



إن $k/1$ ونعلم أن قواسم 1 هي 1 و -1.

إن $k=1$ أو $k=-1$

إذا كان $k=1$ فإن $k'=1$

إذا كان $k=-1$ فإن $k'=-1$

إن $\begin{cases} k=1 \\ k'=1 \end{cases}$ أو $\begin{cases} k=-1 \\ k'=-1 \end{cases}$

إن $a=b$ أو $a=-b$ إن $|a|=|b|$

خاصية:

(*) العلاقة $(/)$ انعكاسية. يعني a/a ($\forall a \in \mathbb{Z}$)

(*) العلاقة $(/)$ متعدية. يعني: $\begin{cases} a/b \\ b/c \end{cases} \Rightarrow a/c$ ($\forall (a,b,c) \in \mathbb{Z}^3$)

(*) $\begin{cases} a/b \\ b/a \end{cases} \Rightarrow |a|=|b|$ ($\forall (a,b) \in \mathbb{Z}^2$)

(*) $\begin{cases} a/b \\ b/a \end{cases} \Rightarrow a=b$ ($\forall (a,b) \in \mathbb{N}^2$)

نقول في هذه الحالة إن العلاقة $(/)$ تخالفية.

(3) القسمة الأقليدية في $\mathbb{Z}$

(a) القسمة الأقليدية في $\mathbb{N}$

مبرهنة:

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

يوجد زوج وحيد $(q,r) \in \mathbb{N} \times \mathbb{N}$ بحيث: $\begin{cases} a = qb + r \\ 0 \leq r < b \end{cases}$

برهان:

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

-1 Existence:

نعتبر المجموعة: $A = \{k \in \mathbb{N} / kb \leq a\}$

* لدينا $0 \in A$ إن $A \neq \emptyset$

* ليكن $k \in A$ لدينا: $kb \leq a$

ولدينا $b \in \mathbb{N}^*$ يعني $b \geq 1$ أي $kb \geq k$

إن $k \leq a$

إن $k \leq a$ ($\forall k \in A$)

إن A مكبورة ب a .

* ولدينا $A \subset \mathbb{N}$. إن A تقبل الأكبر عنصر. نضع $q = \text{Max} A$

و $r = a - bq$

* لنبين أن (q,r) يحقق الشرطين:

لدينا $r = a - bq$ إن $a = bq + r$

لنبين أن $0 \leq r < b$

لدينا $q = \text{Max} A$ إن $q \in A$ ومنه $qb \leq a$

يعني $a - qb \geq 0$

إن $0 \leq r$

لدينا $q = \text{Max} A$ إن $(q+1) \notin A$

إن $(q+1)b > a$

يعني $a < bq + b$

أي $a - bq < b$ يعني $r < b$

I- قابلية القسمة في $\mathbb{Z}$

(1) تعريف:

ليكن $b \in \mathbb{Z}$ من $\mathbb{Z}$. نقول إن b يقسم a إذا وجد عدد k من $\mathbb{Z}$ بحيث $a = kb$. ونكتب b/a .

ملاحظات:

* إذا كان b/a نقول كذلك إن b قاسم ل a مضاعف ل b .

* مجموعة مضاعفات b هي $\{..., -2b, -b, 0, b, 2b, ...\}$

يعني $\{kb / k \in \mathbb{Z}\}$ ونرمز لها ب: $b\mathbb{Z}$

* $1/a$ ($\forall a \in \mathbb{Z}$) (لأن $a=1.a$)

* $-1/a$ ($\forall a \in \mathbb{Z}$) (لأن $a=-1.(-a)$)

* $a/0$ ($\forall a \in \mathbb{Z}$) (لأن $0=0.a$)

* $0/0$ (لأن مثلا $0=0 \times 2$)

* $0 \times a$ ($\forall a \in \mathbb{Z}^*$)

* ليكن b/a و $b \in \mathbb{Z}$ و $a \in \mathbb{Z}^*$ بحيث

لدينا b/a إن يوجد $k \in \mathbb{Z}$ بحيث $a = kb$

إن: $|a| = |k||b|$

ولدينا $a \neq 0$ إن $k \neq 0$ إن $|k| \in \mathbb{N}^*$

يعني $|k| \geq 1$

إن $|b||k| \geq |b|$

يعني $|a| \geq |b|$

إن: $\begin{cases} a \neq 0 \\ b/a \end{cases} \Rightarrow |b| \leq |a|$

* $a/|a|$ ($\forall a \in \mathbb{Z}$)

* $|a|/a$ ($\forall a \in \mathbb{Z}$)

(2) خاصيات قابلية القسمة:

-1 ليكن $a \in \mathbb{Z}$ لدينا: $a=1.a$ إن a/a

إن a/a ($\forall a \in \mathbb{Z}$)

نقول إن علاقة قابلية القسمة انعكاسية.

-2 ليكن a/b و c/b من $\mathbb{Z}$ بحيث $\begin{cases} a/b \\ c/b \end{cases}$

لدينا a/b إن يوجد k من $\mathbb{Z}$ بحيث $b = ka$

ولدينا b/c إن يوجد k' من $\mathbb{Z}$ بحيث $c = k'b$

أي $c = k'ka$

إن a/c

إن $\begin{cases} a/b \\ b/c \end{cases} \Rightarrow a/c$ ($\forall (a,b,c) \in \mathbb{Z}^3$)

نقول إن العلاقة $(/)$ متعدية.

-3 ليكن $b \in \mathbb{Z}$ من $\mathbb{Z}$ بحيث $\begin{cases} a/b \\ b/a \end{cases}$

لدينا a/b إن يوجد k من $\mathbb{Z}$ بحيث $b = ak$

و b/a إن يوجد k' من $\mathbb{Z}$ بحيث $a = b k'$

يعني $a = k k' a$

* إذ كان $a=0$ فإن $b=0$ إن $a=b$

* إذا كان $a \neq 0$ فإن $k k' = 1$

ومنه $0 \leq r \leq b$

إذن يوجد زوج $(q, r) \in \mathbb{N} \times \mathbb{N}$ بحيث: $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

(2) L'unicité :

نفترض أنه يوجد زوجان (q', r') و (q, r) من $\mathbb{N} \times \mathbb{N}$

بحيث $\begin{cases} a = bq' + r' \\ 0 \leq r' < b \end{cases}$ و $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

لدينا: $bq + r = bq' + r'$

$$b(q - q') = r' - r$$

$$|b| \cdot |q - q'| = |r' - r|$$

ولدينا $\begin{cases} 0 \leq r < b \\ 0 \leq r' < b \end{cases}$ يعني $\begin{cases} -b < -r < 0 \\ 0 \leq r' < b \end{cases}$

إذن: $-b < r' - r < b$

يعني: $|r' - r| < b$

يعني: $|b| |q - q'| < b$

يعني: $|q - q'| < 1$

ولدينا $|q - q'| \in \mathbb{N}$ إذن $|q - q'| = 0$

يعني $q = q'$

ومنه $|r - r'| = 0$ يعني $r = r'$

إذن $(q, r) = (q', r')$

وبالتالي يوجد زوج وحيد $(q, r) \in \mathbb{N} \times \mathbb{N}$ يحقق $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

(b) القسمة الإقليدية في $\mathbb{Z}$:

مبرهنة:

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

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

برهان:

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

(1) Existence :

* إذا كان $a \in \mathbb{N}$ فإنه يوجد زوج وحيد يحقق الشرط.

* إذا كان $a \in \mathbb{Z}^+$ فإن $-a \in \mathbb{N}^*$

إذن يوجد زوج وحيد (q', r') من $(\mathbb{N} \times \mathbb{N})$ بحيث:

$$\begin{cases} -a = bq' + r' \\ 0 \leq r' < b \end{cases}$$

لدينا $a = b(-q') - r'$

إذا كان $r' = 0$ فإن $a = b(-q')$

نضع $q = -q'$ و $r = 0$

إذا كان $r' \neq 0$

فإن $a = b(-q') - r'$

$$= b(-q') - b + b - r' = b(-q' - 1) + (b - r')$$

نضع $\begin{cases} r = b - r' \\ q = -q' - 1 \end{cases}$ لدينا $a = bq + r$

ولدينا $0 < r < b$

يعني $0 < b - r' < b$ إذن $0 < r < b$

إذن $0 < r < b$

* وبالتالي يوجد زوج (q, r) بحيث: $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

(2) L'unicité :

بنفس الطريقة السابقة نبين أن الزوج (q, r) وحيد.

(II) الموافقة بترديد n :

(1) تعريف:

ليكن $n \in \mathbb{N}$ و $b \neq 0$ من $\mathbb{Z}$

نقول إن a يوافق b بترديد n إذا وفقط إذا كان

$$a \equiv b[n] \text{ ونكتب } n/a - b$$

ملاحظة:

$$a \equiv b[n] \Leftrightarrow n/a - b$$

$$\Leftrightarrow (\exists k \in \mathbb{Z}) a - b = nk$$

$$\Leftrightarrow a = nk + b$$

(2) خاصيات:

1- ليكن $n \in \mathbb{N}$

(*) $(\forall a \in \mathbb{Z}) a \equiv a[n]$

إذن علاقة الموافقة انعكاسية.

(*) ليكن $b \neq 0$ من $\mathbb{Z}$ بحيث $a \equiv b[n]$

إذن $n/a - b$ يعني يوجد k من $\mathbb{Z}$ بحيث: $a - b = nk$

$$\text{إذن } b - a = n(-k)$$

إذن $n/a - b$ ومنه $b \equiv a[n]$

إذن $a \equiv b[n] \Rightarrow b \equiv a[n]$ علاقة الموافقة تماثلية.

(*) ليكن $b \neq 0$ من $\mathbb{Z}$ بحيث: $\begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases}$

لدينا $a \equiv b[n]$ إذن (1) $a - b = kn$ مع $k \in \mathbb{Z}$.

و $b \equiv c[n]$ إذن (2) $b - c = k'n$ مع $k' \in \mathbb{Z}$.

من (1) + (2) نستنتج $a - c = (k + k')n$ إذن $n/a - c$

$$a \equiv c[n]$$

$$\text{إذن: } \begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Rightarrow a \equiv c[n]$$

علاقة الموافقة متعدية.

خاصية (1):

علاقة الموافقة انعكاسية تماثلية ومتعدية.

نقول إن علاقة الموافقة علاقة تكافؤ.

$$(\forall (a, b, c) \in \mathbb{Z}^3) \quad * a \equiv a[n]$$

$$* a \equiv b[n] \Rightarrow b \equiv a[n] \text{ يعني:}$$

$$* \begin{cases} a \equiv b[n] \\ b \equiv c[n] \end{cases} \Rightarrow a \equiv c[n]$$

خاصية (2):

ليكن $n \in \mathbb{N}^*$

كل عدد a من $\mathbb{Z}$ يوافق بترديد n باقي قسمته على n يعني إذا

كان r هو باقي قسمة a على n فإن $a \equiv r[n]$.

