

# 66

سرویس بر مفاهیم سود و نیاز تک روی اطلاعات

نتیجہ اورڈپی: متوسط احتمال یا اطلاعات موجود در صریح از منع  
Uncertainty Entropy

تعمیر صادف X در میں M حیل باحال صدای  $p_1, \dots, p_M$  را در تصریح کریں:

$$X = \begin{pmatrix} x_1, \dots, x_M \\ p_1, \dots, p_M \end{pmatrix}, \quad \sum_{i=1}^M p_i = 1$$

$$H(X) = H(p_1, \dots, p_M) = \sum_{i=1}^M p_i \log \frac{1}{p_i} = - \sum_{i=1}^M p_i \log p_i = -E[\log p(x)]$$

↓  
bit/sym

کوہی میں منع حیال بستہ سود و نیاز (بطریق متوسط) جو کہ منع راستہ نہ ہے۔

مفہوم اورڈپی:

$$H(X) > 0$$

$$\forall i, j \in \{1, \dots, M\} \quad " = " \text{ iff } p_i = p_j = \frac{1}{M} \quad \Rightarrow H(X) \leq \log M$$

$$H(X, Y) = - \sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log p(x_i, y_j)$$

نہیں

اُرڈپی سسک

joint entropy

$$" = " \text{ iff } X \perp\!\!\!\perp Y \quad \Rightarrow H(X, Y) \leq H(X) + H(Y)$$

## Conditional entropy

آندره سرتی

باور  $H(X|Y)$  میتواند میانگین سریع صادرن  $X$  باز از  $Y$  باشد.

(فیزیک علم بود) تمریع صادرن  $Y$  را با  $p(y)$  داشت.

$$H(X|Y=y_j) = - \sum_{i=1}^M p(x_i|y_j) \log p(x_i|y_j)$$

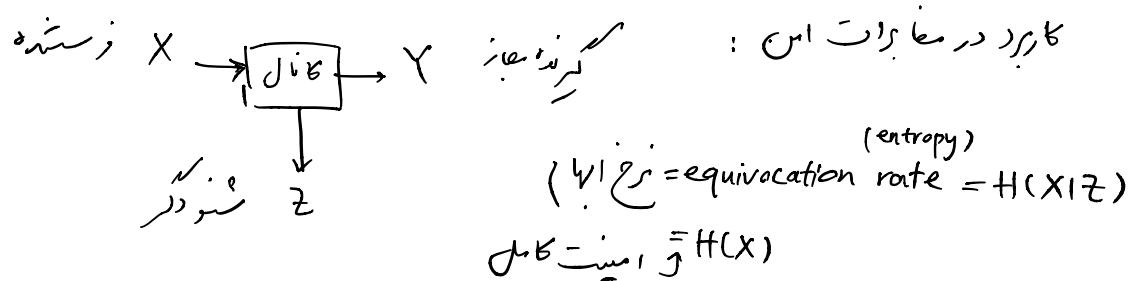
$$H(X|Y) = \sum_{j=1}^L H(X|Y=y_j) p(y_j)$$

$$= - \sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log p(x_i|y_j)$$

: (Chain rule) ارجاعی

$$H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

"=" iff  $X \perp\!\!\!\perp Y$   $\leftarrow H(X|Y) \leq H(X)$  خواست



## Mutual Information

اطلاعات متعارف

$X \rightarrow Y$

$$I(X;Y) \stackrel{\Delta}{=} H(X) - \underbrace{H(X|Y)}_{\begin{array}{l} \text{اولاً} \\ \text{رسور X} \end{array}} = \underbrace{H(Y) - H(Y|X)}_{\begin{array}{l} \text{رسور Y} \\ \text{رسور X} \\ \text{زیرینت Y} \end{array}}$$

$$\begin{aligned} &= H(X) + H(Y) - \underbrace{H(X,Y)}_{H(X) + H(Y|X)} \\ &= H(Y) - H(Y|X) \end{aligned}$$

$$= I(Y; X)$$

$$= \sum_{i=1}^M \sum_{j=1}^L p(x_i, y_j) \log \frac{p(x_i, y_j)}{p(x_i)p(y_j)}$$

$$= D_{KL}(p(x,y) || p(x)p(y))$$

$$I(X;Y) \geq 0, \quad \stackrel{\text{iff}}{=} X \perp\!\!\!\perp Y$$

- حالت

ابدأ بالبرهان ...

# 71

$$I(X;Y) = H(X) - H(X|Y) =$$

$$\rightarrow H(X_1 = \cdot | X_1 Y) \quad \textcircled{1}$$

$$\text{از طرفی } H(X|Y) \leq H(X, K|Y) = H(K|Y) + H(X|Y, K)$$

$$\Rightarrow H(X|Y) \leq H(K|Y) \quad (2)$$

$$\textcircled{1}, \textcircled{2} \Rightarrow H(X) = H(X|Y) \leq H(K|Y) \leq H(K)$$

↑  
ترمله کردن آن را در هزار از این نیز راه

$$\Rightarrow H(X) \leq H(K)$$

نحو درسِ اس کامل طور کلید ہے جو بست بُر اصطلاح سَن اصلی ہے۔

مثلاً دیس کلر بازرس طعلہ :  $|K| = \text{تعداد کلمات} = 2^L$

$$H(X) \leq \log |K| = \log_2^L = L \text{ bits}$$

با فرض قرآن <sup>↑</sup> مکتوّه است کلمه ها  
(هم امثال)

$$I(X;Y) \geq H(X) - H(K)$$

نحوه دریک سیم با کسر کوچکتر شدن رمزه اطلاعات بسته در اینجا  
سندگر را در داده.

$$H(K) \geq H(X)$$

نمایش:  $Y = X \oplus K$  باشد و میتوانیم  $H(K) \geq H(X)$  باشد.  
کافی است.

