

Arithmétique, algèbre modulaire, groupes cycliques

- le fait que $a \wedge b = (a - bq) \wedge b$ pour tout $q \in \mathbb{Z}$ permet parfois des simplifications intéressantes.
- Lorsque l'on manipule des équations avec pgcd et/ou ppcm, il est souvent intéressant de se ramener à des nombres premiers entre eux en posant $x = dx'$ et $y = dy'$ où $d = x \wedge y$.
- Savoir que $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier (et seulement dans ce cas). Cela permet de faire des calculs « un peu comme dans \mathbb{R} ou \mathbb{C} ... ». Si n n'est pas premier, savoir trouver les inversibles de $\mathbb{Z}/n\mathbb{Z}$ (cours) et savoir que les autres sont des diviseurs de 0.
- Pour savoir si des nombres sont premiers entre eux, on peut penser au théorème de Bézout ou revenir à la définition (les diviseurs communs sont triviaux). Penser aussi aux nombres premiers : pas de diviseur premier en commun.
- Pour des problèmes de divisibilité, penser à travailler avec des congruences. On peut aussi travailler dans $\mathbb{Z}/n\mathbb{Z}$.
- Tous les nombres premiers sont impairs... sauf 2, le seul pair. Penser à ce cas particulier. Et 1 n'est pas premier.
- En algèbre modulaire, on ne manipule jamais de grande valeur : penser à réduire systématiquement pour se ramener dans $\llbracket 0, n-1 \rrbracket$ (voire $\llbracket \frac{-n}{2}, \frac{n}{2} \rrbracket \dots$)
- Savoir résoudre des systèmes de congruences : avec des modulus premiers entre eux, c'est le théorème chinois...
- Un exercice sur les groupes cycliques est souvent plus facile à résoudre en pensant à (\mathbb{U}_n, \times) qu'à $(\mathbb{Z}/n\mathbb{Z}, +)$.

1 CCINP 66 2 CCINP 86 - Petit théo³ 3 CCINP 94 rème de Fermat

4 À savoir faire absolument Résoudre, dans \mathbb{Z} , $3x + 11y = 2$ puis $14x + 35y = 5$ et $14x + 35y = 7$.

- 5
- Pour quelles valeurs de n a-t-on $(n^3 + n) \wedge (2n + 1) = 1$?
 - Pour quelles valeurs de $n \in \mathbb{Z}$ a-t-on $(n + 2) \mid (2n^2 + 9n + 13)$?
 - Montrer que pour tout $n \in \mathbb{Z}$, $(21n + 4) \wedge (14n + 3) = 1$.

6 Nombres de Mersenne¹ - Très classique - Oral Centrale

Montrer que si $a \in \mathbb{N}$, $n \in \mathbb{N} \setminus \{0, 1\}$ tel que $a^n - 1$ est premier, alors $a = 2$ et n est premier.

7 Nombres de Fermat³ - Très classique - Oral Mines

- Soient $a, n \in \mathbb{N}^*$, $a \geq 2$. Montrer que si $a^n + 1$ est premier, a est pair et n est une puissance de 2. On appelle nombres de Fermat les nombres $F_n = 2^{2^n} + 1$. Ils sont premiers pour n de 2 à 4, mais ne le sont pas pour n de 5 à 32 (contrairement à ce que conjectura Fermat).
- Démonstration de 1734 d'Euler du fait que F_5 n'est pas premier.
 - Comparer $5^4 + 2^4$ et $1 + 5 \times 2^7$ (sans calculatrice!).
 - En déduire que $5^4 \times 2^{28} \equiv 1 \pmod{641}$.
 - Conclure que 641 divise F_5 .
- Montrer que pour tout $n \in \mathbb{N}$, $F_{n+1} = (F_n - 1)^2 + 1$ et en déduire que F_n et F_{n+1} sont premiers entre eux.
- Pour $n \in \mathbb{N}$, établir que $F_{n+1} = \prod_{k=0}^n F_k + 2$. En déduire que les F_n sont premiers entre eux deux à deux. Retrouver le fait que le nombre de nombres premiers est infini.

