196 EXEMPLES D'EQUATIONS DIOPHANTIENNES

[CAM] p249 (*) [I001] p10

Def 1 Une équation diophantienne est une équation polynôme $P(x_1, \dots, x_n) = 0$ à coefficients dans $\mathbb{Z}$ (resp dans $\mathbb{Q}$) dont on cherche les solutions (x_i) en nombres entiers (resp rationnels) [SAM] p19

Rq Fermat affirmait qu'il savait prouver que $\forall n \geq 3$ $x^n + y^n = z^n$ n'avait pas de solution non triviale. Il fallut attendre 1995 pour en avoir la preuve. [CAM] p275

I. EQUATIONS DU 1er DEGRÉ

1. En 2 variables $ax+by=c$

Prop 2 On considère l'équation $ax+by=c$ avec $a,b,c \in \mathbb{Z}^*$ donnés. On pose $d = \text{pgcd}(a,b)$

- Si $d \nmid c$ il n'y a pas de solution.
- Si $d \mid c$ les solutions sont données par $\left\{ \left(x_0 + \frac{bk}{d} ; y_0 - \frac{ak}{d}\right) \mid k \in \mathbb{Z} \right\}$ où (x_0, y_0) est une solution particulière calculée par exemple avec l'algorithme d'Euclide étendu.

Ex 3 Les solutions de $5x+7y=11$ sont $\{(7k+5, -2-5k) \mid k \in \mathbb{Z}\}$ [I001] exo801

Système d'équations modulaires

Thm 4 (chinois). Soient $m_1, \dots, m_r \in \mathbb{Z}$ premiers entre eux 2 à 2 et $n := m_1 \dots m_r$. Alors $\forall (x_1, \dots, x_r) \in \mathbb{Z}^r$, $\exists!\, x$ (déterminé modulo n) / $x \equiv x_i\ [m_i]$ pour tout $i \in [1, r]$ [VOU] p850 ou [I001] p6

Méthode 5 On pose $\Pi_k = \prod_{i \neq k} m_i$. Les Π_k sont des éléments premiers dans leur ensemble. Bézout donne $1 = \Pi_1 u_1 + \dots + \Pi_r u_r$. Alors $x := \Pi_1 u_1 x_1 + \dots + \Pi_r u_r x_r$ sera une solution particulière du système. Les autres s'obtiennent en ajoutant un multiple de n

Ex 6 Les solutions de $\begin{cases} x \equiv 2\ [4] \\ x \equiv 3\ [5] \\ x \equiv 1\ [9] \end{cases}$ sont les $x = 118 + k180$ où $k \in \mathbb{Z}$. $(4.5.9 = 180)$ [CAM] p249

2. En n variables

Prop 7 Si $a_1, \dots, a_n \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$, $d := \text{pgcd}(a_1, \dots, a_n)$. Alors l'équation $a_1 x_1 + \dots + a_n x_n = b$ $(x_i \in \mathbb{Z})$ admet une solution ssi $d \mid b$.
Dans ce cas, toute solution de cette équation s'écrit de manière unique sous la forme $\alpha V_1 + x_2 V_2 + \dots + x_n V_n$ avec
- $x_2, \dots, x_n \in \mathbb{Z}$
- $\alpha \in \mathbb{Z}$ vérifiant $b = \alpha d$
- les V_i sont les colonnes d'une matrice $V \in GL_n(\mathbb{Z})$ vérifiant $(a_1 \dots a_n) V = (d\ 0 \dots 0)$ [BER] p248

Ex 8 Considérons l'équation $3x + 4y + 7z = b$. On trouve $d = 1$ et $V = \begin{pmatrix} -1 & 4 & -1 \\ 1 & -3 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ par exemple. [BER] p248
Les solutions sont donc $\begin{pmatrix} -b + 4z_1 - z_2 \\ b - 3z_1 - z_2 \\ z_2 \end{pmatrix}$ $z_1, z_2 \in \mathbb{Z}$

