

## الحسابيات

### I- قابلية القسمة في $\mathbb{Z}$

#### 1- تعريف

ليكن  $a$  و  $b$  من  $\mathbb{Z}$   
 نقول إن  $b$  يقسم  $a$  و نكتب  $b/a$  إذا وجد  $k$  في  $\mathbb{Z}$  حيث  $a = kb$   
 $(a; b) \in \mathbb{Z}^2 \quad b/a \Leftrightarrow \exists k \in \mathbb{Z} \quad a = kb$

#### 2- ملاحظات

\*- إذا كان  $b$  يقسم  $a$  إننا نقول إن  $b$  قاسم لـ  $a$  أو  $a$  مضاعف لـ  $b$   
 \*- ليكن  $b \in \mathbb{Z}$  مجموعة مضاعفات العدد  $b$  هي المجموعة  $b \cdot \mathbb{Z} = \{k \cdot b / k \in \mathbb{Z}\}$   
 \*- ليكن  $a \in \mathbb{Z}^*$   $b \in \mathbb{Z}$  :  $b/a \Rightarrow |b| \leq |a|$

#### 3- خاصيات العلاقة " $b/a$ "

\*-  $a/a \quad \forall a \in \mathbb{Z}$  نقول إن العلاقة " $b/a$ " انعكاسية  
 \*-  $\left\{ \begin{array}{l} b/a \\ a/c \end{array} \Rightarrow b/c \right.$   $\forall (a; b; c) \in \mathbb{Z}^3$  نقول إن العلاقة " $b/a$ " متعدية  
 \*-  $\left\{ \begin{array}{l} b/a \\ a/b \end{array} \Rightarrow |a| = |b| \right.$   $\forall (a; b; c) \in \mathbb{Z}^3$

#### ملاحظة

$\forall (a; b; c) \in \mathbb{N}^3$  نقول إن العلاقة " $b/a$ " تخالفية في  $\mathbb{N}$   $\left\{ \begin{array}{l} b/a \\ a/b \end{array} \Rightarrow a = b \right.$

#### تمرين

1- بين أن  $b/a \Leftrightarrow a \cdot \mathbb{Z} \subset b \cdot \mathbb{Z}$   $\forall (a; b) \in \mathbb{Z}^2$   
 2- بين أن  $a/(x_1 - y_1) \wedge a/(x_2 - y_2) \Leftrightarrow a/(x_1 x_2 - y_1 y_2)$   $\forall (a; x_1; x_2; y_1; y_2) \in \mathbb{Z}^5$

### II- القسمة الاقليدية في $\mathbb{Z}$

#### 1- القسمة الاقليدية في $\mathbb{N}$

##### مبرهنة

ليكن  $a$  و  $b$  من  $\mathbb{N}$  حيث  $a \neq b$   
 يوجد زوج وحيد  $(q; r)$  من  $\mathbb{N}^2$  حيث  $a = bq + r$  حيث  $0 \leq r < b$

#### اصطلاحات

العملية التي تمكننا من تحديد  $(q; r)$  بحيث  $a = bq + r$  حيث  $0 \leq r < b$  تسمى القسمة الاقليدية لـ  $a$  على  $b$  في  $\mathbb{N}$   
 العدد  $a$  يسمى المقسوم و العدد  $b$  يسمى المقسوم عليه و العدد  $q$  الخارج و  $r$  الباقي.  
 2- القسمة الاقليدية في  $\mathbb{Z}$

##### مبرهنة

ليكن  $a$  من  $\mathbb{Z}$  و  $b$  في  $\mathbb{N}^*$  حيث  $a \neq b$   
 يوجد زوج وحيد  $(q; r)$  من  $\mathbb{Z} \times \mathbb{N}$  حيث  $a = bq + r$  حيث  $0 \leq r < b$

#### اصطلاحات

العملية التي تمكننا من تحديد  $(q; r)$  من  $\mathbb{Z} \times \mathbb{N}$  بحيث  $a = bq + r$  حيث  $0 \leq r < b$  تسمى القسمة الاقليدية لـ  $a$  على  $b$  في  $\mathbb{Z}$   
 العدد  $a$  يسمى المقسوم و العدد  $b$  يسمى المقسوم عليه و العدد  $q$  الخارج و  $r$  الباقي

## تمرين

حدد الأعداد الصحيحة النسبية  $x$  بحيث يكون للقسمة الاقليدية لـ  $x$  على 7 خارج  $q$  و باقي  $q^2$

## تمرين

بين إذا كان للقسمة الاقليدية لـ  $a$  على  $b$  و القسمة الاقليدية لـ  $a'$  على  $b$  نفس الخارج  $q$  و كان

$$a' < x < a \quad \text{فان } q \text{ خارج القسمة الاقليدية لـ } x \text{ على } b$$

## III- الموافقة بترديد n

### 1- تعريف

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

$$\forall (a;b) \in \mathbb{Z}^2 \quad a \equiv b \quad [n] \Leftrightarrow n/a-b \Leftrightarrow \exists k \in \mathbb{Z} \quad a-b = kn$$

### 2- خاصيات العلاقة " الموافقة بترديد n "

أ-  $\forall a \in \mathbb{Z} \quad a \equiv a \quad [n]$  نقول إن العلاقة " الموافقة بترديد n " انعكاسية  
 ب-  $\forall (a;b) \in \mathbb{Z} \quad a \equiv b \quad [n] \Rightarrow b \equiv a \quad [n]$  نقول إن العلاقة " الموافقة بترديد n " تماثلية  
 ج-  $\forall (a;b) \in \mathbb{Z} \quad (a \equiv b \quad [n]) \text{ et } (b \equiv c \quad [n]) \Rightarrow a \equiv c \quad [n]$  نقول إن العلاقة " الموافقة بترديد n " متعدية  
 نلخص الخاصيات أ و ب و ج بقولنا إن العلاقة " الموافقة بترديد n " علاقة تكافؤ

### د- خاصية

ليكن  $a$  و  $b$  من  $\mathbb{Z}$  و  $n$  من  $\mathbb{N}$   
 $a \equiv b \quad [n]$  تكافئ  $a$  و  $b$  لهما نفس باقي القسمة الاقليدية على  $n$

### البرهان

ليكن  $a$  و  $b$  من  $\mathbb{Z}$  و  $n$  من  $\mathbb{N}$  بحيث  $a = nq_1 + r_1$  و  $b = nq_2 + r_2$  مع  $0 \leq r_1 < n$  و  $0 \leq r_2 < n$   
 ❖ إذا كان  $a$  و  $b$  لهما نفس باقي القسمة الاقليدية على  $n$  أي  $r_1 = r_2$  فان  $a-b = n(q_1 - q_2)$   
 أي أن  $a \equiv b \quad [n]$   
 ❖ عكسيا إذا كان  $a \equiv b \quad [n]$  فانه يوجد  $k$  من  $\mathbb{Z}$  حيث  $a-b = nk$   
 و منه  $r_1 - r_2 = (k - q_1 - q_2)n$  أي  $n$  يقسم  $r_1 - r_2$   
 ولدينا  $0 \leq r_1 < n$  و  $0 \leq r_2 < n$  و منه  $|r_1 - r_2| < n$   
 وبالتالي  $r_1 - r_2 = 0$  أي  $r_1 = r_2$