1. Un tel nombre est alors appelé nombre de Mersenne (mathématicien français 1588-1648). La réciproque est fautive ($2^{11} - 1 = 23 \times 89$). Les plus grands nombres premiers connus actuellement sont des nombres de Mersenne : $2^{77} - 1$ (23 249 425 chiffres en base décimale).

3. Ils interviennent dans la constructibilité à la règle et au compas des polygones réguliers.

8 En s'inspirant de la démonstration sur l'infinité des nombres premiers, montrer qu'il existe une infinité de nombres premiers de la forme $4k - 1$ ⁵.

9 Justifier l'existence de 1000 entiers consécutifs sans nombre premier.

10 Formule de Legendre - Très classique - Oraux divers

Combien y a-t-il de zéros à la fin de 100!? De 1000!? De 2021!?

Montrer que $v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ pour p premier et $n \in \mathbb{N}^*$.

11 On note p_n le n^{e} nombre premier et $\pi(x)$ le nombre de nombres premiers $\leq x$.

- Montrer que pour tout $n \geq 1$, $p_{n+1} \leq p_1 \cdots p_n + 1$.
- Montrer que pour tout $n \geq 1$, $2n - 1 \leq p_n \leq 2^{2^{n-1}}$.
- Justifier⁶ que $\forall x > 0$, $\ln(\ln x) < \pi(x) < x$.

12 En utilisant l'algorithme d'Euclide, montrer que pour tout $n, m \in \mathbb{N}$, $(2^n - 1) \wedge (2^m - 1) = 2^{n \wedge m} - 1$.

13 Oral Centrale Déterminer le chiffre des unités de 1587^{413} .

14 Soit $n = 4444^{4444}$. Calculer la somme des chiffres de la somme des chiffres de la somme des chiffres de n .

15 Oral Mines

Soit $p \geq 5$ un nombre premier. Montrer que 24 divise $p^2 - 1$.

16 Montrer que pour tout $n \in \mathbb{N}$

- | | | |
|--------------------------------|--------------------------------------|---------------------------------|
| 1. $6 \mid 5n^3 + n$ | 3. $5 \mid 2^{2n+1} + 3^{2n+1}$ | 5. $9 \mid 4^n - 1 - 3n$ |
| 2. $7 \mid 3^{2n+1} + 2^{n+2}$ | 4. $11 \mid 3^{8n} 5^4 + 5^{6n} 7^3$ | 6. $15^2 \mid 16^n - 1 - 15n$. |

17 Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui-ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces. Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

18 Résoudre $\begin{cases} x + 5y = 8 \\ 3x + 7y = 9 \end{cases}$ dans $\mathbb{Z}/13\mathbb{Z}$.

5. Le théorème de Dirichlet (difficile) affirme qu'il existe une infinité de nombres premiers congrus à a modulo b si a et b sont premiers entre eux.

6. Le (difficile) théorème de Hadamard et De La Vallée-Poussin dit « Théorème des Nombres Premiers » affirme que $\pi(x) \sim \frac{x}{\ln x}$, ou, de manière équivalente, $p_n \sim n \ln n$.

19 Déterminer les carrés, et les sommes de 2 ou 3 carrés dans $\mathbb{Z}/8\mathbb{Z}$.

En déduire que si $n \in \mathbb{N}$ est de la forme $8k-1$, il ne peut pas s'écrire comme somme de trois carrés d'entiers.

