المحاضرة الثانيـة عشـر

تعريف:

يقال عن $b \in Z$ أنه معكوس أو نظيـر (Inverse) ضـربي للعـدد $a \in Z$ قياس n ، إذا كان $ab \equiv 1 \pmod{n}$.

نلاحظ انه ليس بالضرورة ان يوجد لكل عدد صحيح نظير ضربي بالمقاس n. وبشكل عام لا يوجد نظير ضربي لأي عدد زوجي إذا كان المقاس زوجياً.

مثـال:

$2 \in Z$ معكوس ضربي للعدد $3 \in Z$ قيـاس 5 ، لأن $3 \times 2 \equiv 1 \pmod{5}$ و

$4 \in Z$ معكوس ضربي للعدد $4 \in Z$ قياس 5 ، لأن $4 \times 4 \equiv 1 \pmod{5}$.

لا يوجد نظير ضربي للعدد 2 بالمقاس 4، لان التطابق $2x \equiv 1 (mod\ 4)$، ليس له حل لان (2,4)=2، و $2 \nmid 1$.

نتيجـة (7) :

إذا كان p عدداً أولياً و $p \nmid a$ فإن للتطابق الخطي $ax \equiv b \pmod{n}$ حـل وحيد قياس p .

نتيجـة (8) :

يكون للعدد $a \in Z$ معكوساً ضربياً قياس n إذاً وإذا فقط كان $(a,n)=1$.

البرهان:

نفـرض $b \in Z$ هـو المعكـوس الـضربي للعـدد a قيـاس n . إذا $ab \equiv 1 \pmod{n}$ ، وعليه فإن $n \mid ab-1$ وهذا يعني وجود $r \in Z$ بحيث أن $ab-1=nr$ ومنا نجد أن $ab+n(-r)=1$ ، عليه فـإن $(a,n)=1$ حـسب

ولإثبات العكس نفرض أن $(a,n)=1$. إذاً يوجد عنصر وحيد $b\in Z$ بحيث أن $ab\equiv 1 \pmod n$ حسب مبرهنة (٣-٤-١) ، وعليه يوجد للعنصر $a\in Z$ معكوس ضربي قياس n .

مثال:

حل كلاً من التطابقات الخطية الاتية، ثم جد المكوس:

(أ) $4x \equiv 9 (\mathrm{mod}\ 7)$

(ب) $11x \equiv 25 (\mathrm{mod}\ 60)$

(جـ) $\mathbf{17}x \equiv \mathbf{60}(mod\ \mathbf{94})$

الحل: (أ)

$\mathbf{4}x \equiv \mathbf{9}\ (mod\ \mathbf{7})$

$a = 4, n = 7, b = 9$

7=4(1) +3,

4=3(1) +1,

3=1(3) +0

$\Rightarrow \boldsymbol{d(a,n)} = (\mathbf{4},\mathbf{7}) = \mathbf{1}$, $\exists r, s \in Z$,

$s.t.\ 7r + 4\,s = 1$

1=4-3=4-(7-4) = (2)4 - (1)7

Multiply the above equation by **9**, we get **9= (18)4+(-9)7** ⇒ r=-9, s=18.

للتحقيق:

$\mathbf{4(18)} \equiv \mathbf{9}(mod\ \mathbf{7})$

$\mathbf{72} \equiv \mathbf{9}(mod\ \mathbf{7})$

$\mathbf{7} \setminus (\mathbf{72} - \mathbf{9}) = \mathbf{7} \setminus \mathbf{63} = \mathbf{9}.$

لإيجاد المعكوس

$(4,7) = 1$

Dr. Ghada M. Al-Nafie

$x \equiv 9 \cdot 4^{-1} (mod\ 7)$ & $Z_7 = \{0,1,2,3,4,5,6\}$

$4^{-1} = 2 \in Z_7$

$4 \times 2 = 8 = 1 \in Z_7$

$x = 9 \times 2 \equiv 4\ (mod\ 7)$.

Or, by using

a=4, n=7, b=9, **d= (4, 7) =1**, $d \setminus b = 1 \setminus 9$

4x- 9= 7k ⇒ x= (7k+9)/4

k=0 1 2 3 4 5 6

x= 4 11

(ب)

$11x \equiv 25\ (mod\ 60)$

a=11, n=60, b=25.

