Quelques exemples d'utilisation de combinatoire en théorie des nombres

Monastir, 2014

Emmanuel Royer

Laboratoire de mathématiques
UMR 6620
Université Blaise Pascal
Clermont-Ferrand

Soit f une forme primitive de poids k et niveau sans facteur carré N. On rappelle que l'ensemble $\mathrm{H}_k^*(N)$ de telles formes est une base de l'espace vectoriel des formes modulaires paraboliques qui sont nouvelles. En particulier, si $f \in \mathrm{H}_k^*(N)$, alors f admet un développement de Fourier de la forme

$$f(z) = \sum_{n=1}^{+\infty} \lambda_f(n) n^{(k-1)/2} e(nz).$$

On a

$$\lambda_f(n) = \prod_{p^\nu \| n} \mathrm{X}_\nu\left(\lambda_f(p)\right)$$

où X_ν est un polynôme de Tchebytchef définit sur $[-2, 2]$ par

$$\mathrm{X}_\nu(2\cos\theta) = \frac{\sin(\nu+1)\theta}{\sin\theta}.$$

Si $r \geq 1$, la fonction L de carré symétrique de f est définie par

$$L(\mathrm{Sym}^2 f, s) = \prod_{p \mid N} \left(1 - \frac{\lambda_f(p)^2}{p^s}\right)^{-1} \times \prod_{p \nmid N} \det\left(I - \frac{1}{p^s} \mathrm{Sym}^2 \begin{pmatrix} e^{i\theta_f(p)} & 0 \\ 0 & e^{-i\theta_f(p)} \end{pmatrix}\right)^{-1}$$

où $\theta_f(p) = 2\cos\theta_f(p)$. Le produit eulérien se développe en une série de Dirichlet

$$L(\mathrm{Sym}^2 f, s) = \sum_{n=1}^{+\infty} \lambda_{\mathrm{Sym}^2 f}(n) n^{-s}$$

absolument convergente pour $\mathfrak{Re}\, s > 1$.

La suite $\left(\lambda_{\mathrm{Sym}^2 f}(n)\right)_{n\geq 1}$ jouit d'intéressantes propriétés. Kamel Mazouda a par exemple montré en 2009 que lorsque p est fixé et f varie, alors la suite $\left(\lambda_{\mathrm{Sym}^2 f}(p)\right)_{f\in \mathrm{H}_k^*(N)}$ est asymptotiquement équidistribuée pour la mesure

$$\frac{p+1}{2\pi}\frac{1}{(p^{1/2}+p^{-1/2})^2-(x+1)}\sqrt{\frac{3-x}{1+x}}\,\mathrm{d}x.$$

Si F est continue sur $[-1,3]$, alors

$$\lim_{N\to+\infty}\frac{1}{\mathrm{H}_k^*(N)}\sum_{f\in\mathrm{H}_k^*(N)}F\left(\lambda_{\mathrm{Sym}^2 f}(p)\right)$$
$$=\int_{-1}^{3}F(x)\frac{p+1}{2\pi}\frac{1}{(p^{1/2}+p^{-1/2})^2-(x+1)}\sqrt{\frac{3-x}{1+x}}\,\mathrm{d}x.$$

Grâce aux travaux de Shimura, on sait que la fonction $L(\mathrm{Sym}^2 f, s)$ admet un prolongement en fonction entière et satisfait à l'équation fonctionnelle

$$\begin{aligned} &L\left(\mathrm{Sym}^2 f_\infty, s\right) L\left(\mathrm{Sym}^2 f, s\right) \\ &\qquad = \left(N^2\right)^{-s+1/2} L\left(\mathrm{Sym}^2 f_\infty, 1-s\right) L\left(\mathrm{Sym}^2 f, 1-s\right) \end{aligned}$$

avec

$$L\left(\mathrm{Sym}^2 f_\infty, s\right) = \pi^{-3s/2}\Gamma\left(\frac{s+1}{2}\right)\Gamma\left(\frac{s+k-1}{2}\right)\Gamma\left(\frac{s+k}{2}\right).$$

Pour tout entier $n \geq 0$, on définit

$$\mathrm{M}_{-n}(N) = \frac{1}{\#\mathrm{H}_k^*(N)} \sum_{f \in \mathrm{H}_k^*(N)} L(\mathrm{Sym}^2 f, 1)^{-n-1}.$$

Par des techniques classiques d'analyse, on démontre que

$$\mathrm{M}_{-n}(N) = \mathrm{M}_{-n} + \mathrm{O}_{-n}\left(N^{-\varepsilon} + \frac{N^{\varepsilon}}{\mathrm{P}^-(N)}\right)$$

où $\mathrm{P}^-(N)$ est le plus petit facteur premier de N. Lorsque N tend vers $+\infty$ sans petit facteur carré, les moments négatifs admettent donc une limite que nous voulons étudier.

Cette limite est une série de Dirichlet

$$M_{-n} = \frac{1}{\zeta(2)} \sum_{r=1}^{+\infty} \frac{m_{-n}(r)}{r} = \frac{1}{\zeta(2)} \prod_{p\in\mathcal{P}} \sum_{\nu=0}^{+\infty} \frac{m_{-n}(p^\nu)}{p^\nu}.$$

avec

$$m_{-n}(r) = \sum_{\substack{\boldsymbol{a},\boldsymbol{b},\boldsymbol{c}\in\mathbb{N}^n \\ \prod_{i=1}^n (a_i b_i^2 c_i^3) = r}} \left(\prod_{j=1}^n \mu(a_j b_j c_j) \mu(b_j) \right) \sum_{\substack{\boldsymbol{d}\in\mathcal{E}_n(a_1 b_1, \dots, a_n b_n) \\ \prod_{i=1}^n a_i b_i = \prod_{i=1}^n d_i}} 1$$

où

$$\mathcal{E}_n(\boldsymbol{b}) = \left\{ \boldsymbol{d} \in \mathbb{N}^{n-1} : \, d_i \mid \left(\frac{b_1 \cdots b_i}{d_1 \cdots d_{i-1}}, b_{i+1} \right), \forall i \in [1, n-1] \right\}.$$

La multiplicativité des coefficients de Dirichlet permet de n'avoir à étudier que $m_{-n}(p^\nu)$.

La fonction de Möbius, μ transforme l'étude de $m_{-n}(p^\nu)$ en un question de comptage combinatoire.

Pour $n \geq 2$ et $\nu \geq 0$, on définit $a_n(\nu)$ comme le nombre de

$$(\alpha, \beta, \gamma, \delta) \in \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \times \{0,1,2\}^{n-1}$$

tels que

1. si $i \in \{1, \dots, n\}$, alors $0 \leq \alpha_i + \beta_i + \gamma_i \leq 1$
2. si $i \in \{1, \dots, n-1\}$, alors
$$\delta_i \leq 2 \min\left(\sum_{j=1}^{i} (\alpha_j + \beta_j) - \sum_{j=1}^{i-1} \delta_j, \alpha_{i+1} + \beta_{i+1}\right)$$
3. $$\sum_{i=1}^{n} (\alpha_i + 2\beta_i + 3\gamma_i) = \nu$$
4. $$\sum_{i=1}^{n} (\alpha_i + \beta_i) = \sum_{i=1}^{n-1} \delta_i.$$

On a alors

$$M_n = \frac{1}{\zeta(2)} \prod_{p \in \mathcal{P}} f_n\left(-\frac{1}{p}\right)$$

avec

$$f_n(X) = \sum_{n=0}^{3n} a_n(\nu) X^{\nu}.$$

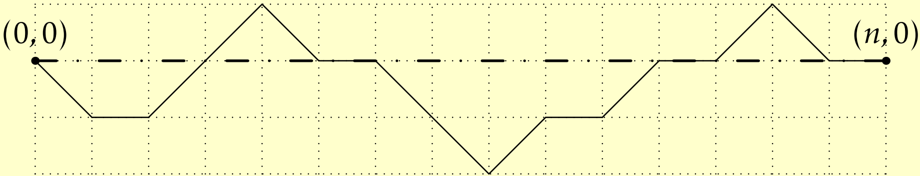
Cette expression conduit ensuite à

$$M_{-n} = \frac{1}{\zeta(2)\zeta(3)^n} \prod_{p \in \mathcal{P}} \sum_{h=0}^{n} (-1)^h \binom{n}{h} R_h \left(\frac{p}{p^2+p+1}\right)^h$$

où R_h est le nombre de chemin de Riordan de longueur $h-2$ ($R_0 = 1, R_1 = 0$).

On appelle nombre de Riordan d'indice $n+2$ le nombre de chemin de $\mathbb{Z}^2$ reliant $(0,0)$ à $(n,0)$

1. par des pas $(1,0)$, $(1,1)$ ou $(1,-1)$
2. sans jamais passer par des points d'ordonnée strictement positive
3. *sauf* par la succession d'un double pas $(1,1)$–$(1,-1)$.



La série génératrice est

$$\sum_{n=0}^{+\infty} R_n x^n = \frac{2}{1+x+\sqrt{1-2x-3x^2}}.$$

On rappelle que

$$M_{-n} = \frac{1}{\zeta(2)\zeta(3)^n} \prod_{p\in\mathcal{P}} \underbrace{\sum_{h=0}^{n} (-1)^h \binom{n}{h} R_h \left(\frac{p}{p^2+p+1}\right)^h}_{\ell_n\left(\frac{p}{p^2+p+1}\right)}$$

La série génératrice des nombres de Riordan permet d'obtenir l'expression intégrale

$$\ell_n(x) = \frac{4}{\pi}\int_0^{\pi/2} \left(1 + x - 4x\sin^2\theta\right)^n \cos^2\theta \,\mathrm{d}\theta$$

puis d'obtenir

$$\log \mathrm{M}_{-n} = n\log\log n + n\log\left(\frac{e^\gamma}{\zeta(2)^2}\right) + \mathrm{O}\left(\frac{n}{\log n}\right).$$

De

$$\log \mathrm{M}_{-n} = n \log\log n + n \log\left(\frac{e^{\gamma}}{\zeta(2)^2}\right) + O\left(\frac{n}{\log n}\right).$$

on déduit, pour tout $K > 0$ l'existence de N et $f \in \mathrm{H}_k^*(N)$ tel que

$$0 \leq L(\mathrm{Sym}^2 f, 1)^{-1} \leq K.$$

Pour $n \geq 0$, on définit

$$\mathrm{M}_n(N) = \frac{1}{\mathrm{H}_k^*(N)} \sum_{f \in \mathrm{H}_k^*(N)} L(\mathrm{Sym}^2 f, 1)^{n-1}$$

et on a

$$\mathrm{M}_n(N) = M_n + \mathrm{O}\left(N^{-\varepsilon} + \frac{N^{\varepsilon}}{\mathrm{P}^-(N)}\right)$$

avec

$$\mathrm{M}_n = \zeta(2)^{n-1} \sum_{r=1}^{+\infty} \frac{m_n(r)}{r} = \zeta(2)^{n-1} \prod_{p \in \mathcal{P}} \sum_{\nu=0}^{+\infty} \frac{m_n(p^\nu)}{p^\nu}$$

et

$$m_n(r) = \sum_{\substack{\boldsymbol{b} \in \mathbb{N}^n \\ \prod_{i=1}^n b_i = r}} \sum_{\substack{\boldsymbol{d} \in \mathcal{E}_n(\boldsymbol{b}) \\ \prod_{i=1}^{n-1} d_i = r}} 1.$$

