his?
ower.
orting
elds.
eriod
ields;
ves
t
$n)^{o(1)}$.
n.

Power-of-2 cyclotomics

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

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

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{8})} B_{128}$$
$$= -88\zeta_8^3 + 104\zeta_8^2 + 56\zeta_8 + 88.$$

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{4})} B_{128}$$
$$= 22912\zeta_4 - 12928.$$

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

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

Power-of-2 cyclotomics

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

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

$\det_{\mathbf{Q}(\zeta_8)}^{\mathbf{Q}(\zeta_{32})} B_{128}$
$= -88\zeta_8^3 + 104\zeta_8^2 + 56\zeta_8 + 88.$

$\det_{\mathbf{Q}(\zeta_4)}^{\mathbf{Q}(\zeta_{32})} B_{128}$
$= 22912\zeta_4 - 12928.$

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

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".

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".

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

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".

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

What about further fields?
Main challenge: fast multiplication.

Power-of-2 cyclotomics

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

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

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{8})} B_{128}$$
$$= -88\zeta_8^3 + 104\zeta_8^2 + 56\zeta_8 + 88.$$

$$\det^{\mathbf{Q}(\zeta_{32})}_{\mathbf{Q}(\zeta_{4})} B_{128}$$
$$= 22912\zeta_4 - 12928.$$

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

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".

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.

f-2 cyclotomics

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

) $B_{128} = B_{128} \cdot \sigma(B_{128})$
)

$_6 - 2\zeta_{16}^6 - 6\zeta_{16}^5 - 6\zeta_{16}^4$
$^3_{16} + 6\zeta_{16}^2 - 2\zeta_{16} - 2$.

) B_{128}

$^3_8 + 104\zeta_8^2 + 56\zeta_8 + 88$.

) B_{128}

$2\zeta_4 - 12928$.

) B_{128}

$92928 = 21121 \cdot 2^{15}$.

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".

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-c

For prim
use long

Use Gau
for each
e.g., for
of $K =$
$\mathrm{tr}^K_F\, \zeta_{17}^1 =$
$\mathrm{tr}^K_F\, \zeta_{17}^3 =$
$\mathrm{tr}^K_F\, \zeta_{17}^2 =$
$\mathrm{tr}^K_F\, \zeta_{17}^6 =$

(Care is
conduct
Breuer c

omics

$= -\zeta_{32}^{15} + \cdots$.

$B_{128} \cdot \sigma(B_{128})$

$6\zeta_{16}^{5} - 6\zeta_{16}^{4}$
$- 2\zeta_{16} - 2$.

$+ 56\zeta_8 + 88$.

28.

$1121 \cdot 2^{15}$.

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".

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 c

For prime p with s
use long tower $\mathbf{Q}$ (

Use Gauss periods
for each subfield F
e.g., for degree-4 s
of $K = \mathbf{Q}(\zeta_{17})$, us
$\mathrm{tr}_F^K \zeta_{17}^{1} = \zeta_{17}^{1} + \zeta_1$
$\mathrm{tr}_F^K \zeta_{17}^{3} = \zeta_{17}^{3} + \zeta_1$
$\mathrm{tr}_F^K \zeta_{17}^{2} = \zeta_{17}^{2} + \zeta_1$
$\mathrm{tr}_F^K \zeta_{17}^{6} = \zeta_{17}^{6} + \zeta_1$

(Care is required f
conductor. Use 19
Breuer credits His

$\cdots$.

$_{128})$

-4
16

.

88.

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
use long tower $\mathbf{Q} \subset \cdots \subset \mathbf{Q}$

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 basi
$\mathrm{tr}^K_F\, \zeta^1_{17} = \zeta^1_{17} + \zeta^4_{17} + \zeta^{-4}_{17} +$
$\mathrm{tr}^K_F\, \zeta^3_{17} = \zeta^3_{17} + \zeta^{-5}_{17} + \zeta^5_{17} +$
$\mathrm{tr}^K_F\, \zeta^2_{17} = \zeta^2_{17} + \zeta^8_{17} + \zeta^{-8}_{17} +$
$\mathrm{tr}^K_F\, \zeta^6_{17} = \zeta^6_{17} + \zeta^7_{17} + \zeta^{-7}_{17} +$

(Care is required for general
conductor. Use 1997 Breuer
Breuer credits Hiss and Lens

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

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

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

ntry–Halevi: This costs

$O(1)$ and "relies heavily on

ial form of . . . $x^n + 1$,

power of two".

also works for $\mathbf{Q}(\zeta_m)$ for

oth positive integer m.

out further fields?

allenge: fast multiplication.

uch–Bernstein–de

-Lange–van Vredendaal

analogous det evaluation

iquadratic fields, built

ast-multiplication

n 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

1968 Ra

$g = g_1 x$

at ζ_{17}^{1}, .

