

2 次体はどのくらい存在するのか？

山田 達也 @Chogorizawa

神戸大学 D1

2026 年 10 月 11 日

- $\mathbb{N}$ は正の整数全体の集合とする. $0 \notin \mathbb{N}$ である.
- $\mathbb{P}$ は素数全体の集合とする.
- $n, m \in \mathbb{Z}$ に対して, $n \mid m \stackrel{\text{def}}{\iff} (n) \supset (m)$.
 $n \mid m$ でないとき, $n \nmid m$ とかく.
- 何もいわずに p は素数を表すものとする.
- 環や体の集合を扱う際は, 同型の違いを除いて考えているものとする.
- 有限集合 S に対して, $\#S := \sum_{s \in S} 1$. すなわち, S の元の個数を表す.
- 集合 S に対して, $\mathbb{1}_S$ で S の指示関数を表す.



スライド (ホームページ)

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理
- ⑤ Theorem 1 の証明
- ⑥ まとめ

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理
- ⑤ Theorem 1 の証明
- ⑥ まとめ

代数体, n 次体とは

環準同型 $\mathbb{Q} \longrightarrow F$ が存在するような体 F を $\mathbb{Q}$ の**拡大体**という.

このとき, $\mathbb{Q} \longrightarrow F$ は単射で, 一意である.

$\mathbb{Q}$ の拡大体 F は, 一意的な単射環準同型 $\mathbb{Q} \longrightarrow F$ によって $\mathbb{Q} \subseteq F$ と考えてよい.

$\mathbb{Q}$ の拡大体 F は, $r \cdot x := rx$ ($r \in \mathbb{Q}, x \in F$) により $\mathbb{Q}$ -ベクトル空間になる.

$\dim_{\mathbb{Q}} F < \infty$ である $\mathbb{Q}$ の拡大体 F を**代数体**という.

$n \in \mathbb{N}$ に対して, $\dim_{\mathbb{Q}} F = n$ である $\mathbb{Q}$ の拡大体 F を n **次体**という.

代数体は整数論においてとても重要な対象である.

$\mathbb{R}$ は $\mathbb{Q}$ の拡大体である. $\dim_{\mathbb{Q}} \mathbb{R} = \infty$ であるから $\mathbb{R}$ は代数体ではない.

θ を $X^3 = 10$ となる唯 1 つの実数 X とすると,
 $K := \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\}$ は $\mathbb{Q}$ の拡大体である. $1, \theta, \theta^2$ は K の $\mathbb{Q}$ -基底となるので, $\dim_{\mathbb{Q}} K = 3$ で 3 次体である.
 $X \mapsto \theta$ とする (θ を代入する) 環準同型 $\mathbb{Q}[X] \rightarrow \mathbb{R}$ で準同型定理を使うと,

$$\mathbb{Q}[X]/(X^3 - 10) \cong K.$$

であることも分かる.

代数体の数え上げとは？ 1

代数体はとても重要な対象



「代数体はどのくらいあるのだろう」というのは自然で素朴な問い



実際、代数体はどのくらいある？

A. 無限個

そういうことやない

例えば、 $\mathbb{N}$ の中で偶数も平方数も素数も無限にあるけど、

- 偶数は全体の半分くらい
- 素数や平方数は偶数よりも少なそう

というイメージがなんとなくあるはず. それは $< X$ で考えている.

$< X$ において正の整数は大体 X 個, その中で

- 偶数の個数は, 大体 $\frac{X}{2}$ 個
- 平方数の個数は, 大体 $X^{1/2}$ 個
- 素数の個数は, 大体 $\frac{X}{\log X}$ 個 (素数定理)

代数体の数え上げとは？ 2

代数体も同じように考えたいが、代数体だと単に $< X$ は考えられない。
代数体に対して定まる「判別式」という不変量 (の絶対値) で $\mathbb{N}$ に落とし込むことで、 $< X$ を考える。

また、代数体だと難しい。今回は代数体の中でも単純な 2 次体の数え上げを扱う。

(注意) $\mathbb{N}$ に落とし込むための代数体の不変量は、判別式が自然だという深い根拠があるわけではない。
どういう不変量が一番本質的なのかはよく分かってない。

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理
- ⑤ Theorem 1 の証明
- ⑥ まとめ

トレースとノルム

F を代数体とし, $n = \dim_{\mathbb{Q}} F$ とする. $\alpha \in F$ に対して,

$T_{\alpha}: F \longrightarrow F$ は $\mathbb{Q}$ -線型写像である.

