Sampling Cubic Rings

Fabian Gundlach

Paderborn University

2025-07-07

The LMFDB has a list of all . . .

- cubic number fields with $0 < \text{disc} < 3{,}375{,}000$
  (Belabas, Olivier)
- elliptic curves over $\mathbb{Q}$ with cond $\leq 500{,}000$
  (Cremona)
- zeros of $\zeta(s)$ with $0 < |\Im| \leq 30{,}610{,}046{,}000$
  (Platt)
- newforms with $\text{weight}^2 \cdot \text{level} \leq 4{,}000$
  (Best, Bober, Booker, Costa, Cremona, Derickx, Lowry-Duda, Lee, Roe, Sutherland, Voight)
- . . .

What if we want a (uniformly) random ...

- cubic number field with $0 < \text{disc} \leq 1{,}000{,}000{,}000{,}000{,}000{,}000$
- elliptic curve over $\mathbb{Q}$ with cond $\leq \ldots$
- zero of $\zeta(s)$ with $0 < |\Im| \leq \ldots$
- newform with weight$^2 \cdot$ level $\leq \ldots$
- ...

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 1 (Rejection sampling)

Ⓗ Ⓗ $\longrightarrow$ $\boxed{1}$

Ⓗ Ⓣ $\longrightarrow$ $\boxed{2}$

Ⓣ Ⓗ $\longrightarrow$ $\boxed{3}$

Ⓣ Ⓣ $\longrightarrow$ start over

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 1 (Rejection sampling)

Ⓗ Ⓗ $\longrightarrow$ $\boxed{1}$

Ⓗ Ⓣ $\longrightarrow$ $\boxed{2}$

Ⓣ Ⓗ $\longrightarrow$ $\boxed{3}$

Ⓣ Ⓣ $\longrightarrow$ start over

Average number of coin flips:
$O\left(1 + \frac{1}{4} + \frac{1}{4^2} + \cdots\right) = O(1)$.

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 1 (Rejection sampling)

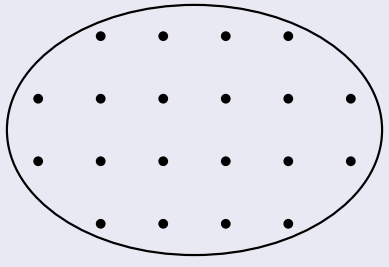
(H) (H) $\longrightarrow$ $\boxed{1}$

(H) (T) $\longrightarrow$ $\boxed{2}$

(T) (H) $\longrightarrow$ $\boxed{3}$

(T) (T) $\longrightarrow$ start over

Average number of coin flips:
$O\left(1 + \frac{1}{4} + \frac{1}{4^2} + \cdots\right) = O(1)$.



Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 1 (Rejection sampling)

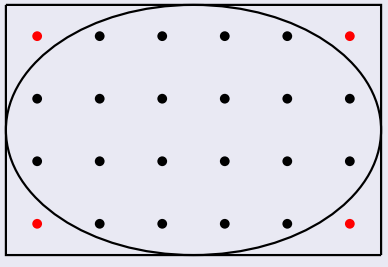
Ⓗ Ⓗ $\longrightarrow$ $\boxed{1}$

Ⓗ Ⓣ $\longrightarrow$ $\boxed{2}$

Ⓣ Ⓗ $\longrightarrow$ $\boxed{3}$

Ⓣ Ⓣ $\longrightarrow$ start over

Average number of coin flips:
$O\left(1 + \frac{1}{4} + \frac{1}{4^2} + \cdots\right) = O(1)$.



Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$x \in [0, \tfrac{1}{3}) \longrightarrow \boxed{1}$$
$$x \in [\tfrac{1}{3}, \tfrac{2}{3}) \longrightarrow \boxed{2}$$
$$x \in [\tfrac{2}{3}, 1) \longrightarrow \boxed{3}$$

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$x \in [0, \tfrac{1}{3}) \longrightarrow \boxed{1}$$
$$x \in [\tfrac{1}{3}, \tfrac{2}{3}) \longrightarrow \boxed{2}$$
$$x \in [\tfrac{2}{3}, 1) \longrightarrow \boxed{3}$$

Pick binary digits of x until you know which interval x lies in.

$$x = 0.???????\ldots_2$$

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$\begin{aligned} x \in [0, \tfrac{1}{3}) &\longrightarrow \boxed{1} \\ x \in [\tfrac{1}{3}, \tfrac{2}{3}) &\longrightarrow \boxed{2} \\ x \in [\tfrac{2}{3}, 1) &\longrightarrow \boxed{3} \end{aligned}$$

