2) Calcule:

d) $(3x^2+2x-4)+(4x^2+2)$ em $\mathbb{Z}_5$

$(7x^2+2x-2)$ em $\mathbb{Z}_5$

$(2x^2+2x-2)$ em $\mathbb{Z}_5$

e) $(3x^2+2x-4)(4x^2+2)\ \mathbb{Z}_5$

$12x^4+6x^2+8x^3+4x-16x^2-8$

$12x^4+8x^3+6x^2-16x^2+4x-8$

$(12x^2+8x^3-10x^2+4x-8)$ em $\mathbb{Z}_5$

$(2x^2+3x^3-0x^2+4x-3)$

$(2x^2+3x^3+4x-3)$ em $\mathbb{Z}_5$.

3) Use o algoritimo da divisão de Euclides para encontrar $q(x)$ e $r(x)$, sendo que $a(x)=q(x)b(x)+r(x)$ com grau $r(x)$ < grau $b(x)$.

a) $a(x)=5x^3+6x^2-3x+4$ e $b(x)=x-2$ em $\mathbb{Z}_7[x]$

$5x^3+6x^2-\underset{=4\in\mathbb{Z}_7}{3x}+4 \quad \underline{|x-\underset{=5\in\mathbb{Z}_7}{2}}$

$$
\begin{array}{l|l}
5x^3+6x^2+4x+4 & x+5 \\
\hline
-5x^3-4x^2 & 5x^2+2x+1 \\
\quad 2x^2+4x+4 & \\
\quad -2x^2-3x & \\
\qquad x+4 & \\
\qquad -x-5 & \\
\qquad\quad -1 \to -1+\underset{=6}{x}\equiv 0 \pmod 7 &
\end{array}
$$

$-1=6\in\mathbb{Z}_7$

, então:

$a(x)=q(x)b(x)+r(x)$

$\underbrace{5x^3+6x^2+4x+4}_{a(x)}=\underbrace{(5x^2+2x+1)}_{q(x)}\underbrace{(x+5)}_{b(x)}\underbrace{+6}_{r}$

8) Quais dos seguintes polinômios são irredutíveis sobre $\mathbb{Q}[x]$?

Critério de Eisenstein: Seja $f(x)=a_nx^n+\dots+a_1x+a_0\in\mathbb{Z}[x]$. Se existe um primo $p\in\mathbb{Z}$ tal que: $p|a_i$ para $i=0,\dots,n-1$, mas $p\nmid a_n$ e $p^2\nmid a_0$, então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

a) $x^4-2x^3+2x^2+x+4$, $a_nx^n=1x^4$ temos que $p\in\mathbb{Z}$ e com 1 é primo temos que $p=1$ ou $p\nmid 1$. Assim $p|a_i$ para $i=0,1,2,3$. Agora se $p\neq 1$ e $p>0\to p\nmid a_n$ e $p\nmid a_1$, logo não é irredutível em $\mathbb{Q}[x]$.

b) x^4-5x^3+3x-2, também não é irredutível em $\mathbb{Q}[x]$

c) $3x^5 - 4x^3 - 6x^2 + 6$

Temos que $p \nmid 3 \rightarrow p = 2$, assim $2|6$, $2|-6$, $2|-4$. Mas $2^2 \nmid 6$ logo é irredutível em $\mathbb{Q}[x]$.

d) $5x^5 - 6x^4 - 3x^2 + 9x - 15$

Temos que $p \nmid 5$, $\rightarrow p = 3$, assim $3|-15$, $3|9$, $3|-3$, $3|-6$. Mas $3^2 \nmid -15$.

Logo é irredutível em $\mathbb{Q}[x]$.

12) Se F é um corpo, mostre que $F[x_1, \ldots, x_n]$ é um domínio de integridade.

13) Mostre que o algoritmo da divisão não se mantém em $\mathbb{Z}[x]$. Porque ele falha?

Teorema 17.6: Algoritmo da divisão: Temos $f(x)$ e $g(x)$ sendo polinômios em $F[x]$, onde F é um corpo e $g(x)$ é um polinômio diferente de zero. Então existe um polinômio único $q(x), r(x) \in F[x]$ sendo que:

$$f(x) = g(x)q(x) + r(x),$$ onde qualquer $grau(r(x)) < grau(g(x))$ ou $r(x)$ é um polinômio zero.

