

剰余 (Residue) を巡って

SHIMURA Masato
<http://japla.sakura.ne.jp>

2015 年 9 月 11 日

目次

1	剰余	2
2	剰余の応用	2
3	剰余とガウスの合同式	5

はじめに

J 言語の `|` は次のように定義されている。

- 単項 絶対値 (Absolute)
- 両項 剰余 (Residue)

0.1 絶対値

1. 絶対値は 次の例で説明されることが多い。

*は `()Signam` でプラス、0、マイナスを判別する

```
i:3
_3 _2 _1 0 1 2 3
```

```
(| ; *) i:3
```

```

+-----+-----+
|3 2 1 0 1 2 3|_1 _1 _1 0 1 1 1|
+-----+-----+

```

2. 複素数の絶対値

$|3j4$
 5

複素数（2元数）の絶対値。 $(x,y) = 3,4$ と原点 0 との距離で、よく見ればピタゴラスである。

*1

1 剰余

剰余のみを求める

$3|i.7$
 $0\ 1\ 2\ 0\ 1\ 2\ 0$ NB. 剰余

$0= 3|i.7$
 $1\ 0\ 0\ 1\ 0\ 0\ 1$ NB. 3の倍数の位置

2 剰余の応用

2.1 ユークリッドの互除法

- $105x + 38y = 1$ を解け
- 次々と剰余を取る。 | は剰余のみを求める

*1 複素数の斜辺と偏角（ラジアン）

$*. 3j4$
 $5\ 0.927295$

```

38 | 105
29
(38 | 105) | 38
9
((38 | 105) | 38) | 29
2

```

- Script と解説

```
euc0=: ],|/@: (/:~@( _2&{.))
```

```

euc0 ^:(i.5) 105 38
105 38 0 0 0 0
105 38 29 0 0 0
105 38 29 9 0 0
105 38 29 9 2 0
105 38 29 9 2 1

```

- 続いて整数解を求める。

```

euc1 euc0 ^:(i.6) 105 38
2 1 3 4 2 _

```

- Script と解説

1. 後ろから 2 個の数を取り出し、小さい順にソートする

```

/:~ _2 {. 105 38
38 105

```

2. |/ で真ん中に | を挿入し、剰余を求める。/は (挿入)Insert

```

|/ /:~ _2 {. 105 38
29

```

3. 解を後尾に連結するに

```

( ], (|/ )@: (/:~ )@(_2 &{.)) 105 38
105 38 29

```

4. Tacit 型のループ ^:(i.6)

1. `{:` は最後尾を取り出す

```
a=: {: euc0 ^:(i.6) 105 38
105 38 29 9 2 1 0
```

2. 前後が重複した 2 個ずつの区切り

```
2<\ a
```

```
+-----+-----+-----+-----+-----+
|105 38|38 29|29 9|9 2|2 1|1 0|
+-----+-----+-----+-----+-----+
```

```
euc1=: 3 : ' <. 2%\ {: y'
```

明示型 (Explicit) で定義した。 `3:0` は
単項の動詞

3. `Box` の中に `%` を挿入する

は他の演算関数に置き換えるこ
とができる。この位置だと `L:0` は
不要

```
2(%/)\ a
```

```
2.76316 1.31034 3.22222 4.5 2 _
```

4. 端数切捨て `<.` 床 (Floor)

```
<. 2(%/)\ a
```

```
2 1 3 4 2 _
```

2.1.1 Script

NB. euclid Gojyohou

```
euc0=: ],|/@: (/:~@(_2&{.)
```

```
euc1=: 3 : ' <. 2%\ {: y'
```

```
NB. Usage:euc1 {: euc0 ^:(i.5) 105 38
```

2.1.2 連分数表示

$$\frac{105}{38} = 2 + \frac{1}{1 + \frac{9}{29}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{2}{9}}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}}$$

3 剰余とガウスの合同式

3.1 ガウスの合同式

ガウスの合同式を体現できる。

$$36 \equiv 6 \pmod{10}$$

両辺を 2 で割った $18 \equiv 3 \pmod{10}$ は成り立たない。 $18 \equiv 3 \pmod{5}$ である。

$$10 \mid 18 \ 3$$

8 3

$$5 \mid 18 \ 3$$

3 3

$$10 \mid 36 \ 6$$

6 6

林檎 5 個を買った場合と梨 3 個の場合のお釣りが同じだから林檎と梨は強い関連があるといわれても..

このような関係に拘り数学の体系を作ったガウスのこだわりと炯眼には敬意を払わなければならない。

3.2 ある有名な公式

-ある数の数字の和が 9 の倍数なら、その数は 9 の倍数である-

1. .

9 | 4906485 NB. 9 の倍数
0

(7#10) #: 4906485 NB. Antibase(\#:) で数を分離
4 9 0 6 4 8 5

+/ (7#10) #: 4906485 NB. 分離した数の合計
36

9 | 4906485 36 9 NB. さらに分離, 合計した 9 も含め 9 の倍数
0 0 0

2. n 多い数にも継承される

9 | 4906492 NB. 剰余は 7
7

(7 # 10) #: 4906402 NB. Antibase(#:) で数を分離
4 9 0 6 4 0 2

+/ (7 # 10) #: 4906492 NB. 分離した数の合計
34

7 = 3 + 4 NB. さらに分離した合計

9 | 7 34 4906492 NB. 3 つの数の剰余は同じ
7 7 7

3.3 乗算の剰余群

	7 */~ i.7
0	0 0 0 0 0 0 0
0	1 2 3 4 5 6
0	2 4 6 8 10 12
0	3 6 9 12 15 18
0	4 8 12 16 20 24
0	5 10 15 20 25 30
0	6 12 18 24 30 36

	7 */~ i.7
0	0 0 0 0 0 0 0
0	1 2 3 4 5 6
0	2 4 6 1 3 5
0	3 6 2 5 1 4
0	4 1 5 2 6 3
0	5 3 1 6 4 2
0	6 5 4 3 2 1

References

銀林 浩「初等整数論入門」ちくま文庫 2015