حل دورة الفصل الثاني

السؤال الأول:

لنشكل أولاً جدول كيلي:

$\circ$	id	$(1\ 4\ 5)$	$(1\ 2)(3\ 5)$
id	id	$(1\ 4\ 5)$	$(1\ 2)(3\ 5)$
$(1\ 4\ 5)$	$(1\ 4\ 5)$	$(1\ 5\ 4)$	$(1\ 2\ 4\ 5\ 3)$
$(1\ 2)(3\ 5)$	$(1\ 2)(3\ 5)$	$(1\ 4\ 3\ 5\ 2)$	id

شرح مفصل عن كيفية الحصول على النتائج الموجودة في الجدول:

لدينا تركيب أي حلقة مع الـ id تبقى الحلقة نفسها.

$$(1\ 4\ 5)(1\ 4\ 5) = (1\ 5\ 4)$$

لإن: أولاً نضع الواحد في بداية الحلقة ثم نلاحظ: $5 \longrightarrow 4 \longrightarrow 1$ وبعدها نضع
مرتبط مرتبط

الخمسة بعد الواحد ثم نلاحظ $4 \longrightarrow 1 \longrightarrow 5$ وأخيراً نضع الأربعة.
مرتبط مرتبط

$$(1\ 4\ 5)(1\ 2)(3\ 5) = (1\ 2\ 4\ 5\ 3)$$

لإن: أولاً نضع الواحد في بداية الحلقة ثم نلاحظ: $2 \longrightarrow 1$ وبعدها نضع الاثنان بعد
مرتبط

الواحد ثم نلاحظ $4 \longrightarrow 1 \longrightarrow 2$ وعندها نضع الأربعة بعد الاثنان ثم نلاحظ 4
مرتبط مرتبط

$5 \longrightarrow$ وبعدها نضع الخمسة ثم نلاحظ $3 \longrightarrow 5$ عندها نضع ثلاثة ثم نلاحظ 3
مرتبط مرتبط

$1 \longrightarrow 5 \longrightarrow$ عندها نغلق الحلقة.
مرتبط مرتبط

$$(1\ 2)(3\ 5)(1\ 4\ 5) = (1\ 4\ 3\ 5\ 2)$$

لإن: أولاً نضع الواحد في بداية الحلقة ثم نلاحظ: $4 \underset{\text{مرتبط}}{\longrightarrow} 1$وبعدها نضع الأربعة بعد الواحد ثم نلاحظ $3 \underset{\text{مرتبط}}{\longrightarrow} 5 \underset{\text{مرتبط}}{\longrightarrow} 4$ وعندها نضع ثلاثة بعد الأربعة ثم نلاحظ أن $5 \underset{\text{مرتبط}}{\longrightarrow}$ عندها نضع الخمسة ثم نلاحظ $2 \underset{\text{مرتبط}}{\longrightarrow} 1 \underset{\text{مرتبط}}{\longrightarrow} 5$ وبعدها نضع الاثنان ثم نلاحظ $1 \underset{\text{مرتبط}}{\longrightarrow} 2$ عندها نغلق الحلقة.

$$(1\ 2)(3\ 5)(1\ 2)(3\ 5) = id$$

لإن كل عدد مرتبط بنفسه أي: $1 \underset{\text{مرتبط}}{\longrightarrow} 2 \underset{\text{مرتبط}}{\longrightarrow} 1$ وَ $2 \underset{\text{مرتبط}}{\longrightarrow} 1 \underset{\text{مرتبط}}{\longrightarrow} 2$ وَ $5 \underset{\text{مرتبط}}{\longrightarrow} 3 \underset{\text{مرتبط}}{\longrightarrow}$

$5 \underset{\text{مرتبط}}{\longrightarrow} 3 \underset{\text{مرتبط}}{\longrightarrow} 5$ وَ $\underset{\text{مرتبط}}{\longrightarrow} 3$

عندها يتشكل الجدول بالكامل.

