計算機数学 NO.14

第 14 回目の主題：**ruby でプログラミング (2)**

1. 今日すること

ruby でプログラミングを行ない、正の数 a, b, m と (大きな) 数 n に対して、a^n を m で割ったあまりを計算する関数 $f(a, n, m)$ を作る。実際に実行してみてプログラムとその結果を verbatim を用いて TeX に取り込んで提出せよ。

◎アイディアその 1. $f(a, n, m) = a^n \mod m$ を求めるのに、わざと少し余分な c も考えて、$g(c, a, n, m) = ca^n \mod m$ を作る。($f(a, n, m) = g(1, a, n, m)$ である。)

◎アイディアその 2. べき指数 n を 2 でわって、$n = 2q + r$ と書くと

$$ca^n \mod m = (c \cdot a^r)(a^2)^q \mod m$$

2. ヒントと問題

◎レベル 5.

```
def torikae(a,b,n)
  r=n% 2                ### r は c を 2で割った余り
  if (r== 0 )
    a1=a
  else
    a1=a*b
  end
  b1=b^2
  n1=n/2
  return([a1,b1,n1])
end
```

上のように (正しく) 入力した後、`torikae(1,2,5)` を実行すると、何が得られるか?

◎利用例 (レベル 6)(レベル 5 の続きに書く。)

```
a,b,n=1,5,1000
while n>=1
  a,b,n=torikae(a,b,n)   ## このように変数をいっぺんに代入できる。
end
```

○一般に正の数 a, b, n を レベル 4 の torikae(a,b,n) で取り替えちゃった後でも ab^n の値は変わらないことを納得せよ。(納得するだけでいい。) その後、上のプログラムをうまく変えて ab^n を求めるプログラムを作れ。

◎最終問題 (レベル 7): $n = 10^{10} + 19$ のとき、$2^{(n-1)/2}$ を n で割ったあまりを求めよ。

ヒント: レベル 5 のプログラムの計算のいくつかのステップで、c, a を それぞれ $c\%m$, $a\%m$ で置き換えて扱う数をあまり大きくならないようにせよ：

なお、積ではなく和や差でも同様のことが成り立つ。

○付記:

ruby では、100/3 は 100 を「あまりを許した割り算」で 3 で割った商 (つまり 33) を指すのが標準の動作であるが、場合によっては (プログラム側で動作を指定することにより) 10/3 を分数 (33.333... と等しいアレ) と認識する場合もある。そのような場合、上で 10/3, n/2 などとある部分は、それぞれ `10.div(3)`, `n.div(2)` などと書いてやるとよい。