L'absence de fonction de Möbius dans l'expression des coefficients de Dirichlet rend la combinatoire plus difficile. On trouve cependant

$$\mathrm{M}_{n+2} = \frac{\zeta(2)^{3n+2}\zeta(3)^n}{\zeta(6)^n} \prod_{in\mathcal{P}} \ell_n\left(-\frac{p}{p^2-p+1}\right).$$

Une première étape consiste à montrer

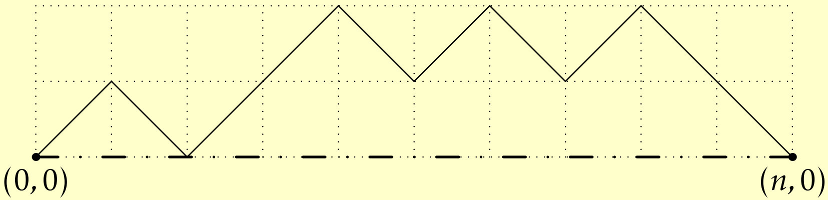
$$\mathrm{M}_n = \zeta(2)^{n-1} \prod_{p\in\mathcal{P}} S_n\left(\frac{1}{p}\right)$$

avec

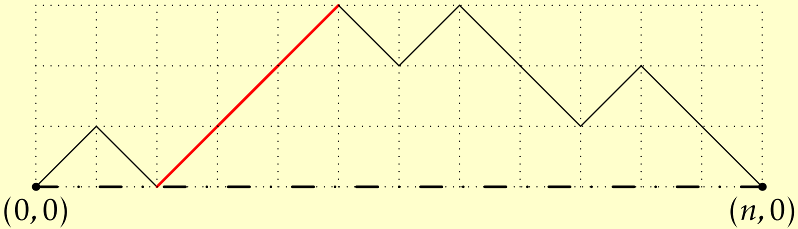
$$S_n(q) = \sum_{\substack{\boldsymbol{\alpha}\in\mathbb{N}^{n+1} \\ \alpha_0=\alpha_n=0}} \prod_{i=0}^{n-1} \left(q^{|\alpha_i-\alpha_{i+1}|} + \cdots + q^{\alpha_i+\alpha_{i+1}}\right).$$

On relie cette quantité aux chemins de Dyck avec statistiques prescrites.

Un chemin de Dyck est un chemin de $\mathbb{Z}^2$ reliant $(0,0)$ à $(n,0)$ par des pas $(1,1)$ ou $(1,-1)$ et ne passant jamais sous l'axe des abscisses.

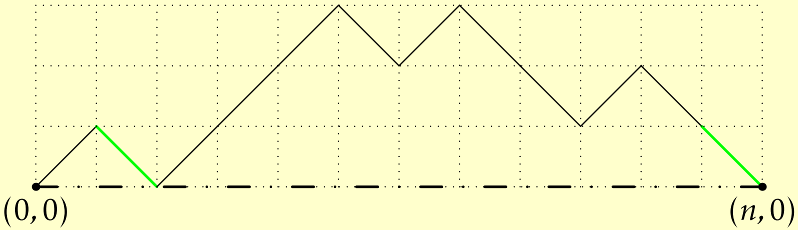


Une double montée d'un chemin de Dyck est une succession de deux pas $(1,1)$.



On note $DBM(D)$ le nombre de montée d'un chemin de Dyck D. Ici, $DBM(D) = 2$.

Un pas de retour d'un chemin de Dyck est un pas dont l'extrémité droite touche l'axe des abscisses.



On note $RET(D)$ le nombre de montée d'un chemin de Dyck D. Ici, $RET(D) = 2$.

On note $\mathcal{D}_n$ l'ensemble des chemins de Dyck de point terminal $(n, 0)$. La fonction génératrice des chemins de $\mathcal{D}_n$ de statistique (RET, DBM) est

$$A_n(x,y) = \sum_{D \in \mathcal{D}_n} x^{RET(D)} y^{DBM(D)}.$$

On montre que

$$\sum_{n=0}^{+\infty} A_n(x,y) t^n = \frac{2 - x + x(y-1)t - x\sqrt{1 - 2(1+y)t + (1-y)^2 t^2}}{2\left(1 - x + x(x+y-1)t\right)}.$$

On a

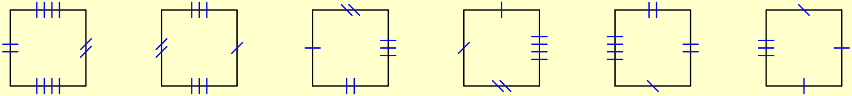
$$S_{n+1}(q) = \frac{1}{(1-q)^n(1-q^2)^n} A_n(1-q, q^2)$$

et, par comparaison des séries génératrices

$$A_n(1-q, q^2) = \frac{(1-q)^n(1+q^3)^{n-1}}{(1-q^2)^{n-1}} \ell_{n-1}\left(-\frac{q}{1-q+q^2}\right).$$

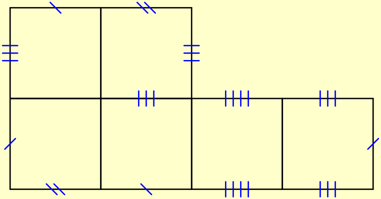
L'expression voulue en résulte.

Une surface à petits carreaux est une collection de carrés unités avec identifications de côtés opposés.



- Chaque côté supérieur est identifié à un unique côté inférieur ;
- Chaque côté gauche est identifié à un unique côté droit.

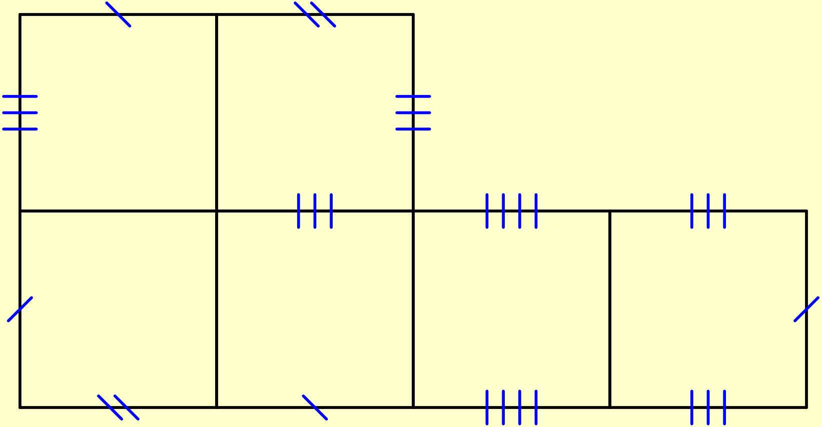
On exige de plus que la surface obtenue après identifications soit connexe.

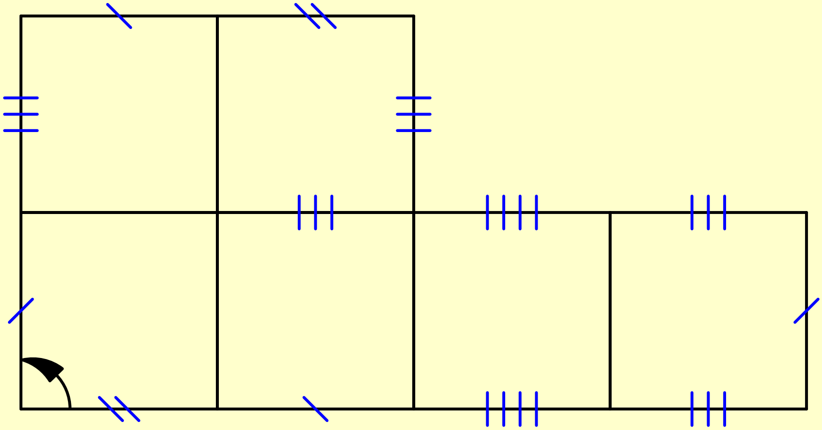


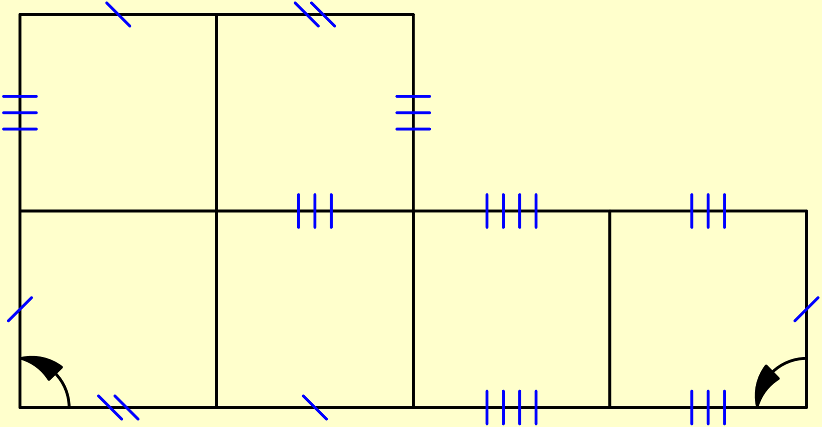
On obtient un revêtement ramifié du tore $\mathbb{R}/\mathbb{Z}$ avec un seul point de ramification (l'origine du tore).
En notant $2\pi(k_i+1)$ les angles des préimages de ce point de ramification, la formule de Riemann-Hürwitz implique que le genre g de la surface à petits carreaux est donné par

