ד) הוכיחו או הפריכו: $(p \to q) \to (\neg p \to \neg q)$ טאוטולוגיה.

(יחידה 10)

ה) הוכיחו או הפריכו: $(\forall x P(x) \to \forall x Q(x)) \to \forall x (P(x) \to Q(x))$

ה) הוכיחו או הפריכו: $(\exists x P(x) \to \exists x Q(x)) \to \exists x (P(x) \to Q(x))$

(יחידה 9)

ד) הוכיחו או הפריכו: $\forall x (P(x) \to Q(x)) \to (\forall x P(x) \to \forall x Q(x))$

ה) הוכיחו או הפריכו: $\exists x (P(x) \to Q(x)) \to (\exists x P(x) \to \exists x Q(x))$

(יחידה 9)

שאלה 4 (25 נקודות)

הוכיחו או הפריכו כל אחת מהטענות הבאות.

יש להוכיח את הטענה או להפריך אותה באמצעות דוגמה נגדית.

א. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(יחידה 7)

ב. $A \setminus (B \cup C) = (A \setminus B) \setminus C$

(יחידה 7)

ג. $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$

(יחידה 7)

ד. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

(יחידה 7)

ג) הוכיחו כי $\frac{1}{\sqrt{2}} \cdot \frac{\sqrt{2}}{2} = \frac{1}{2}$.

ד) הוכיחו כי $\frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{1}{2}$.

ה) הוכיחו כי $\frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{1}{2}$.

ו) הוכיחו כי $\frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{1}{2}$.

ז) הוכיחו כי $\frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{1}{2}$.

ח) הוכיחו כי $\frac{\sqrt{2}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{1}{2}$.

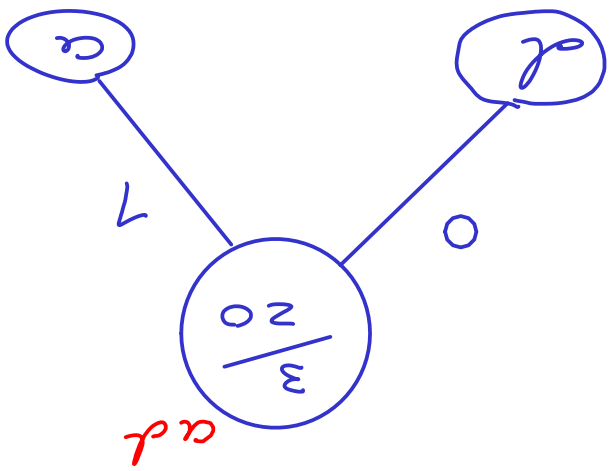
(ג) (4 נק') נתון משתנה מקרי X בעל פונקציית ההסתברות הבאה:

x	a	b	c	d	e
$P_X(x)$	$\frac{1}{10}$	$\frac{1}{2}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{20}$

$$X = \{a, b, c, d, e\}$$

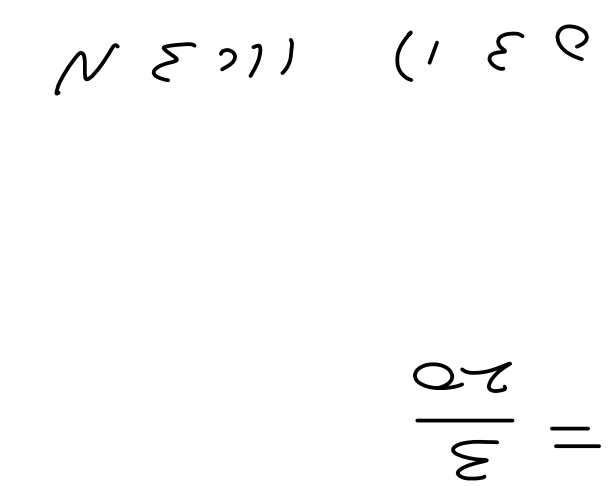
(ד) (4 נק') נתון עץ בינארי T בעל 7 עלים. העלים מסומנים ב-0 או ב-1 כך שהמסלול משורש העץ לכל עלה נותן מחרוזת בינארית שונה. נסמן ב-X את המשתנה המקרי שמקבל את ערכי העלים. נתון כי $P_X(0) = \frac{1}{2}$, $P_X(1) = \frac{1}{20}$, $P_X(d) = \frac{1}{20}$, $P_X(e) = \frac{1}{5}$.