20 Carrés dans $\mathbb{Z}/p\mathbb{Z}$

1. Faire la liste des éléments de $\mathbb{Z}/17\mathbb{Z}$ qui sont des carrés. Combien y-en-a-t-il ?
2. Soit p un nombre premier impair. On note A l'ensemble des carrés dans $\mathbb{Z}/p\mathbb{Z}$: $x \in A \iff \exists y \in \mathbb{Z}/p\mathbb{Z}, x = y^2$.
 - (a) Déterminer le nombre d'éléments de A .
 - (b) Démontrer que, si a est un élément non nul de A , $x \mapsto xa$ est une bijection de A sur lui-même.
 - (c) Démontrer que, si a est un élément de $\mathbb{Z}/p\mathbb{Z} \setminus A$, $x \mapsto xa$ est une bijection de $A \setminus \{0\}$ sur $\mathbb{Z}/p\mathbb{Z} \setminus A$.

21 Résolution d'une équation du second degré dans $\mathbb{Z}/p\mathbb{Z}$

1. Résoudre l'équation
$$x^2 - \overline{13}x + \overline{8} = \overline{0}$$

dans $\mathbb{Z}/17\mathbb{Z}$.

(On essaiera de suivre la même démarche que sur \mathbb{R} : mise sous forme canonique... reprendre donc la démarche suivie dans le cours de première)

2. Résoudre l'équation
$$x^2 - \overline{2}x + \overline{4} = 0$$

dans $\mathbb{Z}/26\mathbb{Z}$.

22 Théorème de Wilson (un test de primalité)

1. Montrer que si $(p-1)! \equiv -1 \pmod{p}$, alors p est premier.
2. Réciproquement, on suppose que p est premier. En rassemblant les termes du produit par paires, justifier que $(p-1)! \equiv -1 \pmod{p}$.

23 Cryptographie à clé publique RSA⁷

La cryptographie à clé publique est une méthode pour crypter un message à destination d'une personne (Alice), par une méthode que tout le monde connaît, mais de façon à ce que seul le destinataire puisse décoder le message. Les messages considérés ici seront des nombres (par exemple fabriqués en remplaçant chacune des lettres du message à envoyer par son code ASCII, après découpage en morceaux pour obtenir des nombres pas trop grands).

La destinataire Alice choisit deux « grands » nombres premiers p et q , et calcule le produit $N = pq$. Elle rend N public et surtout garde pour elle les valeurs de p et q . Elle choisit ensuite un entier e premier avec $(p-1)(q-1)$ et le donne à tout le monde : (N, e) sera la clé publique. Elle choisit en général e ayant peu de termes dans sa décomposition en binaire, pour que le cryptage ne demande pas trop longtemps.

Comme Alice est la seule à connaître p et q , elle est également la seule à pouvoir calculer $(p-1)(q-1)$, et donc à déterminer un entier de Bézout d tel que $de \equiv 1 \pmod{(p-1)(q-1)}$. d sera la clé de décodage, que l'on conserve bien sûr très secrète.

Le principe de la méthode est alors le suivant. Bob, qui veut envoyer un message M à Alice calcule $M' \equiv M^e \pmod{N}$ et envoie M' à Alice. Celle-ci calcule ensuite $M'' \equiv M'^d \pmod{N}$.

Montrer que M et M'' sont égaux modulo N , et donc que Alice peut décoder le message de Bob pourvu que M soit inférieur à N .

7. Rivest, Shamir et Adleman, 1979

24 On note $((\mathbb{Z}/17\mathbb{Z})^\times, \times)$ le groupe des inversibles de l'anneau $(\mathbb{Z}/17\mathbb{Z}, +, \times)$. Montrer qu'il est cyclique (en cherchant, tout simplement, un générateur de ce groupe). Puis donner tous les générateurs de $((\mathbb{Z}/17\mathbb{Z})^\times, \times)$.

On peut montrer que, si p est premier, $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ est cyclique. Ce n'est pas au programme. Ses éléments générateurs sont dit primitifs. On peut montrer qu'il y en a exactement $\varphi(p-1)$.

25 Quels sont les sous-groupes finis de (\mathbb{C}^*, \times) ?

26 Déterminer tous les morphismes de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans (\mathbb{C}^*, \times) .

27 Déterminants arithmétiques Soient $n \in \mathbb{N}^*$, $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{C})$ et $\psi : \mathbb{N} \rightarrow \mathbb{C}$. On suppose que

$$\forall i, j \in \llbracket 1, n \rrbracket, a_{i,j} = \sum_{k \mid i \text{ et } k \mid j} \psi(k)$$

Le but de l'exercice est de calculer $\det A$ à l'aide de ψ .