Pick binary digits of x until you know which interval x lies in.

$$x = 0.0?????? \ldots_2$$

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$\begin{aligned} x \in [0, \tfrac{1}{3}) &\longrightarrow \boxed{1} \\ x \in [\tfrac{1}{3}, \tfrac{2}{3}) &\longrightarrow \boxed{2} \\ x \in [\tfrac{2}{3}, 1) &\longrightarrow \boxed{3} \end{aligned}$$

Pick binary digits of x until you know which interval x lies in.

$$x = 0.01?????\ldots_2$$

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$\begin{aligned} x \in [0, \tfrac{1}{3}) &\longrightarrow \boxed{1} \\ x \in [\tfrac{1}{3}, \tfrac{2}{3}) &\longrightarrow \boxed{2} \\ x \in [\tfrac{2}{3}, 1) &\longrightarrow \boxed{3} \end{aligned}$$

Pick binary digits of x until you know which interval x lies in.

$$x = 0.010???\ldots_2$$

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$\begin{aligned} x \in [0, \tfrac{1}{3}) &\longrightarrow \boxed{1} \\ x \in [\tfrac{1}{3}, \tfrac{2}{3}) &\longrightarrow \boxed{2} \\ x \in [\tfrac{2}{3}, 1) &\longrightarrow \boxed{3} \end{aligned}$$

Pick binary digits of x until you know which interval x lies in.

$$x = 0.0100??? \ldots_2$$

Warmup

How to pick an element of $\{1, 2, 3\}$ (uniformly) at random using coin flips?

Method 2

Pick a real number $x \in [0, 1)$ uniformly at random.

$$\begin{aligned} x \in [0, \tfrac{1}{3}) &\longrightarrow \boxed{1} \\ x \in [\tfrac{1}{3}, \tfrac{2}{3}) &\longrightarrow \boxed{2} \\ x \in [\tfrac{2}{3}, 1) &\longrightarrow \boxed{3} \end{aligned}$$

Pick binary digits of x until you know which interval x lies in.

$$x = 0.0100??? \ldots_2$$

Expected running time: $O(1)$

Goal

Theorem (–)

There is an algorithm which computes a random cubic integral domain S with $0 < \mathrm{disc}(S) \leq T$ in expected time $\tilde{O}(\log T)$. Any such ring S is returned with probability proportional to $1/|\mathrm{Aut}(S)|$.

Goal

Theorem (–)

There is an algorithm which computes a random cubic integral domain S with $0 < \mathrm{disc}(S) \leq T$ in expected time $\tilde{O}(\log T)$. Any such ring S is returned with probability proportional to $1/|\mathrm{Aut}(S)|$.

Parameterization (Levi)

GL_2 acts on $V = \{f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3\}$.

$$\begin{array}{ccc} \{\text{cubic ring } S\} & \longleftrightarrow & \mathrm{GL}_2(\mathbb{Z})\backslash\{f \in V(\mathbb{Z})\} \\ \mathrm{disc}(S) & = & \mathrm{disc}(f) \\ \mathrm{Aut}(S) & \simeq & \mathrm{Stab}(f) \\ \text{integral domain} & \Leftrightarrow & \text{irreducible (over } \mathbb{Z}) \end{array}$$

Goal

Theorem (–)

There is an algorithm which computes a random cubic integral domain S with $0 < \mathrm{disc}(S) \leq T$ in expected time $\tilde{O}(\log T)$. Any such ring S is returned with probability proportional to $1/|\mathrm{Aut}(S)|$.

Parameterization (Levi)

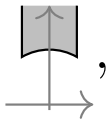
GL_2 acts on $V = \{f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3\}$.

$$\begin{array}{ccc} \{\text{cubic ring } S\} & \longleftrightarrow & \mathrm{GL}_2(\mathbb{Z})\backslash\{f \in V(\mathbb{Z})\} \\ \mathrm{disc}(S) & = & \mathrm{disc}(f) \\ \mathrm{Aut}(S) & \simeq & \mathrm{Stab}(f) \\ \text{integral domain} & \Leftrightarrow & \text{irreducible (over } \mathbb{Z}) \end{array}$$

Want to produce . . .

a random orbit $\mathrm{GL}_2(\mathbb{Z})f$ in $V(\mathbb{Z})$ with $0 < \mathrm{disc}(f) \leq T$ and f irreducible, with probability proportional to $1/|\mathrm{Stab}(f)|$

