

TD d'arithmétique 2022:

1. Divisions euclidiennes et congruences:

- (a) Quels sont le quotient q et le reste r de la division euclidienne de 513 par 25? Déduisez-en le plus petit entier positif n tel que $513 \equiv x \pmod{25}$
- (b) Quels sont le quotient q et le reste r de la division euclidienne de -513 par 25? Déduisez-en le plus petit entier positif n tel que $-513 \equiv x \pmod{25}$
- (c) Quels sont le quotient q et le reste r de la division euclidienne de 768 par 29? Déduisez-en le plus petit entier positif n tel que $768 \equiv x \pmod{29}$
- (d) Quels sont le quotient q et le reste r de la division euclidienne de -768 par 29? Déduisez-en le plus petit entier positif n tel que $-768 \equiv x \pmod{29}$

2. Démontrez les congruences suivantes:

- (a) $149 \equiv 19 \pmod{13}$
- (b) $-111 \equiv 19 \pmod{13}$

3. Etude $\mathbb{Z}/n\mathbb{Z}$ pour $n = 4$:

- (a) Dressez les tables de pythagore pour l'addition et la multiplication de $\mathbb{Z}/n\mathbb{Z}$.
- (b) Etude de $(\mathbb{Z}/n\mathbb{Z})^*$ (l'ensemble des éléments inversibles pour la multiplication de $\mathbb{Z}/n\mathbb{Z}$):
 - i. Donnez en extension $(\mathbb{Z}/n\mathbb{Z})^*$.
 - ii. On note $\varphi(n)$ le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$. Montrez par le calcul que pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$ on a $a^{\varphi(n)} \equiv 1(n)$.
 - iii. Pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$ on note $\langle a \rangle$ l'ensemble des puissances entières positives de a dans $\mathbb{Z}/n\mathbb{Z}$ (i.e. $\langle a \rangle = \{a^k(n), k \in \mathbb{N}\}$). Montrez par le calcul que le cardinal de $\langle a \rangle$ divise $\varphi(n)$ pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$.
- (c) Résolvez l'équation $x^2 = 0(n)$ dans $\mathbb{Z}/n\mathbb{Z}$.
- (d) Résolvez l'équation $3x + 2 = 3(n)$ dans $\mathbb{Z}/n\mathbb{Z}$.
- (e) Reprenez les questions précédentes pour $n = 5$ puis pour $n = 6$.

4. Calculez dans $\mathbb{Z}/7\mathbb{Z}$ (vous donnerez pour chaque calcul le plus petit entier positif représentant une solution):

- (a) $129 + 48(7)$
- (b) $1825 \times 286 \times 37(7)$
- (c) $4^4(7)$
- (d) $1927^{18}(7)$

5. On veut déterminer l'entier $x \in \{0, 1, 2, \dots, 10\}$ tel que $123^{1928} \equiv x \pmod{11}$

- (a) Montrez que $123 \equiv 2 \pmod{11}$
- (b) Complétez le tableau des congruences des puissances de 2 modulo 11 suivant:

ce nombre	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
est congru (modulo 11) à											

- (c) Déduisez-en un entier $y \in \{0, 1, 2, \dots, 10\}$ que $2^{1928} \equiv y \pmod{11}$.
- (d) Trouvez l'entier x .
- (e) En vous inspirant de la méthode précédente trouvez l'entier $z \in \{0, 1, 2, \dots, 6\}$ tel que $123^{1928} \equiv z \pmod{7}$

6. On veut déterminer le chiffre des unités de 7^{98} dans son écriture en base 10:

- (a) Vérifiez que $7^4 \equiv 1 \pmod{10}$
- (b) Conclusion?

7. Vrai ou Faux?

- (a) Si $a \times b \equiv 0 \pmod{6}$ alors $a \equiv 0 \pmod{6}$ ou $b \equiv 0 \pmod{6}$?
- (b) Si $2x \equiv 4 \pmod{12}$ alors $x \equiv 2 \pmod{12}$?
- (c) Si $2x \equiv 4 \pmod{12}$ alors $x \equiv 2 \pmod{6}$?

- (d) Si $7 - x \equiv 5 \pmod{3}$ alors $x \equiv 2 \pmod{3}$?
 (e) $\forall x \in \mathbb{Z}, x^5 \equiv x \pmod{4}$?

8. Nombres de diviseurs d'un entier.

- (a) Soit un entier naturel $a = 2^3 \times 3^4 \times 5^2$. Déterminez le nombre de diviseurs de a .
 (b) Généralisation : Soit a un entier naturel dont la décomposition en facteurs premiers est la suivante: $a = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$. Déterminez le nombre de diviseurs de a .
 (c) Déterminez le nombre de diviseurs de 1000, puis de 7325.