من الجدول نلاحظ أن المجموعة A مع عملية تركيب التباديل لا تشكل زمرة لأنها ليست مغلقة بالنسبة لعملية تركيب التباديل حيث أن: $(1\ 4\ 5)(1\ 4\ 5) = (1\ 5\ 4) \notin A$

رتبة العنصر $(1\ 5\ 3)$ بالتعريف هو العدد r الذي يحقق $\underset{\text{حلقة}}{\sigma}^{r} = id$

$$(1\ 5\ 3)^2 = (1\ 5\ 3)(1\ 5\ 3) = (1\ 3\ 5)$$

لإن: نضع الواحد أولاً $3 \underset{\text{مرتبط}}{\longrightarrow} 5 \underset{\text{مرتبط}}{\longrightarrow} 1$ وَ $5 \underset{\text{مرتبط}}{\longrightarrow} 1 \underset{\text{مرتبط}}{\longrightarrow} 3$ وَ $1 \underset{\text{مرتبط}}{\longrightarrow} 3 \underset{\text{مرتبط}}{\longrightarrow} 5$

عندها نغلق القوس.

$$(1\ 5\ 3)^3 = (1\ 5\ 3)^2(1\ 5\ 3) = (1\ 3\ 5)(1\ 5\ 3) = id$$

لإن كل عنصر مرتبط مع نفسه: $1 \underset{\text{مرتبط}}{\longrightarrow} 5 \underset{\text{مرتبط}}{\longrightarrow} 1$ وَ $5 \underset{\text{مرتبط}}{\longrightarrow} 3 \underset{\text{مرتبط}}{\longrightarrow} 5$ وَ $1 \underset{\text{مرتبط}}{\longrightarrow} 3$

$\underset{\text{مرتبط}}{\longrightarrow} 3$

إذاً فإن رتبة العنصر $(1\ 5\ 3)$ هي: $|(1\ 5\ 3)| = 3$

أو بطريقة أخرى بما أن الحلقة بسيطة فرتبة العنصر هي عدد الأعداد في الحلقة أي

$$\left|(\bar{\bar{1}}\ \bar{\bar{5}}\ \bar{\bar{3}})\right| = 3$$

المجموعة: $< (1\ 5\ 3) >$ حسب التعريف هي:

$$< g > = \{g^m : m \in \mathbb{Z}\}$$

أي رفع العنصر إلى أس حيث هذا الأس من مجموعة الأعداد الصحيحة وذلك حتى نصل إلى الحيادي.

$$\Longrightarrow < (1\ 5\ 3) > = \{(1\ 5\ 3)^0 , (1\ 5\ 3)^1 , (1\ 5\ 3)^2 , (1\ 5\ 3)^3\}$$

$$\Longrightarrow < (1\ 5\ 3) > = \{\ id\ , (1\ 5\ 3), (1\ 3\ 5)\}$$

مقلوب العنصر $(3\ 4\ 2\ )$:

بالتعريف: $\underset{\text{حلقة}}{\sigma} \circ \underset{\text{حلقة}}{\beta} = id$ عندها $\sigma^{-1} = \beta$

$$\Longrightarrow (2\ 4\ 3)^{-1} = (2\ 3\ 4)$$

أولاً نكتب الحلقة $(3\ 4\ 2)$ على شكل تبديل:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{pmatrix}$$

ثم نبادل بين السطرين:

$$\begin{pmatrix} 1 & 4 & 2 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

نرتب السطر الأول تصاعدياً (مع المحافظة على الارتباط):

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}$$

وعليه فإن:

$$(2\ 4\ 3)^{-1} = (2\ 3\ 4)$$

السؤال الثاني:

القسم الأول:

هذه المعادلة من الشكل:

$$x^2 \equiv a \ (mod\ p)$$

نلاحظ أن p لا يقسم a

$$\left(\frac{a}{p}\right) = \left(\frac{84975}{349}\right)$$

بتحليل $a = 84975$ إلى عوامله الأولية:

$$\left(\frac{84975}{349}\right) = \left(\frac{3 \times 5^2 \times 11 \times 103}{349}\right)$$

