

## الحسابيات

**تذكير :**

- 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  $0 \leq r < b$

- خاصيات

$$\begin{aligned} * \text{ ليكن } a \text{ و } b \text{ و } c \text{ من } \mathbb{Z}^* \\ a \wedge b = b \wedge a \quad (a \wedge b) \wedge c = a \wedge (b \wedge c) \quad a \wedge a = |a| \\ a \wedge b = \delta \Rightarrow ca \wedge cb = |c| \delta \\ a \vee b = b \vee a \quad (a \vee b) |c| = ac \vee bc \quad a \wedge a = |a| \\ b/a \Leftrightarrow a \vee b = |a| \\ a \wedge b = 1 \Leftrightarrow a \vee b = |ab| \end{aligned}$$

\* ليكن  $a$  و  $b$  من  $\mathbb{N}^*$  بحيث  $b$  لا يقسم  $a$  و  $r$  باقي القسمة الاقليدية لـ  $a$  على  $b$   
\* ليكن  $a$  و  $b$  من  $\mathbb{Z}^*$  و  $a \vee b = m$  كل مضاعف مشترك لـ  $a$  و  $b$  هو مضاعف للعدد  $m$

- مبرهنة

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

- مبرهنة

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

- مبرهنة

ليكن  $n \in \mathbb{N}$  و  $n \geq 2$   
إذا كان  $n$  غير أولي فانه يوجد عدد أولي موجب  $p$  يقسم  $n$  و  $p^2 \leq n$

- خاصيات

\*- إذا كان عدد أولي يقسم جداء أعداد صحيحة نسبية فانه يقسم أحد عوامل هذا الجداء  
\*- لتكن  $p_1$  و  $p_2$  و ..... و  $p_n$  أعداد أولية موجبة و  $p$  عددا أوليا  
 $p / p_1 \times p_2 \times \dots \times p_n \Rightarrow \exists i \in \{1; 2; \dots; n\} \quad p = p_i$

- مبرهنة

كل عدد صحيح نسبي  $n$  غير منعدم ومخالف لـ 1 و -1 يمكن كتابته بكيفية وحيدة على شكل  
 $n = \varepsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_k^{\alpha_k}$  حيث  $p_1$  و  $p_2$  و ..... و  $p_n$  أعداد أولية مختلفة مثنى مثنى و  $\alpha_1$   
و  $\alpha_2$  و ..... و  $\alpha_n$  أعداد صحيحة طبيعية غير منعدمة و  $\varepsilon = \pm 1$

- 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  $b = \varepsilon p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_k^{\beta_k}$   
وحيث  $p_1$  و  $p_2$  و ..... 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 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  $\{1; 2; \dots; k\}$

## I- 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  $\mathbb{N}$   
 $a \equiv b \quad [n]$  تكافؤ  $a$  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  $|r_1 - r_2| < n$   
و بالتالي  $r_1 - r_2 = 0$  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  $r = r'$   
\*  $\forall (x; n) \in \mathbb{Z} \times \mathbb{N} \quad \exists r \in \{0; 1; \dots; n-1\} / x \in \bar{r}$  ( باقي القسمة الاقليدية على  $n$  )

اذن  $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \overline{(n-1)}$

المجموعة  $\{\bar{0}; \bar{1}; \dots; \overline{(n-1)}\}$  يرمز لها بالرمز  $\mathbb{Z}/n\mathbb{Z}$

عناصر  $\mathbb{Z}/n\mathbb{Z}$  منفصلة مثنى مثنى

### أمثلة

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

$$\bar{6} = \{x \in \mathbb{Z} / x = 7k + 6 \quad (k \in \mathbb{Z})\} \text{ و.....}$$

$$532 \equiv 4 \quad [7] \quad \text{لدينا } \bar{532} = \bar{4} \text{ في } \mathbb{Z}/7\mathbb{Z}$$

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

#### -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  $x \equiv y \quad [n]$  و  $x \equiv y \quad [n]$  و  $z \equiv t \quad [n]$  فان  $x + z \equiv y + t \quad [n]$   
إذا كان  $x \equiv y \quad [n]$  و  $x \equiv y \quad [n]$  و  $z \equiv t \quad [n]$  فان  $x \times z \equiv y \times t \quad [n]$   
نقول إن العلاقة " الموافقة بترديد n" منسجمة مع الجمع والضرب

