ABCDEFGHIJKLMNOPQSTUVWXYZ

كلية العلوم

القسم : الرياضيات

السنة : الرابعة

اسئلة دوراات محلولة

نظرية الأعداد

A 2 Z LIBRARY

Facebook Group : A to Z مكتبة

كلية العلوم (فيزياء ، كيمياء ، رياضيات ،علم الحياة)

بمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app) على الرقم TEL: 0931497960

ABCDEFGHIJKLMNOPQSTUVWXYZ

جامعة طرطوس | امتحان مقرر نظرية الأعداد | اسم الطالب:

كلية العلوم | سنة رابعة رياضيات | المدة: ساعتان

قسم الرياضيات | الدورة الفصلية الأولى – العام الدراسي 2024–2025م | الدرجة: تسعون

السؤال الأول: (50 درجة)

1) أثبت صحّة قضيّتين **فقط** من القضايا التالية:

1. إذا كان $n > 1$ عدداً صحيحاً و $a \in \mathbb{Z}$ بحيث $gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
2. إذا كان m عدداً صحيحاً موجباً و $(m-1)! \equiv -1(mod\ m)$ فإنّ m عدد أولي.
3. يوجد عدد غير منتهٍ من الأعداد الأولية (إثبات اقليدس).

2) أنجز ما يلي:

1. إذا كان n عدداً صحيحاً فردياً لا يقبل القسمة على العدد 3 فأثبت أنّ $n^2 \equiv 1(mod\ 24)$.
2. أثبت أنّ $2 \times (34!) \equiv 36(mod\ 37)$.
3. أوجد باقي قسمة العدد

$$x = \left(\sum_{k=0}^{48}(k+2)!\right)^2$$

على العدد $m = 10$.

3) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $1000x + 72y = 32$.

السؤال الثاني: (40 درجة)

1) ليكن $m = 11$ عندئذٍ:

1. أوجد جذر أساسي بالنسبة للمقاس m بالاعتماد على اختبار لوكاس.
2. أوجد المعكوس الضربي للعدد 5 بالنسبة للمقاس m، ثم أوجد $O_m(5)$.
3. أوجد جميع الأعداد الصحيحة الموجبة a الأقل من $2m$ التي تحقق العلاقة $O_{2m}(a) = 2$.
4. أوجد جدول الأدلة من أجل الجذر الأساسي $g = 2$ للمقاس m، ثم أوجد الحلول المختلفة للتطابق $x^8 \equiv 9\ (mod\ m)$ باستخدام نظرية الأدلة.

2) ليكن $F_n = 2^{2^n} + 1$ حيث n عدد صحيح موجب تماماً والمطلوب أثبت أنّ

$$3^{\frac{F_n - 1}{2}} \equiv -1(mod\ F_n)$$

إذا كان F_n عدداً أوليّاً و كان 3 جذر أساسي بالنسبة للمقاس F_n.

انتهت الأسئلة

تمنياتي بالتوفيق والنجاح

مدرس المقرر: د. أحمد عيسى

A to Z

جامعة طرطوس كلية العلوم قسم الرياضيات

سلم تصحيح امتحان مقرر نظرية الأعداد لطلاب السنة الرابعة رياضيات

الدورة الفصلية الأولى – العام الدراسي 2024–2025م

الدرجة: تسعون

السؤال الأول: (50 درجة)

1) (20 درجة). أثبت صحّة قضيتين **فقط** من القضايا التالية. **(10 درجات لكل قضية يتم اختيارها).**

1. إذا كان $n > 1$ عدداً صحيحاً و $a \in \mathbb{Z}$ بحيث $gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
2. إذا كان m عدداً صحيحاً موجباً و $(m-1)! \equiv -1(mod\ m)$ فإنّ m عدد أولي.
3. يوجد عدد غير منتهٍ من الأعداد الأولية (إثبات اقليدس).

الحلّ:

1. لنأخذ R نظام البواقي المختزل الطبيعي قياس n:

$$R = \mathbb{Z}_n^* = \{t_1, t_2, \dots, t_{\phi(n)}\}; |R| = \phi(n) \ \& \ \gcd(t_i, n) = 1 \ \forall\, 1 \le i \le \phi(n)$$

وهي عبارة عن الأعداد الصحيحة الموجبة الأصغر من n و أولية مع العدد n.

- لدينا R نظام البواقي المختزل الطبيعي قياس n و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ عندئذ

$$aR = a\mathbb{Z}_n^* = \{at_1, at_2, \dots, at_{\phi(n)}\}; |aR| = \phi(n)$$

نظام بواقي مختزل قياس n.

- بما أنّ aR نظام بواقي مختزل قياس n عندئذٍ كل عنصر من aR يطابق عنصر واحد فقط من R عندئذ

$$at_1 at_2 \dots at_{\phi(n)} \equiv t_1 t_2 \dots t_{\phi(n)} (mod\ n)$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} t_i \equiv \prod_{i=1}^{\phi(n)} t_i \ (mod\ n)$$

وبما أنّ $\gcd(t_i, n) = 1$ أياً كان $1 \le i \le \phi(n)$ عندئذ

$$\gcd\left(\prod_{i=1}^{\phi(n)} t_i, n\right) = 1$$

بالتالي

$$a^{\phi(n)} \equiv 1(mod\ n)$$

2. نفرض جدلاً بأن m ليس بعدد أولي عندئذ يوجد عدد أولي p بحيث $p \mid m$ حيث $2 \le p \le m-1$

$$(m-1)! = (m-1) \times (m-2) \times \dots\dots \times 3 \times 2 \times 1$$

A to Z

بالتالي $p \mid (m-1)!$

$$(m-1)! \equiv -1 (mod\ m) \Rightarrow m \mid ((m-1)! + 1)$$

وبما أن $p \mid m$ عندئذ $p \mid ((m-1)! + 1)$ وبما أن $p \mid (m-1)!$ عندئذ $p \mid 1$ وهذا مرفوض، بالتالي m عدد أولي.

3. لتكن S مجموعة كلّ الأعداد الأولية ولنفرض جدلاً أن S تحوي عدد منتهٍ من الأعداد الأولية.

$$|S| = n\,; n \in \mathbb{Z}^+$$

$$S = \{p_1, p_2, p_3, \dots . p_n\};\ p_1 < p_2 < \dots < p_n$$

ولنأخذ $N = p_1 p_2 \dots p_n + 1$

نلاحظ بأنّ $N \notin S$ و $N > 1$ وبالتالي N عدد مؤلف وبالتالي N يملك عامل أولي p حيث $p \mid N$ بالتالي $p \in S$ عندئذ يوجد $n \geq i \geq 1$ بحيث $p = p_i$ عندئذ

أصبح لدينا

$$p \mid N \quad و \quad p \mid p_1 p_2 \dots p_n$$

بالتالي $p \mid (N - p_1 p_2 \dots p_n)$ عندئذ $p \mid 1$ وهذا مرفوض، بالتالي الفرض الجدلي خاطئ بالتالي S مجموعة غير منتهية.

2) (18 درجة). 6 درجات لكل تمرين يتم اختياره.

أنجز ما يلي:

1. إذا كان n عدداً صحيحاً فردياً لا يقبل القسمة على العدد 3 فأثبت أنّ: $n^2 \equiv 1 (mod\ 24)$.
2. أثبت أنّ $2 \times (34!) \equiv 36 (mod\ 37)$.
3. أوجد باقي قسمة العدد

$$x = \left(\sum_{k=0}^{48} (k+2)!\right)^2$$

على العدد $m = 10$.

الحلّ:

1. بما أن n عدد فردي عندئذ $n^2 \equiv 1 (mod\ 8) \dots . (1)$

بما أنّ n عدد لا يقبل القسمة على العدد 3 عندئذ $gcd(3, n) = 1$ بالتالي حسب أولر

$$n^{\phi(3)} \equiv 1 (mod\ 3) \Rightarrow n^2 \equiv 1 (mod\ 3) \dots . . (2)$$

بالتالي من (1) و (2) وكون $\gcd(3, 8) = 1$ عندئذ

$$n^2 \equiv 1 (mod\ 3 \times 8)$$

$$n^2 \equiv 1 (mod\ 24)$$

2. لدينا 37 عدد أولي بالتالي حسب ويلسون نجد: $(37-1)! \equiv -1 (mod\ 37)$ بالتالي

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

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

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

$$\Rightarrow 2 \times 34! \equiv 36 (mod\ 37)$$

3. نضع

A to Z

$$y = \sum_{k=0}^{48} (k+2)! = 2! + 3! + 4! + 5! + 6! + 7! + \cdots + 50!$$

$$x = y^2$$ بالتالي

نلاحظ $n! \equiv 0(mod\ 10)$ أيا كان n عدد صحيح يحقق $n \geq 5$.

$$y \equiv 2! + 3! + 4!\ (mod\ 10)$$
$$y \equiv 2(mod\ 10)$$
$$y^2 \equiv 4(mod\ 10)$$
$$x \equiv 4(mod\ 10)$$

بالتالي باقي القسمة هو العدد 4

3) **(12 درجه)**. أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $1000x + 72y = 32$.

الحل: $1000x + 72y = 32$

لدينا $a = 1000, b = 72, c = 32$ ولنوجد $\gcd(a,b)$ باستخدام طريقة إقليدس

$$1000 = 13 \times 72 + 64$$

$$72 = 1 \times 64 + \mathbf{8}$$

$$64 = 8 \times 8 + 0$$

نلاحظ بأن $d = \gcd(a,b) = 8$ و $d \mid c$ فالمعادلة الديوفانتية قابلة للحل وتملك عدد لانهائي من الحلول، لنوجد حل لها.

$$8 = 72 - 64$$
$$8 = 72 - (1000 - 13 \times 72)$$
$$8 = 1000(-1) + 72(14)$$

نضرب الطرفين بـ $\frac{c}{d} = 4$ نجد: $1000(-4) + 72(56) = 32$

بالتالي $(x_0, y_0) = (-4, 56)$ حل للمعادلة الديوفانتية $1000x + 72y = 32$

أما الصيغة التي نستنتج منها جميع الحلول الصحيحة للمعادلة الديوفانتية:

$$\begin{cases} x = x_0 + \frac{b}{d}t = -4 + 9t \\ y = y_0 - \frac{a}{d}t = 56 - 125t \end{cases} ; t \in \mathbb{Z}$$

السؤال الثاني: (40 درجة)

1) **(33 درجه)**. ليكن $m = 11$ عندئذٍ:

1. أوجد جذر أساسي بالنسبة للمقاس m بالاعتماد على اختبار لوكاس. **(8 درجات)**
2. أوجد المعكوس الضربي للعدد 5 بالنسبة للمقاس m، ثم أوجد $O_m(5)$. **(7 درجات)**
3. أوجد جميع الأعداد الصحيحة الموجبة a الأقل من $2m$ التي تحقق العلاقة: $O_{2m}(a) = 2$. **(6 درجات)**
4. أوجد جدول الأدلة m من أجل الجذر الأساسي $g = 2$ للمقاس m، ثم أوجد الحلول المختلفة للتطابق $x^8 \equiv 9\ (mod\ m)$ باستخدام نظرية الأدلة. **(12 درجه)**

A to Z

الحل:

1. **إيجاد جذر أساسي بالنسبة للمقاس 11 (8 درجات)**

$a \in \mathbb{Z}_{11}^{*} = \{1,2,3,4,5,6,7,8,9,10\}$ جذر أساسي بالنسبة للمقاس $p = 11$ إذا تحقق الشرط التالي

$$a^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 10$.

نلاحظ بأنّ $q = 2$ أو 5

- الشرط لا يتحقق من أجل $a = 1$.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{10}{q}}: \begin{cases} 2^5 \not\equiv 1(mod\ 11) \\ 2^2 = 4 \not\equiv 1(mod\ 11) \end{cases}$$

بالتالي $a = 2$ جذر أساسي بالنسبة للمقاس 11 ولنرمزه بـ $g = 2$.

2.

- **(3 درجات)**.المعكوس الضربي للعدد 5 بالنسبة للمقاس m هو باقي قسمة $5^{\phi(m)-1} = 5^{\phi(11)-1} = 5^9$ على العدد m بالتالي المعكوس الضربي هو العدد 9.
- **(4 درجات)**.لنضع $O_{11}(5) = k$ عندئذٍ $k \mid \phi(11)$

بالتالي k أحد القواسم الموجبة للعدد 10.

$$(5)^1 \not\equiv 1(mod\ 11)$$

$$(5)^2 \not\equiv 1(mod\ 11)$$

$$(5)^5 \equiv 1(mod\ 11)$$

نلاحظ بأنّ $O_{11}(5) = 5$

3. **(6 درجات)**. لدينا 2 جذر أساسي بالنسبة للمقاس $m = 11$ وبما أن 2 عدد زوجي عندئذٍ $\acute{g} = 2 + 11 = 13$ جذر أساسي بالنسبة للمقاس $2m$، عندئذٍ أياً كان $a \in \mathbb{Z}$ بحيث $\gcd(a, 2m) = \gcd(a, 22) = 1$ فإنّ $a \equiv (13)^k (mod\ 22)$ حيث $1 \le k \le \phi(22)$

بالتالي $O_{2m}(a) = O_{2m}((13)^k)$

$$2 = \frac{O_{2m}(13)}{\gcd(k, O_{2m}(13))} = \frac{\phi(22)}{\gcd(k, \phi(22))} = \frac{10}{\gcd(k, 10)}$$

بالتالي $\gcd(k, 10) = 5$ عندئذٍ $k = 5$

$$(13)^5 \equiv 21(mod\ 22)$$

عندئذٍ الأعداد الصحيحة الموجبة a الأقل من $2m$ التي تحقق العلاقة $O_{2m}(a) = 2$ هي:{21}.

4. **(12 درجه)**. نحسب $2^k; 1 \le k \le \phi(11) = 10$ (2 جذر أساسي بالنسبة للمقاس 11).

