アルゴリズム論特論　(塩田)

— Pohlig-Hellman 法実行例 —

問　$p = 109,\ g = 6,\ y = 67$ として $x = \log_g y = \log_6 67$ を求めよ。

もちろんこのような小さい数なら全検索でも一瞬で答えが出るが、Pohlig-Hellman 法を実行してみる。$x = \log_6 67$ は

$$p - 1 = 108 = 2^2 \times 3^3$$

を法とする数なので $x_2 = x \,\%\, 2^2$ と $x_3 = x \,\%\, 3^3$ を求められればあとは中国剰余アルゴリズムを使えばよい。

- 一般に $p-1$ の素因子べき q^e に対して $x_q = x \,\%\, q^e$ を求める手順は次の通り：

  1° $N = (p-1)/(q^e)$ とおく。
  2° $h = g^N$ を求める。
  3° y^N を求める。
  4° h のべき乗 h^a で y^N と一致するものを検索すると $x_q = a$ になる。

  $\because$　$x = x_q + q^e X$ とおけるので $NX = Nx_q + (p-1)X$ であり、フェルマの小定理から $y^N = (g^x)^N = (g^N)^{x_q} = h^{x_q}$. h の位数は q^e であるので $y^N = h^a$ となるべき指数 a が x_q に一致する。□

- $x_2 = x \,\%\, 2^2$ を求める。

  1° $q = 2$ なので $N = (p-1)/(2^2) = 27.$
  2° $h = g^N = 6^{27} \,\%\, 109 = 33.$
  3° $y^N = 67^{27} \,\%\, 109 = 76.$
  4° h のべき乗で $y^N = 76$ と一致するものを検索する：
  $$h^0 = 1, \quad h^1 = 33, \quad h^2 = 108, \quad h^3 = 76.$$
  従って $x_2 = 3.$

- $x_3 = x \,\%\, 3^3$ を求める。

  1° $q = 3$ なので $N = (p-1)/(3^3) = 4.$
  2° $h = g^N = 6^4 \,\%\, 109 = 97.$
  3° $y^N = 67^4 \,\%\, 109 = 73.$
  4° h のべき乗で $y^N = 73$ と一致するものを検索する：
  $$h^0 = 1, \quad h^1 = 97, \quad h^2 = 35, \quad \cdots, \quad h^{14} = 73.$$
  従って $x_3 = 14.$

- 中国剰余アルゴリズムを用いて連立合同式
  $$x \equiv x_2 = 3 \pmod{2^2}, \quad x \equiv x_3 = 14 \pmod{3^3}$$
  を解いて $x = 95.$

- 検算をしておくと $6^{95} \,\%\, 109 = 67.$ 御明算。

もうひと工夫

- $x_3 = x \,\%\, 3^3$ を 3 進数 $x_3 = (a_2a_1a_0)_3$ で表すと、次のように a_0, a_1, a_2 は長さ 3 のリストとの比較で順番に求めることができる。

- まず、
$$x = x_3 + 3^3X = (a_0 + 3a_1 + 9a_2) + 27X = a_0 + 3Y$$
とおけるので、$M = (p-1)/3 = 36$ とおくと
$$Mx = Ma_0 + (p-1)Y$$
従って
$$y^M = (g^x)^M = (g^M)^{a_0} \qquad (\ a_0 = 0, 1 \text{ or } 2\ )$$
実際に数を入れると、$M = 36$, $y^M = 67^{36} \,\%\, 109 = 45$. これとリスト
$$(g^M)^0 = 1, \quad (g^M)^1 = 63, \quad (g^M)^2 = 45$$
を比較して $a_0 = 2$ がわかる。

- $a_0 = 2$ がわかったので、
$$x = (2 + 3a_1 + 9a_2) + 27X = 2 + 3a_1 + 9Z$$
すなわち
$$x - 2 = 3a_1 + 9Z$$
とおける。今度は $M' = (p-1)/(3^2) = 12$ とおくと
$$M'(x-2) = M' \times 3a_1 + (p-1)Z = Ma_1 + (p-1)Z$$
従って
$$(yg^{-2})^{M'} = (g^{x-2})^{M'} = (g^M)^{a_1} \qquad (\ a_1 = 0, 1 \text{ or } 2\ )$$
実際に数を入れると、$M' = 12$, $(yg^{-2})^{M'} = (67 \times 91^2)^{12} \,\%\, 109 = 63$. これとリスト
$$(g^M)^0 = 1, \quad (g^M)^1 = 63, \quad (g^M)^2 = 45$$
を比較して $a_1 = 1$ がわかる。

- $a_0 = 2$, $a_1 = 1$ がわかったので、
$$x = (2 + 3 \times 1 + 9a_2) + 27X$$
すなわち
$$x - 5 = 9a_2 + 27X$$
とおける。今度は $M'' = (p-1)/(3^3) = 4$ とおくと
$$M''(x-5) = M'' \times 9a_2 + (p-1)X = Ma_2 + (p-1)X$$
従って
$$(yg^{-5})^{M''} = (g^{x-1})^{M''} = (g^M)^{a_2} \qquad (\ a_2 = 0, 1 \text{ or } 2\ )$$
実際に数を入れると、$M'' = 9$, $(yg^{-1})^{M''} = (67 \times 91^5)^4 \,\%\, 109 = 63$. これとリスト
$$(g^M)^0 = 1, \quad (g^M)^1 = 63, \quad (g^M)^2 = 45$$
を比較して $a_2 = 1$ がわかる。

- 以上から $x_3 = (112)_3 = 14$ がわかった。

- $x_2 = x \,\%\, 2^2$ についても、2 桁の 2 進数 $x_2 = (b_1b_0)_2$ として表して上と同様の方法で求めることができる。