

**I. قابلية 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 : $a | b$. ومنه : $a | b \Leftrightarrow \exists q \in \mathbb{Z}, b = qa$
في هذه الحالة : نقول إن العدد a قاسم للعدد b ؛ أما العدد b يسمى مضاعف ل a .

2. ملحوظة و أمثلة :

a. 1 و -1 يقسمان جميع الأعداد الصحيحة النسبية . جميع الأعداد النسبية تقسم 0 . a يقسم a وكذلك يقسم $-a$ (مع a من \mathbb{Z})
مثال : $23 | -23$ و $1 | 52$ و $-1 | 52$ و $15 | 0$ و $-7 | 7$ و $7 | -7$.

b. كل عدد نسبي a فهو قابل القسمة على 1 و -1 و a و $-a$.

أما القواسم ل a التي تخالف 1 و -1 و a و $-a$ فتسمى القواسم الفعلية a (**diviseur stricte de b**) .
مثال : قواسم ل 15 هي : 1 و 3 و 5 و 15 و -1 و -3 و -5 و -15 . إذن القواسم الفعلية ل 15 هي : 3 و 5 و 15 و -3 و -5 و -15 .

c. مجموعة قواسم b في \mathbb{Z} هي $D_b = \{d \in \mathbb{Z} / \exists q \in \mathbb{Z}, b = dq\}$ ويرمز لها ب: D_b .

مثال : مجموعة قواسم 15 هي : $D_{15} = \{-15, -5, -3, -1, 1, 3, 5, 15\}$

d. مجموعة مضاعفات a هي: $\{\dots, -qa, \dots, -2a, -a, 0, a, 2a, \dots, qa, \dots\}$ ويرمز لها: $a\mathbb{Z}$.

مثال : مجموعة مضاعفات 6 هي: $6\mathbb{Z} = \{\dots, -18, -12, -6, 0, 6, 12, 18, \dots\}$

e. كل عدد d قاسم ل a و b من \mathbb{Z} فهو يسمى قاسم مشترك ل a و b إذن $d \in D_a \cap D_b$

f. كل عدد m هو مضاعف ل a و b من \mathbb{Z} فهو يسمى مضاعف مشترك ل a و b إذن $m \in a\mathbb{Z} \cap b\mathbb{Z}$.

B. خاصيات قابلية القسمة:**1. خاصية**

ليكن a و b و c و d من \mathbb{Z} .

a. الانعكاسية : $a | a$. (a يقسم a) .

b. $a | b \Rightarrow a | cb ; (c \in \mathbb{Z})$

c. التعددي : $(a | b \text{ و } b | c) \Rightarrow a | c$

d. $(a | b \text{ و } b | a) \Rightarrow |a| = |b|$

e. (α, β) من \mathbb{Z}^2 : $a | b$ و $a | c \Rightarrow a | (\alpha b + \beta c)$. ($\alpha b + \beta c$ تسمى تاليفة خطية ل b و c) .

f. الجداء : $\left. \begin{matrix} a | b \\ c | d \end{matrix} \right\} \Rightarrow ac | bd$. ومنه نستنتج : $a | b \Rightarrow a^n | b^n$ مع $n \in \mathbb{N}^*$ (يمكن أن نأخذ $n \in \mathbb{N}$ مع a و b من \mathbb{Z}^*)

g. $(a | b \text{ و } b \neq 0) \Rightarrow |a| \leq |b|$

2. برهان 1 : (لمعرفة البرهان اضغط هنا) \Rightarrow \square **3. أمثلة :**

مثال 1 :

لنعتبر a و b من \mathbb{Z} .

أ. بين أن : إذا كان $7 | (2x + 3y)$ فإن $7 | (5x + 4y)$.

ب. بين أن : إذا كان $7 | (5x + 4y)$ فإن $7 | (2x + 3y)$.

جواب:



أ. لدينا : $7 | 7(x+2y)$ و $7 | (2x+3y)$ إذن : $7 | [6(2x+3y) - 7(x+2y)]$ (تأليفة خطية)

أي : $7 | (5x+4y)$

خلاصة : إذا كان $7 | (2x+3y)$ فإن $7 | (5x+4y)$.

ب. لدينا : $7 | (5x+4y)$ و $7 | 7(4x+3y)$ إذن : $7 | [6(5x+4y) - 7(4x+3y)]$ (تأليفة خطية)

مثال 2 :

لنعتبر n من \mathbb{N}^* .

ما هي قيم n حيث : $n^2 + 1$ يقسم $n + 1$.

لكي يكون : $(n^2 + 1) | (n + 1)$ يجب أن يكون $(n + 1) \leq (n^2 + 1)$ وهذا يتحقق فقط ل $n = 1$. ونتحقق من بعد ذلك $n = 1$ يكون

حل .

مثال 3 :

لنعتبر n من \mathbb{Z} . ما هي قيم n حيث : $n + 2$ يقسم $5n^3 - n$.
لدينا :

$$5n^3 - n = 5n^3 + 40 - 40 - n$$

$$= 5(n^3 + 8) - 2 - n - 38$$

$$= 5(n + 2)(n^2 - 2n + 4) - (n + 2) - 38$$

$$= (n + 2)[5n^2 - 10n + 19] - 38$$

إذا كان $n + 2$ يقسم $5n^3 - n$ إذن $n + 2$ يقسم $38 - (5n^3 - n) = (n + 2)[5n^2 - 10n + 19] - 38$ ومنه $n + 2$ يقسم 38 .

$$\text{ومنّه : } n + 2 \in D_{38} = \{-38; -19; -2; -1; 1; 2; 19; 38\}$$

$$\text{و بالتالي : } n \in \{-40; -21; -4; -3; -1; 0; 17; 36\}$$

خلاصة : مجموعة قيم n هي $\{-40; -21; -4; -3; -1; 0; 17; 36\}$

II. القسمة الإقليدية - la division Euclidienne.

A. القسمة الإقليدية في \mathbb{Z} .

1. خاصية :

ليكن (a, b) من \mathbb{Z}^2 حيث $a \neq 0$.

