Approfondissement

Solutions

Exercice 1.

1. Quel est le reste de la division euclidienne de 2^8 par 17 ?

   Solution : $2^8 = 17 \times 15 + 1$, donc $2^8 \equiv 1 \mod 17$.

2. En déduire le reste de la division euclidienne de $n = 19^{73}$ par 17.

   Solution : $19^{73} \equiv 2^{73} \equiv 2^{9\times 8+1} \equiv (2^9)^8 \times 2 \equiv 2 \mod 17$.

3. L'entier 323 est-il premier ?

   Solution : En faisant la division de 323 avec tout nombre premier p inférieur à $\sqrt{323} < \sqrt{324} = 18$ on obtient $323 = 17 \times 19$, donc 323 n'est pas premier.

4. Pour tout nombre premier p, calculer la valuation p-adique de 594.

   Solution : $\sqrt{594} = 2 \times 3^3 \times 11$, donc :
   $v_2(594) = 1, \quad v_3(594) = 3, \quad v_{11}(594) = 1, \quad v_p(594) = 0$ pour tout autre p premier.

5. Déterminer l'écriture de 55 en base 2.

   Solution : $\sqrt{55} = 2^5 + 2^4 + 2^2 + 2 + 1$, donc l'écriture de 55 en base 2 : 110111.

6. Calculer 6^{55} modulo 61.

   Solution : $6^2 \equiv 36, \quad 6^4 = (6^2)^2 \equiv 15, \quad 6^8 \equiv 15^2 = -19 \mod 61$
   $6^{16} \equiv (-19)^2 = -5, \quad 6^{32} = (-5)^2 \equiv 25 \mod 61$
   $6^{55} \equiv 6^{2^5} \times 6^{2^4} \times 6^{2^2} \times 6^2 \times 6 \equiv 40 \mod 61$

Exercice 2. Soit $a = 308$ et $b = 202$.

1. Quel est le plus grand commun diviseur d de a et b ?
2. Déterminer deux entiers u et v tels que l'on ait $au + bv = d$.
3. Expliciter l'ensemble des couples $(x, y) \in \mathbb{Z}^2$ tels que l'on ait $ax + by = d$.

Exercice 3. Notons G le groupe additif $(\mathbb{Z}/18\mathbb{Z}, +)$.

1. Quels sont les ordres possibles des éléments de G ?

   Solution : Les ordres possibles sont les diviseurs positifs de 18 : $1, 2, 9, 18$.

2. Quel est le nombre de sous-groupes de G ?

   Solution : Conformément au Théorème 2.4 du cours, le nombre des sous-groupes de G est le nombre de diviseurs positifs de 18, donc il y en a 4.

3. Quel est le nombre de générateurs de G ?

   Solution : Les classes des éléments premiers avec 18 sont des générateurs de G, il y en a $\varphi(18) = 6$.

4. Expliciter l'ensemble des générateurs de G.

   Solution : Les classes des éléments premiers avec 18 : $\{1, 5, 7, 11, 13, 17\}$.

5. Le groupe produit $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, +)$ est-il isomorphe à G ?

Exercice 4. Soit $G = (\mathbb{Z}/12\mathbb{Z})^\times$ et p un nombre premier ≥ 5. Notons $f : G \to G$ l'application définie pour tout $x \in G$ par l'égalité $f(x) = x^p$.

1. Montrer que f est un homomorphisme de groupes.
2. Montrer que f est un automorphisme de groupes.

Exercice 5. Soit G le groupe des éléments inversibles de l'anneau $(\mathbb{Z}/21\mathbb{Z}, +, \times)$.

1. Quel est son ordre ? Expliciter ses éléments.
2. Quel est l'ordre de la classe de 2 dans G ?
3. Le groupe G est-il cyclique ?
4. Résoudre dans G l'équation $x^2 = 1$, ainsi que l'équation $y^3 = 1$.