1. Find a greatest common divisor d of the polynomials

$$f = x^5 + 3x^4 + 3x^3 + 4x + 3 \quad \text{and} \quad g = 2x^3 + 2x^2 + x + 4$$

in the ring $\mathbb{Z}_5[x]$ as well as polynomials $u, v \in \mathbb{Z}_5[x]$ such that $d = uf + vg$.

1)

$$x^5 + 3x^4 + 3x^3 + 4x + 3 \;\big|\; 2x^3 + 2x^2 + x + 4$$
$$-\; x^5 + x^4 + 3x^3 + 2x^2 \;\big|\; 3x^2 + x + 4 \,/ q_1$$
$$2x^4 + 3x^2 + 4x + 3$$
$$-\; 2x^4 + 2x^3 + x^2 + 4x$$
$$3x^3 + 2x^2 + 3$$
$$-\; 3x^3 + 3x^2 + 4x + 1$$
$$4x^2 + x + 2 \,/ r_1$$

Notice $a = a \% 5$

Thus $6x^5 \to x^5$

$-2x^2 \to 3x^2$ and so on

Check: $(3x^2+x+4)(2x^3+2x^2+x+4) + 4x^2+x+2 = 6x^5 + 8x^4 + 13x^3 + 25x^2 + 9x + 18$

$$\Updownarrow \mathbb{Z}_5$$

$$x^5 + 3x^4 + 3x^3 + 4x + 3$$

So $f = q_1 g + r_1 \Rightarrow \gcd(f,g) = \gcd(r_1, g)$

2)

$$2x^3 + 2x^2 + x + 4 \;\big|\; 4x^2 + x + 2$$
$$-\; 2x^3 + 3x^2 + x \;\big|\; 3x + 1 \,/ q_2$$
$$4x^2 + 4$$
$$-\; 4x^2 + x + 2$$
$$4x + 2 \,/ r_2$$

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

$= 12x^3 + 7x^2 + 11x + 4 \equiv 2x^3 + 2x^2 + x + 4$

3)

$$4x^2 + x + 2 \;\big|\; 4x + 2$$
$$-\; 4x^2 + 2x \;\big|\; x + 1 \,/ q_3$$
$$4x + 2$$
$$-\; 4x + 2$$
$$0 \,/ r_3$$

check: $(4x+2)(x+1) + 0 = 4x^2 + 6x + 2 \equiv 4x^2 + x + 2$

Thus $\gcd(f,g) = r_2 = 4x + 2$

b. $4x + 2 \equiv g - (3x+1)(4x^2+x+2)$

$\equiv g - (3x+1)(f - g(3x^2+x+4))$

$\equiv g - f(3x+1) + g(3x^2+x+4)(3x+1)$

$\equiv f\underbrace{(2x+4)}_{u} + g\underbrace{(4x^3+x^2+3x)}_{v}$

If it's required to be monic, multiply RHS and LHS by 4:

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

2. Find explicit formulas for an isomorphism below and its inverse

$$\mathbb{R}[x]/(2x^2+3x-2) \simeq \mathbb{R} \times \mathbb{R}$$

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

So $\mathbb{R}[x](2x^2+3x-2) \simeq \mathbb{R}[x](x+2) \times \mathbb{R}[x](2x-1)$

$\forall f_1 \deg(x) < 1$

this is obviously isomorphic to $\mathbb{R}\times\mathbb{R}$

So, $\varphi : f \bmod 2x^2+3x-2 \mapsto (f \bmod \underset{g}{\underset{\shortparallel}{x+2}}, f \bmod \underset{h}{\underset{\shortparallel}{2x-1}})$

$$\varphi^{-1}(pq) = p \cdot \varphi^{-1}(1,0) + q\,\varphi^{-1}(0,1)$$

$\gcd(x+2, 2x+1) = 1 \Rightarrow 1 = \overset{2/5}{u}(x+2) + \underset{-1/5}{v}(2x-1) \Rightarrow$

$\Rightarrow \varphi^{-1}(pq) = p\cdot vh + qug \pmod{g\cdot h}$

$$\varphi^{-1}(pq) = -\frac{1}{5}(2x-1)p + \frac{2}{5}(x+2)q \pmod{2x^2+3x-2}$$

3. Find all monic irreducible polynomials of degree 2 and 3 over the field $\mathbb{Z}_3$. Compute the number of monic irreducible polynomials of degree 4.

let's just list all monic polynomials of deg 2 ∧ 3 over $\mathbb{Z}_3$:

x^2 $\{0\}$ | x^2+x $\{0\}$ | x^2+2x $\{0\}$

x^2+1 | x^2+x+1 $\{1\}$ | x^2+2x+1 $\{2\}$

x^2+2 $\{1\}$ | x^2+x+2 | x^2+2x+2

Thus (x^2+1), (x^2+x+2), (x^2+2x+2) are monic irreduceable pol.