برهان:

$$\text{لدينا } \begin{cases} a = nq + r \\ 0 \leq r < n \end{cases}$$

من خلال (1) + (2) نجد:
 $(a+c)-(b+d)=(k+k')n$
 $a+c \equiv b+d [n]$ إذن
 $c(a-b) = ckn$ * لدينا من (1):
 $b(c-d) = bk'n$ ومن (2):
 $ac-bd = n(ck+bk')$ وبجمع الطرفين:
 $ac \equiv bd [n]$ ومنه $n \nmid ac-bd$ إذن:
ملاحظة: ليكن $n \in \mathbb{N}$ و a من $\mathbb{Z}$.
 $(\forall k \in \mathbb{Z}) \quad a \equiv a+nk [n]$

تمرين تطبيقي:

(1) لنبين أن: $(\forall n \in \mathbb{N}) \quad 7 \mid 3^{2n} - 2^n$

ملاحظة: $n/a \Leftrightarrow a \equiv 0 [n]$

لدينا:

$$3^2 \equiv 9 [7]$$

$$\equiv 9 - 7 [7]$$

$$\equiv 2 [7]$$

$$3^2 \equiv 2 [7] \text{ إذن}$$

$$3^{2n} \equiv 2^n [7] \text{ إذن}$$

$$\text{إذن } (\forall n \in \mathbb{N}): \quad 7 \mid 3^{2n} - 2^n$$

(2) لنبين أن $17 \mid 3.5^{2n-1} + 2^{3n-2}$ لكل n من $\mathbb{N}^*$
 لدينا:

$$5^{2n-1} = 5^{2(n-1)+1}$$

$$= 5^{2(n-1)} \times 5$$

ولدينا :

$$5^2 \equiv 25 [17]$$

$$\equiv 8 [17]$$

$$5^2 \equiv 2^3 [17]$$

$$5^{2(n+1)} \equiv 2^{3(n-1)} [17] \text{ إذن:}$$

$$5.5^{2(n-1)} \equiv 2^{3(n-1)} \times 5 [17] \text{ يعني:}$$

$$5^{2n-1} \equiv 2^{3(n-1)} \times 5 [17] \text{ يعني:}$$

$$3.5^{2n-1} \equiv 2^{3(n-1)} \times 15 [17] \text{ يعني:}$$

$$3.5^{2n-1} + 2^{3n-2} \equiv 2^{3n-3} \times 15 + 2^{3n-2} [17] \text{ يعني:}$$

$$3.5^{2n-1} + 2^{3n-2} \equiv 2^{3n-3} (15+2) [17] \text{ يعني:}$$

$$\equiv 2^{3n-3} (17) [17] \text{ يعني:}$$

$$3.5^{2n-1} + 2^{3n-2} \equiv 0 [17] \text{ إذن:}$$

$$(\forall n \in \mathbb{N}^*) \quad 17 \mid 3.5^{2n-1} + 2^{3n-2}$$

(3) مجموعة أصناف تكافؤ:

(a) تعريف:

ليكن $a \in \mathbb{N}$ وليكن $x \in \mathbb{Z}$
 نسمي صنف تكافؤ x المجموعة التي نرمز لها بـ $\bar{x}$ أو $\dot{x}$
 والمعرفة بما يلي:

$$\bar{x} = \{y \in \mathbb{Z} / y \equiv x [n]\}$$

ونرمز لمجموعة هذه الأصناف بـ: $\mathbb{Z}/n\mathbb{Z}$

$$\text{إذن } a-r=nq$$

$$\text{ومنه } n/a-r \text{ إذن } a \equiv r [n]$$

خاصية (3):

ليكن $n \in \mathbb{N}^*$ و b, r من $\mathbb{Z}$.
 ليكن r باقي قسمة a على n و r' باقي قسمة b على n .
 لدينا: $a \equiv b [n] \Leftrightarrow r = r'$

برهان:

$$\text{لدينا: } \begin{cases} a = nq + r \\ 0 \leq r < n \end{cases} \text{ و } \begin{cases} b = nq' + r' \\ 0 \leq r' < n \end{cases}$$

* نفترض أن $r = r'$

$$\text{نعلم أن } \begin{cases} a \equiv r [n] \\ b \equiv r [n] \end{cases} \text{ و } \begin{cases} a \equiv r' [n] \\ b \equiv r' [n] \end{cases}$$

$$\text{و } r = r' \text{ إذن } a \equiv b [n]$$

* نفترض أن $a \equiv b [n]$ ولنبين أن $r = r'$

$$\text{لدينا } \begin{cases} a \equiv r [n] \\ b \equiv r [n] \\ r = r' \end{cases} \text{ إذن } r \equiv r' [n]$$

$$\text{أي } r-r' = kn \text{ مع } k \in \mathbb{Z} \text{ إذن } |r-r'| = |k|n$$

$$\text{ولدينا } \begin{cases} 0 \leq r < n \\ 0 \leq r' < n \end{cases}$$

$$\text{إذن } -n < r-r' < n$$

$$\text{أي } |r-r'| < n$$

$$\text{يعني } |k|n < n$$

$$\text{إذن } |k| < 1$$

$$\text{ولدينا } |k| \in \mathbb{N} \text{ إذن } k = 0$$

$$\text{ومنه } r-r' = 0 \text{ إذن } r = r'$$

خاصية (4):

ليكن $n \in \mathbb{N}$

$$(1) \quad (\forall (a, b, c, d) \in \mathbb{Z}^4) \begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d [n] \\ a.c \equiv b.d [n] \end{cases}$$

$$(2) \quad \text{ليكن } a_1, a_2, \dots, a_n \text{ و } b_1, b_2, \dots, b_n \text{ من } \mathbb{Z}$$

$$(\forall i \in \{1, 2, \dots, n\}) a_i \equiv b_i [n] \Rightarrow \begin{cases} \sum_{i=1}^n a_i \equiv \sum_{i=1}^n b_i [n] \\ \prod_{i=1}^n a_i \equiv \prod_{i=1}^n b_i [n] \end{cases}$$

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

$$(4) \quad (\forall (a, b) \in \mathbb{Z}^2) (\forall n' \in \mathbb{N}): a \equiv b [n] \Rightarrow a^{n'} \equiv b^{n'} [n]$$

برهان: لنبرهن على (1)

$$\text{نفترض أن } \begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases}$$

$$\text{* لدينا } a \equiv b [n] \text{ يعني } (1) \quad a-b = kn \quad (k \in \mathbb{Z})$$

$$\text{و } c \equiv d [n] \text{ إذن } (2) \quad c-d = k'n \quad (k' \in \mathbb{Z})$$

* لنبين أن $\mathbb{Z}/n\mathbb{Z} \subset \{0, 1, 2, \dots, (n-1)\}$

ليكن $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$

نعتبر قسمة x على n . ليكن r هو باقي قسمة a على n

$$\begin{cases} x = nq + r \\ 0 \leq r < n \end{cases} \text{ أي:}$$

نعلم أن $x \equiv r[n]$ إذن $\bar{x} = \bar{r}$

ولدينا: $r \in \{0, 1, 2, \dots, n-1\}$

إذن $\bar{r} \in \{0, 1, 2, \dots, (n-1)\}$

ومنه $\mathbb{Z}/n\mathbb{Z} \subset \{0, 1, 2, \dots, (n-1)\}$

بالتالي: $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, (n-1)\}$

* لنحدد $\text{card } \mathbb{Z}/n\mathbb{Z}$

ليكن $r' \neq r$ من $\{0, 1, 2, \dots, n-1\}$ بحيث $r' \neq r$

لنبين أن $\bar{r}' \neq \bar{r}$

نفترض أن $\bar{r}' = \bar{r}$

يعني: $r \equiv r'[n]$

يعني: $r - r' = kn / k \in \mathbb{Z}$ أي $|r - r'| = |k|n$

$$\begin{cases} 0 \leq r < n \\ 0 \leq r' < n \end{cases} \text{ إذن } |r - r'| < n$$

يعني: $|k|n < n$

يعني $|k| < 1$

ولدينا $|k| \in \mathbb{N}$ إذن $k = 0$

ومنه $r = r'$ وهذا تناقض.

إذن $\bar{r}' \neq \bar{r}$

بالتالي: $\text{Card } \mathbb{Z}/n\mathbb{Z} = n$

خاصية:

ليكن $n \in \mathbb{N}^*$

$$\text{Card } \mathbb{Z}/n\mathbb{Z} = n \quad (*)$$

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, (n-1)\} \quad (*)$$

(c) الجمع والضرب في $\mathbb{Z}/n\mathbb{Z}$:

ليكن X, Y من $\mathbb{Z}/n\mathbb{Z}$

نفترض أن: $X = \bar{x} = \bar{x}'$

و: $Y = \bar{y} = \bar{y}'$

$$\begin{cases} x \equiv x'[n] \\ y \equiv y'[n] \end{cases} \text{ إذن}$$

$$\begin{cases} x + y \equiv x' + y'[n] \\ xy \equiv x'y'[n] \end{cases} \text{ إذن}$$

$$\begin{aligned} \overline{x+y} &= \overline{x'+y'} \\ \overline{xy} &= \overline{x'y'} \end{aligned} \text{ إذن}$$

$$\begin{cases} x + y = \overline{x+y} \\ xy = \overline{xy} \end{cases} \text{ نضع إذن}$$

$$\begin{cases} \bar{x} + \bar{y} = \overline{x+y} \\ \bar{x} \cdot \bar{y} = \overline{xy} \end{cases} \text{ يعني:}$$

$$\bar{x} = \{y \in \mathbb{Z} / y \equiv x[3]\}$$

$$= \{y \in \mathbb{Z} / y = x + 3k / k \in \mathbb{Z}\}$$

$$\bar{x} = \{y \in \mathbb{Z} / y = x + 3k / k \in \mathbb{Z}\} \quad \text{إذن}$$

$$\bar{0} = \{3k / k \in \mathbb{Z}\}$$

$$= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$$

$$\bar{1} = \{1 + 3k / k \in \mathbb{Z}\}$$

$$= \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$$

$$\bar{2} = \{2 + 3k / k \in \mathbb{Z}\}$$

$$= \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$$

$$\bar{3} = \{3 + 3k / k \in \mathbb{Z}\}$$

$$= \{\dots, -6, -3, 0, 3, 6, 9, \dots\} = \bar{0}$$

(b) خاصيات:

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

$$\bar{x} = \{y \in \mathbb{Z} / y \equiv x[n]\}$$

$$y \in \bar{x} \Leftrightarrow y \equiv x[n] \Leftrightarrow y = x + nk / k \in \mathbb{Z}$$

$$\bar{x} = \{x + nk / k \in \mathbb{Z}\} \quad \text{إذن:}$$

2- ليكن $n \in \mathbb{N}$ و x, y من $\mathbb{Z}$

لنبين أن: $\bar{x} = \bar{y} \Leftrightarrow x \equiv y[n]$

* ($\Leftarrow$) نفترض أن $x \equiv y[n]$ ولنبين أن $\bar{x} = \bar{y}$

$$z \in \bar{x} \Leftrightarrow z \equiv x[n]$$

$$\Leftrightarrow z \equiv y[n] \quad (x \equiv y[n])$$

$$\Leftrightarrow z \in \bar{y}$$

إذن $\bar{x} = \bar{y}$

* ($\Rightarrow$) نفترض أن $\bar{x} = \bar{y}$ ولنبين أن $x \equiv y[n]$

لدينا $\bar{x} = \bar{y}$ إذن يوجد z من $\mathbb{Z}$ بحيث $z \in \bar{x}$ و $z \in \bar{y}$

$$\text{إذن } \begin{cases} z \equiv x[n] \\ z \equiv y[n] \end{cases} \text{ إذن } x \equiv y[n]$$

3- ليكن $n \in \mathbb{N}$ و x, y من $\mathbb{Z}$ بحيث $x \not\equiv y[n]$

لنبين أن: $\bar{x} \cap \bar{y} = \emptyset$

- نفترض أن $\bar{x} \cap \bar{y} \neq \emptyset$

$$\text{إذن يوجد } z \in \bar{x} \cap \bar{y} \text{ إذن } \begin{cases} z \equiv x[n] \\ z \equiv y[n] \end{cases} \text{ إذن } x \equiv y[n]$$

وهذا غير صحيح. إذن $\bar{x} \cap \bar{y} = \emptyset$

خاصية:

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

$$\bar{x} = \{x + nk / k \in \mathbb{Z}\} \quad (1)$$

$$\bar{x} = \bar{y} \Leftrightarrow x \equiv y[n] \quad (2)$$

$$\bar{x} \cap \bar{y} = \emptyset \Leftrightarrow x \not\equiv y[n] \quad (3)$$

هذا يعني أن صنفين متكافؤا منطبقان أو منفصلان.

