Université de Rennes

Algèbre et Géométrie 2

Feuille d'exercices d'algèbre n°2

Arithmétique dans $\mathbb{Z}$

Révisions n°1

- (*Mayotte - Deuxième épreuve 2021*) Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^*$.
  1 - Démontrer qu'il existe un entier naturel n tel que $nb > a$.
  2 - Soit $S = \{s \in \mathbb{N}, bs > a\}$. Comme S est non vide, on admet qu'il possède un plus petit élément t. En déduire l'existence d'un couple d'entiers naturels (q, r) vérifiant $bq \leqslant a < b(q + 1)$.
  3 - Démontrer l'unicité du couple d'entiers naturels (q, r) vérifiant $a = bq + r$ et $0 \leqslant r < b$. L'opération qui associe au couple (a, b) le couple (q, r) est la ***division euclidienne*** de a par b. a est appelé le ***dividende***, b le diviseur, q le ***quotient*** et r le ***reste*** de la division euclidienne.
  4 - On effectue une division euclidienne où le dividende est égal à 53 et le reste à 5. Quels peuvent être le diviseur et le quotient ?
  5 - On suppose $a > b$ et on divise a et b par leur différence $a - b$. Comparer les quotients et les restes obtenus.
- Que devient le théorème de division euclidienne dans $\mathbb{Z}$? Déterminer tous les sous-groupes de $(\mathbb{Z}, +)$.
- Donner deux caractérisations différentes :
  1) du pgcd de deux entiers naturels 2) du ppcm de deux entiers naturels
- Rappeler le théorème de Bézout et les lemmes de Gauss et d'Euclide.

Exercice n°1

Par combien de zéros se termine l'écriture décimale de 2023! ?

Exercice n°2

Énoncer des critères de divisibilité par 6, par 2 et par 5 à partir de l'écriture en base six d'un nombre.

Exercice n°3 (*Deuxième épreuve 2019*)

Soient a, b, n trois entiers relatifs, a et b étant non nuls. Montrer que PGCD(a, b) =PGCD$(a, b + na)$.

Exercice n°4

Soient m et n deux entiers naturels premiers entre eux. Montrer que tout diviseur d de mn s'écrit de manière unique $d = d_1 d_2$ avec $d_1 | m$, $d_2 | n$ et d_1 et d_2 premiers entre eux.

Exercice n°5 (*CAPES 2012, épreuve sur dossier*)

Le 1er juin 2012, les participants d'un club d'astronomie ont observé le corps céleste $\mathscr{A}$, qui apparaît tous les 51 jours.
Le 28 juin 2012, ils ont observé le corps céleste $\mathscr{B}$, qui apparaît tous les 72 jours.

1) À quelle date devront-ils fixer une nouvelle réunion pour observer simultanément les deux corps ?

2) Un membre du club, qui ne pourra pas être présent à cette date, aura-t-il la possibilité d'observer une nouvelle conjonction des deux corps avant fin 2016 ?

Exercice n°6 (*Mayotte - Deuxième épreuve 2022*)

Vrai ou Faux ? Soit l'équation diophantienne (E) : $3x - 2y = -1$.
PROPOSITION : *Les couples de $\mathbb{Z}^2$ solutions de (E) sont tous formés d'entiers relatifs de même signe.*

Exercice n°7 (*CAPES 2006, épreuve sur dossier*)

1) Soit m un entier relatif. On note (E_m) l'équation $11x + 13y = m$, d'inconnue (x, y). Trouver toutes les solutions (x, y) de (E_m) dans $\mathbb{Z} \times \mathbb{Z}$.

2) On suppose désormais que m est un entier naturel. Montrer qu'il y a autant de solutions (x, y) de l'équation (E_m) dans $\mathbb{N} \times \mathbb{N}$ qu'il y a d'entiers dans le segment $[\frac{5m}{11}, \frac{6m}{13}]$.

3) Montrer que si $m < 143$ (resp. $m \geqslant 143$), alors l'équation (E_m) possède au plus (resp. au moins) une solution (x, y) dans $\mathbb{N} \times \mathbb{N}$.

Exercice n°8

1) Montrer qu'il y a une infinité de nombres premiers.

2) Soit $n \in \mathbb{N}$. Montrer que l'on peut trouver n entiers consécutifs dont aucun n'est premier.

Révisions n°2

- Énoncer le théorème fondamental de l'arithmétique (décomposition en facteurs premiers). En proposer une démonstration.
- Donner les principales propriétés de la congruence modulo n dans $\mathbb{Z}$.
- Énoncer le théorème de Wilson sur les nombres premiers. En proposer une démonstration.

Exercice n°9

On appelle diviseur propre d'un entier naturel non nul n, tout diviseur de n qui soit positif et distinct de n. Tout entier naturel non nul égal à la somme de ses diviseurs propres est dit nombre parfait.