2. monic of deg 3 can not have fre term, since 0 will be the root, it's reduceable by x.

1. x^3+1 $\{2\}$
2. x^3+2 $\{1\}$
3. x^3+x+1 $\{1\}$
4. x^3+x+2 $\{2\}$
5. x^3+2x+1
6. x^3+2x+2
7. x^3+x^2+1 $\{1\}$
8. x^3+x^2+2
9. x^3+x^2+x+1 $\{2\}$
10. x^3+x^2+x+2
11. x^3+x^2+2x+1
12. x^3+x^2+2x+2 $\{2,1\}$
13. x^3+2x^2+1
14. x^3+2x^2+2 $\{2\}$
15. x^3+2x^2+x+1
16. x^3+2x^2+x+2 $\{1\}$
17. x^3+2x^2+2x+1 $\{1,2\}$
18. x^3+2x^2+2x+2

Thus there 8 monic irr. pol. over $\mathbb{Z}_3$ with deg. = 3:

- x^3+2x+1
- x^3+2x+2
- x^3+x^2+2
- x^3+x^2+x+2
- x^3+x^2+2x+1
- x^3+2x^2+1
- x^3+2x^2+x+1
- x^3+2x^2+2x+2

notice that x, $x+1$, $x+2$ are irr

Thus we have $3\,p_1$, $3\,p_2$ and $8\,p_3$

There are $3^4 = 81$ monic polynomials of deg 4 over $\mathbb{Z}_3$:

let denote them f, thus it can be in the form: (p_i is irr. pol of degre i)

$$\left.\begin{array}{ll} 1)\ f = p_1 \cdot p_1 \cdot p_1 \cdot p_1 & \to 12 \\ 2)\ f = p_2 \cdot p_1 \cdot p_1 & \to 18 \\ 3)\ f = p_3 \cdot p_1 & \to 24 \\ 4)\ f = p_2 \cdot p_2 & \to 9 \end{array}\right\} \Rightarrow 66 \Rightarrow 81-63 = 18$$

irreduciable monic pol. of deg. 3 in $\mathbb{Z}_3$

$$x^2+2 \equiv 0 \pmod{x^2+2} \Rightarrow x^2 \equiv -2 \Rightarrow x^2 \equiv 1$$

4. Find all invertible elements in the ring $\mathbb{Z}_3[x]/(x^2+2)$. For each invertible element compute its inverse.

$$\mathbb{Z}_3[x](x^2+2) = \{ax+b \mid a,b \in \mathbb{Z}_3\}$$

list all polynomials:

$1 \quad 2 \quad x \quad 2x$

$\underline{x+1} \quad x+2 \quad 2x+1 \quad 2x+2$

Thus 1 is invertible, and it's inverse is 1

2 is also invertible, inverse is 2 $(2 \cdot 2 = 4 \equiv 1 \pmod 3)$

$(x)(x) = x^2$, $x^2 \equiv 1 \pmod{x^2+2} \Rightarrow x$ is inv.

$(2x)(2x) = 4x^2 \equiv x^2 \equiv 1 \pmod{x^2+2} \Rightarrow 2x$ is inv.

$$\left.\begin{array}{l} (1+x)(2+2x) = 2x^2+4x+2 \equiv 2+4x+2 \equiv x \not\equiv 1 \\ (1+x)(1+x) = x^2+2x+1 \equiv 1+2x+1 \not\equiv 1 \\ (1+x)(2x+1) = 2x^2+3x+1 \equiv 2+3x+1 \equiv 0 \not\equiv 1 \\ (1+x)(x+2) = x^2+3x+2 \equiv 1+3x+2 \equiv 0 \not\equiv 1 \end{array}\right\} \Rightarrow (1+x) \text{ is not inv.}$$

we dont need to check 1, 2, x, 2x, since they already have their inverses.

$$\left.\begin{array}{l} (x+2)(x+2) = x^2+4x+4 \equiv 1+x+1 \equiv x+2 \not\equiv 1 \\ (x+2)(2x+1) = 2x^2+5x+2 \equiv 2+2x+2 \equiv x+2 \not\equiv 1 \\ (x+2)(2x+2) = 2x^2+6x+4 \equiv 2+1 \equiv 0 \not\equiv 1 \end{array}\right\} \Rightarrow (x+2) \text{ is not inv.}$$

$$\left.\begin{array}{l} (2x+1)(2x+1) = 4x^2+4x+1 \equiv 4+x+1 \equiv x+2 \not\equiv 1 \\ (2x+1)(2x+2) = 4x^2+6x+2 \equiv 1+2 \equiv 3 \equiv 0 \not\equiv 1 \end{array}\right\} \Rightarrow (2x+1) \text{ isn't inv.}$$

$(2x+2)(2x+2) = 4x^2+8x+4 \equiv 1+2x+1 \equiv 2x+2 \not\equiv 1 \Rightarrow (2x+2)$ isn't inv.