ARITHMÉTIQUE, ALGÈBRE MODULAIRE, GROUPES CYCLIQUES

1 CCINP 66

On note p un entier naturel supérieur ou égal à 2.

On considère dans $\mathbb{Z}$ la relation d'équivalence $\mathscr{R}$ définie par : $x \mathscr{R} y \overset{\text{déf.}}{\Longleftrightarrow} \exists k \in \mathbb{Z}$ tel que $x - y = kp$.

On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation $\mathscr{R}$.

1. Quelle est la classe d'équivalence de 0 ? Quelle est celle de p ?
2. Donner soigneusement la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbb{Z}/p\mathbb{Z}$.
   On justifiera que ces définitions sont cohérentes.
3. On admet que, muni de ces opérations, $\mathbb{Z}/p\mathbb{Z}$ est un anneau.
   Démontrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

Solution de 1 : CCINP 66

1. Les classes d'équivalences de 0 et de p sont toutes deux égales à l'ensemble des multiples de p, c'est-à-dire à $p\mathbb{Z}$.
2. Soit $(\overline{a}, \overline{b}) \in (\mathbb{Z}/p\mathbb{Z})^2$.
   On pose $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{a} \times \overline{b} = \overline{ab}$.

   Cette définition est cohérente car elle ne dépend pas des représentants a et b choisis pour $\overline{a}$ et $\overline{b}$.
   En effet, soit $(a', b') \in \mathbb{Z}^2$ tel que $\overline{a'} = \overline{a}$ et $\overline{b'} = \overline{b}$.
   Alors il existe $n \in \mathbb{Z}$ tel que $a' = a + np$ et il existe $m \in \mathbb{Z}$ tel que $b' = b + mp$.
   Donc $a' + b' = a + b + (n+m)p$, c'est-à-dire $\overline{a' + b'} = \overline{a+b}$.
   Et $a'b' = ab + (am + bn + nmp)p$, c'est-à-dire $\overline{a'b'} = \overline{ab}$.
3. Supposons p premier.
   Alors $\mathbb{Z}/p\mathbb{Z}$ est commutatif et non réduit à $\{\bar{0}\}$ car $p \geqslant 2$.
   Soit $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ tel que $\bar{a} \neq \bar{0}$.
   $\bar{a} \neq \bar{0}$ donc p ne divise pas a . Or p est premier donc p est premier avec a.
   Par le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + pv = 1$ donc $\bar{a} \times \bar{u} = \bar{1}$.
   Donc $\overline{a}$ est inversible et $(\bar{a})^{-1} = \bar{u}$.

   Ainsi, les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles et finalement $\mathbb{Z}/p\mathbb{Z}$ est un corps.
   Supposons que $\mathbb{Z}/p\mathbb{Z}$ est un corps.

   Soit $k \in [\![2, p-1]\!]$.
   $\overline{k} \neq \bar{0}$ donc, comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, il existe $k' \in \mathbb{Z}$ tel que $\overline{k}\,\overline{k'} = \bar{1}$.
   C'est-à-dire il existe $v \in \mathbb{Z}$ tel que $kk' = 1 + vp$ c'est-à-dire $k'k - vp = 1$.
   Donc, d'après le théorème de Bézout, $k \wedge p = 1$ et donc, comme $k \neq 1$, k ne divise pas p.
   On en déduit que les seuls diviseurs positifs de p sont 1 et p.

   Donc p est premier.

2 CCINP 86 - Petit théorème de Fermat

1. Soit $(a, b, p) \in \mathbb{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
2. Soit p un nombre premier.
   (a) Prouver que $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis en déduire que p divise $\binom{p}{k}$.
   (b) Prouver que : $\forall n \in \mathbb{N}$, $n^p \equiv n\ [p]$.
   Indication : procéder par récurrence.
   (c) En déduire, pour tout entier naturel n, que : p ne divise pas $n \Longrightarrow n^{p-1} \equiv 1\ [p]$.

