**Jméno:** **Místnost:** **2. vnitrosemestrální písemka**

2222 *list* 1 *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

## Příklad 1
**15 bodů**

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

$$p(x) = x^4 - 2x^3 + 3x^2 - 8x - 4, \qquad q(x) = x^4 - x^3 - x^2 - 5x - 2.$$

**Jméno:** **Místnost:** **2. vnitrosemestrální písemka**

2222 ***list*** 2 ***učo*** ***body***

*Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.* 0123456789

Určete všechny komplexní kořeny polynomu $f(x) = x^5 - 3x^4 + x^3 + x^2 - 3x + 1$. **Příklad 2**
**10 bodů**

**Jméno:** **Místnost:** **2. vnitrosemestrální písemka**

2222 *list* 3 *učo* *body*

*Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.* 0123456789

## Příklad 3
**15 bodů**

Definujme zobrazení $f : (\mathbb{Z}_8, +) \to (\mathbb{C}^*, \cdot)$ vztahem $f([a]_8) = \left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)^a$.

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**

2222 *list* 4 *učo* *body*

*Oblast strojově snímatelných informací. Své UČO vyplňte zleva dle přiloženého vzoru číslic. Jinak do této oblasti nezasahujte.* 0123456789

## Příklad 4
**10 bodů**

Amálka zvolila za parametry v kryptosystému ElGamal $p = 13$; $g = 7$, za svůj soukromý klíč zvolila $x = 5$ a zveřejnila veřejný klíč $(p; g; g^x)$. Ukažte, jak Bob zašifruje zprávu $m = 11$ určenou Amálce.

**Jméno:** **Místnost:** **2. vnitrosemestrální písemka**

2222 ***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