BÀI TẬP TUẦN 6

Bài 1. Hãy chứng minh rằng đa thức x^2+1 là đa thức bất khả quy trên $\mathbb{Z}[x]$ nhưng khả quy (có thể phân tích được thành tích các đa thức bất khả quy) trên $\mathbb{F}_2[x]$.

Đa thức x^2+1 bất khả quy trên $\mathbb{Z}[x]$ bởi không tồn tại hai đa thức không khả nghich $f,g \in \mathbb{Z}[x]$ để $x^2+1 = f(x).g(x)$ (dễ thấy $x^2+1=(x+i)(x-i)$ những $x-i, x+i \notin \mathbb{Z}[x]$ bởi $i \notin \mathbb{Z}$)

Nhưng đa thức x^2+1 khả quy trên $\mathbb{F}_2[x]$ bởi $x^2+1=(x+1)(x-1)$ với $x+1 \in \mathbb{F}_2[x]$ và $x-1 \in \mathbb{F}_2[x]$

Bài 2. Sử dụng thuật toán Bezout, hãy chứng tỏ rằng hai đa thức x^2+2 và đa thức $x+1$ là nguyên tố cùng nhau trên vành đa thức $\mathbb{Z}[x]$ nhưng không nguyên tố cùng nhau trên vành đa thức $\mathbb{F}_3[x]$.

Đặt $f(x)=x^2+2, g(x)=x+1, d=gcd(f,g)$
Nhận thấy với thuật toán Euclid trên vành đa thức $\mathbb{Z}[x]$:

$$x^2+2=(x-1)(x+1)+3$$
$$x+1=0.3+(x+1)$$
$$3=0.(x+1)+3$$
$$x+1=0.3+(x+1)$$
$$3=0.(x+1)+3$$
$$x+1=0.3+(x+1)$$
$$3=0.(x+1)+3$$
$$......$$

Rõ ràng với 2 đa thức $f(x)$ và $g(x)$ làm cho thuật toán Euclid bị lặp vô tận trên $\mathbb{Z}[x]$ nên cũng không thể tính được với thuật toán Bezout.
Áp dụng thuật toán Bezout trên vành đa thức $\mathbb{F}_3[x]$

$$(f_0, g_0, d_0) = (1, 0, x^2+2)$$
$$(f_1, g_1, d_1) = (0, 1, x+1)$$

Vậy ước chung của $f(x)$ và $g(x)$ trên vành $\mathbb{F}_3[x]$ là: $x+1 \neq 1$ nên không phải là nguyên tố cùng nhau.

Bài 3. Áp dụng định lý thặng dư Trung Hoa trên vành đa thức $\mathbb{Q}[x]$, với $\mathbb{Q}$ là trường số hữu tỉ, hãy tìm đa thức $\mathbb{P}(x)$ thỏa mãn hệ sau:
a) $\begin{cases} P \equiv x^2+1 \pmod{x^3+2} \\ P \equiv 2x+3 \pmod{2x^2+3} \end{cases}$
b) $\begin{cases} P \equiv x+2 \pmod{x^2+1} \\ P \equiv x^2 \pmod{x^3+2} \end{cases}$

a) đặt $M=(x^3+2)(2x^2+3)=2x^5+3x^3+4x^2+6, n_1=2x^2+3, n_2=x^3+2$
Áp dụng thuật toán Bezout ta tính được:

$$n_1^{-1}=(2x^2+3)^{-1} \equiv \frac{-x\left(\frac{4x}{3}+\frac{16}{9}\right)}{2}+1 \pmod{x^3+2}$$
$$n_2^{-1}=(x^3+2)^{-1} \equiv \frac{4x}{3}+\frac{16}{9} \pmod{2x^2+3}$$

suy ra:
$x \equiv (x^2+1).n_1.n_1^{-1} + (2x+3).n_2.n_2^{-1} = (x^2+1)(2x^2+3)\left(\frac{-x\left(\frac{4x}{3}+\frac{16}{9}\right)}{2}+1\right) + (2x+3)(x^3+2)\left(\frac{4x}{3}+\frac{16}{9}\right)$
$= 41/3 + (112x)/9 + (25x^2)/3 + (8x^3)/9 + (56x^4)/9 + (8x^5)/9 - (4x^6)/3$
$\equiv (74x^4)/9 + (20x^3)/9 + (59x^2)/9 + (148x)/9 + 11 \pmod{2x^5+3x^3+4x^2+6}$

b) đặt $M = (x^2+1)(x^3+2) = x^5+x^3+2x^2+2, n_1 = x^3+2, n_2 = x^2+1$
Áp dụng thuật toán Bezout ta tính được:

$$n_1^{-1} = (x^3+2)^{-1} \equiv x+2 \pmod{x^2+1}$$

$$n_2^{-1} = (x^2+1)^{-1} \equiv -x(x+2)+1 \pmod{x^3+2}$$

suy ra:
$x \equiv (x+2).n_1.n_1^{-1} + x^2.n_2.n_2^{-1} = (x+2)(x^3+2)(x+2) + x^2(x^2+1)(-x(x+2)+1) = -x^6-x^5+4x^4+2x^3+3x^2+8x+8$
$\equiv 5x^4+5x^3+5x^2+10x+10 \pmod{x^5+x^3+2x^2+2}$

Bài 4. Hãy tính tích chập vòng của hai dãy sau lần lượt trên trường số thực $\mathbb{R}$ và trường hữu hạn $\mathbb{F}_7$.

$$a = (1,2,3) \text{ và } b = (4,5,6)$$

+) Tích chập vòng trên trường số thực $\mathbb{R}$:
$c_0 = a_0.b_0 + a_1.b_2 + a_2.b_1 = 1.4 + 2.6 + 3.5 = 31$
$c_1 = a_0.b_1 + a_1.b_0 + a_2.b_2 = 1.5 + 2.4 + 3.6 = 31$
$c_2 = a_0.b_2 + a_1.b_1 + a_2.b_0 = 1.6 + 2.5 + 3.4 = 28$

+) Tích chập vòng trên trường số thực $\mathbb{F}_7$:
$c_0 = a_0.b_0 + a_1.b_2 + a_2.b_1 = 1.4 + 2.6 + 3.5 = 31 = 3$
$c_1 = a_0.b_1 + a_1.b_0 + a_2.b_2 = 1.5 + 2.4 + 3.6 = 31 = 3$
$c_2 = a_0.b_2 + a_1.b_1 + a_2.b_0 = 1.6 + 2.5 + 3.4 = 28 = 0$

Vậy tích chập vòng trên trường số thực $\mathbb{R}$: $\{31, 31, 28\}$
Vậy tích chập vòng trên trường số thực $\mathbb{F}_7$: $\{3, 3, 20\}$

Bài 5. Trên vành đa thức $\mathbb{F}_3[x]$, cho hai đa thức

$$P(x) = 2x^3 + x + 1 \text{ và } Q(x) = x4 + 2x2 + 2.$$

Hãy sử dụng tích chập vòng để tính hệ số của đa thức $U(x)$ trên $\mathbb{F}_3$ với $U = PQ \pmod{x3-1}$

ta có:
$P(x) = 2x^3 + x + 1 \equiv x + 3 \pmod{x^3-1} = x$ (do $\mathbb{F}_3$)
$Q(x) = x^4 + 2x^2 + 2 \equiv 2x^3 + x + 2 \pmod{x^3-1}$
$P = (0,1,0)$
$Q = (2,1,2)$
Ta tính được: $Conv(P,Q) = (2,2,1)$
$U = PQ = 2 + 2x + x^2 \pmod{x^3-1}$