

Contents

1	Functions	2
1.1	arith1 - miscellaneous arithmetic functions	2
1.1.1	floorsqrt – floor of square root	2
1.1.2	floorpowerroot – floor of some power root	2
1.1.3	legendre - Legendre(Jacobi) Symbol	2
1.1.4	modsqrt – square root of a for modulo p	2
1.1.5	expand – p-adic expansion	3
1.1.6	inverse – inverse	3
1.1.7	CRT – Chinese Remainder Theorem	3
1.1.8	AGM – Arithmetic Geometric Mean	3
1.1.9	vp – p -adic valuation	3
1.1.10	issquare - Is it square?	4
1.1.11	log – integer part of logarithm	4
1.1.12	product – product of some numbers	4

Chapter 1

Functions

1.1 arith1 - miscellaneous arithmetic functions

1.1.1 floorsqrt – floor of square root

`floorsqrt(a: integer/Rational) → integer`

a の 2 乗根の小数点切り捨てた値を返す.

1.1.2 floorpowerroot – floor of some power root

`floorpowerroot(n: integer, k: integer) → integer`

n の k 乗根の小数点切り捨てた値を返す.

1.1.3 legendre - Legendre(Jacobi) Symbol

`legendre(a: integer, m: integer) → integer`

Legendre 記号と Jacobi 記号を返す $\left(\frac{a}{m}\right)$.

1.1.4 modsqrt – square root of a for modulo p

`modsqrt(a: integer, p: integer) → integer`

a の 2 乗根が存在する時は p を法とする a の 2 乗根の値を返す。さもなければエラーを返す。

p は素数。

1.1.5 expand – p-adic expansion

`expand(n: integer, m: integer) → list`

n の m 進展開を返す。 .

n は正の整数。 m は 2 以上。 . 出力は降順の係数展開のリスト。 .

1.1.6 inverse – inverse

`inverse(x: integer, p: integer) → integer`

法 p における x の逆関数を返す。 .

p は素数。 .

1.1.7 CRT – Chinese Remainder Theorem

`CRT(nlist: list) → integer`

Return the uniquely determined integer satisfying all modulus conditions given by `nlist`.

入力 `nlist` は 2 つの要素からなるリスト。一つ目は割った余りで二つ目は割る数。どちらも整数。 .

1.1.8 AGM – Arithmetic Geometric Mean

`AGM(a: integer, b: integer) → float`

a と b の算術幾何平均を返す。

1.1.9 vp – p-adic valuation

`vp(n: integer, p: integer, k: integer=0) → tuple`

p 進評価と n の他の部分群を返す。

$\dagger k$ が与えられたら、評価と np^k の他の部分群を返す。

1.1.10 issquare - Is it square?

`issquare(n: integer) → integer`

n が二乗になっていたら根を返し、さもなければ 0 を返す。

1.1.11 log – integer part of logarithm

`log(n: integer, base: integer=2) → integer`

n の対数の整数部分を返す。base.

1.1.12 product – product of some numbers

`product(iterable: list, init: integer/Rational=None)
→ prod: integer/Rational`

iterable のすべての要素からなるものを返す。

If init is given, the multiplication starts with init instead of the first element in iterable.

Input list iterable must be list of numbers including integers, **Rational** etc. The output prod may be determined by the type of elements of iterable and init.

Examples

```
>>> arith1.AGM(10, 15)
12.373402181181522

>>> arith1.CRT([[2, 5], [3, 7]])
17
>>> arith1.CRT([[2, 5], [3, 7], [5, 11]])
192
>>> arith1.expand(194, 5)
[4, 3, 2, 1]
>>> arith1.vp(54, 3)
(3, 2)
>>> arith1.product([1.5, 2, 2.5])
```

```
7.5
>>> arith1.product([3, 4], 2)
24
>>> arith1.product([])
1
```

Bibliography