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

2. برهان : (لمعرفة البرهان اضغط هنا) \square

3. 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 .

الباقي r في القسمة في \mathbb{N} أو في \mathbb{Z} هو عدد موجب ($r \geq 0$).

4. أمثلة :

حدد q و r حيث : أ- $-58 = 13q + r$. ب- $58 = -13q + r$. ج- $-58 = -13q + r$ مع $0 \leq r < 13$

بالنسبة ل : $58 = 13q + r$ لدينا : $58 = 4 \times 13 + 6$ إذن : $q = 4$ و $r = 6$.



بالنسبة ل : $58 = -13q + r$ لدينا : $58 = -13 \times (-4) + 6$ إذن : $q = -4$ و $r = 6$.

بالنسبة ل : $-58 = -13q + r$ لدينا : $-58 = -13 \times 5 + 7$ إذن : $q = 5$ و $r = 7$.

III. الأعداد الأولية - les nombres premiers

A. 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:

الأعداد الأولية الأصغر من 160 هي: $2 - 3 - 5 - 7 - 11 - 13 - 17 - 19 - 23 - 29 - 31 - 37 - 41 - 43 - 47 - 53 - 59 - 61 - 67 - 71 - 73 - 79 - 83 - 89 - 97 - 101 - 103 - 107 - 109 - 113 - 127 - 131 - 137 - 139 - 149 - 151 - 157$.

B. 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 $1 < d \leq \sqrt{a}$. (أي $2 \leq d \leq \sqrt{a}$)

4. برهان 3 : (لمعرفة البرهان اضغط هنا \Rightarrow \square)

C. طريقة لتحديد 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 $2 \leq p \leq \sqrt{a}$.
- إذا كانت جميع الأعداد الأولية p (مع $2 \leq p \leq \sqrt{a}$) لا تقسم a فإن العدد a أولي .
- إذا كان عدد أولي p من بين هذه الأعداد (مع $2 \leq p \leq \sqrt{a}$) يقسم a فإن العدد a غير أولي .

2. أمثلة:

مثال 1:

$a = 109$ لدينا: $\sqrt{a} < 11$ و منه الأعداد الأولية p حيث $2 \leq p \leq \sqrt{109} < 11$ 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 $2 \leq p \leq \sqrt{173} < 14$ هي: 2 و 3 و 5 و 7 و 11 و 13 فهي لا تقسم 173 إذن

173 عدد أولي.

D. مجموعة الأعداد الأولية غير منتهية:

1. خاصية :

مجموعة الأعداد الأولية غير منتهية.



2 برهان 4: (لمعرفة البرهان اضغط هنا) \Rightarrow (X)

E. التفكير إلى جداء من 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 $1 < p_1 < p_2 < \dots < p_n$
- توجد أعداد وحيدة α_1 و α_2 و α_3 و 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 $\mathbb{N} \setminus \{0, 1\}$: $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$
 ب- إذا كان a من $\mathbb{Z}^- \setminus \{0, -1\}$: $a = - p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$

2 ملحوظة:

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

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

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

3 أمثلة:

مثال 1: $a = 990$ مثال 2: $b = 7^5 - 7$ مثال 3: $c = -1980$

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

$$b = 7 \times 48 \times 50$$

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

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

$$990 \quad 2$$

$$495 \quad 3$$

$$165 \quad 3$$

$$55 \quad 5$$

$$11 \quad 11$$

$$1$$

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: $c = -1980 = -2^2 \times 3^2 \times 5 \times 11$

IV. 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: $\delta = \text{pgcd}(a, b)$ أو ب: $\delta = a \wedge b$



2. ملحوظة:

• $a \wedge 1 = 1$ و $a \wedge 0 = |a|$ و $a \wedge (ka) = |a|$ مع $k \in \mathbb{Z}$ و $(a \wedge b) | a$ و $(a \wedge b) | b$ أي $(a \wedge b) | \delta$ و $\delta | b$.

3. خاصيات:

ليكن $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ حيث $a \wedge b = \delta$. لدينا: $a \wedge b \geq 1$ و $\frac{a}{\delta} \wedge \frac{b}{\delta} = 1$.

$$1. (a \wedge b) \wedge c = a \wedge (b \wedge c) \text{ و } a \wedge b = b \wedge a$$

$$2. a/b \Leftrightarrow a \wedge b = |a|$$

3. 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 .

4. إذا كان k يقسم a و b فإن: $\text{pgcd}\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{1}{|k|} \text{pgcd}(a, b)$ و $\text{pgcd}(ka, kb) = |k| \text{pgcd}(a, b)$.

4. برهان 5: (لمعرفة البرهان اضغط هنا \Rightarrow \boxtimes)3. ملحوظة: يمكن تحديد $\text{pgcd}(a, b)$ بثلاثة طرائق:

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

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

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

1. تمهيدة إقليدس Lemme d'Euclide

ليكن $b = aq + r$ القسمة الإقليدية 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: $a \wedge b = \delta$ و $a \wedge r = d$.

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 δ يقسم تأليفة ل a و b . ومنه $\delta | (b - qa)$ 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 أقليدس: Algorithme d'Euclide

1. القسمة المتتالية:

نريد: حساب $\text{pgcd}(a, b)$ 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 أقليدس نحصل على $\text{pgcd}(a, b) = \text{pgcd}(a, r_1)$.