1) a) Établir les listes des diviseurs de 28 et de 496 et montrer que ce sont deux nombres parfaits.

b) Vérifier que 28 et 496 sont de la forme $2^n(2^{n+1} - 1)$, où $n \in \mathbb{N}^*$, avec $2^{n+1} - 1$ premier.

c) Démontrer que, pour tout $n \in \mathbb{N}^*$, si $2^{n+1} - 1$ est premier, alors $2^n(2^{n+1} - 1)$ est parfait.

d) Illustrer par un exemple le fait que, si $2^{n+1} - 1$ n'est pas premier, alors $2^n(2^{n+1} - 1)$ n'est pas parfait.

2) Soit a un nombre pair.

a) Montrer que l'on peut écrire a sous la forme $2^n b$, où b est un entier impair et $n \in \mathbb{N}^*$.

b) On note $s(a)$ la somme de tous les diviseurs positifs de a. Montrer que $s(a) = (2^{n+1} - 1)s(b)$.

c) Montrer que a est un nombre parfait si et seulement si $b = (s(b) - b)(2^{n+1} - 1)$. En déduire que si a est parfait alors $s(b) - b$ est un diviseur de b, puis que b est premier et égal à $2^{n+1} - 1$.

d) Conclure.

Exercice n°10

1) Quel est le nombre de diviseurs de 192 080 000 ?

2) Quel est le chiffre des unités dans l'écriture en base 10 du nombre $7^{7^{7^{7^{7^{7^{7}}}}}}$?

Exercice n°11

Pour $n \in \mathbb{N}^*$, on note d_n le nombre de diviseurs positifs de n.

1) Montrer que si $n = ab$ avec $a \wedge b = 1$, alors $d_n = d_a d_b$.

2) Montrer que n est un carré parfait si et seulement si d_n est impair.

3) Montrer que : $\prod_{d|n} d = \sqrt{n}^{d_n}$.

Exercice n°12

Soit $n \in \mathbb{N}^*$. Montrer que le cardinal de $\{(a, b) \in (\mathbb{N}^*)^2,\ a \vee b = n\}$ est égal au nombre de diviseurs de n^2.

Exercice n°13

On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par $u_n = 1 + 10 + 100 + \ldots + 10^n$

1) Trouver deux entiers naturels distincts n et p tels que $u_n - u_p$ soit divisible par 24.

2) Plus généralement, montrer que, pour tout nombre $a \in \mathbb{N}$, il existe un multiple non nul de a qui s'écrit en écriture décimale uniquement avec les chiffres 1 et 0.

Exercice n°14

1) Montrer que si un produit d'entiers naturels est de la forme $4n - 1$ alors au moins l'un des facteurs est de la même forme. En déduire qu'il existe une infinité de nombres premiers de la forme $4n - 1$.

2) Soient $n \in \mathbb{N}$ et $p \geqslant 3$ un diviseur premier de $n^2 + 1$. Montrer que $p \equiv 1\ [4]$. En déduire qu'il y a une infinité de nombres premiers de la forme $4k + 1$.

Exercice n°15

Pour tout entier $n \geqslant 1$ on pose $a_n = 1! + 2! + \cdots + n!$

On donne la décomposition en facteurs premiers des dix premiers termes de la suite (a_n)

$a_1 = 1$	$a_2 = 3$	$a_3 = 3^2$	$a_4 = 3 \times 11$	$a_5 = 3^2 \times 17$
$a_6 = 3^2 \times 97$	$a_7 = 3^4 \times 73$	$a_8 = 3^2 \times 11 \times 467$	$a_9 = 3^2 \times 131 \times 347$	$a_{10} = 3^2 \times 11 \times 40787$

1) Montrer que a_n n'est jamais divisible par 2, par 5 ni par 7.

2) Peut-on affirmer que a_n est divisible par 11 à partir d'un certain rang ?

3) Peut-on affirmer que, à partir d'un certain rang, a_n est divisible par 3^2 mais pas par 3^3 ?

Exercice n°16 (*Deuxième épreuve 2018*)

On fixe un nombre premier p. Soit a un entier (relatif) tel que p ne divise pas a. Le but de cette question est de démontrer l'égalité suivante, connue sous le nom de petit théorème de Fermat : $a^{p-1} \equiv 1 \bmod p$.

On désigne par A l'ensemble$\{a, 2a, 3a, ..., (p-1)a\}$.

1) Soit k un entier relatif. Montrer que p divise ka si, et seulement si, p divise k. En déduire que p ne divise aucun élément de A.

2) Pour $i \in [\![1, p-1]\!]$, on note α_i le reste modulo p de l'entier ia.
Établir que ces restes sont tous non nuls et deux à deux distincts.
En déduire que $\{\alpha_i, i \in [\![1, p-1]\!]\} = [\![1, p-1]\!]$.

3) On appelle P le produit de tous les éléments de A. Établir que $P = a^{p-1}(p-1)!$ et que $P \equiv (p-1)! \bmod p$.

4) En déduire que pour tout entier relatif a premier avec p , $a^{p-1} \equiv 1 \bmod p$.

