jaro 2013
MB104 - 382 - st. A

(1)

a) Distr. fce: zřejmě pro $x<1$ nebo $y<2$ je $F(x,y)=0$.

Pro $x\in\langle 1,2\rangle$, $y\in\langle 2,4\rangle$ je

$$F(x,y)=\int_1^x\int_2^y f(u,v)\,dv\,du = \dots = \frac{1}{12}\left(4x^2y-xy^2-8x^2+4x-4y+y^2+4\right) = \frac{1}{12}(y-2)(x-1)(4x-y+2)$$

Pro $x\in\langle 1,2\rangle$, $y>4$ je $F(x,y)=F(x,4)=\frac{1}{6}(x-1)(4x-2)$

Pro $x\in(2,\infty)$, $y\in\langle 2,4)$ je $F(x,y)=F(2,y)=\frac{1}{12}(y-2)(10-y)$

Pro $x>2$, $y>4$ je $F(x,y)=1$.

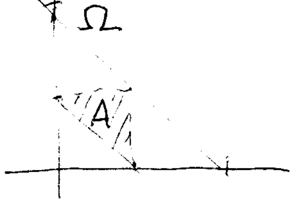
$$P(Y>2X)=\int_2^4\int_1^{y/2}\frac{1}{6}(4x-y)\,dx\,dy = \dots = \frac{1}{3}.$$

$y>2x \iff x<\frac{y}{2}$

b) Označme délky částí x, y, $1-x-y$ (kde $x,y\in\langle 0,1\rangle$, $x+y\le 1$)

Aby bylo možné z částí sestavit Δ, musí platit trojúhelníkové nerovnosti, z nichž: $0\le x<\frac{1}{2}$, $0\le y<\frac{1}{2}$, $x+y>\frac{1}{2}$

Hledaná pravděpodobnost je $\frac{\mu(A)}{\mu(\Omega)} = \frac{\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{1}{2}}{\frac{1}{2}\cdot 1\cdot 1} = \frac{1}{4}$.



(2) Testujeme hypotézu $H_0: \mu_1=\mu_2$ oproti alternativě $H_1: \mu_1\neq\mu_2$ při riziku $\alpha=0{,}1$.
Jde o dvouvýběrový t-test; testujeme např. prostřednictvím oboustranného intervalu spolehlivosti $M_1-M_2 \pm S_* \sqrt{\frac{1}{m}+\frac{1}{n}}\cdot t_{1-\frac{\alpha}{2}}(m+n-2)$, nebo

sestrojením kritického oboru: H_0 zamítneme, pokud $\left|\frac{M_1-M_2-0}{S_*\sqrt{\frac{1}{m}+\frac{1}{n}}}\right| \ge t_{1-\frac{\alpha}{2}}(m+n-2)$

Zde $m=14$, $n=18$, $S_*^2=\frac{(m-1)S_1^2+(n-1)S_2^2}{m+n-2}\approx 1{,}34 \Rightarrow S_*\approx 1{,}158$.

Hodnota statistiky $\frac{M_1-M_2}{S_*\sqrt{\frac{1}{m}+\frac{1}{n}}}\approx 1{,}696 < t_{0{,}95}(30)=1{,}6973$, proto

hypotézu nezamítáme (nelze vyvrátit, že oba stroje produkují součástky velikosti rozměru)

(3) a) $h(x)=(x-4)(x+1)$. Mají-li být $f(x), g(x)$ stupně 4 a každý z nich mít trojnásobný kořen, musí být v jednom případě tímto kořenem být 4 a v druhém -1.

Proto $f(x)=(x-4)^3(x+1)$, $g(x)=(x+1)^3(x-4)$.

Výpočet si zjednodušíme, budeme-li počítat gcd$((x+1)^2,(x-4)^2)$. Dostaneme dělení se zbytkem

$(x-4)^2=(x+1)^2-5(2x-3)$ odkud $125=(13-2x)(x+1)^2+(2x+7)(x-4)^2$ a

$4(x+1)^2=(2x-3)(2x+7)+25$, $125h(x)=(13-2x)f(x)+(2x+7)\cdot g(x)$.

(36) $n=1189$, $e=23$.

Zašifrování $m=13$ $\quad 13^{23} \equiv 1165 \pmod{1189}$

Dešifrování $c=1165 \equiv -24\ (1189)$.

Nalezneme d: $\quad e\cdot d \equiv 1\ (\varphi(n))$

$$23\cdot d \equiv 1\ (28\cdot 40) \Leftrightarrow 23d\equiv 1\ (5) \wedge 23d \equiv 1\ (32) \wedge 23d\equiv 1\ (7)$$

$23d\equiv 1\ (5)$, $d\equiv 2\ (5)$

$23d \equiv 1\ (7)$, $2d\equiv 8\ (7)$, $d\equiv 4\ (7)$

$23d\equiv 1\ (32)$, $-9d\equiv 33\ (32)$, $-3d\equiv 11\ (32)$, $-3d\equiv -21\ (32)$, $d\equiv 7\ (32)$

Odtud $d\equiv 487\ (1120)$

Dešifrování $(-24)^{487} \equiv 13\ (1189)$.

