Arithmétique, algèbre modulaire, groupes cycliques

1 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 1 : 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 $u_1p+v_1a=1$. (1)
   $\exists(u_2,v_2)\in\mathbb{Z}^2$ tel que $u_2p+v_2b=1$. (2)
   En multipliant les équations (1) et (2), on obtient :
   $$\underbrace{(u_1u_2p+u_1v_2b+u_2v_1a)}_{\in\mathbb{Z}}p+\underbrace{(v_1v_2)}_{\in\mathbb{Z}}(ab)=1.$$
   Donc, d'après le théorème de Bézout, $p\wedge(ab)=1$.
2. Soit p un nombre premier.
   (a) Soit $k\in[\![1,p-1]\!]$. $\binom{p}{k}=\dfrac{p!}{k!(p-k)!}=\dfrac{p(p-1)...(p-k+1)}{k!}$.
   Donc $\binom{p}{k}k!=p(p-1)...(p-k+1)$.
   donc $p\,|\binom{p}{k}k!$. (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) $\Longrightarrow p\,|\binom{p}{k}$.
   (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, $(n+1)^p=n^p+\sum_{k=1}^{p-1}\binom{p}{k}n^k+1$. (4)
   Or $\forall k\in[\![1,p-1]\!]$, $p\,|\binom{p}{k}$ donc $p\,|\sum_{k=1}^{p-1}\binom{p}{k}n^k$.
   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).

2 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 : $(a|c$ 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 2 : 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 $(a|c$ 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 $\exists k_1\in\mathbb{Z}\,/\,c=k_1a$. (2)
   De même, $b|c$ donc $\exists k_2\in\mathbb{Z}\,/\,c=k_2b$. (3)
   On multiplie (1) par c et on obtient $cau+cbv=c$.
   Alors, d'après (2) et (3), $(k_2b)au+(k_1a)bv=c$, donc $(k_2u+k_1v)(ab)=c$ et donc $ab|c$.
   On a donc prouvé que $(a|c$ et $b|c)\Longleftrightarrow ab|c$.
3. (a) **Première méthode** (méthode générale) : Soit $x\in\mathbb{Z}$.
   $$\begin{aligned} x \text{ solution de}(S) &\iff \exists(k,k')\in\mathbb{Z}^2 \text{ tel que } \begin{cases} x=6+17k\\ x=4+15k'\end{cases}\\ &\iff \exists(k,k')\in\mathbb{Z}^2 \text{ tel que } \begin{cases} x=6+17k\\ 6+17k=4+15k'\end{cases}\end{aligned}.$$
   Or $6+17k=4+15k'\Longleftrightarrow 15k'-17k=2$.
   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 $17=15\times1+2$ puis $15=7\times2+1$. Alors
   $$1=15-7\times2=15-7\times(17-15\times1)=15-17\times7+15\times7=15\times8-17\times7$$
   Donc $8\times15+(-7)\times17=1$ Ainsi, $16\times15+(-14)\times17=2$.
   On peut prendre alors $k_0'=16$ et $k_0=14$. Ainsi, $x_0=6+17\times k_0=6+17\times14=244$ 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 $(S)\Longleftrightarrow(17|x-x_0$ et $15|x-x_0)$.
   Or $17\wedge15=1$ donc d'après 2., x solution de (S) $\Longleftrightarrow(17\times15)|x-x_0$.
   Donc l'ensemble des solutions de (S) est $\{x_0+17\times15k,\ k\in\mathbb{Z}\}=\{244+255k,\ k\in\mathbb{Z}\}$.

3 À savoir faire absolument

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

4

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 4 :

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 : $1=(au+cv)(bu'+cv')=abU+cV$...
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
$$(n^3+n)\wedge(2n+1)=1\iff\begin{cases} n\wedge(2n+1)=1 \\ (n-2)\wedge(2n+1)=1 \end{cases}\iff(n-2)\wedge(2n+1-2(n-2))=(n-2)\wedge 5=1$$
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 $n\in\mathbb{Z}$,
$$(21n+4)\wedge(14n+3)=(21n+4-(14n+3))\wedge(14n+3)=(7n+1)\wedge(14n+3-2(7n+1))=(7n+1)\wedge 1=1$$
Autre méthode, avec une relation de Bézout :
$$-2(21n+4)+3(14n+3)=1.$$

5 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 5 : 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
$$2^{n_1n_2}-1=(2^{n_1})^{n_2}-1=(2^{n_1}-1)(\ldots)$$
donne la deuxième.

6 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.

Solution de 6 : 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
$$a^n-b^n=(a-b)(\ldots)$$
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

7

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].