Exercice n°17 (*Deuxième épreuve 1992*)

Pour $n \in \mathbb{N}$, on note $E_n = \{z \in \mathbb{Z}[i],\ |z|^2 = 5^n\}$ où $\mathbb{Z}[i] = \{x + iy,\ (x, y) \in \mathbb{Z}^2\}$.
Soit $z = x + iy$ un élément de E_n avec $n \geqslant 1$. Montrer que (x, y) vérifie l'un des systèmes

$$(1) \left\{ \begin{array}{l} 2x - y \equiv 0 \pmod 5 \\ x + 2y \equiv 0 \pmod 5 \end{array} \right. \qquad \text{ou} \qquad (2) \left\{ \begin{array}{r} 2x + y \equiv 0 \pmod 5 \\ -x + 2y \equiv 0 \pmod 5 \end{array} \right.$$

En déduire que l'un des nombres $\dfrac{z}{2+i}$ ou $\dfrac{z}{2-i}$ appartient à E_{n-1}.

Révisions n°3 Polynômes et arithmétique

- Rappeler le théorème de division euclidienne dans $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps. Quand dit-on qu'un polynôme est irréductible ? Donner des exemples.
- Calculer le PGCD de $P_1 = 2X^4 - 3X^2 + 1$ et de $P_2 = X^3 + X^2 - X - 1$ dans $\mathbb{Q}[X]$ et trouver S et T dans $\mathbb{Q}[X]$ tel que $PGCD(P_1, P_2) = P_1.S + P_2.T$

Exercice n°18

1) Calculer le pgcd unitaire D des polynômes $A = X^4 + X^2 - 2X$ et $B = X^3 - X^2 - 4$.

2) Trouver deux polynômes U et V tels que $D = AU + BV$.

3) Déterminer le ppcm unitaire de A et B.

4) Déterminer les décompositions en facteurs irréductibles de A et B dans $\mathbb{R}[X]$ puis dans $\mathbb{C}[X]$.

Exercice n°19

Soient A et B dans $\mathbb{K}[X]$.

1) A-t-on $\text{pgcd}(A, B) = 1 \iff \text{pgcd}(A + B, AB) = 1$?

2) A-t-on $\text{pgcd}(A, B) = \text{pgcd}(A + B, AB)$?

Exercice n°20 *(D'après la deuxième épreuve 2002)*

On note $\mathscr{P}(\mathbb{Z}, \mathbb{Z})$ l'ensemble des polynômes P de $\mathbb{R}[X]$ vérifiant $P(\mathbb{Z}) \subset \mathbb{Z}$.

1) Soient $n \in \mathbb{N}$ et Γ_n le polynôme défini par $\Gamma_0(X) = 1$ et, pour $n > 0$, $\Gamma_n(X) = \dfrac{X(X-1)\cdots(X-n+1)}{n!}$.

a) Soit $n \in \mathbb{N}$. Montrer que $\Gamma_n \in \mathscr{P}(\mathbb{Z}, \mathbb{Z})$ (on pourra discuter suivant les cas $0 \leqslant k < n$, $k \geqslant n$ et $k < 0$).

b) Montrer que pour tout entier naturel m, la famille $(\Gamma_n)_{0 \leqslant n \leqslant m}$ forme une base de l'espace vectoriel des polynômes de $\mathbb{R}[X]$ de degré au plus m.

2) Soit $P \in \mathbb{R}[X]$ de degré au plus m. Montrer que $P \in \mathscr{P}(\mathbb{Z}, \mathbb{Z})$ si et seulement s'il existe $m + 1$ entiers consécutifs en lesquels les valeurs de P sont des entiers.

Exercice n°21

Soit p un nombre premier et $P = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ un polynôme de degré $n \geqslant 1$ à coefficients entiers tel que a_n n'est pas divisible par p, montrer que parmi les nombres $\{0, 1, 2, \ldots, p-1\}$, il n'existe pas plus de n nombres x pour lesquels $P(x)$ soit divisible par p.
Montrer par un contre exemple, que ce résultat n'est plus vrai si p n'est pas premier.

Exercice n°22

1) Quel est le reste dans la division euclidienne de $X^{19} + 4X^{16} + 3X^5 + X + 1$ par $X^2 + X + 1$ dans $\mathbb{R}[X]$?

2) Montrer que si trois polynômes P, Q, R de $\mathbb{R}[X]$ vérifient la relation $P^2 - XQ^2 = XR^2$, ils sont nuls. Est-ce encore vrai dans $\mathbb{C}[X]$?

Exercice n°23

1) Soit un polynôme A de $\mathbb{R}[X]$ non constant, dont tous les coefficients sont entiers. On suppose que le rationnel $\frac{p}{q}$ (où p et q sont deux entiers premiers entre eux) est une racine de A. Montrer que p divise le coefficient constant de A et q divise le coefficient dominant de A.

2) Factoriser le polynôme : $2X^3 - X^2 - 13X + 5$. Le polynôme $X^3 + 3X - 1$ admet il une racine rationnelle ?

3) Montrer que le réel $a = \cos(\pi/9)$ est racine d'un polynôme à coefficients entiers de degré trois et en déduire que ce nombre a est un irrationnel.