Questions d'examen

1. Les principes de la numération orale.

2. Les principes de la numération écrite.

3. Les systèmes de numération historiques (sauf: mésopotamien).

4. Système de numération, arithmétique et tables de calcul en Mésopotamie.

5. Algèbre mésopotamienne.

6. Triangles rectangles rationnels.

7. Algèbre grecque I: l'*Arithmetica* de Diophante (caractères généraux); représentation des nombres comme sommes et différences de deux carrés; méthode d'approximation ("V",9).

8. Algèbre grecque II: Systèmes de deux équations linéaires indéterminées.

9. Le problème de Waring.

10. Mesure de la Terre. Les nombres premiers en Grèce.

11. Développements ultérieurs utilisant des découvertes grecques.

12. Conjectures sur les premiers. Quantité et somme des diviseurs.

13. Les nombres parfaits.

Attention aux dates historiques!

P.-S.: DMA, 2^{e} étage, MA 232.

1) Principes num. orale

- préliminaire : vers nb ⟶ num. orale
  ↓
  - faculté reconnaître si nid manque œuf
  - guêpe : ~20
  - homme : ~4 à 7
- num. orale : – degrés abstraction a) comp. ensemble
  b) abstract. nature objets
  — syst. comptage (p.ex. cailloux = soldats)
  — ⊕ grd. unités (p.ex. boîtes p. ranger cailloux)
  c) base syst. num. p.ex. 10, 2, 4, 8, 3, 20, 60 ...
  + explic.

---

2) Princip. num. écrite

intro : cf. 1).

n écrite : – évolution idéale a) 100 100 100 10 10 1 1 1 1 = 324 ⓐ
b) 3·100 + 2·10 + 4 ⓑ
c) 324 ⓒ

– choix base : a) # symboles à mémoriser ↓
b) 1 nb : # symboles à écrire ↓
c) bcp. diviseurs (pour des raisons pratiques)
d) peu de produits à mémoriser (table multiplic.)
↳ base h : $\#_{\text{mémoriser}} = \frac{1}{2}(h-2)\cdot(h-1)$

– évolution en pratique : – dépend de : a) exist. bases utilisées ultérieur.
b) matériau (support) d'écriture
c) événements politiques
d) structure de la langue + son évolution

---

3) Systèmes de numération historique

Intro : – évolution des syst. numération : – théorie ... cf. 2)
– pratique ... cf. 2)

(– développement de l'écriture cunéiforme : ⟶ pictographique (dessins) (2000)
⟶ combinaison de dessins
⟶ écriture syllabique + diminution nb signes 2000 ⟶ 800
⟶ rotation π/2 ‡ ⟶ +++
⟶ déformation des signes (écrits avec poinçons : abstraction))

– Egyptien : – décimal
– puissances de 10 ≡ dessins (1 mio ≡ 𓁨 (dieu de l'infini)) ⓐ
⟶ s/ pierre
⟶ s/ papyrus
– simplification ultérieure : dessin / III nb. bâtons ≡ nb. fois que dessin apparaît.

– Grec : ~~300~~
i) Ancien : méthode ⓐ
ii) Classique : – vers ~ – 300
– 9 unités, 9 dizaines, 9 centaines, + , devant signe ⟶ ·10³
– ex : ΓΞΟΔ

- indiens : i) — Kharoshti : —
  ii) — Brahmi : — plus répondu
  — 1er syst. positif
  — +595 : 300 40 5 ⟶ 345 : positif. Pourquoi ? Hyp : se servaient de tables de calcul

9	7	α	— ← puis. de 10
≡	?	n	ψ ...

⟶ migration du syst. indien :
i) ~770 : savants indiens ⟶ Bagdad : connaît le syst. à l'extérieur
ii) ~820 : Al-khwarizih écrit un arith. indienne à l'ext. inde
iii) ~1'000 : apices : chiffres ramenés en Espagne
iv) 1150 : conquête chrétienne de l'ESP. ⟶ Al-khwarizih ≡ algorithmi
v) ~13ès : chiffres "arabes" utilisés par les marchands ⟶ se répand

- maya : — signe pour le zéro, mois à 20 jours
- Chinois : — importance : illustre 1è simplification d'écriture avec coeff. pour compter les puissances de la base : 4879 = 4.1000 + 8.100 + 7.10 + 9.1
- Romain : — symboles et 1h symboles : X = 10 ; C = 100
  V = 5 ; L = 50 ...

