Corrigé de l'Examen de Rattrapage du Module Algèbre 1

Exercice 1.

1. Montrer que 2 est un élément primitif modulo 19.

2. Déterminer l'entier $k < 18$ tel que $2^k \equiv 7$ modulo 19.

3. Déterminer suivant les valeurs de l'entier n le reste de la division euclidienne de 7^n par 19.

4. Soit n un entier naturel non divisible par 3. Montrer que $19 \mid 7^n + 7^{2n} + 7^{3n}$.

5. Calculer l'inverse de 7 modulo 19.

6. Résoudre dans $\mathbb{Z}^2$ l'équation (E) $7x + 38y = 2$.

Solution de l'exercice 1.

1. Il faut montrer que l'ordre multiplicatif de 2 modulo 19 est égal à $19 - 1 = 18$.
Modulo 19 on a, $2^5 \equiv 13$, $2^6 \equiv 7$, $2^7 \equiv 14$, $2^8 \equiv 9, 2^9 \equiv 18 \equiv -1$.
Par conséquent $\text{ord}_{19}(2) > 9$. Or $\text{ord}_{19}(2) \mid 19 - 1 = 18$. Donc $\text{ord}_{19}(2) = 18$.

2. D'après les calculs précédents, on a $k = 6$.

3. On a $7 = (2^6)$. Donc l'ordre de 7 modulo 19 est 3. On pose alors $n = 3m + r$ avec $r = 0, 1, 2$
Si $n \equiv 0$ modulo 3, on a $r = 0$ et $7^n = (7^3)^m \equiv 1$ modulo 19.
Si $n \equiv 1$ modulo 3, on a $r = 1$ et $7^n = (7^3)^m \times 7 \equiv 7$ modulo 19.
Si $n \equiv 2$ modulo 3, on a $r = 2$ et $7^n = (7^3)^m \times 7^2 \equiv 49 \equiv 11$ modulo 19.

4. Posons $u_n = 7^n + 7^{2n} + 7^{3n}$. Alors $u_n = 7^n + (7^n)^2 + (7^n)^3$.
Si $n \equiv 1$ modulo 3, on a $u_n \equiv 7 + 7^2 + 7^3 \equiv 7 + 49 + 1 \equiv 57 \equiv 0$ modulo 19.
Si $n \equiv 2$ modulo 3, on a $u_n \equiv 11 + 11^2 + 11^3 \equiv 11 + 121 + 1 \equiv 0$ modulo 19.

5. On utilise l'algorithme d'Euclide ou toute autre méthode, on obtient $7 \times 11 = 4 \times 19 + 1$. Donc l'inverse de 7 modulo 19 est égal à11.

6. Soit à résoudre l'équation (E) $7x + 38y = 2$ dans $\mathbb{Z}^2$. Comme on a $(7 \times 11) - (19 \times 4) = 1$, en multipliant par 2, on obtient $(7 \times 22) - (38 \times 4) = 2$. D'où la solution particulière $(22, -4)$. Et la solution générale est $(22 - 38k, 7k - 4)$, $k \in \mathbb{Z}$.

Exercice 2. Pour tout $n \in \mathbb{N}^*$ on note $E_n = \{x \in \mathbb{N} \,|\, x \leq n - 1\} = \{0, 1 \ldots, n - 1\}$. Soit a un entier naturel premier avec n. On définit sur E_n la relation binaire $\mathcal{R}$ par :

$$\forall x, y \in E_n,\ x\mathcal{R}y \Leftrightarrow \exists k \in \mathbb{N} : a^k x \equiv y \text{ modulo } n$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.

2. On prend $n = 15$, $a = 2$. Déterminer toutes les classes d'équivalence modulo $\mathcal{R}$.

Solution de l'exercice 2.

1. Refexivité : $\forall x \in E_n, x = a^0 x$ donc $x\mathcal{R}x$.
Symétrie : Soient $x, y \in E_n$ tels que $x\mathcal{R}y$, alors $\exists k \in \mathbb{N} : y \equiv a^k x$. Comme a est inversible modulo n, on a d'après le théorème d'Euler $(a^k)^{\phi(n)} \equiv 1$, où $\phi(n)$ est l'indicatrice d'Euler. Donc $(a^k)^{\phi(n)-1} \cdot a^k \equiv (a^k)^{\phi(n)} \equiv 1$. D'où $(a^k)^{\phi(n)-1} \cdot y \equiv x$, d'où $y\mathcal{R}x$.

Transitivité : Soient $x, y, z \in E_n$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors il existe $k, m \in \mathbb{N}$ tels que : $y \equiv a^k x$, $z \equiv a^m y$. Donc on a $z \equiv a^{k+m} x$. D'où $x\mathcal{R}z$

2.

La classe de 0 est $\{0\}$.

La classe de 1 est $\{1, 2, 4, 8, \}$.

La classe de 3 est $\{3, 6, 13, 9\}$.

La classe de 5 est $\{5, 10\}$.

La classe de 7 est $\{7, 14, 13, 11\}$.

Exercice 3.

1. Soient $a, b, n \in \mathbb{N}^*$. Montrer que $a^n \mid b^n \Rightarrow a \mid b$.

2. Soit $x \in \mathbb{Q}$, on suppose qu'il existe un entier naturel n tel que $x^n \in \mathbb{Z}$. Montrer que $x \in \mathbb{Z}$.

3. On considère l'équation algébrique d'inconnue $x \in \mathbb{C}$,

$$(*)\ x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

où les $a_k \in \mathbb{Z}$. Montrer que si $x \in \mathbb{Q}$ est solution de cette équation, alors $x \in \mathbb{Z}$ et $x \mid a_0$.

Solution de l'exercice 3.

1. Posons $a \wedge b = d$ le PGCD de a et b. Alors $a = a'd, b = b'd$, et $a' \wedge b' = 1$. Supposons que $a^n \mid b^n$, alors il existe $k \in \mathbb{N}$ tel que $b^n = b'^n d^n = a^n = ka'^n d^n$, donc $b'^n = ka'^n$ et par suite $a'^n \mid b'^n$. Or $a' \wedge b' = 1$, donc $a'^n \wedge b'^n = 1$. Par conséquent $a'^n = 1$ d'où $a' = 1$ et $a = d$ c'est à dire $a \mid b$.

2. Posons $x = \frac{b}{a}$. On a par hypothèse $x^n = \frac{b^n}{a^n} \in \mathbb{Z}$. Par suite $a^n \mid b^n$. ce qui implique d'après 1 que $a \mid b$, d'où $x \in \mathbb{Z}$.

3. Posons $x = \frac{p}{q}$, avec $q \in \mathbb{N}^*$ et $p \wedge q = 1$. L'équation algébrique $(*)$ donne :

$$p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1 pq^{n-1} + a_0 q^n = 0$$

Donc

$$-p^n = a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \ldots + a_1 pq^{n-1} + a_0 q^n$$

$$-p^n = q(a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + \ldots + a_1 pq^{n-2} + a_0 q^{n-1})$$

Donc $q \mid p^n$, or $p \wedge q = 1$, donc $q = 1$, ce qui implique que $x \in \mathbb{Z}$.

D'autre part $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x = -a_0$. Donc $x \mid a_0$