A to Z

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

$x^8 \equiv 9\ (mod\ 11)$ نطبق نظرية الأدلة للطرفين نجد

$$8\ Indx \equiv Ind\ 9(mod\ \phi(11))$$
$$8\ Indx \equiv 6(mod\ 10)$$

هذا التطابق يملك حلين مختلفين هي $Indx \in \{2,7\}$ بالتالي

$$Indx = 2 \Longrightarrow x = 4$$
$$Indx = 7 \Longrightarrow x = 7$$

بالتالي حلول التطابق المعطى هي $\{4,7\}$

2) (**7 درجات**). ليكن $F_n = 2^{2^n} + 1$ حيث n عدد صحيح موجب تماماً والمطلوب:

أثبت أنّ $3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$ إذا كان F_n عدد أوليّ و كان 3 جذر أساسي بالنسبة للمقاس F_n.

الحلّ: لدينا 3 جذر أساسي بالنسبة للمقاس F_n عندئذ

$$O_{F_n}(3) = \phi(F_n) = F_n - 1$$

$$3^{F_n-1} \equiv 1(mod\ F_n) \Longrightarrow \left(3^{\frac{F_n-1}{2}}\right)^2 - 1 \equiv 0(mod\ F_n)$$

بالتالي $F_n \mid \left(3^{\frac{F_n-1}{2}} - 1\right)\left(3^{\frac{F_n-1}{2}} + 1\right)$

نلاحظ بأنّ $F_n \nmid \left(3^{\frac{F_n-1}{2}} - 1\right)$ لأنه لو كان $F_n \mid \left(3^{\frac{F_n-1}{2}} - 1\right)$ عندئذ $3^{\frac{F_n-1}{2}} \equiv 1(mod\ F_n)$

بالتالي $O_{F_n}(3) \mid \frac{F_n-1}{2}$ بالتالي $\frac{F_n-1}{2} \mid (F_n - 1)$ وهذا مرفوض.

بالتالي عندئذ $F_n \mid \left(3^{\frac{F_n-1}{2}} + 1\right)$

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

ملاحظة

✓ **بعض التمارين تحلّ بأكثر من طريقة، فأي طريقة متبعة من قبل الطالب لحلّ تمرين معين وهذه الطريقة صحيحة ينال الطالب العلامة المخصصة لهذا التمرين.**

مدرس المقرر: د. أحمد عيسى

جامعة طرطوس	امتحان مقرر نظرية الأعداد	اسم الطالب:
كلية العلوم	سنة رابعة رياضيات	المدة: ساعتان
قسم الرياضيات	الدورة الفصلية الثانية – العام الدراسي 2023–2024م	الدرجة: تسعون

السؤال الأول: (46 درجة)

1) أثبت صحّة قضية واحدة فقط من القضيتين التاليتين:

- إذا كان $n > 1$ عدداً صحيحاً و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
- يوجد عدد غير منتهٍ من الأعداد الأولية (إثبات اقليدس).

2) أنجز ما يلي:

1. أثبت أنّ $23 \mid (18! + 1)$.
2. أوجد باقي قسمة العدد

$$x = \left(\sum_{k=0}^{48} k!\right)^2$$

على العدد $m = 6$.

3. أوجد الحلول المختلفة للتطابق الخطي $9x \equiv 21(mod\ 30)$.

3) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $56x + 72y = 40$.

السؤال الثاني: (44 درجة)

1) ليكن $m = 19$ والمطلوب:

1. أوجد جذر أساسي بالنسبة للمقاس m بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس $2m$.
2. أوجد عدد الجذور الأساسية بالنسبه للمقاس m.
3. أوجد جدول الأدلة بالنسبة للمقاس m علماً أنّ $g = 3$ جذر أساسي بالنسبة للمقاس m، ثم أوجد حلول التطابق $x^{14} \equiv 9\ (mod\ m)$ باستخدام نظرية الأدلة.
4. أوجد $O_m(81)$.
5. أوجد الحلين المختلفين للتطابق $x^2 + x + 8 \equiv 0(mod\ m)$.

2) ليكن p, q عددين أوليين مختلفين والمطلوب أثبت أنّ

$$p^{q-1} + q^{p-1} \equiv 1(mod\ pq)$$

---انتهت الأسئلة---

تمنياتي بالتوفيق والنجاح

مدرس المقرر: د. أحمد عيسى

مكتبة A to Z

جامعة طرطوس كلية العلوم قسم الرياضيات

سلم تصحيح امتحان مقرر نظرية الأعداد لطلاب السنة الرابعة رياضيات

الدورة الفصلية الثانية – العام الدراسي 2023-2024م

الدرجة: تسعون

السؤال الأول: (46 درجة)

1) أثبت صحّة **قضيه** واحدة فقط من القضيتين التاليتين: **(10 درجات)**

1. إذا كان $n > 1$ عدداً صحيحاً و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
2. يوجد عدد غير منتهٍ من الأعداد الأولية (إثبات اقليدس).

الحلّ:

1.

- لنأخذ R نظام البواقي المختزل **الطبيعي** قياس n:

$$R = \mathbb{Z}_n^* = \{t_1, t_2, \dots, t_{\phi(n)}\}; |R| = \phi(n) \ \&\ \gcd(t_i, n) = 1 \ \forall\ 1 \le i \le \phi(n)$$

وهي عبارة عن الأعداد الصحيحة الموجبة الأصغر من n و أولية مع العدد n.

- لدينا R نظام البواقي المختزل الطبيعي قياس n و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ عندئذ

$$aR = a\mathbb{Z}_n^* = \{at_1, at_2, \dots, at_{\phi(n)}\}; |aR| = \phi(n)$$

نظام بواقي مختزل قياس n.

- بما أنّ aR نظام بواقي مختزل قياس n عندئذٍ كل عنصر من aR يطابق عنصر واحد فقط من R عندئذ

$$at_1 at_2 \dots at_{\phi(n)} \equiv t_1 t_2 \dots t_{\phi(n)} (mod\ n)$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} t_i \equiv \prod_{i=1}^{\phi(n)} t_i\ (mod\ n)$$

وبما أنّ $\gcd(t_i, n) = 1$ أياً كان $1 \le i \le \phi(n)$ عندئذ $\gcd\left(\prod_{i=1}^{\phi(n)} t_i, n\right) = 1$ بالتالي

$$a^{\phi(n)} \equiv 1(mod\ n)$$

2. لتكن S مجموعة كلّ الأعداد الأولية ولنفرض جدلاً أن S تحوي عدد منتهٍ من الأعداد الأولية.

$$|S| = n\,; n \in \mathbb{Z}^+$$

$$S = \{p_1, p_2, p_3, \dots . p_n\};\ p_1 < p_2 < \dots < p_n$$

ولنأخذ $N = p_1 p_2 \dots p_n + 1$

نلاحظ بأنّ $N \notin S$ و $N > 1$ وبالتالي N عدد مؤلف وبالتالي N يملك عامل أولي p حيث $p \mid N$ بالتالي $p \in S$ عندئذ يوجد $n \geq i \geq 1$ بحيث $p = p_i$ عندئذ أصبح لدينا

$$p \mid N \quad \text{و} \quad p \mid p_1 p_2 \dots p_n$$

بالتالي $p \mid (N - p_1 p_2 \dots p_n)$ عندئذ $p \mid 1$ وهذا مرفوض، بالتالي الفرض الجدلي خاطئ بالتالي S مجموعة غير منتهية.

2) أنجز ما يلي: (24 درجه). 8 درجات لكل تمرين

1. أثبت أنّ $23 \mid (18! + 1)$.
2. أوجد باقي قسمة العدد

$$x = \left(\sum_{k=0}^{48} k!\right)^2$$

على العدد $m = 6$.

3. أوجد الحلول المختلفة للتطابق الخطي $9x \equiv 21(mod\ 30)$.

الحلّ:

1. لدينا 23 عدد أولي بالتالي حسب ويلسون نجد: $(23-1)! \equiv -1(mod\ 23)$ بالتالي

$$(22)! \equiv -1(mod\ 23) \Rightarrow 22 \times 21 \times 20 \times 19 \times 18! \equiv -1(mod\ 23)$$
$$\Rightarrow (-1) \times (-2) \times (-3) \times (-4) \times 18! \equiv -1(mod\ 23)$$
$$\Rightarrow (24) \times 18! \equiv -1(mod\ 23)$$
$$\Rightarrow 18! \equiv -1(mod\ 23)$$
$$\Rightarrow 18! + 1 \equiv 0(mod\ 23) \Rightarrow 23 \mid (18! + 1)$$

2. نضع

$$y = \sum_{k=0}^{48} k! = 0! + 1! + 2! + 3! + 4! + 5! + 6! + 7! + \cdots + 48!$$

بالتالي $x = y^2$

نلاحظ $n! \equiv 0(mod\ 6)$ أيا كان n عدد صحيح يحقق $n \geq 3$.

$$y \equiv 1 + 1 + 2! + 3! + 4! + 5! + 6! + 7! + \cdots + 48!\ (mod\ 6)$$
$$y \equiv 4(mod\ 6)$$
$$y^2 \equiv 16(mod\ 6)$$
$$x \equiv 4(mod\ 6)$$

بالتالي باقي القسمة هو العدد 4

3. $9x \equiv 21(mod\ 30)$

لدينا $a = 9, b = 21, m = 30$ و $d = \gcd(a, m) = 3$. عندئذ التطابق المعطى قابل للحلّ ويملك ثلاث حلول مختلفة بالنسبة للمقاس m

لنوجد حلّ للتطابق $9x \equiv 21(mod\ 30)$

$$9x \equiv 21(mod\ 30)$$
$$3x \equiv 7(mod\ 10)$$
$$9x \equiv 21(mod\ 10)$$

مكتبة A to Z

$$x \equiv 9(mod\ 10); m_1 = \frac{m}{d} = 10$$

بالتالي $x_0 = 9$ بالتالي حلول التطابق المعطى هي $\{9, 19, 29\}$

3) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $56x + 72y = 40$. **(12 درجة)**

الحلّ: $56x + 72y = 40$

لدينا $a = 56, b = 72, c = 40$ ولنوجد $\gcd(a, b)$ باستخدام طريقة إقليدس

$$72 = 1 \times 56 + 16$$
$$56 = 3 \times 16 + \mathbf{8}$$
$$16 = 2 \times 8 + 0$$

نلاحظ بأن $d = \gcd(a, b) = 8$ و $d \mid c$ فالمعادلة الديوفانتية قابلة للحلّ وتملك عدد لانهائي من الحلول. لنوجد حل لها.

$$8 = 56 - 3 \times 16$$
$$8 = 56 - 3 \times (72 - 56)$$
$$8 = 56(4) + 72(-3)$$

نضرب الطرفين بـ $\frac{c}{d} = 5$ نجد: $56(20) + 72(-15) = 40$

بالتالي $(x_0, y_0) = (20, -15)$ حل للمعادلة الديوفانتية $56x + 72y = 40$

أما الصيغة التي نستنتج منها جميع الحلول الصحيحة للمعادلة الديوفانتية:

$$\begin{cases} x = x_0 + \frac{b}{d}t = 20 + 9t \\ y = y_0 - \frac{a}{d}t = -15 - 7t \end{cases} ; t \in \mathbb{Z}$$

مكتبة A to Z

السؤال الثاني: (44 درجة)

1) **(38 درجة)**. ليكن $m = 19$ والمطلوب:

1. أوجد جذر أساسي بالنسبة للمقاس m بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس $2m$.
2. أوجد عدد الجذور الأساسية بالنسبة للمقاس m.
3. أوجد جدول الأدلة بالنسبة للمقاس m علماً أنّ $g = 3$ جذر أساسي بالنسبة للمقاس m، ثم أوجد حلول التطابق $x^{14} \equiv 9\ (mod\ m)$ باستخدام نظرية الأدلة.
4. أوجد $O_m(81)$.
5. أوجد الحلين المختلفين للتطابق $x^2 + x + 8 \equiv 0(mod\ m)$.

الحلّ:

1. **<u>إيجاد جذر أساسي بالنسبة للمقاس 19</u>(7 درجات)**

$a \in \mathbb{Z}_{19}^* = \{1,2,3,4,5,6,7,8,9,10,11, \dots, 18\}$ جذر أساسي بالنسبة للمقاس $p = 19$ إذا تحقق الشرط التالي

$$a^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 18$.

نلاحظ بأنّ $q = 2$ أو 3

- الشرط لا يتحقق من أجل $a = 1$.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{18}{q}}: \begin{cases} 2^{\frac{18}{2}} = 2^9 \not\equiv 1(mod\ 19) \\ 2^{\frac{18}{3}} = 2^6 \not\equiv 1(mod\ 19) \end{cases}$$

بالتالي $a = 2$ جذر أساسي بالنسبة للمقاس 19 ولنرمزه بـ $g = 2$.

<u>إيجاد جذر أساسي بالنسبة للمقاس $2m = 38 = 2 \times 19$</u> (3 درجات).

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس $p = 19$ وبما أنّ g زوجي عندئذ $g + p = 21$ جذر أساسي بالنسبة للمقاس m.

2. **(3 درجات).**

عدد الجذور هو: $\phi(\phi(m)) = \phi(\phi(19)) = \phi(18) = \phi(2) \times \phi(9) = \phi(3^2) = 3^{2-1}(3-1) = 6$

3. **(16 درجات).** نحسب $3^k; 1 \le k \le \phi(19) = 18$ (3 جذر أساسي بالنسبة للمقاس 19).

