JAPLA 研究会資料 2019/6/22

Ｊによる平方剰余(Quadratic Residue)続き－整数論シリーズ４
ガウスの黄金定理 ＝ ふしぎびっくり定理

西川　利男

前回[1]は平方剰余への黄金の山への途中で一休みしてしまった。登り道の途中でいろいろな花が咲いているが、それを愛でることはさておいて、ベテランのガイドさんに従って上を目指して歩を進めることにする。

[1] 西川利男「Ｊによる平方剰余(Quadratic Residue)－整数論シリーズ３
－Ｊでの合同式演算、ルジャンドル表記を見やすくする－」

つまり、法則の証明はさておいて、数値で Legendre 記法の計算書式に慣れることから始める。ここでのガイドとなる教科書は前と同じ以下の本である。

[2] ジョセフ H. シルバーマン、鈴木治朗訳「はじめての数論」
ピアソンエデュケーション (2001).
[3] 金　重明「13 歳の娘に語るガウスの黄金定理」岩波書店(2013).
[4] 高木貞治「初等整数論講義、第２版」共立出版(1977).

１．ガウスの平方剰余の相互法則　[4] p.74-80

使用する法則をまとめて、記すことにする。

１．１　相互法則　ｐ とｑとは相異なる素数とする

$p \equiv 1 \bmod 4,\quad q \equiv 1 \bmod 4$　つまりpまたはqが$4n+1$型素数のとき

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

$p \equiv 3 \bmod 4,\quad q \equiv 3 \bmod 4$　つまりpもqも$4n+3$型素数のとき

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right)$$

相互法則(reciprocal law)などと言わずに
　ひっくり返し法則と言ったほうがよい。
さらに黄金則 (Golden Theorem, Theorema Aureum) ではなく
　ふしぎびっくり法則でよい。

１．２　第１補助法則

$p \equiv 1 \bmod 4$　pが$4n+1$型素数のとき

$$\left(\frac{-1}{p}\right) = 1$$

$p \equiv 3 \bmod 4$　pが$4n+3$型素数のとき

$$\left(\frac{-1}{p}\right) = -1$$

１．３　第２補助法則

$p \equiv 1 \bmod 8$ または $p \equiv 7 \bmod 8$

$$\left(\frac{2}{p}\right) = 1$$

$p \equiv 3 \bmod 8$ または $p \equiv 5 \bmod 8$

$$\left(\frac{2}{p}\right) = -1$$

１．４　積の法則

素数に限らず、一般の整数 a と b とに対して

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

１．５　オイラーの公式

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$$

２．数値による使用例

問１　365 は mod 2609 で平方剰余か？－文献[3] p.173 から

$$\left(\frac{365}{2609}\right)=\left(\frac{5\times 73}{2609}\right)=\left(\frac{5}{2609}\right)\times\left(\frac{73}{2609}\right)$$

$$\left(\frac{5}{2609}\right)=\left(\frac{2609}{5}\right)=\left(\frac{4}{5}\right)=\left(\frac{2}{5}\right)\times\left(\frac{2}{5}\right)=1$$

$$\left(\frac{73}{2609}\right)=\left(\frac{2609}{73}\right)=\left(\frac{54}{73}\right)=\left(\frac{2\times 3^3}{73}\right)=\left(\frac{2}{73}\right)\times\left(\frac{3}{73}\right)^3=1$$

したがって $\left(\frac{365}{2609}\right)=1$

問２　－506 は mod 3989 で平方剰余か？－文献[3] p.173 から

$$\left(\frac{-506}{3989}\right)=\left(\frac{-1}{3989}\right)\times\left(\frac{2}{3989}\right)\times\left(\frac{11}{3989}\right)\times\left(\frac{23}{3989}\right)$$

$$\left(\frac{-1}{3989}\right)=1$$

$$\left(\frac{2}{3989}\right)=-1$$

問　3

$$\left(\frac{11}{3989}\right)=\left(\frac{3989}{11}\right)=\left(\frac{7}{11}\right)=-\left(\frac{11}{7}\right)=-\left(\frac{4}{7}\right)=-\left(\frac{2}{7}\right)\times\left(\frac{2}{7}\right)=-1$$

$$\left(\frac{23}{3989}\right)=\left(\frac{3989}{23}\right)=\left(\frac{5}{23}\right)=\left(\frac{23}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1$$

したがって $\left(\frac{-506}{3989}\right)=1\times(-1)\times(-1)\times(-1)=-1$

37603 は mod 48611 で平方剰余か？－文献[2] p.157 から

$$\left(\frac{37603}{48611}\right)=\left(\frac{31}{48611}\right)\times\left(\frac{1213}{48611}\right)=-\left(\frac{48611}{31}\right)\times\left(\frac{48611}{1213}\right)=-\left(\frac{3}{31}\right)\times\left(\frac{91}{1213}\right)$$

$$=\left(\frac{31}{3}\right)\times\left(\frac{7}{1213}\right)\times\left(\frac{13}{1213}\right)=\left(\frac{1}{3}\right)\times\left(\frac{1213}{7}\right)\times\left(\frac{1213}{13}\right)=\left(\frac{2}{7}\right)\times\left(\frac{4}{13}\right)$$

$$=1$$

ガウスの平方剰余の判定法のポイントは、二乗した数の法の計算は、大きな数の場合には巨大な数の計算となる。それが相互法則を用いると、ひっくり返したものでごく簡単に得られる。たしかに、不思議なびっくり法則だ。なぜそうなるか、その証明は、高木の教科書[4] p. 74-80 を見られたらよい。

３．Ｊによる実行例

Ｊを用いれば、前回[1]に示した平方剰余判定の動詞 qr を用いて、次のようにたった一度の操作で求められる。

```
   365 qr 2609
1
   _506 qr 3989
_1
   37603 qr 48611
1
```

qr および関係する動詞の定義は、再記すれば以下のようになる。

```
NB. 平方剰余 Quadratic Residue ============================
sq_mod =: 3 : 0
:
y. | *: y. | x.
)

NB. Legendre Notation ==============
qr0 =: 3 : 0
(i. y.) e. (i. y.) sq_mod y.
)
zz =: <:`]@.]"(0)
NB.     zz 0 => _1
NB.     zz 1 => 1
NB.     zz 0, 1 => _1 1

qr =: 3 : 0
:
zz x. { qr0 y.
)
```

４．平方剰余相互法則と２次合同方程式の数値解

もう少し、実感を得るため、数値例により、平方剰余相互法則の結果を元に２次合同方程式を解いてみよう。

13 も 17 も 4n+1 型素数であるので、平方剰余相互法則によりルジャンドルの形式で、つぎのようになる。

$$\left(\frac{13}{17}\right)=\left(\frac{17}{13}\right)=1$$

これは、２次合同方程式

$x^2 \equiv 13 \pmod{17}$　と　$x^2 \equiv 17 \pmod{13}$

とに、解があることを示す。それでは、実際に解を求めてみる。

しかし、これらの合同式に多くの値を当てはめて解を求める計算を手で行うとなると、これは相当大変である。そこでＪでやってみよう。

(1)

$x^2 \equiv 13 \pmod{17}$

まず、100 までの整数の集合をつぎのようにつくる。

```
X100 =: i. 100
```

これらそれぞれを２乗して、mod 17 で剰余、100 個の値を Y17 としてつくる。

```
Y17  =: 17 | *: X100
```

X100 と Y17 との対応をＪの動詞 ,: により２行にまとめる。そして最初から 16 項までの部分を 16{. を取り出して示すと次のようである。なお 4j0″: は整数 4 桁出力のフォーマットである。

```
   4j0 ″: 16 {.″(1) X100 ,: Y17
   0    1    2    3    4    5    6    7    8    9   10   11   12   13   14   15   16
   0    1    4    9   16    8    2   15   13   13   15    2    8   16    9    4    1
```

２行目の値が 13 に等しいところの１行目のインデックスがすべて解になる。

最後にこの条件に合うものだけを取り出す。

```
   (13 = {:″(1)  X100 ,. Y17)#X100
8 9 25 26 42 43 59 60 76 77 93 94
```

このようにして、

x=8, x=9, x=25, x=26, ... x=93, x=94, ...

がこの合同方程式の解として得られる。

(2)

$x^2 \equiv 17 \pmod{13}$

この合同式は、考えてみるとちょっと変である。法13、つまり13で割った余りが17になるはずはない。

```
   Y13 =: 13 | *: X100
   4j0 ": 16 {."(1)X100,: Y13
0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15
0   1   4   9   3  12  10  10  12   3   9   4   1   0   1   4
```

平方剰余とは、それを含む類に含まれるかどうか、を示すものであろう。
そこで13 * 2 = 26を法としたものより、17となるものを取り出すようにした。

```
   YY13 =: 26 | *: X100
   4j0 ": 16 {."(1)X100,: YY13
0   1   2   3   4   5   6   7   8   9  10  11  12  13  14  15
0   1   4   9  16  25  10  23  12   3  22  17  14  13  14  17

   (17 = {:"(1)  X100 ,. YY13)#X100
11 15 37 41 63 67 89 93
```

つまり、

x=11, x=15, x=37, x=41, ... x=89, x=93, ...

がこの合同方程式の解として得られる。

たしかに、ガウスの平方剰余の相互法則は不思議であり、黄金則の名に値するものであろう。Jによる数値計算を通して、初めて分かりえた。

整数論のツールとして、Jの環境の強力な便利さをあらためて感じた。