4 pratybos.

Didžiausias bendras daliklis.Polinomų bekvadratė faktorizcija.

Veiksmai $K[x]/(m(x))$.

Bekvadratės faktorizacijos algoritmas.

$f_0(x) := f(x)$, *skaičiuojame* $f_0'(x)$.

$f_1(x) :=BDD(f_0, f_0')$, *skaičiuojame* $f_1'(x)$.

$f_2(x) :=BDD(f_1, f_1')$, *skaičiuojame* $f_2'(x)$.

$f_3(x) :=BDD(f_2, f_2')$, *skaičiuojame* $f_3'(x)$ *ir t.t.*

$g_{\geq 1}(x) := \dfrac{f_0(x)}{f_1(x)},$

$g_{\geq 2}(x) := \dfrac{f_1(x)}{f_2(x)},$

$g_{\geq 3}(x) := \dfrac{f_2(x)}{f_3(x)},$ *ir t.t.*

$F_1(x) := \dfrac{g_{\geq 1}(x)}{g_{\geq 2}(x)},$

$F_2(x) := \dfrac{g_{\geq 2}(x)}{g_{\geq 3}(x)},$

$F_3(x) := \dfrac{g_{\geq 3}(x)}{g_{\geq 4}(x)},$ *ir t.t.*

Taigi, $f(x) = a_n F_1(x) F_2^2(x) \cdots F_k^k(x)$, *čia* F_i *- bekvadračiai polinomai.*

Tam kad kūne $K[x]/(m(x))$, *čia polinomas* $m(x)$ *- neredukuojamas, galėtume rasti nenuliniam polinomui* $f(x)$ *atvirkštinį elementą reikia polinomų porai* $f(x)$ *ir* $m(x)$ *rasti tokius polinomus* $q(x)$ *ir* $r(x)$, *kad* $f(x)q(x) + m(x)r(x) = 1$. *Tada* $q(x) = f^{-1}(x) \bmod m(x)$.

1. Euklido algoritmo pagalba raskite didžiausią bendrą daliklį $d(x)$.Parašykite $d(x)$ tiesinę išraišką.

1) $d(x) =$DBD$(x^8 - 1, x^6 - 1) \in \mathbf{Q}[x]$.

2) $d(x) =$DBD$(x^4 + x^3 + 2x^2 + x + 1, x^3 - 1) \in \mathbf{Q}[x]$.

3) $d(x) =$DBD$(2x^4 - x^3 + x^2 + 3x + 1, 2x^3 - 3x^2 + 2x + 2) \in \mathbf{Q}[x]$.

4) $d(x) =$DBD$(x^7 + 2x^5 + 2x^2 - x + 2, x^6 - 2x^5 - x^4 + x^2 + 2x + 3) \in \mathbf{Q}[x]$.

5) $d(x) =$DBD$(x^7 + 1, x^5 + x^3 + x + 1) \in \mathbf{Z}_2[x]$.

6) $d(x) =$DBD$(x^5 + x + 1, x^6 + x^5 + x^4 + 1) \in \mathbf{Z}_2[x]$.

7) $d(x) =$DBD$(x^5 + x + 1, x^6 + x^5 + x^4 + 1) \in \mathbf{Z}_2[x]$.

8) $d(x)=$DBD$(x^8+2x^5+x^3+x^2+1, 2x^6+x^5+2x^3+2x^2+2) \in \mathbf{Z}_3[x]$.

2. Ar polinomai su racionalaisiais koeficientais $2x^3-2x^2-3x+1$ ir $2x^2-x-2$ yra tarpusavyje pirminiai?

3. Atlikite bekvadratę polinomo faktorizaciją.
1) $4x^5-15x^3+5x^2+15x-9$;
2) $8x^5+4x^4-22x^3-29x^2-13x-2$;
3) $2x^6+6x^5+6x^4+x^3-3x^2-3x-1$;
4) $x^5-6x^4+16x^3-24x^2+20x-8$;
5) $2x^5+3x^4+4x^3+x^2-1$;
6) $x^7-3x^6+5x^5-7x^4+7x^3-5x^2+3x-1$.

4. 1) Įrodykite, kad polinomas x^2+1 yra neredukuojamas virš kūno $\mathbf{Z}_3$.
2) Parašykite visus kūno $\mathbf{Z}_3[x]/(x^2+1)$ elementus.
3) Parašykite daugybos lentelę kūne $\mathbf{Z}_3[x]/(x^2+1)$.
4) Parodykite, kad visi *nenuliniai* kūno $\mathbf{Z}_3[x]/(x^2+1)$ elementai yra elemento $[x+1]$ laipsniai, bet ne visi kūno $\mathbf{Z}_3[x]/(x^2+1)$ elementai yra elemento $[x]$ laipsniai.

5. Atlikite veiksmus faktoržiede $\mathbf{Q}[x]/(m(x))$.
1) $(x^2+x+1)^2$, $m(x)=x^3-1$.
2) $\dfrac{x+2}{x-2}$, $m(x)=x^3+x+1$.
3) $\dfrac{1}{x^2+x+1}$, $m(x)=x^3-2$.

6. Raskite $(x+1)^{-1}$ faktoržiede $Z_2[x]/(x^3+x+1)$.

7. Raskite x^2+x+1 atvirkštinį elementą
1) faktoržiede $\mathbf{Q}[x]/(x^3-2)$,
2) faktoržiede $\mathbf{Z}_3[x]/(x^3+2x^2+x+1)$.

8. Faktoržiede $\mathbf{Z}_3[x]/(x^3+x+1)$ raskite x^{-1} ir $(x+1)^{-1}$ ir panaudoję tai raskite $(x^2+x)^{-1}$.