$\Rightarrow 11x \equiv 25\ (mod\ 60)$

60=11(5) +5,

11=5(2) +1,

5=1(5) +0

$\Rightarrow \boldsymbol{d(a,n) = (11,60) = 1}$, $\exists r, s \in Z, s.t.\ 60r + 11\ s = 1$

1=11-2(5) =11-2(60-11(5)) = (11)11 - (2)60

Multiply the above equation by 25, we get 25= (275)11-(22)60 ⇒ r=-22, s=275.

للتحقيق:

$11(275) \equiv 25\ (mod\ 60)$

$3025 \equiv 25\ (mod\ 60)$

$60 \setminus (3025 - 25) = 60 \setminus 3000 = 50.$

$(11,60) = 1$

Dr. Ghada M. Al-Naemi

$x \equiv 25 \cdot 11^{-1} (mod\ 60)$ & $Z_{60} = \{0, 1, 2, 3, 4, 5, 6, \dots, 58, 59\}$

$11^{-1} = 11 \in Z_{60}$

$11 \times 11 = 1 \in Z_{60}$

$x = 25 \times 11 \equiv 11\ (mod\ 60)$

(⇏)

$17x \equiv 60\ (mod\ 94)$

a=17, n=94, b=60. ⇒ $17x \equiv 60\ (mod\ 94)$

94= 5(17) + 9,

17= 1(9) +8,

9= 1(8) +1,

8= 8(1) + 0

⇒ **d=1**.

$(\mathbf{a}, \mathbf{n}) = \mathbf{1} \Rightarrow (17, 94) = 1$

$\because (\mathbf{17}, \mathbf{94}) = \mathbf{1}$

$\Rightarrow \exists r, s \in Z,\ s.t.\ 94r + 17\ s = 1$

1=9-8 =9- [17-9] = 9-17+ 9 =2(9)-17

=2[94-5(17)] - 17= 2(94) – 10(17) - 17

=2(94) – 11(17)

∴ r=2 & s= -11

$17(-11) \equiv 60\ (mod\ 94)$

$x \equiv 60 \cdot 17^{-1} (mod\ 94)$ & $Z_{94} = \{0, 1, 2, 3, 4, 5, 6, \dots, 92, 93\}$

$17^{-1} \equiv 83 (mod\ 94)$

$\therefore 17 \times 83 = 1\ (mod\ 94)$

$17^{-1} = 83 \in Z_{94}$

$x \equiv 60 \cdot 17^{-1} (mod\ 94)$

Dr. Ghada M. Al-Naemi

$\equiv 60(83)(mod\ 94)$

∴هو حل للتطابق الخطي.

$\mathbf{17(4980) \equiv 60\ (mod\ 94)}$

$\mathbf{84660 \equiv 60\ (mod\ 94)}$

$\mathbf{94 \setminus (84660 - 60) = 94 \setminus 84600 = 1410.}$

مثال:

1- حل كلاً من التطابقات الخطية الاتية $9x \equiv 21(mod\ 30)$.

a=9, n=30, b=21 ⇒ $9x \equiv 21\ (mod\ 30)$.

30=9(3) +3,

9=3(1) + 0.

$(\mathbf{a, n}) = (\mathbf{9, 30}) = \mathbf{3}$, since $d \setminus b = 3 \setminus 21$

$\because (\mathbf{9, 30}) = \mathbf{3} \Rightarrow \exists r, s \in Z,\ s.t.\ 30r + 9\ s = 3$

3= (1)30+ (-3)9

⇒ 21= (7)30 +(-21)9,

⇒r=7 & s=-21.

$x_k = x_0 + \left(\frac{n}{d}\right)k$, k=0, 1, 2, 3, …, d-1.

$x_1 = -21, x_2 = -11, x_3 = -1,$

$x_1 = 9, x_2 = 19, x_3 = 29.$

$9 \equiv -21(mod\ 30), 19 \equiv -11(mod\ 30), 29 \equiv -1(mod\ 30).$

2- حل المتطابقة الخطية الاتية $4x \equiv 3(mod\ 5)$.

a=4, n=5, b=3, d= (4, 5) =1, $d \setminus b = 1 \setminus 5$

4x- 3= 5k ⇒ x= (5k+3)/4

k=0 1 2 3 4

x= 2

Dr Ghada M. Al-Naemi

3- حل كلاً من التطابقات الخطية الاتية $6x - 3 \equiv 1 (mod\ 10)$.

a=6, n=10, b=4, d= (6, 10) =2, $d \setminus b = 2 \setminus 4$

6x- 4= 10k ⇒ x= (10k+4)/6

k=0 1 2 3 4 5 6 7 8 9

x= 4 9

Dr. Ghada M. Al-Naemi