المحاضرة الرابعـة عشـر

نتيجة (9): (مبرهنة فيرما الصغرى Fermat's little Theorem)

اذا كان p عدداً اولياً، وكان $a \in Z$ وكان $a \nmid p$، فأن $a^{p-1} \equiv 1(\text{mod p})$.

البرهان:

بما ان $a \nmid p$، اذاً $(a,p) = 1$، وعليهِ فأن $a^{\varphi(p)} \equiv 1(\text{mod p})$ حسب مبرهنة اولير. لكن

$$\varphi(p) = |\{m \in Z: 1 \leq m \leq p: (m,p) = 1\}| = |\{1,2,3,\dots,p-1\}|$$

آذاً $a^{p-1} \equiv 1(\text{mod p})$.

نتيجة (10):

إذا كان p عدداً أوّلياً فإن $a^p \equiv a \ (\text{mod p})$ لكل عدد صحيح a .

البرهان:

إذا كان $a \mid p$ ، فإن $a \equiv 0 \ (\text{mod p})$ ومنه نجد أن : $a^p \equiv 0 \ (\text{mod p})$.

أي أن $a^p \equiv a \ (\text{mod p})$. أما إذا كان $a \nmid p$ ، فباستخدامنا نتيجة (١) نجد أن :

$a^{p-1} \equiv 1 \ (\text{mod p})$. أي أن $a^p \equiv a \ (\text{mod p})$. ◆

نتيجة (11):

إذا كان $(a , n) = 1$ فإن $a^{\varphi(n)-1}$ نظير ضربي للعدد a قياس n .

البرهان:

بما أن $(a,n) = 1$. اذاً $a^{\varphi(n)} \equiv 1(\text{mod n})$، وعليهِ فأن :

$$a^{\varphi(n)-1} \equiv 1(\text{mod n})$$

ومنها نجد أن $a^{\varphi(n)-1}$ معكوس ضربي للعدد a قياس n.

نتيجة (12):

إذا كان $(a , n) = 1$ فإن الحل الوحيد للتطابق :
$ax \equiv b \pmod{n}$ هو $x \equiv a^{\varphi(n) - 1} b \pmod{n}$.

البرهان:

بما أن $ax \equiv b \pmod{n}$ وأن $(a , n) = 1$ فـإن الحل الـوحـيـد لـلـتـطابق هـو $x \equiv a^{-1} b \pmod{n}$. ولـكـن بـاسـتـخـدام الـنـتـيـجـة (٣) نـعـلـم أن $a^{-1} \equiv a^{\varphi(n) - 1} \pmod{n}$. وبالتالي فإن $x \equiv a^{\varphi(n) - 1} b \pmod{n}$. ◆

نتيجة (13):

إذا كان $(a, n) = (a - 1 , n) = 1$ ، فإن
$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}$.

ملاحظة:

عكس مبرهـنـة فيرمـا لـيس صـحـيحاً . أي أنـه إذا كـان $(a,p) = 1$ و $a^{p-1} \equiv 1 \pmod{p}$ فقد لا يكون p عدداً أولياً كما يوضح ذلك المثال الآتي :
$5^3 \equiv 1 \pmod{4}$ و $(5,4) = 1$ بينما 4 ليس أولياً .

مبرهنة (35):

إذا كـان p,q عـددين أوليـين مختلفـين وكـان $a^p \equiv a \pmod{q}$ ، $a^q \equiv a \pmod{p}$ ، فإن $a^{pq} \equiv a \pmod{pq}$.

امثلـة:

(أ) أثبت ان $a^{37} = a \pmod{1729}$.

بما أن $1729 = (7)(13)(19)$.

اذاً، إذا كان 1= (a, 19) = (a, 13) = (a,7).

فأن

$a^{18} \equiv 1 \ (mod\ 19)$، $a^{6} \equiv 1 \ (mod\ 7)$، $a^{12} \equiv 1 \ (mod\ 13)$

حسب مبرهنة فيرما.

وعليه فأن $a^{18}.a^{6}.a^{12} \equiv 1\ mod\ (1729)$.

وهذا يعني أن

$a^{36} = 1\ (mod\ 1729)$. اذاً $a^{37} = a\ (mod\ 1729)$.

(ب) أوجد المعكوس الضربي للعدد 5 قياس 8.

بما أن 1=(5, 8)، اذاً $5^{-1} = 5^{\varphi(8)-1}$.

لكن $\varphi(8) = 4$، اذاً

$5^{-1} = 5^{3} = 125$، ولكن $125 \equiv 5 (\text{mod} 8)$. اذاً $5^{-1}(mod\ 8) = 5$.

(ت) حل التطابق $3x \equiv 5\ (mod\ 8)$.

بما أن 1=(3, 8)، اذاً الحل الوحيد للتطابق $3x \equiv 5\ (mod\ 8)$ هو

$x = 3^{\varphi(8)-1}.5\ (mod\ 8)$

لكن $\varphi(8) = 4$،

اذا $x = 3^{3}.5\ (mod\ 8)$.

لكن $3^{3}.5 = 135 = 7\ (mod\ 8)$.

اذاً $x \equiv 7\ (mod\ 8)$.

(ث) استخدم مبرهنة فيرما الصغرى لأثبات ان العدد 117 مؤلف.

نريد ان نجد عدداً a بحيث يكون $a^{117} \not\equiv a\ (mod\ 117)$. إذا اخترنا a=2، فأن:

$2^{117} = (2^{7})^{16}.2^{5} \equiv 11^{16} \times 2^{5} \equiv 121^{8} \times 2^{5} \equiv 4^{8} \times 2^{5}$

$\equiv 2^{21} \equiv (2^{7})^{3} \equiv 11^{3} \equiv 4 \times 11 \equiv 44 \not\equiv 2\ (mod\ 117).$

وبالتالي فان 117 مؤلف.

مبرهنة (36): (عكس مبرهنة فيرما)

إذا كان $n \geq 2$ وكان $a^{n-1} \equiv 1 \pmod n$ لكل $1 \leq a \leq n-1$ ، فإن n عدد أولي .

البرهان:

بما أن $a^{n-1} \equiv 1 \pmod n$ لكل $1 \leq a \leq n-1$. إذاً $a^{n-2} \cdot a \equiv 1 \pmod n$ لكل $1 \leq a \leq n-1$ ، وعليه فإن للعنصر a معكوس ضربي هو a^{n-2} ، وبالتالي فإن $(a,n)=1$ لكل $1 \leq a \leq n-1$ حسب

النتيجة التي تنص (اذا كان n>2، فأن n عدد مؤلف، اذا وفقط اذا وجد $a, b \in Z$ بحيث أن n=ab،[n > 1< b])،وعليه فأن $(a, n) = a > 1$ وهذا تناقض كون

(a, n) =1 ، اذاً n عدد اولي.

ملاحظة:

1- نستنتج من مبرهنة فيرما ومبرهنة (22)، أن n عدد اولي إذا وفقط إذا كان $a^{n-1} \equiv 1 \pmod n$ لكل $a \not\equiv 0 \pmod n$.

2- نستنتج من مبرهنة (22)، انه اذا كان $2^{n-1} \not\equiv 1 \pmod n$، فأن n ليس اولياً.

امثلـة:

(أ) 8 عدد غير أولي ، لأن $2^7 \not\equiv 1 \pmod 8$ ، $1 < 2 < 7$.

(ب) 323 ليس أولياً ، لأن $2^{322} \not\equiv 1 \pmod{323}$.