مثال ۱ - طولانی بولن کلید

۲ - در صورت که صنایع از کلید استفاده نموده اسیب نیز کلید را مقابله نماید (دانشمندانه رسم رمزه متناظر)

# 74

## Number Theory

نظریہ اعداد

Stalling { Chapter 2  
Chapter 5

سراج :

Denning: Section 1.6

- الگوریتم اگزیمین جو ایسا سے کوئی دو عدد کا بزرگ ترین فراہم کرنے والا ہے۔  
gcd (greatest common divisor)

لار . Stalling - Sec. 2.2

## Modular Arithmetic

حساب معمولی ایجاد

Congruences

هم المنسقة

تعریف : جو ایسا دعویٰ ہے کہ  $a \equiv b \pmod{n}$  ایسا ہے کہ  $a$  اور  $b$  کو  $n$  کے مول میں بیان کرنے والے بیانات اکر رکھاں جائیں۔

$\exists k \in \mathbb{Z} : a - b = kn$

اک طبقہ نظریہ :

$$n | a - b \Leftrightarrow n \text{ divides } a - b$$

$$a \equiv b \pmod{n}$$

: نسبت

$$a \equiv_n b$$

$$a \equiv^{\text{mod } n} b$$

$$a \equiv^n b$$

$$21 \equiv 5 \pmod{4}$$

٦

$$21 \equiv -9 \pmod{10}$$

( Complete Set of Residues ) مجموعه کامل باقیمانده:

نیز بوسیل جگ نهاد،  $Z_n = \{r_1, \dots, r_n\}$  گروه معمولی است.

$$a \equiv r_i \pmod{n}$$

بافرض  $r_i \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$ :  $\sum r_i \leq n$

$$a \bmod n = r$$

$$J \in \frac{\mathbb{Z}}{4\mathbb{Z}} \rightarrow \begin{cases} [0] = \{-\dots, -12, -8, -4, 0, 4, 8, 12, \dots\} \\ [1] = \{-\dots, -11, -7, -3, 1, 5, 9, 13, \dots\} \end{cases} \quad \text{residue class}$$

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

بعنوان دیگر مجموع اندارهای مخصوص درمانی تغییرات می‌نمایند

• i.e)  $\sigma^1$  (Comutative ring)

انها) حاسبات جمع، نظریه رنگ در ریاضیات و آمار، حاسبات اعداد صحیح و سری

کاصل تیغی در یارانه است لفظ modern یعنی حصر معنی فنیم (هم ریخته) از

حلقة اعلاء الرسم  $\Rightarrow$  حلقة طابع بنيك فوق سبأ ( مقصورة زر )

تخصیص (اصل حساب پیمانه ای) : اگر  $a_1, a_2$  اعداد صحیح احتیاطی از

کلیات  $\mathbb{Z}$  باشند و  $n$  عدد مثبت کوچکتر از  $a_1, a_2$  باشد، آنگاه  $a_1 \times a_2 \mod n = (a_1 \mod n) \times (a_2 \mod n) \mod n$

اعداد صحیح؟ اعداد صحیح نیستند

$$(a_1 \text{ op } a_2) \mod n = [(a_1 \mod n) \text{ op } (a_2 \mod n)] \mod n$$

$$a_1 = k_1n + r_1 \quad \text{و} \quad a_1 \mod n = r_1 \quad \text{این بیان تعریفی است}$$

$$a_2 = k_2n + r_2 \quad \text{و} \quad a_2 \mod n = r_2$$

کل خالص از

$$11 \mod 8 = 3$$

: مثال

$$15 \mod 8 = 7$$

$$(11 \mod 8 + 15 \mod 8) \mod 8 = 10 \mod 8 = 2$$

$$(11 + 15) \mod 8 = 26 \mod 8 = 2$$

$$[(11 \mod 8) \times (15 \mod 8)] \mod 8 = 21 \mod 8 = 5$$

$$(11 \times 15) \mod 8 = 165 \mod 8 = 5$$

نتیجه: ناتوانی در اثبات صدقه دادن

$$a^t \bmod n = \left( \prod_{i=1}^t a \right) \bmod n = \left( \prod_{i=1}^t (a \bmod n) \right) \bmod n$$

$$= (a \bmod n)^t \bmod n$$

$$4^6 \bmod 7 = ? \quad : \text{JLW}$$

$$1. \quad 4^6 = 4096 \longrightarrow 4096 \bmod 7 = 1$$

$$2. \quad 4^6 \bmod 7 = (4^2)^3 \bmod 7 = (16 \bmod 7)^3 \bmod 7$$

$$= 2^3 \bmod 7 = 1$$

$$\text{tn} : a^t \bmod n \neq (a \bmod n)^t \bmod n \quad : \text{Zwischen}$$

$$\text{JLW: } (2^{7 \bmod 5}) \bmod 5 = 2^2 \bmod 5 = 4$$

$$2^7 \bmod 5 = 128 \bmod 5 = 3$$

: (جبر مختلط) صيغة تضليلية

$$(a+b) \bmod n = (b+a) \bmod n \quad \begin{matrix} \text{جبر مختلط} \\ \text{Commutative} \end{matrix}$$

$$(a \times b) \bmod n = (b \times a) \bmod n$$

$$[(a+b)+c] \bmod n = [a+(b+c)] \bmod n \quad \begin{matrix} \text{جبر مختلط} \\ \text{Associative} \end{matrix} - 1$$

$$[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n \quad \begin{matrix} \text{جبر مختلط} \\ \text{Associative} \end{matrix}$$

$$[ax(b+c)]_{mod\ n} = [axb]_{mod\ n} + [axc]_{mod\ n}$$

distributive

$$\begin{aligned} \text{ex. } & (0 + a) \bmod n = a \bmod n & (\text{identity}) & - \text{ex-4} \\ \text{ex. } & (1 \times a) \bmod n = a \bmod n \end{aligned}$$

$\forall a \in \mathbb{Z}_n, \exists a' : a + a' = 0 \pmod{n}$  *ge. 0 ist ein - 5*

$$\forall a \in \mathbb{Z}_n \setminus \{0\} : a' = m - a$$

$$a^{-1} = ?$$

$$\therefore \sqrt{a+b} \equiv a+c \pmod{n}$$

$$\text{+61} \quad b \equiv c \pmod{n}$$

$$\begin{aligned} \text{برهان بالتعويذة:} \\ (-a + (a+b)) &\equiv (-a + (a+c)) \pmod{n} \\ \Rightarrow b &\equiv c \pmod{n} \end{aligned}$$

اگر  $a \equiv b \pmod{n}$  تو  $a^m \equiv b^m \pmod{n}$

جواب سوال نوچه مرحومت کلی منع ایست و زبانی را به منوچ برقرار

این سبک بسیار باشد.