---

4) Mésopotamien : syst. num., arithmétique, tables de calcul

i) Syst. numération : a) Syst. ancien : — -3'100 ~ -2'200 O o, D, D
— signes avec 2 triges de ∅ différent ; stade (a) ⟶ signes répétés
— base 60 : astronomie
⟶ repris par Arabes ⟶ Europe ⟶ degrés, min, ~~heures~~ secondes idem b. 60.

b) Syst. classique : — vers ~ -2'200
— 2 symboles ▽ = 1 ou 60^k ; ≪ = 10 ou $60^k.10$
— syst. positif
— exemple : ▽▽▽ ≪ ▽▽▽ ▽▽ = 3.60+18 = 3,18
— zéro ≡ esp. blancs ⟶ problème !

ii) Tables de calcul : — addition, soustraction : ∄ table
— multiplication, division : ∃ tables (mult : cf. 1 2 3 ...)
— division : table d'inverses : nbrs rationnels à dév. fini.
ex : 2 30 t.q. 2. 20/60 = 1
3 20 t.q. 3. 20/60 = 1

---

5) Algèbre mésopotamienne

Introduction : — syst. numération :
— syst. classique : ~ -2'200 ; sexagésimal, positif

Algèbre : — possibilités de résolution : — systèmes d'ordre 1
— éqn. ordre 2
— systèmes ordre 2
— méthode : i) chgt. de variable
ou ii) substitution inc. éqn. 1 ⟶ éqn. 2.

— propriété : — des textes : chaque étape de calcul est détaillée sans supposer que le lecteur sache faire les manipulations algébriques lui-même.

- exemples : - syst. éqn. 1er ordre : $\begin{cases} x \pm y = k & 1) \\ ax + by = e & 2) \end{cases}$

$\exists$ 2 procédés : i) chgt. var : $z = \frac{x \pm y}{2}$

ii) substit. 1 inc. de éqn. 1) dans 2)

- éqn. degré 2 : i) $ax^2 + bx = c$ $\rightarrow x = \ldots$

ii) $ax^2 = bx + c$ $\rightarrow x = \ldots$

iii) $ax^2 + c = bx$ $\rightarrow x = \ldots$

— Conditions : i) sol. $\in \mathbb{Q}^+$

ii) $a, b, c > 0$

⚠ pratiquement : $p/2 \rightarrow (p/2)^2 \rightarrow (p/2)^2 + q \rightarrow \sqrt{(p/2)^2 + q} \rightarrow \sqrt{(p/2)^2 + q} - \frac{p}{2} = x$

$x^2 + px = q$

- syst. degré 2 : — usage d'identités pour la résolution

i) $\begin{cases} x+y = p \\ x \cdot y = q \end{cases}$ $\left(\frac{x+y}{2}\right)^2 - x \cdot y = \left(\frac{x-y}{2}\right)^2 \rightarrow x = \frac{x+y}{2} + \frac{x-y}{2}$, $y = \frac{x+y}{2} - \frac{x-y}{2}$

ii) $\begin{cases} x^2 + y^2 = p \\ x \cdot y = q \end{cases}$ $\frac{x^2+y^2}{4} \pm \frac{x \cdot y}{2} = \left(\frac{x \pm y}{2}\right)^2 \rightarrow \ldots$

iii) $\begin{cases} x^2 + y^2 = p \\ x + y = q \end{cases}$ $\frac{x^2+y^2}{2} - \left(\frac{x+y}{2}\right)^2 = \left(\frac{x-y}{2}\right)^2 \rightarrow \ldots$

6. Triangles rectangles rationnels

Introduction : — but : — résolution de $x^2 + y^2 = z^2$ dans $\mathbb{Q}$ ($\rightarrow$ dém. Euclide)

— origine : — trouver x t.q. $\ell \begin{cases} \\ \\ \end{cases}$  $\rightarrow x = \ldots$? (planche posée contre mur)

Démarche : i) solution $\in \mathbb{Q} \Rightarrow \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2 = \left(\frac{e}{f}\right)^2 \Rightarrow (adf)^2 + (cbf)^2 = (ebd)^2$

ii) Choix sol : a) $\in \mathbb{N}$

b) solutions fondamentales (autres : obtenues par multiplic. de la sol.)

