MPSI 3 - Fermat Le 16.05.23
2022-2023

Devoir à la maison n°7
CORRECTION

Exercice 533

Coefficients trinomiaux

Soient n et p des éléments de $\mathbb{N}^*$. On désigne par $E_{n,p}$ le nombre de solutions $(x_1, x_2, \dots, x_n)$ dans $\mathbb{Z}^n$ de l'équation :

$$\max(|x_1|, |x_2|, \dots, |x_n|) = p.$$

1. Déterminer les nombres $E_{1,p}$ et $E_{2,p}$.
2. Déterminer, en fonction de n et p, le nombre de solutions dans $\mathbb{Z}^n$ de l'inéquation
$$\max(|x_1|, |x_2|, \dots, |x_n|) \leqslant p.$$
En déduire l'expression de $E_{n,p}$ en fonction de n et p.
3. Déterminer une constante C telle que $\lim_{n\to+\infty} \frac{E_{n,n}}{(2n)^n} = C$.
4. (*)Développer $(a+b+c)^n$.
Déterminer en fonction des paramètres n, p et q dans $\mathbb{N}^*$, le nombre de solutions dans $\mathbb{Z}^n$ du système :
$$\begin{cases} \min(|x_1|, |x_2|, \dots, |x_n|) = q \\ \max(|x_1|, |x_2|, \dots, |x_n|) = p \end{cases}$$

1.
$$E_{1,p} = \text{Card}\{x_1 \in \mathbb{Z} \mid \max(|x_1|) = p\} = \text{Card}\{-p, p\} = 2$$
$$E_{2,p} = \text{Card}\{x_1 \in \mathbb{Z} \mid \max(|x_1|, |x_2|) = p\} = \text{Card}\Big([\![-p+1, p-1]\!]\times\{-p,p\}\cup\{-p,p\}\times[\![-p+1,p-1]\!]\cup\{-p,p\}\times\{-p,p\}\Big)$$
$$E_{2,p} = (2(p-1)+1)\times 2 + 2\times(2(p-1)+1) + 4 = 2\times 2\times(2p-1)+4 = 8p$$
$$\boxed{E_{1,p} = 2 \quad , \quad E_{2,p} = 4p+2}$$

2. On raisonne de manière ensembliste :
$$\max(|x_1|, |x_2|, \dots, |x_n|) \leqslant p \iff \forall\, k \in \mathbb{N}_n, |x_k| \leqslant p \iff \forall\, k \in \mathbb{N}_n, x_k \in [\![-p, p]\!]$$
Notons $M_{n,p}$ l'ensemble des solutions dans $\mathbb{Z}^n$ de l'équation : $\max(|x_1|, \dots, |x_n|) \leqslant p$.
On a alors $M_{n,p} = [\![-p,p]\!]^n$ (produit cartésien).
$$\boxed{\text{Le nombre de solutions dans } \mathbb{Z}^n \text{ de l'inéquation } \max(|x_1|, |x_2|, \dots, |x_n|) \leqslant p \text{ est } \text{Card} M_{n,p} = (2p+1)^n.}$$
Notons que les ensembles $(M_{n,p})_p$ sont croissants : $M_{n,p-1} \subset M_{n,p}$.
Ce que l'on cherche en fait, c'est
$$\boxed{E_{n,p} = \text{Card}(M_{n,p} \setminus M_{n,p-1}) = (2p+1)^n - (2(p-1)+1)^n = (2p+1)^n - (2p-1)^n}$$
Cela peut s'écrire sous forme d'une somme (binôme de Newton, ou petits Bernoullis), mais on laisse pour le moment.
On confirme : pour $n=1$, on a $E_{1,p} = (2p+1)^1 - (2p-1)^1 = 2$ et $E_{2,p} = (2p+1)^2 - (2p-1)^2 = 8p$.

3. On a donc, pour $n \in \mathbb{N}$,
$$\frac{E_{n,n}}{(2n)^n} = \frac{(2n+1)^n}{(2n)^n} - \frac{(2n-1)^n}{(2n)^n} = \left(1 + \frac{1/2}{n}\right)^n - \left(1 - \frac{1/2}{n}\right)^n \longrightarrow e^{1/2} - e^{-1/2} = 2\text{sh}\frac{1}{2}$$
$$\boxed{\lim_{n\to+\infty} \frac{E_{n,n}}{(2n)^n} = e^{1/2} - e^{-1/2} = 2\text{sh}\frac{1}{2} (\approx 1,04219)}$$

