

كلية العلوم

القسم : الرياضيات

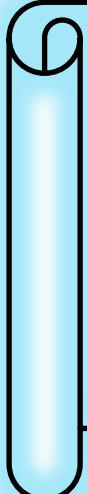
السنة : الرابعة



٩

المادة : نظرية الاعداد

المحاضرة : الثامنة/نظري /



{{{ A to Z مكتبة }}}}

مكتبة A to Z Facebook Group

كلية العلوم ، كلية الصيدلة ، الهندسة التقنية



يمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app-Telegram) على الرقم 0931497960

.....: الدكتور



القسم: الرياضيات

السنة الرابعة

المادة: نظرية الأعداد

التاريخ: / /

A to Z Library for university services

أرضية اليوامق:

النظام البوارجي (النظام قياسي) :

وَتَعْرِفُ:

$$A = \{a_0, a_1, \dots, \dots, a_{n-1}\} \quad \text{كتل}$$

مجموعه من الأعداد الصحيحة عدد ما

يُعَالَجُ أَنْظَامُ بُوَاهِيِّ تَامُ فِيَابِسُ بِإِذَا تَحْقَقَ الْمُرْتَدُ التَّالِيُّ:

$\forall a \in \mathbb{Z} : \exists \ a_i \in A, \ a \equiv a_i \pmod{n}$:

• ملخص

$$A = \{a_0, a_1, \dots, \dots, a_{n-1}\}$$

نظام بحاجة تمام عيادة ٦ (٦) فقط (٦) كاتب:

$$a_i \not\equiv a_j \pmod{n}$$

$$\forall 0 \leq i, j \leq n-1$$

$i \neq j$

مکالمہ

$$Z_n \{0, 1, 2, \dots, n-1\}$$

نظام بعاصي تام عنابر

وَسِرْرَ أَصْيَانَاً نَظَامِ بِعَامِنِيْ تَامِ صَيْعِيْ فَنَاسِيْ



2- نظام بواسطه المختزل فئايس n :

تعريف:

$$A = \{a_1, a_2, \dots, a_5\}$$

مثال عن المجموعة

نظام بواسطه مختزل فئايس n . اذا تحقق الخط التالي:

$$1- \forall x \in A : \gcd(x, n) = 1$$

$$2- x \not\equiv y \pmod{n}$$

$$\forall x, y \in A$$

$$3- |A| = \phi(n)$$

مثال:

$$A = \{1, 3, 7, 9\}$$

نظام بواسطه مختزل فئايس 10

$$B = \{-3, -11, 3, 9\}$$

-2

ليس نظام بواسطه مختزل فئايس 10

$$-3 \equiv -11 \pmod{10}$$

-2

المخطأ:

اذا كان n عدد صحيحا

$$A = \{t_1, t_2, \dots, t_{\phi(n)}\}$$

عندئن المجموعة :

المؤلف من جميع الأعداد الصحيحة الموجبة الأصغر من n والأولى مع العدد n .
 يشكل نظام يواضي مختزل فئاً مس n .
 Z_n^* عبر من له بالمعنى
 يعني أحياناً نظام الواقع المختزل الطبيعي فئاً مس n .

مثال

$$Z_5^* = \{1, 2, 3, 4\} \quad - (1)$$

$$Z_{12}^* = \{1, 5, 7, 11\} \quad - (2)$$

المطلب:

إذان R نظام يواضي مختزل فئاً مس n .

$$\gcd(a, n) = 1 \quad \text{عكلان}$$

$a \in \mathbb{Z}$ حيث

$$aR = \{ar : r \in R\} \quad \text{عنده}$$

نظام يواضي مختزل فئاً مس n .

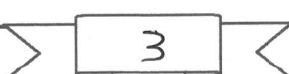
المطلب:

إذان A نظام يواضي مختزل فئاً مس n .