iii) $\Rightarrow$ élimination de sol. par quelles de parité $\Rightarrow$

x	y	z
p	i	i

iv) $\Rightarrow x^2 = z^2 - y^2 = \underbrace{\left(\frac{z}{i} + \frac{y}{i}\right)}_{p} \cdot \underbrace{\left(\frac{z}{i} - \frac{y}{i}\right)}_{p}$

$\Rightarrow \left(\frac{x}{i}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right)$

v) terme de droite $\equiv$ carré d'entier $\Rightarrow \begin{cases} \frac{z+y}{2} = s \cdot u^2 \\ \frac{z-y}{2} = s \cdot v^2 \end{cases}$

vi) $\Rightarrow \{x, y, z\} = \{2suv,\ s(u^2 - v^2),\ s(u^2 + v^2)\}$

vii) Sol. générale : $s = 1 \Rightarrow \exists \infty$ sol. $\{u, v\} \in \mathbb{N}$ premiers entre eux

Historique : — tablettes mésopotamiennes retrouvées avec des couples $\{x, y, z\} \in \mathbb{N}$ t.q. $x^2 + y^2 = z^2$.

— datée de $\sim -1'800$ à $\sim -2'500$

7) Algèbre grecque I : Arithmetica, sommes et différences de □, méthode d'approximation

Intro :

- algèbre de Diophante : — importance car : i) — donne naissance au 17e à la th. nombres (Fermat), Gauss au 18e.
  ii) seul reste conservé d'une algèbre en grec

Arithmetica : — Σ = 13 livres, 10 conservés ; recueil de problèmes avec remarques théoriques
- présentation des pb. i) solutions ∈ ℚ⁺
  ii) symbolisme algébrique (x^2...) et abstraction des énoncés
  iii) résolution : → égalités entre puissances voisines (k et $k \pm 1$)

→ présentation "moderne" des pb.
- écriture : syst. num. grecque

Sommes et diff. □ : — méthode : — va être amené à résoudre des éqn. du type : $ax^2 + bx + c = \square$
→ tjs résolubles ds cas : (astuces algébriques)

i) $\{a = 0, c \neq 0\}$, $\{a \neq 0, c = 0\}$
↓
$\square = m^2 \cdot x^2$

ii) a carré ou c carré : $a^2 \cdot x^2 + bx + c = \square \Rightarrow \square = (ax+n)^2$
$ax^2 + bx + c^2 = \square \Rightarrow \square = (mx+c)^2$

- pb du livre (II) : i) $u^2 + v^2 = k^2$ → $\begin{cases} u = x \\ v = mx - k \end{cases}$ → Fermat : $n \geq 3$ ∄ sol. ∈ ℚ.

ii) $u^2 + v^2 = k$ t.q. $k = k_1^2 + k_2^2$ → $\begin{cases} u = x + k_1 \\ v = mx - k_2 \end{cases}$

iii) $u^2 - v^2 = k$ → $\begin{cases} u = x + m \\ v = x \end{cases}$

iv) $\frac{u^2 - v^2}{v^2 - w^2} = k$ → $\begin{cases} u = x + m \\ v = x + 1 \\ w = x \end{cases}$

Méthode d'approx. : — problème : $\begin{cases} u + v = 1 & (1) \\ u + k = \square & (2) \\ v + k = \square' & (3) \end{cases}$ → $\square = \ldots$, $\square' = \ldots$ (2 carrés proches)

- cond. : i) k pair
  ii) $2k+1$ pas divisible par $x = 4m+3$

→ explic. hyp : • (2) + (3) avec (1) ⇒ $1 + 2k = \square + \square'$
• k impair : $k = 2t + 1$ → $4t + 3 = \square + \square'$ ↯ car :
$\xi = \square + \square' \iff \forall p_i$ de la forme $4m+3$, α_i pair

- méthode : (2) et (3) ⇒ $\begin{cases} \square > k \\ \square' < k+1 \end{cases}$ ⇒ ∃ 2 carrés dans $[k, k+1]$

• p. ex. $k = 6$ → recherche un carré proche de $k + 1/k$:
$k + \frac{1}{2} + p^2 = \square$ + astuces algébr.

8) Algèbre grecque II : Syst. 2 éqn. indéterminées

Intro : cf. 7

Arithmetica : – cf. 7
– livres 4,5 : syst. 2 éq. indéterm.

