الحسابيات

1) تذكير:

قابلية القسمة في $\mathbb{Z}$

ليكن a **و** b **من** $\mathbb{Z}$ **نقول أن** b **يقسم** a **و نكتب** b/a **إذا وجد** k **من** $\mathbb{Z}$ **بحيث :** $a=kb$

- ❖ $(\forall a\in\mathbb{Z})\quad a/a$
- ❖ $(\forall (a,b,c)\in\mathbb{Z}^3)\quad \begin{cases} a/b \\ b/c \end{cases} \Rightarrow a/c$
- ❖ $(\forall (a,b)\in\mathbb{Z}^2)\quad \begin{cases} a/b \\ b/a \end{cases} \Rightarrow |a|=|b|$

القسمة الأقليدية في $\mathbb{Z}$

ليكن a **من** $\mathbb{Z}$ **و** b **من** $\mathbb{N}^*$ **يوجد زوج وحيد** (q,r) **من** $\mathbb{Z}\times\mathbb{N}$ **بحيث :** $\begin{cases} a=bq+r \\ 0\leq r<b \end{cases}$

2) الموافقة بترديد n

ليكن $n\in\mathbb{N}$ **و** a **و** b **من** $\mathbb{Z}$
نقول إن a **يوافق** b **بترديد** n **إذا وفقط إذا كان** $n/a-b$ **و نكتب** $a\equiv b\,[n]$

- ❖ $\forall a\in\mathbb{Z}\quad a\equiv a\,[n]$
- ❖ $\forall (a,b)\in\mathbb{Z}^2\quad a\equiv b\,[n]\Rightarrow b\equiv a\,[n]$
- ❖ $\forall (a,b,c)\in\mathbb{Z}^3\quad \begin{cases} a\equiv b\,[n] \\ b\equiv c\,[n] \end{cases} \Rightarrow a\equiv c\,[n]$
- ❖ **ليكن** $n\in\mathbb{N}^*$ **و** a **من** $\mathbb{Z}$
  إذا كان r **هو باقي قسمة** a **على** n **فإن** $a\equiv r\,[n]$
- ❖ **ليكن** $n\in\mathbb{N}^*$ **و** a **و** b **من** $\mathbb{Z}$
  إذا كان r **هو باقي قسمة** a **على** n **و** r' **هو باقي قسمة** b **على** n
  فإن : $a\equiv b\,[n]\Leftrightarrow r=r'$

❖ **ليكن** $n \in \mathbb{N}$

$$\forall (a,b,c,d) \in \mathbb{Z}^4 \quad \begin{cases} a \equiv b\,[n] \\ c \equiv d\,[n] \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d\,[n] \\ ac \equiv bd\,[n] \end{cases}$$

$$\forall (a,b,c) \in \mathbb{Z}^3 \quad a \equiv b\,[n] \Rightarrow \begin{cases} a+c \equiv b+c\,[n] \\ ac \equiv bc\,[n] \end{cases}$$

$$\forall (a,b) \in \mathbb{Z}^2 ; (\forall m \in \mathbb{N}) \quad a \equiv b\,[n] \Rightarrow a^m \equiv b^m\,[n]$$

مجموعة أصناف تكافؤ

ليكن $n \in \mathbb{N}$ **و ليكن** $x \in \mathbb{Z}$

نسمي صنف تكافؤ x **المجموعة التي نرمز لها ب** $\overline{x}$ **أو** $\dot{x}$ **و هي معرفة بما يلي :** $\overline{x} = \{ y \in \mathbb{Z} / y \equiv x\,[n] \}$

ليكن $n \in \mathbb{N}$ **و ليكن** $x \in \mathbb{Z}$ **و** $y \in \mathbb{Z}$

- $\overline{x} = \{ x + nk / k \in \mathbb{Z} \}$
- $\overline{x} = \overline{y} \Leftrightarrow x \equiv y\,[n]$
- $\overline{x} \cap \overline{y} = \varnothing \Leftrightarrow x \not\equiv y\,[n]$
- $\mathbb{Z}/n\mathbb{Z} = \{ \overline{0}, \overline{1}, \overline{2}, \ldots\ldots, \overline{n-1} \} \quad (n \in \mathbb{N}^*)$
- $\overline{x} + \overline{y} = \overline{x+y}$
- $\overline{x} . \overline{y} = \overline{x.y}$

3) القاسم المشترك الأكبر

ليكن a و b عددين صحيحين نسبيين غير منعدمين

- نرمز للقاسم المشترك الأكبر ل a و b ب : $\Delta(a,b)$ أو $p\gcd(a,b)$ أو $a \wedge b$ و هو أكبر قاسم مشترك موجب قطعا للعددين a و b