• إذا كان $r_1 = 0$ إذن $\text{pgcd}(a, b) = \text{pgcd}(a, r_1) = \text{pgcd}(a, 0) = a$. إذا كان $r_1 \neq 0$ نواصل.

• $a = r_1q_2 + r_2$ و $r_2 = 0$ إذن $\text{pgcd}(a, b) = \text{pgcd}(a, r_1) = \text{pgcd}(r_1, r_2) = r_1$. إذا كان $r_2 \neq 0$ نواصل.

• $r_1 = r_2q_3 + r_3$ و $r_3 = 0$ إذن $\text{pgcd}(a, b) = \text{pgcd}(a, r_1) = \text{pgcd}(r_1, r_2) = \text{pgcd}(r_2, r_3) = r_3$. إذا كان $r_3 \neq 0$ نواصل.

•

• $r_{k-2} = r_{k-1}q_k + r_k$ و $r_k = 0$ إذن $\text{pgcd}(a, b) = \text{pgcd}(a, r_1) = \text{pgcd}(r_1, r_2) = \dots = \text{pgcd}(r_{k-1}, r_k) = r_{k-1}$. إذا كان



$r_k \neq 0$ نواصل.

• $\text{pgcd}(a, b) = \text{pgcd}(a, r_1) = \text{pgcd}(r_1, r_2) = \dots = \text{pgcd}(r_k, 0) = r_k$ إذن $r_{k-1} = r_k q_k + 0$

لدينا: في كل مرحلة الباقي أصغر من الخارج ونعلم أن $0 \leq r_{i+1} < r_i$ إذن القسمة المتتالية تتوقف عند باقي سيكون 0 مع

$$a > r_1 > r_2 > \dots > r_k \geq 0$$

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 القسمة المتتالية ل b على a .

3 أمثلة: مثال 1: من خلال القسمة المتتالية ل b على a . استنتج: $3451 \wedge 275$. نأخذ: $a = 275$ و $b = 3451$. لدينا:

تسمى القسمة المتتالية ل a على b .	$r_1 = 151$: الباقي هو : $3451 = 275 \times 12 + 151$: إذن: القسمة 1
	$r_2 = 124$: الباقي هو : $275 = 151 \times 1 + 124$: إذن: القسمة 2
	$r_3 = 27$: الباقي هو : $151 = 124 \times 1 + 27$: إذن: القسمة 3
	$r_4 = 16$: الباقي هو : $124 = 27 \times 4 + 16$: إذن: القسمة 4
	$r_5 = 11$: الباقي هو : $27 = 16 \times 1 + 11$: إذن: القسمة 5
	$r_6 = 5$: الباقي هو : $16 = 11 \times 1 + 5$: إذن: القسمة 6
	$r_7 = 1$: الباقي هو : $11 = 5 \times 2 + 1$: إذن: القسمة 7
	$r_8 = 0$: الباقي هو : $5 = 1 \times 5 + 0$: إذن: القسمة 8

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

خلاصة: $a \wedge b = 3451 \wedge 275 = 1$

مثال 2: طريقة تطبيق خوارزمية أقليدس لحساب $\text{pgcd}(a, b)$ مع: $a = 226$ و $b = 109$ (109 عدد أولي).

$$226 = \boxed{109} \times 2 + \boxed{8} \quad (r_1 = 8)$$

$$\swarrow \quad \searrow$$

$$\boxed{109} = \boxed{8} \times 13 + \boxed{5} \quad (r_2 = 5)$$

$$\swarrow \quad \searrow$$

$$\boxed{8} = \boxed{5} \times 1 + \boxed{3} \quad (r_3 = 3)$$

$$\swarrow \quad \searrow$$

$$\boxed{5} = \boxed{3} \times 1 + \boxed{2} \quad (r_4 = 2)$$

$$\swarrow \quad \searrow$$

$$\boxed{3} = \boxed{2} \times 1 + \boxed{1} \quad (r_5 = 1)$$

$$\swarrow \quad \searrow$$

$$\boxed{2} = \boxed{1} \times 1 + \boxed{1} \quad (r_6 = 1) \quad (\text{pgcd}(226, 109) = 1)$$

$$\swarrow \quad \searrow$$

$$\boxed{1} = \boxed{1} \times 1 + \boxed{0} \quad (r_7 = 0)$$



خلاصة : $\text{pgcd}(226,109) = 1$

مثال 3 و 4 :

مثال 4 :	مثال 3 :
نحسب : $\text{pgcd}(9945,3003)$	نحسب : $\text{pgcd}(600,124)$
$a = 3003$ و $b = 9945$	$a = 124$ و $b = 600$
$b = aq_1 + r_1$ $9945 = 3003 \times 3 + 936$	نضع : $b = aq_1 + r_1$ $600 = 124 \times 4 + 104$
$3003 = 936 \times 3 + 195$	$124 = 104 \times 1 + 20$
$936 = 195 \times 4 + 156$	$104 = 20 \times 5 + 4$
$195 = 156 \times 1 + 39$	$20 = 4 \times 5 + 0$
$156 = 39 \times 4 + 0$	
خلاصة : $\text{pgcd}(9945,3003) = 39$	خلاصة : $\text{pgcd}(600,124) = 4$

مثال 5 :

طريقة تحديد u و v (معاملتي بيزو coefficients de Bézout) حيث : $600u + 124v = 4$.

