

Arithmétique dans $\mathbb{Z}$

الحسابيات في $\mathbb{Z}$

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

Arithmétique dans Z

الحسابيات في Z

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

ammarimaths-bm	I. خوارزمية أقليدس :
إذا كان $r_1 \neq 0$ ، نقسم r_0 على r_1 ، ونجد: 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: $\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = \dots = \text{pgcd}(r_{n-1}, r_n) = r_n$	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 $\text{pgcd}(a,b) = b$ ، ونقسم 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 $\text{pgcd}(a,b) = \text{pgcd}(b,r_0) = r_0$
ammarimaths-bm	II. تفكيك عدد صحيح إلى جداء عوامل أولية :
بحيث تكون الأعداد p_i أولية، والأعداد α_i صحيحة غير منعدمة.	كل عدد صحيح طبيعي غير منعدم ومخالف للعدد 1 ، يتفكك بشكل وحيد على شكل: $n = p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_n^{\alpha_n}$
ammarimaths-bm	III. مجموعة أصناف التكافؤ : $\mathbb{Z}/n.\mathbb{Z}$
يرمز لمجموعة أصناف التكافؤ $\mathbb{Z}/n.\mathbb{Z}$: $\mathbb{Z}/n.\mathbb{Z} = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \dots, \overline{n-2}, \overline{n-1} \}$ يعرف الجمع والضرب في هذه المجموعة كما يلي: $\begin{cases} \overline{a+b} \equiv \overline{a} + \overline{b} \\ \overline{a.b} \equiv \overline{a} . \overline{b} \end{cases}$ $(\mathbb{Z}/n.\mathbb{Z}, +, \cdot)$ حلقة واحدة تبادلية، بصفة عامة غير تكاملية. إذا كان العدد n أوليا، فإن $(\mathbb{Z}/n.\mathbb{Z}, +, \cdot)$ يكون جسما. $(\overline{a} \text{ inversible dans } \mathbb{Z}/n.\mathbb{Z}) \Leftrightarrow (a \wedge n = 1)$	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: $\alpha = \bar{x} = \{y \in \mathbb{Z} / y \equiv x [\text{modulo } n]\}$
ammarimaths-bm	IV. نظمات العد : $\mathbb{Z}/n.\mathbb{Z}$
نكتب: $(1): b = a_n a_{n-1} \dots a_1 a_0^{(x)}$ ونقول أن هذه الكتابة هي الكتابة المختصرة للعدد b في	ليكن x عددا صحيحا أكبر من أو يساوي 2. كل عدد صحيح b يمكن أن يكتب على الشكل : $b = a_n . x^n + a_{n-1} . x^{n-1} + \dots + a_1 . x + a_0$

Arithmétique dans $\mathbb{Z}$

$\mathbb{Z}$ الحسابيات في

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