Contrôle de cours - ARITH (1 heure)

Nom : Le Cras **Prénom :** Brieuc **Classe :** PA-1

Le barème est sur 30. La note sera ramenée à une note sur 20 par une règle de 3. **Note :** 13 /20

Cours 1 : divisibilité et division euclidienne (4 points)

19,5/30

Soit $(a, b) \in \mathbb{Z}^2$.

1. Donner la définition mathématique de « a divise b »

1 $a \mid b \iff \exists k \in \mathbb{Z}, b = a \times k$

2. Exemple : donner tous les diviseurs positifs de 6 sous forme d'ensemble.

1 $\{k \mid 6, k \in \mathbb{N}\} = \{1, 2, 3, 6\}$

3. On suppose b non nul. Énoncer la théorème de la division euclidienne de a par b.

2 $\forall (a, b) \in \mathbb{Z} \times \mathbb{Z}^*, \exists! (q, r) \in \mathbb{Z}^2 \quad a = bq + r$ avec $0 \leq r < |b|$

Cours 2 : congruences (11,5 points)

1. Soit $(a, b, c) \in \mathbb{Z}^3$. Montrer que $a \mid b$ et $a \mid c \implies \forall (u, v) \in \mathbb{Z}^2, a \mid bu + cv$.

$a \mid b \iff \exists k \in \mathbb{Z}, \quad b = ak$

$a \mid c \iff \exists k' \in \mathbb{Z}, \quad c = ak'$

Soit $(u, v) \in \mathbb{Z}^2$

Si $b \times u = aku$ avec $ku \in \mathbb{Z}$

Si $c \times v = ak'v$ avec $k'v \in \mathbb{Z}$

alors $bu + cv = aku + ak'v$

$bu + cv = ak(ku + k'v)$ avec $k(u+v) \in \mathbb{Z}$

Donc $\forall (u, v) \in \mathbb{Z} \quad a \mid bu + cv$

(!) k et k' n'ont aucune raison d'être égaux

2

2. Soient $n \in \mathbb{N}^*$ et $(a,b,c,d) \in \mathbb{Z}^4$ tels que $a \equiv b\,[n]$ et $c \equiv d\,[n]$. En utilisant la propriété précédente, montrer que : $a+c \equiv b+d\,[n]$ et $a \times c \equiv b \times d\,[n]$

$a \equiv b\,[n] \iff n \mid a-b \iff \exists\, k \in \mathbb{Z},\ a = b + nk$

$c \equiv d\,[n] \iff n \mid c-d \iff \exists\, k' \in \mathbb{Z},\ c = d + nk'$

Donc $a+c = b+nk+d+nk'$
$a+c = b+d+n(k+k')$ avec $k+k' \in \mathbb{Z}$

2

Donc $a+c \equiv b+d\,[n]$

De la même manière, $a \times c = (b+nk)(d+nk')$
$a \times c = b\times d + bnk' + dnk + n^2kk'$
$a \times c = b \times d + n(bk' + dk + nkk')$
avec $(bk'+dk+nkk') \in \mathbb{Z}$

Donc $a \times c \equiv b \times d\,[n]$

3. Exemples : on pose $n = 8$, $a = 18$ et $c = 31$. Trouver modulo 8 : a, c, $a-c$, $a \times c$ et a^5. **Chacune de vos réponses doit être un entier entre 0 et 7.**

$18 \equiv 2\,[8]$ $31 \equiv 7\,[8]$ $31 = 32-1 \equiv -1\,[8] \equiv 7\,[8]$

1

$18 - 31 \equiv 2 - 3\,[8] \equiv \cancel{-1}\,[8]$ $18 \times 31 \equiv 2 \times 3\,[8] \equiv 6\,[8]$

Vrai par chance !!

$18^5 \equiv 2^5\,[8] \equiv 2^3 \times 2^2\,[8] \equiv \cancel{2^2\,[8]}$

4. (a) Énoncer le petit théorème de Fermat.

Soit p un nombre premier et $a \in \mathbb{Z}$, on a :

1

$a^p \equiv a\,[p]$ ~~.......~~ et $a^{(p-1)} \equiv 1\,[p]$ si $p \nmid a$

(b) Application : trouver le reste de la division euclidienne de 15^{14} par 11. Vous mettrez en évidence les étapes des calculs.

