

1  $f, g \in k[x]$  を入力として  $h, A, B$  ( $h = \text{GCD}(f, g), Af + Bg = h$ ) を出力するアルゴリズムを記述せよ

$f = qg + r$  という関係にあるとき, 行列を用いて

$$\begin{pmatrix} g \\ r \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} \quad (1)$$

という式が成り立つ.

ユークリッドの互除法をこの記法を用いて表現すると

$$\begin{pmatrix} h \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix}$$

となり,

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \quad (2)$$

を計算した結果が  $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$  となる.

これを Python で書くと以下のようなになる.

```
def calc(f, g):
    h, s = f, g
    A, B, C, D = 1, 0, 0, 1
    while not s == 0:
        quot = quotient(h, s)
        rem = remainder(h, s)
        h = s
        s = rem
        A, B, C, D = C, D, A - quot * C, B - quot * D

    return A, B
```

(NumPy を使うと実際に動くコードが書けるはずだが省略.)