# CONSTELLATIONS QUELCONQUES DE NOMBRES PREMIERS

Rene-Louis Clerc

# CONSTELLATIONS QUELCONQUES DE NOMBRES PREMIERS

**René-Louis Clerc ( 11/03/2022) ((*))**

## ABSTRACT

**Number theory (prime numbers)**
**ANY CONSTELLATIONS OF PRIME NUMBERS. Following Polignac's conjecture ([1]) stated in 1849, a large number of works on prime numbers, pairs of primes distant by an even integer and constellations of primes have been published ([2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]), with, in particular, Brun's theorem ([2]) in 1919 and Green- Tao ([7]) in 2008.**
**This last theorem demonstrates the existence of arithmetic constellations of length n > 2 and ratio e, for all n; in ([8]) we have established properties allowing us to explicitly determine the possible reasons e of these arithmetic sequences and to exhibit numerous representatives of them.**
**We are considering here constellations where the successive increasing distinct prime numbers of the sequence are distant by any gaps, and there is, a priori, no constraint imposed on these gaps which are therefore independent of each other; we will speak of free or arbitrary constellations (or n-tuples). Using modular arithmetic in N/6N, we will establish constructive properties (as in [12] for specifically arithmetic constellations) to determine representatives of various free n-tuples for n > 2.**
**Theorems on free triples, quadruplets and quintuplets will be established and will perfectly allow to exhibit various representatives of these n-tuples according to the modulo 6 properties of the gaps between the first constituents. For all free n-tuples, n > 2, we will show that for some modulo 6 properties of their gaps, there will be several representatives that we can exhibit, but naturally, all n-tuples with arbitrary gaps cannot not exist, as do all arithmetic tuples for whatever reason.**
**By admitting Polignac's conjecture, we can expand the Green-Tao theorem ([7]) and state that, among prime numbers, there always exist n-tuples, free or not, for all n.**
**For any free n-tuple, the equality modulo 6 of all its gaps will ensure a large number of representatives, as a ratio e equal to a certain primorial (depending on n) did for any arithmetic n-tuple ([12]).**
**In the context of data protection, we finally propose an application of these results to build one-way functions that produce a secret code, in the form of a prime number, associated with digital personal data that could thus be found protected. Thanks to the existence and possible effective construction of very many representatives of free n-tuples (n > 2) it is possible to manufacture and use a very large number of such functions which can therefore be perfectly personalized; a simple example is provided in an appendix link.**
**The proposed numerical illustrations were obtained using the PARI/GP calculation software.**

## INTRODUCTION

**A la suite de la conjecture de Polignac ([1]) énoncée en 1849, de très nombreux travaux sur les nombres premiers, les couples de premiers distants d'un entier pair et les constellations de premiers ont été publiés ([2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]), avec, en particulier, le théorème de Brun ([2]) en 1919 et le théorème de Green-Tao ([7]) en 2008.**
**Ce dernier théorème démontre l'existence de constellations arithmétiques de longueur n > 2 et de raison e, pour tout n; dans ([12]) nous avons établi des propriétés permettant de déterminer explicitement les possibles raisons e de ces suites arithmétiques et d'en exhiber de nombreux représentants.**
**Nous envisageons ici des constellations où les nombres premiers distincts successifs croissants de la suite sont distants d'écarts quelconques, et il n'y a, a priori, aucune contrainte imposée à ces écarts qui sont donc indépendants les uns des autres; on parlera de constellations (ou de n-uplets) libres ou quelconques. Par l'utilisation de l'arithmétique modulaire dans N/6N, nous établirons des propriétés constructives (comme dans [12] pour les constellations spécifiquement arithmétiques) pour déterminer des représentants de divers n-uplets libres pour n > 2.**
**Des théorèmes sur les triplets, quadruplets et quintuplets libres seront établis et permettront**

**parfaitement d'exhiber divers représentants de ces n-uplets suivant les propriétés modulo 6 des écarts entre les premiers les constituant. Pour tous les n-uplets libres, n > 2, nous montrerons que pour certaines propriétés modulo 6 de leurs écarts, il y aura plusieurs représentants que l'on pourra exhiber, mais naturellement, tous les n-uplets avec des écarts quelconques ne pourront pas exister, comme d'ailleurs tous les n-uplets artithmétiques pour des raisons quelconques.**
**En admettant la conjecture de Polignac, on pourra élargir le théorème de Green-Tao ([7]) et énoncer que, parmi les nombres premiers il existe toujours des n-uplets, libres ou pas, pour tout n.**
**Pour tout n-uplet libre, l'égalité modulo 6 de tous ses écarts assurera un grand nombre de représentants, comme une raison e égale à une certaine primorielle (dépendant de n) le faisait pour tout n-uplet arithmétique ([12]).**
**Dans le cadre de la protection des données, nous proposons enfin une application de ces résultats pour construire des fonctions à sens unique qui produisent un code secret, sous la forme d'un nombre premier, associé à des données personnelles numériques qui pourraient ainsi se trouver protégées. Grâce à l'existence et à la construction effective possible de très nombreux représentants de n-uplets libres (n > 2) on peut fabriquer et utiliser un très grand nombre de telles fonctions qui peuvent être donc parfaitement personnalisées; un exemple simple est proposé dans un lien annexe.**
**Les illustrations numériques proposées ont été obtenues en utilisant le logiciel de calcul PARI/GP.**

## 1- TRIPLETS QUELCONQUES DE NOMBRES PREMIERS

**Les couples (ou doublets) de nombres premiers, comme les premiers jumeaux, cousins, sexy ou autres octo, ...ont largement été étudiés ([1], [2], [3], [5]), aussi nous intéresserons-nous ici aux constellations de premiers d'au moins 3 termes.**
**Par définition, nous appellerons constellation $K_n$ de longueur n > 2 ou n-uplet, une suite finie, strictement croissante de n nombres premiers différents successifs (et non nécessairement consécutifs), les écarts entre ces nombres successifs étant absolument quelconques.**
**On parlera de constellation consécutive $K^*_n$ ou de constellation non consécutive (ou simplement constellation) $K_n$ suivant que les premiers qui la constituent sont tous consécutifs ou non.**
**Dans ([12]) nous avions pu illustrer le théorème général d'existence de Green-Tao ([7]) en exhibant de manière constructive les raisons possibles des constellations arithmétiques. Ici notre objectif est d'envisager la construction effective de constellations quelconques.**
**Comme nous l'avions déjà indiqué dans ([12]), l'analyse des suites de premiers est parfaitement efficace et rapide dans N/6N; nous calculerons ici aussi en modulo 6, en rappelant qu'un nombre premier impair est soit 3, soit un nombre 5(6) ou 1(6).**
**Il en résultera, que si pour un certain n-uplet, n > 2, on a toujours des séquences de n nombres avec au moins un 3(6), il ne pourra y avoir, au mieux, que le seul repésentant avec le nombre 3; sinon le n-uplet correspondant n'aura aucun représentant, et fera partie de tous les n-uplets qui ne peuvent pas exister.**
**Certaines constellations n'ont pas de représentant, comme par exemple (p, p+20, p+52, ...) qui fait apparaitre (5(6)-1(6)-3(6)-... ou 1(6)-3(6)-...) un multiple de 3 dès le deuxième ou le troisième terme; d'autres n'ont qu'un seul représentant comme (p, p+2, p+4, p+8) avec le seul (3, 5, 7, 11)...**
**Pour une constellation $(p, p_1, p_2, ..., p_{n-1})$ de longueur n donnée, nous appellerons écarts les $a_i = p_i - p$, i = 1, ...,n - 1, tous différents et strictement croissants, l'écart total étant $e_t = a_{n-1}$; ces $\{a_i\}$ constituent une suite absolument quelconque d'entiers pairs et non nécessairement une suite arithmétique ou de Fibonacci ou liée par toute autre contrainte (nous dirons qu'elle a, a priori, n-1 degrés de liberté).**

### 1-1- TRIPLETS CONSECUTIFS

**Il y a deux triplets consécutifs triviaux à un seul représentant: (2, 3, 5) le seul (p, p+1, p+3) avec le nombre pair 2 et $e_t = 3$,**
**et (3, 5, 7) le seul (p, p+2, p+4) avec $e_t = 4$.**
**Les deux seuls triplets consécutifs avec $e_t = 6$ sont:**
**(p, p+2, p+6): (5, 7, 11), (11, 13, 17), (17, 19, 23), (41, 43, 47) ...**
**(p, p+4, p+6): (7, 11, 13), (13, 17, 19), (37, 41, 43), (67, 71, 73) ...**
**Ils ont tous les deux un grand nombre de représentants qui est d'ailleurs conjecturé infini.**
**Ces 4 types de triplets forment la famille $K^*_3$.**

### 1-2- TRIPLETS NON NECESSAIREMENT CONSECUTIFS

**Pour des $e_t > 6$, on peut naturellement envisager divers triplets non consécutifs et la famille $K_3$ sera manifestement plus nombreuse que $K^*_3$.**
**Il existe plusieurs triplets non consécutifs à un seul représentant:**
**(p, p+8, p+16) avec (3, 11, 19); (p, p+16, p+20) avec (3, 19, 23) ...et aussi (cf. théorème 1 de [12]):**
**(p, p+e, p+2e) avec $e \neq 0(6)$; si 3+e et 3+2e sont premiers, il y a le seul représentant (3, 3+e, 3+2e) (et sinon il n'y a pas de représentant).**
**On montre en effet facilement que pour $e = 2(6)$ ou $e = 4(6)$, il y aura toujours (avec $p = 1(6)$ ou $5(6)$) un $3(6)$ soit comme deuxième terme soit comme troisième et donc pas d'autre solution possible que (3, 3+e, 3+2e).**
**Les triplets (p, p+14, p+22) ou (p, p+20, p+52) n'ont pas de représentant...**
**Beaucoup d'autres ont de nombreux représentants comme va nous le décrire le théorème suivant qui concerne tous les triplets possibles.**

**Théorème 1 (des triplets)**
**Pour tout triplet (p,p+a,p+b), p premier, $a < b$, a et b pairs strictement positifs, on aura:**
**1) Si $a = 0(6)$: pour tout b il existe plusieurs triplets.**
**2) Si $a = 4(6)$:**
**si $b = 2(6)$ et si 3+a et 3+b sont premiers, il y a le seul triplet (3, 3+a, 3+b), sinon 0;**
**si b n'est pas $2(6)$, il existe plusieurs triplets.**
**3) Si $a = 2(6)$:**
**si $b = 4(6)$ et si 3+a et 3+b sont premiers, il y a le seul triplet (3, 3+a, 3+b), sinon 0;**
**si b n'est pas $4(6)$, il existe plusieurs triplets.**
**En particulier, pour $a = 0(6)$ ou $b = 0(6)$ il n'y aura jamais de triplet débutant par 3, et donc soit 0 soit plusieurs triplets (jamais un seul).**

**Démonstration**
**Pour $a = 0(6)$, $p+a = p \bmod 6$, donc pour tout b, on aura toujours soit $p = 1(6)$ soit $p = 5(6)$ qui donnera un 3eme terme $1(6)$ ou $5(6)$ et donc possiblement un premier; il existera donc plusieurs triplets pour tous les p tels que p + a et p + b soient premiers.**
**Pour $a = 4(6)$, $b = 2(6)$, on aura toujours un $3(6)$ dans l'un des deux derniers termes; la seule possibilité sera le nombre 3 à condition que 3+a et 3+b soient premiers.**
**Pour $a = 4(6)$, $b = 0(6)$ ou $b = 4(6)$: dans les deux cas $p = 1(6)$ produira 3 termes tous $1(6)$ ou $5(6)$ donc possiblement premiers, d'où plusieurs triplets pour tous les p tels que p + a et p + b soient premiers.**
**Pour $a = 2(6)$, $b = 4(6)$ donne toujours un $3(6)$ en terme 2 ou 3, et donc pas de solution sauf le nombre 3.**
**Pour $a = 2(6)$, $b = 0(6)$ ou $b = 2(6)$: avec $p = 5(6)$ on aura une séquence $5(6)$-$1(6)$-$5(6)$ ou $5(6)$-$1(6)$-$1(6)$, et donc plusieurs possibles solutions pour tous les p tels que p + a et p + b soient premiers.**
**Enfin si a ou b est $0(6)$, avec $p = 3$, il y aura toujours un $3(6)$ dans la suite des 3 termes, et donc pas de triplet avec $p = 3$.**
**On remarquera que si a et b ne sont pas $0(6)$ mais tels que $a + b = 0(6)$, il y aura au plus un triplet avec $p = 3$.**
**Si l'on ne considère que les triplets avec $p > 3$, il n'y a que deux situations possibles: pour un couple (a, b) donné, ou il n'existe pas de triplet ou il en existe un grand nombre.**
**L'existence effective de plusieurs solutions (triplets avec des p tels que p + a et p + b soient premiers) dans les cas où une condition suffisante est assurée, se déduit de la conjecture de Polignac ([1]), qui n'est, pour le moment, pas contredite et que nous admettrons: tout entier pair est égal à la différence de deux nombres premiers consécutifs, et a fortiori, non nécessairement consécutifs, et ce, d'une infinité de manières. On peut donc dire qu'il existe plusieurs couples de premiers $q_1$, $q_2$, tels que $a = q_2 - q_1$, et plusieurs couples de premiers $q_3$, $q_4$, tels que $b = q_4 - q_3$; dans tous les cas où $q_1 = q_3$ que l'on pourra noter p, on obtiendra un tripet solution. L'infinité des premiers et celle des décompositions de Polignac entraînent que l'on pourra exhiber effectivement de tels nombreux p, ce que confirme l'expérimentation numérique.**
**Si l'on compare avec le théorème 1 de [12] sur les triplets arithmétiques, on observe que la laison $b = 2a$ élimine les possibilités qui conduisent ici (cas 2) avec $a = 4(6)$ et b non $2(6)$; cas 3) avec $a = 2(6)$ et b non $4(6)$) à plusieurs triplets solutions. En ce qui concerne les écarts entre les premiers, les**

**triplets arithmétiques sont à 1 degré de liberté (e), alors que les triplets quelconques sont à 2 d.d.l. (a, b), ce qui permet normalement à ces derniers d'avoir plus de représentants, même si tous n'existent pas nécessairement.**
**Le théorème 1 permet bien de construire effectivement de nombreux triplets possibles, et dans chaque cas où il y aura plusieurs solutions, on pourra conjecturer (au nom de l'infinité des nombres premiers) qu'il y en a une infinité.**
**Exemples.**
**Pour a = 12, b = 28 on obtient (19, 31, 47), (31, 43, 59), (61, 73, 89), ..., (811, 823, 839), ...**
**Pour a = 2 et b = 44456, tous les deux 2(6), on obtiendra, conformément au 3) du théorème 1, plusieurs triplets débutant par des p = 41, 107, 191, ..., 36467, 37361, ..., 99137, 99707, ...**
**Avec a = 7320 et b = 14512, conformément au 1) du théorème 1, on obtiendra plusieurs triplets débutant par des p = 31, 157, 229, ..., 99907, 100129,..., 162727, 163021, ...**
**Avec a = 4444444444006 et b = 8888888888888888884, tous les deux 4(6), conformément au 2) du théorème 1, on obtiendra plusieurs triplets commençant par des p = 6247, 7603, 13933, ..., 530857, 532663, ..., 992917, 999043, ..., 9999193, ...**

## 2- QUADRUPLETS QUELCONQUES DE NOMBRES PREMIERS

**On établira de la même manière un résultat général concernant tous les quadruplets (à termes non nécessairement consécutifs), et on obtiendra, comme plus haut (et comme dans [12] pour les n-uplets spécifiquement arithmétiques) que pour un quadruplet donné, soit il a au maximum un représentant, soit il en a plusieurs.**
**Nous disons souvent solution pour décrire un n-uplet licite de nombres premiers.**

**Théorème 2 (des quadruplets)**
**Pour tout quadruplet (p, p+a, p+b, p+c), a < b < c, avec a, b, c pairs strictement positifs, on aura:**
**1) Si a = 0(6):**
**si (b = 4(6), c = 2(6)) ou (b = 2(6), c = 4(6)): 0 solution.**
**2) Si a = 2(6):**
**si (b = 0(6), c = 4(6)): 0 solution**
**si (b = 4(6) pour tout c): 0 solution ou 1 avec p = 3,**
**si (c = 4(6) pour tout b): 0 solution ou 1 avec p = 3.**
**3) Si a = 4(6):**
**si (b = 0(6), c = 2(6)): 0 solution,**
**si (b = 2(6) pour tout c): 0 solution (ou 1 avec p = 3 si c non nul),**
**si (c = 2(6) pour tout b): 0 solution (ou 1 avec p = 3 si b non nul),**
**si (b = 4(6), c = 2(6)): 0 solution (1 avec p = 3 possible),**
**si (c = 4(6), b = 2(6)): 0 solution (1 avec p = 3 possible).**
**4) Pour tous les autres cas il existe plusieurs solutions (infinité probable) avec tous les p tels que p + a, p + b et p + c soient premiers.**
**En particulier, pour a = 0(6) ou b = 0(6) ou c = 0(6), il n'y aura jamais de quadruplet débutant par 3, et donc soit 0 soit plusieurs quadruplets (jamais un seul), et pour a, b et c tous 0(6) il y aura plusieurs solutions.**

**Démonstration**
**On raisonne toujours dans N/6N en partant d'un premier p (nécessairement égal à 3 ou 1(6) ou 5(6)); s'il y a au moins une séquence complète (avec p = 1(6) ou p = 5(6)) avec seulement des 1(6) ou 5(6), il y a possibilité de plusieurs solutions avec les divers p qui conviennent (tels que p + a, p + b, p + c soient premiers), en revanche si dans les deux types de séquences possibles (départ en 1(6) ou en 5(6)) il apparait un 3(6) il n'y aura pas de solution sauf éventuellement une seule avec p = 3, à condition que 3+a, 3+b, 3+c soient tous les trois des nombres premiers.**
**Enfin si a ou b ou c est 0(6), avec p = 3, il y aura toujours un 3(6) dans la suite des 4 termes et donc pas de quadruplet débutant par 3.**
**Comme plus haut, si l'on se limite aux quadruplets avec p > 3, il n'y a que deux possibilités: pour (a, b, c) donnés, ou il n'existe aucun quadruplet ou il en existe plusieurs; par ailleurs ces quadruplets quelconques à 3 d.d.l. ont plus de représentants que leurs homologues arithmétiques (à 1 d.d.l.**

**seulement).**
**Ici aussi (comme pour les triplets), l'existence effective et constructive de plusieurs solutions sera déduite de la conjecture de Polignac.**
**Exemples.**
**Pour a = 18, b = 26, c = 32 on obtient (5, 23, 31, 37), (11,,29, 37, 43), ...(701, 719, 727, 733), ...**
**Pour a = 16, b = 26, c = 50 on obtient le seul (3, 19, 29, 53), et aucun représentant pour a = 20, b = 36, c = 46.**
**Pour a = 2, b = 24, c = 620, on obtiendra les solutions débutant par des p = 107, 149, 239, ..., 995549, 999959, ...**
**Pour a = 142 , b = 42892, c = 60004, on obtiendra les solutions débutant par des p = 37, 97, 379, ..., 994087, 995227, ...**
**Pour a = 76, b = 604, c= 10204, on obtiendra les solutions débutant par des p = 97, 283, 487, ..., 896293, 900157, ...**

## 3- N-UPLETS QUELCONQUES DE NOMBRES PREMIERS

**De manière générale, en ce qui concerne les écarts des premiers les constituant, si les n-uplets artihmétiques sont (par définition) à 1 d.d.l., les n-uplets quelconques sont à (n-1) d.d.l., ce qui leur permettra d'avoir strictement plus de représentants; on les appellera encore n-uplets libres.**
**La différence essentielle entre les n-uplets libres et les n-uplets arithmétiques, c'est que pour ces derniers il y a le théorème de Green-Tao ([7]) qui assure leur existence pour tout n. Pour le cas présent il n'y a pas encore de propriété d'existence avérée pour tout n, ce qui n'empêchera pas d'établir dans de nombreux cas des conditions au moins suffisantes d'existence, et surtout de proposer des techniques constructives pour exhiber de nombreux représentants de tels n-uplets libres (parmi ceux qui peuvent exister).**
**De manière générale (mis à part le cas du nombre premier 3 facile à régler), dès que pour un certain n-uplet, n > 2, on peut avoir des séquences de n nombres sans 3(6) (donc avec uniquement 1(6) ou 5(6)) on aura potentiellement des possibles repésentants de ce n-uplet avec des premiers (mais plus ou moins faciles à exhiber effectivement): l'absence de 3(6) est une condition suffisante d'existence de représentants du n-uplet, l'existence effective de plusieurs solutions étant déduite (cf. le cas des triplets) de la conjecture de Polignac (supposée assurée) et confortée par les nombreuses solutions numériques obtenues.**

### 3-1- QUINTUPLETS QUELCONQUES

**On établira le résultat suivant pour les quintuplets à 4 d.d.l.**

**Théorème 3 (des quintuplets)**
**Pour tout quintuplet $(p, p+a_1, p+a_2, p+a_3, p+a_4)$, $a_1 < a_2 < a_3 < a_4$, avec des $a_i$ pairs strictement positifs, on aura:**
**1) Si pour tout i, $a_i = 0(6)$ et $a_i \neq 0(30)$:**
**si ces $a_i$ sont en progression arithmétique, on aura éventuellement (si $5 + a_i$, i=1,2,3,4 sont tous premiers) une seule solution avec p = 5 et sinon aucune (cf. théorème 3 de [12]);**
**si les $a_i$ sont quelconques et indépendants (°), il y aura plusieurs solutions possibles.**
**2) Si pour tout i, $a_i = 0(30)$: il y aura toujours plusieurs solutions possibles (avec ou sans contrainte sur les $a_i$).**
**(p = 1(6) et p = 5(6) produisent des séquences sans 3(6), d'où plusieurs solutions possibles)**
**3) S'il existe i tel que $a_i = 0(6)$ et les 3 autres étant 4(6), il y aura plusieurs solutions possibles.**
**(en effet à partir de p = 1(6) on a de bonnes séquences sans 3(6) d'où plusieurs solutions possibles)**
**4) S'il existe i tel que $a_i = 2(6)$ les autres n'étant pas 4(6), il y aura plusieurs solutions possibles.**
**(en effet p = 5(6) peut produire des suites sans 3(6), donc plusieurs solutions possibles)**
**Notons que ceci sera donc en particulier valable pour $a_i = 2(6)$ pour tout i.**
**5) Si pour tout i, $a_1 = 4(6)$, il existera plusieurs solutions potentielles (1(6)-5(6)-5(6)-5(6) possible) et peut-être le nombre 3.**
**6) S'il existe i tel que $a_i = 4(6)$, les autres n'étant pas 2(6), il existera plusieurs solutions potentielles (séquence débutant par 1(6) possible).**
**(°) Toute contrainte sur les $a_i$ modifie, assez normalement, le nombre de solutions à la baisse.**

**On peut par exemple observer que si $a_3 = a_1 + a_2$ et $a_4 = a_2 + a_3$ il n'y aura plus que, éventuellement la seule solution p = 5, ou aucune. Cette contrainte à 2 d.d.l. (de type Fibonacci) sur les $a_i$ fait aussi passer (comme la contrainte arithmétique dans [12]) de plusieurs solutions à au plus une seule. Comme dans le cas des triplets, l'existence effective de solutions sera déduite de la conjecture de Polignac, qui entraînera que plusieurs solutions débutant par certains p seront effectivement exprimables.**

**Exemples**
**Des $a_i$ respectifs (30, 120, 240, 30000) produisent des quintuplets débutant par 11, 29, 71, 109,..., 9994363, ...**
**Des $a_i$ respectifs (8, 14, 122, 600) produisent des quintuplets débutant par 59, 449, 1109, 2129, ..., 9996509, ..**
**Des $a_i$ respectifs (16, 34, 58, 244) produisent des quintuplets débutant par 13, 73, 223, 433, ..., 9950293, ..**
**Des $a_i$ respectifs (38, 92, 602, 1022) produisent des quintuplets débutant par 71, 449, 719, 929, ..., 995339, ..**
**Des $a_i$ respectifs (48, 94, 1204, 11524) produisent des quintuplets débutant par 409, 1693, 2803, 3583, ..., 896443, ...**
**Des $a_i$ respectifs (74, 1200, 11522, 160200) produisent des quintuplets débutant par 167, 2477, 2927, 4079, ..., 3025079, ...**

**3-2- N-UPLETS QUELCONQUES**
**On peut établir, sans prétendre à l'exhaustivité, quelques propriétés générales pour les n-uplets quelconques (ou n-uplets libres).**

**Propriétés des n-uplets quelconques**
**Pour tout n-uplet, $(p, p+a_1, p+a_2+...+p+a_{(n-1)})$, avec des $a_i$ pairs, croissants, strictement positifs distincts et indépendants les uns des autres, on aura:**
**1) Si pour tout i, $a_i = 0(6)$, il pourra exister plusieurs solutions (5-5-5-5-... et 1-1-1-1-... possibles) mais jamais le nombre 3 parmi elles.**
**2) Si pour tout i, $a_i = 4(6)$, il pourra exister plusieurs solutions (p = 1(6) donne 1(6)-5(6)-5(6)-5(6)-...) et peut-être le nombre 3.**
**3) Si pour tout i, $a_i = 2(6)$, il pourra exister plusieurs solutions (p = 5(6) donne 5(6)-1(6)-1(6)-1(6)-...) et peut-être le nombre 3 parmi elles.**
**4) S'il existe un i tel que $a_i = 2(6)$, les autres étant 0(6), il pourra exister plusieurs solutions (p = 5(6) donne des séquences sans 3(6)).**
**5) S'il existe un i tel que $a_i = 0(6)$, il n'y aura jamais le nombre 3 dans un n-uplet de premiers (puisque on aura un 3(6) non premier dans la suite); donc il y aura soit 0 solution soit un grand nombre.**
**6) S'il existe i tel que $a_i = 4(6)$, les autres n'étant pas 2(6), il existera plusieurs solutions potentielles (séquence débutant par 1(6) possible).**
**7) On déduit de 1), 2) et 3) qu'une condition suffisante pour qu'il puisse exister strictement plus d'un n-uplet libre (soit à écarts indépendants les uns des autres) est que $a_i = a_j$ modulo 6, pour tout i,j.**
**Comme plus haut (cas des triplets, quadruplets et quintuplets), le passage de 'plusieurs solutions possibles' à 'plusieurs solutions effectives' sera assuré en admettant la conjecture de Polignac (qui assurera l'existence de plusieurs premiers p tels que les $p + a_i$ soient tous premiers), et sera conforté par l'expérimentation numérique:**
**d'après [1], il existe des couples de premiers $(q_1, q_2)$, $(q_3, q_4)$, ..., chacun en nombre infini, tels que $a_1 = q_2 - q_1$, $a_2 = q_4 - q_3$, ..., et chaque fois que l'on aura $q_1 = q_3 = ...$ que nous noterons p, on obtiendra un n-uplet solution $(p, p + a_1, p + a_2, ...)$. On pourra donc générer et construire plusieurs n-uplets, pour tout n et pour de très nombreux ensembles d'écarts $\{a_i, i = 1, 2, ..., n-1\}$, et conjecturer que dans le cas de plusieurs solutions, elles seront en nombre infini.**
**Rappelons ([12]) que pour une constellation arithmétique de longueur n, il existe un plus petit premier $p_n$ (croissant avec n) tel que la CNS pour qu'il y ait strictement plus d'une constellation**