$$\text{مثال: } 6 \times 3 \mod 8 = 2 \mod 8$$

$$6 \times 7 \mod 8 = 2 \mod 8 \rightarrow 3 \neq 7 \mod 8$$

محاسبه معلوس اعداد دوستی

معلوس (خوب) در یافته  $a \in [0, n-1]$  ایست اگر و فقط

$(x \in [0, n-1] \text{ در صفحه } \bar{x}) \quad ax \equiv 1 \mod n$  ای

مثال هر عدد ممکن  $x \in [0, n-1]$  که معمول است به اول

بُشْر (غیر معلوس) است.  $(\gcd(a, n) = 1)$

$$4 \times 5 \stackrel{19}{\equiv} 1 \Rightarrow x = \bar{a}^{-1} = 5 \quad : n=19, a=4 *$$

$$4 \times x \stackrel{20}{\equiv} 1 \quad : n=20, a=4 *$$

$$\hookrightarrow \quad \begin{cases} 4 \\ 20 \end{cases} \rightarrow 4^{-1} \mod 20 = \text{دستور}$$

$\forall i < j < n \quad (a_{i,n}) = 1$  : الگوریتم در این صورت برای کل اعداد  $i < j < n$

$$a_{i \bmod n} \neq a_{j \bmod n} : \text{لزوم}$$

فیض خواهد بود از عناصر مجموع کافی باشند و مجزایی

باشد که مجموع کافی باشد  $a_{i \bmod n} = a_{j \bmod n}$  . ولذ است

اصل طوفانی اساس  $\rightarrow a_{i \bmod n} = a_{j \bmod n}$

$$\rightarrow a(i-j) = kn$$

$$\xrightarrow{(a,n)=1} n \mid i-j \rightarrow \text{جهدی}$$

$$n=7, \quad \text{جهدی} = \mathbb{Z}_7 = \{0, 1, 2, 3, \dots, 6\} : \text{جهدی}$$

$$a=5 \quad \rightarrow 5i \bmod 7, \quad \forall i \in \mathbb{Z}_7$$

$i$	$5i \bmod 7$
0	0
1	5
2	3
3	1
4	6
5	4
6	2

اگر  $a$  اول ناٹن خاصت فوق بروار است .

مثال:  $n=4 \rightarrow \mathbb{Z}_4 = \{0, 1, 2, 3\}$

$$a=2$$

$i$	$2i \bmod 4$
0	0
1	2
2	0
3	2

→

1. جواب ممکن است  
2. نتیجہ طبی برای  
     $\mathbb{Z}_4$  است

نتیجہ ( وجود دینے بی معلوم درج ) :

اگر  $(a, n) = 1$  اور  $x$  در مجموعه  $\{0, 1, \dots, n-1\}$  باشد .

: اسے رجوار کر بے طریق کے  $0 < x < n$

$$ax \bmod n = 1$$

ابت :  $a \equiv b \pmod{n}$

س طریق بینی :-  
کامل ماندها  $\mathbb{Z}_n = \{0, 1, \dots, n-1\} \equiv \{a \pmod{n}\}$   
(جایگزین)

نیازی :-

$$\exists x \ni ax \equiv 1 \pmod{n}$$

با عویض کم در صورت فعل است .

ترین : مجموع کاظن نویسندگان

The reduced set of residues

برای مجموع از مجموع کاظن نویسندگان

عنوان نسبت به اول باید

مثال:  $n=10$

$$\mathbb{Z}_n = \{0, 1, \dots, 9\}$$

مجموع کاظن نویسندگان =  $\{1, 3, 7, 9\}$

لذا: اگر عدد اول باشد!

$$\begin{aligned} \text{مجموع کاظن نویسندگان} &= \{1, \dots, n-1\} = \mathbb{Z}_n \setminus \{0\} \\ &= \mathbb{Z}_n^r \end{aligned}$$

مُرِسْتَ تَابِعُ اُولُو لِّرِ (n) φ(n)

## Euler's totient function

نکتہ: اول بسیار سادھے ہے۔

$$= \text{اندازه مجموع کوچکترین ساخته مانند} = |\mathbb{Z}_n^r|$$

$$\text{وارد} : \varphi(1) \stackrel{?}{=} 1$$

Jes:  $\varphi(5) = 4$ ,  $\varphi(8) = 4$ ,  $\varphi(10) = 4$

$$\varphi(p) = p-1 \quad : \quad \text{أول } p \text{ عدد صحيح، حيث } \varphi(p) \text{ يساوي }$$

$p-1$  دالة العدد الصحيح، حيث  $\varphi(p)$  يساوي

$$p-1 = p - \text{عدد أول}$$

$$:\varphi(a, n) = \text{أول } p$$

$$z_n^r = \left\{ r_1, \dots, r_{\varphi(n)} \right\} \stackrel{\text{دالة}}{\equiv} \left\{ ar_i \bmod n, 1 \leq i \leq \varphi(n) \right\}$$

مقدمة إلى كسرات

$$\left\{ ar_1 \bmod n, ar_2 \bmod n, \dots, ar_{\varphi(n)} \bmod n \right\}$$

اُسپاٹ:

$$(a, n) = 1$$

$$(r_i, n) = 1$$

$$(a r_i, n) = 1$$

سے کراس نہیں کر سکتے  $\{a r_i \bmod n\}$  (یہ ایک نئی

نیو مولٹیپلیکٹر کو جلیں گے  $n$  کے لئے نیو مولٹیپلیکٹر

$i \bmod n = j \bmod n \Leftrightarrow a i \bmod n = a j \bmod n$  کے لئے  $a$  کو جلیں گے

سے کراس نہیں کر سکتے ایک  $\{a r_i \bmod n\}$  (یہ ایک نئی

نیز این مجموع کا مولٹیپل  
ماں وہ حصہ است کہ درجہ کا موقع تا طبیعی بدل دیں۔

12

$$\phi(pq) = \phi(p) \phi(q) \quad \text{کیونکہ } p \text{ اور } q \text{ میں ممکنہ طور پر ایک ایسا عوامی عدد نہیں۔$$

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q).$$

اعداد  $q, p$  و  $n = pq$  الـ  $\varphi(n)$   $\rightarrow$

اعلـ  $\varphi(n)$   $\rightarrow$

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

ایساک:  $\varphi(n) = |\mathbb{Z}_n^r|$  اور  $\mathbb{Z}_n^r$  بـ  $\mathbb{Z}_n$  اول صـ عد (نسبـ بـ  $n$ ) اور

