



Projet d'Initiation à la Recherche

Nombres premiers jumeaux :

Critique des travaux de
M. Marc WOLF et M. François WOLF

Sujet proposé par M. Pierre Dusart
Réalisé par Mlle COUTURIER Lucie et M. COTTIER Baptiste

Table des matières

1	Introduction	4
2	Théorie approfondie	5
2.1	Nombres premiers jumeaux	5
2.2	Extension aux constellations premières	6
3	15 formules qui relient les nombres premiers	9
3.1	Présentation du document	9
3.2	Critique du document	9
3.2.1	Introduction	9
3.2.2	Partie I : ensemble W et entiers impairs jumeaux	10
3.2.3	Partie II : Fonctions trigonométriques associées à l'ensemble W	13
3.2.4	Partie III : Séquence - Suites arithmétiques	14
3.2.5	Partie IV : Les 3 paramètres qui définissent le nombre de couples de nombres premiers jumeaux	15
3.2.6	Partie V : Détermination des 3 paramètres	16
3.2.7	Partie VI : Infinité des couples de nombres premiers jumeaux	17
3.2.8	Partie VII : Formules reliant les couples de nombres premiers jumeaux	18
3.3	Bilan de la critique	19
4	Application informatique	20
5	Références	22
5.1	Webographie	22
5.2	Bibliographie	22
6	Conclusion	23

1 Introduction

Marc WOLF et François WOLF sont deux frères jumeaux, ingénieurs en informatique (parcours 3IL à Limoges), et docteurs en sciences des matériaux. Ils ne possèdent pas de réelles formation en mathématiques, ce qui ne les empêche pas de s'y adonner depuis plusieurs années. Dans un premier document les frères WOLF s'intéressent à des formules permettant de relier les couples de nombres premiers jumeaux. Dans un second, ils fournissent, ce qu'ils appellent le "*Théorème de la stabilité des nombres premiers composés par référence dynamique*". Autrement dit, une répartition non-aléatoire des nombres impairs composant, impliquant une répartition non-aléatoire des nombres impairs non composés, donc premiers. Nous allons seulement étudier le premier dans le cadre de ce projet.

Les premières preuves probables d'exploitation de nombres premiers datent de plus de 20 000 ans, et proviennent des os d'Ishango. Aujourd'hui encore, les nombres premiers sont exploités, par exemple, dans la cryptographie. Au fil des années, les nombres premiers ont suscité la curiosité des plus grands mathématiciens et scientifiques, tels qu'Euclide, Mersenne ou encore Fermat. Dans *Les Éléments* d'Euclide, une démonstration de l'infini des nombres premiers est faite. La chasse au plus grand nombre premier ne sera donc jamais terminée. Actuellement, le plus grand nombre premier connu est le nombre premier de Mersenne $2^{74207281} - 1$.

La répartition des nombres premiers apporte, elle aussi, son intérêt. Le Théorème des nombres premiers, démontré parallèlement par Hadamard et La Vallée Poussin en 1896, nous dit ceci :

Soit $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x , alors, quand $x \rightarrow \infty$ on a :

$$\pi(x) \sim \frac{x}{\ln(x)}.$$

On va s'intéresser ici à un cas précis de répartition des nombres premiers : le cas des nombres premiers jumeaux.

2 Théorie approfondie

2.1 Nombres premiers jumeaux

Les nombres premiers jumeaux sont les couples de nombres premiers différant de deux unités. Le premier est $(3, 5)$. Excepté le couple $(2, 3)$, c'est le plus petit écart possible pour un couple de nombres premiers.

Il existe une caractérisation des nombres premiers jumeaux. Cette dernière découle du théorème de Wilson, et a été remarquée par P. A. Clément en 1949. Pour tout entier $n > 2$, le couple $(n, n + 2)$ est constitué de nombres premiers jumeaux si et seulement si :

$$4[(n-1)! + 1] + n \equiv 0 \pmod{n(n+2)}$$

En voici une démonstration :

(i) Supposons n et $n + 2$ premiers. Le théorème de Wilson nous donne :

$$(n-1)! + 1 \equiv 0 \pmod{n} \quad (1)$$

$$(n+1)! + 1 \equiv 0 \pmod{n+2} \quad (2)$$

$$\text{Or } (n+1)! = n(n+1) \times (n-1)! = (n^2 + n) \times (n-1)!$$

$$\text{De plus : } (n^2 + n) = n(n+2) - n \equiv -n \equiv 2 \pmod{n+2}$$

Finalement, (2) peut s'écrire $2[(n-1)!] + 1 \equiv 0 \pmod{n+2}$ d'où :

$$2[(n-1)!] + 1 = k(n+2), k \in \mathbb{Z} \quad (3)$$

En multipliant par 2 l'équation (1), on a :

$$2[(n-1)!] + 1 \equiv k(n+2) + 1 \equiv 2k + 2n + 1 \equiv 2k + 1 \equiv 0 \pmod{n} \text{ d'où :}$$

$$2k + 1 = pn, p \in \mathbb{Z}.$$

En multipliant par 2 l'équation (3) on a :

$$4[(n-1)!] + 2 = 2k(n+2) = (2k+1)(n+2) - (n+2) = pn(n+2) - (n+2) \Leftrightarrow$$

$$4[(n-1)!] + 2 + (n+2) = 2k(n+2) \Leftrightarrow 4[(n-1)! + 1] + n = pn(n+2). \text{ Ainsi, on a :}$$

$$4[(n-1)! + 1] + n \equiv 0 \pmod{n(n+2)}$$

(ii) Supposons qu'on ait $4[(n-1)! + 1] + n \equiv 0 \pmod{n(n+2)} \quad (1).$

$$\text{On a : } (1) \Leftrightarrow \begin{cases} 4[(n-1)! + 1] + n \equiv 0 \pmod{n} & (2) \\ 4[(n-1)! + 1] + n \equiv 0 \pmod{n+2} & (3) \end{cases}$$

$$(2) \Leftrightarrow 4[(n-1)! + 1] \equiv 0 \pmod{n} \Leftrightarrow [(n-1)! + 1] \equiv 0 \pmod{n}.$$

Ainsi, d'après le théorème de Wilson, n est premier. Ensuite, on a :

$$(3) \Leftrightarrow 4[(n-1)! + 1] \equiv 2 \pmod{n+2} \Leftrightarrow 4[(n-1)!] \equiv -2 \pmod{n+2}$$

$$\text{De plus on a } n(n+1) \equiv -n \equiv 2 \pmod{n+2} \quad \text{D'où } 4[(n+1)!] \equiv -4 \pmod{n+2}$$

$$\text{Ce qui s'écrit aussi } 4[(n+1)! + 1] \equiv 0 \pmod{n+2}$$

Finalement, on a $(n+1)! + 1 \equiv 0 \pmod{n+2}$ ce qui d'après le théorème de Wilson implique que $n+2$ est premier.

Ainsi n et $n + 2$ forment bien un couple de nombres premiers jumeaux.

Contrairement au cas des nombres premiers, il n'existe aucune démonstration de l'infinité des nombres premiers jumeaux, mais les mathématiciens sont convaincus de leur infinité. Une conjecture — la conjecture de Dubner — stipule que tout nombre pair supérieur à 4208 s'écrit comme étant somme de deux nombres premiers ayant chacun un jumeau. Cette conjecture, proche de celle de Goldbach, a été vérifiée pour tous les nombres pairs jusqu'à 4×10^{11} . Si cette conjecture est démontrée, cela impliquerait effectivement qu'il y a une infinité de couples de nombres premiers jumeaux.

Actuellement, le couple de nombres premiers jumeaux record est $2\,996\,863\,034\,895 \times 2^{1\,290\,000} \pm 1$. Chacun de ces nombre s'écrit avec 388 342 chiffres.

Comme énoncé précédemment, l'infinité des couples de nombres premiers jumeaux n'est qu'une conjecture, qui constitue un des "huitième" problème de Hilbert, ainsi qu'un des 4 problèmes de Landau. Cette conjecture se généralise sous le nom de première conjecture de Hardy-Littlewood, qui s'énonce ainsi : Soit $\pi_2(x)$ le nombre de couples de nombres premiers jumeaux de la forme $(p, p+2)$ avec $p < x$, alors on a :

$$\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\ln t)^2}$$

avec :

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.66016316$$

C_2 est appelée constante des nombres premiers jumeaux et on a $C_2 \approx 0.66016$.

Cette constante ne doit pas être confondue avec la constante de Brun qui annonce que la série suivante est convergente ou finie :

$$\sum_{p \in \mathbb{P}_2} \left(\frac{1}{p} + \frac{1}{p+2} \right) = \left(\frac{1}{3} + \frac{1}{5} \right) + \left(\frac{1}{5} + \frac{1}{7} \right) + \left(\frac{1}{11} + \frac{1}{13} \right) + \dots \approx 1.9022$$

où $\mathbb{P}_2 = \{p \in \mathbb{N}, p \text{ et } p+2 \text{ premiers}\}$.

Le nombre expérimental de couples de nombres premiers jumeaux inférieurs à 10^8 est 440312 tandis que la conjecture de Hardy-Littlewood donne une approximation de 440368 couples.

2.2 Extension aux constellations premières

Définition : une constellation, ou k-uplet premier, est un k-uplet de nombres, de telle sorte que la différence entre le premier et le dernier nombre de ce k-uplet est, dans un certain sens, le plus petit réalisable. Plus précisément, un k-uplet premier est une suite de nombres premiers (p_1, p_2, \dots, p_k) où $p_k - p_1 = s(k)$ est le plus petit nombre s pour lequel il existe k entiers $b_1 < b_2 < \dots < b_k$ avec $b_k - b_1 = s$, et pour tout nombre premier p , tous les restes modulo p ne sont pas représentés par l'un des b_i , $i \in \llbracket 1, k \rrbracket$

Exemples : (97, 101, 103, 107, 109) est une constellation :

97, 101, 103, 107, 109 sont 5 nombres premiers consécutifs et pour tout p premier, ce 5-uplet ne contient pas tous les restes possibles modulo p . (il faudrait au maximum $p = 5$ pour qu'il y ait au plus 5 restes différents, mais pour $p = 3$ ou $p = 5$, aucune de ces nombres ne vaut 0 modulo p . C'est donc bien une constellation.

A contrario, le 5-uplet (3, 5, 7, 11, 13) est bien constitué de 5 nombres premiers consécutifs, mais pour $p = 3$, $(3, 5, 7, 11, 13) = (0, 2, 1, 2, 1) \pmod{p}$. Ainsi, tous les restes possibles modulo 3 sont présents. Ce n'est donc pas une constellation.

Ainsi, en prenant $s(2) = 2$, on obtient les 2-uplets (i.e. couples) premiers de la forme $(p, p+2)$, ce qui correspond aux couples de nombres premiers jumeaux. De même :

$s(2) = 4$ correspond aux couples premiers de la forme $(p, p+4)$; ce sont les nombres premiers cousins. Avec $s(2) = 6$, on obtient les nombres premiers sexy. On notera que $s(k)$ est toujours pair.

Excepté le triplet (3, 5, 7), où $s(3) = 4$, tous les autres triplets premiers ont $s(3) = 6n$. Pour $n = 1$, on a deux familles de constellations possibles : $(p, p+2, p+6)$ et $(p, p+4, p+6)$. Pour $n = 2$, les constellations sont de la forme $(p, p+6, p+12)$.

En 1938, Hardy et Wright ont émis la conjecture qu'il existait une infinité de constellations de la forme $(p, p+2)$, $(p, p+2, p+6)$ et $(p, p+4, p+6)$. Cette conjecture demeure indémontrée, mais est acceptée.

C'est ce même Hardy, Godfrey de son prénom, qui est à la base de la conjecture de Hardy-Littlewood vue précédemment. Cette conjecture s'étant à de nombreuses autres constellations. Soit C une constellation, on appelle $P_x(C)$ le nombre de constellations C avec $p < x$ où p est le premier élément de la constellation.

On a :

$$P_x(p, p+4) \sim 2 \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dt}{(\ln t)^2}$$

$$P_x(p, p+6) \sim 4 \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \int_2^x \frac{dt}{(\ln t)^2}$$

$$P_x(p, p+2, p+6) \sim \frac{9}{2} \prod_{p \geq 3} \frac{p^2(p-3)}{(p-1)^2} \int_2^x \frac{dt}{(\ln t)^3}$$

$$P_x(p, p+4, p+6) \sim \frac{9}{2} \prod_{p \geq 3} \frac{p^2(p-3)}{(p-1)^2} \int_2^x \frac{dt}{(\ln t)^3}$$

Toutes ces équivalences ne sont que des conjectures, mais on peut remarquer que l'estimation du nombre de couples premiers jumeaux est équivalente à l'estimation du nombre de couples premiers cousins.

Nombre de constellations premières $\leq 10^8$			
Constellation	Découvertes	Approximation	Record
$(p, p+2)$	440312	440368	$2\,996\,863\,034\,895 \times 2^{1\,290\,000} \pm 1$
$(p, p+4)$	440258	440368	(p_r, p_r+4)
$(p, p+2, p+6)$	55600	55491	$3221449497221499 \times 34567 + d, d \in \{-1, 1, 5\}$
$(p, p+4, p+6)$	55556	55491	$6521953289619 \times 255555 + d, d \in \{-5, -1, 1\}$

$p_r = 311778476 \times 587502 \times 9001\# \times (587502 \times 9001\# + 1) + 210) \times (587502 \times 9001\# - 1)/35 + 1$
où $9001\#$ est la primorielle de 9001 On constate que la théorie est très proche de la pratique

3 15 formules qui relient les nombres premiers

3.1 Présentation du document

Ce document présente 15 formules permettant de relier les nombres premiers. Autrement dit, après avoir mis au point une description de la structure des nombres impairs, les frères WOLF en ont déduit 15 formules reliant tous les couples de nombres premiers à l'exception des couples (3, 5) et (5, 7). Malheureusement, ces formules ne permettent pas une caractérisation des nombres premiers jumeaux.

Ce document est composé d'une introduction suivie de 8 parties, que nous allons étudier et critiquer, de façon aussi constructive que possible. La nouvelle théorie sera présentée dans les 3 premières parties. La quatrième partie montrera que le calcul du nombre de couples de nombres premiers jumeaux s'effectue à l'aide de 3 formules, qui seront étudiées et déterminées dans la cinquième partie. Une nouvelle conjecture sur les couples de nombres premiers jumeaux sera mis en avant dans l'antépénultième partie. La septième partie sera l'aboutissement aux 15 formules. Une dernière partie démontrera l'infinité des couples de nombres premiers jumeaux virtuels.

3.2 Critique du document

3.2.1 Introduction

La première remarque est l'absence de présentation du travail réalisé par la suite. Il n'est jamais expliqué ce qu'est un couple de nombres premiers jumeaux. Une présentation historique des connaissances déjà acquises à ce sujet aurait été appréciable afin de savoir d'où on part, pour comprendre où l'on va, ainsi que l'apport mathématique concret de ces 15 nouvelles formules.

Dans la définition littéraire des paramètres, $A1$ est exprimé en fonction de p , mais on ne le retrouve pas dans la définition mathématique. La définition suivante n'est pas la même que celle présentée dans leur document, mais est plus cohérente avec l'utilisation faite par la suite :

$$A1(p) := \#\{(6m-1, 6m+1), m \in \mathbb{N}^*, 6m-1 < p\}$$

On note qu'il n'est pas nécessaire de définir l'ensemble I puisque les nombres de la forme $6m \pm 1$ sont forcément impairs.

Une remarque similaire est valable pour $B1(p)$ et $C1(p)$, que l'on pourrait remplacer par :

$$O := \{n = 6m \pm 1, m \in \mathbb{N}^*, n \text{ non premier}\}$$

$$B1(p) := \#\{n \in O, n < p\}$$

$$C1(p) := \#\{(n, n+2) \in O^2, n < p\}.$$

L'introduction est essentiellement constitué d'une réécriture du sommaire. Comme dit plus haut, il aurait été préférable d'y développer l'aspect historique et contributif de ce document. Les motivations ayant conduit les frères WOLF à travailler sur ce sujet aurait aussi eu sa place dans cette introduction.

3.2.2 Partie I : ensemble W et entiers impairs jumeaux

La définition de l'ensemble C se fait en trois points. Cela aurait pu être fait de façon plus concise, en écrivant simplement :

$$C := \{n = 2k + 3, k \in \mathbb{N} \mid \exists m \in \mathbb{N}, m \wedge n \neq 1\}$$

Pour la définition 4, il existe une notation mathématique propre à ce genre d'intervalles. Ce que les frères WOLF notent $[1, 3]$ correspond à ce qui est communément noté $\llbracket 1, 3 \rrbracket$ en mathématiques

Dans la propriété 1, des informations sont redondantes. P a déjà été défini quelques lignes plus haut, comme étant l'ensemble des nombres premiers, il n'est pas nécessaire de le redéfinir. N'écrire que :

Soit $p \in \mathbb{N}$, $p \in W \Leftrightarrow N_k = 2k + 3 \notin P$ est suffisant. D'un point de vue plus rigoureux, cette propriété n'apporte rien. Dans l'introduction, W a été défini comme étant l'ensemble regroupant les indices de nombres impaires composés, i.e., non premier. De plus, la définition donnée de W dans la **définition 1.2.1** n'est pas intuitive. Ainsi, peut-être aurait-il été plus cohérent de ne pas écrire la définition 1.2.1, et d'écrire une propriété montrant que tout élément de W peut s'écrire sous la forme $(2j + 3)n + j$ avec $j \in \mathbb{N}, n \in \mathbb{N}^*$. De plus, la démonstration serait la même à celle fournie ici. Dans la démonstration, la phrase "La multiplication de deux nombres impairs génère toujours un nombre impair. Donc un nombre composé impair se décompose en deux nombres impairs." est litigieuse. La multiplication d'un nombre pair et d'un nombre impair génère toujours un nombre pair. Ce n'est pas pour autant qu'un nombre composé pair se décompose en un nombre pair et un nombre impair. L'emploi du "donc" est à remettre en cause. De plus, l'apport de cette phrase est facultative étant donnée la phrase précédente qui dit la même chose. Dans la phrase suivante, il est dit que 3 est le plus petit facteur d'un nombre impair. Il serait bon de préciser que c'est le plus petit facteur possible d'un nombre impair.

De façon générale dans la démonstration, il faut faire attention à l'usage du "donc". C'est un connecteur logique, et il est parfois difficile d'y voir la logique.

Pour établir la **propriété 2**, prendre la contraposée d'une équivalence n'a pas de sens. La contraposée est propre à l'équivalence. Ici, il s'agit plutôt de la négation de la **propriété 1**. Ainsi :

$$\neg(p \in W) \Leftrightarrow \neg(N_k = 2k + 3 \notin P), \text{ i.e. :}$$

$$p \in M \Leftrightarrow N_k = 2k + 3 \in P$$

Pour la représentation dans un repère des ensembles W_j , il y a un problème de formulation. Les ensembles W_j ne sont pas représentés par des points, mais par les ordonnées de ces points. Une formulation plus appropriée serait :

W_j est représenté par l'ensemble des images non nulles des entiers naturels par la fonction $k_j(n)$, $n \in \mathbb{N}$

Problème de notation. Si j'écris $k_2(3)$, est-ce que ça vaut $5 \times 3 + 6 = 21$ ou bien $7 \times 3 + 2 = 23$. On a donc 2 images possibles pour $k_2(3)$. En remplaçant k par k' dans la section 1.3.3 cela règle le problème.

Pour montrer que $W_k = W'_k + 1$, il suffit de montrer que tout élément s'écrivant $(2j + 3)n + j$ peut aussi s'écrire $(2j' + 1)n' + 3j'$.

En posant $k = n - 1$ on a :

$$(2j + 3)n + j = (2j + 3)(k + 1) + j = (2(j + 1) + 1)k + 3(j + 1) = (2j' + 1)k + 3j'$$

L'égalité étant une relation d'équivalence, il n'est pas nécessaire de montrer la réciproque.

La **propriété 4** dit :

la raison de W_j est $2j + 3$.

Cette phrase n'a pas de sens car un ensemble n'a pas de raison. Il serait alors préférable de prendre une notation de suite pour W_j , ou de formuler la phrase ainsi :

La raison de la suite générant les éléments de, ou associée à W_j est $2j + 3$.

Pourquoi renommer la raison qu'on a défini dans la définition 1.3.3.2? Autant la nommer "période" dès ce moment là, ou alors, garder l'appellation "raison" pour la suite du document.

Pour la **propriété 5** l'écriture $W_j \subset \bigcup_{r=0}^{j-1} W_r$ ne retranscrit pas ce qui est dit littéralement. Ici, les certains éléments de W_j pourrait se retrouver dans certains des W_r , sans que tous y soit dans un seul. Un contre exemple :

$$\{1, 2\} \subset \{1, 3, 5\} \cup \{2, 4\} \text{ alors que } \{1, 2\} \not\subset \{1, 3, 5\} \text{ et } \{1, 2\} \not\subset \{2, 4\}.$$

Une reformulation correcte serait :

$\exists r < j$ tel que $W_j \subset W_r$.

Pour la démonstration, on aurait pu reprendre la propriété citée au paragraphe 1.3.1. – cela aurait été pratique aussi de numéroté toutes les propriétés –. Ainsi, si $2j + 3 = (2r + 3)(2n + 1)$, les multiples de $2j + 3$ sont aussi multiples de $2r + 3$, donc tout élément de W_j est élément de W_r , i.e. $W_j \subset W_r$.

Pour introduire la notion de nombre remarquable de W_j , montrer d'abord que $k_j(j + 1)$ est un carré, et ensuite appelé ce nombre "nombre remarquable" aurait été plus élégant. En effet, le fait que ce soit un carré n'a pas été observée après l'avoir appelé ainsi. Il a plutôt été appelé ainsi parce que c'est un carré.

Dans la **définition 1.4.3**, au delà la faute de frappe (des crochets utilisés pour la notation de partie entière), il est possible d'alléger la formule car on a :

$$\left\lfloor \frac{\lfloor \sqrt{N_j} \rfloor - 3}{2} \right\rfloor = \left\lfloor \frac{\sqrt{N_j} - 3}{2} \right\rfloor$$

La démonstration de la **propriété 7** est un peu précipitée. Certes, elle repose essentiellement sur la **propriété 2**, mais il y a d'autres argument à ajouter. Notamment, pourquoi a-t-on :

$$p \notin \bigcup_{j=0}^{j_{\max}(N_p)} W_j \Rightarrow p \in M$$

Dans le point 2 de la **définition 1.4.4**, il est évident que $4j + 7$ est impair. Or, $\forall j \in \mathbb{N}$, $k_{GW}(j)$ est impair, et la différence de deux impairs donne toujours un nombre pair. Calculons $|k_{GW}(j + 1) - k_{GW}(j)|$:

$$|2(j + 1)^2 + 6(j + 1) + 3 - (2j^2 + 6j + 3)| = |2j^2 + 4j + 2 + 6j + 6 + 3 - 2j^2 - 6j - 3| = 4j + 8$$

Il y a donc bien une erreur dans la définition de la distance. Cependant, la longueur de l'intervalle est bien $4j + 7$ car $[k_{gw}(j), k_{gw}(j + 1)[= [k_{gw}(j), k_{gw}(j + 1) - 1]$.

De plus, en lisant le point 3, on définit l'unité de base $Ugw(j)$ comme étant la distance entre deux nombres remarquables, et ce coup ci, c'est bien la valeur $4j + 8$ qui est "attribuée". Il y a donc globalement un problème de vocabulaire.

Une dernière remarque est l'apparition du C_j . Est-ce une nouvelle notation ? Si oui, pourquoi avoir introduit $Ugw(j)$?

Quant au point 4, on dit que les intervalles de base forment une *partition* de $\mathbb{N} \setminus \{0, 1, 2\}$

Par conséquent, les valeurs du tableau sont donc erronées. Une solution envisageable serait définir d_j ainsi : $d_j = d(|k_{GW}(j + 1); k_{GW}(j)|) = |k_{GW}(j + 1) - k_{GW}(j)| - 1$

Cela donnerait bien $4j + 7$ comme valeur, mais cette définition de la distance ne vérifie pas l'inégalité triangulaire. Ce n'est donc pas une distance.

Étudions à présent la **propriété 8**. Dans l'énoncé de la propriété, il serait bon de préciser dans quel ensemble est pris m . S'il est pris dans \mathbb{Q} , la propriété devient fausse.

La démonstration n'est pas fausse, mais le fait que " $j^2 + 1$ n'est pas divisible par 3" mériterait d'être développé. De plus, une démonstration plus rapide est possible : $k_{gw}(j) \equiv 2j^2 + 6j + 3 \equiv 2j^2 \pmod{3}$

$$3m + 1 \equiv 1 \pmod{3}$$

$$\begin{cases} j \equiv 0 \pmod{3} \\ j \equiv 1 \pmod{3} \\ j \equiv 2 \pmod{3} \end{cases} \Rightarrow \begin{cases} j^2 \equiv 0 \pmod{3} \\ j^2 \equiv 1 \pmod{3} \\ j^2 \equiv 1 \pmod{3} \end{cases} \Rightarrow \begin{cases} 2j^2 \equiv 0 \pmod{3} \\ 2j^2 \equiv 2 \pmod{3} \\ 2j^2 \equiv 2 \pmod{3} \end{cases}$$

Ainsi, $\forall j \in \mathbb{N}, 2j^2 \not\equiv 1 \pmod{3} \Rightarrow k_{GW}(j) \neq 3m + 1, \forall m \in \mathbb{N}$

3.2.3 Partie II : Fonctions trigonométriques associées à l'ensemble W

La pertinence du **paragraphe II.1** est discutable. Ce n'est qu'une reformulation de la **propriété 7**.

La numérotation des propriétés passe de 8 à 11. Il faut penser à rectifier cela. De plus, la **propriété 11** reprend ce qui est dit dans la remarque de la **définition 2.2.1**, mais de façon falsifiée. Il n'y a pas équivalence entre f_j s'annule en x et $x \in W_j$. On a simplement le fait que $x \in W_j \Rightarrow f_j(x) = 0$. Pour avoir l'équivalence, il faut se limiter aux cas $x > 0$. Cela se retrouve dès la première phrase de l'introduction.

Supposer que $f_j(x) = 0$ n'implique pas qu'il existe un entier naturel $k > 0$ tel que $x = \pi k$, mais qu'il existe un entier RELATIF tel que $x = \pi k$. Un contre-exemple : Posons $x = -\pi$; $f(x) = 0$, mais $\forall k \in \mathbb{N}, \pi k \neq -\pi$. Par conséquent, la démonstration est erronée. Cependant, la démonstration de la réciproque reste vraie et est à conserver.

En supposant $x > 0$, il n'y a rien à dire sur la **propriété 12**.

Il aurait bien dans cette partie de savoir quelles vont être les utilités de ce résultat, et pourquoi elles ont été introduites à cet instant.

3.2.4 Partie III : Séquence - Suites arithmétiques

En réécrivant la **définition 3.1** on a qu'une séquence j est tous les éléments de la forme $j + (2j + 3)n, n \in \mathbb{N} = W_j$. En réalité, on ne fait que redéfinir l'ensemble W_j . On aurait pu simplement faire une remarque mettant en avant que W_j pouvait se définir comme étant les termes d'une suite arithmétique $(k_j)_{n \in \mathbb{N}}$ de premier terme j et de raison $2j + 3$. Cela aurait évité l'introduction de la notion de "séquence" et ce qui est appelé "séquence j " peut être remplacé par "suite k_j ".

La notion de combinaison est d'abord définie, puis des exemples sont donnés, puis redéfinie.

La première définition est peu claire. Déjà, l'écriture $A = b + x, x \in \mathbb{Z}$ n'a pas de sens. De plus, à aucun moment il n'est précisé que le critère dont on parle est x . Une définition plus rigoureuse serait :

"On définit une combinaison de critère $z \in \mathbb{Z}$ entre 2 séquences A et B de points distinctes l'ensemble suivant : $\{(a, b) \in A \times B / a = b + z\}$

Ensuite, prendre trois exemples est un peu trop généreux. Deux, voire un seul avec le détail de la résolution de l'équation diophantienne aurait suffi.

Dans le paragraphe suivant les exemple, il est dit que $r = r_0 * r_1$. Qui sont r_0 et r_1 ? Cela est précisé plus tard, mais il faudrait introduire ces valeurs avant de les utiliser.

"Le nombre de combinaisons distinctes est lié aux nombres d'éléments, de chaque ensemble, présents dans un intervalle de longueur égal au produit des raisons des 2 suites arithmétiques moins 1". Comment le savez-vous? D'où sort ce résultat? Pourquoi cet intervalle précis?

3.2.5 Partie IV : Les 3 paramètres qui définissent le nombre de couples de nombres premiers jumeaux

Cette partie définit les 3 paramètres $A1$, $B1$ et $C1$ présentés en introduction ainsi que la formule qui les lie pour calculer le nombre de couples de nombres premiers jumeaux.

La première chose que l'on remarque c'est que les ensembles dont ils sont les cardinaux ne sont plus nommés de la même façon qu'en introduction et qu'ils ne sont plus définis explicitement comme fonction de p . Nous noterons de plus l'apparition d'un 4ème paramètre.

La **propriété 1.1** est là pour justifier la formule $\pi' = 2 \times A1 - B1$ qui apparaît pourtant en fin de démonstration de la propriété.

La formule $\pi 2' = A1 - B1 + C1$ calculant le nombre de couple de nombre premier jumeaux se déduit effectivement aisément des arguments définis précédemment cependant le cheminement décrit manque de connecteurs logiques liant les égalités données.

3.2.6 Partie V : Détermination des 3 paramètres

Alors que jusqu'ici les indices des nombres étaient donnés en fonction de n , ils apparaissent ici en fonction de m . Cela ne change rien mathématiquement cependant la compréhension en est troublée.

- *Le paramètre A1* : **La propriété 2.1** nous donne la formule pour calculer $A1(p) :=$ le nombre de couple de nombres impaires de la forme $(6m - 1; 6m + 1)$ dans l'intervalle $[0; Np]$ où $Np = 2p + 3$.

Cependant la démonstration tiens plus du tâtonnement. Nous pouvons la réécrire ainsi : Rechercher le nombre de couples $(6m - 1; 6m + 1)$ dans l'intervalle $[0; Np]$ revient à chercher le nombre de couple d'indice $(3n + 1; 3n + 2)$ dans l'intervalle $[0; p]$. Pour se faire il suffit de calculer combien de nombres s'écrivent sous la forme $3n + 2$ dans cet intervalle.

$\#[0; p] = p + 1$. De plus on sait qu'un nombre sur trois s'écrit sous cette forme. D'où :

$$A1(p) = \left\lfloor \frac{p+1}{3} \right\rfloor \text{ étant donné que } A1(p) \in \mathbb{N}$$

Le reste du paragraphe consiste en une étude de $A1(j)$, nous ne nous attarderons pas dessus.

- *Le paramètre B1* : Dès le début de ce paragraphe on remarque une énorme erreur. En effet, on nous dit que "Les nombres premiers ne font pas partie de cet ensemble "(i.e. W_j). Or $W_j = \{(2j+3)n+j, j \in \mathbb{N}, n \in \mathbb{N}^*\}$, on a donc $W_1 = \{6, 11, \dots\}$ et 11 est premier. Peut-être est-ce un problème de compréhension de notre part, mais cela impliquerait une mauvaise rédaction de la part des frères WOLF. De plus, W_j est mal défini. Une définition exacte est celle donnée en **Définition 3.1**.

On aimerait penser que ce n'est qu'une erreur sans importance, or vient ensuite la **propriété 3.1** qui repose sur un changement de variable qui n'apporte rien et une démonstration bancal : Pourquoi est-ce que $B1(j) = n$? En regardant l'exemple associé on lit alors « La séquence W_j correspond aux multiples du nombre premier 5. Or on vient de calculer les premiers nombres de cette séquence et on n'y voit aucun multiple de 5. Suite à cela, il n'a pas été jugé nécessaire d'analyser la suite de ce chapitre étant donné que l'ensemble $B1(j)$ et $C1(j)$ dépendent de W . Même s'il en ressort qu'un travail important y a été réalisé malgré des notations parfois incohérentes ou maladroites.

Cela remet en question toute la suite du dossier puisque le dénombrement ne repose plus sur des définitions stables. Dans la démonstration de la **propriété 3-4**, il est incorrect d'écrire :

$$\lim_{j \rightarrow \infty} B1(j) = 2a_b j^2 + 10a_b j + 8 - \pi'$$

Une limite ne peut s'écrire en fonction de la variable que l'on fait tendre vers la limite. L'écriture exacte serait donc :

$$\lim_{j \rightarrow \infty} B1(j) = \lim_{j \rightarrow \infty} 2a_b j^2 + 10a_b j + 8 - \pi'(j)$$

De plus, d'après la **propriété 2-3** l'écriture $B1 = A2 - \pi'$ n'est que conditionnelle. Elle n'est valable que "lorsque la valeur de j est égale à un multiple du PGCD($p+1; 3$)" La validité de la démonstration est donc à remettre en cause.

3.2.7 Partie VI : Infinité des couples de nombres premiers jumeaux

Reprenons la conjecture de Hardy-Littlewood pour le cas des nombres premiers jumeaux. Elle stipule ceci :

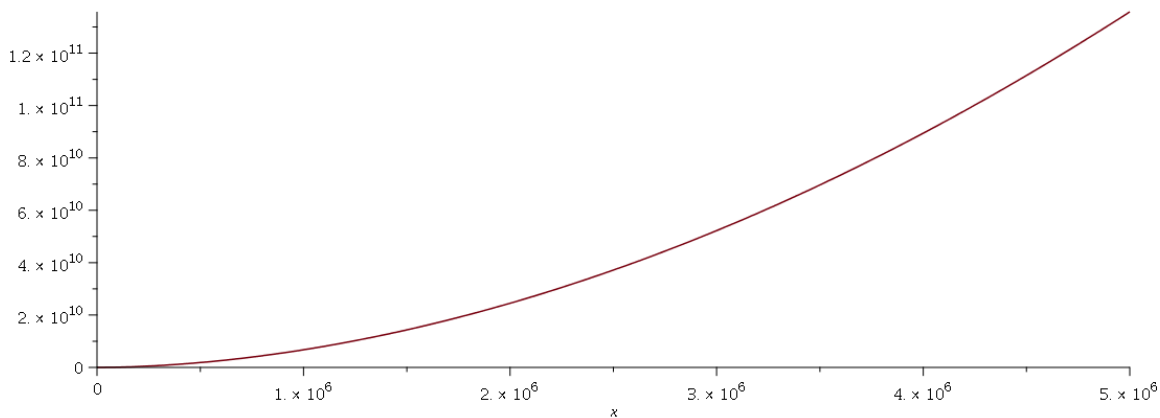
$$\pi_2(x) \sim 2C_2 \int_2^x \frac{dt}{(\ln t)^2}$$

avec :

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.66016316$$

Grâce au logiciel Maple, on sait que $\pi'_2(100000000000001) \approx 1.3578 \times 10^{11}$. Ce qui correspond visuellement au graphique donné. Bien évidemment, cela ne le confirme pas pour autant. Mais une incohérence l'aurait infirmé.

Observons à présent la courbe représentative de $\pi_2(j = 4x^2 + 20x + 25)$ pour $x \in [0, 5000170]$



Représentation graphique de $\pi(j)$

La courbe est fortement similaire à celle obtenue par les frères WOLF. On peut donc supposer que leur travail est correct. Cela dit, étant donné l'échelle du graphique, une petite erreur ne serait pas visible à l'œil nu.

Quant à la conjecture qui suit, elle semble intéressante. En effet, si elle vient à être démontrée, cela prouverait l'infinité des couples de nombres premiers jumeaux. Cela dit, la conjecture des frères WOLF repose sur la conjecture de Legendre, qui, par définition n'a pas été démontrée, alors que dans leur écrit, ils la considèrent démontrée : "*La conjecture de Legendre nous indique que le nombre de nombres premiers $\pi'(N_p) = \pi(N_p) - 2$ est aussi une fonction strictement croissante en fonction de j* "

3.2.8 Partie VII : Formules reliant les couples de nombres premiers jumeaux

Après avoir étudié le résultat de ce chapitre, on s'est rendu compte que le travail réalisé revenait à écrire un nombre n sous la forme $n = 210q + k$, $k \in \llbracket 0, 209 \rrbracket$ et à ne garder que les k tels que $\text{PGCD}(k, 210) \times \text{PGCD}(k+2, 210) = 1$ car cela implique que chacun des PGCD vaille 1, donc, que k et $k+2$ soient premiers avec 210. Les valeurs ne respectant pas ce critère, ne sont pas premières avec 210, donc n ne peut forcément pas être premier.

Ainsi, les seules possibilités pour que le couple $(n, n+2)$ soit un couple de nombres premiers jumeaux sont :

Valeur possible de n		
$210q + 11$	$210q + 71$	$210q + 167$
$210q + 17$	$210q + 101$	$210q + 179$
$210q + 29$	$210q + 107$	$210q + 191$
$210q + 41$	$210q + 137$	$210q + 197$
$210q + 59$	$210q + 149$	$210q + 209$

Ce qui coïncide parfaitement avec les résultats des frères WOLF.

De même, on peut procéder ainsi pour déterminer de "nouvelles" formules. Voici le nombre C_n de formules obtenues en considérant la division euclidienne par le produit des n premiers nombres premiers :

n	C_n
4	15
5	135
6	1485
7	22275
8	378675

La suite C_i est référencée dans l'encyclopédie en ligne des suites entières sous le nom A059861. Elle se définit ainsi :

$$C_n = \prod_{i=2}^n (\pi_i - 2)$$

où π_i est le i -ème nombre premier.

La méthode présentée ici est facilement extensible à de plus grandes valeurs de n .

3.3 Bilan de la critique

Le fond, tout comme la forme du travail réalisé par les frères WOLF témoigne d'un manque d'expérience mathématique. Ce qui est compréhensible étant donné que ce n'est pas leur domaine de prédilection.

Sur le fond, ce dossier n'apporte rien de nouveau. Comme on l'a vu précédemment, leur "nouvelle" conjecture est dépendante de la conjecture de Legendre ; et leurs 15 formules reliant les couples de nombres premiers jumeaux sont des formules facilement retrouvables. En effet, elles ne sont pas clairement écrites dans des livres ou sur internet, mais uniquement parce que leur apport mathématique est inexistant. En guise de métaphore, à prendre au sens humoristique, c'est comme faire Limoges—Clermont-Ferrand en passant par Lille, Strasbourg, Marseille et Les Sables d'Olonne. Le point d'arrivée est le bon, mais le trajet pris n'est pas optimal. De plus, plusieurs démonstrations sont maladroites, voire incorrectes, ce qui rend instable l'établissement des résultats.

Sur le plan de la rédaction, il faut se le dire, c'est très difficile à lire et à assimiler. On se perd facilement dans les notations, dans les formules. Certains paramètres sont définis trop tôt, d'autres sont définis plusieurs fois de façons différentes. Il serait appréciable de faire une page récapitulative. De plus, il est courant que les articles mathématiques soient rédigés en \LaTeX pour des raisons de confort de lecture et d'organisation du-dit article, ce qui aurait été apprécié pour ce dernier. Cela aurait évité des erreurs de mises en formes. Une dernière remarque est sur l'apparition subite d'une phrase en anglais. À la **page 39**, on peut lire : *The pairs of composite numbers $(6q - 1, 6q + 1)$ are multiple of pairs of prime numbers $(P1, P2)$* . On est en droit de se demander si une relecture rigoureuse a été réalisée avant la remise de l'article.

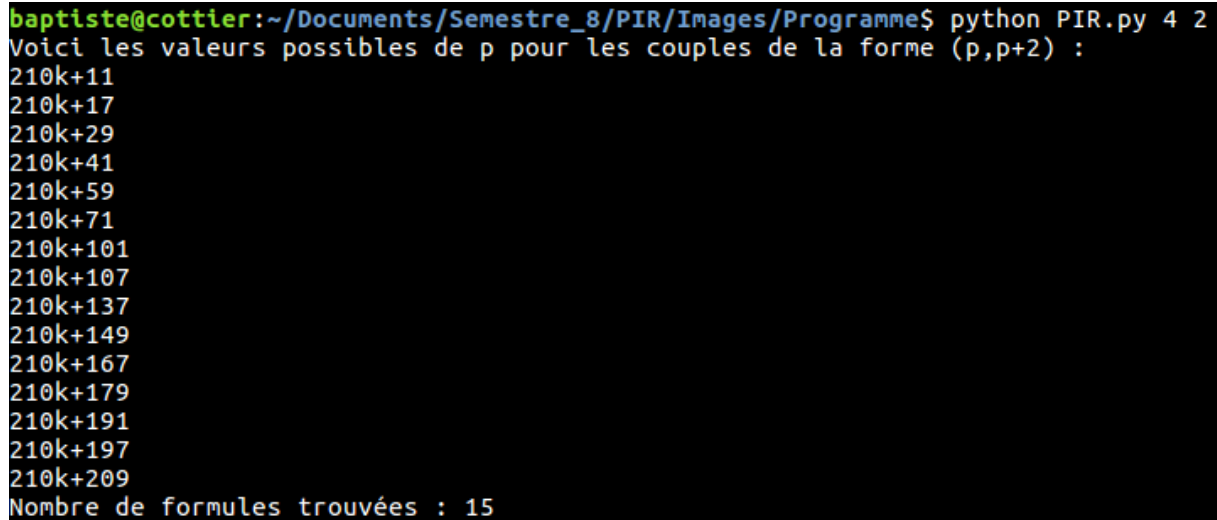
4 Application informatique

Après avoir trouvé la démonstration précédente, il est devenu simple de créer un programme permettant de retrouver ces résultats. Ce dernier a été réalisé dans le langage Python. Ce programme – disponible sous le nom `PIR.py` dans l'archive – permet de lister l'ensemble des valeurs possibles de p pour les couples de la forme $(p, p+k)$, où k est le deuxième argument de la fonction. Le premier argument détermine le nombre de nombres premiers à considérer.

– Exemple sur les nombres premiers jumeaux –

On exécute la ligne de commande suivante :

```
$python PIR.py 4 2
```



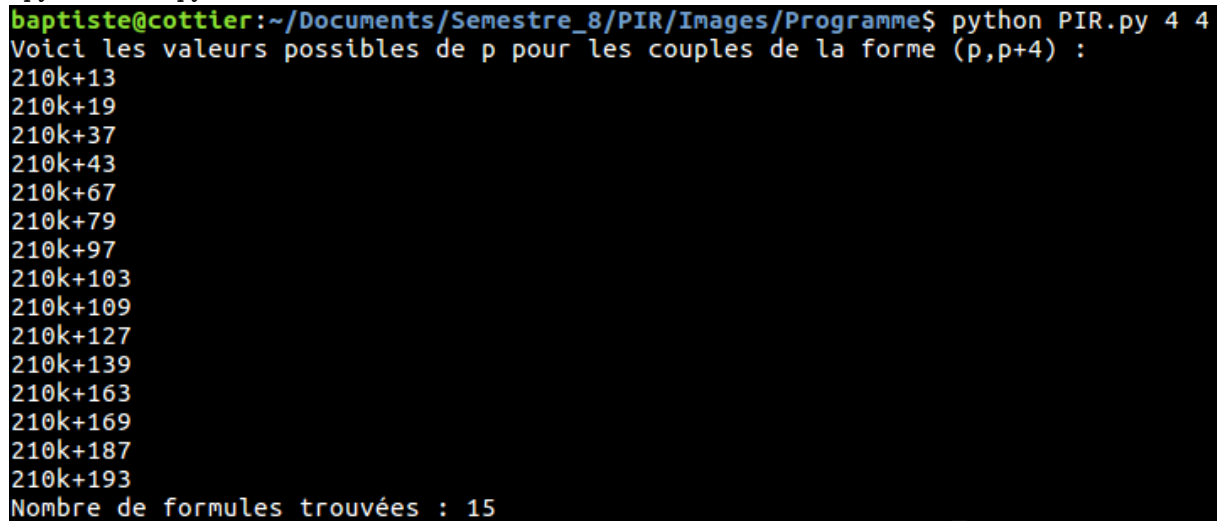
```
baptiste@cottier:~/Documents/Semestre_8/PIR/Images/Programme$ python PIR.py 4 2
Voici les valeurs possibles de p pour les couples de la forme (p,p+2) :
210k+11
210k+17
210k+29
210k+41
210k+59
210k+71
210k+101
210k+107
210k+137
210k+149
210k+167
210k+179
210k+191
210k+197
210k+209
Nombre de formules trouvées : 15
```

On retrouve bien les 15 formules trouvées par les frères WOLF.

– Exemple sur les nombres premiers cousins –

On exécute la ligne de commande suivante :

```
$python PIR.py 4 4
```



```
baptiste@cottier:~/Documents/Semestre_8/PIR/Images/Programme$ python PIR.py 4 4
Voici les valeurs possibles de p pour les couples de la forme (p,p+4) :
210k+13
210k+19
210k+37
210k+43
210k+67
210k+79
210k+97
210k+103
210k+109
210k+127
210k+139
210k+163
210k+169
210k+187
210k+193
Nombre de formules trouvées : 15
```

On obtient 15 nouvelles formules.

– Exemple sur les nombres premiers sexy –

On exécute la ligne de commande suivante :

```
$python PIR.py 4 6
```

```
baptiste@cottier:~/Documents/Semestre_8/PIR/Images/Programme$ python PIR.py 4 6
Voici les valeurs possibles de p pour les couples de la forme (p,p+6) :
210k+11
210k+13
210k+17
210k+23
210k+31
210k+37
210k+41
210k+47
210k+53
210k+61
210k+67
210k+73
210k+83
210k+97
210k+101
210k+103
210k+107
210k+121
210k+131
210k+137
210k+143
210k+151
210k+157
210k+163
210k+167
210k+173
210k+181
210k+187
210k+191
210k+193
Nombre de formules trouvées : 30
```

Considérons à présent 5 nombres premiers.

– Exemple sur les nombres premiers jumeaux –

On exécute la ligne de commande suivante :

```
$python PIR.py 5 2
```

```
baptiste@cottier:~/Documents/Semestre_8/PIR/Images/Programme$ python PIR.py 5 2
Voici les valeurs possibles de p pour les couples de la forme (p,p+2) :
2310k+17
2310k+29
2310k+41
...
2310k+2249
2310k+2267
2310k+2279
2310k+2291
2310k+2309
Nombre de formules trouvées : 135
```

De cette manière, on peut déterminer autant de formules que l'on veut en modifiant les paramètres de la fonction.

5 Références

5.1 Webographie

- https://fr.wikipedia.org/wiki/Nombres_premiers_jumeaux
- <http://www.math.stonybrook.edu/~moira/mat331-spr10/papers/1949%20ClementCongruences20for%20Sets%20of%20Primes.pdf>
- https://fr.wikipedia.org/wiki/Conjecture_de_Dubner
- <http://mathworld.wolfram.com/CousinPrimes.html>

5.2 Bibliographie

- Hans RIESEL : *Prime Numbers and Computer Methods for Factorization* – p.65-67

6 Conclusion

Le sujet de PIR que l'on nous a donné était différent de ceux habituellement donnés. En effet, il s'agissait de critiquer un travail et non pas de faire à proprement parler des recherches sur un sujet précis. C'est notamment pour cette raison que l'on a choisi ce sujet. Le sujet en lui-même nous semblait intéressant. Malheureusement, il s'en est avéré autrement. Comme dit précédemment, l'article des frères WOLF n'est pas très agréable à lire. Puis quand on a compris que les formules pouvaient se retrouver en quelques lignes, cela nous a découragé d'étudier les 80 pages de leur article.