jaro 2013
MB104 - zk 2-st. B

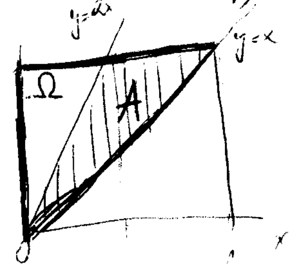
① a) $F(x,y) = \begin{cases} 0 & x \le -1 \\ \frac{1}{\pi^2}(\arcsin x + \frac{1}{2})(\mathrm{arctg}\, y + \frac{\pi}{2}) & |x| < 1 \\ \frac{1}{\pi}(\mathrm{arctg}\, y + \frac{\pi}{2}) & x \ge 1 \end{cases}$

Hustota $f(x,y) = \begin{cases} 0 & \text{pro } x \notin (-1,1) \\ \frac{\partial^2 F(x,y)}{\partial x \partial y} = \frac{1}{\pi^2 \sqrt{1-x^2}(1+y^2)} & \text{pro } x \in (-1,1) \end{cases}$

Marginální hustoty: $f_X(x) = \int_{-\infty}^{\infty} f(x,y)\,dy = \frac{1}{\pi^2} \cdot \frac{1}{\sqrt{1-x^2}} \cdot [\mathrm{arctg}\, y]_{-\infty}^{\infty} = \frac{1}{\pi^2} \cdot \frac{1}{\sqrt{1-x^2}} \cdot \pi$
$= \frac{1}{\pi} \cdot \frac{1}{\sqrt{1-x^2}}$ pro $x \in (-1,1)$
jinak 0

$f_Y(y) = \int_{-1}^{1} f(x,y)\,dx = \frac{1}{1+y^2} \cdot \frac{1}{\pi^2} [\arcsin x]_{-1}^{1} = \frac{1}{\pi} \cdot \frac{1}{1+y^2}$

X, Y jsou stochasticky nezávislé, neboť $\forall x,y \in \mathbb{R}: f(x,y) = f_X(x) \cdot f_Y(y)$.



b) Položme $x = |OB|$, $y = |OC|$, že zadání $0 \le x < y \le 1$.
$|BC| = y - x < |OB| = x \iff y < 2x$.
Tedy $x < y < 2x$. Celkem $\mu(A) = \frac{1}{2} \cdot 1 \cdot \frac{1}{2} = \frac{1}{4}$
$\mu(\Omega) = \frac{1}{2} \cdot 1 \cdot 1 = \frac{1}{2}$
Hledaná pst je rovna $\frac{\mu(A)}{\mu(\Omega)} = \frac{1}{2}$.

② Levostranný interval spolehlivosti $1-\alpha$ pro $\mu_1 - \mu_2$ je
$\left(M_1 - M_2 - \sqrt{\frac{\sigma^2}{m} + \frac{\sigma^2}{n}} \cdot u_{1-\alpha}, \infty\right)$, kde $M_1 - M_2 = 0{,}2$; $\sigma^2 = 0{,}25$; $m = 40$, $n = 50$
$u_{0,95} = 1{,}65$.
Vypočteme, že $0 \notin (0{,}2 - 0{,}175; \infty)$ proto s rizikem 0,05 zamítáme hypotézu $H_0: \mu_1 = \mu_2$ oproti jednostranné alternativě (a lze tedy tvrdit, že přípravek tvrdost vody snižuje).

③ a) $h(x) = (x+2)(x-3)$, zadáním trojnásobným kořenem musí být v jednom případě 3 a ve druhém -2. Tedy $f(x) = (x-3)^3 \cdot (x+2)$, $g(x) = (x+2)^3 \cdot (x-3)$. Vypočteme $a(x), b(x)$ aby $1 = a(x) \cdot (x-3)^2 + b(x)(x+2)^2$, pak totiž $h(x) = a(x) \cdot f(x) + b(x) \cdot g(x)$.

Podobně jako ve sk. A: $(x+2)^2 = (x-3)^2 + 5(2x-1)$
$4 \cdot (x-3)^2 = (2x-1) \cdot (2x-11) + 25$,
odkud $125 = (2x+9)(x-3)^2 - (2x-11) \cdot (x+2)^2$ a tedy
$125 h(x) = (2x+9) f(x) - (2x-11) \cdot g(x)$

b) $p = 29$

i) 2 je generátor (primitivní kořen) $(\mathbb{Z}_{29}^{\times}, \cdot)$, neboť $\varphi(29) = 28$, řád dělí 28 a platí:

x	2	4	7	8	12	14	28
$2^x (29)$	4	16	12	-4	7	-1	1

$\forall d \mid 28$; $0 < d < 28$ je $2^d \not\equiv 1 (29)$.

ii) $a = 21$ Alice vypočte $2^{21} \equiv 17 \ (29)$ a pošle Bobovi, ten vypočte klíč $17^{13} \equiv 17 (29)$

$b = 13$ Bob vypočte $2^{13} \equiv 14$ a pošle Alici, jež vypočte klíč $14^{21} \equiv 14 (29)$

Sdílený klíč je tedy $K = 17$.