4. On peut appliquer dirrectement la formule du trinôme de Newton, on peut aussi faire deux binômes :
$$(a+b+c)^n = ((a+b)+c)^n = \sum_{h=0}^{n} \binom{n}{h} (a+b)^h c^{n-h} = \sum_{h=0}^{n}\sum_{i=0}^{h} \binom{n}{h}\binom{h}{i} a^i b^{h-i} c^{n-h}$$

Or $\binom{n}{h}\binom{h}{i} = \dfrac{n!h!}{h!(n-h)!i!(h-i)!} = \dfrac{n!}{i!(h-i)!(n-h)!}$. Donc

$$(a+b+c)^n = \sum_{0\leqslant i\leqslant h\leqslant n} \frac{n!}{i!(h-i)!(n-h)!}a^i b^{h-i}c^{n-h} = \sum_{i=0}^{n}\sum_{h=i}^{n} \frac{n!}{i!(h-i)!(n-h)!}a^i b^{h-i}c^{n-h} = \sum_{i=0}^{n}\sum_{j=0}^{n-i} \frac{n!}{i!j!(n-i-j)!}a^i b^j c^{n-i-j}$$

en faisant le changement de variable : h remplacé en $j = h - i$.

On facilite la notation en considérant la variable muette k, le nombre égal à $n-i-j$, i.e tel que $i+j+k = n$:

$$\boxed{(a+b+c)^n = \sum_{i+j+k=n} \frac{n!}{i!j!k!}a^i b^j c^k}$$

Pour $n = 1$, on trouve les nombres $E_{1,p,q} = 0$ si $p \neq q$ et $E_{1,p,p} = 2$.

Pour $n = 2$, on trouve les nombres

$E_{2,p,q} = \text{Card}\{(p,q),(p,-q),(-p,q),(-p,-q),(q,p),(q,-p),(-q,p),(-q,-p)\} = 8$ si $p \neq q$

et $E_{2,p,p} = \text{Card}\{(p,p),(-p,p),(p,-p),(-p,-p)\} = 4$.

Dans le cas n général, mais pour $p = q$, on trouve $E_{n,p,p} = 2^n$

(pour chaque x_i, on a deux possibilités : $x_i = p$ ou $x_i = -p$).

On suppose donc maintenant que $p > q$.

On note i, le nombre de termes dont la valeurs absolues vaut p, j ceux qui valent q.

En fait, plus précisément, on a l'équivalent :

$$\begin{cases} \min(|x_1|,|x_2|,\dots,|x_n|) = q \\ \max(|x_1|,|x_2|,\dots,|x_n|) = p \end{cases} \Longleftrightarrow \exists\, i,j \in \mathbb{N} \text{ tel que } (\star) \begin{cases} \text{Card}\{h \mid |x_h| = p\} = i \geqslant 1, \\ \text{Card}\{h \mid |x_h| = q\} = j \geqslant 1, \\ \text{Card}\{h \mid q < |x_h| < p\} = n-i-j \geqslant 0 \end{cases}$$

Notons $A_{i,j,p,q,n} = \{(x_1,x_2,\dots x_n) \in \mathbb{Z}^n \mid (\star)\}$.

Un élément de $A_{i,j,p,q,n}$ est parfaitement déterminé par :

— le choix des i nombres dont la valeur absolue vaut p : $\binom{n}{i}$ possibilités.

— Puis, pour chacun de ces i nombres, il y a 2 possibilités de valeurs : p ou $-p$. Donc 2^i possibilités.

— Puis, le choix des j nombres dont la valeur absolue vaut q : $\binom{n-i}{j}$ possibilités.

— Puis pour chacun de ces j nombres, il y a 2 possibilités de valeurs : q ou $-q$. Donc 2^j possibilités.

— Puis, pour les $n-i-j$ nombres restants, il y a $\text{Card}([\![-p+1,-q-1]\!] \cup [\![q+1,p-1]\!]) = 2(p-q-1)$. Donc $(2(p-q-1))^{n-i-j}$ possibilités.

