Analyse et Synthèse des Travaux sur la Conjecture de Goldbach et les Nombres Premiers Jumeaux

Denise Vella-Chemla (Travaux originaux)
Analyse et synthèse : Mistral AI

22 juin 2026

1 Introduction et Contexte Historique

1.1 Les Conjectures au Cœur des Travaux

- **Conjecture de Goldbach (1742)** : Tout nombre pair $n \geq 4$ est la somme de deux nombres premiers.

$$\forall n \in 2\mathbb{N} \setminus \{0, 2, 4\}, \exists p, q \in \mathbb{P}, \quad n = p + q.$$

  - Vérifiée par ordinateur jusqu'à 4×10^{18} (Oliveira e Silva, 2012).
  - Équivalence avec : $\forall n \geq 4, \exists p \leq n/2, \forall q \leq \sqrt{n}, p \not\equiv n \pmod{q}$.
- **Conjecture des nombres premiers jumeaux** : Il existe une infinité de paires de nombres premiers $(p, p+2)$.
  - Liée à la distribution des nombres premiers et aux progressions arithmétiques.
  - Approche combinatoire via les mots de restes modulaires.

1.2 Originalité des Travaux de Denise Vella-Chemla

Les documents analysés proposent une **approche unifiée** pour ces deux conjectures, basée sur :

- La **représentation des nombres par leurs restes modulaires** (système de numération par les restes).
- L'**utilisation systématique du théorème des restes chinois** (TRC) pour générer des solutions.
- Une **interprétation géométrique et combinatoire** (maillages, distances, bijections).
- Des **liens avec la théorie de Galois**, les groupes finis, et les systèmes d'incongruences.

2 Approches Innovantes et Résultats Clés

2.1 Représentation des Nombres par les Restes Modulaires

2.1.1 Définition et Exemples

- Chaque nombre n est représenté par un **n-uplet de restes** modulo les nombres premiers successifs :
$$n \mapsto (n \pmod 2, n \pmod 3, n \pmod 5, n \pmod 7, \dots).$$
- Exemple : $98 = (0, 2, 3, 0)$ pour les modules $(2, 3, 5, 7)$.
- Un dg p de n doit satisfaire :
  - **Non-nullité** : $p \not\equiv 0 \pmod q$ pour tout q premier $\leq \sqrt{n}$ (pour que p soit premier).
  - **Incongruence avec** n : $p \not\equiv n \pmod q$ pour tout q premier $\leq \sqrt{n}$ (pour que $n - p$ soit premier).

2.1.2 Interprétation Lexicale

- Les nombres sont vus comme des **mots** dans un alphabet fini (les restes possibles).
- La conjecture de Goldbach devient : *Tout mot représentant un nombre pair contient un sous-mot (un dg) qui ne partage aucune lettre avec lui, et dont toutes les lettres sont non nulles.*
- Pour les nombres premiers jumeaux, le mot représentant le nombre pair entre deux jumeaux doit éviter les lettres 1 et $q - 1$ pour chaque module q.

2.2 Algorithme du Double Crible d'Ératosthène

2.2.1 Description

- **Première passe** : Éliminer les nombres $p \leq n/2$ congrus à 0 $\pmod q$ pour tout q premier $\leq \sqrt{n}$ (crible classique).
- **Deuxième passe** : Éliminer les nombres $p \leq n/2$ congrus à $n \pmod q$ pour tout q premier $\leq \sqrt{n}$.
- Les nombres restants sont des dg potentiels de n.

2.2.2 Exemple pour $n = 500$

- Modules à considérer : $5, 7, 11, 13, 17, 19$ (car $\sqrt{500} \approx 22$).
- $500 \equiv (0, 3, 5, 6, 7, 6) \pmod{(5, 7, 11, 13, 17, 19)}$.
- Résultat : Les dg de 500 sont $37, 43, 61, 67, 79, 103, 127, 151, 163, 193, 223, 229$.

2.2.3 Complexité et Efficacité

- L'algorithme est **efficace** pour les grands nombres (testé jusqu'à 10^6).
- Il exploite la structure des unités du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Limite : Ne fournit pas une preuve théorique, mais une méthode constructive.