x	a	b	c	d	e
$P_X(x)$	$\frac{1}{20}$	$\frac{1}{10}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{2}$



(ה) (4 נק') נתון עץ בינארי T בעל 7 עלים. העלים מסומנים ב-0 או ב-1 כך שהמסלול משורש העץ לכל עלה נותן מחרוזת בינארית שונה. נסמן ב-X את המשתנה המקרי שמקבל את ערכי העלים. נתון כי $P_X(a) = \frac{1}{20}$, $P_X(b) = \frac{1}{10}$, $P_X(c) = \frac{3}{20}$, $P_X(d) = \frac{1}{5}$, $P_X(e) = \frac{1}{2}$.

x	a	b	c	d	e
$P_X(x)$	$\frac{1}{20}$	$\frac{1}{10}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{2}$



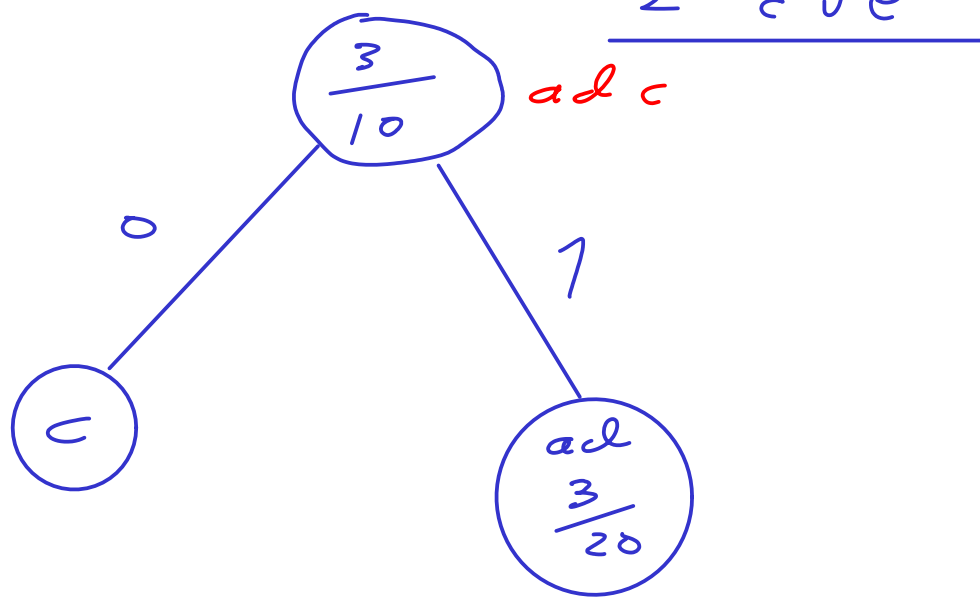
ad	c	e	b
$\frac{3}{20}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{2}$