Prop 10 Partition d'un entier en parts fixées
Si $a_1, \dots, a_k \in \mathbb{N}^*$ premiers entre eux dans leur ensemble. Alors $u_n := \text{Card}\{(x_1, \dots, x_k) \in \mathbb{N}^k / a_1 x_1 + \dots + a_k x_k = n\}$ $\underset{n \to \infty}{\sim} \frac{1}{a_1 \dots a_k} \frac{n^{k-1}}{(k-1)!}$ [FGNan2] exo3.5

II. METHODES PRATIQUES DE RESOLUTION

1. Descente infinie

Def 11 (Principe de la méthode, due à Fermat)
On suppose par l'absurde qu'il existe une

solution non triviale

[SAT] p21 b) On montre qu'il existe alors une solution non triviale plus petite construite à partir de la première.

Par récurrence il existe une suite strictement décroissante d'entiers solutions non triviales ce qui est contradictoire (toute suite décroissante dans $\mathbb{N}$ est stationnaire / stationnaire)

[Con] p275 Rq12 On peut remplacer b) et c) en considérant une solution avec un élément minimal puis arriver à une contradiction en obtenant une solution avec le même élément plus petit

[Con] p275 Ex13 $x^4 + y^4 = z^2$ n'a pas de solution non triviale

Def14 Un triangle pythagoricien est un triplet $(a,b,c) \in \mathbb{N}^3$ tel que $a^2+b^2=c^2$.

[HELLE] p12 Thm15 L'aire d'un triangle pythagoricien ne peut pas être un carré.

App16 L'équation de Fermat pour $n=4$ n'a pas de solution non triviale.

[COL] exo854 Ex17 L'équation $x^3 + 2y^3 = 4z^3$ n'a pas de solution non triviale.

DVPT [FGNal] Ex18 Théorème de Sophie Germain (1823)
Si p est un nombre premier tel que $2p+1$ est premier alors $\nexists (x,y,z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \ [p]$ et $x^p + y^p + z^p = 0$

" exo438 Ex $n \in \mathbb{N}$, $x \in \mathbb{N}$ $x > n \geq 2$. $x^{x_1} + \dots + x^{x_n} = x^{x_{n+1}}$ n'a pas de solution non triviale

2. Réduction modulaire [Coo] si non précisé

exo787 Ex19 L'équation $x^3 + 5 = 117 y^3$ n'a pas de solution (modulo 9)

exo844 Ex20 Les équations $x^3 + y^3 + z^3 = 4$ ou 5 n'ont pas de solution entière (modulo 9)

[Con] p275 Ex20 bis Si $p \equiv 3 \ [4]$ (p premier) $x^2 + y^2 = pz^2$ n'a pas de solution non triviale (modulo p + descente infinie)
Rq si $p \equiv 1$ ou $2 \ [4]$ il y en a une infinité

Ex21 L'équation $x^2 + y^3 = 8z + 7$ n'a pas de solution entière (modulo 8) exo855

Ex22 L'équation $x^4 - x^3 = y^4 + 5$ exo857

Ex23 $2^n - 1$ n'est jamais le carré d'un nombre pour $n \geq 3$. (réduire modulo 4) [Sans référence]

Ex24 Trouver les entiers m et n tels que 2^m et 3^n soient consécutifs (modulo 8 et 4) [SIER] exo V.185 p16 V.184
($m=2$ $n=1$ / $m=n=1$ / $m=3$ $n=2$)

3. Méthode géométrique [Con] p273-276 si non précisé

Il s'agit d'utiliser la paramétrisation rationnelle d'une conique (ou d'une courbe plus généralement) et de chercher les points à coordonnées rationnelles.

Rq25 Résoudre $x^4 + y^4 = 1$ revient à trouver les points à coordonnées rationnelles sur le cercle écrasé.
[Siw] p3 + cf Annexe 1

Méthode26 La méthode est applicable à des équations de type $P(X,Y,Z)=0$ avec $P \in \mathbb{Z}[X]$ polynôme homogène tel que la courbe plane d'équation $p(x,y,1)=0$ possède un bon paramétrage rationnel.

