TD1 : Arithmétique des entiers

M1 MIC – Algèbre

19 septembre 2024

Exercice 1. Combien de diviseurs le nombre 1 000 000 possède-t-il ?

Exercice 2. Échauffements.

(a) Quel est le dernier chiffre de 7777^{7777} ?

(b) Quel est le reste de la division euclidienne de 900^{200} par 13 ?

(c) Déterminer $101^{102^{103}} \bmod 13$, $31^{32^{33}} \bmod 7$, et $100^{100^{100}} \bmod 12$.

Exercice 3. Résoudre les équations diophantiennes suivantes.

(a) $3x + 7y = 4$;

(b) $189x + 255y = 3$;

(c) $12x + 51y = 7$;

(d) $43x - 11y = 10$;

(e) $xy = 2x + 3y$;

(f) $x^2 - y^2 - x + 3y = 30$;

(g) $x^2 - 5y^2 = 3$.

Exercice 4. Résoudre les congruences suivantes :

(a) $2x \equiv 1 \pmod 7$;

(b) $5x \equiv -1 \pmod 8$;

(c) $171x \equiv 7 \pmod{212}$;

(d) $68x \equiv 100 \pmod{120}$.

Exercice 5. Résoudre les systèmes de congruences suivants :

(a) $\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod{11} \end{cases}$
(b) $\begin{cases} x \equiv 4 \pmod{21} \\ x \equiv 10 \pmod{33} \end{cases}$
(c) $\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod 6 \end{cases}$

Exercice 6. Déterminer la périodicité de la fonction g définie par $g : \mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}, \quad g(n) := 5^n + n$.
Trouver toutes les solutions de l'équation $g(n) = 0$. Une solution sans calcul fastidieux sera appréciée !

Exercice 7. Démontrer que pour tout $n \in \mathbb{N}$, $2^{3n+5} + 3^{n+1}$ est un multiple de 5.

Exercice 8. Démontrer que pour tout $n \in \mathbb{Z}$, $n^5 - n$ est un multiple de 30.

Exercice 9. Soit n un entier fixé. Démontrer que $\forall a \in \mathbb{N},\ a^n - a \equiv 0 \pmod n$ si et seulement si n est sans facteur carré et si $p - 1$ divise $n - 1$ pour tout facteur premier p de n.

Exercice 10. Déterminer les $n \in \mathbb{N}$ tels que $n + 1$ divise $n^2 + 1$.

Exercice 11. Soient $a, b \in \mathbb{N}$ premiers entre eux. Démontrer que ab est un carré parfait si et seulement si a et b le sont. Si $n \in \mathbb{N}$, quand est-ce que $n(n + 1)$ est un carré parfait ?

Exercice 12. Soit $n \geq 1$ un entier. Démontrer que $a \wedge b = 1$ si et seulement si $a^n \wedge b^n = 1$.

Exercice 13. Démontrer que $a \wedge b = 1$ si et seulement si $(a + b) \wedge (ab) = 1$.

Exercice 14. (Équation diophantienne.) On considère l'équation $y(y - 1) = x^2$, avec $x, y \in \mathbb{Z}$.

(a) Démontrer que si l'équation est vérifiée alors y et $y - 1$ sont des carrés parfaits (à inversibles près).

(b) En déduire que l'équation n'admet que deux solutions que l'on déterminera.

Exercice 15. Démontrer qu'il existe des suites d'entiers consécutifs non premiers de longueur arbitraire. (Indication : $n! + 2$, $n! + 3$, $n! + 4$, etc.)

Exercice 16. Soit $n \geq 2$ un entier.

(a) Si n n'est pas premier, démontrer que n possède un facteur premier $\leq \sqrt{n}$.

(b) En déduire que si $10 \leq n \leq 100$, alors n est premier si et seulement s'il est premier avec 210.

Exercice 17. (Crible d'Ératosthène.) Pour déterminer les nombres premiers inférieurs ou égaux à un entier $n \geq 2$ fixé, on applique l'algorithme suivant. On liste tous les entiers compris entre 2 et n. Tant qu'il reste dans cette liste qui ne sont ni barrés, ni entourés, on applique l'opération suivante : on entoure le premier entier qui reste, puis on barre tous ses multiples dans la liste.

(a) Appliquer l'algorithme pour $n = 20$ et vérifier qu'on retrouve bien les nombres premiers ≤ 20.

(b) Démontrer que l'algorithme produit bien la liste des nombres premiers $\leq n$.

(c) Démontrer qu'on ne barre plus d'entiers si ceux qui restent sont $> \sqrt{n}$.

(d) En déduire un algorithme de complexité temporelle $O(n)$ pour lister les premiers $\leq n$.

Exercice 18. Nombres de Mersenne.

(a) Soient $a \geq 2$ et $n \geq 2$ des entiers. Démontrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier.

Les nombres de cette forme sont appelés les nombres de Mersenne et sont notés $M_n = 2^n - 1$.

