Algèbre modulaire

1 CCINP 86 - Petit théorème de Fermat

2 CCINP 94

3 Oral Centrale

Déterminer le chiffre des unité de 1587^{413}.

Solution de 3 : Oral Centrale

7

4 Oral Centrale

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

Solution de 4 : Oral Centrale

$f : k \mapsto$ (somme des chiffres de k). Calculer $f \circ f \circ f(n)$.
$f(n) \equiv n$ [9]. Or $4444 = 9 \times 493 + 7$, donc $4444 \equiv 7$ [9] et $4444^{4444} \equiv 7^{4444}$ [9].
Mais $7^2 \equiv 4$ [9], $7^3 \equiv -2$ [9] et $7^3 \equiv 1$ [9]. D'où $7^{4444} = 7^{3k+1} \equiv 7$ [9] donc $f(n) \equiv 7$ [9]. Puis $f(f(f(n))) \equiv 7$ [9].
De plus, $n \leqslant 10000^{5000} = 10^{20000}$. Donc n possède au plus 20 000 chiffres et $f(n) \leqslant 9 \times 20000 = 180000$.
Puis $f(f(n)) \leqslant 1 + 8 + 4 \times 9 = 45$ et $f(f(n)) \equiv f(n) \equiv 7$ [9].
Donc $f(f(f(n))) < 4 + 9 = 13$ et $f(f(f(n))) \equiv 7$ [9]. Donc $f(f(f(n))) = 7$.

5

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

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

6

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 ?

7

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

8

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.

9 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 $\mathbb{Z}/p\mathbb{Z} \setminus A$.

10 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 essayera 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 $\mathbb{Z}/26\mathbb{Z}$.

11 Théorème de Wilson (un test de primalité)

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

12 Cryptographie à clé publique RSA [1]

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 $de \equiv 1 \ [(p-1)(q-1)]$. 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 $M' \equiv M^e \ [N]$ et envoie M' à Alice. Celle-ci calcule ensuite $M'' \equiv M'^d \ [N]$.

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.

13

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 $\varphi(p-1)$.

14

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

Solution de 14 :

Soit G un sous-groupe fini de $(\mathbb{C}^*, \times)$. Tous ses éléments sont d'ordre fini, divisant l'ordre du groupe. Soit $d = |G|$. Tous les éléments de G vérifient $z^d = 1$. Donc G est inclus dans $\mathbf{U}_d$. Mais ils ont même cardinal, ils sont donc égaux.

1. Rivest, Shamir et Adleman, 1979

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

Solution de 15 :

Soit ϕ un tel morphisme. Si on connaît $\phi(\overline{1})$, on connaît ϕ.

[Plus généralement, pour connaître un morphisme d'un groupe cyclique $(G,*)$ dans un groupe $(H,.)$, il suffit de connaître l'image par ce morphisme d'un générateur de G. En effet, si g est un tel générateur, on a pour tout $n\in\mathbb{Z}$: $\phi(g^n)=\big(\phi(g)\big)^n$, ce qui donne l'image par ϕ de tous les éléments de G].

Soit $\omega=\phi(\overline{1})$. On a, par propriété de morphisme (en essayant de ne pas trop se tromper de loi : au départ, l'addition, à l'arrivée la multiplication),

$$\phi(n\overline{1})=\omega^n$$

Mais $n\overline{1}=\overline{n}=\overline{n}=\overline{0}$, et un morphisme transforme l'élément neutre du groupe de départ en l'élément neutre du groupe d'arrivée. Donc $\omega^n=1$. Et donc $\omega\in\mathcal{U}_n$.

Réciproquement, soit ω un élément de $\mathbb{U}_n$. On montre que l'application

$$\phi_\omega : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{C}^* \\ \overline{a} & \longmapsto & \omega^a \end{array} \right.$$

est bien définie (il s'agit pour cela de montrer que, si $a\equiv b[n]$, $\omega^a=\omega^b$, ce qui se fait sans trop de mal). C'est assez clairement un morphisme. Les ϕ_ω, $\omega\in\mathbb{U}_n$ sont les morphismes cherchés.

16 Déterminants arithmétiques

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

$$\forall\, i,j \in [\![1,n]\!],\quad a_{i,j} = \sum_{k \mid i \text{ et } k \mid j} \psi(k)$$

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

1. On introduit la matrice $B = (b_{i,j})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{C})$ où $b_{i,j} = \delta_{i \mid j} = \begin{cases} 1 & \text{si } i \mid j, \\ 0 & \text{sinon.} \end{cases}$.
   (a) Montrer que $A = B^{\intercal} D B$ où D est diagonale dont les cœfficients sont à préciser.
   (b) Justifier que $\det B = 1$.
   (c) Exprimer $\det A$ en fonction de ψ.
2. **Applications**.
   (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.
   (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.
   (a) Pour $k \geqslant 2$, on appelle $\varphi(k)$ le nombre d'entiers ℓ tels que $0 \leqslant \ell \leqslant k-1$ 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 $\frac{q}{m}$ où $1 \leqslant q \leqslant m$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?
      ii. Montrer que, si $m \in \mathbb{N}^*$, $m = \sum_{k \mid m} \varphi(k)$.
   (b) En déduire $\det A$ en fonction de φ.

