Dan Shanks' CUFFQI Algorithm Resurrected

Renate Scheidler

rscheidl@ucalgary.ca

UNIVERSITY OF CALGARY

Celebrating 75 Years of Mathematics of Computation
ICERM (Providence, RI)
November 1, 2018

What is CUFFQI?

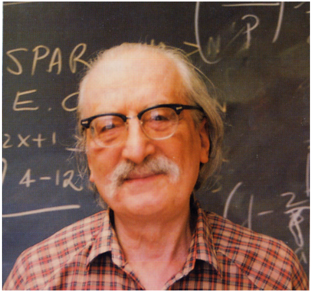
Short for Cubic Fields From Quadratic Infrastructure

What is CUFFQI?

Short for Cubic Fields From Quadratic Infrastructure

- Invented by Dan Shanks (1987)

  Editor for Math. Comp. 1959-1996



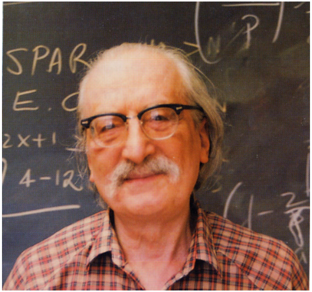
What is CUFFQI?

Short for Cubic Fields From Quadratic Infrastructure

- Invented by Dan Shanks (1987)

  Editor for Math. Comp. 1959-1996

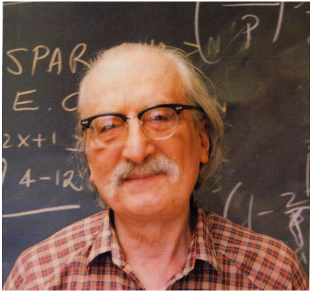
- Made practical and implemented by Gilbert Fung (1990)



What is CUFFQI?

Short for Cubic Fields From Quadratic Infrastructure

- Invented by Dan Shanks (1987)
  Editor for Math. Comp. 1959-1996
- Made practical and implemented by Gilbert Fung (1990)
- Unpublished (to appear as Chapter 4 in *Cubic Fields With Geometry* by S. Hambleton & H. C. Williams, Springer Monograph 2018/19)



Cubic Fields

A cubic field of discriminant D has a generating polynomials of the form

$$f(x) = x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda)$$

- λ is an algebraic integer in $\mathbb{Q}(\sqrt{-3D})$
- Norm and trace are taken in $\mathbb{Q}(\sqrt{-3D})/\mathbb{Q}$
- $N(\lambda) \in \mathbb{Z}^3$

(Berwick 1925)

Cubic Fields

A cubic field of discriminant D has a generating polynomials of the form

$$f(x) = x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda)$$

- λ is an algebraic integer in $\mathbb{Q}(\sqrt{-3D})$
- Norm and trace are taken in $\mathbb{Q}(\sqrt{-3D})/\mathbb{Q}$
- $N(\lambda) \in \mathbb{Z}^3$

(Berwick 1925)

Roots of $f(x)$ (Cardano 1545):

$$\zeta^i \lambda^{1/3} + \zeta^{-i}\overline{\lambda}^{1/3} \qquad (i = 0, 1, 2)$$

where ζ is a primitive cube root of unity

Example: $D = 44806173$

Naively $\big($take λ to be the fundamental unit of $\mathbb{Q}(\sqrt{-3 \cdot 44806173})$ $\big)$:

$$f(x) = x^3 - 3x + 963135381187786734040565836 6$$

Naively $\Big($take λ to be the fundamental unit of $\mathbb{Q}(\sqrt{-3 \cdot 44806173})$ $\Big)$:

$$f(x) = x^3 - 3x + 963135381187786734040565836 6$$

Using CUFFQI (all 13 cubic fields with $D = 44806173$):

$$\begin{aligned}
f_1(x) &= x^3 - 61x^2 + 697x - 330 \\
f_2(x) &= x^3 - 279x^2 + 441x - 170 \\
f_3(x) &= x^3 - 63x^2 + 423x - 8 \\
f_4(x) &= x^3 - 69x^2 + 435x - 216 \\
f_5(x) &= x^3 - 63x^2 + 603x - 494 \\
f_6(x) &= x^3 - 83x^2 + 297x - 54 \\
f_7(x) &= x^3 - 63x^2 + 837x - 494 \\
f_8(x) &= x^3 - 257x^2 + 477x - 216 \\
f_9(x) &= x^3 - 87x^2 + 273x - 36 \\
f_{10}(x) &= x^3 - 62x^2 + 546x - 261 \\
f_{11}(x) &= x^3 - 60x^2 + 660x - 97 \\
f_{12}(x) &= x^3 - 165x^2 + 273x - 90 \\
f_{13}(x) &= x^3 - 127x^2 + 185x - 62
\end{aligned}$$

Cubic Field Construction

Problem with Berwick construction: polynomial coefficients can be HUGE!
$\Big($E.g. $Tr(\varepsilon) \approx \varepsilon \approx \exp(\sqrt{|D|})$ for the fundamental unit $\varepsilon \in \mathbb{Q}(\sqrt{-3D})\Big)$

CUFFQI to the rescue!

Cubic Field Construction

Problem with Berwick construction: polynomial coefficients can be HUGE!
$\big($E.g. $Tr(\varepsilon) \approx \varepsilon \approx \exp(\sqrt{|D|})$ for the fundamental unit $\varepsilon \in \mathbb{Q}(\sqrt{-3D})\big)$

CUFFQI to the rescue!