والآن للحل سنستخدم أحد الخواص التالية:

$$1)\ a \equiv b(mod\ p) \iff \frac{a}{p} = \frac{b}{p} \quad \text{إذا كان}$$

$$2)\ -\frac{1}{p} = (-1)^{\frac{p-1}{2}}$$

$$3)\ \frac{a \cdot b}{p} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$4)\ \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

$$5)\ \left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$$

والآن حسب الخاصة (٣) نحصل على:

$$\left(\frac{84975}{349}\right) = \left(\frac{3 \times 5^2 \times 11 \times 103}{349}\right)$$

$$= \left(\frac{3}{349}\right)\left(\frac{5^2}{349}\right)\left(\frac{11}{349}\right)\left(\frac{103}{349}\right)$$

الحد $\left(\frac{5^2}{349}\right) = \left(\frac{5}{349}\right)\left(\frac{5}{349}\right)$ أما كلاهما (-1) أو كلاهما (1) وبالتالي جدائهم في الحالتين يساوي (1).

الحد $\left(\frac{3}{349}\right)$ لحسابه نستخدم الخاصة (٤):

$$\left(\frac{3}{349}\right)\left(\frac{349}{3}\right) = -1 \Longrightarrow \left(\frac{3}{349}\right) = -1\left(\frac{349}{3}\right)$$

حسب الخاصة (١):

$$\Longrightarrow 349 \equiv \underbrace{1}_{\text{باقي قسمة 349 على 3}} \pmod 3$$

$$\Longrightarrow \left(\frac{3}{349}\right) = -1\left(\frac{1}{3}\right) = \left(-\frac{1}{3}\right)$$

حسب الخاصة (٢)

$$\Longrightarrow \left(\frac{3}{349}\right) = \left(-\frac{1}{3}\right) = -1$$

الحد $\left(\frac{11}{349}\right)$ حسب الخاصة (٤):

$$\left(\frac{11}{349}\right)\left(\frac{349}{11}\right) = -1$$

$$\Longrightarrow \left(\frac{11}{349}\right) = -1\left(\frac{349}{11}\right)$$

حسب الخاصة (١):

$$349 \equiv \underbrace{8}_{\text{باقي قسمة 349 على 11}} \pmod{11}$$

$$\Longrightarrow \left(\frac{11}{349}\right) = -1\left(\frac{8}{11}\right)$$

حسب الخاصة (٣):

$$\left(\frac{11}{349}\right) = -1\left(\frac{8}{11}\right) = -1\left(\frac{2\times 2\times 2}{11}\right) = -1\left(\frac{2}{11}\right)\left(\frac{2}{11}\right)\left(\frac{2}{11}\right)$$

حسب الخاصة (٥):

$$\left(\frac{2}{11}\right) = -1$$

$$\Longrightarrow \left(\frac{11}{349}\right) = (-1)(-1)(-1)(-1) = 1$$

الحد $\left(\frac{103}{349}\right)$ حسب الخاصة (٤):

$$\left(\frac{103}{349}\right)\left(\frac{349}{103}\right) = -1$$

$$\Longrightarrow \left(\frac{103}{349}\right) = -1\ \left(\frac{349}{103}\right)$$

حسب الخاصة (١):

$$349 \equiv \underbrace{40}_{\text{باقي قسمة 349 على 103}} \quad (mod\ 103)$$

$$\Longrightarrow \left(\frac{103}{349}\right) = -1\left(\frac{40}{103}\right)$$

وحسب الخاصة (٣):

$$\Longrightarrow \left(\frac{103}{349}\right) = -1\left(\frac{40}{103}\right) = -1\left(\frac{2}{103}\right)\left(\frac{2}{103}\right)\left(\frac{2}{103}\right)\left(\frac{5}{103}\right)$$

