

EXEMPLES D'EQUATIONS DIOPHANTIENNES

Def 1 Une equation diophantienne est une equation polynome $P(x_1, \dots, x_n) = 0$ à coefficients dans \mathbb{Z} (ou dans \mathbb{Q}) dont on cherche les solutions (x_i) en nombres entiers (ou p-entiers) [581] p19

Ex 1 Fermat affirmait qu'il serait prouvé que $\forall n \geq 3$ $x^n + y^n = z^n$ n'admet pas de solution non triviale. Il fut réfuté ultérieurement en 1995 par un autre la preuve. [581] p19

I. EQUATIONS DU 1er DEGRE

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

Prop 2 On considère l'équation $ax + by = c$ avec $a, b, c \in \mathbb{Z}$ données. 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

$$\left\{ \begin{matrix} ax + by = c \\ x = x_0 + \frac{b}{d}k \\ y = y_0 - \frac{a}{d}k \end{matrix} \right. \quad k \in \mathbb{Z}$$

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

$$\left\{ (7k + 5, -2 - 5k) \mid k \in \mathbb{Z} \right\} \quad \text{avec } (0, 0) \text{ et } (8, 0)$$

2. Systemes d'équations modulaires

Thm 4 (Chinois). Soient $m_1, \dots, m_r \in \mathbb{Z}$ premiers entre eux

avec $2 \leq r$ et $n_i = m_1 \dots m_r$. Soit $\forall i \in \{1, \dots, r\} \exists ! x_i \pmod{m_i}$

$\exists ! x \pmod{n_i}$ (déterminée modulo n_i) / $x \equiv x_i \pmod{m_i}$ pour tout $i \in \{1, \dots, r\}$

Méthode 5 On pose $\Pi_k = \prod_{j \neq k} m_j$ des Π_k sont des

diviseurs premiers deux deux entre eux. Soit dans $\mathbb{Z} = \mathbb{N} \cup \{0\} + \mathbb{N} \cup \{0\}$ on pose $x_i = \Pi_i u_i + \dots + \Pi_r u_r$. Soit $x_i \equiv x_i \pmod{m_i}$ pour une solution particulière du système, les autres s'obtiennent en ajoutant un multiple de n_i

Ex 6 Les solutions de $\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{9} \end{cases}$ sont $x \equiv 148 + k \cdot 180 \pmod{180}$ où $k \in \mathbb{Z}$. [581] p248

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 $a_1 x_1 + \dots + a_n x_n = b$ (où $x_i \in \mathbb{Z}$) admet une solution si et seulement si $d \mid b$.

Dans ce cas, toute solution de cette équation s'écrit de manière unique sous la forme $x = V_1 + z_1 V_2 + \dots + z_{n-1} V_n$ avec $x_i \in \mathbb{Z}$, $z_i \in \mathbb{Z}$

• $x \in \mathbb{Z}$ vérifiant $b = xd$

• Les V_i sont les colonnes d'une matrice $V \in \mathbb{G}_n(\mathbb{Z})$ vérifiant $(a_1, \dots, a_n)V = (d, 0, \dots, 0)$

Ex 8 Considérons l'équation $3x + 4y + 7z = b$. On suppose $d = 1$ et $V = \begin{pmatrix} -1 & 4 & 0 \\ 1 & -3 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ par exemple.

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 Restes d'un entier en petits facteurs

Si $a_1, \dots, a_n \in \mathbb{N}^*$ premiers entre eux dans \mathbb{N} entre eux. Soit $u_i = \text{Gcd}(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in \mathbb{N}$ $\forall i \in \{1, \dots, n\}$ + $\text{Gcd}(a_1, \dots, a_n) = 1$

$$n \sim \frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n} - \frac{n-1}{\text{Gcd}(a_1, \dots, a_n)}$$

II. METHODES PRATIQUES DE RESOLUTION

1. Descente lignée

Def 11 (Principe de la méthode, due à Fermat) Soit une équation diophantienne à n variables. On suppose que l'équation admet une solution particulière (x_0, \dots, x_n) . On pose $x_i = x_0 + u_i t_i$ et on obtient une équation à n-1 variables.

[581] p248

[581] p248

solution non triviale
On montre qu'il existe alors une solution non triviale plus petite constante à partir de la première.

