問題解答 (2013.12.12 出題)

1. GCD$(x^5 - x^4 + x^2 - 1, x^5 - x^4 + x - 1)$ を求めよ.

   $f_1 = x^5 - x^4 + x^2 - 1$, $f_2 = x^5 - x^4 + x - 1$ とおくと $f_3 = f_1 \bmod f_2 = x^2 - x$, $f_4 = f_2 \bmod f_3 = x - 1$, $f_5 = f_3 \bmod f_4 = 0$ より GCD$(f_1, f_2) = x - 1$.

2. 連立方程式 $\begin{cases} f_1 = x^2 + xy + y^2 = 0 \\ f_2 = x^2 - y^2 + 1 = 0 \end{cases}$ を変形して $\begin{cases} x - h(y) = 0 \\ g(y) = 0 \end{cases}$ $(h(y),\ g(y)$ は y の多項式) の形にせよ.

   $x > y$ なる辞書式で考える. f_1, f_2 の先頭項はともに x^2 なので $f_3 = S(f_1, f_2) = f_1 - f_2 = xy + y^2 - 1$. $f_4 = S(f_1, f_3) = yf_1 - xf_3 = -xy^2 + x + y^3$ で, f_4 を f_3 で割ったあまりは $f_5 = f_4 + yf_3 = x + 3y^3 - y$ となる. よって $h(y) = -3y^3 + y$ とおけば $f_5 = x - h(y)$ の形となる. $x = h(y)$ を $f_2 = 0$ に代入すると, $g(y) = f_2(h(y), y) = 9y^6 - 6y^4 + 1$ となる.