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

N: هو باقي قسمة 3^k على العدد 19. $IndN$: دليل العدد N

نطبق نظرية الأدلة للطرفين نجد $x^{14} \equiv 9\ (mod\ 19)$

$$14\ Indx \equiv Ind\ 9(mod\ \phi(19))$$
$$14\ Indx \equiv 2(mod\ 18)$$

هذا التطابق يملك حلين مختلفين هي $Indx \in \{4,13\}$ بالتالي

$$Indx = 4 \Longrightarrow x = 5$$
$$Indx = 13 \Longrightarrow x = 14$$

بالتالي حلول التطابق هي $\{5,14\}$

4. **(3 درجات).**

$$O_m(81) = O_{19}(3^4) = \frac{O_{19}(3)}{\gcd(4, O_{19}(3))} = \frac{\phi(19)}{\gcd(4, \phi(19))} = \frac{18}{\gcd(4,18)} = \frac{18}{2} = 9$$

5. **(6 درجات).**

لدينا $a = 1$ و $b = 1$ و $c = 8$ و $p = m = 19$

- نوجد $d = b^2 - 4ac = -31$
- نلاحظ بأن $d \equiv 7(mod\ p)$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$

$y^2 \equiv d(mod\ p)$ وهي $\{8,11\}$

✓ من أجل $y_0 = 8$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 19)$ فنجد

$$2x \equiv 7(mod\ 19) \Longrightarrow x \equiv 13(mod\ 19) \Longrightarrow x = 13$$

✓ من أجل $y_0 = 11$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 19)$ فنجد

$$2x \equiv -9(mod\ 19) \Longrightarrow x \equiv 5(mod\ 19) \Longrightarrow x = 5$$

بالتالي حلول التطابق هي $\{5, 13\}$

2) (6 درجات). ليكن p, q عددين أوليين مختلفين والمطلوب أثبت أنّ

$$p^{q-1} + q^{p-1} \equiv 1(mod\ pq)$$

الحلّ:

$$\gcd(p,q) = 1 \Longrightarrow p^{\phi(q)} \equiv 1\ (mod\ q) \Longrightarrow p^{q-1} \equiv 1\ (mod\ q)$$
$$p^{q-1} + q^{p-1} \equiv 1 + q^{p-1}(mod\ q)$$
$$p^{q-1} + q^{p-1} \equiv 1\ (mod\ q) \ldots\ldots (1)$$
$$\gcd(p,q) = 1 \Longrightarrow q^{\phi(p)} \equiv 1\ (mod\ p) \Longrightarrow q^{p-1} \equiv 1(mod\ p)$$
$$q^{p-1} + p^{q-1} \equiv 1 + p^{q-1}(mod\ p)$$
$$p^{q-1} + q^{p-1} \equiv 1\ (mod\ p) \ldots\ldots (2)$$

من (1) و (2) و كون $\gcd(p,q) = 1$ نجد

$$p^{q-1} + q^{p-1} \equiv 1(mod\ pq)$$

ملاحظة

✓ **بعض التمارين تحلّ بأكثر من طريقة، فأي طريقة متبعة من قبل الطالب لحلّ تمرين معين وهذه الطريقة صحيحة ينال الطالب العلامة المخصصة لهذا التمرين.**

مكتبة A to Z

مدرس المقرر: د. أحمد عيسى

جامعة طرطوس
كلية العلوم
قسم الرياضيات

امتحان مقرر نظرية الأعداد
سنة رابعة رياضيات
الدورة الفصلية الأولى – العام الدراسي 2023-2024م

اسم الطالب:
المدة: ساعتان
الدرجة: تسعون

السؤال الأول: (50 درجة)

1) أثبت صحة **قضيتين** فقط من القضايا الآتية:

1. يوجد عدد غير منتهٍ من الأعداد الأولية (إثبات اقليدس).
2. إذا كان p عدداً أولياً فردياً يُحقق $p \equiv 1(mod\ 4)$ فإنّ التطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ.
3. إذا كان m عدداً صحيحاً موجباً و $(m-1)! \equiv -1(mod\ m)$ فإنّ m عدد أولي.

2) أنجز **ثلاثة** فقط مما يأتي:

1. أثبت أنّ $37 \mid (31 \times (33!) + 1)$.
2. أوجد الحلين المختلفين للتطابق $x^2 - 4x - 1 \equiv 0(mod\ 11)$.
3. بيّن فيما إذا كان التطابق $x^6 \equiv 5(mod\ 17)$ قابل للحلّ أم لا باستخدام مبرهنة أولر المعممة.
4. أوجد باقي قسمة العدد

$$x = \left(\sum_{k=0}^{98}(k+2)!\right)^3$$

على العدد $m = 10$.

3) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $121x + 9y = 2$.

السؤال الثاني: (40 درجة)

1) ليكن $m = 26$ والمطلوب:

1. أوجد جذر أساسي بالنسبة للمقاس 13 بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس m، ثم استنتج جذر أساسي بالنسبة للمقاس $\frac{m^2}{4}$.
2. أوجد جميع الجذور الأساسية الأخرى بالنسبة للمقاس 13.
3. أوجد المعكوس الضربي للعدد 3 بالنسبة للمقاس m.
4. هل المجموعة $\{7^1, 7^2, 7^3, \ldots\ldots, 7^{12}\}$ نظام بواقي مختزل قياس 13 أم لا، ولماذا؟
5. أوجد الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة: $O_m(a) = 3$.
6. أوجد جدول الأدلة بالنسبة للمقاس 13 علماً أنّ $g = 6$ جذر أساسي بالنسبة للمقاس 13، ثم أوجد حلول التطابق $x^9 \equiv 5\ (mod\ 13)$ باستخدام نظرية الأدلة.

2) ليكن $F_n = 2^{2^n} + 1$ حيث n عدد صحيح موجب تماماً والمطلوب: أثبت أنّ $F_n \equiv 5(mod\ 12)$.

انتهت الأسئلة

طرطوس: الأحد 2024/1/21م

تمنياتي بالتوفيق والنجاح

مدرس المقرر: د. أحمد عيسى

جامعة طرطوس كلية العلوم قسم الرياضيات

سلم تصحيح امتحان مقرر نظرية الأعداد لطلاب السنة الرابعة رياضيات

الدورة الفصلية الأولى – العام الدراسي 2023–2024م

الدرجة: تسعون

مكتبة A to Z

السؤال الأول: (50 درجة)

1) أثبت صحّة قضيتين فقط من القضايا الآتية: 18 درجة (9 درجات لكلّ قضية)

1. يوجد عدد غير منتهٍ من الأعداد الأولية (إثبات اقليدس).
2. إذا كان p عدداً أولياً فردياً يُحقق $p \equiv 1(mod\ 4)$ فإنّ التطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ.
3. إذا كان m عدداً صحيحاً موجباً و $(m-1)! \equiv -1(mod\ m)$ فإنّ m عدد أولي.

الحلّ:

1. لتكن S مجموعة كلّ الأعداد الأولية ولنفرض جدلاً أن S تحوي عدد منتهٍ من الأعداد الأولية.

$$|S| = n\ ; \in \mathbb{Z}^+$$
$$S = \{p_1, p_2, p_3, \dots . p_n\};\ p_1 < p_2 < \dots < p_n$$

ولنأخذ $N = p_1 p_2 \dots p_n + 1$

نلاحظ بأنّ $N \notin S$ و $N > 1$ وبالتالي N عدد مؤلف وبالتالي N يملك عامل أولي p حيث $p \mid N$ بالتالي $p \in S$ عندئذ يوجد $n \geq i \geq 1$ بحيث $p = p_i$ عندئذ أصبح لدينا

$$p \mid p_1 p_2 \dots p_n \quad \text{و} \quad p \mid N$$

بالتالي $p \mid (N - p_1 p_2 \dots p_n)$ عندئذ $p \mid 1$ وهذا مرفوض، بالتالي الفرض الجدلي خاطئ بالتالي S مجموعة غير منتهية.

2. بما أن p عدد أولي عندئذ حسب ويلسون نجد $(p-1)! \equiv -1(mod\ p)$

بالتالي:

$$(p-1)! = 1 \times 2 \times \dots \times \frac{p-3}{2} \times \frac{p-1}{2} \times \frac{p+1}{2} \times \frac{p+3}{2} \times \dots \times (p-2) \times (p-1)$$

لدينا

$$(p-1) \equiv -1(mod\ p)$$
$$(p-2) \equiv -2(mod\ p)$$

وهكذا

$$\frac{p+3}{2} \equiv -\left(\frac{p-3}{2}\right)(mod\ p)$$

$$\frac{p+1}{2} \equiv -\left(\frac{p-1}{2}\right)(mod\ p)$$

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}}\left(1 \times 2 \times 3 \ldots \times \frac{p-3}{2} \times \frac{p-1}{2}\right)^2 (mod\ p)$$

لدينا $p \equiv 1(mod\ 4)$ عندئذ $\frac{p-1}{2}$ عدد زوجي عندئذ

$$\left(1 \times 2 \times 3 \ldots \times \frac{p-3}{2} \times \frac{p-1}{2}\right)^2 \equiv (p-1)!\,(mod\ p)$$

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1(mod\ p)$$

بالتالي $x_0 = \left(\frac{p-1}{2}\right)!$ هو حل للتطابق $x^2 \equiv -1(mod\ p)$ عندئذ التطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ.

3. نفرض جدلاً بأن m ليس بعدد أولي عندئذ يوجد عدد أولي p بحيث $p \mid m$ حيث $2 \leq p \leq m-1$

$$(m-1)! = (m-1) \times (m-2) \times \ldots\ldots \times 3 \times 2 \times 1$$

بالتالي $p \mid (m-1)!$

$$(m-1)! \equiv -1(mod\ m) \Rightarrow m \mid \left((m-1)! + 1\right)$$

وبما أن $p \mid m$ عندئذ $p \mid \left((m-1)! + 1\right)$ وبما أن $p \mid (m-1)!$ عندئذ $p \mid 1$ وهذا مرفوض، بالتالي m عدد أولي.

2) أنجز ثلاثة فقط مما يأتي: 21 درجة (7 درجات لكلّ تمرين يتم اختياره).

1. أثبت أنّ $37 \mid (31 \times (33!) + 1)$.
2. أوجد الحلين المختلفين للتطابق $x^2 - 4x - 1 \equiv 0(mod\ 11)$..
3. بيّن فيما إذا كان التطابق $x^6 \equiv 5(mod\ 17)$ قابل للحلّ أم لا باستخدام مبرهنة أولر المعممة.
4. أوجد باقي قسمة العدد

$$x = \left(\sum_{k=0}^{98}(k+2)!\right)^3$$

على العدد $m = 10$.

الحلّ:

1. لدينا 37 عدد أولي بالتالي حسب ويلسون نجد: $(37-1)! \equiv -1(mod\ 37)$ بالتالي

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

2. لدينا $a = 1$ و $b = -4$ و $c = -1$ و $p = 11$
   - نوجد $d = b^2 - 4ac = 20$
   - نوجد حلول التطابق $y^2 \equiv d(mod\ p)$ وهي $\{-3, 3\}$
     - ✓ من أجل $y_0 = 3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 11)$ فنجد

$$2x \equiv 7(mod\ 11) \Rightarrow 2x \equiv -4(mod\ 11) \Rightarrow x \equiv 9(mod\ 11) \Rightarrow x = 9$$

     - ✓ من أجل $y_0 = -3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 11)$ فنجد

A to Z مكتبة

$$2x \equiv 1(mod\ 11) \Longrightarrow x \equiv 6(mod\ 11) \Longrightarrow x = 6$$

بالتالي حلول التطابق هي $\{6, 9\}$

3. $x^6 \equiv 5(mod\ 17)$

التطابق $x^n \equiv a(mod\ m)$ قابل للحل إذا وفقط إذا كان $a^{\frac{\phi(m)}{d}} \equiv 1(mod\ m)$ حيث $d = \gcd(n, \phi(m))$ (مبرهنة أولر المعممة)

التطابق المعطى هو: $x^6 \equiv 5(mod\ 17)$

لدينا $n = 6, a = 5, m = 17$

$$\phi(m) = 16 \qquad d = \gcd(n, \phi(m)) = 2$$

نلاحظ بأنّ

$$a^{\frac{\phi(m)}{d}} = 5^8 \not\equiv 1(mod\ 17)$$

بالتالي التطابق غير قابل للحلّ.

4. نضع

$$y = \sum_{k=0}^{98} (k+2)! = 2! + 3! + 4! + 5! + 6! + 7! + \cdots + 100!$$

بالتالي $x = y^3$

نلاحظ $n! \equiv 0(mod\ 10)$ أيا كان n عدد صحيح يحقق $n \geq 5$.

بالتالي

$$y \equiv 2! + 3! + 4! + 5! + 6! + 7! + \cdots + 100!\ (mod\ 10)$$
$$y \equiv 2! + 3! + 4!\ (mod\ 10)$$
$$y \equiv 32(mod\ 10)$$
$$y \equiv 2(mod\ 10)$$
$$y^3 \equiv 8(mod\ 10)$$
$$x \equiv 8(mod\ 10)$$

بالتالي باقي القسمة هو العدد 8

3) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $121x + 9y = 2$. **(11 درجه)**

الحل: $121x + 9y = 2$

لدينا $a = 121, b = 9, c = 2$ ولنوجد $\gcd(a, b)$ باستخدام طريقة إقليدس

$$121 = 13 \times 9 + 4$$
$$9 = 2 \times 4 + 1$$
$$4 = 4 \times 1 + 0$$

نلاحظ بأن $d = \gcd(a, b) = 1$ و $d \mid c$ فالمعادلة الديوفانتية قابلة للحلّ وتملك عدد لانهائي من الحلول. لنوجد حل لها.

$$1 = 9 - 2 \times 4$$
$$1 = 9 - 2 \times (121 - 13 \times 9)$$
$$1 = 121(--2) + 9(27)$$

A to Z مكتبة

نضرب الطرفين بـ2 $\frac{c}{d} = 2$ نجد: $121(-4) + 9(54) = 2$

بالتالي $(x_0, y_0) = (-4, 54)$ حل للمعادلة الديوفانتية $121x + 9y = 2$

أما الصيغة التي نستنتج منها جميع الحلول الصحيحة للمعادلة الديوفانتية:

$$\begin{cases} x = x_0 + \frac{b}{d}t = -4 + 9t \\ y = y_0 - \frac{a}{d}t = 54 - 121t \end{cases} ; t \in \mathbb{Z}$$

السؤال الثاني: (40 درجة)

1) ليكن $m = 26$ والمطلوب:

1. أوجد جذر أساسي بالنسبة للمقاس 13 بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس m، ثم استنتج جذر أساسي بالنسبة للمقاس $\frac{m^2}{4}$.
2. أوجد جميع الجذور الأساسية الآخرى بالنسبة للمقاس 13.
3. أوجد المعكوس الضربي للعدد 3 بالنسبة للمقاس m.
4. هل المجموعة $\{7^1, 7^2, 7^3, \ldots\ldots, 7^{12}\}$ نظام بواقي مختزل قياس 13 أم لا، ولماذا؟
5. أوجد الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 3$.
6. أوجد جدول الأدلة بالنسبة للمقاس 13 علماً أنّ $g = 6$ جذر أساسي بالنسبة للمقاس 13، ثم أوجد حلول التطابق $x^9 \equiv 5 \pmod{13}$ باستخدام نظرية الأدلة.

