

Arithmétique dans Z**Z الحسابيات في**

ammarimaths		I . القسمة الأقليدية / قابلية القسمة / الموافقة :
<p><u>الموافقة بترديد n:</u></p> <p>نعتبر عددا طبيعيا غير منعدم n . a و b عدنان صحيحان نسبيا؛ نقول أن العدد a موافق للعدد b بترديد n، إذا وجد عدد صحيح k بحيث:</p> $a - b = k.n$ <p>نكتب : $a \equiv b [\text{modulo } n]$</p>	<p><u>قابلية القسمة:</u></p> <p>a و b عدنان صحيحان؛ نقول أن b يقسم a (أو a مضاعف ل b)؛ إذا و فقط إذا وجد عدد صحيح q بحيث: $a = b.q$</p>	<p><u>خاصية القسمة الأقليدية:</u></p> <p>مهما يكن العدد الصحيح النسبي a ، ومهما يكن العدد الصحيح الطبيعي ، غير المنعدم، b ، يوجد عدنان صحيحان وحيدان q و r ، بحيث : $a = b.q + r$ و $0 \leq r < b$</p>
ammarimaths-bm		II . خاصيات قابلية القسمة و الموافقة :
<p><u>قابلية القسمة:</u></p> a / a $(a / b \text{ et } c / d) \Rightarrow ac / bd$ $(a / b \text{ et } b / c) \Rightarrow a / c$ $(a / b \text{ et } b / a) \Rightarrow a = b $ $(\delta / a \text{ et } \delta / b) \Rightarrow (\forall (\alpha, \beta) \in Z^2) ; \delta / \alpha.a + \beta.b$ $a^n / b \Rightarrow a / b$ <p><u>الموافقة:</u></p> $a \equiv b [n] \Leftrightarrow a - b = k.n \Leftrightarrow n / a - b$ $\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d [n] \\ a.c \equiv b.d [n] \end{cases}$		
ammarimaths-bm		III . القاسم المشترك الأكبر والمضاعف المشترك الأصغر :
<p><u>القاسم المشترك الأكبر:</u></p> <p>نرمز له : $d = \text{pgdc}(a, b) = a \wedge b$ يحقق القاسم المشترك الأكبر، الخاصيات التالية:</p> $(d = a \wedge b) \Leftrightarrow (\exists (a', b') \in Z^2) ; \begin{cases} a = d.a' \\ b = d.b' \end{cases} \text{ et } a' \wedge b' = 1$ $\begin{cases} d' / a \\ d' / b \end{cases} \Rightarrow d' / a \wedge b$ <p><u>المضاعف المشترك الأصغر:</u></p> <p>يحقق المضاعف المشترك الأصغر، الخاصيات التالية:</p> $(m = a \vee b) \Rightarrow \begin{cases} a / m \\ b / m \end{cases} ; \begin{cases} a / c \\ b / c \end{cases} \Rightarrow a \wedge b / c$		
<p><u>خاصية مشتركة:</u></p> $\forall (a, b) \in Z^2 ; (a \vee b).(a \wedge b) = a.b $		
ammarimaths-bm:		IV . الأعداد الأولية فيما بينها / خاصيات
<u>خاصيات أخرى:</u>	<u>الأعداد الأولية فيما بينها:</u>	

Arithmétique dans Z**Z الحسابيات في**

$(a/c \text{ et } b/c \text{ et } a \wedge b = 1) \Rightarrow (a.b/c)$ $(a \wedge b = 1 \text{ et } a \wedge c = 1) \Rightarrow (a \wedge b.c) = 1$ $(a \wedge b = 1) \Leftrightarrow \forall (m,n) \in \mathbb{N}^* \times \mathbb{N}^* ; (a^m \wedge b^n = 1)$ $(a = b.q + r \text{ et } 0 \leq r < b) \Rightarrow (a \wedge b = r \wedge b)$	<p>نقول أن العددين a و b أوليان فيما بينهما إذا وفقط إذا كان:</p> $\text{pgcd}(a,b) = 1.$ <p>مبرهنة كوص:</p> $(c/a.b \text{ et } c \wedge a = 1) \Rightarrow (c/b)$
ammarimaths-bm	V. الأعداد الأولية / خاصيات :
<p>خاصيات: ليكن p عددا أوليا، لدينا:</p> $(p/a.b) \Rightarrow (p/a \text{ ou } p/b)$ $(p/a^n) \Rightarrow (p/a)$ $(p/a_1.a_2 \dots a_n) \Leftrightarrow \exists i \in \{1,2,\dots,n\} ; (p/a_i)$ $(p/a) \Rightarrow p \wedge a = p \text{ et } (p \text{ ne divise pas } a) \Rightarrow p \wedge a = 1$	<p>يكون عدد صحيح، عددا أوليا إذا وفقط إذا كان يقبل قاسمين موجبين بالضبط 2، 3، 5، 7... العددان 1 و 1- ليسا أوليان.</p> <p>مجموعة الأعداد الأولية مجموعة غير منتهية...</p>