#### ب- نتائج

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

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

#### أمثلة

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

#### تمرين

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

#### تمرين

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

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

#### تمرين

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

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

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

#### -II- الأعداد الأولية فيما بينها

#### 1- تعريف

$a$  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  $\mathbb{Z}^*$

$$\text{إذا كان } a \wedge b = 1 \text{ فانه } \exists (u; v) \in \mathbb{Z}^2 / \quad au + bv = 1$$

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

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

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

#### 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 كوس Théorème de GAUSS

أ- مبرهنة

ليكن  $a$  و  $b$  و  $c$  من  $\mathbb{Z}^*$  إذا كان  $c$  يقسم  $ab$  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  $b = b \times 1 = b(au + cv) = bau + bcv = kcu + bcv = c(ku + bv)$  إذن  $c$  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، و لا يقبل القسمة على  $24 = 6 \times 4$

b- مبرهنة

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

البرهان

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

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

و حيث أن  $a \wedge n = 1$  فإن  $n/(b - c)$  إذن  $b \equiv c \ [n]$

#### 5- خاصيات

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

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

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

نتيجة

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

تمرين محلول

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

الحل

الطريقة 1

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

أي  $-17(x-2) = 3(y-20)$   
 ومنه  $3/17(x-2)$  وحيث أن  $17 \wedge 3 = 1$  فإن  $3/(x-2)$  أي  $x-2 = 3k$   $\exists k \in \mathbb{Z}$   
 وبالتالي  $x = 3k + 2$   $\exists k \in \mathbb{Z}$   
 ومنه  $17(3k+2) + 3y = 94$   $\exists k \in \mathbb{Z}$  و بالتالي  $y = -17k + 20$   
 إذن  $S = \{(3k+2; -17k+20) / k \in \mathbb{Z}\}$   
 الطريقة 2

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

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

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

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

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

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

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

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- مبرهنة فيرما FERMAT

نشاط

ليكن  $p$  عددا أوليا

1- بين أن  $p$  يقسم  $C_p^k$  مهما كان  $k$  حيث  $1 \leq k \leq p-1$

2- استنتج أن  $\forall n \in \mathbb{N} \quad p \mid [(n+1)^p - (n^p + 1)]$

3- أ/ بين بالترجع أن  $\forall n \in \mathbb{N} \quad n^p \equiv n \quad [p]$

ب/ استنتج أن  $\forall n \in \mathbb{N} \quad n^{p-1} \equiv 1 \quad [p]$  بحيث  $p \wedge n = 1$

4- استنتج أن  $\forall a \in \mathbb{Z} \quad a^p \equiv a \quad [p]$  و أن  $\forall a \in \mathbb{Z} \quad a^{p-1} \equiv 1 \quad [p]$  بحيث  $p \wedge a = 1$

الجواب

1- بين أن  $p$  يقسم  $C_p^k$

$$k!C_p^k = p(p-1)(p-2)\dots(p-k+1) \Leftrightarrow C_p^k = \frac{p!}{k!(p-k)!}$$

أي  $p$  يقسم  $k!C_p^k$  و بما أن  $k < p$  فإن عوامل الجداء  $k!$  أصغر من  $p$  ومنه  $p \wedge k! = 1$

و حسب مبرهنة كوفس فإن  $p$  يقسم  $C_p^k$

2- نستنتج أن  $\forall n \in \mathbb{N} \quad p \mid [(n+1)^p - (n^p + 1)]$

حسب الصيغة الحدانية لدينا  $(n+1)^p = \sum_{i=0}^p C_n^i n^i$  أي  $(n+1)^p = 1 + n^p + \sum_{i=1}^{p-1} C_n^i n^i$

$$(n+1)^p - (1+n^p) = \sum_{i=1}^{p-1} C_n^i n^i \text{ ومنه}$$

و حسب السؤال الاول  $p$  يقسم  $C_p^i$   $1 \leq i < p$  اذن  $p$  يقسم  $\sum_{i=1}^{p-1} C_n^i n^i$

$$\forall n \in \mathbb{N} \quad p \mid [(n+1)^p - (n^p + 1)] \text{ ومنه}$$

3- نبين بالترجع أن  $[p] \quad n^p \equiv n$   $\forall n \in \mathbb{N}$

من أجل  $n=0$  لدينا  $[p] \quad 0^p \equiv 0$

نفترض أن  $[p] \quad n^p \equiv n$  و نبين أن  $[p] \quad (n+1)^p \equiv n+1$

$$[p] \quad n^p \equiv n \Rightarrow [p] \quad n^p + 1 \equiv n + 1$$

و حيث أن  $\forall n \in \mathbb{N} \quad p \mid [(n+1)^p - (n^p + 1)]$  فان  $[p] \quad (n+1)^p \equiv n^p + 1$

$$[p] \quad (n+1)^p \equiv n+1 \text{ ومنه}$$

$$[p] \quad n^p \equiv n \quad \forall n \in \mathbb{N} \quad \text{إذن}$$

ب/ نستنتج أن  $[p] \quad n^{p-1} \equiv 1 \quad \forall n \in \mathbb{N}$  بحيث  $p \wedge n = 1$

لدينا  $[p] \quad n^p \equiv n$  و  $p \wedge n = 1$  إذن  $[p] \quad n^{p-1} \equiv 1$

حسب الخاصية التي تقول  $[n] \quad \begin{cases} ab \equiv ac \\ a \wedge n = 1 \end{cases} \Rightarrow b \equiv c$

4- نستنتج أن  $[p] \quad a^p \equiv a \quad \forall a \in \mathbb{Z}$  وأن  $[p] \quad a^{p-1} \equiv 1 \quad \forall a \in \mathbb{Z}$  بحيث  $p \wedge a = 1$

ليكن  $a \in \mathbb{Z}$

إذا كان  $a \in \mathbb{N}$  فالنتيجة تم برهنتها سابقا

إذا كان  $a < 0$  فان  $-a > 0$

من أجل  $p=2$  لدينا  $a^2 - a = a(a-1)$  ومنه 2 يقسم  $a^2 - a$  لان جداء عددين متتاليين زوجي

إذا كان  $p > 2$  فان  $p$  فردي

$$[p] \quad (-a)^p \equiv -a \quad \text{أي} \quad [p] \quad -(a^p) \equiv -a \quad \text{ومنه} \quad [p] \quad a^p \equiv a$$

$$[p] \quad a^p \equiv a \quad \forall a \in \mathbb{Z} \quad \text{اذن}$$

$$[p] \quad a^p \equiv a \quad \text{و} \quad p \wedge a = 1 \Rightarrow [p] \quad a^{p-1} \equiv 1$$

**خاصية**

ليكن  $p$  عددا أوليا

$$[p] \quad a^p \equiv a \quad \forall a \in \mathbb{Z}$$

**مبرهنة فيرما**

ليكن  $p$  عددا أوليا

$$[p] \quad a^{p-1} \equiv 1 \quad \forall a \in \mathbb{Z} \quad \text{بحيث} \quad p \wedge a = 1$$

## 7- الأعداد الأولية فيما بينها في مجموعها

تعريف

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

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

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  $\exists k \in \mathbb{Z} \quad x = 64k - 45$  و منه  $\exists k \in \mathbb{Z} \quad y = 1075k + 756$

عكسيا إذا كان  $x = 64k - 45$  ;  $y = 1075k + 756$  فإنهما يحققان المعادلة  $1075x + 64y = 9$

إذن  $S = \{(64k - 45; 1075k + 756) / k \in \mathbb{Z}\}$

ب - الحالة العامة

نعتبر المعادلة  $(x; y) \in \mathbb{Z}^2 \quad ax + by = c$  حيث  $a \neq 0$  و  $b \neq 0$

نضع  $\delta = a \wedge b$  و منه  $a' \wedge b' = 1$  و  $a = \delta a'$  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  $1 = a' \wedge b'$  فإنه يوجد  $(u_0; v_0)$  من  $\mathbb{Z}^{*2}$  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  $a'(x-c'u_0)=-b'(y-c'v_0)$  و  $a'/b'(c'v_0-y)$  و حيث أن  $1=a' \wedge b'$  فإن  $a'/(c'v_0-y)$  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

### III- 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)  $A_n \neq \emptyset$  إذن  $\forall b \in \mathbb{N} \quad b > 1 \Rightarrow \forall n \in \mathbb{N} \quad \exists k_n \in \mathbb{N} \quad b^{k_n+1} > b^{k_n} > n$

$A_n \subset \mathbb{N}$  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 نرزم في الكتابة لرقم  $\alpha$  ب  $\beta$
- أساس نظمة العد الثماني هو 8. الأرقام المستعملة هي 0 و 1 و 2 و 3 و 4 و 5 و 6 و 7
- أساس 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  $n = 0$  فان نتيجة بديهية

