ÁLGEBRA II – VE1 — 24/04/2014
GABARITO

PROFESSOR MARCO

Exercício 1. (2 pts) Lembre que um intéiro $n \in \mathbb{Z}$ é dito *irredutível* se toda vez que n é escrito como $n = a \cdot b$, $a, b \in \mathbb{Z}$, logo a ou b são invertíveis em $\mathbb{Z}$ (isto é igualis a 1 ou -1). Prove que se um intéiro irredutível n divide um produto de intéiros $a_1 \cdot a_2 \cdots a_n$, logo n divide pelo menos um dos a_i's.

Solução: Escrevemos $a_1 \cdot a_2 \cdots a_n = p \cdot b$. Pelo teorema fundamental da aritmetica, todo intéiro possui uma fatoração em irredutíveis, que é única a menos de permutação. Logo a fatoração do produto $a_1 \cdot a_2 \cdots a_n$ é obtida juntando as fatorações de cada um dos a_i's. Tal fatoração deve ser a mesma fatoração do intéiro $p \cdot b$, onde aparece com certeza p como fator. Logo p aparece como fator em alguma das fatorações dos a_i's, i.e. p divide pelo menos um dos a_i's.

Exercício 2. (3 pts) Considere os seguintes polinómios em $\mathbb{Q}[x]$:

$$f(x) = x^4 + 1 \qquad \text{e} \qquad g(x) = 2x^3 - 2$$

(i) Encontre o $\text{MDC}(f, g) \in \mathbb{Q}[x]$ usando o algoritmo euclidiano e ache polinómios $\alpha(x)$ e $\beta(x)$ em $\mathbb{Q}[x]$ de forma que a seguinte identidade de Bézout seja satisfeita:

$$\alpha(x) \cdot f(x) + \beta(x) \cdot g(x) = \text{MDC}(f, g).$$

(ii) Seja p um primo impar e considere $f(x)$ e $g(x)$ como polinómios no anel $\mathbb{Z}_p[x]$. Encontre o $\text{MDC}(f, g) \in \mathbb{Z}_p[x]$.

Solução: (i) Vamos implementar o algoritmo euclidiano. Fazendo as divisões, obtemos:

$$f(x) = g(x) \cdot q_0(x) + r_0(x), \text{ onde } q_0(x) = \frac{1}{2} \cdot x \text{ e } r_0(x) = x + 1, \tag{0.1}$$

$$g(x) = r_0(x) \cdot q_1(x) + r_1(x), \text{ onde } q_1(x) = 2x^2 - 2x + 2 \text{ e } r_1(x) = -4, \tag{0.2}$$

$$r_0(x) = r_1(x) \cdot q_2(x) + r_2(x), \text{ onde } q_2(x) = -\frac{1}{4} \cdot r_0(x) \text{ e } r_2(x) = 0. \tag{0.3}$$

Como o último resto não nulo é $r_1(x) = -4$, logo o $\text{MDC}(f, g) = 1$.

Para encontrar a identidade de Bézout, escrevemos:

$$r_1(x) = g(x) - r_0(x) \cdot q_1(x) = g(x) - (f(x) - g(x) \cdot q_0(x)) \cdot q_1(x) =$$
$$= -q_1(x) \cdot f(x) + (1 - q_0(x) \cdot q_1(x)) \cdot g(x).$$

Logo temos

$$\text{MDC}(f, g) = -\frac{1}{4} \cdot r_1(x) = \frac{q_1(x)}{4} \cdot f(x) + \left(-\frac{1}{4} + \frac{q_0(x) \cdot q_1(x)}{4} \right) \cdot g(x).$$

Portanto os polinómios $\alpha(x)$ e $\beta(x)$ em $\mathbb{Q}[x]$ procurados são:

$$\alpha(x) = \frac{x^2}{2} - \frac{x}{2} + \frac{1}{2} \qquad \text{e} \qquad \beta(x) = \frac{x^3}{4} - \frac{x^2}{4} + \frac{x}{4} - \frac{1}{4}.$$

(ii) Seja p um primo impar. Como $2 \not\equiv 0 \bmod(p)$ e $4 \not\equiv 0 \bmod(p)$, logo as equações (0.1), (0.2) e (0.3) ainda são validas, onde $1/2$ e $1/4$ denotam os inversos de 2 e 4 em $\mathbb{Z}_p$. O último resto não nulo é mais uma vez $r_1(x) = -4$ e o $\mathrm{MDC}(f, g) = 1$.