11 premier et

On remarque que $11 \nmid 15$ donc $15^{10} \equiv 1\,[11]$

1

On transforme 14 sous une forme de division euclidienne : $14 = 10 \times 1 + 4$

donc $15^{14} = 15^{10\times1+4} = 15^{10} \cancel{\times} 15^4$

$15^{14} \equiv 15^{10} \times 15^4\,[11] \equiv 1 \times 15^4\,[11]$

$15 \equiv 4\,[11]$ $15^2 \equiv 4^2\,[11] \equiv 5\,[11]$ $15^3 \equiv 3 \times 5\,[11] \equiv 27\,[11] \equiv 5\,[11]$

$15^4 \equiv 3 \times 5\,[11] \equiv 15\,[11] \equiv 4\,[11]$

Donc $15^{14} \equiv 4\,[11]$

Cours 3 : nombres premiers et pgcd (2 points)

On considère les entiers $a = 700$ et $b = 2 \times 3 \times 5^3 \times 7^2 \times 11$.

1. Décomposer a en produits de facteurs premiers.

$a = 2^2 \times 3^0 \times 5^2 \times 7^1 \times 11^0$ ✓

1

2. Trouver $a \wedge b$.

$a \wedge b = 2 \times 3^0 \times 5^2 \times 7^1 \times 11^0 = 2 \times 5^2 \times 7 = 350$ ✓

1

Cours 4 : polynômes 1 (2,5 points)

Effectuer la division euclidienne de $A = X^5 - X^3 + 2X^2 - 4$ par $X^3 + X + 1$.

Écrire le résultat sous forme d'égalité.

$X^5 - X^3 + 2X^2 - 4 = (X^3 + X + 1) \times X^2 + X^2 - 4$

$X^3 + X + 1 = (X^2 - 4) \times X + 5X + 1$??

$X^2 - 4 = (5X + 1) \times X + (-4X^2 - X - 4)$

0 Posez la division euclidienne !

[Tournez la page pour **Cours 5**]

Cours 5 : polynômes 2 (10 points)

Les questions sont indépendantes. **Pour les questions 2., 3. et 4., ce n'est pas la peine de donner les polynômes sous une forme développée.**

1,5

1. Soit $P \in \mathbb{R}[X]$ de degré strictement supérieur à 3. Mettre les symboles $\Longrightarrow$, $\Longleftarrow$ ou $\Longleftrightarrow$ à la place des pointillés.

   a) -2 racine de P ..$\Longleftrightarrow$?.. $(X+2) \mid P$ b) $P(3) = 0$ ..$\cancel{\Leftarrow}$?.. $(X-3)^2 \mid P$

   c) $\exists Q \in \mathbb{R}[X],\ P(X) = (X-1)Q(X)$ ..$\Longleftarrow$.. $(X-1)$ divise P et $(X-1)^2$ ne divise pas P

   d) $(X-1)^3 \mid P$ ..$\Longrightarrow$?.. $P(1) = P'(1) = 0$

0

2. Soit $P(X) = X^5 - 3X^4 + X^2$. Sans utiliser la notion de dérivée, expliquer pourquoi 0 est une racine d'ordre de multiplicité exactement 2 de P.

   ....

   ....

0

3. Donner un exemple d'un polynôme de $Q \in \mathbb{R}[X]$, de degré 5 ayant -2 comme racine d'ordre de multiplicité exactement égal à 3.

   ....

0

4. Donner un exemple d'un polynôme de $A \in \mathbb{R}[X]$, de degré 4 vérifiant $A(1) = 0$ et $A(-3) = A'(-3) = 0$.

   ....

5. On se donne les polynômes suivants :

   a) $A = X^2 + X$ b) $B = X^2 + 1$ c) $C = X^3 + X + 1$ d) $D = X^2 - 3X + 2$ e) $E = X^2 + X + 1$

   Dire pour chacun d'entre eux s'ils sont irréductibles dans $\mathbb{R}[X]$ (entourer « OUI » ou « NON ») en justifiant votre choix :

   a) OUI NON

   car $\Delta = 1$ donc $\Delta > 0$

   b) OUI NON

   car $\Delta = -4$ donc $\Delta < 0$

5

   c) OUI NON

   car un polynôme est irréductible dans $\mathbb{R}[X]$ que si il est de degré 1 ou de degré 2 avec un $\Delta < 0$ or C est de degré 3

   d) OUI NON

   car $\Delta = 1$ donc $\Delta > 0$

   e) OUI NON

   car $\Delta = -3$ donc $\Delta < 0$