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

يأجراء 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 التمهييدة 1 لدينا  $n = b^k q_k + r_k$  و  $0 \leq r_k < b^k$  و  $0 \leq q_k < b$

بتطبيق التمهييدة 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 التمهييدة 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  $\{1; 2; \dots; k\}$

## تمهيدة 2

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

لدينا

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

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

$$\dots$$

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

$$n \geq q_1 \geq q_2 \geq \dots \geq q_k$$

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

ومنه

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

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

$$\dots$$

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

$$q_k = r_k$$

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

$$n = bq_1 + r_0$$

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

$$\dots$$

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

$$\dots$$

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

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

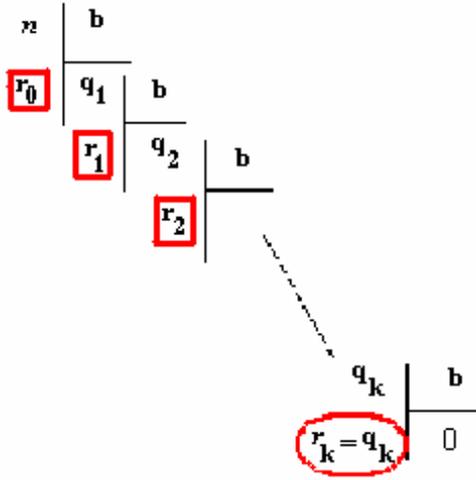
بجمع أطراف المتساويات نحصل على  $n = \sum_{i=0}^{i=k} b^i r_i$  و  $i \in \{1; 2; \dots; k\}$  و  $0 \leq r_i < b$

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

طريقة عملية

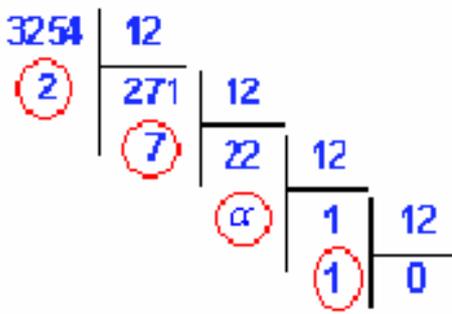
لتحديد تمثيل للعدد  $n$  في نظمة العد ذات الأساس  $b$   
نحسب البواقي  $r_i$  ( $0 \leq i \leq k$ )

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

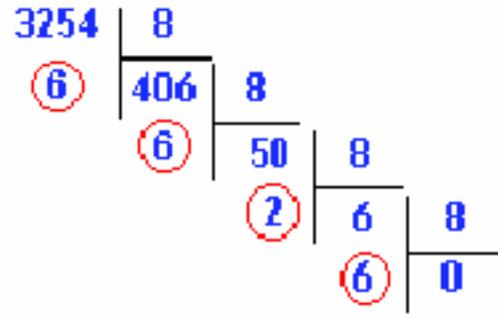


مثال

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



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



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

### 3- مقارنة عددين ممثلين في نفس النظمة

خاصية

ليكن  $x$  و  $y$  ممثلين في نفس نظمة 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  $m > n$  فإن  $y > x$

خاصية

ليكن  $x$  و  $y$  ممثلين في نفس نظمة 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  $c_n = a_n$   $c_{n-1} = a_{n-1}$   $\dots$   $c_{i+1} = a_{i+1}$   $\dots$   $c_i \neq a_i$  فإن ترتيب  $x$  و  $y$  هو نفس ترتيب  $a_i$  و  $c_i$

### 5- تغيير أساس نظمة عد

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

تمرين

هل توجد نظمة العد ذات الأساس  $b$  حيث  $xxx \times xxx = yyyyyy$

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

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

$$x \equiv 0 \quad [4] \Leftrightarrow 4 \mid \overline{a_1 a_0}$$

$$x \equiv 0 \quad [5] \Leftrightarrow a_0 = 0 \quad \text{ou} \quad a_1 = 5$$

$$x \equiv 0 \quad [5] \Leftrightarrow \overline{a_1 a_0} \in \{00; 25; 50; 75\}$$

$$x \equiv 0 \quad [3] \Leftrightarrow \sum_{i=0}^{i=n} a_i \equiv 0 \quad [3]$$

$$x \equiv 0 \quad [9] \Leftrightarrow \sum_{i=0}^{i=n} a_i \equiv 0 \quad [9]$$

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