**soit que l'on ait une raison e = 0($p_n$#). On observera que pour un n-uplet libre avec $a_i$ = 0(6) pour tout i, il y aura strictement plusieurs solutions, alors que si on impose la contrainte arithmétique (ou une contrainte de type Fibonacci ou autre...) sur ces $a_i$, ce ne sera assuré que si on a $a_i$ = 0($p_n$#).**
**Pour adapter la propriété 6) aux n-uplets arithmétiques, il faut avoir des 0(6) et n < 5, sinon à partir de n = 5 ([12] théorème 3) il y aura au plus un représentant de n-uplet et il faudra passer à 0(p#), p >3 (primorielle supérieure à 3#) pour avoir plusieurs solutions.**
**Grâce aux propriétés constructives établies ici, on peut affirmer qu'il existe toujours, pour tout n, des n-uplets à (n-1) d.d.l.; pour obtenir strictement plus d'un représentant il suffit que tous ses écarts soient égaux modulo 6.**
**On notera le rôle de 3# pour les n-uplets libres et celui des primorielles supérieures pour les n-uplets avec contrainte pour n > 4.**
**On observera cependant que pour des écarts égaux modulo des primorielles supérieures (5#, 7#, ...), qui sont en particulier des multiples de 10, on obtient numériquement plus facilement des représentants de n-uplets pour des n > 9 (cf. exemples plus bas).**
**Illustrations numériques**
**Prenons l'exemple du quintuplet arithmétique avec e = 6 qui ne possède que le seul représentant (5, 11, 17, 23, 29); le quintuplet libre avec $a_1$ = 6, $a_2$ = 12, $a_3$ = 18, $a_4$ = 72 (qui ne diffère que par le $a_4$ qui passe de 24 à 72) possède quant à lui un grand nombre (probablement infini) de représentants qui débutent par les premiers 11, 41, 601, 1091, ...., 13451, ..., 99773881, 99861661, ...**
**Le sextuplet avec les écarts 2(6), (8, 38, 74, 86, 110) produit des repésentants débutant par 12503, 25943, 56393, ..., 9616853, ...**
**Le septuplet avec les écarts 2(6), (14, 20, 26, 38, 50, 86) produit des représentants qui débutent par 3, 4973, 5393, ..., 937621793, 991712963, ...**
**Celui avec des écarts 4(6), (16,22,28,40,52,88) produit des septuplets débutant par 1471, 1207291, 6202561, 6862381, 9929851, ...**
**Alors que le septuplet arithmétique avec e = 6 (= 3#), ou e = 30 (= 5#) n'a aucun représentant, mais celui avec e = 210 (= 7#) fournit 47, 179, ..., 8150209, 8177303, ..., 98909273, 99922541, ...**
**L'octuplet défini par des écarts (4, 16, 24, 84, 108, 120, 124) produira des représentants débutant par 43, 3274153, 46785313, ..., 916791373, 959366143, ... et illustre la propriété 6).**
**Dès que n croît quelque peu, les premiers n-uplets solutions peuvent débuter par des p assez grands, ou devenant très vite assez grands ...**
**L'octuplet défini par des écarts 2(6), (8, 14, 26, 38, 56, 86, 2504) produira des représentants débutant par 151523, 9955163, 21727553, ..., 1578735383, ...**
**Le 10-uplet défini par des écarts 0(6), (12, 18, 30, 42, 54, 72, 84, 114, 1284) produira des représentants débutant par 1586238289, 5159237399, 5553918049, 6869628739, 7879692409, ...**
**Le 10-uplet défini par les écarts (30, 36, 54, 86, 234, 2502, 36000, 120000, 300030) produira des représentants débutant par 46617917, 81204077, 598599347, ...(ce cas illustre la propriété 4) plus haut)**
**Le 10-uplet défini par des écarts 4(6), (4, 16, 28, 40, 58, 76, 88, 118, 1288) produira des représentants débutant par 13, 2540477113, 15964547773, 25074868333, 34524055843, ...**
**Le 10-uplet défini par des écarts 2(6), (14, 44, 74, 104, 164, 194, 314, 374, 614) produira des représentants débutant par 9223662587, 13560540377, 16868323877, 30168191423, 39583620173, 43824613853,...**
**Le 11-uplet défini par (30, 90, 120, 180, 210, 360, 420, 450, 720, 1200) produira des représentants débutant par 239753, 6986311, 727879211, ...**
**Le 11-uplet défini par (210, 420, 1050, 2100, 2310, 4200, 4620, 6300, 12600, 12810) produira des représentants débutant par 59243, 85411, 243056543, 281595277, ...**
**Le 12-uplet défini par (210, 420, 630, 1260, 2100, 4200, 6300, 6410, 6830, 8400, 8820) produira des représentants débutant par 809, 20918531, 63477377, 688633259, ...**
**Le 13-uplet défini par (210, 630, 840, 1050, 1260, 1680, 2100, 2940, 6300, 12600, 12810, 16800) produira des représentants débutant par 3451115303, 3880689877, ...**

### 3-3- PROLONGEMENTS DE CONSTELLATIONS

**Etant donné un n-uplet quelconque de premiers, peut-on construire un n+m-uplet, m > 2 avec une m-suite de premiers ?**
**On pourra, par exemple, facilement prolonger certains n-uplets par une suite arithmétique de**

**raison 0(6) (qui ne produira pas de 3(6) dans les termes ajoutés), mais jamais par une de raison 2(6) ou 4(6) (qui, l'une et l'autre, produiront, dès le deuxième ou troisème terme ajouté, un 3(6) rédhibitoire); on peut donc prolonger par des suites de premiers sexy ou super-sexy mais jamais par des suites de premiers de type jumeaux ou cousins.**
**Par exemple le quadruplet cité plus haut, 11-29-37-43 peut être prolongé (raison 18) par le triplet 61-79-97 pour constituer un 7-uplet mais pas par des suites de raison 2(6) ou 4(6)...**
**Cette propriété souligne encore le rôle important des écarts 0(6) pour les constellations quelconques, les écarts de type primorielles 0(r) (r > 3#) étant moins essentiels que dans le cas des suites arithmétiques (cf. [12]). D'autres types de prolongements de constellations sont certainement envisageables ...**

## 3-4- CONSTELLATIONS DE FIBONACCI

**En dehors des constellations absolument quelconques (tous les $a_i$ sont quelconques et indépendants), on peut envisager de nombreux types de n-uplet avec d d.d.l., 1 < d < n-1 en imposant une certaine contrainte sur les $a_i$.**
**On appellera constellation de Fibonacci, tout n-uplet de premiers, n > 3, $(p, p+a_1, p+a_2, ..., p+a_{(n-1)})$ dont les écarts sont à 2 d.d.l. et définis par:**
**$a_j = a_{j-1} + a_{j-2}$, j = 3,...,n-1; seuls $a_1$ et $a_2$ sont quelconques et indépendants des autres $a_j$, j > 2. Les propriétés de ces constellations seront probablement (cf. 1) théorème 3 par exemple) assez semblables à celles des constellations arithmétiques, mais méritent, sans doute, d'être étudiées plus en détails ...elles feront en particulier jouer un rôle plus important aux primorielles supérieures à 3#. Peut-être, d'ailleurs, peut-on établir un théorème d'existence de telles constellations similaire à celui de Green-Tao ([7]) pour les constellations arithmétiques?.**
**Exemples.**
**Le quintuplet de Fibonacci avec des $a_i$ respectifs (36, 48, 84, 132) produit un seul quintuplet débutant par p = 5.**
**Le quintuplet arithmétique défini par e = 36, n'a aucun représentant.**
**Le quintuplet de Fibonacci avec des $a_i$ respectifs (30, 120, 150, 270) produit plusieurs représentants débutant par 7, 43, 79, 163, ..., 899971, ...**
**Le quintuplet arithmétique défini par e = 30 produit plusieurs représentants débutant par 7, 11, 37, 107, ..., 896557, ... Le sextuplet de Fibonacci avec (12, 42, 54, 96, 150) produit plusieurs représentants débutant par 17, 467, 2297, ..., 980677, 997057, ...**
**Les sextuplets arithmétiques avec e = 12, 18, 24 n'ont pas de représentant alors qu'avec e = 30 (= 5#) il y en a plusieurs débutant par 7, 107, 359, ..., 891557, 984307, ...**

## 4- APPLICATION: FONCTIONS A SENS UNIQUE

**On sait qu'une fonction à sens unique (ou fonction unidirectionnelle ou one-way function) est une fonction calculable facilement (quels que soient ses arguments), mais difficile (voire impossible) à inverser. De telles fonctions sont largement utilisées en cryptographie asymétrique ([14]) ou dans le hachage cryptographique ([13]), ou simplement dans la protection des données (par exemple avec un grand nombre B de l'ordre de 300 chiffres, produit de deux premiers B=p*q; p et q difficiles (!) à déterminer à partir de la seule donnée de B).**
**A partir des divers résultats précédents, on peut assez facilement construire de telles fonctions. En utilisant, par exemple, les propriétés des quadruplets, en prenant des données a, b, c, légèrement modifiées pour être dans un cas du théorème 2 conduisant à plusieurs solutions, ou pourra construire tel ou tel réprésentant du k-ème quadruplet et obtenir ainsi un nombre premier associé aux données choisies; celles-ci seront assez difficilement récupérables à partir de la seule connaissance de ce nombre premier. On peut ainsi déterminer un code, sous la forme d'un nombre premier, associé à des données personnelles, impossibles à retrouver à partir de ce nombre.**
**On pourrait même utiliser un représentant d'un n-uplet avec n suffisamment grand pour construire un nombre premier à partir d'un plus grand nombre de données personnelles numériques, ce nombre premier pouvant avoir le nombre de chiffres souhaité, permettant ainsi la protection de ces données, inaccessibles à partir de la connaissance de ce seul nombre premier.**
**Les nombres premiers, véritables atomes de l'arithmétique, devraient continuer à jouer un rôle de plus en plus essentiel pour la sécurité informatique et pour la protection des données, et l'existence**

**de toutes ces constellations libres ou pas devrait y contribuer.**
**Un exemple simple d'une telle fonction comme générateur d'un nombre premier personnel permet d'associer un nombre premier de 6 à 8 chiffres à quatre données numériques personnelles de type date et numéro de département.**

## CONCLUSION

**Le théorème de Green-Tao ([7]) assure que pour tout n > 2, il existe toujours des constellations arithmétiques de longueur n; nous avons montré dans ([12]) que les raisons pouvant conduire à strictement plus d'une solution, pour un n donné, sont exclusivement des 0(6), et que pour n croissant il existe un plus petit premier $p_n$ qui permet d'assurer strictement plus d'un représentant d'une telle constellation dès que e = 0($p_n$#).**
**Nous avons établi ici des théorèmes sur les triplets, quadruplets et quintuplets libres qui permettent parfaitement d'exhiber divers représentants de ces n-uplets suivant les propriétés modulo 6 des écarts entre les premiers les constituant.**
**Plus généralement, en admettant la conjecture de Polignac, on a pu montrer que pour tout n > 2 donné, il existe toujours des n-uplets à (n-1) d.d.l. et dès que tous ses écarts $a_i$ sont égaux modulo 6, il en existe plusieurs représentants que l'on peut exhiber.**
**Avec une contrainte de type atithmétique imposée à ces $a_i$, la condition suffisante d'obtention de strictement plus d'une solution (et probablement d'une infinité) devient des écarts égaux à 0($p_n$#), $p_n$ étant un premier très vite plus grand que 3 dès que n croit, les primorielles supérieures remplaçant 3# ([12]).**
**En admettant la conjecture de Polignac, le théorème de Green-Tao [7] pourrait donc encore s'exprimer par: dans la suite des nombres premiers il existe toujours des n-uplets, libres ou pas, pour tout n.**
**Les diverses illustrations numériques proposées ont été obtenues par des codes réalisés avec le logiciel de calcul PARI/GP, spécialement adapté à la théorie des nombres.**
**L'existence et la possible constructivité de très nombreux représentants de n-uplets libres (n > 2), permettent de définir de très nombreuses fonctions à sens unique, pouvant générer un certain nombre premier associé à diverses données personnelles numériques, qu'il pourrait ainsi protéger, les fonctions à utiliser pouvant elles-mêmes être personnalisées. Un exemple simple codé en PHP est proposé dans un lien annexe directement utilisable en ligne.**

---

**(*)Professeur honoraire Université Paul Sabatier, Toulouse, France, Webmaster du site SAYRAC.**

---

## REFERENCES

**[1] de Polignac A., Recherches nouvelles sur les nombres premiers, CRAc.Sc.Paris, t.29, p.397-401, 1849.**
**[2] Vigo Brun, La série 1/5+1/7+1/11+1/13+1/17+1/19+1/29+1/31+1/41+1/43+1/59+1/ 61+..., où les dénominateurs sont nombres premiers jumeaux est convergente ou finie, Bulletin des Sciences Mathématiques Vol. 43 : p.100-104, et p.124-128, 1919.**
**[3] G.H.Hardy and J.E. Littlewood, Some problems of Partitio Numerorum III: On the expression of a number as a sum of primes, Acta Mathematica 44, p.1-70, 1922.**
**[4] Paul Erdős et Paul Turán, On some sequences of integers, Journal of the London Mathematical Society, vol. 11, no 4, p. 261–264, 1936.**
**[5] E. Bombieri and H. Davenport, Small differences between prime numbers, Proc. Roy. Soc. Ser. A 293, 1–18, 1966.**
**[6] E. Bombieri, J. B. Friedlander, and H. Iwaniec, Primes in arithmetic progressions to large moduli,Acta Math. 156, 203–251, 1986.**
**[7] Ben J. Green et Terence Tao, The primes contain arbitrarily long arithmetic progressions, Annals of Mathematics, vol. 167, p. 481-547, 2008 (arXiv math.NT/0404188).**
**[8] D. A. Goldston, J. Pintz, and C. Y. Yildirim, Primes in tuples I, Ann. Math. 170, 819–862, 2009.**
**[9] Yitang Zhang. Bounded gaps between primes, Annals of Mathematics, 179 :1121–1174, 2014.**

**[10] James Maynard, Small gaps between primes, Annals of Mathematics, 181 :383–413, 2015.**
**[11 ] A. Granville, Primes in intervals of bounded length, Bull. Amer. Math. Soc. 52, 171–222, 2015.**

**[12] R.L.Clerc, Sous-ensembles et constellations arithmétiques de nombres premiers, p.1-10, ( https://hal.archives-ouvertes.fr/hal-03589472 ), 2022.**
**[13] M. Naor et M. Yung, Universal one-way hash functions and their cryptographic applications, STOC, ACM, p.33–43, 1989.**
**[14] Oded Goldreich, Foundations of Cryptography, vol.2, Cambridge University Press, 2004.**

---

**Page index de SAYRAC**