مكتبة A to Z

الحلّ:

1. **إيجاد جذر أساسي بالنسبة للمقاس 13 (7 درجات)**

$a \in \mathbb{Z}_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$ جذر أساسي بالنسبة للمقاس $p = 13$ إذا تحقق الشرط التالي

$$a^{\frac{p-1}{q}} \not\equiv 1 (mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 12$.

نلاحظ بأنّ $q = 2$ أو 3

- الشرط لا يتحقق من أجل $a = 1$.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{12}{q}}: \begin{cases} 2^{\frac{12}{2}} = 2^6 \not\equiv 1 (mod\ 13) \\ 2^{\frac{12}{3}} = 2^4 \not\equiv 1 (mod\ 13) \end{cases}$$

بالتالي $a = 2$ جذر أساسي بالنسبة للمقاس 13 ولنرمزه بـ $g = 2$.

إيجاد جذر أساسي بالنسبة للمقاس $m = 26 = 2 \times 13$ (درجتان)

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس $p = 13$ وبما أنّ g زوجي عندئذ $g + p = 15$ جذر أساسي بالنسبة للمقاس m.

إيجاد جذر أساسي بالنسبة للمقاس $\frac{m^2}{4} = 169 = 13^2$ (درجتان)

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس $p = 13$

$$g^{p-1} = 2^{12} \not\equiv 1(mod\, p^2)$$

بالتالي $g = 2$ جذر أساسي بالنسبة للمقاس $\frac{m^2}{4} = p^2 = 169$

2. **إيجاد الجذور الآخرى بالنسبة للمقاس 13 .(4 درجات)**

نشكّل المجموعة التالية علماً أنّ 2 جذر أساسي بالنسبة للمقاس $p = 13$.

$$\{(2)^k; 1 \le k \le \phi(13)\ \&\ \gcd(k, \phi(13)) = 1\}$$

$$\{(2)^k; 1 \le k \le 12\ \&\ \gcd(k, 12) = 1)\} = \{(2)^1, (2)^5, (2)^7, (2)^{11}\}$$

وبما أنّ $(2)^1 \equiv 2(mod\ 13)$, $(2)^5 \equiv 6(mod\ 13)$, $(2)^7 \equiv 11(mod\ 13)$, $(2)^{11} \equiv 7(mod\ 13)$

بالتالي الجذور الأخرى بالنسبة للمقاس 13 هي $\{2, 6, 7, 11\}$.

3. **(درجتان)** المعكوس الضربي للعدد 3 بالنسبة للمقاس m هو باقي قسمة $3^{\phi(m)-1} = 3^{\phi(26)-1} = 3^{11}$ على العدد m

بالتالي المعكوس هو 9.

4. **(درجتان)** بما أنّ 7 جذر أساسي بالنسبة للمقاس $m = 13$ عندئذ المجموعة

$\{7^1, 7^2, 7^3, \ldots\ldots, 7^{\phi(13)}\} = \{7^1, 7^2, 7^3, \ldots\ldots, 7^{12}\}$ نظام بواقي مختزل قياس m.

5. **(5 درجات)** لدينا 15 جذر أساسي بالنسبة للمقاس $m = 26$ عندئذ أياً كان $a \in \mathbb{Z}$ بحيث $\gcd(a, 26) = 1$ فإنّ

$$a \equiv (15)^k(mod\ 26)$$ بالتالي $O_m(a) = O_m((15)^k)$

$$3 = \frac{O_m(15)}{\gcd(k, O_m(15))} = \frac{\phi(26)}{\gcd(k, \phi(26))} = \frac{12}{\gcd(k, 12)}$$

بالتالي $\gcd(k, 12) = 4$ عندئذٍ $k \in \{4, 8\}$

$$(15)^k \in \{(15)^4, (15)^8, \}$$

وبما أنّ $(15)^4 \equiv 3(mod\ 26)$, $(15)^8 \equiv 9(mod\ 26)$

عندئذٍ الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 3$ هي: $\{3, 9\}$.

6. **(10 درجات)**. نحسب $6^k; 1 \le k \le \phi(13) = 12$ (6 جذر أساسي بالنسبة للمقاس 13).

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

N: هو باقي قسمة 6^k على العدد 13.

N دليل العدد : $IndN$

نطبق نظرية الأدلة للطرفين نجد $x^9 \equiv 5\ (mod\ 13)$

$$9\ Indx \equiv Ind\ 5(mod\ \phi(13))$$

$$9\ Indx \equiv 9(mod\ 12)$$

هذا التطابق يملك ثلاث حلول مختلفة هي $Indx \in \{1,5,9\}$ بالتالي

$$Indx = 1 \Rightarrow x = 6$$

A to Z مكتبة

$$Indx = 5 \Longrightarrow x = 2$$
$$Indx = 9 \Longrightarrow x = 5$$

بالتالي حلول التطابق هي $\{2,5,6\}$

2) **(6 درجات)**. ليكن $F_n = 2^{2^n} + 1$ حيث n عدد صحيح موجب تماماً والمطلوب:

أثبت أنّ $F_n \equiv 5(mod\ 12)$.

الحل:

الطريقة الأولى:

يجب أن نثبت أنّ $F_n \equiv 5(mod\ 3)$ و $F_n \equiv 5(mod\ 4)$

- بما أنّ $2 \equiv -1(mod\ 3)$ بالتالي $F_n = 2^{2^n} + 1 \equiv (-1)^{2^n} + 1(mod\ 3)$

  بالتالي $F_n \equiv 2(mod\ 3)$ عندئذ $F_n \equiv 5(mod\ 3)$

- لدينا $F_n = 2^{2^n} + 1 = 2^{2^{n-1} \times 2^1} + 1 = \left(2^{2^1}\right)^{2^{n-1}} + 1 = (4)^{2^{n-1}} + 1 \equiv 1(mod\ 4)$

  بالتالي $F_n \equiv 5(mod\ 4)$

مما سبق نجد $F_n \equiv 5(mod\ 3)$ و $F_n \equiv 5(mod\ 4)$ و $gcd(3,4) = 1$ عندئذ

$$F_n \equiv 5(mod\ 12)$$

الطريقة الثانية : باستخدام طريقة الاستقراء الرياضي

----------**ملاحظة**----------

✓ **بعض التمارين تحلّ بأكثر من طريقة، فأي طريقة متبعة من قبل الطالب لحلّ تمرين معين وهذه الطريقة صحيحة ينال الطالب العلامة المخصصة لهذا التمرين.**

طرطوس: الأحد 2024/1/21م

مدرس المقرر: د. أحمد عيسى

A to Z مكتبة

جامعة طرطوس كلية العلوم قسم الرياضيات

سلم تصحيح امتحان مقرر نظرية الأعداد لطلاب السنة الرابعة رياضيات

الدورة التكميلية – العام الدراسي 2022–2023م

الدرجة: تسعون

السؤال الأول: (54 درجة)

1) أثبت صحّة **قضيتين** فقط من القضايا الآتية **(12 درجة لكلّ قضية) المجموع 24 درجة**

1. إذا كان $n > 1$ عدداً صحيحاً و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
2. إذا كان p عدداً أوليّاً فردياً والتطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ فإنّ $p \equiv 1(mod\ 4)$.
3. إذا كان m عدداً صحيحاً موجباً أولياً فإنّ $(m-1)! \equiv -1(mod\ m)$.

الحلّ:

1.

- لنأخذ نظام البواقي المختزل **الطبيعي** قياس n:

$$R = \mathbb{Z}_n^* = \{t_1, t_2, \dots, t_{\phi(n)}\}\ ; |R| = \phi(n)\ \&\ \gcd(t_i, n) = 1\ \ \forall\ \ 1 \le i \le \phi(n)$$

وهي عبارة عن الأعداد الصحيحة الموجبة الأصغر من n و أوليّة مع العدد n.

- لدينا R نظام البواقي المختزل الطبيعي قياس n و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ عندئذ

$$aR = a\mathbb{Z}_n^* = \{at_1, at_2, \dots, at_{\phi(n)}\}\ ; |aR| = \phi(n)$$

نظام بواقي **مختزل** قياس n.

- بما أنّ aR نظام بواقي مختزل قياس n عندئذٍ كل عنصر من aR يطابق عنصر واحد فقط من R عندئذ

$$at_1 at_2 \dots at_{\phi(n)} \equiv t_1 t_2 \dots t_{\phi(n)} (mod\ n)$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} t_i \equiv \prod_{i=1}^{\phi(n)} t_i\ (mod\ n)$$

وبما أنّ $\gcd(t_i, n) = 1$ حيث $1 \le i \le \phi(n)$ عندئذ $\gcd\left(\prod_{i=1}^{\phi(n)} t_i, n\right) = 1$ بالتالي

$$a^{\phi(n)} \equiv 1(mod\ n)$$

2. نفرض بأن التطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ وليكن x_0 حلاً له عندئذٍ

$${x_0}^2 \equiv -1(mod\ p) \Rightarrow p \mid ({x_0}^2 + 1)$$

نلاحظ بأنّ $\gcd(x_0, p) = 1$ (لأنه لو كان $\gcd(x_0, p) \neq 1$ عندئذ $\gcd(x_0, p) = p$ عندئذ

$$p \mid x_0 \Rightarrow p \mid {x_0}^2$$

وبما أنّ $p \mid (x_0^2 + 1)$ عندئذ $p \mid 1$ وهذا مرفوض).

لدينا $\gcd(x_0, p) = 1$ عندئذ حسب مبرهنة فيرما نجد $x_0^{p-1} \equiv 1(mod\ p)$ بالتالي

$$(x_0^2)^{\frac{p-1}{2}} \equiv 1(mod\ p) \Longrightarrow (-1)^{\frac{p-1}{2}} \equiv 1(mod\ p)$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} -1\ if\ \text{فردي}\ \dfrac{p-1}{2} \\ 1\ if\ \text{زوجي}\ \dfrac{p-1}{2} \end{cases}$$

إذا كان $\frac{p-1}{2}$ فردي عندئذ $-1 \equiv 1(mod\ p)$ بالتالي $p \mid 2$ وهذا مرفوض. بالتالي $\frac{p-1}{2}$ زوجي عندئذ

$$\frac{p-1}{2} = 2k; \quad k \in \mathbb{Z} \Longrightarrow p = 4k + 1 \Longrightarrow p \equiv 1(mod\ 4)$$

.3

✓ **الحالة الأولى:** $m = 2$

$$(2-1)! = 1! = 1 \equiv -1(mod\ 2)$$

✓ **الحالة الثانية:** m **عدد أوليّ فردي**

- لنأخذ المجموعة $A = \mathbb{Z}_m^* = \{1,2,3,\dots,m-1\}\ ;\ |A| = \phi(m) = m - 1$

أيا كان $a \in A$ فإنّ $\gcd(a, m) = 1$ بالتالي التطابق الخطي $ax \equiv 1\ (mod\ m)$ يملك حلّ وحيد لأنّ $\gcd(a, m) \mid 1$. نرمز للحل الوحيد بـ $\bar{a}$ (المعكوس الضربي للعدد a بالنسبة للمقاس m)، $\bar{a} \in A$.

- إذا كان $a = \bar{a}$ عندئذ $a^2 \equiv 1\ (mod\ m)$ بالتالي $m \mid (a^2 - 1)$ بالتالي $m \mid (a-1)(a+1)$

إما $m \mid (a-1)$ عندئذ $a = 1$.

أو $m \mid (a+1)$ عندئذ $a = m - 1$.

نستنتج أنّ $a = \bar{a}$ إذا كان $a = 1$ أو $a = m - 1$

إذا كان $a \neq \bar{a}$ $a \in A \backslash \{1, m-1\} = \{2,3,\dots,m-2\}$

- عدد عناصر المجموعة $\{2,3,\dots,m-2\}$ زوجي عندئذ

$$2 \times 3 \times \dots \times (m-2) \equiv 1\ (mod\ m)$$
$$1 \times 2 \times 3 \times \dots \times (m-2) \equiv 1\ (mod\ m)$$
$$1 \times 2 \times 3 \times \dots \times (m-2) \times (m-1) \equiv m - 1\ (mod\ m)$$
$$(m-1)! \equiv -1(mod\ m)$$

2) أنجز **خمسة** فقط مما يأتي: (**لكلّ تمرين 6 درجات**) .**المجموع 30 درجة**

1. أوجد الحلول المختلفة للتطابق الخطي $8x \equiv 16(mod\ 20)$.
2. أثبت أنّ $18! \equiv 22(mod\ 23)$.
3. أوجد الحلين المختلفين للتطابق $x^2 + 7x + 10 \equiv 0(mod\ 11)$.
4. بيّن فيما إذا كان التطابق $x^6 \equiv 10(mod\ 19)$ قابل للحلّ أم لا.
5. أثبت أنّ $8 \mid (7^{4n^2+2} + 3^{2n+1} - 4)$ حيث n عدد صحيح موجب.
6. أوجد $O_{40}(3)$ و $O_{40}(27)$.

الحلّ:

1. $8x \equiv 16(mod\ 20)$

لدينا $a = 8, b = 16, m = 20$ و $d = \gcd(a, m) = 4$، $d \mid b$ عندئذ التطابق المعطى قابل للحلّ ويملك أربع حلول مختلفه بالنسبة للمقاس m.

لنوجد حلّ للتطابق $8x \equiv 16(mod\ 20)$

$$2x \equiv 4(mod\ 5) \Longrightarrow x \equiv 2(mod\ 5); m_1 = \frac{m}{d} = 5$$

بالتالي $x_0 = 2$ بالتالي حلول التطابق المعطى هي $\{2, 7, 12, 17\}$.