Solution de 2 : CCINP 86 - Petit théorème de Fermat

1. On suppose $p \wedge a = 1$ et $p \wedge b = 1$.
   D'après le théorème de Bézout,
   $\exists (u_1, v_1) \in \mathbb{Z}^2$ tel que $u_1 p + v_1 a = 1$. (1)
   $\exists (u_2, v_2) \in \mathbb{Z}^2$ tel que $u_2 p + v_2 b = 1$. (2)
   En multipliant les équations (1) et (2), on obtient :

   $\underbrace{(u_1 u_2 p + u_1 v_2 b + u_2 v_1 a)}_{\in \mathbb{Z}} p + \underbrace{(v_1 v_2)}_{\in \mathbb{Z}}(ab) = 1.$

   Donc, d'après le théorème de Bézout, $p \wedge (ab) = 1$.
2. Soit p un nombre premier.
   (a) Soit $k \in [\![1, p-1]\!]$. $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)!} = \dfrac{p(p-1)...(p-k+1)}{k!}$.

   Donc $\binom{p}{k} k! = p(p-1)...(p-k+1)$.

   donc $p \mid \binom{p}{k} k!$. (3)

   Or, $p \wedge k = 1$ (car p est premier) donc, d'après 1., $p \wedge k! = 1$.

   Donc, d'après le lemme de Gauss, (3) $\Longrightarrow p \mid \binom{p}{k}$.

   (b) Procédons par récurrence sur n.
   Pour $n = 0$ et pour $n = 1$, la propriété est vérifiée.
   Soit $n \in \mathbb{N}$.
   Supposons que la propriété (P_n) : $n^p \equiv n\ [p]$ soit vérifiée.

   Alors, d'après la formule du binôme de Newton, $(n+1)^p = n^p + \sum\limits_{k=1}^{p-1} \binom{p}{k} n^k + 1$. (4)

   Or $\forall k \in [\![1, p-1]\!]$, $p \mid \binom{p}{k}$ donc $p \mid \sum\limits_{k=1}^{p-1} \binom{p}{k} n^k$.
   Donc d'après (4) et (P_n), $(n+1)^p \equiv n+1\ [p]$ et (P_{n+1}) est vraie.

   (c) Soit $n \in \mathbb{N}$ tel que p ne divise pas n.
   Comme p est premier, alors $p \wedge n = 1$.
   La question précédente donne p divise $n^p - n = n(n^{p-1} - 1)$.
   Or comme p est premier avec n, on en déduit, d'après le lemme de Gauss, que p divise $n^{p-1} - 1$.
   Ce qui signifie que $n^{p-1} \equiv 1\ [p]$. (petit théorème de Fermat).

3 CCINP 94

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux. Soit $c \in \mathbb{N}$. Prouver que : $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.
3. On considère le système (S) : $\begin{cases} x \equiv 6 \mod(17) \\ x \equiv 4 \mod(15) \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.
   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Solution de 3 : CCINP 94

1. Théorème de Bézout :
   Soit $(a, b) \in \mathbb{Z}^2$.
   $a \wedge b = 1 \Longleftrightarrow \exists (u, v) \in \mathbb{Z}^2 / au + bv = 1$.
2. Soit $(a, b) \in \mathbb{N}^2$. On suppose que $a \wedge b = 1$.
   Soit $c \in \mathbb{N}$.

   Prouvons que $ab|c \Longrightarrow a|c$ et $b|c$.
   Si $ab|c$ alors $\exists k \in \mathbb{Z} / c = kab$.
   Alors, $c = (kb)a$ donc $a|c$ et $c = (ka)b$ donc $b|c$.

Prouvons que $(a|c \text{ et } b|c) \Longrightarrow ab|c$.

$a \wedge b = 1$ donc $\exists (u,v) \in \mathbb{Z}^2 \,/\, au + bv = 1$. (1)
De plus $a|c$ donc $\exists k_1 \in \mathbb{Z} \,/\, c = k_1 a$. (2)
De même, $b|c$ donc $\exists k_2 \in \mathbb{Z} \,/\, c = k_2 b$. (3)
On multiplie (1) par c et on obtient $cau + cbv = c$.
Alors, d'après (2) et (3), $(k_2 b)au + (k_1 a)bv = c$, donc $(k_2 u + k_1 v)(ab) = c$ et donc $ab|c$.
On a donc prouvé que $(a|c \text{ et } b|c) \Longleftrightarrow ab|c$.

