J の Math/misc について

Masato SHIMURA
JCD02773@nifty.com

2020 年 1 月 28 日

math/misc

addons/math/misc

1　数の色々な道具類

1.1　各種平均

math/misc/mean

```
NB. arithmean   arithmetic mean
NB. geomean     geometric mean
NB. harmean     harmonic mean
NB. commonmean  common mean
```

$$G = \sqrt{ab}$$

$$G = \sqrt[n]{x_1 x_2 \cdots x_n}$$

$$\frac{1}{H} = \frac{1}{2}\left(\frac{1}{a} + \frac{1}{b}\right)$$

$$\frac{1}{H} = \frac{1}{n}\left(\frac{1}{x_1} + \frac{1}{x_2} \cdots \frac{1}{x_n}\right)$$

売り上げの 5 年間の平均伸び率を求める。→ 幾何平均

$$\begin{pmatrix} 1 & 2,000 & \\ 2 & 2,500 & 1.25 \\ 3 & 4,000 & 1.6 \\ 4 & 8,000 & 2.0 \\ 5 & 12,000 & 1.50 \\ 6 & 15,000 & 1.25 \end{pmatrix}$$

$\sqrt[5]{1.25 \times 1.6 \times 2 \times 1.5 \times 1.25}$

```
   geomean 1.25 1.6 2 1.5 1.25
1.49628
```

平均伸び率 1.496%

```
   12j10 ": geomean 1.25 1.6 2 1.5 1.25
2000* 1.4962778697^5
   2000* 1.4962778697^5
15000
```

調和平均の例として速度の例が良く出される。金融ではドルコスト平均法が調和平均にあたる。

株価	株数	投資額
100	20	2000
200	10	2000
400	5	2000
100	20	1000

投資金額が一定なので平均できる

```
   harmean 100 200 400 100
145.455    NB. 平均購入株価

   % (1r4)* +/ % 100 200 400 100
145.455

  commonmean=: {. @ ((geomean,arithmean) ^: _)
```

1.2 数列の生成

integer $i.4 \rightarrow 0123$

$i : 4 \rightarrow$ `_4 _3 _2 _1 0 1 2 3 4`

```
NB. inta   augmented integers     inta 4    is  1 2 3 4
NB. inte   extended integers      inte 4    is  0 1 2 3 4
NB. ints   symmetric integers     ints 4    is  _4 _3 _2 _1 0 1 2 3 4
NB. intm   minus integers         intm _4   is  _1 _2 _3 _4
NB. intn   normal integers        intn _4   is  0 _1 _2 _3
NB. intr   reflexive integers     intr 4    is  3 2 1 0 1 2 3
NB. jint   complex integers       jint 2 3  is  (j. i.2) +/ i.3
NB. jints  complex symmetric ints jints 1 2 is  (j. i:1) +/ i:2
```

1.3 色々な数

```
NB. Various number definitions (Stirling, Euler ...)
NB. version: 1.0.0

NB.  bell              Bell numbers
NB.  bernoulli         Bernoulli numbers
NB.  catalan           Catalan numbers
NB.  cycle             Stirling cycle numbers
NB.  cycles            Stirling cycle number table
NB.  euler             Euler numbers
NB.  eulers            Euler numbers table
NB.  fibonacci         Fibonacci numbers
NB.  lucas             Lucas numbers
NB.  subset            Stirling subset numbers
NB.  subsets           Stirling subset number table
NB.  tangent           tangent numbers
```

1.4 円関数/三角関数の定義

trig　円関数の定義ファイル?
degree ↔ *radian* の変換関数は便利

```
dfr=: *&(180%pi)
rfd=: *&(pi%180)
```

2 数論

2.1 素数

prime

2.2 ユークリッドの互除法と GCD

$$mx + ny = gcd(m, n)$$

```
   contfrac 32r20
1 1 1 2
```

$$\frac{32}{20} = 1 + \frac{12}{20}$$

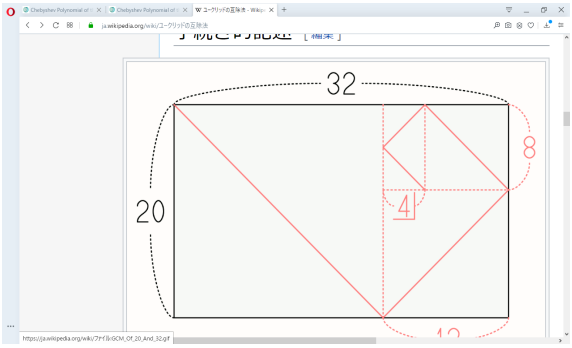
$$\frac{20}{12} = 1 + \frac{8}{12}$$

$$\frac{12}{8} = 1 + \frac{4}{8}$$

$$\frac{8}{4} = 2$$

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}$$

ユークリッド互除法のイメージ (wiki ユークリッド互除法の項より)




```
   >: % >:  % >: 1r2
8r5     NB. = 32r20
```

2.3 連分数

misc/contfrac

NB. Continued fraction utilities

NB. contfrac create continued fraction

NB. contfracx expand continued fraction

```
   7 contfrac o.1
3 7 15 1 292 1 1


   contfrac 55r34
1 1 1 1 1 1 1 2

   50j48 ": 55r34
```

```
1.6176470588235294117647058823529411764705882352941
1.6/1764705882352941/1764705882352941/176470588235294
```

```
   contfrac  1071r1029
1 24 2
```