Les ensembles $A_{i,j,p,q,n}$ sont disjoints, on a cherche donc :

$$\text{Card}\left(\bigcup_{1\leqslant i,1\leqslant j,i+j\leqslant n} A_{i,j,p,q,n}\right) = \sum_{i=1}^{n-1}\sum_{j=1}^{n-i} \frac{n!}{i!j!(n-i-j)!}2^i 2^j (2(p-q-1))^{n-i-j}$$

Avec $k = n-i-j$, on trouve le nombre (avec une formule de crible) :

$$\sum_{i+j+k=n} \frac{n!}{i!j!k!}2^i 2^j (2(p-q-1))^k - \underbrace{\sum_{j+k=n} \frac{n!}{j!k!}2^j (2(p-q-1))^k}_{i=0} - \underbrace{\sum_{i+k=n} \frac{n!}{i!k!}2^i (2(p-q-1))^k}_{j=0} + \underbrace{\sum_{k=n} \frac{n!}{k!}(2(p-q-1))^k}_{i=0,j=0}$$

$$\boxed{\begin{aligned} E_{n,p,q} &= (2+2+2(p-q-1))^n - (2+2(p-q-1))^n - (2+2(p-q-1))^n + (2(p-q-1))^n \\ &= (2+2p-2q)^n - 2(2p-2q)^n + (2p-2q-2)^n \end{aligned}}$$

Exercice 538

Indicatrice d'Euler

On note pour tout $n \in \mathbb{N}$, $\varphi(n) = \text{Card}(\{m \in \mathbb{N}^* \leqslant n \mid m \wedge n = 1\}$.

1. Que vaut $\varphi(n)$ si n est un nombre premier.
2. Montrer que si n est un nombre de la forme p^a, avec p premier, alors $\varphi(n) = n\frac{p-1}{p}$
3. On suppose que $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r}$, décomposition en produit de nombres premiers. On note A_i, l'ensemble des multiples de p_i, plus petit que n.
   (a) Exprimer simplement $\varphi(n)$ en fonction de $A_1 \cup A_2 \cdots \cup A_r$.
   (b) Montrer que $\text{Card}(A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k})$ se calcule facilement (une division)
   (c) Développer le produit $n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$
   (d) En exploitant le crible de Poincaré, montrer que si $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r}$,
   $$\varphi(n) = n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})$$
4. Autre méthode (sans exploiter la question précédente).
   (a) Montrer que pour tout $n, m \in \mathbb{N}$, $\varphi(n \times m) = \varphi(n) \times \varphi(m)$.

(b) Retrouver que si $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r}$,

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})$$

5. Montrer que pour tout $n \in \mathbb{N}$, $\displaystyle\sum_{d|n} \varphi(d) = n$.

On note pour tout $n \in \mathbb{N}$, $\varphi(n) = \text{Card}(\{m \in \mathbb{N}^* \leqslant n \mid m \wedge n = 1\}$.

1. Si n est premier, alors pour tout $m \in \{1, 2, \dots, n-1\}$, $m \wedge n = 1$.

$$\boxed{\text{Donc } \varphi(n) = \text{Card}\big([\![1, n-1]\!]\big) = (n-1) - 1 + 1 = n - 1.}$$

2. Soit p un nombre premier et $a \in \mathbb{N}^*$.
Soit $m \in [\![1, p^a]\!]$, et $\delta = m \wedge p^a$, alors δ divise p^a.
Comme p est premier, alors δ est une puissance de p et donc ou bien $\delta = 1$ ou $p|\delta$.
Dans le second cas, on a donc $p|m$.
Ainsi, $m \wedge p^a \neq 1 \Longrightarrow p|m \Longleftrightarrow m \in \{p, 2p, 3p, \dots kp\}$ avec $kp \leqslant p^a < (k+1)p$ $(*)$.
La réciproque est vraie : si $p|m$, alors $p|m \wedge p^a$ et donc $m \wedge p^a \neq 1$.
En divisant par p les inégalités $(*)$, on trouve $k \leqslant p^{a-1} < k + 1$.
et comme p^{a-1} est entier, on a donc $k = p^{a-1}$.

$$\boxed{\varphi(p^a) = \text{Card}\big(\mathbb{N}_{p^a} \setminus \{p, 2p, \dots kp\}\big) = p^a - k = p^a - p^{a-1} = (p-1)p^{a-1} = (p-1)\frac{p^a}{p}}$$

3. On suppose que $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r}$, décomposition en produit de nombres premiers.
On note A_i, l'ensemble des multiples de p_i, plus petit que n.
(a) En raisonnant avec les valuations p-adique, on a : $m \wedge n = 1 \Longleftrightarrow \forall\, i \in \mathbb{N}_r, v_{p_i}(m) = 0$.

$$m \wedge n \neq 1 \Longleftrightarrow \exists\, i \in \mathbb{N}_r, v_{p_i}(m) > 0 \Longleftrightarrow \exists\, i \in \mathbb{N}_r, m \in A_i \Longleftrightarrow m \in A_1 \cup A_2 \cup \cdot \cup A_r$$