Par récurrence il existe une suite strictement décroissante d'entiers solution non triviale de (1) et convergente (toute suite décroissante dans \mathbb{N} est stationnaire)

Prop 12 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

Ex 13 $x^4 + y^4 = z^4$ n'a pas de solution non triviale
Prop 14 Un triangle pythagoricien est un triplet $(a, b, c) \in \mathbb{N}^3$ tel que $a^2 + b^2 = c^2$.

Thm 15 L'aire d'un triangle pythagoricien ne peut pas être un carré.

App 16 L'équation de Fermat pour $n = 4$ n'a pas de solution non triviale.

Ex 17 L'équation $x^3 + 2y^3 = 4z^3$ n'a pas de solution non triviale.

Ex 18 Théorème de Sophie Germain (1823)
Si p est un nombre premier tel que $2p+1$ est premier alors $\exists (x, y, z) \in \mathbb{Z}^3$ tel que $xy^2z \neq 0$ (p) et $x^p + y^p + z^p = 0$

Ex 19 Réduction modulaire [con] n'a pas de solution (modulo 9)

Ex 20 L'équation $x^3 + 5 = 117y^3$ n'a pas de solution (modulo 9)

Ex 21 L'équation $x^2 + y^3 + z^3 = 4$ ou 5 n'ont pas de solution entière (modulo 9)

Ex 22 bis Si $p \equiv 3 \pmod{4}$ (premier) $x^2 + y^2 = pz^2$ n'a pas de solution non triviale (modulo p + descente infinie)

Prop 23 $p \equiv 1 \pmod{2}$ [1] $\exists y$ en a une infinie.

[SAT] p 1

[con] p 25

[con] p 25

[Felle] p 12

[con] exo 854

[DPT] [FGN ad]

exo 438

exo 787

exo 844

[con] p 25

Ex 21 L'équation $x^2 + y^3 = 8z + 7$ n'a pas de solution entière (modulo 8) exo 855

Ex 22 L'équation $x^4 - z^2 = y^4 + 5$ exo 857

Ex 23 $2^n - 1$ n'est jamais le carré d'un nombre pour $n \geq 3$ (modulo modulo 4) [sans réponse]

Ex 24 Trouver les entiers m et n tels que 2^m et 3^n soient consécutifs (modulo 8 et 4) [Sier] exo 185 p 16 $(m=2, n=1 / m=n=1 / m=3, n=2)$

3. Méthode géométrique [con] p 23 - 24 si on peut TD s'agit d'utiliser la paramétrisation rationnelle d'une conique (ou d'une courbe plus généralement) et de chercher les points à coordonnées rationnelles. Prop 25 résoudre $x^4 + y^4 = 1$ revient à trouver les points à coordonnées rationnelles sur le cercle unité.

[Siu] p 3 + cf Annexe 1

Méthode 26 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 $p(x, y, z) = 0$ possède un bon paramétrage rationnel.

Ex 27 (cercle et triangles pythagoriciens) $(x, y, z) \in \mathbb{N}^3$ est solution de $x^2 + y^2 = z^2$ si $\exists d \in \mathbb{N}, u, v \in \mathbb{N}^*$ premiers entre eux / $(x, y, z) = (y, x, z)$ soit appl à $(d(u^2 - v^2), 2d(uv), d(u^2 + v^2))$

Ex 28 (Solu de Descartes) $x^3 + y^3 = zxy$ $\rightarrow \exists y$ a déjà $(x, -x, 0)$ pour $xy \in \mathbb{Z}$ \rightarrow avec la paramétrisation, on trouve $\{(uv^2, u^2v, u^3 + v^3) / u \in \mathbb{Z}^*, v \in \mathbb{N}^*, u, v \neq 1\}$

+ voir fun (Utilisation des réseaux)

III UTILISATIONS DES CORPS QUADRATIQUES

1. Introduction (DMV) p48 et suivantes.

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

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

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

Ex 31 $\frac{4 + \sqrt{5}}{2}$ est entier de $\mathbb{Q}(\sqrt{5})$.

