1h'32 sans étape 5 ni crayon à papier.

CARDINAL DE $GL_2(\mathbb{Z}/_n\mathbb{Z})$ $n \geq 1$

FGN Alg 2
3.23 + adaptat° du 3.24

Prérequis : théorème chinois, p premier $\Leftrightarrow \mathbb{Z}/_p\mathbb{Z}$ corps
1er thm d'isomorphisme

Remarques préliminaires :

- Si $f : G \to G'$ est un morphisme de groupes avec G et G' des groupes finis. Alors, par le 1er théorème d'isomorphisme, $\mathrm{Im} f \simeq \frac{G}{\ker f}$ et ainsi $|\mathrm{Im} f| \times |\ker f| = |G|$.
- Si A est un anneau commutatif, $B \in GL_n(A) \Leftrightarrow \det B \in A^\times$. On sait que $\det B \in A$

$\rightarrow$ Si $B \in GL_n(A)$, $1 = \det(BB^{-1}) = \det B \det B^{-1}$ d'où $\det B \in A^\times$
$\rightarrow$ Réciproquement, $B\,{}^t\mathrm{Com}B = \det B\, I_n$ d'où $\frac{{}^t\mathrm{Com}B}{\det B} \in \mathcal{M}_n(A)$ donc $B \in GL_n(A)$

Soit $n \geq 1$.

Étape 1 : On se ramène au calcul de $|GL_2(\mathbb{Z}/_{p^\alpha}\mathbb{Z})|$, p premier, $\alpha \in \mathbb{N}^\times$

On commence par décomposer n en facteurs premiers $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ où les p_i sont 2 à 2 distincts

D'après le théorème chinois, on a un isomorphisme d'anneaux entre $\mathbb{Z}/_n\mathbb{Z}$ et $\prod_{i=1}^{s} \mathbb{Z}/_{p_i^{\alpha_i}}\mathbb{Z}$.

Celui-ci induit un isomorphisme d'anneaux entre $\mathcal{M}_2(\mathbb{Z}/_n\mathbb{Z})$ et $\prod_{i=1}^{s} \mathcal{M}_2(\mathbb{Z}/_{p_i^{\alpha_i}}\mathbb{Z})$

Or un isomorphisme d'anneaux induit un isomorphisme entre les groupes des inversibles.
Si $f = A \to B$, est un isomorphisme d'anneaux soit $\tilde{f} = A^\times \to B^\times$ morphisme de groupes
. Si $a \in A^\times$ alors $1 = f(aa^{-1}) = f(a)f(a^{-1})$ d'où $f(a) \in B^\times$ $\rightarrow$ bien définie
. Si $\tilde{f}(a) = 1$, alors $a = 1$ car f injective $\rightarrow \tilde{f}$ injective
. Si $b \in B^\times$ il existe $a \in A$ tq $f(a) = b$ par surj de f et $c \in A$ tq $f(c) = b^{-1}$
d'où $f(ac) = f(a)f(c) = bb^{-1} = 1$ d'où $ac = 1$ par injectivité de f d'où $a \in A^\times \rightarrow \tilde{f}$ surj

On a donc un isomorphisme de groupes entre $GL_2(\mathbb{Z}/_n\mathbb{Z})$ et $\left(\prod_{i=1}^{s} \mathcal{M}_2(\mathbb{Z}/_{p_i^{\alpha_i}}\mathbb{Z})\right)^\times$
Or le groupe des inversibles d'un produit d'anneaux est le produit des groupes des inversibles
Si $a \in (A_1 \times \cdots \times A_n)$, $a = (a_1, \ldots, a_n)$
$a \in (A_1 \times \cdots \times A_n)^\times \Leftrightarrow \exists b = (b_1, \ldots, b_n),\ ab = 1 \Leftrightarrow \exists b_i\ a_i b_i = 1\ \forall i \Leftrightarrow \forall i\ a_i \in A_i^\times$
$\Leftrightarrow a \in A_1^\times \times \cdots \times A_n^\times$

On a donc un isomorphisme de groupes entre $GL_2(\mathbb{Z}/_n\mathbb{Z})$ et $\prod_{i=1}^{s} GL_2(\mathbb{Z}/_{p_i^{\alpha_i}}\mathbb{Z})$.

