Arithmétique dans Z
الحسابيات في Z

I. القسمة الأقليدية / قابلية القسمة / الموافقة :	ammarimaths

خاصية القسمة الأقليدية:	قابلية القسمة:	الموافقة بترديد n:
مهما يكن العدد الصحيح النسبي a ، ومهما يكن العدد الصحيح الطبيعي غير المنعدم، b ، يوجد عددان صحيحان وحيدان q و r ، بحيث : $a = b.q + r$ و $0 \le r \prec b$	a و b عددان صحيحان؛ نقول أن b يقسم a (أو a مضاعف ل b)؛ إذا وفقط إذا وجد عدد صحيح q بحيث: $a = b.q$	نعتبر عددا طبيعيا عير منعدم n . a و b عددان صحيحان نسبيان؛ نقول أن العدد a موافق للعدد b بترديد n ، إذا وجد عدد صحيح k بحيث: $a - b = k.n$ نكتب : $a \equiv b[modulo]$

II. خاصيات قابلية القسمة و الموافقة :	ammarimaths-bm

قابلية القسمة:

$$a / a$$
$$(a / b \;\; et \;\; c / d) \Rightarrow ac / bd$$
$$(a / b \;\; et \;\; b / c) \Rightarrow a / c$$
$$(a / b \;\; et \;\; b / a) \Rightarrow |a| = |b|$$
$$(\delta / a \;\; et \;\; \delta / b) \Rightarrow (\forall (\alpha, \beta) \in Z^2) \; ; \; \delta / \alpha.a + \beta.b$$
$$a^n / b \Rightarrow a / b$$

الموافقة:

$$a \equiv b[n] \Leftrightarrow a - b = k.n \Leftrightarrow n / a - b$$
$$\begin{cases} a \equiv b[n] \\ c \equiv d[n] \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d[n] \\ a.c \equiv b.d[n] \end{cases}$$

III. القاسم المشترك الأكبر والمضاعف المشترك الأصغر :	ammarimaths-bm

القاسم المشترك الأكبر:

نرمز له : $d = pgdc(a,b) = a \wedge b$

يحقق القاسم المشترك الأكبر، الخاصيات التالية:

$$(d = a \wedge b) \;\Leftrightarrow\; (\exists (a',b') \in Z^2) \; ; \; \begin{cases} a = d.a' \\ b = d.b' \end{cases} \; et \;\; a' \wedge b' = 1$$

$$\begin{cases} d' / a \\ d' / b \end{cases} \quad \Rightarrow \quad d' / a \wedge b$$

المضاعف المشترك الأصغر:

يحقق المضاعف المشترك الأصغر، الخاصيات التالية:

$$(m = a \vee b) \;\Rightarrow\; \begin{cases} a / m \\ b / m \end{cases} \quad ; \quad \begin{cases} a / c \\ b / c \end{cases} \;\Rightarrow\; a \wedge b / c$$

خاصية مشتركة:

$$\forall (a,b) \in Z^2 ; (a \vee b).(a \wedge b) = |a.b|$$

IV. الأعداد الأولية فيما بينها / خاصيات	ammarimaths-bm:

الأعداد الأولية فيما بينها:	خاصيات أخرى:

Citation : « La mathématique est la rêne de la science et l'Arithmétique est la rêne des mathématique »

Arithmétique dans Z

الحسابيات في Z

نقول أن العددين a b أوليان فيما بينهما إذا وفقط إذاكان:

pgcd (a,b)=1.

مبرهنة كوص:

$\left(c/a.b \text{ et } c\wedge a=1\right) \Rightarrow (c/b)$

$\left(a/c \text{ et } b/c \text{ et } a\wedge b=1\right) \Rightarrow (a.b/c)$

$\left(a\wedge b=1 \text{ et } a\wedge c=1\right) \Rightarrow (a\wedge b.c)=1$

$\left(a\wedge b=1\right) \Leftrightarrow \forall(m,n)\in IN^{*}xIN^{*} \;;\; (a^{m}\wedge b^{n}=1)$

$\left(a=b.q+r \text{ et } 0\le r\prec b\right) \Rightarrow (a\wedge b=r\wedge b)$

V. الأعداد الأولية / خاصيات :

ammarimaths-bm

يكون عدد صحيح، عددا أوليا إذا وفقط إذا كان يقبل قاسمين موجبين بالضبط 2، 3 ،5، 7 ... العددان 1 و 1- ليسا أوليان.

مجموعة الأعداد الأولية مجموعة غير منتهية...

