

# Contents

<b>1</b>	<b>Classes</b>	<b>2</b>
1.1	quad – 虚二次体	2
1.1.1	ReducedQuadraticForm – 簡約二次形式クラス	2
1.1.1.1	inverse	4
1.1.1.2	disc	4
1.1.2	ClassGroup – 類群クラス	4
1.1.3	class_formula	5
1.1.4	class_number	5
1.1.5	class_group	5
1.1.6	class_number_bsgs	5
1.1.7	class_group_bsgs	6

# Chapter 1

## Classes

### 1.1 quad – 虚二次体

- Classes
  - **ReducedQuadraticForm**
  - **ClassGroup**
- Functions
  - **class\_formula**
  - **class\_number**
  - **class\_group**
  - **class\_number\_bsgs**
  - **class\_group\_bsgs**

#### 1.1.1 ReducedQuadraticForm – 簡約二次形式クラス

##### Initialize (Constructor)

**ReducedQuadraticForm(f: list, unit: list) → *ReducedQuadraticForm***

ReducedQuadraticForm オブジェクトを作成.

f, unit は 3 整数 [a, b, c] のリストでなければならず, 二次形式を  $ax^2 + bxy + cy^2$  と表記. unit は単元形式を表す.

##### Operations

operator	explanation
$M * N$	$M$ と $N$ の合成を返す.
$M ** a$	$M$ の $a$ 乗を返す.
$M / N$	二次形式の除算.
$M == N$	$M$ と $N$ が等しいかどうか返す.
$M != N$	$M$ と $N$ が等しくないかどうか返す.

## Methods

### 1.1.1.1 inverse

`inverse(self)`  $\rightarrow$  *ReducedQuadraticForm*

`self` の逆元を返す.

### 1.1.1.2 disc

`disc(self)`  $\rightarrow$  *ReducedQuadraticForm*

`self` の判別式を返す.

## 1.1.2 ClassGroup – 類群クラス

### Initialize (Constructor)

`ClassGroup(disc: integer, cl: integer, element: integer=None)`  
 $\rightarrow$  *ClassGroup*

`ClassGroup` オブジェクトを作成.

## Methods

### 1.1.3 class\_formula

```
class_formula(d: integer, uprbd: integer) → integer
```

類数公式を使い, 判別式  $d$  を持つ類数  $h$  の近似値を返す.

$$\text{類数公式 } h = \frac{\sqrt{|d|}}{\pi} \prod_p \left( 1 - \left( \frac{d}{p} \right) \frac{1}{p} \right)^{-1}.$$

入力する数  $d$  は int 型, long 型 または **Integer** でなければならない.

### 1.1.4 class\_number

```
class_number(d: integer, limit_of_d: integer=1000000000)
→ integer
```

簡約形式の数を数えることにより判別式  $d$  を持つ類数を返す.

$d$  は基本判別式とは限らない.

入力する数  $d$  は int 型, long 型 または **Integer** でなければならない.

### 1.1.5 class\_group

```
class_group(d: integer, limit_of_d: integer=1000000000)
→ integer
```

簡約形式の数を数えることにより判別式  $d$  を持つ類数と類群を返す.

$d$  は基本判別式とは限らない.

入力する数  $d$  は int 型, long 型 または **Integer** でなければならない.

### 1.1.6 class\_number\_bsgs

```
class_number_bsgs(d: integer) → integer
```

Baby-step Giant-step アルゴリズムを使い, 判別式  $d$  を持つ類数を返す.

$d$  は基本判別式とは限らない.

入力する数  $d$  は int 型, long 型 または **Integer** でなければならない.

### 1.1.7 class\_group\_bsgs

```
class_group_bsgs(d: integer, cl: integer, qin: list)
    → integer
```

判別式  $\text{disc}$  を持つ位数  $p^{exp}$  の類群の構造を返す。 $qin = [p, exp]$  である。

入力する数  $d, cl$  は `int` 型, `long` 型 または **Integer** でなければならない。

#### Examples

```
>>> quad.class_formula(-1200, 100000)
12
>>> quad.class_number(-1200)
12
>>> quad.class_group(-1200)
(12, [ReducedQuadraticForm(1, 0, 300), ReducedQuadraticForm(3, 0, 100),
ReducedQuadraticForm(4, 0, 75), ReducedQuadraticForm(12, 0, 25),
ReducedQuadraticForm(7, 2, 43), ReducedQuadraticForm(7, -2, 43),
ReducedQuadraticForm(16, 4, 19), ReducedQuadraticForm(16, -4, 19),
ReducedQuadraticForm(13, 10, 25), ReducedQuadraticForm(13, -10, 25),
ReducedQuadraticForm(16, 12, 21), ReducedQuadraticForm(16, -12, 21)])
>>> quad.class_number_bsgs(-1200)
12L
>>> quad.class_group_bsgs(-1200, 12, [3, 1])
([ReducedQuadraticForm(16, -12, 21)], [[3L]])
>>> quad.class_group_bsgs(-1200, 12, [2, 2])
([ReducedQuadraticForm(12, 0, 25), ReducedQuadraticForm(4, 0, 75)],
[[2L], [2L, 0]])
```

# Bibliography