مثال		
نحسب : $\text{pgcd}(600,124)$		
$a = 124$ و $b = 600$		طريقة تحديد معاملي بيزو
نضع : $b = aq_1 + r_1$ $600 = 124 \times 4 + 104$		$4 = 124 \times (-5) + (600 - 124 \times 4) \times 6 = 600 \times 6 + 124 \times (-29)$
$124 = 104 \times 1 + 20$		$4 = 104 - (124 - 104 \times 1) \times 5 = 124 \times (-5) + 104 \times 6$
$104 = 20 \times 5 + 4$		$4 = 104 - 20 \times 5$
$20 = 4 \times 5 + 0$		
خلاصة : $\text{pgcd}(600,124) = 4$		معاملي بيزو هما $u = 6$ و $v = -29$ إذن : $6 \times 600 + (-29) \times 124 = 4$

VI. عدنان أوليان فيما بينهما : les nombres premiers entre eux

A. عدنان أوليان فيما بينهما :

1. تعريف :

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

2. مثال :

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

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

3. ملحوظة :

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

4. تمرين تطبيقي :

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

VII. المضاعف المشترك الأصغر :A. المضاعف المشترك الأصغر :1. تعريف :

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

أصغر مضاعف مشترك موجب قطعال a و b يسمى المضاعف المشترك الأصغر ل a و b ويرمز له ب: $\text{ppcm}(a,b)$ أو أيضا:

$a \vee b$. نأخذ m كقيمة ل $a \vee b$ ومنه $a \vee b = m$.

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 $a \vee b$.

لدينا : $a \vee 1 = a$.

3. مثال :

أوجد : $36 \vee (-30)$.

لدينا : $36 = 4 \times 9 = 2^2 \times 3^2$ و $30 = 6 \times 5 = 2 \times 3 \times 5$ ومنه : $36 \vee (-30) = 2^2 \times 3^2 \times 5 = 180$.

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: $(a \text{ يقسم } b) \Leftrightarrow a \vee b = |b|$.

$(a \text{ يقسم } b)$ 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. $(a \text{ يقسم } b) \Leftrightarrow a \vee b = |b|$

4. إذا كان M مضاعف مشترك غير منعدم ل a و b فإن $m \leq |M|$.

5. m يقسم ab .

VIII 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: $a \wedge p = 1 \Leftrightarrow a$ لا يقسم p .

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_1 و p_2 و و p_n أعداد أولية موجبة.

إذا كان p يقسم الجداء $p_1 \times p_2 \times p_3 \times \dots \times p_n$ فإن p يساوي أحد العوامل p_i مع $i \in \{1, 2, 3, \dots, n\}$ (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 $a = \epsilon p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_3^{\alpha_3} \times \dots \times p_n^{\alpha_n}$.
 لدينا : القواسم الموجبة ل a هي : $d = p_1^{\gamma_1} \times p_2^{\gamma_2} \times p_3^{\gamma_3} \times \dots \times p_n^{\gamma_n}$ حيث $\gamma_1 \in \{0, 1, \dots, \alpha_1\}$ و $\gamma_2 \in \{0, 1, \dots, \alpha_2\}$ و \dots و $\gamma_n \in \{0, 1, \dots, \alpha_n\}$.

2. ملحوظة:

كل جداء جزئي من هذه العوامل الأولية للتفكيك ل a فهو يقسم العدد a
 عدد القواسم الموجبة ل a هو $(\alpha_1 + 1)(\alpha_2 + 1) \times \dots \times (\alpha_n + 1)$
 عدد القواسم الموجبة و السالبة ل a هو $2 \times (\alpha_1 + 1)(\alpha_2 + 1) \times \dots \times (\alpha_n + 1)$

3. تطبيق:

نعتبر العدد $a = 60 = 2^2 \times 3 \times 5$ عدد القواسم الموجبة ل a هي $(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) = (2 + 1)(1 + 1)(1 + 1) = 12$

C. تفكيك a و b من أجل تحديد $a \wedge b$ و $a \vee b$:1. مفردات و رموز :

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

2. خاصية :

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

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

3. تطبيق: نأخذ : $a = -60 = -2^2 \times 3 \times 5$ و $b = 130 = 2 \times 5 \times 13$.

لدينا : $130 \wedge 60 = \text{P.G.D.C}(130, 60) = 2^1 \times 3^0 \times 5^1 \times 13^0 = 2 \times 5 = 10$.

$130 \vee 60 = \text{P.P.M.C}(130, 60) = 2^2 \times 3^1 \times 5^1 \times 13^1 = 4 \times 3 \times 5 \times 13 = 780$.

IX. الموافقة بترديد n La congruence modulo n :A. الموافقة بترديد n :1. تعريف :ليكن $(a, b) \in \mathbb{Z}^2$ و $n \in \mathbb{N}^*$.نقول إن : a يوافق b بترديد n لنعني أن n يقسم $b - a$. نكتب : $a \equiv b \pmod{n}$ أو أيضا $a \equiv b \pmod{n}$.2. مثال :

أتمم : باستعمال الرمز المناسب من بين : \equiv أو \neq . $[3] \ 1 \dots 5$ ؛ $[3] \ 1 \dots 4$ ؛ $[3] \ 12 \dots 6$ ؛ $[3] \ 4 \dots 5$.

B. خاصيات الموافقة بترديد n :

1. خصائص:

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

1.

