

الحساب المقاسي

Modular Arithmetic

يمكن أن يكون البحث في هذا المجال من الحساب في عصر الكمبيوتر ممل أو فيه نوع من عدم الاستفادة ، لكن مهمى تطورت التقنيات لا يمكن الاستغناء عن الطرق الفكرية و العقلية التي كان لها الدور المهم في ترقى هذه التقنيات . الحساب المقاسي هو طريقه و يمكن القول عنه هو نظريه يمكن من خلالها الخوض في عالم الأعداد .

يعتبر الحساب المقاسي من المواضيع المهمة في نظرية الأعداد ، و من خلاله يمكن حساب قابلية القسمة بين الأعداد و باقي تقسيم عدد على عدد آخر . أول من أدخل هذه الطريقة في نظرية الأعداد هو عالم الرياضيات الألماني غاوس (Carl Friedrich Gauss) و أستعمل علامة التكافئ (\equiv) في روابط هذا الحساب عوضاً عن علامة التساوي (=) . هناك أعداد عظيمة و كبيرة جداً لا يمكن معرفة قابلية تقسيمها على عدد آخر حتى من خلال الحاسوب لكن من خلال هذا الحساب البسيط يمكن معرفة قابلية القسمة و بسرعة عالية جداً . كذلك ساهم الحساب المقاسي في تطور نظرية الأعداد الأولى و هناك قضايا عديدة في نظرية الأعداد الأولى يمكن البحث فيها من خلال هذا الحساب .

الحساب المقاسي في نظرية الأعداد هو للأعداد الصحيحة فقط أي الأعداد الطبيعية السالبة

و الموجبه و الصفر أي : $Z = \dots, -2, -1, 0, 1, 2, \dots$

إذا كان باقي تقسيم العدد a على العدد n هو العدد b في هذه الحالة يمكن كتابة العدد a بهذه الطريقة :

$$a = n \times r + b \Rightarrow a \equiv b \pmod{n}$$

هذا التعبير $a \equiv b \pmod{n}$ هو جوهر العمليات الحسابية في الحساب المقاسي ، و من خلال هذا التعبير أو التعريف يمكن أستنتاج بعض الروابط ، سنستعرض هذه الروابط بعد مثال بسيط يبين الأرتباط العددي في هذه الرابطة .

مثال :

$$11 \equiv 3 \times 2 + 5 \Rightarrow 11 \equiv 5 \pmod{3}$$

$$11 \equiv 3 \times 4 - 1 \Rightarrow 11 \equiv -1 \pmod{3} \quad a = n \times r - b \Rightarrow a \equiv -b \pmod{n}$$

أهم الروابط في الحساب المقاسي :

$$\left. \begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array} \right\} \Rightarrow a \equiv c \pmod{n}$$

$$\left. \begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array} \right\} \Rightarrow a \pm c \equiv b \pm d \pmod{n}$$

$$\left. \begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array} \right\} \Rightarrow a \times c \equiv b \times d \pmod{n}$$

لكل عدد يمكن كتابة هذه الرابطة : $a \equiv a \pmod{n}$

إذا كان العدد a يقبل القسمة على n إذن : $a \equiv 0 \pmod{n}$

من الروابط المهمة في الحساب المقاسي هذه الرابطة و نذكرها مع الأثبات لها :

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

أثبات :

$$a \equiv n \times r + b \Rightarrow a^m \equiv (n \times r + b)^m \Rightarrow a^m \equiv (n \times r)^m + (n \times r)^{m-1} \times b + \dots + b^m$$

