

باسم تعالیٰ

نیم ساعه

مبانی ریاضی و منطق

پویش دانش - 94104185

دکتر میرحسین

$$m(x) = x^3 + x + 1$$

$$a = x + 1 \quad \rightarrow \quad (x+1)(x^2+x) = x^3 + 2x^2 + x = x^3 + x \pmod{m(x)} = 1 \pmod{m(x)}$$

با مشاهده ضرایب داریم

$$\Rightarrow (x+1)^{-1} = x^2 + x \pmod{m(x)} \quad GF(2^3)$$

- ۲- (5.3) مجموعه معین شده خواص اعداد را دارد
- ① $\checkmark (R, +) \rightarrow$ گروه جابجایی
 - ② $\checkmark a, b \in R \Rightarrow a \times b \in R$ (دفعه ضرب)
 - ③ \checkmark کسرت پذیری تحت \times (حلقه غیر جابجایی است)
 - ④ \checkmark بخش ضرب روی صفر (۵۰ مورد فوق را اثبات کنیم)

①: $(R, +) \rightarrow ?$ گروه

1. $\forall a, b \in R \rightarrow a + b \in R \checkmark$ (تایید اصول جمع)
2. $(a+b)+c \stackrel{?}{=} a+(b+c) \checkmark$

$a+b = b+a = c$

که طبق جدول جمع هر عنصر افزودن ۰، و جمع دو عنصر تفاوت برابر عنصر دوم می شود

③: \checkmark نایز $(R, +)$ و گروه

3. $\checkmark 0 =$ عضو ۰ $0 + \frac{a}{b} = \frac{a}{b} + 0 = \frac{a}{b} \checkmark$
4. $a + a = 0 \checkmark$ (عضو قرینه هر عنصر، خودش می باشد)

طبق جدول ضرب

$$\Rightarrow \forall a, b \in \mathbb{R} \Rightarrow a \times b \in \mathbb{R} \checkmark$$

*
طبق جدول ضرب داریم: $x \in \mathbb{R}$

$$\textcircled{c} \quad a \times (b+c) \stackrel{?}{=} \underbrace{a \times b}_b + \underbrace{a \times c}_c \checkmark$$

$$\begin{cases} 0 \times x = x \times 0 = 0 \\ a \times x = x \\ b \times x = x \\ c \times x = 0 \end{cases}$$

$$a \times (a+b) \stackrel{?}{=} \underbrace{a \times a}_a + \underbrace{a \times b}_b \checkmark$$

$$a \times (b+a) \stackrel{?}{=} \underbrace{a \times a}_a + \underbrace{a \times a}_a \checkmark$$

برسخت a را درسم

برسخت b نیز درسم a است

$$c \times x = 0 \text{ فوق بار } c$$

بنابر این همه سخت برایش برقرار است!

نهایتاً باید این سه سخت را برای a و b درستی ثابت کنیم!

$$(b+c) \times a \stackrel{?}{=} \underbrace{b \times a}_b + \underbrace{c \times a}_c$$

\rightarrow \times
این دو را نمیدانیم!

بنابر این حتماً نادرست!

$$\text{a)} \quad \begin{array}{r} x^3 + 1 \quad | \quad x^2 + x + 1 \\ x^3 + x^2 + x \\ \hline x^2 + x + 1 \\ x^2 + x + 1 \\ \hline 0 \end{array}$$

$$\Rightarrow (x^2 + x + 1, x^3 + 1) = x^2 + x + 1 \checkmark$$

$$\text{b)} \quad \begin{array}{r} x^3 + x + 1 \quad | \quad x^2 + 1 \\ x^3 + x \\ \hline x + 1 \end{array}$$

$$\begin{array}{r} x^2 + 1 \quad | \quad 1 \\ x^2 + 1 \\ \hline 0 \end{array} \Rightarrow (x^3 + x + 1, x^2 + 1) = 1 \checkmark$$

$$c) \quad x^3 - 2x + 1 \equiv x^3 + 3x + 1, \quad x^2 - x - 2 \equiv x^2 + 4x + 3$$

$$\Rightarrow \begin{array}{r} x^3 + 3x + 1 \quad | \quad x^2 + 4x + 3 \\ \underline{x^3 + 4x^2 + 3x} \\ x^2 + 1 \\ \underline{x^2 + 4x + 3} \\ x + 3 \end{array}$$

$$\begin{array}{r} x^2 + 4x + 3 \quad | \quad x + 3 \\ \underline{x^2 + 3x} \\ x + 3 \\ \underline{x + 3} \\ 0 \end{array}$$

$$\Rightarrow (x^3 + 3x + 1, x^2 + 4x + 3) = x + 3 \quad \checkmark$$

$$d) \quad x^4 + 8x^3 + 7x + 8 \quad | \quad 2x^3 + 9x^2 + 10x + 1$$

$$\begin{array}{r} x^4 + 8x^3 + 5x^2 + 6x \\ \underline{9x^3 + 6x^2 + x + 8} \\ 9x^3 + 2x^2 + x + 16 \\ \underline{4x^2 + 9} \end{array}$$