Solution de 7 :

S'intéresser aux diviseurs premiers de $N=4p_1\cdots p_n-1$ si les nombres premiers de la forme $4k-1$ sont exactement $p_1,\ldots,p_n$.

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.
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.

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

Solution de 8 :

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

9 **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 $n\in\mathbb{N}^*$.

Solution de 9 : Formule de Legendre - Très classique - Oraux divers

Les multiples de q s'écrivent $k=q\ell$ avec $\ell\in\mathbb{Z}$ uniquement déterminé par k et q, et alors $1\leqslant k=q\ell\leqslant n$ si et seulement si $\frac{1}{q}\leqslant\ell\leqslant\frac{n}{q}$ si et seulement si $1\leqslant\ell\leqslant\left\lfloor\frac{n}{q}\right\rfloor$ avec $\ell\in\mathbb{Z}$.

Le nombre de multiples de q entre 1 et n est donc $\left\lfloor\frac{n}{q}\right\rfloor$.

Ainsi, la valuation p-adique de $n!$ avec p premier s'obtient en ajoutant les valuations p-adiques des entiers entre 1 et m, d'après la question précédente :

- les $\left\lfloor\frac{n}{p}\right\rfloor$ multiples de p fournissent chacun (au moins) un facteur p,
- les $\left\lfloor\frac{n}{p^2}\right\rfloor$ multiples de p^2 fournissent chacun (au moins) un facteur p supplémentaire,
- les $\left\lfloor\frac{n}{p^3}\right\rfloor$ multiples de p^3 fournissent chacun (au moins) un facteur p supplémentaire,
- et ainsi de suite.

Le décompte s'arrête car la suite entière $\left(\left\lfloor\frac{n}{p^i}\right\rfloor\right)_{i\in\mathbb{N}^*}$ finit par s'annuler et on obtient la formule de Legendre (avec un nombre fini de termes non nuls) :

$$\boxed{v_p(n!)=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.}$$

Autre rédaction possible : on peut dénombrer les entiers entre 1 et n ayant une valuation q-adique exactement égale à $i\in\mathbb{N}$: il s'agit des multiples de q^i qui ne sont pas multiples de q^{i+1} et qui sont au nombre de $\left\lfloor\frac{n}{q^i}\right\rfloor-\left\lfloor\frac{n}{q^{i+1}}\right\rfloor$, d'où la formule (les sommes étant toujours faussement infinies)

$$v_p(n!)=\sum_{i=0}^{+\infty}i\cdot\left(\left\lfloor\frac{n}{p^i}\right\rfloor-\left\lfloor\frac{n}{p^{i+1}}\right\rfloor\right)=\sum_{i=1}^{+\infty}i\cdot\left\lfloor\frac{n}{p^i}\right\rfloor-\sum_{i=1}^{+\infty}(i-1)\cdot\left\lfloor\frac{n}{p^i}\right\rfloor=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.$$

10 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 $\forall\, x>0,\ \ \ln(\ln x)<\pi(x)<x$.

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

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

Solution de 12 : Oral Centrale

7

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, $p_n\sim n\ln n$.

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

Solution de 13 :

$f\ :\ k\mapsto$(somme des chiffres de k). Calculer $f\circ f\circ f(n)$.

$f(n)\equiv n$ [9]. Or $4444=9\times493+7$, donc $4444\equiv7$ [9] et $4444^{4444}\equiv7^{4444}$ [9].

Mais $7^2\equiv4$ [9], $7^3\equiv-2$ [9] et $7^3\equiv1$ [9]. D'où $7^{4444}=7^{3k+1}\equiv7$ [9] donc $f(n)\equiv7$ [9]. Puis $f(f(f(n)))\equiv7$ [9].

De plus, $n\leqslant10000^{5000}=10^{20000}$. Donc n possède au plus $20\,000$ chiffres et $f(n)\leqslant9\times20000=180000$.

Puis $f(f(n))\leqslant1+8+4\times9=45$ et $f(f(n))\equiv f(n)\equiv7$ [9].

Donc $f(f(f(n)))<4+9=13$ et $f(f(f(n)))\equiv7$ [9]. Donc $f(f(f(n)))=7$.

14 **Oral Mines**

Soit $p\geqslant5$ un nombre premier. Montrer que 24 divise p^2-1.

Solution de 14 : 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.

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

1. $6\mid5n^3+n$
2. $7\mid3^{2n+1}+2^{n+2}$
3. $5\mid2^{2n+1}+3^{2n+1}$
4. $11\mid3^{8n}5^4+5^{6n}7^3$
5. $9\mid4^n-1-3n$
6. $15^2\mid16^n-1-15n$.

