一次合同式と中国人の剰余定理

一次合同式

- 一次合同式：ax=b (mod q)の解の個数
  - 一般に、一次合同式は、d=(a,q)であるとき、d|bであるときにのみ解を持つ。解をもつとき、法qで相異なる解の個数はd個である。
  - まず最初に、d=1の場合（解が一つある）について説明する。
- 一次合同式の解き方（(a,q)=1とする）
  1. 1=sa+tq となる、s,tを拡張ユークリッドの互除法により求める
  2. ax=b (mod q)の両辺に1.で求めたsを掛けることで解が求まる。

     sax=sb (mod q) ⇒ x = sb (mod q)

     ∵1.において、sa-1=-tq であるので、合同式の定義より、
     sa=1 (mod q)である

一次合同式の解法（例）

- 8x=5 (mod 19) を解きなさい。
  - (8,19)=1であるので、この一次合同式は解を1つだけ持つ
  - 8と19について拡張ユークリッドの互除法を実行する

    19=8×2+3　　　1=-8+3×(19-8×2)=$\boxed{-7\times 8+3\times 19}$
    8=3×2+2　　　1=3-(8-3×2)=-8+3×3
    3=2×1+1　　　1=3-2×1
  - 従って、s=-7である。sを両辺に掛けて

    $\underbrace{(-7)\times 8}_{(=1)}\times x = (-7)\times 5 \pmod{19}$

    x = -35 (mod 19)　（x=-35でも間違いではないが、一般に合同式で
    x = 3 (mod 19)　　は0～nの範囲で解を表すので-35+19×2=3）
  - （確認）x=3を代入して、8×3=24=5 (mod 19)であるので正しい。

一次合同式の解法（一般の場合）

- 一次合同式$ax = b(mod\ q)$(式1）においては$d = (a, q)$とする。このとき、$a = a'd$、$q = q'd$とおけるから、これを一次合同式に代入すると、合同式の定義により、

$$a'dx - b = q'dt\ (t \in Z)$$

  が成り立つ。この両辺を比較すれば、$d|b$でなければ解をもたないことがわかる。$b = b'd$とおいて上式に代入し、両辺をdで割ると、$a'x = b'(mod\ q')$を得る。$(a', q') = 1$であるから、これは解が１つの場合に帰着する。この解を $x_0(0 < x_0 < q')$と する。このとき、$x = x_0 + q's\ (s \in Z)$　は、式１を満たすので式１の解である（代入して式１を満足することを確認してみよ）

一次合同式の解法（一般の場合、続き）

- 一次合同式$ax = b(mod\ q)$　の解は$x = x_0 + q's(s \in Z)$となる。
- 次に解の個数（sの範囲）を求める。いま、

$$x_0 + q's = x_0 + q's'(mod\ q)$$

とする。$q = q'd$なので、上式は$q's - q's' = q'dt\ (t \in Z)$を意味し、これは、$s = s'(mod\ d)$と同じことである。すなわち、$s = s'(mod\ d)$のとき、$x = x_0 + q's$と$x' = x_0 + q's'$は法$q$の下で同じ解となる。まとめると、一次合同式$ax = b\ (mod\ q)$の解は、$x = x_0 + q's\ (0 \leq s < d)$　となる。

一次合同式の解法（一般の場合、例）

- $24x = 15\ (mod\ 57)$　　（式2）を解く。
  $d = (24{,}57) = 3$　であり、$3|15$　なので、解は３つ存在する。
  式２の24, 15, 57をそれぞれd=3で割って

  $$8x = 5\ (mod\ 19)$$

  を得る。拡張ユークリッドの互除法により$12 \times 8 = 1\ (mod\ 19)$　なので、両辺に12を掛けて$x = 60 = 3\ (mod\ 19)$を得る。したがって、式２の一般解は、$x = 3 + 19s\ (s = 0{,}1{,}2)$　となる。
- $x = 3{,}22{,}41$　を式2に代入し、確認しよう。
  $x = 60$　も式2を満たすが、$60 = 3(mod\ 57)$　なので法57の下では3と同じ解であることに注意しよう。

連立一次合同式

$$\begin{cases} x = a_1 (\mathrm{mod}\ q_1) \\ x = a_2 (\mathrm{mod}\ q_2) \\ \vdots \\ x = a_m (\mathrm{mod}\ q_m) \end{cases}$$

- [中国人の剰余定理]
  連立一次合同式において、法$q_1, q_2, \cdots, q_m$が互いに素（どの2つの組み合わせでも互いに素）であるとき、$q = q_1 q_2 \cdots q_m$ を法として唯一つの解を持つ