4- تحديد $\mathbb{Z}/n\mathbb{Z}$ مع $n \in \mathbb{N}^*$

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, (n-1)\}$$

* لدينا:

$$\{0, 1, 2, \dots, (n-1)\} \subset \mathbb{Z}/n\mathbb{Z}$$

تعريف:

تعريف الجمع والضرب في $\mathbb{Z}/n\mathbb{Z}$ بما يلي:

$$\bar{x} + \bar{y} = \overline{x+y}$$

$$\bar{x} \cdot \bar{y} = \overline{xy}$$

مثال:

ضع جدول الجمع والضرب في $\mathbb{Z}/6\mathbb{Z}$

- لدينا: $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$\nearrow +$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

$\nearrow \times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

تمرين تطبيقي:

(*) حل في $\mathbb{Z}$ المعادلة: $4x \equiv 2[6]$

لدينا في $\mathbb{Z}/6\mathbb{Z}$:

$$4x \equiv 2[6] \Leftrightarrow \bar{4}x = \bar{2}$$

$$\Leftrightarrow \bar{4} \cdot \bar{x} = \bar{2}$$

$$\Leftrightarrow \begin{cases} \bar{x} = \bar{2} \\ \bar{x} = \bar{5} \end{cases} \quad (\text{من خلال الجدول})$$

$$\Leftrightarrow x \equiv 2[6] \text{ أو } x \equiv 5[6]$$

$$\Leftrightarrow x = 2 + 6k \text{ أو } x = 5 + 6k \quad (k \in \mathbb{Z})$$

$$\text{إذن: } S = \{2 + 6k, 5 + 6k / k \in \mathbb{Z}\}$$

(*) حل في $\mathbb{Z}$ المعادلة:

$$3x \equiv 1[5]$$

لدينا في $\mathbb{Z}/5\mathbb{Z}$

$$3x \equiv 1[5] \Leftrightarrow \bar{3}x = \bar{1}$$

$$\Leftrightarrow \bar{3} \cdot \bar{x} = \bar{1}$$

$$\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

بالتعويض نستنتج أن:

$$\bar{x} = \bar{2}$$

$$x \equiv 2[5]$$

$$x = 2 + 5k$$

$$S = \{2 + 5k / k \in \mathbb{Z}\}$$

خصائص:

(*) الجمع والضرب وتبادليان في $\mathbb{Z}/n\mathbb{Z}$

(*) الضرب توزيعي بالنسبة للجمع في $\mathbb{Z}/n\mathbb{Z}$

(*) $\bar{0}$ هو العنصر المحايد بالنسبة للجمع.

(*) $\bar{1}$ هو العنصر المحايد بالنسبة للضرب.

(*) $\bar{x}$ يقبل مقابل $-\bar{x}$ ونرمز له ب $-\bar{x}$.

تلخص هذه الخصائص بقولنا $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ حلقة تبادلية وواحدية.

برهان:

- لنبين أن (+) تجميعي.

لدينا:

$$\bar{x} + (\bar{y} + \bar{z}) = \bar{x} + \overline{(y+z)}$$

$$= \overline{x + (y+z)} = \overline{(x+y)+z}$$

$$= \overline{(x+y)} + \bar{z}$$

$$\bar{x} + (\bar{y} + \bar{z}) = (\bar{x} + \bar{y}) + \bar{z} \quad \text{إذن}$$

ملاحظة:

$$(\forall (x, y) \in \mathbb{Z}^2) \bar{x} \cdot \bar{y} = \bar{0} \Rightarrow \bar{x} = \bar{0} \text{ أو } \bar{y} = \bar{0}$$

مثل مضاد:

في $\mathbb{Z}/6\mathbb{Z}$ لدينا $\bar{3} \cdot \bar{4} = \bar{0}$

و $\bar{4} \neq \bar{0}$ و $\bar{3} \neq \bar{0}$

III- القاسم المشترك الأكبر.

1) تعريف:

ليكن b و a من $\mathbb{Z}^*$

نعتبر المجموعة $A = \{d \in \mathbb{N}^* / d \mid a \text{ و } d \mid b\}$

(*) لدينا $A \neq \emptyset$ (لأن $1 \in A$)

(*) لدينا: $(\forall d \in A) d \mid a$

إذن $d \leq |a|$

إذن A مكبورة ب $|a|$

(*) ولدينا $A \subset \mathbb{N}$

إذن A تقبل أكبر عنصر.

نضع $\delta = \max A$

δ يسمى القاسم المشترك الأكبر ل b و a

ونكتب $\delta = a \wedge b$.

تعريف:

ليكن b و a من $\mathbb{Z}^*$

نسمي القاسم المشترك الأكبر ل b و a أكبر قاسم موجب قطعاً

مشترك بين b و a . نرمز له ب $a \wedge b$ أو $a \Delta b$ أو $\text{pgcd}\{a, b\}$

مثال:

لنحدد $48 \wedge 36$

القواسم الموجبة ل 48 هي: 1, 2, 3, 4, 6, 8, 12, 16, 24, 48.

القواسم الموجبة ل 36 هي: 1, 2, 3, 4, 6, 9, 12, 18, 36.

إذن القواسم المشتركة: 1, 2, 3, 4, 6, 12. إذن $48 \wedge 36 = 12$

ملاحظة:

- $a \wedge b = b \wedge a$ (*)
- $0 \wedge b = |b|$ إذا كان $b \neq 0$ نضع $0 \wedge 0$ غير معرف.
- $a \wedge b = |a|$ فإن a/b (*)
- $a \wedge b = d$ يعني $\begin{cases} d/a \\ d/b \end{cases}$ وإذا كان $d' \leq d$ فإن $\begin{cases} d'/a \\ d'/b \end{cases}$ (*)

(2) خاصيات:

- 1 ليكن b من $\mathbb{Z}^*$ ليكن $d = a \wedge b$ لنبين أنه يوجد (u, v) من $\mathbb{Z} \times \mathbb{Z}$ بحيث $d = au + bv$ * نعتبر المجموعة: $A = \{au + bv / u, v \in \mathbb{Z}\}$ - لدينا $A \neq \emptyset$ لأن $n = a^2 + b^2 \in A$ - لدينا A مصغورة ب 1. - ولدينا $A \subset \mathbb{N}$ إذن لدينا p صاغر ل A و $p \in A$ إذن يوجد (u, v) من $\mathbb{Z}^2$ بحيث $p = au + bv$ * لنبين أن $d = p$ - لدينا $\begin{cases} d/a \\ d/b \end{cases}$ إذن $\begin{cases} d/au \\ d/bv \end{cases}$ إذن $d/au + bv$ يعني d/p إذن $|d| \leq |p|$ يعني $d \leq p$ (1) - لنبين أن p/a

- نعتبر القسمة الأقليدية ل a على p يعني $\begin{cases} a = pq + r \\ 0 \leq r < p \end{cases}$ لنبين أن $r = 0$: نفترض أن $r \neq 0$ إذن $0 < r < p$ $r = a - pq$ $r = a - (au + bv)q$ $r = a(1 - uq) + b(-Vq)$ لدينا:

- لدينا $\begin{cases} r = aU + bV \\ r \in \mathbb{N}^* \end{cases}$ إذن $r \in A$ ولدينا $r < p$ و $p = \sin A$ هذا تناقض. إذن $r = 0$ ومنه p/a

- وبنفس الطريقة نبين أن p/b إذن p قاسم مشترك ل b و $a \wedge b = d$ إذن $p \leq d$ (2)

- من (1) و (2) نستنتج أن: $p = d$ $d = au + bv$ إذن:

خاصية (1):

- ليكن b من $\mathbb{Z}^*$ إذا كان $a \wedge b = d$ فإنه يوجد زوج (u, v) من $\mathbb{Z}^2$ بحيث: $d = au + bv$

ملاحظة:

- ليكن b من $\mathbb{Z}^*$ وليكن $d = a \wedge b$ * العدد d هو أصغر عدد طبيعي غير منعدم يكتب على شكل $d = au + bv$ * الزوج (u, v) ليس وحيدا. -2 ليكن b من $\mathbb{Z}^*$ و $d = a \wedge b$

$$\begin{cases} d/a \\ d/b \end{cases} \Leftrightarrow d/d$$

(*) نفترض أن d/d

$$\begin{cases} d/a \\ d/b \end{cases} \text{ ولدينا } \begin{cases} d/a \\ d/b \end{cases} \text{ إذن: } \begin{cases} d/a \\ d/b \end{cases}$$

$$\begin{cases} d/a \\ d/b \end{cases} \Leftrightarrow d/d$$

لدينا $d = a \wedge b$ إذن $d = au + bv$ مع $(u, v) \in \mathbb{Z}^2$

$$\begin{cases} d/a \\ d/b \end{cases} \text{ ولدينا } \begin{cases} d/au \\ d/bv \end{cases} \text{ إذن } d/au + bv \text{ يعني } d/d$$

خاصية (2):

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

$$\begin{cases} d/a \\ d/b \end{cases} \Leftrightarrow d/d$$

وهذا يعني أن القواسم المشتركة ل b هي بالضبط قواسم d

$$\begin{cases} d/a \\ d/b \end{cases} \Leftrightarrow d/a \wedge b$$

ملاحظة:

ليكن b من $\mathbb{Z}^*$

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

برهان:

لنبين أن: $|a| \wedge |b| = a \wedge b$

$$d' = |a| \wedge |b| \text{ و } d = a \wedge b \text{ نضع}$$

$$\begin{cases} d/a \\ d/b \end{cases} \text{ ولدينا } d = a \wedge b \text{ إذن } \begin{cases} d/a \\ d/b \end{cases}$$

$$\begin{cases} d/a \\ d/b \end{cases} \text{ ولدينا: } \begin{cases} a/|a| \\ b/|b| \end{cases} \text{ إذن } \begin{cases} d/|a| \\ d/|b| \end{cases} \text{ يعني } d/|a| \wedge |b|$$

يعني d/d' (1)

$$\begin{cases} a/|a| \\ b/|b| \end{cases} \text{ ولدينا } \begin{cases} d'/|a| \\ d'/|b| \end{cases} \text{ إذن } d' = |a| \wedge |b|$$

$$\begin{cases} d/a \\ d/b \end{cases} \text{ إذن } \begin{cases} d'/a \\ d'/b \end{cases} \text{ يعني } d'/a \wedge b \text{ يعني } d'/d \text{ (2)}$$

من (1) و (2) نستنتج أن $|d| = |d'|$

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

(*) إذن يلغي البحث عن طرق تحديد القاسم المشترك الأكبر لعددين موجبين.

(5) خوارزمية إقليدس:

خاصية (1)

ليكن b من $\mathbb{N}^*$

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \text{ إذا كان } r \text{ هو باقي قيمة } a \text{ على } b \text{ يعني:}$$

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

برهان:

$$\text{لدينا } \begin{cases} a = bq + r \\ 0 \leq r < b \end{cases} \text{ لنبين أن } a \wedge b = b \wedge r$$

نضع: $d = d'$ لنبين أن $d' = b \wedge r$ و $d \neq a$

$$\text{لدينا: } \begin{cases} d \wedge bq \\ d \wedge r \end{cases} \text{ إذن } \begin{cases} d \wedge a \\ d \wedge r \end{cases}$$

يعني $d \wedge a$

$$\text{إذن } \begin{cases} d \wedge a \\ d \wedge b \end{cases} \text{ يعني } d \wedge a \wedge b \text{ يعني } d \wedge d \quad (1)$$

$$\text{لدينا } \begin{cases} d \wedge a \\ d \wedge b \end{cases} \text{ إذن } \begin{cases} d \wedge a \\ d \wedge bq \end{cases} \text{ إذن } d \wedge a - bq \text{ يعني}$$

$$\begin{cases} d \wedge b \\ d \wedge r \end{cases} \text{ إذن } d \wedge r \text{ يعني: } d \wedge b \wedge r \text{ يعني}$$

$$(2) \quad d \wedge d'$$

من (1) و (2) نستنتج أن $|d| = |d'|$

وبما أن d و d' وجبان قطعاً فإن $d = d'$

$$\text{يعني } a \wedge b = b \wedge r$$

ملاحظة:

في البرهان م نستعمل كون $0 \leq r < b$. إذن بصفة عامة:

$$\text{إذا كان } a = bq + r \text{ فإن } a \wedge b = b \wedge r$$

مثال:

$$\text{لنحدد } 416 \wedge 76$$

$$\text{لدينا } \begin{array}{r|l} 416 & 76 \\ 36 & 5 \end{array}$$

$$\text{إذن } 416 = 76 \times 5 + 36$$

$$\text{إذن } 416 \wedge 76 = 76 \wedge 36$$

$$\text{ولدينا: } 76 = 2 \times 36 + 4$$

$$\text{إذن } 76 \wedge 36 = 36 \wedge 4$$

$$\text{ولدينا } 36 = 9 \times 4 + 0$$

$$\text{إذن: } 4/36 \text{ ومنه: } 4 = |4| = 4 \wedge 4$$

$$\text{بالتالي: } 76 \wedge 36 = 4$$

$$\text{أي: } 416 \wedge 76 = 4$$

نلخص هذا في الجدول التالي:

416	76	36	4
	5	2	9
36	4	0	

تعميم:

ليكن b و a من $\mathbb{N}^*$ بحيث $a > b$

* نقوم بقسمة a على b : $a = bq_1 + r_1$, $0 \leq r_1 < b$

- إذا كان $r_1 = 0$ فإن $b \wedge a = b$ إذن $a \wedge b = b$

- إذا كان $r_1 \neq 0$ فإن $a \wedge b = b \wedge r_1$

نقوم بقسمة b على r_1 : $b = r_1 q_2 + r_2$, $0 \leq r_2 < r_1$

- إذا كان $r_2 = 0$ فإن $r_1 \wedge b = r_1$ إذن $b \wedge r_1 = r_1$

- إذا كان $r_2 \neq 0$ فإن $b \wedge r_1 = r_1 \wedge r_2$

وهكذا نتائج القسمة المتتالية حتى نحصل على باقي منعدم (ومن الضروري الحصول على باقي منعدم لأن هذه البواقي موجبة وتتاقص قطعاً).

