تذكير

I. القسمة في $\mathbb{Z}$:

A. مضاعف لعدد نسبي - قاسم لعدد نسبي :

1. تعريف:

ليكن a و b من $\mathbb{Z}$.

- نقول أن : a يقسم b ، إذا وجد عدد نسبي q حيث $b = qa$ و نكتب : $a \mid b$. و منه: $a \mid b \Leftrightarrow \exists q \in \mathbb{Z}, b = qa$
- في هذه الحالة : نقول إن العدد a قاسم للعدد b ؛ أما العدد b يسمى مضاعف ل a .

2. ملحوظة :

- 1 يقسم جميع الأعداد الصحيحة النسبية . جميع الأعداد النسبية تقسم 0 .
- مجموعة قواسم b في $\mathbb{Z}$ هي $D_b = \{d \in \mathbb{Z} / \exists q \in \mathbb{Z}, b = qd\}$ يرمز لها ب: D_b .
- مجموعة مضاعفات a هي: $\{\cdots, -qa, \cdots, -2a, -a, 0, a, 2a, \cdots, qa, \cdots\}$ و يرمز لها: $a\mathbb{Z}$

B. خاصيات :

ليكن a و b و c و d من $\mathbb{Z}$.

- الانعكاسية : $a \mid a$. (a يقسم a) .
- التعدي : $(a \mid b \text{ و } b \mid c) \Rightarrow a \mid c$
- $(a \mid b \text{ و } b \mid a) \Leftrightarrow |a| = |b|$.
- (k, k') من $\mathbb{Z}^2$: $(a \mid b \text{ و } a \mid c) \Rightarrow a / (kb + k'c)$. ($kb + k'c$ تسمى تأليفة خطية ل b و c).
- الجداء : $\left.\begin{matrix} a \mid b \\ c \mid d \end{matrix}\right\} \Rightarrow ac \mid bd$. ومنه نستنتج : $a \mid b \Rightarrow a^n \mid b^n$
- $(a \mid b \text{ و } b \neq 0) \Rightarrow |a| \leq |b|$.
- $(a \mid b \text{ و } d \neq 0) \Rightarrow ad \mid bd$.

II. القسمة الإقليدية في $\mathbb{Z}$: la division Euclidienne.

1. خاصية:

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

يوجد زوج وحيد (q, r) من $\mathbb{Z} \times \mathbb{N}$ حيث: $\begin{cases} b = qa + r \\ 0 \leq r < a \end{cases}$.

2. مفردات :

- العدد b يسمى المقسوم . العدد a يسمى المقسوم عليه. العدد q يسمى الخارج . العدد r يسمى الباقي .
- العملية التي تمكننا من الحصول على q و r تسمى القسمة الإقليدية ل b على a .
- $r = 0$ نقول أن b يقبل القسمة على a .

3. أمثلة : مثال 1 : حدد q و r حيث : $56 = 13q + r$.

مثال 2 : حدد q و r حيث : أ- $-56 = 13q + r$. ب - $56 = -13q + r$. ج - $-56 = -13q + r$ مع $0 \leq r < 13$.

III. الموافقة بترديد n La congruence modulo n .

A. الموافقة بترديد n :

1. تعريف :

ليكن $n \in \mathbb{N}^*$ و $(a,b) \in \mathbb{Z}^2$.

نقول إن : a يوافق b بترديد n لنعني أن n يقسم $b-a$. نكتب : $a \equiv b\ [n]$ أو أيضا $a \equiv b \bmod (n)$

2. مثال :

أتمم : باستعمال الرمز المناسب من بين: $\equiv$ أو $\not\equiv$. $1 \cdots 5\ [3]$ ؛ $1 \cdots 4\ [3]$ ؛ $12 \cdots 6\ [3]$ ؛ $-4 \cdots 5\ [3]$

B. خاصيات الموافقة بترديد n :

1. نشاط :

$(a,b,c) \in \mathbb{Z}^3$ و $n \in \mathbb{N}^*$.

1. بين أن : $a \equiv b\ [n] \Leftrightarrow \exists k \in \mathbb{Z} / b = a + kn$. ثم استنتج بالتفصيل مجموعة الأعداد التي توافق a بترديد n .
2. بين أن :
   - أ- $a \equiv a\ [n]$ (الترديد هو انعكاسي).
   - ب- $b \equiv a\ [n] \Leftrightarrow a \equiv b\ [n]$ (الترديد هو تماثلي)
   - ج- $a \equiv c\ [n] \Rightarrow \Rightarrow (a \equiv b\ [n]$ و $b \equiv c\ [n])$ (الترديد هو متعدي)
3. بين أن : $a \equiv b\ [n]$ يكافئ أن $a = kn + r$ و $b = k'n + r$ مع k و 'k من $\mathbb{Z}$ (أي a b لهما نفس باقي القسمة على n).
4. بين أن :
   - أ- $a + c \equiv b + d\ [n] \Rightarrow$ (نقول أن الموافقة منسجمة مع الجمع)
   - ب- $a \times c \equiv b \times d\ [n] \Rightarrow (a \equiv b\ [n]$ و $c \equiv d\ [n])$ (نقول أن الموافقة منسجمة مع الضرب)
   - ج- $(\forall k \in \mathbb{N}\ ;\ a^k \equiv b^k\ [n]) \Rightarrow a \equiv b\ [n]$. يمكنك استعمال المتطابقة التالية :

$$a^n - b^n = (a-b)\left(a^{n-1}b^0 + a^{n-2}b^1 + a^{n-3}b^2 + \cdots + a^1b^{n-1} + a^0b^{n-1}\right)$$

جواب:

1. نبين :

لدينا :

$$a \equiv b\ [n] \Leftrightarrow n \mid (b-a)$$
$$\Leftrightarrow \exists k \in \mathbb{Z}\ /\ b - a = kn$$
$$\Leftrightarrow \exists k \in \mathbb{Z}\ /\ b = a + kn$$

و منه : b تأخذ القيم التالية $\cdots a-3n, a-2n, a-n, a, a+n, a+2n, a+3n, \cdots$

خلاصة : مجموعة الأعداد التي توافق a بترديد n هي : $\{\cdots a-3n, a-2n, a-n, a, a+n, a+2n, a+3n, \cdots\}$.

2. نبين أن :
   - أ- الانعكاسية :

لدينا : n يقسم $a - a = 0 \times n$ يكافئ $a \equiv a\ [n]$

ومنه الانعكاسية .

ب- التماثلية :

لدينا : $a\equiv b\ [n]\Leftrightarrow n|(b-a)\Leftrightarrow n|-(b-a)\Leftrightarrow n|(a-b)\Leftrightarrow b\equiv a\ [n]$

ومنه : التماثلية.

ج- التعدي :

لدينا :

$$(c\equiv d\ [n] \text{ و } a\equiv b\ [n]) \Rightarrow n/(b-a) \text{ و } a/(c-b)$$
$$\Rightarrow n/(b-a) \text{ و } a/(c-b)$$
$$\Rightarrow n/((b-a)+(c-b))$$
$$\Rightarrow n/(c-a)$$
$$\Rightarrow a\equiv c\ [n]$$

و منه التعدي :

3. نبين أن :

نضع : $a=kn+r$ و $b=k'n+r'$ مع k و k' من $\mathbb{Z}$. و $0\le r<n$ و $0\le r'<n$ إذن $(1):|r'-r|<n$.

لدينا :

$$a\equiv b\ [n]\Leftrightarrow n/(b-a)$$
$$\Leftrightarrow b-a=k''n$$
$$\Leftrightarrow k'n+r'-(kn+r)=k''n$$
$$\Leftrightarrow (k'-k)n+r'-r=k''n$$
$$\Leftrightarrow r'-r=(k''+k-k')n$$
$$\Leftrightarrow r'-r=Kn\ ;\ (K=k''+k-k')$$
$$\Leftrightarrow n/(r'-r)$$
$$\Leftrightarrow (r'-r)=0\ ;\ (|r'-r|<n\ (1))$$
$$\Leftrightarrow r'=r$$

خلاصة : a b لهما نفس باقي القسمة على n.

4. نبين أن :

1. الموافقة منسجمة مع الجمع :

لدينا:

$$(a\equiv b\ [n] \text{ و } c\equiv d\ [n]) \Rightarrow n/(b-a) \text{ و } n/(d-c)$$
$$\Rightarrow n/((b-a)+(d-c))$$
$$\Rightarrow n/((b+d)-(a+c))$$
$$\Rightarrow (a+c)\equiv(b+d)\ [n]$$

خلاصة : الموافقة منسجمة مع الجمع .

2. الموافقة منسجمة مع الضرب .

لدينا : $a\equiv b\ [n]$ و $c\equiv d\ [n]$ و نبين أن : $a\times c\equiv b\times d\ [n]$

لدينا :

$$(c\equiv d\ [n] \text{ و } a\equiv b\ [n]) \Rightarrow n/(b-a) \text{ و } n/(d-c)$$

3.
$$\Rightarrow n/(b-a)\times c \text{ و } n/(d-c)\times b$$
$$\Rightarrow n/\left[(b-a)\times c+(d-c)\times b\right]$$
$$\Rightarrow n/\left[bc-ac+db-cb\right]$$
$$\Rightarrow n/\left[db-ac\right]$$
$$\Rightarrow ac\equiv bd\ [n]$$

خلاصة : الموافقة منسجمة مع الضرب .

5. نبين ان: $\forall k\in\mathbb{N}\ ;\ a^k\equiv b^k\ [n]$. نأخذ : $k\in\mathbb{Z}$.

لدينا:
$$a\equiv b\ [n]\ \Rightarrow\ n/(b-a)$$
$$\Rightarrow\ n/(b-a)\left(a^{k-1}b^0+a^{k-2}b^1+a^{k-3}b^2+\cdots+a^1b^{k-1}+a^0b^{k-1}\right)$$
$$\Rightarrow\ n/\left(b^k-a^k\right)$$
$$\Rightarrow\ a^k\equiv b^k\ [n]$$

خلاصة : $a\equiv b\ [n]\ \Rightarrow\ \left(\forall k\in\mathbb{N}^*\ ;\ a^k\equiv b^k\ [n]\right)$.

2. خاصيات:

$(a,b,c)\in\mathbb{Z}^3$ و $n\in\mathbb{N}^*$.

1.
أ- $a\equiv b\ [n]\ \Leftrightarrow\ \exists k\in\mathbb{Z}\ /\ b=a+kn$.
ب- مجموعة الأعداد التي توافق a بترديد n هي : $\{\cdots a-3n,a-2n,a-n,a,a+n,a+2n,a+3n,\cdots\}$.

2.
1. الانعكاسية : $\forall a\in\mathbb{Z} : a\equiv a\ [n]$
2. التماثلية : $\forall a,b\in\mathbb{Z} : a\equiv b\ [n]\ \Leftrightarrow\ b\equiv a\ [n]$.
3. التعدية : $\forall a,b,c,d\in\mathbb{Z} : \left(a\equiv b\ [n] \text{ و } b\equiv c\ [n]\right)\ \Rightarrow\ a\equiv c\ [n]$

3. $a\equiv b\ [n]$ يكافئ أن $a=kn+r$ و $b=k'n+r$ مع k و k' من $\mathbb{Z}$ (أي a و b لهما نفس باقي القسمة على n).

4.
1. $\left(c\equiv d\ [n] \text{ و } a\equiv b\ [n]\right)\ \Rightarrow\ a+c\equiv b+d\ [n]$ (نقول أن الموافقة منسجمة مع الجمع)
2. $\left(c\equiv d\ [n] \text{ و } a\equiv b\ [n]\right)\ \Rightarrow\ a\times c\equiv b\times d\ [n]$ (نقول أن الموافقة منسجمة مع الضرب).
3. $a\equiv b\ [n]\ \Rightarrow\ \left(\forall k\in\mathbb{N}\ ;\ a^k\equiv b^k\ [n]\right)$

IV. أصناف التكافؤ – المجموعة $\mathbb{Z}/n\mathbb{Z}$.

A. أصناف التكافؤ بترديد n : classes d'équivalence modulo n

1. تعريف :

ليكن : $n\in\mathbb{N}^*$ و a عدد من $\mathbb{Z}$. حيث: $a=kn+r$.
الأعداد x من $\mathbb{Z}$ التي توافق a بترديد n تكون مجموعة تسمى صنف التكافؤ a ونرمز له ب: $\bar{a}$.