Donc $|GL_2(\mathbb{Z}/_n\mathbb{Z})| = \prod_{i=1}^{s} |GL_2(\mathbb{Z}/_{p_i^{\alpha_i}}\mathbb{Z})|$.

Étape 2 : Calcul de $|GL_2(\mathbb{Z}/_{p^\alpha}\mathbb{Z})|$, p premier, $\alpha \in \mathbb{N}^\times$: on se ramène à $\alpha = 1$.

Soit $\pi : \mathbb{Z} \to \mathbb{Z}/_p\mathbb{Z}$ la projection canonique. C'est un morphisme d'anneaux surjectif. Or $p^\alpha\mathbb{Z} \subset \underbrace{\ker \pi}_{= p\mathbb{Z}}$ donc π se factorise en $\tilde{\pi} : \mathbb{Z}/_{p^\alpha}\mathbb{Z} \to \mathbb{Z}/_p\mathbb{Z}$ qui est un morphisme d'anneaux surjectif et de noyau $\frac{p\mathbb{Z}}{p^\alpha\mathbb{Z}}$ par le thm ~~d'isomorphisme~~ de factorisation.
$\hookrightarrow$ de cardinal $p^{\alpha-1}$

On a donc un morphisme de groupes $\psi : GL_2(\mathbb{Z}/p^\alpha\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{pmatrix} \tilde\pi(a) & \tilde\pi(b) \\ \tilde\pi(c) & \tilde\pi(d) \end{pmatrix}$$

* ψ est bien définie : Si $A \in GL_2(\mathbb{Z}/p^\alpha\mathbb{Z})$ alors $\det A \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

donc comme $\tilde\pi$ induit un morphisme de groupes de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$, $\tilde\pi(\det A) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Or $\tilde\pi(\det A) = \det \psi(A)$ car $\tilde\pi$ est un morphisme d'anneaux donc $\psi(A) \in GL_2(\mathbb{Z}/p\mathbb{Z})$. On peut aussi dire : $\det A \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times \Leftrightarrow x \wedge p^\alpha = 1$

(**) $\Leftrightarrow x \wedge p = 1 \Leftrightarrow \tilde\pi(\det A) \in (\mathbb{Z}/p\mathbb{Z})^\times$ où x est un représentant de $\det A$ dans $\mathbb{Z}$

* Surjectivité : Soit $B \in GL_2(\mathbb{Z}/p\mathbb{Z})$. Soit $A \in \mathcal{M}_2(\mathbb{Z}/p\mathbb{Z})$ obtenue par surjectivité de $\tilde\pi$.

Il reste à montrer que $A \in GL_2(\mathbb{Z}/p^\alpha\mathbb{Z})$ i.e. $\det A \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Or $\tilde\pi(\det A) = \det B \in (\mathbb{Z}/p\mathbb{Z})^\times$ car $B \in GL_2(\mathbb{Z}/p\mathbb{Z})$ donc par (**)

on a bien $\det A \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

* Cardinal du noyau :

1ère méthode : on a vu que $\ker\tilde\pi = \dfrac{p\mathbb{Z}}{p^\alpha\mathbb{Z}}$ d'où $|\ker\tilde\pi| = p^{\alpha-1}$ donc tous les $|\tilde\pi^{-1}(\{x_0\})| = p^{\alpha-1}$ on a donc $p^{\alpha-1}$ antécédents dans $\mathbb{Z}/p^\alpha\mathbb{Z}$ pour chaque coefficient de la matrice donc $(p^{\alpha-1})^4$ pour la matrice. Or il n'y a pas de condition pour être inversible, comme on l'a vu dans la surjectivité : $I_2 \in GL_2(\mathbb{Z}/p\mathbb{Z})$ implique que tout relèvement est inversible.