$$6x + 10$$

$$\begin{array}{r} 2x^3 + 9x^2 + 10x + 1 \quad | \quad 4x^2 + 9 \\ \underline{2x^3 + 10x} \\ 9x^2 + 1 \\ \underline{9x^2 + 1} \\ 0 \end{array}$$

$$\Rightarrow (x^4 + 8x^3 + 7x + 8, 2x^3 + 9x^2 + 10x + 1) = 4x^2 + 9 \quad \checkmark$$

$$m(x) = x^5 + x^4 + x^3 + x + 1 \quad GF(2^5)$$

$$\Rightarrow g^5 + g^4 + g^3 + g + 1 = 0 \Rightarrow g \equiv -g^4 - g^3 - g - 1 \equiv g^4 + g^3 + g + 1$$

0	0	00000	0
$g (= g^0)$	1	00001	1
g^1	g	00010	2
g^2	g^2	00100	4
g^3	g^3	01000	8

g^4	g^4	10000	16	g^{21}	$g^4 + 1$	10001	17
g^5	$g^4 + g^3 + g + 1$	11011	27	g^{22}	$g^4 + g^3 + 1$	11001	25
g^6	$g^3 + g^2 + 1$	01101	13	g^{23}	$g^3 + 1$	01001	9
g^7	$g^4 + g^3 + g$	11010	26	g^{24}	$g^4 + g$	10010	18
g^8	$g^3 + g^2 + g + 1$	01111	15	g^{25}	$g^4 + g^3 + g^2 + g + 1$	11111	31
g^9	$g^4 + g^3 + g^2 + g$	11110	30	g^{26}	$g^2 + 1$	00101	5
g^{10}	$g^2 + g + 1$	00111	7	g^{27}	$g^3 + g$	01010	10
g^{11}	$g^3 + g^2 + g$	01110	14	g^{28}	$g^4 + g^2$	10100	20
g^{12}	$g^4 + g^3 + g^2$	11100	28	g^{29}	$g^4 + g + 1$	10011	19
g^{13}	$g + 1$	00011	3	g^{30}	$g^4 + g^3 + g^2 + 1$	11101	29
g^{14}	$g^2 + g$	00110	6	g^{31}	1	00001	1
g^{15}	$g^3 + g^2$	01100	12				
g^{16}	$g^4 + g^3$	11000	24				
g^{17}	$g^3 + g + 1$	01011	11				
g^{18}	$g^4 + g^2 + g$	10110	22				
g^{19}	$g^4 + g^2 + g + 1$	10111	23				
g^{20}	$g^4 + g^2 + 1$	10101	21				

$$\begin{cases} G_P = T_C & , G=6, T=19 \\ O_P = J_C & , O=14, J=9 \end{cases}$$

$$C = PK_1 + K_2 \quad \text{نظمی:}$$

$$\Rightarrow \begin{cases} 19 \equiv 6K_1 + K_2 & (*) \\ 9 \equiv 14K_1 + K_2 & (**)$$

الامثلة بعد

$$(+) - (+) \rightarrow 10 \equiv -8K_1 \xrightarrow{\div 2} 5 \equiv -4K_1 \Rightarrow 8 \equiv 2K_1$$

$$\Rightarrow K_1 \equiv 2 \Rightarrow \begin{cases} K_1 = 2 \\ \text{or} \\ K_1 = 15 \end{cases}$$

۲ صحت دارد و معادله داریم و K_2
را پیدا کنیم (الترقال قبل باشد)

$$\textcircled{1} K_1 = 2 \rightarrow \begin{cases} (*) \Rightarrow 19 \equiv 2 \times 6 + K_2 \Rightarrow K_2 \equiv 7 \\ (++) \Rightarrow 9 \equiv 14 \times 2 + K_2 \Rightarrow K_2 \equiv 7 \end{cases} \checkmark \Rightarrow K_2 \equiv 7$$

$$\textcircled{2} K_1 = 15 \rightarrow \begin{cases} (*) \Rightarrow 19 \equiv 6 \times 15 + K_2 \Rightarrow K_2 \equiv 7 \\ (++) \Rightarrow 9 \equiv 14 \times 15 + K_2 \Rightarrow K_2 \equiv 7 \end{cases} \checkmark \Rightarrow K_2 \equiv 7$$

$$\Rightarrow \begin{cases} K_1 = 2 \\ K_1 = 15 \end{cases} \text{ و } K_2 = 7 \text{ صحت ۲ صحت}$$

۷ - (3.6) این سطر صحت معادله دارد و جنبی توی (مانند جایی و...) حداقل ۵ نفر

این آن نه شده ایم.
لیست طوب کی که ممکن است صحت باشد همان ۵ نفر در نظر گرفت:

این آدمی نوشته شد، در دوام بخش خاصی از یک کتاب است که می دهد. طبق جدول یعنی 534، 534 صفت

از کتاب از طرف... طبقه دوم به C2 یعنی Column 2، ستون دوم جدول آن صفی از آن می دهد

اعداد یعنی نشان دهنده ی کلمات آن ستون هستند و مدخله است و نهایتاً کلمات "DOUGLAS" و

BIRLSTONE، چهارمین کلماتی هستند که در آن صفی حذف شده!