إذن :

$$a^m \equiv n \times (n^{m-1} \times r^m + n^{m-2} \times r^{m-1} \times b + \dots) + b^m$$

$$a^m \equiv b^m \pmod{n}$$

■

مثال : ما هو باقي تقسيم العدد $5^{9n+1} - 7 \times 2^{10n+3}$ على 32 ؟

$$5^3 \equiv 1 \pmod{31} \Rightarrow (5^3)^{3n} \equiv 1 \pmod{31} \Rightarrow 5^{9n+1} \equiv 5 \pmod{31}$$

$$2^5 \equiv 1 \pmod{31} \Rightarrow (2^5)^{2n} \equiv 1 \pmod{31} \Rightarrow 2^{10n+3} \equiv 8 \pmod{31}$$

$$5^{9n+1} - 7 \times 2^{10n+3} \equiv 5 - 56 \pmod{31} \equiv -51 \pmod{31}$$

إذن :

$$5^{9n+1} - 7 \times 2^{10n+3} \equiv -51 \pmod{31}$$

و بما أن :

$$11 \equiv -51 \pmod{31}$$

لذلك :

$$5^{9n+1} - 7 \times 2^{10n+3} \equiv 11 \pmod{31}$$

إذن باقي التقسيم يساوي 11 .

الحساب المقاسي على الدوال العددية :

$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{n} \\ a_2 \equiv b_2 \pmod{n} \\ \cdot \\ \cdot \\ \cdot \\ a_m \equiv b_m \pmod{n} \end{array} \right\} \Rightarrow \begin{cases} a_1 + a_2 + \dots + a_m \equiv b_1 + b_2 + \dots + b_m \pmod{n} \\ a_1 \times a_2 \times \dots \times a_m \equiv b_1 \times b_2 \times \dots \times b_m \pmod{n} \end{cases}$$

إذن :

$$a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}$$

مثال :

نفرض هذه الدالة

$$F(x) = x^3 + 4x^2 + 5x - 1$$

إذا كان $13 \equiv 1 \pmod{3}$ إذن :

$$\left. \begin{array}{l} f(13) = 13^3 + 4 \times 13^2 + 5 \times 13 - 1 \\ f(1) = 1^3 + 4 \times 1^2 + 5 \times 1 - 1 \end{array} \right\} \Rightarrow f(13) \equiv f(1) \pmod{3}$$

إذن :

$$2937 \equiv 9 \pmod{3}$$

كذلك يمكن كتابة هذه الرابطة بهذا الشكل :

$$2937 \equiv 0 \pmod{3}$$

و هذا بمعنى أن العدد 2937 يقبل القسمة على 3 .

بعض أهم القضايا في الحساب المقاسي :

■ قضية فرما الصغيرة : إذا كان P عدداً أولياً و a لا يقبل القسمة على P ، في هذه الحالة :

$$a^{P-1} \equiv 1 \pmod{P}$$

مثال : باقي تقسيم العدد 2^{1137} على 17 ؟

العدد 2^{1137} كبير جداً ، لكن باستعانة قضية فرما الصغيرة هذه يمكن كتابة

$$2^{16} \equiv 1 \pmod{17}$$

لذلك :

$$2^{16} \equiv 1 \pmod{17} \Rightarrow (2^{16})^{71} \times 2^1 \equiv 2^1 \pmod{17} \Rightarrow 2^{1137} \equiv 2 \pmod{17}$$

و باقي التقسيم يساوي 2 .

■ قضية ويلسن : إذا كان P عدداً أولياً في هذه الحالة :

$$(P-1)! \equiv -1 \pmod{P}$$

مثال : إذا كانت P تساوي 7 إذن :

$$1 \times 2 \times 3 \times 4 \times 5 \times 6 \equiv -1 \pmod{7} \Rightarrow 720 \equiv -1 \pmod{7}$$

و هذا بمعنى أن 721 يقبل القسمة على 7 .

■ **قضيه** : إذا كان P عدد أولي فردي تصدق هذه الرابطة :

$$x^2 \equiv -1(\text{mod } p)$$

إلا إذا كان :

$$p \equiv 1(\text{mod } 4)$$

مثال : $p=13$

$$13 = 4 \times 3 + 1 \Rightarrow 13 \equiv 1(\text{mod } 4)$$

إذن :

$$5^2 \equiv -1(\text{mod } 13)$$

أي:

$$25 = 13 \times 2 - 1$$



موقع جلال الحاج عبد

www.jalalalhajabed.com

البريد الإلكتروني :

jalal.alhajabed@hotmail.com

jalal.alhajabed@yahoo.com