高校生のための現代数学講座
「素数」
講義 (3)　坪井　俊

東京大学
玉原国際セミナーハウス
2012 年 7 月 14 日

「便利な合同式」

1　余りによる合同式と加法、乗法

- **定義**
  m を 2 以上の整数とする。「2 つの整数 a_1 と a_2 が m を法として合同である」ことを「$a_1 - a_2$ が m で割り切れる」ことであると定義する。このとき、

$$a_1 \equiv a_2 \pmod{m}$$

  と書く。m を法として合同であることは、m で割った余りが同じであることと同値である。

- **例**
  $a_1 \equiv a_2 \pmod 2$ は、a_1, a_2 が、ともに偶数であるか、ともに奇数であることを表している。

- 整数 r に対して r を m で割った余りを r_0 とすれば、r_0 は、$r \equiv r_0 \pmod m$ であり $0 \leq r_0 \leq m-1$ を満たす整数である。
  一方、m 個の整数、$0, 1, \ldots, m-1$ は、どの 2 つも m を法として合同ではない。
  （$m+1$ 個以上の整数をとると、その中に合同な 2 つの整数を見つけることができる。）

- **例**
  5 を法とすると、任意の整数は 0, 1, 2, 3, 4 のどれか（1 つ）と合同である。

- **計算規則**
  a_1 と a_2 が m を法として合同、b_1 と b_2 が m を法として合同なら $a_1 + b_1$ と $a_2 + b_2$ が m を法として合同となる。差と掛け算についても上と同様のことが成り立つ。

$$\begin{cases} a_1 \equiv a_2 \pmod m \\ b_1 \equiv b_2 \pmod m \end{cases} \Longrightarrow \begin{cases} a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod m \\ a_1 b_1 \equiv a_2 b_2 \pmod m \end{cases}$$

- 従って、合同式の計算は、自分の好きな時に合同な整数に置き換えて計算するとよい。

- **例**
  $10 = -1 \pmod{11}$, $9 = -2 \pmod{11}$, ... だから、

$$\begin{aligned} 10! &\equiv 1 \times 2 \times \cdots \times 10 \pmod{11} \\ &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdot 3 \cdot (-3) \cdot 4 \cdot (-4) \cdot 5 \cdot (-5) \pmod{11} \\ &\equiv (-1)^5 \cdot 1 \cdot 4 \cdot 9 \cdot 16 \cdot 25 \pmod{11} \\ &\equiv (-1) \cdot 1 \cdot 4 \cdot (-2) \cdot 5 \cdot 3 \pmod{11} \\ &\equiv (-3) \cdot 4 \pmod{11} \\ &\equiv -1 \pmod{11} \end{aligned}$$

2 合同式における除法

- 整数の掛け算が $2 \times 3 = 6$ のように行われるとき、
  $6 \div 2 = 3$ あるいは $6 \div 3 = 2$ のように割り算がおこなわれる。
  余りのない割り算なので、
  $6/2 = 3$ あるいは $6/3 = 2$ のように書く方が良い。

- 掛け算が $2 \times 3 = 1 \pmod 5$ のように計算されるとすると、余りのない割り算が、
  $1/2 = 3 \pmod 5$ あるいは $1/3 = 2 \pmod 5$ のようにおこなわれると言って良い。
  余りのない割り算は、有理数における割り算と同じようなものである。

- **練習**
  mod 5 と mod 6 の掛け算の表を書いてみよう。

mod 5	0	1	2	3	4
0					
1					
2					
3					
4					

mod 6	0	1	2	3	4	5
0						
1						
2						
3						
4						
5						

- **観察**
  mod 5 の掛け算の表の縦の列、あるいは横の行に、1, 2, 3, 4 がすべて表れていることは、mod 5 の割り算「/」が、有理数のようにできることを表している。

- **観察**
  mod 6 の掛け算の表をみると、$2/3 \bmod 6$ は定義できないことがわかる。
  他の説明のしかたをすると、

  $$3 \times n = 2 \pmod 6$$

  を満たす整数 n があれば、ある整数 b で

  $$3n + 6b = 2$$

  を満たすものがあるはずである。左辺は 3 の倍数になり、2 は 3 の倍数ではないので、$3 \times n = 2 \pmod 6$ を満たす整数 $2/3 \bmod 6$ は存在しない。