ammarimaths-bm	I. خوارزمية أقليدس :
<p>إذا كان $r_1 \neq 0$، نقسم r_0 على r_1، ونجد: الخ. بعد عدد محدود من العمليات نحصل على باقي منعدم (ذلك لأن متتالية البواقي هي متتالية تناقصية لأعداد صحيحة) ليكن r_n آخر باقي غير منعدم، يكون لدينا إذن: $\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$</p>	<p>نعتبر العددين الصحيحين الطبيعيين a و b، بحيث: $a > b$ نقسم العدد a (العدد الأكبر) على العدد b ونجد: (1): $a = b.q_0 + r_0 \text{ et } 0 \leq r_0 < b$ إذا كان $r_0 = 0$، فإن $\text{pgcd}(a,b) = b$ ونجد: إذا كان $r_0 \neq 0$، نقسم b على r_0، ونجد: (2): $b = r_0.q_1 + r_1 \text{ et } 0 \leq r_1 < r_0 < b$ إذا كان $r_1 = 0$، فإن $\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = r_0$</p>
ammarimaths-bm	II. تفكيك عدد صحيح إلى جداء عوامل أولية :
<p>بحيث تكون الأعداد p_i أولية، والأعداد α_i صحيحة غير منعدمة.</p>	<p>كل عدد صحيح طبيعي غير منعدم ومخالف للعدد 1، يتفكك بشكل وحيد على شكل: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_n^{\alpha_n}$</p>
ammarimaths-bm	III. مجموعة أصناف التكافؤ : Z/n.Z
<p>يرمز لمجموعة أصناف التكافؤ $Z/n.Z$: $Z/n.Z = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \bar{n-2}, \bar{n-1} \}$ يعرف الجمع والضرب في هذه المجموعة كما يلي: $\begin{cases} \overline{a+b} \equiv \overline{a+b} \\ \overline{a.b} \equiv \overline{a.b} \end{cases}$ ($Z/n.Z, +, \cdot$) حلقة واحدة تبادلية، بصفة عامة غير تكاملية. إذا كان العدد n أوليا، فإن ($Z/n.Z, +, \cdot$) يكون جسما. $(\bar{a} \text{ inversible dans } Z/n.Z) \Leftrightarrow (a \wedge n = 1)$</p>	<p>علاقة التوافق: $a \equiv b [n] \Leftrightarrow a - b = k.n \Leftrightarrow n/a - b$ هي علاقة تكافؤ في مجموعة الأعداد الصحيحة النسبية، منسجمة مع قانوني الجمع والضرب: $\begin{cases} a \equiv b [n] \\ c \equiv d [n] \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d [n] \\ a.c \equiv b.d [n] \end{cases}$ صنف تكافؤ العدد الصحيح النسبي x، هو المجموعة المعرفة كما يلي: $\alpha = \bar{x} = \{ y \in Z / y \equiv x [\text{modulo } n] \}$</p>
ammarimaths-bm	IV. نظمت العد : Z/n.Z
<p>نكتب: (1): $b = \overline{a_n a_{n-1} \dots a_1 a_0}^{(x)}$ ونقول أن هذه الكتابة هي الكتابة المختصرة للعدد b في</p>	<p>ليكن x عددا صحيحا أكبر من أو يساوي 2. كل عدد صحيح b يمكن أن يكتب على الشكل: $b = a_n.x^n + a_{n-1}.x^{n-1} + \dots + a_1.x + a_0$</p>

Arithmétique dans \mathbb{Z} **الحسابيات في \mathbb{Z}**

نظمة العد الذي أساسه x .	بحيث: $a_n \neq 0$ et $(\forall i \in [0, n]) ; a_i \in [0, n-1]$
V . تحديد القاسم المشترك الأكبر والمصاعف المشترك الأصغر لعددين :	
$a \wedge b = \prod_{i=1}^n p_i^{\inf(\alpha_i, \beta_i)}$ $a \vee b = \prod_{i=1}^n p_i^{\sup(\alpha_i, \beta_i)}$	<p>نعتبر :</p> $a = \prod_{i=1}^n p_i^{\alpha_i} \quad \text{et} \quad b = \prod_{i=1}^n p_i^{\beta_i}$ <p>التفكيك الى جداء عوامل أولية للعددين a و b . نجد:</p>