Méthodes résolution livre 2 : i) $u^2+v^2=k^2$
ii) $u^2+v^2=k$ t.q. $k=k_1^2+k_2^2$
iii) $u^2-v^2=k$
iv) $\frac{u^2-v^2}{v^2-w^2}=k$
} cf. 7

Syst. 2 éqn. : – pb. : $\alpha_1 x^{k+1} + \beta_1 x^k = \square$
$\alpha_2 x^{k+1} + \beta_2 x^k = \square'$

→ k pair : $\cdot \frac{1}{x^k}$
↘ k impair : $\cdot \frac{1}{x^{k+1}}$

$\Rightarrow \begin{cases} a_1 x + b_1 = \square & (1) \\ a_2 x + b_2 = \square & (2) \end{cases}$

– Cas : a_1, a_2 du rapport de 2 $\square$: $a_1 = s\cdot u^2$, $a_2 = \pm s\cdot v^2 \Rightarrow a_2 = \frac{u^2}{t^2}\cdot a_1$

$\Rightarrow \begin{cases} q^2 a_1 x + b_1 q^2 = \square & (1) \\ q^2 a_1 x + b_2 = \square' & (2) \end{cases}$

i) a_1, a_2 même signe $\Rightarrow$ $(1)-(2)$ $\Rightarrow$ iii) (méthode iii)
ii) a_1, a_2 signe différent $\Rightarrow$ $(1)+(2)$ $\Rightarrow$ ii) si $k = k_1^2 + k_2^2$
iii) b_1^2, b_2^2 (b_1, b_2 sont des carrés) $\Rightarrow (1)\cdot b_2^2 + (2)\cdot b_1^2 \Rightarrow$ iv)

---

9) Pb. Waring

Intro :

– Pb : i) représentation d'un naturel comme somme de n puissances d'entiers : $N = \sum_{i=1}^{g(N)} x_i^k$, k = cte
ii) pour une puissance k fixée, $\exists$ une borne supérieure pour le nb. de termes : $\forall N\ g(N) \leq g(k)$.

– conjecture Waring (1770) : $\forall n \in \mathbb{N}$ on n'a besoin d'un nb. limité de coefficients associés à la puissance k pour représenter n.

$k=2$: • Lagrange 1770 : $g(2)=4$; $G(2)=g(2)$
• dém : $N = \prod_{i=1}^{e} p_i^{\alpha_i}$, $p_i = \{2, 4m+1, 4m+3\}$

→ $p_i = 4m+1 \Rightarrow p_i = \sum_{k=1}^{2} n_k^2$
↘ $p_i = 4m+3 \Rightarrow p_i = \sum_{k=1}^{3,4} n_k^2$
} dans $N = \prod$ et développer $\Rightarrow N = \sum_{i=1}^{\beta < \infty} u_i^2$

$k=3$ • Wieferich 1909 : $g(3)=9$, $G(3) \leq 7$
• démarche : – calculateurs prodige (Zarnow, Dase)

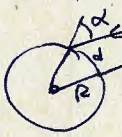
$k=4$: • Ordinateur, 1985 : $g(4)=19$, $G(4)=16$
• Historique : • Cranville : $g(4) \leq 53$; Wieferich (1909) : $g(4) \leq 37$; Hardy & Littlewood (1925) : $g(4) \leq 21$
• 1970 $g(4)=19$ prouvé $\forall N \notin [10^{310}; 10^{1409}] = I$
$\Rightarrow$ 1985 ordinateur : vérification que $g(4)=19\ \forall N \in I$ #

Johan-Albrecht (fils Euler) : $g(k) \leq 2^k \cdot E\left[\left(\frac{3}{2}\right)^k\right] - 2$
(1772)
— vrai sauf par nb. $< \infty$ de k
— résultat exact pour $k \leq 5$.

10) Mesure de la terre — nb. premiers en grèce

i) Mesure de la terre : — représentation :
~ -450 : école pythagore : terre ≡ ronde
~ -450;-330 : Preuves : i) navires sortant H2O ⇒ courbure
ii) marins : constellations changes si déplace N→S
iii) éclipses de lune : bord circulaire ombré de la terre vu sur la lune

— mesure du rayon : Eratosthène -235



— 2 villes sur m. méridien : solstice été :
• Assuan : soleil reflété fond puits
• Alexandrie : mesure de angle des γ avec la verticale
⟶ erreur relative à la valeur exacte : ~0,1 %

ii) nb. premiers en Grèce : — origine : — école de pythagore (~ -580 à -520) "secrète" + mystérieux nb.
⟶ élève : Euclide
⟶ ses écrits connus.

— déf. nb. premier + déf. moderne.

— Thm Euclide : — tout nb. composé est divisé par un nb. premier
— $\mathbb{P}$ infini des nb. premiers réels : $\text{card}\,\mathbb{P} = \infty$
↳ dém : $\alpha = \prod_{i=1}^{e} p_i + 1$ ⟶ α premier
⟶ α pas premier
⇒ α composé
⇒ $\exists h$ t.q. h premier et $\frac{\alpha}{h} \in \mathbb{N}$
⇒ développer et ad absurde
$h \in \{p_1, \dots, p_e\}$

— crible Eratosthène (~-250) : {impairs} : $3 + k \cdot 3$ biffé, $5 + k \cdot 5$ biffé, ... $k \geq 1$.

11) Développ. ultérieurs utilisant des découvertes grecques

Intro : — vers 17è - 19è siècle
— étude des nb. premiers

premiers jusqué à N : • $\Pi(N) = N - D(N) + \Pi(\sqrt{N}) - 1$
avec : $D(N) =$ # nb. jusqu'à N qui sont divisibles par les premiers $p_1 \dots p_e$ jusque à $\sqrt{N}$

$$= \sum_{i=1}^{e} \left[\frac{N}{p_i}\right] - \sum_{\substack{i,j=1 \\ i \neq j}}^{e} \left[\frac{N}{p_i \cdot p_j}\right] + \dots + (-1)^{e+1} \left[\frac{N}{\prod_{i=1}^{e} p_i}\right]$$

densité de nb. premiers : — espacement moyen entre 2 premiers ↑ si les nb. ↑.

Lejeune-Dirichlet : 1850 : $a + k \cdot b$, a, b premiers entre eux ⟶ $\exists \infty$ premiers de cette suite

Polynôme de Euler : 17è : $X^2 - X + 41$, $X = 1, \dots, 40$ ⟶ premier à coup sûr
(formule à premiers) ; $X^2 - 79X + 1601$ ⟶ $X = 1, \dots, 79$

∞ de nb. premiers de la forme $4n+3$ ≡ extension de la dém. d'Euclide $\text{card}(P_i) = \infty$.

• dém: $\alpha = 4 \cdot \prod_{i=1}^{e} p_i - 1 = 4\underbrace{\left(\prod_{i=1}^{e} p_i - 1\right)}_{n} + 3$

i) α premier → Petit ☺

ii) α composé → hypothèse: • e premiers de la forme $4n+3$
• tous les premiers sont de la forme $\{2, 4n+1, 4n+3\}$

→ voit: $\frac{\alpha}{2} \notin \mathbb{N}$, $\frac{\alpha}{4n+1} \notin \mathbb{N}$

→ par divisible par $4n+1$ ⇒ nouveau premier de la forme $4n+3$

---

12) Conjectures ∀ premiers. Qtité et somme des diviseurs

Intro: étude des premiers: • école pythagore: ~ −500 → Euclide (∞ de premiers)
• 17e: – ∃∞ premiers de la forme $4n+3$
– Lejeune-Dirichlet: 1'850: $a+kb$, a,b p. entre eux → ∞ prem.

Qq. nq résolues: i) → ∃∞? de premiers jumeaux
– ∃∞? premiers (n^2+1), n pair
– " (2^n-1)
– " (2^n+1)

ii) Conjectures: – Goldbach (1842): $n \geq 4$: $n \overset{\text{pair}}{=} \alpha+\beta$; $n \geq 7$: $n \overset{\text{impair}}{=} \alpha+\beta+\gamma$
– Polignac (1842): $n \overset{\text{pair}}{=} x_i - x_j$, x_i, x_j premiers conséc.

Qtité et Σ des diviseurs ($\nu(N)$, $\sigma(N)$): i) $\nu(N)$; $N = \prod_{i=1}^{e} p_i^{\alpha_i}$ → $\nu(p_1^{\alpha_1}) = \alpha_1 + 1$
→ $\nu(N) = \prod_{i=1}^{e} (\alpha_i + 1)$

ii) $\sigma(N)$; → $\sigma(p_1^{\alpha_1}) = \sum_{i=0}^{\alpha_1} p_1^i = \frac{1 - p_1^{\alpha_1+1}}{1-p_1}$
→ $\sigma(N) = \prod_{i=1}^{e} \left(\frac{1 - p_i^{\alpha_i+1}}{1-p_i}\right)$

Rem: – $\nu(N)$ donné → ∃ $N \in \mathbb{N}$ t.q. N a exact. $\nu(N)$ diviseurs
– preuve: – développer $\nu(N)$, et a vu: autant de décomp. de $\nu(N)$ que de déc. canon. de N.

---

13) Nb. Parfaits

Intro: – étude des nb.: • école pythagore ~ −500 → Euclide
• Pythagore: "él. premier univers ≡ nb." ⇒ mystique du nb.
⇒ nous: dénominations: parfait, premier, amicable, abondant, déficients

Déf: – $\nu(N)$; $\sigma(N)$
– somme des diviseurs hormis lui-même: $s(N) = \sigma(N) - N$
– parfaits, déficients, abondants
– nb. mersenne

Thm :- Euclide : $M_n = 2^n - 1 \Longrightarrow 2^{n-1}\cdot\underbrace{(2^n-1)}_{=M_n} = N$ parfait

- **Preuve :** à var : $\sigma(N) = N \Rightarrow 2\cdot N = \sigma(N)$

  • $\sigma(N) = \underbrace{\sigma(2^{n-1})}_{2^n-1}\cdot\underbrace{\sigma(2^n-1)}_{1+(2^n-1)=2^n} = 2^n\cdot(2^n-1) = 2\cdot N$ #

⟹ recherche nb. parfaits ≡ recherche nb. mersenne M_n avec les critères :

i) n premier

ii) Critère de Lucas : $V_1 = 4$; $M_n \geq 2 \Leftrightarrow M_n$ divise V_{n-1} ; $V_k = V_{k-1}^2 - 2$
(form. récurrence)

Rem : forme des nb. parfaits pair / impairs :

- +1750 : Euler montre que Parfait pair $\Leftrightarrow 2^n(2^n-1)$

  Preuve : $\Rightarrow$) évident

  $\Leftarrow$) $2^{n-1}\cdot(2^n-1) \sim 2^n\cdot a \rightarrow \sigma(\underbrace{2^k a}_{N}) = \ldots = 2N$

  $\rightarrow a = \ldots$

- question : $\exists$ M_n impair ? Pas encore trouvés, mais pas démontré que $\nexists$ de tels nb.

Théorème: – soit $\mathbb{P}$ l'ensemble des nb. premiers, alors $\text{card}(\mathbb{P}) = \infty$.

Preuve: – soit $(p_1, \dots, p_\ell)$ une quantité finie de nb. premiers, i.e. $\ell < \infty$, soit :

$$\alpha = 1 + \prod_{i=1}^{\ell} p_i$$

– alors $\exists$ 2 alternatives pour α

i) α est premier, alors on a montré que avec $\ell < \infty$ nb. premiers on a pu en trouver un autre, i.e. on a formé $\ell+1 < \infty$ premiers.

ii) α n'est pas premier, alors on sait que, par un autre thm. d'Euclide, c'est un nb. composé, donc $\exists h$ t.q. $\alpha / h \in \mathbb{N}$ t.q. h est premier

Supposons que $h \neq \{p_1, \dots p_\ell\}$, alors on a montré que avec $\ell < \infty$ nb. premiers, on en a découvert un nouveau, i.e. on a $\ell+1 < \infty$ nb. premiers.
Démontrons cette dernière supposition: par l'absurde, supposons que $\exists p_i$, $i = 1, .., \ell$ t.q. $h = p_i$, alors :

$$\frac{\alpha}{h} = \frac{1 + \prod_{i=1}^{\ell} p_i}{h} = \frac{1}{h} + \frac{\prod_{i=1}^{\ell} p_i}{h} \in \mathbb{N}$$

avec :

$$\frac{\prod_{i=1}^{\ell} p_i}{h} = \prod_{\substack{i=1 \\ i \neq k}}^{\ell} p_i \in \mathbb{N} \text{ t.q. } p_k = h$$

$$\Rightarrow \frac{1}{h} = \frac{1}{p_k} \in \mathbb{N}$$

Mais comme p_k est premier, alors $1/p_k \notin \mathbb{N} \Rightarrow \lightning \Rightarrow \nexists k$ t.q. $p_k = h$
$\Rightarrow h$ est un nouveau premier.