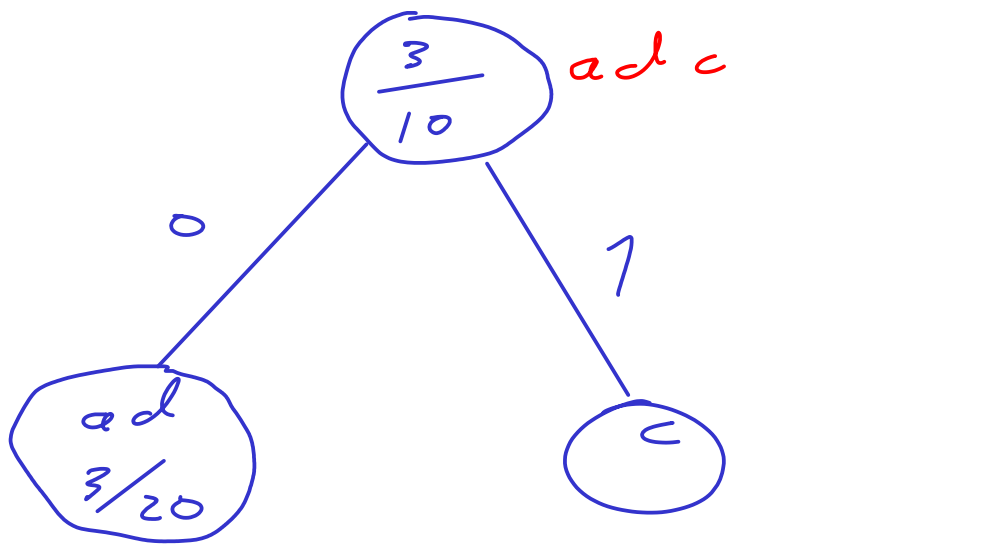
$\frac{6}{20} = \frac{3}{10}$

11c

c	ad	e	b
$\frac{3}{20}$	$\frac{3}{20}$	$\frac{1}{5}$	$\frac{1}{2}$

2 > de



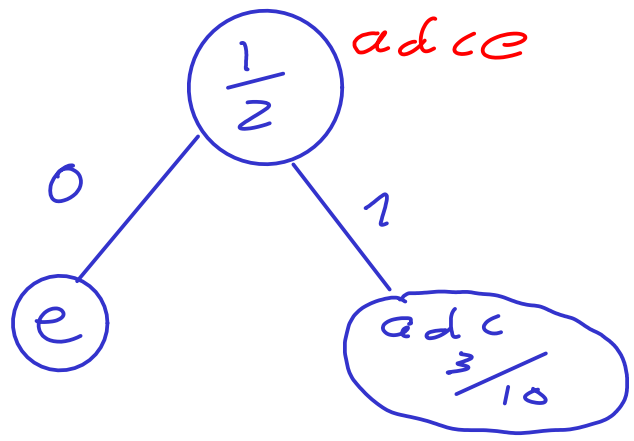


e	adc	b
$\frac{1}{5} = \frac{2}{10}$	$\frac{3}{10}$	$\frac{1}{2} = \frac{5}{10}$

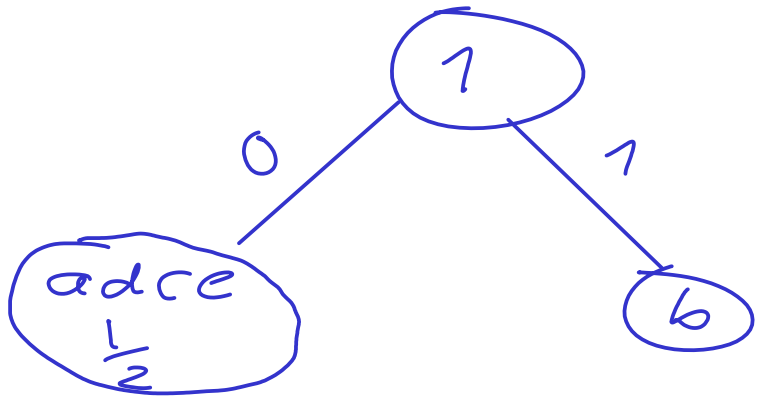
$\frac{5}{10} = \frac{1}{2}$

$\frac{1}{2}$

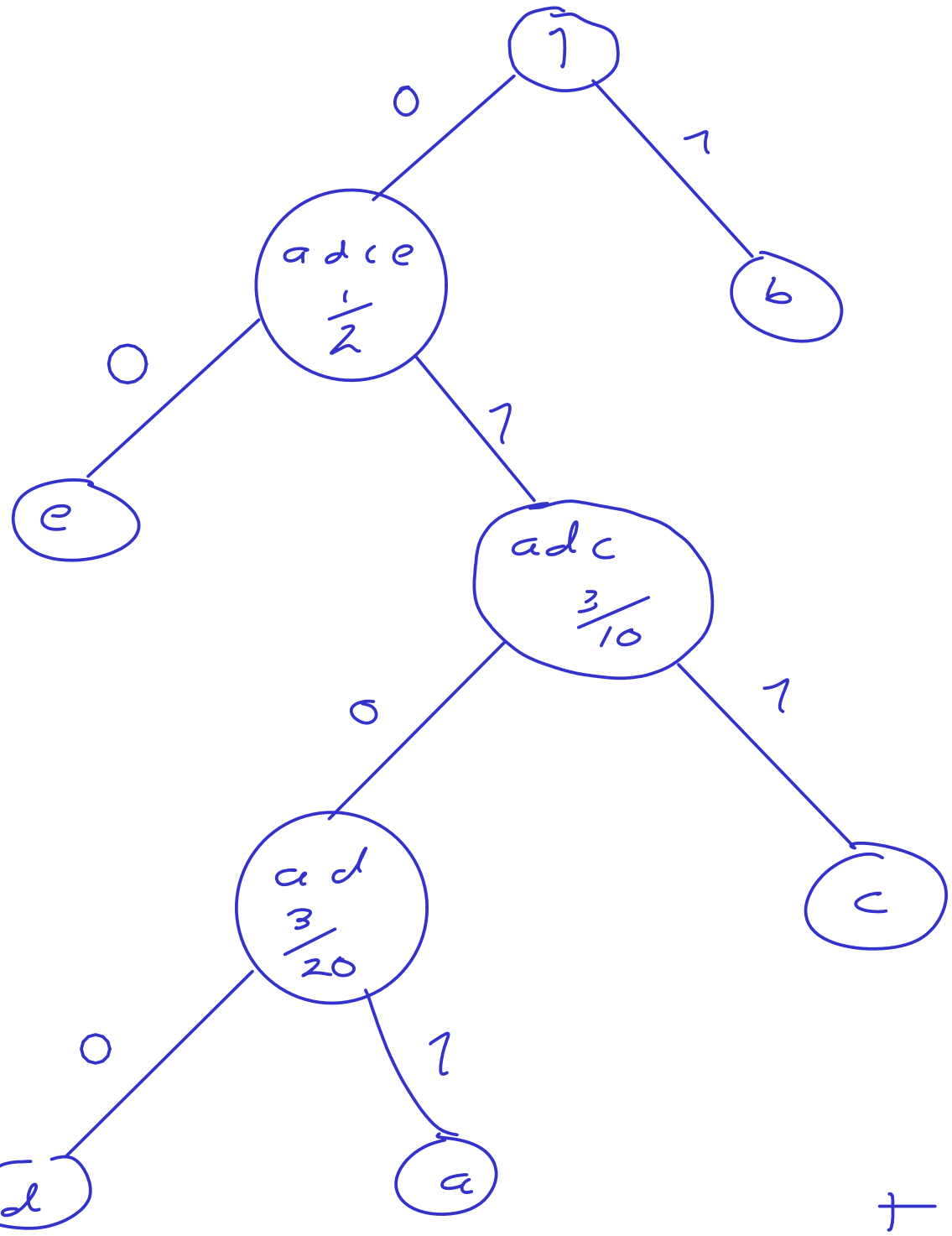
3 > de



adce	b
$\frac{1}{2}$	$\frac{1}{2}$



4 > de



$$f : \Sigma^{+} \longrightarrow \{0,1\}^{*}$$

x	f(x)
a	0 1 0 1
b	1
c	0 1 1
d	0 1 0 0
e	0 0

(د) 9.3 ס

$H[X] = -\sum_{x \in X} P_X(x) \log_2(x)$ (הסימן)

$= 1.9232$

$= -\frac{1}{10} \log_2\left(\frac{1}{10}\right) - \frac{1}{2} \log_2\left(\frac{1}{2}\right) - \frac{3}{20} \log_2\left(\frac{3}{20}\right)$