Goal: for a a given fundamental discriminant D, produce all the cubic fields of discriminant D à la Berwick via generating polynomials with small coefficients

The Berwick Map

There is a map from the set of unordered triples of conjugate cubic fields

$$\{ \mathbb{K}, \mathbb{K}', \mathbb{K}'' \} \qquad \text{disc}(\mathbb{K}) = D$$

to the set of unordered pairs of 3-torsion ideal classes

$$\{ [\mathfrak{a}], [\overline{\mathfrak{a}}] \}$$

in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ via

$$x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda) \quad \longmapsto \quad \{ [\mathfrak{a}], [\overline{\mathfrak{a}}] \} \qquad \text{where } \mathfrak{a}^3 = (\lambda)$$

The Berwick Map

There is a map from the set of unordered triples of conjugate cubic fields

$$\{\ \mathbb{K},\ \mathbb{K}',\ \mathbb{K}''\ \} \qquad \text{disc}(\mathbb{K}) = D$$

to the set of unordered pairs of 3-torsion ideal classes

$$\{\ [\,\mathfrak{a}\,]\,,\ [\,\overline{\mathfrak{a}}\,]\ \}$$

in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ via

$$x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda) \quad \longmapsto \quad \{\,[\mathfrak{a}],\ [\overline{\mathfrak{a}}]\,\} \qquad \text{where } \mathfrak{a}^3 = (\lambda)$$

For $D > 0$:

bijection onto non-principal ideal classes
nothing maps to the principal class

For $D < 0$:

3-to-1 onto non-principal ideal classes
1-to-1 onto to the principal class

Some Counting

Put

$$r = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$$

$$s = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$$

Some Counting

Put

$$r = \text{3-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$$
$$s = \text{3-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$$

Number of cubic fields of discriminant D (Hasse 1929): $\frac{3^r - 1}{2}$

Some Counting

Put

$$r = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$$
$$s = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$$

Number of cubic fields of discriminant D (Hasse 1929): $\dfrac{3^r - 1}{2}$

Number of cubic fields produced by the Berwick map:

For $D > 0$: $\dfrac{3^s - 1}{2}$

For $D < 0$: $3 \cdot \dfrac{3^s - 1}{2} + 1 = \dfrac{3^{s+1} - 1}{2}$

Some Counting

Put

$$r = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$$
$$s = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$$

Number of cubic fields of discriminant D (Hasse 1929): $\dfrac{3^r - 1}{2}$

Number of cubic fields produced by the Berwick map:

For $D > 0$: $\dfrac{3^s - 1}{2}$

For $D < 0$: $3 \cdot \dfrac{3^s - 1}{2} + 1 = \dfrac{3^{s+1} - 1}{2}$

Connection between r and s (Scholz 1932):

$|r - s| \leq 1$

If $r \neq s$, then the imaginary quadratic field has the bigger 3-rank

Case $D > 0$:

$r = s$: $$\frac{3^s - 1}{2} = \frac{3^r - 1}{2}$$ ☺

$r = s - 1$: $$\frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r$$ ☹

Case $D > 0$:

$$r = s: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

$$r = s - 1: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + \color{red}{3^r} \qquad ☹$$

Case $D < 0$:

$$r = s: \qquad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} + \color{red}{3^r} \qquad ☹$$

$$r = s + 1: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

More Counting

Case $D > 0$:

$$r = s: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \quad ☺$$

$$r = s - 1: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r \quad ☹$$

Case $D < 0$:

$$r = s: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} + 3^r \quad ☹$$

$$r = s + 1: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} \quad ☺$$

So what are these extra 3^r cubic fields?

More Counting

Case $D > 0$:

$$r = s: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

$$r = s - 1: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

Case $D < 0$:

$$r = s: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

$$r = s + 1: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

So what are these extra 3^r cubic fields?

Answer: they are the complete collection of cubic fields of discriminant

$$9D \quad \text{if} \quad 3 \mid D, \qquad 81D \quad \text{if} \quad 3 \nmid D$$

In the ☺ cases there are no fields of these discriminants

Berwick Construction Algorithm

Input: D and a basis of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D})[3]$
$\big($For $D < 0$, also the regulator R of $\mathbb{Q}(\sqrt{-3D})\big)$

Output: generating polynomials of all cubic fields of discriminant D

Algorithm:

For each basis class $\mathcal{C}$ of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D})[3]$, collect generators λ of

one ideal in $\mathcal{C}$ whose cube has a small generator when $D > 0$

three ideals in $\mathcal{C}$ whose cube has a small generator when $D < 0$

Collect a small element λ ($\notin \mathbb{Z}$) in some principal ideal when $D < 0$

For each λ collected

compute $f(x) = x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda)$

if $\mathrm{disc}(f) = D$, output $f(x)$

Reduced Ideals

An ideal $\mathfrak{a}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ is **reduced** if no non-zero element $\alpha \in \mathfrak{a}$ satisfies

$$|\alpha| < N(\mathfrak{a}) \quad \text{and} \quad |\overline{\alpha}| < N(\mathfrak{a})$$

Reduced Ideals

An ideal $\mathfrak{a}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ is **reduced** if no non-zero element $\alpha \in \mathfrak{a}$ satisfies

$$|\alpha| < N(\mathfrak{a}) \quad \text{and} \quad |\overline{\alpha}| < N(\mathfrak{a})$$

If $\mathfrak{a}$ is reduced, then

$$N(\mathfrak{a}) < \begin{cases} \sqrt{|D'|/3} & \text{when } D' < 0 \\ \sqrt{D'} & \text{when } D' > 0 \end{cases}$$

where $D' = -D/3$ when $3 \mid D$ and $D' = -3D$ when $3 \nmid D$.

Reduced Ideals

An ideal $\mathfrak{a}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-3D})}$ is **reduced** if no non-zero element $\alpha \in \mathfrak{a}$ satisfies

$$|\alpha| < N(\mathfrak{a}) \quad \text{and} \quad |\overline{\alpha}| < N(\mathfrak{a})$$

If $\mathfrak{a}$ is reduced, then

$$N(\mathfrak{a}) < \begin{cases} \sqrt{|D'|/3} & \text{when } D' < 0 \\ \sqrt{D'} & \text{when } D' > 0 \end{cases}$$

where $D' = -D/3$ when $3 \mid D$ and $D' = -3D$ when $3 \nmid D$.

If $\mathfrak{a}$ is reduced and $\mathfrak{a}^3 = (\lambda)$, then

$$N(\lambda) < \begin{cases} (|D'|/3)^{3/2} & \text{when } D' < 0 \\ (D')^{3/2} & \text{when } D' > 0 \end{cases}$$

Hence, to get λ of small norm, use reduced ideals (exist in every ideal class)

Generators λ of Small Trace, $D' < 0$

Here, the reduced ideal $\mathfrak{a}$ is unique.