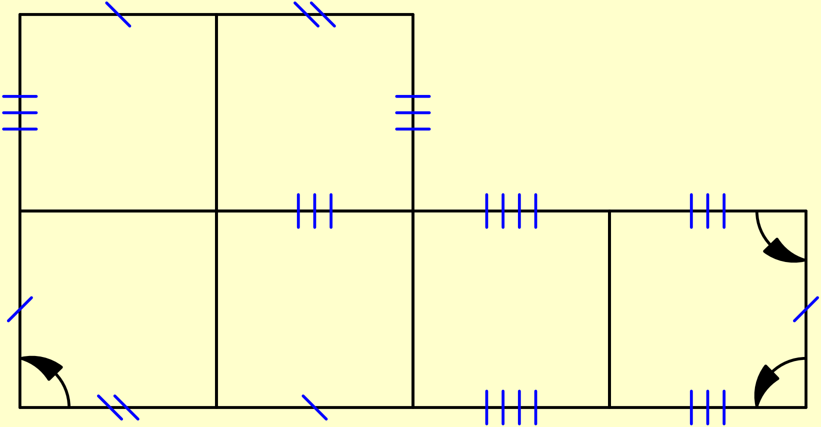
$$\sum_i k_i = 2g-2.$$

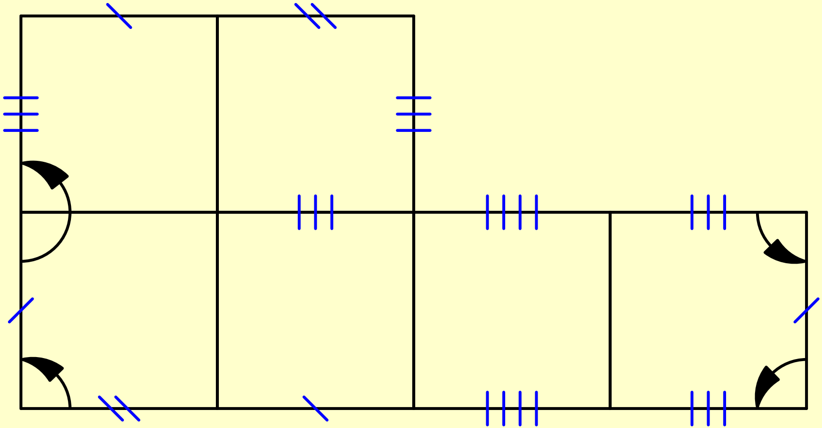
On note $\mathcal{H}(k_1,\ldots,k_d)$ l'ensemble des surfaces (non équivalentes) d'angles $2\pi(k_i+1)$.

