# المحاضرة السـابعـة

## الاعداد الاولية Prime Numbers:

تكمن اهمية الاعداد الاولية في تطبيقاتها الهندسية من جهة، واعتبارها حجر الاساس في بناء الاعداد الصحيحة من جهة اخرى.

---

**تعريف:**

2, 3, 5, 7, 11, 13, 17, 19,…..

(أ) يقال عن $P \in N^*$ أنه عدد أولي (Prime Number) ، إذا كان $p > 1$ ولا يقبل القسمة إلا على $P$ و $1$ .

(ب) يقال عن $1 < a \in Z$ ، أنه عـدد مؤلــف (Composite number) ، إذا كان $a$ عدداً غير أولي .

---

**ملاحظة:**

1- أي عدد صحيح أكبر من 1 وليس عدداً اولياً يقال له رقم مركب أو مؤلف ( Composite number)

2- الاعداد الاولية التي أصغر من 100 هي

| | | | | |
|---|---|---|---|---|
| 2 | 3 | 5 | 7 | 11 |
| 13 | 17 | 19 | 23 | 29 |
| 31 | 37 | 41 | 43 | 47 |
| 53 | 59 | 61 | 57 | 71 |
| 73 | 79 | 83 | 89 | 97 |

---

**امثلـة:**

1- بالأعداد 2, 3, 5, 7, 11, 13, 17, 19, 23 كلها اولية، بينما 6 عدد مؤلف لأنه يقبل القسمة على 2.

2- $5! + 2$ عدد مؤلف لأنه يقبل القسمة على **2**. لاحظ

$1 < 61 < 5! + 2 \;\&\; 5! + 2 = 2(61)$

**للتوضيح:** $i.e.\ 5! + 2 = 5.4.3.2.1 + 2 = 2(5.4.3.1 + 1) = 2(61)$

-3 $\mathbf{5! + 2}$ عدد مؤلف لأنه يقبل القسمة على **3**. لاحظ

$1 < 41 < 5! + 3 \;\&\; 5! + 3 = 3(41).$

---

**مبرهنة (14):** اذا كان $n > 2$، فأن n عدد مؤلف اذا وفقط اذا وجد $a, b \in Z$، بحيث أن $n = ab$، $1 < a < n$، $1 < b < n$. يسمى كل من a, b عامل من عوامل n.

**البرهان:**

إذا كان $n = ab$ ، $1 < a < n$ ، $1 < b < n$ ، فمن الواضح أن n عدد مؤلف . ولإثبات العكس نفرض أن n عدد مؤلف . إذاً يوجد $1 \neq a \neq n$ و $a \backslash n$ وعليه يوجد $b \in Z$ بحيث أن $n = ab$ ، لكن $n, a \in Z^+$ . إذاً $b \in Z^+$ ، وعليه فإن $1 \leq a$ ، $1 \leq b$ . لكن $a \backslash n$ و $b \backslash n$ . إذا $a \leq n$ و $b \leq n$ . لكن $a \neq 1$ ، $a \neq n$ . إذاً $1 < a < n$ . وإذا كان $b = 1$ ، فإن $a = n$ وهذا غير ممكن . إذاً $b \neq 1$ . وإذا كان $b = n$، فإن $a = 1$ وهذا غير ممكن . إذاً $1 < b < n$ .

---

**ملاحظة:**

كل الأعداد الأولية فردية ما عدا العدد 2 ، وكل منها على الشكل $4m + 1$ أو $4m - 1$ حيث $m \in Z^+$ ، لأن أي عدد صحيح يمكن كتابته بالشكل

$$4m\ ,\ 4m + 1\ ,\ 4m + 2\ ,\ 4m + 3\quad ،\quad m \in Z$$

لكن $4m$ ليس أولياً ، كما أن $2 \backslash 4m + 2$ ، وعليه فإن $4m + 2$ عدد أولي عندما $m = 0$ و 2 عدد أولي زوجي . إذاً أي عدد أولي فردي على الشكل

$4m+1$ ، $4m+3$ . لكن $S=\{4m+3 \mid m\in n\}=\{4m-1 \mid m\in n^*\}$

إذاً كل عدد أولي فردي على الشكل $4m-1$ أو $4m+1$ ، $m\in n^*$

ولأهمية الأعداد الأولية وضع العلماء تخمينـــات (Conjectures) كثيـــرة عليهـــا منها :

(أ) يوجد عدد لا نهائي من الأعداد الأولية على الشكل $n^2+1$ ، $n\in n^*$

وهذا الحدس أو التخمين لم يثبت بعد . لاحظ أن $2=1^2+1$ ، $5=2^2+1$ ، $17=4^2+1$ ، $37=6^2+1$ ، $197=(14)^2+1$ .

