الأربعاء: 2015/5/27

المحاضرة التاسعة عشر:

مبرهنة:

يوجد للعدد m جذر أولي إذا وفقط إذا كان $m=2$ أو $m=4$ أو $m=p^n$ أو $m=2p^n$ حيث p عدد أولي فردي و n عدد صحيح موجب

$$(a,m)=1 \quad , \quad a^1 \equiv 1 \pmod 2$$

دليل:

تعريف الدليل:

إذا كان r جذراً أولياً للعدد m وإذا كان b عدد صحيح موجب وأولياً نسبياً مع m أي $(b,m)=1$ فإن أصغر عدد صحيح موجب k حيث $1 \le k \le \phi(m)$ يحقق $r^k \equiv b \pmod m$ يسمى دليل العدد b بالنسبة للجذر r والمقياس m ونكتب:

$$r^{Indb} \equiv b \pmod m \iff k = Ind_r b \leftarrow \text{رمز الدليل}$$

مثال

الجذر الأولي للعدد 5، لدينا:

$$T(5) = \{1, 2, 3, 4\}$$

$\phi(5) = 4$ وإن رتبة العدد 2 هي

$$(*)\ 2^1 \equiv 2 \pmod 5 \quad , \quad 2^2 \equiv 4 \pmod 5 \quad 2^3 \equiv 3 \pmod 5$$
$$2^4 \equiv 1 \pmod 5$$

2 جذر أولي للعدد 5

من (*) نجد أن

$$Ind_2 2 = 1 \quad , \quad Ind_2 4 = 2$$

$$Ind_2 3 = 3 \quad , \quad Ind_2 1 = 4$$

b	1	2	3	4
$Ind_2 b$	4	1	3	2

خواص الأدلة:

إذا كان r جذراً أولياً للعدد m ، إذا كان $N, M \in \mathbb{Z}^+$ وكان $(N.M, m)=1$

فإن:

1] $Ind_r N \equiv Ind_r M \pmod{\varphi(m)} \iff N \equiv M \pmod{m}$

تحت الإثبات

البرهان:

من تعريف الأدلة نكتب

$$N \equiv r^{Ind N} \pmod{m} \quad \wedge \quad M \equiv r^{Ind M} \pmod{m}$$

$$N \equiv M \pmod{m} \iff r^{Ind_r N} \equiv r^{Ind_r M} \pmod{m}$$

وحسب مبرهنة سابقة فإن

$$r^{Ind_r N} \equiv r^{Ind_r M} \pmod{m} \iff Ind_r N \equiv Ind_r M \pmod{\varphi(m)}$$

2] $Ind_r N.M \equiv (Ind_r N + Ind_r M) \pmod{\varphi(m)}$

3] $Ind_r M^k \equiv k \, Ind_r M \pmod{\varphi(m)} \quad ; \quad k \in \mathbb{Z}^+$

4] إذا كان r, s جذرين أوليين للعدد m فإن:

$$Ind_r N \equiv Ind_s N \cdot Ind_r s \pmod{\varphi(m)}$$

حل التطابقات غير الخطية باستخدام الأدلة:

$$a x^k \equiv b \pmod{m}$$

إذا كان $k = 2$ تسمى التطابقات التربيعية

تمرين :

آكتب جدول الأدلة للعدد $m=11$ (وظيفة)
وأوجد الجذر الأولي الأصغر للعدد 11.

جدول الأدلة للعدد 13 بالنسبة للأساس 2.
وجدنا أن $r=2$ هو جذر أولي للعدد 13

b	1	2	3	4	5	6	7	8	9	10	11	12
Ind_{2}^{b}	12	1	4	2	9	5	11	3	8	10	7	6

$2^{1} \equiv 2 \pmod{13} \Rightarrow Ind_2 2 = 1$

$2^{2} \equiv 4 \pmod{13} \Rightarrow Ind_2 4 = 2$

$2^{3} \equiv 8 \pmod{13} \Rightarrow Ind_2 8 = 3$

$2^{4} \equiv 3 \pmod{13} \Rightarrow Ind_2 3 = 4$

$2^{5} \equiv 6 \pmod{13} \Rightarrow Ind_2 6 = 5$

$2^{6} \equiv 12 \pmod{13} \Rightarrow Ind_2 12 = 6$

$2^{7} \equiv 11 \pmod{13} \Rightarrow Ind_2 11 = 7$

$2^{8} \equiv 9 \pmod{13} \Rightarrow Ind_2 9 = 8$

$2^{9} \equiv 5 \pmod{13} \Rightarrow \text{Ind}_2 5 = 9$

$2^{10} \equiv 10 \pmod{13} \Rightarrow \text{Ind}_2 10 = 10$

$2^{11} \equiv 7 \pmod{13} \Rightarrow \text{Ind}_2 7 = 11$

$2^{12} \equiv 1 \pmod{13} \Rightarrow \text{Ind}_2 1 = 12$

جدول الأدلة للعدد $n=17$ بالنسبة للأساس 3

b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\text{Ind}_{3=y}^{b}$	16	14	1	12	5	5	11	10	2	3	7	13	4	9	6	8