Ex27 (cercle et triangle pythagoricien) $(x,y,z) \in \mathbb{N}^3$ est solution de $x^2+y^2=z^2$ ssi $\exists d \in \mathbb{N}$, $u, v \in \mathbb{N}^*$ premiers entre eux / (x,y,z) ou (y,x,z) soit égal à $(d(u^2-v^2),\ 2duv,\ d(u^2+v^2))$

Ex28 (Folium de Descartes) $x^3 + y^3 = axyz$
↳ il y a déjà $(x,-x,0)$ pour $x \in \mathbb{Z}$
↳ avec la paramétrisation on trouve
$\{(uv^2,\ u^2v,\ u^3+v^3) \ / \ u \in \mathbb{Z}^*,\ v \in \mathbb{N}^*,\ u \wedge v = 1\}$

+ voir fin (Utilisation des réseaux)

III UTILISATION DES CORPS QUADRATIQUES

1. Introduction [DUV] p48 et suivantes

Soit d un entier sans facteur carré. On se place dans le corps $\mathbb{Q}(\sqrt{d}) = \{z \in \mathbb{C} \mid z = \alpha + \beta\sqrt{d} \mid \alpha, \beta \in \mathbb{Q}\}$

Def 29 On définit une norme N sur $\mathbb{Q}(\sqrt{d})$ telle que si $z = \alpha + \beta\sqrt{d}$ alors $N(z) = \alpha^2 - d\beta^2 \in \mathbb{Q}$

Def 30 z est un entier de $\mathbb{Q}(\sqrt{d})$ s'il est racine d'un polynôme de degré 2 sur $\mathbb{Z}$.

Ex 31 $\frac{1+\sqrt{5}}{2}$ est entier de $\mathbb{Q}(\sqrt{5})$.

Def 32 En posant $K := \mathbb{Q}(\sqrt{d})$, on note A_K l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$

Thm 33
- Si $d \equiv 2$ ou 3 [4] $\quad A_K = \mathbb{Z}(\sqrt{d})$
- Si $d \equiv 1$ [4] $\quad A_K = \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right)$

Def/Prop 34 $A_K^* = \{\varepsilon \in A_K \mid \varepsilon \text{ inversible}\}$ et l'ens. $= \{\varepsilon \in A_K \mid N(\varepsilon) = \pm 1\}$ des unités de A_K. C'est un groupe pour la multiplication

Thm 35 Si $d > 0$, $\exists!\, \omega > 1$ (unité fondamentale) tq $A_K^* = \{\pm \omega^n \mid n \in \mathbb{Z}\}$.

2. Equation de Pell [DUV]

p42 Il s'agit de l'équation $x^2 - dy^2 = 1$. où $d \in \mathbb{N}^*$ n'est pas un carré.

p43 **Thm 36** [ARNIS]. L'équation de Pell a toujours une infinité de solution.

p51 **Thm 37** Soit (x_1, y_1) la plus petite solution non triviale de l'équation de Pell. (x_n, y_n) les solutions de $\mathbb{N}^2$ rangées dans l'ordre croissant. Alors, pour tout $n \in \mathbb{N}$

a) $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$

b) $x_{n+2} = 2x_1x_{n+1} - x_n$ et $y_{n+2} = 2x_1y_{n+1} - y_n$

p42 Rq Ce n'est pas facile de trouver la plus petite solution non triviale (théorie des fractions continues)

Rq 38 $x^2 - dy^2 = n$ n'a pas toujours de solution p43

Ex 39 $x^2 - 19y^2 = 1$. La solution triviale est $(1, 0)$. p51 et la plus petite non triviale $(170, 39)$. On peut aussi trouver par exemple une autre solution (x_4, y_4)

$(x_4, y_4) = (668144880, 153282948)$

3. Cas où A_K euclidien [DUV]

Prop 40 A_K est euclidien pour $d = -11, -7, -3, -2, -1, 2, 3, 5, 13$ p55

- $d = -1$

Prop 41 $A_K = \mathbb{Z}[i]$ et $A_K^* = \{\pm 1, \pm i\}$ p49

Thm 42 Soit $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2 \quad a, b \in \mathbb{N}\}$. p premier impair. $p \in \Sigma$ ssi $p \equiv 1$ [4] p61

Cor 43 $n \in \mathbb{N}$. $n \in \Sigma$ ssi les facteurs premiers de sa décomposition en produit de facteurs premiers y figurent avec un exposant pair. (Thm des 2 carrés) [DVT]

Ex 44 L'équation de Nodell $y^2 = x^3 - 1$ a pour unique solution $(1, 0)$ p56

Ex 45 L'équation $y^2 + 4 = z^3$ n'a de solutions entières que $(\pm 11, 5)$ ou $(\pm 2, 2)$ [STE] p94 ou [NOU] p251

- $d = -7$

Ex 46 Les seules solutions entières de $x^2 + 7 = 2^n$ sont $(\pm 1, 3)$ $(\pm 3, 4)$ $(\pm 5, 5)$ $(\pm 11, 7)$ et $(181, 15)$ [STE] p96

- $d = -2$ Ex 47 $x^3 - 2 = y^2$ dans $\mathbb{Z} \to (\pm 5, 3)$ [NOU] p251

Fin du II 2 | Utilisation des réseaux [STE] p139 ou [TAU] p

Thm (Minkowski) Soit L un réseau de dimension n de $\mathbb{R}^n$, de domaine fondamental τ et soit X un convexe symétrique borné. Si $\mathrm{vol}(X) > 2^n \mathrm{vol}(\tau)$, alors X contient un point de L non nul.

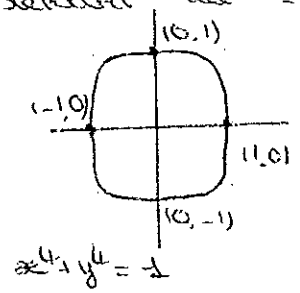
Rq On peut retrouver le Thm des 2 carrés.

App Thm des 4 carrés : L'équation $x^2 + y^2 + z^2 + t^2 = n$ admet des solutions pour tout n.

[TAU] Tauvel, Géométrie

[SAM] Samuel, Théorie algébrique des nombres.
[COM] Combes, Algèbre et Géométrie (connexions historiques)
[NOU] Nourdin, Agreg de Maths epreuve orale
[SILV] Silverman - Tate / Rational points on elliptic curves
[BER] Berhuy, Modules, théorie, pratique ... et un peu d'arithmétique
[FGNA2] Oraux X-ENS Analyse 2
[FGNA1] Fresnel - Giaquinta Nicolas. (" mais Algèbre)
[HELLE] Hellegouarch, Invitation aux mathématiques de Fermat-Wiles
[COR] De Koninck / Mercier - 1001 problèmes en théorie classique des nombres (plein d'exemples!!)
[SIER] Sierpinski - 250 problèmes in elementary number theory (existe aussi en français)
[DUV] Duverney - Théorie des nombres
[STE] Stewart / Tall - Algebraic number theory and Fermat's last theorem

Annexe 1



(*) Thm 3 bis : $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$. Le système $\begin{cases} x \equiv a \ [m] \\ x \equiv b \ [n] \end{cases}$ possède des solutions si pgcd(m,n) divise $a-b$.

[COR] Thm 2.76

Théorème des deux carrés

Thomas THOUPLET et Laura GAY d'après M. VARVENNE et C. ROBET

Référence : PERRIN : Cours d'algèbre p.56,57,58 ou RISLER-BOYER : Algèbre pour le L3 Problème 1.4 p23+159

Soit $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2;\ a, b \in \mathbb{N}\}$.

Théorème (*des deux carrés*)

Soit p un nombre premier impair[1].
On a l'équivalence suivante :

$$p \in \Sigma \Longleftrightarrow p \equiv 1\ [4]$$

Pour démontrer ce théorème, l'idée est de penser que si $n \in \Sigma$, alors $n = a^2 + b^2 = (a + ib)(a - ib)$ dans $\mathbb{C}$. On va donc introduire l'anneau des entiers de Gauss $\mathbb{Z}[i]$.

