كلية العلوم

القسم : الرياضيات

السنة : الرابعة

المادة : نظرية الاعداد

المحاضرة : العاشرة /عملي/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

10

المحاضرة العاشرة
(عملي)

السؤال الأول:

1. أوجد الحلول المختلفة للتطابق $x^8 \equiv 16(mod\ 17)$.
2. أوجد الحلين المختلفين للتطابق $3x^2 - 2x - 6 \equiv 0(mod\ 17)$.

الحلّ:

1. لدينا $g = 3$ جذر أساسي بالنسبة للمقاس 17 حسب اختبار لوكاس.

ولنوجد جدول الأدلة بالنسبة للمقاس 17 علماً أن $g = 3$ جذر أساسي بالنسبة للمقاس 17.

نحسب 3^k حيث $1 \le k \le \phi(17) = 16$.

3^k	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9	3^{10}	3^{11}	3^{12}	3^{13}	3^{14}	3^{15}	3^{16}
N	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
$IndN$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

N: هو باقي قسمة 3^k على العدد 17. $IndN$: دليل العدد N

نطبق نظرية الأدلة للطرفين نجد $x^8 \equiv 16(mod\ 17)$

$$8\ Indx \equiv Ind16(mod\ \phi(17))$$
$$8\ Indx \equiv 8(mod\ 16)$$

نضع $Indx = y$ بالتالي التطابق الخطي

$$8\ y \equiv 8(mod\ 16)$$

يملك ثمان حلول مختلفه بالنسبة للمقاس 16 هما $Indx = y \in \{1,3,5,7,9,11,13,15\}$ بالتالي

$$Indx = 1 \Longrightarrow x = 3$$
$$Indx = 3 \Longrightarrow x = 10$$
$$Indx = 5 \Longrightarrow x = 5$$
$$Indx = 7 \Longrightarrow x = 11$$
$$Indx = 9 \Longrightarrow x = 14$$
$$Indx = 11 \Longrightarrow x = 7$$
$$Indx = 13 \Longrightarrow x = 12$$
$$Indx = 15 \Longrightarrow x = 6$$

بالتالي حلول التطابق $x^8 \equiv 16(mod\ 17)$ هي

$$\{3,5,6,7,10,11,12,14\}$$

2. لدينا $a = 3$ و $b = -2$ و $c = -6$ و $p = 17$

- نوجد $d = b^2 - 4ac = 76$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$، أي لنوجد حلول التطابق $y^2 \equiv 76(mod\ 17)$

أي لنوجد حلول التطابق

$$y^2 \equiv 8(mod\ 17)$$

وهي $\{-5,5\}$

✓ من أجل $y_0 = 5$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 17)$$

فنجد

$$6x \equiv 7(mod\ 17) \Longrightarrow x \equiv 4(mod\ 17) \Longrightarrow x = 4$$

✓ من أجل $y_0 = -5$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 17)$$

فنجد

$$6x \equiv -3(mod\ 17) \Longrightarrow x \equiv 8(mod\ 17) \Longrightarrow x = 8$$

بالتالي حلول التطابق $3x^2 - 2x - 6 \equiv 0(mod\ 17)$ هي

$$\{4, 8\}$$

السؤال الثاني:

1. بيّن فيما إذا كان التطابق $x^6 \equiv 10(mod\ 19)$ قابل للحلّ أم لا في مجموعة الأعداد الصحيحة؟
2. أوجد الحلول المختلفة للتطابق $x^5 \equiv 11(mod\ 19)$.
3. أوجد الحلين المختلفين للتطابق $3x^2 - 2x - 8 \equiv 0(mod\ 19)$.