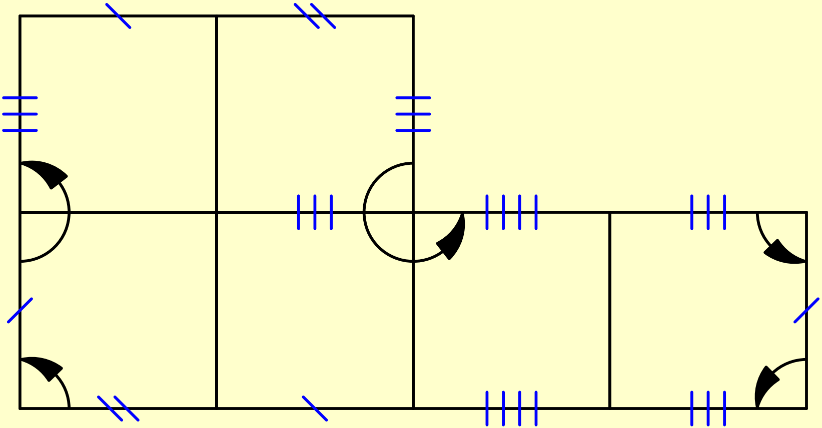


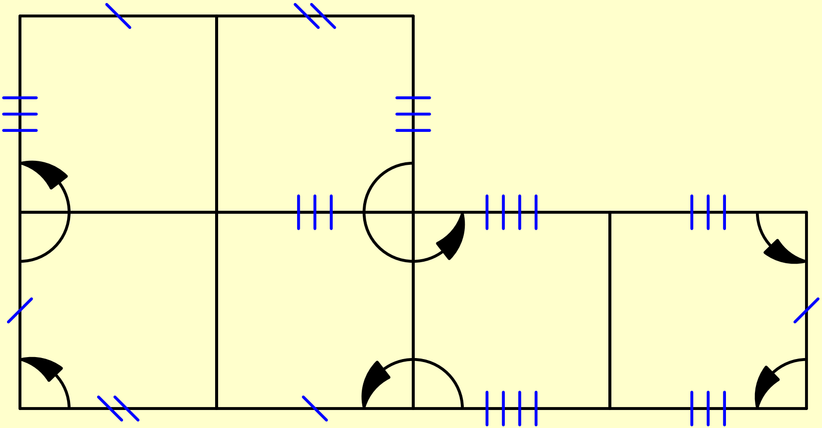


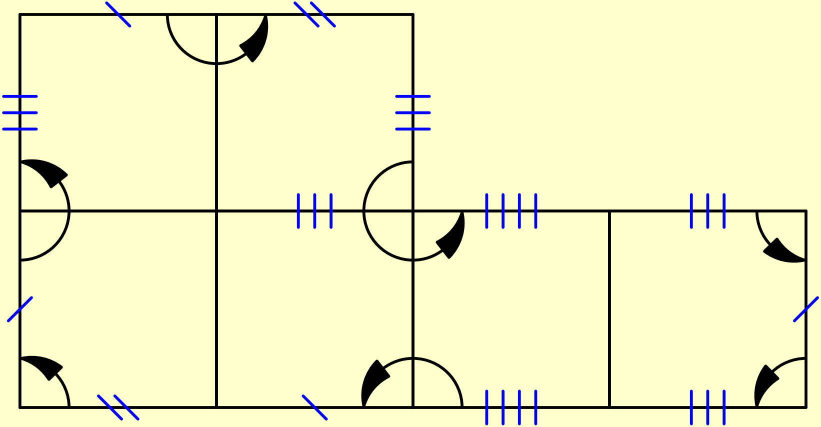




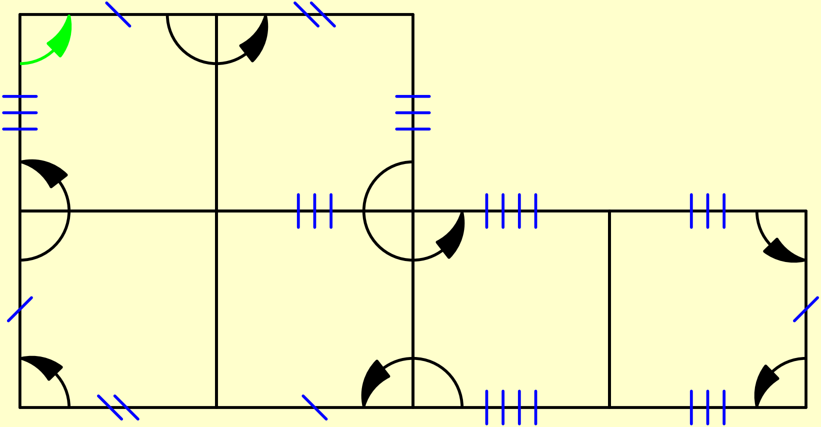




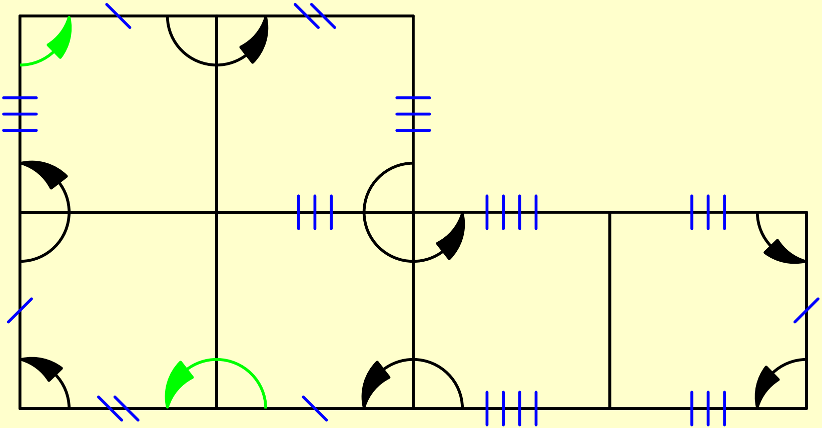




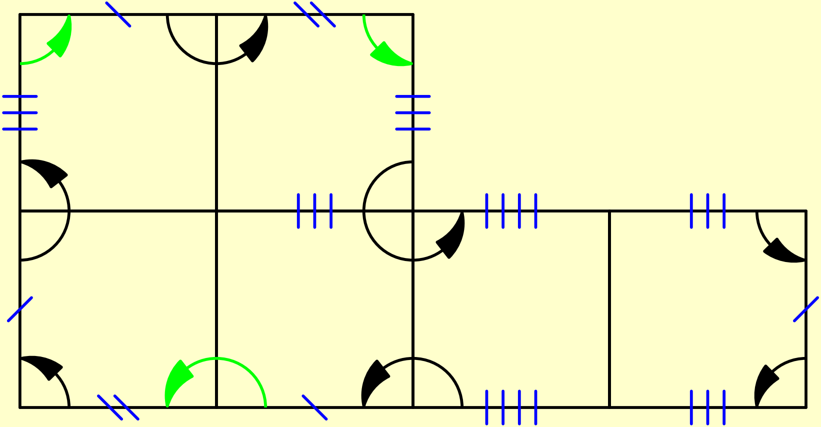
Un angle de 6π



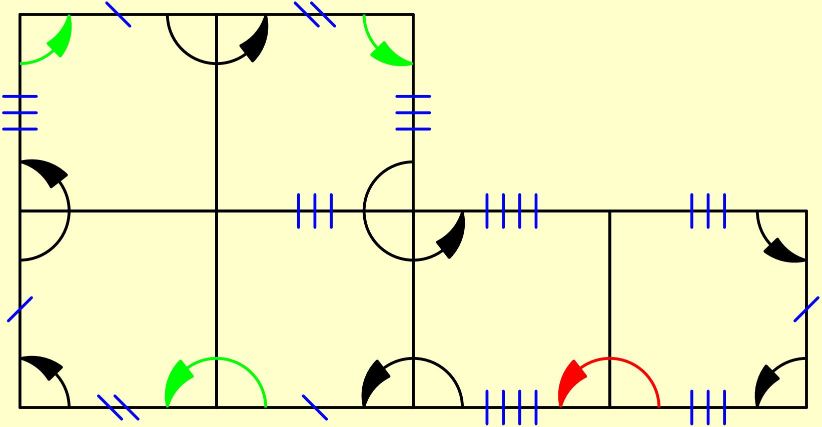
Un angle de 6π



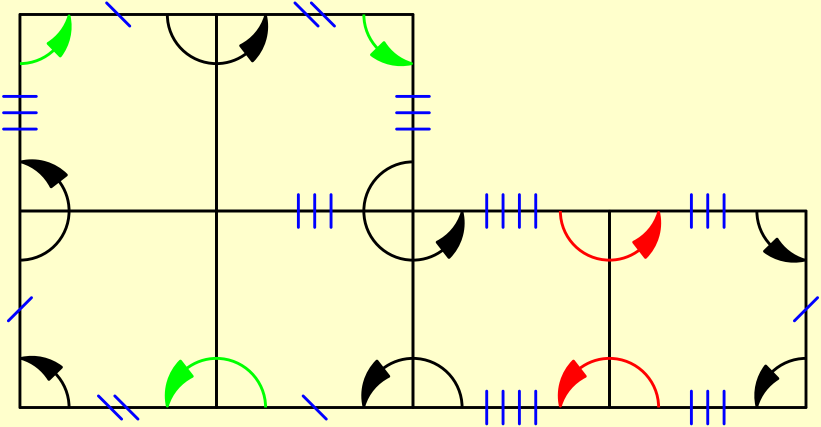
Un angle de 6π



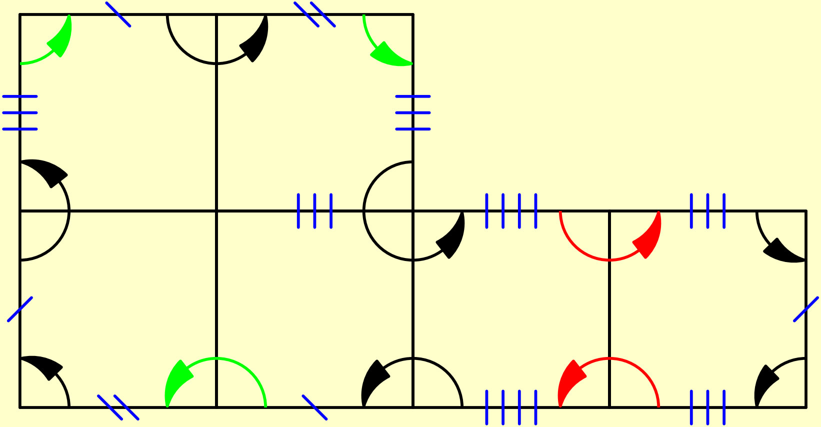
Un angle de 6π, un angle de 2π



Un angle de 6π, un angle de 2π

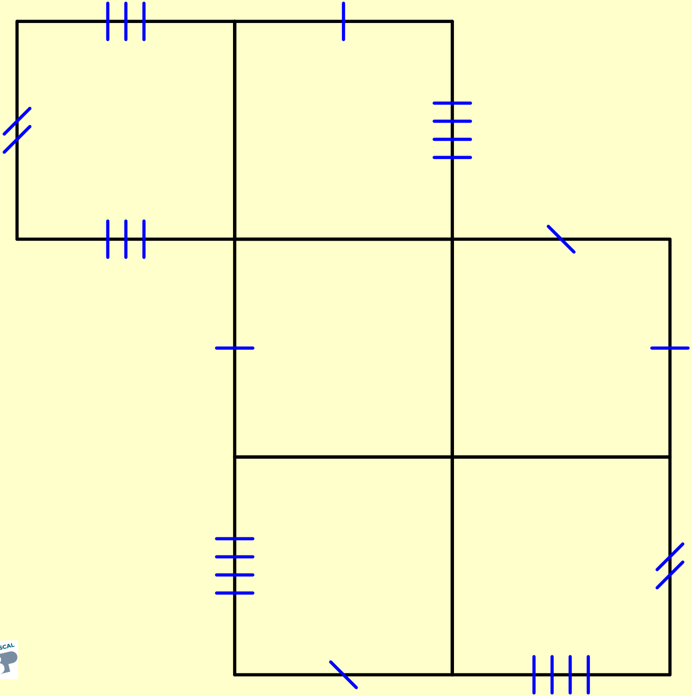


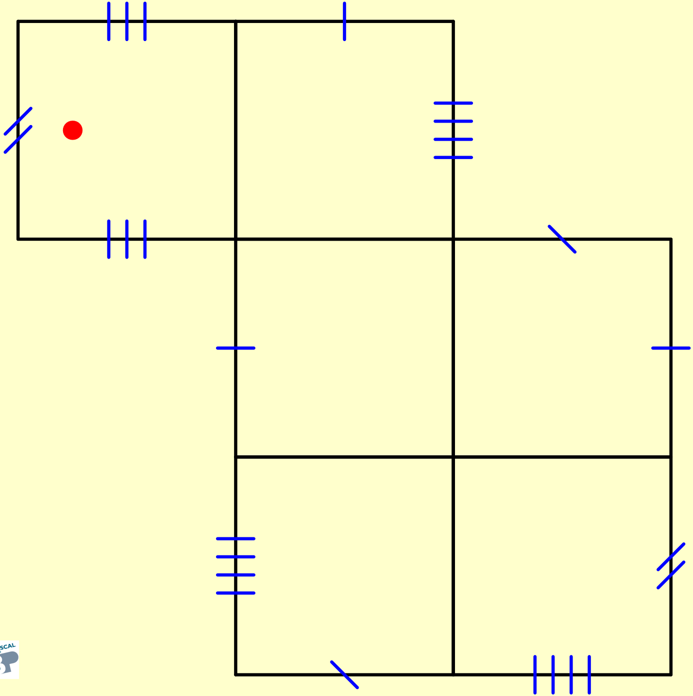
Un angle de 6π, un angle de 2π, un angle de 2π.

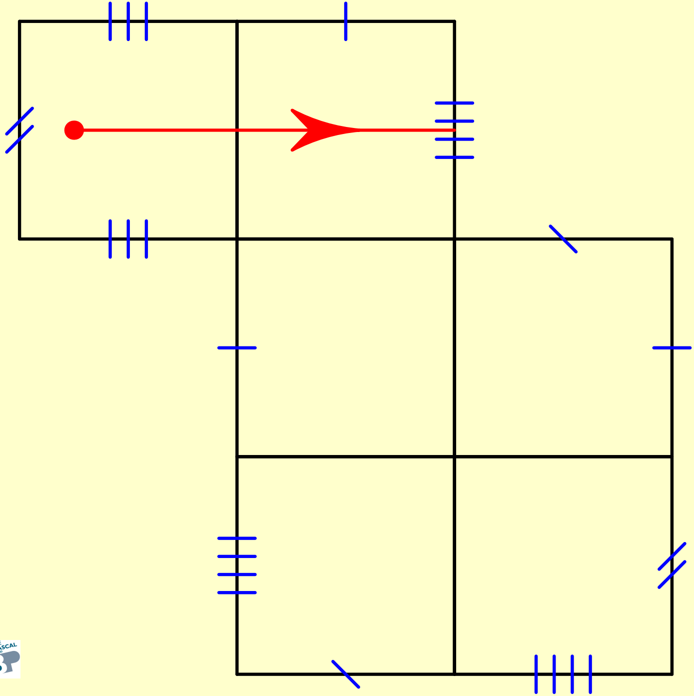


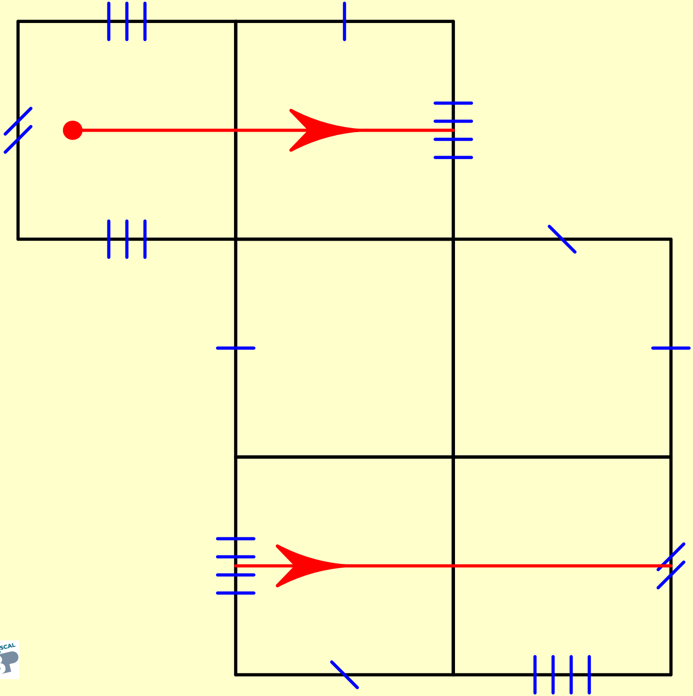
Un angle de 6π, un angle de 2π, un angle de 2π. Une seule préimage est critique, d'angle $6\pi = 2\pi(2+1)$ donc la surface est dans $\mathcal{H}(2)$.

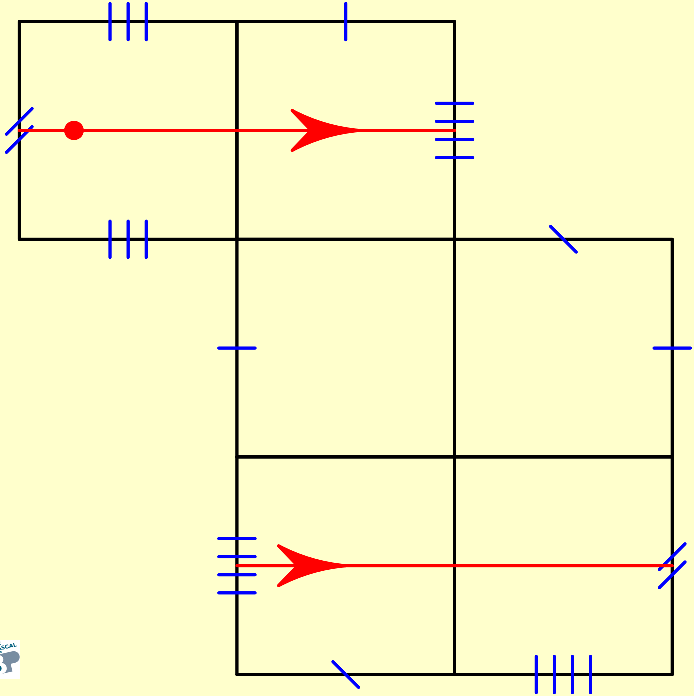
En traçant des géodésiques passant par les points intérieurs, il est possible de décomposer les surfaces de $\mathcal{H}(2)$ en cylindres. On obtient toujours un ou deux cylindres.

