Contents

Chapter 1

Functions

1.1 ecpp – elliptic curve primality proving

このモジュールは ECPP (Elliptic Curve Primality Proving) の様々な関数から作られている。
It is probable that the module will be refactored in the future so that each function be placed in other modules.

ecpp モジュールは mpmath のダウンロードが必要。

1.1.1 ecpp – elliptic curve primality proving

ecpp(n: *integer*, era: *list*=None) → *bool*

楕円曲線素数証明を行う。
もし n が素数なら True を返す。さもなければ False を返す。

また、era とは素数ののリストである。(これは ERAtosthenes に基づいている。)

n は巨大な整数。

1.1.2 hilbert – Hilbert class polynomial

hilbert(D: *integer*) → *(integer, list)*

類数と Hilbert 類方程式 for 虚 2 次体 with fundamental 判別式 D の値を返す。

この関数は Hilbert 類方程式の係数のリストを返す。
† もし **HAVE_NET** を設定してしているなら 、まず http://hilbert-class-polynomial.appspot.com/ を検索し. もし ramD に一致する情報が見つからなければ Hilbert

類方程式を直接計算してください。
D は int または long. [1] 参照。

1.1.3 dedekind – Dedekind's eta function

dedekind(tau: *mpmath.mpc*, floatpre: *integer*) → *mpmath.mpc*

Return Dedekind のイータ of a complex number tau in the upper half-plane.

Additional argument floatpre specifies the precision of calculation in decimal digits.

floatpre must be positive int.

1.1.4 cmm – CM method

cmm(p: *integer*) → *list*

CM 曲線のカーブパラメータの値を返す。

もし一つだけ楕円曲線でよいのならば **cmm_order** を使うとよい。

p は奇素数でなければならない。
この関数は (a, b) のリストを返す。(a, b) は Weierstrass' short form を表している。

1.1.5 cmm_order – CM method with order

cmm_order(p: *integer*) → *list*

CM 曲線のカーブパラメータの値と位数を返す。

もし一つだけ楕円曲線でよいのならば **cmm_order** を使うとよい。

p は奇素数でなければならない。
この関数は (a, b, order) のリストを返す。(a, b) は Weierstrass' short form を表し、 order は楕円曲線での位数を表す。

1.1.6 cornacchiamodify – Modified cornacchia algorithm

cornacchiamodify(d: *integer*, p: *integer*) → *list*

$(u,\ v)$ of $u^2 - \mathtt{d}v^2 = 4\mathtt{p}$ の解を返す。

もし解がなければ ValueError を返す。

p は素数。d は $d < 0$ and $d > -4p$ with $d \equiv 0, 1 \pmod 4$ を充たす整数。

Examples

```
>>> ecpp.ecpp(300000000000000000053)
True
>>> ecpp.hilbert(-7)
(1, [3375, 1])
>>> ecpp.cmm(7)
[(6L, 3L), (5L, 4L)]
>>> ecpp.cornacchiamodify(-7, 29)
(2, 4)
```

Bibliography

[1] Richard Crandall and Carl Pomerance. *Prime Numbers*. Springer, 1st. edition, 2001.