(2016/7/18)

拡張ユークリッド互除法

Extended Euclidean Algorithm

中野 嘉弘 (93 歳 6 ケ月、札幌市)

$ 1 はしがき

ユークリッドの互除法は、古来、「2 数の最大公約数 GCD」を求める手段として知られて居た。最近では、1 次不定式の解を求める方法として、有効な事で有名であるが、その話だけで、実際の使い方は、面倒くさいらしく、改めて、Yahoo 知恵袋の質問対象になって居て、最近は新潟大学の数学教室あたりから、この表題の如き、特別な解説が発行されて居て、一挙に計算を狙うほどである(文献 1)。

http://www2.cc.niigata-u.ac.jp/~takeuchi/tbasic/BackGround/ExEuclid.html

我々、J 言語研究グループとしても、多々、関係論文やコメント類で賑やかにお付き合いしているので(文献 4, 5, 6)、さらに、一筆を加えたく思う。J 言語は、カナダ産で、http://www.jsoftware.com から自由 DL 可能である。 尖閣諸島の向こう側の若者には好評だが、日本でも、慶応大理工学部(日吉)や会津大学さらに、文科省統計数理研究所辺りで同好であり、 英国からは、Vector の誌名で、有益な研究雑誌も出版されて居る。

先ず、話の糸口として、初歩的例題を 2 ケ述べよう。

① 2 数、2163 と 630 の最大公約数(GCD)を求めよ。

出典は文献 2 (岩波 数学入門辞典 p.619)で、解は、

2163 = 630*3 + 273 、 630 = 273*2 + 84 。
273 = 84*3 + 21、 84 =. 21* 4 。
∴ GCD = 21 である。

これを、我々馴染みの J 言語で演算すれば、

```
   2163 euclidnc0 630
2163
630

|2163|=|3|*|630|+|273|
|630|=|2|*|273|+|84|
|273|=|3|*|84|+|21|
|84|=|4|*|21|+|0|   。
```

ここに、| 21 | 等は絶対値と理解されたい。

② 5 リットルの枡と 2 リットルの枡を使って、1 リットルを
量ることが出来るか？

出典は文献１（新潟大学の資料を転用)で、解は、

```
 5 euclidna 2

 5 - 2 * 2 = 1 と、直解可能である。
```

これらから、発展する話題を提供しよう。

$ 2 １次不定式の整数解

前節＄1 の 例題②を、13 リットル枡と 5 リットル枡で実現する

にはと変更してみと 13X + 5Y = 1 の整数解を求めよとなる。

これが、新潟大学に資料内の原問題であるが、 私の解は、

```
 13 euclidna 5

|13|-|5|*|2| = |3| ①

 |5|-|3|*|1| = |2| ②

 |3|-|2|*|1| = |1| ③
```

ここで、|3|等は絶対値であると理解されよ。

最下の ③式の左辺の数 2 を消去する為に、その上式 ② の

右辺の数 2 の左辺の式を代入すれば、

```
 3 - ( 5 - 3 * 1)* 1 = 1  ③'  。
```

整理すれば、負数は記号アンダーバー付きで示す事ありとして、

```
 5 * (_1) + 3 * (1 + 1) = 1  即ち、

 5 * (_1 ) + 3 * 2 = 1  ③'' 。
```

この ③'' 式の左辺の数 3 を消去する為に、最上式 ① の右辺

の 3 の 左辺を代入すると、

5 * (_1) + (13 - 5* 2) * 2 = 1 ③''' 。

再び、整理すれば、

13 * 2 + 5 * (_1 + _2 * 2) = 1 即ち、

13 * (2)+ 5 * (_5) = 1 ③'''' 。

これを与題 13X + 5Y = 1 と 比較すれば、

整数解 (x, y) = (2 , _5) が得られる。

即ち、13リットルの枡で 2回 加法し、5リットルの枡で5回 減法

すれば、 1 リットルが残る事になる。

$ 3 複雑な問題では マトリックス の利用を ！

これは元来、志村正人氏の論文(文献3 等々) を参考にしたもの

である。

複雑な数値例、例えば

問題 3-1) 12707X + 12319Y = 1 の整数解を求めよ等では、

消去法が簡単には出来かねて、まごつきそうである？

長大数では、拡張精度多倍長指定 x: 付きで計算するのが良い。

x: 12707 euclidnc0 12319

12707 = 1 * 12319 + 388

12319 = 31* 388 + 291

388 = 1 + 291 +97

291 = 3 * 97 + 0

この後、肝腎なのは、上記の互除計算表中の、正則連分数の

行テキスト表現 RA = [1; 31, 1, 3] であって、この数値を、

2x2 行列の(1,1) 要素とするものを3ケ用意する。

m1 =. 2 2 $ 1 1 1 0、 m31=. 2 2 $ 31 1 1 0 、再び m1、

そして m3=. 2 2 $ 3 1 1 0 である。

行列の内積(inner prouct)操作を ip として、連合積 mRA =.

m1 ip m31 ip m1 ip m3 を作り、その値(行列式値) を求めると

det mRA = 131*32 - 33* 127 = 4192 - 4191 = 1 を得る。

これは即ち、 131X - 127Y = 1 ･･･(5) の整数解が

(32, 33) である事と同値である。

実は元来、 12707 = 97*131、 12319 = 97* 127 なので

(5) 式は、 12707X - 12319Y = 97*(131X - 127Y) = 97*1

と同じ意味なのである。

偶には、こう云う利点まで伴うが、一般に、複雑な計算が簡単に

実行可能になる長所を有して居る。

$ 4 むすび

このマトリックス計算法を、是非、ユークリッド互除法の拡張案

の内に取り入れたいものである。

文 献 ・ 資料

1)新潟大学数学教室:
http://www2.cc.niigata-u.ac.jp/~takeuchi/tbasic/BackGround/ExEuclid.html

2)岩波 数学入門辞典(2005) p.619

3) 志村正人: 剰余(Residue)を巡って
J 研報告 2015/9/11

4) 中野嘉弘: ユークリッド互除法と連分数と近似分数
J 研報告 2015/10/17

5) 中野嘉弘 : 連除法の決着法の例
J 研報告 2015/12/23 (予定だったが未刊)

6) 中野嘉弘: 連分数を電卓で計算する話
J 研報告 2016/6/25