

第 15 回目の主題 : ruby でプログラミング (3)

1. 今日すること

ruby で (拡張された) ユークリッドの互除法を実装せよ。そのプログラムと結果を verbatim を用いて TeX に取り込んで pdf ファイルを提出せよ。

- メール の 件名 は 「計算機数学レポート No.15」 .
- 提出 は pdf ファイル。
- 不明な点、うまくいかない点がある場合には、該当のファイルも添付していただくとありがたいです。

(拡張された) ユークリッドの互除法とは:

◎問題

与えられた整数 a, b に対して、その最大公約数 d と、

$$al + bm = d$$

を満たす整数 l, m を求めよ。

2. ヒントと問題

◎今回は ruby で行列を用いる。require "matrix" と書くことで行列が使えるようになる。

- 行列の成分は 0 行目や 0 列目、と 0 から数え始める。
- 和は +, 積は (maxima とは違って) *.

◎ ユークリッドの互除法 (初級)

$$v_0 = \begin{pmatrix} a \\ b \end{pmatrix}$$

に対して、 b を a で割った商を q , 余りを r とおく。

$$A(q) = \begin{pmatrix} -q & 1 \\ 1 & 0 \end{pmatrix}$$

とおくと、

$$v_1 = A(q)v_0 = \begin{pmatrix} r \\ a \end{pmatrix}$$

v_1 に対して同様な操作を行なう。これを繰り返すことにより、ベクトル v_0, v_1, \dots , を得る。これが互除法の操作と一致することを確認せよ。

○ ruby による $A(q)$ の実装例 (ruby では大文字小文字を区別する。ここでは小文字の変数や関数しか扱わないことにする。)

```
def amatrix(q)
  return(Matrix[[-q,1],[1,0]])
end
```

◎拡張されたユークリッドの互除法

$$v_0 = \begin{pmatrix} a \\ b \end{pmatrix}$$

から出発して、 $A(q)$ の形の行列をどんどん掛けることで、最終的に

$$\begin{pmatrix} 0 \\ d \end{pmatrix}$$

の形のベクトルを得るのが前の問題の趣旨であった。

今度は v_0 の他にもうひとつ単位行列 E をならべる。

$$B_0 = (v_0|E) = \left(\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array} \right)$$

a, b に $A(q)$ の形の行列を掛ける際に、後ろの行列にも同じ行列を掛ける。
これを何度か繰り返せば、

$$\left(\begin{array}{c|cc} 0 & p & q \\ \hline d & r & s \end{array} \right)$$

という行列を得る。これをうまく利用せよ。

プログラム例

```
require "matrix"
def amatrix(q)
  return(Matrix[[-q,1],[1,0]])
end

def gojoho(a,b)
  v=Vector[a,b]
  m=Matrix.I(2)          ###m の初期値は単位行列
  while (true)          ###無限ループ
    if (v[0]==0) then   ### == に注意。
      return([v[1],m]) ### v[0]=0 なら脱出
    end
    q1=v[1].div(v[0])
    m1=amatrix(q1)
    v=m1*v
    m=m1*m
  end
end

### 実行例
p gojoho(113,25)
```

最終問題: $a = 10^8 - 1$ と $b = 30^7$ とおくとき、 m, n の最大公約数 d と、 $ax + by = d$ を満たす整数の組 (x, y) の例をあげよ。