$\Psi \qquad \qquad \Psi$

$x \longmapsto \alpha x$

$\mathrm{Tr}_F(\alpha) := \mathrm{Tr}(T_{\alpha}) \in \mathbb{Q}$, $N_F(\alpha) := \det(T_{\alpha}) \in \mathbb{Q}$ をそれぞれ α の **トレース**, **ノルム** という.

代数体の判別式

「あるモニックな $f \in \mathbb{Z}[X]$ が存在して、 $f(\alpha) = 0$ 」を満たす $\alpha \in F$ 全体の集合を $\mathcal{O}_F$ とかく。

これは、 $\mathbb{Q}$ において $\mathbb{Z}$ にあたるものを F で考えたものであり、 $\mathcal{O}_F$ は F の部分環となるので、 $\mathcal{O}_F$ を F の**整数環**という。次の事実が知られている。

- $\alpha \in \mathcal{O}_F$ については、 $\text{Tr}_F(\alpha), N_F(\alpha) \in \mathbb{Z}$

$\mathcal{O}_F$ は環であるだけでなく、階数 n の自由 $\mathbb{Z}$ -加群にもなっている、すなわち、

$$\mathcal{O}_F = \omega_1 \mathbb{Z} \oplus \omega_2 \mathbb{Z} \oplus \dots \oplus \omega_n \mathbb{Z}$$

となる $\omega_1, \omega_2, \dots, \omega_n \in \mathcal{O}_F$ がとれる。このとき、 $\det\left((\text{Tr}_F(\omega_i \omega_j))_{i,j}\right) \in \mathbb{Z}$ は $\omega_1, \omega_2, \dots, \omega_n$ のとり方によらない。この値を F の**判別式**といい、 $\text{Disc}(F)$ とかく。 $\text{Disc}(F) \neq 0$ となる。

数え上げ関数の定義

$X > 0$ に対して, $N_2^\pm(X) := \#\{F: 2 \text{ 次体} \mid 0 < \pm \text{Disc}(F) < X\}$ と定義する. $N_2^\pm(X)$ について調べたい, もっというと,

$$N_2^\pm(X) = (\text{よく知られた } X \text{ の関数}) + (\text{誤差})$$

と表すのが目標.

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理
- ⑤ Theorem 1 の証明
- ⑥ まとめ

パラメータ付けの準備

$m \in \mathbb{Z}$ がスクエアフリー

$\stackrel{\text{def}}{\iff}$ 任意の $p \in \mathbb{P}$ に対して $p^2 \nmid m$

$\iff \exists \epsilon \in \{\pm 1\}, \exists S: \mathbb{P} \text{ の有限部分集合 s.t. } m = \epsilon \cdot \prod_{p \in S} p$

例) 1, 15, -70 はスクエアフリーだが, 0, 12, -54 はスクエアフリーでない.

- SF: スクエアフリーな整数全体の集合
- $P \subseteq \mathbb{P}$ に対して

$$\text{SF}_P^+ := \left\{ \prod_{p \in S} p \mid S: P \text{ の有限部分集合} \right\}$$

$\text{SF}_{\mathbb{P}}^+ = \text{SF} \cap \mathbb{N}$ が成り立つので, $\text{SF}_{\mathbb{P}}^+$ を単に SF^+ とかく.

$m \in \text{SF} \setminus \{1\}$ に対して, $F_m := \mathbb{Q}[X]/(X^2 - m)$ とする.
また, $\mathcal{F}_2 := \{F_m \mid m \in \text{SF} \setminus \{1\}\}$ とする.

Proposition 1

- ① $\mathcal{F}_2$ は全ての 2 次体を含む.
- ② $\mathcal{F}_2$ の元は全て 2 次体である.

