

Jméno:

Místnost:

2. vnitrosemestrální písemka

4444

list

|

učo

body

Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.

0 1 2 3 4 5 6 7 8 9

Určete všechny komplexní kořeny polynomů p a q , jestliže víte, že mají společný kořen. Dále tyto polynomy rozložte na součin ireducibilních polynomů nad \mathbb{C} , \mathbb{R} , \mathbb{Z} .

Příklad 1
15 bodů

$$p(x) = x^4 - 4x^3 + 5x^2 - 16x + 4, \quad q(x) = x^4 - 3x^3 - 4x^2 + 5x - 1.$$

Jméno:

Místnost:

2. vnitrosemestrální písemka

4444

list

2

učo

body

Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.

0 1 2 3 4 5 6 7 8 9

Určete všechny komplexní kořeny polynomu $f(x) = x^5 + 5x^4 + 9x^3 + 9x^2 + 5x + 1$.

Příklad 2
10 bodů

Jméno:

Místnost:

2. vnitrosemestrální písemka

4444

list

3

učo

body

Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.

0 1 2 3 4 5 6 7 8 9

Definujme zobrazení $f : (\mathbb{Z}_6, +) \rightarrow (\mathbb{C}^*, \cdot)$ vztahem $f([a]_6) = \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^a$.

Příklad 3
15 bodů

1. Dokažte, že je f skutečně zobrazení.
2. Dokažte, že je f homomorfismus grup.
3. Rozhodněte, zda je f injektivní. Své tvrzení dokažte.
4. Rozhodněte, zda je f surjektivní. Své tvrzení dokažte.

Jméno:

Místnost:

2. vnitrosemestrální písemka

4444

list

4

učo

body

Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.

0123456789

Amálka zvolila za parametry v kryptosystému ElGamal $p = 11$; $g = 7$, za svůj soukromý klíč zvolila $x = 5$ a zveřejnila veřejný klíč $(p; g; g^x)$. Ukažte, jak Bob zašifruje zprávu $m = 9$ určenou Amálce.

Příklad 4
10 bodů

Jméno:

Místnost:

2. vnitrosemestrální písemka

4444

list

5

učo

body

Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.

0 1 2 3 4 5 6 7 8 9