$\mathbb{Z}_n^r$   $\rightarrow$   $\mathbb{Z}_n^r$   $\rightarrow$   $\mathbb{Z}_n^r$   $\rightarrow$   $\mathbb{Z}_n^r$

$$\mathbb{Z}_n = \{0, 1, \dots, pq-1\}$$

جـ  $\rightarrow$   $\mathbb{Z}_n^r$  اول صـ عد (نسبـ بـ  $n$ ) اور  $\mathbb{Z}_n^r$   $\rightarrow$   $\mathbb{Z}_n^r$

جـ  $\rightarrow$   $\mathbb{Z}_n^r$   $\rightarrow$   $\mathbb{Z}_n^r$   $\rightarrow$   $\mathbb{Z}_n^r$

$$\cdot \{p, 2p, \dots, (q-1)p\}, \quad \{q, 2q, \dots, (p-1)q\}$$

جملة  $q-1$   جملة  $p-1$  

$$Q(n) = |Z_n^r| = n - (q-1) - (p-1) - 1$$

$\vdots$   
 $e$

$$= pq - q - p + 1 = (p-1)(q-1)$$

$$Q(15) = ? : \text{ما}^{\ell}$$

$$Z_{15}^r = \begin{matrix} /-0 \\ \text{مجموع اعداد متباعدة} \\ 15 \text{ اول سبیب} \end{matrix} .1$$

$$= \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$$\rightarrow Q(15) = 8$$

$$\varphi(15) = \varphi(3 \times 5) = (3-1)(5-1) = 8^2$$

محاسبة  $\varphi(n)$  اول طریق (لصواید):

Stalling, Table 2.6  $\rightarrow \varphi(n), n \leq 30$

$$: \underbrace{\varphi(n)}_{P_1, \dots, P_t} = n - \sum_{i=1}^t p_i$$

$$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t} = \prod_{i=1}^t p_i^{e_i}$$

$$\varphi(n) = \prod_{i=1}^t p_i^{e_i-1} (p_i - 1) = n \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right)$$

: جواب

: (Euler's product formula) مع

all  $n \geq 1$  :  $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$

Ques:  $\varphi(36) = ?$

1.  $Z^r_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25,$   
 $29, 31, 35\}$

$\rightarrow \varphi(36) = 12$

2.  $\varphi(36) = \varphi(2^2 \times 3^2) = 2^1(2-1) \times 3^1(3-1)$   
 $= 12$

$$3. \varphi(36) = 36 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 12$$

خواص  $\varphi$  (أمثلة على خواص  $\varphi$ )

$$\varphi(p^k) = p^{k-1}(p-1) \quad : \text{أمثلة على } \varphi$$

$$: \varphi(mn) = \varphi(m)\varphi(n) \frac{d}{\varphi(d)} \quad \checkmark$$

$$\varphi(mn) = \varphi(m)\varphi(n) \frac{d}{\varphi(d)}$$

$$\varphi(a) | \varphi(b) \iff a | b \quad \checkmark$$

n برای  $\varphi(n)$  عدد زیج است. آنرا

: دلایل و فال تور خود را در اینجا بخواهیم

$$2^r \mid \varphi(n)$$

(Euler - Fermat) قضیه اول - فرمات

اگر  $a^{\varphi(n)}$  باشد  $(a, n) = 1$

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\text{الكلمة المطلوبة} = \mathbb{Z}_n^r = \{r_1, \dots, r_{\varphi(n)}\}^r = \text{الكلمة المطلوبة}$$

$$0 < r_i < n , \quad i=1, \dots, \varphi(n)$$

$$\{\text{أرجون} \bmod n, \quad i=1, \dots, \varphi(n)\} \quad \text{معينة } (a, n) = 1 \quad \text{والآن}$$

لما  $a r_i \bmod n$  ) لما  $\mathbb{Z}_n^r$  في الكلمة المطلوبة

(  $i \neq j$  :  $a r_j \bmod n \neq a r_i \bmod n$ , لما  $\mathbb{Z}_n^r$  في  $n$  ?

$$\prod_{i=1}^{\varphi(n)} (a r_i \bmod n) = \prod_{i=1}^{\varphi(n)} r_i$$

$$\Rightarrow (a^{\varphi(n)}) \left( \prod_{i=1}^{\varphi(n)} r_i \right) \equiv \prod_{i=1}^{\varphi(n)} r_i \quad \bmod n$$

$$\prod_{i=1}^{\varphi(n)} ( \prod_{r_i \mid n} r_i ) = 1$$

$$\implies a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$a^{\varphi(n)} \pmod{n} = 1$$

□

Dus P/j: (Fermat) wijst

$$a^{p-1} \equiv 1 \pmod{p}, \text{ omtrent } p \nmid a, n!$$

: (Little Fermat Theorem) wijst

: (a) (maar a, P, 1) P is of 1

$$a^p \equiv a \pmod{p}$$

عینک  $(a,p)=1$  پس  $a \not\equiv 0 \pmod{p}$

$$a \mod p = \frac{a}{p} \cdot p + a \pmod{p}$$

$$\rightarrow a^p \mod p = 0$$

برای اثبات

برای

$$\text{جذب: } p=5, a=3 \rightarrow a^p = 3^5 = 243 \equiv 3 \pmod{5}$$

$$p=5, a=10 \rightarrow a^p = 10^5 \equiv 10 \pmod{5} \equiv 0 \pmod{5}$$

عین اسکوچل میگان مخفی اول رنگ را زیر

: فرم زیر معمولی

$$a^{\varphi(n)+1} \equiv a \pmod{n}$$

•  $\min_{n \geq 1} (a, n) = 1$  سایر نتایج

دکس:  $a=3, n=10 \rightarrow 3^4 \equiv 1 \pmod{10}$

$$a^{\varphi(n)} = 3^4 = 81 \equiv 1 \pmod{10}$$

$$a=2, n=11 \rightarrow 2^{10} \equiv 1 \pmod{11}$$

$$a^{\varphi(n)} = 2^{10} = 1024 \equiv 1 \pmod{11}$$

ست اهل بورن :

در بیان از الگوریتم حاصل مترنها کی مقایز داریم تا می-

اعداد اول بزرگ استحباب کنم . درین کارایه برای

آسید بعنیم سی عدده صادر فی بزرگ اهل است یا خواهد

و مجموع ندارد . الگوریتم زیر به اچال نیاز ندارد اهل بورن

اعداد را استحباب و مجموع

## Miller-Rabin

الMiller-Rabin

$$\begin{array}{c} \text{اعداد صیغ} \\ \text{فرد بزرگتر از 3} \\ n \end{array} \xrightarrow[\exists k > 0]{\text{اخطاء}} n-1 = 2^k q$$

فرد  $q$

کافیست  $n-1$  را بر  $2^k$  قسم کنیم (بار) تا به عدد زد (ق)

بایزیس  $\leftarrow$   $k, n$  برابر باشد سیقت

و دلیم (تازهانی که بین راست ! بین).