2. ملحوظة و مفردات و رموز :

a عدد من $\mathbb{Z}$. حيث: $a = kn + r$.

- $a \equiv r\ [n]$. لأن : $a \equiv r\ [n] \Leftrightarrow a - r = kn,\ (k \in \mathbb{Z}) \Leftrightarrow a - r = kn + r - r,\ (k \in \mathbb{Z})$.

إذن : $a \equiv r\ [n]$ ومنه $\bar{a} \equiv \bar{r}\ [n]$.

صنف التكافؤ $\bar{a}$ يتكون من كل الأعداد من $\mathbb{Z}$ التي لها نفس الباقي r باقي القسمة على n .

إذن: $\bar{a} = \{a + kn / k \in \mathbb{Z}\}$ أو أيضا : $\bar{a} = \{k \in \mathbb{Z} / x \equiv a\ [n]\}$ أي $\bar{a} = \{k \in \mathbb{Z} / a \equiv x\ [n]\}$ (حسب الانعكاسية)

- أصناف التكافؤ هي : $\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}$.

بمأن : $0 \le r < n$ و $r \in \mathbb{N}$ إذن : $r \in \{0,1,2,3,\cdots,n-1\}$. بالتالي أصناف التكافؤ هي : $\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}$.

إذن : $\bar{0} = \{kn / k \in \mathbb{Z}\} = \{\cdots,-3n,-2n,-n,0,n,2n,3n,\cdots\}$

$\bar{1} = \{kn + 1 / k \in \mathbb{Z}\} = \{\cdots,-3n+1,-2n+1,-n+1,1,n+1,2n+1,3n+1,\cdots\}$

$\bar{2} = \{kn + 2 / k \in \mathbb{Z}\} = \{\cdots,-3n+2,-2n+2,-n+2,2,n+2,2n+2,3n+2,\cdots\}$.

$\bar{3} = \{kn + 3 / k \in \mathbb{Z}\} = \{\cdots,-3n+3,-2n+3,-n+3,3,n+3,2n+3,3n+3,\cdots\}$.

....

$\overline{n-1} = \{kn + n - 1 / k \in \mathbb{Z}\} = \{k'n - 1 / k' \in \mathbb{Z}\} = \{\cdots,-3n-1,-2n-1,-n-1,-1,n-1,2n-1,3n-1,3n+1,\cdots\}$

- المجموعة المخرجة هي:

هذه الأصناف تكون مجموعة هي : $\{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ و تسمى المجموعة المخرجة و يرمز لها ب : $\mathbb{Z}/_{n\mathbb{Z}}$ إذن :

$\mathbb{Z}/_{n\mathbb{Z}} = \{\bar{x} / x \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$.

3. أمثلة :

مثال 1 : $n = 1$. إذن : $\bar{0} = \mathbb{Z}$ $\mathbb{Z}/_{\mathbb{Z}} = \{\bar{0}\}$.

مثال 2 : $n = 2$

إذن : $\bar{0} = \{2k / k \in \mathbb{Z}\} = \{\cdots,-6,-4,-2,0,2,4,6,\cdots\}$ و $\bar{1} = \{2k + 1 / k \in \mathbb{Z}\} = \{\cdots,-5,-3,-1,1,3,5,7,\cdots\}$

و منه : $\mathbb{Z}/_{2\mathbb{Z}} = \{\bar{0}, \bar{1}\}$

مثال 3 : $n = 4$

إذن: $\bar{0} = \{4k / k \in \mathbb{Z}\} = \{\cdots,-12,-8,-4,0,4,8,12,\cdots\}$ و $\bar{1} = \{4k + 1 / k \in \mathbb{Z}\} = \{\cdots,-11,-7,-3,1,5,9,11,\cdots\}$

$\bar{2} = \{4k + 2 / k \in \mathbb{Z}\} = \{\cdots,-10,-6,-2,2,6,10,14,\cdots\}$ و $\bar{3} = \{4k + 3 / k \in \mathbb{Z}\} = \{\cdots,-9,-5,-1,3,7,11,15,\cdots\}$

و منه : $\mathbb{Z}/_{4\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

B. الجمع و الضرب في المجموعة $\mathbb{Z}/_{n\mathbb{Z}}$.

1. تعريف :

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

أ- الجمع في $\mathbb{Z}/_{n\mathbb{Z}}$: $\bar{a} + \bar{b} = \overline{a+b}$.

ب- الضرب في $\mathbb{Z}/_{n\mathbb{Z}}$: $\bar{a} \times \bar{b} = \overline{a \times b} = \overline{ab}$

2. أمثلة :

مثال n=5

جدول $\left(\mathbb{Z}/5\mathbb{Z},+\right)$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

جدول $\left(\mathbb{Z}/5\mathbb{Z},\times\right)$

×	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

3. تمارين تطبيقية :

1. حدد باقي القسمة الإقليدية ل 73^{2014} على 7.

لدينا : $73\equiv 3\ [7]$ إذن : $73^{2014}\equiv 3^{2014}\ [7]$

لدينا : $3^{2014}\equiv\left(3^2\right)^{1007}\equiv 2^{1007}\equiv\left(2^3\right)^{335}\times 2^2\equiv 1^{335}\times 4\equiv 4\ [7]$

خلاصة : 4 هو باقي القسمة الإقليدية ل 73^{2014} على 7.

طريقة 2 :

$73\equiv 3\ [7]$ و $73^2\equiv 3^2\equiv 2\ [7]$ و $73^3\equiv 3^3\equiv 6\ [7]$ و $73^4\equiv 3^4\equiv 4\ [7]$ و $73^5\equiv 3^4\times 3\equiv 4\times 3\equiv 5\ [7]$ و $73^6\equiv 3^6\equiv 3^3\times 3^3\equiv 6\times 6\equiv 35\equiv 1\ [7]$.

و منه : $2014=335\times 6+4$ و بالتالي : $73^{2014}\equiv 73^{335\times 6+4}\equiv 73^{335\times 6}\times 73^4\equiv\left(73^6\right)^{335}\times 73^4\equiv 1^{335}\times 4\equiv 4\ [7]$

خلاصة : 4 هو باقي القسمة الإقليدية ل 73^{2014} على 7.

2. حدد رقم الوحدات للعدد : 24537^{2014} .

لدينا: $24537\equiv 7\ [10]$ إذن : $24537^{2014}\equiv 7^{2014}\equiv\left(7^2\right)^{1007}\equiv 9^{1007}\equiv 9^{2\times 503+1}\equiv\left(9^2\right)^{503}\times 9\equiv 1^{503}\times 9\equiv 9\ [10]$.

إذن باقي القسمة ل 24537^{2014} على 10 هو 9 و منه : $\left(k\in\mathbb{Z}\right)$ $24537^{2014}=10k+9$ و منه رقم الوحدات هو 9.

3. عدد صحيح طبيعي $x=dcba$ حيث رقم الوحدات هو a و رقم العشرات هو b و رقم المئات هو c و رقم الألاف هو d .

بين أن : $x\equiv\left(a-b+c-d\right)\ [11]$.

لدينا : $x=dcba=a\times 10^0+b\times 10^1+c\times 10^2+d\times 10^3$

نعلم أن : $10\equiv -1\ [11]$ إذن : $10^n\equiv\left(-1\right)^n\ [11]$ مع $n\in\mathbb{N}$.

و منه :

$$x\equiv\left(a\times 10^0+b\times 10^1+c\times 10^2+d\times 10^3\right)\ [11]$$

$$x\equiv\left(a\times\left(-1\right)^0+b\times\left(-1\right)^1+c\times\left(-1\right)^2+d\times\left(-1\right)^3\right)\ [11]$$

$$x\equiv\left(a-b+c-d\right)\ [11]$$

خلاصة : $x\equiv\left(a-b+c-d\right)\ [11]$

4. ما هو باقي القسمة ل 24789 على 11.

لدينا : $24789\equiv 9-8+7-4+2\equiv 6\ [11]$.

خلاصة : 6 هو باقي القسمة ل 24789 على 11.

V. القاسم المشترك الأكبر: PGDC

A. قاسم مشترك :

1. تعريف:

ليكن : $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$ (أي $(a,b)\neq(0,0)$) .

- كل عدد d من $\mathbb{Z}$ يقسم كلتا العددين a و b يسمى قاسم مشترك ل a و b.
- كل عدد m من $\mathbb{Z}$ مضاعف في نفس الوقت للعددين a و b يسمى مضاعف مشترك ل a و b .

2. مثال :

قاسم مشترك ل 30 و 48 لدينا كل عدد من الأعداد التالية : 1 و 1- و 2 و 2- و 3 و 3- و 6 و 6- هو قاسم مشترك ل 30 و 48 .

B. القاسم المشترك الأكبر:

1. تعريف:

ليكن : $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$ (أي $(a,b)\neq(0,0)$) .

أكبر قاسم مشترك موجب δ ل a و b يسمى القاسم المشترك الأكبر ل a و b. يرمز له ب: $\delta=pgcd(a,b)$ أو ب : $\delta=a\wedge b$

2. ملحوظة:

- $a\wedge0=|a|$ و $a\wedge1=1$ و $a\wedge(ka)=|a|$ مع $k\in\mathbb{Z}$.
- $(a\wedge b)|a$ و $(a\wedge b)|b$ أي $\delta|a$ و $\delta|b$.

3. خاصيات:

ليكن $(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}$ حيث: $a\wedge b=\delta$. لدينا :

1. $a\wedge b\geq1$.
2. $a\wedge b=b\wedge a$ و $(a\wedge b)\wedge c=a\wedge(b\wedge c)$
3. $a/b\Leftrightarrow a\wedge b=|a|$.
4. كل d قاسم مشترك ل a و b. فهو يحقق $d\leq\delta$ (أي $d\leq a\wedge b$). القواسم المشتركة ل a و b هي قواسم δ.
5. $\frac{a}{\delta}\wedge\frac{b}{\delta}=1$.
6. إذا كان k يقسم a و b. فإن : $pgcd\left(\frac{a}{k},\frac{b}{k}\right)=\frac{1}{|k|}pgcd(a,b)$ و $pgcd(ka,kb)=|k|pgcd(a,b)$.

4. برهان :

نأخذ : $a=\delta a_1$ و $b=\delta b_1$.باستعمال الخلف بين أن : $a_1\wedge b_1=1$ (أي $\frac{a}{\delta}\wedge\frac{b}{\delta}=1$).

جواب :

δ هو قاسم ل a إذن $a=\delta a_1$ مع $a_1\in\mathbb{Z}$. كذلك δ هو قاسم ل b إذن $b=\delta b_1$ مع $b_1\in\mathbb{Z}$.

نفترض بأن : $a_1\wedge b_1=d$ مع $d>1$ (1). إذن d يقسم a_1 و b_1 ومنه $a_1=kd$ و $b_1=k'd$ مع k و k' من $\mathbb{Z}$.

بالتالي : $a=\delta a_1=\delta kd$ و $b=\delta k'd$ ومنه δd قاسم مشترك ل a و b. ومنه $\delta d\leq\delta$ أي $d\leq1$ و هذا يناقض (1).

و بالتالي الافتراض كان خاطئا .

خلاصة : $a_1 \wedge b_1 = d = 1$

3. ملحوظة: يمكن تحديد $pgcd(a,b)$ بثلاثة طرائق:

- تفكيك العددين إلى جداء من العوامل الأولية. (مقر للجذع المشترك علوم و للسنة الأولى علوم رياضية)
- باستعمال القسمات الإقليدية المتتالية (أو المتتابعة) و ذلك بأخذ آخر الباقي الغير المنعدم (خوارزمية أقليديس). (الفقرة الموالية)
- أو استعمال مبرهنة بيزو (Bézout). (الفقرات الموالية)

VI. خوارزمية إقليدس لتحديد $a\wedge b$ L'algorithme d'Euclide pour déterminer $a\wedge b$

A. تمهيدة أقليديس : $pgcd(a,b) = pgcd(a,r)$ مع $b = qa + r$ و $r \neq 0$

1. تمهيدة أقليديس Lemme d'Euclide

> ليكن $b = qa + r$ القسمة الاقليدية ل b من $\mathbb{Z}$ على a من $\mathbb{N}^*$ مع $r \neq 0$. لدينا: $a\wedge b = a\wedge r$.