1 L'anneau $\mathbb{Z}[i]$

Définition

On définit l'anneau $\mathbb{Z}[i]$ par :

$$\mathbb{Z}[i] = \{a + ib \in \mathbb{C} | a, b \in \mathbb{Z}\}$$

Cet anneau est intègre car inclus dans $\mathbb{C}$. De plus, on dispose d'un automorphisme de $\mathbb{Z}[i]$ donné par la conjugaison :

$$\begin{array}{rccc} \sigma & : & \mathbb{Z}[i] & \to & \mathbb{Z}[i] \\ z = a + ib & & \mapsto & & \bar{z} = a - ib \end{array}$$

Cet automorphisme nous permet de définir une "norme"

$$\begin{array}{rccc} N & : & \mathbb{Z}[i] & \to & \mathbb{N} \\ a + ib & & \mapsto & & z\bar{z} = a^2 + b^2 \end{array}$$

qui est multiplicative, c'est à dire $N(zz') = N(z)N(z')$.
L'introduction de cette norme permet de calculer les inversibles de $\mathbb{Z}[i]$:

Proposition 1

On a $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Preuve :
Si $z \in \mathbb{Z}[i]^*$, $\exists z' \in \mathbb{Z}[i]^*$ tel que $zz' = 1$, d'où $N(z)N(z') = 1$.
Donc $N(z) = N(z') = 1 \Rightarrow a^2 + b^2 = 1 \Rightarrow (a = 0 \text{ et } b = \pm 1)$ ou $(a = \pm 1 \text{ et } b = 0)$.
D'où le résultat. ■

Proposition 2

L'ensemble Σ des sommes de deux carrés est stable par multiplication.

Preuve :
On traduit la propriété $n \in \Sigma$ en termes d'entiers de Gauss :

$$n \in \Sigma \Leftrightarrow \exists z \in Z[i] \ / \ n = N(z)$$

Alors, si $n, n' \in \Sigma$, on a $n = N(z)$ et $n' = N(z')$ donc $nn' = N(zz') \in \Sigma$ ■

1. Il est clair que $2 \in \Sigma$ car $2 = 1^2 + 1^2$ mais $2 \not\equiv 1\ [4]$.

Proposition 3

L'anneau $\mathbb{Z}[i]$ est euclidien (relativement à la fonction N), donc principal.

Preuve :

Soient $z, t \in \mathbb{Z}[i]\backslash\{0\}$. On a $z/t \in \mathbb{C}$ qui est de la forme $z/t = x + iy$.

On veut approximer $\frac{z}{t}$ par un entier de Gauss $q = a + ib$ où a et b sont tels que $|x-a| \leqslant \frac{1}{2}$ et $|y-b| \leqslant \frac{1}{2}$. Ainsi,

$$\left|\frac{z}{t} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1$$

On pose alors $r = z - qt$ et ainsi $r \in \mathbb{Z}[i]$ (car z, q et t le sont) et $r = t\left(\frac{z}{t} - q\right)$ d'où

$$|r| = |t| \left|\frac{z}{t} - q\right| < |t| \text{ et en élevant au carré, } N(r) < N(t).$$

On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$ et le résultat est démontré. ■

2 Démonstration du théorème des deux carrés

On rapelle le théorème à démontrer :

Théorème

Soit p un nombre premier impair.
On a l'équivalence suivante :

$$p \in \Sigma \Longleftrightarrow p \equiv 1\ [4]$$

Remarquons déjà (ce sera redémontré dans la suite) que la condition $p \equiv 1\ [4]$ est clairement nécessaire car $\forall (a,b) \in \mathbb{N}^2$, $a^2 + b^2 \equiv 0, 1, 2\ [4]$ et comme p est premier, $p \not\equiv 0$ ou $2\ [4]$.

Lemme

On a l'équivalence suivante :

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i].$$

Preuve du Lemme :

($\Rightarrow$) : Si $p = a^2 + b^2$, on a $p = (a + ib)(a - ib)$ et a, b sont $\neq 0$, donc $a + ib$, $a - ib$ ne sont pas $\mathbb{Z}[i]^*$ d'où p n'est pas irréductible.
($\Leftarrow$) : Si $p = zz'$ avec z, z' non inversibles (donc $N(z), N(z')$ sont $\neq 1$), on a $N(p) = N(z)N(z') = p^2$, donc comme p est premier, nécessairement $p = N(z)$ d'où $p \in \Sigma$ et le lemme est démontré. ■

Preuve du Théorème :

$\mathbb{Z}[i]$ est factoriel (car euclidien pour la norme N).
On a donc l'équivalence suivante :

$$\begin{aligned} p \text{ n'est pas irréductible dans } \mathbb{Z}[i] &\iff (p) \text{ n'est pas premier dans } \mathbb{Z}[i] \\ &\iff \mathbb{Z}[i]/(p) \text{ non intègre.} \end{aligned}$$

De plus, $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ donc on a :

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2+1, p) \simeq (\mathbb{Z}[X]/(p))/(X^2+1) \simeq \mathbb{F}_p[X]/(X^2+1)$$

D'où,

$$\begin{aligned} p \text{ est réductible dans } \mathbb{Z}[i] &\iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i] \\ &\iff X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p[X] \\ &\underset{\text{car } X^2+1 \text{ est de deg 2}}{\iff} X^2+1 \text{ admet une racine dans } \mathbb{F}_p \\ &\iff -1 \text{ est un carré dans } \mathbb{F}_p. \end{aligned}$$

D'après le lemme, il nous reste donc juste à démontrer que :

$$-1 \text{ est un carré dans } \mathbb{F}_p \iff p \equiv 1\ [4]$$

Or si p impair, on a

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si} \quad p \equiv 1\ [4] \\ -1 & \text{sinon} \end{cases}$$

Et finalement, le théorème est démontré. ■

Corollaire

Soit $n \in \mathbb{N}^*$. On décompose n en produit de facteurs premiers : $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$ où $\mathcal{P} = \{\text{nombres premiers}\}$.

Alors,

$$n \in \Sigma \iff \forall p \in \mathcal{P} \text{ tel que } p \equiv 3\ [4], \quad \nu_p(n) \text{ est pair.}$$

Preuve :

($\Leftarrow$) On décompose n de la façon suivante car lorsque $p \equiv 3\ [4]$, $\nu_p(n)$ est pair :

$$n = \left(\prod_{p \equiv 3\ [4]} p^{\frac{\nu_p(n)}{2}}\right)^2 \left(\prod_{p \not\equiv 3\ [4]} p^{\nu_p(n)}\right)$$

Le produit de gauche est un carré parfait donc il appartient à Σ.
Dans le produit de droite, chaque p est congru à 1 modulo 4 ou égal à 2 donc dans Σ.
La stabilité par multiplication de Σ permet alors de conclure.

($\Rightarrow$) Soit $n = a^2 + b^2 \in \Sigma$ et soit $p \in \mathcal{P}, p \equiv 3[4]$. Si $\nu_p(n) = 0$, le résultat est vrai. Sinon, cela signifie que p divise n. Remarquons alors que, puisque $p \equiv 3\ [4]$, p est irréductible dans $\mathbb{Z}[i]$. p divise $(a + ib)(a - ib)$ donc p divise (par exemple) $a + ib$. p étant réel, p divise a et b. On peut noter $a = pa'$ et $b = pb'$. Alors $n = a^2 + b^2 = p^2(a'^2 + b'^2)$ donc

$$\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma \text{ et } \nu_p\left(\frac{n}{p^2}\right) = \nu_p(n) - 2$$

Par récurrence, on peut donc montrer que $\nu_p(n)$ est paire, ce qui conclut le théorème.

■

Notes :

♣ Carl GAUSS (1777 - 1855) est un mathématicien, astronome et physicien allemand. Il a apporté de très importantes contributions à ces trois domaines. Surnommé "le prince des mathématiciens" (Mathematicorum Principi), il est considéré comme l'un des plus grands mathématiciens de tous les temps. La qualité extraordinaire de ses travaux scientifiques était déjà reconnue par ses contemporains. Il dirigea l'Observatoire de Göttingen et ne travailla pas comme professeur de mathématiques – d'ailleurs il n'aimait guère enseigner – mais il encouragea plusieurs de ses étudiants, qui devinrent d'importants mathématiciens, notamment EISENSTEIN et RIEMANN. Il a beaucoup échangé avec Sophie GERMAIN et était assez admirateur (un féministe !).

Théorème de Sophie Germain

Thomas THOUPLET et Laura GAY d'après M. VARVENNE et C. ROBET

Référence : FGNAL1 : p.168 (Théorème) et p.140 (Lemme)

Lemme

Si le produit de deux entiers a et b premiers entre eux est une puissance k-ième (avec $k \geqslant 2$), alors a et b sont tous les deux des puissances k-ièmes.

Preuve du Lemme :

Soient a et b deux entiers premiers entre eux tels que $ab = c^k$ avec $c \in \mathbb{Z}$ et $k \geqslant 2$. Écrivons la décomposition en facteurs premiers de a, b et c :

$$a = \prod_{p \text{ premier}} p^{\alpha_p},\ b = \prod_{p \text{ premier}} p^{\beta_p} \text{ et } c = \prod_{p \text{ premier}} p^{\gamma_p}$$

où α_p, β_p et γ_p sont des familles d'entiers à support fini.
Comme $ab = c^k$, on obtient par unicité de la décomposition $\alpha_p + \beta_p = k\gamma_p$ pour tout p premier. De plus, comme $\text{pgcd}(a,b) = 1$ on a $\alpha_p\beta_p = 0$ [1] pour tout p premier. Il en résulte que pour tout p premier, α_p et β_p sont divisibles par k. Finalement, a et b sont bien des puissances k-ièmes. ■

Théorème (*de Sophie Germain - 1823*)

Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p + 1$ soit premier. Alors

$$\nexists\ (x,y,z) \in \mathbb{Z}^3 \text{ tel que } xyz \not\equiv 0\ [p] \text{ et } x^p + y^p + z^p = 0$$

Preuve du théorème :

On raisonne par l'absurde.
On suppose donné dans la suite un triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0\ [p]$ et $x^p + y^p + z^p = 0$.
Soit $d = \text{pgcd}(x,y,z)$. Quitte à poser $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$, on peut supposer [2] $d = 1$.

Etape 1 Montrons que x, y, z sont premiers entre eux deux à deux.
Supposons par l'absurde que $\text{pgcd}(x,y) > 1$ et soit p_0 un facteur premier qui divise x et y. Alors $p_0 | x^p + y^p$ donc $p_0 | z^p$ et donc $p_0 | z$ (Lemme d'Euclide) ce qui contredit le fait que $\text{pgcd}(x,y,z) = 1$.
Ainsi $\text{pgcd}(x,y) = 1$. De même, on en déduit que $\text{pgcd}(x,z) = 1$ et $\text{pgcd}(y,z) = 1$.

Etape 2 Montrons l'existence de $(a,\alpha) \in \mathbb{Z}^2$ tels que $y + z = a^p$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p$:

On remarque que :

$$y^p + z^p = (y+z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = -x^p = (-x)^p \quad (\star)$$

D'après le **Lemme**, il suffit donc de montrer que $(y+z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux.

Supposons par l'absurde qu'il existe p' premier qui divise $(y+z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$.

Alors d'après $(\star)$, p'^2 divise x^p donc p' divise x.
Comme $y \equiv -z\ [p']$, on en déduit une nouvelle "égalité"

$$\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \begin{cases} \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1}\ [p'] \\ \equiv 0\ [p'] \ (\text{car } p' \Big| \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k) \end{cases}$$

1. car α_p ou β_p doit être nul
2. On aura toujours $x'y'z' \not\equiv 0\ [p]$ et $x'^p + y'^p + z'^p = 0$.

Donc $p' \mid py^{p-1}$. D'après le lemme d'Euclide[3], $p'|p$ ou $p'|y^{p-1}$ dont $p'|y$.
$\hookrightarrow$ Si $p'|p$ (ie $p' = p$), cela signifie que $p|x$ (absurde par hypothèse).
$\hookrightarrow$ Si $p'|y$, cela contredit le fait que $\text{pgcd}(x, y) = 1$
D'où $(y + z)$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux.

D'après le **Lemme**, comme leurs produits est une puissant p-ième $(-x^p)$ il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que

$$\underline{y + z = a^p \text{ et } \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p}$$

Par symétrie, il existe $(b, c) \in \mathbb{Z}^2$ tel que $\underline{x + y = c^p \text{ et } x + z = b^p}$.