### 3- المجموعة $\mathbb{Z}/n\mathbb{Z}$

\*  $\forall (a;n) \in \mathbb{Z} \times \mathbb{N} \quad \exists (q;r) \in \mathbb{Z} \times \mathbb{N} \quad a = nq + r \quad \text{et} \quad 0 \leq r < n$   
 -  $\forall (a;n) \in \mathbb{Z} \times \mathbb{N} \quad \exists r \in \mathbb{N} \quad a \equiv r \quad [n] \quad \text{et} \quad r \in \{0;1;\dots;n-1\}$   
 - المجموعة  $\{x \in \mathbb{Z} / x \equiv r \quad [n]\}$  هي مجموعة الأعداد الصحيحة النسبية التي لها نفس الباقي  $r$  في القسمة الاقليدية على  $n$  نرمز لها بـ  $\bar{r}$   
 المجموعة  $\bar{r}$  تسمى صنف تكافؤ  $r$  بالنسبة للعلاقة " الموافقة بترديد n " في  $\mathbb{Z}$   
 -  $x \in \bar{r} \Leftrightarrow x \equiv r \quad [n]$   
 \*  $\forall a \in \mathbb{Z} \quad \exists r \in \{0;1;\dots;n-1\} / \bar{a} \equiv \bar{r}$  أي  $\forall a \in \mathbb{Z} \quad \exists r \in \{0;1;\dots;n-1\} / a \equiv r \quad [n]$   
 \* إذا كان  $\bar{r} = \bar{r}'$  و  $0 \leq r < n$  و  $0 \leq r' < n$  فان  $r = r'$   
 \*  $\forall (x;n) \in \mathbb{Z} \times \mathbb{N} \quad \exists r \in \{0;1;\dots;n-1\} / x \in \bar{r}$  (  $r$  باقي القسمة الاقليدية على  $n$  )  
 اذن  $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \overline{(n-1)}$   
 المجموعة  $\{\bar{0}; \bar{1}; \dots; \overline{(n-1)}\}$  برمز لها بالرمز  $\mathbb{Z}/n\mathbb{Z}$   
 عناصر  $\mathbb{Z}/n\mathbb{Z}$  منفصلة مثنى مثنى

أمثلة

$$\bar{1} = \{x \in \mathbb{Z} / x = 2k + 1 \ (k \in \mathbb{Z})\} \text{ و } \bar{0} = 2 \cdot \mathbb{Z} \text{ حيث } \mathbb{Z}/2\mathbb{Z} = \{\bar{0}; \bar{1}\} *$$
$$\bar{1} = \{x \in \mathbb{Z} / x = 7k + 1 \ (k \in \mathbb{Z})\} \text{ و } \bar{0} = 7 \cdot \mathbb{Z} \text{ حيث } \mathbb{Z}/7\mathbb{Z} = \{\bar{0}; \bar{1}; \bar{2}; \bar{3}; \bar{4}; \bar{5}; \bar{6}\} *$$
$$\bar{3} = \{x \in \mathbb{Z} / x = 7k + 3 \ (k \in \mathbb{Z})\} \text{ و } \bar{2} = \{x \in \mathbb{Z} / x = 7k + 2 \ (k \in \mathbb{Z})\} \text{ و}$$
$$\bar{6} = \{x \in \mathbb{Z} / x = 7k + 6 \ (k \in \mathbb{Z})\} \text{ و} \dots \dots \dots$$

$$532 \equiv 4 \ [7] \text{ لدينا } \bar{532} = \bar{4} \text{ لأن } [7]$$

$$-36 \equiv 6 \ [7] \text{ لأن } \bar{-36} = \bar{6}$$

4- انسجام العلاقة " الموافقة بترديد n " مع الجمع والضرب  
أ- خاصية

ليكن  $x$  و  $y$  و  $z$  و  $t$  من  $\mathbb{Z}$  و  $n$  من  $\mathbb{N}$   
إذا كان  $x \equiv y \ [n]$  و  $x \equiv y \ [n]$  و  $z \equiv t \ [n]$  فإن  $x + z \equiv y + t \ [n]$   
إذا كان  $x \equiv y \ [n]$  و  $x \equiv y \ [n]$  و  $z \equiv t \ [n]$  فإن  $x \times z \equiv y \times t \ [n]$   
نقول إن العلاقة " الموافقة بترديد n " منسجمة مع الجمع والضرب

ب- نتائج

$$- * \text{ إذا كانت } x \in \bar{r} \text{ و } x' \in \bar{r}' \text{ فإن } x + x' \in \overline{r + r'} \text{ و } x \times x' \in \overline{r \times r'} \text{ نكتب } \overline{r + r'} = \overline{r} + \overline{r}'$$
$$\text{ و } \overline{r \times r'} = \overline{r} \times \overline{r}'$$

$$- * \text{ } \forall (a; b) \in \mathbb{Z}^2 \quad \forall (p; n) \in \mathbb{N}^* \times \mathbb{N} \quad a \equiv b \ [n] \Rightarrow a^p \equiv b^p \ [n]$$

أمثلة

$$* \text{ في } \mathbb{Z}/5\mathbb{Z} \quad \bar{3} + \bar{4} = \bar{7} = \bar{2} \quad , \quad \bar{0} + \bar{1} + \bar{2} + \bar{3} + \bar{4} = \bar{10} = \bar{0} \quad , \quad \bar{3} \times \bar{4} = \bar{12} = \bar{2}$$

تمرين

$$\text{حدد مجموعة الأعداد الصحيحة النسبية } x \text{ حيث في } \mathbb{Z}/7\mathbb{Z} \quad \bar{x} + \bar{5} = \bar{2}$$

تمرين

1- أعط جدول الجمع ثم الضرب في  $\mathbb{Z}/4\mathbb{Z}$

2- بين أن العدد  $2^{70} + 3^{70}$  قابلة للقسمة على 13

تمرين

1- بين أن  $\forall n \in \mathbb{N} \quad n(n^4 - 1) \equiv 0 \ [n]$

2- بين أن 17 يقسم  $3 \times 5^{2n-1} + 2^{3n-2}$  لكل  $n$  من  $\mathbb{N}^*$

3- ليكن  $n$  من  $\mathbb{N}$  ، حدد بواقي القسمة الاقليدية للأعداد  $1^n + 2^n + 3^n + 4^n$  على 4

IV- القاسم المشترك الأكبر

نرمز لمجموعة قواسم العدد الصحيح النسبي  $a$  بالرمز  $D_a$

1- تعريف

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$   
القاسم المشترك الأكبر للعددين  $a$  و  $b$  هو أكبر قاسم مشترك موجب قطعاً لـ  $a$  و  $b$  يرمز له  
 $a \wedge b$

$$\delta = a \wedge b \Leftrightarrow \begin{cases} \delta \in D_a \cap D_b \\ \forall x \in D_a \cap D_b \quad x \leq \delta \end{cases}$$

ليكن  $a$  و  $b$  و  $c$  من  $\mathbb{Z}^*$

$$a \wedge b = b \wedge a$$

$$(a \wedge b) \wedge c = a \wedge (b \wedge c)$$

$$a \wedge a = |a|$$

مثال  $48 \wedge 60 = 12$

3- خوارزمية اقليدس أو طريقة " القسمة المتتالية " لتحديد القاسم المشترك  
أ- ملاحظة

$$\forall a \in \mathbb{Z}^* \quad D_a = D_{-a} \quad *$$

ب- ليكن  $a$  و  $b$  من  $\mathbb{N}^*$   $\forall (a;b) \in \mathbb{Z}^{*2} \quad a \wedge b = |a| \wedge |b| \quad *$   
ومنه تحديد القاسم المشترك الأكبر لعددتين صحيحين نسبيين  
يرجع إلى تحديد القاسم المشترك الأكبر لعددتين صحيحين طبيعيين.