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

Thm 33 Si $d \equiv 1 \pmod{4}$ ou $3 \pmod{4}$ $N_{K/\mathbb{Q}} = \mathbb{Z} \left(\frac{1 + \sqrt{d}}{2} \right)$.
Si $d \equiv 2 \pmod{4}$ ou $0 \pmod{4}$ $N_{K/\mathbb{Q}} = \mathbb{Z}$

Def Prop 34 $A_{nk}^* = \{ \epsilon \in A_{nk} \mid \epsilon \text{ inversible} \}$ et ϵ est un des unités de A_{nk} . C'est un groupe pour la multiplication.

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

2. Equation de Pell (DMV)
On s'agit de l'équation $x^2 - d y^2 = 1$, où $d \in \mathbb{N}^*$ n'est pas un carré.

Thm 36 (GROSIS) L'équation de Pell a toujours une infinité de solutions.

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 engendrées dans l'ordre croissant. Pour tout $n \in \mathbb{N}$

a) $x_{2n} + y_{2n} \sqrt{d} = (x_1 + y_1 \sqrt{d})^{2n}$

b) $x_{2n+1} + y_{2n+1} \sqrt{d} = (x_1 + y_1 \sqrt{d})^{2n+1}$

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

Rq 38 $x^2 - d y^2 = n$ n'a pas toujours de solution p33

Ex 39 $x^2 - 19 y^2 = 1$. La solution triviale est $(1, 0)$.
La plus petite non triviale $(170, 39)$. On peut aussi trouver par exemple une autre solution $(84, 19)$
 $(x_2, y_2) = (668144, 1532829)$