$- \frac{1}{20} \log_2\left(\frac{1}{20}\right) - \frac{1}{5} \log_2\left(\frac{1}{5}\right)$

$H[X] = -P_X(a) \log_2 P_X(a) - P_X(b) \log_2 P_X(b)$

$- P_X(c) \log_2 P_X(c) - P_X(d) \log_2 P_X(d)$

$- P_X(e) \log_2 P_X(e)$

$=$ 2.3219 bits

(ה) 9.3 ס

נוסחת ההסתברות השלמה: $P_X(x) = \sum_{y \in Y} P_{X,Y}(x,y)$

$$= \frac{1}{10}(\text{ب}) + \frac{1}{2}(1) + \frac{3}{20}(\text{ج}) + \frac{1}{20}(\text{د}) + \frac{1}{5}(\text{ه})$$

$$= \frac{39}{20} = 1.95$$

نأخذ N بحيث $N \geq 1$ / N عدد طبيعي $\in \mathbb{N}$

$$H(X) \leq \gamma[f] \leq H(X) + 1 .$$

$$H(X)+1 = 2.92 \implies H(X) = 1.92 \quad \text{: 1)}$$

$$\gamma[f] = 1.95$$

$$\gamma[f] = P_X(a)|f(a)| + \cdots + P_X(e)|f(e)|$$

X	$f(x)$	$\lvert f(x)\rvert$
a	0 1 0 1	a
b	1	1
c	0 1 1	3
d	0 1 0 0	d
e	0 0	2

نأخذ الأقل عدد ممكن

$\gamma[f)$ $\geq$ 1.92 $\leq$ N $\in$ $\mathbb{N}$ عدد طبيعي

$\gamma[f)$

(ב) $a^{12} \equiv b^4 \pmod{m}$ אבל $a \equiv b \pmod{m}$ לכן

(ג) $\gcd(c,b)=1$ ו- $c \mid ab$ לכן $c \mid a$

(ד) $\gcd(a,b)=\gcd(a,a+cb)$ (ז)

(ב) $\gcd(c,m)=1$ ולכן c הפיך מודולו m.
$a \equiv b \pmod{m}$ אבל $c \equiv c \pmod{m}$ ולכן
$ac \equiv bc \pmod{m}$.

(ג) $\gcd(a,b)=1$ ולכן a הפיך מודולו m.
$ac \equiv bc \pmod{m}$ אבל $a \equiv b \pmod{m}$ ולכן
$c \equiv c \pmod{m}$.

$\gcd(c,d)=1$ ו- $c \mid ab$ לכן $c \mid a$ או $c \mid b$.

$H(X) \le \log|\{x : f(x)>0\}| \le \log 6 \approx 1.792$

$H(X) \ge H(X \mid Y) = \frac{1}{6}\cdot 0 + \frac{5}{6}\cdot H(\tfrac{1}{5},\dots,\tfrac{1}{5}) = \frac{5}{6}\log 5 \approx 1.935$

$a \equiv b \bmod m$.

: تعريف 1.8.3

$a \equiv b \bmod m$ $\Leftrightarrow$ $m \mid a-b$

$a \not\equiv b \bmod m$ $\Leftrightarrow$ $m \nmid a-b$

مثال 2.8.3 ○

1) $3 \equiv 7 \bmod 4$ لأن $4 \mid 3-7$

2) $-3 \equiv 5 \bmod 4$ لأن $4 \mid -3-5$

3) $a \equiv b \bmod 2$ $\Leftrightarrow$ a, b لهما نفس الزوجية

4) $a \equiv 0 \bmod 2$ $\Leftrightarrow$ a زوجي

5) $a \equiv 1 \bmod 2$ $\Leftrightarrow$ a فردي

6) $a \equiv b \bmod 1$ دائماً

7) $a \equiv b \bmod m$ $\Leftrightarrow$ a, b لهما نفس الباقي على القسمة على m

8) $a \equiv 0 \bmod m$ $\Leftrightarrow$ $m \mid a$

9) $a \equiv b \bmod 0$ $\Leftrightarrow$ $a = b$

10) $a \equiv b \bmod m$ $\Leftrightarrow$ $a = b + mk$ لعدد صحيح k

11) $a \equiv b \bmod m$ $\Leftrightarrow$ $a = mq + r$ و $b = mq' + r$ لأعداد صحيحة q, q', r حيث $0 \le r < m$