- **問**
  $3/2 \bmod 6$ も定義できないことを説明せよ。

3 合同式の解き方

- 整数 m, a, c が与えられているとする。m を法とする合同式

  $$an \equiv c \pmod m$$

  は、

  $$an + bm = c$$

  を満たす整数 b が存在することと同値である。

- 左辺 $an+bm$ は、a と m の最大公約数 $d=\mathrm{GCD}(a,m)$ で割り切れるから、上の方程式の整数解 b が存在するためには、c は $d=\mathrm{GCD}(a,m)$ の倍数でなければならない。
- c が $d=\mathrm{GCD}(a,m)$ の倍数であるとする。

$$c=kd$$

ユークリッドの互除法により、$d=\mathrm{GCD}(a,m)$ に対しては、

$$an_0+b_0m=d$$

をみたす整数 n_0, b_0 が存在する。このとき、両辺を k 倍して、$n=kn_0$ が、$an+(kb_0)m=c$ を満たす。すなわち $an\equiv c\pmod m$ の解である。

- a と m の最大公約数が1、すなわち a と m が互いに素のとき、合同式 $an\equiv c\pmod m$ は、c の値によらず解を持ち、解は、m を法として一意的である。
一意的であるのは次のように示される。整数 n_1, n_2 を解とすると、

$$an_1+b_1m=c \quad \text{かつ} \quad an_2+b_2m=c$$

となる整数 b_1, b_2 が存在する。従って、

$$a(n_2-n_1)+(b_2-b_1)m=0$$

であるが、a と m は互いに素だから、n_2-n_1 は m で割り切れる。

- a と m が互いに素ではないときには、解は一意的ではない。例えば、$2n\equiv 2\pmod 6$ の解は、$n=1,4\pmod 6$ であり、$3n\equiv 3\pmod 6$ の解は、$n=1,3,5\pmod 6$ である。

- **問題**
鶴と亀がいる。足の数を合わせたものを9で割ると3余り、頭の数を合わせてものを9で割ると4余る。鶴の数は9で割ると何匹余るか？

- **問題**
m が素数であるとする。m の倍数ではない a に対し、合同式 $an\equiv c\pmod m$ は、整数 c の値によらず解を持ち、解は m を法として一意的であることを示せ。

4 冪についての合同式

- 2以上の自然数 n について、2乗 n^2, 3乗 n^3, 4乗 n^5, 5乗 n^5, ... を考えると、この数列は「指数的に」増大する。
n^k を自然数 m で割った余りを考えると $n^k\pmod m$ は面白い挙動をする。

- **例**
$m=21$ として、1行目の数 n を2乗して m で割った余りを2行目、1行目の数 n を3乗して m で割った余りを3行目、…というように書いていくと次を得る。

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
n^2	1	4	9	16	4	15	7	1	18	16	16	18	1	7	15	4	16	9	4	1
n^3	1	8	6	1	20	6	7	8	15	13	8	6	13	14	15	1	20	15	13	20
n^4	1	16	18	4	16	15	7	1	9	4	4	9	1	7	15	16	4	18	16	1
n^5	1	11	12	16	17	6	7	8	18	19	2	3	13	14	15	4	5	9	10	20
n^6	1	1	15	1	1	15	7	1	15	1	1	15	1	7	15	1	1	15	1	1
n^7	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

同様に、$m = 11$ として、

n	1	2	3	4	5	6	7	8	9	10
n^2	1	4	9	5	3	3	5	9	4	1
n^3	1	8	5	9	4	7	2	6	3	10
n^4	1	5	4	3	9	9	3	4	5	1
n^5	1	10	1	1	1	10	10	10	1	10
n^6	1	9	3	4	5	5	4	3	9	1
n^7	1	7	9	5	3	8	6	2	4	10
n^8	1	3	5	9	4	4	9	5	3	1
n^9	1	6	4	3	9	2	8	7	5	10
n^{10}	1	1	1	1	1	1	1	1	1	1
n^{11}	1	2	3	4	5	6	7	8	9	10

- **問**
  これらの縦の列が周期的になっているのはなぜか。

- $n, n^2, n^3, \ldots$ を m で割った余りを考えると、$0, \ldots, m-1$ の値しか取れないので、同じものが出てくる。すなわち、2つの異なる自然数 i, j $(i < j)$ に対し、$n^i = n^j \pmod m$ となる。
  ここで、n が m と互いに素であったとすると、合同式の解法で述べたように、合同式を n で割ることができる。従って、（n^i で割って）$n^{j-i} \equiv 1 \pmod m$ となる。
  すなわち、n が m と互いに素ならば、$n^x \equiv 1 \pmod m$ となる自然数 x が存在する。このとき $n^{x+1} \equiv n \pmod m$ となる。

5 電卓での計算と観察

- $\bmod m$ で冪の計算をするとき、整数 n に対し、$n^x = 1 \pmod m$ となる最小の x を n の**位数**と呼ぶことにする。n が m と互いに素でないときには位数は存在しない。

- いろいろな m に対して、$1, 2, \ldots$ の位数の表を作る。電卓で $n \div m$ の余りの計算をするには、n/m の整数部分を m 倍して、n を引き、符号を変えればよい。

- 以下の m を法とする n の位数の表を作れ。ただし、m と互いに素でない n については×を書くことにする。

- **例**　$m = 5$

n	1	2	3	4
位数	1	4	4	2

- **例**　$m = 6$

n	1	2	3	4	5
位数	1	×	×	×	2

- **問**　$m = 7$

n	1	2	3	4	5	6
位数	1					

- **問**　$m = 9$

n	1	2	3	4	5	6	7	8
位数	1		×			×		

- **問**　$m = 10$

n	1	2	3	4	5	6	7	8	9
位数	1								

- **問**　$m = 11$

n	1	2	3	4	5	6	7	8	9	10
位数	1									

- **問**　$m = 13$

n	1	2	3	4	5	6	7	8	9	10	11	12
位数	1											

- **問**　$m = 15$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
位数	1													

- **問**

(1)　m を法とする時に、n の位数として現れる数は、ある数の約数である。上の m についてその数を求めよ。

(2)　m が素数のとき、その数（n の位数の最小公倍数）はすぐにわかるか。

(3)　一般の m について、m の素因数分解と、その数（n の位数の最小公倍数）には関係があるか。

- 以下については、位数となる数を予想して、位数を計算せよ。

- **問**　$m = 17$

n	1	2	3	4	5	6	7	8	9
位数	1								

- **問**　$m = 19$

n	1	2	3	4	5	6	7	8	9
位数	1								

- **問**　$m = 21$

n	1	2	3	4	5	6	7	8	9
位数	1								

- **問**　$m = 23$

n	1	2	3	4	5
位数	1				

- **問**　$m = 101$

n	1	2	3	4	5
位数	1				

- **問**　$m = 11 \times 23 = 253$

n	1	2	3	4	5
位数	1				

- **問**　$m = 23 \times 47 = 1081$

n	1	2	3	4	5
位数	1				

6 冪の計算

- 3^{113} は、3 を掛ける操作を 112 回行うことで得られる数であり、

$$3^{113} = 8216782349860225013320438177913146043582421707992003 23$$

となる。
２進展開と冪の指数の計算法則を使うと計算の回数を減らすことができる。

- **冪の指数の計算法則**

$$a^x a^y = a^{x+y}, \quad (a^x)^y = a^{xy}$$

- **２進法**
113 を 2 進展開をすると次のようになる。

$$113 = (1110001)_2 = 2^6 + 2^5 + 2^4 + 1$$

- これを変形すると

$$113 = (((1 \times 2 + 1) \times 2 + 1) \times 2 \times 2 \times 2 \times 2 + 1$$

となる。

- 従って

$$3^{113} = (((((3^2 \times 3)^2 \times 3)^2)^2)^2)^2 \times 3$$

のように計算すると、２乗の操作を 6 回、3 をかける操作を 3 回行う、あわせて 9 回の操作で 3^{113} が計算できる。

- 通常の計算では、2 乗するとき桁数がおよそ倍になる。計算機などで計算をする場合、扱う最大の桁数を決めておくことが多い。このようなときには、m を法とする計算がきわめて有効である。

- m を法として計算では、

$$a^x \equiv b,\ a^y \equiv c \pmod{m} \Longrightarrow a^{x+y} \equiv bc \pmod{m}$$

$$a^x \equiv b \pmod{m} \Longrightarrow a^{xy} \equiv b^y \pmod{m}$$

である。

- 上の計算法則を使って計算するには、m の 2 倍の桁数を準備すればよい
（a は、$a \pmod{m}$ を使う）。

- 前の節で観察したことを基にすると、多くの m に対して、$a^k = 1 \pmod{m}$ あるいは $a^{k+1} = a \pmod{m}$ となる k があり、その値もわかる。

- **問**
$a^k = 1 \pmod{m}$ となる k について、
(1) $d \equiv 1 \pmod{k}$ ならば、$a^d \equiv a \pmod{m}$ となることを示せ。
(2) $uv \equiv 1 \pmod{k}$ かつ $b \equiv a^u \pmod{m}$ ならば、$b^v \equiv a \pmod{m}$ となることを示せ。