2. لدينا 23 عدد أولي بالتالي حسب ويلسون نجد: $(23-1)! \equiv -1(mod\ 23)$ بالتالي

$$(22)! \equiv -1(mod\ 23) \Longrightarrow 22 \times 21 \times 20 \times 19 \times (18)! \equiv -1(mod\ 23)$$
$$\Longrightarrow (-1) \times (-2) \times (-3) \times (-4) \times (18)! \equiv -1(mod\ 23)$$
$$\Longrightarrow 24 \times (18)! \equiv -1(mod\ 23) \Longrightarrow (18)! \equiv -1(mod\ 23)$$
$$\Longrightarrow (18)! \equiv 22(mod\ 23)$$

3. لدينا $a = 1$ و $b = 7$ و $c = 10$ و $p = 11$

- نوجد $d = b^2 - 4ac = 9$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$ وهي $\{-3, 3\}$

✓ من أجل $y_0 = 3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 11)$ فنجد

$$x = 9$$

✓ من أجل $y_0 = -3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 11)$ فنجد

$$x = 6$$

بالتالي حلول التطابق هي $\{6, 9\}$

4. التطابق $x^n \equiv a(mod\ m)$ قابل للحل إذا وفقط إذا كان $a^{\frac{\phi(m)}{d}} \equiv 1(mod\ m)$ حيث $d = \gcd(n, \phi(m))$ (مبرهنة أولر المعممة)

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

لدينا $n = 6, a = 10, m = 19$

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

نلاحظ بأنّ

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

بالتالي التطابق غير قابل للحلّ.

5. $8 \mid (7^{4n^2+2} + 3^{2n+1} - 4)$

$$7 \equiv -1(mod\ 8) \Longrightarrow 7^{4n^2+2} \equiv 1(mod\ 8) \ldots\ldots (1)$$
$$3^2 = 9 \equiv 1(mod\ 8) \Longrightarrow 3^{2n} \equiv 1(mod\ 8) \Longrightarrow 3^{2n+1} \equiv 3(mod\ 8) \ldots\ldots (2)$$

بالجمع نجد:

$$7^{4n^2+2} + 3^{2n+1} \equiv 4(mod\ 8)$$

$$7^{4n^2+2} + 3^{2n+1} - 4 \equiv 0(mod\ 8) \Longrightarrow 8 \mid (7^{4n^2+2} + 3^{2n+1} - 4)$$

6. $O_{40}(3)$ و $O_{40}(27)$

بفرض $O_{40}(3) = k$ عندئذ $k \mid \phi(40)$:

$$\phi(40) = 16$$

نحسب القوى 3^k حيث $k \in \{1,2,4,8,16\}$

$$3^1 \not\equiv 1\ (mod 40)$$
$$3^2 \not\equiv 1\ (mod 40)$$
$$3^3 \not\equiv 1\ (mod 40)$$
$$3^4 \equiv 1\ (mod 40)$$

بالتالي

$$O_{40}(3) = 4$$
$$O_{40}(27) = O_{40}(3^3) = \frac{O_{40}(3)}{\gcd(3, O_{40}(3))} = 4$$

السؤال الثاني: (36 درجة)

1) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $56x + 72y = 40$. **(15 درجة)**

الحلّ: $56x + 72y = 40$

لدينا $a = 56, b = 72, c = 40$ ولنوجد $\gcd(a, b)$ باستخدام طريقة إقليدس

$$72 = 1 \times 56 + 16$$
$$56 = 3 \times 16 + \mathbf{8}$$
$$16 = 2 \times 8 + 0$$

نلاحظ بأن $d = \gcd(a, b) = 8$ و $d \mid c$

فالمعادلة الديوفانتية قابلة للحلّ وتملك عدد لانهائي من الحلول.

لنوجد حل لها.

$$8 = 56 - 3 \times 16$$
$$8 = 56 - 3 \times (72 - 56)$$
$$8 = 56(4) + 72(-3)$$

نضرب الطرفين بـ $5 = \frac{c}{d}$ نجد:

$$56(20) + 72(-15) = 40$$

بالتالي $(x_0, y_0) = (20, -15)$ حل للمعادلة الديوفانتية $56x + 72y = 40$

أما الصيغة التي نستنتج منها جميع الحلول الصحيحة للمعادلة الديوفانتية:

$$\begin{cases} x = x_0 + \frac{b}{d}t = 20 + 9t \\ y = y_0 - \frac{a}{d}t = -15 - 7t \end{cases} \quad ;t \in \mathbb{Z}$$

2) **(21 درجة)** ليكن $m = 14$ عندئذٍ:

1. أوجد جذر أساسي بالنسبة للمقاس 7 بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس m، ثم أوجد الجذور الأساسية الآخرى بالنسبة للمقاس m.
2. أوجد الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 3$.

A to Z

3. أوجد المعكوس الضربي للعدد 3 بالنسبة للمقاس m.
4. أوجد جدول الأدلة بالنسبة للمقاس 7 ثم أوجد حلول التطابق $x^4 \equiv 2\ (mod\ 7)$ باستخدام الأدلة.

الحلّ:

1. **<u>إيجاد جذر أساسي بالنسبة للمقاس 7</u>(5 درجات)**

$a \in \mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ جذر أساسي بالنسبة للمقاس $p = 7$ إذا تحقق الشرط التالي

$$a^{\frac{p-1}{q}} \not\equiv 1(mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 6$.

نلاحظ بأنّ $q = 2$ أو 3

- الشرط لا يتحقق من أجل $a = 1$.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{6}{q}}: \begin{cases} 2^{\frac{6}{2}} = 2^3 \equiv 1(mod\ 7) \\ 2^{\frac{6}{3}} = 2^2 \not\equiv 1(mod\ 7) \end{cases}$$

بالتالي $a = 2$ ليس جذر أساسي بالنسبة للمقاس 7 .

- من أجل $a = 3$ نلاحظ بأنّ

$$3^{\frac{6}{q}}: \begin{cases} 3^{\frac{6}{2}} = 3^3 \not\equiv 1(mod\ 7) \\ 3^{\frac{6}{3}} = 3^2 \not\equiv 1(mod\ 7) \end{cases}$$

بالتالي $a = 3$ جذر أساسي بالنسبة للمقاس 7 ولنرمزه بـ $g = 3$.

<u>إيجاد جذر أساسي بالنسبة للمقاس $m = 14 = 2 \times 7$</u> (درجتان)

لدينا $g = 3$ جذر أساسي بالنسبة للمقاس $p = 7$ وبما أنّ g فردي عندئذ $g = 3$ جذر أساسي بالنسبة للمقاس m.

<u>الجذور الأخرى بالنسبة للمقاس $m = 14$</u>(درجتان)

عدد الجذور هو: $\phi(\phi(m)) = \phi(\phi(14)) = \phi(\phi(2 \times 7)) = \phi(\phi(2) \times \phi(7)) = \phi(6) = \phi(2) \times \phi(3) = 2$

نوجد الجذور بالشكل التالي

$$\{(3)^k; k < \phi(14)\ \&\ \gcd(k, \phi(14) = 1)\}$$
$$\{(3)^k; k < 6\ \&\ \gcd(k, 6) = 1)\} = \{(3)^1, (3)^5\}$$

وبما أنّ $(3)^1 \equiv 3(mod\ 14), (3)^5 \equiv 5(mod\ 14)$

بالتالي الجذور الأخرى بالنسبة للمقاس 14 هي $\{3,5\}$.

2. **(4 درجات)** لدينا 3 جذر أساسي بالنسبة للمقاس $m = 14$ عندئذ أياً كان $a \in \mathbb{Z}$ بحيث $\gcd(a, m) = 1$ فإنّ $a \equiv (3)^k (mod\ 14)$ بالتالي $O_m(a) = O_m((3)^k)$

A to Z

$$3 = \frac{O_m(3)}{\gcd\left(k, O_m(3)\right)} = \frac{\phi(14)}{\gcd\left(k, \phi(14)\right)} = \frac{6}{\gcd(k,6)}$$

بالتالي $\gcd(k,6) = 2$ عندئذٍ $k \in \{2,4\}$

بالتالي الأعداد الصحيحة التي رتبتها 3 بالنسبة للمقاس $m = 14$ هي:$\{(3)^2, (3)^4\}$

وبما أنّ $(3)^2 \equiv 9(mod\ 14), (3)^4 \equiv 11(mod\ 14)$

عندئذٍ الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 3$ هي:$\{9, 11\}$

3. **(3 درجات)**

$$\phi(m) = \phi(14) = \phi(2 \times 7) = \phi(2)\phi(7) = 6$$

المعكوس الضربي للعدد 3 بالنسبة للمقاس m هو باقي قسمة $3^{\phi(m)-1} = 3^{\phi(14)-1} = 3^5$ على العدد m بالتالي

المعكوس هو 5.

4. **(5 درجات)**. نحسب $3^k; 1 \le k \le \phi(7) = 6$ (3 جذر أساسي بالنسبة للمقاس 7).

3^k	3^1	3^2	3^3	3^4	3^5	3^6
N	3	2	6	4	5	1
$IndN$	1	2	3	4	5	6

N: هو باقي قسمة 3^k على العدد 7. $IndN$: دليل العدد N

نطبق نظرية الأدلة للطرفين نجد $x^4 \equiv 2\ (mod\ 7)$

$$4\ Indx \equiv Ind2(mod\ \phi(7))$$
$$4\ Indx \equiv 2(mod\ 6)$$

بالتالي $Indx \in \{2,5\}$ هذا التطابق يملك حلين مختلفين هما

$$Indx = 2 \Longrightarrow x = 2$$
$$Indx = 5 \Longrightarrow x = 5$$

بالتالي حلول التطابق هي $\{2,5\}$.

ملاحظة

- ✓ **بعض التمارين تحلّ بأكثر من طريقة، فأي طريقة متبعة من قبل الطالب لحلّ تمرين معين وهذه الطريقة صحيحة ينال الطالب العلامة المخصصة لهذا التمرين.**

مدرس المقرر: د. أحمد عيسى

A to Z

جامعة طرطوس كلية العلوم قسم الرياضيات

سلم تصحيح امتحان مقرر نظرية الأعداد لطلاب السنة الرابعة رياضيات

الدورة الفصلية الثانية – العام الدراسي 2022-2023م

الدرجة: تسعون

السؤال الأول: (48 درجة)

1) أثبت صحة قضيتين فقط من القضايا الآتية: 20 درجة (10 درجات لكلّ قضية يتم اختيارها)

1. إذا كان m عدداً صحيحاً موجباً أولياً فإنّ $(m-1)! \equiv -1(mod\ m)$.
2. إذا كان p عدداً أولياً فردياً والتطابق $x^2 \equiv -1(mod\ p)$ قابل للحل فإنّ $p \equiv 1(mod\ 4)$.
3. إذا كان $a \in \mathbb{Z}$ و $n, m \in \mathbb{Z}^+$ و $\gcd(a,m) = 1$ عندئذ $a^n \equiv 1(mod\ m)$ إذا وفقط إذا كان $O_m(a) \mid n$.

الحلّ:

1.

✓ **الحالة الأولى:** $m = 2$

$$(2-1)! = 1! = 1 \equiv -1(mod\ 2)$$

✓ **الحالة الثانية:** m **عدد أولي فردي**

- لنأخذ المجموعة $A = \mathbb{Z}_m^* = \{1,2,3,\dots,m-1\}\ ;\ |A| = \phi(m) = m-1$

أيا كان $a \in A$ فإنّ $\gcd(a,m) = 1$ بالتالي التطابق الخطي $ax \equiv 1\ (mod\ m)$ يملك حلّ وحيد لأنّ $\gcd(a,m) \mid 1$. نرمز للحل الوحيد بـ $\bar{a}$ (المعكوس الضربي للعدد a بالنسبة للمقاس m)، $\bar{a} \in A$.

- إذا كان $a = \bar{a}$ عندئذ $a^2 \equiv 1\ (mod\ m)$ بالتالي $m \mid (a^2-1)$ بالتالي $m \mid (a-1)(a+1)$

إما $m \mid (a-1)$ عندئذ $a = 1$.

أو $m \mid (a+1)$ عندئذ $a = m-1$.

نستنتج أنّ $a = \bar{a}$ إذا كان $a = 1$ أو $a = m-1$

إذا كان $a \neq \bar{a}$ $a \in A\backslash\{1, m-1\} = \{2,3,\dots,m-2\}$

- عدد عناصر المجموعة $\{2,3,\dots,m-2\}$ زوجي عندئذ

$$2 \times 3 \times \dots \times (m-2) \equiv 1\ (mod\ m)$$
$$1 \times 2 \times 3 \times \dots \times (m-2) \equiv 1\ (mod\ m)$$
$$1 \times 2 \times 3 \times \dots \times (m-2) \times (m-1) \equiv m-1\ (mod\ m)$$
$$(m-1)! \equiv -1(mod\ m)$$

A to Z

2. نفرض بأن التطابق $x^2 \equiv -1(mod\ p)$ قابل للحل وليكن x_0 حلاً له عندئذٍ

$$x_0{}^2 \equiv -1(mod\ p) \Longrightarrow p \mid (x_0{}^2 + 1)$$

نلاحظ بأنّ $\gcd(x_0, p) = 1$ (لأنه لو كان $\gcd(x_0, p) \neq 1$ عندئذ $\gcd(x_0, p) = p$ عندئذ

$$p \mid x_0 \Longrightarrow p \mid x_0{}^2$$

وبما أنّ $p \mid (x_0{}^2 + 1)$ عندئذ $p \mid 1$ وهذا مرفوض).