نفترض أن r_{n+1} أول باقي منعدم.

$$\text{يعني: } r_{n+1} = 0 \text{ و } r_n \neq 0$$

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

$$b \wedge r_1 = r_1 \wedge r_2 \quad 0 \leq r_2 < r_1 \quad b = r_1 q_2 + r_2$$

$$\text{لدينا } r_{n+1} = 0 \text{ إذن } r_n / r_{n-1} \quad r_{n+1} = r_n q_{n+1} + r_{n+1}$$

$$\text{ومنه } r_{n-1} \wedge r_n = r_n$$

إذن $a \wedge b = r_n$ وهو آخر باقي غير منعدم.

خاصية:

ليكن $\mathbb{N}^*$

القاسم المشترك الأكبر هو آخر باقي غير منعدم في القسمة المتتالية (خوارزمية أقليدس).

ملاحظة:

نلخص هذه النتائج في الجدول:

a	b	r ₁	r ₂	...	...	...
	q ₁	q ₂	q ₃			
r ₁	r ₂	r ₃	-	-	r _n	0

مثال:

$$\text{لنحدد: } 792 \wedge 36$$

لدينا:

792	36	16	4
	21	2	4
16	4	0	

$$\text{إذن: } 792 \wedge 36 = 4$$

(4) الأعداد الأولية فيما بينها:

(a) تعريف:

ليكن $\mathbb{Z}^*$

نقول إن a و b أوليان فيما بينهما إذا وفقط إذا كان $a \wedge b = 1$

$$\text{مثال: } 9 \wedge 4 = 1$$

إذن 9 و 4 أوليان فيما بينهما.

(b) خاصيات:

مبرهنة (1): (مبرهنة Bezout)

ليكن $\mathbb{Z}^*$

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

برهان:

($\Rightarrow$) نفترض أن $a \wedge b = 1$ من خلال خاصية سابقة نستنتج أن:

$$(\exists (u, v) \in \mathbb{Z}^2): 1 = au + bv$$

($\Leftarrow$) نفترض أن $(\exists (u, v) \in \mathbb{Z}^2): 1 = au + bv$ لنبين أن $a \wedge b = 1$

نضع $d = a \wedge b$ ولنبين أن: $d = 1$

$$\text{لدينا: } \begin{cases} d \wedge a \\ d \wedge b \end{cases} \text{ إذن } \begin{cases} d \wedge au \\ d \wedge bv \end{cases} \text{ إذن } d \wedge au + bv \text{ أو } d \wedge -1$$

يعني $d \wedge 1$

$$\text{إذن } d = 1 \text{ أو } d = -1$$

ولدينا $d > 0$ إذن $d = 1$ يعني $a \wedge b = 1$.

مثال:

ليكن $n \in \mathbb{Z}$ مع $n \neq 0$ و $n \neq -1$. لنحدد: $(n+1) \wedge n$

$$\text{لدينا: } 1(n+1) - 1(n) = 1$$

$$\text{إذن } (n+1) \wedge (n) = 1$$

ملاحظة:

$$\begin{cases} a_1/b \\ a_2/b \\ a_n/b \end{cases} \Rightarrow a_1 \cdot a_2 \dots a_n / b$$

أولية فيما بينها مثلى

مبرهنة (7):

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

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

ملاحظة:

إذا كان $a \wedge n + 1$ فإن الاستلزام خاطئ.

مثل: $3 \cdot 2 \equiv 3 \cdot 4[6]$ لكن $2 \not\equiv 4[6]$

برهان:

لدينا $ax \equiv ay[n]$ يعني $n \mid ax - ay$

يعني $n \mid a(x - y)$

ولدينا $a \wedge n = 1$ إذن حسب (Gauss) نستنتج أن:

$$n \mid x - y$$

يعني $x \equiv y[n]$

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

(5) حل المعادلة $ax + by = c$ في $\mathbb{N}$.

(a) أمثلة:

مثال 1: لنحل في $\mathbb{Z}^2$ المعادلة $3x - 4y = 1$ (1).

* لدينا $3 \wedge 4 = 1$ إذن حسب Bezout: يوجد زوج (u, v) من $\mathbb{Z}$.

$$3u + 4v = 1$$

$$3u - 4(-v) = 1$$

إذن $(u, -v)$ حل للمعادلة (1)

وبالتالي المعادلة (1) تقبل حلا على الأقل.

* لنبحث عن حل خاص للمعادلة (1).

نلاحظ أن $(-1, -1)$ حل للمعادلة (1).

* لنحدد جميع الحلول:

ليكن (x, y) حل للمعادلة (1).

$$\text{لدينا } 3(-1) - 4(-1) = 1 \quad (2)$$

$$\text{ولدينا } (-1, -1) \text{ حل إذن: } 3(-1) - 4(-1) = 1 \quad (3)$$

من (3) - (2) نستنتج أن: $3(x+1) - 4(y+1) = 0$

$$3(x+1) = 4(y+1) \text{ يعني}$$

$$\text{إذن } 3/4(y+1)$$

ولدينا $3 \wedge 4 = 1$ إذن حسب (Gauss) لدينا: $3/4(y+1)$.

$$\text{يعني } y+1 = 3k \text{ يعني: } y = 3k - 1$$

وبالتعويض في (2) نحصل على:

$$3x - 4(3k - 1) = 1$$

$$3x = 12k - 3 \text{ يعني}$$

$$x = 4k - 1 \text{ يعني}$$

$$\begin{cases} y = 3k - 1 \\ x = 4k - 1 \end{cases} \quad (k \in \mathbb{Z}) \text{ إذن:}$$

عكسا

نلاحظ أنه تم حساب x انطلاقا من المعادلة (2) إذن y يحققان المعادلة (1)

وبالتالي: $S = \{(4k-1; 3k-1) / k \in \mathbb{Z}\}$

مثال 2:

لنحل في $\mathbb{Z}^2$ المعادلة: $67x + 57y = 2$ (E)

* لنحدد $67 \wedge 57$

67	57	10	7	3	1
	1	5	1	2	3
10	7	3	□	0	

إذن $67 \wedge 57 = 1$

وحسب Bezout فإنه يوجد (u, v) بحيث $67u + 57v = 1$

$$67(2u) + 57(2v) = 2 \text{ يعني}$$

إذن الزوج $(2u, 2v)$ حل للمعادلة (E).

إذن (E) تقبل حلا على الأقل.

* لنبحث عن حل خاص للمعادلة (E).

خوارزمية أقليدس تمكننا من البحث عن حل خاص إذا لم يكن هناك حل واضح.

$$\text{لدينا: } 67 = 1 \times 57 + 10 \quad (1)$$

$$57 = 5 \times 10 + 7 \quad (2)$$

$$10 = 1 \times 7 + 3 \quad (3)$$

$$7 = 2 \times 3 + 1 \quad (4)$$

$$\text{نضع } b = 57 \text{ و } a = 67$$

من (1) نحصل على: $10 = a - b$

من (2) نحصل على: $7 = 5b - 5a$ أي $b = 5(a - b) + 7$

من (3) نحصل على: $3 = 6a - 7b$ أي $a - b = (6b - 5a) + 3$

من (4) نحصل على: $1 = 6b - 5a = 2(6a - 7b) + 1$ أي

$$-17a + 20b = 1$$

$$\text{يعني: } 67(-17) + 57(20) = 1$$

$$\text{يعني: } 67(-34) + 57(40) = 2$$

إذن $(-34, 40)$ حل للمعادلة (E).

* لنحدد جميع حلول المعادلة (E).

ليكن (x, y) حل للمعادلة.

$$\text{إذن } 67x + 57y = 2 \quad (1)$$

ولدينا $(-34, 40)$ حل إذن:

$$67(-34) + 57(40) = 2 \quad (2)$$

من (1) - (2) نستنتج أن:

$$67(x+34) + 57(y-40) = 0$$

$$\text{يعني } 67(x+34) = -57(y-40)$$

$$\text{إذن } 57/67(x+34)$$

وبما أن $57 \wedge 67 = 1$ فإن $57/x + 34$

$$x + 34 = 57k \text{ أي}$$

$$x = 57k - 34 \text{ إذن}$$

وبالتعويض في (1) نجد:

$$57y = -67 \times 57k + 2280$$

$$y = -67k + 40 \text{ ومنه}$$

2- خاصيات:

خاصية (1):

ليكن $a_1, a_2, \dots, a_n$ من $\mathbb{Z}^*$

$$d = a_1 \wedge a_2 \wedge \dots \wedge a_n \Rightarrow \exists (u_1, u_2, \dots, u_n) \in \mathbb{Z}^n / d = \sum_{i=1}^n a_i u_i$$

خاصية (2):

ليكن: $d = a_1 \wedge a_2 \wedge \dots \wedge a_n$

قواسم d هي بالضبط القواسم المشتركة للأعداد a_i

$$\begin{cases} d'/a_1 \\ d'/a_2 \end{cases} \Leftrightarrow d'/a_1 \wedge d'/a_2 \wedge \dots \wedge d'/a_n = d$$

يعني:

خاصية (3):

ليكن a, b, c من $\mathbb{Z}^*$

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

لدينا: هذا يعني أنه عندك حساب القاسم المشترك الأكبر لعدة أعداد يمكن تعويض كل اثنين بالقاسم المشترك الأكبر لهما.

(3) الأعداد الأولية فيما بينها:

(a) تعريف:

نقول إن الأعداد $a_1, a_2, \dots, a_n$ من $\mathbb{Z}^*$ أولية فيما بينها إذا وفقط إذا كان

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = 1$$

لاحظة:

لا يجب الخلط بين أعداد أولية فيما بينها وأعداد أولية فيما بينها متنى متنى.

مثلا: الأعداد 9, 12, 16, 4, 30 أولية فيما بينها.

لكنها ليست أولية فيما بينها متنى متنى.

(b) خاصيات:

خاصية (1):

ليكن $a_1, a_2, \dots, a_n$ من $\mathbb{Z}^*$

$$a_1 \wedge a_2 \wedge \dots \wedge a_n = 1 \Leftrightarrow \exists (u_1, u_2, \dots, u_n) \in \mathbb{Z}^n / 1 = \sum_{i=1}^n a_i u_i$$

خاصية (2):

ليكن $a_1, a_2, \dots, a_n$ من $\mathbb{Z}^*$ و $d > 0$

$$d = a_1 \wedge a_2 \wedge \dots \wedge a_n \Leftrightarrow \begin{cases} d/a_1 \text{ et } d/a_2 \dots d/a_n \\ \frac{a_1}{d} \wedge \frac{a_2}{d} \wedge \dots \wedge \frac{a_n}{d} = 1 \end{cases}$$

لدينا:

(V) المضاعف المشترك الأصغر:

(1) تعريف:

ليكن a, b من $\mathbb{Z}^*$

$$E = \{m \in \mathbb{N}^* / a/m \text{ et } b/m\}$$

- لدينا $E \neq \emptyset$ (لأن $|ab| \in E$).

- E مصغرة ب 0.

- $E \subset \mathbb{N}$

إن E تقبل الأصغر عنصر نضع: $q = \min E$

q يسمى المضاعف المشترك الأصغر ل a و b . ونكتب

$$q = a \vee b$$

$$\begin{cases} x = 57k + 34 \\ y = -67k + 40 \end{cases} \quad (k \in \mathbb{Z})$$

إذن:

عكسيا: (x, y) يحققان (E) لأنه تم تحديد y انطلاقا من (E)

* وبالتالي: $S = \{(57k + 34; -67k + 40) / k \in \mathbb{Z}\}$

(b) تعميم:

نعتبر المعادلة (E) $ax + by = c$ مع $a \neq 0$ و $b \neq 0$

- نضع $d = a \wedge b$

-1 إذا كان $d \nmid c$

نفترض أن المعادلة تقبل حلا (x, y) .

$$ax + by = c$$

إذن

$$\begin{cases} d/a \\ d/b \end{cases} \text{ إذن } \begin{cases} d/ax \\ d/by \end{cases} \text{ إذن } d/ax + by \text{ يعني } d/c$$

وهذا يتناقض. إذن المعادلة ليس لها حل.