من أجل الحد $\left(\frac{2}{103}\right)$ حسب الخاصة (٥):

$$\Longrightarrow \left(\frac{2}{103}\right) = -1$$

ومن أجل الحد $\left(\frac{5}{103}\right)$ حسب الخاصة (٤):

$$\left(\frac{5}{103}\right)\left(\frac{103}{5}\right) = -1$$

$$\Longrightarrow \left(\frac{5}{103}\right) = -1\left(\frac{103}{5}\right)$$

حسب الخاصة (١):

$$103 \equiv 3\ (mod\ 5)$$

$$\Longrightarrow \left(\frac{5}{103}\right) = -1\left(\frac{3}{5}\right)$$

من أجل الحد $\left(\frac{3}{5}\right)$ حسب الخاصة (٤):

$$\left(\frac{3}{5}\right)\left(\frac{5}{3}\right) = 1 \Longrightarrow \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right)$$

$$\Longrightarrow \left(\frac{5}{103}\right) = -1\left(\frac{5}{3}\right)$$

حسب الخاصة (١):

$$5 \equiv 2 \ (mod\ 3)$$
$$\Longrightarrow \left(\frac{5}{103}\right) = -1\left(\frac{2}{3}\right)$$

وبالتالي حسب الخاصة (٥):

$$\Longrightarrow \left(\frac{5}{103}\right) = -1\left(\frac{2}{3}\right) = 1$$
$$\Longrightarrow \left(\frac{103}{349}\right) = -1\left(\frac{2}{103}\right)\left(\frac{2}{103}\right)\left(\frac{2}{103}\right)\left(\frac{5}{103}\right)$$
$$= (-1)(-1)(-1)(-1)(1) = 1$$
$$\Longrightarrow \left(\frac{84975}{349}\right) = \underbrace{\left(\frac{3}{349}\right)}_{-1}\underbrace{\left(\frac{5^2}{349}\right)}_{1}\underbrace{\left(\frac{11}{349}\right)}_{1}\underbrace{\left(\frac{103}{349}\right)}_{1} = -1$$

أي ليس للمعادلة حل.

القسم الثاني:

$$2016x \equiv 3 \ (mod\ 11) \ldots\ldots (1)'$$
$$5x + 2016 \equiv 2 \ (mod\ 3) \ldots\ldots (2)'$$
$$2x \equiv 2016 \ (mod\ 50) \ \ldots\ldots\ldots (3)'$$

المعادلة الأولى:

$$x \equiv 3\ [2016]^{-1} \ (mod\ 11)$$

إيجاد مقلوب 2016 بما أن $\gcd(2016, 11) = 1$

فإن: $2016 = (183)(11) + 3$

$$11 = (3)(3) + 2$$
$$3 = (1)(2) + 1$$
$$\Rightarrow 1 = 4(2016) - 733(11)$$
$$\Longrightarrow [2016]^{-1} = [4]$$
$$\Longrightarrow x \equiv 12 \ (mod\ 11)$$

لكن $12 \notin \frac{Z}{(11)Z}$

$$\Longrightarrow [12] - [11] = [1]$$

$$\Longrightarrow x \equiv 1\ (mod\ 11) \dots (1)$$

المعادلة الثانية:

$$5x + 2016 \equiv 2\ (mod\ 3)$$

$$\Longrightarrow 5x \equiv -2014\ (mod\ 3)$$

$$\Longrightarrow x \equiv -2014[5]^{-1}\ (mod\ 3)$$

إيجاد مقلوب 5 بما أن $\gcd(3\ ,5) = 1$

$$5 = 1(3) + 2$$

$$3 = 1(2) + 1$$

$$\Rightarrow 1 = 2(3) - 1(5)$$

$$\Longrightarrow [5]^{-1} = [-1]$$

$$\Longrightarrow x \equiv 2014\ (mod\ 3)$$

لكن $2014 \notin \frac{Z}{(3)Z}$

وعليه فإن باقي قسمة 2014 على 3 هو 1.

