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*

Return the cubic root of `a` modulo prime `p`. (i.e. solutions of the equation $x^3 = \mathtt{a} \pmod{\mathtt{p}}$).

`p` must be a prime integer.
This function returns the list of all cubic roots of `a`.

1.1.2 c_residue – cubic residue mod p

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

Check whether the rational integer `a` is cubic residue modulo prime `p`.

If `p` | `a`, then this function returns 0, elif `a` is cubic residue modulo `p`, then it returns 1, otherwise (i.e. cubic non-residue), it returns −1.

`p` must be a prime integer.

1.1.3 c_symbol – cubic residue symbol for Eisenstein-integers

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

Return the (Jacobi) cubic residue symbol of two Eisenstein-integers $\left(\frac{\mathtt{a1}+\mathtt{a2}\omega}{\mathtt{b1}+\mathtt{b2}\omega}\right)_3$, where ω is a primitive cubic root of unity.

If $\mathtt{b1}+\mathtt{b2}\omega$ is a prime in $\mathbb{Z}[\omega]$, it shows $\mathtt{a1}+\mathtt{a2}\omega$ is cubic residue or not.

We assume that $\mathtt{b1}+\mathtt{b2}\omega$ is not divisible $1-\omega$.

1.1.4 decomposite_p – decomposition to Eisenstein-integers

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

Return one of prime factors of p in $\mathbb{Z}[\omega]$.

If the output is (a, b), then $\frac{\mathtt{p}}{\mathtt{a}+\mathtt{b}\omega}$ is a prime in $\mathbb{Z}[\omega]$. In other words, p decomposes into two prime factors $\mathtt{a}+\mathtt{b}\omega$ and $\mathtt{p}/(\mathtt{a}+\mathtt{b}\omega)$ in $\mathbb{Z}[\omega]$.

p must be a prime rational integer. We assume that $\mathtt{p} \equiv 1 \pmod 3$.

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

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

Return the solution of $x^2 + \mathtt{d}y^2 = \mathtt{p}$.

This function uses Cornacchia's algorithm. See [1].

p must be prime rational integer. d must be satisfied with the condition $0 < \mathtt{d} < \mathtt{p}$. This function returns (x, y) as one of solutions of the equation $x^2 + \mathtt{d}y^2 = \mathtt{p}$.

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.