ب- إذا كان  $b/a$  فان  $a \wedge b = b$

- إذا كان  $b$  لا يقسم  $a$  فانه يوجد زوج وحيد  $(q;r)$  من  $\mathbb{N} \times \mathbb{N}^*$  حيث  $a = bq + r$  و  $0 < r < b$   
بما أن  $r = a - bq$  فان كل قاسم مشترك لـ  $a$  و  $b$  يقسم  $r$   
وبالتالي قاسم قاسم مشترك لـ  $a$  و  $b$  هو قاسم مشترك لـ  $r$  و  $b$  أي  $D_a \cap D_b \subset D_r \cap D_b$   
عكسيا كل قاسم مشترك لـ  $b$  و  $r$  يقسم  $a$  ( لأن  $a = bq + r$  )  
ومنه كل قاسم مشترك لـ  $b$  و  $r$  هو قاسم مشترك لـ  $a$  و  $b$  أي  $D_r \cap D_b \subset D_a \cap D_b$   
إذن  $D_a \cap D_b = D_r \cap D_b$  وبالتالي  $a \wedge b = r \wedge b$

تمهيدة

ليكن  $a$  و  $b$  من  $\mathbb{N}^*$  بحيث  $b$  لا يقسم  $a$  و  $r$  باقي القسمة الاقليدية لـ  $a$  على  $b$   
 $a \wedge b = r \wedge b$

ج- ليكن  $a$  و  $b$  من  $\mathbb{N}^*$  نفترض أن  $b < a$

بإجراء القسمة الاقليدية لـ  $a$  على  $b$  نحصل على  $a = bq_1 + r_1$  حيث  $0 \leq r_1 < b$

❖ إذا كان  $r_1 = 0$  فان  $b/a$  و منه  $a \wedge b = b$

❖ إذا كان  $r_1 > 0$  نجري القسمة الاقليدية لـ  $b$  على  $r_1$  ونحصل على  $b = r_1q_2 + r_2$  و  $0 \leq r_2 < r_1$

إذا كان  $r_2 = 0$  فان  $b \wedge r_1 = r_1$  و منه  $a \wedge b = b \wedge r_1 = r_1$

إذا كان  $r_2 > 0$  نجري القسمة الاقليدية لـ  $r_1$  على  $r_2$  ونحصل على  $r_1 = r_2q_3 + r_3$  و  $0 \leq r_3 < r_2$

.....

بإجراء العملية n مرة نحصل على

$$a \wedge b = b \wedge r_1, \quad 0 < r_1 < b, \quad a = bq_1 + r_1$$

$$b \wedge r_1 = r_1 \wedge r_2, \quad 0 < r_2 < r_1, \quad b = r_1q_2 + r_2$$

$$r_1 \wedge r_2 = r_2 \wedge r_3, \quad 0 < r_3 < r_2, \quad r_1 = r_2q_3 + r_3$$

⋮  
⋮  
⋮  
⋮  
⋮

$$r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n, \quad 0 < r_n < r_{n-1}, \quad r_{n-2} = r_{n-1}q_n + r_n$$

و منه نستنتج  $a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = r_2 \wedge r_3 = \dots = r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n$

$$0 < r_n < r_{n-1} < \dots < r_3 < r_2 < r_1 < b$$

نضع  $A = \{r_1; r_2; r_3; \dots; r_n; \dots\}$

A جزء من  $\mathbb{N}$  مكبور بالعدد  $b$  و منه A مجموعة منتهية

$$\exists p \in \mathbb{N} / r_{p+1} = 0 ; r_p \neq 0$$

$$r_{p-1} \wedge r_p = r_b \text{ و منه } r_{p-1} = r_p q_{p+1} \text{ فان } r_{p+1} = 0$$

$$\text{إذن } a \wedge b = r_p$$

نتيجة

ليكن  $a$  و  $b$  من  $\mathbb{N}^*$   
القاسم المشترك الأكبر للعددين  $a$  و  $b$  هو آخر باقي غير منعدم في طريقة القسمة المتتالية لـ  $a$  على  $b$

**مثال** باستعمال طريقة القسمة المتتالية، نحدد القاسم المشترك الأكبر للعددين 156 و 1640

$$1640 = 156 \times 10 + 80$$

$$156 = 80 \times 1 + 76$$

$$80 = 76 \times 1 + 4$$

$$76 = 4 \times 19 + 0$$

$$\text{إذن } 1640 \wedge 156 = 4$$

-3- خاصيات

أ- مبرهنة

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $\delta = a \wedge b$   
يوجد عدنان  $u$  و  $v$  من  $\mathbb{Z}$  حيث  $\delta = au + bv$

البرهان

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $\delta = a \wedge b$

نعتبر  $A = \{n \in \mathbb{N}^* / n = au + bv ; (u; v) \in \mathbb{Z}^2\}$

لدينا  $A \neq \emptyset$  لأن  $a^2 + b^2 \in A$

$A \subset \mathbb{N}$  و بالتالي  $\forall x \in A \quad x \geq p$

ليكن  $p = au_0 + bv_0$  نبرهن أن  $\delta = p$

❖ بما أن  $\delta/a$  و  $\delta/b$  فان  $\delta/p$  و منه  $\delta \leq p$

❖ بإنجاز القسمة لـ  $a$  على  $p$  نحصل على  $a = pq + r$  ;  $0 \leq r < p$   $\exists (q; r) \in \mathbb{Z} \times \mathbb{N}$

❖ و منه  $r = a - q(au_0 + bv_0) = a(1 - qu_0) + b(-qv_0)$

إذا كان  $r > 0$  فان  $r \in A$  و منه  $r \geq p$  و هذا يتناقض مع كون  $r < p$

و بالتالي  $r = 0$  أي  $p/a$  و بنفس الطريقة نبرهن أن  $p/b$

و منه  $p$  قاسم مشترك لـ  $a$  و  $b$  و بالتالي  $\delta \geq p$

لدينا  $\delta \leq p$  و  $\delta \geq p$  إذن  $\delta = p$

ب- استنتاجات

\* من البرهان السابق نستنتج  $\delta = a \wedge b$  هو أصغر عدد موجب قطعاً من المجموعة

$$B = \{n \in \mathbb{Z}^* / n = au + bv ; (u; v) \in \mathbb{Z}^2\}$$

\* بما أن  $\delta$  قاسم مشترك لـ  $a$  و  $b$  فان أي قاسم لـ  $\delta$  يقسم  $a$  و  $b$

عكسياً إذا كان  $c$  قاسم مشترك لـ  $a$  و  $b$  فان  $a = k_1 c$  ;  $b = k_2 c$   $\exists (k_1; k_2) \in \mathbb{Z}^2$

بما أن  $\delta = a \wedge b$  فانه  $\delta = au + bv$   $\exists (u; v) \in \mathbb{Z}^2 /$

و منه  $\delta = (k_1 u + k_2 v) c$  أي  $\delta$  يقسم  $c$

مبرهنة

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $\delta = a \wedge b$

مجموعة قواسم  $\delta$  هي مجموعة القواسم المشتركة لـ  $a$  و  $b$  ( $D_a \cap D_b = D_\delta$ )

نتيجة

إذا كان  $a$  و  $b$  و  $c$  أعداد من  $\mathbb{Z}$  فان

$$a \wedge b = \delta \Rightarrow ca \wedge cb = |c| \delta$$

#### 4- القاسم المشترك الأكبر لعدة أعداد

تعريف

ليكن  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_k$  أعداد من  $\mathbb{Z}^*$   
أكبر عدد صحيح طبيعي يقسم في آن واحد  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_k$  يسمى القاسم المشترك الأكبر لـ  $a_1$   
و  $a_2$  و  $a_3$  و ..... و  $a_k$

$$\text{مثال } 12 \wedge -18 \wedge 15 = 3$$

نتيجة

إذا كان  $\delta$  هو القاسم المشترك الأكبر لـ  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_k$  فإنه توجد أعداد  $\alpha_1$  و  $\alpha_2$  و  $\alpha_3$  و ..... و

$$\alpha_k \text{ من } \mathbb{Z} \text{ حيث } \sum_{i=1}^k \alpha_i a_i$$

V- الأعداد الأولية فيما بينها

1- تعريف

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

2- مبرهنة Bezout

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$   
إذا كان  $a \wedge b = 1$  فإنه  $\exists (u; v) \in \mathbb{Z}^2 / au + bv = 1$   
عكسيا: ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  حيث  $\exists (u; v) \in \mathbb{Z}^2 / au + bv = 1$   
ومنه كل قاسم مشترك لـ  $a$  و  $b$  يقسم 1 و بالتالي  $D_a \cap D_b = \{-1; 1\}$  أي  $a \wedge b = 1$