Exercício 3. (3 pts) (i) Diga para quais valores de $a \in \mathbb{Z}$ o seguinte polinómio em $\mathbb{Z}[x]$ é irredutível sobre os racionais:

$$f(x) = 50x^7 - 7ax^4 + 14a^2x^2 + 28$$

(ii) Diga se os seguintes polinómios em $\mathbb{Z}_2[x]$ são irredutível sobre $\mathbb{Z}_2$

$$f(x) = x^5 + x^3 + x^2 + 1$$
$$g(x) = x^4 + x^3 + x^2 + x + 1$$

Solução: (i) Pelo teorema de Gauss, para provarmos que $f(x)$ é irredutível sobre $\mathbb{Q}$, basta provar que ele é irredutível sobre $\mathbb{Z}$. Para isso vamos aplicar o critério de Eisenstein. Temos que 7 não divide o coeficiente do termo lider do polinómio e divide todos os demais coeficientes de f. Além disso, 7^2 não divide o termo constante de f. Logo pelo critério de Eisenstein, f é irredutível para todo $a \in \mathbb{Z}$.

(ii) Temos que f possui a raiz $x = 1$ sobre $\mathbb{Z}_2$, logo pelo teorem de Ruffini o polinómio f é divisível por $x - 1$ sobre $\mathbb{Z}_2$. Em particular, $f(x)$ não é irredutível sobre $\mathbb{Z}_2$.

Note que $g(x)$ não possui raizes sobre $\mathbb{Z}_2$. Porém isto não garante que $g(x)$ seja irredutível sobre $\mathbb{Z}_2$, mas somente que $g(x)$ não tem fatores lineares (pelo teorema de Ruffini). Portanto, sabemos que se $g(x)$ fatora, logo é produto de dois polinómios de $\mathbb{Z}_2[x]$ de grau 2. Vamos então ver se é possível escrever

$$x^4 + x^3 + x^2 + x + 1 = (ax^2 + bx + c)(dx^2 + ex + f), \text{ com } a, b, c, d, e, f \in \mathbb{Z}_2.$$

Tomando os termos de grau quatro e zero, obtemos $ad = 1$ e $cf = 1$. Como os coeficientes estão em $\mathbb{Z}_2$, isto implica que $a = d = c = f = 1$. Tomando os termos de grau dois, obtemos $af + be + cd = 1$, isto é $1 + be + 1 = 1$, isto é $be = 1$, que implica também $b = e = 1$. Logo a fatoração seria

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + x + 1)^2$$

que é uma contradião pois o polinómio a direita é igual a $x^4 + x^2 + 1$.

Exercício 4. (2 pts) Responda as seguintes perguntas:

(i) Quais são os polinómios irredutíveis sobre $\mathbb{C}$? E sobre $\mathbb{R}$?

(ii) Qual é o enunciado do teorema de Gauss?

(iii) Prove ou disprove a seguinte afirmação, i.e. prove caso a afirmação seja verdadeira, ou encontre um contra-exemplo caso afirmação seja falsa:

Seja $f(x) \in \mathbb{Z}[x]$ e seja p um primo. Se a redução módulo p de $f(x)$ é redutível sobre $\mathbb{Z}_p$, logo $f(x)$ é redutível sobre $\mathbb{Z}$.

Solução: (i) Os únicos polinómios irredutíveis sobre $\mathbb{C}$ são os polinómios de grau 1. Os polinómios irredutíveis sobre $\mathbb{R}$ são aqueles de grau 1 e aqueles de grau 2 com invariante Δ negativo.

(ii) Teorema de Gauss: se um polinómio em $\mathbb{Z}[x]$ é produto de dois polinómios com coeficientes racionais, logo ele é produto de dois polinómios com coeficientes intéiros com os mesmos graus.

(iii) A afirmação é falsa: Por exemplo tome o polinómio $f(x) = x^p + p$. Pelo critério de Eisenstein, $f(x)$ é irredutível sobre $\mathbb{Z}$. Porem a redução módulo p de $f(x)$ é x^p, que é claramente um polinómio redutível.