$a = mq + r$, $b = mq' + r$

$a - b = m(q - q')$

$m \mid a - b$

$a \equiv b \bmod m$

12) $a \equiv b \bmod m$ $\Leftrightarrow$ $a = b + mk$ لعدد صحيح k

$a = mq + r$

$\Rightarrow a = mq + b - r$

$= m(q - 1) + b + (m - r)$

$a - b = (q, m + b)(q_2 m + r)$ ، $q_2 \in \mathbb{N}$

$a - b \in \mathbb{N}$ ، $q_2 \in \mathbb{N}$ ، $q, m + b > 0$ لأن $a > b$ (*1) و (*2):

(*2) $c = q_1 m + d$ و $c \equiv d \bmod m$ $\Rightarrow$ $q_1 \in \mathbb{Z}$ و $0 \le d < m$

(*1) $a = q m + b$ و $a \equiv b \bmod m$ $\Rightarrow$ $q \in \mathbb{Z}$ و $0 \le b < m$

(1.8.3)

$a \equiv b \bmod m$ و $c \equiv d \bmod m$ $\Rightarrow$ $a + c \equiv b + d \bmod m$

: تعريف 3.8.3

$a \equiv b \bmod m$ ، $c \equiv d \bmod m$

$a \not\equiv b \bmod m$ و $c \not\equiv d \bmod m$

1.8.3

2.8.3

$\Leftarrow \quad a^{k+1} \equiv b^{k+1} \bmod m.$

$\gcd(c,b) = 1$ إذا كان $c \mid ab$

$c \mid a$

تمرين 3.19:

$ab = kc$ حيث $k \in \mathbb{Z}$ و $\frac{ab}{c} \in \mathbb{Z}$

الحل:

$a^k \equiv b^k \bmod m$ فإن $a \equiv b \bmod m$

(تذكر أن $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + b^{k-1})$)

تمرين 3.20: أثبت أن $2^{340} \equiv 1 \bmod 341$

الحل:

$2^{10} = 1024 \equiv 1 \bmod 11$

$2^{340} = (2^{10})^{34} \equiv 1^{34} \bmod 11$

$2^{340} \equiv 1 \bmod 11$

$2^5 = 32 \equiv 1 \bmod 31$

$2^{340} = (2^5)^{68} \equiv 1^{68} \bmod 31$

$2^{340} \equiv 1 \bmod 31$

$\gcd(11, 31) = 1$ و $341 = 11 \cdot 31$

$2^{340} \equiv 1 \bmod 341$

$\gcd(a+cb, b) = \gcd(a, b)$.

(d ∤ 1 ∩

:الحل

$\gcd(b, c) = \gcd(3, 7) = 1$ ،

$7 + 3$ $b + c$ ، a ∩ b ∩ c ∩ d ∩ e ∩ f ∩ g ∩ h ∩ i ∩ j ∩ k ∩ l ∩ m ∩ n ∩ o ∩ p ∩ q ∩ r ∩ s ∩ t ∩ u ∩ v ∩ w ∩ x ∩ y ∩ z ∩ $3 \mid 6$ ∩ $p \nmid n$.

$\gcd(b, c) = 1$ ∩ $\frac{a}{c} \in \mathbb{Z}$ ∩ $a \mid bc$.

$\int \ln x \, dx$: $a = 6$ ، $b = 7$ ، $c = 3$.

$c \mid \alpha$ $f > 1$.

$\int \frac{\alpha}{c} \, dx$ $f > 1$ ∩ $\gcd(b, c) = 1$ ∩ $f > 1$ ∩ $\int \frac{b}{c} \, dx$.