次のように表せる

$$\frac{1071}{1029} = 1 + \frac{42}{1029}$$

$$\frac{1029}{42} = 24 + \frac{21}{42}$$

$$\frac{42}{21} = 2$$

連分数では

$$\frac{1071}{1029} = 1 + \frac{1}{24 + \frac{1}{2}}$$

```
   contfracx 1071r1029
51r49
```

```
   1071 1029 % 21
51 49
```

2.4 GCD

1. /math/gcd
2. Example

```
   gcd 1029 1071
+--+------+
|21|25 _24|
+--+------+
```

3. math

$$mx + ny = gcd(m, n)$$

$gcd(1029, 1071) = 21$

$21 = 25 \times 1029 + -24 \times 1071$

4. J の gcd のプリミティブ

```
   1029 +. 1071
```

```
   21
```

2.5 ルジャンドル記号

/math/misc/regendre

a が p の平方剰余であるとき，$(ap) = 1$ と定義する。

a が p の平方剰余でないとき，$(ap) = -1$ と定義する。

NB.*legendre v Legendre symbol (n/p) for integer n, odd prime p

NB. form: p legendre n

```
   7 legendre 2
1
   7 legendre 3
_1
```

```
   7 legendre >:i.7
1 1 _1 1 _1 _1 0
```

$$\left(\frac{2}{7}\right) \equiv 2^3 \equiv 1 mod 7$$

$$\left(\frac{2}{3}\right) \equiv 2^1 \equiv -1 mod 3$$

```
   131 legendre 74
1
```

$$\left(\frac{74}{131}\right) = \left(\frac{2}{131}\right)\left(\frac{131}{37}\right)$$

$$= \left(\frac{2}{131}\right)\left(\frac{20}{37}\right)$$

$$= \left(\frac{2}{131}\right)\left(\frac{4}{37}\right)\left(\frac{5}{37}\right)$$

$$= \left(\frac{2}{131}\right)\left(\frac{4}{37}\right)\left(\frac{37}{5}\right)$$

$$= \left(\frac{2}{131}\right)\left(\frac{4}{37}\right)\left(\frac{2}{5}\right)$$

$$= -1 \cdot 1 \cdot -1 = 1$$

2.6 Pollard の素因数分解法

/ math/misc/pollard

1975 John Pollard(G.B.) が発明

```
NB. pollardrho       Pollard rho factorization   NB. Pollard rho 法
NB. pollardpm1       Pollard p-1 factorization   NB. Pollard p-1 法
```

合成数 n の、ある素因数 p について,$(p-1)$ が小さな素数の積に分解できる場合、解くことができる、という性質がある。

RSA 暗号が解きやすいかどうかのチェックができる

フェルマーの小定理

ある自然数 a が存在して $a^n \equiv amodn$ が成り立てば n は合成数

$a = 2 \rightarrow 2^4 = 16 \neq 2mod4$

```
   4|16
0            NB. 合成数
```

フェルマーの小定理によれば、$\neq p$ と互いに素な整数 a について、次が成り立つ。$a^{p-1} \equiv 1(modp)$

そのため、 $p - 1 \mid L$ となるような整数 L は、$a^L \equiv 1(modp)$

が成り立つ。 よって、 $gcd(a^L - 1, n)$ は、 n の非自明な因数となり、素因数分解できる。

```
   pollardrho 540143
421 24


   pollardpm1 540143
421 6


   q: 540143
421 1283

   pollardrho 8051
97 3
```

片方の素数と?を表示

$$
\begin{array}{ll}
X_{k+1} = X_k^2 + 1 & mod(n) \\
X_0 = 1 \text{ を選定} & \\
X_1 = 2 & (GCD(x_1 - x_0, n) = 1 \\
X_2 = 5 & (5^2 + 1) \\
X_3 = 26 & \\
X_4 = 677 & \\
X_5 = 7474 & GCD(x_5 - x_3, n) = 1 \\
X_6 = 2839 & GCD(x_6 - x_4, n) = 97
\end{array}
$$

$$
p = \frac{n}{97} = 83 \qquad q = 97
$$

```
   8051 | *:677
7473  NB.  --> 7474

8051 | *: 7474
2838


   8051 +.  (2839-677)
1   NB. ???
```

2.7 パイの計算/Bigpi

NB. Calculate several digits of pi

NB. from Borwein

- Borwein 兄弟の公式
- David H. Bailey, Jonathan M. Borwein, Peter B. Borwein, and Simon Plouffe. ”The Quest for Pi”. Mathematical Intelligencer (Volume 19, p.50-57). 1997. (CiteSeer)
- 2,3,4,5,9 次の収束公式がある

```
   bigpi 72
31415926535897932384626433832795028841971693993751
05820974944592307816406286208998628034825342117067
98214808651328230664709384460955058223172535940812
84811174502841027019385211055596446229489549303819
64428810975665933446128475648233786783165271201909145648...
```

3 微分と積分

3.1 積分

1. 所在

/math/misc/integral

2. 関数

`NB. integrate`	`Aitken extrapolation on Gauss integrals`
`NB. simpson`	`Simpson's method`
`NB. adapt`	`Adaptive Quadrature using Simpson's method`

3. 数式

$$I_i = \int_{xi-1}^{xi+1} f(x)dx \approx \frac{h}{3}(f_{i+1} + 4f_i + f_{i+1})$$

$$I \approx \frac{f}{3}(f_0 + 4\sum_{i=1}^{n} f_{2i-1} + 2\sum_{i=1}^{n-1} f_{2i} + f_{2n})$$