On a alors, en terme de cardinal :

$$\boxed{\varphi(n) = \text{Card}\left(\mathbb{N}_n \setminus \big(A_1 \cup A_2 \cup \cdot \cup A_r\big)\right) = n - \text{Card}(A_1 \cup A_2 \cup \cdot \cup A_r)}$$

(b) On a encore les équivalences : $h \in A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k} \Longleftrightarrow \forall\, s \in \mathbb{N}_k, h \in A_{i_s} \Longleftrightarrow \forall\, s \in \mathbb{N}_k, p_{i_s}|h$
Comme les nombres p_{i_s} sont premiers entre eux, on a donc (corollaire de Gauss) :

$$h \in A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k} \Longleftrightarrow p_1 p_2 \dots p_{i_k}|h$$

Donc $A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k} = p_1 p_2 \dots p_{i_k}\mathbb{Z}$.
En ajoutant la condition que les nombre h sont plus petit que n, on trouve

$$\boxed{\text{Card} A_{i_1} \cap A_{i_2} \cdots \cap A_{i_k} = \left\lfloor \frac{n}{p_1 p_2 \dots p_{i_k}} \right\rfloor = \frac{n}{p_1 p_2 \dots p_{i_k}} \text{ (division exacte)}}$$

(c) On rappelle que $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r}$, donc

$$\begin{aligned} n(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_r}) &= \frac{p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1)}{p_1 p_2 \dots p_r} \\ &= \underbrace{p_1^{a_1 - 1} p_2^{a_2 - 1} \dots p_r^{a_r - 1}}_{=:P} (-1)^r (1 - p_1)(1 - p_2) \cdots (1 - p_r) \\ &= (-1)^r [P - (p_1 P + p_2 P + \dots p_r P) + (p_1 p_2 P + p_1 p_3 P + \dots p_{r-1} p_r P) \\ &\quad - \cdots + (-1)^r p_1 p_2 \dots p_r P] \end{aligned}$$

Donc avec $P = \dfrac{n}{p_1 p_2 \dots p_r} = p_1^{a_1 - 1} p_2^{a_2 - 1} \dots p_r^{a_r - 1}$, on a $((-1)^{r+h} = (-1)^{r-h})$:

$$\boxed{n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r}) = P \times \left(\sum_{h=0}^{r} (-1)^{r-h} \prod_{i_1 < i_2 \cdots < i_h} p_{i_1} p_{i_2} \cdots p_{i_h} \right)}$$

(d) On suppose toujours que $n = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_r^{a_r}$. On a vu en 3.$a$)

$$\varphi(n) = n - \text{Card}\left(\bigcup_{i=1}^{r} A_i \right) = n - \sum_{k=1}^{r} (-1)^{k-1} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \text{Card}(A_{i_1} \cap \cdots \cap A_{i_k})$$

$$\varphi(n) = n + \sum_{k=1}^{r} (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}$$

d'après la formule du crible de Poincaré.
En faisant le changement de variable : $\{i_1,\dots i_k\}\mapsto\big(\mathbb{N}_r\setminus\{i_1,\dots i_k\}\big)=\{j_1,\dots j_h\}$, on trouve (avec $h=r-k$) :

$$\varphi(n)=n+\sum_{h=0}^{r-1}(-1)^{r-h}\sum_{1\leqslant j_1<\dots<j_h\leqslant n}\frac{n}{p_1p_2\cdots p_r}p_{j_1}\dots p_{j_h}$$

Ce qui donne le même résultat qu'à la question précédente :

$$\boxed{\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_r})}$$

4. Autre méthode (sans exploiter la question précédente).
(a) Soient $n,m\in\mathbb{N}$ avec $n\wedge m=1$.
C'est une conséquence du lemme des restes chinois. Mais nous n'en parlons pas ici.
Notons, pour tout entier N, $P_N=\{k\in[\![0,N-1]\!]\mid k\wedge N=1\}$. On a donc $\varphi(N)=\mathrm{Card}P_N$.
Commençons par une équivalence importante :