すなわち, $\mathcal{F}_2$ は 2 次体全体の集合である.

この Proposition 1 を証明する.

$\mathcal{F}_2$ は全ての 2 次体を含むか 1

任意の 2 次体 F をとる.

$\dim_{\mathbb{Q}} F = 2$ より, $1, \alpha$ が F の $\mathbb{Q}$ -基底となるような $\alpha \in F$ がとれる.

$a, b \in \mathbb{Q}$ が存在して, $\alpha^2 = a \cdot \alpha + b \cdot 1 = a\alpha + b$.

$1, \alpha$ は線型独立より $\alpha - \frac{a}{2} = 1 \cdot \alpha - \frac{a}{2} \cdot 1 \neq 0$ であるから

$$0 \neq \left(\alpha - \frac{a}{2}\right)^2 = \frac{4b - a^2}{4}.$$

よって, $4b - a^2 = k^2 m$ ($k \in \mathbb{Q}^\times, m \in \text{SF}$) と一意的に分解できる.

ここで $m = 1$ と仮定すると, $\left(\alpha - \frac{a-k}{2}\right)\left(\alpha - \frac{a+k}{2}\right) = 0$ より

$\alpha - \frac{a-k}{2} = 0$ または $\alpha - \frac{a+k}{2} = 0$ となるから, $1, \alpha$ が線型独立であることに矛盾. $m \in \text{SF} \setminus \{1\}$ である.

$\mathcal{F}_2$ は全ての2次体を含むか 2

環準同型 $f: \mathbb{Q}[X] \rightarrow F$ を $f(X) = \frac{2}{k}(\alpha - \frac{a}{2})$ により定めると,

$$f(1) = 1, \quad f\left(\frac{k}{2}X + \frac{a}{2}\right) = \alpha$$

より f は全射.

$$f(X^2 - m) = f(X)^2 - m = \frac{4}{k^2}\left(\alpha - \frac{a}{2}\right)^2 - \frac{4b - a^2}{k^2} = 0$$

より $(X^2 - m) \subseteq \text{Ker } f \subsetneq \mathbb{Q}[X]$. $X^2 - m$ は $\mathbb{Q}[X]$ の既約元であり, $\mathbb{Q}[X]$ は PID より $(X^2 - m)$ は $\mathbb{Q}[X]$ の極大イデアルであるから,
 $(X^2 - m) = \text{Ker } f$. 準同型定理より $F_m \cong F$.

よって, $\mathcal{F}_2$ は全ての2次体を含むことがわかった.

$\mathcal{F}_2$ の元は全て 2 次体か

$m \in \text{SF} \setminus \{1\}$ をとると, $X^2 - m$ は $\mathbb{Q}[X]$ の既約元.

$\mathbb{Q}[X]$ は PID より $(X^2 - m)$ は $\mathbb{Q}[X]$ の極大イデアルであるから, F_m は体である.

環準同型 $\mathbb{Q} \rightarrow \mathbb{Q}[X] \rightarrow F_m$ があるので, F_m は $\mathbb{Q}$ の拡大体.

$1 + (X^2 - m), X + (X^2 - m)$ は F_m の $\mathbb{Q}$ -基底となり, F_m は 2 次体である.

よって, $m \in \text{SF} \setminus \{1\}$ について, $\mathcal{F}_2$ の元は全て 2 次体である.

以上より, $\mathcal{F}_2 = \{2 \text{ 次体}\}$ である. □

F_m の元 $X + (X^2 - m)$ を $\sqrt{m}$ とかく. F_m の $\mathbb{Q}$ -基底として $1, \sqrt{m}$ をとると, $\alpha = a + b\sqrt{m} \in F_m$ ($a, b \in \mathbb{Q}$) に対して, T_α の表現行列は $\begin{pmatrix} a & bm \\ b & a \end{pmatrix}$

である. よって,
$$\begin{cases} \text{Tr}_{F_m}(\alpha) = 2a, \\ N_{F_m}(\alpha) = a^2 - b^2 m. \end{cases}$$

F_m の整数環と判別式

$m \in \text{SF} \setminus \{1\}$ とする.