$$\Longrightarrow x \equiv 1\ (mod\ 3) \dots . (2)$$

المعادلة الثالثة:

$$2x \equiv 2016\ (mod\ 50)$$

$$\Longrightarrow x \equiv 1008\ (mod\ 25)$$

لكن $1008 \notin \frac{Z}{(25)Z}$

وعليه فإن باقي قسمة 1008 على 25 هو 8.

$$\Longrightarrow x \equiv 8\ (mod\ 25) \dots . (3)$$

نلاحظ أن: $\gcd(11,3)=1$ وَ $\gcd(11,25)=1$ وَ $\gcd(3,25)=1$

فإن لجملة المعادلات حل وحيد في $\frac{Z}{(825)Z}=\frac{Z}{(11\times3\times25)Z}$

نحل المعادلة (١) مع (٢):

$$x\equiv \underbrace{1}_{a}\ (mod\ \overbrace{11}^{m})\ \text{ وَ }\ x\equiv \underbrace{1}_{b}\ (mod\ \overbrace{3}^{n})$$

$$\gcd(11,3)=1$$

$$\Rightarrow 1=\underbrace{-1}_{y}\overbrace{(11)}^{m}\underbrace{+4}_{z}\overbrace{(3)}^{n}$$

فالحل هو: $x=b\cdot y\cdot m+a\cdot z\cdot n$

$$\Rightarrow [x]=1\in\frac{Z}{(33)Z}$$

$$\Longrightarrow x\equiv 1\ (mod\ 33)\ldots.(*)$$

نحل المعادلة (٣) مع (*):

$$x\equiv \overbrace{8}^{a}\ (mod\ \underbrace{25}_{m})\ \text{ وَ }\ x\equiv \underbrace{1}_{b}\ (mod\ \overbrace{33}^{n})$$

$$\gcd(25,33)=1$$

$$\Rightarrow 1=\underbrace{4}_{y}\overbrace{(25)}^{m}\underbrace{-3}_{z}\overbrace{(33)}^{n}$$

فالحل هو: $x=b\cdot y\cdot m+a\cdot z\cdot n$

$$\Rightarrow [x]=-692$$

الصف المكافئ الموجب له هو $[825]+[-692]=[133]$

$$\Rightarrow [x]=133\in\frac{Z}{(825)Z}$$

القسم الثالث:

تم حذفه من قبل الدكتورة لأننا لم نأخذ فكرة عنه ضمن المنهاج.

السؤال الثالث:

القسم الأول:

لتكن $g = \gcd(a^m - 1\,, a^n - 1)$

ولتكن $(*) \ldots d = \gcd(m\,, n)$

وعليه فإن: $a^{\gcd(m\,,n)} - 1 = a^d - 1$

هدفنا إثبات أن g يقسم $a^d - 1$ و $a^d - 1$ يقسم g وعليه يكون $g = a^d - 1$

من $(*)$ وتعريف القاسم المشترك الأكبر فإن: $d\backslash n$ وَ $d\backslash m$

بما أن:

$$a^{\gcd(m\,,n)} \equiv 1 \left(mod\ a^{\gcd(m\,,n)} - 1\right)$$

أي أن:

$$a^d \equiv 1\ (mod\ a^d - 1)$$

عندها:

$$a^m - 1 = (a^d)^{d\backslash m} - 1$$
$$\Longrightarrow a^{m\ddot{}} - 1 = (1)^{d\backslash m} - 1 \equiv 0\ (mod\ddot{} a^d - 1)$$

وعليه فإن $a^d - 1$ يقسم $a^m - 1$

كما أن:

$$a^n - 1 = (a^d)^{d\backslash n} - 1$$
$$\Longrightarrow a^{n\ddot{}} - 1 = (1)^{d\backslash n} - 1 \equiv 0\ (mod\ddot{} a^d - 1)$$