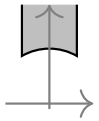
Bhargava's trick

$$\mathcal{F} := \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1/s & 0 \\ 0 & s \end{pmatrix} k \;\middle|\; (n, s^2) \in \text{  }, \; k \in O_2(\mathbb{R}) \right\}$$

fund. dom. for $\mathrm{GL}_2(\mathbb{Z})$ left acting on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$

$\mathrm{d}g :=$ Haar measure on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$ with $\int_{\mathcal{F}} \mathrm{d}g = 1$

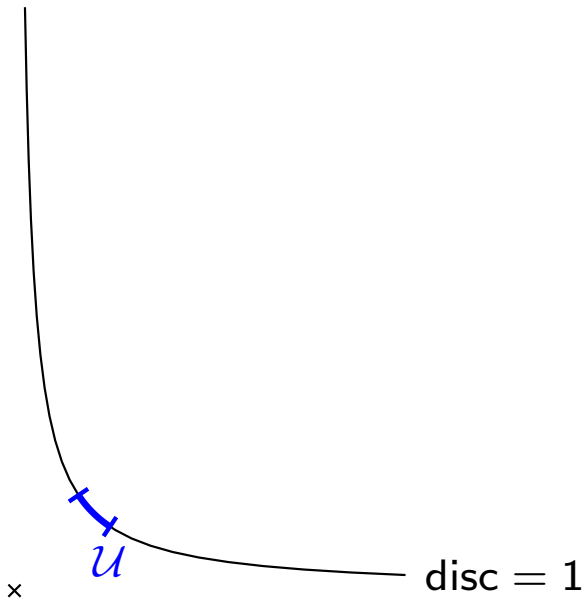
Bhargava's trick

$$\mathcal{F} := \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1/s & 0 \\ 0 & s \end{pmatrix} k \;\middle|\; (n, s^2) \in \text{  }, \; k \in O_2(\mathbb{R}) \right\}$$

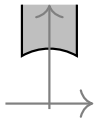
fund. dom. for $\mathrm{GL}_2(\mathbb{Z})$ left acting on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$

$\mathrm{d}g :=$ Haar measure on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$ with $\int_{\mathcal{F}} \mathrm{d}g = 1$

$$\mathcal{U} := \{f \in V(\mathbb{R}) \mid \mathrm{disc} = 1\} \cap (\text{some open ball}) \neq \emptyset$$



Bhargava's trick

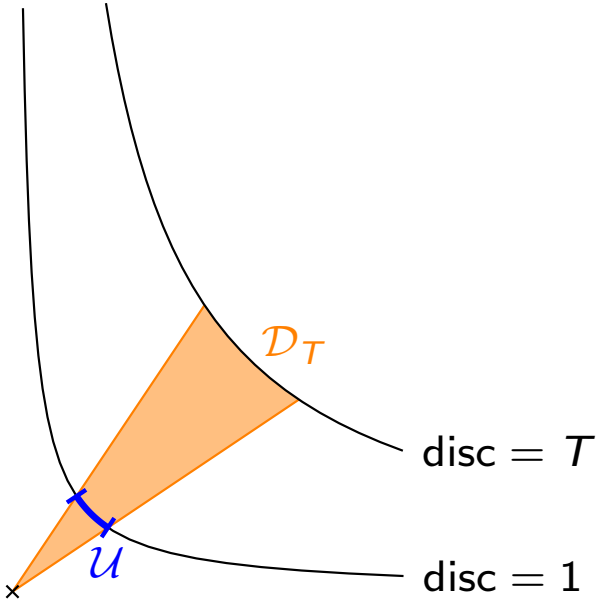
$$\mathcal{F} := \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1/s & 0 \\ 0 & s \end{pmatrix} k \;\middle|\; (n, s^2) \in \text{  }, \; k \in O_2(\mathbb{R}) \right\}$$

fund. dom. for $\mathrm{GL}_2(\mathbb{Z})$ left acting on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$

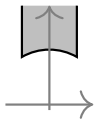
$\mathrm{d}g :=$ Haar measure on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$ with $\int_{\mathcal{F}} \mathrm{d}g = 1$

$$\mathcal{U} := \{f \in V(\mathbb{R}) \mid \mathrm{disc} = 1\} \cap (\text{some open ball}) \neq \emptyset$$