Proposition 2

$m \in \text{SF} \setminus \{1\}$ に対して

$$\mathcal{O}_{F_m} = \begin{cases} \mathbb{Z} \oplus \frac{1 + \sqrt{m}}{2} \mathbb{Z} & \text{if } m \equiv 1 \pmod{4}, \\ \mathbb{Z} \oplus \sqrt{m} \cdot \mathbb{Z} & \text{if } m \equiv 2, 3 \pmod{4}. \end{cases}$$

この Proposition 2 から, $\Delta_m := \text{Disc}(F_m)$ とすると,

$$\Delta_m = \text{Disc}(F_m) = \begin{cases} m & \text{if } m \equiv 1 \pmod{4}, \\ 4m & \text{if } m \equiv 2, 3 \pmod{4}. \end{cases}$$

Proposition 2 の証明

Proposition 2 の証明のため, Proposition 2 の右辺を R_m とおく.

$\frac{1+\sqrt{m}}{2}$ が $X^2 - X + \frac{1-m}{4} \in \mathbb{Z}[X]$ の根であることに注意すれば, $\mathcal{O}_{F_m} \supseteq R_m$.

$\alpha = a + b\sqrt{m} \in \mathcal{O}_{F_m}$ ($a, b \in \mathbb{Q}$) と仮定すると,

$\text{Tr}_{F_m}(\alpha), N_{F_m}(\alpha) \in \mathbb{Z}$ であるから, $2a, a^2 - b^2m \in \mathbb{Z}$.

よって, $(2b)^2m = (2a)^2 - 4(a^2 - b^2m) \in \mathbb{Z}$ であり, $m \in \text{SF}$ より, $2b \in \mathbb{Z}$.

また, $(2a)^2 \equiv (2b)^2m \pmod{4}$.

- $m \equiv 1 \pmod{4}$ のとき, $(2a)^2 \equiv (2b)^2 \pmod{4}$ より,
 $2a, 2b$ の偶奇は一致し, $a - b \in \mathbb{Z}$. よって,

$$a + b\sqrt{m} = (a - b) + \frac{1 + \sqrt{m}}{2} \cdot (2b) \in R_m.$$

- $m \equiv 2, 3 \pmod{4}$ のとき, $(2a)^2, (2b)^2 \equiv 0, 1 \pmod{4}$ より,
 $(2a)^2 \equiv (2b)^2 \equiv 0 \pmod{4}$ であるから, $a, b \in \mathbb{Z}$. よって,

$$a + b\sqrt{m} \in R_m.$$

□

$N_2^\pm(X)$ の分割

便利のため, $\Delta_1 := 1$ とする.

$n, m \in \text{SF}$ について, $n \neq m \implies \Delta_n \neq \Delta_m \implies F_n \neq F_m$ であるから,

$$\begin{aligned}
 N_2^\pm(X) + \mathbb{1}_{(0,X)}(\pm 1) &= \sum_{\substack{m \in \text{SF} \\ 0 < \pm \Delta_m < X}} 1 \\
 &= \sum_{\substack{m \in \text{SF} \\ m \equiv 1 \pmod{4} \\ 0 < \pm m < X}} 1 + \sum_{\substack{m \in \text{SF} \\ m \equiv 2 \pmod{4} \\ 0 < \pm m < X/4}} 1 + \sum_{\substack{m \in \text{SF} \\ m \equiv 3 \pmod{4} \\ 0 < \pm m < X/4}} 1 \\
 &= \sum_{\substack{s \in \text{SF} \\ s \equiv 1 \pmod{4} \\ 0 < \pm s < X}} 1 + \sum_{\substack{s \in \text{SF} \\ s \equiv 1 \pmod{2} \\ 0 < \pm s < X/8}} 1 + \sum_{\substack{s \in \text{SF} \\ s \equiv 3 \pmod{4} \\ 0 < \pm s < X/4}} 1.
 \end{aligned}$$

$\epsilon \in \{\pm 1\}$, $(t, a) \in \{(2, 1), (4, 1), (4, 3)\}$ で, 次の $N_\epsilon(Y, a; t)$ を調べたい.

