2011年7月19日配布
2011年7月26日提出
2011年8月2日返却

1. $A = \mathbb{Z}/5\mathbb{Z}[x]$ の元 $a = x^4 + 2x^2 + 4x + 1$ と $b = x^3 + 4x^2 + 2$ に対して $d = \gcd(a, b)$ を求め、$sa + tb = d$ となる $s, t \in A$ を一組求めなさい。

解答

　a を b で割ると
$$a = (x+1)b + 3x^2 + 2x + 4. \tag{1}$$
次に、b を $3x^2 + 2x + 4$ で割ると
$$b = (2x)(3x^2 + 2x + 4) + 2x + 2 \tag{2}$$
次に、$3x^2 + 2x + 4$ を $2x + 2$ で割ると
$$3x^2 + 2x + 4 = (2x+2)(4x+2)$$
となるので、$\gcd(a, b) = x + 1$ であり、
$$\begin{aligned} x + 1 &= 3(2x+2) \\ &= 3(b - (2x)(3x^2 + 2x + 4)) && ((2)\ \text{より}) \\ &= 3b - x(3x^2 + 2x + 4) \\ &= 3b - x(a - (x+1)b) && ((1)\ \text{より}) \\ &= 4xa + (x^2 + x + 3)b. \end{aligned}$$
よって
$$s = 4x, \quad t = x^2 + x + 3$$
とすればよい。

2. $A = \mathbb{Z}/2\mathbb{Z}$ を係数とする多項式環 $A[x]$ において、$x^7 + 1$ を既約多項式の積に因数分解せよ。
$$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1).$$
実際、$x^3 + x + 1$ は既約である。なぜなら、既約でないとすると1次式で割り切れる。しかし1次式は x と $x+1$ しかなく、これらのどちらでも割り切れないからである。同様の理由で $x^3 + x^2 + 1$ も既約である。