1. On introduit la matrice $B = (b_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{C})$ où $b_{i,j} = \begin{cases} 1 & \text{si } i \mid j \\ 0 & \text{sinon.} \end{cases}$

- 1.a) Montrer que $A = B^T D B$ où D est diagonale dont les coefficients sont à préciser.
- 1.b) Justifier que $\det B = 1$.
- 1.c) Exprimer $\det A$ en fonction de ψ .

2. Applications.

- 2.a) Calculer $\det A$ lorsque $a_{i,j}$ est le nombre de diviseurs communs à i et j .
On pourra conjecturer le résultat avec un logiciel de calcul numérique ou formel.
 - 2.b) Calculer $\det A$ lorsque $a_{i,j}$ est la somme des diviseurs communs à i et j .
On pourra conjecturer le résultat avec un logiciel de calcul numérique ou formel.
3. On souhaite calculer le déterminant de Smith : $\det A$ lorsque $a_{i,j} = i \wedge j$ est le plus grand diviseur commun à i et j .
 - 3.a) Pour $k \geq 2$, on appelle $\varphi(k)$ le nombre d'entiers ℓ tels que $0 \leq \ell \leq k-1$ et $k \wedge \ell = 1$, et on pose $\varphi(1) = 1$. La fonction φ de \mathbb{N}^* dans \mathbb{N} ainsi définie est appelée *indicatrice d'Euler*.
 - (i) Soient $m \in \mathbb{N}^*$ et $k \in \mathbb{N}$ un diviseur de m . Parmi tous les nombres rationnels de la forme $\frac{a}{m}$ où $1 \leq a \leq m$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?
 - (ii) Montrer que, si $m \in \mathbb{N}^*$, $m = \sum_{k \mid m} \varphi(k)$.
 - 3.b) En déduire $\det A$ en fonction de φ .

28 Oral Centrale Soit $(G, *)$ un groupe. On suppose que le cardinal de G s'écrit pq , avec q premier et $p < q$. Montrer que G contient au plus un sous-groupe de cardinal q .

29 Oral Mines Soit (G, \cdot) un groupe fini tel que $\forall g \in G, g^2 = e$ où e est le neutre de G . On suppose G non réduit à $\{e\}$.
Montrer qu'il existe $n \in \mathbb{N}^*$ tel que G est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.
Indication : on pourra interpréter G comme un $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel.

30 **Oral X** Soit G un groupe. Pour $(a, b) \in G^2$, on note $[a, b] = aba^{-1}b^{-1}$. On note D_G le sous-groupe de G engendré par les éléments de la forme $[a, b]$, i.e. le plus petit sous-groupe de G contenant les éléments de la forme $[a, b]$.

1. Montrer que $\forall g \in G, \quad gD_Gg^{-1} = D_G$.
2. Montrer que $\forall g \in G, \quad gD_G = D_Gg$.
3. On pose $\mathcal{Q}_G = \{xD_G ; x \in G\}$.
 - (a) Montrer que \mathcal{Q}_G est une partition de G .
 - (b) Montrer que la fonction $(xD_G, yD_G) \mapsto (xy)D_G$ est convenablement définie et munit \mathcal{Q}_G d'une structure de groupe, puis montrer que $x \mapsto xD_G$ est un morphisme de G dans \mathcal{Q}_G .
 - (c) Montrer que \mathcal{Q}_G est abélien.

31 **Oral ENS** Soit (G, \cdot) un groupe, $\text{Aut}(G)$ l'ensemble de ses automorphismes.

1. Montrer que $(\text{Aut}(G), \circ)$ est un groupe.
2. Déterminer les groupes finis tels que $\text{Aut}(G)$ soit réduit à un élément.