كلية العلوم

القسم : **الرياضيات**

السنة : **الرابعة**

المادة : نظرية الاعداد

المحاضرة : الرابعة /نظري/

{{ مكتبة A to Z }}

Facebook Group : مكتبة A to Z

2025

يمكنكم طلب المحاضرات برسالة نصية (SMS) أو عبر (What's app-Telegram) على الرقم 0931497960

* التحليل إلى جداء عوامل أولية بطريقة فيرما:

أوجد فيرما طريقة لتحليل العدد الصحيح الموجب إلى عوامله الأولية حيث نتعامل فقط مع الأعداد الفردية، لأنه إذا كان n زوجي فيمكن بساطة أن نكتب بالشكل:

$$n = 2^i m$$

حيث m عدد فردي

عندئذ يمكن تحليل m إلى عوامله الأولية بطريقة فيرما حيث تعتمد طريقة فيرما على الحقيقة التالية:

مبرهنة

ليكن n عدد صحيح موجب فردي

عندئذ، n يكتب كحاصل ضرب عددين صحيحين موجبين a و b

إذا وفقط إذا أمكن كتابة n كفرق بين مربّعين عددين صحيحين

الإثبات:

$n = ab \Leftarrow$ a و b فرديان معاً

نلاحظ

$$\frac{a+b}{2} \quad , \quad \frac{a-b}{2}$$

أعداد صحيحة

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

$$\exists\ x = \frac{a+b}{2} \quad \& \quad y = \frac{a-b}{2}$$

$$\therefore n = x^2 - y^2$$

$\Rightarrow$ لدينا $n = x^2 - y^2$

$$= (x-y)(x+y)$$

$$= a \times b$$

* طريقة فيرما في تحليل العدد الفردي:

إن طريقة فيرما في تحليل العدد الفردي n موجب إلى جداء عاملين تعتمد على كتابة n بالشكل:

$$n = x^2 - y^2$$

$$x^2 - n = y^2$$

وتتلخص بالخطوات التالية:

1- نوجد أصغر عدد صحيح موجب k بحيث $k \geq \sqrt{n}$

2- نكتب بالتتالي

$k^2 - n$ ، $(k+1)^2 - n$ ، $(k+2)^2 - n$ ، ...

TEL:0931497960 - Facebook Group: A to Z مكتبة

فنلاحظ قيمة $m \geq \sqrt{n}$ يجعل $m^2 - 2$ مربع كامل

أي:

$$m^2 - n = d^2 \Rightarrow n = m^2 - d^2$$
$$= (m-d)(m+d)$$

إن خطوات العمل من دون شك منتهية لأنه لابد أن نصل إلى الخطوة الأخيرة

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

وعندها $n = n.1$

مما يدل على أنه أولي وذلك إذا لم نصل على (m^2-2) مربعاً كعدد صحيح من خطوة سابقة.

مثال:

حلّل العدد $n = 23449$ بطريقة فيرما

الحل:

$$\sqrt{n} = 153.13$$

$K \geq \sqrt{n}$ (عدد طبيعي)

$$K = 154$$

$$K^2 - n = (154)^2 - n = 267$$

ليس مربع كامل.

TEL:0931497960 - Facebook Group: A to Z مكتبة

$(k+1)^2 - n = (155)^2 - n$

$= 576 = (24)^2$

$n = (k+1)^2 - (24)^2$

$= (155)^2 - (24)^2$

$= (155 - 24)(155 + 24)$

$= 131 \times 179$

مثال:

حلّل العدد $n = 630$ الى جداء عواملها الأولية

الحل:

$n = 2 \times 315$

لتحلل العدد $m = 315$ بطريقة فيرما

$\sqrt{m} = 17.64$

$k \geq \sqrt{m}$ (عدد طبيعي)