$g(\zeta_{17}^{3^b})$ =

vi: This costs
relies heavily on
f . . . $x^n + 1$,
two".

for $\mathbf{Q}(\zeta_m)$ for
ve integer m.

er fields?
ast multiplication.

stein–de
n Vredendaal
s det evaluation
fields, built
lication
e 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 $\mathbf{Q}(\zeta_p)$

1968 Rader FFT:
$g = g_1 x^1 + g_2 x^2$
at $\zeta_{17}^{1}, \ldots, \zeta_{17}^{16}$, no
$g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3}$

osts
vily on
- 1,

) for
m.

ication.

laal
uation
ilt

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

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

(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 evaluat
$g = g_1x^1 + g_2x^2 + \cdots + g_{16}$
at $\zeta_{17}^1, \ldots, \zeta_{17}^{16}$, notice that
$g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g$

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 $g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g_{3^{-a}} \zeta_{17}^{3^{b-a}}$.

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

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

(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 $g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g_{3^{-a}} \zeta_{17}^{3^{b-a}}$.

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 $g(\zeta_{17}^1), g(\zeta_{17}^3), g(\zeta_{17}^9), \ldots, g(\zeta_{17}^6)$.

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 $g = g_1x^1 + g_2x^2 + \cdots + g_{16}x^{16}$ 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.

onductor cyclotomics

ne p with smooth $p-1$:
tower $\mathbf{Q} \subset \cdots \subset \mathbf{Q}(\zeta_p)$.

ss periods as a basis
subfield $F \subseteq \mathbf{Q}(\zeta_p)$:
degree-4 subfield F
$\mathbf{Q}(\zeta_{17})$, use the basis
$= \zeta_{17}^{1} + \zeta_{17}^{4} + \zeta_{17}^{-4} + \zeta_{17}^{-1}$,
$= \zeta_{17}^{3} + \zeta_{17}^{-5} + \zeta_{17}^{5} + \zeta_{17}^{-3}$,
$= \zeta_{17}^{2} + \zeta_{17}^{8} + \zeta_{17}^{-8} + \zeta_{17}^{-2}$,
$= \zeta_{17}^{6} + \zeta_{17}^{7} + \zeta_{17}^{-7} + \zeta_{17}^{-6}$.

required for general
or. Use 1997 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
$g(\zeta_{17}^{3^b}) = \sum_j g_j \zeta_{17}^{3^b j} = \sum_a g_{3^{-a}} \zeta_{17}^{3^{b-a}}$.
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 Ari
FFT for
mention

2022 pa
Applicat
Analysis

And bey
Generali
conducto
part is 1
Sage scr
conducto
Fast C s
for the p

cyclotomics

smooth $p-1$:

$\subset \cdots \subset \mathbf{Q}(\zeta_p)$.

as a basis

$F \subseteq \mathbf{Q}(\zeta_p)$:

subfield F

se the basis

$_7 + \zeta_{17}^{-4} + \zeta_{17}^{-1}$,

$^{-5}_7 + \zeta_{17}^{5} + \zeta_{17}^{-3}$,

$_7 + \zeta_{17}^{-8} + \zeta_{17}^{-2}$,

$_7 + \zeta_{17}^{-7} + \zeta_{17}^{-6}$.

or general

997 Breuer;

s and Lenstra.)

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

FFT for prime con

mention of Gauss

2022 paper: Appli

Application of seg

Analysis and comp

And beyond prime

Generalization to a

conductor (Sectior

part is 1978 Winog

Sage scripts for ar

conductor (Appen

Fast C software (A

for the power-of-2

s

$- 1$:

(ζ_p).

s

:

s

ζ_{17}^{-1},

ζ_{17}^{-3},

ζ_{17}^{-2},

ζ_{17}^{-6}.

r;

stra.)

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 R
FFT for prime conductor. (N
mention of Gauss periods, R

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

And beyond prime conducto
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 stud

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 $g(\zeta_{17}^{3^b}) = \sum_j g_j\zeta_{17}^{3^bj} = \sum_a g_{3^{-a}}\zeta_{17}^{3^{b-a}}$.
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.