Generators λ of Small Trace, $D' < 0$

Here, the reduced ideal $\mathfrak{a}$ is unique.

Write $\lambda = \dfrac{A + B\sqrt{D'}}{2}$ $(A, B \in \mathbb{Z})$. Then

$$4N(\lambda) = A^2 - B^2 D' = A^2 + B^2 |D'|$$

Generators λ of Small Trace, $D' < 0$

Here, the reduced ideal $\mathfrak{a}$ is unique.

Write $\lambda = \dfrac{A + B\sqrt{D'}}{2}$ $(A, B \in \mathbb{Z})$. Then

$$4N(\lambda) = A^2 - B^2 D' = A^2 + B^2 |D'|$$

$N(\lambda) < (|D'|/3)^{3/2}$ implies

$$|\mathrm{Tr}(\lambda)| \;=\; |A| \;<\; \frac{1}{2}\left(\frac{|D'|}{3}\right)^{3/4}$$

Generators λ of Small Trace, $D' < 0$

Here, the reduced ideal $\mathfrak{a}$ is unique.

Write $\lambda = \dfrac{A + B\sqrt{D'}}{2}$ $(A, B \in \mathbb{Z})$. Then

$$4N(\lambda) = A^2 - B^2 D' = A^2 + B^2|D'|$$

$N(\lambda) < (|D'|/3)^{3/2}$ implies

$$|\mathrm{Tr}(\lambda)| \ = \ |A| \ < \ \frac{1}{2}\left(\frac{|D'|}{3}\right)^{3/4}$$

Happily, the reduced ideal also yields a small trace!

Infrastructures, $D' > 0$

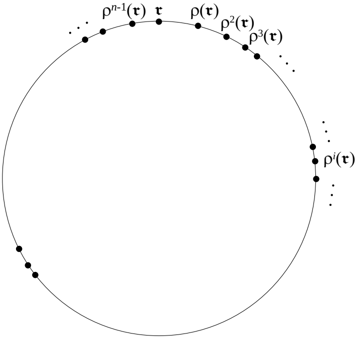
For any ideal class $\mathcal{C}$, the **infrastructure** of the $\mathcal{C}$ is the collection of all reduced ideals in $\mathcal{C}$ (Shanks 1972)

Infrastructures, $D' > 0$

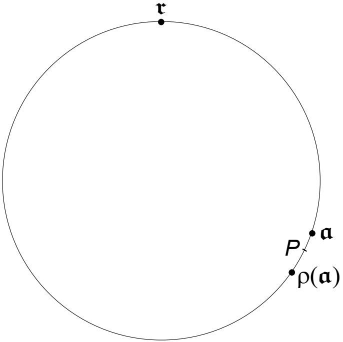
For any ideal class $\mathcal{C}$, the **infrastructure** of the $\mathcal{C}$ is the collection of all reduced ideals in $\mathcal{C}$ (Shanks 1972)

- Infrastructures are finite.
- Can move from one infrastructure ideal $\mathfrak{a}$ to its *neighbour* $\rho(\mathfrak{a})$ via one step in a simple continued fraction expansion
- Infrastructure ideals are discretely spaced on a circle of circumference R, the regulator of $\mathbb{Q}(\sqrt{D'})$
- For any point P on the circle, there is a unique reduced ideal *closest* to P (efficiently computable)

Infrastructures, $D' > 0$



Infrastructure of $\mathcal{C} = [\mathfrak{r}]$



$\mathfrak{a}$ is closest to P

Suitable Reduced Ideals, $D' < 0$

$\lambda \in \mathcal{O}_{\mathbb{Q}(\sqrt{D'})}$ is **small** if

$$1 < \lambda < (D')^{3/2}, \qquad |N(\lambda)| < (D')^{3/2}$$

Suitable Reduced Ideals, $D' < 0$

$\lambda \in \mathcal{O}_{\mathbb{Q}(\sqrt{D'})}$ is **small** if

$$1 < \lambda < (D')^{3/2}\,, \qquad |N(\lambda)| < (D')^{3/2}$$

The following reduced ideals have cubes with small generators (Shanks):

- For the principal ideal class, the reduced ideal closest to

$$\frac{R}{3} + \frac{\log(D')}{4}$$

Suitable Reduced Ideals, $D' < 0$

$\lambda \in \mathcal{O}_{\mathbb{Q}(\sqrt{D'})}$ is **small** if

$$1 < \lambda < (D')^{3/2}\,, \qquad |N(\lambda)| < (D')^{3/2}$$

The following reduced ideals have cubes with small generators (Shanks):

- For the principal ideal class, the reduced ideal closest to

$$\frac{R}{3} + \frac{\log(D')}{4}$$

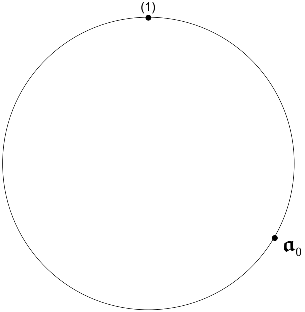
- For any non-principal ideal class $\mathcal{C}$, the three reduced ideals closest to

$$d\,, \quad \frac{R}{3} + d\,, \quad \frac{2R}{3} + d$$

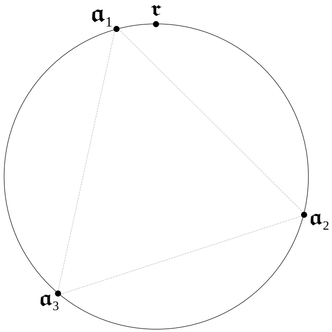
  where $0 < d < R/3$ and z can be explicitly computed

  (z depends on the representative of $\mathcal{C}$)

Suitable Reduced Ideals, $D' < 0$



Principal infrastructure



Non-principal infrastructures

Finding Small Generators, $D' > 0$

Shanks' strategy for finding λ (or $\overline{\lambda}$):

- Search the infrastructures of $[\mathfrak{a}]$ and of $[\,\overline{\mathfrak{a}}\,]$ simultaneously to find λ or $\overline{\lambda}$
- The two infrastructures are mirror images of each other