3. (a) **Première méthode** (méthode générale) :
Soit $x \in \mathbb{Z}$.

$$x \text{ solution de}(S) \iff \exists (k,k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6 + 17k \\ x = 4 + 15k' \end{cases}$$
$$\iff \exists (k,k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6 + 17k \\ 6 + 17k = 4 + 15k' \end{cases}$$

Or $6 + 17k = 4 + 15k' \iff 15k' - 17k = 2$.
Pour déterminer une solution particulière x_0 de (S), il suffit donc de trouver une solution particulière (k_0, k'_0) de l'équation $15k' - 17k = 2$.
Pour cela, cherchons d'abord, une solution de l'équation $15u + 17v = 1$.
17 et 15 sont premiers entre eux.
Déterminons alors un couple (u_0, v_0) d'entiers relatifs tel que $15u_0 + 17v_0 = 1$.
On a : $17 = 15 \times 1 + 2$ puis $15 = 7 \times 2 + 1$.
Alors $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15 \times 1) = 15 - 17 \times 7 + 15 \times 7 = 15 \times 8 - 17 \times 7$
Donc $8 \times 15 + (-7) \times 17 = 1$
Ainsi, $16 \times 15 + (-14) \times 17 = 2$.

On peut prendre alors $k'_0 = 16$ et $k_0 = 14$.

Ainsi, $x_0 = 6 + 17 \times k_0 = 6 + 17 \times 14 = 244$ est une solution particulière de (S).

Deuxième méthode :
En observant le système (S), on peut remarquer que $x_0 = -11$ est une solution particulière.
Cette méthode est évidemment plus rapide mais ne fonctionne pas toujours.

(b) x_0 solution particulière de (S) donc $\begin{cases} x_0 = 6 \; [17] \\ x_0 = 4 \; [15] \end{cases}$.

On en déduit que x solution de (S) si et seulement si $\begin{cases} x - x_0 = 0 \; [17] \\ x - x_0 = 0 \; [15] \end{cases}$
c'est-à-dire x solution de $(S) \iff (17|x - x_0 \text{ et } 15|x - x_0)$.
Or $17 \wedge 15 = 1$ donc d'après 2., x solution de (S) $\iff (17 \times 15)|x - x_0$.
Donc l'ensemble des solutions de (S) est $\{x_0 + 17 \times 15k,\ k \in \mathbb{Z}\} = \{244 + 255k,\ k \in \mathbb{Z}\}$.

4 À savoir faire absolument

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

5

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

Solution de 5 :

1. $(n^3 + n) \wedge (2n + 1) = 1$ si et seulement si
$$n(n^2 + 1) \wedge (2n + 1) = 1$$
si et seulement si
$$\begin{cases} n \wedge (2n + 1) = 1 \\ (n^2 + 1) \wedge (2n + 1) = 1 \end{cases}$$

Il s'agit de la propriété $ab \wedge c = 1 \iff a \wedge c = 1$ et $b \wedge c = 1$: le sens direct s'obtient avec le théorème de Bézout ou en s'intéressant au diviseurs communs possibles de a et c d'une part et de b et c d'autre part, le sens réciproque s'obtient en multipliant des relations de Bézout : $1 = (au + cv)(bu' + cv') = abU + cV\ldots$
Or, en se souvenant de la propriété d'Euclide $a \wedge b = (a - bq) \wedge b$ (pas nécessairement une division euclidienne), on obtient $n \wedge (2n + 1) = n \wedge 1 = 1$ toujours vrai.
Puis, toujours avec cette propriété $(n^2 + 1) \wedge (2n + 1) = (n^2 - 2n) \wedge (2n + 1) = n(n - 2) \wedge (2n + 1)$.
Donc

$$(n^3+n)\wedge(2n+1) = 1 \iff \begin{cases} n \wedge (2n + 1) = 1 \\ (n - 2) \wedge (2n + 1) = 1 \end{cases} \iff (n-2)\wedge(2n+1) = 1 \iff (n-2)\wedge\big(2n+1-2(n-2)\big) = (n-2)\wedge 5 = 1$$