$$N_\epsilon(Y, a; t) := \sum_{\substack{s \in \text{SF} \\ s \equiv a \pmod{t} \\ 0 < \epsilon s < Y}} 1$$

Gegenbauer の定理

Theorem 1 Gegenbauer の定理 (合同条件付き)

$\epsilon \in \{\pm 1\}$, $(t, a) \in \{(2, 1), (4, 1), (4, 3)\}$ に対して

$$N_{\epsilon}(Y, a; t) := \sum_{\substack{s \in \text{SF} \\ s \equiv a \pmod{t} \\ 0 < \epsilon s < Y}} 1 = \frac{8}{\pi^2 t} Y + O(Y^{1/2}) \quad (Y > 0).$$

もしこの Theorem 1 が示されれば、次の定理が得られる。

Theorem

$$N_2^{\pm}(X) = \frac{3}{\pi^2} X + O(X^{1/2}) \quad (X > 0).$$

実際, $\mathbb{1}_{(0, X)}(\pm 1) = O(X^{1/2})$ と Theorem 1 より

$$\begin{aligned} N_2^{\pm}(X) &= -\mathbb{1}_{(0, X)}(\pm 1) + N_{\pm 1}(X, 1; 4) + N_{\pm 1}\left(\frac{X}{8}, 1; 2\right) + N_{\pm 1}\left(\frac{X}{4}, 3; 4\right) \\ &= \frac{3}{\pi^2} X + O(X^{1/2}). \end{aligned}$$

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理**
- ⑤ Theorem 1 の証明
- ⑥ まとめ

Möbius 関数の定義

$$f: \mathbb{N} \longrightarrow \mathbb{C} \text{ が乗法的関数} \stackrel{\text{def}}{\iff} \begin{cases} f \neq 0 \text{ (i.e. } \exists n \in \mathbb{N} \text{ s.t. } f(n) \neq 0), \\ n, m \text{ が互いに素} \implies f(nm) = f(n)f(m). \end{cases}$$

乗法的関数 f は $f(1) = 1$ を満たし, $f(p^k)$ ($p \in \mathbb{P}, k \in \mathbb{N}$) の値によって一意に決まる.

Definition (Möbius 関数)

$\mu(p) = -1, \mu(p^2) = \mu(p^3) = \mu(p^4) = \dots = 0$ により定まる乗法的関数 $\mu: \mathbb{N} \longrightarrow \mathbb{C}$ を **Möbius 関数** という.

μ の値域は $\{-1, 0, 1\}$ であり, $n \in \mathbb{N}$ に対して $\mu(n) \neq 0 \iff n \in \text{SF}^+$.

Proposition 3 (Möbius の反転公式, $\mu * \mathbf{1} = \varepsilon$)

$n \in \mathbb{N}$ に対して

$$\sum_{d|n} \mu(d) = \mathbb{1}_{\{1\}}(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \neq 1. \end{cases}$$

ただし, 左辺の総和は, n の正の約数全体を渡る.

$n = 1$ のときは明らか. $n \neq 1$ とすると

$$\sum_{d|n} \mu(d) = \sum_{\substack{q|n \\ q \in \text{SF}}} \mu(q) = \sum_{\substack{q|n \\ q \in \text{SF}}} \prod_{p|q} \mu(p) = \prod_{p|n} (1 + \mu(p)) = 0.$$

□

包除原理の例

Q. 2 の倍数でも, 3 の倍数でも, 5 の倍数でもないような 1 から 100 の整数は何個あるでしょう？

ベン図を使って考えると分かりやすく,

$$\begin{aligned} & (2, 3, 5 \text{ の倍数でない}) \\ &= (\text{全体}) - (2 \text{ の倍数}) - (3 \text{ の倍数}) - (5 \text{ の倍数}) \\ &\quad + (6 \text{ の倍数}) + (15 \text{ の倍数}) + (10 \text{ の倍数}) - (30 \text{ の倍数}) \\ &= 100 - 50 - 33 - 20 + 16 + 6 + 10 - 3 = 26 \text{ 個} \end{aligned}$$

「2, 3, 5 の倍数でもない」というのは扱いにくいので, 「2, 3 の倍数」や「2, 3, 5 の倍数」などの扱いやすいものの足し引きを考えることで求めた。
→ 雑にいうとこれが包除原理の考え方

Theorem (包除原理)

S を有限集合とし, 各 $p \in \mathbb{P}$ に対して, $S_p \subseteq S$ が与えられているとする.
また, $P \subseteq \mathbb{P}$ は次の条件を満たすと仮定する.