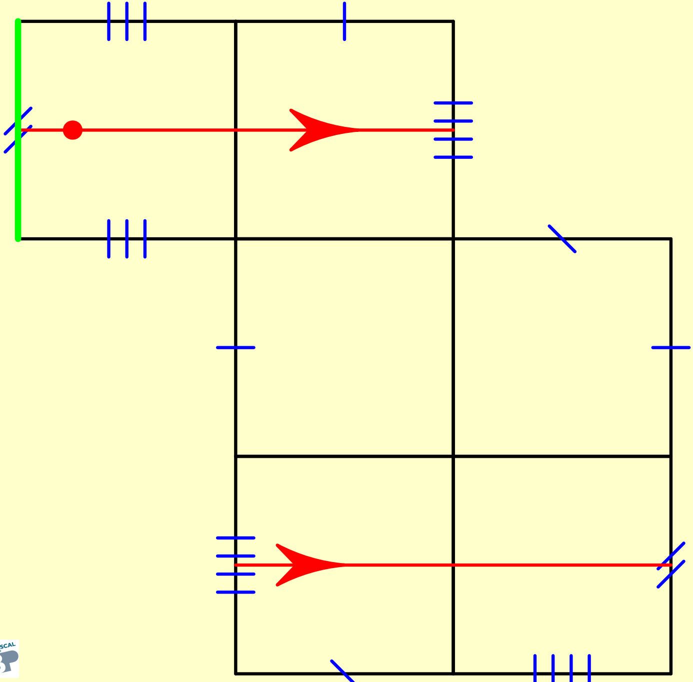


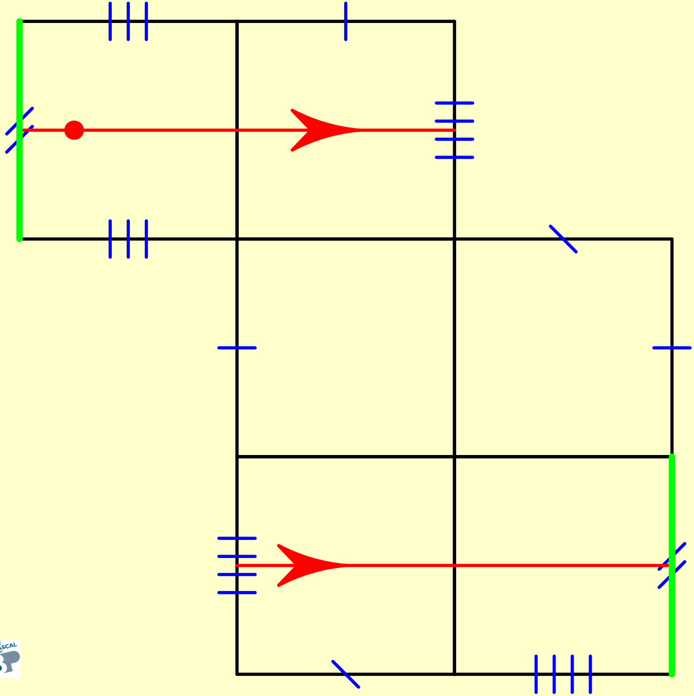


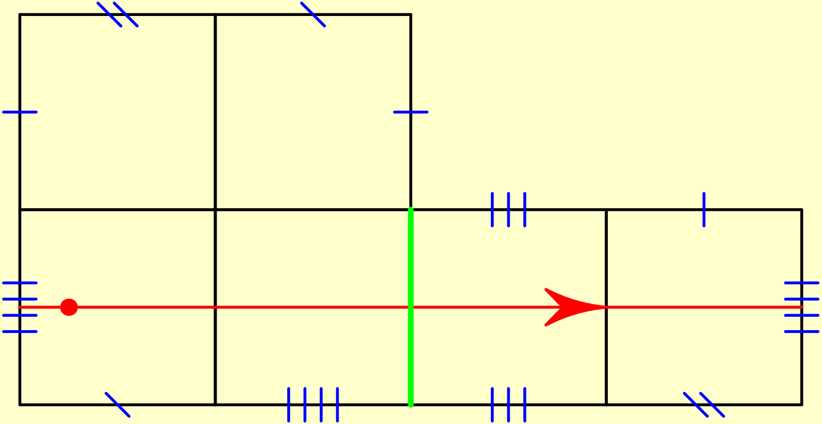


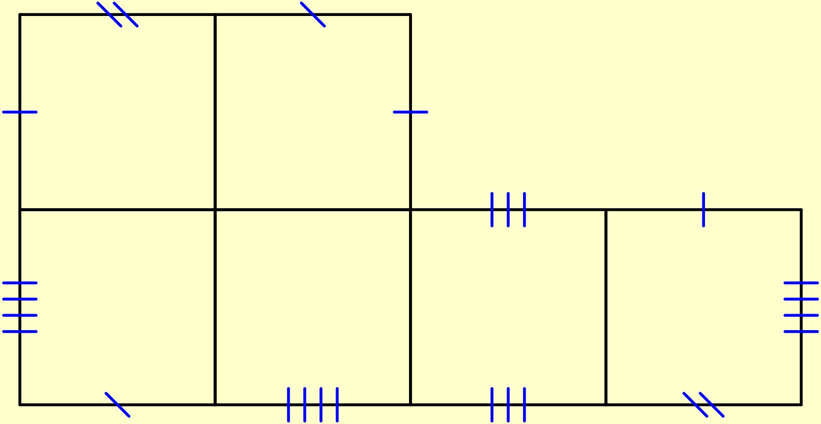






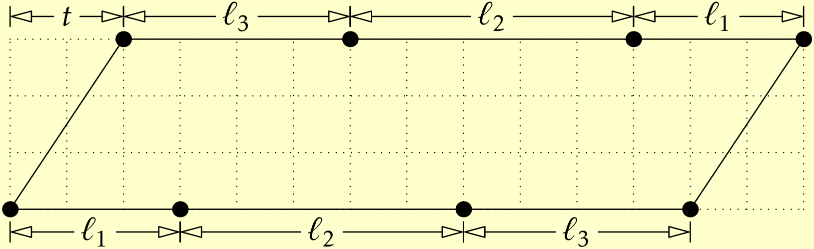




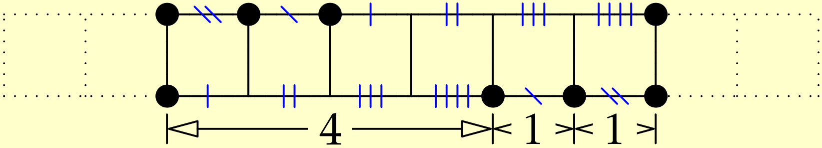


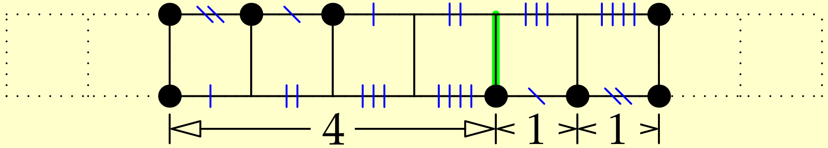
On obtient une surface à deux cylindres.

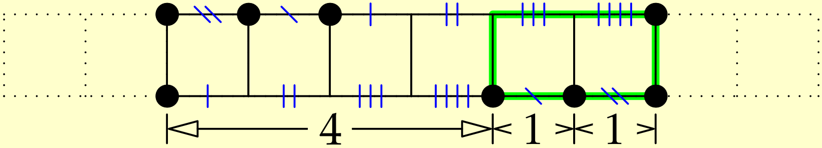
On introduit un paramétrage des surfaces de $\mathcal{H}(2)$ à un cylindre.

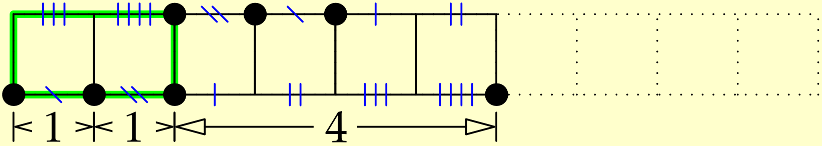


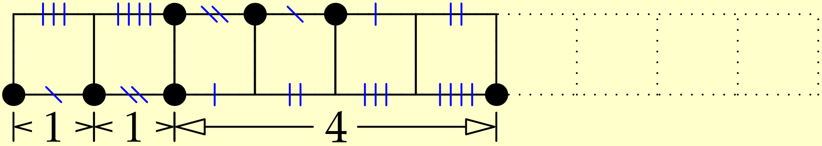
Le point représente le point d'angle 6π et (ℓ_1,ℓ_2,ℓ_3) est minimal pour l'ordre lexicographique parmi (ℓ_1,ℓ_2,ℓ_3), (ℓ_2,ℓ_3,ℓ_1) et (ℓ_3,ℓ_1,ℓ_2). Cela définit un paramètre de torsion t.

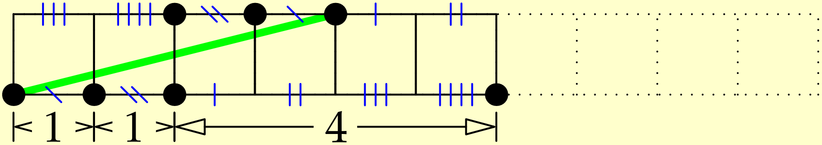

4
1
1

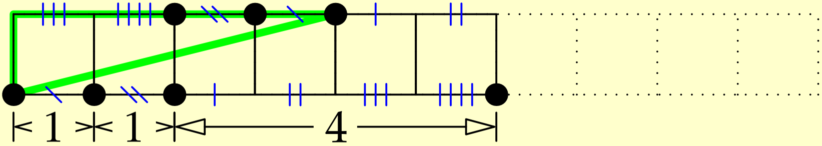

4
1
1

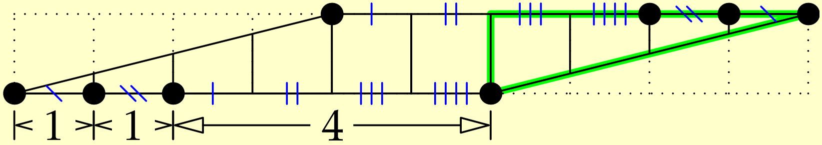

4
1
1

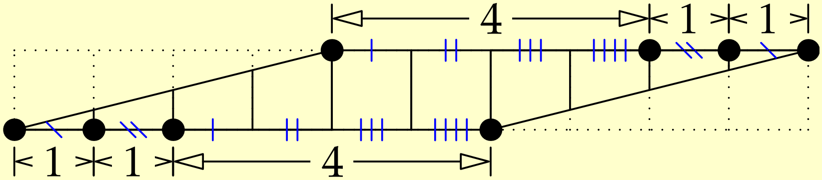

1
1
4

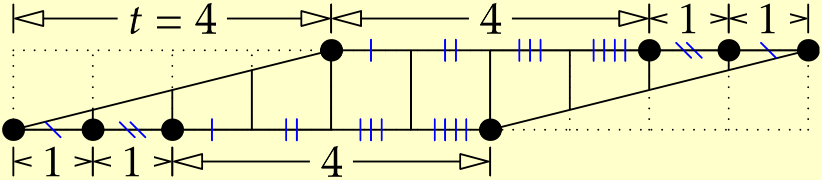

1
1
4


1
1
4


1
1
4


1
1
4


4
1
1
1
1
4



$t = 4$
4
1
1
1
1
4

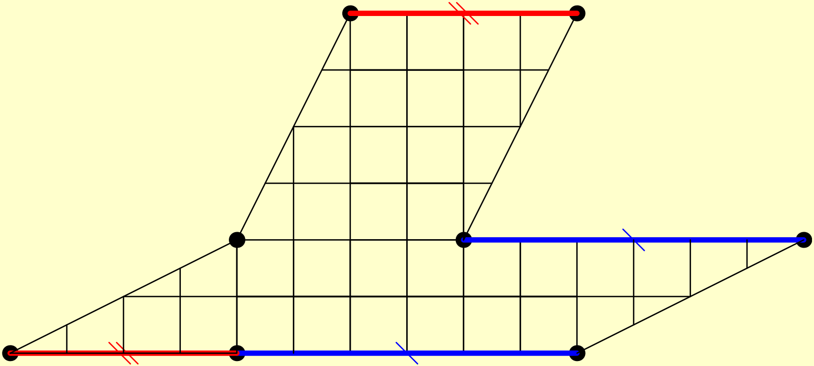
L'ensemble des surfaces de $\mathcal{H}(2)$ à un cylindre et n carreaux est donc paramétré par

$$\left\{ (\ell_1, \ell_2, \ell_3, t) \in \mathbb{N}^4 : \left| \begin{array}{l} \ell_1 + \ell_2 + \ell_3 \mid n \\ (\ell_1, \ell_2, \ell_3) \text{ minimal} \\ t \in [0, \ldots, \ell_1 + \ell_2 + \ell_3 - 1] \end{array} \right. \right\}.$$