لدينا $\gcd(x_0, p) = 1$ عندئذ حسب مبرهنة فيرما نجد $x_0{}^{p-1} \equiv 1(mod\ p)$ بالتالي

$$(x_0{}^2)^{\frac{p-1}{2}} \equiv 1(mod\ p) \Longrightarrow (-1)^{\frac{p-1}{2}} \equiv 1(mod\ p)$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} -1\ if\ \text{فردي}\ \dfrac{p-1}{2} \\ 1\ if\ \text{زوجي}\ \dfrac{p-1}{2} \end{cases}$$

إذا كان $\frac{p-1}{2}$ فردي عندئذ $-1 \equiv 1(mod\ p)$ بالتالي $p \mid 2$ وهذا مرفوض، بالتالي $\frac{p-1}{2}$ زوجي عندئذ

$$\frac{p-1}{2} = 2k; \quad k \in \mathbb{Z} \Longrightarrow p = 4k + 1 \Longrightarrow p \equiv 1(mod\ 4)$$

3. **لزوم الشرط:** لدينا فرضاً $a^n \equiv 1(mod\ m)$ ولنثبت أن $O_m(a) \mid n$

باستخدام خوارزمية القسمة الاقليدية نجد: $n = q \times O_m(a) + r; 0 \leq r < O_m(a)$

ومنه نجد أنّ

$$a^n = \left(a^{O_m(a)}\right)^q \times a^r \equiv (1)^q \times a^r (mod\ m) \equiv a^r (mod\ m)$$

$$a^n \equiv a^r (mod\ m) \Longrightarrow a^r \equiv 1\ (mod\ m)$$

إذا كان $a^r \equiv 1\ (mod\ m)$ حيث $0 < r < O_m(a)$ بالتالي هذا مستحيل.

بالتالي $r = 0$ عندئذٍ $n = q \times O_m(a)$ بالتالي $O_m(a) \mid n$

كفاية الشرط: لدينا فرضاً $O_m(a) \mid n$ بالتالي $n = k \times O_m(a); k \in \mathbb{Z}^+$ بالتالي

$$a^n = \left(a^{O_m(a)}\right)^k \equiv (1)^k \equiv 1(mod\ m)$$

2) أنجز <u>أربعة</u> فقط مما يأتي: **24 درجة** (6 درجات لكلّ تمرين يتم اختياره)

1. أوجد الحلول المختلفة للتطابق الخطي $9x \equiv 21(mod\ 30)$.
2. أثبت أنّ $67 \mid (43 \times (65!) + 4!)$.
3. أوجد الحلين المختلفين للتطابق $5x^2 + 7x + 2 \equiv 0(mod\ 13)$.
4. بيّن فيما إذا كان التطابق $x^6 \equiv 5(mod\ 17)$ قابل للحل أم لا.
5. إذا كان $n \in \mathbb{Z}$ بحيث $gcd(n, 35) = 1$ فأثبت أنّ $n^{12} \equiv 1(mod\ 35)$.

الحلّ:

1. $9x \equiv 21(mod\ 30)$

لدينا $a = 9, b = 21, m = 30$ و $d = \gcd(a, m) = 3$. $d \mid b$ عندئذ التطابق المعطى قابل للحلّ ويملك ثلاث

حلول مختلفة بالنسبة للمقاس m.

لنوجد حلّ للتطابق $9x \equiv 21(mod\ 30)$

$$3x \equiv 7(mod\ 10); m_1 = \frac{m}{d} = 10$$

$$x \equiv 9(mod\ 10)$$

بالتالي $x_0 = 9$ بالتالي حلول التطابق المعطى هي $\{9, 19, 29\}$

2. لدينا 67 عدد أولي بالتالي حسب ويلسون نجد: $(67-1)! \equiv -1(mod\ 67)$ بالتالي

$$(66)! \equiv -1(mod\ 67) \Longrightarrow 66 \times (65)! \equiv -1(mod\ 67)$$

$$\Longrightarrow (65)! \equiv 1(mod\ 67)$$

$$\Longrightarrow 43 \times (65)! \equiv 43(mod\ 67) \Longrightarrow 43 \times (65)! + 4! \equiv 43 + 4!\ (mod\ 67)$$

$$\Longrightarrow 43 \times (65)! + 4! \equiv 67(mod\ 67) \Longrightarrow 43 \times (65)! + 4! \equiv 0(mod\ 67)$$

$$\Longrightarrow 67 \mid (43 \times (65!) + 4!)$$

3. لدينا $a = 5$ و $b = 7$ و $c = 2$ و $p = 13$.

- نوجد $d = b^2 - 4ac = 9$
- نوجد حلول التطابق $y^2 \equiv d(mod\ p)$ وهي $\{-3, 3\}$

✓ من أجل $y_0 = 3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 13)$ فنجد

$$10x \equiv -4(mod\ 13) \Longrightarrow -3x \equiv 9(mod\ 13) \Longrightarrow x \equiv -3(mod\ 13)$$

$$\Longrightarrow x \equiv 10(mod\ 13) \Longrightarrow x = 10$$

✓ من أجل $y_0 = -3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 13)$ فنجد

$$10x \equiv -10(mod\ 13) \Longrightarrow x \equiv -1(mod\ 13) \Longrightarrow x \equiv 12(mod\ 13) \Longrightarrow x = 12$$

بالتالي حلول التطابق $5x^2 + 7x + 2 \equiv 0(mod\ 13)$ هي $\{10, 12\}$

4. $x^6 \equiv 5(mod\ 17)$

التطابق $x^n \equiv a(mod\ m)$ قابل للحل إذا وفقط إذا كان $a^{\frac{\phi(m)}{d}} \equiv 1(mod\ m)$ حيث $d = \gcd(n, \phi(m))$ (مبرهنة أولر المعممة)

التطابق المعطى هو: $x^6 \equiv 5(mod\ 17)$

لدينا $n = 6, a = 5, m = 17$

$$\phi(m) = 16, \qquad d = \gcd(n, \phi(m)) = 2$$

نلاحظ بأنّ

$$a^{\frac{\phi(m)}{d}} = 5^8 \not\equiv 1(mod\ 17)$$

بالتالي التطابق $x^6 \equiv 5(mod\ 17)$ غير قابل للحلّ.

5. لدينا $n \in \mathbb{Z}$ بحيث $\gcd(n, 35) = 1$ بالتالي $\gcd(n, 5) = \gcd(n, 7) = 1$

لدينا $\gcd(n, 5) = 1$ عندئذ حسب مبرهنة أولر نجد $n^{\phi(5)} \equiv 1(mod\ 5)$ بالتالي

$$n^4 \equiv 1(mod\ 5) \Longrightarrow n^{12} \equiv 1(mod\ 5) \ldots\ldots (1)$$

لدينا $\gcd(n, 7) = 1$ عندئذ حسب مبرهنة أولر نجد $n^{\phi(7)} \equiv 1(mod\ 7)$ بالتالي

$$n^6 \equiv 1(mod\ 7) \Longrightarrow n^{12} \equiv 1(mod\ 7) \ldots\ldots (2)$$

من (1) و (2) وكون $\gcd(5, 7) = 1$ بالتالي $n^{12} \equiv 1(mod\ 5 \times 7)$ عندئذ $n^{12} \equiv 1(mod\ 35)$

A to Z

السؤال الثاني: (46 درجة)

1) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $1000x + 72y = 32$. **(12 درجة)**

الحل: $1000x + 72y = 32$

لدينا $a = 1000, b = 72, c = 32$ ولنوجد $\gcd(a, b)$ باستخدام طريقة اقليدس

$$1000 = 13 \times 72 + 64$$
$$72 = 1 \times 64 + 8$$
$$64 = 8 \times 8 + 0$$

نلاحظ بأن $d = \gcd(a, b) = 8$ و $d \mid c$ فالمعادلة الديوفانتية قابلة للحل وتملك عدد لانهائي من الحلول، لنوجد حل لها.

$$8 = 72 - 64$$
$$8 = 72 - (1000 - 13 \times 72)$$
$$8 = 1000(-1) + 72(14)$$

نضرب الطرفين بـ $\frac{c}{d} = 4$ نجد: $1000(-4) + 72(56) = 32$

بالتالي $(x_0, y_0) = (-4, 56)$ حل للمعادلة الديوفانتية $1000x + 72y = 32$

أما الصيغة التي نستنتج منها جميع الحلول الصحيحة للمعادلة الديوفانتية:

$$\begin{cases} x = x_0 + \frac{b}{d}t = -4 + 9t \\ y = y_0 - \frac{a}{d}t = 56 - 125t \end{cases} ; t \in \mathbb{Z}$$

2) ليكن $m = 34$ عندئذٍ **(30 درجة)**

1. أوجد جذر أساسي بالنسبة للمقاس 17 بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس m، ثم أوجد عدد الجذور الأساسية بالنسبة للمقاس m.
2. أوجد المعكوس الضربي للعدد 3 بالنسبة للمقاس m.
3. أوجد الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 4$.
4. أوجد جدول الأدلة بالنسبة للمقاس 17 ثم أوجد حلول التطابق $x^{12} \equiv 16 \pmod{17}$ باستخدام الأدلة.

الحلّ:

1. **إيجاد جذر أساسي بالنسبة للمقاس 17 (5 درجات)**

$a \in \mathbb{Z}_{17}^* = \{1,2,3, \dots, 16\}$ جذر أساسي بالنسبة للمقاس $p = 17$ إذا تحقق الشرط التالي

$$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 16$.

نلاحظ بأنّ $q = 2$

- الشرط لا يتحقق من أجل $a = 1$.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{16}{q}}: \quad 2^{\frac{16}{2}} = 2^8 \equiv 1 \pmod{17}$$

A to Z

بالتالي $a = 2$ ليس جذر أساسي بالنسبة للمقاس 17.

- من أجل $a = 3$ نلاحظ بأنّ

$$3^{\frac{16}{q}}: \quad 3^{\frac{16}{2}} = 3^8 \not\equiv 1(mod\ 17)$$

بالتالي $a = 3$ جذر أساسي بالنسبة للمقاس 17 ولنرمزه بـ $g = 3$.

<u>إيجاد جذر أساسي بالنسبة للمقاس $m = 34 = 2 \times 17$</u> (3 درجات)

لدينا $g = 3$ جذر أساسي بالنسبة للمقاس $p = 17$ وبما أنّ g فردي عندئذ $g = 3$ جذر أساسي بالنسبة للمقاس m.

<u>عدد الجذور الأخرى بالنسبة للمقاس $m = 34$</u>(3 درجات)

عدد الجذور هو: $\phi(\phi(m)) = \phi(\phi(34)) = \phi(\phi(2 \times 17)) = \phi(\phi(2) \times \phi(17)) = \phi(16) = \phi(2^4) = 8$

ملاحظة: إذا وجد الطالب الجذور الاخرى بالشكل التالي ثم استنتج عددها ينال الطالب العلامة المخصصة لهذا الطلب

$$\{(3)^k; k < \phi(34)\ \&\ \gcd(k, \phi(34)) = 1\}$$

$$\{(3)^k; k < 16\ \&\ \gcd(k, 16) = 1)\} = \{(3)^1, (3)^3, (3)^5, (3)^7, (3)^9, (3)^{11}, (3)^{13}, (3)^{15}\}$$

وبما أنّ $(3)^1 \equiv 3(mod 34)$ $(3)^3 \equiv 27(mod 34)$, $(3)^5 \equiv 5(mod\ 34)$ $(3)^7 \equiv 11(mod 34)$,

وبما أنّ $(3)^9 \equiv 31(mod\ 34)$ $(3)^{11} \equiv 7(mod 34)$, $(3)^{13} \equiv 29(mod 34)$ $(3)^{15} \equiv 23(mod\ 34)$,

بالتالي الجذور الأخرى بالنسبة للمقاس 34 هي $\{3, 5, 7, 11, 23, 27, 29, 31\}$ بالتالي عدد الجذور 8.

2. (3 درجات) المعكوس الضربي للعدد 3 بالنسبة للمقاس m هو باقي قسمة $3^{\phi(m)-1} = 3^{\phi(34)-1} = 3^{15}$ على العدد m بالتالي المعكوس هو 23.

3. (5 درجات)

لدينا 3 جذر أساسي بالنسبة للمقاس $m = 34$ عندئذ أياً كان $a \in \mathbb{Z}$ بحيث $\gcd(a, m) = 1$ فإنّ

$a \equiv (3)^k (mod\ 34)$ بالتالي $O_m(a) = O_m((3)^k)$

$$4 = \frac{O_m(3)}{\gcd(k, O_m(3))} = \frac{\phi(34)}{\gcd(k, \phi(34))} = \frac{16}{\gcd(k, 16)}$$

بالتالي $\gcd(k, 16) = 4$ عندئذٍ $k \in \{4,\ 12\}$

بالتالي الأعداد الصحيحة التي رتبتها 4 بالنسبة للمقاس $m = 34$ هي:$\{(3)^4, (3)^{12}\}$

وبما أنّ $(3)^4 \equiv 13(mod\ 34)$, $(3)^{12} \equiv 21(mod\ 34)$

عندئذٍ الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 4$ هي:$\{13, 21\}$.

4. (11 درجات). نحسب $1 \le k \le \phi(17) = 16$; 3^k (3 جذر أساسي بالنسبة للمقاس 17).

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

A to Z

امتحان مقرر نظرية الأعداد — اسم الطالب:

سنة رابعة رياضيات — المدة: ساعتان

يات — الدورة الفصلية الأولى – العام الدراسي 2022–2023م — الدرجة: تسعون

ل الأول: (48 درجة)

) أثبت صحّة **قضيتين** فقط من القضايا الآتية:

1. إذا كان $n > 1$ عدداً صحيحاً و$a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
2. إذا كان p عدداً أولياً فردياً والتطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ فإنّ $p \equiv 1(mod\ 4)$.
3. إذا كان m عدداً صحيحاً موجباً و$(m-1)! \equiv -1(mod\ m)$ فإنّ m عدد أولي.

2) أنجز **أربعة** فقط مما يأتي:

1. أوجد الحلول المختلفة للتطابق الخطي $8x \equiv 16(mod\ 20)$.
2. أثبت أنّ $37 \mid (2 \times (34!) + 1)$.
3. أوجد الحلين المختلفين للتطابق $x^2 + 7x + 10 \equiv 0(mod\ 11)$.
4. بيّن فيما إذا كان التطابق $x^6 \equiv 10(mod\ 19)$ قابل للحلّ أم لا.
5. إذا كان $n \in \mathbb{Z}$ بحيث $\gcd(n,6) = 1$ فأثبت أنّ $n^4 \equiv 1(mod\ 24)$.

السؤال الثاني: (42 درجة)

1) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $56x + 72y = 40$.