Fung's Work

In his 1990 PhD dissertation, Fung

- translated CUFFQI from Shanksian into a form suitable for computation
- implemented CUFFQI in Fortran on an Amdahl 5870 mainframe computer
- produced a number of examples, including the

$$\frac{3^6 - 1}{2} = 364$$

cubic fields of the 19-digit discriminant

$$D = -3161659186633662283$$

in under 3 CPU minutes

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$

CUFFFQI — Function Fields

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$
- $\mathbb{Z} \to \mathbb{F}_q[x]$

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$
- $\mathbb{Z} \to \mathbb{F}_q[x]$
- $D \to D(t) \in \mathbb{F}_q[t]$ square-free

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$
- $\mathbb{Z} \to \mathbb{F}_q[x]$
- $D \to D(t) \in \mathbb{F}_q[t]$ square-free
- $K = \mathbb{F}_q(t, x)$, $[K : \mathbb{F}_q(t)] = 3$

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$
- $\mathbb{Z} \to \mathbb{F}_q[x]$
- $D \to D(t) \in \mathbb{F}_q[t]$ square-free
- $K = \mathbb{F}_q(t, x)$, $[K : \mathbb{F}_q(t)] = 3$

  minimal polynomial $f(x) = x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda) \in \mathbb{F}_q[t, x]$

CUFFFQI — Function Fields

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$
- $\mathbb{Z} \to \mathbb{F}_q[x]$
- $D \to D(t) \in \mathbb{F}_q[t]$ square-free
- $K = \mathbb{F}_q(t, x)$, $[K : \mathbb{F}_q(t)] = 3$

  minimal polynomial $f(x) = x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda) \in \mathbb{F}_q[t, x]$
- $\mathbb{R} \to \mathbb{F}_q((x^{-1}))$

Jacobson, Lee, S. and Williams, Int. J. Number Theory **11** (2015)

Dictionary:

- $\mathbb{Q} \to \mathbb{F}_q(t)$, q a prime power, $\gcd(q, 6) = 1$
- $\mathbb{Z} \to \mathbb{F}_q[x]$
- $D \to D(t) \in \mathbb{F}_q[t]$ square-free
- $K = \mathbb{F}_q(t, x)$, $[K : \mathbb{F}_q(t)] = 3$

  minimal polynomial $f(x) = x^3 - 3N(\lambda)^{1/3}x + Tr(\lambda) \in \mathbb{F}_q[t, x]$
- $\mathbb{R} \to \mathbb{F}_q((x^{-1}))$
- $\mathbb{C} \to \mathbb{F}_{q^2}((x^{-1}))$ or $\mathbb{F}_q((x^{-1/2}))$

Problems

- Infinite place of $\mathbb{F}_q(t)$ is archimedian — can decompose in any way

Problems

- Infinite place of $\mathbb{F}_q(t)$ is archimedean — can decompose in any way
- $f(x)$ need not have a root in $\mathbb{F}_q((x^{-1}))$

Problems

- Infinite place of $\mathbb{F}_q(t)$ is archimedean — can decompose in any way
- $f(x)$ need not have a root in $\mathbb{F}_q((x^{-1}))$
- $\mathbb{F}_q(t, \sqrt{-3D}) = \mathbb{F}_q(t, \sqrt{D})$ if $q \equiv 1 \pmod 3$

Problems

- Infinite place of $\mathbb{F}_q(t)$ is archimedian — can decompose in any way
- $f(x)$ need not have a root in $\mathbb{F}_q((x^{-1}))$
- $\mathbb{F}_q(t, \sqrt{-3D}) = \mathbb{F}_q(t, \sqrt{D})$ if $q \equiv 1 \pmod 3$
- Extra fields? $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{9D}) = \mathbb{F}_q(t, \sqrt{81D})$

Problems

- Infinite place of $\mathbb{F}_q(t)$ is archimedian — can decompose in any way
- $f(x)$ need not have a root in $\mathbb{F}_q((x^{-1}))$
- $\mathbb{F}_q(t, \sqrt{-3D}) = \mathbb{F}_q(t, \sqrt{D})$ if $q \equiv 1 \pmod 3$
- Extra fields? $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{9D}) = \mathbb{F}_q(t, \sqrt{81D})$
- Hasse count is wrong

Problems

- Infinite place of $\mathbb{F}_q(t)$ is archimedean — can decompose in any way
- $f(x)$ need not have a root in $\mathbb{F}_q((x^{-1}))$
- $\mathbb{F}_q(t, \sqrt{-3D}) = \mathbb{F}_q(t, \sqrt{D})$ if $q \equiv 1 \pmod 3$
- Extra fields? $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{9D}) = \mathbb{F}_q(t, \sqrt{81D})$
- Hasse count is wrong
- There are three types of quadratic fields

Let $D(t) \in \mathbb{F}_q[t]$ be squarefree

Let $\operatorname{sgn}(D) \in \mathbb{F}_q^*$ denote the leading coefficient of $D(t)$.

Quadratic Function Fields

Let $D(t) \in \mathbb{F}_q[t]$ be squarefree

Let $\mathrm{sgn}(D) \in \mathbb{F}_q^*$ denote the leading coefficient of $D(t)$.

$\mathbb{F}_q(t, \sqrt{D})$ is

imaginary if $\deg(D)$ is odd

infinite place of $\mathbb{F}_q(t)$ ramifies

Let $D(t) \in \mathbb{F}_q[t]$ be squarefree

Let $\mathrm{sgn}(D) \in \mathbb{F}_q^*$ denote the leading coefficient of $D(t)$.

$\mathbb{F}_q(t, \sqrt{D})$ is

- imaginary if $\deg(D)$ is odd
  - infinite place of $\mathbb{F}_q(t)$ ramifies
- real if $\deg(D)$ is even and $\mathrm{sgn}(D)$ is a square in $\mathbb{F}_q$
  - infinite place of $\mathbb{F}_q(t)$ splits

Quadratic Function Fields

Let $D(t) \in \mathbb{F}_q[t]$ be squarefree

Let $\mathrm{sgn}(D) \in \mathbb{F}_q^*$ denote the leading coefficient of $D(t)$.