مبرهنة Bezout

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$   
 $a \wedge b = 1 \Leftrightarrow \exists (u; v) \in \mathbb{Z}^2 / au + bv = 1$

3- نتيجة

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $d$  قاسم مشترك لـ  $a$  و  $b$   
 $a \wedge b = |d| \Leftrightarrow \frac{a}{|d|} \wedge \frac{b}{|d|} = 1$

ملاحظة

إذا كان  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $a \wedge b = \delta$  فإن يوجد  $p$  و  $q$  من  $\mathbb{Z}^*$   
حيث  $p \wedge q = 1$  ;  $a = \delta p$  ;  $b = q\delta$

4- مبرهنة كوص Théorème de GAUSS

أ- مبرهنة

ليكن  $a$  و  $b$  و  $c$  من  $\mathbb{Z}^*$   
إذا كان  $c$  يقسم الجداء  $ab$  و كان  $a \wedge c = 1$  فإن  $c$  يقسم  $b$

البرهان

ليكن  $a$  و  $b$  و  $c$  من  $\mathbb{Z}^*$  حيث  $c/ab$  و  $a \wedge c = 1$   
ومنه  $\exists (u; v; k) \in \mathbb{Z} / au + cv = 1$  ;  $ab = kc$   
و بالتالي  $b = b \times 1 = b(au + cv) = bau + bcv = kcu + bcv = c(ku + bv)$   
اذن  $c$  يقسم  $b$

ب- استنتاجات

a - مبرهنة

ليكن  $a$  و  $b$  و  $c$  من  $\mathbb{Z}^*$   
 $a \wedge b = 1$  et  $a/c$  et  $b/c \Rightarrow ab/c$

مثال يكون  $x$  قابل للقسمة على 6 اذا كان قابل للقسمة على 2 و 3

ملاحظة

الشرط  $a \wedge b = 1$  ضروري

مثال 36 يقبل القسمة على 4 و 2 و 6، ولا يقبل القسمة على  $24 = 4 \times 6$

b- مبرهنة

$$\text{ليكن } a \text{ و } b \text{ و } c \text{ من } \mathbb{Z}^* \text{ و } n \text{ من } \mathbb{N}^* \\ \begin{cases} ab \equiv ac \quad [n] \\ a \wedge n = 1 \end{cases} \Rightarrow b \equiv c \quad [n]$$

البرهان

$$ab \equiv ac \quad [n] \Leftrightarrow \exists k \in \mathbb{Z} \quad ab - ac = kn$$

$$\Leftrightarrow n/a(b-c)$$

وحيث أن  $a \wedge n = 1$  فإن  $n/(b-c)$  اذن  $b \equiv c \quad [n]$

5- خاصيات

$$\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Leftrightarrow a \wedge bc = 1 \quad \text{-* ليكن } a \text{ و } b \text{ و } c \text{ من } \mathbb{Z}^*$$

$$a \wedge b = 1 \Leftrightarrow a \wedge b^n = 1 \quad \text{-* ليكن } a \text{ و } b \text{ من } \mathbb{Z}^* \text{ و } n \text{ من } \mathbb{N}^*$$

$$a \wedge b = 1 \Leftrightarrow a^m \wedge b^n = 1 \quad \text{-* ليكن } a \text{ و } b \text{ من } \mathbb{Z}^* \text{ و } n \text{ و } m \text{ من } \mathbb{N}^*$$

نتيجة

$$\text{ليكن } a \text{ و } b \text{ من } \mathbb{Z}^* \\ \text{إذا كان } a \wedge b = 1 \text{ فإن } \exists (u; v) \in \mathbb{Z}^2 \quad x = au + bv \quad \forall x \in \mathbb{Z}$$

تمرين محلول

تمرين حدد الأعداد الصحيحة النسبية حيث  $17x + 3y = 94$

الحل

الطريقة 1

$$\text{لدينا } 17 \times 2 + 3 \times 20 = 94 \text{ و } 17x + 3y = 94 \text{ ومنه } 17(x-2) + 3(y-20) = 0$$

$$\text{أي } -17(x-2) = 3(y-20)$$

$$\text{ومنه } 3/17(x-2) \text{ وحيث أن } 17 \wedge 3 = 1 \text{ فإن } 3/(x-2) \text{ أي } x-2 = 3k \quad \exists k \in \mathbb{Z}$$

$$\text{وبالتالي } x = 3k + 2 \quad \exists k \in \mathbb{Z}$$

$$\text{ومنه } 17(3k+2) + 3y = 94 \quad \exists k \in \mathbb{Z} \text{ و بالتالي } y = -17k + 20 \quad \exists k \in \mathbb{Z}$$

$$\text{إذن } S = \{(3k+2; -17k+20) / k \in \mathbb{Z}\}$$

الطريقة 2

$$17x + 3y = 94 \Leftrightarrow 17x - 94 = 3y$$

$$\Leftrightarrow 17x \equiv 94 \quad [3]$$

$$\Leftrightarrow 2x \equiv 1 \quad [3]$$

$$\Leftrightarrow -x \equiv 1 \quad [3]$$

$$\Leftrightarrow -x \equiv -(-1) \quad [3]$$

$$\text{بما أن } -1 \wedge 3 = 1 \text{ فإن } x = -1 \quad [3] \text{ ومنه } x = 3k - 1 \quad \exists k \in \mathbb{Z}$$

$$\text{و بالتالي } y = 17k + 37 \quad \exists k \in \mathbb{Z}$$

$$\text{إذن } S = \{(3k-1; 17k+37) / k \in \mathbb{Z}\}$$

## تمرين

حدد الأعداد  $q$  و  $u_0$  من المجموعة  $\mathbb{N}^*$  بحيث  $u_0 \wedge q = 1$  و الأعداد  $u_0$  و  $u_1$  و  $u_2$  و  $u_3$  حدود المتتالية الهندسية التي أساسها  $q$  و تحقق  $u_1 + 2u_3 = 44u_0^2$

## تمرين

بين إذا كان  $a \wedge b = 1$  فإن  $(a+b) \wedge b = 1$  و  $(a+b) \wedge ab = 1$

استنتج أن  $\frac{2n+3}{n^2+3n+2}$  غير قابلة للاختزال

## تمرين

بين أن العدد  $\sqrt{\frac{2}{3}}$  عدد لاجدري

6- الأعداد الأولية فيما بينها في مجموعها

## تعريف

نقول إن الأعداد  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_n$  من  $\mathbb{Z}^*$  أولية فيما بينها في مجموعها إذا كان القاسم المشترك الأكبر لهذه الأعداد هو 1

## ملاحظة

عندما نقول إن الأعداد  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_n$  من  $\mathbb{Z}^*$  أولية فيما بينها في مجموعها هذا

لا يعني أولية فيما بينها مثنى مثنى

## مبرهنة

نقول إن الأعداد  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_n$  من  $\mathbb{Z}^*$  أولية فيما بينها في مجموعها إذا وفقط وجدت أعداد  $u_1$  و  $u_2$  و  $u_3$  و ..... و  $u_n$  من  $\mathbb{Z}^*$  حيث  $\sum_{i=1}^n u_i a_i = 1$

حل المعادلة  $(x; y) \in \mathbb{Z}^2$   $ax + by = c$

## أ- مثال

نحل في  $\mathbb{Z}^2$   $1075x + 64y = 9$   
نطبق خوارزمية اقليدس لتحديد  $1075 \wedge 64$   
 $1075 = 64 \times 16 + 51$   
 $64 = 51 \times 1 + 13$   
 $51 = 13 \times 3 + 12$   
 $13 = 12 \times 1 + 1$   
 $12 = 12 \times 1 + 0$