2ème méthode : Soit $k \in \mathbb{Z}/p^\alpha\mathbb{Z}$, soit x un représentant dans $\mathbb{Z}$, on peut décomposer x dans la base p : $x = \sum_{i=0}^{+\infty} x_i p^i$ où $x_i \in [\![0, p-1]\!]$. Comme les x_i $0 \leq i \leq \alpha-1$ ne dépendent que de k et pas du choix de x, $k = x_0 + x_1 p + \dots + x_{\alpha-1} p^{\alpha-1}$. On a alors $\tilde\pi(x) = x_0$. Une condition sur $\tilde\pi(x)$ laisse donc le choix des valeurs pour $x_1, \dots, x_{\alpha-1}$: $p^{\alpha-1}$. Or il n'y a pas de condition supplémentaire pour être inversible.

Donc $|\ker\psi| = (p^{\alpha-1})^4$.

On peut donc appliquer la remarque préliminaire : $|GL_2(\mathbb{Z}/p\mathbb{Z})|\,|\ker\psi| = |GL_2(\mathbb{Z}/p^\alpha\mathbb{Z})|$

Etape 3 : Calcul de $|GL_2(\mathbb{Z}/p\mathbb{Z})|$, p premier. 3.23

Ici, $\mathbb{Z}/p\mathbb{Z}$ est un corps donc le calcul est plus simple. Pour définir une matrice inversible, on choisit d'abord sa première colonne qui doit être non nulle : p^2-1 possibilités. Puis la 2nde colonne qui ne doit pas être colinéaire à la première : p^2-p possibilités. (Si on n'a pas un anneau intègre, c'est plus dur de calculer les possibilités pour la 2e colonne et les suivantes)

Donc $|GL_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$.

Étape 4 : Conclusion :

En remettant toutes nos égalités ensemble, on obtient,

$|GL_2(\mathbb{Z}/p^\alpha\mathbb{Z})| = (p^2-1)(p^2-p)(p^{\alpha-1})^4$

d'où $|GL_2(\mathbb{Z}/n\mathbb{Z})| = \prod_{i=1}^{s} (p_i^2-1)(p_i^2-p_i)(p_i^{\alpha_i-1})^4$.

Étape 5 : Bonus : calcul de $|SL_2(\mathbb{Z}/n\mathbb{Z})|$

3.23

On considère $f : GL_2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$, $A \longmapsto \det A$, f est un morphisme de groupes bien défini par la remarque préliminaire.

- $\ker f = \{A \in GL_2(\mathbb{Z}/n\mathbb{Z}),\ \det A = 1\} = SL_2(\mathbb{Z}/n\mathbb{Z})$
- f est surjectif : si $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, la matrice $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ est de déterminant x et inversible.

Ainsi par la remarque préliminaire, $|SL_2(\mathbb{Z}/n\mathbb{Z})| \times |(\mathbb{Z}/n\mathbb{Z})^\times| = |GL_2(\mathbb{Z}/n\mathbb{Z})|$

donc $|SL_2(\mathbb{Z}/n\mathbb{Z})| = \dfrac{|GL_2(\mathbb{Z}/n\mathbb{Z})|}{\varphi(n)}$ où φ est l'indicatrice d'Euler

$$= \frac{\prod_{i=1}^{s} (p_i^2-1)\overbrace{(p_i^2-p_i)}^{p_i(p_i-1)}(p_i^{\alpha_i-1})^4}{\prod_{i=1}^{s} p_i^{\alpha_i-1}\cancel{(p_i-1)}}.$$

$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{\alpha_i})$

$$= \prod_{i=1}^{s} (p_i^2-1)\,p_i\,(p_i^{\alpha_i-1})^3$$