9. Algorithme d'Euclide:

Utilisez l'algorithme d'Euclide "à la main" pour calculer les pgcd suivants:

- (a) $43 \wedge 16$
 (b) $204 \wedge 156$
 (c) $3791 \wedge 1717$
 (d) $44231 \wedge 2750$

10. Divisibilité et décomposition en produits de facteurs premiers :

- (a) On considère les entiers suivants:

$$a = 2^3 \times 3^4 \times 5^2 \times 7^2$$

$$b = 3^2 \times 5 \times 7$$

$$c = 2^3 \times 3^4 \times 11$$

$$d = 2^2 \times 3^4 \times 5^2 \times 7$$

Sans aucun calcul, déterminez les entiers (parmi a,b,c et d) qui divisent a .

- (b) Soient a et b deux entiers. On suppose que b divise a . Que peut-on dire de la décomposition en produits de facteurs premiers de b par rapport à celle de a ? La réciproque est-elle vraie?

11. PGCD et décomposition en produits de facteurs premiers:

- (a) On considère deux nombres entiers a et b dont les décompositions en produits de facteurs premiers sont données par:

$$a = 2^3 \times 3^4 \times 5^2 \times 7$$

$$b = 2 \times 3^5 \times 5^4$$

Donnez la décomposition en produit de facteurs premiers de $a \wedge b$.

- (b) Généralisation: Comment obtenir la décomposition de $a \wedge b$ (a et b deux entiers quelconques) à partir de la décomposition de a et b .

12. Décomposez les nombres suivants en produits de facteurs premiers:

(vous pouvez vous aider de la liste suivante:

Liste des nombres premiers ≤ 100 : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97).

- (a) 111
 (b) 137
 (c) 1025
 (d) 1111
 (e) 5678
 (f) 6788

13. **Euclide-Etendu:**

Donnez une trace de l'algorithme d'Euclide-étendu pour les entrées suivantes et déterminez $a \wedge b$ ainsi que deux entiers u et v tels que $au + bv = a \wedge b$ (identité de Bézout):

- (a) $a = 25; b = 17$
- (b) $a = 48; b = 15$
- (c) $a = 133; b = 72$
- (d) $a = 365; b = 127$

14. **Exponentiation modulaire:**

Calculez les puissances suivantes en utilisant l'algorithme d'exponentiation modulaire:

- (a) $2^{100} (11)$
- (b) $7^{45} (13)$

15. Déterminez les inverses de chacun des éléments de $(\mathbb{Z}/7\mathbb{Z})^*$.

16. On considère $(\mathbb{Z}/16\mathbb{Z})^*$:

- (a) Combien y a-t-il d'éléments dans $(\mathbb{Z}/16\mathbb{Z})^*$?
- (b) Vérifiez que 7 est dans $(\mathbb{Z}/16\mathbb{Z})^*$ et déterminez son inverse.

17. On considère deux nombres entiers distincts p_1 et p_2 et on pose $n = p_1 \times p_2$.

- (a) Donnez $\varphi(p_1)$ en fonction de p_1 .
- (b) Donnez $\varphi(n)$ en fonction de p_1 et p_2 .

18. On considère $(\mathbb{Z}/65\mathbb{Z})^*$:

- (a) Combien y a-t-il d'éléments dans $(\mathbb{Z}/65\mathbb{Z})^*$?
- (b) Vérifiez que 12 est dans $(\mathbb{Z}/65\mathbb{Z})^*$ et déterminez son inverse.

19. On considère la fonction caractéristique d'Euler φ . Calculez:

- (a) $\varphi(3)$
- (b) $\varphi(4)$
- (c) $\varphi(5)$
- (d) $\varphi(6)$
- (e) $\varphi(7)$
- (f) $\varphi(8)$
- (g) $\varphi(35)$
- (h) $\varphi(77)$

20. Déterminez $\langle 5 \rangle$ (l'ensemble de toutes les puissances entières de 5 dans $\mathbb{Z}/13\mathbb{Z}$) et vérifiez que $|\langle 5 \rangle|$ divise $\varphi(13)$.

21. On considère l'ensemble $(\mathbb{Z}/11\mathbb{Z})^*$:

- (a) Déterminez $\varphi(11)$.
- (b) Donnez en extension $(\mathbb{Z}/11\mathbb{Z})^*$.
- (c) Déterminez en extension l'ensemble $A = \{x \in (\mathbb{Z}/11\mathbb{Z})^*, \exists y \in (\mathbb{Z}/11\mathbb{Z})^* \text{ tel que } x \equiv y^2(11)\}$ (c'est à dire le sous-ensemble des carrés de $(\mathbb{Z}/11\mathbb{Z})^*$).
- (d) Pour chacun des éléments x de A déterminez son ordre $\omega(x)$.