7- (3.4) ابتدائی حروف! درست کیا کریں (کچھ ان کے علاوہ اضافی) ہیں

ان منطق پر روشنی ملے، مرقعہ، پائیں، قدر حروف اہل طبقہ (چھوڑ دینے حروف دارم)
درجہ دہ، پراس کی حالت میں دماغی پریم ان، روشنی کی لیم.

بہترین نمائندگی $N \rightarrow e$ و $0Zn \rightarrow the$ بہترین نمائندگی
نیز درست آکسیجن $\rightarrow \begin{cases} 2 \rightarrow h \\ 0 \rightarrow t \end{cases}$

O \rightarrow t (0Zn \rightarrow the)

S \rightarrow i (nsoZng \rightarrow either)

Z \rightarrow h (0Zn \rightarrow the)

L \rightarrow o (ol \rightarrow to)

Q \rightarrow a (q \rightarrow a)

C \rightarrow s (sc \rightarrow is)

F \rightarrow n (flo \rightarrow not)

J \rightarrow r (lj \rightarrow or)

* حال، حروف نمائندگی باہر کی پروازیں

(T, A, O, N, I, R, S, H)

درجہ دہ، ترتیب درست آکسیجن (نور) ترتیب نوشتہ شود

نیت، و این ترتیب پراس نمائندگی درجہ دہ

حال حروف نمائندگی مرقعہ

(D, L, U, C, M)

R \rightarrow l (qnqrc \rightarrow meals)

G \rightarrow m (Zsg \rightarrow him)

B \rightarrow d (qfb \rightarrow and)

E \rightarrow u (leo \rightarrow out)

X \rightarrow c \rightarrow نیت "c" باقی ماندہ ✓

* نیت حروف نمائندگی پائیں

(P, F, y, w, G, B, v)

W \rightarrow w (wZsxZ \rightarrow which)

K \rightarrow f (kjSnfbc \rightarrow friends)

D \rightarrow v (Zqdu \rightarrow have)

Y \rightarrow g (klyg \rightarrow fog)

H → P (Zghhnt → happen)
P → b (OqPrn → table)
v → y (lfrv → only)

M → K (mflwf → known)
A → X (KSanb → fixed)

جوز مر :

(y, k, q, x, z)

I }
T } → { Q
U } { J
{ Z

→ رقص نسیه
زواره قبل است
ممنون
دولاد
آه-آه

I → Q
T → J
U → Z

صل طه فر :

P	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
C	q	p	x	b	n	k	y	z	s	t	m	r	g	f	l	h

P	Q	R	S	T	U	V	W	X	Y	Z
C	i	j	c	o	e	d	w	a	v	u

نسیه قس لیلی :

Phileas Fogg was not known to have either wife or children, which may happen to the most honest people; either relatives or near friends, which is certainly more unusual. he lived alone in his house in Saville Row, whither none penetrated. a single domestic sufficed to serve him. he breakfasted and dined at the club, at mathematically fixed, in the same room, at the same table, never taking his meals with other members, much less bringing a guest with him; and went home

✓






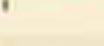




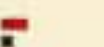

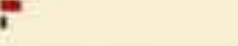
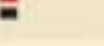

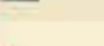

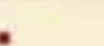
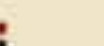
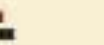



at exactly midnight, only to retire at once to bed, he never used the cosy chambers which the reform provides for its favoured members. he passed ten hours out of the twenty-four in Saville row either in sleeping or making his toilet. ■

— — — —

^

Occurency and Frequency Analysis

% calculated | % expected

↑↓	↑↓	↑↓	↑↓
N	84×	14.69%	
O	49×	8.57%	
S	46×	8.04%	
Z	43×	7.52%	
L	38×	6.64%	
Q	37×	6.47%	
C	37×	6.47%	
F	36×	6.29%	
J	36×	6.29%	
R	23×	4.02%	
G	22×	3.85%	
B	18×	3.15%	
E	14×	2.45%	
X	14×	2.45%	
W	13×	2.27%	
K	12×	2.1%	
D	10×	1.75%	
Y	10×	1.75%	
H	9×	1.57%	
P	8×	1.4%	
V	7×	1.22%	
M	4×	0.7%	
A	2×	0.35%	

#N : 23 Σ = 572.00 Σ = 100.01 #N : 23