Comme 5 est premier, on en déduit que les solutions sont les entiers n tels que $5 \nmid (n - 2)$ c'est-à-dire tels que $\boxed{n \not\equiv 2 \; [5].}$

2. On écrit $2n^2 + 9n + 13 = 2(n + 2)^2 + n + 5 = 2(n + 2)^2 + (n + 2) + 3$.
Donc $(n + 2)|(2n^2 + 9n + 13)$ si et seulement si $n + 2|3$ si et seulement si $n + 2 \in \{-1, 1, -3, 3\}$. Les solutions sont $\boxed{-3, -1, -5, 1}$ (ce que l'on peut effectivement vérifier).
3. Avec la propriété d'Euclide, si $n \in \mathbb{Z}$,
$$(21n + 4) \wedge (14n + 3) = \big(21n + 4 - (14n + 3)\big) \wedge (14n + 3) = (7n + 1) \wedge \big(14n + 3 - 2(7n + 1)\big) = (7n + 1) \wedge 1 = 1$$
Autre méthode, avec une relation de Bézout :
$$-2(21n + 4) + 3(14n + 3) = 1.$$

6 Nombres de Mersenne [1] - 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.

Solution de 6 : Nombres de Mersenne [2] - Très classique - Oral Centrale

La factorisation
$$a^n - 1 = (a - 1)(a^{n-1} + \cdots + 1)$$
donne la première réponse, puis
$$2^{n_1 n_2} - 1 = (2^{n_1})^{n_2} - 1 = (2^{n_1} - 1)(\ldots)$$
donne la deuxième.

7 Nombres de Fermat [3] - Très classique - Oral Mines

1. Soient $a, n \in \mathbb{N}^*$, $a \geqslant 2$. 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).
2. Démonstration de 1734 d'Euler du fait que F_5 n'est pas premier.
   (a) Comparer $5^4 + 2^4$ et $1 + 5 \times 2^7$ (sans calculatrice !).
   (b) En déduire que $5^4 \times 2^{28} \equiv 1 \; [641]$.
   (c) Conclure que 641 divise F_5.
3. 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.
4. 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 fausse ($2^{11} - 1 = 23 \times 89$). Les plus grands nombres premiers connus actuellement sont des nombres de Mersenne : $2^{77\,232\,917} - 1$ a été découvert le 26 décembre 2017 (23 249 425 chiffres en base décimale).
3. Ils interviennent dans la constructibilité à la règle et au compas des polygones réguliers.

Solution de 7 : Nombres de Fermat [4] - Très classique - Oral Mines

Si n a un facteur premier impair p, on écrit

$$2^n+1=2^{mp}+1=(2^m)^p+1$$

Or on connaît très bien

$$a^n-b^n=(a-b)(\dots)$$

Mais, si n est impair, remplaçant b par $-b$, on en déduit

$$a^n+b^n=(a+b)(a^{n-1}-ba^{n-2}+\cdots+b^{n-1})$$

Appliqué à notre situation, on trouve

$$2^n+1=(2^m+1)(2^{m(p-1)}-2^{m(p-2)}\cdots+1)$$

On prend bien soin de justifier que c'est une vraie factorisation ($1<2^m+1<2^n+1$). Et on a résolu la première question. Comme souvent, c'est l'exercice classique sur les nombres de Mersenne (si a^n-1 est premier, $a=2$ et n est premier) qui peut donner l'idée

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.

Solution de 9 :

Il suffit de considérer les entiers de $1001!+2$ à $1001!+1001$.

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 $\leqslant x$.