(b) Est-ce que M_2, M_3, M_5, M_7 et M_{11} sont premiers ?

(c) Soit p premier, $p \equiv 3 \pmod 4$. Démontrer que $2p + 1$ est premier si et seulement si $2^p \equiv 1 \pmod{2p+1}$.

(d) En déduire que M_{11}, M_{23}, M_{83} et M_{131} ne sont pas premiers.

Exercice 19. Soit $a \geq 2$ un entier.

(a) Démontrer que pour tout $n \geq 2$, $a - 1$ divise $a^n - 1$.

(b) Démontrer que si $\frac{(a^n-1)}{(a-1)}$ est premier, alors n est premier.

(c) La réciproque est-elle vraie ?

Exercice 20. (Théorème de Wilson.) Démontrer que $p \geq 2$ est premier si et seulement si $(p - 1)! \equiv -1 \pmod p$.

Exercice 21. En quoi l'indicatrice d'Euler φ permet-elle de généraliser le petit théorème de Fermat ?

Exercice 22. (Chiffrement RSA.) Alice veut envoyer à Bob un message privé sur un réseau public. Bob choisit deux nombres premiers $p \neq q$ et note $n = pq$, $\lambda = (p - 1) \vee (q - 1)$. Il détermine un entier e premier avec λ. Il calcule un entier d tel que $de \equiv 1 \pmod \lambda$. Il dévoile sa clé publique (n, e) et garde secrète sa clé privée d.

Le message d'Alice pour Bob est une suite d'entiers naturels $M < n$. Elle calcule le message chiffré $M' = M^e \pmod n$ qu'elle envoie à Bob. Pour déchiffrer le message, Bob calcule $M'' = (M')^d \pmod n$.

(a) Est-ce que Bob a correctement déchiffré le message d'Alice ?

Ève a écouté l'échange ! Elle sait que la clé publique de Bob est $(n, e) = (851,\ 5)$ et qu'Alice a envoyé le message chiffré suivant à Bob : $(2,\ 333,\ 739,\ 797,\ 333,\ 561,\ 206)$.

(b) Est-ce qu'Ève est en mesure de déchiffrer le message ? Que lui manque-t-il ?

(c) D'où vient la difficulté de reconstituer la clé privée à partir de la clé publique ?

Exercice 23. Calculer les symboles de Legendre suivants :

(a) $\left(\frac{-1}{17}\right)$, (c) $\left(\frac{13}{17}\right)$, (e) $\left(\frac{-8}{23}\right)$.

(b) $\left(\frac{2}{29}\right)$, (d) $\left(\frac{7}{19}\right)$,

Exercice 24. (a) Est-ce que 1475 est un résidu quadratique modulo 2389 (qui est premier) ?

(b) Soit $n \in \mathbb{N}$ tel que $p = 4n + 3$ et $q = 2n + 1$ sont premiers. Quand est-ce que 3 est une racine primitive de l'unité modulo p ?

Exercice 25. Déterminer les nombres premiers p tels que 6 soit un résidu quadratique mod p.

Exercice 26. Étant donné un premier p, on s'intéresse au cardinal N_p de la courbe $\mathcal{C} = \{(x,y) \in \mathbb{Z}/p\mathbb{Z} \mid y^2 = x^3 - x\}$.

(a) Démontrer que l'on a la formule :

$$N_p = p + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{x^3 - x}{p}\right).$$

(b) Calculer N_7. Généraliser le calcul aux nombres premiers p tels que $p \equiv 3 \pmod 4$.

Exercice 27. Soit p un nombre premier impair.

(a) Démontrer que la fonction suivante est une bijection :

$$\mathbb{Z}/p\mathbb{Z} \setminus \{1\} \to \mathbb{Z}/p\mathbb{Z} \setminus \{-1\}, \quad x \mapsto \frac{1+x}{1-x}.$$

(b) En déduire que l'égalité suivante est vraie :

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{1-x^2}{p}\right) = (-1)^{(p+1)/2}.$$

(c) Quel est le nombre de points du cercle unité ($x^2 + y^2 = 1$) modulo p ?

Exercice 28. (Test de Solovay–Strassen) Soit $n \geq 3$ un entier impair. On définit :

$$G_n = \left\{ a \in \mathbb{Z}/n\mathbb{Z} \mid 0 \neq \left(\frac{a}{n}\right) = a^{(n-1)/2} \pmod n \right\}.$$

(a) Démontrer que G_n est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z})^\times$.

(b) Si n est premier, quel est ce sous-groupe ?

(c) Démontrer que la réciproque est vraie.

(d) Lorsque n n'est pas premier, démontrer que $|G_n| < \frac{(n-1)}{2}$.

Exercice 29. Calculer le symbole de Jacobi $\left(\frac{610}{983}\right)$. Sachant que $610^{491} \equiv 1 \pmod{983}$, est-ce que le test de Solovay–Strassen pour le témoin 610 permet de dire si 983 est premier ?