- ليكن a و b من $\mathbb{Z}^*$
إذا كان $a \wedge b = d$ فإنه يوجد زوج (u,v) من $\mathbb{Z}^2$ بحيث : $d = au + bv$
- ليكن a و b من $\mathbb{Z}^*$ و $a \wedge b = d$
$$\begin{cases} d'/a \\ d'/b \end{cases} \Leftrightarrow \quad d'/d$$
- خوارزمية أقليدس
ليكن a و b من $\mathbb{N}^*$
إذا كان r هو باقي قسمة a على b ($\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$) فإن $a \wedge b = b \wedge r$
- ليكن a و b من $\mathbb{N}^*$
القاسم المشترك الأكبر لعددين a و b هو آخر باقي غير منعدم في القسمات المتتالية

4) المضاعف المشترك الأصغر:

ليكن a و b عددين صحيحين نسبيين غير منعدمين

- نرمز للمضاعف المشترك الأصغر ل a و b ب : $M(a,b)$ أو $pp\,cm(a,b)$ أو $a \vee b$ و هو أصغر مضاعف مشترك موجب للعددين a و b

- ليكن a و b من $\mathbb{Z}^*$ و $m = a \vee b$
$$\begin{cases} a/m' \\ b/m' \end{cases} \Rightarrow m/m'$$
- $(a \wedge b) \times (a \vee b) = |ab|$
- $(ac \vee bc) = |c|.(a \vee b)$

5) الأعداد الأولية فيما بينها :

❖ ليكن a و b من $\mathbb{Z}^*$
a و b أوليان فيما بينهما إذا وفقط إذا كان $a \wedge b = 1$

مبرهنة بوزو (Bezout)

ليكن a و b من $\mathbb{Z}^*$

$$a \wedge b = 1 \Leftrightarrow \left(\exists(u,v) \in \mathbb{Z}^2\right), au + bv = 1$$

❖ ليكن a و b و c من $\mathbb{Z}^*$

$$ac \wedge bc = |c|.(a \wedge b)$$

❖ ليكن a و b من $\mathbb{Z}^*$ و $d \in \mathbb{N}^*$

$$a \wedge b = d \Leftrightarrow \begin{cases} d/a \quad ; \quad d/b \\ \dfrac{a}{d} \wedge \dfrac{b}{d} = 1 \end{cases}$$

❖ ليكن a و b و c من $\mathbb{Z}^*$

لدينا :

$$\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow \quad a \wedge bc = 1$$

مبرهنة كوص (Gauss)

ليكن a و b و c من $\mathbb{Z}^*$

$$\begin{cases} a/c \\ b/c \\ a \wedge b = 1 \end{cases} \Rightarrow \quad ab/c$$

ليكن a و b من $\mathbb{Z}^*$ و $n \in \mathbb{N}^*$

$$\begin{cases} ax \equiv ay\,[n] \\ a \wedge n = 1 \end{cases} \Rightarrow \quad x \equiv y\,[n]$$

6) الأعداد الأولية :

❖ **ليكن** $p \in \mathbb{Z}^* \setminus \{-1,1\}$

نقول أن p **أولي إذا وفقط إذا كان له أربع قواسم بالضبط :** 1 **و** -1 **و** p **و** $-p$

ملاحظة :

- **إذاكان** p **أولي فإن** $-p$ **أولي**
- **طريقة لتحديد الأعداد الأولية الموجبة :**

ليكن $n \in \mathbb{N}^* \setminus \{1\}$
للتحقق هل n **أولي :**

- **أولا نحسب** $\sqrt{n}$
- **ثانيا نحدد جميع الأعداد الأولية الأصغر من** $\sqrt{n}$
- **إذا كان** n **لا يقبل القسمة على أي من هذه الأعداد الأولية الأصعر من جدر مربعه فهو يكون أوليا أما إذا قبل القسمة على أحدها فهو غير أولي**

✓ **ليكن** a_1 ، a_2 ، .... ، a_n **من** $\mathbb{Z}$ **و** p **عدد أولي**

$$p / a_1 \times a_2 \times ..... \times a_n \Rightarrow \left(\exists i \in \{1,2,.....,n\}\right) : p / a_i$$

✓ **ليكن** p ، p_1 ، p_2 ، .... ، p_n أعداد أولية

$$p / p_1 \times p_2 \times ..... \times p_n \Rightarrow \left(\exists i \in \{1,2,.....,n\}\right) : |p| = |p_i|$$