(条件) 各 $s \in S$ について, $s \in S_p$ となる $p \in P$ は有限個

このとき, $\bigcap_{p|q} S_p \neq \emptyset$ である $q \in \text{SF}_P^+$ は有限個で,

$$\# \bigcap_{p \in P} (S \setminus S_p) = \sum_{q \in \text{SF}_P^+} \mu(q) \# \bigcap_{p|q} S_p.$$

包除原理の証明 1

$s \in S$ に対して $n_s := \prod_{\substack{p \in P \\ s \in S_p}} p$ とする. (仮定より有限積)

$q \in \text{SF}_P^+$ に対して, $S_q := \bigcap_{p|q} S_p$ とすると,

$$\begin{aligned} S_q \neq \emptyset &\iff \exists s \in S \text{ s.t. } \forall p \mid q, s \in S_p \\ &\iff \exists s \in S \text{ s.t. } q \mid n_s \\ &\implies q \mid \prod_{s \in S} n_s \end{aligned}$$

よって, $S_q \neq \emptyset$ である $q \in \text{SF}_P^+$ は有限個.

$$\begin{aligned} \sum_{q \in \text{SF}_P^+} \mu(q) \# S_q &= \sum_{q \in \text{SF}_P^+} \mu(q) \sum_{s \in S} \mathbb{1}_{S_q}(s) \\ &= \sum_{s \in S} \sum_{q \in \text{SF}_P^+} \mu(q) \mathbb{1}_{S_q}(s) \end{aligned}$$

包除原理の証明 2

ここで, $s \in S, q \in \text{SF}_P^+$ に対して,

$$\mathbb{1}_{S_q}(s) = 1 \iff \forall p \mid q, s \in S_p \iff q \mid n_s$$

であるから,

$$\begin{aligned} \sum_{s \in S} \sum_{q \in \text{SF}_P^+} \mu(q) \mathbb{1}_{S_q}(s) &= \sum_{s \in S} \sum_{\substack{q \in \text{SF}_P^+ \\ q \mid n_s}} \mu(q) \\ &= \sum_{s \in S} \sum_{q \mid n_s} \mu(q) \\ &= \sum_{\substack{s \in S \\ n_s=1}} 1 = \# \bigcap_{p \in P} (S \setminus S_p). \end{aligned}$$

□

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理
- ⑤ Theorem 1 の証明
- ⑥ まとめ

包除原理の適用

Theorem 1 (再掲) Gegenbauer の定理 (合同条件付き)

$\epsilon \in \{\pm 1\}, (t, a) \in \{(2, 1), (4, 1), (4, 3)\}$ に対して

$$N_\epsilon(Y, a; t) := \sum_{\substack{s \in \text{SF} \\ s \equiv a \pmod{t} \\ 0 < \epsilon s < Y}} 1 = \frac{8}{\pi^2 t} Y + O(Y^{1/2}) \quad (Y > 0).$$

$S = \{s \in \mathbb{Z} \mid 0 < \epsilon s < Y, s \equiv a \pmod{t}\}$ とし, $p \in \mathbb{P}$ に対して,
 $S_p = \{s \in S \mid p^2 \mid s\}$ とする. また, $P := \mathbb{P} \setminus \{2\}$ とする.
これらを用いると,

$$N_\epsilon(Y, a; t) = \sum_{\substack{s \in \text{SF} \\ s \equiv a \pmod{t} \\ 0 < \epsilon s < Y}} 1 = \# \bigcap_{p \in P} (S \setminus S_p)$$

と表せる. 包除原理より,

$$N_\epsilon(Y, a; t) = \sum_{q \in \text{SF}_P^+} \mu(q) \# \bigcap_{p|q} S_p.$$