$$\mathcal{D}_T := (0, T^{1/4}] \cdot \mathcal{U}$$



Bhargava's trick

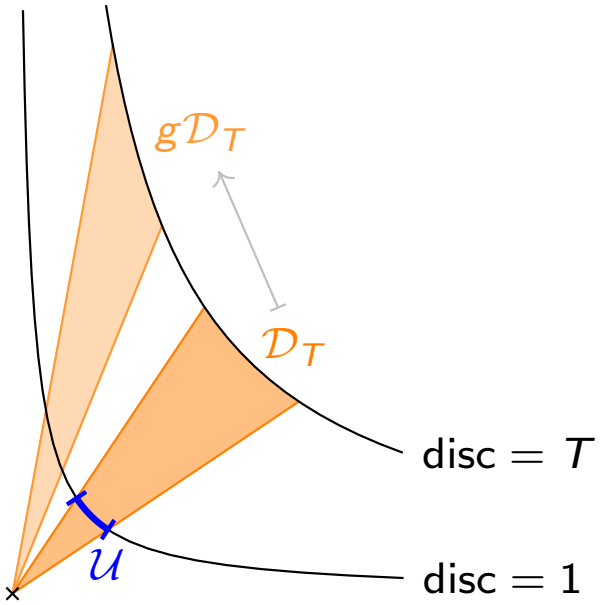
$$\mathcal{F} := \left\{ \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1/s & 0 \\ 0 & s \end{pmatrix} k \;\middle|\; (n, s^2) \in \text{  }, \; k \in O_2(\mathbb{R}) \right\}$$

fund. dom. for $\mathrm{GL}_2(\mathbb{Z})$ left acting on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$

$\mathrm{d}g :=$ Haar measure on $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) = \pm 1\}$ with $\int_{\mathcal{F}} \mathrm{d}g = 1$

$$\mathcal{U} := \{f \in V(\mathbb{R}) \mid \mathrm{disc} = 1\} \cap (\text{some open ball}) \neq \emptyset$$

$$\mathcal{D}_T := (0, T^{1/4}] \cdot \mathcal{U}$$



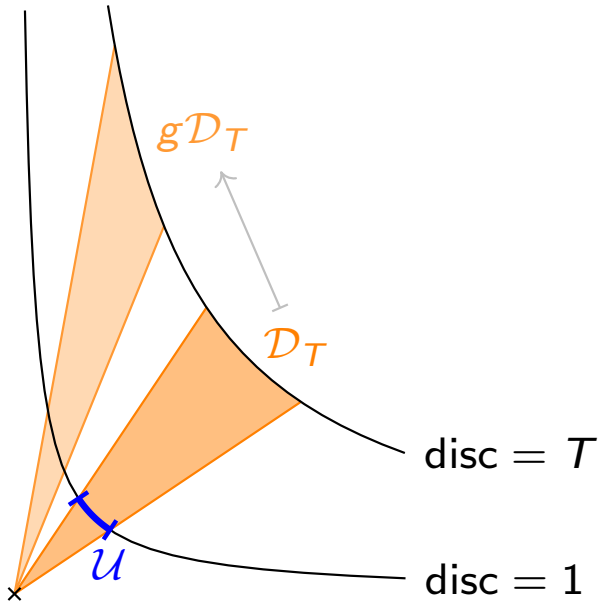
Bhargava's Lemma

There is a constant $C > 0$ such that for any orbit $\mathrm{GL}_2(\mathbb{Z})f$ in $V(\mathbb{Z})$,

$$\int_{\mathcal{F}} \#\Big(g\mathcal{D}_T \cap \big(\mathrm{GL}_2(\mathbb{Z})f\big)\Big)\mathrm{d}g$$

$$= \begin{cases} \frac{C}{|\mathrm{Stab}(f)|} & \text{if } 0 < \mathrm{disc}(f) \leq T, \\ 0 & \text{otherwise.} \end{cases}$$

Idea of the Algorithm



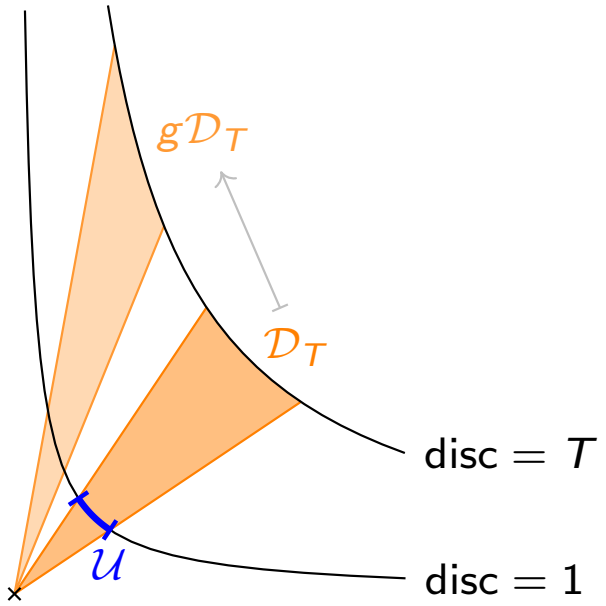
Bhargava's Lemma

There is a constant $C > 0$ such that for any orbit $\mathrm{GL}_2(\mathbb{Z})f$ in $V(\mathbb{Z})$,

