A (1.)

a) $E(XY) = E(X)\cdot E(Y) \Leftarrow X, Y$ jsou nekorelované!

Za příklad stačí zvolit dvě nezávislé náhodné veličiny, např.

$X \sim A(1/2)$, $Y \sim A(\frac{1}{2})$, pak $E(X) = \frac{1}{2}$, $E(Y) = \frac{1}{2}$; $P(X\cdot Y = 0) = \frac{3}{4}$, $P(X \cdot Y = 1) = \frac{1}{4}$

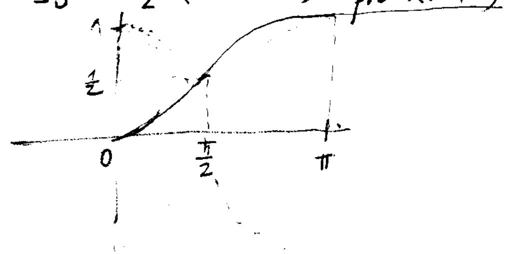
$\Rightarrow E(X\cdot Y) = \frac{1}{4}$.

b) $f_X(x) = \frac{\sin x}{2}$ pro $x \in (0, \pi)$.

Distribuční funkce $F_X(x) = \int_0^x \frac{\sin t}{2}\, dt = \frac{1}{2}[-\cos t]_0^x = \frac{1}{2}(1-\cos x)$ pro $x \in (0,\pi)$

$F_X(x) = 0$ pro $x \le 0$

$F_X(x) = 1$ pro $x \ge \pi$.



$Y = X^2$: $F_Y(y) = P(Y \le y) = P(X^2 \le y) = P(-\sqrt{y} \le X \le \sqrt{y}) =$

$\overset{X \text{ je nezáp.}}{=} P(X \le \sqrt{y}) = F_X(\sqrt{y}) = \frac{1}{2}(1-\cos\sqrt{y})$.

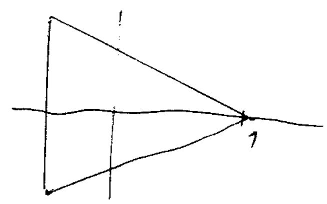
Odtud hustota $f_Y(y) = \frac{1}{2}(1-\cos\sqrt{y})' = \frac{1}{4}\frac{\sin\sqrt{y}}{\sqrt{y}}$ pro $y \in (0, \pi^2)$.

$E(Y) = E(X^2) = \int_0^\pi t^2 \frac{\sin t}{2}\, dt = \left| \dots 2\times \text{ per partes} \dots \right| = \frac{\pi^2}{2} - 2$

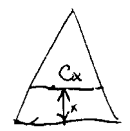
$D(X) = E(X^2) - E(X)^2 = \frac{\pi^2}{2} - 2 - \left(\frac{\pi}{2}\right)^2 = \frac{\pi^2}{4} - 2$

$E(X) = \int_0^\pi t\, \frac{\sin t}{2}\, dt = |\text{per partes}| = \frac{\pi}{2}$ ⇑

c) Jde o rovnostranný trojúhelník s délkou strany $\sqrt{3}$.



Distribuční funkce $F_X(x) = P(X \le x)$.. pst, že není dále od vybrané strany než x. $P(X \le x) = \frac{S_{\square}}{S_{\Delta}}$, kde $S_{\square} = \frac{a + c_x}{2}\cdot x$,



$a = \sqrt{3}$
$v = \frac{3}{2}$
$S = \frac{av}{2} = \frac{3\sqrt{3}}{4}$

příčnou c_x určíme z podobnosti Δ: $\frac{v - x}{v} = \frac{c_x}{a}$, odtud $c_x = a(1 - \frac{x}{v})$.

Tedy $P(X \le x) = \frac{\frac{a(2 - \frac{x}{v})}{2}\cdot x}{\frac{av}{2}} = \frac{ax(1 - \frac{x}{2v})}{\frac{av}{2}} = \frac{x}{v}(2 - \frac{x}{v})$ pro $x \in \langle 0, \frac{3}{2} \rangle$ ($\frac{3}{2} = v$)

(2) a) $f(x) = x^5 - ax^2 - ax + 1$ pro $a \ne -5$ jednoduchý kořen $x = -1$

	1	0	0	$-a$	$-a$	1	
-1	1	-1	1	$-1-a$	1	0	
-1	1	-2	3	$-4-a$	$5+a$		
$a=-5$	1	-2	3	1	0		
-1	1	-3	6	-5			

pro $a = -5$ jde o dvojnásobný kořen $x = -1$.