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

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

2.

$$\forall a \in \mathbb{Z} : a \equiv a [n] \text{ الانعكاسية : 1}$$

$$\forall a, b \in \mathbb{Z} : a \equiv b [n] \Leftrightarrow b \equiv a [n] \text{ التماثلية : 2}$$

$$\forall a, b, c, d \in \mathbb{Z} : (a \equiv b [n] \text{ و } b \equiv c [n]) \Rightarrow a \equiv c [n] \text{ التعدية : 3}$$

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

4.

$$(c \equiv d [n] \text{ و } a \equiv b [n]) \Rightarrow a + c \equiv b + d [n] \text{ (نقول أن الموافقة منسجمة مع الجمع)}$$

$$(c \equiv d [n] \text{ و } a \equiv b [n]) \Rightarrow a \times c \equiv b \times d [n] \text{ (نقول أن الموافقة منسجمة مع الضرب)}$$

$$a \equiv b [n] \Rightarrow (\forall k \in \mathbb{N} ; a^k \equiv b^k [n]) \text{ 3}$$

2. برهان 6: (لمعرفة البرهان اضغط هنا \Rightarrow \boxtimes)

3. ملحوظة:

• علاقة الموافقة منسجمة مع الجمع و الفرق و الضرب .

• انتبه ! علاقة الموافقة غير منسجمة مع القسمة و الجذر المربع :

مثال 1: $44 \equiv 8 [6]$ و لكن لا يمكن أن نقسم ب 4 لكي نؤكد أن 11 يوافق 2 بترديد 6مثال 2: $4 \equiv 16 [12]$ و لكن لا يمكن أن نستعمل الجذر المربع لنؤكد أن 2 يوافق 4 بترديد 12 .

• لا يمكن أن نختزل في الموافقة كما نختزل في المتساويات

مثال: $2x \equiv 2y [p]$ لا يمكن أن نختزل ب 2 .

4. أمثلة:

• نحدد باقي القسمة ل 3^n على 7 .• لدينا r باقي القسمة ل x على 7 هي $r \in \{0, 1, 2, 3, 4, 5, 6\}$.• لدينا: $x \equiv r [7]$.• نعطي جدول يعطي بواقي القسمة للأعداد الأولى من 3^n على 7 .

3^n	3^0	3^1	3^2	3^3	3^4	3^5	3^6
r	1	3	2	6	4	5	1

• ومنه: لكل أس يكون مضاعف ل 6 الباقي هو 1 إذن لكل $k \in \mathbb{N}, 3^{6k} \equiv (3^6)^k \equiv 1^k \equiv 1 [7]$ • من جهة أخرى: ليكن $n \in \mathbb{N}$ نستعمل القسم الإقليدية ل n على 6 ومنه يوجد زوج وحيد (q, r) من \mathbb{N}^2 حيث $n = 6q + r$ مع

$$r \in \{1, 2, 3, 4, 5, 6\} \text{ أي } 0 \leq r < 6$$

$$\text{إذن : } [7] \quad 3^n \equiv 3^{6q+r} \equiv (3^6)^q \times 3^r \equiv 3^r$$

ومنه : الجدول التالي يعطي r باقي القسمة ل 3^n على 7 .

n	6k	6k+1	6k+2	6k+3	6k+4	6k+5	6k+6
$3^n \equiv$	3^0	3^1	3^2	3^3	3^4	3^5	3^6
r	1	3	2	6	4	5	1

• نحدد باقي القسمة ل 1515^{2015} على 7 .

$$2012 \equiv 287 \times 7 + 3 \quad [7]$$

$$\equiv 287 \times 7 + 3 \quad [7]$$

$$\equiv 3 \quad [7] ; \left(\begin{array}{l} 7 \equiv 0 \Rightarrow 287 \times 7 \equiv 287 \times 0 \quad [7] \\ 287 \times 7 \equiv 287 \times 0 \Rightarrow 287 \times 7 + 3 \equiv 287 \times 0 + 3 \quad [7] \end{array} \right)$$

لدينا : $2012 = 287 \times 7 + 3$ إذن

من جهة أخرى :

$$1512 \equiv 3 [7] \Rightarrow 1512^{2015} \equiv 3^{2015} \quad [7]$$

$$\Rightarrow 1512^{2015} \equiv 3^{335 \times 6 + 5} \quad [7]$$

$$\Rightarrow 1512^{2015} \equiv 3^{335 \times 6} \times 3^5 \quad [7]$$

$$\Rightarrow 1512^{2015} \equiv (3^6)^{335} \times 3^5 \quad [7]$$

$$\Rightarrow 1512^{2015} \equiv 1^{335} \times 3^5 \quad [7]$$

$$\Rightarrow 1512^{2015} \equiv 3^5 \quad [7]$$

$$\Rightarrow 1512^{2015} \equiv 5 \quad [7]$$

ومنه : باقي القسمة ل 1515^{2015} على 7 هو 5 .

• نحدد مجموعة الأعداد الصحيحة الطبيعية n حيث $2^n \equiv n^2 \quad [9]$.

نعطي جدول للقيم الممكنة ل 2^n و n^2 بترديد 9 .

n	0	1	2	3	4	5	6	7	8
2^n	1	2	4	8	7	5	1	2	4
n^2	0	1	4	0	7	7	0	4	1

من خلال الجدول نستنتج أن : $2^n \equiv n^2 \quad [9]$ إذا كان $n \equiv 2 \quad [9]$ أو $n \equiv 4 \quad [9]$

ومنه : قيم الأعداد الصحيحة الطبيعية n حيث $2^n \equiv n^2 \quad [9]$ هي التي على شكل $n = 9k + 2$ أو $n = 9k + 4$ مع $k \in \mathbb{N}$.

X . 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 : $a = kn + r$.

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

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 : $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}$.

