كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : **السابعة /نظري/**

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

أنظمة البواقي:

1 نظام البواقي التام قياس n:

تعريف: لتكن $A=\{a_0,a_1,\dots,a_{n-1}\}$ مجموعة الأعداد الصحيحة عددها n يقال بأنّ A نظام بواقي تام قياس n إذا تحقّق الشرط التالي:

$$\forall a\in Z \quad \exists a_i\in A \;;\; a\equiv a_i \pmod n$$

ملاحظة: وهيد
$A=\{a_0,\dots,a_{n-1}\}$ نظام بواقي تام قياس n إذا وفقط إذا كان:

$$a_i\not\equiv a_j \pmod n \;;\; i\neq j \;\&\; 0\le i,j\le n-1$$

مثال: $Z_n=\{0,1,2,\dots,n-1\}$
نظام بواقي تام قياس n ويسمّى بنظام البواقي التام الطبيعي قياس n

2 نظام البواقي المختزل قياس n:

يقال عن المجموعة $A=\{a_0,\dots,a_s\}$ نظام بواقي مختزل قياس n إذا تحقّقت الشروط التالية:

1. $\forall a\in A \;;\; gcd(a,n)=1$
2. $a\not\equiv b \pmod n$ لكل a و b من A و $a\neq b$
3. $|A|=S=\phi(n)$ حيث ϕ دالة أويلر

مثال: $A=\{1,3,7,9\}$ نظام بواقي مختزل قياس $n=10$

مثال: $A=\{-3,-11,3,9\}$ ليس بنظام بواقي مختزل قياس 10

لأنّ $9 \equiv -11 \pmod{10}$

ملاحظة: إذا كانَ $n>1$ عدداً صحيحاً موجباً عندئذٍ المجموعة $A=\{t_1, t_2, \ldots, t_{\phi(n)}\}$ المؤلفة من جميع الأعداد الصّحيحة الموجبة الأصغر من n وأوليةٍ مع العدد n تشكّل نظام بواقي مختزل قياس n ويرمز له بالرمز Z_n^* ويسمّى بـ نظام البواقي المختزل الطبيعي قياس n.

مثال:
- $Z_5^* = \{1,2,3,4\}$ ← قدرتها $\phi(5)$ لـ نظام البواقي المختزل قياس 5
- $Z_{12}^* = \{1,5,7,11\}$ ← قدرتها $\phi(12)$ لـ نظام البواقي المختزل الطبيعي قياس 12

ملاحظة: إذا كانَ R نظام بواقي مختزل قياس n وليكن $a \in Z_n$ بحيث $\gcd(a,n)=1$ عندئذٍ ؛ aR نظام بواقي مختزل قياس n.

ملاحظة: إذا كانَ 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 كانَ $n>1$ عدداً صحيحاً موجباً وكانَ $a \in Z$ بحيث $\gcd(a,n)=1$ عندئذٍ $a^{\phi(n)} \equiv 1 \pmod{n}$

الإثبات:

- لنأخذ نظام البواقي المختزل الطبيعي قياس n وليكن $R=Z_n^*$

$$R=\{t_1, t_2, \ldots, t_{\phi(n)}\}$$

وهو عبارة عن جميع الأعداد الصحيحة الموجبة الأصغر من n وأوليةٍ مع العدد n حيث $|R| = \phi(n)$.

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

• لدينا $R = Z_n^*$ نظام بواقي مختزل قياس n ولدينا $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ عندئذٍ:

$$aR = a Z_n^* = \{at_1, at_2, \dots, at_{\phi(n)}\}$$

نظام بواقي مختزل قياس n

• لدينا aR نظام بواقي مختزل قياس n

$R = Z_n^*$ نظام بواقي مختزل طبيعي قياس n

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

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

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

وبما أنّ

$\gcd(t_i, n) = 1$ عندئذٍ $\forall\ \phi(n) \geq i \geq 1$

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

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

• عكس مبرهنة أولر:

إذا كان $n > 1$ عدداً صحيحاً موجباً و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ عندئذٍ $a^{\phi(n)} \equiv 1 \pmod n$

الإثبات:

لدينا فرضاً $a^{\phi(n)} \equiv 1 \pmod n$ عندئذٍ:

$$a^{\phi(n)} = 1 + qn \quad ; \quad q \in \mathbb{Z}$$

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

نضع $x = a^{\phi(n)-1}$ و $y = -q$ فنجد

$$1 = ax + yn$$

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

مبرهنة فيرما: ليكن $a \in \mathbb{Z}$ عندئذٍ: إذا كان p عدد أولي عندئذٍ $a^{p-1} \equiv 1 \pmod{p}$ حيث $p \nmid a$

الاثبات:

لدينا $p \nmid a$ عندئذٍ $\gcd(a,p)=1$ بالتالي حسب أويلر:

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

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

نتيجة إذا كان p عدداً أولياً فإنّ $a^p \equiv a \pmod{p}$ من أجل أي عدد صحيح a

الاثبات: لدينا $p \mid a$ أو $p \nmid a$

- $p \nmid a \xrightarrow{\text{حسب فيرما}} a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$
- $p \mid a \Rightarrow a \equiv 0 \pmod{p} \Rightarrow a^p \equiv 0 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$

ملاحظة: عكس مبرهنة فيرما غير صحيح بصورة عامة أي إذا كان: $a^{m-1} \equiv 1 \pmod{m}$ فقد لا يكون m أولي.

وكمثال على ذلك $a=5$, $m=4$ و $\gcd(a,m)=1$

$$a^{m-1} = 5^3 \equiv 1 \pmod{m}$$

لكن $m=4$ ليس عدد أولي

مثال: إذا كان $\gcd(a,35)=1$ فأثبت أنّ $a^{12} \equiv 1 \pmod{35}$

الاثبات:

يكفي أن نثبت أنّ $a^{12} \equiv 1 \pmod{5}$ & $a^{12} \equiv 1 \pmod{7}$

حيث $\gcd(5,7)=1$

- لدينا فرضاً $\gcd(a,35)=1 \Leftarrow \gcd(a,5)=1$ & $\gcd(a,7)=1$
- $\gcd(a,5)=1 \xrightarrow{\text{حسب أويلر}} a^{\phi(5)} \equiv 1 \pmod{5}$

$\Rightarrow a^4 \equiv 1 \pmod 5 \Rightarrow a^{12} \equiv 1 \pmod 5$ (1)

$\gcd(a,7)=1 \xrightarrow{\text{حسب أولر}} a^{\phi(7)} \equiv 1 \pmod 7 \Rightarrow a^6 \equiv 1 \pmod 7$

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

من ① و ② وكون $\gcd(5,7)=1$ نجد أنّ

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

$\Rightarrow a^{12} \equiv 1 \pmod{35}$ وهو المطلوب

مثال: إذا كان $\gcd(n,42)=1$ فأثبت أنّ $504 \mid (n^6-1)$

الحل:

لدينا $42 = 3\times 2\times 7$ و $\gcd(n,42)=1$

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

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

$\gcd(n,2)=1$

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

$\Rightarrow n^{\phi(2^3)} \equiv 1 \pmod 8 \Rightarrow n^4 \equiv 1 \pmod 8$ & $n^2 \equiv 1 \pmod 8 \Rightarrow$

$n^6 \equiv 1 \pmod 8$ ①

$\gcd(n,3)=1 \Rightarrow \gcd(n,3^2)=1 \Rightarrow n^{\phi(3^2)} \equiv 1 \pmod 9$

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

$\gcd(n,7)=1$

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

من ① و ② و ③ وكون $\gcd(2^3,3^2,7)=1$

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

$\Rightarrow n^6-1 \equiv 0 \pmod{504}$

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

مثال: إذا كان $gcd(a,n)=gcd(a-1,n)=1$ عندئذٍ:

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

الحل:

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

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

بما أنّ $gcd(a,n)=1$ $\Leftarrow$ حسب أويلر

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

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

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

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

بالتّالي:

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

وبما أنّ $gcd(a-1,n)=1$ بالتّالي

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

أمثلة وظيفة:

1. إذا كان $gcd(n,m)=1$ عندئذٍ:

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

2. أوجد باقي قسمة 3^{439} على العدد 5.

انتهت المحاضرة