Etape 3 Un et un seul des 3 entiers x, y, z est divisible par q :
Soit $m \in \mathbb{Z}$ tel que $m \not\equiv 0\ [q]$, d'après le petit théorème de Fermat

$$m^{q-1} \equiv 1\ [q] \Rightarrow m^{2p} \equiv 1\ [q] \Rightarrow m^p \equiv \pm 1\ [q] \quad (\text{car } \mathbb{Z}/q\mathbb{Z} \text{ est un corps})^4$$

Supposons par l'absurde qu'aucun des trois entiers x, y, x n'est divisible par q.
Alors $x^p \equiv \pm 1\ [q]$, $y^p \equiv \pm 1\ [q]$ et $z^p \equiv \pm 1\ [q]$.
Donc $(0 =)x^p + y^p + z^p$ est congru à $3, 1, -1$ ou -3 ce qui est absurde car $q > 5$ donc on ne peut pas avoir $3, -1, 1, -3 \equiv 0[q]$.
On peut donc supposer sans perte de généralité que $\underline{x \text{ est divisible par } q}$ (et c'est le seul car x, y, z sont premiers entre eux deux à deux).

Etape 4 Contradiction et conclusion :
On a $y + z = a^p$, $x + z = b^p$ et $x + y = c^p$ donc $b^p + c^p - a^p = 2x \equiv 0\ [q]$ $(\star\star)$.
D'autre part, $y \equiv c^p\ [q]$ car $x \equiv 0\ [q]$.
De plus, q ne divise pas y donc ne divise pas c^p et donc ne divise pas c. D'où $\underline{y \equiv c^p \equiv \pm 1\ [q]}$ (c'est le début de l'étape 3).
De même, $\underline{z \equiv \pm 1\ [q]}$.

Supposons q ne divise pas a, alors $a^p \equiv \pm 1\ [q] \Rightarrow c^p + b^p - a^p \equiv \pm 1$ ou $\pm 3\ [q]$ (absurde d'après $(\star\star)$).
Donc q divise a ie $y + z \equiv 0\ [q]$.
Avec cette dernière congruence, on peut écrire d'autre part

$$\begin{aligned} \alpha^p = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k &\equiv py^{p-1}\ [q] \\ &\equiv p(\pm 1)^{p-1}\ [q] \\ &\equiv^5 p\ [q] \end{aligned}$$

Or une puissance p-ième $\equiv 0, \pm 1\ [q]$ (c'est le Fermat du début de l'étape 3 qui nous dit ça).
Dans tous les cas, on aboutit à une contradiction (si c'est congru à 0 ça nous donne $p \equiv 0\ [q]$ absurde, si c'est ± 1 ça nous donne $p \equiv \pm 1\ [q]$ ie $2p + 1 = q \equiv \pm 2 + 1 = 3$ ou $-1\ [q]$ absurde).
On en déduit finalement que

$$\underline{\nexists\ (x, y, z) \in \mathbb{Z}^3 \text{ tel que } xyz \not\equiv 0\ [p] \text{ et } x^p + y^p + z^p = 0.}$$

■

Notes :

✓ Le plus grand nombre premier de Sophie Germain actuellement connu est $39051 \times 2^{6001} - 1$ trouvé en 1986. On conjecture qu'il en existe un infinité.
♣ Marie-Sophie GERMAIN (1776 - 1831), est une mathématicienne et philosophe française. Elle est connue pour le théorème d'arithmétique qui porte son nom, pour ses échanges avec le mathématicien GAUSS et pour ses travaux sur l'élasticité des corps. Elle avait pour nom d'emprunt Antoine Auguste Le Blanc. Lorsqu'elle se voit obligée de réveler son identité, GAUSS devient encore plus fan d'elle et lui envoie une lettre de "déclaration" d'admiration.

3. et non Gauss comme écrit dans le livre
4. Dans $\mathbb{Z}/q\mathbb{Z}$ on a $(m^p)^2 - 1 = 0$ donc $(m^p - 1)(m^p + 1) = 0$ et par intégrité -car c'est un corps-, c'est bon
5. car $p - 1$ est pair