Um domínio euclidiano (também chamado anel euclidiano) é um tipo de anel em que o algoritmo de Euclides pode ser usado, e temos que todo domínio euclidiano é um domínio de ideais principais, e também

14) Prove ou disprove: $x^p + a$ é irredutível para qualquer $a \in \mathbb{Z}_p$, onde p é primo.

Dado o polinômio $(x^p + a)$ e qualquer $a \in \mathbb{Z}_p$, afirmamos que (x^p+a) é irredutível para qualquer $a \in \mathbb{Z}_p$. Temos que a afirmação é falsa. Logo se tomarmos $a = 0$ e $0 \in \mathbb{Z}_p$, então $x^p + a = x^p + 0 = x^p$. Mas $x^p = x \cdot x^{p-1}$, onde x e x^{p-1} são não unidades, e x^p é irredutível. Por exemplo, se $p = 3$ então $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Então se $a = \bar{2}$ e $f(x) = x^3 + \bar{2}$

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}\} = \frac{\mathbb{Z}}{p} = \frac{\mathbb{Z}}{3}$$

Então $f(\bar{1}) = (\bar{1})^3 + \bar{2} = \bar{1} + \bar{2} = \bar{3} \equiv 0 \pmod 3$, assim $f(x)$ tem raiz em $\mathbb{Z}_3$ e então $x^3 + \bar{2}$ não é irredutível sobre $\mathbb{Z}_3$.

20) Polinômios ciclotômicos. O polinômio:

$$\Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + x + 1$$

É chamado de polinômio ciclotômico. Mostre que $\Phi_p(x)$ é irredutível sobre $\mathbb{Q}$ para qualquer primo p.

O polinômio $\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$, tomamos um p primo.

Afirmamos que $\Phi_p(x)$ é irredutível sobre $\mathbb{Q}$.

Seja $f(x) = \Phi_p(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \dots + \binom{p}{1}$

Temos que todo coeficiente exceto x^{p-1} é divisível por p e o termo constante não é divisível por p^2, pelo critério Eisenstein, $f(x)$ é irredutível sobre $\mathbb{Q}$. Então, se $\Phi_p(x) = g(x)h(x)$ é dita uma fatoração não trivial de $\Phi_p(x)$ sobre $\mathbb{Q}$, então $f(x) = \Phi_p(x+1) = g(x+1) \cdot h(x+1)$ deveria ser uma fatoração não trivial de $f(x)$ sobre $\mathbb{Q}$. De fato isto é impossível, assim concluímos que $\Phi_p(x)$ é irredutível em $\mathbb{Q}$.

24) Mostre que $x^p - x$ tem p distinto de zero em $\mathbb{Z}_p$, para qualquer primo p. Conclua que: $x^p - x = x(x-1)(x-2)\dots(x-(p-1))$.

Utilizando o pequeno teorema de Fermat temos que $a^{p-1} \equiv 1 \pmod{p}$, onde p é um primo que não divide a. Multiplicando ambos os lados por a,

$$a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p} \rightarrow a^p \equiv a \pmod{p}$$

Este resultado também é verdadeiro se p divide a, então:

$$a^p \equiv a \pmod{p} \quad \forall a \rightarrow a^p - a \equiv 0 \pmod{p} \quad (I)$$

Assim para qualquer $a \in \mathbb{Z}_p$, temos que a é uma raiz da equação de $x^p - x$ em $\mathbb{Z}_p$.

Como $\mathbb{Z}_p$ tem p elementos distintos de zero $\{0, 1, \dots, p-1\}$ para qualquer p, e todos elementos satisfazem (I). Então, $(x^p - x)$ tem p elementos distintos de zero em $\mathbb{Z}_p$ para qualquer primo p.

Assim dividindo por x, temos que $(1, \dots, p-1)$ são todas raízes da equação $(x^{p-1} - 1)$ sobre $\mathbb{Z}_p$, então elas são fatores como:

$$(x-1)(x-2)\dots(x-(p-1)) \text{ em } \mathbb{Z}_p[x]$$

26) Temos que F é um corpo. Mostre que $F[x]$ nunca é um corpo.

Tomamos $p(x) = x \in F[x]$ então se $F[x]$ é um corpo, temos seu inverso em $g(x) = x^{-1}$, assim $p(x) \cdot g(x) = x \cdot x^{-1} = 1 \in F[x]$. Mas $g(x) = x^{-1}$ não é um polinômio, com isso temos uma contradição. E $p(x)$ não é unidade, portanto, $F[x]$ não pode ser um corpo.