Équations Diophantiennes, Groupe C

15 janvier 2023

1 Cours

Méthodes courantes :
1 : « Factoriser » + « nombre premiers»
Par exemple pour résoudre

$$ab = 15$$

On peut utiliser que les facteurs premiers de 15 sont 3 et 5.

En général il ne faut pas oublier d'utiliser des identités remarquables. Par exemple pour

$$a^2 - b^2 = 15$$
$$(a-b)(a+b) = 15$$

$$\Rightarrow a + b = 5, 3, ...$$

Comme identité remarquable on a aussi

— Pour tout n,

$$a^n - b^n = (a-b)(a^{n-1} + ba^{n-2} + b^2a^{n-3} + \cdots + b^{n-1})$$

— Si n est impair Pour tout n,

$$a^n + b^n = (a+b)(a^{n-1} - ba^{n-2} + b^2a^{n-3} + \cdots + b^{n-1})$$

— Avec un polynome $P(a) = p_0 + p_1a + \cdots + p_na^n$

$$P(b) - P(a) = p_1(b-a) - b_2(b^2 - a^2) + \cdots + p_n(b^n - a^n)$$

$$\Rightarrow b - a | P(b) - P(a)$$

— Moins connu : Égalité de Sophie Germain

$$\begin{aligned}
a^4 + 4b^4 &= (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2) \\
&= a^4 - 2a^3b + 2a^2b^2 + 2a^3b - 4a^2b^2 + 4ab^3 \\
&+ 2b^2a^2 - 4ab^3 + 4b^4 \\
&= a^4 + 4b^4
\end{aligned}$$

2- Autre idée TRÈS COURANTE est d'utiliser « Modulo ».

Parfois choisir un bon modulo (être astucieux !) donne des éléments de preuve voir résoud complètement l'exercice.

Astuce pour un modulo p avec p premier : En règle général on souhaite que lorsque l'on considère $x, x^2, x^3, \cdots x^k = 1[p]$ on ait k le plus petit possible. Avec le petit Théorème de Fermat les ordres des éléments divise $(p-1)$. Donc Idée : « choisir p » tel que les puissances qui apparaissent dans l'exerice divise $p-1$.

3- «Trouver des bornes » et se restreindre à un nombre fini de cas.

Obtenir des inégalités sur les entiers. Puis tester tous les cas (si il ne sont pas trop nombreux).

2 Exercices

Exercice 1. Trouver tous les entiers $n \geq 1$ tels que $3^{n-1} + 5^{n-1}$ divise $3^n + 5^n$.

Solution 1. « Idée : essayer de tuer le plus grand élément »

$$\begin{aligned}
&3^{n-1} + 5^{n-1} | 3^n + 5^n \\
\Rightarrow &3^{n-1} + 5^{n-1} | 3^n + 5^n - 5 \times (3^{n-1} + 5^{n-1}) \\
\Rightarrow &3^{n-1} + 5^{n-1} | 3^n - 5 \times 3^{n-1} \\
\Rightarrow &3^{n-1} + 5^{n-1} | 2 \times 3^{n-1}
\end{aligned}$$

Plusieurs manières pour terminer :

Lemme 1. *$a|b$ alors $|a| \leq |b|$.*

Si $n - 1 > 0$

$$3^{n-1} + 5^{n-1} > 3^{n-1} + 3^{n-1} = 2 \times 3^{n-1}$$

$\Rightarrow$ pas de solution

Si $n = 1$:

$$3^{n-1} + 5^{n-1} = 1 + 1 = 2$$
$$3^n + 5^n = 3 + 5 = 8$$

on a bien 2|8 donc pour n=1 OK.

Autre méthode Nombre premiers :

Lemme 2. *Si $x | p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ alors $x = p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k}$ avec $\beta_1 \leq \alpha_1$, $\beta_2 \leq \alpha_2$...*

Dans notre cas

$$x | 2 \times 3^{n-1} \Rightarrow x = 2^\alpha 3^\beta \quad \alpha \leq 1 \quad \text{et} \quad \beta \leq n-1$$

Donc $3^{n-1} + 5^{n-1} | 2 \times 3^{n-1} \Rightarrow$ Tous les facteurs premiers de $3^{n-1} + 5^{n-1}$ sont soit 2 soit 3 et de plus 4 ne divise pas $3^{n-1} + 5^{n-1}$.

Si $n > 1$

$$3 | 3^{n-1} + 5^{n-1} \Rightarrow 3 | 5^{n-1} \quad \text{Absurde}$$

Conclusion $n = 1$ est l'unique solution.

Exercice 2. Montrer que $n^4 + 4^n$ n'est jamais un nombre premier pour $n > 1$.

Solution 2. Remarque si $n = 0[2]$ alors $n^4 + 4^n$ est pair donc n'est pas premier.