$\mathbb{F}_q(t, \sqrt{D})$ is

- imaginary if $\deg(D)$ is odd
  - infinite place of $\mathbb{F}_q(t)$ ramifies
- real if $\deg(D)$ is even and $\mathrm{sgn}(D)$ is a square in $\mathbb{F}_q$
  - infinite place of $\mathbb{F}_q(t)$ splits
- unusual if $\deg(D)$ is even and $\mathrm{sgn}(D)$ is a non-square in $\mathbb{F}_q$
  - infinite place of $\mathbb{F}_q(t)$ is inert – *no number field analogue!*

Decomposition at Infinity in $\mathbb{K}$

Let $\mathbb{K}$ be a cubic extension of $\mathbb{F}_q(t)$ of square-free discriminant $D \in \mathbb{F}_q[t]$

Decomposition at Infinity in $\mathbb{K}$

Let $\mathbb{K}$ be a cubic extension of $\mathbb{F}_q(t)$ of square-free discriminant $D \in \mathbb{F}_q[t]$

Let ∞ denote the place at infinity in $\mathbb{F}_q(t)$.

Decomposition at Infinity in $\mathbb{K}$

Let $\mathbb{K}$ be a cubic extension of $\mathbb{F}_q(t)$ of square-free discriminant $D \in \mathbb{F}_q[t]$

Let ∞ denote the place at infinity in $\mathbb{F}_q(t)$.

deg(D) odd: $\infty = \mathfrak{p}\mathfrak{q}^2$ in $\mathbb{K}$

Decomposition at Infinity in $\mathbb{K}$

Let $\mathbb{K}$ be a cubic extension of $\mathbb{F}_q(t)$ of square-free discriminant $D \in \mathbb{F}_q[t]$

Let ∞ denote the place at infinity in $\mathbb{F}_q(t)$.

deg(D) odd: $\infty = \mathfrak{p}\mathfrak{q}^2$ in $\mathbb{K}$

deg(D) even:

- $q \equiv 1 \pmod 3$:
  - $\mathrm{sgn}(D) = \square$: $\infty = \mathfrak{p}\mathfrak{q}\mathfrak{r}$ or $\mathfrak{p}^3$ or $\mathfrak{p}$ in $\mathbb{K}$
  - $\mathrm{sgn}(D) \neq \square$: $\infty = \mathfrak{p}\mathfrak{q}$ in $\mathbb{K}$
- $q \equiv -1 \pmod 3$:
  - $\mathrm{sgn}(D) = \square$: $\infty = \mathfrak{p}\mathfrak{q}\mathfrak{r}$ or $\mathfrak{p}$ in $\mathbb{K}$
  - $\mathrm{sgn}(D) \neq \square$: $\infty = \mathfrak{p}\mathfrak{q}$ or $\mathfrak{p}^3$ in $\mathbb{K}$

Let $\mathbb{K}$ be a cubic extension of $\mathbb{F}_q(t)$ of square-free discriminant $D \in \mathbb{F}_q[t]$

Let ∞ denote the place at infinity in $\mathbb{F}_q(t)$.

deg(D) odd: $\infty = \mathfrak{p}\mathfrak{q}^2$ in $\mathbb{K}$

deg(D) even:

$q \equiv 1 \pmod 3$:

sgn(D) $= \square$: $\infty = \mathfrak{p}\mathfrak{q}\mathfrak{r}$ or $\mathfrak{p}^3$ or $\mathfrak{p}$ in $\mathbb{K}$

sgn(D) $\neq \square$: $\infty = \mathfrak{p}\mathfrak{q}$ in $\mathbb{K}$

$q \equiv -1 \pmod 3$:

sgn(D) $= \square$: $\infty = \mathfrak{p}\mathfrak{q}\mathfrak{r}$ or $\mathfrak{p}$ in $\mathbb{K}$

sgn(D) $\neq \square$: $\infty = \mathfrak{p}\mathfrak{q}$ or $\mathfrak{p}^3$ in $\mathbb{K}$

Hasse count does not include the red cases.

The Berwick Map

As before, triples of conjugate cubic function fields are mapped onto pairs of 3-torsion ideal classes in $\mathbb{F}_q[t, \sqrt{D}]$.

The Berwick Map

As before, triples of conjugate cubic function fields are mapped onto pairs of 3-torsion ideal classes in $\mathbb{F}_q[t, \sqrt{D}]$.

For $\mathbb{F}_q(t, \sqrt{-3D})$ imaginary or unusual:

bijection onto non-principal ideal classes
nothing maps to the principal class

For $\mathbb{F}_q(t, \sqrt{-3D})$ real:

3-to-1 onto non-principal ideal classes
1-to-1 onto to the principal class

Some Counting

Put

$$r = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D})\big)$$
$$s = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D})\big)$$

Same field unless $\deg(D)$ even and $q \equiv -1 \pmod 3$

Some Counting

Put

$$r = \text{3-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$$
$$s = \text{3-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$$

Same field unless $\deg(D)$ even and $q \equiv -1 \pmod 3$

Number of cubic fields of discriminant D with at least two infinite places:

$$\frac{3^r - 1}{2}$$

Some Counting

Put

$$r = \text{3-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$$
$$s = \text{3-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$$

Same field unless $\deg(D)$ even and $q \equiv -1 \pmod 3$

Number of cubic fields of discriminant D with at least two infinite places:

$$\frac{3^r - 1}{2}$$

Number of cubic fields produced by the Berwick map:

For $\mathbb{F}_q(t, \sqrt{-3D})$ imaginary or unusual: $\dfrac{3^s - 1}{2}$

For $\mathbb{F}_q(t, \sqrt{-3D})$ real: $\dfrac{3^{s+1} - 1}{2}$

Some Counting

Put

$r = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{D}))\big)$

$s = 3\text{-rank}\big(\mathrm{Cl}(\mathbb{Q}(\sqrt{-3D}))\big)$

Same field unless $\deg(D)$ even and $q \equiv -1 \pmod 3$

Number of cubic fields of discriminant D with at least two infinite places:

$$\frac{3^r - 1}{2}$$

Number of cubic fields produced by the Berwick map:

For $\mathbb{F}_q(t, \sqrt{-3D})$ imaginary or unusual: $\dfrac{3^s - 1}{2}$

For $\mathbb{F}_q(t, \sqrt{-3D})$ real: $\dfrac{3^{s+1} - 1}{2}$

Connection between r and s (Lee 2007):

$|r - s| \leq 1$

If $r \neq s$, then the unusual quadratic field has the bigger 3-rank

More Counting

If $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{-3D})$ (imaginary or real), then $r = s$ ☺

More Counting

If $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{-3D})$ (imaginary or real), then $r = s$ ☺

Case $\mathbb{F}_q(t, \sqrt{-3D})$ unusual, $\mathbb{F}_q(t, \sqrt{D})$ real:

$$r = s: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

$$r = s - 1: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

More Counting

If $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{-3D})$ (imaginary or real), then $r = s$ ☺

Case $\mathbb{F}_q(t, \sqrt{-3D})$ unusual, $\mathbb{F}_q(t, \sqrt{D})$ real:

$$r = s: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

$$r = s - 1: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

Case $\mathbb{F}_q(t, \sqrt{-3D})$ real, $\mathbb{F}_q(t, \sqrt{D})$ unusual:

$$r = s: \qquad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

$$r = s + 1: \qquad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

If $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{-3D})$ (imaginary or real), then $r = s$ ☺

Case $\mathbb{F}_q(t, \sqrt{-3D})$ unusual, $\mathbb{F}_q(t, \sqrt{D})$ real:

$$r = s: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

$$r = s - 1: \qquad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

Case $\mathbb{F}_q(t, \sqrt{-3D})$ real, $\mathbb{F}_q(t, \sqrt{D})$ unusual:

$$r = s: \qquad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} + 3^r \qquad ☹$$

$$r = s + 1: \qquad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} \qquad ☺$$

So what are these extra 3^r cubic fields?

More Counting

If $\mathbb{F}_q(t, \sqrt{D}) = \mathbb{F}_q(t, \sqrt{-3D})$ (imaginary or real), then $r = s$ ☺

Case $\mathbb{F}_q(t, \sqrt{-3D})$ unusual, $\mathbb{F}_q(t, \sqrt{D})$ real:

$$r = s: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} \quad ☺$$

$$r = s - 1: \quad \frac{3^s - 1}{2} = \frac{3^r - 1}{2} + 3^r \quad ☹$$

Case $\mathbb{F}_q(t, \sqrt{-3D})$ real, $\mathbb{F}_q(t, \sqrt{D})$ unusual:

$$r = s: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} + 3^r \quad ☹$$

$$r = s + 1: \quad \frac{3^{s+1} - 1}{2} = \frac{3^r - 1}{2} \quad ☺$$

So what are these extra 3^r cubic fields?

Answer: they are the fields with one infinite place that are missing from the Hasse count. In the ☺ cases, there are no such fields.

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \dfrac{\deg(D) - 1}{2} \right\rfloor$

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

An ideal $\mathfrak{a}$ in $\mathbb{F}_q(t, \sqrt{-3D})$ is **reduced** if $\deg(N(\mathfrak{a})) \leq g$

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \dfrac{\deg(D) - 1}{2} \right\rfloor$

An ideal $\mathfrak{a}$ in $\mathbb{F}_q(t, \sqrt{-3D})$ is **reduced** if $\deg(N(\mathfrak{a})) \leq g$

Equivalent: $|N(\mathfrak{a})| < \sqrt{|D|}$ where $|\cdot| = q^{\deg(\cdot)}$

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \dfrac{\deg(D) - 1}{2} \right\rfloor$

An ideal $\mathfrak{a}$ in $\mathbb{F}_q(t, \sqrt{-3D})$ is **reduced** if $\deg(N(\mathfrak{a})) \leq g$

Equivalent: $|N(\mathfrak{a})| < \sqrt{|D|}$ where $|\cdot| = q^{\deg(\cdot)}$

Every ideal class of $\mathbb{F}_q[t, \sqrt{-3D}]$ contains

- a unique reduced ideal when $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \dfrac{\deg(D) - 1}{2} \right\rfloor$

An ideal $\mathfrak{a}$ in $\mathbb{F}_q(t, \sqrt{-3D})$ is **reduced** if $\deg(N(\mathfrak{a})) \leq g$

Equivalent: $|N(\mathfrak{a})| < \sqrt{|D|}$ where $|\cdot| = q^{\deg(\cdot)}$

Every ideal class of $\mathbb{F}_q[t, \sqrt{-3D}]$ contains

- a unique reduced ideal when $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary
- either a unique reduced ideal or $q + 1$ "almost" reduced ideals (degree $g + 1$) when $\mathbb{F}_q(t, \sqrt{-3D})$ is unusual (Artin 1924)

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \frac{\deg(D) - 1}{2} \right\rfloor$

An ideal $\mathfrak{a}$ in $\mathbb{F}_q(t, \sqrt{-3D})$ is **reduced** if $\deg(N(\mathfrak{a})) \leq g$

Equivalent: $|N(\mathfrak{a})| < \sqrt{|D|}$ where $|\cdot| = q^{\deg(\cdot)}$

Every ideal class of $\mathbb{F}_q[t, \sqrt{-3D}]$ contains

- a unique reduced ideal when $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary
- either a unique reduced ideal or $q + 1$ "almost" reduced ideals (degree $g + 1$) when $\mathbb{F}_q(t, \sqrt{-3D})$ is unusual (Artin 1924)
- many reduced ideals when $\mathbb{F}_q(t, \sqrt{-3D})$ is real.

Reduced Ideals

The **genus** of $\mathbb{F}_q(t, \sqrt{-3D})$ is $\left\lfloor \dfrac{\deg(D) - 1}{2} \right\rfloor$

An ideal $\mathfrak{a}$ in $\mathbb{F}_q(t, \sqrt{-3D})$ is **reduced** if $\deg(N(\mathfrak{a})) \le g$

Equivalent: $|N(\mathfrak{a})| < \sqrt{|D|}$ where $|\cdot| = q^{\deg(\cdot)}$

Every ideal class of $\mathbb{F}_q[t, \sqrt{-3D}]$ contains

- a unique reduced ideal when $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary
- either a unique reduced ideal or $q + 1$ "almost" reduced ideals (degree $g + 1$) when $\mathbb{F}_q(t, \sqrt{-3D})$ is unusual (Artin 1924)
- many reduced ideals when $\mathbb{F}_q(t, \sqrt{-3D})$ is real.