$$\int_{\mathcal{F}} \#\Big(g\mathcal{D}_T \cap \big(\mathrm{GL}_2(\mathbb{Z})f\big)\Big)\mathrm{d}g$$
$$= \begin{cases} \frac{C}{|\mathrm{Stab}(f)|} & \text{if } 0 < \mathrm{disc}(f) \leq T, \\ 0 & \text{otherwise.} \end{cases}$$

To produce a random orbit $\mathrm{GL}_2(\mathbb{Z})f$ with $0 < \mathrm{disc}(f) \leq T$ and f irreducible:

Idea of the Algorithm



Bhargava's Lemma

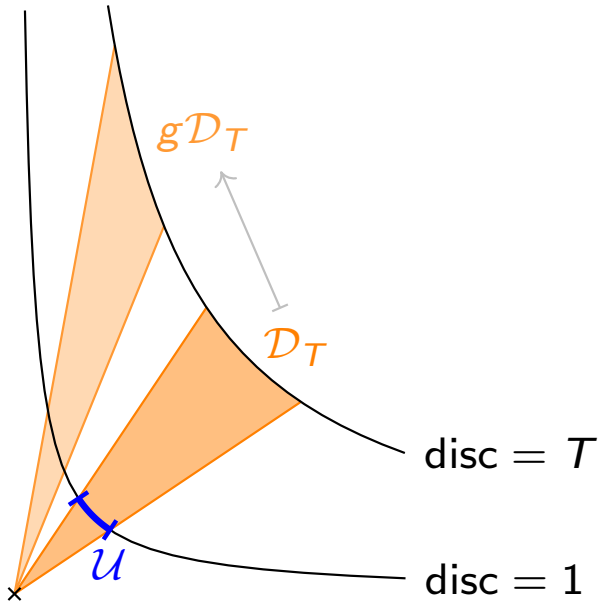
There is a constant $C > 0$ such that for any orbit $\mathrm{GL}_2(\mathbb{Z})f$ in $V(\mathbb{Z})$,

$$\int_{\mathcal{F}} \#\Big(g\mathcal{D}_T \cap \big(\mathrm{GL}_2(\mathbb{Z})f\big)\Big)\mathrm{d}g$$
$$= \begin{cases} \frac{C}{|\mathrm{Stab}(f)|} & \text{if } 0 < \mathrm{disc}(f) \leq T, \\ 0 & \text{otherwise.} \end{cases}$$

To produce a random orbit $\mathrm{GL}_2(\mathbb{Z})f$ with $0 < \mathrm{disc}(f) \leq T$ and f irreducible:

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

Idea of the Algorithm



Bhargava's Lemma

There is a constant $C > 0$ such that for any orbit $\mathrm{GL}_2(\mathbb{Z})f$ in $V(\mathbb{Z})$,

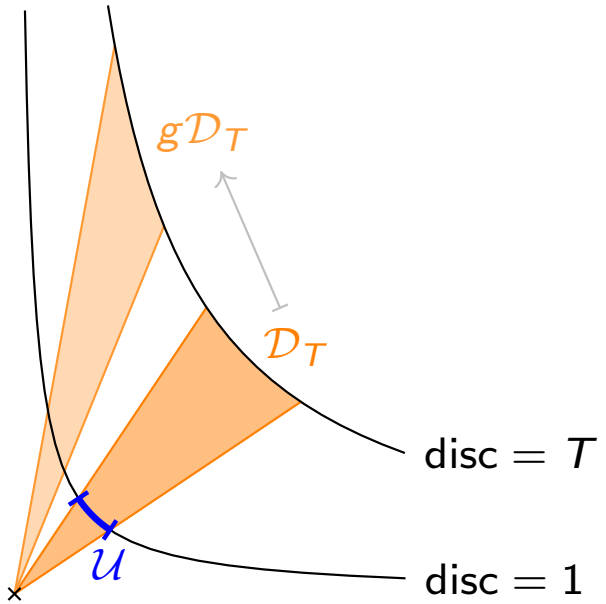
$$\int_{\mathcal{F}} \#\Big(g\mathcal{D}_T \cap \big(\mathrm{GL}_2(\mathbb{Z})f\big)\Big)\,\mathrm{d}g$$
$$= \begin{cases} \frac{C}{|\mathrm{Stab}(f)|} & \text{if } 0 < \mathrm{disc}(f) \le T, \\ 0 & \text{otherwise.} \end{cases}$$

To produce a random orbit $\mathrm{GL}_2(\mathbb{Z})f$ with $0 < \mathrm{disc}(f) \le T$ and f irreducible:

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1).