-2 إذا كان $d \mid c$

$$\begin{cases} a = da' \\ b = db' \\ c = dc' \end{cases} \text{ مع } a' \wedge b' = 1$$

إذن (E) تصبح:

$$a'x + b'y = c'$$

* لدينا $a' \wedge b' = 1$

إذن يوجد (u, v) بحيث $a'u + b'v = 1$

يعني: $a'(c'u) + b'(c'v) = c'$

إذن $(c'u, c'v)$ حل للمعادلة (E') .

إذن (E) لها حل.

* لنبحث عن حل خاص:

باستعمال خوارزمية أقليدس إذا لم يكن هناك حل واضح.

نفترض أن (x_0, y_0) حل خاص للمعادلة.

$$(1) \quad a'x_0 + b'y_0 = c'$$

* ليكن (x, y) حل للمعادلة يعني: $a'x + b'y = c'$

من (1) و (2) نجد: $a'(x - x_0) + b'(y - y_0) = 0$

$$a'(x - x_0) = -b'(y - y_0)$$

$$b'/a'(x - x_0)$$

$$x = b'k + x_0 \text{ يعني } b'/(x - x_0) \text{ إذن } a' \wedge b' = 1$$

وبالتعويض في (E') نجد

$$a'(b'k + x_0) + b'y = c'$$

$$b'y = c' - a'x - a'b'k$$

يعني:

$$a'x_0 = c' - b'y_0 \quad (1)$$

$$b'y = c' - a'x - a'b'k$$

$$y = -a'k + y_0$$

عكسيا: (x, y) يحقق (E) لأنه تم حساب y انطلاقا من (E)

$$S = \{(b'k + x_0, -a'k + y_0) / k \in \mathbb{Z}\}$$

وبالتالي:

(IV) القاسم المشترك الأكبر لعدة أعداد:

1- تعريف:

ليكن $a_1, a_2, \dots, a_n$ أعداد غير منعمة

نسمي القاسم المشترك الأكبر لهذه الأعداد أكبر قاسم مشترك

موجب قطعاً لهذه الأعداد. ونرمز له ب $a_1 \wedge a_2 \wedge \dots \wedge a_n$

(1) تعريف:

ليكن $\mathbb{Z}^*$ هو $\mathbb{Z}^*$ من
نسمي المضاعف المشترك الأصغر للعددين a و b أصغر
مضاعف موجب مشترك بين a و b . ونرمز له بـ $a \vee b$.

* ملاحظة:

$$\begin{cases} a/m \\ b/m \end{cases} \text{ يعني } m = a \vee b$$

وإذا كان m' مضاعف مشترك لـ a و b فإن $m \leq m'$

$$b \vee a = a \vee b$$

$$a \vee a = |a|$$

إذا كان a/b فإن $a \vee b = |b|$

(2) خاصيات:

خاصية (1):

ليكن a و b من $\mathbb{Z}^*$ و $m = a \vee b$ هي بالضبط المضاعفات المشتركة لـ a و b .

$$\text{يعني: } \begin{cases} a/m' \\ b/m' \end{cases} \Leftrightarrow m = a \vee b/m'$$

برهان:

($\Leftarrow$) نفترض أن a/m' و b/m'

$$\text{ولدينا } \begin{cases} a/m' \\ b/m' \end{cases} \text{ إذن } \begin{cases} a/m \\ b/m \end{cases}$$

($\Rightarrow$) نفترض أن: a/m' و b/m' لنبين أن m/m'

$$\text{نعتبر قسمة } m' \text{ على } m \text{ يعني: } \begin{cases} m' = mq + r \\ 0 \leq r < m \end{cases}$$

لنبين أن $r = 0$

نفترض العكس. يعني $r \neq 0$

$$\text{إذن } 0 < r < m$$

$$\text{لدينا: } r = m' - mq$$

$$\text{ولدينا } \begin{cases} a/m' \\ a/m \end{cases} \text{ إذن } a/m' - mq \text{ يعني } a/r$$

وبنفس الطريقة نجد b/r

إذن r مضاعف مشترك لـ a و b .

وجدنا أن r مضاعف مشترك لـ a و b ويحقق $0 < r < m$ وهذا

تناقض لأن $a \vee b = m$

إذن $r = 0$ ومنه m/m' .

ملاحظة:

$$|a| \vee |b| = |a \vee b| = a \vee b$$

خاصية (2):

ليكن a و b من $\mathbb{Z}^*$

$$\text{لدينا: } (a \wedge b) \cdot (a \vee b) = |ab|$$

برهان:

$$\begin{cases} d = a \wedge b \\ m = a \vee b \end{cases} \text{ نضع}$$

$$\text{نضع } \begin{cases} a = \alpha d \\ b = \beta d \end{cases} \text{ مع } \alpha \wedge \beta = 1$$

$$\text{ونضع } \begin{cases} m = \gamma a \\ m = \varphi b \end{cases}$$

ولدينا: $\gamma a = \varphi b$ يعني: $\gamma \alpha d = \varphi \beta d$

يعني: $\gamma \alpha = \varphi \beta$

إذن $\alpha/\varphi \beta$

ولدينا $\alpha \wedge \beta = 1$ إذن α/φ يعني: $\varphi = dk$

إذن: $m = \varphi b$

يعني: $m = \alpha k \beta d$ إذن $\alpha \beta d/m$ (1)

* لنبين أن $m/\alpha \beta d$

$$\text{لدينا: } \alpha \beta d = \alpha b \text{ و } \alpha \beta d = \beta a \text{ إذن } \begin{cases} b/\alpha \beta d \\ a/\alpha \beta d \end{cases} \text{ إذن}$$

$$a \vee b/\alpha \beta d$$

يعني: $m/\alpha \beta d$ (2)

من (1) و (2) نستنتج أن:

$$|m| = |\alpha \beta d|$$

$$m = |\alpha \beta d| \text{ يعني:}$$

$$dm = |\alpha \beta d|^2 \text{ يعني:}$$

$$dm = |ab| \text{ يعني:}$$

$$(a \wedge b) \cdot (a \vee b) = |ab| \text{ ومنه:}$$

خاصية (3):

ليكن a و b من $\mathbb{Z}^*$

$$\text{لدينا: } ac \vee bc = |c|(a \vee b)$$

برهان:

$$\text{نعلم أن: } (ac \wedge bc)(ac \vee bc) = |ac \cdot bc|$$

$$\text{يعني: } |c|(a \wedge b) \cdot (ac \vee bc) = |ab| \cdot |c|^2$$

$$\text{يعني: } (a \wedge b) \cdot (ac \vee bc) = (a \wedge b)(a \vee b)|c|$$

$$\text{يعني: } (ac \vee bc) = |c|(a \vee b)$$

تمرين:

ليكن a و b من $\mathbb{Z}^*$ و $m > 0$

$$m = a \vee b \Leftrightarrow \begin{cases} a/m \text{ et } b/m \\ \frac{m}{a} \wedge \frac{m}{b} = 1 \end{cases}$$

(3) المضاعف المشترك الأصغر لعدة أعداد:

تعريف:

ليكن $a_1, a_2, \dots, a_n$ من $\mathbb{Z}^*$

المضاعف المشترك الأصغر لهذه الأعداد هو أصغر مضاعف

موجب مشترك بين هذه الأعداد.

خاصية:

ليكن $a_1, a_2, \dots, a_n$ من $\mathbb{Z}^*$ و $m = a_1 \vee a_2 \vee \dots \vee a_n$

مضاعفات m هي بالضبط المضاعفات المشتركة للأعداد a_i .

(VI) الأعداد الأولية:

(1) تعريف:

تعريف (1):

ليكن a من $\mathbb{Z}^*$.

نسمي قاسم فعلي لـ a كل قاسم d لـ a يخالف $-1, 1, -a, a$

يعني $d \notin \{-1, 1, -a, a\}$.

تعريف (2):

ليكن $p \in \mathbb{Z}^* - \{-1, 1\}$

نقول إن p أولي إذا وفقط إذا كان لا يقبل أي قاسم فعلي يعني إذا

كان يقبل 4 قواسم بالضبط هي $1, -1, p, -p$

أمثلة:

(*) $1, 0, -1$ ليست أولية.

(*) 4 ليس أولي لأن 2 قاسم فعلي ل 4.

(*) 2, 3, 5, 7 أعداد أولية.

(2) خاصية (1):

خاصية (1):

ليكن $\{ -1, 1 \} - \mathbb{Z}^*$ a غير أولي.

أصغر قاسم فعلي موجب ل a يكون أوليا.

برهان:

لتكن A مجموعة القواسم الفعلية الموجبة ل a .

- لدينا $A \neq \emptyset$ (لأن a ليس أولي وبالتالي يقبل قاسم فعلي موجب)

- لدينا A مصغورة ب 0.

- $A \subset \mathbb{N}$

إذن A تقبل الأصغر عنصر. نضع $p = \min A$

- لنبين أن p أولي:

لدينا p قاسم فعلي ل a إذن $\{ -1, 1 \} \notin p$ لأن $a \neq 0$

لنبين أن p لا يقبل قاسما فعليا.

نفترض أن p يقبل قاسما فعليا p'

لدينا $\left\{ \begin{array}{l} p'/p \\ p/a \end{array} \right\}$ إذن p'/a

- لدينا p'/p إذن $|p'| \leq |p|$

يعني: $|p'| \leq p$

ولدينا $\left\{ \begin{array}{l} p' \neq p \\ p' \neq -p \end{array} \right\}$ إذن $|p'| < p$

ولدينا p/a إذن $|p| < |a|$ أي $|p'| < |a|$

إذن $|p'| < |a|$

إذن $|p'| \neq |a|$

ولدينا $|p'| \neq 1$

إذن $|p'|$ قاسم فعلي ل a

ولدينا $|p'| < p$

وجدنا قاسما فعليا موجبا ل a ويحقق $|p'| < p$

وهذا تناقض لأن p أصغر قاسم فعلي موجب.

ومنه p لا يقبل قاسما فعليا.

وبالتالي p أولي.

ملاحظة:

كل عدد $\{ -1, 1 \} - \mathbb{Z}^*$ a غير أولي يقبل قاسم فعلي أولي موجب.

خاصية (2):

مجموعة الأعداد الأولية غير منتهية.

برهان:

لتكن P مجموعة الأعداد الأولية الموجبة.

لنبين أن P غير مكبورة.

نفترض العكس. يعني P مكبورة.

- لدينا $P \neq \emptyset$ (لأن $2 \in P$).

- $P \subset \mathbb{N}$

إذن P تقبل الأكبر عنصر. نضع: $q = \max P$

- نضع $p = q! + 1$

لنبين أن p أولي:

نفترض العكس. يعني p يقبل قاسما فعليا أولي موجب p_0 .

لدينا $P = \{ 2, 3, 5, 7, \dots, q \}$

ولدينا $p_0 \in P$ أولي موجب إذن $p_0 \in P$

إذن p_0 هو أحد عوامل $q!$ إذن $p_0/q!$

ولدينا p_0/p

إذن $p_0/p - q!$

يعني $p_0/1$

يعني $p_0 = 1$ أو $p_0 = -1$

وهذا تناقض لأن p_0 أولي.

إذن p أولي.

- وجدنا إذن p أولي و $p > q$ وهذا تناقض لأن q هو أكبر عدد أولي.

بالتالي P غير مكبورة.

ومنه P غير منتهية.

(3) طريقة عملية لتحديد الأعداد الأولية:

ملاحظة:

إذا كان p عدد أولي فإن $-p$ أولي. وبالتالي يكفي البحث عن طرق لتحديد الأعداد الأولية الموجبة.

خاصية:

ليكن $n \in \mathbb{N}^* - \{1\}$

إذا كان n غير أولي فإنه يوجد عدد أولي p بحيث $\left\{ \begin{array}{l} p/n \\ p^2 \leq n \end{array} \right\}$

برهان:

نفترض أن n غير أولي.

