كلية علوم الحاسوب والرياضيات

قسم الرياضيات

المرحلة الثالثة

نظريـة الاعـداد
Number Theory

2025-2024

أ. د. غادة مؤيد النعيـمي

المحاضرة الاولى

مقدمـــة:

العدد هو لغة العلم، وأفضل وسيلة للتعبير عنه هو الرموز، والارقام هي اشكال تكتب بها رموز الاعداد، والحساب او نظرية الاعداد. جانبه النظري يعالج الارقام والاعداد، مراتبها والنسب التي بينها وتكرارها على نسق معين، وانواعها وكيفية بانئها ودراسة خواصها والعلاقات بينها، وجانبه العملي يتناول الحسبان، ومعرفة المطلوب بالعمليات الاربعة.

نظرية الاعداد تعنى بدراسة الاعداد الصحيحة وخواصها. أن اهتمام الانسان بدراسة الاعداد يرجع الى قدم العصور وتشهد الاثار التي عثر عليها على ماقام به البابليون وقدماء المصريين والهنود والصينيون في هذا المضمار. كما ساهم الاغريق في اثراء هذا العلم منذ انشاء مدرسة فيثاغورس قبل 2500 عام ق. م. ومن اكبر انجازاتهم ماقدمه اقليدس الذي عاش في القرن الرابع قبل الميلاد، اذ كان اول من برهن على وجود عدد غير منته من الاوليات كما قدم طريقة حسابية لايجاد القاسم المشترك الاعظم لعددين بالاضافة الى نتائج اخرى ذكرها في كتبه الثلاثة عشر في الرياضيات (العناصر). وبعد الاغريق جاء دور العرب والمسلمين في تطوير المعرفة الانسانية بالاعداد، ويبدو هذا جلياً من خلال بعض المصطلحات التي مازالت تستخدم الى يومنا هذا، فكلمة (Algorithm) والتي تعني طريقة الحساب هي تحريف لكلمة خوارزم او بالاحرى الخوارزمي وهو العالم الرياضي المعروف (ابو عبدالله محمد بن موسى الخوارزمي الذي عاش في القن الثالث الهجري، ولقد كان كتابه "الجبر والمقابلة" من افضل كنب الرياضيات المؤلفة في ذلك العصر.

ان النظام العشري للاعداد الذي نستخدمه في عصرنا الحاضر هو نظام طوره العرب والمسلمون بعد ان ابتدعه الهنود ولايزال الغربيون يشيرون الى رموز 1, 2, 3, ..., 8, 9 بالارقام العربية.

Number Theory

ان قدم علم الاعداد لايعني انه علم جامد لايواكب العصر، بل ان التقنيات الحديثة وخاصة الحاسوب ابرزت اهمية هذا العلم وتفاعلت معه. فالتقدم الهائل في علم الحاسوب يبرز اهمية خواص الاعداد ودؤاستها. ومن ناحية اخرى ساهمت الحواسيب السريعة في تقدم نظرية الاعداد خلال التعرف على بعض خواصها وصياغة بعض الاحداس. كذلك برزت اهمية دراسة الاعداد في علم التعمية وموضوع امن المعلومات.

$$\mathbb{N} = \{1, 2, 3, \cdots\} \quad (\text{the } \textbf{natural numbers} \text{ or } \textbf{positive integers})$$
$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\} \quad (\text{the } \textbf{integers})$$
$$\mathbb{Q} = \left\{\frac{n}{m} \mid n, m \in \mathbb{Z} \text{ and } m \neq 0\right\} \quad (\text{the } \textbf{rational numbers})$$
$$\mathbb{R} = \text{the } \textbf{real numbers}$$

Note that $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

الاعداد الطبيعيـة والصحيـحـة:

هي مجموعة الاعداد الطبيعية الموجبة والصفر ويرمز لها بالرمز N حيث أن:

$$N = \{0,1, 2, 3, \dots\}$$

اما العداد الطبيعية بدون 0، فتعرف بـ:

$$N^* = \{1, 2, 3, \dots\} = N - \{0\}$$

هي مجموعة الاعداد الصحيحة الموجبة ومجموعة الاعداد الصحيحة السالبة والصفر ويرمز لها بالرمز Z حيث أن:

$$Z = \{0, \pm1, \pm2, \pm3, \dots\}$$

اما العداد الصحيحة بدون 0، فتعرف بـ:

$$Z^* = \{\pm1, \pm2, \pm3, \dots\} = Z - \{0\}$$

والاعداد الطبيعية الموجبة، فتعرف بـ:

$$Z^+ = \{1, 2, 3, \dots\}$$

والاعداد الطبيعية السالبة، فتعرف بـ:

$$Z^- = \{-1, -2, -3, \dots\}.$$

خواص الاعداد الصحيحة:

يمكن بناء الاعداد الصحيحة من مجموعة الاعداد الطبيعية

$$N = \{1, 2, 3, \dots\}$$

حيث اننا نستنتج منها الخواص التالية:

إذا كان $a, b, c \in Z$ فإن :

1) $a \cdot b = b \cdot a , a + b = b + a$

أي أن جمع وضرب الأعداد الصحيحة إبدالي

2) $(a \cdot b) \cdot c = a \cdot (b \cdot c) , (a + b) + c = a + (b + c)$

أي أن جمع وضرب الأعداد الصحيحة تجميعي

3) $a \cdot 1 = 1 \cdot a = a , a + 0 = 0 + a = a$

4) $\forall a \epsilon Z \; \exists -a \epsilon Z \; st: a + (-a) = (-a) + a = 0$

5) $(a + b) \cdot c = a \cdot c + b \cdot c , a \cdot (b + c) = a \cdot b + a \cdot c$

أي أن الضرب توزيعي على الجمع .

6) إذا كان : $a + b = a + c$ فإن: $b = c$

7) لكل $a, b \in N$ نجد ان $a + b \in N , a \cdot b \epsilon N$

مبرهنة:

أ) إذا كان : $a,b,c \in Z$ وكان : $a < b$ و $b < c$ فإن : $a < c$.

ب) إذا كان : $a,b,c \in Z$ وكان $a < b$ و $c > 0$ فإن $ac < bc$.

ج) إذا كان : $a , b \in Z$ فواحدة فقط من هذه العبارات صحيحة : إما $a < b$ او $a = b$.

البرهان:

أ) بما أن $b - a \in N^* \Leftrightarrow a < b$ و $b < c$ إذا $c - b \in N^*$

$(c - b) + (b - a) \in N^*$ وعليه فان : $c - a \in N^*$ ومنه ينتج أن : $a < c$

ب) بما أن : $a < b \Leftrightarrow b - a \in N^*$ وبما أن : $c \in N^*$ إذن :

$(b - a)\, c = bc - ac \in N^*$ وعليه فإن : $ac < bc$.

ج) نفرض أن : $a < b$ و $a = b$ إذا : $b < b$ وهذا تناقض وإذا كان : $a > b$ فإن : $a = b$ و $b > b$ وهذا تناقض أيضا .أما إذا كان :

$a < b$ و $a > b$ فإن : $a < a$ حسب (أ) وهذا تناقض أيضا : إذن واحدة فقط من العبارات أعلاه صحيحة

مبرهنة:

إذا كان $a, b \in Z$ فإن

أ) $|a| \geq 0$

ب) $|a| = 0 \Leftrightarrow a = 0$

ج) $-|a| \leq a \leq |a|$

د) $|-a| = |a|$

ه) $|ab| = |a|\,|b|$

و) $b \leq a \leq b \Leftrightarrow |a| \leq b$

ز) $|a + b| \leq |a| + |b|$

ح) $|a - b| \geq |a| - |b|$

البرهان:

أ) إذا كان :$a \geq 0$ فإن : $|a| = a \geq 0$ و إذا كان : $a < 0$ فإن : $|a| = -a > 0$ إذن $|a| \geq 0$.