Si $n = 2k + 1$ alors

$$\begin{aligned} n^4 + 4^n &= n^4 + 4 \times 4^{2k} \\ &= n^4 + 4 \times 2^{4k} \\ &= n^4 + 4 \times (2^k)^4 \\ &= (n^2 + 2n \times 2^k + 2 \times 2^{2k})(n^2 - 2n \times 2^k + 2 \times 2^{2k}) \end{aligned}$$

où on a utilisé l'égalité de Sophie Germain

$$«a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)»$$

On a trouvé une factorisation. On peut vérifier que $n^2 - 2n \times 2^k + 2 \times 2^{2k} > 1$. Conclusion $n^4 - 4^n$ n'est pas premier.

Exercice 3. L'équation $a^2 + b^2 = 1003$ n'admet aucune solution.

Solution 3. Ici on regarde modulo 4.

x	0	1	2	3
x^2	0	1	0	1

Donc un carré modulo 4 est toujours égale à 0 ou 1. $1003 = 3[4]$. Pas de solutions possible (au plus de carrés donnerait 2 modulo 4).

Exercice 4. Soient $m, n \geq 1$ des entiers. Montrer que $3^m + 3^n + 1$ n'est pas un carré parfait.

Remarque : ici modulo 4 n'est pas suffisant m pair et n impair

$$3^m + 3^n + 1 = 1 - 1 + 1 = 1[4]$$

pourrait être un entier à priori.

Solution 4. Ici on regarde modulo 8 (Astuce : $(-x)^2 = x^2$ donc le tableau est symétrique)

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1

Les carrés modulo 8 sont $0, 1, 4$. On a également

$$\begin{aligned} 3^2 &= 9 = 1[8] \\ 3^{2k} &= 1^k = 1[8] \\ 3^{2k+1} &= 3 \times 1^k = 3[8] \end{aligned}$$

Les puissances de 3 sont égales à 1 ou 3 modulo 8. Pour finir

$$3^n + 3^m + 1 = \begin{cases} 1 + 1 + 1 = 3[8] \\ 3 + 1 + 1 = 5[8] \\ 3 + 3 + 1 = 7[8] \end{cases}$$

Donc ce n'est jamais un carré.

Exercice 5. Trouver tous les entiers $a, b \geq 1$ tels que les deux quantités

$$\frac{a^2+b}{b^2-a} \quad \text{et} \quad \frac{b^2+a}{a^2-b}$$

soient des nombres entiers.

Indication : $(n+1)^2 - n^2 = 2n+1$: En particulier la différence entre 2 carrés $b^2 - a^2$ est au moins $\geq 2a+1$

.

Solution 5. On a

$$b^2 - a | a^2 + b \quad \text{et} \quad a^2 - b | b^2 + a$$
$$\Rightarrow b^2 - a \leq a^2 + b \quad \text{et} \quad a^2 - b \leq b^2 + a$$

Idée : On devrait avoir $b^2 \lesssim a^2$ et $a^2 \lesssim b^2$ car les carrés devrait être plus grand que le reste. On aimerait essayer de prouver que a et b sont très proche.

Ici on peut échanger a et b. Donc supposons que $b \geq a$.

Si $b > a+1$ alors

$$b^2 - b = b(b-1) > (a+1)a = a^2 + a$$

Absurde car $b^2 - b \leq a^2 + a$. Conclusion $a \leq b \leq a+1$

(Autre méthode

$$\begin{aligned} b^2 - a^2 \leq b + a &\Rightarrow (b-a)(a+b) \leq (b+a) \\ &\Rightarrow b - a \leq 1 \end{aligned}$$

Conclusion $b = a$ ou $b = a+1$.

— Cas $b = a$

$$\begin{aligned} a^2 - a | a^2 + a &\Rightarrow a - 1 | a + 1 \\ &\Rightarrow a - 1 | a + 1 - (a-1) \\ &\Rightarrow a - 1 | 2 \end{aligned}$$

Donc $a = 2$ ou $a = 3$.

Pour $a = 2$: $4 + 2 = 6$ et $4 - 2 = 2$ OK.

Pour $a = 3$: $9 - 3 = 6$ et $9 + 3 = 12$ et $6 | 12$ OK.

Cas $a = 1$ est interdit (ne pas diviser par 0).

— Cas $b = a+1$

$$b^2 - a = a^2 + a + 1$$

$$a^2 + b = a^2 + a + 1$$

OK. et $(a^2 - b | b^2 + a)$

$$a^2 - b = a^2 - a + 1$$

$$b^2 + a = a^2 + 3a + 1$$

Alors

$$\begin{aligned}
&a^2 - a + 1 | a^2 + 3a + 1 \\
\Rightarrow &a^2 - a + 1 | a^2 + 3a + 1 - (a^2 - a + 1) \\
\Rightarrow &a^2 - a + 1 | 4a
\end{aligned}$$

On a toujours $a^2 - a = a(a-1) = 0[2]$ donc a $a^2 - a + 1 = 1[2]$ (donc premier avec 4). Rappel :

Lemme 3. *(Lemme de Gauss) