

1 Introduction sur la conjecture de Goldbach et objet du document :

-Enoncé-Originé de la conjecture (source Wikipédia) :

"La conjecture de Goldbach est l'assertion mathématique qui s'énonce
comme suit :

*Tout nombre entier pair supérieur à 3 peut s'écrire comme une somme de
deux nombres premiers.*

Formulée en 1742 par Christian Goldbach, c'est l'un des plus vieux
problèmes non résolus de la théorie des nombres et des mathématiques.

Il partage avec l'hypothèse de Riemann et la conjecture des nombres
premiers jumeaux le numéro 8 des problèmes de Hilbert, énoncés par
celui-ci en 1900."

-Ce document se propose de démontrer la conjecture de Goldbach.
Ainsi pour $N=9$: $2.9 = 9 + 9 = 7 + 11 = 5 + 13$.

2 Résumé de la démonstration :

Cette section réalise un résumé de la démonstration.

Les autres sections de ce document traitent la démonstration proprement dite en détails.

Deux groupes $(G, \otimes)$ et $(Z_R, \oplus)$ sont construits. G contient un sous ensemble G_{gen} contenant tous les couples (a,b) tels que $a+b = 2.N$ de la conjecture et $a,b > 1$.

Ces 2 groupes ont la particularité de posséder des formes, écritures multiples de l'élément neutre n_e pour G et n_z pour Z_R .

Ainsi ces formes $F(K)$ sont des couples (K,K) et ces formes ont la valeur logique : $F(K)=n_e$ pour G ou $F(K)=n_z$ pour Z_R .

Ensuite un morphisme de groupes par une application $f :$
 $(G, \otimes) \rightarrow (Z_R, \oplus)$ entre G et Z_R est défini.

On montre alors que l'image par f ($Im(f) = f(G)$) est un sous-groupe de Z_R comme c'est le cas pour des groupes ne possédant qu'une seule forme, écriture de l'élément neutre.

L'élément neutre de Z_R étant le couple $(1,1)$ ceci indique qu'il existe alors au moins un élément de G tel que $f(e_p) = (1,1)$
et selon la définition de l'application, que $e_p = (P_i, P_j)$ ou $= (P_i, P_i)$ avec P_i, P_j des nombres premiers et $P_i + P_j = 2.N$ de la conjecture.

En fin de démonstration on montre que e_p appartient au sous-ensemble de $G : G_{gen}$.

La conjecture est alors démontrée.

3 Caractéristiques des groupes $(G_{Fm}, \otimes)$ possédant des formes multiples de l'élément neutre n_e :

3.1 Proposition :

Cette section se propose de décrire tous les axiomes posés pour la définition d'un groupe $(G, *)$.

Ces axiomes possèdent néanmoins des spécificités formant alors une famille de groupes.

Cette famille de groupes est aussi utilisée à plusieurs reprises par la suite.

C'est pourquoi une notation spécifique est utilisée pour toute la suite de ce document.

Ces groupes seront alors notés : $(G_{Fm}, \otimes)$ et nommés : groupes à formes multiples de l'élément neutre du groupe.

3.1.1 Notations utilisées :

Ainsi ces groupes $(G, *)$ seront notés $(G_{Fm}, \otimes)$:

L'ensemble G_{Fm} en remplacement de l'ensemble G et la loi de composition

$\otimes$ en remplacement de la loi de composition $*$.

3.2 Définition de l'ensemble G_{Fm} :

Cette sous-section définit l'ensemble G_{Fm} comme l'union ($\cup$) de deux sous-ensembles (G_{gen} et G_{comp}).

Cette sous-section définit alors ces deux sous-ensembles : le sous-ensemble G_{gen} contenant des éléments dits générateurs ;

le sous-ensemble G_{comp} contenant tous les éléments issus d'au moins une composition avec le loi $\otimes$ du groupe et à partir d'éléments du sous ensemble G_{gen} .

$$G_{Fm} = G_{gen} \cup G_{comp}.$$

3.2.1 Sous-ensemble G_{gen} , Eléments générateurs :

Remarque : Les définitions qui suivent présupposent connues :

la loi de composition interne (ici $\otimes$),

l'existence de l'élément symétrique d'un élément ($e_i \otimes \bar{e}_i = n_e$)

et l'existence de l'élément neutre du groupe (n_e).

Axiome – E_1 : Soit l'ensemble G_{gen} , nommé partie génératrice, cet ensemble possède un nombre fini d'éléments e_i distincts, i variant de 1 à N , possède les N éléments $\bar{e}_i$ symétriques des éléments e_i ainsi que l'élément neutre n_e .

$$G_{gen} = \{e_1, e_2, \dots, e_N, \bar{e}_1, \bar{e}_2, \dots, \bar{e}_N, n_e, \text{ avec } N > 0\}.$$

Axiome – E₂ : Tous ces éléments e_i , $\overline{e_i}$ et n_e sont dits générateurs car il n'existe pas d'éléments e_j , $e_k \dots e_l$ parmi ces $N+N+1$ éléments de G_{gen} tels que $(e_i$ ou $\overline{e_i}$ ou $n_e)$ soit $= e_j \otimes e_k \otimes \dots \otimes e_l$ et avec j et $k \dots l$ différents de i .

Ainsi $\forall e \in G_{gen}$ et hors n_e , $\nexists e_j, e_k, \dots e_l \in G_{gen}$ tels que $e = e_j \otimes e_k \otimes \dots \otimes e_l$.

Remarques :

Une exception est faite pour l'élément neutre n_e car par définition :

$e_i \otimes \overline{e_i} = n_e$.

De plus, le fait que j et $k \dots l$ soient différents de i pour l'expression

$e_i = e_j \otimes e_k \dots e_l$ est justifié pour les égalités avec n_e : $n_e = n_e \otimes n_e$,

$e_i \otimes n_e = e_i$ et $\overline{e_i} \otimes n_e = \overline{e_i}$.

3.2.2 Sous-ensemble G_{comp} , Eléments composés :

Axiome – E₃ : Soit l'ensemble G_{comp} , les éléments de cet ensemble sont tous issus d'au moins une composition avec la loi $\otimes$ et entre 2 éléments de l'ensemble G_{gen} .

Ainsi $G_{comp} = \{e_c = e_j \otimes e_k \otimes \dots \otimes e_l \text{ avec } e_j, e_k, \dots e_l \in G_{gen}\}$.

3.2.3 Ensemble G_{Fm} :

Axiome – E₄ : L'ensemble $G_{Fm} = G_{gen} \cup G_{comp}$.

3.3 Loi de composition interne $\otimes$:

Axiome – L₁ : La loi de composition interne $\otimes$ est une application f du produit cartésien $G_{Fm} \times G_{Fm}$ dans G_{Fm} pour laquelle $f(e_j, e_k) = e_l$ et notée $e_j \otimes e_k = e_l$.

(e_j et $e_k \in G_{Fm}$ alors pour la composition $e_j \otimes e_k = e_l$, $e_l \in G_{Fm}$)

Axiome – L₂ : La loi $\otimes$ est commutative : $e_i \otimes e_j = e_j \otimes e_i$.

Axiome – L₃ : La loi $\otimes$ est associative : $e_i \otimes (e_j \otimes e_k) = (e_i \otimes e_j) \otimes e_k$.

Axiome – L₄ : la loi $\otimes$ possède une loi dite inverse notée $\otimes^{-1}$ telle que pour tout élément $e_c \in G_{Fm}$,

et soient $e_1, e_2, e_k, e_i \in G_{gen}$ et soit $e_c = e_1 \otimes e_2$ alors $e_c(\otimes^{-1}e_1) = e_2$,

$e_c(\otimes^{-1}e_2) = e_1$

et $e_i \otimes \otimes^{-1}e_k = \text{Impossible}$: calcul impossible pour un élément générateur.

Algorithme – L₅ : On peut alors construire un algorithme qui permet de savoir pour un élément e_c , à priori déjà composé et pour un nombre limité de compositions,

si $e_c \in (G_{Fm}, \otimes)$ ou si $e_c \notin (G_{Fm}, \otimes)$.

Ainsi on effectue un ensemble de calculs appelé cycle de calculs, cycle car on peut être amené à le réaliser plusieurs fois.

Chaque cycle va correspondre à une sous-décomposition de niveau k de e_c .
Le premier cycle correspondant au niveau 1.

Ainsi on calcule $e_c \otimes^{-1}e_i$ pour tous les éléments $\in G_{gen}$.

Le calcul donne :

soit $e_c \otimes^{-1}e_i = \text{Impossible}$, et pour ce cas on refait le calcul avec un autre élément de G_{gen} ;

soit $e_c \otimes^{-1}e_i = e_{c_{2,i}}$ et pour ce cas on mémorise $e_{c_{2,i}}$ et on refait le calcul avec un autre élément de G_{gen} .

Le premier cycle terminé, et si l'on a trouvé un ou plusieurs éléments $e_{c_{2,i}}$, on recommence alors un autre cycle pour le calcul $e_{c_{2,i}} \otimes^{-1}e_i$, ceci pour chaque $e_{c_{2,i}}$ mémorisé au cycle précédent et toujours pour tous les éléments $\in G_{gen}$.

Le cardinal de G_{gen} est fini comme le nombre supposé de compositions de l'élément e_c .

Aussi l'algorithme s'arrête avec le résultat : $e_{c_{k,i}} \otimes^{-1}e_i = \text{Impossible}$ pour tous les éléments $\in G_{gen}$, ($e_{c_{k,i}}$: k ème sous-décomposition de e_c).

Selon k et i on peut obtenir plusieurs éléments : $e_{c_{k,i}}$.

Et chaque $e_{c_{k,i}}$ correspond au dernier élément issu du dernier calcul non "Impossible".

Alors si au moins un des éléments $e_{c_{k,i}} \in G_{gen}$, on conclut que $e_c \in (G_{Fm}, \otimes)$.

Et si tous les éléments $e_{c_{k,i}} \notin G_{gen}$, on conclut que $e_c \notin (G_{Fm}, \otimes)$.

(rappel : $e_i \otimes^{-1}e_k = \text{Impossible}$: calcul impossible pour un élément générateur ($e_i, e_k \in G_{gen}$)).

D'autres algorithmes peuvent être construits pour d'autres recherches de compositions.

3.4 Élément neutre n_e du groupe $(G_{Fm}, \otimes)$ - Élément symétrique $\bar{e}_i$ de l'élément e_i :

Axiome – Ne₁ : $\forall e_c \in (G_{Fm}, \otimes) \exists ! n_e$ nommé élément neutre et tel que $e_c \otimes n_e = e_c$.

Axiome – Es₁ : Pour chaque élément générateur e_i de l'ensemble G_{gen} il existe un unique élément symétrique $\bar{e}_i$, lui aussi générateur, tel que $e_i \otimes \bar{e}_i = n_e$.

Soit $\forall e_i \in G_{gen}, \exists ! \bar{e}_i \in G_{gen}$ tel que $e_i \otimes \bar{e}_i = n_e$.

Axiome – F₀ : Définition d'une forme $F(K)$:

soit un élément $e_c \in G_{Fm}$, e_c s'écrit : $e_c = (v_1, v_2, \dots, v_n)$ car composé de n variables entières v_i .

Un forme $F(K)$ est un élément de G_{Fm} pour lequel la valeur des variables v_i se résume à K ($v_i = K$), soit :

$$F(K) = (K, K, \dots, K).$$

K ne prend pas forcément toutes les valeurs entières >0 , soit toutes les formes $F(K)$ n'existent pas forcément.

Axiome – F₁ : Définition d'une forme élémentaire de l'élément neutre $(F(K_i))$:

soit n_e l'élément neutre du groupe $(G_{Fm}, \otimes)$,

soient deux éléments e_i et son symétrique $\bar{e}_i$ de l'ensemble G_{gen} , alors

$$F(K_i) = e_i \otimes \bar{e}_i = n_e.$$

Avec $K_i \in \mathbb{N}^*$ et donc $F(K_i) \in G_{Fm}$.

La forme $F(K_i)$ est appelée forme élémentaire de l'élément neutre car elle a la valeur logique de l'élément neutre $F(K_i) = n_e$;

et élémentaire car d'autres formes peuvent exister par composition entre elles.

Axiome – F₂ : Propriété d'une forme de l'élément neutre :

soient deux formes de l'élément neutre $F(K_1)$ et $F(K_2) \in G_{Fm}$, soient

$$(K_1 \text{ et } K_2) \in \mathbb{N}^* \text{ alors } F(K_1) \otimes F(K_2) = F(K_3) = n_e,$$

avec $K_3 \in \mathbb{N}^*$, $F(K_3) \in G_{Fm}$,

et $K_3 = f(K_1, K_2)$, (K_3 : fonction de K_1 et K_2).

Justification des axiomes *Axiome – F₁* et *Axiome – F₂* :

l'expression, l'écriture de n_e est appelé Forme de l'élément neutre et s'écrit par exemple : $(K_{n_e}, K_{n_e}, K_{n_e}, \dots, K_{n_e}) = F(K_{n_e})$ (forme pour la valeur K_{n_e}).

Cette forme est aisément reconnaissable parmi tous les éléments de l'ensemble.

La définition de n_e dépend alors d'une valeur du paramètre numérique K_{n_e} .

Ainsi $n_e = F(K_{n_e})$ et $F(K_{n_e})$ est appelée forme de l'élément neutre n_e .

Les autres formes de n_e sont obtenues pour chaque composition :

$e_i \otimes \bar{e}_i = F(K_i)$ ou $e_j \otimes \bar{e}_j = F(K_j)$.

$F(K_i)$ et $F(K_j)$ ont la même définition, la même valeur logique :

$F(K_i) = F(K_j) = n_e$.

enfin d'autres formes sont possibles par composition entre formes.

Ainsi, si toutes les compositions se font avec des éléments de G_{Fm} alors à la vue d'un forme $F(K)$ on peut déclarer immédiatement que $F(K) = n_e$.

Exemple : $F(K) = (K, K)$ avec K naturel ≥ 1 et $F(K_{n_e}) = (1, 1)$. Ainsi

$(1, 2) \oplus (2, 1) = (3, 3) = F(3)$ et $(1, 1) = (2, 2) = (3, 3) = (K, K) = n_e$.

(Lire : "Exemple de groupe $(G_{Fm}, \otimes)$ possédant des formes multiples de l'élément neutre : $(Z_{Fm}, \oplus)$ " en fin de document)

Analyse sur la valeur K_{n_e} recherchée de la forme $F(K_{n_e}) = n_e$:

A ce stade on a défini n_e qu'au travers de l'axiome *Axiome* – Ne_1

$(e_c \otimes n_e = e_c)$.

Or on sait par les axiomes *Axiome* – F_1 et *Axiome* – F_2 , que n_e doit posséder une forme $F(K_{n_e})$.

n_e est un élément générateur alors $F(K_{n_e})$ doit l'être aussi, c'est à dire non composée avec une des formes décrites par les axiomes *Axiome* – F_1 et *Axiome* – F_2 ($F(K_i) = e_i \otimes \bar{e}_i$ ou $F(K_1) \otimes F(K_2) = F(K_3)$).

De plus, pour les groupes étudiés dans la suite du document, la fonction f évoquée pour *Axiome* – F_2 ($K_3 = f(K_1, K_2)$) est croissante. Aussi Soit $K_{n_e} < \text{Min}(K_i)$,

(Plus petite valeur parmi les valeurs K_i des formes $F(K_i)$ de l'axiome *Axiome* – F_1).

Axiome – F_3 : Valeur de K_{n_e} pour la forme $F(K_{n_e}) = n_e$:

Après calcul de toutes les formes $F(K_i)$ décrites par l'axiome *Axiome* – F_1 et K_i les valeurs issues de ce calcul,

soient $K_m = \text{Min}(K_i)$ (Plus petite valeur parmi les valeurs K_i),
alors $K_{n_e} < K_m = \text{Min}(K_i)$.

Comme $K_{n_e} < K_m$ il est possible que plusieurs choix soient alors possibles.

Ces valeurs de K_{n_e} sont alors appelées des valeurs acceptables, acceptées.

Analyse préalable au lemme suivant : *Lemme* – F_3 :

A ce stade tous les axiomes nécessaires à la définition d'un groupe ont été posés.

Ceci donc dans le cadre de la Théorie des groupes.

On est alors, vis à vis de l'élément neutre, en présence de deux familles de groupes :

G_u , ceux avec un élément neutre n'ayant qu'une forme,
et la famille de groupes G_{fm} possédant des formes multiples de l'élément neutre.

Les valeurs de K_{n_e} sont des valeurs acceptables, acceptées pour la définition de ces groupes.

Aussi tous les résultats obtenus dans la théorie des groupes et impliquant l'élément neutre, doivent être identiques pour les 2 familles de groupes G_u et G_{fm} et alors pour toutes les valeurs acceptables de K_{n_e} .

Fin de l'analyse.

Lemme – F_3 : Tous les résultats obtenus dans la théorie des groupes et impliquant l'élément neutre, doivent être identiques pour les 2 familles de groupes :

G_u : groupes avec un élément neutre n'ayant qu'une forme et

G_{fm} : groupes avec formes multiples de l'élément neutre et alors pour toutes les valeurs acceptables de K_{n_e} .

Algorithme – L_6 : Réduction, simplification d'éléments :

Il est indiqué précédemment, que si toutes les compositions se font avec des éléments de G_{fm} alors à la vue d'une forme $F(K)$ on peut déclarer immédiatement que $F(K) = n_e$.

Par contre un élément e_c composé avec une forme de l'élément neutre $F(K)$ ou n_e donne une forme différente de e_c or

$$e_c \otimes f(K) = e_c \otimes n_e = e_c.$$

Aussi peut-on similairement à *Algorithme – L_5* , créer un algorithme

Algorithme – L_6 en utilisant la loi $\otimes^{-1}$ et la liste des formes $F(K_i)$ et n_e , pour dans notre exemple, retrouver la forme de e_c avant composition.

4 Caractéristiques des groupes $(G, \otimes)$:

4.1 Proposition :

Cette sous-section de propose de montrer que les groupes $(G, \otimes)$ ont les mêmes caractéristiques que les groupes $(G_{fm}, \otimes)$ possédant des formes multiples de l'élément neutre n_e .

Les groupes $(G, \otimes)$ sont construits suivant la question posée par la conjecture et résumée ainsi : " $2.N = P_1 + P_2$ avec $2.N > 3$?".

Ainsi tous les Axiomes abordés pour les groupes $(G_{Fm}, \otimes)$ sont aussi abordés pour ces groupes pour preuve ou définition.

4.2 Définition de l'ensemble G :

Cette sous-section définit l'ensemble G comme l'union ($\cup$) de deux sous-ensembles (G_{gen} et G_{comp}).

Cette sous-section définit alors ces deux sous-ensembles : le sous-ensemble G_{gen} contenant des éléments dits générateurs ;
le sous-ensemble G_{comp} contenant tous les éléments issus d'au moins une composition avec le loi $\otimes$ du groupe et à partir d'éléments du sous ensemble G_{gen} .
 $G = G_{gen} \cup G_{comp}$.

4.2.1 Sous-ensemble G_{gen} , Eléments générateurs :

Remarque : Les définitions qui suivent présupposent connues :
la loi de composition interne (ici $\otimes$),
l'existence de l'élément symétrique d'un élément ($e_i \otimes \bar{e}_i = n_e$)
et l'existence de l'élément neutre du groupe (n_e).

Axiome – E_1 : Soit l'ensemble G_{gen} , nommé partie génératrice, cet ensemble possède un nombre fini d'éléments e_i distincts, i variant de 1 à $(N-2)$, possède les $(N-2)$ éléments $\bar{e}_i$ symétriques des éléments e_i ainsi que l'élément neutre n_e .

$$G_{gen} = \{e_1, e_2, \dots, e_{N-2}, \bar{e}_1, \bar{e}_2, \dots, \bar{e}_{N-2}, n_e, \text{ avec } (N-2) > 0. \}$$

Définition des éléments générateurs :

$$G_{gen} = \{e_1, e_2, \dots, e_{N-2}, \bar{e}_1, \bar{e}_2, \dots, \bar{e}_{N-2}, n_e, \text{ avec } (N-2) > 0 \}.$$

Ces éléments sont écrits sous forme d'un couple de nombres entiers : (n_i, n_j) et tels que $n_i, n_j \in \mathbb{N}$, $n_i + n_j = 2.N$, $n_i \geq 2, n_j \geq 2$, de plus les n_i, n_j sont aussi écrits comme produit de nombres premiers p_k : $n_i = \prod_{k_i} p_{k_i}$ et $n_j = \prod_{k_j} p_{k_j}$.

On peut donc écrire que :

pour la question de la conjecture : a-t-on $2.N = P_1 + P_2$? pour $2.N > 3$, P_1 et P_2 étant des nombres premiers,

$$e_i = (N - i, N + i), i \text{ variant de } 1 \text{ à } N-2 > 0, \text{ alors } N \geq 3$$

$$\bar{e}_1 = (N + i, N - i), i \text{ variant de } 1 \text{ à } N-2 > 0, \text{ alors } N \geq 3$$

$$n_e = (N, N) : \text{ cet élément étant abordé plus loin dans le texte.}$$

Ainsi, pour le nombre $2.N$ de la conjecture, le cardinal de G_{gen} est égal à $(N-2) + (N-2) + 1 = 2.N - 3$: le nombre d'éléments de G_{gen} est égal à $2.N - 3$.

Pour $N=3$, $2.N=6$ et alors $6=3+3=2+4$ alors la conjecture est vérifiée et $P_1 = P_2 = 3$.

Pour $N=2$, $2.N=4$ et alors $4=2+2$ alors la conjecture est vérifiée et $P_1 = P_2 = 2$.

→ **Par la suite l'étude portera pour $N \geq 4$ soit $2.N \geq 8$.**

Exemple : pour $(G, \otimes)$ et $2.N=18$, les éléments générateurs sont :

(le caractère "." qui suit correspond à la multiplication entre entiers)

$$n_e = (9, 9) = (3.3, 3.3)$$

$$e_1 = (8, 10) = (2.2.2, 2.5) \text{ et } \overline{e_1} = (10, 8) = (2.5, 2.2.2)$$

$$e_2 = (7, 11) = (7, 11) \text{ et } \overline{e_2} = (11, 7) = (11, 7)$$

$$e_3 = (6, 12) = (2.3, 2.2.3) \text{ et } \overline{e_3} = (12, 6) = (2.2.3, 2.3)$$

$$e_4 = (5, 13) = (5, 13) \text{ et } \overline{e_4} = (13, 5) = (13, 5)$$

$$e_5 = (4, 14) = (2.2, 2.7) \text{ et } \overline{e_5} = (14, 4) = (2.7, 2.2)$$

$$e_6 = (3, 15) = (3, 3.5) \text{ et } \overline{e_6} = (15, 3) = (3.5, 3)$$

$$e_7 = (2, 16) = (2, 2.2.2.2) \text{ et } \overline{e_7} = (16, 2) = (2.2.2.2, 2)$$

Axiome – E_2 : Tous ces éléments e_i , $\overline{e_i}$ et n_e sont dits générateurs car il n'existe pas d'éléments e_j , $e_k \dots e_l$ parmi ces $(2.N - 3)$ éléments de G_{gen} tels que $(e_i \text{ ou } \overline{e_i} \text{ ou } n_e)$ soit $= e_j \otimes e_k \otimes \dots \otimes e_l$ et avec j et $k \dots l$ différents de i .

Ainsi $\forall e \in G_{gen}$ et hors n_e , $\nexists e_j, e_k, \dots e_l \in G_{gen}$ tels que $e = e_j \otimes e_k \otimes \dots \otimes e_l$.
Preuve : fournie à la sous-section qui suit et qui définit l'expression de la loi de composition $\otimes$.

Remarques : Une exception est faite pour l'élément neutre n_e car par définition : $e_i \otimes \overline{e_i} = n_e$.

De plus, le fait que j et $k \dots l$ soient différents de i pour l'expression $e_i = e_j \otimes e_k \dots e_l$ est justifié pour les égalités avec n_e : $n_e = n_e \otimes n_e$, $e_i \otimes n_e = e_i$ et $\overline{e_i} \otimes n_e = \overline{e_i}$.

4.2.2 Sous-ensemble G_{comp} , Eléments composés :

Axiome – E_3 : Soit l'ensemble G_{comp} , les éléments de cet ensemble sont tous issus d'au moins une composition avec la loi $\otimes$ et entre 2 éléments de l'ensemble G_{gen} .

Ainsi $G_{comp} = \{e_c = e_j \otimes e_k \otimes \dots \otimes e_l \text{ avec } e_j, e_k, \dots, e_l \in G_{gen}\}$.

Ceci ne réclame pas de preuve.

4.2.3 Ensemble G :

Axiome – E_4 : L'ensemble $G = G_{gen} \cup G_{comp}$.

4.3 Loi de composition interne $\otimes$:

Axiome – L_1 : La loi de composition interne $\otimes$ est une application f du produit cartésien $G \times G$ dans G pour laquelle $f(e_j, e_k) = e_l$ et notée $e_j \otimes e_k = e_l$. (e_j et $e_k \in G$ alors pour la composition $e_j \otimes e_k = e_l$, $e_l \in G$)

Expression de la loi $\otimes$:

(le caractère "." qui suit correspond à la multiplication entre entiers)

Soient $e_1 = (n_{11}, n_{12}) \in (G, \otimes)$, $e_2 = (n_{21}, n_{22}) \in (G, \otimes)$, avec $n_{ij} > 1 \in \mathbb{N}$
et $n_{11} + n_{12} = n_{21} + n_{22} = 2.N$

Alors la loi interne $\otimes$ est telle que $e_1 \otimes e_2 = (n_{11}.n_{21}, n_{12}.n_{22}) = e_{12}$. Si l'on écrit e_1 et e_2 comme le produit de nombres premiers alors

$$e_1 \otimes e_2 = (\prod_{k_{11}} p_{k_{11}} \cdot \prod_{k_{21}} p_{k_{21}}, \prod_{k_{12}} p_{k_{12}} \cdot \prod_{k_{22}} p_{k_{22}})$$

Axiome – E_2 : Tous ces éléments e_i , $\bar{e}_i$ et n_e sont dits générateurs car il n'existe pas d'éléments e_j , $e_k \dots e_l$ parmi ces $(2.N - 3)$ éléments de G_{gen} tels que $(e_i \text{ ou } \bar{e}_i \text{ ou } n_e)$ soit $= e_j \otimes e_k \otimes \dots \otimes e_l$ et avec j et $k \dots l$ différents de i .

Ainsi $\forall e \in G_{gen}$ et hors n_e , $\nexists e_j, e_k, \dots, e_l \in G_{gen}$ tels que $e = e_j \otimes e_k \otimes \dots \otimes e_l$.

Preuve :

soit $e \in G_{gen}$ tel que $e = (N \pm i, N \mp i)$,

soit $e_j \in G_{gen}$ tel que $e_j = (N \pm j, N \mp j)$,

soit $e_k \in G_{gen}$ tel que $e_k = (N \pm k, N \mp k)$,

alors $e_j \otimes e_k = ((N \pm j).(N \pm k), (N \mp j).(N \mp k))$ ce qui ne peut être égal à $e = (N \pm i, N \mp i)$ et encore moins avec une autre composition.

Axiome – L_2 : La loi $\otimes$ est commutative : $e_i \otimes e_j = e_j \otimes e_i$.

Preuve : Cette propriété est héritée de la multiplication arithmétique ".".

Axiome – L_3 : La loi $\otimes$ est associative : $e_i \otimes (e_j \otimes e_k) = (e_i \otimes e_j) \otimes e_k$.

Preuve : Cette propriété est héritée de la multiplication arithmétique ".".

*Axiome – L_4 : la loi $\otimes$ possède une loi dite inverse notée $\otimes^{-1}$ telle que pour tout élément $e_c \in G_{Fm}$,
et soient $e_1, e_2, e_k, e_i \in G_{gen}$ et soit $e_c = e_1 \otimes e_2$ alors $e_c \otimes^{-1} e_1 = e_2$,
 $e_c \otimes^{-1} e_2 = e_1$
et $e_i \otimes^{-1} e_k = Impossible : calcul impossible pour un élément générateur.$*

Cette loi existe et correspond à la division euclidienne $\div$.

*Algorithme – L_5 : On peut alors construire un algorithme qui permet de savoir pour un élément e_c , à priori déjà composé et pour un nombre limité de compositions,
si $e_c \in (G, \otimes)$ ou si $e_c \notin (G, \otimes)$: Admis, non développé .*

Remarques et Exemple pour $(G, \otimes)$ (2.N=18) :

$$e_1 = (8, 10) = (2.2.2, 2.5)$$

$$e_2 = (4, 14) = (2.2, 2.7)$$

$$e_1 \otimes e_2 = (2.2.2.2.2, 2.5.2.7) = e_{12} = (32, 140)$$

(Axiome – L_1) $e_{12} \in (G, \otimes)$ car il est composé de 2 éléments de $(G, \otimes)$ et même si $32+140$ n'est plus égal à $9+9=18$.

(Axiome – L_1 – Algorithme – L_5) Si l'on ne connaît que $e_{12} = (32, 140)$ on peut décomposer 32 et 140 en produit de nombres premiers : $(2.2.2.2.2, 2.5.2.7)$ et connaissant les éléments générateurs $(G, \otimes)$, on peut construire un algorithme avec la loi $\div$ qui permet de trouver e_1 et e_2 à l'origine de la composition et affirmer, dans notre cas, que $e_{12} \in (G, \otimes)$ car exclusivement composé d'éléments de $(G, \otimes)$.

4.4 Elément neutre n_e du groupe $(G, \otimes)$ - Elément symétrique $\overline{e_i}$ de l'élément e_i :

Axiome – Ne_1 : $\forall e_c \in (G, \otimes) \exists ! n_e$ nommé élément neutre et tel que $e_c \otimes n_e = e_c$.

*Axiome – Es_1 : Pour chaque élément générateur e_i de l'ensemble G_{gen} il existe un unique élément symétrique $\overline{e_i}$, lui aussi générateur, tel que $e_i \otimes \overline{e_i} = n_e$.
Soit $\forall e_i \in G_{gen}, \exists ! \overline{e_i} \in G_{gen}$ tel que $e_i \otimes \overline{e_i} = n_e$.*

Preuve de l'existence de l'élément symétrique (Axiome – Es₁) :

Soit l'élément générateur $e_1 = (n_{11}, n_{12})$ de $(G, \otimes)$ alors $\overline{e_1} = (n_{12}, n_{11})$ et tel que :
 $e_1 \otimes \overline{e_1} = (n_{11}.n_{12}, n_{12}.n_{11}) = (m_1, m_1) = n_e$ avec $m_1 = n_{11}.n_{12} = n_{12}.n_{11}$.
 (m_1, m_1) étant une forme de l'élément neutre : sujet abordé plus loin dans le texte.

$\overline{e_1}$ est bien un élément générateur de $(G, \otimes)$ car
 $n_{12} + n_{11} = n_{11} + n_{12} = 2.N$.

Preuve de l'unicité de l'élément symétrique (Axiome – Es₁) :

Soit $\overline{e_2} = (a_2, b_2)$ un autre élément générateur et symétrique de e_1 alors
 $a_2 + b_2 = 2.N$,
 $e_1 \otimes \overline{e_2} = (n_{11}.a_2, n_{12}.b_2) = (m_2, m_2)$,
on a donc $n_{11}.a_2 = n_{12}.b_2 = m_2$, alors
 $a_2 = n_{12}.b_2/n_{11}$ et $\in \mathbb{N}$ ce qui donne $b_2 = n_{11}.k$ et $a_2 = n_{12}.k$.
Donc $\overline{e_2} = (n_{12}.k, n_{11}.k)$ soit $k.(n_{12} + n_{11}) = k.(2.N) = 2.N$ car $\overline{e_2}$ doit
 $\in (G, \otimes)$,
ce qui n'est vrai que pour $k = 1$, soit $\overline{e_2} = \overline{e_1}$: l'élément symétrique $\overline{e_1}$ est bien unique.

Pour un autre élément $e_2 \otimes \overline{e_2} = (m_2, m_2)$ avec m_2 différent de m_1 . Comme n_e est unique, on dit que les 2 couples : (m_1, m_1) et (m_2, m_2) sont des formes différentes de n_e l'élément neutre. Car elles ont la même valeur logique, la même définition que l'élément neutre.

Axiome – F₀ : Définition d'une forme $F(K)$:

soit un élément $e_c \in G$, e_c s'écrit : $e_c = (v_1, v_2)$ car composé de 2 variables entières v_i .

Un forme $F(K)$ est un élément de G pour lequel la valeur des variables v_i se résume à K ($v_i = K$), soit :

$$F(K) = (K, K).$$

K ne prend pas forcément toutes les valeurs entières >0 , soit toutes les formes $F(K)$ n'existent pas forcément.

Axiome – F₁ : Définition d'une forme élémentaire de l'élément neutre ($F(K_i)$) :

soit n_e l'élément neutre du groupe $(G, \otimes)$,
soient deux éléments e_i et son symétrique $\overline{e_i}$ de l'ensemble G_{gen} , alors

$$F(K_i) = e_i \otimes \overline{e_i} = n_e.$$

Avec $K_i \in \mathbb{N}^*$ et donc $F(K_i) \in G$.

La forme $F(K_i)$ est appelée forme élémentaire de l'élément neutre car elle a la valeur logique de l'élément neutre $F(K_i) = n_e$;
et élémentaire car d'autres formes peuvent exister par composition entre elles.

Calcul de toutes les formes $F(K_i) = e_i \otimes \bar{e}_i = n_e$:

On sait que pour i variant de 1 à $(N-2)$:
 $e_i = (N - i, N + i)$ et $\bar{e}_i = (N + i, N - i)$.
De plus $e_i \otimes \bar{e}_i = ((N - i).(N + i), (N + i).(N - i)) = F(K_i)$
Alors $F(K_i) = (N^2 - i^2, N^2 - i^2)$,
soit $K_i = N^2 - i^2$ pour i variant de 1 à $(N-2)$.

Axiome – F_2 : Propriété d'une forme de l'élément neutre :

soient deux formes de l'élément neutre $F(K_1)$ et $F(K_2) \in G$, soient
 $(K_1 \text{ et } K_2) \in \mathbb{N}^*$ alors $F(K_1) \otimes F(K_2) = F(K_3) = n_e$,
avec $K_3 \in \mathbb{N}^*$, $F(K_3) \in G$,
et $K_3 = f(K_1, K_2)$, (K_3 : fonction de K_1 et K_2).

Calcul de $F(K_1) \otimes F(K_2) = F(K_3)$:

Soient $F_1 = (K_1, K_1)$ et $F_2 = (K_2, K_2)$ alors
 $F(K_3) = F(K_1) \otimes F(K_2) = (K_1.K_2, K_1.K_2)$, *la fonction f est donc croissante.*

Axiome – F_3 : Valeur de K_{n_e} pour la forme $F(K_{n_e}) = n_e$:

Après calcul de toutes les formes $F(K_i)$ décrites par l'axiome *Axiome – F_1*
et K_i les valeurs issues de ce calcul,
soient $K_m = \text{Min}(K_i)$ (Plus petite valeur parmi les valeurs K_i),
alors $K_{n_e} < K_m$.

Détermination de l'élément neutre n_e en fixant la valeur unique K_{n_e} :

On sait que $F(K_i) = (N^2 - i^2, N^2 - i^2)$ pour i variant de 1 à $(N-2)$ et donc
que $K_i = N^2 - i^2$,

alors $K_m = \text{Min}(K_i) = 4.N - 4 = 4.(N - 1)$

(Plus petite valeur parmi les valeurs K_i et pour $i = N-2$). Ainsi

$K_m = N^2 - (N - 2)^2 = N^2 - N^2 + 4.N - 4 = 4.N - 4$

Cependant il existe une forme parmi les éléments générateurs non issue de composition : (N, N) .

C'est cette valeur qui est retenue pour K_{n_e} : $K_{n_e} = N$ et l'on a bien

$K_{n_e} < K_m$.

Alors $n_e = (N, N)$.

Ce choix est arbitraire et d'autres choix sont possibles.

Ainsi on peut montrer que $n_e = (P^n, P^n)$ avec $n > 0$ et P nombre premier $> 2.N$ de la conjecture est aussi un choix possible.

Autres possibilités de déclaration de l'élément neutre n_e :

on peut par exemple, déclarer, choisir $n_e = (P_1^n, P_1^n)$ avec $n \geq 1$ et P_1 nombre premier supérieur au plus grand nombre premier rencontré lors de chaque décomposition des e_i en produit de nombres premiers.

Cette déclaration correspond bien à un élément générateur car on ne peut obtenir $n_e = e_i \otimes \bar{e}_i = (m_i, m_i) = F(K_i) = (P_1^n, P_1^n)$ ou $n_e = F(K_i) \otimes F(K_j)$ puisque m_k décomposé en produit de nombres premiers, ne contient pas P_1 .

La seule différence est que $P_1 + P_1 \neq N + N$, ce qui ne pose pas de problème en soit.

Exemple : Formes multiples de l'élément neutre pour $(G, \otimes)$ avec $2.N=18$:

$$F_{(0,9)} = (9, 9) = (3.3, 3.3)$$

$$F_{(1,9)} = (80, 80) = (\boxed{2}.2.2.2.\boxed{5}, 2.2.2.2.5) \text{ pour } (8, 10) \otimes (10, 8)$$

$$F_{(2,9)} = (77, 77) = (\boxed{7}.\boxed{11}, 7.11) \text{ pour } (7, 11) \otimes (11, 7)$$

$$F_{(3,9)} = (72, 72) = (2.\boxed{3}.2.2.3, 2.3.2.2.3) \text{ pour } (6, 12) \otimes (12, 6)$$

$$F_{(4,9)} = (65, 65) = (5.\boxed{13}, 13.5) \text{ pour } (5, 13) \otimes (13, 5)$$

$$F_{(5,9)} = (56, 56) = (2.2.2.7, 2.2.2.7) \text{ pour } (4, 14) \otimes (14, 4)$$

$$F_{(6,9)} = (45, 45) = (3.3.5, 3.3.5) \text{ pour } (3, 15) \otimes (15, 3)$$

$$F_{(7,9)} = (32, 32) = (2.2.2.2.2, 2.2.2.2.2) \text{ pour } (2, 16) \otimes (16, 2)$$

Le plus grand nombre premier rencontré lors de chaque décomposition des e_i en produit de nombres premiers est $\boxed{13}$.

Aussi peut on aussi choisir $n_e = (17^n, 17^n)$, $n \geq 1$, car 17 nombre premier > 13 .

Lemme – F_3 : Tous les résultats obtenus dans la théorie des groupes et impliquant l'élément neutre, doivent être identiques pour les 2 familles de

groupes :

G_u : groupes avec un élément neutre n'ayant qu'une forme et

G_{fm} : groupes avec formes multiples de l'élément neutre et alors pour toutes les valeurs acceptables de K_{n_e} .

Algorithme – L_6 : Réduction, simplification d'éléments :

Il est indiqué précédemment, que si toutes les compositions se font avec des éléments de G_{Fm} alors à la vue d'une forme $F(K)$ on peut déclarer immédiatement que $F(K) = n_e$.

Par contre un élément e_c composé avec une forme de l'élément neutre $F(K)$ ou n_e donne une forme différente de e_c or

$$e_c \otimes F(K) = e_c \otimes n_e = e_c.$$

Aussi peut-on similairement à *Algorithme – L_5* , créer un algorithme *Algorithme – L_6* en utilisant la loi $\otimes^{-1}$ (ici $\div$) et la liste des formes $F(K_i)$ et n_e , pour dans notre exemple, retrouver la forme de e_c avant composition.

5 Caractéristiques du groupe $(Z_R, \oplus)$:

5.1 Proposition :

Cette sous-section propose de montrer que le groupe $(Z_R, \oplus)$ possède les mêmes caractéristiques que les groupes $(G_{Fm}, \otimes)$ possédant des formes multiples de l'élément neutre n_z .

Ainsi tous les axiomes abordés pour les groupes $(G_{Fm}, \otimes)$ sont aussi abordés pour ce groupe pour preuve ou définition.

5.2 Définition de l'ensemble Z_R :

Cette sous-section définit l'ensemble Z_R comme l'union ($\cup$) de deux sous-ensembles (Z_{gen} et Z_{comp}).

Cette sous-section définit alors ces deux sous-ensembles : le sous-ensemble Z_{gen} contenant des éléments dits générateurs ; le sous-ensemble Z_{comp} contenant tous les éléments issus d'au moins une composition avec le loi $\oplus$ du groupe et à partir d'éléments du sous ensemble Z_{gen} .

$$Z_R = Z_{gen} \cup Z_{comp}.$$

5.2.1 Sous-ensemble Z_{gen} , Éléments générateurs :

Remarque : Les définitions qui suivent présupposent connues : la loi de composition interne (ici $\oplus$),

l'existence de l'élément symétrique d'un élément ($e_1 \oplus \overline{e_1} = n_z$)
et l'existence de l'élément neutre du groupe (n_z).

Expression des éléments de Z_R , Définition de Z_{gen} :

Les éléments de Z_R sont écrits sous forme de couple de nombres entiers :
(n_i, n_j) avec n_i et $n_j \in \mathbb{N}^*$.

*Axiome – E_1 : Soit l'ensemble Z_{gen} , nommé partie génératrice,
cet ensemble possède un nombre fini d'éléments : e_1 ,
 $\overline{e_1}$ l'élément symétrique de l'élément e_1 ainsi que l'élément neutre n_z .
 $Z_{gen} = \{e_1, \overline{e_1}, n_z\}$.
 $e_1 = (1, 2)$
 $\overline{e_1} = (2, 1)$
 $n_z = (1, 1)$: la justification de cet élément est abordé plus loin dans le
texte.*

*Axiome – E_2 : Tous ces éléments e_1 , $\overline{e_1}$ et n_z sont dits générateurs car il
n'existe pas d'autres éléments qui permettraient par composition, de les
obtenir.*

5.2.2 Sous-ensemble Z_{comp} , Eléments composés :

*Axiome – E_3 : Soit l'ensemble Z_{comp} , les éléments de cet ensemble sont
tous issus d'au moins une composition avec la loi $\oplus$ et entre 2 éléments de
l'ensemble Z_{gen} .*

Ainsi $Z_{comp} = \{e_c = e_j \otimes e_k \otimes \dots \otimes e_l \text{ avec } e_j, e_k, \dots, e_l \in Z_{gen}\}$.

Ceci ne réclame pas de preuve.

5.2.3 Ensemble Z_R :

Axiome – E_4 : L'ensemble $Z_R = Z_{gen} \cup Z_{comp}$.

5.3 Loi de composition interne $\oplus$:

*Axiome – L_1 : La loi de composition interne $\oplus$ est une application f
du produit cartésien $Z_R \times Z_R$ dans Z_R pour laquelle $f(e_j, e_k) = e_l$ et notée
 $e_j \oplus e_k = e_l$.*

(e_j et $e_k \in Z_R$ alors pour la composition $e_j \oplus e_k = e_l, e_l \in Z_R$)

Expression de la loi $\oplus$:

soient a, b, c, d entiers > 0 et $+$: l'addition arithmétique,
soient $e_j = (a, b)$ et $e_k = (c, d) \in Z_R$

alors $e_j \oplus e_k = (a + c, b + d) = e_l$ et $e_l \in Z_R$.

Axiome – L₂ : La loi $\oplus$ est commutative : $e_i \oplus e_j = e_j \oplus e_i$.

Preuve : Cette propriété est héritée de l'addition arithmétique $+$.

Axiome – L₃ : La loi $\oplus$ est associative : $e_i \oplus (e_j \oplus e_k) = (e_i \oplus e_j) \oplus e_k$.

Preuve : Cette propriété est héritée de l'addition arithmétique $+$.

*Axiome – L₄ : la loi $\oplus$ possède une loi dite inverse notée $\oplus^{-1}$ telle que pour tout élément $e_c \in Z_R$,
et soient $e_1, e_2, e_k, e_i \in Z_R$ et soit $e_c = e_1 \oplus e_2$ alors $e_c \oplus^{-1} e_1 = e_2$,
 $e_c \oplus^{-1} e_2 = e_1$
et $e_i \oplus^{-1} e_k = \text{Impossible}$: calcul impossible pour un élément générateur.*

Cette loi existe et correspond à la soustraction arithmétique $(-)$.

*Algorithme – L₅ : On peut alors construire un algorithme qui permet de savoir pour un élément e_c , à priori déjà composé et pour un nombre limité de compositions,
si $e_c \in (Z_R, \oplus)$ ou si $e_c \notin (Z_R, \oplus)$: Admis, non développé.*

5.4 Élément neutre n_z du groupe $(Z_R, \oplus)$ - Élément symétrique $\bar{e}_i$ de l'élément e_i :

Axiome – Ne₁ : $\forall e_c \in (Z_R, \oplus) \exists ! n_z$ nommé élément neutre et tel que $e_c \oplus n_z = e_c$.

Axiome – Es₁ : Pour chaque élément générateur e_i de l'ensemble Z_{gen} il existe un unique élément symétrique $\bar{e}_i$, lui aussi générateur, tel que $e_i \oplus \bar{e}_i = n_z$.

Soit $\forall e_i \in Z_{gen}, \exists ! \bar{e}_i \in Z_{gen}$ tel que $e_i \oplus \bar{e}_i = n_z$.

Preuve :

$e_1 = (1, 2)$, $\bar{e}_1 = (2, 1)$ alors

$e_1 \oplus \bar{e}_1 = (1, 2) \oplus (2, 1) = (2 + 1, 1 + 2) = (3, 3) = n_z$.

Axiome – F₀ : Définition d'une forme $F(K)$:

soit un élément $e_c \in Z_R$, e_c s'écrit : $e_c = (v_1, v_2)$ car composé de 2 variables entières v_i .

Un forme $F(K)$ est un élément de Z_R pour lequel la valeur des variables v_i se résume à K ($v_i = K$), soit :

$$F(K) = (K, K).$$

K ne prend pas forcément toutes les valeurs entières >0 , soit toutes les formes $F(K)$ n'existent pas forcément.

Axiome – F_1 : Définition d'une forme élémentaire de l'élément neutre ($F(K_i)$) :

soit n_z l'élément neutre du groupe $(Z_R, \oplus)$,

soient deux éléments e_i et son symétrique $\bar{e}_i$ de l'ensemble Z_{gen} , alors

$$F(K_i) = e_i \oplus \bar{e}_i = n_z.$$

Avec $K_i \in \mathbb{N}^*$ et donc $F(K_i) \in Z_R$.

La forme $F(K_i)$ est appelée forme élémentaire de l'élément neutre car elle a la valeur logique de l'élément neutre $F(K_i) = n_z$;
et élémentaire car d'autres formes peuvent exister par composition entre elles.

Calcul des formes $F(K_i)$:

Comme vu précédemment : $e_1 = (1, 2)$, $\bar{e}_1 = (2, 1)$ alors
 $e_1 \oplus \bar{e}_1 = (1, 2) \oplus (2, 1) = (2 + 1, 1 + 2) = (3, 3) = F(3)$,
et $F(3)$ est la seule forme de ce type.

Axiome – F_2 : Propriété d'une forme de l'élément neutre :

soient deux formes de l'élément neutre $F(K_1)$ et $F(K_2) \in Z_R$, soient
 $(K_1 \text{ et } K_2) \in \mathbb{N}^*$ alors $F(K_1) \oplus F(K_2) = F(K_3) = n_z$,
avec $K_3 \in \mathbb{N}^*$, $F(K_3) \in Z_R$,
et $K_3 = f(K_1, K_2)$, (K_3 : fonction de K_1 et K_2).

$$F(K_1) \oplus F(K_2) = (K_1, K_1) \oplus (K_2, K_2) = (K_1 + K_2, K_1 + K_2) = F(3)$$

, $K_3 = f(K_1, K_2)$, f est donc une fonction croissante.

Axiome – F_3 : Valeur de K_{n_z} pour la forme $F(K_{n_z}) = n_z$:

Après calcul de toutes les formes $F(K_i)$ décrites par l'axiome *Axiome – F_1*
et K_i les valeurs issues de ce calcul,
soient $K_m = \text{Min}(K_i)$ (Plus petite valeur parmi les valeurs K_i),
alors $K_{n_z} < K_m$.

La seule forme issue du calcul entre symétrique est $F(3) = (3, 3) = K_m$ et
comme $K_{n_z} < K_m$, on choisit $K_{n_z} = (1, 1)$.

Lemme – F_3 : Tous les résultats obtenus dans la théorie des groupes et impliquant l'élément neutre, doivent être identiques pour les 2 familles de groupes :

G_u : groupes avec un élément neutre n'ayant qu'une forme et

G_{fm} : groupes avec formes multiples de l'élément neutre et alors pour toutes les valeurs acceptables de K_{n_e} .

Algorithme – L_6 : Réduction, simplification d'éléments :

Il est indiqué précédemment, que si toutes les compositions se font avec des éléments de Z_R alors à la vue d'un forme $F(K)$ on peut déclarer immédiatement que $F(K) = n_z$.

Par contre un élément e_c composé avec une forme de l'élément neutre

$F(K)$ ou n_z donne une forme différente de e_c or

$$e_c \oplus F(K) = e_c \oplus n_z = e_c.$$

Aussi peut-on similairement à *Algorithme – L_5* , créer un algorithme

Algorithme – L_6 en utilisant la loi $\otimes^{-1}$ (ici la soustraction (-)) et la liste des formes $F(K_i)$ et n_z , pour dans notre exemple, retrouver la forme de e_c avant composition.

soit $e = (a, b) \in Z_R$ et $m = \text{Min}(a, b)$ (plus petite valeur entre a et b) et $a > 1$ $b > 1$, alors la forme simplifiée de (a,b) est $(a - m + 1, b - m + 1)$.

Vérification : $(a - m + 1, b - m + 1) \oplus (m - 1, m - 1) =$

$$(a - m + 1 + m - 1, b - m + 1 + m - 1) = (a, b).$$

6 Morphisme de groupe entre $(G, \otimes)$ et $(Z_R, \oplus)$:

6.1 Proposition :

Cette section se propose de construire, par une application f , un morphisme de groupes entre les 2 groupes abordés dans les sections précédentes :

$(G, \otimes)$ et $(Z_R, \oplus)$.

Alors on doit obtenir : $\forall (x, y) \in G^2, f(x \otimes y) = f(x) \oplus f(y)$.

Démonstration d'un morphisme de groupe par une application $f : (G, \otimes) \rightarrow (Z_R, \oplus)$:

Soit une application f du produit cartésien $G \times G$ dans $Z_R : G \longrightarrow^f Z_R$.

Soit $e_i = (a, b) \in (G, \otimes)$ et a et b écrits sous forme de produit des facteurs premiers composants a et b.

$$\Rightarrow e_i = (a, b) = (\prod_{k_i=1}^{k_i=n_{i,1}} p_{k_i}, \prod_{l_i=1}^{l_i=n_{i,2}} p_{l_i}).$$

Soit encore : $e_i = (\text{Produit de } n_{i,1} \text{ nombres premiers } p_{k_i}, \text{Produit de } n_{i,2} \text{ nombres premiers } p_{l_i})$.

$$\begin{aligned} & \text{Alors :} \\ \Rightarrow f(e_i) &= (n_{i,1}, n_{i,2}). \end{aligned}$$

En appliquant pour un autre élément e_j , la notation utilisée pour e_i

$$\begin{aligned} & \text{Alors :} \\ \Rightarrow f(e_j) &= (n_{j,1}, n_{j,2}). \\ \text{Et } \Rightarrow f(e_i) \oplus f(e_j) &= (n_{i,1}, n_{i,2}) \oplus (n_{j,1}, n_{j,2}) = (n_{i,1} + n_{j,1}, n_{i,2} + n_{j,2}). \end{aligned}$$

Calcul de $f(e_i \otimes e_j)$:

$$\begin{aligned} \Rightarrow f(e_i \otimes e_j) &= f((\prod_{k_i=1}^{k_i=n_{i,1}} p_{k_i}) \cdot (\prod_{k_j=1}^{k_j=n_{j,1}} p_{k_j}), (\prod_{l_i=1}^{l_i=n_{i,2}} p_{l_i}) \cdot (\prod_{l_j=1}^{l_j=n_{j,2}} p_{l_j})). \\ f(e_i \otimes e_j) &= f(\prod_{k_{ij}=1}^{k_{ij}=n_{i,1}+n_{j,1}} p_{k_{ij}}, \prod_{l_{ij}=1}^{l_{ij}=n_{i,2}+n_{j,2}} p_{l_{ij}}) \\ &= (n_{i,1} + n_{j,1}, n_{i,2} + n_{j,2}) = f(e_i) \oplus f(e_j). \end{aligned}$$

$$\begin{aligned} & \text{On obtient alors :} \\ \Rightarrow f(e_i \otimes e_j) &= f(e_i) \oplus f(e_j) \end{aligned}$$

Fin de la Démonstration

Exemple : pour $(G, \otimes)$:

$$e_1 = (8, 10) = (2.2.2, 2.5) \Rightarrow f(e_1) = (3, 2).$$

$$e_2 = (4, 14) = (2.2, 2.7) \Rightarrow f(e_2) = (2, 2).$$

$$e_1 \otimes e_2 = (2.2.2.2.2, 2.5.2.7) \Rightarrow f(e_1 \otimes e_2) = (5, 4) = f(e_1) \oplus f(e_2) = (3 + 2, 2 + 2).$$

6.2 Formes multiples de l'élément neutre : $F_z(K_i) = (K_i, K_i)$.

$$\begin{aligned} & \text{Si } f(e_i) = (n_{i,1}, n_{i,2}), \text{ alors } f(\bar{e}_i) = (n_{i,2}, n_{i,1}), \\ f(e_i \otimes \bar{e}_i) &= f(e_i) \oplus f(\bar{e}_i) = (n_{i,1} + n_{i,2}, n_{i,1} + n_{i,2}) = (K_i, K_i) = F_z(K_i), \\ f(e_i \otimes \bar{e}_i) &= f(F_{(i,N)}). \end{aligned}$$

Ainsi à chaque forme multiple de l'élément neutre de $(G, \otimes) : F_{(i,N)}$,
correspond une forme multiple de l'élément neutre de $(Z, \oplus)$:

$$F_z(K_i) = (K_i, K_i), \text{ avec } K_i \in \mathbb{N} > 1.$$

L'élément neutre retenu pour $(G, \otimes)$:

$$\begin{aligned} n_e &= F_{(0,N)} = (N, N) = (\prod_{k=1}^{k=n_{0,e}} p_k, \prod_{k=1}^{k=n_{0,e}} p_k), \\ \text{aussi } f(n_e) &= (n_{0,e}, n_{0,e}) = F_z(n_{0,e}) = F_z(K_{0,e}), (K_{0,e} = n_{0,e}). \end{aligned}$$

7 Fin de la démonstration de la conjecture :

7.1 Proposition :

Cette section se propose de clore la démonstration de la conjecture.

Une des propriétés des morphismes de groupes indique que l'image $Im(f) = f(G)$ du morphisme de groupes $f : (G, \otimes) \rightarrow (Z_R, \oplus)$ est un sous-groupe de Z_R ; cette propriété est aussi démontrée pour ces groupes avec des formes multiples de l'élément neutre.

On déduit alors qu'il existe au moins un élément $e_p \in G$ tel que $f(e_p) = (1, 1)$ (car $Im(f) = f(G)$ est un sous-groupe).

On recherche alors cet élément dans G :

On montre que $f(n_e) = (n, n)$ avec quelque soit $n > 0$, n'est pas forcément cet élément.

On montre enfin que l'élément $e_p \in G_{gen}$.

Ainsi $e_p = (P_i, P_j)$ (P_i peut être égal à P_j) et $f(e_p) = (1, 1)$ ce qui clos la démonstration.

Théorème :

$\Rightarrow$ il existe au moins un élément $e_p \in G_{gen}$ et pour $2.N > 3$ tel que

$e_p = (P_i, P_j)$ (ou $P_i = P_j$),

(et pour $2.N \geq 8 : e_p \in \{G_{gen} - \{n_e\}\}$)

$\Rightarrow$ avec P_i et P_j des nombres premiers tels que $P_i + P_j = 2.N$.

Ce qui équivaut à :

Tout nombre entier pair supérieur à 3 peut s'écrire comme une somme de deux nombres premiers.

7.2 Démonstration que l'image $Im(f) = f(G)$ du morphisme de groupe est un sous-groupe. :

Rappels :

Rappel 1 :

Soit une application f du produit cartésien $G \times G$ dans $Z_R : G \xrightarrow{f} Z_R$.

Soit $e_i = (a, b) \in (G, \otimes)$ et a et b écrits sous forme de produit des facteurs premiers composants a et b .

$$\Rightarrow e_i = (a, b) = (\prod_{k_i=1}^{k_i=n_{i,1}} p_{k_i}, \prod_{l_i=1}^{l_i=n_{i,2}} p_{l_i}).$$

Soit encore : $e_i = (\text{Produit de } n_{i,1} \text{ nombres premiers } p_{k_i}, \text{Produit de } n_{i,2} \text{ nombres premiers } p_{l_i})$.

Alors :

$$\Rightarrow f(e_i) = (n_{i,1}, n_{i,2}).$$

Rappel 2 :

Lemme – F_3 : Tous les résultats obtenus dans la théorie des groupes et impliquant l'élément neutre, doivent être identiques pour les 2 familles de groupes :

G_u : groupes avec un élément neutre n'ayant qu'une forme et
 G_{fm} : groupes avec formes multiples de l'élément neutre et alors pour
toutes les valeurs acceptables de K_{ne} .

Rappel 3 :

Détermination de l'élément neutre n_e en fixant la valeur unique K_{ne} :

*On sait que $F(K_i) = (N^2 - i^2, N^2 - i^2)$ pour i variant de 1 à $(N-2)$ et donc
que $K_i = N^2 - i^2$,*

alors $K_m = \text{Min}(K_i) = 4.N - 4 = 4.(N - 1)$

(Plus petite valeur parmi les valeurs K_i et pour $i = N-2$). Ainsi

$K_m = N^2 - (N - 2)^2 = N^2 - N^2 + 4.N - 4 = 4.N - 4$

*Cependant il existe une forme parmi les éléments générateurs non issue de
composition : (N, N) .*

C'est cette valeur qui est retenue pour K_{ne} : $K_{ne} = N$ et l'on a bien

$K_{ne} < K_m$.

Alors $n_e = (N, N)$.

Ce choix est arbitraire et d'autres choix sont possibles.

Ainsi on peut montrer que $n_e = (P^n, P^n)$ avec $n > 0$ et P nombre premier $>$
 $2.N$ de la conjecture est aussi un choix possible.

Fin des rappels.

Analyse des formes des images par f des éléments de G :

ces images peuvent être de la forme : (a,b) ou (b,a) ou (c,c) avec a,b,c des
entiers ≥ 1 , a différent de b , les couples appartenant à Z_R : soit $f(e) =$
 (a,b) ou (b,a) ou (c,c) .

Si la forme (a,b) existe alors son symétrique (b,a) aussi.

Pour la forme (c,c) , c peut être égal à 1, soit $(1,1)$ et alors par la définition
de f , l'élément e de G est (P_1, P_2) , P_1 et P_2 étant des nombres premiers et
donc décomposé en un seul facteur premier.

L'élément e de G tel que $f(e) = (1,1)$ ne peut appartenir au sous-ensemble
de G : G_{comp} car ces éléments sont issus de compositions avec la loi $\otimes$ et
dans ce cas le nombre de facteurs premiers est ≥ 2 et ne peut donc pas être
 $= 1$.

Fin de l'analyse des formes des images par f des éléments de G .

Pour un morphisme de groupes avec des éléments neutres respectivement
 e et e' ne possédant qu'une forme,

$f(e) = e'$ et l'image de ce morphisme est un sous-groupe.

Pour un morphisme de groupes avec des formes multiples des éléments neutres
respectivement n_e et n_z , $f(n_e) = (n, n)$ avec n arbitraire > 0 est une forme
de l'élément neutre n_z mais avec une valeur logique : $f(n_e) = (n, n) = n_z$.

Faisons l'hypothèse que l'image $Im(f) = f(G)$ ne soit pas un sous-groupe de Z_R :

alors pour $n=1$, $f(n_e) = (n, n) = (1, 1)$ alors $Im(f) = f(G)$ est un sous-groupe de Z_R .

et pour $n>1$, alors $Im(f) = f(G)$ n'est pas un sous-groupe de Z_R .

Or d'après le *Lemme – F_3* : Tous les résultats obtenus dans la théorie des groupes et impliquant l'élément neutre, doivent être identiques pour les 2 familles de groupes :

G_u : groupes avec un élément neutre n'ayant qu'une forme et

G_{fm} : groupes avec formes multiples de l'élément neutre et alors pour toutes les valeurs acceptables de K_{n_e} .

Les résultats sont contradictoires, aussi c'est l'hypothèse de départ qui est fausse et donc : $Im(f) = f(G)$ est un sous-groupe de Z_R .

Ainsi il existe au moins un élément de G : e_c tel que $f(e_c) = (1, 1)$.

Alors $f(n_e) = (n, n)$ correspond à $n-1$ compositions $\oplus$ avec $(1, 1)$ et en effet, n'influe pas sur la structure de l'image du morphisme.

$Im(f) = f(G)$ du morphisme de groupes $f : (G, \otimes) \rightarrow (Z_R, \oplus)$ est donc un sous-groupe de Z_R .

7.3 Recherche de l'élément e_p de G tel que $f(e_p) = (1, 1)$:

$Im(f) = f(G)$ est un sous-groupe de Z_R on se propose alors de rechercher au moins un élément e_p de G

tel que $f(e_p) = (1, 1) = n_z, n_z$ étant l'élément neutre de Z_R .

Rappel : $G = G_{gen} \cup G_{comp}$

Si $e_p \in G_{comp}$ alors si $e_p = (a, b)$ et si l'on écrit a et b en produit de facteurs premiers alors a et b ne sont pas des premiers ;

Aussi $e_p \in G_{gen}$ et l'on vient de montrer que ne doit pas tenir compte de n_e , ainsi $e_p \in \{G_{gen} - \{n_e\}\}$

Comme il a été vu précédemment :

Pour $N=3$, $2.N=6$ et alors $6=3+3=2+4$ alors la conjecture est vérifiée et $P_1 = P_2 = 3$.

Pour $N=2$, $2.N=4$ et alors $4=2+2$ alors la conjecture est vérifiée et $P_1 = P_2 = 2$.

Ainsi l'étude a porté pour $N \geq 4$ soit $2.N \geq 8$ et la conjecture est vérifiée pour $2.N=4$ et $2.N=6$.

Le résultat concerne alors $2.N > 3$ comme indiqué dans la conjecture.

Théorème :

$\Rightarrow$ il existe au moins un élément $e_p \in G_{gen}$ et pour $2.N > 3$ tel que $e_p = (P_i, P_j)$,

(et pour $2.N \geq 8$: $e_p \in \{G_{gen} - \{n_e\}\}$)

$\Rightarrow$ avec P_i et P_j des nombres premiers tels que $P_i + P_j = 2.N$.

Ce qui équivaut à :

Tout nombre entier pair supérieur à 3 peut s'écrire comme une somme de deux nombres premiers.

8 Exemple de groupe possédant des formes multiples de l'élément neutre : $(Z_{Fm}, \oplus)$:

(Axiome – E_1) Les éléments générateurs de $(Z_{Fm}, \oplus)$ sont :

$$G_{gen} = \{e_1, e_2, e_3, \bar{e}_1, \bar{e}_2, \bar{e}_3, n_e\} :$$

$$e_i : (1,2), (1,3), (1,5)$$

$$\bar{e}_i : (2,1), (3,1), (5,1)$$

$$n_e : (1,1) \text{ ou } (2,2).$$

$$e_i \oplus \bar{e}_i :$$

$$(1,2) \oplus (2,1) = (3,3) = F(3) = F(K_1)$$

$$(1,3) \oplus (3,1) = (4,4) = F(4) = F(K_2)$$

$$(1,5) \oplus (5,1) = (6,6) = F(6) = F(K_3)$$

(Axiome – L_1) La loi de composition $\oplus$ est telle que $(a,b) \oplus (c,d) = (a+c, b+d)$

avec $a, b, c, d \in \mathbb{N} > 0$, la loi $+$ est l'addition entre ces nombres.

