Contents

Chapter 1

Functions

1.1 cubic_root – cubic root, residue, and so on

1.1.1 c_root_p – cubic root mod p

c_root_p(a: *integer*, p: *integer*) → *list*

a 法 p の a の 3 乗根の値を返す。 (すなわち、 $x^3 = \mathtt{a} \pmod{\mathtt{p}}$).

p は素数。
この関数は a の 3 乗根のすべての値をリストで返す。

1.1.2 c_residue – cubic residue mod p

c_residue(a: *integer*, p: *integer*) → *integer*

法 p で有理数 a が 3 乗になっているか調べる。

もし p | a なら 0 を返す。また、法 p で a が 3 乗になっているならば 1 を返す。
そうでなければ (3 乗になっていいないとき)−1 を返す。

p は素数。

1.1.3 c_symbol – cubic residue symbol for Eisenstein-integers

c_symbol(a1: *integer*, a2: *integer*, b1: *integer*, b2: *integer*)
→ *integer*

二つの Eisenstein 整数である (Jacobi) 立方剰余記号の値を返す。$\left(\frac{\mathtt{a1}+\mathtt{a2}\omega}{\mathtt{b1}+\mathtt{b2}\omega}\right)_3$, ω

は 1 の 3 乗根の値である。

もし b1 + b2ω が $\mathbb{Z}[\omega]$ に含まれる素数であるならば、a1 + a2ω は立方剰余かわかる。

b1 + b2ω は $1-\omega$ に分けられないと仮定する。.

1.1.4 decomposite_p – decomposition to Eisenstein-integers

decomposite_p(p: *integer*) → (*integer*, *integer*)

$\mathbb{Z}[\omega]$ に含まれる素数の一つ p の値を返す。

もし出力が (a, b) なら、$\frac{p}{a+b\omega}$ は $\mathbb{Z}[\omega]$. に含まれる素数である。すなわち p が $\mathbb{Z}[\omega]$. に含まれる a + bω and p/(a + bω) の二つの素因数に分解することができる。

p は有理数かつ素数。$p \equiv 1 \pmod 3$ と仮定する。

1.1.5 cornacchia – solve $x^2 + dy^2 = p$

cornacchia(d: *integer*, p: *integer*) → (*integer*, *integer*)

$x^2 + dy^2 = p$ の値を返す。

この関数は Cornacchia のアルゴリズムを使用。 [1] 参照。

p は有理数かつ素数。d は $0 < d < p$ の関係を充たす。. この関数は $x^2 + dy^2 = p$ の値として (x, y) を返す。

Examples

```
>>> cubic_root.c_root_p(1, 13)
[1, 3, 9]
>>> cubic_root.c_residue(2, 7)
-1
>>> cubic_root.c_symbol(3, 6, 5, 6)
1
>>> cubic_root.decomposite_p(19)
(2, 5)
>>> cubic_root.cornacchia(5, 29)
(3, 2)
```

Bibliography

[1] Henri Cohen. *A Course in Computational Algebraic Number Theory.* GTM138. Springer, 1st. edition, 1993.