لدينا $n \in \mathbb{N}^* - \{1\}$

ليكن p أصغر قاسم فعلي موجب ل n .

من خلال الخاصية (1) لدينا p أولي.

إذن p أولي و p/n

لنبين أن $p^2 \leq n$

لدينا: p/n يعني $n = kp$

لنبين أن k قاسم فعلي ل n

لدينا $k \nmid 0$

- نفترض أن $k=1$ إذن $n=p$ وهذا تناقض لأن:

n غير أولي و p أولي.

إذن $k \neq 1$

- نفترض أن $k=n$ إذن $p=1$ وهذا تناقض لأن p أولي.

إذن $k \neq n$

- ولدينا $k > 0$ إذن $k \neq \#$ و $k \neq -1$

إذن k قاسم فعلي موجب ل n .

- وبما أن p هو أصغر قاسم فعلي موجب ل n .

فإن: $p \leq k$

يعني: $p^2 \leq kp$

يعني $p^2 \leq n$

- إذن يوجد p أولي بحيث: $\left\{ \begin{array}{l} p/n \\ p^2 \leq n \end{array} \right\}$

ملاحظة:

1- ليكن $n \in \mathbb{N}^* - \{1\}$

إذا أردنا أن نتحقق هل n أولي، نتبع ما يلي:

+ نعتبر الأعداد الأولية p التي تحقق $p^2 \leq n$

- إذا كان أحد هذه الأعداد يقسم n فإن n غير أولي لأنه يقبل قاسما فعليا.

- إذا كانت جميع هذه الأعداد لا تقسم n فإن n أولي.

مثال:

- لنحدد جميع الأعداد الأولية أصغر من 100.

بالنسبة للأعداد الأصغر من 100، الأعداد الأولية p التي يمكن

أن تحقق $p^2 \leq n$ هي 2, 3, 5, 7.

إذن الأعداد الأولية الأصغر من 100 هي الأعداد التي لا تقبل

القسمة على 2, 3, 5, 7 إضافة إلى الأعداد 2, 3, 5, 7.

- إذن هذه الأعداد هي:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,

53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

2- ليكن $n \in \mathbb{N}^* - \{1\}$

لكي نتحقق هل n أولي يمكن اتباع الخوارزمية التالية.

نقوم بقسمة n على الأعداد الأولية p انطلاقا من 2 على التوالي،

ونقف عند إحدى الحالات:

- إذا أصبح الخارج q أصغر من p قطعاً، والباقي غير منعدم

فيكون في هذه الحالة العدد n أولي.

- إذا حصلنا على باقي منعدم. فيكون n غير أولي.

برهان:

(*) إذا حصلنا على باقي منعدم فإن n يقبل قاسما فعليا.

إذن n غير أولي.

(*) نفترض أن حصلنا على $q < p$ قبل $r = 0$

لدينا $n = qp + r$ $0 \leq r < p$

لدينا: $q < p \Rightarrow q + 1 \leq p$

$\Rightarrow pq + p \leq p^2$

ولدينا $r < p$

إذن $pq + r < p + pq \leq p^2$

إذن $pq + r \leq p^2$ يعني $n \leq p^2$

إذن أجرينا قسمة n على p ولم نحصل على باقي منعدم حتى

أصبح $p^2 \geq n$ هذا يعني أن n لا يقبل على أي عدد أولي p

يحقق $p^2 \leq n$. إذن n أولي.

مثال:

لنتحقق هل 179 أولي:

p	2	3	5	7	11	13	17
q	89	59	35	25	16	13	10
r	1	2	4	4	3	10	9

إذن 179 أولي.

(4) الأعداد الأولية وقابلية القسمة:

خاصية (1):

ليكن $a \in \mathbb{Z}^*$ و p أولي.

$p \wedge a = 1 \Leftrightarrow p \times a$

برهان:

($\Rightarrow$) نفترض أن $p \wedge a = 1$ ولنبين أن $p \times a$

- نفترض p/a

إذن $p \wedge a = |p|$ إذن $|p| = 1$

يعني $p = 1$ أو $p = -1$

وهذا تناقض لأن p أولي.

إذن $p \times a$

($\Leftarrow$) نفترض أن $p \times a = 1$ لنبين أن $p \wedge a = 1$

نضع $d = p \wedge a$

إذن $\begin{cases} d/p \\ d/a \end{cases}$ ونعلم أن قواسم p هي: $-1, 1, -p, p$

ولدينا $\begin{cases} p \times a \\ -p \times a \end{cases}$ إذن $d \neq -p$ و $d \neq p$

ولدينا $d \neq -1$ لأن $d > 0$

إذن $d = 1$ ومنه $p \wedge a = 1$

خاصية (2):

ليكن p, q أوليين:

$p \wedge q = 1 \Leftrightarrow |p| \neq |q|$

برهان:

$p \wedge q = 1 \Leftrightarrow p \times q$

$\Leftrightarrow p \notin \{1, -1, q, -q\}$

$\Leftrightarrow p \notin \{q, -q\}$

$\Leftrightarrow p \neq q$ و $p \neq -q$

$\Leftrightarrow |p| \neq |q|$

خاصية (3):

ليكن $a_1, a_2, \dots, a_n$ من $\mathbb{Z}$ و p أولي.

$p/a_1 a_2 \dots a_n \Rightarrow (\exists i \in \{1, 2, \dots, n\}) p/a_i$

برهان:

نفترض أن $p/a_1 a_2 \dots a_n$. لنبين أن: p/a_i $\exists i \in \{1, 2, \dots, n\}$

* إذا كان أحد الأعداد a_i منعدم.

مثلا $a_{i_0} = 0$ فإن p/a_{i_0}

* إذا كانت جميع الأعداد a_i تخالف 0.

نفترض أن: $p \times a_i : (\forall i \in \{1, 2, \dots, n\})$

يعني $p \wedge a_i = 1$

إذن $P \wedge \prod_{i=1}^n a_i = 1$ يعني $P \times \prod_{i=1}^n a_i$

وهذا تناقض.

إذن $p/a_i : (\exists i \in \{1, 2, \dots, n\})$.

ملاحظة:

1- ليكن $a \in \mathbb{Z}$ و p أولي و $n \in \mathbb{N}$.

(*) $p/a^n \Rightarrow p/a$

(*) $p/ab \Rightarrow p/a$ أو p/b

2- ليكن p أولي موجب.

(*) $(\forall 1 \leq k < p) : p \wedge k = 1$

(*) $(\forall k \in \mathbb{Z}/1 \leq |k| < p) : p \wedge k = 1$

خاصية (4):

ليكن $p, p_1, p_2, \dots, p_n$ أعداد أولية.

$p/p_1 p_2 \dots p_n \Rightarrow (\exists i \in \{1, 2, \dots, n\}) |p| = |p_i|$

برهان:

لدينا:

$$p/p_1 p_2 \dots p_n$$

إذن يوجد i بحيث p/p_i

ونعلم أن قواسم p_i هي: $-1, 1, -p_i, p_i$

ولدينا $p \neq 1$ و $p \neq -1$ إذن $p_i = p$ أو $-p_i = p$

يعني $|p| = |p_i|$

ملاحظة:

$$p/p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n} \Rightarrow (\exists i \in \{1, 2, \dots, n\}) |p| = |p_i| \quad (*)$$

(*) إذا كانت الأعداد p_i موجبة

$$p/p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n} \Rightarrow (\exists i \in \{1, 2, \dots, n\}) p = p_i \quad \text{فإن:}$$

تطبيق:

ليكن p عدد أولي موجب.

(1) بين أن p/C_p^k لكل $1 \leq k \leq p-1$

$$(2) \text{ بين أن } (\forall a \in \mathbb{N}) (a+1)^p \equiv a^p + 1[p]$$

$$(3) \text{ (a) بين أن: } n^p \equiv n[p] \quad (\forall n \in \mathbb{N})$$

(b) استنتج أن: $n^{p-1} \equiv 1[p]$ لكل n من $\mathbb{N}$ بحيث $n \wedge p = 1$

$$(4) \text{ (a) بين أن } a^p \equiv a[p] \quad (\forall a \in \mathbb{Z})$$

(b) بين أن $a^{p-1} \equiv 1[p]$ لكل a من $\mathbb{Z}$ بحيث $a \wedge p = 1$

(1) لنبين أن p/C_p^k لكل $1 \leq k \leq p-1$

ليكن $1 \leq k \leq p-1$. لنبين أن p/C_p^k

لدينا:

$$C_p^k = \frac{p!}{k!(p-k)!} = \frac{1.2 \dots (p-k)(p-k+1) \dots p}{k!(1.2 \dots (p-k))}$$

$$= \frac{(p-k+1) \dots p}{k!}$$

$$\text{إذن } k!C_p^k = (p-k+1) \dots p$$

$$\text{إذن } p/k!C_p^k$$

$$\forall i \in \{1, 2, \dots, k\} \quad 1 \leq i < p \quad \text{ولدينا:}$$

$$\text{إذن } p \times i$$

$$\text{إذن } p \wedge i = 1$$

إذن $p \wedge k! = 1$ حسب Gauss:

$$\text{لدينا } p/C_p^k \quad (\forall 1 \leq k \leq p-1)$$

$$(2) \text{ ليكن } a \in \mathbb{N} \text{ لنبين أن: } (a+1)^p \equiv a^p + 1[p]$$

لدينا:

$$(a+1)^p - (a^p + 1) = \sum_{k=0}^p a^k \cdot 1^{p-k} - (a^p + 1)$$

$$= \sum_{k=0}^p C_p^k a^k - (a^p + 1)$$

$$= 1 + a^p + \sum_{k=1}^{p-1} C_p^k a^k - (a^p + 1)$$

$$= \sum_{k=1}^{p-1} C_p^k a^k$$

$$\text{ولدينا } p/C_p^k \quad 1 \leq k \leq p-1$$

$$\text{إذن } p/C_p^k a^k$$

$$\text{إذن } p / \sum_{k=1}^{p-1} C_p^k a^k$$

$$\text{يعني: } p / ((a+1)^p - (a^p + 1))$$

$$\text{بالتالي: } (a+1)^p \equiv a^p + 1[p]$$

$$(3) \text{ (a) ليكن } n \in \mathbb{N} \text{ لنبين أن } n^p \equiv n[p]$$

نعلم أن:

$$\text{ليكن } n \in \mathbb{N}^* \quad (a+1)^p \equiv a^p + 1[p] \quad (\forall a \in \mathbb{N})$$

$$\text{إذن } 1^p \equiv 1[p]$$

$$2^p \equiv 1^p + 1[p]$$

$$3^p \equiv 2^p + 1[p]$$

$$n^p \equiv (n-1)^p + 1[p]$$

بجمع أطراف المتساويات طرف طرف نستنتج أن:

$$n^p \equiv 1 + 1 + \dots + 1[p]$$

n مرة

$$\text{يعني: } n^p \equiv n[p]$$

ونلاحظ أن الخاصية تبقى صحيحة من أجل $n=0$

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

(b) ليكن $n \in \mathbb{N}$ بحيث $n \wedge p = 1$. لنبين أن: $n^{p-1} \equiv 1[p]$

$$\text{لدينا مما سبق: } n^p \equiv n[p]$$

$$\text{يعني } p/n^{p-1} - n$$

$$\text{يعني } p/n(n^{p-1} - 1)$$

$$\text{وبما أن } n \wedge p = 1$$

$$\text{فإن } p/n^{p-1} - 1$$

$$\text{يعني } n^{p-1} \equiv 1[p] \text{ لكل } n \text{ بحيث } n \wedge p = 1$$

$$(4) \text{ (a) ليكن } a \in \mathbb{Z} \text{ لنبين أن } a^p \equiv a[p]$$

← إذا كان $a \geq 0$

$$\text{فإنه من خلال ما سبق: } a^p \equiv a[p]$$

← إذا كان $a \leq -1$

$$\text{فإن } -a \geq 1 \quad \text{إذن } (-a)^p \equiv -a[p]$$

- إذا كان $p \neq 2$ فإن p فردي.

$$\text{إذن: } (-a)^p = -a^p$$

$$\text{إذن } -a^p \equiv -a[p]$$

$$\text{إذن } a^p \equiv a[p]$$

$$- \text{ إذا كان } p = 2 \quad \text{فإن: } (-a)^2 \equiv -a[2]$$

$$\text{يعني: } a^2 \equiv -a[2]$$

$$\text{ولدينا } -a \equiv a[2]$$

$$\text{إذن } a^2 \equiv a[2]$$

إذن:

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

(b) ليكن $a \in \mathbb{Z}$ بحيث $a \wedge p = 1$. لنبين أن $a^{p-1} \equiv 1[p]$

$$\text{لدينا: } a^p \equiv a[p]$$

$$\text{يعني } p/a^{p-1} - a$$

$$\text{أي } p/a^{p-1} - 1$$

$$\text{وبما أن } a \wedge p = 1 \quad \text{فإن } p/a^{p-1} - 1$$

$$\text{إذن } a^{p-1} \equiv 1[p]$$

مبرهنة Fermat:

ليكن p أولي موجب.