(Almost) reduced ideals produce λ with small norm: $|N(\lambda)| \le |D|^{3/2}$

Generators λ of Small Trace

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary or unusual

Generators λ of Small Trace

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary or unusual

Write $\lambda = A + B\sqrt{-3D}$ $(A, B \in \mathbb{F}_q[t])$. Then

$$N(\lambda) = A^2 + 3B^2 D$$

Generators λ of Small Trace

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary or unusual

Write $\lambda = A + B\sqrt{-3D}$ $(A, B \in \mathbb{F}_q[t])$. Then

$$N(\lambda) = A^2 + 3B^2 D$$

If $\deg(D)$ is odd, or $\deg(D)$ is even and $\operatorname{sgn}(-3D) \neq \square$, then there is no cancellation of leading coefficients on the right hand side.

Generators λ of Small Trace

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary or unusual

Write $\lambda = A + B\sqrt{-3D}$ $(A, B \in \mathbb{F}_q[t])$. Then

$$N(\lambda) = A^2 + 3B^2 D$$

If $\deg(D)$ is odd, or $\deg(D)$ is even and $\operatorname{sgn}(-3D) \neq \square$, then there is no cancellation of leading coefficients on the right hand side.

$|N(\lambda)| \leq |D|^{3/2}$ implies

$$|\mathrm{Tr}(\lambda)| \;=\; |A| \;\leq |N(\lambda)|^{1/2} \leq |D|^{3/4}$$

Generators λ of Small Trace

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is imaginary or unusual

Write $\lambda = A + B\sqrt{-3D}$ $(A, B \in \mathbb{F}_q[t])$. Then

$$N(\lambda) = A^2 + 3B^2 D$$

If $\deg(D)$ is odd, or $\deg(D)$ is even and $\mathrm{sgn}(-3D) \neq \square$, then there is no cancellation of leading coefficients on the right hand side.

$|N(\lambda)| \leq |D|^{3/2}$ implies

$$|\mathrm{Tr}(\lambda)| \ = \ |A| \ \leq |N(\lambda)|^{1/2} \leq |D|^{3/4}$$

Yields again a small trace.

Generators λ of Small Trace (Cont'd)

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is real

Generators λ of Small Trace (Cont'd)

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is real

- Same infrastructure framework (Stein 1992)
- Can also use arithmetic in the divisor class group of $\mathbb{F}_q(t, \sqrt{-3D})$ via balanced divisors (Galbraith, Harrison, Mireles Morales 2008)

Generators λ of Small Trace (Cont'd)

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is real

- Same infrastructure framework (Stein 1992)
- Can also use arithmetic in the divisor class group of $\mathbb{F}_q(t, \sqrt{-3D})$ via balanced divisors (Galbraith, Harrison, Mireles Morales 2008)

λ **small**: $\deg(Tr(\lambda)) \leq 3g + 1$, $\deg(N(\lambda)) \leq 3g$

Generators λ of Small Trace (Cont'd)

Suppose $\mathbb{F}_q(t, \sqrt{-3D})$ is real

- Same infrastructure framework (Stein 1992)
- Can also use arithmetic in the divisor class group of $\mathbb{F}_q(t, \sqrt{-3D})$ via balanced divisors (Galbraith, Harrison, Mireles Morales 2008)

λ **small**: $\deg(Tr(\lambda)) \leq 3g+1$, $\deg(N(\lambda)) \leq 3g$

- Principal class: take reduced ideal closest to $\lceil R/3 + g/2 \rfloor$
- Non-principal classes: take ideals closest to d, $R/3 + d$, $2R/3 + d$ where $-g/2 \leq d < R/3 - g/2$ and d can be explicitly computed **using integer arithmetic only!**

Example — Different 3-Rank

$q = 11, \quad D(x) = 7x^{10} + x^7 + 3x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 2x$

Example — Different 3-Rank

$q = 11, \quad D(x) = 7x^{10} + x^7 + 3x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 2x$

$r = 3, \ \ s = 2 \ \Rightarrow \ (3^3 - 1)/2 = 13$ fields, all with $\infty = \mathfrak{pq}$ in $\mathbb{K}$.

Example — Different 3-Rank

$q = 11, \quad D(x) = 7x^{10} + x^7 + 3x^6 + 2x^5 + 7x^4 + 8x^3 + 4x^2 + 2x$

$r = 3, \ \ s = 2 \ \Rightarrow \ (3^3 - 1)/2 = 13$ fields, all with $\infty = \mathfrak{pq}$ in $\mathbb{K}$.

$f(x) = x^3 - S(t)x + T(t)$ with

#	$S(t)$	$T(t)$
1	$5t^3 + 10t + 4$	$4t^6 + t^5 + t^3 + 9t^2 + 6t + 4$
2	$10t^4 + 9t^3 + t^2 + 5t + 9$	$10t^6 + 8t^5 + 5t^3 + 5t^2 + 5t + 3$
3	$6t^4 + 4t^3 + 10t + 4$	$5t^6 + 4t^5 + 3t^4 + 5t^3 + 3t^2 + t + 7$
4	$9t^4 + 4t^3 + 6t^2 + 5t + 1$	$t^6 + 4t^5 + 8t^4 + 9t^3 + 4t^2 + 7t + 5$
5	$4t^4 + 7t^3 + 10t^2 + 5t + 4$	$6t^6 + 6t^5 + 4t^4 + 4t^3 + 8t^2 + 10t + 4$
6	$9t^3 + 4t^2 + 8t + 9$	$t^6 + 3t^5 + 3t^3 + 6t + 3$
7	$t^4 + 3t^3 + 9t + 3$	$t^6 + 2t^5 + 2t^4 + 3t^3 + 6t^2 + 3t + 2$
8	$t^4 + 8t^3 + 6t^2 + 3t + 1$	$t^6 + 9t^5 + 7t^4 + 4t^3 + 6t^2 + 3t + 6$
9	$7t^4 + 4t^3 + 9t^2 + 6t$	$9t^6 + 10t^5 + 10t^4 + 9t^3 + 6t^2$
10	$6t^4 + 4t^3 + 5t^2 + 9t + 4$	$5t^6 + 10t^4 + 2t^3 + 5t^2 + 8t + 7$
11	$3t^4 + 5t^3 + 4t^2 + 6t + 9$	$8t^6 + 10t^5 + 4t^4 + 4t^3 + 8t^2 + 2t + 3$
12	$5t^4 + 6t^2 + 8t + 9$	$2t^6 + 10t^5 + 3t^4 + t^3 + t^2 + 10t + 3$
13	$4t^4 + 3t^3 + 5t^2 + 10t + 9$	$8t^6 + 5t^4 + 3t^3 + 9t^2 + t + 3$