$3^{1} \equiv 3 \pmod{17} \Rightarrow \text{Ind}_3 3 = 1$

$3^{2} \equiv 9 \pmod{17} \Rightarrow \text{Ind}_3 9 = 2$

$3^{3} \equiv 10 \pmod{17} \Rightarrow \text{Ind}_3 10 = 3$

$3^{4} \equiv 13 \equiv -4 \pmod{17} \Rightarrow \text{Ind}_3 13 = 4$

$3^{5} \equiv 5 \pmod{17} \Rightarrow \text{Ind}_3 5 = 5$

$3^{6} \equiv 15 \pmod{15} \Rightarrow \text{Ind}_3 15 = 6$

وهكذا بنفس الطريقة ...

حل تمارين صفحة 183

أوجد حلول التطابقة: (5/183)

$3x^{3} = 3 \pmod{13}$

الحل =

2 هو جذر أولي للعدد 13 ، $\phi(13)=12$

نأخذ دليل الطرفين في التطابقة بالنسبة للأساس 2

$$Ind_2(3x^3) \equiv Ind_2 3 \pmod{\phi(13)}$$

حسب الخاصية [2]

$$Ind_2 3 + 3 Ind_2 x \equiv Ind_2 3 \pmod{12}$$

$$4+3y \equiv 4 \pmod{12} \quad ; \quad y = Ind_2 x$$

$$3y \equiv 0 \pmod{12}$$

$(3,12)=3$

$3 \mid 0 \Rightarrow$ للتطابقة ثلاثة حلول غير متطابقة بالمقياس 12

$$y \equiv 0 \pmod 4$$

و تأخذ y قيم

$y \equiv 4 \Rightarrow x \equiv 3 \pmod{13}$

$y \equiv 8 \Rightarrow x \equiv 9 \pmod{13}$

$y \equiv 12 \Rightarrow x \equiv 1 \pmod{13}$

أوجد حل التطابقة: $x^8 \equiv 10 \pmod{13}$

الحل:

لدينا: $\phi(13)=12$ ، نأخذ دليل الطرفين بالنسبة للأساس 2

$$8 Ind_2 x \equiv Ind_2 10 \pmod{\phi(13)}$$

$$8y \equiv 10 \pmod{12}$$

$(8,12)=4 \nmid 10$ ليس للتطابقة حل

وبالتالي لا يوجد حل للتطابقة المعطى

9/183) أوجد حل التطابقة: $x^{12} \equiv 13 \pmod{17}$

الحل:

لدينا: $\varphi(17)=16$ ، نأخذ دليل الطرفين بالنسبة للأساس 3

$$12\ \mathrm{Ind}_3 x \equiv \mathrm{Ind}_3 13 \pmod{\varphi(17)}$$

$$12y \equiv 4 \pmod{16} \quad ; \quad \mathrm{Ind}_3 x = y$$

$(12,16)=4 \mid 4$ للتطابقة أربعة حلول مختلفة بالقاس 16

$$3y \equiv 1 \pmod 4$$

$$y=3 \Rightarrow x \equiv 10 \pmod{17}$$
$$y \equiv 7 \Rightarrow x \equiv 11 \pmod{17}$$
$$y \equiv 11 \Rightarrow x \equiv 7 \pmod{17}$$
$$y \equiv 15 \Rightarrow x \equiv 6 \pmod{17}$$

ملاحظة: جدول الدليل لا يوجد فيه تكرار للقيم.

أوجد حل التطابقة: $9x^8 \equiv 8 \pmod{17}$

الحل:

3 جذر أولي ، $\varphi(17)=16$

$$8y \equiv 8 \pmod{16}$$

$(8,16)=8 \mid 8$ للتطابقة 8 حلول مختلفة.

$$y \equiv 1 \pmod 2$$

$$y \equiv 1 \Rightarrow x \equiv 3 \pmod{17}$$
$$y \equiv 3 \Rightarrow x \equiv 10 \pmod{17}$$
$$y \equiv 5 \Rightarrow x \equiv 5 \pmod{17}$$
$$y \equiv 7 \Rightarrow x \equiv 11 \pmod{17}$$

$y \equiv 9 \Rightarrow x \equiv 14 \pmod{17}$

$y \equiv 11 \Rightarrow x \equiv 7 \pmod{17}$

$y \equiv 13 \Rightarrow x \equiv 12 \pmod{17}$

$y \equiv 15 \Rightarrow x \equiv 6 \pmod{17}$

لنتوقف للمحاضرة ...