2. نشاط :

a من $\mathbb{N}^*$ و b من $\mathbb{Z}$ حيث: $b = qa + r$ مع $r \neq 0$. نضع: $a\wedge r = d$ و $a\wedge b = \delta$.

- لدينا: $a\wedge r = d$ إذن : $d|a$ و $d|r$ ومنه : d يقسم تأليفة ل a و r ومنه : $d|(qa+r)$ أي $d|b$.
  لدينا : $d|a$ و $d|b$ إذن $d \leq a\wedge b$ أي $d \leq \delta$ (1) .
- لدينا: $a\wedge b = \delta$ إذن : $\delta|a$ و $\delta|b$ إذن يقسم تأليفة ل a و b. و منه : $\delta|(b-qa)$ أي $\delta|r$.
- $\delta|a$ و $\delta|r$ إذن $\delta|d$ (2).

من خلال : (1) و (2) نحصل على $\delta = d$ أي $a\wedge b = a\wedge r$.خلاصة: $a\wedge b = a\wedge r$

B. خوارزمية أقليديس : Algorithme d'Euclide

1. القسمات المتتالية :

نريد : حساب $pgcd(a,b)$ حيث : a و b من $\mathbb{N}^*$ و $b \geq a$ و $b = aq_1 + r_1$.

- إجراء القسمة ل b على a نحصل على : $b = aq_1 + r_1$ و حسب تمهيدة أقليديس نحصل على $pgcd(a,b) = pgcd(a,r_1)$.
  إذا كان $r_1 = 0$ إذن $pgcd(a,b) = pgcd(a,r_1) = pgcd(a,0) = a$. إذا كان $r_1 \neq 0$ نواصل.
- $a = r_1q_2 + r_2$ و $r_2 = 0$ إذن $pgcd(a,b) = pgcd(a,r_1) = pgcd(r_1,r_2) = r_1$. إذا كان $r_2 \neq 0$ نواصل.
- $r_1 = r_2q_2 + r_3$ و $r_3 = 0$ إذن $pgcd(a,b) = pgcd(a,r_1) = pgcd(r_1,r_2) = pgcd(r_2,r_3) = r_3$. إذا كان $r_3 \neq 0$ نواصل.
- ....
- $r_{k-2} = r_{k-1}q_k + r_k$ و $r_k = 0$ إذن $pgcd(a,b) = pgcd(a,r_1) = pgcd(r_1,r_2) = \cdots = pgcd(r_{k-1},r_k) = r_{k-1}$. إذا كان $r_k \neq 0$ نواصل.
- $r_{k-1} = r_kq_k + 0$ إذن $pgcd(a,b) = pgcd(a,r_1) = pgcd(r_1,r_2) = \cdots = pgcd(r_k,0) = r_k$.

لدينا : في كل مرحلة الباقي أصغر من الخارج ونعلم أن $0 \leq r_{i+1} < r_i$ إذن القسمات المتتالية تتوقف عند باقي سيكون 0 مع
$a > r_1 > r_2 > \cdots > r_k \geq 0$

2. مبرهنة :

> ليكن a من $\mathbb{N}^*$ و b من $\mathbb{Z}$ حيث: a لا يقسم b ، القاسم المشترك الأكبر للعددين a و b هو آخر باقي غير منعدم في طريقة القسمات المتتالية ل b على a .

3. مثال:

مثال 1 و 2 :

مثال 2:	مثال 1:
نحسب : $p\gcd(9945,3003)$	نحسب : $p\gcd(600,124)$
$b=9945$ و $a=3003$	$b=600$ و $a=124$
$b=aq_1+r_1$ $9945=3003\times3+936$ $3003=936\times3+195$ $936=195\times4+156$ $195=156\times1+39$ $156=39\times4+0$	نضع : $b=aq_1+r_1$ $600=124\times4+104$ $124=104\times1+20$ $104=20\times5+4$ $20=4\times5+0$
خلاصة : $p\gcd(9945,3003)=39$	خلاصة : $p\gcd(600,124)=4$

مثال 3 : من خلال القسمات المتتالية ل b على a . استنتج : $3451\wedge275$

نأخذ : $a=275$ و $b=3451$. لدينا:

القسمة 1 : إذن: $3451=275\times12+151$ الباقي هو : $r_1=151$

القسمة 2 : إذن: $275=151\times1+124$ الباقي هو : $r_2=124$

القسمة 3 : إذن: $151=124\times1+27$ الباقي هو : $r_3=27$

القسمة 4 : إذن: $124=27\times4+16$ الباقي هو : $r_4=16$

القسمة 5 : إذن: $27=16\times1+11$ الباقي هو : $r_5=11$

القسمة 6 : إذن: $16=11\times1+5$ الباقي هو : $r_6=5$

القسمة 7 : إذن: $11=5\times2+1$ الباقي هو : $r_7=1$

القسمة 8 : إذن: $5=1\times5+0$ الباقي هو : $r_8=0$

تسمى القسمات المتتالية ل a على b .

$r_7=1$ هو : آخر باقي غير منعدم إذن : القاسم المشترك الأكبر ل $a=275$ و $b=3451$ هو : $r_7=1$

خلاصة : $a\wedge b=3451\wedge275=1$

مثال 4 :

حدد u و v حيث: $3451u+275v=1$.

جواب: لدينا:

$\Leftrightarrow 1=-3\times124+14\times27 \quad ; \rightarrow \quad 11-5\times2=1 \Leftrightarrow 11-(16-11\times1)=1$

$\Leftrightarrow 1=-3\times124+14\times(151-124\times1) \quad ; \quad \Leftrightarrow -16+2\times11=1$

$\Leftrightarrow 1=-17\times124+14\times151 \quad ; \quad \Leftrightarrow -16+2\times11=1$

$\Leftrightarrow 1=-17\times(275-151\times1)+14\times151 \quad ; \quad \Leftrightarrow -16+2\times(27-16\times1)=1$

$\Leftrightarrow 1=-17\times275+31\times151 \quad ; \quad \Leftrightarrow -3\times16+2\times27=1$

$\Leftrightarrow 1=-17\times275+31\times(3451-275\times12) \quad \uparrow\!\rightarrow \quad \Leftrightarrow -3\times(124-27\times4)+2\times27=1$

$\Leftrightarrow -389\times275+31\times3451=1$

ومنه : $u=31$ و $v=-389$ نسميهما معاملي بيزو coefficients de Bézout

VII. عددان أوليان فيما بينهما - الأعداد الأولية: les nombres premiers entre eux – les nombres premiers

A. عددان أوليان فيما بينهما :

1. تعريف :

> a و b من $\mathbb{Z}$. نقول إن عددين a و b أوليان فيما بينهما لنعني أن : $pgcd(a,b)=a\wedge b=1$.

2. مثال :

4 و 15 أوليان فيما بينهما لأن : $4\wedge15=1$.

45 و 21 ليس أوليان فيما بينهما لأن : $45\wedge21=3$.

3. ملحوظة :

a و b من $\mathbb{Z}$ حيث $a\wedge b=d$ لدينا : $\left.\begin{matrix}a=da'\\ b=db'\end{matrix}\right\}$ مع a' و b' من $\mathbb{Z}$ و $a'\wedge b'=1$.

4. تمرين تطبيقي :

نبين : $(a+1)\wedge a=1$, $\forall a\in\mathbb{Z}$. ماذا تستنتج ؟

ليكن d قاسم مشترك ل $a+1$ و a إذن : $d|a$ و $d|(a+1)$ ومنه $d|((a+1)-a)$ (تأليفة خطية ل $a+1$ و a)

إذن $d|1$ ومنه $d=1$ أو $d=-1$ و بالتالي أكبر قاسم مشترك ل $a+1$ و a هو 1 ومنه $(a+1)\wedge a=1$.

نستنتج أن : $a+1$ و a أوليان فيما بينهما.

B. عدد أولي :

1. تعريف:

> ليكن p من $\mathbb{Z}\setminus\{-1,1\}$. نقول إن p هو عدد أولي عندما يكون قواسمه الموجبة فقط هي 1 و p . (أي p ليس له قواسم موجبة فعلية)

2. ملحوظة:

- الأعداد 0 و 1 و -1 ليست بأعداد أولية .
- a أولي يكافئ $-a$ عدد أولي.
- a أولي له 4 قواسم بالضبط هي : 1 و p و -1 و $-p$.
- a عدد ليس بأولي يسمى عدد مركب.

3. أمثلة:

أوجد 10 أعداد أولية: 2 – 3 – 5 – 7 – 11 – 13 – 17 – 19 – 23 – 29 – 31 – 37 – 41 – 43 – 47 – 53 –

C. خاصيات الأعداد الأولية:

1. خاصية :

- a من $\mathbb{Z}\setminus\{-1,0,1\}$. إذا كان $d>1$ أصغر قاسم ل a فإن d عدد أولي .
- إذا كان $d>1$ أصغر قاسم ل a غير أولي من $\mathbb{N}^*\setminus\{1\}$ فإن d هو عدد أولي و $1<d\le\sqrt{a}$. (أي $2\le d\le\sqrt{a}$)

2. برهان :

- نفترض أن : d ليس بعدد أولي . (1)

إذن d يقبل قاسم فعلي موجب d' (أي $d'\notin\{1,d\}$) إذن $1<d'<d$ (1)

بما أن $d'|d$ و $d|a$ فإن $d'|a$ (2) .

من خلال (1) و (2) إذن d' هو أصغر قاسم ل a و هذا يناقض d أصغر قاسم ل a .

إذن الافتراض كان خاطئا و الصحيح هو d عدد أولي .

خلاصة : a عدد أولي.

- a ليس بعدد أولي نبين $d\le\sqrt{n}$.

$d|a$ إذن $a=dd'$ و لدينا : $d>1$ و $d<a$ (لأن a ليس بأولي إذن له قاسم فعلي) .

$d'|a$ و $d'>1$ و بما أن d أصغر قاسم إذن $d'\ge d$.

من خلال $d'\ge d$ نحصل على $d\times d'\ge d^2$ (الضرب ب d) أي $a\ge d^2$ أي $a\ge\sqrt{d}$ ومنه : $\sqrt{d}\le a$.

خلاصة : $\sqrt{d}\le a$

D. طريقة تحديد الأعداد الأولية :

1. ملحوظة :

حسب الخاصية السابقة :
لكي نتحقق أن عدد صحيح طبيعي $a>1$ هو عدد أولي أو ليس بعدد أولي

- معرفة جميع الأعداد الأولية p و التي تحقق $p\in\left[2,\sqrt{a}\right]$.
- إذا كانت جميع الأعداد الأولية p (مع $p\in\left[2,\sqrt{a}\right]$) لا تقسم a فإن العدد a أولي .
- إذا كان عدد أولي p من بين هذه الأعداد (مع $p\in\left[2,\sqrt{a}\right]$) يقسم a فإن العدد a غير أولي .

2. أمثلة:

مثال 1:

$a=109$ لدينا: $\sqrt{a}<11$ و منه الأعداد الأولية p حيث $2\le p\le\sqrt{109}<11$ هي 2 و 3 و 5 و 7 فهي لا تقسم 109 إذن 109 عدد أولي.

مثال 2:

$a=173$ لدينا: $\sqrt{a}<14$ و منه الأعداد الأولية p حيث $2\le p\le\sqrt{173}<14$ هي: 2 و 3 و 5 و 7 و 11 و 13 فهي لا تقسم 173 إذن 173 عدد أولي.

E. مجموعة الأعداد الأولية غير منتهية:

1. خاصية :

مجموعة الأعداد الأولية غير منتهية.

2. برهان :

لتكن P مجموعة الأعداد الأولية الموجبة .

