كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الثامنة/نظري/

# {{ A to Z مكتبة }}

Facebook Group : A to Zمكتبة

# أنظمة البواقي:

## 1- نظام البواقي التام قياس n:

**تعريف:**

لتكن $A=\{a_0,a_1,\dots,a_{n-1}\}$

مجموعة من الأعداد الصحيحة عددها n

يُقال بأنّ A نظام بواقي تام قياس n إذا تحقق الشرط التالي:

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

**ملاحظة:**

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

نظام بواقي تام قياس n إذا وفقط إذا كان:

$$a_i \not\equiv a_j \pmod n$$
$$\forall\ 0\le i,j\le n-1$$
$$i\ne j$$

**مثال:**

$\mathbb{Z}_n\ \{0,1,2,\dots,n-1\}$

نظام بواقي تام قياس n

ويسمى أحياناً نظام بواقي تام طبيعي قياس n

## 2- نظام البواقي المختزل قياس n :

• تعريف :

يُقال عن المجموعة $A=\{a_1, a_2, \dots, a_s\}$

نظام بواقي مختزل قياس n إذا تحققت الشروط التالية :

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

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

وذلك $\forall x, y \in A$

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

• مثال :

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

نظام بواقي مختزل قياس 10

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

ليس نظام بواقي مختزل قياس 10

لأنّ $9 \equiv -11 \pmod{10}$

• ملاحظة :

إذا كان $n>1$ عدداً صحيحاً

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

المؤلفة من جميع الأعداد الصحيحة الموجبة الأصغر من $n$ والأولية مع العدد $n$،
تشكل نظام بواقي مختزل قياس $n$
ويرمز له بالرمز $Z_n^*$
ويسمى أحياناً بنظام البواقي المختزل الطبيعي قياس $n$.

• مثال:

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

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

• ملاحظة:

إذا كان $R$ نظام بواقي مختزل قياس $n$
وكان $gcd(a, n) = 1$
حيث $a \in \mathbb{Z}$
عندئذ $aR = \{ar ; r \in R\}$
نظام بواقي مختزل قياس $n$

• ملاحظة:

إذا كان $A$ نظام بواقي مختزل قياس $n$
عندئذٍ من أجل كل $a_i \in A$
يوجد $r_i \in Z_n^*$ وحيد
بحيث $a_i \equiv r_i \pmod{n}$

مبرهنة أولر:

إذا كان $n>1$ عدداً صحيحاً موجباً

وكان $a$ عدداً صحيحاً يحقق الشرط

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

عندئذٍ:

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

الإثبات:

لنأخذ نظام البواقي المختزل الطبيعي قياس $n$:

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

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

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

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

وبما أن

نظام بواقي مختزل قياس $n$ $\quad R = \mathbb{Z}_n^*$

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

نظام بواقي مختزل قياس $n$

★ لدينا $aR$ نظام بواقي مختزل قياس $n$
و $R = Z_n^*$ نظام بواقي مختزل طبيعي قياس $n$

⟸ عندئذٍ كل عنصر من $aR$ يطابق عنصر واحد فقط من $R = Z_n^*$

$$at_1, at_2, \ldots, at_{\phi(n)} \equiv t_1, t_2 \ldots t_{\phi(n)} \pmod{n}$$

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

لدينا:

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

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

عندئذٍ:

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

عكس مبرهنة أولر (مبرهنة):

اذا كان $n > 1$ عدداً صحيحاً موجباً
وكان $a$ عدداً صحيحاً بحيث:

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

عندئذٍ: $\gcd(a,n) = 1$

الاثبات:

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

$$\Rightarrow a^{\phi(n)} = 1 + qn$$

$$a\, a^{\phi(n)-1} - qn = 1$$

لنأخذ:

$$y = -q \quad , \quad x = a^{\phi(n)-1}$$

عندئذٍ:

$$xa + yn = 1$$

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

مبرهنة فيرما:

إذا كان $p$ عدداً أولياً وكان $a$ عدداً صحيحاً بحيث $p \nmid a$

عندئذٍ:

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

الاثبات:

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

أولر $\Leftarrow$

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

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

**نتيجة:**

إذا كان $p$ عدداً أولياً عندئذٍ:

$a^p \equiv a \pmod p$ مهما $a$

**الإثبات:**

أي عدد صحيح $a$

① $p \mid a \Leftarrow$

$a \equiv 0 \pmod p$

$a^p \equiv 0 \pmod p$

$\Rightarrow a^p \equiv a \pmod p$

② $p \nmid a \Leftarrow$ حسب فيرما:

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

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

$\Rightarrow a^p \equiv a \pmod p$

من ① و ② النتيجة صحيحة.

**تمرين (1):**

إذا كان $\gcd(a, 35) = 1$

عندئذٍ $a^{12} \equiv 1 \pmod{35}$

**الحل:**

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

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

★ $\gcd(a, 5) = 1$

أولر $\Rightarrow a^{\phi(5)} \equiv 1 \pmod 5$

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

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

$\Rightarrow a^{12} \equiv 1 \pmod 5$ . . . . ①

★ $\gcd(a, 7) = 1$

أولر $\Rightarrow a^{\phi(7)} \equiv 1 \pmod 7$

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

$\Rightarrow a^{12} \equiv 1 \pmod 7$ . . . ②

من ① و ② وكون $\gcd(5,7) = 1$

عندئذٍ:

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

$\equiv 1 \pmod{35}$

تمرين (2):

إذا كان $\gcd(n, m) = 1$ فإنَّ:

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

الحل:

يجب أن نثبت أنّ:

$$\left.\begin{array}{l} m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n} \\ \& \\ m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{m} \end{array}\right\}$$

(A) لدينا $\gcd(n,m) = 1 \overset{\text{أولر}}{\Longrightarrow}$

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

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

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

(A) $\gcd(n,m) = 1 \overset{\text{أولر}}{\Longrightarrow}$

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

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

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

من ① و ② وكون $\gcd(n,m)=1$

$\Leftarrow$

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

تمرين (3) :

إذا كان $\gcd(a,n) = \gcd(a-1,n) = 1$

عندئذٍ :

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

الإثبات :

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

$$\Rightarrow (a-1)(1 + a + a^2 + \cdots + a^{\phi(n)-1}) = a^{\phi(n)} - 1 \quad \text{①}$$

بما أنّ : $\gcd(a,n)=1$

أويلر $\Leftarrow$

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

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

من ① نجد :

$$(a-1)(1 + a + a^2 + \cdots + a^{\phi(n)-1})$$

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

$\equiv 0 \pmod{n}$

لدينا $\gcd(a-1, n) = 1$

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

تمرين (4):

إذا كان $\gcd(n, 42) = 1$

أثبت أنه

$504 \mid (n^6 - 1)$

الحل:

$\gcd(n, 42) = 1$

$42 = 3 \times 2 \times 7$

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

$504 = 2^3 \times 3^2 \times 7$

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

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

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

نعلم بأنه $n^2 \equiv 1 \pmod{2^3}$ ($n$ فردي)

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

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

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

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

$n^6 \equiv 1 \pmod{3^2}$ ---- 2

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

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

$n^6 \equiv 1 \pmod 7$ ---- 3

من 1 و 2 و 3 وكون

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

$\Leftarrow$

$n^6 \equiv 1 \mod (2^3 \times 3^2 \times 7)$

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

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

انتهت