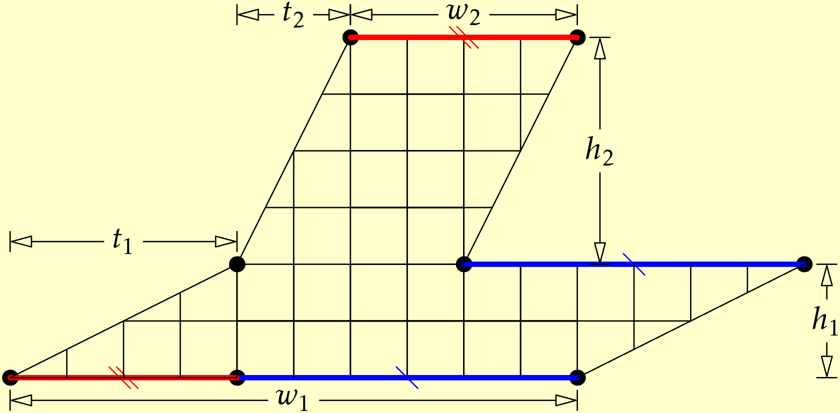
Le nombre de ces surfaces est

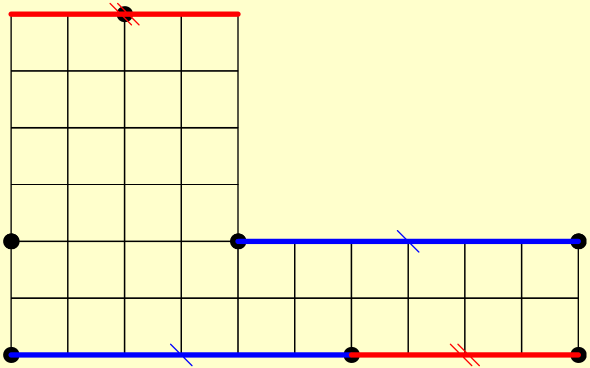
$$\frac{1}{3} \sum_{\ell \mid n} \sum_{\substack{(\ell_1, \ell_2, \ell_3) \in \mathbb{N}^3 \\ \ell_1 + \ell_2 + \ell_3 = n}} \ell = \frac{1}{6} \sigma_3(n) - \frac{1}{2} \sigma_2(n) + \frac{1}{3} \sigma_1(n).$$

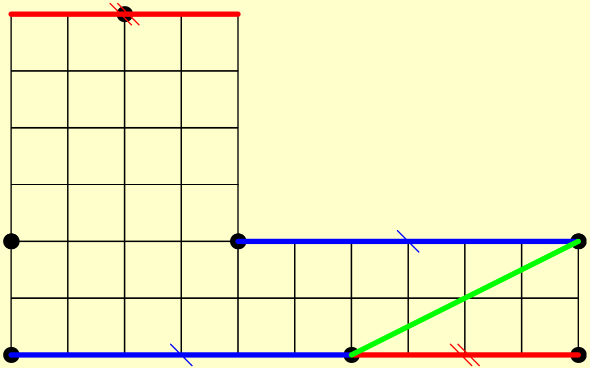
Par couper-coller, on peut transformer toute surface de $\mathcal{H}(2)$ à deux cylindres en une surface semblable à

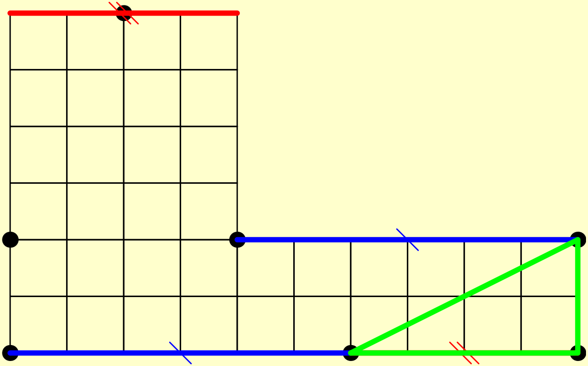


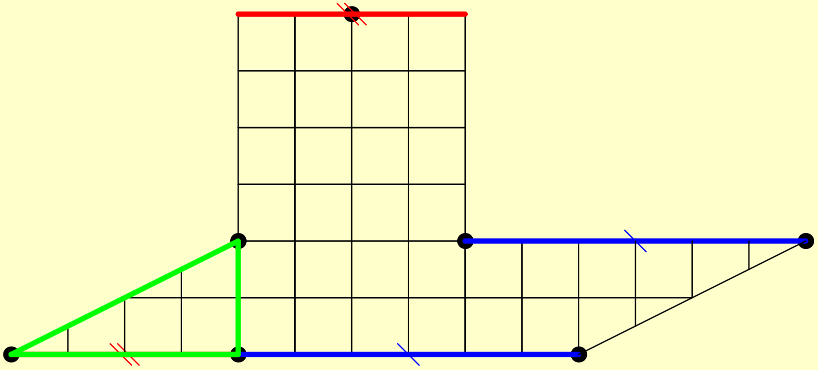
On peut alors definir deux hauteurs h_1 et h_2, deux longueurs $w_1 > w_2$ et deux torsions $t_1 \in [0, w_1]$ et $t_2 \in [0, w_2]$.