Idea of the Algorithm



Bhargava's Lemma

There is a constant $C > 0$ such that for any orbit $\mathrm{GL}_2(\mathbb{Z})f$ in $V(\mathbb{Z})$,

$$\int_{\mathcal{F}} \#\Big(g\mathcal{D}_T \cap \big(\mathrm{GL}_2(\mathbb{Z})f\big)\Big)\,\mathrm{d}g = \begin{cases} \frac{C}{|\mathrm{Stab}(f)|} & \text{if } 0 < \mathrm{disc}(f) \le T, \\ 0 & \text{otherwise.} \end{cases}$$

To produce a random orbit $\mathrm{GL}_2(\mathbb{Z})f$ with $0 < \mathrm{disc}(f) \le T$ and f irreducible:

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

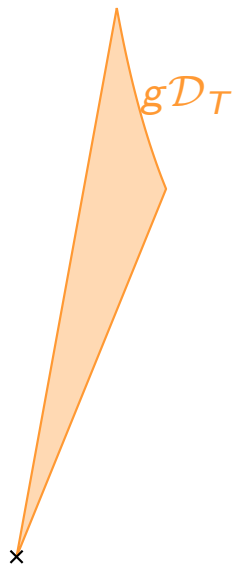
(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

$\Rightarrow$ Any particular orbit $\mathrm{GL}_2(\mathbb{Z})f$ will be returned with probability $\frac{C}{|\mathrm{Stab}(f)|} \cdot p_T$.

Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

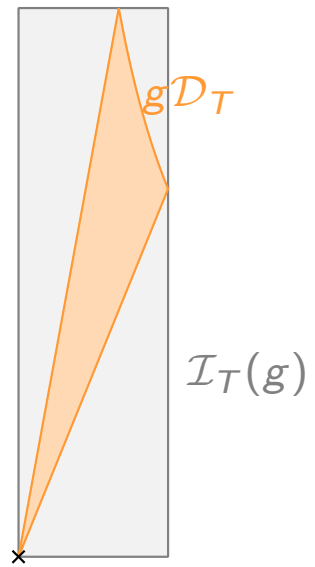


Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.



Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

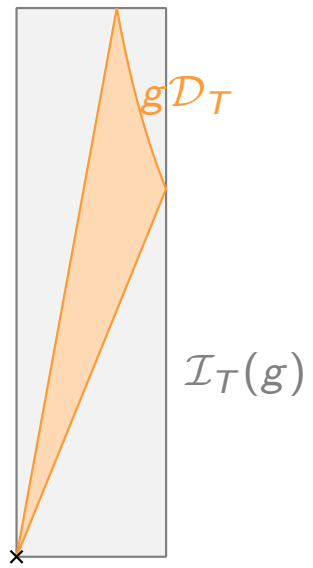
(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.

If every $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$ **has** X^3**-coefficient** $a = 0$**:**

$\Rightarrow$ There is no irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$.

$\rightarrow$ Start over with (1).



Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.

If every $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$ **has** X^3**-coefficient** $a = 0$**:**

$\Rightarrow$ There is no irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$.

$\rightarrow$ Start over with (1).

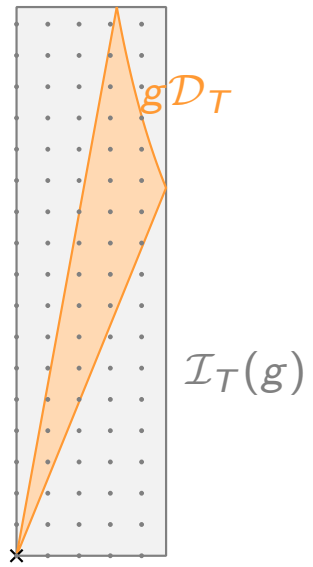
Otherwise:

$\rightarrow$

Pick a uniformly random $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$.

If $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ and f is irreducible, return $\mathrm{GL}_2(\mathbb{Z})f$.

Otherwise, start over with (1).



Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.

If every $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$ **has** X^3**-coefficient** $a = 0$**:**

$\Rightarrow$ There is no irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$.

$\rightarrow$ Start over with (1).