3. Cas où A_{nk} euclidien (DMV)

Prop 40 A_K est euclidien pour $d = -1, -2, -3, -7, -11, -19, -41, -59, -83, -107, -131, -155, -179, -211, -239, -263, -287, -311, -335, -359, -383, -407, -431, -455, -479, -503, -527, -551, -575, -599, -623, -647, -671, -695, -719, -743, -767, -791, -815, -839, -863, -887, -911, -935, -959, -983, -1007, -1031, -1055, -1079, -1103, -1127, -1151, -1175, -1199, -1223, -1247, -1271, -1295, -1319, -1343, -1367, -1391, -1415, -1439, -1463, -1487, -1511, -1535, -1559, -1583, -1607, -1631, -1655, -1679, -1703, -1727, -1751, -1775, -1799, -1823, -1847, -1871, -1895, -1919, -1943, -1967, -1991, -2015, -2039, -2063, -2087, -2111, -2135, -2159, -2183, -2207, -2231, -2255, -2279, -2303, -2327, -2351, -2375, -2399, -2423, -2447, -2471, -2495, -2519, -2543, -2567, -2591, -2615, -2639, -2663, -2687, -2711, -2735, -2759, -2783, -2807, -2831, -2855, -2879, -2903, -2927, -2951, -2975, -2999, -3023, -3047, -3071, -3095, -3119, -3143, -3167, -3191, -3215, -3239, -3263, -3287, -3311, -3335, -3359, -3383, -3407, -3431, -3455, -3479, -3503, -3527, -3551, -3575, -3599, -3623, -3647, -3671, -3695, -3719, -3743, -3767, -3791, -3815, -3839, -3863, -3887, -3911, -3935, -3959, -3983, -4007, -4031, -4055, -4079, -4103, -4127, -4151, -4175, -4199, -4223, -4247, -4271, -4295, -4319, -4343, -4367, -4391, -4415, -4439, -4463, -4487, -4511, -4535, -4559, -4583, -4607, -4631, -4655, -4679, -4703, -4727, -4751, -4775, -4799, -4823, -4847, -4871, -4895, -4919, -4943, -4967, -4991, -5015, -5039, -5063, -5087, -5111, -5135, -5159, -5183, -5207, -5231, -5255, -5279, -5303, -5327, -5351, -5375, -5399, -5423, -5447, -5471, -5495, -5519, -5543, -5567, -5591, -5615, -5639, -5663, -5687, -5711, -5735, -5759, -5783, -5807, -5831, -5855, -5879, -5903, -5927, -5951, -5975, -5999, -6023, -6047, -6071, -6095, -6119, -6143, -6167, -6191, -6215, -6239, -6263, -6287, -6311, -6335, -6359, -6383, -6407, -6431, -6455, -6479, -6503, -6527, -6551, -6575, -6599, -6623, -6647, -6671, -6695, -6719, -6743, -6767, -6791, -6815, -6839, -6863, -6887, -6911, -6935, -6959, -6983, -7007, -7031, -7055, -7079, -7103, -7127, -7151, -7175, -7199, -7223, -7247, -7271, -7295, -7319, -7343, -7367, -7391, -7415, -7439, -7463, -7487, -7511, -7535, -7559, -7583, -7607, -7631, -7655, -7679, -7703, -7727, -7751, -7775, -7799, -7823, -7847, -7871, -7895, -7919, -7943, -7967, -7991, -8015, -8039, -8063, -8087, -8111, -8135, -8159, -8183, -8207, -8231, -8255, -8279, -8303, -8327, -8351, -8375, -8399, -8423, -8447, -8471, -8495, -8519, -8543, -8567, -8591, -8615, -8639, -8663, -8687, -8711, -8735, -8759, -8783, -8807, -8831, -8855, -8879, -8903, -8927, -8951, -8975, -8999, -9023, -9047, -9071, -9095, -9119, -9143, -9167, -9191, -9215, -9239, -9263, -9287, -9311, -9335, -9359, -9383, -9407, -9431, -9455, -9479, -9503, -9527, -9551, -9575, -9599, -9623, -9647, -9671, -9695, -9719, -9743, -9767, -9791, -9815, -9839, -9863, -9887, -9911, -9935, -9959, -9983, -10007, -10031, -10055, -10079, -10103, -10127, -10151, -10175, -10199, -10223, -10247, -10271, -10295, -10319, -10343, -10367, -10391, -10415, -10439, -10463, -10487, -10511, -10535, -10559, -10583, -10607, -10631, -10655, -10679, -10703, -10727, -10751, -10775, -10799, -10823, -10847, -10871, -10895, -10919, -10943, -10967, -10991, -11015, -11039, -11063, -11087, -11111, -11135, -11159, -11183, -11207, -11231, -11255, -11279, -11303, -11327, -11351, -11375, -11399, -11423, -11447, -11471, -11495, -11519, -11543, -11567, -11591, -11615, -11639, -11663, -11687, -11711, -11735, -11759, -11783, -11807, -11831, -11855, -11879, -11903, -11927, -11951, -11975, -11999, -12023, -12047, -12071, -12095, -12119, -12143, -12167, -12191, -12215, -12239, -12263, -12287, -12311, -12335, -12359, -12383, -12407, -12431, -12455, -12479, -12503, -12527, -12551, -12575, -12599, -12623, -12647, -12671, -12695, -12719, -12743, -12767, -12791, -12815, -12839, -12863, -12887, -12911, -12935, -12959, -12983, -13007, -13031, -13055, -13079, -13103, -13127, -13151, -13175, -13199, -13223, -13247, -13271, -13295, -13319, -13343, -13367, -13391, -13415, -13439, -13463, -13487, -13511, -13535, -13559, -13583, -13607, -13631, -13655, -13679, -13703, -13727, -13751, -13775, -13799, -13823, -13847, -13871, -13895, -13919, -13943, -13967, -13991, -14015, -14039, -14063, -14087, -14111, -14135, -14159, -14183, -14207, -14231, -14255, -14279, -14303, -14327, -14351, -14375, -14399, -14423, -14447, -14471, -14495, -14519, -14543, -14567, -14591, -14615, -14639, -14663, -14687, -14711, -14735, -14759, -14783, -14807, -14831, -14855, -14879, -14903, -14927, -14951, -14975, -14999, -15023, -15047, -15071, -15095, -15119, -15143, -15167, -15191, -15215, -15239, -15263, -15287, -15311, -15335, -15359, -15383, -15407, -15431, -15455, -15479, -15503, -15527, -15551, -15575, -15599, -15623, -15647, -15671, -15695, -15719, -15743, -15767, -15791, -15815, -15839, -15863, -15887, -15911, -15935, -15959, -15983, -16007, -16031, -16055, -16079, -16103, -16127, -16151, -16175, -16199, -16223, -16247, -16271, -16295, -16319, -16343, -16367, -16391, -16415, -16439, -16463, -16487, -16511, -16535, -16559, -16583, -16607, -16631, -16655, -16679, -16703, -16727, -16751, -16775, -16799, -16823, -16847, -16871, -16895, -16919, -16943, -16967, -16991, -17015, -17039, -17063, -17087, -17111, -17135, -17159, -17183, -17207, -17231, -17255, -17279, -17303, -17327, -17351, -17375, -17399, -17423, -17447, -17471, -17495, -17519, -17543, -17567, -17591, -17615, -17639, -17663, -17687, -17711, -17735, -17759, -17783, -17807, -17831, -17855, -17879, -17903, -17927, -17951, -17975, -17999, -18023, -18047, -18071, -18095, -18119, -18143, -18167, -18191, -18215, -18239, -18263, -18287, -18311, -18335, -18359, -18383, -18407, -18431, -18455, -18479, -18503, -18527, -18551, -18575, -18599, -18623, -18647, -18671, -18695, -18719, -18743, -18767, -18791, -18815, -18839, -18863, -18887, -18911, -18935, -18959, -18983, -19007, -19031, -19055, -19079, -19103, -19127, -19151, -19175, -19199, -19223, -19247, -19271, -19295, -19319, -19343, -19367, -19391, -19415, -19439, -19463, -19487, -19511, -19535, -19559, -19583, -19607, -19631, -19655, -19679, -19703, -19727, -19751, -19775, -19799, -19823, -19847, -19871, -19895, -19919, -19943, -19967, -19991, -20015, -20039, -20063, -20087, -20111, -20135, -20159, -20183, -20207, -20231, -20255, -20279, -20303, -20327, -20351, -20375, -20399, -20423, -20447, -20471, -20495, -20519, -20543, -20567, -20591, -20615, -20639, -20663, -20687, -20711, -20735, -20759, -20783, -20807, -20831, -20855, -20879, -20903, -20927, -20951, -20975, -20999, -21023, -21047, -21071, -21095, -21119, -21143, -21167, -21191, -21215, -21239, -21263, -21287, -21311, -21335, -21359, -21383, -21407, -21431, -21455, -21479, -21503, -21527, -21551, -21575, -21599, -21623, -21647, -21671, -21695, -21719, -21743, -21767, -21791, -21815, -21839, -21863, -21887, -21911, -21935, -21959, -21983, -22007, -22031, -22055, -22079, -22103, -22127, -22151, -22175, -22199, -22223, -22247, -22271, -22295, -22319, -22343, -22367, -22391, -22415, -22439, -22463, -22487, -22511, -22535, -22559, -22583, -22607, -22631, -22655, -22679, -22703, -22727, -22751, -22775, -22799, -22823, -22847, -22871, -22895, -22919, -22943, -22967, -22991, -23015, -23039, -23063, -23087, -23111, -23135, -23159, -23183, -23207, -23231, -23255, -23279, -23303, -23327, -23351, -23375, -23399, -23423, -23447, -23471, -23495, -23519, -23543, -23567, -23591, -23615, -23639, -23663, -23687, -23711, -23735, -23759, -23783, -23807, -23831, -23855, -23879, -23903, -23927, -23951, -23975, -23999, -24023, -24047, -24071, -24095, -24119, -24143, -24167, -24191, -24215, -24239, -24263, -24287, -24311, -24335, -24359, -24383, -24407, -24431, -24455, -24479, -24503, -24527, -24551, -24575, -24599, -24623, -24647, -24671, -24695, -24719, -24743, -24767, -24791, -24815, -24839, -24863, -24887, -24911, -24935, -24959, -24983, -25007, -25031, -25055, -25079, -25103, -25127, -25151, -25175, -25199, -25223, -25247, -25271, -25295, -25319, -25343, -25367, -25391, -25415, -25439, -25463, -25487, -25511, -25535, -25559, -25583, -25607, -25631, -25655, -25679, -25703, -25727, -25751, -25775, -25799, -25823, -25847, -25871, -25895, -25919, -25943, -25967, -25991, -26015, -26039, -26063, -26087, -26111, -26135, -26159, -26183, -26207, -26231, -26255, -26279, -26303, -26327, -26351, -26375, -26399, -26423, -26447, -26471, -26495, -26519, -26543, -26567, -26591, -26615, -26639, -26663, -26687, -26711, -26735, -26759, -26783, -26807, -26831, -26855, -26879, -26903, -26927, -26951, -26975, -26999, -27023, -27047, -27071, -27095, -27119, -27143, -27167, -27191, -27215, -27239, -27263, -27287, -27311, -27335, -27359, -27383, -27407, -27431, -27455, -27479, -27503, -27527, -27551, -27575, -27599, -27623, -27647, -27671, -27695, -27719, -27743, -27767, -27791, -27815, -27839, -27863, -27887, -27911, -27935, -27959, -27983, -28007, -28031, -28055, -28079, -28103, -28127, -28151, -28175, -28199, -28223, -28247, -28271, -28295, -28319, -28343, -28367, -28391, -28415, -28439, -28463, -28487, -28511, -28535, -28559, -28583, -28607, -28631, -28655, -28679, -28703, -28727, -28751, -28775, -28799, -28823, -28847, -28871, -28895, -28919, -28943, -28967, -28991, -29015, -29039, -29063, -29087, -29111, -29135, -29159, -29183, -29207, -29231, -29255, -29279, -29303, -29327, -29351, -29375, -29399, -29423, -29447, -29471, -29495, -29519, -29543, -29567, -29591, -29615, -29639, -29663, -29687, -29711, -29735, -29759, -29783, -29807, -29831, -29855, -29879, -29903, -29927, -29951, -29975, -29999, -30023, -30047, -30071, -30095, -30119, -30143, -30167, -30191, -30215, -30239, -30263, -30287, -30311, -30335, -30359, -30383, -30407, -30431, -30455, -30479, -30503, -30527, -30551, -30575, -30599, -30623, -30647, -30671, -30695, -30719, -30743, -30767, -30791, -30815, -30839, -30863, -30887, -30911, -30935, -30959, -30983, -31007, -31031, -31055, -31079, -31103, -31127, -31151, -31175, -31199, -31223, -31247, -31271, -31295, -31319, -31343, -31367, -31391, -31415, -31439, -31463, -31487, -31511, -31535, -31559, -31583, -31607, -31631, -31655, -31679, -31703, -31727, -31751, -31775, -31799, -31823, -31847, -31871, -31895, -31919, -31943, -31967, -31991, -32015, -32039, -32063, -32087, -32111, -32135, -32159, -32183, -32207, -32231, -32255, -32279, -32303, -32327, -32351, -32375, -32399, -32423, -32447, -32471, -32495, -32519, -32543, -32567, -32591, -32615, -32639, -32663, -32687, -32711, -32735, -32759, -32783, -32807, -32831, -32855, -32879, -32903, -32927, -32951, -32975, -32999, -33023, -33047, -33071, -33095, -33119, -33143, -33167, -33191, -33215, -33239, -33263, -33287, -33311, -33335, -33359, -33383, -33407, -33431, -33455, -33479, -33503, -33527, -33551, -33575, -33599, -33623, -33647, -33671, -33695, -33719, -33743, -33767, -33791, -33815, -33839, -33863, -33887, -33911, -33935, -33959, -33983, -34007, -34031, -34055, -34079, -34103, -34127, -34151, -34175, -34199, -34223, -34247, -34271, -34295, -34319, -34343, -34367, -34391, -34415, -34439, -34463, -34487, -34511, -34535, -34559, -34583, -34607, -34631, -34655, -34679, -34703, -34727, -34751, -34775, -34799, -34823, -34847, -34871, -34895, -34919, -34943, -34967, -34991, -35015, -35039, -35063, -35087, -35111, -35135, -35159, -35183, -35207, -35231, -35255, -35279, -35303, -35327, -35351, -35375, -35399, -35423, -35447, -35471, -35495, -35519, -35543, -35567, -35591, -35615, -35639, -35663, -35687, -35711, -35735, -35759, -35783, -35807, -35831, -35855, -35879, -35903, -35927, -35951, -35975, -35999, -36023, -36047, -36071, -36095, -36119, -36143, -36167, -36191, -36215, -36239, -36263, -36287, -36311, -36335, -36359, -36383, -36407, -36431, -36455, -36479, -36503, -36527, -36551, -36575, -36599, -36623, -36647, -36671, -36695, -36719, -36743, -36767, -36791, -36815, -36839, -36863, -36887, -36911, -36935, -36959, -36983, -37007, -37031, -37055, -37079, -37103, -37127, -37151, -37175, -37199, -37223, -37247, -37271, -37295, -37319, -37343, -37367, -37391, -37415, -37439, -37463, -37487, -37511, -37535, -37559, -37583, -37607, -37631, -37655, -37679, -37703$

