Jméno: **Skupina: A** **Místnost: D1** **2. zkouška**

0001 *příklad* 1 *učo* *body* 0

0 1 2 3 4 5 6 7 8 9

Příklad 1

Náhodné veličiny (8 bodů):

(a) Uveďte příklad náhodných veličin X, Y, pro něž $E(X \cdot Y) = E(X) \cdot E(Y)$. Určete, zda jsou ve vašem případě X a Y nekorelované. Vše zdůvodněte. (1)

(b) Náhodná veličina X má na intervalu $(0, \pi)$ hustotu pravděpodobnosti $f(x) = \frac{\sin x}{2}$ a jinde nulovou. Určete distribuční funkci náhodné veličiny X a a načrtněte její graf s vyznačením významných bodů. Dále určete hustotu náhodné veličiny $Y = X^2$ (nezapomeňte na uvedení příslušných intervalů) a vypočtěte $E(Y), D(X)$. (4)

(c) V lese tvaru trojúhelníka s vrcholy v bodech $(1, 0), (-\frac{1}{2}, \frac{\sqrt{3}}{2})$ a $(-\frac{1}{2}, -\frac{\sqrt{3}}{2})$ se ztratilo dítě. Pravděpodobnost výskytu dítěte v určité části lesa je úměrná velikosti této části, nikoliv umístění této části. Určete rozdělení vzdálenosti dítěte od zvolené strany lesa. (3)

Jméno: **Skupina: A** **Místnost: D1** **2. zkouška**

0001 *příklad* 2 *učo* *body* 0

0 1 2 3 4 5 6 7 8 9

Příklad 2

Polynomy a kryptografie (8 bodů):

(a) V závislosti na hodnotě parametru $a \in \mathbb{R}$ určete násobnost kořene -1 polynomu $x^5 - ax^2 - ax + 1$. (2)

(b) O kubickém polynomu $f(x) = x^3 + ax + b$ víte, že má tři různé kořeny x_1, x_2, x_3. Sestavte normovaný polynom (s koeficienty vyjádřenými pomocí a, b), který bude mít právě kořeny $x_1 + x_2, x_1 + x_3, x_2 + x_3$. (2)

(c) Adam si v kryptosystému RSA zvolil za veřejný klíč modul $n = 1189$ a exponent $e = 19$. Zašifrujte pro Adama zprávu $m = 11$. V pozici Adama, kdy navíc znáte rozklad $n = 29 \cdot 41$, vypočtěte jeho soukromý klíč a zprávu zašifrovanou v předchozím kroku dešifrujte. Uveďte teoretické zdůvodnění funkčnosti tohoto postupu. (4)

Jméno: **Skupina: A** **Místnost: D1** **2. zkouška**

0001 *příklad* 3 *učo* *body* 0

0 1 2 3 4 5 6 7 8 9

Algebra (4 body) : Nechť S_n značí grupu permutací na n-prvkové množině s operací skládání zobrazení.

Příklad 3

(a) Určete, pro která $n \in \mathbb{N}$ je grupa S_n komutativní a v nekomutativních případech ukažte příklad nekomutujících prvků. (1)

(b) Určete všechna $m \in \mathbb{N}$ pro něž v S_7 existuje prvek řádu m. (1)

(c) Vyčíslete počet permutací řádu 3 v S_7. (1)

(d) Určete všechny permutace $s \in S_7$ pro něž platí $s^2 \circ (6,7) \circ s^2 = (6,7) \circ s^2 \circ (6,7)$. (1)

Vše zdůvodňujte.

Jméno: **Skupina: B** **Místnost: D1** **2. zkouška**

0002 *příklad* 1 *učo* *body* 0

0 1 2 3 4 5 6 7 8 9

Náhodné veličiny (8 bodů):

Příklad 1

(a) Uveďte příklad náhodných veličin X, Y, pro něž $D(X+Y) = D(X) + D(Y)$. Určete, zda jsou ve vašem případě X a Y nekorelované. Vše zdůvodněte. (1)

(b) Náhodná veličina X má na intervalu $(0, \frac{\pi}{2})$ hustotu pravděpodobnosti $f(x) = \cos x$ a jinde nulovou. Určete distribuční funkci náhodné veličiny X a a načrtněte její graf s vyznačením významných bodů. Dále určete hustotu náhodné veličiny $Y = X^2$ (nezapomeňte na uvedení příslušných intervalů) a vypočtěte $E(Y), D(X)$. (4)

(c) V lese tvaru trojúhelníka s vrcholy v bodech $(0,0), (1,0)$ a $(0,1)$ se ztratilo dítě. Pravděpodobnost výskytu dítěte v určité části lesa je úměrná velikosti této části, nikoliv umístění této části. Určete rozdělení vzdálenosti dítěte od nejdelší strany lesa. (3)

Jméno: **Skupina: B** **Místnost: D1** **2. zkouška**

0002 *příklad* 2 *učo* *body* 0

0 1 2 3 4 5 6 7 8 9

Polynomy a kryptografie (8 bodů):

Příklad 2

(a) V závislosti na hodnotě parametru $a \in \mathbb{R}$ určete násobnost kořene -1 polynomu $x^6 - ax^4 - ax^2 - 1$. (2)

(b) O kubickém polynomu $f(x) = x^3 + ax^2 + bx - 1$ víte, že má tři různé kořeny x_1, x_2, x_3. Sestavte normovaný polynom (s koeficienty vyjádřenými pomocí a, b), který bude mít právě kořeny x_1x_2, x_1x_3, x_2x_3. (3)

(c) Alice si chce s Bobem pomocí protokolu Diffieho a Hellmana vyměnit klíč pro symstrickou komunikaci. Zvolí parametr $p = 29$. (3)

i) Určete generátor grupy $(\mathbb{Z}_{29}^{\times}, \cdot)$.

ii) Alice zvolila číslo $a = 10$ a Bob $b = 20$. Vypočtěte sdílený klíč a popište postup, jak se na něm dohodli.

Jméno: **Skupina: B** **Místnost: D1** **2. zkouška**

0002 *příklad* 3 *učo* *body* 0

0 1 2 3 4 5 6 7 8 9

Algebra (4 body) : Nechť S_n značí grupu permutací na n-prvkové množině s operací skládání zobrazení, A_n její podgrupu sudých permutací. **Příklad 3**

(a) Určete, pro která $n \in \mathbb{N}$ je grupa A_n komutativní a v nekomutativních případech ukažte příklad nekomutujících prvků. (1)

(b) Určete všechna $m \in \mathbb{N}, m \leq 8$ pro něž v A_7 existuje prvek řádu m. (1)

(c) Vyčíslete počet permutací řádu 5 v A_7. (1)

(d) Určete počet inverzí permutace $\sigma = (1, 4, 5)(2, 3, 6) \in S_7$ (1)

Vše zdůvodňujte.

Jméno: **Skupina:** **Místnost:** **2. zkouška**

příklad ***učo*** ***body*** 0 1 2 3 4 5 6 7 8 9