عنده صياغة كل لـ $a_i \in A$.

$$a_i \equiv r_i \pmod{n} \quad \text{لـ}$$

$$a_i = r_i \pmod{n} \quad \text{لـ}$$



مقدمة أولى :

إذا كان $a > n$ عددًا صحيحًا موجبًا

وكان a عددًا صحيحًا يحقق b^k

$$\gcd(a, n) = 1$$

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

برهان :

لما كان نظام العاشر المختزل الطبيعي فيما يلي :

$$R = \mathbb{Z}_n^* = \{t_1, t_2, \dots, t_{\phi(n)}\}$$

$$|R| = \phi(n)$$

$$\gcd(t_i, n) = 1 \quad \forall 1 \leq i \leq \phi(n)$$

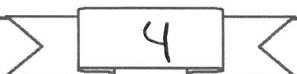
$$\gcd(a, n) = 1 \quad \forall a \in \mathbb{Z}$$

بيان

نظام عاشر مختزل فيما يلي $R = \mathbb{Z}_n^*$

$$aR = \{at_1, at_2, \dots, at_{\phi(n)}\}$$

نظام عاشر مختزل فيما يلي



نظام يعاني مختلف قيم aR لـ \star
 نوافذ مختلف طبع $R = \mathbb{Z}_n^*$ ،

$R = \mathbb{Z}_n^*$ هو نظام مختلف طبع aR هو مختلف لـ \star

$a_1, a_2, \dots, a_{\phi(n)} \equiv t_1, t_2, \dots, t_{\phi(n)} \pmod{n}$

$$a \prod_{i=1}^{\phi(n)} t_i \equiv \prod_{i=1}^{\phi(n)} t_i \pmod{n}$$

لـ \star

$$\left\{ \begin{array}{l} \gcd(t_i, n) = 1 \\ 1 \leq i \leq \phi(n) \end{array} \right.$$

$$\gcd\left(\prod_{i=1}^{\phi(n)} t_i, n\right) = 1$$

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

عكس المول (عـ)

إذا كان $n > 1$ صحيح

عكس صحيح a له

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

$$\gcd(a, n) = 1$$

كِتَابُ الْمُكَفَّفِينَ

Φ(η)

$$d \equiv 1 \pmod{n}$$

$$\Rightarrow \frac{\phi(n)}{d} = 1 + q \cdot n$$

$$d \cdot a - q \cdot n = 1$$

الله

$$y = -q, \quad n = d$$

جیسا

$$x_0 + y_0 = 1$$

$$\Rightarrow \gcd(a, n) = 1$$

عِرْقَةُ خِرْعَا:

لذات P عددًا أولياً وكان a عددًا صحيًا، حيث

... it is

$$a^{p-1} \equiv 1 \pmod{p}$$

ادبیات:

$$\gcd(p, a) = 1$$

...left.

$$\phi(p) \\ d \equiv 1 \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$



١- شرط :

$$\text{لذلك } d^p \equiv a \pmod{p}$$

البرهان :

d معروفة

$$d \equiv a \pmod{p} \quad \leftarrow p \nmid a \quad ①$$

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

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

لذلك $\leftarrow p \nmid a \quad ②$

$$d^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow d \times d^{p-1} \equiv a \pmod{p}$$

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

البرهان صحيح $\therefore ② \rightarrow ①$

تمرين (1) :

$$\text{لذلك } \gcd(a, 35) = 1$$

$$d^{12} \equiv 1 \pmod{35}$$

الحل :

$$\gcd(a, 35) = 1 \Rightarrow \gcd(a, 5)$$

$$= \gcd(a, 7) = 1$$





* $\gcd(a, 5) = 1$

$$\text{Let } \rightarrow a^{\phi(5)} \equiv 1 \pmod{5}$$

$$\rightarrow a^4 \equiv 1 \pmod{5}$$

$$\rightarrow (a^4)^3 \equiv 1^3 \pmod{5}$$

$$\rightarrow a^{12} \equiv 1 \pmod{5} \quad \textcircled{1}$$

* $\gcd(a, 7) = 1$

$$\text{Let } \rightarrow a^{\phi(7)} \equiv 1 \pmod{7}$$

$$\rightarrow a^6 \equiv 1 \pmod{7}$$

$$\rightarrow a^{12} \equiv 1 \pmod{7} \quad \textcircled{2}$$

$\gcd(5, 7) = 1$

إذن $\textcircled{1} \circ \textcircled{2}$ هي

لذلك

$$a^{12} \equiv 1 \pmod{5 \times 7}$$

$$\equiv 1 \pmod{35}$$

تمرين (2)

عَلَى $\gcd(n, m) = 1$

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{nm}$$



١٤١

$$\frac{\phi(n)}{m} + \frac{\phi(m)}{n} \equiv 1 \pmod{n}$$

$$\frac{\phi(n)}{m} + \frac{\phi(m)}{n} \equiv 1 \pmod{m}$$

Ⓐ $\text{L} \vdash \gcd(n, m) = 1 \Rightarrow$

$$\frac{\phi(n)}{m} \equiv 1 \pmod{n}$$

$$\Rightarrow \frac{\phi(n)}{m} + \frac{\phi(m)}{n} \equiv 1 + \frac{\phi(m)}{n} \pmod{n}$$

$$\Rightarrow \frac{\phi(n)}{m} + \frac{\phi(m)}{n} \equiv 1 \pmod{n} \quad (1)$$