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

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

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

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

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

.....
 $\bar{n-1} = \{kn + n - 1 / k \in \mathbb{Z}\} = \{k'n - 1 / k' \in \mathbb{Z}\}$

$= \{\dots, -3n - 1, -2n - 1, -n - 1, -1, n - 1, 2n - 1, 3n - 1, 3n + 1, \dots\}$

▪ المجموعة المخرجة هي:

هذه الأصناف تكون مجموعة هي : $\{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$ وتسمى المجموعة المخرجة ويرمز لها ب : $\mathbb{Z}/n\mathbb{Z}$ إذن :

$\mathbb{Z}/n\mathbb{Z} = \{\bar{x} / x \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \bar{n-1}\}$

3. أمثلة :

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

مثال 2 : $n = 2$

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

ومنه : $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$

مثال 3 : $n = 4$

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

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

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

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 :

جدول $(\mathbb{Z}/5\mathbb{Z}, \times)$						مثال n=5	جدول $(\mathbb{Z}/5\mathbb{Z}, +)$					
\overline{x}	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$		$\overline{+}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$	$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$	$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$	$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	

3. تمارين تطبيقية :1. حدد باقي القسمة الإقليدية ل 73^{2014} على 7.

$$\text{لدينا: } 73 \equiv 3 \pmod{7} \text{ إذن: } 73^{2014} \equiv 3^{2014} \pmod{7}$$

$$\text{لدينا: } 3^{2014} \equiv (3^2)^{1007} \equiv 2^{1007} \equiv (2^3)^{335} \times 2^2 \equiv 1^{335} \times 4 \equiv 4 \pmod{7}$$

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

طريقة 2:

$$73 \equiv 3 \pmod{7} \text{ و } 73^2 \equiv 3^2 \equiv 2 \pmod{7} \text{ و } 73^3 \equiv 3^3 \equiv 6 \pmod{7} \text{ و } 73^4 \equiv 3^4 \equiv 4 \pmod{7} \text{ و } 73^5 \equiv 3^4 \times 3 \equiv 4 \times 3 \equiv 5 \pmod{7}$$

$$\text{و } 73^6 \equiv 3^6 \equiv 3^3 \times 3^3 \equiv 6 \times 6 \equiv 35 \equiv 1 \pmod{7}$$

$$\text{و منه: } 2014 = 335 \times 6 + 4 \text{ وبالتالي: } 73^{2014} \equiv 73^{335 \times 6 + 4} \equiv 73^{335 \times 6} \times 73^4 \equiv (73^6)^{335} \times 73^4 \equiv 1^{335} \times 4 \equiv 4 \pmod{7}$$

خلاصة: 4 هو باقي القسمة الإقليدية ل 73^{2014} على 7.2. حدد رقم الوحدات للعدد: 24537^{2014} .

$$\text{لدينا: } 24537 \equiv 7 \pmod{10} \text{ إذن: } 24537^{2014} \equiv 7^{2014} \equiv (7^2)^{1007} \equiv 9^{1007} \equiv 9^{2 \times 503 + 1} \equiv (9^2)^{503} \times 9 \equiv 1^{503} \times 9 \equiv 9 \pmod{10}$$

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

$$\text{بين أن: } x \equiv (a - b + c - d) \pmod{11}$$

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

$$\text{نعلم أن: } 10 \equiv -1 \pmod{11} \text{ إذن: } 10^n \equiv (-1)^n \pmod{11} \text{ مع } n \in \mathbb{N}$$

و منه:

$$x \equiv (a \times 10^0 + b \times 10^1 + c \times 10^2 + d \times 10^3) \pmod{11}$$

$$x \equiv (a \times (-1)^0 + b \times (-1)^1 + c \times (-1)^2 + d \times (-1)^3) \pmod{11}$$

$$x \equiv (a - b + c - d) \pmod{11}$$

خلاصة: $x \equiv (a - b + c - d) \pmod{11}$

4. ما هو باقي القسمة ل 24789 على 11.

$$\text{لدينا: } 24789 \equiv 9 - 8 + 7 - 4 + 2 \equiv 6 \pmod{11}$$

خلاصة: 6 هو باقي القسمة ل 24789 على 11.



نهاية الدرس (ما تبقى فقط البراهين للفقرات السابقة)

1. برهان 1: (لرجوع إلى الدرس اضغط هنا) \Rightarrow (X)

a. لدينا: $a = 1 \times a$ إذن a يقسم a .

خلاصة: $a | a$

b. لدينا: $a | b \Rightarrow \exists k \in \mathbb{Z} / b = ka$

إذن: $\Rightarrow \exists k \in \mathbb{Z} / bc = kca = (kc)a$

ومنه: $\Rightarrow \exists k' = kc \in \mathbb{Z} / bc = k'a$

أي: $\Rightarrow a | cb$

خلاصة: $a | b \Rightarrow a | cb ; (c \in \mathbb{Z})$

c. لدينا: $(a | b \text{ و } b | c) \Rightarrow (\exists k, k' \in \mathbb{Z} / b = ka \text{ و } c = k'b)$

إذن: $\Rightarrow (\exists k, k' \in \mathbb{Z} / c = k'(ka) = (kk')a$

أي: $\Rightarrow \exists k'' = kk' \in \mathbb{Z} / c = k''a$

ومنه: $\Rightarrow a | c$

خلاصة: $(a | b \text{ و } b | c) \Rightarrow a | c$.

d. لدينا: $(a | b \text{ و } b | a) \Rightarrow |a| = |b|$

d. لدينا: $(a | b \text{ و } b | a) \Rightarrow (\exists k, k' \in \mathbb{Z} / b = ka \text{ و } a = k'b)$

إذن: $a = k'b = k'(ka) = (kk') \times a$

ومنه: $(1 - kk') \times a = 0$ إذن $a = 0$ أو $1 - kk' = 0$ (أي $kk' = 1$)

حالة 1: $a = 0$

لدينا: $b = ka = k \times 0 = 0$ ومنه: $|a| = |b|$.