(ب) حدس جولدباخ (١٦٩٠-١٧٦٤م) عام ١٧٤٢م :

يمكن التعبير عن أي عدد صحيح زوجي أكبر من 2 كمجموع عـــددين أوليين .

لاحـــــــــــظ أن $4=2+2$ ، $6=3+3$ ، $8=3+5$ ، $1=3+7$ ، $12=5+7$ ، $14=7+7$ ، $16=5+11$ .

وإذا كان حدس جولدباخ صحيحا ، فإن ذلك يعني أنه يمكن العبير عـــن أي عدد فردي أكبر في 5 كمجموع ثلاثة أعداد فرديـــة ، لأن إذا كـــان $n>5$ عدداً فردياً فإن $n-3$ عدد زوجي أكبر من 2 وعليه فإن $n-3=p+q$ ، حيث $p,q$ عددين أوليين وبالتالي فإن $n=p+q+3$ .

(ج) يوجد عدد لا نهائي من الأعداد الأولية على الشكل $p,p+2$ ، حيث $p$ عـــدد أولي . يـــسمى مثـــل تلـــك الأعـــداد أعـــداد أوليـــة توأميـــه (Twin primes). مثل $3,5$ ، $11,13$ ، $17,19$ .

(د) تخمين أو حدس الفرنسي لاجرانج (١٧٣٦-١٨١٣) عام ١٧٧٥م : إذا كان $n$ عدداً صحيحاً فردياً أكبر من 5 ، فإن $n=p_1+2p_2$ ، حيث $p_1$، $p_2$ عددين أوليين .

---

**تعريف:**

الترتيب الطبيعي للأعداد الأولية هو $p_1=2,p_3=5,\cdots,p_n,\cdots$ ويـــسمى $p_n$ العدد الأولى النوني في الترتيب الطبيعي .

---

**مبرهنة (15):** $P_n \leq 2^{2^{n-1}}$ لكل $n \in N^*$.

---

**نتيجة (3):**

إذا كان $n \geq 1$ عددا صحيحا ، فيوجد على الأقل $n+1$ من الأعداد الأولية كـل منها أقل من $2^{2^n}$ .

---

**مبرهنة (16):**

(أ) إذا كان $a,b \in Z$ ، $p$ عدداً أولياً كان $p \backslash ab$ فإما $p \backslash a$ أو $p \backslash b$ .

(ب) إذا كان $a_1,\cdots,a_n \in Z$ و $p$ عدداً أولياً وكان $p \backslash a_1a_2\cdots a_n$ فإن $p \backslash a_i$ لبعض قيم $1 \leq i \leq n$ .

---

**مبرهنة (17):**

(أ) كل عدد صحيح أكبر من الواحد يقبل القسمة على عدد أولي .

(ب) مجموعة الأعداد الأولية لا نهائية .

(ج) اذا كان $n > 1, a > 1$ عددين صحيحين وكان $a^n - 1$ عددا اولياً، فان a=2 وn عدد اولي.

---

**نتيجة (4):**

لكل عدد مؤلف $n$ قاسم أولي $p$ بحيث أن $p \leq \sqrt{n}$ .

---

**نتيجة (5):**

إذا لم يكن للعدد $n > 1$ قاسماً أولياً أقل من أو يساوي $\sqrt{n}$ ، فإن $n$ عدد أولي

**البرهان:** نفرض ان n عدد غير اولي. اذا n عدد مؤلف وعليه يوجد عدد اولي p بحيث ان $p \backslash n$ وحسب نتيجة (4)، $p \leq \sqrt{n}$ وهذا تناقض.

---

**مثال:** 1- **أثبت أن 257 عدد اولي**

$$\because\ \mathbf{16} < \sqrt{\mathbf{257}} < \mathbf{17}$$

الاعداد الاولية اقل او تساوي $\sqrt{257}$ هي 13 ,11 ,7 ,5 ,3 ,2.

257= 128(2) + 1

257= 85(3) + 2

257= 51(5) + 2

257= 36(7) + 5

257= 23(11) + 4

257= 9(13) + 10

∴257 لايقبل القسمة على اي من 13 ,11 ,7 ,5 ,3 ,2، فهو عدد اولي.

**2-هل العدد 175 عدد اولي؟**

$$\because\ \mathbf{13} < \sqrt{\mathbf{175}} < \mathbf{14}$$

الاعداد الاولية اقل او تساوي $\sqrt{175}$ هي 11 ,7 ,5 ,3 ,2.

175= 87(2) + 1

175= 58(3) + 3

175= 35(5) + 0

∴175 يقبل القسمة على 5، وعليه فأن 175 ليس عدد اولي.

---

**:H.W.** 1- هل الاعداد الاتية اعداداً اولية:

307 -4 461 -3 239 -2 13345 -1