ومنه  $1075 \wedge 64 = 1$

ومنه يوجد  $(x; y)$  من  $\mathbb{Z}^2$  حيث  $1075x + 64y = 9$

لنضع  $a = 1075$  و  $b = 64$

من خوارزمية اقليدس نستنتج أن

$$51 = a - 16b$$

$$13 = b - (a - 16b)$$

$$12 = a - 16b - 3(b - (a - 16b))$$

$$1 = b - (a - 16b) - (a - 16b - 3(b - (a - 16b)))$$

$$1 = -5a + 84b$$

ومنه  $9 = -45a + 756b$  أي  $9 = -45 \times 1075 + 756 \times 64$

ومنه  $(-45; 756)$  حل للمعادلة  $1075x + 64y = 9$  و بالتالي  $1075(x + 45) + 64(y - 756) = 0$

و بالتالي  $64/1075(x + 45)$  و حيث أن  $1075 \wedge 64 = 1$  فإن  $64/(x + 45)$



إذن  $\exists k \in \mathbb{Z} \quad x+45=64k$  أي  $\exists k \in \mathbb{Z} \quad x=64k-45$  ومنه  $\exists k \in \mathbb{Z} \quad y=1075k+756$  فإنهما يحققان المعادلة  $1075x+64y=9$  إذن  $S = \{(64k-45; 1075k+756) / k \in \mathbb{Z}\}$

### ب - الحالة العامة

نعتبر المعادلة  $(E) \quad (x; y) \in \mathbb{Z}^2 \quad ax+by=c$  حيث  $a \neq 0$  و  $b \neq 0$   
 نضع  $\delta = a \wedge b$  ومنه  $a' \wedge b' = 1$   $a = \delta a'$  et  $b = \delta b'$   $\exists (a'; b') \in \mathbb{Z}^{*2} /$   
 \* إذا كان  $\delta/c$  فإن المعادلة تصبح  $a'x+b'y=c'$  بوضع  $c = \delta c'$   
 بما أن  $a' \wedge b' = 1$  فإنه يوجد  $(u_0; v_0) \in \mathbb{Z}^{*2}$  حيث  $a'u_0 + b'v_0 = c'$  أي المعادلة  $a'x+b'y=c'$  تقبل حلا  
 \* عكسيا إذا كان للمعادلة  $ax+by=c$  في  $\mathbb{Z}^2$  ليكن  $(x_0; y_0)$  حلا للمعادلة أي  $ax_0 + by_0 = c$  ومنه  $\delta(a'x_0 + b'y_0) = c$  إذن  $\delta/c$

### خاصية

ليكن  $(a; b)$  من  $\mathbb{Z}^2$  و  $\delta = a \wedge b$   
 للمعادلة  $ax+by=c$  حلول في  $\mathbb{Z}^2$  إذا وفقط إذا كان  $\delta/c$   
 حل المعادلة  $ax+by=c$

لنفترض أن  $\delta/c$  إذن حل المعادلة يرجع إلى حل المعادلة  $a'x+b'y=c'$   
 بما أن  $a' \wedge b' = 1$  فإنه يوجد  $(u_0; v_0)$  حيث  $a'x+b'y=1$  أي  $a'c'u_0 + b'c'v_0 = c'$   
 ومنه  $a'(x-c'u_0) + b'(y-c'v_0) = 0$  وبالتالي  $a'(x-c'u_0) = -b'(y-c'v_0)$   
 وبالتالي  $a'/b'(c'v_0 - y) = 1 = a' \wedge b'$  و  $a'/b'(c'v_0 - y) = 1$  فإن  $a'(c'v_0 - y) = b'$   
 إذن  $y = -a'k + c'v_0$  حيث  $k \in \mathbb{Z}$  ومنه نستنتج أن  $x = kb' + c'u_0$   
 عكسيا نتأكد أن  $(kb' + c'u_0; -a'k + c'v_0)$  هو حل للمعادلة  $a'x+b'y=c'$   
 إذن  $\{(kb' + c'u_0; -a'k + c'v_0) / k \in \mathbb{Z}\}$

### تمرين

حل في  $\mathbb{Z}^2$  المعادلة  $7x-3y=1$   
 ليكن  $a$  من  $\mathbb{N}$  بحيث باقي القسمة الاقليدية لـ  $a$  على 7 و 3 على التوالي 1 و 2  
 حدد باقي القسمة الاقليدية لـ  $a$  على 35

### VI- المضاعف المشترك الأصغر

#### 1- تعريف

ليكن  $(a; b) \in \mathbb{Z}^{*2}$   
 المضاعف المشترك الأصغر لـ  $a$  و  $b$  هو أصغر مضاعف مشترك موجب لـ  $a$  و  $b$  نرمز له بـ  $a \vee b$

#### 2- خاصيات

أ- \* ليكن  $a$  و  $b$  و  $c$  من  $\mathbb{Z}^*$   
 $a \vee b = b \vee a$

$$(a \vee b) | c = ac \vee bc$$

$$a \wedge a = |a|$$

$$b/a \Leftrightarrow a \vee b = |a|$$

ب- \* ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $a \vee b = m$   
 كل مضاعف مشترك لـ  $a$  و  $b$  هو مضاعف للعدد  $m$

#### ج- مبرهنة

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $a \vee b = m$  و  $a \wedge b = \delta$   
 $m\delta = |ab|$

## نتيجة

$$\text{ليكن } a \text{ و } b \text{ من } \mathbb{Z}^* \\ a \wedge b = 1 \Leftrightarrow a \vee b = |ab|$$

### 3- المضاعف المشترك لعدة أعداد

#### تعريف

$a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_k$  أعداد من  $\mathbb{Z}^*$   
أصغر مضاعف مشترك موجب للأعداد  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_k$  يسمى المضاعف المشترك الأصغر لـ  $a_1$  و  $a_2$  و  $a_3$  و ..... و  $a_k$

## VII- الأعداد الأولية

### 1- تعريف

أ- القواسم الفعلية لعدد صحيح نسبي

#### تعريف

ليكن  $a \in \mathbb{Z}$   
نقول إن العدد  $d$  قاسم فعلي للعدد  $a$  إذا و فقط إذا كان  $d$  يقسم  $a$  و  $d \notin \{-1; 1; -a; a\}$

#### أمثلة

\*- القواسم الفعلية للعدد 6 هي 2 و -2 و 3 و -3  
\*- لدينا  $D_7 = \{1; -1; 7; -7\}$  العدد 7 لا يقبل قواسم فعلية

### ب- الأعداد الأولية

#### تعريف

ليكن  $a \in \mathbb{Z}$   
نقول إن العدد  $a$  أولي إذا و فقط إذا كان  $a$  يخالف 1 و -1 و ليس له قواسم فعلية  
 $a$  أولي  $\Leftrightarrow D_a = \{1; -1; a; -a\}$  و  $|a| \neq 1$

نرمز لمجموعة الأعداد الأولية بـ  $P$

### 2- خاصيات

أ- إذا كان  $p$  و  $q$  عددين أوليين و  $|q| \neq |p|$  فانهما أوليين فيما بينهما ( العكس غير صحيح )  
ب- إذا كان  $p$  أولي فانه أولي مع أي عدد  $a$  من  $\mathbb{Z}$  بحيث  $p$  لا يقسم  $a$   
ج- ليكن  $a$  عددا غير أولي في  $\mathbb{Z}^*$  و يخالف 1 و -1 .  
أصغر قاسم فعلي موجب للعدد  $a$  هو عدد أولي  
د- مجموعة الأعداد الأولية غير منتهية