16 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 ?

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

18 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.

19 **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 $\mathbb{Z}/p\mathbb{Z}\setminus A$.

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

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

22 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.

23

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 $\varphi(p-1)$.

24

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

Solution de 24 :

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 U_d. Mais ils ont même cardinal, ils sont donc égaux.

7. Rivest, Shamir et Adleman, 1979

25

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

Solution de 25 :

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 $n\in\mathbb{Z}$: $\phi(g^n)=(\phi(g))^n$, 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 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, $\omega\in\mathrm{U}_n$ sont les morphismes cherchés.

26 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

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

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 $b_{i,j}=\delta_{i|j}=\begin{cases}1 & \text{si } i|j,\\ 0 & \text{sinon.}\end{cases}$.
   (a) Montrer que $A=B^{\intercal}DB$ 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 $m\in\mathbb{N}^*$, $m=\sum_{k|m}\varphi(k)$.
   (b) En déduire $\det A$ en fonction de φ.

Solution de 26 : Déterminants arithmétiques

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

   (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 $\det B=1$.

   (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. (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 $\boxed{\det A=1.}$

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

   (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.

27 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.

Solution de 27 : Oral Centrale

Soit H un sous-groupe de cardinal q. Tout élément de H est d'ordre divisant q, donc d'ordre 1 ou q. Donc tout élément de H qui n'est pas d'ordre 1 (donc qui n'est pas l'élément neutre) est d'ordre q, donc engendre H. Supposons qu'il y ait deux sous-groupes H et H' d'ordre q, distincts. Alors $H\cap H'=\{e\}$ (car si $h\in H\cap H'$, si $h\neq e$, alors h engendre à la fois H et H', qui sont alors égaux). Montrons que l'application
$$(h,h')\longmapsto h*h'$$
est alors injective. En effet, si $h_1*h_1'=h_2*h_2'$, on a $h_2^{-1}*h_1=h_2'*(h_1')^{-1}$, cet élément de G étant à la fois dans H et H' est donc égal à e, d'où $h_1=h_2$ et $h_1'=h_2'$. Il y aurait donc au moins q^2 éléments dans G, ce qui est contraire à l'hypothèse.

28 Oral Mines

Soit $(G,*)$ 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.

Solution de 28 : Oral Mines

Le groupe $(G,*)$ est abélien. En effet, pour tout $x\in G$, on a $x^{-1}=x$ donc, pour $x,y\in G$, $(xy)^{-1}=xy$. Or $(xy)^{-1}=y^{-1}x^{-1}=yx$ donc $xy=yx$.

Pour $\bar 0,\bar 1\in\mathbb{Z}/2\mathbb{Z}$ et $x\in G$, posons $\bar 0\cdot x=e=x^0$ et $\bar 1\cdot x=x=x^1$.

On vérifie que l'on définit alors un produit externe sur G munissant le groupe abélien $(G,*)$ d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. En effet, pour $(x,y)\in G^2$ et $(\lambda,\mu)\in(\mathbb{Z}/2\mathbb{Z})^2$, on a
$$(\lambda+\mu)\cdot x=\lambda\cdot x*\mu\cdot x\qquad\lambda\cdot(x+y)=\lambda\cdot x*\lambda\cdot y\qquad\lambda\cdot(\mu\cdot x)=(\lambda\mu)\cdot x\qquad\bar 1\cdot x=x.$$

De plus, cet espace est de dimension finie car $|G|$ est fini (sinon, on pourrait construire une famille libre infinie), il est donc isomorphe à l'espace $\big((\mathbb{Z}/2\mathbb{Z})^n,+,\cdot\big)$ pour un certain $n\in\mathbb{N}^*$.

En particulier, le groupe $(G,*)$ est isomorphe à $\big((\mathbb{Z}/2\mathbb{Z})^n,+\big)$.

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

Solution de 29 : Oral X

1. Soit $(a,b)\in G^2$. Alors
$$g[a,b]g^{-1}=gaba^{-1}b^{-1}g^{-1}=gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1}=[gag^{-1},gbg^{-1}]$$
L'application $h\longmapsto ghg^{-1}$ est un automorphisme du groupe G ; elle transforme les sous-groupes de G en sous-groupes de G. Elle laisse invariant $A=\{[a,b]\ ;\ (a,b)\in G^2\}$. Elle transforme donc les sous-groupes contenant A en les sous-groupes contenant A. Et comme elle préserve l'inclusion, elle transforme le plus petit d'entre eux, D_G, en lui-même. On a donc $gD_Gg^{-1}=D_G$, un peu mieux que la question posée (on voulait $gD_Gg^{-1}\subset D_G$.