- لينا : $P \neq \varnothing$ (لأن $5 \in P$) .
- نستدل على ذلك بالخلف: نفترض أن : P مجموعة منتهية (أي P تحتوي على عدد منتهي من الأعداد الأولية). نضع : $P = \{p_1, p_2, p_3, ..., p_n\}$.
- نعتبر العدد $N = p_1 \times p_2 \times \cdots \times p_n + 1$.
- N عدد صحيح طبيعي $N > 1$ نضع d أصغر قاسم ل N إذن d عدد أولي ومنه : d ينتمي إلى P (لأنها تحتوي على جميع الأعداد الأولية) ومنه d يقسم العدد $p_1 \times p_2 \times \cdots \times p_n$ أي d يقسم $N - p_1 \times p_2 \times \cdots \times p_n$ إذن d يقسم 1 وبالتالي $d = 1$ (نهتم فقط بالأعداد الموجبة) .
- $d = 1$ غير ممكن لأن d عدد أولي (أو $1 \notin P$) .
- الافتراض P مجموعة منتهية غير ممكن و بالتالي P مجموعة غير منتهية .

خلاصة : P مجموعة غير منتهية.

F. التفكيك إلى جداء عوامل أولية:

1. مبرهنة:

$a \in \mathbb{Z} \setminus \{-1, 0, 1\}$.
- توجد أعداد أولية موجبة p_1 و p_2 و ..... و p_n حيث $1 < p_1 < p_2 < \cdots < p_n$.
- توجد أعداد وحيدة α_1 و α_2 و α_3 و ..... α_n من $\mathbb{N}^*$.
- حيث a يكتب على شكل وحيد (أو أيضا a يفكك على شكل وحيد إلى جداءات من العوامل الأولية):

أ- إذا كان a من $\mathbb{N} \setminus \{0, 1\}$: $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \cdots \times p_n^{\alpha_n}$.

ب- إذا كان a من $\mathbb{Z}^- \setminus \{0, -1\}$: $a = -p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \cdots \times p_n^{\alpha_n}$.

2. ملحوظة :

السبب الوحيد الذي جعل عدم اختيار العددين 1 و -1 بأنهما غير أوليين هو التفكيك للعدد a يصبح غير وحيد :

مثال 1: $a = 45 = 3^2 \times 5 = 1 \times 3^2 \times 5 = 1^2 \times 3^2 \times 5 = 1^3 \times 3^2 \times 5 = \cdots$.

مثال 2 : $a = -45 = -3^2 \times 5 = (-1)^3 \times 3^2 \times 5$.

3. أمثلة:

مثال 1 : $a = 1980$ مثال 2 : $b = 7^5 - 7$ مثال 3 : $c = -1980$

1980	2
990	2
495	3
165	3
55	5
11	11
1	

$b = 7(7^2 - 1)(7^2 + 1)$

$b = 7 \times 48 \times 50$

$b = 7 \times 8 \times 6 \times 2 \times 5^2$

$b = 2^5 \times 3 \times 5^2 \times 7$

و منه : $a = 1980 = 2^2 \times 3^2 \times 5 \times 11$ و منه : $b = 7^5 - 7 = 2^5 \times 3 \times 5^2 \times 7$ لدينا : $c = -1980 = -2^2 \times 3^2 \times 5 \times 11$

VIII. مبرهنة بيزو : Théorème de Bézout مبرهنة كوس Théorème de Gauss

A. مبرهنة بيزو : Théorème de Bézout (Etienne Bézout 1730-1783 mathématicienne français)

1. مبرهنة : Bézout

يوجد زوج (u_0, v_0) من $\mathbb{Z}^2$ حيث: $u_0 a + v_0 b = pgcd(a, b)$. مع a و b من $\mathbb{Z}$ حيث $(a, b) \neq (0, 0)$

2. ملحوظة :

- المبرهنة نتيجة لخوارزمية إقليدس .
- العددان u_0 و v_0 ليس بوحدين نسميهما معاملي بيزو .
- نحصل على u_0 و v_0 بشكل "تصاعدي" لخوارزمية أقليديس. حيث نعوض الباقي في السطر i عندما نواصل في السطر الموالي $i-1$ حسب ما هو مكتوب في هذا السطر $i-1$ (ودائما الطرف الأول للمتساوية يكون آخر باقي غير منعدم (حسب المثال الموالي آخر باقي هو $r=4$) تابع المثال التالي .
- إذا كان $au+bv=d$ مع u و v من $\mathbb{Z}$ فليس بالضرورة $a\wedge b=d$. (مثال مضاد: $6\times3+3\times(-5)=3$ ولكن $6\wedge3=3$)

3. مثال :

		مثال
		نحسب : $pgcd(600,124)$
طريقة تحديد معاملي بيزو		$a=124$ و $b=600$
$4=124\times(-5)+(600-124\times4)\times6=600\times6+124\times(-29)$ $4=104-(124-104\times1)\times5=124\times(-5)+104\times6$ $4=104-20\times5$		نضع : $b=aq_1+r_1$ $600=124\times4+104$ $124=104\times1+20$ $104=20\times5+4$ $20=4\times5+0$
معاملي بيزو هما $v=-29$ و $u=6$ إذن : $6\times600+(-29)\times124=4$		خلاصة : $pgcd(600,124)=4$

4. لازمة 1 : Corollaire 1 لمبرهنة Bezout :

a و b من $\mathbb{Z}$ حيث $(a,b)\neq(0,0)$. لدينا التكافؤ التالي : $a\wedge b=1\Leftrightarrow\left(\exists(u,v)\in\mathbb{Z}^2 : ua+vb=1\right)$.

5. برهان :

$\Rightarrow$ الاستلزام المباشر : هو نتيجة لمبرهنة بيزو Bézout

$\Leftarrow$ العكس: نفترض أنه يوجد عددان صحيحة نسبية u و v حيث $ua+vb=1$ نبين أن: $pgcd(a,b)=1$.

نضع : $pgcd(a,b)=g$ إذن $g|au$ و $g|bv$ ومنه $g|au+bv$ (تأليفة خطية) .إذن $g=1$ (لأن $ua+vb=1$) إذن : $a\wedge b=1$

6. لازمة :

a و b من $\mathbb{Z}$ حيث $pgcd(a,b)=d$. يوجد u و v من $\mathbb{Z}$ حيث $au+bv=d$.

7. لازمة 2 : Corollaire 2 لمبرهنة Bézout :

a و b من $\mathbb{Z}$ حيث $(a,b)\neq(0,0)$ لدينا التكافؤ التالي :

$$pgcd(a,b)=d\Leftrightarrow\begin{cases}\exists(a',b')\in\mathbb{Z}^2 : a'\wedge b'=1\\ a=a'd\\ b=b'd\end{cases}$$

8. برهان :

⇐ الاستلزام المباشر : إذا كان $pgcd(a,b)=d$ إذن يوجد a' و b' من $\mathbb{Z}$ حيث $a=a'd$ و $b=b'd$ ليكن $a'\wedge b'=k$ إذن kd يقسم كل من a و b ومنه : $|kd|\le d$ أي $d|k|\le d$ (لأن $d>0$) ومنه $|k|\le 1$ إذن $k=1$.

⇒ الاستلزام العكسي : نفترض أن $a'\wedge b'=1$: $\exists(a',b')\in\mathbb{Z}^2$ و $a=a'd$ و $b=b'd$ ومنه d قاسم مشترك لـ a و b.

وبما أن : $a'\wedge b'=1$ حسب مبرهنة Bézout يوجد u و v من $\mathbb{Z}$ حيث $a'u+b'v=1$ ومنه : $d(a'u+b'v)=1\times d$ أي $au+bv=d$ ومنه كل عدد يقسم a و b فهو يقسم d ومنه d هو أكبر قاسم مشترك لـ a و b وبالتالي : $pgcd(a,b)=d$.

خلاصة : التكافؤ صحيح .

B. مبرهنة كوس théorème de Gauss

1. مبرهنة : Gauss

> $(a,b)\in(\mathbb{Z}^*)^2$. لدينا الاستلزام التالي : $\left.\begin{array}{l} a\mid bc \\ a\wedge b=1\end{array}\right\}\Rightarrow a\mid c$

2. برهان :

نبين أن a/c .

- لدينا : $pgcd(a,b)=1$ إذن حسب مبرهنة Bezout يوجد عددان صحيحة نسبية u و v حيث $ua+vb=1$ و منه: $cau+cbv=c$ (1)
- و نعلم أن : a/bc (2) إذن حسب : (1) و $a\mid cau$ نستنتج أن : a تقسم ($cau+cbv=c$ تأليفة خطية) ومنه a/c .

3. ملحوظة :

شرط ضروري $a\wedge b=1$ مثال مضاد : 1: يقسم $4\times5=20$ و 10 لا يقسم 4 (لأن $10\wedge4\ne1$) و كذلك 10 لا يقسم 5 (لأن $10\wedge5\ne1$).

4. مثال:

لدينا : 5 تقسم 70 و $10\times7=70$ و 5 أولي مع 7 إذن حسب مبرهنة كوس 5 تقسم 10.

5. خاصية :

> a و b و c من $\mathbb{Z}$. لدينا الاستلزام التالي : $\left.\begin{array}{l} a\mid c \\ b\mid c \\ a\wedge b=1\end{array}\right\}\Rightarrow ab\mid c$

6. برهان :

لدينا : $a\mid c$ إذن $c=c'a$ و لدينا $b\mid c$ ومنه $b\mid c'a$.

ومنه : $b\mid c'a$ و $a\wedge b=1$ إذن $b\mid c'$ (حسب Gauss) ومنه $c'=kb$ مع $k\in\mathbb{Z}$ و بالتالي $c=kab$ أي ab يقسم c

خلاصة : $ab\mid c$.

7. خاصية :

> a و b و c من $\mathbb{Z}$. لدينا الاستلزام التالي : $\left.\begin{array}{l} a\wedge b=1 \\ a\wedge c=1\end{array}\right\}\Rightarrow a\wedge(bc)=1$

8. برهان :

لدينا :

$a\wedge b=1\Rightarrow(\exists(u_0,v_0)\in\mathbb{Z}^2 : au_0+bv_0=1)$.

. $a\wedge c=1 \Rightarrow \left(\exists(u_1,v_1)\in\mathbb{Z}^2 : au_1+cv_1=1\right)$

ومنه : $(au_0+bv_0)(au_1+cv_1)=1$

إذن : $a(au_0u_1+cu_0v_1+bv_0u_1)+bcv_0v_1=1 \quad (1)$

نضع : $u=au_0u_1+cu_0v_1+bv_0u_1$ و $v=v_0v_1$ مع u و v من $\mathbb{Z}$ ومنه (1) تكتب على الشكل التالي: $au+(bc)v=1$.

حسب مبرهنة Bézout نستنتج أن : $a\wedge bc=1$.

9. نتائج :

- إذا كان $p\gcd(a,b)=d$ فإن $a^n\wedge b^m=1$ و ذلك لكل m و n من $\mathbb{Z}$.
- x و y و a من $\mathbb{Z}$ لدينا : $x\equiv y\ [n] \Rightarrow (ax\equiv ay\ [n]$ و $a\wedge n=1)$.

C. حل المعادلة : $(x,y)\in\mathbb{Z}\times\mathbb{Z}/ax+by=c$ مع a و b و c من $\mathbb{Z}$ $ax+by=c$ équations diophantiennes

1. تعريف :

كل معادلة مجاهلها أعداد صحيحة (من $\mathbb{Z}$) و معاملاتها من $\mathbb{Z}$ تسمى معادلة diophantienne. (نسبة للعالم الرياضي Diophante).

2. أمثلة :

1. $x\in\mathbb{Z}/x^3=2k-5$
2. $(x,y,z)\in\mathbb{Z}^3 / 2x+3y^2=z$
3. $x\in\mathbb{Z}/ 2!+4!+6!+\cdots+(2n)!=2x^2$

3. خاصية 2 :

نعتبر المعادلة $(x,y)\in\mathbb{Z}\times\mathbb{Z}/ax+by=c \ : \ (E)$ حيث معاملاتها a و b و c من $\mathbb{Z}^*$.