#### البرهان

نبرهن أن مجموعة الأعداد الأولية غير منتهية

لتكن  $P^+$  مجموعة الأعداد الأولية الموجبة

$$P^+ \neq \emptyset \text{ لأن } 2 \in P^+$$

لنفترض أن  $P^+$  منتهية و ليكن  $p$  أكبر عنصر من  $P^+$  . لنعبر  $m = p! + 1$  لدينا  $m > p$

ومنه  $m \notin P^+$  أي  $m$  ليس أوليا و بالتالي للعدد  $m$  قاسم أولي  $q$  ومنه  $q \in P^+$  و  $q \leq p$

$q \leq p$  يستلزم  $q$  يقسم  $p!$  لأن (  $q$  أحد عوامل  $p!$  )

لدينا  $q/m$  و  $q/p!$  ومن  $q/(m-p!)$  أي  $q/1$  وهذا يتناقض مع كون  $q$  أولي

ومنه  $P^+$  غير منتهية إذن  $P$  غير منتهية

### 3- طريقة عملية لتحديد الأعداد الأولية

#### مبرهنة

ليكن  $n \in \mathbb{N}$  و  $n \geq 2$

إذا كان  $n$  غير أولي فانه يوجد عدد أولي موجب  $p$  يقسم  $n$  و  $p^2 \leq n$

#### البرهان

ليكن  $n \in \mathbb{N}$  و  $n \geq 2$  و  $n$  غير أولي و ليكن  $p$  أصغر قاسم فعلي موجب لـ  $n$  إذن  $p$  أولي ومنه يوجد

$$n = pk \text{ حيث } k \in \mathbb{N}^*$$

بما أن  $1 < p < n$  فإن  $1 < k < kp = n$  إذن  $k$  قاسم فعلي موجب للعدد  $n$  و بالتالي  $p \leq k$

$$\text{إذن } p^2 \leq pk = n$$

ملاحظة

ليكن  $n \in \mathbb{N}$  و  $n \geq 2$

لتأكد من أن  $n$  هل أولي أم لا. نرى هل يقبل القسمة على أحد الأعداد الأولية  $p$  حيث  $p^2 \leq n$

❖ فإذا كان يقبل القسمة على أحدهم فإن  $n$  غير أولي

❖ وإذا كان لا يقبل القسمة على أي واحد مهن فإن  $n$  عدد أولي

( عمليا نتوقف عندما تكون  $p^2 > n$  )

مثال العدد 179 لا يقبل القسمة على أي عدد من الأعداد الأولية التالية 2 و 3 و 5 و 7 و 11 و 13

$$17^2 = 289 ; 13^2 = 169$$

#### 4- خاصيات

##### خاصية

\*- إذا كان عدد أولي يقسم جداء أعداد صحيحة نسبية فإنه يقسم أحد عوامل هذا الجداء

البرهان

ليكن  $p$  عددا أوليا و  $a = a_1 \times a_2 \times \dots \times a_n$  جداء  $n$  من الأعداد الصحيحة النسبية

نفترض أن  $p/a$  نبين  $p/a_i$   $\exists i \in \{1; 2; \dots; n\}$

من أجل  $n = 2$  لدينا  $p/a_1 \times a_2$  . إذا كان  $p/a_1$  فإن ذلك هو المطلوب

إذا كان  $p$  لا يقسم  $a_1$  فإن  $a_1 \wedge p = 1$  وحيث  $p/a_1 \times a_2$  فإن حسب GAUSS  $p/a_2$

لنفرض أن الخاصية صحيحة بالنسبة لـ  $n$  لنبره صحتها بالنسبة لـ  $n+1$

ليكن  $b = a_1 \times a_2 \times \dots \times a_n \times a_{n+1}$  بحيث  $p/b$

إذا كان  $p/a_{n+1}$  فإن ذلك هو المطلوب

إذا كان  $p$  لا يقسم  $a_{n+1}$  فإن  $a_{n+1} \wedge p = 1$  وحيث  $p/b$  فإن حسب GAUSS  $p/a_1 \times a_2 \times \dots \times a_n$

ومنه  $p/a_i$   $\exists i \in \{1; 2; \dots; n\}$

#### نتيجة

لتكن  $p_1$  و  $p_2$  و  $p_3$  و  $p_4$  و  $p_5$  و  $p_6$  أعداد أولية موجبة و  $p$  عددا أوليا

$$p = p_i \quad \exists i \in \{1; 2; \dots; n\} \Rightarrow p/p_1 \times p_2 \times \dots \times p_n$$

#### 5- التفكيك الى جداء من عوامل أولية

##### 1- مبرهنة

كل عدد صحيح نسبي  $n$  غير منعدم ومخالف لـ 1 و -1 يمكن كتابته بكيفية وحيدة على شكل

$$n = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$$

و  $\alpha_2$  و  $\alpha_3$  و  $\alpha_4$  و  $\alpha_5$  و  $\alpha_6$  أعداد صحيحة طبيعية غير منعدمة و  $\varepsilon = \pm 1$

ملاحظة عندما نكتب  $n$  على شكل  $n = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$  فاننا نقول اننا فككنا  $n$  الى جداء

عوامل أولية

مثال فكك العدد 1752- إلى جداء عوامل أولية

##### 2- تطبيقات

##### (A) نتيجة 1

ليكن  $n = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$  حيث  $p_1$  و  $p_2$  و  $p_3$  و  $p_4$  و  $p_5$  و  $p_6$  أعداد أولية

يكون عدد  $d$  قاسما للعدد  $n$  اذا وفقط اذا كان تفكيك  $d$  الى عوامل جداء أولية على شكل

$$d = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$$

حيث  $0 \leq \beta_i \leq \alpha_i$  لكل  $i$  من  $\{1; 2; \dots; k\}$

##### نتيجة 2

ليكن  $n = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$  حيث  $p_1$  و  $p_2$  و  $p_3$  و  $p_4$  و  $p_5$  و  $p_6$  أعداد أولية

يكون عدد  $m$  مضاعفا للعدد  $n$  إذا وفقط إذا كان تفكيك  $m$  إلى عوامل جداء أولية على شكل

$$d = \varepsilon p_1^{\lambda_1} \times p_2^{\lambda_2} \times \dots \times p_k^{\lambda_k}$$

حيث  $0 \leq \alpha_i \leq \lambda_i$  لكل  $i$  من  $\{1; 2; \dots; k\}$

(B) القاسم المشترك الأكبر - المضاعف المشترك الأصغر  
+ القاسم المشترك الأكبر  
نتيجة

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  حيث  $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$  و  $b = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$  و  $p_1$  و  $p_2$  و  $\dots$  و  $p_n$  أعداد أولية

القاسم المشترك الأكبر للعددين  $a$  و  $b$  هو العدد  $\delta = p_1^{\lambda_1} \times p_2^{\lambda_2} \times \dots \times p_k^{\lambda_k}$  حيث  $\lambda_i = \inf(\alpha_i; \beta_i)$  و  $i$  تنتمي  $\{1; 2; \dots; k\}$

+ المضاعف المشترك الأصغر  
نتيجة

ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  حيث  $a = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$  و  $b = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$  و  $p_1$  و  $p_2$  و  $\dots$  و  $p_n$  أعداد أولية

المضاعف المشترك الأصغر للعددين  $a$  و  $b$  هو العدد  $m = p_1^{\lambda_1} \times p_2^{\lambda_2} \times \dots \times p_k^{\lambda_k}$  حيث  $\lambda_i = \sup(\alpha_i; \beta_i)$  و  $i$  تنتمي  $\{1; 2; \dots; k\}$

مثال حدد  $-180 \wedge 1170$  و  $-180 \vee 1170$

تمرين

ليكن  $n \in \mathbb{N}$  و  $p$  عددا أوليا في  $\mathbb{N}$

1- بين أن  $\forall d \in \mathbb{N} \quad p/d \Rightarrow [\exists m \in \mathbb{N} \quad \exists d' \in \mathbb{N} \quad d = p^m d' \quad p \wedge d' = 1]$