حالة 2: $kk' = 1$

بما أن $k, k' \in \mathbb{Z}$ إذن: $k = k' = 1$ أو $k = k' = -1$

إذن: $(b = ka = 1 \times a \text{ و } a = k'b = 1 \times b)$ أو $(b = ka = -1 \times a \text{ و } a = k'b = -1 \times b)$

إذن: $a = b$ أو $a = -b$

إذن: $|a| = |b|$

خلاصة: $(a | b \text{ و } b | a) \Rightarrow |a| = |b|$.

e. لدينا: $(a | b \text{ و } a | c) \Rightarrow (a | \alpha b \text{ و } a | \beta c)$

إذن: $\Rightarrow (\exists k, k' \in \mathbb{Z} / \alpha b = ka \text{ و } \beta c = k'a)$

ومنه: $\Rightarrow (\exists k, k' \in \mathbb{Z} / \alpha b + \beta c = ka + k'a = (k + k')a$

ومنه: $\Rightarrow (\exists k'' = k + k' \in \mathbb{Z} / \alpha b + \beta c = k''a$

إذن: $\Rightarrow a | (\alpha b + \beta c)$

خلاصة: $(a | b \text{ و } a | c) \Rightarrow a | (\alpha b + \beta c)$

f. لدينا: $\left. \begin{array}{l} a | b \\ c | d \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \exists k \in \mathbb{Z} / b = ka \\ \exists k' \in \mathbb{Z} / d = k'c \end{array} \right.$

ومنه: $\Rightarrow \exists k, k' \in \mathbb{Z} / bd = ka \times k'c = (kk')ac$

$$\Rightarrow \exists k'' = kk' \in \mathbb{Z} / bd = k''(ac) \quad \text{إذن:}$$

$$\Rightarrow ac | bd \quad \text{إذن:}$$

$$\left. \begin{array}{l} a | b \\ c | d \end{array} \right\} \Rightarrow ac | bd \quad \text{خلاصة:}$$

$$n \in \mathbb{N}^* \text{ مع } a | b \Rightarrow a^n | b^n \quad \text{نستنتج أن:}$$

نستدل على ذلك بالترجع:

أ. نتحقق بالنسبة ل $n=1$. لدينا: $a | b \Rightarrow a^1 | b^1$ ($a^1 = a$, $b^1 = b$) إذن العلاقة صحيحة ل $n=1$.

ب. نفترض أن العلاقة صحيحة إلى الرتبة n أي $a^n | b^n$ (معطيات التراجع)

ج. نبين أن: العلاقة صحيحة للرتبة $n+1$ أي نبين أن $a^{n+1} | b^{n+1}$

$$\left. \begin{array}{l} a | b \\ a^n | b^n \end{array} \right\} \Rightarrow a \times a^n | b \times b^n \quad \text{لدينا: (حسب الخاصية السابقة)}$$

$$\Rightarrow a^{n+1} | b^{n+1} \quad \text{إذن:}$$

$$\text{خلاصة: } a | b \Rightarrow a^n | b^n$$

د. نبين أن: $|a| \leq |b|$ ($a | b$ و $b \neq 0$)

بما أن: a تقسم b و $b \neq 0$ إذن: $b = ka; k \in \mathbb{Z} \Rightarrow |b| = |ka| = |k||a|$

من جهة أخرى: $b \neq 0$ ومنه $k \neq 0$ إذن: $|k| \geq 1$ ومنه:

$$|k| \geq 1 \Rightarrow |a||k| \geq |a|$$

$$\Rightarrow |b| \geq |a|$$

خلاصة: $|a| \leq |b|$ ($a | b$ و $b \neq 0$)

برهان 2: (لرجوع إلى الدرس اضغط هنا) \square

نذكر: $E(x) \leq x < E(x) + 1$ (الجزء الصحيح ل x) (1)

• نبين الوجودية:

حالة 1: $a > 0$

$$\text{نضع } q = E\left(\frac{b}{a}\right) \text{ (الجزء الصحيح ل } \frac{b}{a} \text{) و } r = b - aq$$

من خلال (1) نحصل على:

$$E\left(\frac{b}{a}\right) \leq \frac{b}{a} < E\left(\frac{b}{a}\right) + 1 \Leftrightarrow q \leq \frac{b}{a} < q + 1$$

$$\Leftrightarrow aq \leq b < a(q+1) \quad ; \quad a > 0$$

$$\Leftrightarrow aq \leq aq + r < a(q+1)$$

$$\Leftrightarrow 0 \leq r < a$$

$$\Leftrightarrow 0 \leq r < |a| \quad ; \quad |a| = a$$

حالة 2: $a < 0$

بما أن $a < 0$ إذن $-a$ من \mathbb{N}^* . حسب الحالة 1 إذن $b = (-a)q' + r = a(-q') + r = aq + r$

مع $(-q' = q)$ مع $a < 0$ أي $0 \leq r < |a|$ لأن $|a| = -a$

$$b = aq + r \text{ و } 0 \leq r < |a| \text{ ومنه}$$

بالنسبة للوحدانية :

$$\text{إذا كان : } b = aq + r = aq' + r' \text{ إذن : } a(q - q') = r' - r \text{ ومنه : } a \text{ يقسم } r' - r \text{ (1)}$$

$$\text{لدينا : } \begin{cases} 0 \leq r' < a \\ 0 \leq r < a \end{cases} \text{ إذن } -a < r' - r < a \text{ أي } |r' - r| < |a| \text{ (2)}$$

من خلال (1) و (2) نستنتج أن : $r' - r = 0$ إذن $r' = r$ ومنه $q = q'$

3. برهان 3 : (لرجوع إلى الدرس اضغط هنا) \Rightarrow (X)

▪ نفترض أن : d ليس بعدد أولي . (1)

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

$$\text{بما أن } d' | d \text{ و } d' | a \text{ فإن } d | a \text{ (2) .}$$

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

إذن الافتراض كان خاطئا والصحيح هو d عدد أولي .