$\Leftarrow$ $\int \frac{\alpha}{c} \, dx$ ∩ $\int \frac{b}{c} \, dx$.

$\cos(\alpha-\beta) = \frac{4}{5}\cdot\frac{4}{5} + \frac{3}{5}\cdot\frac{3}{5} = \frac{25}{25} = 1$ נציב בנוסחת הקוסינוס של ההפרש

$\alpha-\beta = 0$ ולכן $\alpha = \beta$ כלומר הזוויות שוות.

ב. $\alpha+\beta = 90°$ אם $\cos\alpha = \sin\beta$

$\cos\alpha = \sin(90°-\alpha)$ לפי נוסחת הקוסינוס של ההפרש

$\sin(\alpha+\beta) = \sin\alpha\cdot\cos\beta + \cos\alpha\cdot\sin\beta$ לפי נוסחת הסינוס של הסכום

$\sin(\alpha+\beta) = \frac{3}{5}\cdot\frac{4}{5} + \frac{4}{5}\cdot\frac{3}{5} = \frac{24}{25}$

$\cos(\alpha+\beta) = \frac{4}{5}\cdot\frac{4}{5} - \frac{3}{5}\cdot\frac{3}{5} = \frac{7}{25}$

$\sin(\alpha+\beta) + \cos(\alpha+\beta) = \frac{24}{25} + \frac{7}{25} = \frac{31}{25}$

ג. $\alpha+\beta = 90°$ אם $\cos\alpha = \sin\beta$

$\cos\alpha = \sin(90°-\alpha)$ לפי נוסחת הקוסינוס של ההפרש

$\sin(\alpha+\beta) = \sin\alpha\cdot\cos\beta + \cos\alpha\cdot\sin\beta$ לפי נוסחת הסינוס של הסכום

$\sin(\alpha+\beta) = \frac{3}{5}\cdot\frac{4}{5} + \frac{4}{5}\cdot\frac{3}{5} = \frac{24}{25}$

$\cos(\alpha+\beta) = \frac{4}{5}\cdot\frac{4}{5} - \frac{3}{5}\cdot\frac{3}{5} = \frac{7}{25}$

$\sin(\alpha+\beta) + \cos(\alpha+\beta) = \frac{24}{25} + \frac{7}{25} = \frac{31}{25}$

ד. $\alpha+\beta = 90°$ אם $\cos\alpha = \sin\beta$

$\cos\alpha = \sin(90°-\alpha)$ לפי נוסחת הקוסינוס של ההפרש

$\sin(\alpha+\beta) = \sin\alpha\cdot\cos\beta + \cos\alpha\cdot\sin\beta$ לפי נוסחת הסינוס של הסכום

$\sin(\alpha+\beta) = \frac{3}{5}\cdot\frac{4}{5} + \frac{4}{5}\cdot\frac{3}{5} = \frac{24}{25}$

$\cos(\alpha+\beta) = \frac{4}{5}\cdot\frac{4}{5} - \frac{3}{5}\cdot\frac{3}{5} = \frac{7}{25}$

$\sin(\alpha+\beta) + \cos(\alpha+\beta) = \frac{24}{25} + \frac{7}{25} = \frac{31}{25}$

ה. $\alpha+\beta = 90°$ אם $\cos\alpha = \sin\beta$

$\cos\alpha = \sin(90°-\alpha)$ לפי נוסחת הקוסינוס של ההפרש

$\sin(\alpha+\beta) = \sin\alpha\cdot\cos\beta + \cos\alpha\cdot\sin\beta$ לפי נוסחת הסינוס של הסכום

$\sin(\alpha+\beta) = \frac{3}{5}\cdot\frac{4}{5} + \frac{4}{5}\cdot\frac{3}{5} = \frac{24}{25}$

$\cos(\alpha+\beta) = \frac{4}{5}\cdot\frac{4}{5} - \frac{3}{5}\cdot\frac{3}{5} = \frac{7}{25}$

$\sin(\alpha+\beta) + \cos(\alpha+\beta) = \frac{24}{25} + \frac{7}{25} = \frac{31}{25}$

x				
$y \in \mathbb{Z}_{26}$	6	8	1	14
$x \in$	5	I	13	0

תרגיל 5

נתון $f(x) = x^3 + 2x + 1$ מעל $\mathbb{Z}_5$. מצא את כל השורשים של $f(x)$ ב-$\mathbb{Z}_5$.