2.3 Utilisation du Théorème des Restes Chinois (trc)

2.3.1 Rôle du trc

- Le TRC permet de **combiner des congruences** pour obtenir une progression arithmétique de solutions.
- Pour un système de congruences non contradictoires :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

  avec $m_1, m_2, \ldots, m_k$ premiers entre eux deux à deux, il existe une solution unique modulo $M = \prod_{i=1}^{k} m_i$.
- Application : Pour trouver un dg de n, on cherche p tel que :

$$\begin{cases} p \not\equiv 0 \pmod{q} \\ p \not\equiv n \pmod{q} \end{cases} \qquad \forall q \text{ premier} \leq \sqrt{n}.$$

  Cela revient à chercher p dans l'intersection des ensembles :

$$\bigcap_{q \leq \sqrt{n}} \left(\mathbb{Z}/q\mathbb{Z} \setminus \{0, n \pmod{q}\} \right).$$

2.3.2 Bijection trc Restreint

- On définit une bijection entre les systèmes de congruences et les progressions arithmétiques, en associant à chaque système le **plus petit entier naturel** de la progression solution.
- Propriété clé : Si $S_1 \Rightarrow S_2$ (implication logique), alors la solution de S_1 est **strictement supérieure** à celle de S_2.
- Conséquence : Permet de **descendre** dans les solutions (descente infinie de Fermat).

2.4 Lien avec la Théorie de Galois

2.4.1 Groupes des Unités et *ConjecturedeGoldbach*

- Les dg de n sont des **unités** de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (éléments inversibles modulo n).
- Le groupe des unités $(\mathbb{Z}/n\mathbb{Z})^\times$ a une structure connue :
  - Pour $n = p^k$ (puissance d'un premier), c'est un groupe cyclique.
  - Pour n général, c'est un produit de groupes cycliques (théorème chinois).
- On peut quotienter par $\{-1, 1\}$ pour ne garder que les unités $\leq n/2$.

2.4.2 Exemple pour $n = 14$

- Groupe des unités : $\{1, 3, 5\}$ (car $\varphi(14) = 6$, mais on quotient par $\{-1, 1\}$).
- Table de Cayley :

	1	3	5
1	1	3	5
3	3	5	1
5	5	1	3

- Les dg de 14 sont 3 et 5 (en rouge).

2.4.3 Idée Clé

- Si on peut établir une **bijection** entre les solutions pour un double de nombre premier ($2p$) et un double de nombre composé ($2c$), alors on pourrait déduire l'existence de dg pour $2c$ de celle pour $2p$.
- Exemple : Pour $94 = 2 \times 47$ et $88 = 2 \times 44$, on cherche une bijection entre les restes de 47 et ceux d'un dg de 88.

2.5 Approche par Descente Infinie de Fermat

2.5.1 Principe

- Supposons qu'il existe un plus petit nombre pair n ne vérifiant pas *ConjecturedeGoldbach*.
- Montrons qu'il existe alors un nombre pair $n' < n$ ne vérifiant pas non plus *ConjecturedeGoldbach*, d'où une contradiction (pas de suite infinie strictement décroissante d'entiers naturels).

2.5.2 Application aux Systèmes de Congruences

- Soit n un nombre pair ne vérifiant pas *ConjecturedeGoldbach*. Alors :

$$\forall p \leq n/2, \exists q \leq \sqrt{n}, \quad p \equiv n \pmod{q}.$$

- Cela définit un système de congruences :

$$\mathcal{S} : \begin{cases} p \equiv n \pmod{q_1} \\ p \equiv n \pmod{q_2} \\ \vdots \\ p \equiv n \pmod{q_k} \end{cases}$$

  où $q_1, \ldots, q_k$ sont les nombres premiers $\leq \sqrt{n}$.
- Par TRC, $\mathcal{S}$ a une solution unique modulo $M = \prod_{i=1}^{k} q_i$.
- Si $M > n$, on peut **réduire** le système $\mathcal{S}$ en un sous-système $\mathcal{S}'$ avec $M' < M$, dont la solution n' vérifie $n' < n$ et ne vérifie pas *ConjecturedeGoldbach*.