$$k\wedge(mn)=1\Longleftrightarrow k\wedge m=1 \text{ et } k\wedge n=1$$

Soit $\varphi:[\![0,nm-1]\!]\mapsto[\![0,n-1]\!]\times[\![0,m-1]\!]$, $c\mapsto(a,b)$,
où $a=c\%n$ (reste dans la division euclidienne de c par n) et $b=c\%m$.
φ est parfaitement définie.
Alors si $c\wedge nm=1$, nécessairement : $c\wedge n=1$ et donc $a\wedge n=1$ et $b\wedge m=1$.
Par conséquent, $\varphi(P_{nm})\subset P_n\times P_m$.
Montrons la surjectivité : Soit $(a,b)\in P_n\times P_m$.
Comme $n\wedge m=1$, il existe $u,v\in\mathbb{Z}$ tq $un+vm=1$ et donc $u(a-b)n+v(a-b)m=a-b$.
Soit $k_1=v(a-b)\%n$ et $k_2=u(a-b)\%m$ et enfin $c=k_2n+a$.
Alors comme $k_2\leqslant m-1$, $c\leqslant n(m-1)+a\leqslant n(m-1)+(n-1)=nm-1$.
Puis $c\equiv a[n]$ et mieux : $c\%n=a$, car $a\in[\![0,n-1]\!]$.
Enfin $c=k_2n+a=(u(a-b)+Km)n+a=v(a-b)m+b-a+Kmn+a$
$c=(k_1+K'n)m+b+Kmn=b+K''m$.
Donc $c\equiv b[m]$ et comme $b\in[\![0,m-1]\!]$, $b=c\%m$.
Ainsi, $\varphi(c)=(a,b)$. En enfin, $c\wedge mn=1$ (par l'absurde).
Donc φ établit une surjection de P_{nm} sur $P_n\times P_m$.
Reste à montrer l'injectivité.
Soit $c,c'\in P_{nm}$ tels que $\varphi(c)=\varphi(c')$.
Alors $c\%n=c'\%n$, donc $n|c-c'$ et de même $m|c-c'$.
Donc $nm|c-c'$ car $n\wedge m=1$. Donc $c-c'\in(nm)\mathbb{Z}$
Or $c-c'\in[\![-nm+1,nm-1]\!]$. La seule possibilité : $c=c'$.
On a donc en regardant les cardinaux, pour tout $n,m\in\mathbb{N}$ avec $n\wedge m=1$:

$$\boxed{\varphi(n\times m)=\mathrm{Card}P_{nm}=\mathrm{Card}(P_n\times P_m)=\mathrm{Card}P_n\times\mathrm{Card}P_m=\varphi(n)\times\varphi(m).}$$

(b) On applique la relation précédente, par récurrence, puisque $p_s^{a_s}\wedge\big(p_1^{a_1}\times\dots\times p_{s-1}^{a_{s-1}}\big)=1$. Donc

$$\varphi(n)=\prod_{i=1}^{r}\varphi(p_i^{a_i})=\prod_{i=1}^{r}p_i^{a_i-1}(1-p_i)$$

On retrouve un calcul numérique de la question 3.(c). Donc

$$\boxed{\text{Donc si } n=p_1^{a_1}\times p_2^{a_2}\times\dots\times p_r^{a_r},\ \varphi(n)=n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\cdots(1-\tfrac{1}{p_r}).}$$

5. Notons d'abord que $\varphi(1)=1=\sum_{d|1}\varphi(d)$. Le résultat est vrai pour $n=1$.
Considérons ensuite le cas $n=p^a$, où p est un nombre premier.
Alors $d|n\Leftrightarrow d=p^i$ avec $i\in[\![0,a]\!]$. Donc

$$\sum_{d|p^a}\varphi(d)=\sum_{i=0}^{a}\varphi(p^i)=\varphi(1)+\sum_{i=1}^{a}p^i\frac{p-1}{p}=1+(p-1)\times\sum_{i=1}^{a}p^{i-1}=1+(p-1)\frac{1-p^a}{1-p}=p^a=n$$

Montrons maintenant le résultat sur r le nombre de nombres premiers dans la décomposition de n.
Supposons que le résultat est vraie pour tout n décomposé en r nombres premiers.
Considérons $n=\underbrace{p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}}_{n'}p_{r+1}^{a_{r+1}}$.
$d|n\Longleftrightarrow\exists\ i\in[\![0,a_{r+1}]\!]$ tel que $d=d'p_{r+1}^i$ avec $d'|n'$.
Donc $\{d\in\mathbb{N}\mid d|n\}=\{d'\times p_{r+1}^i\mid d'|n',i\in[\![0,a_{r+1}]\!]\}$.

$$\sum_{d|n}\varphi(d)=\sum_{i=0}^{a_{r+1}}\sum_{d'|n'}\varphi(d'p_{r+1}^i)=\sum_{i=0}^{a_{r+1}}\varphi(p_{r+1}^i)\times\sum_{d'|n'}\varphi(d')=p_{r+1}^{a_{r+1}}\times n'=n$$

car $d'\wedge p_{r+1}^i=1$ et d'après $\mathcal{P}_n$.

$$\boxed{\sum_{d|n}\varphi(d)=n}$$