Example — Same 3-Rank

$q = 11, \quad D(x) = 2x^8 + x^6 + 5x^4 + 6x^2 + 7$

Example — Same 3-Rank

$q = 11, \quad D(x) = 2x^8 + x^6 + 5x^4 + 6x^2 + 7$

$$r = s = 2 \Rightarrow \begin{cases} (3^2 - 1)/2 = 4 & \text{fields with } \infty = \mathfrak{p}\mathfrak{q} \text{ in } \mathbb{K} \\ 3^2 = 9 & \text{fields with } \infty = \mathfrak{p}^3 \text{ in } \mathbb{K} \end{cases}$$

Example — Same 3-Rank

$q = 11, \quad D(x) = 2x^8 + x^6 + 5x^4 + 6x^2 + 7$

$$r = s = 2 \Rightarrow \begin{cases} (3^2-1)/2 = 4 & \text{fields with } \infty = \mathfrak{p}\mathfrak{q} \text{ in } \mathbb{K} \\ 3^2 = 9 & \text{fields with } \infty = \mathfrak{p}^3 \text{ in } \mathbb{K} \end{cases}$$

$f(x) = x^3 - S(t)x + T(t)$ with

#	$S(t)$	$T(t)$
1	$9t^2+6$	$t^6 + 7^t4 + 6t^2$
2	$7t^3+7t+8$	$6t^6+7t^5+8t^4+5t^3+4t^2+4$
3	$9t^3+3t^2+8t+1$	$2t^6+6t^5+6t^4+t^3+5t+5$
4	$9t^3+2t^2+8t+4$	$4t^6+6t^5+4t^3+3t^2+t+5$
5	$4t^3+4t^2+6t+2$	$10t^5+4t^4+8t^3+10t$
6	$5t^2+8t+5$	$2t^5+6t^3+2t+10$
7	$10t^3+5t^2+5t+1$	$8t^5+6t^4+6t^3+9t^2+t+6$
8	$5t^2+3t+5$	$9t^5+5t^3+9t+10$
9	t^3+5t^2+6t+1	$8t^5+5t^4+6t^3+2t^2+t+5$
10	$7t^3+4t^2+5t+2$	$10t^5+7t^4+8t^3+10t$
11	$5t^2+1$	$10t^4+2t^2+1$
12	$3t^2+4$	$10t^4+6t^2+6$
13	$3t^2$	$10t^4+6t^2+3$

BIG Example — Same 3-Rank

$q = 125, \quad D = 2x^{12} + 3x^9 + x^3 + 1$

BIG Example — Same 3-Rank

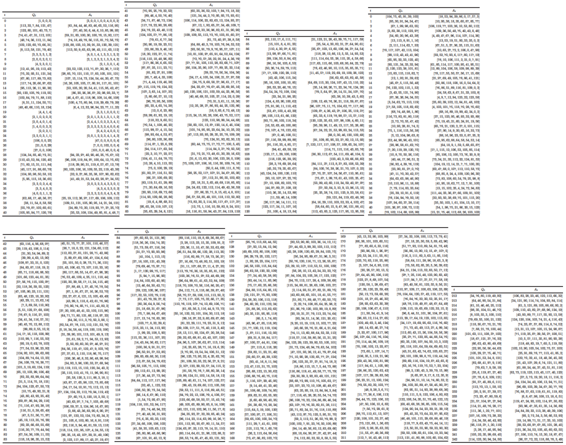
$q = 125, \quad D = 2x^{12} + 3x^9 + x^3 + 1$

$$r = s = 5 \;\Rightarrow \begin{cases} (3^5 - 1)/2 = 121 & \text{fields with } \infty = \mathfrak{p}\mathfrak{q} \text{ in } \mathbb{K} \\ 3^5 = 243 & \text{fields with } \infty = \mathfrak{p}^3 \text{ in } \mathbb{K} \end{cases}$$

BIG Example — Same 3-Rank

$q = 125, \quad D = 2x^{12} + 3x^9 + x^3 + 1$

$$r = s = 5 \;\Rightarrow \begin{cases} (3^5 - 1)/2 = 121 & \text{fields with } \infty = \mathfrak{p}\mathfrak{q} \text{ in } \mathbb{K} \\ 3^5 = 243 & \text{fields with } \infty = \mathfrak{p}^3 \text{ in } \mathbb{K} \end{cases}$$



364 fields

Concluding Remarks

- CUFFQI's run time dominated is dominated by 3-torsion and regulator computation

Concluding Remarks

- CUFFQI's run time dominated is dominated by 3-torsion and regulator computation

- CUFFQI can be extended to non-fundamental discriminants via basic cass field theory and Kummer theory
  - Number Fields: Cohen, *Advanced Topics in Computational Number Theory*, Ch. 5
  - Function Fields: Weir, S & Howe, ANTS-X, 2012 (Dihedral degree p extensions)

Concluding Remarks

- CUFFQI's run time dominated is dominated by 3-torsion and regulator computation
- CUFFQI can be extended to non-fundamental discriminants via basic cass field theory and Kummer theory
  - Number Fields: Cohen, *Advanced Topics in Computational Number Theory*, Ch. 5
  - Function Fields: Weir, S & Howe, ANTS-X, 2012 (Dihedral degree p extensions)
- Ideas can be extended to higher degree fields with quadratic resolvent fields

Thank You — Questions?