ج) نفرض أن : $a \geq 0$ اذن $|a| = a$ وعليه فإن : $|a| \geq 0$ ومنه ينتج أن : $-|a| \leq 0$ اذن :

$$-|a| \leq a \leq |a| \text{ وعليه فإن : } -|a| \leq 0 \leq a = |a|$$

أما إذا كان : $a < 0$ فإن : $-a < 0$ وعليه فإن : $|a| = -a > 0$ ومنه ينتج أن :

$$-|a| \leq a \leq |a| \text{ وعليه فإن : } -|a| = a < 0 < -a = |a| \text{ إذن : } -|a| < 0$$

ه) إذا كان : $a, b \geq 0$ فإن : $ab \geq 0$ وعليه فإن : $|a| = a\,,\ |b| = b$ ومنه ينتج أن :

$$|ab| = ab = |a||b| \text{ وإذا كان: } a \geq 0\,, b < 0 \text{ فإن : } ab < 0 \text{ وعليه فإن :}$$

$$a < 0\,, b \geq 0 \text{ وإذا كان : } |ab| = a(-b) = |a||b| \text{ إذن : } |a| = a\,, |b| = -b$$

فإن : $ab < 0$ و $|b| = b$ و $|a| = -a$ وعليه فإن : $|ab| = -(ab) = (-a)b = |a||b|$

وإذا كان : $a, b < 0$ فإن : $|b| = -b$ و $|a| = -a$ وعليه فإن : $|ab| = ab$ ومنه يبتج أن :

$$|ab| = |a||b|$$

(هـ) إذا كان $a \geq 0$ ، $b \geq 0$ ، فإن $ab \geq 0$ وعليه فإن $|a| = a$ ، $|b| = b$ ومنه ينتج أن $|ab| = ab = |a|\,|b|$. وإذا كان $a \geq 0$، $b < 0$، فإن $ab < 0$، وعليه فإن $|a| = a$ ، $|b| = -b$. إذاً $|ab| = a(-b) = |a|\,|b|$. وإذا كان $a < 0$ ، $b \geq 0$ ، فإن $ab < 0$ و $|a| = -a$ و $|b| = b$ ، وعليه فإن $|ab| = -(ab) = (-a)b = |a|\,|b|$. وإذا كان $a < 0$ ، $b < 0$، فإن $ab > 0$ ، $|a| = -a$ ، $|b| = -b$ ، وعليه فإن $|ab| = ab$ ومنه ينتج أن $|ab| = |a|\,|b|$

(ز) بما أن $|a| \leq a \leq |a|$ و $-|b| \leq b \leq |b|$ حسب (ج) . إذاً $-(|a| + |b|) \leq a + b \leq |a| + |b|$ وحيث أن $a, b \in Z$. إذاً إما $a + b \geq 0$ أو $a + b < 0$ فإذا كان $a + b \geq 0$ ، فإن $|a + b| = a + b$ وعليه فإن $|a + b| \leq |a| + |b|$ أما إذا كان $a + b < 0$ ، فإن $|a + b| = -(a + b)$. لكن $a + b \leq -(|a| + |b|)$. إذاً $|a| + |b| \geq -(a + b)$ ، وعليه فإن $|a + b| \leq |a| + |b|$.

ز) بما أن : $-|b| \leq b \leq |b|$ and $a \leq |a| \leq a$ حسب (ج) إذن :

$-(|a| + |b|) \leq a + b \leq |a| + |b|$ وحيث أن : $a, b \in Z$ إذا إما :

$a + b \geq 0$ أو $a + b < 0$ فاذا كان $a + b \geq 0$ فإن $|a + b| = a + b$

وعليه فإن $|a + b| \leq |a| + |b|$ أما إذا كان $a + b < 0$

فإن $|a + b| = -(a + b)$ لكن $a + b \leq -(|a| + |b|)$ إذن

$|a| + |b| \geq -(a + b)$ وعليه فإن $|a + b| \leq |a| + |b|$