2) ليكن $m = 22$ عندئذٍ:

1. أوجد جذر أساسي بالنسبة للمقاس 11 بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس m ثم أوجد عدد الجذور الأساسية بالنسبة للمقاس m.
2. هل المجموعة $\{(13)^1, (13)^2, (13)^3, (13)^4, (13)^5, (13)^6, (13)^7, (13)^8, (13)^9, (13)^{10}\}$ نظام بواقي مختزل قياس m أم لا.
3. أوجد المعكوس الضربي للعدد 3 بالنسبة للمقاس m.
4. أوجد الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 5$.
5. أوجد جدول الأدلة بالنسبة للمقاس 11 ثم أوجد حلول التطابق $x^4 \equiv 4\ (mod\ 11)$ باستخدام الأدلة.

---انتهت الأسئلة---

تمنياتي بالتوفيق والنجاح

طرطوس: الأحد 2023/1/15م — مدرس المقرر: د. أحمد عيسى

الممسوحة ضوئيا بـ CamScanner

جامعة طرطوس كلية العلوم قسم الرياضيات

سلم تصحيح امتحان مقرر نظرية الأعداد لطلاب السنة الرابعة رياضيات

الدورة الفصلية الأولى – العام الدراسي 2022–2023م

الدرجة: تسعون

السؤال الأول: (48 درجة)

1) أثبت صحّة قضيتين فقط من القضايا الآتية: 20 درجة (10 درجات لكلّ قضية)

1. إذا كان $n > 1$ عدداً صحيحاً و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ فإنّ $a^{\phi(n)} \equiv 1(mod\ n)$ حيث ϕ دالة أولر.
2. إذا كان p عدداً أولياً فردياً والتطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ فإنّ $p \equiv 1(mod\ 4)$.
3. إذا كان m عدداً صحيحاً موجباً و $(m-1)! \equiv -1(mod\ m)$ فإنّ m عدد أولي.

الحلّ:

1.

- لنأخذ R نظام البواقي المختزل **الطبيعي** قياس n:

$$R = \mathbb{Z}_n^* = \{t_1, t_2, \dots, t_{\phi(n)}\}; |R| = \phi(n) \ \&\ \gcd(t_i, n) = 1 \ \forall\, 1 \le i \le \phi(n)$$

وهي عبارة عن الأعداد الصحيحة الموجبة الأصغر من n و أولية مع العدد n.

- لدينا R نظام البواقي المختزل الطبيعي قياس n و $a \in \mathbb{Z}$ بحيث $\gcd(a,n) = 1$ عندئذ

$$aR = a\mathbb{Z}_n^* = \{at_1, at_2, \dots, at_{\phi(n)}\}; |aR| = \phi(n)$$

نظام بواقي مختزل قياس n.

- بما أنّ aR نظام بواقي مختزل قياس n عندئذٍ كل عنصر من aR يطابق عنصر واحد فقط من R عندئذ

$$at_1 at_2 \dots at_{\phi(n)} \equiv t_1 t_2 \dots t_{\phi(n)} (mod\ n)$$

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} t_i \equiv \prod_{i=1}^{\phi(n)} t_i \ (mod\ n)$$

وبما أنّ $\gcd(t_i, n) = 1$ أياً كان $1 \le i \le \phi(n)$ عندئذ $\gcd\left(\prod_{i=1}^{\phi(n)} t_i, n\right) = 1$ بالتالي

$$a^{\phi(n)} \equiv 1(mod\ n)$$

2. نفرض بأن التطابق $x^2 \equiv -1(mod\ p)$ قابل للحلّ وليكن x_0 حلاً له عندئذٍ

$$x_0{}^2 \equiv -1(mod\ p) \Rightarrow p \mid (x_0{}^2 + 1)$$

نلاحظ بأنّ $\gcd(x_0, p) = 1$ (لأنه لو كان $\gcd(x_0, p) \neq 1$ عندئذ $\gcd(x_0, p) = p$ عندئذ

$$p \mid x_0 \Rightarrow p \mid x_0{}^2$$

الممسوحة ضوئيا بـ CamScanner

وبما أنّ $p \mid (x_0^2 + 1)$ عندئذ $p \mid 1$ وهذا مرفوض).

لدينا $\gcd(x_0, p) = 1$ عندئذ حسب مبرهنة فيرما نجد $x_0^{p-1} \equiv 1(mod\ p)$ بالتالي

$$(x_0^2)^{\frac{p-1}{2}} \equiv 1(mod\ p) \Rightarrow (-1)^{\frac{p-1}{2}} \equiv 1(mod\ p)$$

$$(-1)^{\frac{p-1}{2}} = \begin{cases} -1\ if\ \text{فردي}\ \frac{p-1}{2} \\ 1\ if\ \text{زوجي}\ \frac{p-1}{2} \end{cases}$$

إذا كان $\frac{p-1}{2}$ فردي عندئذ $1 \equiv -1(mod\ p)$ بالتالي $p \mid 2$ وهذا مرفوض. بالتالي $\frac{p-1}{2}$ زوجي عندئذ

$$\frac{p-1}{2} = 2k; \quad k \in \mathbb{Z} \Rightarrow p = 4k + 1 \Rightarrow p \equiv 1(mod\ 4)$$

3. نفرض جدلاً بأن m ليس بعدد أولي عندئذ يوجد عدد أولي p بحيث $p \mid m$ حيث $1 < p \leq m - 1$

$$(m-1)! = (m-1) \times (m-2) \times \ldots\ldots \times 3 \times 2 \times 1$$

بالتالي $p \mid (m-1)!$

$$(m-1)! \equiv -1(mod\ m) \Rightarrow m \mid ((m-1)! + 1)$$

وبما أن $p \mid m$ عندئذ $p \mid ((m-1)! + 1)$ وبما أن $p \mid (m-1)!$ عندئذ $p \mid 1$ وهذا مرفوض. بالتالي m عدد أولي.

2) أنجز <u>أربعة</u> فقط مما يأتي: 28 درجة (7 درجات لكلّ تمرين يتم اختياره)

1. أوجد الحلول المختلفة للتطابق الخطي $8x \equiv 16(mod\ 20)$.
2. أثبت أنّ $37 \mid (2 \times (34!) + 1)$.
3. أوجد الحلين المختلفين التطابق $x^2 + 7x + 10 \equiv 0(mod\ 11)$.
4. بيّن فيما إذا كان التطابق $x^6 \equiv 10(mod\ 19)$ قابل للحلّ أم لا.
5. إذا كان $n \in \mathbb{Z}$ بحيث $\gcd(n, 6) = 1$ فأثبت أنّ $n^4 \equiv 1(mod\ 24)$.

الحلّ:

1. $8x \equiv 16(mod\ 20)$

لدينا $a = 8, b = 16, m = 20$ و $d = \gcd(a, m) = 4$ عندئذ التطابق المعطى قابل للحلّ ويملك أربع $d \mid b$.

حلول مختلفة بالنسبة للمقاس m

لنوجد حلّ للتطابق $8x \equiv 16(mod\ 20)$

$$x \equiv 2(mod\ 5); m_1 = \frac{m}{d} = 5$$

بالتالي $x_0 = 2$ بالتالي حلول التطابق المعطى هي $\{2, 7, 12, 17\}$

2. لدينا 37 عدد أولي بالتالي حسب ويلسون نجد: $(37-1)! \equiv -1(mod\ 37)$ بالتالي

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

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

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

3. لدينا $a = 1$ و $b = 7$ و $c = 10$ و $p = 11$
   - نوجد $d = b^2 - 4ac = 9$
   - نوجد حلول التطابق $y^2 \equiv d(mod\ p)$ وهي $\{-3, 3\}$

الممسوحة ضوئيا بـ CamScanner

✓ من أجل $y_0 = 3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 11)$ فنجد

$$2x \equiv -4(mod\ 11) \Rightarrow x \equiv 9(mod\ 11) \Rightarrow x = 9$$

✓ من أجل $y_0 = -3$ نحل التطابق الخطي $2ax \equiv y_0 - b(mod\ 11)$ فنجد

$$2x \equiv -10(mod\ 11) \Rightarrow x \equiv 6(mod\ 11) \Rightarrow x = 6$$

بالتالي حلول التطابق هي $\{6, 9\}$

4. $x^6 \equiv 10(mod\ 19)$

التطابق $x^n \equiv a(mod\ m)$ قابل للحل إذا وفقط إذا كان $a^{\frac{\phi(m)}{d}} \equiv 1(mod\ m)$ حيث $d = \gcd(n, \phi(m))$ (مبرهنة أولر المعممة)

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

لدينا $n = 6, a = 10, m = 19$

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

نلاحظ بأنّ

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

بالتالي التطابق غير قابل للحلّ.

5. لدينا $n \in \mathbb{Z}$ بحيث $\gcd(n, 6) = 1$ بالتالي $\gcd(n, 3) = \gcd(n, 2) = 1$.

$$24 = 3 \times 8$$

إذا كان $\gcd(n, 2) = 1$ عندئذٍ $\gcd(n, 8) = 1$ عندئذٍ حسب مبرهنة أولر نجد $n^{\phi(8)} \equiv 1(mod\ 8)$ بالتالي

$$n^4 \equiv 1(mod\ 8) \ldots\ldots (1)$$

إذا كان $\gcd(n, 3) = 1$ عندئذٍ حسب مبرهنة أولر نجد $n^{\phi(3)} \equiv 1(mod\ 3)$ بالتالي

$$n^2 \equiv 1(mod\ 3) \Rightarrow n^4 \equiv 1(mod\ 3) \ldots\ldots (2)$$

من (1) و (2) وكون $\gcd(3, 8) = 1$ بالتالي $n^4 \equiv 1(mod\ 3 \times 8)$ عندئذٍ $n^4 \equiv 1(mod\ 24)$.

السؤال الثاني: (42 درجة)

i) أوجد صيغة تستنتج من خلالها جميع الحلول الصحيحة للمعادلة الديوفانتية $56x + 72y = 40$. **(12 درجة)**

الحلّ: $56x + 72y = 40$

لدينا $a = 56, b = 72, c = 40$ ولنوجد $\gcd(a, b)$ باستخدام طريقة إقليدس

$$72 = 1 \times 56 + 16$$
$$56 = 3 \times 16 + \mathbf{8}$$
$$16 = 2 \times 8 + 0$$

نلاحظ بأن $d = \gcd(a, b) = 8$ و $d \mid c$ فالمعادلة الديوفانتية قابلة للحلّ وتملك عدد لانهائي من الحلول. لنوجد حل لها.

$$8 = 56 - 3 \times 16$$
$$8 = 56 - 3 \times (72 - 56)$$
$$8 = 56(4) + 72(-3)$$

نضرب الطرفين بـ $\frac{c}{d} = 5$ نجد: $56(20) + 72(-15) = 40$

بالتالي $(x_0, y_0) = (20, -15)$ حل للمعادلة الديوفانتية $56x + 72y = 40$

الممسوحة ضوئيا بـ CamScanner

أما الصيغة التي نستنتج منها جميع الحلول الصحيحة للمعادلة الديوفانتية:

$$\begin{cases} x = x_0 + \frac{b}{d}t = 20 + 9t \\ y = y_0 - \frac{a}{d}t = -15 - 7t \end{cases} ; t \in \mathbb{Z}$$

2) ليكن $m = 22$ عندئذٍ (30 درجة)

1. أوجد جذر أساسي بالنسبة للمقاس 11 بالاعتماد على اختبار لوكاس، ثم استنتج جذر أساسي بالنسبة للمقاس m ثم أوجد عدد الجذور الأساسية بالنسبة للمقاس m.
2. هل المجموعة $\{(13)^1, (13)^2, (13)^3, (13)^4, (13)^5, (13)^6, (13)^7, (13)^8, (13)^9, (13)^{10}\}$ نظام بواقي مختزل قياس m أم لا.
3. أوجد المعكوس الضربي للعدد 3 بالنسبة للمقاس m.
4. أوجد الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 5$.
5. أوجد جدول الأدلة بالنسبة للمقاس 11 ثم أوجد حلول التطابق $x^4 \equiv 4 \pmod{11}$ باستخدام الأدلة.

الحل:

1. **إيجاد جذر أساسي بالنسبة للمقاس 11 (7 درجات)**

$a \in \mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10\}$ جذر أساسي بالنسبة للمقاس $p = 11$ إذا تحقق الشرط التالي

$$a^{\frac{p-1}{q}} \not\equiv 1 (mod\ p)$$

وذلك من أجل كل قاسم أولي q للعدد $p - 1 = 10$.

نلاحظ بأنّ $q = 2$ أو 5

- الشرط لا يتحقق من أجل $a = 1$.
- من أجل $a = 2$ نلاحظ بأنّ

$$2^{\frac{10}{q}}: \begin{cases} 2^{\frac{10}{2}} = 2^5 \not\equiv 1 (mod\ 11) \\ 2^{\frac{10}{5}} = 2^2 \not\equiv 1 (mod\ 11) \end{cases}$$

بالتالي $a = 2$ جذر أساسي بالنسبة للمقاس 11 ولنرمز له بـ $g = 2$.

إيجاد جذر أساسي بالنسبة للمقاس $m = 22 = 2 \times 11$ (درجتان)

لدينا $g = 2$ جذر أساسي بالنسبة للمقاس $p = 11$ وبما أنّ g زوجي عندئذ $g + p = 13$ جذر أساسي بالنسبة للمقاس m.

عدد الجذور الأخرى بالنسبة للمقاس $m = 22$(درجتان)

$$\phi(\phi(m)) = \phi(\phi(22)) = \phi(\phi(2 \times 11)) = \phi(\phi(2) \times \phi(11)) = \phi(10) = \phi(2) \times \phi(5) = 4$$ عدد الجذور هو:

ملاحظة: إذا وجد الطالب الجذور الأخرى بالشكل التالي ثم استنتج عددها ينال العلامة المخصصة لهذا الطلب.

$$\{(13)^k; k < \phi(22) \ \&\ \gcd(k, \phi(22)) = 1\}$$

$$\{(13)^k; k < 10 \ \&\ \gcd(k, 10) = 1\} = \{(13)^1, (13)^3, (13)^7, (13)^9\}$$

وبما أنّ $(13)^1 \equiv 13 (mod\ 22)$, $(13)^3 \equiv 19 (mod\ 22)$, $(13)^7 \equiv 7 (mod\ 22)$, $(13)^9 \equiv 17 (mod\ 22)$

بالتالي الجذور الأخرى بالنسبة للمقاس 22 هي $\{7, 13, 17, 19\}$ بالتالي عدد الجذور 4.

