Algèbre modulaire

- Savoir que $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier (et seulement dans ce cas, on peut alors le noter $\mathbb{F}_p$). 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 des problèmes de divisibilité, penser à travailler avec des congruences. On peut aussi travailler dans $\mathbb{Z}/n\mathbb{Z}$.
- En algèbre modulaire, on ne manipule jamais de grande valeur : penser à réduire systématiquement pour se ramener dans $[\![0, n-1]\!]$ (voire $\left[\!\left[\frac{-n}{2}, \frac{n}{2}\right]\!\right]$...)
- Savoir résoudre des systèmes de congruences : avec des modulos 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 86 - Petit théorème de Fermat 2 CCINP 94

3 Oral Centrale

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

4 Oral Centrale

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

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 $(\mathbb{C}^*, \times)$?

15

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

1. Rivest, Shamir et Adleman, 1979

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

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

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.