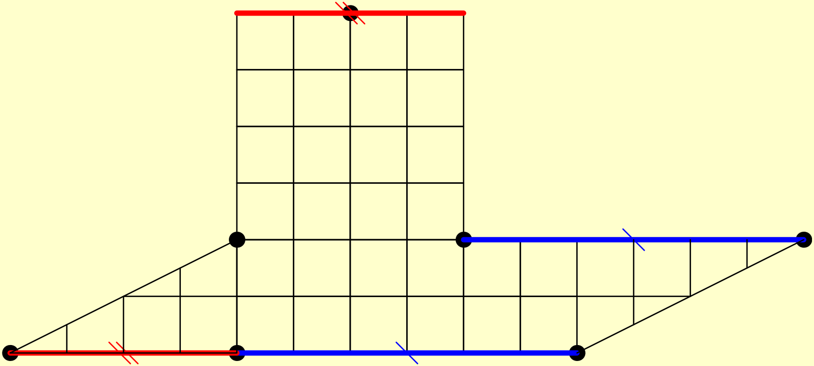


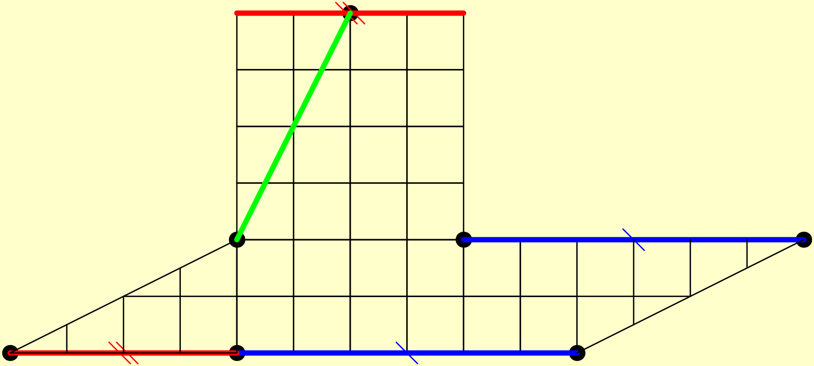


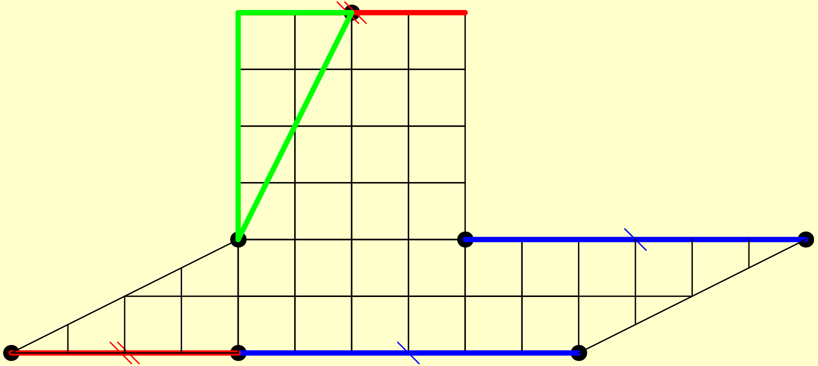


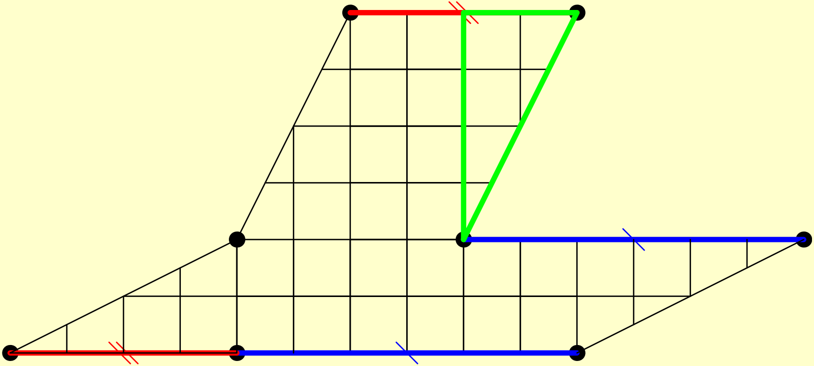


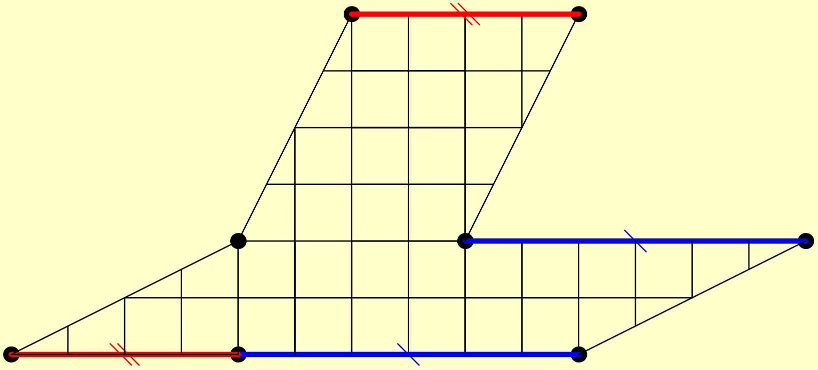


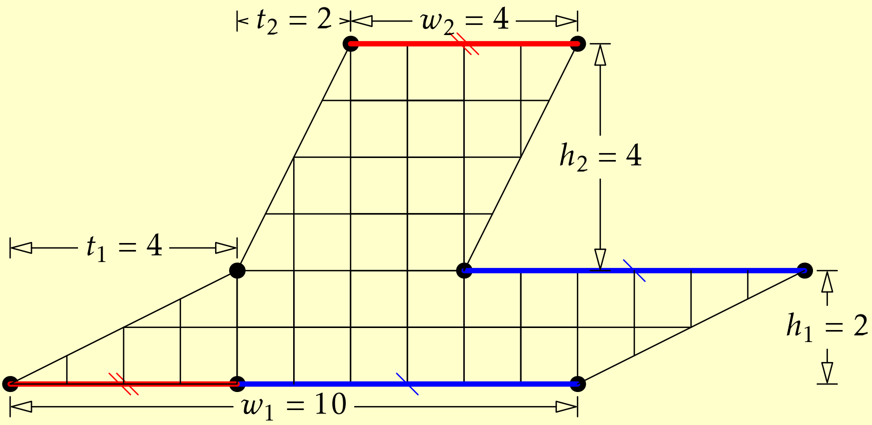











$t_2 = 2$
$w_2 = 4$
$h_2 = 4$
$t_1 = 4$
$h_1 = 2$
$w_1 = 10$

Le nombre total de surfaces de $\mathcal{H}(2)$ à deux cylindres et n carreaux est donc

$$\sum_{\substack{(h_1,h_2,w_1,w_2)\in\mathbb{N}^4\\ w_1>w_2\\ h_1w_1+h_2w_2=n}} w_1w_2 = \frac{1}{2}\sum_{s=1}^{n-1}\sigma_1(s)\sigma_1(n-s) - \frac{1}{2}n\sigma_1(n) + \frac{1}{2}\sigma_2(n)$$

et le nombre total de surfaces de $\mathcal{H}(2)$ à n carreaux est

$$e(n) = \frac{1}{6}\sigma_3(n) + \frac{1}{2}\sum_{s=1}^{n-1}\sigma_1(s)\sigma_1(n-s) - \frac{1}{2}n\sigma_1(n) + \frac{1}{3}\sigma_1(n).$$

Soit

$$E_2(z) = 1 - 24 \sum_{n=1}^{+\infty} \sigma_1(n) e^{2i\pi nz}$$

et

$$E_4(z) = 1 + 240 \sum_{n=1}^{+\infty} \sigma_3(n) e^{2i\pi nz}.$$

Soit

$$\mathrm{D} = \frac{1}{2i\pi} \frac{\mathrm{d}}{\mathrm{d}z}.$$

Alors,

$$\sum_{n=1}^{+\infty} e(n) e^{2i\pi nz} = \frac{9}{640} + \frac{1}{1440} E_4 - \frac{1}{64} E_2 + \frac{1}{1152} E_2^2 + \frac{1}{48} \mathrm{D}\, E_2.$$

Nous allons voir que cette fonction est une combinaison linéaire de formes quasimodulaires et utiliser ce fait pour obtenir une expression simplifiée de $e(n)$.

Une fonction holomorphe f sur le demi-plan de Poincaré ($\{z \in \mathbb{C} \colon \mathfrak{Im}\, z > 0\}$) est une forme quasimodulaire de poids k et de profondeur s s'il existe des fonctions holomorphes $f_0, \ldots, f_s$ ($f_s \neq 0$) telles que

$$(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) = \sum_{j=0}^{s} f_j(z) \left(\frac{c}{cz+d}\right)^j$$

pour toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. La fonction E_2 est une forme quasimodulaire de poids 2 et profondeur 1 :

$$(cz+d)^{-2} E_2\left(\frac{az+b}{cz+d}\right) = E_2(z) + \frac{6}{i\pi} \frac{c}{cz+d}.$$

On en déduit que E_2^2 est une forme quasimodulaire de poids 4 et profondeur 2. On en déduit aussi que $\mathrm{D}(E_2)$ est une forme quasimodulaire de poids 4 et profondeur 2.

L'espace vectoriel sur $\mathbb{C}$ des formes quasimodulaires de poids 4 et profondeur inférieure ou égale à 2 est de dimension 2. Une base est $(E_4, \mathrm{D}\, E_2)$. On en déduit que

$$E_2^2 = E_4 + 12\,\mathrm{D}\,E_2$$

puis que

$$\sum_{n=1}^{+\infty} e(n) e^{2i\pi nz} = \frac{1}{640}\left(9 - 10E_2(z) + 20\,\mathrm{D}\,E_2(z) + E_4(z)\right).$$

Autrement dit,

$$e(n) = \frac{3}{8}\left(\sigma_3(n) - (2n-1)\sigma_1(n)\right).$$

Soit $\mathbb{Q}(\sqrt{D})$ le corps quadratique de discriminant D. On note $\mathcal{C}_D$ son groupe des classes. Si $\mathcal{I}_D$ est le groupe des idéaux fractionnaires de l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ et si $\mathcal{P}_D$ est le sous-groupe des idéaux principaux, alors

$$\mathcal{C}_D = {}^{\mathcal{I}_D}/_{\mathcal{P}_D}.$$

On note $\mathcal{P}_D^+$ le sous-groupe de $\mathcal{I}_D$ formé des idéaux principaux engendré par par élément de norme positive. Le groupe des classes au sens étroit de $\mathbb{Q}(\sqrt{D})$ est

$$\mathcal{C}_D^+ = {}^{\mathcal{I}_D}/_{\mathcal{P}_D^+}.$$

- Si $D > 0$, on a $\mathcal{C}_D = \mathcal{C}_D^+$.
- Si $D < 0$, c'est plus subtil. On note ε_D l'unité fondamentale de $\mathbb{Q}(\sqrt{D})$. Alors, $\mathcal{C}_D = \mathcal{C}_D^+$ si ε_D est de norme négative. Si ε_D est de norme positive, on a seulement

$$\left|\mathcal{C}_D^+\right| = 2|\mathcal{C}_D|.$$

Puisque le groupe $\mathcal{C}_D^+$ est abélien fini, il est isomorphe à un produit du type

$$\bigoplus_{j=1}^{\ell} \mathbb{Z}\big/ p_j^{\alpha_j}\mathbb{Z}$$

où les nombres premiers p_j peuvent ne pas être distincts.
Si p est premier, le p^k-rang de $\mathbb{Q}(\sqrt{D})$ est

$$\mathrm{rk}_{p^k}(D) = \{i \in [1, \ell] \colon p_i = p \text{ et } \alpha_i \geq k\}.$$

Plus intrinsèquement,

$$\mathrm{rk}_{p^k}(D) = \dim_{\mathbb{F}_p} \left(\mathcal{C}_D^+\right)^{p^{k-1}} \Big/ \left(\mathcal{C}_D^+\right)^{p^k}.$$

Le 2-rang est bien connu grâce à la théorie du genre :

$$\mathrm{rk}_2(D) = \omega(D) - 1.$$

Pour le 3-rang, on a l'inégalité miroir suivante due à Scholz : si $D \geq 1$ est sans facteur carré, alors

$$\mathrm{rk}_3(D) \leq \mathrm{rk}_3(-3D) \leq \mathrm{rk}_3(D) + 1.$$

Cet encadrement a été généralisé pour le 4-rang en 1970 par Damey & Payan. Si $D \geq 1$, alors

$$\mathrm{rk}_4(D) \leq \mathrm{rk}_4(-D) \leq \mathrm{rk}_4(D) + 1.$$

L'objectif de cette partie d'exposé est de montrer l'encadrement de Damey & Payan en utilisant des techniques combinatoires appliquées à des formules de Fouvry & Klüners.
On se restreint à

$$D \geq 1 \qquad D \equiv 1 \pmod 4$$

mais des techniques semblables s'appliquent pour traiter tous les cas.

Comme D est un discriminant fondamental, notre restriction impose que D est sans facteur carré. Fouvry & Klüners ont établi les égalités

$$2^{\mathrm{rk}_4(D)} = \frac{1}{2}\#\left\{(a,b)\in\mathbb{N}^2\colon D=ab, \left| \begin{array}{ll} -a\equiv\square & \pmod{b} \\ b\equiv\square & \pmod{a} \end{array}\right.\right\}$$

et

$$\begin{aligned} 2^{\mathrm{rk}_4(-4D)} &= \frac{1}{2}\#\left\{(a,b)\in\mathbb{N}^2\colon D=ab, \left| \begin{array}{ll} a\equiv\square & \pmod{b} \\ b\equiv\square & \pmod{a} \end{array}\right.\right\} \\ &\quad + \frac{1}{2}\#\left\{(a,b)\in\mathbb{N}^2\colon D=ab, \left| \begin{array}{ll} 2a\equiv\square & \pmod{b} \\ 2b\equiv\square & \pmod{a} \end{array}\right.\right\} \end{aligned}$$

On introduit

$$\mathcal{E}_D(u,v) = \left\{ (a,b) \in \mathbb{N}^2 \colon D = ab, \left| \begin{array}{ll} ua \equiv \square & \pmod{b} \\ vb \equiv \square & \pmod{a} \end{array} \right. \right\}$$

de sorte que

$$2^{\mathrm{rk}_4(D)} = \frac{1}{2} \# \mathcal{E}_D(-1,1)$$

et

$$2^{\mathrm{rk}_4(-4D)} = \frac{1}{2} \# \mathcal{E}_D(-1,1) + \frac{1}{2} \# \mathcal{E}_D(2,2).$$

Pour tous nombres premiers impairs distincts p et q, on définit $\alpha(p,q)$ et $\beta_u(p)$ dans $\mathbb{F}_2$ par

$$\left(\frac{p}{q}\right) = (-1)^{\alpha(p,q)} \quad \text{et} \quad \left(\frac{u}{p}\right) = (-1)^{\beta_u(p)}.$$

On écrit

$$D = \prod_{i=1}^{\omega(D)} p_i$$

où les nombres premiers p_i sont distincts. On encode chaque diviseur a de D par

$$\boldsymbol{x} = (x_1, \ldots, x_{\omega(D)}) \in \mathbb{F}_2^{\omega(D)} \text{ avec } \begin{cases} x_i = 1 & \text{si } p_i \mid a \\ x_i = 0 & \text{sinon.} \end{cases}$$

Soit $a \mid D$ et $b = D/a$. Étudions la condition $vb \equiv a\square \pmod{b}$. Elle est satisfaite si et seulement si vb est un carré modulo tout diviseur premier de a. Pour tout i tel que $x_i = 1$, on doit donc avoir

$$1 = \left(\frac{vb}{p_i}\right) = \left(\frac{v}{p_i}\right) \prod_{p|b} \left(\frac{p}{p_i}\right) = (-1)^{\beta_v(p_i) + \sum_{j \neq i} \alpha(p_j, p_i)(1-x_j)}$$

puisque

$$p_j \mid b \Leftrightarrow 1 - x_j \neq 0 \Leftrightarrow 1 - x_j = 1.$$

La condition $vb = \square \pmod{a}$ est donc

$$x_i = 1 \Rightarrow \beta_v(p_i) + \sum_{j \neq i} \alpha(p_j, p_i)(1 - x_j) = 0.$$

De façon identique, la condition $ua = \square \pmod{b}$ est

$$x_i = 0 \Rightarrow \beta_u(p_i) + \sum_{j \neq i} \alpha(p_j, p_i) x_j = 0.$$

Ces deux équations sont les deux faces d'une même équation

$$\beta_u(p_i)(1 - x_i) + \beta_v(p_i) x_i + \sum_{j \neq i} \alpha(p_j, p_i) \Big[x_i(1 - x_j) + x_j(1 - x_i) \Big] = 0.$$

Cette dernière équation équivaut à

$$\left(\beta_u(p_i) + \beta_v(p_i) + \sum_{j \neq i} \alpha(p_j, p_i) \right) x_i + \sum_{j \neq i} \alpha(p_j, p_i) x_j = \beta_u(p_i).$$

Notons $\mathcal{F}_D(u,v)$ l'espace affine défini par les $\omega(D)$ équations

$$\left(\beta_u(p_i)+\beta_v(p_i)+\sum_{j\neq i}\alpha(p_j,p_i)\right)x_i+\sum_{j\neq i}\alpha(p_j,p_i)x_j=\beta_u(p_i).$$

Alors,

$$\#\mathcal{E}_D(u,v)=\#\mathcal{F}_D(u,v).$$

On a

$$2^{\mathrm{rk}_4(D)} = \frac{1}{2}\#\mathcal{E}_D(-1,1) = \frac{1}{2}\#\mathcal{F}_D(-1,1).$$

Comme $\beta_1 = 0$, l'espace $\mathcal{F}_D(-1,1)$ contient le point $(1,\ldots,1)$ et est donc non vide. Ainsi,

$$\mathrm{rk}_4(D) = \dim_{\mathbb{F}_2} \overrightarrow{\mathcal{F}}_D(-1,1) - 1.$$

On a

$$2^{\mathrm{rk}_4(-4D)} = \frac{1}{2}\#\mathcal{F}_D(1,1) + \frac{1}{2}\#\mathcal{F}_D(2,2).$$

Comme $\beta_1+\beta_1=\beta_2+\beta_2$, les espaces affines $\mathcal{F}_D(1,1)$ et $\mathcal{F}_D(2,2)$ ont même direction. De plus, $\beta_1=0$ donc $\mathcal{F}_D(1,1)$ contient 0 et $\mathcal{F}_D(1,1)=\vec{\mathcal{F}}_D(1,1)$. On en tire

$$\frac{1}{2}\#\mathcal{F}_D(1,1) = 2^{\dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(1,1)-1}.$$

Enfin,

- soit $\#\mathcal{F}_D(2,2)=0$
- soit $\#\mathcal{F}_D(2,2)=2^{\dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(2,2)}=2^{\dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(1,1)}$.

Ainsi,

$$2^{\mathrm{rk}_4(-4D)} \in \left\{2^{\dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(1,1)}, 2^{\dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(1,1)-1}\right\}$$

et

$$\mathrm{rk}_4(-4D) \in \left\{\dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(1,1), \dim_{\mathbb{F}_2}\vec{\mathcal{F}}_D(1,1)-1\right\}.$$

On a donc

$$\mathrm{rk}_4(D) = \dim_{\mathbb{F}_2} \overrightarrow{\mathcal{F}}_D(-1,1) - 1.$$

et

$$\mathrm{rk}_4(-4D) \in \left\{\dim_{\mathbb{F}_2} \overrightarrow{\mathcal{F}}_D(1,1), \dim_{\mathbb{F}_2} \overrightarrow{\mathcal{F}}_D(1,1) - 1\right\}.$$

On va montrer, par des méthodes arithmétiques, que

$$\dim_{\mathbb{F}_2} \overrightarrow{\mathcal{F}}_D(1,1) = \dim_{\mathbb{F}_2} \overrightarrow{\mathcal{F}}_D(-1,1)$$

pour conclure

$$\mathrm{rk}_4(-4D) \in \{\mathrm{rk}_4(D)+1, \mathrm{rk}_4(D)\}.$$

On veut montrer

$$\dim_{\mathbb{F}_2} \vec{\mathcal{F}}_D(1,1) = \dim_{\mathbb{F}_2} \vec{\mathcal{F}}_D(-1,1).$$

Comme les espaces affines $\mathcal{F}_D(1,1)$ et $\mathcal{F}_D(-1,1)$ sont non vides, cela revient à montrer

$$\#\mathcal{E}_D(1,1) = \#\mathcal{E}_D(-1,1).$$

En posant

$$S_D(u,v) = \sum_{D=ab} \prod_{p|b} \left(1 + \left(\frac{ua}{p}\right)\right) \prod_{p|a} \left(1 + \left(\frac{vb}{p}\right)\right)$$

on a

$$\#\mathcal{E}_D(u,v) = 2^{-\omega(D)} S_D(u,v)$$

et il suffit donc de montrer que

$$S_D(1,1) = S_D(-1,1).$$

On a

$$S_D(u,v) = \sum_{D=a'b'} \sum_{\substack{c|a' \\ d|b'}} \left(\frac{ua'}{d}\right)\left(\frac{vb'}{c}\right) = \sum_{D=abcd} \left(\frac{ua}{d}\right)\left(\frac{vb}{c}\right)\left(\frac{c}{d}\right)\left(\frac{d}{c}\right).$$

La loi de réciprocité quadratique donne

$$\left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = (-1)^{(c-1)(d-1)/4}.$$

Or,

$$\left(\frac{-1}{c}\right) = (-1)^{(c-1)/2} = (-1)^{\beta_{-1}(c)}$$

donc

$$\left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = (-1)^{\beta_{-1}(c)\beta_{-1}(d)}$$

et

$$S_D(u,v) = \sum_{D=abcd} (-1)^{\beta_{-1}(c)\beta_{-1}(d)+\beta_u(d)+\beta_v(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right).$$

De

$$S_D(u,v) = \sum_{D=abcd} (-1)^{\beta_{-1}(c)\beta_{-1}(d)+\beta_u(d)+\beta_v(d)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right).$$

on déduit

$$\begin{aligned} S_D(1,1) - S_D(-1,1) &= \sum_{D=abcd} (-1)^{\beta_{-1}(c)\beta_{-1}(d)} \left[1 - (-1)^{\beta_{-1}(d)}\right] \left(\frac{a}{d}\right)\left(\frac{b}{c}\right) \\ &= 2 \sum_{\substack{D=abcd \\ \beta_{-1}(d)=1}} (-1)^{\beta_{-1}(c)} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right). \end{aligned}$$

On échange les variables b et c dans l'une des deux copies de la somme et on trouve

$$S_D(1,1) - S_D(-1,1) = \sum_{\substack{D=abcd \\ \beta_{-1}(d)=1}} \left(\frac{a}{d}\right)\left[(-1)^{\beta_{-1}(c)}\left(\frac{b}{c}\right) + (-1)^{\beta_{-1}(b)}\left(\frac{c}{b}\right)\right].$$

Une nouvelle application de la loi de réciprocité quadratique conduit à

$$\begin{aligned} & S_D(1,1) - S_D(-1,1) \\ = & \sum_{\substack{D=abcd \\ \beta_{-1}(d)=1}} (-1)^{\beta_{-1}(c)}\left(\frac{a}{d}\right)\left(\frac{b}{c}\right)\left[1 + (-1)^{\beta_{-1}(b)+\beta_{-1}(c)+\beta_{-1}(b)\beta_{-1}(c)}\right] \end{aligned}$$

et donc

$$S_D(1,1) - S_D(-1,1) = 2 \sum_{\substack{D=abcd \\ \beta_{-1}(d)=1 \\ \beta_{-1}(b)=\beta_{-1}(c)=0}} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right).$$

Comme $D \equiv 1 \pmod 4$, on a

$$\left(\frac{-1}{D}\right) = 1$$

d'où

$$\beta_{-1}(a) + \beta_{-1}(b) + \beta_{-1}(c) + \beta_{-1}(d) = 0$$

et

$$S_D(1,1) - S_D(-1,1) = 2 \sum_{\substack{D=abcd \\ \beta_{-1}(d)=\beta_{-1}(a)=1 \\ \beta_{-1}(b)=\beta_{-1}(c)=0}} \left(\frac{a}{d}\right)\left(\frac{b}{c}\right).$$

Dans l'une des deux copies, on permute a et b. On obtient

$$S_D(1,1) - S_D(-1,1) = \sum_{\substack{D=abcd \\ \beta_{-1}(d)=\beta_{-1}(a)=1 \\ \beta_{-1}(b)=\beta_{-1}(c)=0}} \left(\frac{b}{c}\right)\left(\left(\frac{a}{d}\right) + \left(\frac{d}{a}\right)\right).$$

Or,

$$\left(\frac{a}{d}\right)\left(\frac{d}{a}\right) = (-1)^{\beta_{-1}(a)\beta_{-1}(d)} = -1$$

car $\beta_{-1}(d) = \beta_{-1}(a) = 1$ donc

$$S_D(1,1) - S_D(-1,1) = 0.$$