$\lambda$ : اگر  $P$  اول بوده روشنیت زیر برقرار است:

الف) جیاں  $a$  بر  $p$  کو  $a$  قسم کنیم

$$a^2 \bmod p = 1 \iff \begin{cases} a \bmod p = 1 \\ a \bmod p = -1 \bmod p = p-1 \end{cases}$$

$$p-1 = 2^k q \quad \exists k \geq 0 \quad p > 2 \quad \left. \begin{array}{l} j \in \{1, \dots, p\} \\ 1 < a < p-1 \end{array} \right\} \text{such that } a^j \equiv 1 \pmod{p}$$

$$1 < a < p-1 \rightarrow \text{exists } a$$

$$\therefore \text{exists } a \text{ such that } a^{2^k} \equiv 1 \pmod{p}$$

$$a^{2^k} \equiv 1 \pmod{p} \quad .1$$

$$\exists j \in \{1, \dots, k\} : a^{2^{j-1}q} \bmod p = -1 \bmod p = p-1$$

$$(جواب مذکور در اینجا)$$

$$a^q \bmod p, a^{2q} \bmod p, a^{4q} \bmod p, \dots, a^{2^{k_1}q} \bmod p, \dots, a^{2^{k_l}q} \bmod p, \underbrace{a^{2^{k_l}q} \bmod p}_{=1}$$

نایابی:

دنباله زیر را بارگیرید:

$$(a^q, a^{2q}, \dots, a^{2^{k-1}q}, a^{2^k q})_{\text{mod } n}$$

اگر  $n$  اول باشد، می‌توانیم حلیم رسانی به عنوان  $1$  است  
تا  $\frac{1}{n}$  عبارت  $\text{عکس}(x)$  برای  $n-1$  است

صیغه کامپیوئنیست  $\Leftrightarrow$  اول نست

سؤال: آیا چند عدد در دو سطر اول توالی فهرست  $n$  هست؟

اول است؟

کل رفعی از درست موقع برقرار نماید

n اول نسبت

$$\text{حل: } n = 2047 = 23 \times 89$$

$$n - 1 = 2 \times 1023$$

$$2^{1023} \mod 2047 = 1$$

نے سرست صورت کا نہیں کیا اور نسبت

: الـ

TEST (n)

1. Find integers  $k, q$ , with  $k > 0$ ,  $q$  odd, so that  $(n - 1 = 2^k \cdot q)$ ;
2. Select a random integer  $a$ ,  $1 < a < n - 1$ ;
3. **if**  $a^q \bmod n = 1$  **then** return("inconclusive");
4. **for**  $j = 0$  **to**  $k - 1$  **do**
5.   **if**  $a^{2^j} \bmod n = n - 1$  **then** return("inconclusive");
6. return("composite");

قطعاً اول سنت

نهاية اول باعث

اختبر  $a$

$$1 < a < n-1 \implies \Pr(\text{inconclusive}) < \frac{1}{q}$$

اختبر  $n$

نهاية اول باعث  
نهاية اول باعث

$$\Pr(\text{inconclusive}) < \left(\frac{1}{q}\right)^t$$

جواب معنی داشت:  $(a, n) = 1$  : اگر

:  $n$  بر  $a$  مخصوص نباشد

$$ax \equiv b \pmod{n}$$

$$x = ba^{q(n)-1} \pmod{n} : \text{برای اینجا}$$

اُسَّت: اگر  $x$  جواب اُسَّت زیرا:

$$\begin{aligned} ax \pmod{n} &= ba^{q(n)} \pmod{n} = (b \pmod{n}) \underbrace{\left(a^{q(n)} \pmod{n}\right)}_{=1} \\ &= b \pmod{n} \end{aligned}$$

: اینجا  $x_1, x_2$  را داشت: جواب

$$ax_1 \equiv ax_2 \pmod{n} \xrightarrow{\exists k} a(x_1 - x_2) = kn$$

$$\xrightarrow{(a, n) = 1} n | x_1 - x_2 \rightarrow \text{جواب}$$

~~نکته~~

مقدمة في عددي عدد صحيح ملائقي : المضلع  
 $(ax \equiv 1 \pmod{n})$

$$(a, n) = 1 \implies a^{-1} \equiv a^{\varphi(n)-1} \pmod{n}$$

$$d \mid p \implies a^{-1} \equiv a^{p-2} \pmod{p}$$

مقدمة في عددي عدد صحيح ملائقي : المضلع

$$5x \equiv 3 \pmod{24}$$

$$(5, 24) = 1 \implies \text{أحادي}$$

$$\varphi(24) = \varphi(2^3 \times 3) = 2^2(2-1)(3-1) = 8$$

$$x = 3 \times 5^{\varphi(24)-1} \pmod{24} = 3 \times 5 \pmod{24} = 15$$

$$5^{8-1} \pmod{24} = (5^2)^3 \times 5 \pmod{24}$$

$$1 \leftarrow = (5^2 \pmod{24})^3 \times 5 \pmod{24} = 5$$

$d \mid b$ ,  $\therefore \gcd(a, n) = d$   $\checkmark$ :  $\exists k \in \mathbb{Z}$

$ax \equiv b \pmod{n}$   $\Leftrightarrow a \mid b$

$x \equiv k \pmod{n} \Rightarrow \text{جواب } x = k + n\mathbb{Z}$

$\left\{ t, t + \frac{n}{d}, t + \frac{2n}{d}, \dots, t + (d-1)\frac{n}{d} \right\}$   $\stackrel{\text{جوابات}}{\checkmark}$

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

$$25x \equiv 15 \pmod{120} \quad : \text{مسئلہ}$$

حل:

$$\gcd(25, 120) = 5, \quad 5 \mid 15$$

: معاویہ دار اس 5 جواب زیرِ ایسا تھے:

$$\frac{25}{5}x \equiv \frac{15}{5} \pmod{\frac{120}{5}} \quad : \text{ابتدئی}$$

$$\rightarrow 5x \equiv 3 \pmod{24} \rightarrow t=15$$

$$x_i \Rightarrow x_i = 15 + i \cdot 24 \quad i=0, 1, \dots, 4$$

$$\rightarrow \{15, 39, 63, 87, 111\}$$

# النظرية الصينية للمحالات

---

## Chinese Remainder Theorem (CRT)

---

محالات

---

در این درس نسبت هرچند که محالات را در

دلیل:

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{5} \end{cases} \longrightarrow x = 6 \quad \left\{ \begin{array}{l} (2,5) = 1 \end{array} \right.$$

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{4} \end{cases} \longrightarrow \text{ناممکن} \quad \left\{ \begin{array}{l} (2,4) \neq 1 \end{array} \right.$$

سُكْنِي دِرْسِمَ كے رَكَعَاتِ حِصْنِ الْأَرْضِ خَطِي

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ اسْتَغْفِرُ

اللَّهُ أَكْبَرُ مَعَكَ دِرْسِمَ جَوَابُ الْمُؤْمِنِ

اَللّٰهُمَّ بِسْمِكَ حِصْنِ الْأَرْضِ اَولُ بُشْرٍ

(Stelling Prob. 2.33- بیان اول ) مَعْلَمَاتٍ مُعَلَّمَاتٍ

الراغب في المعرفة

نست بحص اول سن ( $i \neq j$  :  $(m_i, m_j) = 1$ )

اعداد صحيح اعشاری باشند  $a_1, \dots, a_k$  ، در این صورت روابط زیر معتبرند

$$\left\{ \begin{array}{l} b_1 x_1 \equiv a_1 \pmod{m_1} \\ \vdots \\ b_k x_k \equiv a_k \pmod{m_k} \end{array} \right. : \text{Sistema} \quad \text{PSS}$$

## ۸۔ صورتِ ذکر می باشد:

$$x = b'_1 a_1 M_1 M'_1 + \dots + b'_K a_K M_K M'_K$$

$$M_i = \frac{M}{m_i} \rightarrow (M_i, m_i) = 1 \quad : \quad \text{عوالي}$$

$$M'_i = M_i^{-1} \pmod{m_i}$$

$$b'_i = b_i^{-1} \pmod{m_i}$$

الآن نحسب  $x \pmod{m_i}$  :

$$x \pmod{m_i} = a_i \pmod{m_i} \quad (\text{براعون})$$

:

مُعَادَلَاتٍ مُنْسَبَةٍ

$$\left\{ \begin{array}{l} ax \equiv b \pmod{d_i} \\ i=1, \dots, r \end{array} \right. \iff \left\{ \begin{array}{l} ax \pmod{n} = b \\ n = d_1, \dots, d_r \\ (d_i, d_j) = 1 \quad i \neq j \end{array} \right.$$

مُعَادَلَاتٍ مُنْسَبَةٍ : 2 مُعَادَلَاتٍ مُنْسَبَةٍ

• مُعَادَلَاتٍ مُنْسَبَةٍ (  $f(x) \equiv 0 \pmod{m}$  )

مقدار معمولی می باشد

$$\begin{array}{l} 3x \bmod 10 = 1 \\ \downarrow \\ \text{لذ} \end{array}$$

$$\begin{cases} 3x \bmod 2 = 1 \\ 3x \bmod 5 = 1 \end{cases}$$

CRT

$$x = b'_1 \alpha'_1 M_1 M'_1 + b'_2 \alpha'_2 M_2 M'_2$$

$$\frac{M=10}{\longrightarrow} \rightarrow \begin{cases} m_1=2 \rightarrow M_1=5 \rightarrow M'_1=5^{-1} \bmod 2 = 1 \\ m_2=5 \rightarrow M_2=2 \rightarrow M'_2=2^{-1} \bmod 5 = 3 \end{cases}$$

$$\begin{cases} b'_1 = 3^{-1} \bmod 2 = 1 \\ b'_2 = 3^{-1} \bmod 5 = 2 \end{cases}$$

$$\begin{aligned} \longrightarrow x &= (1 \times 1 \times 5 \times 1 + 2 \times 1 \times 2 \times 3) \bmod 10 \\ &= 7 \bmod 10 \end{aligned}$$

تَصْبِيْه بِعِيْدَه حِسَنَه (Stalling Sec. 2.7 - مِنْ سِلْكِ دَرْجَه)

حُصُور صَفِيع درِيْكِ بِعِيْدَه رَاسَ تَوَان بِبِعِيْدَه هَارَه آن

حُصُور بِعِيْدَه هَارَه اول تَان دَر  
ثَالِث

مَسَال : حُصُور صَفِيع درِيْكِ بِعِيْدَه 10 رَاسَ تَوَان

$$\left\{ \begin{array}{l} 10 = 2 \times 5 \\ (2, 5) = 1 \end{array} \right. \xrightarrow{\text{5, 2}} \text{5 سَال دَر}$$

حُصُور صَفِيع درِيْكِ بِعِيْدَه 10 بِرَبِّ بِعِيْدَه اَز اَعْصَى  $Z_{10}$  است:

$$Z_{10} = \{0, 1, \dots, 9\}$$

$$\left\{ \begin{array}{l} r_2 = 0 \rightarrow x \bmod 2 = 0 \\ r_5 = 3 \rightarrow x \bmod 5 = 3 \end{array} \right. \longrightarrow x = 8$$

$$M = \prod_{i=1}^k m_i$$

میں تھے : فرض کی

$(m_i, m_j) = 1$   $i \neq j$  میں  $m_i$  دوہرے دونستہ بھم اول ہے۔

حدود صحیح درج کرنے کا سلسلہ میں

: سال نادیشی  $(Z_{m_i}, \dots)$

عکس  
\*)  $A \longleftrightarrow (a_1, a_2, \dots, a_k)$

$$, a_i \in Z_{m_i}, A \in Z_M$$

کیا

$$a_i = A \bmod m_i \quad 1 \leq i \leq k$$

: درجیا درج : CRT

ادعای ۱: معادله مساله  $\Leftrightarrow$  نکته

$\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k} \rightarrow \mathbb{Z}_M$  دستیابی

$0 \leq A \leq M$  برای هر عدد  $\exists$  نکته

ویرایش  $(a_1, \dots, a_k)$  مطابق  $\Leftrightarrow$   $a_i \in \mathbb{Z}_{m_i}$

نکته:  $A \rightarrow (a_1, \dots, a_k)$

کافی است:  $a_i = A \pmod{m_i}$

$(a_1, \dots, a_k) \rightarrow A$

$M_i = \frac{M}{m_i}$   $i=1, \dots, k$   $\xrightarrow{(M_i, m_i)=1}$  اول  
 $M'_i = M_i^{-1} \pmod{m_i}$