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

$$a \wedge p = 1 / \mathbb{Z} \quad \text{لكل } a \quad a^{p-1} \equiv 1[p] \quad (*)$$

(5) تفكيك عدد إلى عداد عوامل أولية:

(a) مبرهنة:

كل عدد a من $\mathbb{Z}^* - \{-1, 1\}$ يكتب بطريقة وحيدة على شكل

$$a = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

حيث:

(*) الأعداد p_i أولية موجبة ومختلفة مثلي مثلي.

(*) الأعداد α_i طبيعية غير منعدمة.

(*) $\varepsilon = 1$ إذا كان $a > 0$

(*) $\varepsilon = -1$ إذا كان $a < 0$

(b) تطبيقات:

← قابلية القسمة:

خاصية:

ليكن b من $\mathbb{N}^* - \{1\}$

ليكن: $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ تفكيك a إلى جداد عوامل أولية.

b/a إذا وفقط إذا كان b يكتب على شكل:

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

حيث: $\beta_i \in \{0, 1, 2, \dots, \alpha_i\} = E_i$

كل ترتيبية $(\beta_1, \beta_2, \dots, \beta_r)$ من $E_1 \times E_2 \times \dots \times E_r$ تعطينا قاسم

موجب ل a هو: $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$

إن عدد القواسم الموجبة ل a هو عدد الترتيبات $(\beta_1, \beta_2, \dots, \beta_r)$

ونعلم أن عدد هذه الترتيبات هو: $\text{card}(E_1 \times E_2 \times \dots \times E_r)$

$$= (\text{card} E_1)(\text{card} E_2) \times \dots (\text{card} E_r)$$

$$= (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_r)$$

خاصية:

ليكن a من $\mathbb{N}^* - \{1\}$ و $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ تفكيك a إلى جداد

عوامل أولية.

$$\alpha = \prod_{i=1}^r (1 + \alpha_i) \quad \text{هو: عدد القواسم الموجبة ل } a$$

مثال:

لنحدد القواسم الموجبة للعدد 54:

لنفكك 54:

54	2
27	3
9	3
3	3
1	

$$\text{إن } 54 = 2 \times 3^3$$

— عدد القواسم الموجبة ل 54 هو:

$$\alpha = (1+1)(1+3) = 8$$

وهذه القواسم هي الأعداد التي تكتب على شكل:

$$\beta_1 \in \{0, 1\} \quad \text{حيث } d = 2^{\beta_1} \cdot 3^{\beta_2}$$

$$\beta_2 \in \{0, 1, 2, 3\} \quad \text{و}$$

إن هذه القواسم هي:

$$2^0 \cdot 3^0 = 1 \quad ; \quad 2^0 \cdot 3^1 = 3 \quad ; \quad 2^0 \cdot 3^2 = 9$$

$$2^0 \cdot 3^3 = 27 \quad ; \quad 2^1 \cdot 3^0 = 2 \quad ; \quad 2^1 \cdot 3^1 = 6$$

$$2^1 \cdot 3^2 = 18 \quad ; \quad 2^1 \cdot 3^3 = 54.$$

← القاسم المشترك الأكبر والمضاعف المشترك الأصغر:

ليكن $p_1, \dots, p_r$ الأعداد الأولية التي تظهر في تفكيك b و

نضع: $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$ حيث $0 \leq \alpha_i$

$$\text{و } b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_r^{\beta_r} \quad \text{و } 0 \leq \beta_i$$

حيث $0 = \alpha_i$ إذا كان p_i لا يظهر في تفكيك a .

و $0 = \beta_i$ إذا كان p_i لا يظهر في تفكيك b .

نضع $d = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \dots p_r^{\gamma_r}$ حيث: $\gamma_i = \inf(\alpha_i, \beta_i)$

$$\text{لنبين أن } d = a \wedge b$$

$$* \text{ لدينا: } \forall i \in \{1, 2, \dots, r\} \quad \gamma_i \leq \alpha_i$$

$$\text{و } \gamma_i \leq \beta_i$$

$$\text{إذن } \begin{cases} d/a \\ d/b \end{cases} \text{ إذن لا قاسم مشترك ل } b \text{ و } a$$

* ليكن d' قاسم مشترك ل b و a . لنبين أن $d' \leq d$

$$\text{لدينا: } \begin{cases} d'/a \\ d'/b \end{cases} \text{ إذن } d' \text{ يكتب على شكل: } d' = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \dots p_r^{\lambda_r}$$

$$\text{حيث } 0 \leq \lambda_i \leq \alpha_i$$

$$0 \leq \lambda_i \leq \beta_i$$

$$\text{إذن } 0 \leq \lambda_i \leq \inf(\alpha_i, \beta_i)$$

$$\text{إذن } 0 \leq \lambda_i \leq \gamma_i$$

$$\text{إذن } d'/d$$

$$\text{إذن } d = a \wedge b$$

← بنفس الطريقة نجد المضاعف المشترك الأصغر.

خاصية:

ليكن a و b من $\mathbb{N}^* - \{1\}$

$$\text{نضع } a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

$$\text{و } b = p_1^{\beta_1} \cdot p_2^{\beta_2} \dots p_r^{\beta_r}$$

حيث p_i هي الأعداد الأولية التي تظهر في تفكيك a أو b

$\alpha_i = 0$ إذا كان p_i لا يظهر في تفكيك a

$\beta_i = 0$ إذا كان p_i لا يظهر في تفكيك b

$$\text{لدينا: } a \wedge b = \prod_{i=1}^r p_i^{\inf(\alpha_i, \beta_i)}$$

$$\text{و } a \vee b = \prod_{i=1}^r p_i^{\sup(\alpha_i, \beta_i)}$$

ملاحظة:

(*) القاسم المشترك الأكبر ل b و a هو جداء العوامل الأولية المشتركة مرفوعة إلى أصغر أس.

(*) $a \vee b$ هو جداء العوامل الأولية المشتركة وغير المشتركة مرفوعة إلى أكبر أس.

مثال:

لنحدد: $76 \vee 632$ و $76 \wedge 632$

76	2	632	2
38	2	316	2
19	19	158	2
1		79	79
		1	

$$\text{إذن } 76 = 2^2 \cdot 19$$

$$\text{إذن } 632 = 2^3 \cdot 79$$

$$76 \wedge 632 = 2^2 = 4$$

لدينا:

$$0 \leq r_1 < b \quad q_0 = bq_1 + r_1$$

(*) إذا كان $q_1 \neq 0$: نقسم q_1 على b :

$$0 \leq r_2 < b \quad q_1 = bq_2 + r_2$$

وهكذا نتابع القسمة حتى نحصل على خارج منعدم.
ومن الضروري أن نحصل على خارج منعدم، لأن:

$$1 < b \Rightarrow q_0 < q_0 b < q_0 b + r_0 = n \quad \text{لدينا:}$$

$$q_0 < n \quad \text{إذن}$$

$$1 < b \Rightarrow q_1 < q_1 b < q_1 b + r_1 = q_0 \quad \text{إذن}$$

$$q_1 < q_0$$

إذن $0 < q_2 < q_1 < q_0 < n$
هذه الخوارج تناقصية قطعاً. وبالتالي ضروري أن نحصل على خارج منعدم.
- نفترض أن q_p هو أول خارج منعدم.

يعني: $\forall i \in \{0, \dots, (p-1)\} \quad q_i \neq 0$

$$0 \leq r_0 < b \quad n = q_0 b + r_0 \quad (b^0)$$

$$0 \leq r_1 < b \quad q_0 = q_1 b + r_1 \quad (b^1)$$

$$0 \leq r_2 < b \quad q_1 = q_2 b + r_2 \quad (b^2)$$

$$q_{p-1} = b \cdot q_p + r_p \quad (b^p)$$

بضرب الأسطر في $b^0, b^1, b^2, \dots, b^p$ على التوالي نحصل على
وبجمع أطراف المتساويات نحصل على:

$$n = r_0 + r_1 b + r_2 b^2 + \dots + r_p b^p + \underbrace{q_p b^{p+1}}_{=0} \quad (q_p = 0)$$

$$n = r_p b^p + r_{p-1} b^{p-1} + \dots + r_1 b + r_0 \quad \text{إذن:}$$

$$0 \leq r_i < b \quad \text{حيث}$$

$$r_p = q_{p-1} b \neq 0 \quad \text{و}$$

$$n = r_p r_{p-1} \dots r_0 \quad \text{إذن}$$

خاصية:

$$b \in \mathbb{N}^* - \{1\} \text{ و } b \in \mathbb{N}^* \text{ يمكن}$$

نقوم بالقسمة المتتالية للخوارج على b بدءاً من n .
وإذا كانت $r_0, r_1, \dots, r_p$ هي بواقي هذه القسمة حيث r_p هو باقي

أول قسمة نحصل فيها على خارج منعدم

$$n = r_p r_{p-1} \dots r_0 \quad \text{فإن:}$$

ونلخص هذه القسمة في الجدول التالي:

$$\begin{array}{r} n \mid b \\ \hline q_0 \mid b \\ \hline q_1 \mid b \\ \hline q_2 \mid b \\ \hline \vdots \\ \hline 0 = q_p \end{array}$$

مثال:

$$n = 798 \quad \text{نعتبر العدد}$$

لنمثل n في أنظمة العد ذات الأساس 7.

$$\begin{array}{r} 798 \mid 7 \\ \hline 114 \mid 7 \\ \hline 16 \mid 7 \\ \hline 2 \mid 7 \\ \hline 0 \end{array}$$

$$76 \vee 632 = 2^3 \cdot 19 \cdot 79 = 12008$$

(VII) نظمات العد:

1- أمثلة:

مثال 1: نعتبر العدد $n = 526$

$$n = 526 = 500 + 20 + 6$$

$$= 510^2 + 210^1 + 6$$

(*) لدينا:

إذن العدد n يكتب باستعمال العشرة أرقام 0, 1, 2, ..., 9 وقوى 10.

نقول إن الكتابة $n = 256$ تمثيل عشري للعدد n أو تمثيل n في
نظمة العد العشري، أو تمثيل العدد n في نظمة العد ذات الأساس 10.

(*) ويمكن كتابة n باستعمال 3 أرقام فقط 0, 1, 2 وقوى 3:

$$n = 526 = 486 + 40$$

$$= 2 \cdot 3^5 + 27 + 13$$

$$= 2 \cdot 3^5 + 3^3 + 9 + 4$$

$$= 2 \cdot 3^5 + 3^3 + 3^2 + 3 + 1$$

$$\text{إذن } n = 2 \cdot 3^5 + 0 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3 + 1$$

$$n = 201111_{(3)} \quad \text{ونكتب:}$$

وهذه الكتابة تسمى تمثيل n في نظمة العد ذات الأساس 3.

مثال 2: نعتبر العدد $n = 200$

- لنكتب تمثيل n في نظمة العد ذات الأساس 3.

$$n = 200 = 162 + 38$$

$$= 2 \cdot 3^4 + 27 + 11$$

$$= 2 \cdot 3^4 + 3^3 + 3^2 + 2$$

$$= 2 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3 + 2$$

$$\text{إذن: } n = 21102_{(3)}$$

2- تمثيل عدد طبيعي في نظمة العد ذات الأساس b

ميرهنة:

$$\text{ليكن } b \in \mathbb{N}^* - \{1\}$$

كل عدد n من $\mathbb{N}^*$ يكتب بطريقة وحيدة على شكل:

$$n = \alpha_p b^p + \alpha_{p-1} b^{p-1} + \alpha_{p-2} b^{p-2} + \dots + \alpha_1 b^1 + \alpha_0$$

حيث:

$$\left\{ \begin{array}{l} \alpha_i \in \mathbb{N} \\ 0 \leq \alpha_i < b \end{array} \right. \quad \forall i \in \{0, 1, 2, \dots, p\} \quad \text{و } \alpha_p \neq 0$$

$$b^p \leq n < b^{p+1}$$

$$n = \alpha_p \alpha_{p-1} \dots \alpha_1 \alpha_0 \quad \text{ونكتب:}$$

وتسمى هذه الكتابة تمثيل العدد n في نظمة العد ذات الأساس 5.