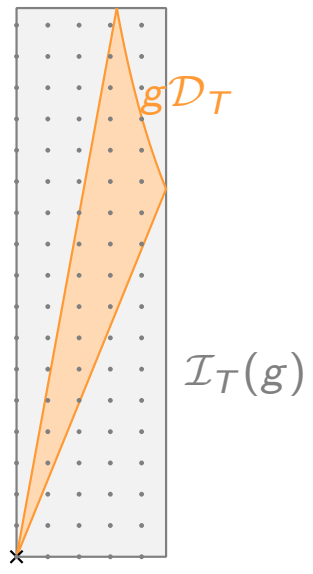
Otherwise:

$\rightarrow$ With probability $\frac{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}{E_T}$:

Pick a uniformly random $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$.

If $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ and f is irreducible, return $\mathrm{GL}_2(\mathbb{Z})f$.

Otherwise, start over with (1).



Any irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ is returned with probability

$$\frac{1}{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}$$

Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.

If every $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$ **has** X^3**-coefficient** $a = 0$**:**

$\Rightarrow$ There is no irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$.

$\rightarrow$ Start over with (1).

Otherwise:

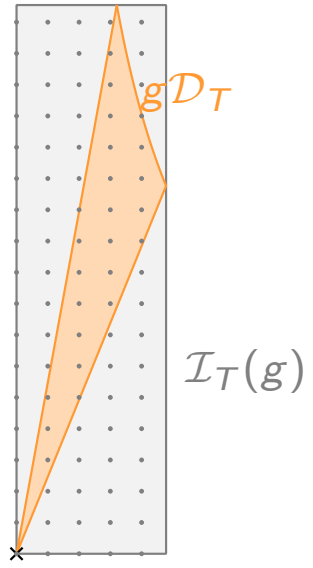
$\Rightarrow \#(\mathcal{I}_T(g) \cap V(\mathbb{Z})) \leq E_T$ for some constant E_T

$\rightarrow$ With probability $\frac{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}{E_T}$:

Pick a uniformly random $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$.

If $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ and f is irreducible, return $\mathrm{GL}_2(\mathbb{Z})f$.

Otherwise, start over with (1).



Any irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ is returned with probability

$$p_T = \frac{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}{E_T} \cdot \frac{1}{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))} = \frac{1}{E_T}.$$

Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.

If every $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$ **has** X^3**-coefficient** $a = 0$**:**

$\Rightarrow$ There is no irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$.

$\rightarrow$ Start over with (1).

Otherwise:

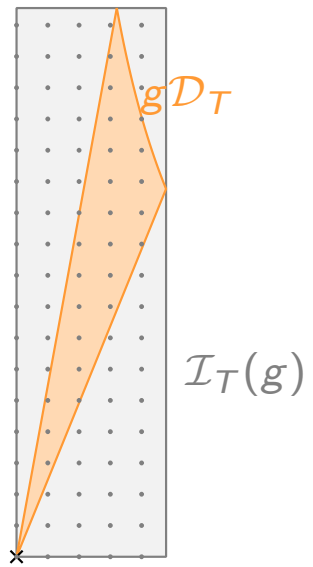
$\Rightarrow \#(\mathcal{I}_T(g) \cap V(\mathbb{Z})) \leq E_T$ for some constant E_T

$\rightarrow$ With probability $\frac{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}{E_T}$:

Pick a uniformly random $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$.

If $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ and f is irreducible, return $\mathrm{GL}_2(\mathbb{Z})f$.

Otherwise, start over with (1).



Any irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ is returned with probability

$$p_T = \frac{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}{E_T} \cdot \frac{1}{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))} = \frac{1}{E_T}.$$

Since there are $\asymp T$ valid orbits, the success probability is $\asymp T \cdot \frac{1}{E_T}$

Implementation of Step (2)

(1) Pick random g from $\mathcal{F}$ with probability measure $\mathrm{d}g$.

(2) Either return $\mathrm{GL}_2(\mathbb{Z})f$ for a random irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$, or start over with (1). *Every* such element f should be picked with the *same* probability $p_T > 0$ *independent of* g.

Let $\mathcal{I}_T(g)$ be the smallest axis-parallel box containing $g\mathcal{D}_T$.

If every $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$ **has** X^3**-coefficient** $a = 0$**:**

$\Rightarrow$ There is no irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$.

$\rightarrow$ Start over with (1).