$A = \sum a_i M_i M'_i \pmod{M}$

ادعاء ٢ : عمليات على المجموعات

طور عمليات على مجموعات مترافق

$$(A \text{ op } B) \text{ mod } M \iff ((a_1 \text{ op } b_1) \text{ mod } m_1, \dots, (a_k \text{ op } b_k) \text{ mod } m_k)$$
$$\text{op} \in \{+, -, \times\}$$

كاراكتريزهارز : ممكنت  $\rightarrow$  مجموعات

ساده كائن ( $M$ ) بشرطه كـ عوامل

أمثل  $M$  شخص يبني

$$A = 973 \bmod 1813$$

: Jw<sup>o</sup>

$$M = 1813 = 37 \times \underbrace{49}_{m_1} \times \underbrace{m_2}_{m_2}$$

$$M_1 = 49 \rightarrow M'_1 = 49^{-1} \bmod 37 = 34 \bmod 37$$

$$\varphi(37) = 36$$

$$(49, 37) = 1 \rightarrow 49^{-1} \bmod 37 = 49^{35} \bmod 37$$

$$= (49)^{32} \bmod 37 \cdot (49)^2 \bmod 37 \cdot 49 \bmod 37$$
$$= 7 \times 33 \times 12 = 34 \bmod 37$$

$$\left\{ \begin{array}{l} 49 \bmod 37 = 12 \\ (49)^2 \bmod 37 = 12^2 \bmod 37 = 33 \end{array} \right.$$

$$(49)^{32} \bmod 37 = 7$$

$$M_2 = 37 \rightarrow M'_2 = 37^{-1} \bmod 49 = \underbrace{4}_{\varphi(49)} \bmod 49$$

$$\varphi(49) = 7(7-1) = 42 \rightarrow 37^{41} \bmod 49$$

$$\begin{cases} 973 \bmod 37 = 11 \\ 973 \bmod 49 = 42 \end{cases}$$

$$973 \bmod 1813 \longleftrightarrow (11, 42)$$

$$678 \bmod 1813 \longleftrightarrow (12, 41)$$

$$678 + 973 \bmod 1813$$

$$(11+12 \bmod 37, 42+41 \bmod 49) = (23, 34)$$

$$\begin{aligned} (23, 34) &\longleftrightarrow a_1 M_1 M'_1 + a_2 M_2 M'_2 \bmod M \\ &= (23 \times 49 \times 34 + 34 \times 37 \times 4) \bmod 1813 \\ &= 43350 \bmod 1813 \\ &= 1651 \end{aligned}$$

## Discrete Logarithm

لگاریتم سنتی

کاربرد زاداں در ریاضی کا ریکارڈ کرنا ہے جس کی بحث کرو ہو۔

اللوریم ہائی مورف دینی - حلیم (توانی کیا)

و اسکا دیکھیں۔

$$\text{لگاریتم} \rightarrow a^{(a_1 n)} = 1 \quad a^{\varphi(n)} \equiv 1 \pmod{n}$$

ستہ  $a$  کا نمبر  $n$  کا کچھ عدیہ مل جائے ।

ستہ  $m$  کے لئے کچھ ان را طے کریں اپنے پریمیں۔

$$a^m \equiv 1 \pmod{n} : \text{اے نامہ } m \pmod{n}, a$$

لطفاً  $a^n \equiv 1 \pmod{m}$  ای و هر دلخواه  $n$  باشد.

طول دوره تناوب  $\tau(a)$  کو طبق آن  $m$  -  
نامانی  $a$  -

$$\text{ذ.}: \quad 7^1 \equiv 7 \pmod{19}$$

$$7^2 \equiv 11 \pmod{19}$$

$$7^3 \equiv 1 \pmod{19}$$

$$7^4 \equiv 7 \pmod{19}$$

$$7^5 \equiv 11 \pmod{19}$$

$$\longrightarrow m = 3$$

$a$  مرسن،  $(a, n) = 1$  پس  $(\mathbb{Z}/n\mathbb{Z})^*$  را  $\Psi(n)$  نویسند.

تعریف ریشه اولی یا بینایی (primitive root)  $a$  برای  $\Psi(n)$  است.

اگر  $a$  برای  $\Psi(n)$  اولی باشد، آنگاه  $a^k \mod n$  اعداد جمیع

از  $\Psi(n)$  ممکن است (عنصر اعداد جمیع)

در کرانه  $n$ . در این صورت، توان های متوالی

$a^r$  را درجه  $r$  نویسند.  
 $\{a^i \mod n\}_{i=1}^{\varphi(n)} = \mathbb{Z}_n^*$

$\Rightarrow \{a, a^2, \dots, a^{\varphi(n)}\}$

نکره ها می توانند رله بسته باشند

نمایه ای داریم

مله: آگر  $a$  اولین جزو

$$\{a, a^2, \dots, a^{p-1}\} \subset \mathbb{Z}_p^\times \text{ مجموعه ای است mod } p$$

مله:  $\{1, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\}$  مجموعه ای است

مله: مجموعه ای اعداد صحیح که زیرمجموعه ای از اعداد نатурال است.

باز اعداد صحیح که زیرمجموعه ای از اعداد زوج هستند

$\alpha = \text{عدد اول زوج} \rightarrow \alpha = \text{عدد اول زوج می باشد}$

لها کم سنه

لطفاً در اعداد حقیقی، علاوه بر این، سانی است.

$$x^{\text{tag}_x(y)} = y$$

نیز مادپ اولیه از  $a$ ، عدراوی  $p$  نیز

$$\begin{aligned} \{a, a^2, \dots, a^{p-1}\} &= \{1, 2, \dots, p-1\} = \mathbb{Z}_p \setminus \{0\} \\ &\equiv \{a^0, a^1, a^2, \dots, a^{p-2}\} \end{aligned}$$

لُون هر عَدْدٍ بِسَطْرٍ (عَيْنَى) سَعْي

• ( $b \equiv r \pmod{p}$ ) (عَيْنَى) سَعْي  $\exists p \ni$   
 $0 \leq r \leq p-1$