- مجموعة حلول المعادلة (E) غير فارغ إذا وفقط إذا كان $a\wedge b=d$ يقسم c .
- في حالة $a\wedge b=d$ يقسم c مجموعة حلول المعادلة (E) هي $S=\{(x_0+kb',y_0-ka')/k\in\mathbb{Z}\}$ مع (x_0,y_0) حل خاص للمعادلة (E).

4. برهان :

1. نبرهن على صحة الخاصية 1

- $\Rightarrow$ الاستلزام المباشر :

ليكن (x_1,y_1) من S (مع $S\neq\varnothing$) مجموعة حلول المعادلة (E) إذن $ax_1+by_1=c$ ومنه $a'dx_1+b'dy_1=c$ (لأن $a=a'd$ و $b=b'd$ مع $a\wedge b=d$ و $a'\wedge b'=1$) ومنه $d(a'x_1+b'y_1)=c$ أي $dk=c$ ومنه d يقسم c .

إذن : الاستلزام المباشر صحيح .

- $\Leftarrow$ الاستلزام العكسي :

نعتبر d يقسم c ومنه : $\exists c'\in\mathbb{Z} : c=dc'$.

بما أن : $a'\wedge b'=1$ حسب مبرهنة بيزو Bézout إذن $\exists u,v\in\mathbb{Z} \ : \ a'u+b'v=1$

ومنه : $\exists u,v\in\mathbb{Z} \ : \ dc'(a'u+b'v)=dc'\times 1=c \ ; \ (c=dc')$

أي : $\exists u,v\in\mathbb{Z} \ : \ a(c'u)+b(c'v)=c \ ; \ (a=da' \ , \ b=db')$

وهذا يثبت أن S غير فارغ

- خلاصة : مجموعة حلول المعادلة (E) غير فارغ إذا وفقط إذا كان $a\wedge b=d$ يقسم c .

2. نبرهن على صحة الخاصية 1

بما أن $a\wedge b=d$ إذن يوجد a' و b' من $\mathbb{Z}$ حيث $a'\wedge b'=1$ و $a=da'$ و $b=db'$. (1)

$a\wedge b=d$ يقسم c نحدد مجموعة حلول المعادلة (E).

بمأن $a\wedge b=d$ يقسم c إذن : $\exists c'\in\mathbb{Z} : c=dc'$ (2) و مجموعة حلول المعادلة (E) تحقق ما يلي $S\neq\varnothing$.

ليكن (x_0,y_0) من S إذن $ax_0+by_0=c$ أي. $a'dx_0+b'dy_0=dc'$ (3) حسب (1) و (2)

لنعتبر (x,y) حل للمعادلة (E) إذن (x,y) من S و بالتالي $ax+by=c$ أي. $a'dx+b'dy=dc'$ (4) حسب (1) و (2)

الفرق ل (3) و (4) يعطي لنا : $a'd(x-x_0)+b'd(y-y_0)=0$ أي. $d\left(a'(x-x_0)+b'(y-y_0)\right)=0$ أي

$a'(x-x_0)+b'(y-y_0)$ (لأن $d\neq 0$) ومنه : $a'(x-x_0)=b'(y_0-y)$ (5)

بمأن : $pgcd(a',b')=1$ و حسب مبرهنة Gauss نستنتج أن : b' تقسم الجداء $(x-x_0)$.

بالتالي : يوجد k من $\mathbb{Z}$ حيث : $x-x_0=kb'$ أي $x=x_0+kb'$.

نعوض في العلاقة (5) : $a'(x-x_0)=b'(y_0-y)$ نحصل على :

$$\begin{aligned}(5)&\Leftrightarrow a'kb'=b'(y_0-y)\\&\Leftrightarrow a'k=y_0-y\\&\Leftrightarrow y=y_0-ka'\end{aligned}$$

ومنه الزوج $(x,y)=(x_0+kb',y_0-ka')$ حيث $k\in\mathbb{Z}$.

خلاصة : $a\wedge b=d$ يقسم c مجموعة حلول المعادلة (E) هي : $S=\left\{(x_0+kb',y_0-ka')/k\in\mathbb{Z}\right\}$.

5. طريقة : METHODE مراحيل لحل المعدلات من نوع : $(x,y)\in\mathbb{Z}\times\mathbb{Z}/ax+by=c$: (E)

A. نختزل ب : $d=a\wedge b$ (أي ب $d=pgcd(a,b)$. وفي هذه المرحلة هناك حالتين .

أ- إذا كان $a\wedge b$ لا يقسم c المعادلة ليس لها حل إذن مجموعة المعادلة هي $S=\varnothing$.

ب- إذا كان $a\wedge b$ يقسم c المعادلة (E) ترجع كتابتها على ما يلي : $a'x+b'y=c'$ (لأن $a=da'$ و $b=db'$ و $c=dc'$)

مع العلم أن a' و b' أوليان فيما بينهما .

B. نبحث عن حل خاص (x_0,y_0) (نحصل على الحل الخاص و هما معاملي Bézout بعد إجراء القسمات المتتاليات بين a' و b' أو

نلاحظ بأن هناك حل خاص عندما يكون ل a' و b' قيمتين صغيرتين بالخصوص أو التمرين يطلب من التحقق من حل خاص) .

C. نبحث عن الحل العام : و ذلك بأجراء الفرق بين المعادلة التي تمثل الحل العام و الأخرى التي تمثل الحل الخاص ونحصل على ما يلي :

$a'(x-x_0)+b(y-y_0)=0$ ومن بعد ذلك نستعمل مبرهنة Gauss لنستنتج أن الحلول هي الأزواج التي على شكل :

(x_0+kb',y_0-ka') مع $k\in\mathbb{Z}$ و (x_0,y_0) حل خاص للمعادلة (E).(غير مجدي بحفظ هذه الصيغة و لكن يجب معرفة اتباع هذه المراحل) .

6. ملحوظة :

للحصول على حل خاص نستعمل المعادلة $a'x+b'y=c'$ هناك عدة طرائق :

طريقة 1 : نلاحظ بأن هناك حل خاص عندما يكون ل a' و b' قيمتين صغيرتين

مثال : $5x+6y=17$ نلاحظ أن الزوج $(x_0,y_0)=(1,2)$ حل للمعادلة.)

طريقة 2 : التمرين يطلب بالتحقق بأن الزوج كذا يحقق المعادلة .

طريقة 3 :

بمأن $pgcd(a',b')=1$ حسب مبرهنة Bézout يوجد زوج (u,v) من $\mathbb{Z}$ حيث : $a'u+b'v=1$. (يمكن استعمال القسمات المتتالية لتحديد (u,v) انظر الفقرات السابقة)

ضرب في c' نحصل على : $c'a'u+c'b'v=c\times 1$.

ومنه الزوج : $(u,v)=(uc',vc')$ هو حل خاص للمعادلة $a'u+b'v=c'$ (و كذلك حل خاص للمعادلة ل $(E) : ax+by=c$)

7. أمثلة.

1. نحل المعادلة : $(E) : 6x+8y=3$.

لدينا $=6$ و $b=8$ و $c=3$ و $pgcd(6,8)=2$ غير قاسم ل $c=3$.

خلاصة : إذن المعادلة المقترحة ليس لها حل .

2. نحل المعادلة : $(E) : 6x+8y=14$.

- أول خطوة : نبدأ بتبسيط المعادلة (ب 2) :إذن نحصل على $(E') : 3x+4y=7$.
- ثاني خطوة : نبحث عن حل خاص للمعادلة (E').

لهذا ، يجب تحديد زوج (u,v) من $\mathbb{Z}^2$ يحقق (E') أي: $3u+4v=7$.

لدينا : $pgcd(3,4)=1$ حسب مبرهنة Bézout يوجد زوج (u,v) من $\mathbb{Z}$ حيث : $3u+4v=1$

هذه الحالة بسيطة يمكن ذهنيا تحديد (u,v) وذلك باستعمال مضاعفات العددين 3 و 4.

مضاعفات 3 : 3 – 6 – 9 -12 – 15 .... مضاعفات 4 : 4 – 8 – 12 – 16 ....

يكفي أن نجد مضاعفين حيث فرقيهما يكون 1 .

نأخذ مثالا : $3\times 3+4(-2)=1 \Leftrightarrow 9-8=1$. ومنه : الزوج $(u,v)=(3,-2)$ يحقق المعادلة $3u+4v=1$.

ومنه الزوج : $(7u,7v)=(21,-14)$ هو حل خاص للمعادلة (E') و بالتالي هو حل خاص للمعادلة (E) .

ملحوظة : يمكن استعمال القسمات المتتالية لتحدد (u,v) انظر الفقرات السابقة .

- ثالث خطوة : نحدد الحل العام .

نضع : (x,y) زوج حل ما ل (E') (ملحوظة 1 : نعلم بأنه يوجد زوج حل حسب الخاصية السابقة) (ملحوظة 2 : يمكنك أن تضع : (x,y) زوج حل ما ل (E) ولكن في المراحل الموالية يجب الاختزال ب 2 قبل استعمال مبرهنة Gauss إذن استعمال (E') أفضل)

- نضع النظمة المتكونة من هذا الحل و الحل الخاص ل (E') : $\begin{cases} 3u+4v=7 \\ 3\times 7u+4\times 7v=7 \end{cases}$.
- ثم الفرق طرف بطرف نحصل على: $3(x-7u)+4(y-7v)=0$

$$3(x-7u)=4(7v-y)$$

$$3(x-7\times 3)=4(7\times(-2)-y)$$ (نعوض u v بقمتيهما) أي $(u,v)=(3,-2)$)

$$3(x-21)=4(-14-y) \quad (I)$$

- نستنتج 4 يقسم الجداء $3(x-7\times 3)$ إذن 4 يقسم $x-21$ (لأن $pgcd(3,4)=1$ حسب مبرهنة Gauss).
- إذن يوجد k من $\mathbb{Z}$ حيث : $x-2=4k$ أي $x=21+4k$.
- نعوض في المعادلة (I) نحصل على: $3\times 4k=4(-14-y)$

$$3\times k=-14-y$$

$$y=-14-3k$$

خلاصة : $(x,y)=(21+4k,-14-3k)$ حيث k من $\mathbb{Z}$ هي حلول المعادلة .

D. القاسم المشترك الأكبر لعدة أعداد نسبية :

1. تعريف :

ليكن $a_1,a_2,a_3,\cdots$ و a_n أعداد من $\mathbb{Z}$ ليست كلها منعدمة .
أكبر قاسم مشترك لهذه الأعداد يسمى القاسم المشترك الأكبر لها .
نرمز له ب : $a_1\wedge a_2\wedge a_3\cdots\wedge a_n$ أو أيضا $p\gcd(a_1,a_2,a_3,\cdots,a_n)$.

2. ملحوظة :

- أي عدد d قاسم مشترك للأعداد $a_1,a_2,a_3,\cdots$ و a_n فهو يقسم $a_1\wedge a_2\wedge a_3\cdots\wedge a_n$
- يحقق : $d\leq p\gcd(a_1,a_2,a_3,\cdots,a_n)$.
- حالة : $a_1\wedge a_2\wedge a_3\cdots\wedge a_n=1$ نقول أن الأعداد $a_1,a_2,a_3,\cdots$ و a_n أولية فيما بينها في مجموعها .
- $\left(\exists(u_1,u_2,u_3,\cdots,u_n)\in\mathbb{Z}^n : a_1u_1+a_2u_2+\cdots+a_nu_n=p\gcd(a_1,a_2,a_3,\cdots,a_n)\right)$

3. مبرهنة بيزو : Théorème de Bézout

$a_1,a_2,a_3,\cdots$ و a_n أولية فيما بينها إذا و فقط إذا كان : $\left(\exists(u_1,u_2,u_3,\cdots,u_n)\in\mathbb{Z}^n : a_1u_1+a_2u_2+\cdots+a_nu_n=1\right)$

4. مثال:

نحدد : $45\wedge18\wedge51$.
لدينا : $45\wedge18\wedge51=(45\wedge18)\wedge51=(9(5\wedge2))\wedge(3\times17)=(9\times1)\wedge(3\times17)=3(3\wedge17)=3\times1=3$.
خلاصة : $45\wedge18\wedge51=3$.

IX. المضاعف المشترك الأصغر:

A. المضاعف المشترك الأصغر:

1. تعريف:

ليكن : $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$.
أصغر مضاعف مشترك موجب قطعا ل a و b يسمى المضاعف المشترك الأصغر ل a و b و يرمز له ب: $ppcm(a,b)$ أو أيضا: $a\vee b$. نأخذ m كقيمة ل $a\vee b$ ومنه $a\vee b=m$.
لدينا: $a\vee1=a$.

2. ملحوظة:

$m=ka$ مع $k\in\mathbb{Z}$ و $m=k'b$ مع $k'\in\mathbb{Z}$.
أصغر عنصر من المجموعة $(a\mathbb{Z}\cap b\mathbb{Z})\cap\mathbb{N}^*$ هو $a\vee b$

3. مثال :

أوجد : $36\vee(-30)$.
لدينا: $36=4\times9=2^2\times3^2$ و $30=6\times5=2\times3\times5$ و منه : $36\vee(-30)=2^2\times3^2\times5=180$.

4. نشاط:

من خلال : أصغر عنصر من المجموعة $(a\mathbb{Z}\cap b\mathbb{Z})\cap\mathbb{N}^*$ هو $a\vee b$.

1. بين أن : $a \vee b = b \vee a$.
2. بين أن: (a يقسم b) $\Leftrightarrow$ $a \vee b = |b|$.
3. بين أن : إذا كان M مضاعف مشترك غير منعدم ل a و b فإن $m \leq |M|$.

جواب:

1. نبين أن : $a \vee b > 0$
أصغر عنصر من المجموعة $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*$ هو $a \vee b$. إذن : $a \vee b \in (a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^*$ ومنه : $a \vee b \in \mathbb{N}^*$ ومنه: $a \vee b > 0$.
2. نبين أن : $a \vee b = b \vee a$
من خلال : $(a\mathbb{Z} \cap b\mathbb{Z}) \cap \mathbb{N}^* = (b\mathbb{Z} \cap a\mathbb{Z}) \cap \mathbb{N}^*$ إذن: $a \vee b = b \vee a$.
3. نبين أن : (a يقسم b) $\Leftrightarrow$ $a \vee b = |b|$.
(a يقسم b) يكافئ $b\mathbb{Z} \subset a\mathbb{Z}$
يكافئ $b\mathbb{Z} \cap a\mathbb{Z} = b\mathbb{Z}$
يكافئ $(b\mathbb{Z} \cap a\mathbb{Z}) \cap \mathbb{N}^* = b\mathbb{Z} \cap \mathbb{N}^*$
يكافئ $a \vee b = |b|$.
4. نبين أن : إذا كان M مضاعف مشترك غير منعدم ل a و b فإن $m \leq |M|$.

5. خاصيات:

ليكن : $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ حيث: $a \vee b = m$.

1. $a \vee b = b \vee a$.
2. كل من a و b يقسمان $a \vee b$.
3. (a يقسم b) $\Leftrightarrow$ $a \vee b = |b|$.
4. إذا كان M مضاعف مشترك غير منعدم ل a و b فإن $m \leq |M|$.
5. m يقسم ab .

X. تحديد القاسم المشترك الأكبر – المضاعف المشترك الأصغر باستعمال التفكيك إلى جداء من العوامل الأولية:

A. القسمة بعدد أولي p :

1. نشاط:

ليكن : $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*$ حيث: $a \vee b = m$ و $a \wedge b = \delta$. p عدد أولي.

1. بين أن : p لا يقسم a $\Leftrightarrow$ $a \wedge p = 1$.
2. أعط الخاصية.

جواب:

القواسم الموجبة ل p هي 1 و $|p|$ إذن : $a \wedge p = 1$ أو $a \wedge p = |p|$. وبالتالي : p يقسم a $\Leftrightarrow$ $a \wedge p = |p|$.

إذن : نفي التكافؤ هو : p لا يقسم a $\Leftrightarrow$ $a \wedge p \neq |p|$. يصبح p لا يقسم a $\Leftrightarrow$ $a \wedge p = 1$.

2. خاصية:

ليكن : $a \in \mathbb{Z}$ و p عدد أولي لدينا : p لا يقسم a $\Leftrightarrow$ $a \wedge p = 1$.

3. خاصية :

ليكن : $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$ و p عدد أولي.

إذا كان : p يقسم ab فإن : p يقسم a أو p يقسم b .

4. خاصية:

p و p_1 و p_2 و ...... p_n أعداد أولية موجبة .

إذا كان p يقسم الجداء $p_1\times p_2\times p_3\times\cdots\times p_n$ فإن p يساوي أحد العوامل p_i مع $i\in\{1,2,3,\cdots,n\}$ (أي يوجد i حيث $p=p_i$)

B. عدد قواسم a :

1. مبرهنة :

$a\in\mathbb{Z}\setminus\{-1,0,1\}$ حيث تفكيك a إلى جداء من عوامل أولية هو $a=\varepsilon p_1^{\alpha_1}\times p_2^{\alpha_2}\times p_3^{\alpha_3}\times\cdots\times p_n^{\alpha_n}$.

لدينا : القواسم الموجبة ل a هي : $d=p_1^{\gamma_1}\times p_2^{\gamma_2}\times p_3^{\gamma_3}\times\cdots\times p_n^{\gamma_n}$ حيث $\gamma_1\in\{0,1,\cdots,\alpha_1\}$ و $\gamma_2\in\{0,1,\cdots,\alpha_2\}$ و .... و $\gamma_n\in\{0,1,\cdots,\alpha_n\}$.

2. ملحوظة:

عدد القواسم الموجبة ل a هو $(\alpha_1+1)(\alpha_2+1)\times\cdots\times(\alpha_n+1)$

عدد القواسم الموجبة و السالبة ل a هو $2\times(\alpha_1+1)(\alpha_2+1)\times\cdots\times(\alpha_n+1)$

3. تطبيق:

نعتبر العدد $a=60=2^2\times3\times5$ عدد الواسم الموجبة ل a هي $(\alpha_1+1)(\alpha_2+1)\times(\alpha_3+1)=(2+1)(1+1)(1+1)=12$

C. تفكيك a و b من أجل تحديد $a\vee b$ و $a\wedge b$:

1. مفردات و رموز :

- أصغر العددين : $a=13$ و $b=17$ هو 13 نرمز له ب $\inf(13,17)=13$ أو أيضا $\inf(a,b)=13$.
- أكبر العددين : $a=13$ و $b=17$ هو 17 نرمز له ب $\sup(13,17)=17$ أو أيضا $\inf(a,b)=13$.

2. خاصية :

ليكن: $(a,b)\in\mathbb{Z}^*\times\mathbb{Z}^*$ حيث : $a=\varepsilon p_1^{\alpha_1}\times p_2^{\alpha_2}\times p_3^{\alpha_3}\times\cdots\times p_n^{\alpha_n}$ و $b=\varepsilon' p_1^{\beta_1}\times p_2^{\beta_2}\times p_3^{\beta_3}\times\cdots\times p_n^{\beta_n}$ مع $\varepsilon=\pm$ و $\varepsilon'=\pm$

- $a\wedge b=p\gcd(a,b)=p_1^{\gamma_1}\times p_2^{\gamma_2}\times p_3^{\gamma_3}\times\cdots\times p_n^{\gamma_n}$ مع $\gamma_i=\inf(\alpha_i,\beta_i)$ و $i\in\{0,1,\cdots,n\}$.
- $a\vee b=\mathrm{ppcm}(a,b)=p_1^{\sigma_1}\times p_2^{\sigma_2}\times p_3^{\sigma_3}\times\cdots\times p_n^{\sigma_n}$ مع $\sigma_i=\sup(\alpha_i,\beta_i)$ و $i\in\{0,1,\cdots,n\}$.

3. تطبيق: نأخذ : $a=-60=-2^2\times3\times5$ و $b=130=2\times5\times13$.

لدينا: $130\wedge60=P.G.D.C(130,60)=2^1\times3^0\times5^1\times13^0=2\times5=10$.

$130\vee60=P.P.M.C(130,60)=2^2\times3^1\times5^1\times13^1=4\times3\times5\times13=780$.

XI. مبرهنة فيرما : petit théorème de Fermat (Fermat Pierre 1601-1665)

1. تمهيدة :

p عدد أولي موجب لدينا لكل k من $\mathbb{N}^*$ حيث $1 \le k \le p-1$: لدينا p يقسم C_p^k .

2. برهان :

لدينا : $C_p^k = \dfrac{p!}{k!(p-k)!}$ ومنه : $p! = k!(p-k)!C_p^k$.

و بالتالي : p يقسم $p! = k!(p-k)!C_p^k$ ؛ بما أن : $1 \le k \le p-1$ إذن p لا يقسم $k!$ و كذلك p لا يقسم $(p-k)!$.

إذن : p يقسم C_p^k .

خلاصة : p يقسم C_p^k .

3. مبرهنة فيرما : petit théorème de Fermat

p عدد أولي موجب و a من $\mathbb{Z}$ لدينا : $a^p \equiv a\ [p]$ (أي p يقسم $a^p - a$) .

4. برهان :

نضع $a = n$ مع a من $\mathbb{Z}$ ونبين أن : $n^p \equiv n\ [p]\ \ (1)$

حالة 1 : $n \in \mathbb{N}$. نستدل على ذلك بالترجع :

- نتحقق أن : العلاقة صحيحة ل $n = 0$ لدينا p يقسم $0^p - 0 = 0$ ومنه : $0^p \equiv 0\ [p]$ إذن العلاقة (1) صحيحة .
- نفترض أن العلاقة (1) صحيحة إلى n أي $n^p \equiv n\ [p]$ هي صحيحة (معطيات الترجع)
- نبين أن العلاقة (1) صحيحة ل $n+1$ أي نبين أن $(n+1)^p \equiv n+1\ [p]$.

حسب حدانية Newton : لدينا : $(n+1)^p = \sum_{k=0}^{k=p} C_p^k n^k 1^{p-k} = \sum_{k=0}^{k=p} C_p^k n^k = C_p^0 n^0 + \sum_{k=0}^{k=p} C_p^k n^k + C_p^p n^p = 1 + \sum_{k=0}^{k=p} C_p^k n^k + n^p$

ومنه : $(n+1)^p = 1 + \sum_{k=0}^{k=p} C_p^k n^k + n^p$

حسب التمهيدة : p يقسم C_p^k إذن p يقسم $C_p^k n^k$ ومنه : p يقسم $\sum_{k=0}^{k=p} C_p^k n^k$ ومنه : $\sum_{k=0}^{k=p} C_p^k n^k \equiv 0\ \ [p]$

إذن :
$$\begin{aligned}(n+1)^p &\equiv 1 + \sum_{k=0}^{k=p} C_p^k n^k + n^p\ \ [p]\\ &\equiv 1 + n^p\ \ [p]\\ &\equiv 1 + n\ \ [p]\end{aligned}$$
(حسب معطيات الترجع $n^p \equiv n\ [p]$)

خلاصة : $n \in \mathbb{N}$: $n^p \equiv n\ [p]$ (أي $a \in \mathbb{N}$ ؛ $a^p \equiv a\ [p]$)

حالة 2 : $n \in \mathbb{Z}^-$.

في هذه الحالة : $-n \in \mathbb{N}$ ومنه : $(-n)^p \equiv -n\ [p]$. بما أن : p عدد أولي موجب إذن $p = 2$ أو p يكون عدد فردي .

بالنسبة ل $p = 2$. لدينا : $(-n)^p \equiv -n\ [p]$ تكتب بما يلي $(-n)^2 \equiv -n\ [2]$ أي $n^2 + n \equiv 0\ [2]$ أي $n(n+1) \equiv 0\ [2]$

وهذا صحيح لأن $n(n+1)$ عدد زوجي إذن يقبل القسمة على 2 .

بالنسبة ل $p \neq 2$. لدينا : $(-n)^p \equiv -n\ [p]$ تكتب بما يلي : $-n^p \equiv -n\ [p]$. أي $-1\times(-n^p) \equiv -1\times(-n)\ [p]$ (الموافقة منسجمة مع الضرب) . إذن : $n^p \equiv n\ [p]$. ومنه : $n \in \mathbb{Z}^- : n^p \equiv n\ [p]$ (أي $a \in \mathbb{N}$ ؛ $a^p \equiv a\ [p]$)

خلاصة : $n \in \mathbb{Z} : n^p \equiv n\ [p]$

5. لازمة مبرهنة فيرما corollaire de petit théorème de Fermat

> إذا كان p عدد أولي و a عدد نسبي لا يقبل القسمة ب p . لدينا : $a^{p-1} \equiv 1\ [p]$

XII. نظمات العد systèmes de numération

1. تمهيد :

الإنسان منذ فجر التاريخ يقوم بالعد . بدأ بالعد بالاعتماد على أصابعه العشر، لهذا اليوم يستخدم النظام العشري أو قاعدة العشرة نصطلح على تسميته نظام العد العشري لأنه يستعمل عشرة أرقام . و بالتالي العدد 62327 هو وفقا نظام الترقيم المعتاد عندنا يكتب على الشكل التالي : $6\times10^4+2\times10^3+3\times10^2+2\times10^1+7\times10^0$.

- الحياة اليومية فرضت منذ القدام نظام العد العشري هو 10 (système de numération décimal) يستعمل الأرقام العشر التالية : 0 ؛ 1 ؛ 2 ؛ 3 ؛ 4 ؛ 5 ؛ 6 ؛ 7 ؛ 8 ؛ 9)
- أجهزة الكمبيوتر لديها نظام العد الثنائي هو 2 (système de numération binaire) . (يستعمل الرقمين التاليين: 0 ؛ 1)
- أما نظام العد ذات الأساس 12 يستعمل الأرقام 0 ؛ 1 ؛ 2 ؛ 3 ؛ 4 ؛ 5 ؛ 6 ؛ 7 ؛ 8 ؛ 9 و α يمثل 10 و β يمثل 11) .
- الناس الذين يقومون ببرمجة أجهزة الكمبيوتر التي تستخدم قاعدة رمز المجمع 16 (النظام العد ستة العشري) . (système de numération hexadécimal) يستعمل الأرقام العشر التالية : 0 ؛ 1 ؛ 2 ؛ 3 ؛ 4 ؛ 5 ؛ 6 ؛ 7 ؛ 8 ؛ 9 ؛ A ؛ B ؛ C ؛ D ؛ E ؛ F) تمثل 10 و 11 و 12 و 13 و 14 و 15 على التوالي)
- المتصفحات التعبير عن خطوط الطول والعرض في درجة و الدقائق و ثواني؛ بحيث يصبح لديهم قاعدة الستين النظمات العد الستيني .

2. تعريف :

> أساس نظمة العد هو عدد الأرقام المستعملة في هذه النظمة لتمثيل الأعداد الطبيعية .

3. تمثيل عدد في نظمة العد ذات الأساس b حيث $b \in \mathbb{N}\setminus\{0,1\}$

مبرهنة (تقبل)

> ليكن b من $\mathbb{N}\setminus\{0,1\}$.
>
> لكل a من $\mathbb{N}$ يكتب على شكل وحيد $a=\sum_{k=0}^{k=n} c_k b^k = c_0b^0+c_1b^1+c_2b^2+\cdots+c_nb^n$ حيث $c_k \in\{0,1,2,\cdots,b-1\}$ وذلك لكل $i\in\{0,1,2,\cdots,n\}$ مع :
>
> إذا كان $a \neq 0$ فإن $c_n \neq 0$. (أي $a=\sum_{k=0}^{k=n} c_k b^k = c_0b^0+c_1b^1+c_2b^2+\cdots+c_nb^n$ مع $c_n \neq 0$)
>
> إذا كان $a=0$ فإن $n=0$. (أي $a=0=c_0b^0=0b^0$).
>
> ونكتب : $a=\overline{c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0}^{(b)}$. نقول أن مثلنا a في نظمة العد ذات الأساس b .
>
> المتتالية : $c_n,c_{n-1},\cdots,c_2,c_1,c_0,$ تسمى نشر ل a في الأساس b .

4. ملحوظة:

- الكتابة $\overline{c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0}^{(10)}$ تكتب باختصار : $a = c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0$.
- الخارج q_0 و الباقي للقسمة r_0 الإقليدية ل a على b هما على التوالي $q_0 = \overline{c_nc_{n-1}c_{n-2}\cdots c_2c_1}^{(b)}$ و $r_0 = c_0$.
- الخارج q_1 و الباقي للقسمة r_1 الإقليدية ل q_0 على b هما على التوالي $q_1 = \overline{c_nc_{n-1}c_{n-2}\cdots c_2}^{(b)}$ و $r_0 = c_1$.
- وهكذا يمكننا أن نحدد جميع الأرقام للعدد الصحيح الطبيعي a حيث الكتابة في الأساس b .

5. أمثلة :

1. نظام العد العشري $b = 10$:

مثال 1 : نحول العدد 133 إلى نظام العد السداسي (أو إلى الأساس 6)

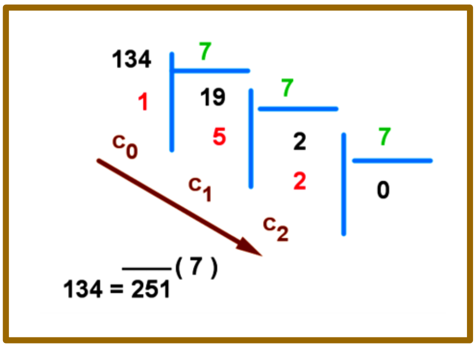
لدينا : $133 = 3\times6^2 + 4\times6^1 + 1\times6^0$ إذن : $133 = \overline{341}^{(6)}$.

مثال 2 : نحول العدد 121 إلى نظام العد الخماسي (أو إلى الأساس 5)

لدينا : $121 = 4\times5^2 + 4\times5^1 + 1\times5^0$ إذن : $121 = \overline{441}^{(5)}$.

مثال 3 : نحول العدد 134 إلى نظام العد السباعي (أو إلى الأساس 7)

نستعمل طريقة أخرى : هي إجراء القسمات المتتالية ب 7 (أنظر الشكل أمامه) :



إذن : $134 = \overline{251}^{(7)}$.

2. نظام العد الثنائي (système de numération binaire)

مثال 1 : نمثل العدد $\overline{1001010}^{(2)}$ في نظمة العد العشري (أي نظمة العد ذات الأساس $b = 10$) .

لدينا : العدد 1001010 متكون من 7 أرقام إذن $n = 7$ و $b = 2$ إذن نكتب :

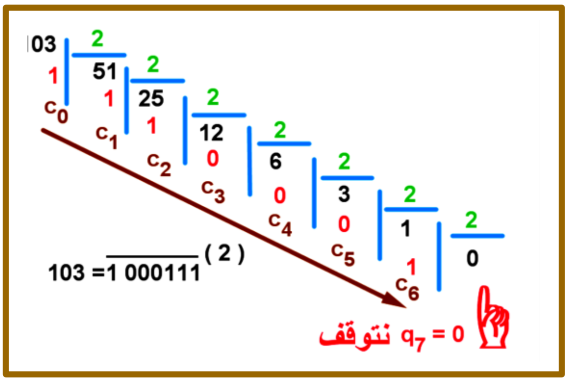
$$\overline{1001010}^{(2)} = \underbrace{1\times2^6 + 0\times2^5 + 0\times2^4 + 1\times2^3 + 0\times2^2 + 1\times2^1 + 0\times2^0}_{\overleftarrow{1\quad 0\quad 0\quad 1\quad 0\quad 1\quad 0}} = 64 + 8 + 2 = 74$$

ومنه : $\overline{1001010}^{(2)} = 74$.

مثال 2 : نمثل العدد 103 في نظمة العد الثنائي $b = 2$:

مثال 1 : نظام العد الثنائي (système de numération binaire)

من خلال القسمات المتتاليات ب 2 (أنظر الشكل أمامه) :



نستنتج أن : $103 = \overline{1000111}^{(2)}$

3. نظام العد السداسي عشر (système de numération hexadécimal)

نذكر (يستعمل الأرقام العشر التالية : 0 ؛ 1 ؛ 2 ؛ 3 ؛ 4 ؛ 5 ؛ 6 ؛ 7 ؛ 8 ؛ 9 ؛ A ؛ B ؛ C ؛ D ؛ E ؛ F) (تمثل 10 و 11 و 12 و 13 و 14 و 15 على التوالي)

مثال 1 :نمثل العدد $\overline{3C2EB}^{(16)}$ في نظمة العد العشري (أي نظمة العد ذات الأساس $b = 10$) .

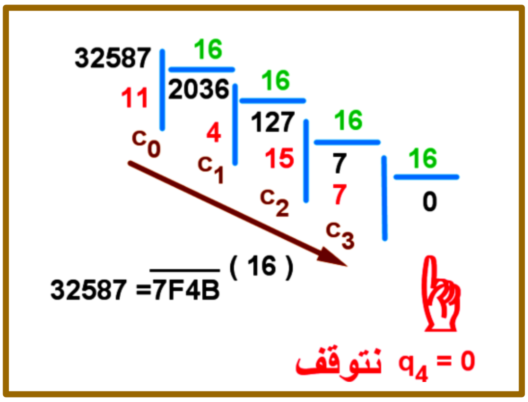
لدينا : العدد 3C2EB متكون من 5 أرقام إذن $n = 5$ و $b = 16$ إذن نكتب :

$$\overline{3C2EB}^{(16)} = \underbrace{3\times16^4 + 12\times16^3 + 2\times16^2 + 14\times16^1 + 11\times16^0}_{\overleftarrow{3\quad C\quad 2\quad E\quad B}} = 196608 + 49152 + 512 + 224 + 11 = 246507$$

ومنه : $\overline{3C2EB}^{(16)} = 246507$.

مثال 2 : نمثل العدد 32587 في نظمة العد السداسي عشر العشري $b=16$:

من خلال القسمات المتتاليات ب 16 نستنتج أن: $32587=\overline{7F4B}^{(16)}$



6. مقارنة عددين ممثلين في نفس النظمة العد (أي نفس الأساس b)

لنعتبر العددين $x=\overline{c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0}^{(b)}$ و $y=\overline{a_ma_{m-1}a_{m-2}\cdots a_2a_1a_0}^{(b)}$ مع $c_n\neq 0$ و $a_m\neq 0$.

- إذا كان $n<m$ فإن $x<y$.
- إذا كان $n=m$ نقارن c_n و a_m .

أ- حالة 1 : $c_n<a_m$ (مع $n=m$) فإن $x<y$.

ب- حالة 2 : $c_n<a_m$ (مع $n=m$) و .....و $c_{i+1}=a_{i+1}$ و $c_i<a_i$ فإن $x<y$.

7. أمثلة :

- $x=\underbrace{\overline{52534}}_{n=4}{}^{(6)}$ و $y=\underbrace{\overline{110034}}_{m=5}{}^{(6)}$ إذن $y>x$.
- $x=\underbrace{\overline{52534}}_{n=4}{}^{(6)}$ (مع $c_n=c_4=5$) و $y=\underbrace{\overline{22534}}_{m=4}{}^{(6)}$ (مع $a_m=a_4=2$) إذن $y<x$.
- $x=\underbrace{\overline{52534}}_{n=4}{}^{(6)}$ (مع $c_n=c_4=5$ و $c_2=5\,;c_3=2$) و $y=\underbrace{\overline{52540}}_{m=4}{}^{(6)}$ (مع $a_n=a_4=5$ و $a_2=5\,;a_3=2$) إذن

$y<x$ لأن $c_1=4\,;c_1=3$

ويمكن استعمال الوضعية التالية $\begin{matrix} x=\overline{52534}^{(6)} \\ y=\overline{52540}^{(6)} \end{matrix}$ للمقارنة بين العددين .