Jinak. -1 je kořen – snadno z dosazení. $f'(x) = 5x^4 - 2ax - a \Rightarrow f'(-1) = 5 + a = 0 \Leftrightarrow a = -5$

$f''(x) = 20x^3 - 2a \Rightarrow f''(-1) = -20 - 2a \ne 0 \Leftrightarrow a = -10$

$\Rightarrow$ pro $a = -5$ dvojnásobný kořen

b) $f(x) = x^3 + ax + b = (x-x_1)(x-x_2)(x-x_3)$, kde $x_1+x_2+x_3 = 0$
$x_1x_2 + x_1x_3 + x_2x_3 = a$
$x_1x_2x_3 = -b$.

Chceme polynom
$$(x-(x_1+x_2))(x-(x_1+x_3))(x-(x_2+x_3)) =$$
$$= (x+x_3)(x+x_2)(x+x_1) = x^3 + (x_1+x_2+x_3)x^2 + (x_1x_2+x_1x_3+x_2x_3)x + x_1x_2x_3 =$$
$$= x^3 + ax - b$$

c) $m = 11$, $e = 19$, $n = 1189$, zašifroval text $c \equiv m^e \pmod n$
$c \equiv 11^{19}$ (1189)
$c \equiv 682$ (1189)

$n = 29 \cdot 41$, Adam hledal d takové, aby $e \cdot d \equiv 1 \pmod{\varphi(n)}$
$19d \equiv 1$ $(28 \cdot 40)$
$19d \equiv 1121$ (1120)
$d \equiv 59$

Adamův soukromý klíč je 59; pak $c^d = 682^{59} \equiv 11 \pmod{1189}$, tedy dešifroval původní zprávu.
Vše funguje díky Eulerově větě: $e \cdot d \equiv 1 \pmod{\varphi(n)} \Rightarrow m^{ed} \equiv m \pmod n$
$(m^e)^d$

(3) S_n

a) $n = 1, 2$, pro $n \geq 3$ např. $(1,2)\circ(2,3) \neq (2,3)\circ(1,2)$

b) Cyklus má řád rovný počtu prvků v cyklu $\Rightarrow$ ex. pro $m \leq 7$.
Dále pro nezávislé cykly řádu r, s má jejich součin řád $[r,s]$.
Proto existují permutace řádu $10 = 2 \cdot 5$, $12 = 3 \cdot 4$ (pro součiny $2 \cdot 7, 3 \cdot 5, 3 \cdot 7, 4 \cdot 5, 4 \cdot 7, 5 \cdot 6, 5 \cdot 7$, $6 \cdot 7$ nemáme „dost" prvků, resp. byly cykly nezávislé)

~~c) $\binom{7}{5} = 35$, jde o různé trojprvkové cykly~~

d) Neexistuje – levá/obrana je lichá permutace, zatímco pravá strana sudá!

c) Jde o různé cykly tvaru (a,b,c) nebo $(a,b,c)(d,e,f)$.
Trojcyklů je $\binom{7}{3} \cdot 2 = 70$ (vybereme trojici a určíme jeden ze 2 možných cyklů)
Dvojic nezávislých trojcyklů je $7 \cdot 5 \cdot 4 \cdot 2$ ($\binom{7}{6}$... vybereme šestici, 5 možností pro obraz nejmenšího čísla, 4 pro „obraz obrazu"; zbývá trojice, kde máme 2 možné cykly)

Celkem $\binom{7}{3} \cdot 2 + 7 \cdot 5 \cdot 4 \cdot 2 = 350$ prvků S_7 řádu 3.

B

① a) $D(X+Y) = D(X) + D(Y) + 2C(X,Y)$ obecně.

Tedy $D(X+Y) = D(X) + D(Y) \Leftrightarrow X$ a Y jsou nekorelované.

Stačí např. zvolit libovolné nezávislé náh. veličiny X, Y – např.

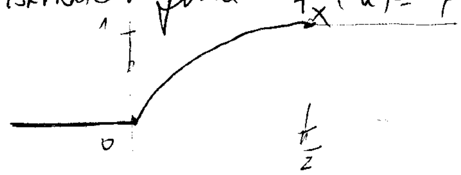
~~$X \sim Rs(0,1)$ rovnoměrné spojité na int $\langle 0,1)$~~ X i Y nechť je konstantní

$P(X=a) = 1,\ P(Y=b) = 1$, pak $D(X) = 0,\ D(Y) = 0$

$P(X \cdot Y = a \cdot b) = 1 \Rightarrow D(X \cdot Y) = 0.$

b) $f_X(x) = \cos x$ pro $x \in (0, \frac{\pi}{2})$

Distribuční funkce $F_X(x) = P(X \le x) = \int_0^x \cos t \, dt = [\sin t]_0^x = \sin x$ – pro $x \in (0, \frac{\pi}{2})$



$F_X(x) = 0$ pro $x \le 0$

$F_X(x) = 1$ pro $x \ge \frac{\pi}{2}$.