الممسوحة ضوئيا بـ CamScanner

2. **(درجتان)** بما أنّ 13 جذر أساسي بالنسبة للمقاس $m = 22$ عندئذ المجموعة
$\{(13)^1, (13)^2, \ldots\ldots, (13)^{\phi(22)}\}$ بالتالي

$\{(13)^1, (13)^2, (13)^3, (13)^4, (13)^5, (13)^6, (13)^7, (13)^8, (13)^9, (13)^{10}\}$ نظام بواقي مختزل قياس m

3. **(درجتان)** المعكوس الضربي للعدد 3 بالنسبة للمقاس m هو باقي قسمة $3^{\phi(m)-1} = 3^{\phi(22)-1} = 3^9$ على العدد m بالتالي المعكوس هو 15.

4. **(5 درجات)** لدينا 13 جذر أساسي بالنسبة للمقاس $m = 22$ عندئذ أياً كان $a \in \mathbb{Z}$ بحيث $\gcd(a, m) = 1$ فإنّ
$a \equiv (13)^k (mod\ 22)$ بالتالي $O_m(a) = O_m((13)^k)$

$$5 = \frac{O_m(13)}{\gcd\left(k, O_m(13)\right)} = \frac{\phi(22)}{\gcd\left(k, \phi(22)\right)} = \frac{10}{\gcd(k, 10)}$$

بالتالي $\gcd(k, 10) = 2$ عندئذٍ $k \in \{2, 4, 6, 8\}$

بالتالي الأعداد الصحيحة التي رتبتها 5 بالنسبة للمقاس $m = 22$ هي:$\{(13)^2, (13)^4, (13)^6, (13)^8\}$

وبما أنّ $(13)^2 \equiv 15(mod\ 22)$, $(13)^4 \equiv 5(mod\ 22)$, $(13)^6 \equiv 9(mod\ 22)$, $(13)^8 \equiv 3(mod\ 22)$

عندئذٍ الأعداد الصحيحة الموجبة a الأقل من m التي تحقق العلاقة $O_m(a) = 5$ هي:$\{3, 5, 9, 15\}$.

5. **(10 درجات)**. نحسب $2^k; 1 \le k \le \phi(11) = 10$ (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

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

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

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

بالتالي حلول التطابق هي $\{3, 8\}$

----------ملاحظة----------

✓ بعض التمارين تحلّ بأكثر من طريقة، فأي طريقة متبعة من قبل الطالب لحلّ تمرين معين وهذه الطريقة صحيحة ينال الطالب العلامة المخصصة لهذا التمرين.

طرطوس: الأحد 2023/1/15م

مدرس المقرر: د. أحمد عيسى

الممسوحة ضوئيا بـ CamScanner

مع تصحيح فرض نظرية الأعداد
سنة رابعة رياضيات
الدورة التكميلية 2011-2012

السؤال الأول (60 درجة)

1- نقول العدد صحيح الأول p إذا كان p ≥ 2 وكان القواسم الموجبة للعدد p هي 1 و p فقط.
- أثبت أن العدد 341 ليس أولي.
- تقبل المعادلة 543x+5y=250 حلول صحيحة. عين الحلول الموجبة للمعادلة.
- أثبت أن 97! + 96 مركب. (4)
- أثبت أن m ∈ Z+ عدد أولي إذا وفقط إذا كان (m-1)! ≡ -1 (mod m) (8)
- بما أن 8,12 = 4 فإن 10^3 ≡ (-2)^3 ≡ -1 (mod 13) لذلك حسب أولر 10^6 ≡ 1 (mod 13)
العبارة ليس لها حل. (4)
- حل التطابقة x^8 ≡ 10 (mod 13) باستخدام نظرية الأدلمان. (9)
حلول التطابقة هي x ∈ {2, 8, 9, 7, 15, 4}
- حسب المميز لدينا Δ = 49 ثم حل التطابقة y^2 ≡ 49 (17) هذا يكافئ y = ±7 فنجد حلول التطابقة هي {4, 9}
- أثبت أن التطابقة x^2 ≡ a (mod p) ليس لها حل إذا وفقط إذا كان a^{(p-1)/2} ≡ -1 (mod p) (6)
- أحل في Z التطابقة 3x ≡ 2 (mod 10) ، 3x ≡ 6 (mod 12) ثم x ≡ 12 (mod 60). (9)

السؤال الثاني (20 درجة)

1- نقبل هذه النتيجة بدون برهان
- لتكن الأعداد q حيث (q, 250) = 1 ، σ(q) = 5 (5)
250

- حل التطابقة x^2 ≡ 2 (mod 17^2) (8)
- بما أن M_p | 9 فإن M_p ≡ 0 (mod 9) بالتالي حسب (7) 2^p ≡ 1 (mod 9) ومنه σ(2) = p بالتالي حسب المبرهنة السابقة 9 ≡ 1 (mod p) وبالتالي p | 9-1 = 8 (5)
- أثبت أن العدد M_11 مركب

$\varphi_0(t) = f(x_1) = 4(2-4t)^2 - 4(3-4t)(2-4t) + 2(3-4t)^2$

$\varphi_0(t) = 10 - 32t + 32t^2$

$\varphi_0'(t) = 0 \Rightarrow -32 + 64t = 0 \Rightarrow \boxed{t = \frac{1}{2}}$

$X_2 = \begin{bmatrix} 4t_1 \\ 1-4t_1 \end{bmatrix}$ ، $\nabla f(x_1) = \begin{bmatrix} -4 \\ 4 \end{bmatrix}$

$\varphi_1(t) = 160t^2 - 32t + 2$

$\varphi_1'(t) = 0 \Rightarrow \boxed{t = \frac{1}{10}}$

$X_2 = \begin{bmatrix} \frac{2}{5} \\ \frac{3}{5} \end{bmatrix}$

سؤال الرابع

$\min f(x) = x^2 - 7x + 12$

$n = 4$ ، $[a_1, b_1] = [2, 4]$

$x_1^1 = \frac{F_2}{F_4}(2) + a_1 = 2.8$

$x_2^1 = \frac{F_3}{F_4}(2) + a_1 = 3.2$

$f(x_1^1) = 0.24$ ، $f(x_2^1) = 0.16$

$f(x_1^1) > f(x_2^1) \Rightarrow [a_2, b_2] = [2.8, 4]$

$x_1^2 = x_2^1 = 3.2$

$x_2^2 = a_2 + \frac{F_2}{F_3}(1.2) = 3.6$

$f(x_1^2) = -0.16$ ، $f(x_2^2) = -0.24$

$f(x_2^2) < f(x_1^2)$

$[a_3, b_3] = [3.2, 4]$

$x_1^3 = x_2^2 = 3.6$

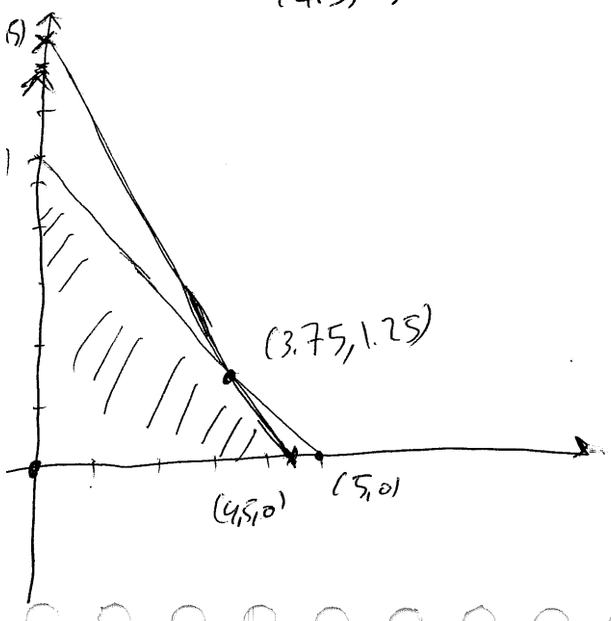
$x_2^3 = a_3 + \frac{F_1}{F_2}(b_3 - a_3) = 3.6$

$x_1^3 = x_2^3 = 3.6 \Rightarrow x^* = 3.6$

سؤال الخامس

نرسم المتباينة: $d_1: x_1 + x_2 = 5$ (0,5) (5,0)

$d_2: 10x_1 + 6x_2 = 45$ ، أي نقطة (0, 7.5) (4.5, 0)



d_1 و d_2 يتقاطعان في النقطة (3.75, 1.25)

Z	x_1	x_2
0	0	0
-22.5	9.5	0
-23.75	3.75	1.25
-20	0	5

$X^* = (3.75, 1$

$Z^* = -23.75$

السؤال الأول: g_1, g_2 دالة خطية، بما أن g_1 بصفة عامة فيمكن أن $\nabla g_1 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

يكون الشرط الكافي لتحقق شرط KKT هو $\det(\nabla^2 g_2 - \lambda I) = 0$ فالقيمة الذاتية $\lambda_1 = \lambda_2 = 2 > 0$

① $\nabla f(\bar{x}) + \lambda_1 \nabla g_1(\bar{x}) + \lambda_2 \nabla g_2(\bar{x}) = 0 \Leftrightarrow \begin{bmatrix} 2+2\lambda_1 x_1 + 2\lambda_2 \\ 1+2\lambda_1 x_2 - \lambda_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Leftrightarrow 2+2\lambda_1 x_1 + 2\lambda_2 = 0$

$1+2\lambda_1 x_2 - \lambda_2 = 0$

$\lambda_1 g_1 = 0 \Rightarrow \lambda_1 (x_1^2 + x_2^2 - 4) = 0$ ③ ، $\lambda_2 g_2 = 0 \Rightarrow \lambda_2 (x_1 - x_2) = 0$ ④

Case1: $\lambda_1 = \lambda_2 = 0 \Rightarrow \lambda = 0$ مرفوضة

Case2: $\lambda_1 = 0, x_1 - x_2 = 0 \Rightarrow x_1 = x_2$ ، بالتعويض في ①، ② نجد $\lambda_2 = -1$

Case3: $\lambda_2 = 0, x_1^2 + x_2^2 = 4 \Rightarrow x_1 = \frac{-1}{2\lambda_1}, x_2 = \frac{-1}{2\lambda_1}, \frac{1}{4\lambda_1^2} + \frac{1}{4\lambda_1^2} = 4 \Rightarrow \frac{5}{4\lambda_1^2} = 4$

$\lambda_1^2 = \frac{5}{16} \Rightarrow \lambda_1 = \pm \frac{\sqrt{5}}{4}$

الحل الممكن: $\lambda_1 = \frac{\sqrt{5}}{4}$ بالتالي: $x_1 = \frac{-4}{\sqrt{5}}$ ، $x_2 = \frac{-4}{2\sqrt{5}}$ إذا $x^* = (\frac{-4}{\sqrt{5}}, \frac{-2}{\sqrt{5}}, \frac{\sqrt{5}}{4}, 0)$

[3] $x_1 - x_2 = \frac{-2}{\sqrt{5}} < 0$, $\frac{16}{5} + \frac{9}{5} - 4 < 0$ حيث kkT شرط ⑤ محقق بالتالي $f(x^*) = \frac{-10}{\sqrt{5}}$ هي القيمة الدنيا

السؤال 2: نعوض أبعاد العلبة بدلالة x, y, z

$V(x,y,z) = xyz$

s.t $xy + 2yz + 2xz = 27$

$z = \frac{27 - xy}{2(x+y)}$

$\Rightarrow V = \frac{27xy - x^2y^2}{2(x+y)}$

$\frac{\partial V}{\partial x} = 0 \wedge \frac{\partial V}{\partial y} = 0 \Leftrightarrow \frac{x^2(27 - 2xy - y^2)}{2(x+y)^2} = 0 \wedge \frac{y^2(27 - 2xy - x^2)}{2(x+y)^2} = 0$

$\begin{cases} 27 - 2xy - x^2 = 0 \\ 27 - 2xy - y^2 = 0 \end{cases} \Leftrightarrow x = y$ ⑤ $x = 3, y = 3, z = 15$ وهذا الحل مرفوض لأن $x = y = 0$

$\begin{cases} \frac{\partial \ell}{\partial x} + \lambda \frac{\partial G}{\partial x} = 0 \\ \frac{\partial \ell}{\partial y} + \lambda \frac{\partial G}{\partial y} = 0 \\ xy + 2yz + 2xz = 27 \\ \frac{\partial \ell}{\partial z} + \lambda \frac{\partial G}{\partial z} = 0 \end{cases}$

$yz + \lambda(y + 2z) = 0$ ⑤

$xy + \lambda(x + 2z) = 0$ ⑥

$xy + \lambda(2y + 2x) = 0$ ⑦

$xy + 2yz + 2xz = 27$ ⑧

$xyz = -\lambda(xy + 2xz)$ ⑨

$xyz = -\lambda(xy + 2yz)$ ⑩

$xyz = -\lambda(2yz + 2xz)$ ⑪

من (6)، (5) نجد: $xz = yz$ ، بما أن $z \neq 0$ فإن $x = y$

بالتعويض في (7)، (6) نجد $y = 2z$ ومنه $x = y = 2z$ (4) بالتعويض في (8) نجد $12z^2 = 27$

$z = 15, x = y = 3$

السؤال الثالث: $\min f(x,y) = 4x^2 - 4xy + 2y^2$ ، $x_0 = (2,3)$

$x_1 = x_0 - t_0 \nabla f(x_0)$

$\nabla f(x) = \begin{bmatrix} 8x - 4y \\ -4x + 4y \end{bmatrix}$ ، $\nabla f(x_0) = \begin{bmatrix} 4 \\ 4 \end{bmatrix}$

$x_1 = \begin{bmatrix} 2 - 4t_0 \\ 3 - 4t_0 \end{bmatrix}$