Otherwise:

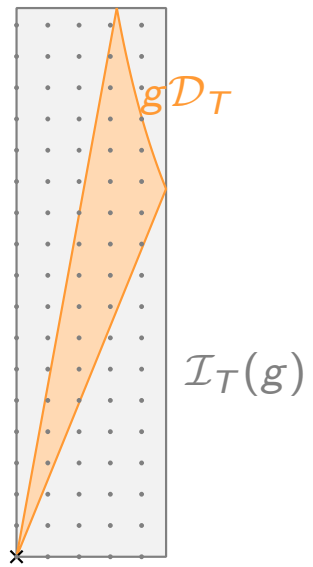
$\Rightarrow \#(\mathcal{I}_T(g) \cap V(\mathbb{Z})) \leq E_T$ for some constant $E_T \asymp T$.

$\rightarrow$ With probability $\frac{\#(\mathcal{I}_T(g)\cap V(\mathbb{Z}))}{E_T}$:

Pick a uniformly random $f \in \mathcal{I}_T(g) \cap V(\mathbb{Z})$.

If $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ and f is irreducible, return $\mathrm{GL}_2(\mathbb{Z})f$.

Otherwise, start over with (1).



Any irreducible $f \in g\mathcal{D}_T \cap V(\mathbb{Z})$ is returned with probability

$$p_T = \frac{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))}{E_T} \cdot \frac{1}{\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))} = \frac{1}{E_T}.$$

Since there are $\asymp T$ valid orbits, the success probability is $\asymp T \cdot \frac{1}{E_T} \asymp 1$.

Variants

1) Negative discriminants.

   Just flip some signs.

Variants

1) Negative discriminants.

   Just flip some signs.

2) Return all S with the *same* probability, rather than with probability proportional to $1/|\mathrm{Aut}(S)|$.

   Only accept S with probability $|\mathrm{Aut}(S)|/3$, reject otherwise.

Variants

1) Negative discriminants.

   Just flip some signs.

2) Return all S with the *same* probability, rather than with probability proportional to $1/|\mathrm{Aut}(S)|$.

   Only accept S with probability $|\mathrm{Aut}(S)|/3$, reject otherwise.

3) Random cubic integral domain S with $T \leq \mathrm{disc}(S) \leq T + T^{5/6+\varepsilon}$ in expected time $\tilde{O}_\varepsilon(\log T)$.

   Replace $\mathcal{D}_T = (0, T^{1/4}] \cdot \mathcal{U}$ by $(T^{1/4}, (T + T^{5/6+\varepsilon})^{1/4}] \cdot \mathcal{U}_T$.

   Pick g with probability measure proportional to

   (upper bound on $\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))) \cdot \mathrm{d}g$.

Variants

1) Negative discriminants.
   Just flip some signs.
2) Return all S with the *same* probability, rather than with probability proportional to $1/|\mathrm{Aut}(S)|$.
   Only accept S with probability $|\mathrm{Aut}(S)|/3$, reject otherwise.
3) Random cubic integral domain S with $T \leq \mathrm{disc}(S) \leq T + T^{5/6+\varepsilon}$ in expected time $\tilde{O}_\varepsilon(\log T)$.
   Replace $\mathcal{D}_T = (0, T^{1/4}] \cdot \mathcal{U}$ by $(T^{1/4}, (T + T^{5/6+\varepsilon})^{1/4}] \cdot \mathcal{U}_T$.
   Pick g with probability measure proportional to
   (upper bound on $\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))) \cdot \mathrm{d}g$.
4) Random pair (S, I) where S is a *quadratic* integral domain with $0 < \pm\mathrm{disc}(S) \leq T$ and I is an invertible ideal class of S, with probability proportional to $\mathrm{Reg}(S)/\omega_S$.

Variants

1) Negative discriminants.
   Just flip some signs.
2) Return all S with the *same* probability, rather than with probability proportional to $1/|\mathrm{Aut}(S)|$.
   Only accept S with probability $|\mathrm{Aut}(S)|/3$, reject otherwise.
3) Random cubic integral domain S with $T \leq \mathrm{disc}(S) \leq T + T^{5/6+\varepsilon}$ in expected time $\tilde{O}_\varepsilon(\log T)$.
   Replace $\mathcal{D}_T = (0, T^{1/4}] \cdot \mathcal{U}$ by $(T^{1/4}, (T + T^{5/6+\varepsilon})^{1/4}] \cdot \mathcal{U}_T$.
   Pick g with probability measure proportional to
   (upper bound on $\#(\mathcal{I}_T(g) \cap V(\mathbb{Z}))) \cdot \mathrm{d}g$.
4) Random pair (S, I) where S is a *quadratic* integral domain with $0 < \pm\mathrm{disc}(S) \leq T$ and I is an invertible ideal class of S, with probability proportional to $\mathrm{Reg}(S)/\omega_S$.
5) Theoretically: quartic and quintic rings.