Solution de 16 : Déterminants arithmétiques

1. (a) Si $i,j \in [\![1,n]\!]$,
$$a_{i,j} = \sum_{k \mid i \text{ et } k \mid j} \psi(k) = \sum_{k=1}^{n} \delta_{k \mid i} \psi(k) \delta_{k \mid j} = \sum_{k=1}^{n} b_{k,i} \psi(k) b_{k,j} = (B^{\intercal} D B)_{i,j}$$
avec $D = \operatorname{diag}(\psi(1), \dots, \psi(n))$.
   (b) Pour tout i,j, $i \mid i$ et si $i > j$, $i \nmid j$ donc B est triangulaire supérieure avec des 1 sur la diagonale, donc $\det B = 1$.
   (c) On a obtenu dans la question précédente $A = B^{\intercal} C B$ donc $\det A = \det B^{\intercal} \det C \det B$. Et comme $\det B^{\intercal} = \det B = 1$ d'après **c)**, $\det A = \det C = \begin{vmatrix} \psi(1) & & \\ & \ddots & \\ & & \psi(n) \end{vmatrix}$. Finalement, $\boxed{\det A = \prod_{k=1}^{n} \psi(k).}$
2. (a) Remarquons que le nombre de diviseurs communs à i et j est $a_{i,j} = \sum_{k \mid i \text{ et } k \mid j} 1$. On peut donc appliquer le résultat de la question **1.** avec $\psi \equiv 1$ et donc $\boxed{\det A = 1.}$
   (b) Remarquons que la somme des diviseurs communs à i et j est $a_{i,j} = \sum_{k \mid i \text{ et } k \mid j} k$. On peut donc appliquer le résultat de la question **1.** avec $\psi = \mathrm{id}$ et donc $\boxed{\det A = \prod_{k=1}^{n} k = k!.}$
3. (a) i. Notons F_k l'ensemble des nombres rationnels de la forme $\frac{q}{m}$ où $1 \leqslant q \leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur et $E_k = \{\ell \in [\![0, k-1]\!] \mid \ell \wedge k = 1\}$ si $k \neq 1$ (remarquons qu'alors $0 \notin E_k$), $E_1 = \{1\}$.
   L'application $f : \begin{vmatrix} E_k & \longrightarrow & F_k \\ \ell & \longmapsto & \frac{\ell}{k} \end{vmatrix}$ est *bijective*[2]. En effet,

2. On peut aller un peu plus vite oralement en invoquant simplement l'existence et l'unicité de la forme irréductible des fractions.

- si $k=1$, f est l'identité de $F_1=E_1=\{1\}$;
- sinon,
  - ⋆ elle est *bien définie* car si $\ell\in E_k$, $\frac{\ell}{k}$ est un nombre rationnel de la forme $\frac{q}{m}$ car $k|m$ avec $1\leqslant q\leqslant m$ car $\frac{\ell}{k}\in]0,1]$, qui s'écrit sous forme irréductible avec k au dénominateur car $\ell\wedge k=1$ et donc $f(\ell)\in F_k$;
  - ⋆ elle est *injective* car si $\ell,\ell'\in E_k$ tels que $f(\ell)=f(\ell')$, alors $\frac{\ell}{k}=\frac{\ell'}{k}$ donc $\ell=\ell'$;
  - ⋆ elle est *surjective* car si $r\in F_k$, $r\in\mathbb{Q}\cap]0,1]$ et r s'écrit forme irréductible avec k au dénominateur, donc on a $l\in[\![1,k]\!]$ avec $k\wedge\ell=1$ tel que $r=\frac{\ell}{k}$. Comme $k\neq 1$, $\ell\neq k$ donc $\ell\in[\![1,k-1]\!]$, $\ell\in E_k$ et donc $r=f(\ell)$.

  Ainsi, le nombre de rationnels de la forme $\frac{q}{m}$ où $1\leqslant q\leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur est le nombre d'entiers l tels que $0\leqslant l\leqslant k-1$ et $k\wedge l=1$ si $k\neq 1$, 1 sinon : il y en a donc $\varphi(k)$.

ii. Si on note $F=\left\{\frac{q}{m}\ ;\ 1\leqslant q\leqslant m\right\}$, alors $F=\bigsqcup_{k|m}F_k$ car tout rationnel de F s'écrit de manière unique sous forme irréductible avec un diviseur de m au dénominateur.

Donc $|F|=\sum_{k|m}|F_k|$, et comme $|F|=|[\![1,m]\!]|=m$, $\boxed{m=\sum_{k|m}\varphi(k)}$ d'après la question précédente.

(b) $\det\left((i\wedge j)_{i,j}\right)$: D'après la question précédente, pour tous i,j, $i\wedge j=\sum_{k|i\wedge j}\varphi(k)$, donc comme $k|i\wedge j$ si et seulement si $k|i$ et $k|j$, $a_{i,j}=i\wedge j=\sum_{k|i\text{ et }k|j}\varphi(k)$. On peut donc appliquer la question 1. qui nous dit que $\boxed{\det A=\prod_{k=1}^{n}\varphi(k).}$