$k = 18$

$k^2 - n = (18)^2 - 315$

$= 9 = 3^2$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$n = k^2 - 3^2$

$= 18^2 - 3^2$

$= (18-3)(18+3)$

$m = 315 = 15 \times 21$

$\Rightarrow m = 3^2 \times 5 \times 7$

$\Rightarrow n = 2 \times 3^2 \times 5 \times 7$

(وهي الصيغة القانونية لكتابة عدد)

مثال:

أثبت أن 43 عدد أولي باستخدام طريقة فيرما

الحل:

$n = 43$

$\sqrt{n} = 6.55$

$k \geq \sqrt{n}$

$k = 7$

$k^2 - n = 6$ ليس مربع كامل

$(k+1)^2 - n = 21$ ليس مربع كامل

$(k+2)^2 - n = 38$ ليس مربع كامل

$(k+3)^2 - n = 57$ ليس مربع كامل

TEL:0931497960 - Facebook Group: A to Z مكتبة

$(k+14)^2 - n = 398$ ليس مربع كامل

$(k+15)^2 - n = (22)^2 - 43$

$(22)^2 - n = 441 = (21)^2$

$n = 43 = (22)^2 - (21)^2$

$= (22-21)(22+21)$

$= 1 \times 43$

* التطابقات:

قدّم الرياضي الألماني غاوس (1777 - 1855)

مفهوم التطابق بالنسبة لمقياس عدد صحيح موجب m

يُعد مفهوم التطابق أداة قوية في برهان الكثير من المسائل الرياضية

تعريف

ليكن $a, b \in Z$ ، $m \in Z^+$

يُقال إن العدد a يطابق b بالمقياس m

ونكتب:

$a \equiv b \pmod{m}$

أو $a \underset{m}{\equiv} b$

إذا كان:

$m \mid (a-b)$ ($(a-b)$ يقسم m)

TEL:0931497960 - Facebook Group: A to Z مكتبة

ملاحظة

إذا كان $m \nmid (a-b)$

عندئذٍ:

$$a \not\equiv b \pmod{m}$$

$$21 \equiv 1 \pmod{5}$$
$$21 \equiv 1 \pmod{4}$$
$$21 \equiv 2 \pmod{3}$$
$$112 \equiv 7 \pmod{11}$$
$$21 \equiv -3 \pmod{6}$$

مبرهنة

إذا كان $a, b \in \mathbb{Z}$ ، $m \in \mathbb{Z}^+$

فإن:

$$a \equiv b \pmod{m} \iff \text{يوجد } q \in \mathbb{Z}$$

بحيث: $a = b + qm$

الإثبات:

$$a \equiv (\mathrm{mod}\, m) \Rightarrow m \mid (a-b)$$

$\Rightarrow$ يوجد $q \in \mathbb{Z}$ بحيث:

$$a - b = qm$$

TEL:0931497960 - Facebook Group: A to Z مكتبة

$\Rightarrow a = b + q\,m$

لدينا فرضاً $\Rightarrow$ $a = b + q\,m$ $\Leftarrow$

$a - b = q\,m$

$m \mid (a-b) \Leftarrow$

$a \equiv b \pmod{m} \Leftarrow$

* ملاحظات:

1- $\forall a, b \in \mathbb{Z} : a \equiv b \pmod{1}$

أي عددين صحيحين متطابقين بالقياس العدد 1 (بالقاس 1)

2- أي عدد صحيح a يطابق باقي قسمته على m بالقياس العدد m

$a = qm + r \quad ; \quad 0 \leq r < m$

$a \equiv r \pmod{m}$

3- $m \mid a \Leftrightarrow a \equiv 0 \pmod{m}$

TEL:0931497960 - Facebook Group: A to Z مكتبة

4- إذا كان $m \mid n$

وكان $a \equiv b \pmod{n}$

$\Rightarrow a \equiv b \pmod{m}$

5- إذا كان $a, b \in \mathbb{Z}$

فإن

$a \equiv b \pmod{m} \Leftrightarrow$

باقي قسمة a على m = باقي قسمة b على m

انتهت المحاضرة

TEL:0931497960 - Facebook Group: A to Z مكتبة