خلاصة : a عدد أولي.

▪ a ليس بعدد أولي نبين $d \leq \sqrt{a}$.

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

$$d' > 1 \text{ و } d' | a \text{ و بما أن } d \text{ أصغر قاسم إذن } d' \geq d \text{ .}$$

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

خلاصة : $\sqrt{d} \leq a$

4. برهان 4 : (لرجوع إلى الدرس اضغط هنا) \Rightarrow (X)

لتكن P مجموعة الأعداد الأولية الموجبة .

$$\bullet \text{ لدينا : } P \neq \emptyset \text{ (لأن } 5 \in P \text{) .}$$

• نستدل على ذلك بالخلف: نفترض أن : P مجموعة منتهية (أي P تحتوي على عدد منتهى من الأعداد الأولية) . نضع :

$$P = \{p_1, p_2, p_3, \dots, p_n\}$$

$$\bullet \text{ نعتبر العدد } N = p_1 \times p_2 \times \dots \times p_n + 1$$

• 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 $p_1 \times p_2 \times \dots \times p_n$ أي d يقسم $N - p_1 \times p_2 \times \dots \times p_n$ إذن d يقسم 1 وبالتالي $d = 1$ (نهتم

فقط بالأعداد الموجبة) .

$$\bullet d = 1 \text{ غير ممكن لأن } d \text{ عدد أولي (أو } P \text{ غير } 1 \text{) .}$$

• الافتراض P مجموعة منتهية غير ممكن وبالتالي P مجموعة غير منتهية .

خلاصة : P مجموعة غير منتهية.

5. برهان 5 : (لرجوع إلى الدرس اضغط هنا) \Rightarrow (X)

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

جواب :

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

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

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

و بالتالي الافتراض كان خاطئا .

خلاصة: $a_1 \wedge b_1 = d = 1$

6. برهان 6: (لرجوع إلى الدرس اضغط هنا) \Rightarrow (X)

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

1. نبين:

لدينا:

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

$$\Leftrightarrow \exists k \in \mathbb{Z} / b - a = kn$$

$$\Leftrightarrow \exists k \in \mathbb{Z} / b = a + kn$$

ومنه: b تأخذ القيم التالية $\dots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \dots$

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

2. نبين أن:

أ- الانعكاسية:

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

ومنه الانعكاسية.

ب- التماثلية:

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

ومنه: التماثلية.

ج- التعدي:

لدينا:

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

$$\Rightarrow n / (b - a) \text{ و } a / (c - b)$$

$$\Rightarrow n / ((b - a) + (c - b))$$

$$\Rightarrow n / (c - a)$$

$$\Rightarrow a \equiv c [n]$$

ومنه التعدي:

3. نبين أن:

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

لدينا:

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

$$\Leftrightarrow b - a = k''n$$

$$\Leftrightarrow k'n + r' - (kn + r) = k''n$$

$$\Leftrightarrow (k' - k)n + r' - r = k''n$$

$$\Leftrightarrow r' - r = (k'' + k - k')n$$

$$\Leftrightarrow r' - r = Kn ; (K = k'' + k - k')$$

$$\Leftrightarrow n / (r' - r)$$

$$\Leftrightarrow (r' - r) = 0 ; (|r' - r| < n \text{ (1)})$$

$$\Leftrightarrow r' = r$$



خلاصة: $a \equiv b \pmod{n}$ لهما نفس باقي القسمة على n .

4. نبين أن:

1. الموافقة منسجمة مع الجمع:

لدينا:

$$\begin{aligned} (a \equiv b \pmod{n} \text{ و } c \equiv d \pmod{n}) &\Rightarrow n \mid (b-a) \text{ و } n \mid (d-c) \\ &\Rightarrow n \mid ((b-a) + (d-c)) \\ &\Rightarrow n \mid ((b+d) - (a+c)) \\ &\Rightarrow (a+c) \equiv (b+d) \pmod{n} \end{aligned}$$

خلاصة: الموافقة منسجمة مع الجمع.

2. الموافقة منسجمة مع الضرب.

لدينا: $a \equiv b \pmod{n}$ و $c \equiv d \pmod{n}$ و نبين أن: $a \times c \equiv b \times d \pmod{n}$

لدينا:

$$\begin{aligned} (c \equiv d \pmod{n} \text{ و } a \equiv b \pmod{n}) &\Rightarrow n \mid (b-a) \text{ و } n \mid (d-c) \\ &\Rightarrow n \mid (b-a) \times c \text{ و } n \mid (d-c) \times b \\ &\Rightarrow n \mid [(b-a) \times c + (d-c) \times b] \\ &\Rightarrow n \mid [bc - ac + db - cb] \\ &\Rightarrow n \mid [db - ac] \\ &\Rightarrow ac \equiv bd \pmod{n} \end{aligned}$$

خلاصة: الموافقة منسجمة مع الضرب.

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

لدينا:

$$\begin{aligned} a \equiv b \pmod{n} &\Rightarrow n \mid (b-a) \\ &\Rightarrow n \mid (b-a)(a^{k-1}b^0 + a^{k-2}b^1 + a^{k-3}b^2 + \dots + a^1b^{k-1} + a^0b^{k-1}) \\ &\Rightarrow n \mid (b^k - a^k) \\ &\Rightarrow a^k \equiv b^k \pmod{n} \end{aligned}$$

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

أ. حالة $a=3$ (أي قسمة n على 3) نحصل على: $n=3q$ أو $n=3q+1$ أو $n=3q+2$ (لأن $r \in \{0,1,2\}$).