$k \in \mathbb{Z}_{26}^{2\times 2}$ לכן יש לפענח את האותיות

של הטקסט מוצפן בקבוצות של 2 אותיות

כל פעם. לפי הכלל מפענח:

$$d_k(y_1, y_2) = (y_1, y_2)\,k^{-1} \bmod 26.$$

<u>נחשב את ההופכית k^{-1}:</u>

$$k^{-1} = |k|^{-1} C^{t}$$

$$|k| = \begin{vmatrix} 3 & 4 \\ 7 & 11 \end{vmatrix} = 5 \bmod 26.$$

$$1 = \gcd(5, 26) = \gcd(|k|, 26)$$

לכן קיים $|k|^{-1}$ לכן הצפן ניתן לפענח.

$$|k|^{-1} \bmod 26 = 5^{-1} \bmod 26 \overset{\text{נוסחאון}}{=\!=} 21$$

המטריצה של הקופקטורים:

$$C = \begin{pmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{pmatrix} \qquad k = \begin{pmatrix} 3 & 4 \\ 7 & 11 \end{pmatrix}$$

C_{11}

$K = \begin{pmatrix} 3 & 4 \\ 7 & 11 \end{pmatrix}$ $\quad C_{11} = (-1)^{1+1} |11| = 11$

C_{12}

$K = \begin{pmatrix} 3 & 4 \\ 7 & 11 \end{pmatrix}$ $\quad C_{12} = (-1)^{1+2} |7| = -7$

C_{21}

$K = \begin{pmatrix} 3 & 4 \\ 7 & 11 \end{pmatrix}$ $\quad C_{21} = (-1)^{1+2} |4| = -4$

C_{22}

$K = \begin{pmatrix} 3 & 4 \\ 7 & 11 \end{pmatrix}$ $\quad C_{22} = (-1)^{2+2} |3| = 3$

$C = \begin{pmatrix} 11 & -7 \\ -4 & 3 \end{pmatrix} \Rightarrow C^t = \begin{pmatrix} 11 & -4 \\ -7 & 3 \end{pmatrix}$ $\mod 26$

$K^{-1} = |K|^{-1} C^t = 21 \begin{pmatrix} 11 & -4 \\ -7 & 3 \end{pmatrix} \mod 26$

$$= \begin{pmatrix} 231 & -84 \\ -147 & 63 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 23 & 20 \\ 9 & 11 \end{pmatrix}.$$

$Y \in C$	G	I	B	O
$y \in \mathbb{Z}_{26}$	6	8	1	14
x	2	6	17	18

$$(6 \quad 8)\, k^{-1} \bmod 26 = (6 \quad 8)\begin{pmatrix} 23 & 20 \\ 9 & 11 \end{pmatrix} \bmod 26$$

$$= (210 \quad 208) \bmod 26$$

$$= (2 \quad 0)$$

$$(1 \quad 14)\, k^{-1} = (1 \quad 14)\begin{pmatrix} 23 & 20 \\ 9 & 11 \end{pmatrix} \bmod 26$$

$$= (149 \quad 174) \bmod 26$$

$$= (19 \quad 18)$$

x	c	e	h	s
$x \in \mathbb{Z}_{26}$	2	6	12	18
$y \in \mathbb{Z}_{26}$	6	8	1	14
$y \in c$	G	I	B	O

$$\text{تمرين 1: } 26 \equiv 12 \times 2 \pmod{26}$$

$$\text{حل المعادلة } 7x \equiv 15 \pmod{26}$$