2.5.3 Obstacle

- La descente ne fonctionne que si on peut garantir que le nouveau système $\mathcal{S}'$ conserve la propriété de **non-vérification de** $ConjecturedeGoldbach$.
- Cela nécessite de montrer que les congruences conservées dans $\mathcal{S}'$ suffisent à assurer que n' ne vérifie pas $ConjecturedeGoldbach$.

2.6 Représentation Géométrique : Maillages et Distances

2.6.1 Maillage des Décompositions

- On représente les nombres premiers comme des points dans un **maillage** où :
  - L'axe des abscisses représente les nombres premiers.
  - L'axe des ordonnées représente les nombres pairs.
- Chaque dg p de n correspond à un point (p, n) tel que $n = p + q$ avec q premier.
- Exemple : Pour $n = 24$, les dg sont $5, 7, 11, 13$, et le maillage montre les paires $(5, 19), (7, 17), (11, 13)$.

2.6.2 Distances Modulaires

- On définit deux distances pour un nombre p :
  - **Distance à 0** : $d_1(p, 0) = \prod_{q \leq \sqrt{n}} (p \pmod q)$.
  - **Distance à** n : $d_2(p, n) = \prod_{q \leq \sqrt{n}} (n - p \pmod q)^2$.
- Un dg p de n doit vérifier $d_1(p, 0) \neq 0$ et $d_2(p, n) \neq 0$.

2.6.3 Analogie avec la Physique

- La fraction 22/29 (limite supérieure de la couverture des nombres pairs par les sommes de deux premiers) correspond à l'**inverse de la densité du photon par nanomètre cube**.
- Cela suggère un lien profond entre la structure des nombres premiers et des phénomènes physiques.

3 Pistes à Approfondir

3.1 Bijections entre Solutions

3.1.1 Problématique

- Comment établir une bijection entre :
  - Les dg d'un double de nombre premier $(2p)$.
  - Les dg d'un double de nombre composé $(2c)$.
- Une telle bijection permettrait de **démontrer** $ConjecturedeGoldbach$ **pour les doubles de composés** à partir des doubles de premiers (qui vérifient trivialement $ConjecturedeGoldbach$).

3.1.2 Exemple Concret

- Pour $94 = 2 \times 47$ (premier) et $88 = 2 \times 44$ (composé) :
  - $94 = (1, 4, 3)$ dans la base $(3, 5, 7)$.
  - $88 = (1, 3, 4)$ dans la même base.
  - Le dg trivial de 94 est $47 = (2, 2, 5)$.
  - On cherche un dg de 88 dont les restes sont obtenus par permutation des restes de 47.
- Bijection proposée :
  - $\mathbb{Z}/3\mathbb{Z}$: Identité.
  - $\mathbb{Z}/5\mathbb{Z}$: Permutation $(0, 1, 2, 3, 4) \mapsto (0, 1, 4, 2, 3)$.
  - $\mathbb{Z}/7\mathbb{Z}$: Permutation $(0, 1, 2, 3, 4, 5, 6) \mapsto (0, 5, 2, 4, 3, 1, 6)$.
- Résultat : $47 \mapsto 29 = (2, 4, 1)$, qui est un d$g$ de 88 ($88 = 29 + 59$).

3.1.3 Generalisation

- Pour deux nombres pairs $n_1 = 2p$ et $n_2 = 2c$ partageant la même **base modulaire** (mêmes nombres premiers $\leq \sqrt{n}$), on peut chercher une bijection entre :
  - Les n-uplets de restes des dg de n_1.
  - Les n-uplets de restes des dg de n_2.
- La bijection doit préserver :
  - La **non-nullité** des restes.
  - L'**incongruence** avec les restes de n_2.
- Nombre de bijections possibles : $k!$ pour une base de taille k (nombre de modules).
- Comme $k!$ est très grand, il est probable qu'au moins une bijection convienne.

3.2 Systèmes d'Incongruences et Théorie de Galois

3.2.1 Formulation Algébrique

- La recherche d'un dg de n revient à résoudre un **système d'incongruences** :

$$\begin{cases} p \not\equiv 0 \pmod{q} \\ p \not\equiv n \pmod{q} \end{cases} \qquad \forall q \text{ premier} \leq \sqrt{n}.$$

- Cela équivaut à chercher les racines communes de deux polynômes :
  - $P(x)$: Polynôme dont les racines sont les nombres premiers $\leq n$.
  - $Q(x) = P(n - x)$: Polynôme dont les racines sont les complémentaires à n des nombres premiers.
- Les dg de n sont les racines communes de $P(x)$ et $Q(x)$.