- 中国人の剰余定理を使うと、大きな法$q = q_1 q_2 \cdots q_m$ の計算を小さな法$q_1, q_2, \cdots, q_m$ の計算に分けて行えるので便利

連立一次合同式の解法

1. $Q_1, Q_2, \cdots, Q_m$を以下のように決める
   $q=q_1Q_1=q_2Q_2=\cdots=q_mQ_m$
2. 以下の一次合同式を解いて、$t_1,t_2,\cdots,t_m$を求める
   $Q_it_i=1 \pmod{q_i}$ $(i=1,2,\cdots,m)$
3. この時、連立一次合同式の解xは以下で与えられる
   $x=a_1Q_1t_1+a_2Q_2t_2+\cdots+a_mQ_mt_m \pmod{q}$

これが解であることは、Step3のxを連立一次合同式の各式に代入することで確かめることができる。例えば、xを第1式に代入すると、
$Q_i=0 \pmod{q_1}$ $(i=2,3,\cdots,m)$なので、第2〜m項は全て0であり、
$Q_1t_1=1 \pmod{q_1}$であることより、$x=a_1 \pmod{q_1}$となる。

連立一次合同式（具体例）

$$\begin{cases} x = 2 \pmod 3 \\ x = 3 \pmod 5 \\ x = 2 \pmod 7 \end{cases}$$

を解きなさい。（法3,5,7は互いに素であるので、これは、q=3×5×7=105を法として唯一つの解を持つ）

1. $Q_1=q_2q_3=35$, $Q_2=q_1q_3=21$, $Q_3=q_1q_2=15$ となる
2. $35t_1=1 \pmod 3$, $21t_2=1 \pmod 5$, $15t_3=1 \pmod 7$を各々解いて、$t_1=2$, $t_2=1$, $t_3=1$を得る
3. 解x=2×35×2+3×21×1+2×15×1=23 (mod 105) となる

（確認）x=23を連立一次合同式の各式に代入すると、いずれも正しいことを確認できる。

合成数を法とする合同式の解

- 一般に、q　の素因数分解を$q = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$　とするとき、合同式$f(x) = 0 \ (mod\ q)$　は、連立合同式

$$\begin{cases} f(x) = 0 \ (mod\ p_1^{e_1}) \\ f(x) = 0 \ (mod\ p_2^{e_2}) \\ \vdots \\ f(x) = 0 \ (mod\ p_r^{e_r}) \end{cases}$$

  と同値である。
- 連立合同式の各式において解を求め、それらを連立一次合同式により合成することで法qにおける解を求められる。

前頁の証明

- $f(a) = 0\ (mod\ q)$　とすれば、$f(a) = 0\ \left(mod\ p_i^{e_i}\right)\ (i = 1,2,\ldots,r)$ である。なぜなら、一般に$s = t(mod\ dq')$　のとき、$s = t(mod\ q')$が言えるからである（証明してみよ）。
- 逆に、$f(a) = 0\ \left(mod\ p_i^{e_i}\right)\ (i = 1,2,\ldots,r)$ならば、$f(a) = 0\ (mod\ q)$　が言える。なぜなら、合同式の定義より、$p_i^{e_i}|f(a)(i = 1,2,\cdots,r)$　であり、これから $LCM\left(p_1^{e_1}, p_2^{e_2}, \cdots, p_r^{e_r}\right)|f(a)$　が言える。すなわち、$q|f(a)$　である。

例（合成数を法とする二次合同式）

- $x^2 = 1\ (mod\ 55)$　を解く。
  $55 = 5 \times 11$　であるので、$x^2 = 1\ (mod\ 5)$　と$x^2 = 1\ (mod\ 11)$の連立合同式を解けばよい。各式の解を代入により求めると、$x = 1{,}4\ (mod\ 5)$　および、$x = 1{,}10\ (mod\ 11)$である。これより
- $\begin{cases} x = 1\ (mod\ 5) \\ x = 1\ (mod\ 11) \end{cases}$` $\begin{cases} x = 1\ (mod\ 5) \\ x = 10\ (mod\ 11) \end{cases}$`
  $\begin{cases} x = 4\ (mod\ 5) \\ x = 1\ (mod\ 11) \end{cases}$` $\begin{cases} x = 4\ (mod\ 5) \\ x = 10\ (mod\ 11) \end{cases}$`
  の各一次合同式を解けばよい。

  これらを各々解いて、$x = 1, 21{,}34{,}54\ (mod\ 55)$　が解。
- 二次式だが、解が 4 つあることに注意しよう。
- 素数を法とする場合は、代入によらず効率的に平方根を求めるアルゴリズムが知られている。