خاصيات: ***ليكن p عددا أوليا، لدينا:***

$\left(p/a.b\right) \Rightarrow (p/a \quad ou \quad p/b)$

$\left(p/a^{n}\right) \Rightarrow (p/a)$

$\left(p/a_1.a_2...a_n\right) \Leftrightarrow \exists i\in(1,2,...,n) \;;\; (p/a_i)$

$(p/a)\Rightarrow p\wedge a=p \text{ et } (p \text{ ne divise pas } a)\Rightarrow p\wedge a=1$

I. خوارزمية أقليدس :

ammarimaths-bm

نعتبر العددين الصحيحين الطبيعيين a و b ، بحيث:

$a>b$

نقسم العدد a (العدد الأكبر) على العدد b ونجد:

$(1): \quad a=b.q_0+r_0 \quad \text{et} \quad 0\le r_0\prec b$

إذا كان $r_0=0$ ، فإن $pgcg(a,b)=b$

إذا كان $r_0 \# 0$ ، نقسم b على r_0 ، ونجد:

$(2): \quad b=r_0.q_1+r_1 \quad \text{et} \quad 0\le r_1\prec r_0\prec b$

إذا كان $r_1=0$ ، فإن $pgcd(a,b)=pgcd(b,r_0)=r_0$

إذا كان $r_1 \# 0$ ، 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:

$pgcd(a,b)=pgcd(b,r_0)=\ldots=pgcd(r_{n-1},r_n)=r_n$

II. تفكيك عدد صحيح الى جداء عوامل أولية :

ammarimaths-bm

كل عدد صحيح طبيعي غير منعدم ومخالف للعدد1 ، يتفكك بشكل وحيد على شكل:

$n=p_1^{\alpha_1}.p_2^{\alpha_2}...p_n^{\alpha_n}$

بحيث تكون الأعداد *pi* أولية، والأعداد α_i صحيحة غير منعدمة.

III. مجموعة أصناف التكافؤ : Z/n.Z

ammarimaths-bm

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 و الضرب:

$$\begin{cases}a\equiv b[n]\\ c\equiv d[n]\end{cases}\Rightarrow\begin{cases}a+c\equiv b+d\,[n]\\ a.c\equiv b.d\,[n]\end{cases}$$

صنف تكافؤ العدد الصحيح النسبي x ، هو المجموعة المعرفة كما يلي:

$\alpha=\overline{x}=\{y\in Z/ \;\; y\equiv x[\text{modulo } n]\}$

يرمز لمجموعة أصناف التكافؤ : $Z/n.Z$

$Z/n.Z=\left\{\overline{0},\overline{1},\overline{2},\overline{3},\ldots\ldots,\overline{n-2},\overline{n-1}\right\}$

يعرف الجمع والضرب في هذه المجموعة كما يلي:

$$\begin{cases}\overline{a}+\overline{b}\equiv\overline{a+b}\\ \overline{a}.\overline{b}\equiv\overline{a.b}\end{cases}$$

(Z/n.Z , + , x) حلقة واحدية تبادلية، بصفة عامة غير تكاملية.

إذا كان العدد n أوليا، فإن (Z/n.Z , + , x) يكون جسما.

$\left(\overline{a} \text{ inversible dans } Z/n.Z\right) \Leftrightarrow (a\wedge n=1)$

IV. نظمة العد : Z/n.Z

ammarimaths-bm

ليكن x عددا صحيحا أكبر من أو يساوي 2.

كل عدد صحيح b يمكن أن يكتب على الشكل :

$b=a_n.x^{n}+a_{n-1}.x^{n-1}+\ldots.+a_1.x+a_0$

نكتب:

$(1): \quad b=\overline{a_n a_{n-1}\ldots a_1 a_0}^{\,(x)}$

ونقول أن هذه الكتابة هي الكتابة المختصرة للعدد b في

*Citation : « **La mathématique est la rêne de la science et l'Arithmétique est la rêne des mathématique** »*

Arithmétique dans Z

الحسابيات في Z

بحيث: $a_n \neq 0$ et $(\forall i \in [0, n])$; $a_i \in [0, n-1]$	نظمة العد الذي أساسه x .

V . تحديد القاسم المشترك الأكبر والمضاعف المشترك الأصغر لعددين : ammarimaths-bm

نعتبر : $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$ التفكيك الى جداء عوامل أولية للعددينم a و b . نجد:	$a \wedge b = \prod_{i=1}^{n} p_i^{\inf(\alpha_i, \beta_{iç})}$ $a \vee b = \prod_{i=1}^{n} p_i^{\sup(\alpha_i, \beta_{iç})}$

*Citation : « **La mathématique est la rêne de la science et l'Arithmétique est la rêne des mathématique** »*