2. Facile conséquence de ce qu'on a fait précédemment.
3. (a) Supposons $xD_G \cap yD_G \neq \varnothing$; il existe alors h_1, h_2 dans D_G tels que

$$xh_1 = yh_2$$

Mais alors, si $h \in D_G$,

$$xh = y\underbrace{h_2 h_1^{-1} h}_{\in D_G} \in yD_G$$

d'où $xD_G \subset yD_G$ et, symétriquement, $yD_G \subset xD_G$, donc xD_G et yD_G sont, s'ils ne sont pas la même partie de G, deux parties disjointes de G.

(b) Pour la définition convenable, il s'agit de s'assurer que si $xD_G = x'D_G$ et $yD_G = y'D_G$ alors $xyD_G = x'y'D_G$. Ou encore, de manière équivalente, on doit montrer que si $x^{-1}x'$ et $y^{-1}y'$ sont dans D_G, alors $(xy)^{-1}x'y' \in D_G$. Mais...

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = \underbrace{y^{-1}y'}_{\in D_G}\ y'^{-1}\left(\underbrace{x^{-1}x'}_{\in D_G}\right)y'$$

et il suffit d'appliquer **1.** pour conclure.
Il est clair qu'on définit ainsi une loi interne sur $\mathcal{Q}_G$.
Cette loi est associative, la vérification en est très formelle : avec des notations évidentes,

$$xD_G(yD_G\ zD_G) = xD_G(yzD_G) = x(yz)D_G = (xy)zD_G = (xy)D_G\ zD_G = (xD_G\ yD_G)zD_G$$

L'élément $D_G = eD_G$ de $\mathcal{Q}_G$ est neutre. Et l'élément $x^{-1}D_G$ est symétrique de l'élément xD_G. La propriété de morphisme demandée est alors très simple à écrire, elle découle de la définition.

(c) Il s'agit de montrer que, pour tous x, y dans G,

$$(xy)D_G = (yx)D_G$$

ou encore que $(xy)^{-1}yx \in D_G$ ce qui est bien simple vu la définition de D_G.

30 Oral ENS

Soit $(G,.)$ un groupe, Aut(G) l'ensemble de ses automorphismes.

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

Solution de 30 : Oral ENS

La première question est simple, c'est une entrée en matière dans laquelle il faut montrer clarté et précision.
Soit G un groupe fini tel que Aut(G) soit réduit à un élément. Alors, pour tout $g \in G$,

$$\phi_g\ :\ h \longmapsto ghg^{-1}$$

étant dans Aut(G), est égal à Id_G. On en déduit que G est commutatif.
Mais alors $x \longmapsto x^{-1}$ est aussi dans Aut(G), et donc est égal à Id_G. On en déduit que $(G,.)$ est un groupe fini tel que pour tout $g \in G$, $g^2 = e$.
Il existe alors des éléments $g_1, \ldots, g_m$ de G tels que, en notant $\langle g_1, \ldots, g_k\rangle$ le sous-groupe engendré par $\{g_1, \ldots, g_k\}$ (i.e. le plus petit sous-groupe contenant $g_1, \ldots, g_k$), on ait

$$\forall k \in [\![2, m \qquad g_k \notin \langle g_1, \ldots, g_{k-1}\rangle$$

et $G = \langle g_1, \ldots, g_m\rangle$ (sinon, on pourrait construire par récurrence une suite $(g_n)_{n\geqslant 1}$ d'éléments de G tels que

$$\forall k \leqslant 2 \qquad g_k \notin \langle g_1, \ldots, g_{k-1}\rangle$$

ce qui contredirait la finitude de G). On vérifie alors que

$$(h_1, \ldots, h_m) \longrightarrow h_1 \ldots h_m$$

est un isomorphisme de $C_{g_1} \times \cdots \times C_{g_m}$ sur $(G,.)$ où $C_g = \{e, g\}$ est le sous-groupe engendré par g. Ou encore, tout élément de G s'écrit de manière unique sous la forme

$$g_1^{\epsilon_1} \ldots g_m^{\epsilon_m}$$

où les ϵ_k sont dans $\{0, 1\}$. L'application

$$g_1^{\epsilon_1} \ldots g_m^{\epsilon_m} \longmapsto g_1^{\epsilon_2} g_2^{\epsilon_2} \ldots g_m^{\epsilon_m}$$

définit alors un automorphisme de G autre que Id si $m \geqslant 2$. Les seuls groupes finis ayant un seul automorphisme sont donc $\{e\}$ et $\{e, g\}$ avec $g^2 = e$.