2- برهن أن  $\forall q \in \mathbb{N}^* - \{1\} \quad q/p^m \Leftrightarrow [\exists k \in \{1; 2; \dots; n\} \quad q = p^k]$  و استنتج عدد قواسم  $p^n$

3- ليكن  $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_n^{\alpha_n}$  تفكيك للعدد الصحيح الطبيعي  $a$  إلى جداء من عوامل أولية و  $\varphi(a)$  عدد قواسم  $a$

بين أن  $\varphi(a) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n)$  و استنتج عدد قواسم عدد صحيح نسبي

VIII- نظمات العد

1- نشاط تمهيدي

1- بين أن  $\forall (m; n) \in \mathbb{N}^2 \quad m \geq 1 \Rightarrow m^n \geq 1 + n(m-1)$

2- استنتج أن  $\forall m \in \mathbb{N} \quad m > 1 \Rightarrow \forall p \in \mathbb{N} \quad \exists n \in \mathbb{N} \quad m^n > p$

3- بين أن  $\forall b \in \mathbb{N} \quad b > 1 \Rightarrow \forall n \in \mathbb{N} \quad \exists! k \in \mathbb{N} \quad b^k \leq n < b^{k+1}$

1- نبين أن  $\forall (m; n) \in \mathbb{N}^2 \quad m \geq 1 \Rightarrow m^n \geq 1 + n(m-1)$

ليكن  $(m; n) \in \mathbb{N}^2$  لدينا  $m^n = ((m-1) + 1)^n = \sum_{i=0}^{i=n} C_n^i (m-1)^i = 1 + n(m-1) + \sum_{i=2}^{i=n} C_n^i (m-1)^i$

و حيث أن  $m-1 \geq 0$  فإن  $m^n \geq 1 + n(m-1)$

2- نستنتج أن  $\forall m \in \mathbb{N} \quad m > 1 \Rightarrow \forall p \in \mathbb{N} \quad \exists n \in \mathbb{N} \quad m^n > p$

ليكن  $m \in \mathbb{N}$  حيث  $m > 1$

إذا وجدت  $n$  فإن  $m^n \geq 1 + n(m-1)$

ليكن  $p \in \mathbb{N}$

حسب أرخميدس يوجد  $n$  من  $\mathbb{N}$  حيث  $n(m-1) > p-1$  أي  $1 + n(m-1) > p$  إذن  $m^n > p$

3- نبين أن  $\forall b \in \mathbb{N} \quad b > 1 \Rightarrow \forall n \in \mathbb{N} \quad \exists! k \in \mathbb{N} \quad b^k \leq n < b^{k+1}$

نعتبر  $A_n = \{k \in \mathbb{Z} / n < b^{k+1}\}$

حسب (2)  $b^{k_{n_0}+1} > b^{k_n} > n$   $\forall b \in \mathbb{N} \quad b > 1 \Rightarrow \forall n \in \mathbb{N} \quad \exists k_n \in \mathbb{N}$  إذن  $A_n \neq \emptyset$

$A_n \subset \mathbb{N}$  و منه  $A_n$  يقبل أصغر عنصر  $k_{n_0}$  أي أن  $b^{k_{n_0}} \leq n < b^{k_{n_0}+1}$

لأن لو كان  $b^{k_{n_0}} > n$  و  $n \geq 2$  فإن  $b^{k_{n_0}} \geq 2 > 1$  ومنه  $k_{n_0} \geq 1$  و بالتالي  $k_{n_0} - 1 \geq 0$

وحيث  $b^{(k_{n_0}-1)+1} > n$  فإن  $k_{n_0} - 1 \in A_n$  وهذا يتناقض مع كون  $k_{n_0}$  أصغر عنصر لـ  $A_n$

لو أن  $n = 1$  فإن  $k_{n_0} = 0$   $(b^0 \leq 1 \leq b^{0+1})$

## -2 تعريف

أساس نظمة عد هو عدد الأرقام التي تستعمل لتمثيل الأعداد الصحيحة الطبيعية

أمثلة

- أساس نظمة العد العشري هو 10. الأرقام المستعملة هي 0 و 1 و 2 و 3 و 4 و 5 و 6 و 7 و 8 و 9
- أساس نظمة العد الاثنائي هو 2. الأرقام المستعملة هي 0 و 1
- أساس نظمة العد الاثنى عشري هو 12. الأرقام المستعملة هي 0 و 1 و 2 و 3 و 4 و 5 و 6 و 7 و 8 و 9 و 10 و 11 نرسم في الكتابة لرقم  $\alpha$  بـ  $\beta$
- أساس نظمة العد الثماني هو 8. الأرقام المستعملة هي 0 و 1 و 2 و 3 و 4 و 5 و 6 و 7
- 3- نظمة العد ذات الأساس  $b$ .  $(b > 1)$

## أ- تمهيدة 1

ليكن  $b$  عددا صحيحا طبيعيا حيث  $(b > 1)$

لكل عدد صحيح طبيعي  $n$  يوجد  $k$  و  $r_k$  و  $q_k$  في  $\mathbb{N}$  حيث  $n = b^k q_k + r_k$  و  $0 \leq r_k < b^k$  و  $0 \leq q_k < b$

البرهان

ليكن  $(b; n) \in \mathbb{N}^2$  حيث  $(b > 1)$

إذا كان  $n = 0$  فإن نتيجة بديهية

إذا كان  $n \in \mathbb{N}^*$  فإنه حسب النشاط التمهيدي  $\exists! k \in \mathbb{N} \quad b^k \leq n < b^{k+1}$

بإجراء القسمة الاقليدية للعدد  $n$  على  $b^k$  نحصل على  $n = b^k q_k + r_k$  و  $0 \leq r_k < b^k$  و  $q_k \in \mathbb{N}$

لنبين أن  $0 \leq q_k < b$

إذا كان  $q_k \geq b$  ومنه  $q_k b^k \geq b^{k+1}$  و بالتالي  $n = b^k q_k + r_k \geq b^{k+1}$  وهذا يتناقض مع كون  $n < b^{k+1}$

إذن  $0 \leq q_k < b$

ب- حسب التمهيدة 1 لدينا  $n = b^k q_k + r_k$  و  $0 \leq r_k < b^k$  و  $0 \leq q_k < b$

بتطبيق التمهيدة على  $r_k$  نحصل على  $r_k = b^{k-1} q_{k-1} + r_{k-1}$  و  $0 \leq r_{k-1} < b^{k-1}$  و  $0 \leq q_{k-1} < b$  (لأن

$r_k < b^k$ )

نطبق التمهيدة على  $r_{k-1}$  وهكذا حت نصل الى  $r_1$  فنحصل على

$$0 \leq q_{k-2} < b \quad \text{و} \quad 0 \leq r_{k-2} < b^{k-2} \quad \text{و} \quad r_{k-1} = b^{k-2} q_{k-2} + r_{k-2}$$

$$\vdots$$

$$0 \leq q_1 < b \quad \text{و} \quad 0 \leq r_1 < b \quad \text{و} \quad r_2 = b q_1 + r_1$$

$$q_0 = r_1 \quad \text{و} \quad r_1 = 1 \times q_0$$

بجمع جميع أطراف المتساويات نحصل على الكتابة في شكلها الوحيد  $n = \sum_{i=0}^{i=k} q_i b^i$

حيث  $0 \leq q_i < b$  و  $i$  تنتمي  $\{1; 2; \dots; k\}$

ليكن  $b$  عددا صحيحا طبيعيا حيث  $(b > 1)$

لكل عدد صحيح طبيعي  $n$  يوجد عدد صحيح طبيعي  $k$  حيث  $n = \sum_{i=0}^{i=k} q_i b^i$  بحيث  $0 \leq q_i < b$