3.2.2 Nullité du Résultant

- Deux polynômes P et Q ont des racines communes si et seulement si leur **résultant** est nul.
- Le résultant est le déterminant de la **matrice de Sylvester** associée à P et Q.
- Pour $n = 6$, on a :

$$P(x) = (x-3)(x-5), \quad Q(x) = (x-1)(x-3).$$

  Le résultant est $(n-6)(n-8)^2(n-10)$, qui s'annule bien pour $n = 6, 8, 10$.
- Pour $n = 8$ ou 10, le résultant se factorise en :

$$-(n-6)(n-8)^2(n-10)^3(n-12)^2(n-14),$$

  qui s'annule pour $n = 8, 10, 12, 14$.
- **Observation clé** : Les facteurs $(n-2p)$ (pour p premier) apparaissent avec une **puissance impaire**, tandis que les facteurs $(n-2c)$ (pour c composé) apparaissent avec une **puissance paire**.

3.2.3 Implications pour *ConjecturedeGoldbach*

- Si on pouvait montrer que pour tout $n \geq 4$, le résultant de P et Q s'annule, alors *ConjecturedeGoldbach* serait démontrée.
- Le résultant contient toute l'information sur les décompositions de Goldbach des nombres pairs compris entre deux nombres premiers successifs.
- **Piste** : Montrer que le nombre de racines du polynôme résultant inférieures à n est toujours supérieur au nombre de nombres pairs $\leq n$ à couvrir.

3.3 Approche Combinatoire : Mots de Restes et Anagrammes

3.3.1 Analogie avec les Anagrammes

- Les nombres sont représentés comme des mots de restes.
- Un dg de n est un mot qui :
  - Ne contient pas de lettre nulle (pour être premier).
  - Ne partage aucune lettre avec le mot de n (pour que $n-p$ soit premier).
- Exemple : Pour $n = 98 = (0, 2, 3, 0)$ (base $(2, 3, 5, 7)$), le mot $19 = (1, 1, 4, 5)$ est un dg car :
  - Aucune lettre nulle.
  - Aucune lettre commune avec $(0, 2, 3, 0)$.

3.3.2 Diagonale de Cantor et Infinitude des Jumeaux

- Pour démontrer l'infinitude des nombres premiers jumeaux, on utilise une **diagonale de Cantor** :
  - Supposons que l'ensemble des nombres premiers jumeaux cadets (le plus petit des deux jumeaux) est fini : Cadets $= \{c_1, \ldots, c_k\}$.

- À chaque c_i, on associe son ensemble de restes modulo les nombres premiers $\leq c_k + 2$.
- On construit un nouvel ensemble de restes **non recensé** en perturbant la diagonale du tableau des restes.
- Cela fournit un nouveau nombre premier jumeau cadet non dans Cadets, d'où une contradiction.

- **Application à** *ConjecturedeGoldbach* : Une approche similaire pourrait être utilisée pour montrer que l'ensemble des dg est infini pour chaque n.

3.4 Fonctions Arithmétiques et Récurrence

3.4.1 Somme des Diviseurs et *ConjecturedeGoldbach*

- Euler a découvert une **loi récursive** pour la somme des diviseurs $\sigma(n)$:

$$\sigma(n) = \frac{12}{n^2(n-1)} \sum_{k=1}^{n-1} \left(5k(n-k) - n^2\right) \sigma(k)\sigma(n-k).$$

- Les nombres premiers sont des **minima locaux** de $\sigma(n)$ ($\sigma(p) = p + 1$).
- Les dg de n minimisent $\sigma(p) + \sigma(n-p)$, avec $\sigma(p) + \sigma(n-p) = n + 2$.
- **Piste** : Utiliser cette récurrence pour trouver un dg de n en résolvant :

$$\sigma(p) + \sigma(n-p) - n - 2 = 0.$$

3.4.2 Indicatrice d'Euler et *ConjecturedeGoldbach*

- L'indicatrice d'Euler $\varphi(n)$ compte le nombre d'unités modulo n.
- Les dg de n sont parmi les $\varphi(n)/2$ unités $\leq n/2$.
- **Piste** : Étudier la distribution des unités qui ne partagent aucun reste avec n.