(Axiome – L_2 – Axiome – L_3) La loi de composition $\oplus$ est commutative et associative, propriétés héritées de la loi $+$ entre les nombres naturels.

(Axiome – Ne_1 – Axiome – Ne_2) Pour tout $K \in \mathbb{N} > 0$, Une forme $F(K)$ de l'élément neutre est $F(K) = (K, K)$ ainsi toute forme $F(K)$ correspond à l'élément neutre n_e .

L'élément symétrique doit être défini en même temps que $F(K)$.

(Axiome – Es_1) Pour un élément $e_i = (a, b)$, son symétrique est donc défini comme : $\bar{e}_i = (b, a)$, il est unique et $e_i \oplus \bar{e}_i = (a+b, b+a) = F(a+b)$.

(Axiome – Es_1) De plus les éléments e_i ne doivent pas être symétriques entre-eux, soit : si $e_i = (a, b)$ et $e_j = (c, d)$ alors $e_i \oplus e_j$ ne peut être égal à une forme $F(K)$.

Dans ce cas $(a+c, b+d) \text{ non } = (K, K)$ soit $a-b \neq d-c$. Ce qui est le cas dans notre exemple $(2-1=1, 3-1=2, 5-1=4)$.

Recherche de la valeur K_{n_e} :

1-la valeur K_{n_e} doit être différente des valeurs K_i , soit ici 3, 4 et 6.

2-à chaque composition entre formes : $F(K_i) \oplus F(K_j) = F(K_i + K_j)$, la valeur résultante est croissante.

Aussi la valeur K_{n_e} peut être inférieure à la plus petite des valeurs K_i , soit ici 2 ou 1 (<3).

La forme générateur de n_e peut donc être $F(1) = (1, 1)$, ou $F(2) = (2, 2)$.

On peut aussi montrer que $n_e = (1, 1)$ est générateur car on ne peut avoir de composition $(a, b) \oplus (c, d) = (a + c, b + d) = (1, 1)$ pour $a, b, c, d > 0$.

Des similitudes existent entre $(Z_{Fm}, \oplus)$ et celui des nombres relatifs $\mathbb{Z}(+)$. Ainsi pour un élément (n_1, p_1) de $(Z_{Fm}, \oplus)$, n_1 est alors un nombre négatif, p_1 nombre positif et à (n_1, p_1) correspond dans $\mathbb{Z}(+)$: $-n_1 + p_1$. Les formes $F(1) = F(3) = F(4) = (1, 1) = (3, 3) = (4, 4)$ dans $(Z_{Fm}, \oplus)$ et dans $\mathbb{Z}(+)$: $-1+1=-3+3=-4+4=0$.

9 Exemple : Application au groupe $(G, \otimes)$ pour $2.N=18$:

Ce paragraphe ne sert qu'à illustrer les résultats obtenues sur un groupe particulier : $(G, \otimes)$.

9.1 Liste des $f(e_i)$ et $F_z(K_i)$ pour $(G, \otimes)$:

(le caractère "." qui suit correspond à la multiplication entre entiers)

$$f(n_e) = f((9, 9)) = f((3.3, 3.3)) = (2, 2) \\ F_z(K_{0,e}) = (2, 2)$$

$$f(e_1) = f((8, 10)) = f((2.2.2, 2.5)) = (3, 2) \text{ et } f(\overline{e_1}) = f((10, 8)) = (2, 3) \\ f(e_1) \oplus f(\overline{e_1}) = F_z(5) = (5, 5)$$

$$f(e_2) = f((7, 11)) = (1, 1) \text{ et } f(\overline{e_2}) = f((11, 7)) = (1, 1) \\ f(e_2) \oplus f(\overline{e_2}) = F_z(2) = (2, 2)$$

$$f(e_3) = f((6, 12)) = f((2.3, 2.2.3)) = (2, 3) \text{ et } f(\overline{e_3}) = f((12, 6)) = (3, 2) \\ f(e_3) \oplus f(\overline{e_3}) = F_z(5) = (5, 5)$$

$$f(e_4) = f((5, 13)) = (1, 1) \text{ et } f(\overline{e_4}) = f((13, 5)) = (1, 1) \\ f(e_4) \oplus f(\overline{e_4}) = F_z(2) = (2, 2)$$

$$f(e_5) = f((4, 14)) = f((2.2, 2.7)) = (2, 2) \text{ et } f(\overline{e_5}) = f((14, 4)) = (2, 2) \\ f(e_5) \oplus f(\overline{e_5}) = F_z(4) = (4, 4)$$

$$f(e_6) = f((3, 15)) = f((3, 3.5)) = (1, 2) \text{ et } f(\overline{e_6}) = f((15, 3)) = (2, 1) \\ f(e_6) \oplus f(\overline{e_6}) = F_z(3) = (3, 3)$$

$$f(e_7) = f((2, 16)) = f((2, 2.2.2.2)) = (1, 4) \text{ et } f(\overline{e_7}) = f((16, 2)) = (4, 1) \\ f(e_7) \oplus f(\overline{e_7}) = F_z(5) = (5, 5)$$

9.2 Éléments distincts $e_{i,z}$ de $(Z, \oplus)$ (2.N=18) :

$f(n_e) = (2, 2) = F_z(2)$, élément que l'on garde qu'il soit ou non distinct des autres éléments.

$$e_{1,z} = (3, 2) \text{ et } \overline{e_{1,z}} = (2, 3), e_{1,z} \oplus \overline{e_{1,z}} = F_z(5),$$

$$e_{2,z} = (1, 2) \text{ et } \overline{e_{2,z}} = (2, 1), e_{2,z} \oplus \overline{e_{2,z}} = F_z(3),$$

$$e_{3,z} = (1, 4) \text{ et } \overline{e_{3,z}} = (4, 1), e_{3,z} \oplus \overline{e_{3,z}} = F_z(5),$$

$$e_{4,z} = (1, 1) = F_z(1).$$

(et $(2, 2)$ qui n'est pas générateur car composé avec $(1, 1)$:
 $(2, 2) = (1, 1) \oplus (1, 1)$).

10 Fin du document : le 14 juillet 2026

Table des matières

1	Introduction sur la conjecture de Goldbach et objet du document :	1
2	Résumé de la démonstration :	2
3	Caractéristiques des groupes $(G_{Fm}, \otimes)$ possédant des formes multiples de l'élément neutre n_e :	3
3.1	Proposition :	3
3.1.1	Notations utilisées :	3
3.2	Définition de l'ensemble G_{Fm} :	3
3.2.1	Sous-ensemble G_{gen} , Eléments générateurs :	3
3.2.2	Sous-ensemble G_{comp} , Eléments composés :	4
3.2.3	Ensemble G_{Fm} :	4
3.3	Loi de composition interne $\otimes$:	4
3.4	Elément neutre n_e du groupe $(G_{Fm}, \otimes)$ - Elément symétrique $\overline{e_i}$ de l'élément e_i :	6
4	Caractéristiques des groupes $(G, \otimes)$:	8
4.1	Proposition :	8
4.2	Définition de l'ensemble G :	9
4.2.1	Sous-ensemble G_{gen} , Eléments générateurs :	9
4.2.2	Sous-ensemble G_{comp} , Eléments composés :	11
4.2.3	Ensemble G :	11
4.3	Loi de composition interne $\otimes$:	11
4.4	Elément neutre n_e du groupe $(G, \otimes)$ - Elément symétrique $\overline{e_i}$ de l'élément e_i :	12
5	Caractéristiques du groupe $(Z_R, \oplus)$:	16
5.1	Proposition :	16
5.2	Définition de l'ensemble Z_R :	16
5.2.1	Sous-ensemble Z_{gen} , Eléments générateurs :	16
5.2.2	Sous-ensemble Z_{comp} , Eléments composés :	17
5.2.3	Ensemble Z_R :	17
5.3	Loi de composition interne $\oplus$:	17
5.4	Elément neutre n_z du groupe $(Z_R, \oplus)$ - Elément symétrique $\overline{e_i}$ de l'élément e_i :	18
6	Morphisme de groupe entre $(G, \otimes)$ et $(Z_R, \oplus)$:	20
6.1	Proposition :	20
6.2	Formes multiples de l'élément neutre : $F_z(K_i) = (K_i, K_i)$.	21

7	Fin de la démonstration de la conjecture :	21
7.1	Proposition :	21
7.2	Démonstration que l'image $Im(f) = f(G)$ du morphisme de groupe est un sous-groupe. :	22
7.3	Recherche de l'élément e_p de G tel que $f(e_p) = (1, 1)$:	24
8	Exemple de groupe possédant des formes multiples de l'élé- ment neutre : $(Z_{Fm}, \oplus)$:	26
9	Exemple : Application au groupe $(G, \otimes)$ pour 2.N=18 :	27
9.1	Liste des $f(e_i)$ et $F_z(K_i)$ pour $(G, \otimes)$:	27
9.2	Eléments distincts $e_{i,z}$ de $(Z, \oplus)$ (2.N=18) :	28
10	Fin du document : le 14 juillet 2026	28