S_p の共通部分

各 $q \in \text{SF}_p^+$ に対して, t と q は互いに素であり, $q^2 \equiv 1 \pmod t$ であるから,

$$\begin{aligned}\bigcap_{p|q} S_p &= \{s \in \mathbb{Z} \mid 0 < \epsilon s < Y, s \equiv a \pmod t, p^2 \mid s \ (\forall p \mid q)\} \\ &= \{s \in \mathbb{Z} \mid 0 < \epsilon s < Y, s \equiv a \pmod t, q^2 \mid s\} \\ &= \{s \in \mathbb{Z} \mid 0 < \epsilon s < Y, s \equiv aq^2 \pmod{tq^2}\}\end{aligned}$$

よって,

$$N_\epsilon(Y, a; t) = \sum_{q \in \text{SF}_p^+} \mu(q) \sum_{\substack{0 < \epsilon s < Y \\ s \equiv aq^2 \pmod{tq^2}}} 1.$$

内側の和の評価

Lemma 1

$k \in \mathbb{Z}, m \in \mathbb{N}$ とすると, $X > 0$ に対して, 次が成り立つ.

$$\sum_{\substack{0 < \epsilon n < X \\ n \equiv k \pmod{m}}} 1 = \frac{X}{m} + O(1), \quad \sum_{\substack{0 < \epsilon n < X \\ n \equiv k \pmod{m}}} 1 \leq \frac{X}{R_m(\epsilon k)}.$$

ただし, $R_m(\epsilon k)$ は $\epsilon k \equiv b \pmod{m}$ となる最小の $b \in \mathbb{N}$ を表す.

ここでパラメータ Q をとり, q の和を $q < Q$ と $q \geq Q$ に分割する.

$$\begin{aligned} N_\epsilon(Y, a; t) &= \sum_{q \in \text{SF}_P^+} \mu(q) \sum_{\substack{0 < \epsilon s < Y \\ s \equiv aq^2 \pmod{tq^2}}} 1 \\ &= \underbrace{\sum_{\substack{q \in \text{SF}_P^+ \\ q < Q}} \mu(q) \sum_{\substack{0 < \epsilon s < Y \\ s \equiv aq^2 \pmod{tq^2}}} 1}_{=: A_1} + \underbrace{\sum_{\substack{q \in \text{SF}_P^+ \\ q \geq Q}} \mu(q) \sum_{\substack{0 < \epsilon s < Y \\ s \equiv aq^2 \pmod{tq^2}}} 1}_{=: A_2}. \end{aligned}$$

A_2 の評価

Lemma 1 と $R_{tq^2}(aq^2) \geq q^2$ より

$$\begin{aligned} |A_2| &\leq \sum_{\substack{q \in \text{SF}_P^+ \\ q \geq Q}} |\mu(q)| \left| \sum_{\substack{0 < \epsilon s < Y \\ s \equiv aq^2 \pmod{tq^2}}} 1 \right| \\ &\leq \sum_{\substack{q \in \text{SF}_P^+ \\ q \geq Q}} 1 \cdot \frac{Y}{R_{tq^2}(aq^2)} \\ &\leq Y \sum_{q \geq Q} \frac{1}{q^2} \\ &\leq Y \int_Q^\infty \frac{1}{x^2} dx \\ &= O\left(\frac{Y}{Q}\right). \end{aligned}$$

A_1 の評価

$$\begin{aligned} A_1 &= \sum_{\substack{q \in \text{SF}_P^+ \\ q < Q}} \mu(q) \left(\frac{Y}{tq^2} + O(1) \right) \\ &= \frac{Y}{t} \sum_{q \in \text{SF}_P^+} \frac{\mu(q)}{q^2} - \frac{Y}{t} \sum_{\substack{q \in \text{SF}_P^+ \\ q \geq Q}} \frac{\mu(q)}{q^2} + O \left(\sum_{\substack{q \in \text{SF}_P^+ \\ q < Q}} |\mu(q)| \right) \\ &= \frac{Y}{t} \sum_{q \in \text{SF}_P^+} \frac{\mu(q)}{q^2} + O \left(Y \sum_{q \geq Q} \frac{1}{q^2} \right) + O \left(\sum_{0 < q < Q} 1 \right) \\ &= \frac{Y}{t} \sum_{q \in \text{SF}_P^+} \frac{\mu(q)}{q^2} + O \left(\frac{Y}{Q} \right) + O(Q) \end{aligned}$$