1. Montrer que pour tout $n\geqslant 1$, $p_{n+1}\leqslant p_1\cdots p_n+1$.
2. Montrer que pour tout $n\geqslant 1$, $2n-1\leqslant p_n\leqslant 2^{2^{n-1}}$.
3. Justifier [6] que $\forall x>0,\ \ln(\ln x)<\pi(x)<x$.

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

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

Solution de 13 : Oral Centrale

7

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

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, $p_n\sim n\ln n$.

Solution de 14 :

$f:\ k\mapsto$ (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 $f(f(f(n)))=7$.

15 **Oral Mines**

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

Solution de 15 : Oral Mines

p est congru à 1 ou à -1 modulo 3 (car $p>3$), donc $p+1$ ou $p-1$ est divisible par 3. Donc p^2-1, leur produit, l'est. De plus, p, premier et impair car >2, est congru à 1, 3, 5 ou 7 modulo 8. Donc son carré est congru à 1, 1, 1 ou 1 modulo 8. Donc p^2-1 est divisible par 3 et par 8, qui sont premiers entre eux, il est donc divisible par 24.

Autre méthode : remarquer que parmi $p-1$, p et $p+1$, l'un est divisible par 3 et parmi $p-1$, p, $p+1$, $p+2$, l'un est divisible par 4.

16 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. $15^2\mid 16^n-1-15n$.

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

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

22 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 $(p-1)! \equiv -1\ [p]$.

23 Cryptographie à clé publique RSA [7]

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.

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

Solution de 25 :

Soit G un sous-groupe fini de $(\mathbf{C}^*, \times)$. 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.

26

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

Solution de 26 :

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 $n \in \mathbf{Z}$: $\phi(g^n) = (\phi(g))^n$, 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 $\omega \in \mathscr{U}_n$.

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

$$\phi_\omega : \mathbf{Z}/n\mathbf{Z} \mapsto \mathbf{C}^* \overline{a} \omega^a$$

7. Rivest, Shamir et Adleman, 1979

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, $\omega \in \mathbf{U}_n$ sont les morphismes cherchés.

27 Déterminants arithmétiques

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

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

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

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

- **1.a)** Montrer que $A = B^\intercal DB$ où D est diagonale dont les cœfficients 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 $k \geqslant 2$, 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 $m \in \mathbb{N}^*$, $m = \sum_{k|m} \varphi(k)$.
- **3.b)** En déduire $\det A$ en fonction de φ.

Solution de 27 : Déterminants arithmétiques

1.

1.a) Si $i, j \in [\![1, n]\!]$,

$$a_{i,j} = \sum_{k|i \text{ et } k|j} \psi(k) = \sum_{k=1}^{n} \delta_{k|i} \psi(k) \delta_{k|j} = \sum_{k=1}^{n} b_{k,i} \psi(k) b_{k,j} = (B^\intercal DB)_{i,j}$$

avec $D = \operatorname{diag}(\psi(1), \dots, \psi(n))$.

1.b) Pour tout i, j, $i|i$ et si $i > j$, $i \nmid j$ donc B est triangulaire supérieure avec des 1 sur la diagonale, donc $\det B = 1$.

1.c) On a obtenu dans la question précédente $A = B^\intercal CB$ 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.

2.a) Remarquons que le nombre de diviseurs communs à i et j est $a_{i,j} = \sum_{k|i \text{ et } k|j} 1$. On peut donc appliquer le résultat de la question **1.** avec $\psi \equiv 1$ et donc $\boxed{\det A = 1.}$

2.b) Remarquons que la somme des diviseurs communs à i et j est $a_{i,j} = \sum_{k|i \text{ et } k|j} k$. 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.

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 $f : \left| \begin{array}{ccc} E_k & \longrightarrow & F_k \\ \ell & \longmapsto & \frac{\ell}{k} \end{array} \right.$ est *bijective*[8]. En effet,

- 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 $|F| = \left|[\![1, m]\!]\right| = m$, $\boxed{m = \sum_{k|m} \varphi(k)}$ d'après la question précédente.

3.b) $\det\big((i \wedge j)_{i,j}\big)$: 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

$$\boxed{\det A = \prod_{k=1}^{n} \varphi(k).}$$

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