الحلّ:

1. التطابق $x^n \equiv a(mod\ m)$ قابل للحل إذا وفقط إذا كان

$$a^{\frac{\phi(m)}{d}} \equiv 1(mod\ m)$$

حيث

$$d = \gcd\big(n, \phi(m)\big)$$

(مبرهنة أولر المعممة)

التطابق المعطى هو: $x^6 \equiv 10(mod\ 19)$

لدينا $n = 6, a = 10, m = 19$

$$\phi(m) = 18, \qquad d = \gcd\big(n, \phi(m)\big) = 6$$

نلاحظ بأنّ

$$a^{\frac{\phi(m)}{d}} = 10^3 \not\equiv 1(mod\ 19)$$

بالتالي التطابق غير قابل للحلّ في مجموعة الأعداد الصحيحة.

2. لدينا $g = 2$ جذر أساسي بالنسبة للمقاس 19، ولنوجد جدول الأدلة بالنسبة للمقاس 19 علماً أنّ $g = 2$ جذر أساسي بالنسبة للمقاس 19.

نحسب 2^k حيث $1 \le k \le \phi(19) = 18$.

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	2^{15}	2^{16}	2^{17}	2^{18}
N	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$IndN$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

N: هو باقي قسمة 2^k على العدد 19. $IndN$: دليل العدد N

نطبق نظرية الأدلة للطرفين نجد $x^5 \equiv 11(mod\ 19)$

$$5\ Indx \equiv Ind11(mod\ \phi(19))$$

$$5\ Indx \equiv 12(mod\ 18)$$

نضع $Indx = y$ بالتالي التطابق الخطي

$$5\ y \equiv 12(mod\ 18)$$

يملك حل وحيد هو $y = Indx = 6$ بالتالي

$$Indx = 6 \Longrightarrow x = 7$$

بالتالي حلول التطابق $x^5 \equiv 11(mod\ 19)$ هي

$$\{7\}$$

3. لدينا $a = 3$ و $b = -2$ و $c = -8$ و $p = 19$

- نوجد $d = b^2 - 4ac = 100$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$، أي لنوجد حلول التطابق $y^2 \equiv 5(mod\ 19)$ وهي $\{-10, 10\}$

✓ من أجل $y_0 = 10$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 19)$$

فنجد

$$6x \equiv 12(mod\ 19) \Longrightarrow x \equiv 2(mod\ 19) \Longrightarrow x = 2$$

✓ من أجل $y_0 = -10$ نحل التطابق الخطي

$$2ax \equiv y_0 - b(mod\ 19)$$

فنجد

$$6x \equiv -8(mod\ 19) \Longrightarrow x \equiv 5(mod\ 19) \Longrightarrow x = 5$$

بالتالي حلول التطابق $3x^2 - 2x - 8 \equiv 0(mod\ 19)$ هي

$$\{2, 5\}$$

السؤال الثالث:

أوجد جدول الأدلة بالنسبة للمقاس 11 علماً أنّ $g = 2$ جذر أساسي بالنسبة للمقاس 11، ثم أوجد حلول التطابق $x^4 \equiv 4\ (mod\ 11)$ باستخدام الأدلة.

الحلّ:

1. نحسب $2^k; 1 \leq k \leq \phi(11) = 10$ (2 جذر أساسي بالنسبة للمقاس 11).

2^k	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
N	2	4	8	5	10	9	7	3	6	1
$IndN$	1	2	3	4	5	6	7	8	9	10

N: هو باقي قسمة 2^k على العدد 11. $IndN$: دليل العدد N

$x^4 \equiv 4\ (mod\ 11)$ نطبق نظرية الأدلة للطرفين نجد

$$4\ Indx \equiv Ind4(mod\ \phi(11))$$
$$4\ Indx \equiv 2(mod\ 10)$$

نضع $Indx = y$ بالتالي التطابق الخطي

$$4y \equiv 2(mod\ 10)$$

هذا التطابق يملك حلين مختلفين هما $y = Indx \in \{3, 8\}$ بالتالي

$$Indx = 3 \Longrightarrow x = 8$$
$$Indx = 8 \Longrightarrow x = 3$$

بالتالي حلول التطابق $x^4 \equiv 4\ (mod\ 11)$ هي

$$\{3, 8\}$$