كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الخامسة /عملي/

{{ A to Z مكتبة }}

Facebook Group : A to Z مكتبة

5

المحاضرة الخامسة (عملي)

السؤال الأول:

ليكن n عدد صحيحاً لا يقبل القسمة على أي من الأعداد $2, 3, 5, 7$ فإنّ

$$840 \mid (n^{12} - 1)$$

الحلّ:

بما أن n عدد صحيحاً لا يقبل القسمة على أي من الأعداد $2, 3, 5, 7$ عندئذ يكون:

$$gcd(2, n) = gcd(3, n) = gcd(5, n) = gcd(7, n) = 1$$

بما أنّ

$$840 = 2^3 \times 3 \times 5 \times 7$$

$$gcd(2, n) = 1 \Longrightarrow gcd(2^3, n) = 1 \Longrightarrow n^{\phi(2^3)} \equiv 1(mod\ 2^3) \Longrightarrow n^4 \equiv 1(mod\ 2^3)$$

بالتالي

$$n^{12} \equiv 1(mod\ 2^3) \ldots..(1)$$

$$gcd(3, n) = 1 \Longrightarrow n^{\phi(3)} \equiv 1(mod\ 3) \Longrightarrow n^2 \equiv 1(mod\ 3)$$

بالتالي

$$n^{12} \equiv 1(mod\ 3) \ldots..(2)$$

$$gcd(5, n) = 1 \Longrightarrow n^{\phi(5)} \equiv 1(mod\ 5) \Longrightarrow n^4 \equiv 1(mod\ 5)$$

بالتالي

$$n^{12} \equiv 1(mod\ 5) \ldots..(3)$$

$$gcd(7, n) = 1 \Longrightarrow n^{\phi(7)} \equiv 1(mod\ 7) \Longrightarrow n^6 \equiv 1(mod\ 7)$$

بالتالي

$$n^{12} \equiv 1(mod\ 7) \ldots..(4)$$

من (1) و (2) و (3) و (4) وكون المقاسات أولية فيما بينها مثنى مثنى عندئذ

$$n^{12} \equiv 1(mod\ 2^3 \times 3 \times 5 \times 7)$$

بالتالي

$$n^{12} \equiv 1(mod\ 840)$$

عندئذ $840 \mid (n^{12} - 1)$

السؤال الثاني:

إذا كان n عدداً فردياً لا يقبل القسمة على العدد 3 فأثبت أنّ

$$n^2 \equiv 1(mod\ 24)$$

الحلّ:

بما أن n عدد فردي عندئذ $n^2 \equiv 1(mod\ 8) \ldots.(1)$

بما أنّ n عدد لا يقبل القسمة على العدد 3 عندئذ $gcd(3, n) = 1$ بالتالي حسب أولر

$$n^{\phi(3)} \equiv 1(mod\ 3) \Longrightarrow n^2 \equiv 1(mod\ 3) \ldots..(2)$$

بالتالي من (1) و (2) وكون $gcd(3, 8) = 1$ عندئذ

$$n^2 \equiv 1(mod\ 3 \times 8)$$

بالتالي

$$n^2 \equiv 1(mod\ 24)$$

السؤال الثالث:

ليكن n عدداً صحيحاً بحيث $\gcd(n,30)=1$ فأثبت أنّ $240 \mid (n^8+239)$

الحلّ:

$$30 = 2\times 3\times 5$$

بما أن $\gcd(n,30)=1$ عندئذ يكون:

$$gcd(2,n)=gcd(3,n)=gcd(5,n)=1$$

بما أنّ

$$240 = 2^4\times 3\times 5$$

$$gcd(2,n)=1 \Longrightarrow gcd(2^4,n)=1 \Longrightarrow n^{\phi(2^4)} \equiv 1(mod\ 2^4) \Longrightarrow n^8 \equiv 1(mod\ 2^4)$$

بالتالي

$$n^8 \equiv 1(mod\ 2^4)\ \ldots..(1)$$

$$gcd(3,n)=1 \Longrightarrow n^{\phi(3)} \equiv 1(mod\ 3) \Longrightarrow n^2 \equiv 1(mod\ 3)$$

بالتالي

$$n^8 \equiv 1(mod\ 3)\ \ldots..(2)$$

$$gcd(5,n)=1 \Longrightarrow n^{\phi(5)} \equiv 1(mod\ 5) \Longrightarrow n^4 \equiv 1(mod\ 5)$$

بالتالي

$$n^8 \equiv 1(mod\ 5)\ \ldots..(3)$$

من (1) و (2) و (3) وكون المقاسات أولية فيما بينها مثنى مثنى عندئذ

$$n^8 \equiv 1(mod\ 2^4\times 3\times 5)$$

بالتالي

$$n^8 \equiv 1(mod\ 240)$$

عندئذ

$$n^8+239 \equiv 1+239(mod\ 240)$$

عندئذ

$$n^8+239 \equiv 0(mod\ 240)$$

عندئذ

$$240 \mid (n^8+239)$$

السؤال الرابع:

ليكن p,q عددين أوليين فرديين مختلفين وليكن

$$a^p \equiv a(mod\ q)$$
$$a^q \equiv a(mod\ p)$$

حيث $\gcd(a,p)=\gcd(a,q)=1$ فإنّ

$$a^{pq} \equiv a(mod\ pq)$$

الحلّ :

$$a^p \equiv a(mod\ q) \Longrightarrow\ a^{pq} \equiv a^q(mod\ q)$$

وبما أنّ q عدد أولي عندئذ حسب نتيجة حصلنا عليها من فيرما نجد:

$$a^q \equiv a(mod\ q)$$

بالتالي

$$a^{pq} \equiv a(mod\ q) \ldots.(1)$$

$$a^q \equiv a(mod\ p) \Longrightarrow\ a^{pq} \equiv a^p(mod\ p)$$

وبما أنّ p عدد أولي عندئذ حسب نتيجة حصلنا عليها من فيرما نجد:

$$a^p \equiv a(mod\ p)$$

بالتالي

$$a^{pq} \equiv a(mod\ p) \ldots.(2)$$

من (1) و (2) وكون $\gcd(p,q) = 1$ عندئذ

$$a^{pq} \equiv a(mod\ pq)$$

السؤال الخامس:

ليكن p,q عددين أوليين فرديين مختلفين حيث

$$(p-1) \mid (q-1)$$

فأثبت أنّ

$$a^{q-1} \equiv 1(mod\ pq)$$

حيث $\gcd(a,pq) = 1$

الحلّ : بما أنّ $\gcd(a,pq) = 1$ عندئذ $\gcd(a,p) = 1$ و $\gcd(a,q) = 1$

$$\gcd(a,q) = 1 \Longrightarrow a^{q-1} \equiv 1(mod\ q) \ldots.(1)$$

$$\gcd(a,p) = 1 \Longrightarrow a^{p-1} \equiv 1(mod\ p)$$

وبما أنّ

$$(p-1) \mid (q-1)$$

عندئذ $q-1 = t(p-1)$ حيث $t \in \mathbb{Z}^+$ بالتالي

$$a^{q-1} = (a^{p-1})^t \equiv (1)^t(mod\ p) \equiv 1(mod\ p)$$

بالتالي

$$a^{q-1} \equiv 1(mod\ p) \ldots.(2)$$

من (1) و (2) وكون $\gcd(p,q) = 1$ عندئذ

$$a^{q-1} \equiv 1(mod\ pq)$$
