

Jméno:

Skupina: A

Místnost:

2. zkouška



příklad



učo



body



0 1 2 3 4 5 6 7 8 9

Náhodné veličiny a pravděpodobnost (7 bodů):

Příklad 1

- (a) Určete distribuční funkci náhodného vektoru  $(X, Y)$ , jehož hustota je

$$f(x, y) = \begin{cases} \frac{1}{6}(4x - y) & \text{pro } 1 \leq x \leq 2, 2 \leq y \leq 4, \\ 0 & \text{jinak.} \end{cases}$$

Určete dále  $P(Y > 2X)$ . (4)

- (b) Tyč délky 1 je náhodně rozlomena na 3 části. Určete pravděpodobnost, že z těchto částí půjde sestavit trojúhelník. (3)

Jméno:

Skupina: A

Místnost:

2. zkouška

0001

*příklad*

2

*učo**body*

0123456789

**Statistika (6 bodů):** Na dvou soustruzích se vyrábějí tytéž součástky, **Příklad 2** u nichž se měří vnitřní průměr (předpokládá se normální rozdělení). Byl pořízen náhodný výběr rozsahu 14 z produkce prvního soustruhu a rozsahu 18 z produkce druhého soustruhu. Příslušné výběrové průměry jsou 37,5 mm, resp. 36,8 mm a výběrové rozptyly  $1,21 \text{ mm}^2$ , resp.  $1,44 \text{ mm}^2$ . Testujte hypotézu o rovnosti střední hodnoty kontrolovaných rozměrů v produkci obou strojů oproti oboustranné alternativě při  $\alpha = 0,1$ . Svůj závěr explicitně zformulujte.

Jméno:

Skupina: A

Místnost:

2. zkouška

0001

příklad

3

učo

body

0123456789

Algebra a aplikace (7 bodů) :

Příklad 3

- (a) Nalezněte polynomy  $f(x), g(x) \in \mathbb{Q}[x]$  stupně 4, které mají (každý) trojnásobný racionální kořen a jejichž největší společný dělitel je  $h(x) = x^2 - 3x - 4$ . Polynom  $h$  vyjádřete jako lineární kombinaci polynomů  $f(x), g(x)$  (Bezoutova rovnost). (4)
- (b) Adam si v kryptosystému RSA zvolil za veřejný klíč modul  $n = 1189$  a exponent  $e = 23$ . Zašifrujte pro Adama zprávu  $m = 13$ . V pozici Adama, kdy navíc znáte rozklad  $n = 29 \cdot 41$ , vypočtete jeho soukromý klíč a uveďte, jak se zpráva dešifruje (výpočet již neprovádějte). (3)

Jméno:

Skupina: B

Místnost:

2. zkouška

0002

příklad

|

učo

body

0 1 2 3 4 5 6 7 8 9

Náhodné veličiny (7 bodů):

Příklad 1

- (a) Určete hustotu pravděpodobnosti náhodného vektoru  $(X, Y)$ , jehož distribuční funkce je

$$F(x, y) = \begin{cases} 0 & \text{pro } x \leq -1 \\ \frac{1}{\pi^2}(\arcsin x + \frac{1}{2})(\operatorname{arctg} y + \frac{\pi}{2}) & \text{pro } |x| < 1 \\ \frac{1}{\pi}(\operatorname{arctg} y + \frac{\pi}{2}) & \text{pro } x \geq 1. \end{cases}$$

Určete rovněž marginální hustoty a rozhodněte, jsou-li veličiny  $X$  a  $Y$  stochasticky nezávislé. (4)

- (b) Na úsečce  $OA$  délky 1 jsou náhodně zvolené body  $B$  a  $C$  tak, že  $|OB| < |OC|$ . S využitím geometrické pravděpodobnosti určete pravděpodobnost, že  $|BC| < |OB|$ . Předpokládejte, že pravděpodobnost volby bodu na konkrétní úsečce má rovnoměrné spojitě rozdělení. (3)

Jméno:

Skupina: B

Místnost:

2. zkouška

0002

*příklad*

2

*učo**bodů*

0123456789

**Statistika (6 bodů):** Předpokládáme, že přidáním speciálních přípravků je možné snížit tvrdost vody. Náhodným výběrem 40 vzorků vody byla zjištěna průměrná tvrdost 4,0. Po přidání přípravku pak byla změřena na 50 vzorcích průměrná tvrdost 3,8. Na hladině významnosti 5% testujte nulovou hypotézu oproti předpokládané jednostranné alternativě za předpokladu, že oba výběry pocházejí z normálního rozdělení s rozptylem 0,25. Svůj závěr explicitně zformulujte.

**Příklad 2**

Jméno:

Skupina: B

Místnost:

2. zkouška

0002

*příklad*

3

*učo**body*

0 1 2 3 4 5 6 7 8 9

Algebra a aplikace (7 bodů) :

Příklad 3

- (a) Nalezněte polynomy  $f(x), g(x) \in \mathbb{Q}[x]$  stupně 4, které mají (každý) trojnásobný racionální kořen a jejichž největší společný dělitel je  $h(x) = x^2 - x - 6$ . Polynom  $h$  vyjádřete jako lineární kombinaci polynomů  $f, g$  (Bezoutova rovnost). (4)
- (b) Alice si chce s Bobem pomocí protokolu Diffieho a Hellmana vyměnit klíč pro symetrickou komunikaci. Zvolí parametr  $p = 29$ . (3)
- Určete generátor grupy  $(\mathbb{Z}_{29}^\times, \cdot)$ .
  - Alice zvolila číslo  $a = 21$  a Bob  $b = 13$ . Vypočtěte sdílený klíč a popište postup, jak se na něm dohodli.