وعليه فإن $a^d - 1$ يقسم $a^n - 1$

وبالتالي فإن $a^d - 1$ يقسم $g = \gcd(a^m - 1\,, a^n - 1) \ldots\ldots (١)$

من جهة أخرى:

$g = \gcd(a^m - 1\,, a^n - 1)$ فحسب تعريف القاسم المشترك الأكبر فإن:

g يقسم $a^m - 1 \iff a^m - 1 \equiv 0\ (mod\ g) \iff a^m \equiv 1\ (mod\ g)$

وأيضاً g يقسم $a^n - 1 \iff a^n - 1 \equiv 0\ (mod\ g) \iff a^n \equiv 1\ (mod\ g)$

وبما أن: $d = \gcd(m\,, n)$

أيضاً حسب تعريف القاسم المشترك الأكبر فإن:

$$\exists\ s\,, t : d = m \cdot s + n \cdot t$$

$$\Longrightarrow a^d - 1 = a^{(m \cdot s + n \cdot t)} - 1 = (1)^s (1)^t - 1 \equiv 0\ (mod\ g)$$

وذلك لكون $a^d - 1$ يقسم g.

أي أن g يقسم $a^d - 1 \ldots$(٢)

من العلاقة (١) و(٢) فإن: $g = a^d - 1$

أي أن: $\gcd(a^m - 1\,, a^n - 1) = a^{\gcd(m\,,n)} - 1$

القسم الثاني:

ليكن $\underbrace{111 \ldots 111}_{\text{مرة } n}$ يقبل القسمة على 91 ولنفرض جدلاً n لا تقبل القسمة على 6

أي أن:

$$n = 6k + r\,, \qquad r \in \{0\,, 1\,, 2, 3\,, 4\,, 5\}$$

$$\underbrace{111 \ldots 111}_{\text{مرة } n} = \underbrace{111 \ldots 111}_{\text{مرة } 6k}\ \underbrace{0000..0}_{\text{مرة } r} + \underbrace{111 \ldots 1}_{\text{مرة } r}$$

$$\underbrace{111 \ldots 111}_{\text{مرة } 6k} = \underbrace{111111}_{\text{مرة } 6} \times \underbrace{1\ \underbrace{00000}_{\text{مرة } 5}\ 1000001 \ldots..100000\ 1}_{\text{مرة } k-1}$$

نلاحظ 111111 يقبل القسمة على 91 حيث: $111111 = 91 \times 1221$

وبالتالي $\underbrace{111\ldots111}_{6k\text{ مرة}}$ يقبل القسمة على 91 وفرضنا $\underbrace{111\ldots111}_{n\text{ مرة}}$ يقبل القسمة على 91

وعليه فإن $\underbrace{1\ldots111}_{r\text{ مرة}}$ يقبل القسمة على 91 لكن في حال $r \in \{1,2,3,4,5\}$

لا يتحقق أن $\underbrace{1\ldots111}_{r\text{ مرة}}$ يقبل القسمة على 91 فالفرض الجدلي خاطئ ومنه $r = 0$ وبالتالي

$\underbrace{111\ldots111}_{n\text{ مرة}}$ يقبل القسمة على 91 إذا كان n يقبل القسمة على 6.

العكس: n تقبل القسمة على 6

$$\Longrightarrow n = 6k$$

$$\underbrace{111\ldots111}_{n=6k\text{ مرة}} = \underbrace{111111}_{\substack{6\text{ مرة}\\ \text{يقبل القسمة على 91}}} \times \underbrace{1\,\underbrace{00000}_{5\text{ مرة}}\,1000001\ldots\ldots100000\,1}_{k-1\text{ مرة}}$$

و بالتالي: $\underbrace{111\ldots111}_{n\text{ مرة}}$ يقبل القسمة على 91.

انتهى الحل....

ريم الرحبي...

مع تمنياتي لكم بالنجاح