Conclusion : i) et ii) $\Rightarrow \forall p_1, .., p_\ell$, $\ell < \infty$ on peut former un nouveau premier h t.q. $h \notin \{p_1, .., p_\ell\} \Rightarrow$ on a $\ell+1$ premiers, et en posant $\ell := \ell+1$, alors si $\ell \to \infty$ on trouve que $\exists \infty$ de premiers ⁂

Problème de Waring: développement : $k=2$

(Pour $k=2$, alors Diophante a déjà montré que $\forall n \in \mathbb{N}$, $\exists q_i \in \mathbb{Q}$ t.q. $N = \sum_{i=1}^{k} q_i^2$, $k \in [1,4]$) pas nécessaire (1)

Soit la décomposition canonique:

$$N = \prod_{i=1}^{e} p_i^{\alpha_i} \tag{2}$$

$$p_i = \{2, 4m+1, 4m+3\} \tag{3}$$

Par exemple pour les valeurs de p_i :

2 ; $4m+1$: $\{1, 5, 9, \dots\}$
$4m+3$: $\{3, 7, 12, \dots\}$

Une autre identité démontrée par Fermat qui va nous être utile:

$$\forall N \text{ t.q. } N = 4.m+1, \quad N = \sum_{k=1}^{2} n_k^2, \quad n_k \in \mathbb{N} \tag{4}$$

Cela permet d'écrire que $\forall p_i$ t.q. $p_i = 4.m+1$, alors $p_i = \beta_{1i}^2 + \beta_{2i}^2$. Par l'identité de Lagrange qui dit que:

$$(a^2+b^2)\cdot(c^2+d^2) = (ac \pm bd)^2 + (ad \mp bc)^2 \tag{5}$$

Alors on va voir que avec la décomposition primaire on peut démontrer que tout naturel peut s'écrire comme somme de carrés d'entiers: avant d'en arriver là, on doit encore voir si on peut écrire tout nombre p_i t.q. $p_i = 4.m+3$ comme somme de carrés. Par une autre identité que on ne démontre pas ici:

$$\forall N \text{ t.q. } N = 4m+3, \quad N = \sum_{k=1}^{p} n_k^2, \quad n_k \in \mathbb{N}, \quad p = \{3,4\} \tag{7}$$

Ce qui permet d'écrire que $\forall p_i$ t.q. $p_i = 4m+1$, alors: $p_i = \tilde{\beta}_{1i}^2 + \tilde{\beta}_{2i}^2 + \tilde{\beta}_{3i}^2 + \tilde{\beta}_{4i}^2$.

Par une identité de Euler:

$$\left(\sum_{i=1}^{4} a_i^2\right)\cdot\left(\sum_{i=1}^{4} b_i^2\right) = \sum_{i=1}^{4} u_i^2, \quad u_i \text{ univoq. dét. (c.f.p. 16)} \tag{8}$$

on va démontrer que tout naturel s'écrit comme une somme de carrés d'entiers. Soit la décomposition primaire:

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_e^{\alpha_e} \tag{9}$$

i) Si $p_i = 2$, alors: $p_i^{\alpha_i} = 2^{\alpha_i} = \begin{cases} 2 \cdot 2^{\alpha_i - 1} = (1^2+1^2)\cdot\left(1^{\alpha_i-1} + 1^{\alpha_i-1}\right), & \alpha_i \text{ impair} \\ \left(1^{\alpha_i} + 1^{\alpha_i}\right) & \alpha_i \text{ pair} \end{cases}$ (10)

ii) Si $p_i = 4m+1$: (4) $\Rightarrow$ $p_i = \beta_{1i}^2 + \beta_{2i}^2$

(5) $\Rightarrow$ $p_i^{\alpha_i} = \left(\beta_{1i}^2 + \beta_{2i}^2\right)^{\alpha_i} = \begin{cases} \alpha_i = 1: & (\beta_{1i}^2 + \beta_{2i}^2) \\ \alpha_i \neq 1: & (u_1^2 + u_2^2)^{\alpha_i - 2} \cdot \underbrace{(a^2+b^2)^2 \cdot (a^2+b^2)^{\alpha_i-2}}_{a^4+b^4+2a^2b^2 = (a^2)^2+(b^2)^2+(1^2+1^2)\cdot(ab)^2} \\ \alpha_i = 2: & (u_1^2)^2 + (u_2^2)^2 + 2(u_1 u_2)^2 \\ \alpha_i = \text{pair} > 2: & (u_1^2 + u_2^2)^{\alpha_i - 2} \dots \text{etc.} \end{cases}$ (11)