لُون هر عَدْدٍ وَصَدَارَةٍ  
 $N \ni$  بِسَطْرٍ لُون هر عَدْدٍ

$$0 \leq \mu \leq p-2$$

$$\therefore a^\mu \equiv b \pmod{p}$$

لُون  $a \pmod{p}$  سَيْفَى  $\rightarrow b$  سَيْفَى  $\mu$

$$\mu = \text{dflag}_{a,p}^{(b)}$$

رسان

$$\left\{ \begin{array}{l} \text{dflag}_{a,p}^{(1)} = 0 \xrightarrow{\text{O}} a^0 \pmod{p} = 1 \\ \text{dflag}_{a,p}^{(a)} = 1 \xrightarrow{} a^1 \pmod{p} = a \end{array} \right.$$

لطفاً فریض کریں کہ  $n$  اور  $a$  میں ایک عوامی اول عدد نہیں ہے۔

جس:

تمم طریقہ

$$n = 9 \rightarrow \varphi(n) = 6$$

$$a = 2 \text{ میں اول}$$

$a^i$	$r$	$\text{mod } n$
$2^0$	1	
$2^1$	2	
$2^2$	4	
$2^3$	8	
$2^4$	7	
$2^5$	5	
$2^6$	1	

$r$	1	2	4	5	7	8
$d_{\text{lag}}(r)$	0	1	2	5	4	3

:  $\tilde{w} \in \text{mod}_{\mathbb{F}_p}[G]$ ,  $a \in \mathbb{F}_p$

$$\text{dlog}_{a,p}(xy) \equiv \text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y) \pmod{\ell(p)}$$

پیچیدگی محاسباتی کو کم کر کر لسته :

$$y = g^x \bmod p$$

اگر  $x$  بزرگ باشد را دانسته باشیم  
ساده است.

اگر  $y, g, p$  را دانسته باشیم  
 $x$  سخت است.

- بهترین روش از مرتبت تجزیه اعداد اول بود

- تأکید بر روش تجزیه الگوریتم پیچیدگی

محاسباتی از مرتبت  $(\ln p)^{1/3} (\ln(\ln(p)))^{2/3}$

# Finite Fields میدان های سیمیت

Stallings - chapter 5

GF(p) ← Galois Field - میدان گالوا

---

Modern algebra جبر

Abstract algebra

? میدان های سیمیت  
جواب (op)

(group)  $\xrightarrow{\sigma}$

تعریف: یہ مجموعہ کو باہر اور بارہ کر دیا جائے تو مجموعہ سوداگر سُر اُن راستے زیر برداشتیں

$\forall a, b \in G \Rightarrow a * b \in G$  بستے ہوں - 1

: (associative) سُرت پڑکر - 2

$\forall a, b, c \in G \Rightarrow a * (b * c) = (a * b) * c$

: (identity element)  $\exists e \in G$  - 3

$\exists e \in G : \forall a \in G \Rightarrow a * e = e * a = a$

٤- مُطْرَقِ مُحْلُوك (inverse element) :

$$\forall a \in G; \exists a' \in G \Rightarrow a * a' = a' * a = e$$

گروه ساده (G)  
کراندار  
 $|G| = \text{مرتبه گروه}$

(Abelian) گروه طبیعتی است  
شرط زیر را نیز دارد است:

$$\forall a, b \in G : a * b = b * a$$

مُعَالٌ .

- مجموع مدار  $\sum_{e=1}^m$  تَمَتْ اِنْتَرِجُونَ  
کروه چابخانه  $\mod m$  است .

نَصَّتْ اِنْتَرِجُونَ  $\{0, 1, \dots, m-1\}$  .

کیک روه چابخانه  $\mod m$  است .

برای  $p$  اول که  $\{1, 2, \dots, p-1\}$  .

کروه خوبی از مرتبه  $1-p$  است .

## حلقه (Ring)

لُرْفَتْ : مجموع  $R$  حمراء بارداً و ابرانور بازی

لُرْفَتْ : مجموع  $R$  حمراء بارداً و ابرانور بازی  
باشد :

- مجموع  $R$  نصف ابرانور + نصف رده

$a$  .  $\frac{1}{2} \pi r^2$  .  $l$  .  $\frac{1}{2} \pi r^2$

$-a$  مجموع معلوم

ناتیجہ میں  $x$  نصف  $R$  - 2

$$\forall a, b \in R \implies axb \in R$$

3 - سُرْتٌ پُرِّیکَ تَعَتَّ  $\times$  بِرَارِبَدَ.

4 - اِپِرِ اَنْوَرِ خَرَبَ وَهُجَّعَ تَوزَعَ بِلَدَ

$\forall a, b, c \in R$ : دَبِيْل (distributive)

$$a \times (b + c) = a \times b + a \times c$$

$$(a + b) \times c = a \times c + b \times c$$

$$\text{مُسْكَن} : a - b = a + (-b)$$

حلَّقَ : مَعْوَنِيَّةِ مَوَانِئِ

اِسْبُونِ كَرَكَ آنِ انْهَاوِدَلَ.

$\forall a, b \in R$ : حل معادله طبقاً لـ

$$a \times b = b \times a$$

أولاً درست نظرية الارتباط: ✓

$\exists 1 \in R$ :

$\forall a \in R$ ;  $a \times 1 = 1 \times a = a$

$$a \times 1 = 1 \times a = a$$

$\forall a, b \in R, a \times b = 0 \Rightarrow a = 0 \text{ ли } b = 0$

integral - مقدار انتها  $\leftarrow$   
domain

مقدار انتها  $\times$  مجموع  $\int_{-\infty}^{\infty} f(x) dx$  ←  
هي المقدار المطلوب.

## میدان Field

میدان مجموعه  $F$  تھت دو ایک تو رہا زل " " ،  
میدان ناسیدہ ہند اگر سڑا طیز کے  
مع بزرگ رہا سند :

1 - مجموعہ  $F$  تھت ایک تو رہا مع " " میں  
گردہ جا بھاندہ کر رہا۔ مصروفی رہا " " ۔  
نالہ میں

2. مجموعه  $F\{0\}$  نسبت اپراتور  $\oplus$

مشکل پی روده جایجا نیز نهاد

عمرانی ۱۱۱

3. اپراتور  $\ominus$  روی مجموع کوچک نیز (جنسیتی)

با

$$\overline{\overline{a}} = \frac{a}{b} = a \cdot (b^{-1})$$

میدان مجموع ایک سرواں + وسیع  $\times 1 - \cdot +$  انتها

مثال :

میلان → اعداد لوگی ، اعداد صحیح

اعداد صحیح → میلان سست