XIII. مجموع و جداء عددين ممثلين في نفس النظمة :

1. المجموع :

مثال 1 : $x=\overline{1}^{(4)}$ و $y=\overline{3}^{(4)}$ ومنه : $x+y=\overline{10}^{(4)}$

عمليا نحسب المجموع على الطريقة المألوفة :

$$\begin{array}{r} {}^{1} \\ 01 \\ +\quad 3 \\ \hline =\quad 10 \end{array}$$

مثال 2 : $x=\overline{2}^{(4)}$ و $y=\overline{3}^{(4)}$ ومنه : $x+y=\overline{11}^{(4)}$

عمليا نحسب المجموع على الطريقة المألوفة :

$$\begin{array}{r} {}^{1} \\ 02 \\ +\quad 3 \\ \hline =\quad 11 \end{array}$$

مثال 3 : $x=\overline{23321}^{(4)}$ و $y=\overline{3203}^{(4)}$

لدينا : $x=\overline{23321}^{(4)}=2\times4^4+3\times4^3+3\times4^2+2\times4^1+1\times4^0$ و $y=\overline{3203}^{(4)}=3\times4^3+2\times4^2+0\times4^1+3\times4^0$ ومنه:

$$x=\overline{23321}^{(4)}=2\times4^4+3\times4^3+3\times4^2+2\times4^1+1\times4^0$$
$$y=\overline{3203}^{(4)}=3\times4^3+2\times4^2+0\times4^1+3\times4^0$$
$$x+y=2\times4^4+(4+2)\times4^3+(4+1)\times4^2+2\times4^1+4\times4^0$$
$$x+y=2\times4^4+\left(4^4+2\times4^3\right)+\left(4^3+4^2\right)+2\times4^1+4^1$$
$$x+y=3\times4^4+3\times4^3+4^2+3\times4^1$$
$$x+y=3\times4^4+3\times4^3+4^2+3\times4^1+0\times4^0$$

خلاصة : $\overline{23321}^{(4)}+\overline{3203}^{(4)}=\overline{33130}^{(4)}$

عمليا نحسب المجموع على الطريقة المألوفة :

$$\begin{array}{r} {}^{1\,1\;\;1}\\ 23321\\ +\quad 3203\\ \hline =\; 33130 \end{array}$$

خلاصة : $x+y=\overline{33130}^{(4)}$

2. الجداء :

مثال 1 : $x=\overline{2}^{(5)}$ و $y=\overline{4}^{(5)}$.

لدينا : $x=\overline{2}^{(5)}=2\times5^0=2\ ;\ y=\overline{2}^{(5)}=4\times5^0=4$

ومنه : $x\times y=\overline{2}^{(5)}\times\overline{4}^{(5)}=\left(2\times5^0\right)\times\left(4\times5^0\right)=2\times4=8=5+3=1\times5^1+3\times5^0=\overline{13}^{(5)}$.

عمليا نحسب الجداء على الطريقة المألوفة :

$$\begin{array}{r} {}^{1}\;\;\\ 04\\ \times\quad 2\\ \hline =\; 13 \end{array}$$

خلاصة : $\overline{2}^{(5)}\times\overline{4}^{(5)}=\overline{13}^{(5)}$

مثال 2 : $x=\overline{3}^{(4)}$ و $y=\overline{12}^{(4)}$ ومنه : $x\times y=\overline{210}^{(4)}$

لدينا : $x=\overline{3}^{(4)}=3\times4^0=3\ ;\ y=\overline{12}^{(4)}=1\times4^1+2\times4^0=6$

ومنه :

$$x\times y=\overline{3}^{(4)}\times\overline{12}^{(4)}=\left(3\times4^0\right)\left(1\times4^1+2\times4^0\right)=3\times6=18=16+2=1\times4^2+2\times4^0=1\times4^2+0\times4^1+2\times4^0=\overline{102}^{(4)}$$

عمليا نحسب المجموع على الطريقة المألوفة :

$$\begin{array}{r} {}^{1}\;\;\\ 12\\ \times\quad 3\\ \hline =\; 102 \end{array}$$

خلاصة : $\overline{3}^{(4)}\times\overline{12}^{(4)}=\overline{102}^{(4)}$

مثال 3 : $x=\overline{23321}^{(7)}$ و $y=\overline{32}^{(7)}$

لدينا :

$$\begin{array}{rr} \text{reste}\times 3\rightarrow & 1\ 2\ 1 \\ \text{reste}\times 2\rightarrow & 1\ 1 \\ & 53641 \\ \times & 32 \\ \hline & 130612 \\ & 224553\bullet \\ \hline = & 2306442 \end{array}$$

خلاصة : $\overline{23321}^{(7)}\times\overline{32}^{(7)}=\overline{2306442}^{(7)}$

XIV. مصادق قابلية القسمة عدد x من نظمة العد العشري على الأعداد 2 ؛ 3 ؛ 4 ؛ 5 ؛ 9 ؛ 11 ؛ 25 :

نعتبر x من $\mathbb{N}^*$ حيث تمثيله في نظمة العد العشري هو :

$x=\overline{c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0}^{(10)}=c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0=\sum_{k=0}^{k=n}c_k10^k=c_010^0+\sum_{k=1}^{k=n}c_k10^k$ حيث $c_i\in\{0,1,2,\cdots,9\}$.

1. قابلية القسمة على 2 :

لدينا :

$\begin{cases} 2\equiv 0 & [2] \\ 2\times5\equiv 0\times 5 & [2] \\ 10\equiv 0 & [2] \end{cases}$ ومنه $\forall k\in\mathbb{N}^* : 10^k\equiv 0\ [2]$. ($k\neq 0$ مشكل 0^0 وهو 1)

إذن : $x=c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0=\sum_{k=0}^{k=n}c_k10^k=c_010^0+\sum_{k=1}^{k=n}c_k10^k$

ومنه : $x\equiv c_010^0+\sum_{k=1}^{k=n}c_k\underbrace{10^k}_{\equiv 0}\ [2]$

$x\equiv c_0\ [2]$

خلاصة : $x=c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0$ من $\mathbb{N}^*$ قابل للقسمة على 2 إذا وفقط إذا كان : رقم الوحدات c_0 في تمثيله حسب نظمة العد العشري قابل للقسمة على 2 (أي c_0 رقم الوحدات زوجي أو $c_0\in\{0,2,4,6,8\}$) .

2. قابلية القسمة على 3 :

لدينا :

$10\equiv 1\ [3]$ ومنه $\forall k\in\mathbb{N}^* : 10^k\equiv 0\ [2]$.

إذن : $x=c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0=\sum_{k=0}^{k=n}c_k10^k=c_010^0+\sum_{k=1}^{k=n}c_k10^k=c_0+\sum_{k=1}^{k=n}c_k10^k$

$x\equiv c_0+\sum_{k=1}^{k=n}c_k\underbrace{10^k}_{\equiv 1}\ [3]$

ومنه : $x\equiv c_0+\sum_{k=1}^{k=n}c_k\ [3]$

$x\equiv\sum_{k=0}^{k=n}c_k\ [3]$

خلاصة : $x=c_nc_{n-1}c_{n-2}\cdots c_2c_1c_0$ من $\mathbb{N}^*$ قابل للقسمة على 2 إذا وفقط إذا كان :مجموع أرقامه c_0 و c_1 و .... و c_{n-1} و c_n في تمثيله حسب نظمة العد العشري قابل للقسمة على 3 (أي العدد $c_n+c_{n-1}+c_{n-2}+\cdots+c_2+c_1+c_0$ قابل للقسمة على 3) .

3. قابلية القسمة على 5 :

لدينا :

$10 \equiv 0 \quad [5]$ ومنه $\forall k \in \mathbb{N}^* : 10^k \equiv 0 \ [5]$.

إذن : $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0 = \sum_{k=0}^{k=n} c_k 10^k = c_0 10^0 + \sum_{k=1}^{k=n} c_k 10^k$.

ومنه : $x \equiv c_0 + \sum_{k=1}^{k=n} c_k \underbrace{10^k}_{\equiv 0} \quad [5]$

$\equiv c_0 \quad [5]$

خلاصة : $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0$ من $\mathbb{N}^*$ قابل للقسمة على 5 إذا وفقط إذا كان : رقم الوحدات c_0 في تمثيله حسب نظمة العد العشري قابل للقسمة على 5 (أي c_0 رقم الوحدات هو 0 أو 5) .

4. قابلية القسمة على 4 أو 25 :

لدينا :

$10^2 \equiv 0 \quad [100]$ ومنه $\forall k \in \mathbb{N}^* : 10^k \times 10^2 \equiv 0 \ [2]$.

إذن : $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0 = \sum_{k=0}^{k=n} c_k 10^k = \left(c_0 10^0 + c_1 10^1\right) + \sum_{k=2}^{k=n} c_k 10^k = \overline{c_1 c_0} + \sum_{i=0}^{i=n-2} c_{i+2} 10^{i+2} \ ; (k = i+2)$

$= \overline{c_1 c_0} + \sum_{i=0}^{i=n-2} c_{i+2} 10^i \times 10^2$

ومنه : $x \equiv \overline{c_1 c_0} + \sum_{i=0}^{i=n-2} c_{i+2} 10^i \times \underbrace{10^2}_{0} \quad [100]$

$\equiv \overline{c_1 c_0} \quad [100]$

بما أن : 100 تقبل القسمة على 4 و 25 إذن : $x \equiv \overline{c_0 c_1} \quad [4]$ و $x \equiv \overline{c_0 c_1} \quad [25]$

ومنه : $x \equiv \overline{c_0 c_1} \quad [4]$ أي x يقبل القسمة على 4 يكافئ $c_0 c_1$ يقبل القسمة على 4 .

ومنه : $x \equiv \overline{c_0 c_1} \quad [25]$ أي x يقبل القسمة على 25 يكافئ $c_0 c_1$ يقبل القسمة على 25 .

خلاصة :

- $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0$ من $\mathbb{N}^*$ قابل للقسمة على 4 إذا وفقط إذا كان : العدد $c_0 c_1$ الممثل ب رقم العشرات و الوحدات في تمثيله حسب نظمة العد العشري قابل للقسمة على 4 .
- $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0$ من $\mathbb{N}^*$ قابل للقسمة على 25 إذا وفقط إذا كان : العدد $c_0 c_1$ الممثل ب: رقم العشرات و الوحدات في تمثيله نظمة العد العشري قابل للقسمة على 25 .

ملحوظة : يمكن استعمال هذه الطريقة للقسمة على 2 و 5 .

5. قابلية القسمة على 11 :

لدينا :

$10 \equiv -1 \quad [11]$ ومنه $\forall k \in \mathbb{N} : 10^k \equiv (-1)^k \ [11]$.

إذن : $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0 = \sum_{k=0}^{k=n} c_k 10^k$

ومنه :

$$x \equiv \sum_{k=0}^{k=n} c_k \underbrace{10^k}_{\equiv(-1)^k} \quad [11]$$

$$x \equiv \sum_{k=0}^{k=n} c_k (-1)^k \quad [11]$$

خلاصة : $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0$ من $\mathbb{N}^*$ قابل للقسمة على 11 إذا وفقط إذا كان العدد: $\sum_{k=0}^{k=n} c_k (-1)^k$ قابل للقسمة على 11

أو أيضا المجموع $(-1)^n c_n + (-1)^{n-1} c_{n-1} + \cdots + c_2 - c_1 + c_0$ قابل للقسمة على 11 .

- أو أيضا : الفرق $S_1 - S_2$ قابل للقسمة على 11 . (مع S_1 مجموع الأرقام في الترتيب الفردي و S_2 مجموع الأرقام في الترتيب الزوجي وذلك في تمثيل هذا العدد في نظمة العد العشري ابتداء من اليمين للعدد) .

6. تمرين :

- بين أن : $x = c_n c_{n-1} c_{n-2} \cdots c_2 c_1 c_0$ من $\mathbb{N}^*$ قابل للقسمة على 8 إذا وفقط إذا كان : العدد $c_2 c_1 c_0$ الممثل ب رقم الوحدات و رقم العشرات و رقم المئات في تمثيله حسب نظمة العد العشري قابل للقسمة على 8 .
- تطبيق : العدد 5233120 قابل للقسمة على 8 لأن العدد 120 قابل للقسمة على 8 .

نهاية درس : الحسابيات في $\mathbb{Z}$