$Y = X^2$: $F_Y(y) = P(Y \le y) = P(X^2 \le y) = P(-\sqrt{y} \le X \le \sqrt{y}) \overset{X \text{ nezápor.}}{=} P(X \le \sqrt{y}) =$

$= F_X(\sqrt{y}) = \sin\sqrt{y}$ pro $\sqrt{y} \le \frac{\pi}{2}$, tj. $y \le \frac{\pi^2}{4}$

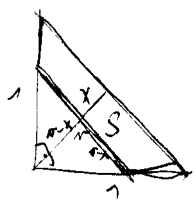
$f_Y(y) = (\sin\sqrt{y})' = \frac{\cos\sqrt{y}}{2\sqrt{y}}$ pro $0 < y < \frac{\pi^2}{4}$, jinde nulová.

$E(Y) = E(X^2) = \int_0^{\pi/2} x^2 \cos x \, dx = \left| 2\times \text{ per partes} \right| = \frac{\pi^2}{4} - 2$

$D(X) = E(X^2) - E(X)^2 = \frac{\pi^2}{4} - 2 - (\frac{\pi}{2} - 1)^2 = \pi - 3$

kde $E(X) = \frac{\pi}{2} - 1$?!

c) Jde o pravoúhlý rovnoramenný Δ o obsahu $\frac{1}{2}$, s délkou výšky $v = \frac{\sqrt{2}}{2}$.



Distr. funkce $F_X(x) = P(X \le x)$ ... pst, že není dál než x od přepony

$P(X \ge x) = \frac{S}{\frac{1}{2}}$, kde $S = \frac{1}{2} - (v - x)^2$, tedy

$P(X \le x) = 1 - 2(v - x)^2 = 1 - 2(\frac{\sqrt{2}}{2} - x)^2 = 2x(\sqrt{2} - x)$ pro $x \in \langle 0, \frac{\sqrt{2}}{2} \rangle$

② a) $f(x) = x^6 - ax^4 + ax^2 - 1$

	1	0	−a	0	+a	0	−1
−1	1	−1	1−a	a−1	1	−1	0
−1	1	−2	3−a	2a−4	5−2a	2a−6	
a=3	1	−2	0	2	−1	0	
−1	1	−3	3	−1	0		
−1	1	−4	7	−8	×		

pro $a \ne 3$ jednoduchý kořen −1

pro $a = 3$ trojnásobný kořen −1

b) $f(x) = x^3 + ax^2 + bx - 1 = (x - x_1)(x - x_2)(x - x_3)$, tj.: $x_1 + x_2 + x_3 = -a$

$x_1x_2 + x_1x_3 + x_2x_3 = b$

$x_1 x_2 x_3 = 1$

Chceme polynom $(x - x_1x_2)(x - x_1x_3)(x - x_2x_3) =$

$$= \left(x - \frac{1}{x_3}\right)\left(x - \frac{1}{x_2}\right)\left(x - \frac{1}{x_1}\right) = x^3 - \left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}\right)x^2 + \left(\frac{1}{x_1x_2} + \frac{1}{x_1x_3} + \frac{1}{x_2x_3}\right)x - \frac{1}{x_1x_2x_3} =$$

$$= x^3 - bx^2 - ax - 1$$

c) $p = 29$;

i) 2 je generátor $(\mathbb{Z}_{29}^{\times}, \cdot)$, neboť $\varphi(29) = 28$

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

řád dělí 28

ii) $a = 10$ Alice vypočte $2^{10} \equiv 9\ (29)$ a pošle Bobovi, ten vypočte $9^{20} \equiv 16$

$b = 20$, Bob vypočte $2^{20} \equiv 23\ (29)$ a pošle Alici, ta vypočte $23^{10} \equiv 16$, což je klíč.

(3) a) pro $n \leq 2$ je $|A_n| = 1$, tedy komutativní

$A_3 = \{id, (1,2,3), (1,3,2)\}$ - cyklická, tedy komutativní

pro $n \geq 4$ je $(1,2,3), (1,2,4) \in A_n$, přičemž $(1,2,3) \circ (1,2,4) = (1,3)(2,4)$

$(1,2,4) \circ (1,2,3) = (1,4)(2,3)$ #

b) Existuje pro $m \leq 7$, pro $m = 8$ neexistuje

prvek	id	$(1,2)(3,4)$	$(1,2,3)$	$(1,2,3,4)(5,6)$	$(1,2,3,4,5)$	$(1,2,3)(4,5)(6,7)$	$(1,2,3,4,5,6,7)$
řád	1	2	3	4	5	6	7

c) $4!\binom{7}{5} = 21 \cdot 24 = 504$ [[illegible] $\binom{7}{5}$ možností pro výběr pětice, první prvek cyklu zafixujeme, pro další máme 4! možností)

d) Inverzí je $2+3+2+3 = 10$.