كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : السادسة /عملي/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

6

المحاضرة السادسة (عملي)

تعريف: (العدد الشبه الأولي بالنسبة لأساس ما)

إذا كان m عدداً صحيحاً موجباً وليس أولياً ووجد على الأقل عدد صحيح a بحيث $gcd(a,m)=1$ و $a^{m-1}\equiv 1(mod\ m)$، فإنّ m يدعى عدد شبه أولي للأساس a.

السؤال الأول:

أثبت أنّ العدد $m=341$ عدد شبه أولي للأساس 2.

الحلّ:

بما أن

$$m=341=11\times 31$$

فهو عدد صحيح موجب ليس أولي.

لدينا $a=2$ لنثبت أنّ

$$2^{m-1}\equiv 1(mod\ m)$$

أي لنثبت أنّ

$$2^{340}\equiv 1(mod\ 341)$$

من أجل $a=2$ نجد:

$$gcd(2,11)=gcd(2,31)=1$$
$$gcd(2,11)=1\Longrightarrow 2^{\phi(11)}\equiv 1(mod\ 11)\Longrightarrow 2^{10}\equiv 1(mod\ 11)\Longrightarrow (2^{10})^{34}\equiv 1(mod\ 11)$$
$$\Longrightarrow 2^{340}\equiv 1(mod\ 11)\ldots.(1)$$
$$gcd(2,31)=1\Longrightarrow 2^{\phi(31)}\equiv 1(mod\ 31)\Longrightarrow 2^{30}\equiv 1(mod\ 31)$$
$$2^{340}=2^{30\times 11+10}=(2^{30})^{11}\times 2^{10}\equiv 2^{10}(mod\ 31)\equiv 1(mod\ 31)$$
$$\Longrightarrow 2^{340}\equiv 1(mod\ 31)\ldots.(2)$$

من (1) و (2) وكون $\gcd(11,31)=1$ عندئذ

$$2^{340}\equiv 1(mod\ 11\times 31)$$
$$\Longrightarrow 2^{m-1}\equiv 1(mod\ m)$$

نستنتج مما سبق $m=341$عدد شبه أولي للأساس 2.

السؤال الثاني:

ليكن n عدد شبه أولي للأساس 2 والمطلوب أثبت أنّ $M_n=2^n-1$ عدد شبه أولي للأساس 2.

الحلّ:

- لدينا n عدد شبه أولي للأساس 2 فإنّ n عدد مؤلف

$$n=rs;1<r<n\ \&\ 1<s<n$$
$$M_n=2^n-1=2^{rs}-1=(2^r)^s-1=(2^r-1)((2^r)^{s-1}+(2^r)^{s-2}\ldots+(2^r)+1)$$

لنضع $k=2^r-1$ و $t=(2^r)^{s-1}+(2^r)^{s-2}\ldots+2^r+1$

عندئذٍ

$$M_n=kt;1<k<M_n\ \&\ 1<t<M_n$$

بالتالي M_n ليس بعدد أولي أي M_n عدد مؤلف.

- بما أنّ n عدد شبه أولي للأساس 2 عندئذ

$$2^{n-1}\equiv 1(mod\ n)$$

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

بالتالي

$$2^n - 2 = tn$$

حيث $t \in \mathbb{Z}^+$

$$2^{M_n-1} - 1 = 2^{2^n-2} - 1 = (2^n)^t - 1 = (2^n - 1)((2^n)^{t-1} + (2^n)^{t-2} \dots + (2^n) + 1)$$
$$= M_n \times l$$

حيث $l = (2^n)^{t-1} + (2^n)^{t-2} \dots + (2^n) + 1$

بالتالي

$$2^{M_n-1} - 1 \equiv 0(mod\ M_n)$$

بالتالي

$$2^{M_n-1} \equiv 1(mod\ M_n)$$

مما سبق نجد أنّ $M_n = 2^n - 1$ عدد شبه أولي للأساس 2

تعريف: عدد كارميكل

إذا كان m عدداً صحيحاً موجباً وليس أولياً وكان $a^{m-1} \equiv 1(mod\ m)$ أياً كان العدد الصحيح a بحيث $gcd(a,m) = 1$ فإنّ m يدعى عدد كارميكل.