ملاحظة:

هناك عدة نظمات العد أهمها:

- نظمة العد العشري وهي النظمة المتداولة.

- نظمة العد الثنائي والأرقام المستعملة هي 0, 1.

- نظمة العد ذات الأساس 8. والأرقام المستعملة هي: 0, 1, ..., 7.

- نظمة العد ذات الأساس 12. والأرقام المستعملة 0, 1, ..., 9, α, β .

3- طريقة عملية لتمثيل عدد n في نظمة عد أساسها b .

$$\text{ليكن } b \in \mathbb{N}^* - \{1\} \text{ و } n \in \mathbb{N}^*$$

$$n = bq_0 + r_0 \quad \text{مع } 0 \leq r_0 < b \quad \text{نقسم } n \text{ على } b$$

$$(*) \text{ إذا كان } q_0 \neq 0 \text{ : نقسم } q_0 \text{ على } b$$

إذن: $799 = \overline{2220}_{(7)}$

(4) تغيير الأساسية:

(*) إذا أردنا المرور من التمثيل العشري إلى نظمة عد أساسها b نتبع الخوارزمية السابقة.

(*) إذا أردنا المرور من التمثيل في نظمة عد أساسها b إلى نظمة

العد العشري، نستعمل: $n = \overline{d_p d_{p-1} \dots d_0}_{(b)}$

$$= \alpha_p b^p + \alpha_{p-1} b^{p-1} \dots + \alpha_1 b + \alpha_0$$

مثال:

$$n = \overline{3450}_{(6)} = 3.6^3 + 4.6^2 + 5.6 + 0 = 822$$

(*) إذا أردنا المرور من التمثيل في نظمة عد أساسها b إلى نظمة عد أساسها b' ، نمر من b إلى التمثيل العشري ومن التمثيل العشري إلى b' .

(5) مقارنة عددين:

خاصية:

نعتبر العددين: $x = \overline{\alpha_p \alpha_{p-1} \dots \alpha_0}_{(b)}$

$$y = \overline{\beta_q \beta_{q-1} \dots \beta_0}_{(b)}$$

إذا كان $p > q$ يعني عدد أرقام x أكبر قطعاً من عدد أرقام y .
فإن $x > y$.

خاصية 2:

نعتبر العددين:

$$x = \overline{\alpha_p \dots \alpha_0}_{(b)}$$

$$y = \overline{\beta_p \dots \beta_0}_{(b)}$$

(*) x و y لهما نفس عدد الأرقام

نفترض أن $\alpha_i \neq \beta_i, \dots, \alpha_{p-1} = \beta_{p-1}, \alpha_p = \beta_p$

– إذا كان $\alpha_i > \beta_i$ فإن $x > y$

– إذا كان $\alpha_i < \beta_i$ فإن $x < y$

(6) الجمع والضرب في نظمة عد أساسها b .

عمليتا الجمع والضرب في نظمة عد أساسها b تتم بنفس الطريقة في نظمة العد العشري.

هناك فرق فقط في الاحتفاظ، حيث عند حساب $\alpha_i \beta_i$ أو $\alpha_i + \beta_i$ إذا حصلنا على رقم $\gamma < b$ نكتب γ . وإذا حصلنا على $\gamma \geq b$ نقوم

بقسمة γ على b مع $\gamma = bq + r$ مع $0 \leq r < b$

نكتب r ونحتفظ ب q .

مثال:

$$3675_{(8)} + 2764_{(8)} = 6661_{(8)} \quad (*)$$

$$5624_{(7)} \times 56_{(7)} = 50313_{(7)} + 41356_{(7)} = 464203_{(7)} \quad (*)$$

(7) مضاعف القسمة على 2, 3, 4, 5, 9, 11, 25.

نعتبر العدد $x = \overline{\alpha_p \alpha_{p-1} \dots \alpha_0}_{(10)}$

$$x = \alpha_p 10^p + \alpha_{p-1} 10^{p-1} + \dots + \alpha_1 10 + \alpha_0$$

لدينا:

$$2/x \Leftrightarrow 2/\alpha_0$$

(*) لنبين أن: $10 \equiv 0[2]$ إذن $\forall i \in \{1, \dots, p\} \quad 10^i \equiv 0[2]$

$$\alpha_i 10^i \equiv 0[2] \quad \text{يعني}$$

$$\sum_{i=1}^p \alpha_i 10^i \equiv 0[2]$$

إذن:

$$\sum_{i=1}^p -\alpha_i 10^i + \alpha_0 \equiv \alpha_0 [2] \quad \text{يعني:}$$

$$x \equiv \alpha_0 [2] \quad \text{يعني:}$$

إذن:

$$2/x \Leftrightarrow x \equiv 0[2]$$

$$\Leftrightarrow \alpha_0 \equiv 0[2] \quad (x \equiv \alpha_0 [2])$$

$$\Leftrightarrow 2/\alpha_0$$

$$2/x \Leftrightarrow 2/\alpha_0$$

وبالتالي:

(*) لنبين أن:

$$3/x \Leftrightarrow 3/\sum_{i=0}^p \alpha_i$$

لدينا $10 \equiv 1[3]$

$$\forall i \in \{1, 2, \dots, p\} \quad 10^i \equiv 1[3] \quad \text{إذن}$$

$$\alpha_i 10^i \equiv \alpha_i [3] \quad \text{يعني}$$

إذن:

$$\sum_{i=1}^p \alpha_i 10^i \equiv \sum_{i=1}^p \alpha_i [3]$$

$$\sum_{i=1}^p \alpha_i 10^i + \alpha_0 \equiv \sum_{i=1}^p \alpha_i [3]$$

إذن:

$$x \equiv \sum_{i=0}^p \alpha_i [3]$$

أي:

إذن:

$$3/x \Leftrightarrow x \equiv 0[3]$$

$$\Leftrightarrow \sum_{i=0}^p \alpha_i \equiv 0[3] \quad \left(x \equiv \sum_{i=0}^p \alpha_i [3] \right)$$

$$\Leftrightarrow 3/\sum_{i=0}^p \alpha_i$$

$$3/x \Leftrightarrow 3/\sum_{i=0}^p \alpha_i$$

وبالتالي:

$$4/x \Leftrightarrow 4/\overline{\alpha_1 \alpha_0}$$

$$\forall i \in \{2, \dots, p\} : 10^i = 10^2 \cdot 10^{i-2}$$

$$= 100 \cdot 10^{i-2}$$

$$= 4.25 \cdot 10^{i-2}$$

$$\forall i \in \{2, \dots, p\} \quad 10^2 \equiv 0[4] \quad \text{إذن}$$

$$\alpha_i 10^i \equiv 0[4] \quad \text{إذن}$$

$$\sum_{i=2}^p \alpha_i \cdot 10^i \equiv 0[4]$$

إذن:

إذن:

$$\sum_{i=2}^p \alpha_i 10^2 + \alpha_1 10 + \alpha_0 \equiv \alpha_1 10 + \alpha_0 [4]$$

$$x \equiv \alpha_1 \cdot 10 + \alpha_0 [4] \quad \text{يعني:}$$

$$x \equiv \overline{\alpha_1 \alpha_0} [4] \quad \text{يعني}$$

$$4/x \Leftrightarrow x \equiv 0[4] \quad \text{إذن:}$$

$$\Leftrightarrow \overline{\alpha_1 \alpha_0} \equiv 0[4] \quad (x \equiv \overline{\alpha_1 \alpha_0} [4])$$

$$\Leftrightarrow 4/\overline{\alpha_1 \alpha_0}$$

$$4/x \Leftrightarrow 4/\overline{\alpha_1 \alpha_0}$$

وبالتالي:

وبالتعويض في (1) نحصل على:

$$5(265a + 2c) = 271.5$$

$$265a + 2c = 271 \quad \text{يعني}$$

$$2c = 271 - 265a \quad \text{يعني (*)}$$

ولدينا $2c > 0$ إذن $271 - 265a > 0$

$$0 < a < \frac{271}{265} = 1 \quad \text{يعني:}$$

إذن: $a = 1$

وبالتعويض في (*) نجد: $c = 3$

بالتالي:

$$\begin{cases} a = 1 \\ b = 5 \\ c = 3 \end{cases}$$

- لنبين أن: $11/x \Leftrightarrow \alpha_0 + \alpha_1 + \dots \equiv \alpha_1 + \alpha_3 + \dots [11]$

لدينا: $\forall i \in \{1, \dots, p\} \quad 10 \equiv -1 [11]$

إذن $10^i \equiv (-1)^i [11]$

إذن $\alpha_i 10^i \equiv \alpha_i (-1)^i [11]$

إذن: $\sum_{i=1}^p \alpha_i 10^i \equiv \sum_{i=1}^p \alpha_i (-1)^i [11]$

أي: $\sum_{i=1}^p \alpha_i 10^i + \alpha_0 \equiv \sum_{i=1}^p \alpha_i (-1)^i + \alpha_0 [11]$

يعني: $x \equiv \sum_{i=1}^p \alpha_i (-1)^i [11]$

يعني: $x \equiv \sum_{i=0}^p \alpha_i (-1)^i + \sum_{i=0}^p \alpha_i (-1)^i [11]$

$$x \equiv \sum_{i=0}^p \alpha_i - \sum_{i=0}^p \alpha_i [11]$$

إذن: $11/x \Leftrightarrow x \equiv 0 [11]$

$$\Leftrightarrow \sum_{i=0}^p \alpha_i - \sum_{i=0}^p \alpha_i \equiv 0 [11]$$

$$\Leftrightarrow \sum_{i=0}^p \alpha_i \equiv \sum_{i=0}^p \alpha_i [11]$$

بالتالي: $11/x \Leftrightarrow \alpha_0 + \alpha_2 + \dots = \alpha_1 + \alpha_3 + \dots [11]$

خاصية:

نعتبر العدد $x = \overline{\alpha_p \alpha_{p-1} \dots \alpha_0}_{(10)}$

لدينا: $2/x \Leftrightarrow \overline{\alpha_0}_{(2)}$

$3/x \Leftrightarrow 3 \overline{\sum_{i=0}^p \alpha_i}$

$4/x \Leftrightarrow 4 \overline{\alpha_1 \alpha_0}$

$5/x \Leftrightarrow \alpha_0 \in \{0, 5\}$

$9/x \Leftrightarrow 9 \overline{\sum_{i=0}^p \alpha_i}$

$11/x \Leftrightarrow \alpha_0 + \alpha_2 + \alpha_4 + \dots \equiv \alpha_1 + \alpha_3 + \alpha_5 + \dots [11]$

$25/x \Leftrightarrow \overline{\alpha_1 \alpha_0} \in \{\overline{00}, \overline{25}, \overline{50}, \overline{75}\}$

تمرين تطبيقي:

حدد الأعداد الطبيعية غير المنعدمة c, b, a بحيث:

$$\overline{bbac}_{(7)} = \overline{abca}_{(11)}$$

نلاحظ أن c, b, a أصغر قطعا من 11 و 7.

وبالتالي فهي محصورة قطعا بين 0 و 7.

وبالتالي فهي محصورة بين 1 و 6.

لدينا:

$$\begin{aligned} \overline{bbac}_{(7)} = \overline{abca}_{(11)} &\Leftrightarrow b7^3 + b7^2 + a7 + c = a11^3 + b11^2 + c11 + a \\ &\Leftrightarrow 343b + 49b + 7a + c = 1331a + 121b + 11c + a \\ &\Leftrightarrow 1325a - 271b + 10c = 0 \\ &\Leftrightarrow 1325a + 10c = 271b \\ &\Leftrightarrow 5(265a + 2c) = 271b \quad (1) \end{aligned}$$

إذن $5/271b$

ولدينا: $271 \wedge 5 = 1$ إذن حسب Gauss نستنتج أن $5/b$

وبما أن $1 \leq b \leq 6$ فإن $b = 5$