Ⓐ $\gcd(n, m) = 1 \Rightarrow$

$$\frac{\phi(m)}{n} \equiv 1 \pmod{m}$$

$$\Rightarrow \frac{\phi(m)}{n} + \frac{\phi(n)}{m} \equiv 1 + \frac{\phi(n)}{m} \pmod{m}$$

$$\Rightarrow \frac{\phi(m)}{n} + \frac{\phi(n)}{m} \equiv 1 \pmod{m} \quad (2)$$

$$\gcd(n, m) = 1 \quad \text{وَلَعْنَهُ} \quad \text{وَلَعْنَهُ} \quad \text{وَلَعْنَهُ} \quad \text{وَلَعْنَهُ}$$

$$\frac{\phi(n)}{m} + n \equiv 1 \pmod{n m}$$

لـ (3) تـ

$$\gcd(a, n) = \gcd(a-1, n) = 1 \quad \text{لـ (1) لـ (1)}$$

$$1 + a + a^2 + \dots + a^{\phi(n)-1} \equiv 0 \pmod{n}$$

$$1 + a + a^2 + \dots + a^{\phi(n)-1} = \frac{a^{\phi(n)} - 1}{a - 1}$$

$$\Rightarrow (a-1) \left(1 + a + a^2 + \dots + a^{\phi(n)-1} \right) = a^{\phi(n)} - 1 \quad \text{لـ (1)}$$

$$\gcd(a, n) = 1 \quad \text{لـ (1) لـ (1)}$$

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

$$\Rightarrow a^{\phi(n)} - 1 \equiv 0 \pmod{n}$$

لـ (1) لـ (1)

$$(a-1) \left(1 + a + a^2 + \dots + a^{\phi(n)-1} \right)$$

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

$$\equiv 0 \pmod{n}$$

$$\gcd(a-1, n) = 1 \quad \text{لذلك}$$

$$1 + a + a^2 + \dots + a^{\phi(n)-1} \equiv 0 \pmod{n} \quad \Leftarrow$$

1.4) إثبات

$$\gcd(n, 42) = 1 \quad \text{أولاً} \quad \text{أثبات}$$

$$5 \cdot 4 \mid (n^6 - 1)$$

1.5) إثبات

$$\gcd(n, 42) = 1$$

$$42 = 3 \times 2 \times 7$$

$$\Rightarrow \gcd(n, 2) = \gcd(n, 3) = \gcd(n, 7) = 1$$

$$5 \cdot 4 = 2^3 \times 3^2 \times 7$$

$$*) \quad \gcd(n, 2) = 1 \Rightarrow \gcd(n, 2^3) = 1$$

$$\text{لذلك} \Rightarrow n^{\phi(2^3)} \equiv 1 \pmod{8}$$

$$\Rightarrow n^4 \equiv 1 \pmod{8}$$

$$(\text{عوض}) \quad n^2 \equiv 1 \pmod{2^3} \quad \text{نعلم}$$

$$\Rightarrow n^4 \cdot n^2 \equiv 1 \pmod{3}$$

$$\Rightarrow n^6 \equiv 1 \pmod{3} \quad \text{①}$$

$$*) \quad \gcd(n, 3) = 1 \Rightarrow \gcd(n, 3^2) = 1$$

$$\text{لذلك} \Rightarrow n^{\phi(3^2)} \equiv 1 \pmod{3^2}$$



$$n^6 \equiv 1 \pmod{3^2} \quad (2)$$

$$\text{1. } \gcd(n, 7) = 1$$

$$\text{So } \Rightarrow n^{\phi(7)} \equiv 1 \pmod{7}$$

$$n^6 \equiv 1 \pmod{7} \quad (3)$$

ولذلك (3), (2), (1) true

$$\gcd(2^3, 3^2, 7) = 1$$

\Leftrightarrow

$$n^6 \equiv 1 \pmod{(2^3 \times 3^2 \times 7)}$$

$$n^6 \equiv 1 \pmod{504}$$

$$\Rightarrow 504 \nmid (n^6 - 1)$$

- end -



مكتبة
A to Z