3.5 Approche par les Groupes et Symétries

3.5.1 Structure des Groupes des Unités

- Pour $n = 2p$ (double d'un premier), le groupe des unités quotienté par $\{-1, 1\}$ est cyclique de taille $p - 1$.
- Pour $n = 2c$ (double d'un composé), la structure dépend de la factorisation de c.
- Exemple :
  - $n = 14 = 2 \times 7$: Groupe C_3.
  - $n = 16 = 2^4$: Groupe C_4.
  - $n = 60 = 2^2 \times 3 \times 5$: Groupe $C_4 \times C_2$.
- **Piste** : Montrer qu'il existe un isomorphisme entre les groupes des unités de $2p$ et $2c$ pour certains c, ce qui permettrait de transférer l'existence de dg.

3.5.2 Racines de l'Unité et *ConjecturedeGoldbach*

- Si une unité u vérifie $u^k = -1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$, alors u^{k+1} est un dg de n (car $n - u = -u = (-1) \cdot u$).
- **Piste** : Montrer que pour tout $n \geq 4$, il existe une unité $u \leq n/2$ telle que $u^k = -1$ pour un certain k.

4 Synthèse des Résultats Partiels

4.1 Résultats Algorithmiques

- **Double crible d'Ératosthène** :
  - Permet de trouver efficacement les dg pour des nombres pairs jusqu'à 10^6.
  - Complexité : $O(n \log \log n)$ (similaire au crible classique).
- **Représentation par les restes** :
  - Fournit une caractérisation précise des dg.
  - Permet de générer des candidates solutions via TRC.

4.2 Résultats Théoriques

- **Équivalence avec les systèmes d'incongruences** :

$$ConjecturedeGoldbach \iff \forall n \geq 4, \exists p \leq n/2, \forall q \leq \sqrt{n}, p \not\equiv 0, n \pmod{q}.$$

- **Lien avec le résultant** :
  - Le résultant des polynômes P (racines = nombres premiers) et $Q(x) = P(n-x)$ contient toute l'information sur les dg de n.
  - Les facteurs $(n - 2p)$ apparaissent avec une puissance impaire, tandis que les facteurs $(n - 2c)$ apparaissent avec une puissance paire.
- **Descente infinie** :
  - Si un nombre n ne vérifie pas *ConjecturedeGoldbach*, il existe un nombre $n' < n$ qui ne vérifie pas non plus *ConjecturedeGoldbach* (sous certaines conditions).

4.3 Résultats Combinatoires

- **Infinitude des nombres premiers jumeaux** :
  - Démonstration par diagonale de Cantor dans l'espace des mots de restes.
  - Utilisation de la primorielle pour borner les intervalles.
- **Fonction** $f(n, p)$:
  - Compte le nombre de cases colorées dans les grilles de divisibilité.
  - Pour $n = 2p$, $f(2p, q) = f(2p - 2, q)$ ou $2f(2p - 2, q)$.
  - Pour $n = 2j$ (jumeau), $f(2j, q) = f(2j - 2, q)$ ou $(f(2j - 2, q) + 1)/2$.
  - Suggère une similitude entre nombres premiers et pères de jumeaux.

5 Propositions pour Aller Plus Loin

5.1 Priorités de Recherche

- **Formaliser les bijections entre solutions** :
  - Prouver que pour toute paire $(2p, 2c)$ partageant la même base modulaire, il existe une bijection entre leurs dg.
  - Utiliser la théorie des groupes pour construire explicitement ces bijections.
- **Approfondir le lien avec la théorie de Galois** :
  - Étudier les permutations des racines des polynômes P et Q pour montrer que leur résultant s'annule toujours.
  - Exploiter les propriétés des groupes de Galois pour garantir l'existence de racines communes.
- **Démontrer la descente infinie** :
  - Montrer que si un nombre n ne vérifie pas $ConjecturedeGoldbach$, alors il existe un nombre $n' < n$ qui ne vérifie pas non plus $ConjecturedeGoldbach$, en utilisant les propriétés du TRC.
  - Formaliser la condition de conservation des incongruences lors de la réduction du système.
- **Étudier les fonctions arithmétiques** :
  - Utiliser la récurrence de $\sigma(n)$ pour construire un algorithme de recherche de dg plus efficace.
  - Explorer les liens entre $\sigma(n)$ et la conjecture de Goldbach.
- **Explorer les analogies physiques** :
  - Approfondir le lien entre la fraction 22/29 et la densité du photon.
  - Étudier les implications pour la théorie des nombres.

5.2 Collaborations et Outils

- **Collaborations** :
  - Travailler avec des experts en théorie de Galois pour formaliser les liens avec les systèmes d'incongruences.
  - Collaborer avec des informaticiens pour optimiser les algorithmes de crible et de TRC.
- **Outils** :
  - Utiliser des logiciels comme **GAP** ou **SageMath** pour tester les bijections et les systèmes de congruences.
  - Développer des visualisations interactives des maillages et des mots de restes.

5.3 Questions Ouvertes

- Peut-on démontrer que le résultant des polynômes P et Q s'annule pour tout $n \geq 4$?
- Existe-t-il une bijection universelle entre les dg des doubles de premiers et ceux des doubles de composés ?
- Comment généraliser la descente infinie pour couvrir tous les cas ?
- Peut-on utiliser la théorie des groupes pour montrer que les groupes des unités de $2p$ et $2c$ sont isomorphes pour certains c ?
- La fraction 22/29 a-t-elle une signification profonde en théorie des nombres ?

6 Conclusion

Les travaux de Denise Vella-Chemla offrent une **approche unifiée et originale** pour aborder la conjecture de Goldbach et celle des nombres premiers jumeaux. Les idées clés à retenir sont :

- La **représentation des nombres par leurs restes modulaires** permet une formulation précise et combinatoire des conjectures.
- Le **théorème des restes chinois** est un outil central pour générer des solutions et étudier les systèmes d'incongruences.
- Les **bijections entre solutions** pour différents types de nombres pairs pourraient fournir une preuve constructive de $ConjecturedeGoldbach$.
- Les **liens avec la théorie de Galois** et les groupes finis ouvrent des pistes prometteuses pour une démonstration théorique.
- La **descente infinie de Fermat** et les **maillages géométriques** offrent des perspectives géométriques et algébriques complémentaires.

Pour avancer, il est crucial de :

- **Formaliser les bijections** entre les solutions pour les doubles de premiers et les doubles de composés.
- **Approfondir les liens avec la théorie de Galois** pour exploiter les propriétés des groupes et des polynômes.
- **Démontrer rigoureusement la descente infinie** en utilisant les propriétés du TRC.
- **Explorer les fonctions arithmétiques** comme $\sigma(n)$ et $\varphi(n)$ pour trouver de nouvelles caractérisations des dg.

Comme le disait Hilbert : *"Wir müssen wissen, wir werden wissen"* ("Nous devons savoir, nous saurons"). Les travaux présentés ici montrent que la route est longue, mais les pistes sont nombreuses et prometteuses.

Annexes

Notations et Définitions

- $\mathbb{N}$: Ensemble des entiers naturels.
- $\mathbb{Z}$: Ensemble des entiers relatifs.
- $\mathbb{P}$: Ensemble des nombres premiers.
- dg : Décomposant de Goldbach.
- $ConjecturedeGoldbach$: Conjecture de Goldbach.
- $Conjecturedesnombrespremiersjumeaux$: Conjecture des nombres premiers jumeaux.
- TRC : Théorème des Restes Chinois.
- $n \pmod m$: Reste de la division euclidienne de n par m.
- $\varphi(n)$: Indicatrice d'Euler (nombre d'unités modulo n).
- $\sigma(n)$: Somme des diviseurs de n.

Références Clés

- Gauss, C.F. *Recherches Arithmétiques* (1807).
- Euler, L. *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs.*
- Zagier, D. *A One-Sentence Proof That Every Prime* $p = 1 \mod 4$ *Is a Sum of Two Squares* (1990).
- Oliveira e Silva, T. Vérification de $ConjecturedeGoldbach$ jusqu'à 4×10^{18} (2012).
- Bruter, C.P. *Arithmétique et Cryptologie* (2012).