السؤال الثالث

أثبت أنّ $m = 561$ عدد كارميكل

الحلّ: بما أن $m = 561 = 3 \times 11 \times 17$

أياً كان العدد الصحيح a بحيث $gcd(a, 561) = 1$ فإنّ

$$gcd(a,3) = gcd(a,11) = gcd(a,17) = 1$$

$$gcd(a,3) = 1 \Longrightarrow a^{\phi(3)} \equiv 1(mod\ 3) \Longrightarrow a^2 \equiv 1(mod\ 3) \Longrightarrow (a^2)^{280} \equiv 1(mod\ 3)$$
$$\Longrightarrow a^{560} \equiv 1(mod\ 3) \dots .(1)$$

$$gcd(a,11) = 1 \Longrightarrow a^{\phi(11)} \equiv 1(mod\ 11) \Longrightarrow a^{10} \equiv 1(mod\ 11) \Longrightarrow (a^{10})^{56} \equiv 1(mod\ 11)$$
$$\Longrightarrow a^{560} \equiv 1(mod\ 11) \dots .(2)$$

$$gcd(a,17) = 1 \Longrightarrow a^{\phi(17)} \equiv 1(mod\ 17) \Longrightarrow a^{16} \equiv 1(mod\ 17) \Longrightarrow (a^{16})^{35} \equiv 1(mod\ 17)$$
$$\Longrightarrow a^{560} \equiv 1(mod\ 17) \dots .(3)$$

من (1) و (2) و(3) وكون $\gcd(3,11,17) = 1$ عندئذ

$$a^{560} \equiv 1(mod\ 3 \times 11 \times 17)$$
$$\Longrightarrow a^{m-1} \equiv 1(mod\ m)$$

بالتالي $m = 561$ عدد كارميكل.

السؤال الرابع

أثبت أنّ $m = 1729$ عدد كارميكل

الحلّ: بما أن $m = 1729 = 7 \times 13 \times 19$

أياً كان العدد الصحيح a بحيث $gcd(a, 1729) = 1$ فإنّ

$$gcd(a,7) = gcd(a,13) = gcd(a,19) = 1$$

$$gcd(a,7) = 1 \Longrightarrow a^{\phi(7)} \equiv 1(mod\ 7) \Longrightarrow a^6 \equiv 1(mod\ 7) \Longrightarrow (a^6)^{288} \equiv 1(mod\ 7)$$

$$\Rightarrow a^{1728} \equiv 1(mod\ 7) \ldots . (1)$$

$$gcd(a,13) = 1 \Rightarrow a^{\phi(13)} \equiv 1(mod\ 13) \Rightarrow a^{12} \equiv 1(mod\ 13) \Rightarrow (a^{12})^{144} \equiv 1(mod\ 13)$$

$$\Rightarrow a^{1728} \equiv 1(mod\ 13) \ldots . (2)$$

$$gcd(a,19) = 1 \Rightarrow a^{\phi(19)} \equiv 1(mod\ 19) \Rightarrow a^{18} \equiv 1(mod\ 19) \Rightarrow (a^{18})^{96} \equiv 1(mod\ 19)$$

$$\Rightarrow a^{1728} \equiv 1(mod\ 19) \ldots . (3)$$

من (1) و (2) و(3) وكون $\gcd(7,13,19) = 1$ عندئذ

$$a^{1728} \equiv 1(mod\ 7 \times 13 \times 19)$$

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

بالتالي$m = 1729$ عدد كارميكل.

السؤال الخامس

إذا كان $m = p_1 p_2 \ldots p_s$ حيث p_i أعداد أولية مختلفة و

$$(p_i - 1) \mid (m - 1)$$

لكلّ $1 \le i \le s$ فإن m عدد كارميكل.

الحلّ: يجب أن نثبت: أياً كان العدد الصحيح a بحيث $gcd(a,m) = 1$ فإنّ $a^{m-1} \equiv 1(mod\ m)$.