و  $i$  تنتمي  $\{1; 2; \dots; k\}$  و  $q_k > 0$  اذا كان  $n > 0$

ملاحظة

الكتابة  $n = \sum_{i=0}^{i=k} q_i b^i$  حيث  $0 \leq q_i < b$  و  $i$  تنتمي  $\{1; 2; \dots; k\}$  تبين أنه لتمثيل عدد صحيح طبيعي  $n$  في نظمة العد ذات الأساس  $b$

نحتاج الى  $b$  رمز و نمثل العدد  $n$  في نظمة العد ذات الأساس  $b$  بكتابة  $n = \overline{q_k q_{k-1} \dots q_0}_{(b)}$

أمثلة

\* في نظمة العد العشري كتابة العدد 2703 هي  $2703 = 2 \times 10^3 + 7 \times 10^2 + 0 \times 10 + 3$

\* في نظمة العد الثنائي كتابة العددين 8 و 15 هي

$$\overline{1000} \quad 8 = 1 \times 2^3 + 0 \times 2^2 + 0 \times 2 + 0$$

$$\overline{1111} \quad 15 = 1 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

\* في نظمة العد الثماني

$$15 = \overline{17}_{(8)} \quad \text{ومنه} \quad 15 = 1 \times 8 + 7$$

$$131 = \overline{203}_{(8)} \quad \text{ومنه} \quad 131 = 2 \times 8^2 + 0 \times 8 + 3$$

ج- طريقة عملية لإيجاد تمثيل عدد صحيح طبيعي في نظمة عد ما

ليكن  $b \in \mathbb{N}$  ;  $b > 1$  ;  $n \in \mathbb{N}$

لدينا

$$0 \leq r_0 < b \quad ; \quad n = bq_1 + r_0$$

$$0 \leq r_1 < b \quad ; \quad q_1 = bq_2 + r_1$$

$$0 \leq r_k < b \quad ; \quad q_k = bq_{k+1} + r_k$$

$$n \geq q_1 \geq q_2 \geq \dots \geq q_q$$

بما أن المجموعة  $A = \{q_1; q_2; \dots\}$  مكبورة في  $\mathbb{N}$  وغير فارغة فإنه يوجد  $k$  بحيث  $q_k = r_k$

ومنه

$$0 \leq r_0 < b \quad ; \quad n = bq_1 + r_0$$

$$0 \leq r_1 < b \quad ; \quad q_1 = bq_2 + r_1$$

$$0 \leq r_{k-1} < b \quad ; \quad q_{k-1} = bq_k + r_{k-1}$$

$$q_k = r_k$$

و بضرب طرفي المتساوية رقم  $i$  بالعدد  $b^i$  نحصل على

$$n = bq_1 + r_0$$

$$bq_1 = b^2 q_2 + br_1$$

$$b^i q_i = b^{i+1} q_{i+1} + b^i r_i$$

$$b^{k-1}q_{k-1} = b^k q_k + b^{k-1}r_{k-1}$$

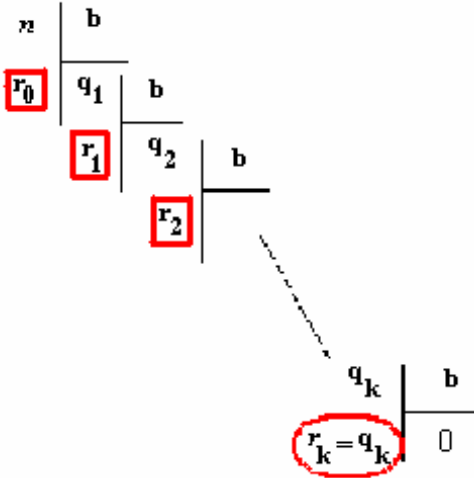
$$b^k q_k = b^k r_k$$

$$i \in \{1; 2; \dots; k\} \text{ و } 0 \leq r_i < b$$

$$n = \sum_{i=0}^{i=k} b^i r_i \text{ بجمع أطراف المتساويات نحصل على}$$

$$n = r_k r_{k-1} \dots r_1 r_0 \text{ إذا كان } r_k \neq 0 \text{ فان}$$

طريقة عملية



لتحديد تمثيل للعدد n في أنظمة العد ذات الأساس b  
نحسب البواقي  $r_i$  ( $0 \leq i \leq k$ )

$$n = r_k r_{k-1} \dots r_1 r_0 (b)$$

مثال

لنبحث عن تمثيل للعدد 3254 في أنظمة العد الثماني ثم أنظمة العد الاثنا عشري

$$\begin{array}{r} 3254 \text{ } | \text{ } 12 \\ \hline (2) \text{ } | \text{ } 271 \text{ } | \text{ } 12 \\ \hline (7) \text{ } | \text{ } 22 \text{ } | \text{ } 12 \\ \hline (\alpha) \text{ } | \text{ } 1 \text{ } | \text{ } 12 \\ \hline (1) \text{ } | \text{ } 0 \end{array}$$

$$3254 = \overline{1\alpha 72}_{(12)}$$

$$\begin{array}{r} 3254 \text{ } | \text{ } 8 \\ \hline (6) \text{ } | \text{ } 406 \text{ } | \text{ } 8 \\ \hline (6) \text{ } | \text{ } 50 \text{ } | \text{ } 8 \\ \hline (2) \text{ } | \text{ } 6 \text{ } | \text{ } 8 \\ \hline (6) \text{ } | \text{ } 0 \end{array}$$

$$3254 = \overline{6266}_{(8)}$$

4- مقارنة عددين ممثلين في نفس النظام  
خاصية

ليكن  $x$  و  $y$  ممثلين في نفس أنظمة العد بـ  $x = \overline{a_n a_{n-1} \dots a_0}_{(b)}$  و  $y = \overline{c_m c_{m-1} \dots c_0}_{(b)}$

إذا كان  $m > n$  فان  $y > x$

خاصية

ليكن  $x$  و  $y$  ممثلين في نفس أنظمة العد بـ  $x = \overline{a_n a_{n-1} \dots a_0}_{(b)}$  و  $y = \overline{c_n c_{n-1} \dots c_0}_{(b)}$

إذا كان  $c_n = a_n$   $c_{n-1} = a_{n-1}$   $\dots$   $c_{i+1} = a_{i+1}$   $\dots$   $c_i \neq a_i$  فان ترتيب  $x$  و  $y$  هو نفس ترتيب  $a_i$  و  $c_i$

5- تغيير أساس أنظمة عد

لتمثيل عدد  $x$  في أنظمة عد ذات الأساس  $b$  نمثله أولاً في أنظمة العد العشري و نحدد تمثيله في أنظمة عد ذات الأساس  $b$

تمرين

هل توجد أنظمة العد ذات الأساس  $b$  حيث  $\overline{xxx} \times \overline{xxx} = \overline{yyyyyy}$

## 6- مصاديق قابلية القسمة على بعض الأعداد في أنظمة العد العشري

ليكن  $x = \overline{a_n a_{n-1} \dots a_1 a_0}$  عدد صحيح طبيعي كتابته في أنظمة العد العشري هي

$$x \equiv 0 \pmod{4} \Leftrightarrow \overline{a_1 a_0} \equiv 0 \pmod{4}$$

$$x \equiv 0 \pmod{5} \Leftrightarrow a_0 = 0 \text{ ou } a_1 = 5$$

$$x \equiv 0 \pmod{25} \Leftrightarrow \overline{a_1 a_0} \in \{00; 25; 50; 75\}$$

$$x \equiv 0 \pmod{3} \Leftrightarrow \sum_{i=0}^{i=n} a_i \equiv 0 \pmod{3}$$

$$x \equiv 0 \pmod{9} \Leftrightarrow \sum_{i=0}^{i=n} a_i \equiv 0 \pmod{9}$$

$$x \equiv 0 \pmod{11} \Leftrightarrow \sum_{i=0}^{i=n} (-1)^i a_i \equiv 0 \pmod{11}$$