[ETAU] Tauxel, Géométrie

[SATI] Samuel, Théorie algébrique des nombres.

[COM] Combes, Algèbre et Géométrie ^(connaissances historiques)

[NOU] Nouvelin, Agrég de Maths épreuve orale.

[SILV] Silverman - Tate / Rational points on elliptic curves

[BER] Berkey, Modules: théorie, pratique ...
et un peu d'arithmétique

[FGNA 2] Oeuvres X-ENS Analyse 2

[FGNA1] Fresnel - Girard, Nicolas.

" mais Algèbre)

[HELLE] Hellegouarch, Invitation aux mathématiques de Fermat - Wile.

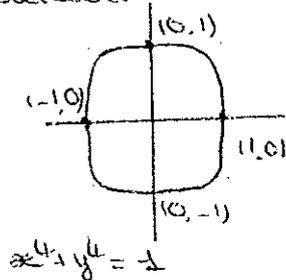
[1001] De Koningde / Percier - 1001 problèmes
en théorie classique des nombres
(plein d'exemples!!)

[SIEP] Sierpinski - 250 problèmes ni élémentary
number theory (existe aussi en français)

[DUN] Dumortier - 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
$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$
 possède des solutions si $\text{pgcd}(m, n)$
divise $a - b$.

[1001] pages 2-76

Théorème des deux carrés

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

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 impair¹.
On a l'équivalence suivante :

$$p \in \Sigma \iff p \equiv 1 \pmod{4}$$

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 :

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

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

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

Cet automorphisme nous permet de définir une "norme"

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

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 $N(z) = N(z') = 1 \Rightarrow a^2 + b^2 = 1 \Rightarrow (a = 0 \text{ et } b = \pm 1) \text{ ou } (a = \pm 1 \text{ et } b = 0)$.

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 :

$$n \in \Sigma \iff \exists z \in \mathbb{Z}[i] / n = N(z)$$

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 $2 \not\equiv 1 \pmod{4}$.

Proposition 3

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

Preuve :

Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$. 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 $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. Ainsi,

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

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 rappelle le théorème à démontrer :

Théorème

Soit p un nombre premier impair.

On a l'équivalence suivante :

$$p \in \Sigma \iff p \equiv 1 \pmod{4}$$

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

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,

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

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

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

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 $\mathcal{P} = \{\text{nombre premiers}\}$.

Alors,

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

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. ROBOT

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 $k \geq 2$), 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 $k \geq 2$. Écrivons la décomposition en facteurs premiers de a, b et c :

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

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 $\alpha_p\beta_p = 0$ 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 $d = 1$.

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 :

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

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 (*), p'^2 divise x^p donc p' divise x .

Comme $y \equiv -z [p']$, on en déduit une nouvelle "égalité"

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

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'Euclide³, $p' \mid p$ ou $p' \mid y^{p-1}$ dont $p' \mid y$.
 \leftrightarrow Si $p' \mid p$ (ie $p' = p$), cela signifie que $p \mid x$ (absurde par hypothèse).
 \leftrightarrow Si $p' \mid y$, 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 puissance p -ième $(-x^p)$ il existe $(a, \alpha) \in \mathbb{Z}^2$ tel que

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

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

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

Supposons par l'absurde qu'aucun des trois entiers x, y, z 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 $(0 \equiv) x^p + y^p + z^p$ 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 x 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 $b^p + c^p - a^p = 2x \equiv 0 [q]$ (**).

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 $y \equiv c^p \equiv \pm 1 [q]$ (c'est le début de l'étape 3).

De même, $z \equiv \pm 1 [q]$.

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 (**)).

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

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

■

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 infini.

♣ 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 révéler 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