$\alpha_i - 2 - 2 - \dots = 2$

iii) $p_i = 4m+3$, (7) $\Rightarrow$ $p_i = \sum_{k=1}^{4} \tilde{\beta}_{ki}^2$

(8) $\Rightarrow$ $p_i^{\alpha_i} = \left(\sum_{k=1}^{4} \tilde{\beta}_{ki}^2 \right)^{\alpha_i} =$ (12)

- $\alpha_i = 1$: $\sum_{k=1}^{4} \tilde{\beta}_{ki}^2$
- $\alpha_i \neq 1$: $\left(\sum_{i=1}^{4} u_i^2 \right)^{\alpha_i - 2}$
- $\alpha_i = 2$: produit de carrés donné par: $\left(\sum_{k=1}^{4} u_i^2 \right)^2$
- α_i pair, $\alpha_i > 2$: $\left(\sum_{i=1}^{4} u_i^2 \right)^{\alpha_i - 2}$, $\alpha_i - 2 - 2 - 2 \cdots \rightarrow = 2$ #

Conclusion: (10), (11), (12) $\Rightarrow$

$$\forall N \in \mathbb{N} \quad \exists X_i \in \mathbb{N} \text{ t.q. } N = \sum_{i=1}^{\gamma(N)} X_i^2$$

Méthode de l'approche graduelle de la solution : trouver u, v

Soit : $\left.\begin{array}{l} u+v=1 \\ u+k=\square \\ v+k=\square' \end{array}\right\}$ t.q. i) k pas impair
ii) $(2k+1)$ pas divisible par un nb. entier x de la forme $x=4m+3$

Alors par les équations posées, on a :

$$u<1 \ , \ v<1 \quad , v,u \neq 0$$

donc les équations se reformulent pour donner :

$$\begin{array}{l} k = \square - u \ < \square \\ k = \square' - v \ < \square' \end{array} \qquad \text{ou bien : } \quad \square' = k + \underbrace{v}_{<1} \ < k+1$$

Donc on a les 2 conditions suivantes :

$$\begin{array}{l} \square > k \\ \square' < k+1 \end{array}$$

De plus, il faut que k satisfasse aux conditions i) et ii). On peut par exemple choisir $k=6$, alors k est pair, et $2k+1 = 13$ est premier, donc satisfait aussi ii). On aura donc :
↳ k impair : marche pas

$$\begin{array}{l} k=6 \\ \square > 6 \\ \square' < 7 \end{array}$$

Maintenant on applique un 'algorithme' qui consiste dans un premier temps à rechercher un carré proche de $k+1/2$ tel que ; trouver p :

$$\boxed{k + 1/2 + p^2 = \square \qquad , p^2 = \square}$$ à partir de là, ce sont des astuces de calcul

Comme ici $k=6$, alors pour garder des carrés des deux côtés, on multiplie par 4 :

$$4 \cdot \left(6 + 1/2 + \square \right) = 4 \cdot \square$$
$$\Rightarrow \ 26 + 4\square = 4 \cdot \square$$

On fait un changement de variable qui n'est rien d'autre qu'une astuce algébrique : soit $4\square = \frac{1}{y^2}$, alors :

$$26 + \frac{1}{y^2} = 4 \cdot \square$$

On multiplie le tout par y^2 et on obtient :

$$26y^2 + 1 = 4 \cdot \square \cdot y^2$$

On va égaler cette dernière relation à $(5y+1)^2$, ce qui est encore une autre astuce :

$$26y^2 + 1 = (5y+1)^2 = 25y^2 + 1 + 10y$$
$$\Rightarrow \ y^2 - 10y = 0$$
$$\Rightarrow \ y = 10$$

On a donc l'équation, en remplaçant la valeur de y :

$$26 + \frac{1}{100} = 4 \cdot \square$$

On refait les mêmes démarches dans l'ordre inverse, i.e. on avait multiplié par 4, alors on divise à nouveau par 4 pour revenir à l'expression $k + 1/2 + p^2 = \square$:

$$6 + 1/2 + \frac{1}{400} = \square$$

Mais en mettant l'expression de droite sous le même dénominateur, on sait que on doit aboutir à une expression au carré, ce qui donc :

$$\square = \left(\frac{81}{20} \right)^2$$

On passe à l'étape suivante du calcul. Maintenant que on a trouvé le premier $\square$, on veut trouver $\square'$,