主要項の係数

ここで,

$$\left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right) \left(\sum_{q=1}^{\infty} \frac{\mu(q)}{q^2} \right) = \sum_{m=1}^{\infty} \sum_{\substack{n, q \\ nq=m}} \frac{\mu(q)}{n^2 q^2} = \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{q|m} \mu(q) = 1.$$

また,

$$\begin{aligned} -\frac{1}{4} \sum_{q \in \text{SF}_P^+} \frac{\mu(q)}{q^2} &= \sum_{q \in \text{SF}_P^+} \frac{\mu(2q)}{(2q)^2} = \sum_{q \in \text{SF}^+ \setminus \text{SF}_P^+} \frac{\mu(q)}{q^2} \\ &= \sum_{q \in \text{SF}^+} \frac{\mu(q)}{q^2} - \sum_{q \in \text{SF}_P^+} \frac{\mu(q)}{q^2}. \end{aligned}$$

よって,

$$\sum_{q \in \text{SF}_P^+} \frac{\mu(q)}{q^2} = \frac{4}{3} \sum_{q \in \text{SF}^+} \frac{\mu(q)}{q^2} = \frac{4}{3} \sum_{q=1}^{\infty} \frac{\mu(q)}{q^2} = \frac{4}{3} \left(\sum_{n=1}^{\infty} \frac{1}{n^2} \right)^{-1} = \frac{8}{\pi^2}.$$

Q の選択

以上より,

$$N_{\epsilon}(Y, a; t) = \frac{8}{\pi^2 t} Y + O\left(\frac{Y}{Q}\right) + O(Q)$$

Q が大きければ $\frac{Y}{Q}$ は小さく, Q が小さければ $\frac{Y}{Q}$ は大きいので, いい塩梅の Q を選択する. いい塩梅とは $Q = \frac{Y}{Q}$ が成り立つ Q で, それは $Q = Y^{1/2}$. このとき,

$$N_{\epsilon}(Y, a; t) = \frac{8}{\pi^2 t} Y + O\left(Y^{1/2}\right).$$

□

目次

- ① 導入
- ② 代数体の判別式の定義
- ③ 2 次体のパラメータ付け
- ④ 包除原理
- ⑤ Theorem 1 の証明
- ⑥ まとめ

2 次体の数え上げの漸近公式

Theorem (再掲)

$$N_2^\pm(X) = \frac{3}{\pi^2}X + O\left(X^{1/2}\right) \quad (X > 0).$$

主要項の係数 $\frac{3}{\pi^2}$ は大体 0.3039635509... くらい.

$O(X^{1/2})$ より良い誤差の評価として, $O\left(X^{1/2} \exp\left(-\frac{c(\log X)^{3/5}}{(\log \log X)^{1/5}}\right)\right)$ が知られている (予想は $O_\varepsilon(X^{1/4+\varepsilon})$).

2次体以外の数え上げの例

Theorem (Bhargava–Taniguchi–Thorne, 2024)

$$\#\{F: 3 \text{ 次体} \mid |\text{Disc}(F)| < X\} = cX + kX^{5/6} + O_\varepsilon(X^{2/3+\varepsilon}).$$

Theorem (McGown–Tucker, 2024)

$$\#\{F: 4 \text{ 次体} \mid \text{Aut}(F) \cong C_2, |\text{Disc}(F)| < X\} = AX + O_\varepsilon(X^{5/8+\varepsilon}).$$

Theorem (Y.)

$$\begin{aligned} \#\{F: 6 \text{ 次体} \mid \text{Aut}(F) \cong S_3, |\text{Disc}(F)| < X\} \\ = CX^{1/3} + KX^{5/18} + O_\varepsilon(X^{8/29+\varepsilon}). \end{aligned}$$

ただし, $\text{Aut}(F)$ は環 (準) 同型 $F \rightarrow F$ 全体が合成を演算としてなす群を表す.