أياً كان العدد الصحيح a بحيث $gcd(a,m) = 1$ فإنّ $gcd(a,p_i) = 1$ لكلّ $1 \le i \le s$

$$\Rightarrow a^{\phi(p_i)} \equiv 1(mod\ p_i) \Rightarrow a^{p_i - 1} \equiv 1(mod\ p_i)$$

وبما أنّ

$$(p_i - 1) \mid (m - 1)$$

عندئذ $m - 1 = t_i(p_i - 1)$ حيث $t_i \in \mathbb{Z}^+$ لكلّ $1 \le i \le s$ بالتالي

$$a^{m-1} = (a^{p_i - 1})^{t_i} \equiv (1)^{t_i}(mod\ \ p_i) \equiv 1(mod\ \ p_i)$$

$$\Rightarrow a^{m-1} \equiv 1(mod\ \ p_i) \ \ \forall\, 1 \le i \le s$$

$$\Rightarrow a^{m-1} \equiv 1\left(mod\ \ \prod_{i=1}^{s} p_i\right)$$

بالتالي$a^{m-1} \equiv 1(mod\ m)$. مما سبق نجد أنّ m عدد كارميكل.

السؤال السادس

أثبت أنّ $37 \mid (2 \times 34! + 1)$.

الحلّ: لدينا 37 عدد أولي بالتالي حسب ويلسون نجد:

$$(37 - 1)! \equiv -1(mod\ 37)$$

بالتالي

$$36! \equiv -1(mod\ 37) \Rightarrow 36 \times 35 \times 34! \equiv -1(mod\ 37)$$

$$\Rightarrow (-1) \times (-2) \times 34! \equiv -1(mod\ 37)$$

$$\Rightarrow 2 \times 34! + 1 \equiv 0(mod\ 37) \Rightarrow 37 \mid (2 \times 34! + 1)$$

السؤال السابع

أثبت أنّ $37 \mid (31 \times 33! + 1)$.

الحلّ: لدينا 37 عدد أولي بالتالي حسب ويلسون نجد:

$$(37-1)! \equiv -1(mod\ 37)$$

بالتالي

$$36! \equiv -1(mod\ 37) \Longrightarrow 36 \times 35 \times 34 \times 33! \equiv -1(mod\ 37)$$
$$\Longrightarrow (-1) \times (-2) \times (-3) \times 33! \equiv -1(mod\ 37)$$
$$\Longrightarrow (-6) \times 33! \equiv -1(mod\ 37)$$
$$\Longrightarrow (31) \times 33! \equiv -1(mod\ 37)$$
$$\Longrightarrow 31 \times 33! + 1 \equiv 0(mod\ 37) \Longrightarrow 37 \mid (31 \times 33! + 1)$$

السؤال الثامن

أثبت أنّ $19 \mid (18! + 1)$.

الحلّ: لدينا 19 عدد أولي بالتالي حسب ويلسون نجد:

$$(19-1)! \equiv -1(mod\ 19)$$

بالتالي

$$18! \equiv -1(mod\ 19) \Longrightarrow 18! + 1 \equiv 0(mod\ 19)$$
$$\Longrightarrow 19 \mid (18! + 1)$$

السؤال التاسع

أوجد باقي قسمة العدد $26! \times 2$ على العدد 29.

الحلّ: لدينا 29 عدد أولي بالتالي حسب ويلسون نجد:

$$(29-1)! \equiv -1(mod\ 29)$$

بالتالي

$$28! \equiv -1(mod\ 29) \Longrightarrow 28 \times 27 \times 26! \equiv -1(mod\ 29)$$
$$\Longrightarrow (-1) \times (-2) \times 26! \equiv -1(mod\ 29)$$
$$\Longrightarrow 2 \times 26! \equiv -1(mod\ 29)$$
$$\Longrightarrow 2 \times 26! \equiv 28(mod\ 29)$$

الباقي هو العدد 28

السؤال العاشر

أوجد باقي قسمة العدد $255!$ على العدد الأولي 257.

الحلّ: لدينا 257 عدد أولي بالتالي حسب ويلسون نجد:

$$(257-1)! \equiv -1(mod\ 257)$$

بالتالي

$$256! \equiv -1(mod\ 257) \Longrightarrow 256 \times 255! \equiv -1(mod\ 257)$$
$$\Longrightarrow (-1) \times 255! \equiv -1(mod\ 257)$$
$$\Longrightarrow 255! \equiv 1(mod\ 257)$$

الباقي هو العدد 1
