JAPLA 研究会資料 2019/1/19

Ｊと Modulus(法)計算(ガウスの合同式)

西川　利男

別稿のテーマである整数論では法(modulus)による計算がポイントととなっている。これは、ガウスによる合同式(Congruence)とも呼ばれる。

整数論と言うと、日常とは離れたアカデミックな数学と思われているが、次のような「週の曜日の計算」や「時計の計算」である。

１．曜日の計算と合同式

今年１月のカレンダーを見てみる。

日	月	火	水	木	金	土
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

そこで、例えば、

1 日、8 日、15 日、22 日、29 日

は、火曜日になる。

これは

8-1、15-8、22-15、29-22

が、すべて 7 になることで、確かめられる。

また、いずれも 7 で割ると 1 余る。

これを、整数論では

$8 \equiv 1,\quad 15 \equiv 1,\quad 22 \equiv 1,\quad 29 \equiv 1$　そして $1 \equiv 1 \pmod 7$

と表し、法(modulus)による計算、あるいは合同式と呼んでいる。

そして、つぎの関係が成り立つ。

$A \equiv a \pmod p,\quad B \equiv b \pmod p$　であれば

$$A + B \equiv a + b \pmod p,\quad A - B \equiv a - b \pmod p,\quad A * B \equiv a * b \pmod p$$

すなわち、合同式は普通の演算式と同様に行える。つい見過ごされてしまいそうだが、ガウスにより始められたというこの合同式が、整数論の基本の第一歩になっている。

２．合同式計算のメリット

・1から100までの和を13で割った余りを求めよ。

1+2+3+ .. +100 = 5050であるから、5050÷13 = 388 余り 6

このようなことをしないで、つぎのようにする。

それぞれにmod 13をとり、その総和591について、さらにmod 13をとれば、答えは6となる。

・1から100までの積を13で割った余りを求めよ。

1*2*3* .. *100

こんな計算にたえるプログラム言語などそうはない！　やはり上と同様にして、まずそれぞれにmod 13をとる。

1 2 3 4 5 6 7 8 9 10 11 12 0 1 2 3 …

13、26などは割り切れるので余りは0になる。したがって、積は0である。

３．Ｊによる整数論の計算の大きな機能

Cをはじめとして通常のプログラミング言語で、法(modulus)の計算を備えているものは極めて少ない。BASICの演算子では、MODというのがあった。

Jではプリミティブ動詞 | として、modulus計算がごく容易に行える。

また、拡張数値x　およびプリミティブ動詞 x: が備えられている。

上の計算はJでは次のようになる。

```
   A =: }. i. 101
   A
1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  … 95  96  97  98  99
100
   B =: 13 | A
1  2  3  4  5  6  7  8  9  10  11  12  0  1  2  3  4  5  6  7 … 5  6  7  8  9
   +/ B
591
   13 | +/ B
6
   */ B
0
```

このように、Jの環境を用いてこそ、整数論数学が、容易に行われ、楽しむことが出来る、といえる。ちなみに、かってMS-DOS上で動くUBASICという整数論のための言語があって、筆者は愛用していたが、現在どうなったか。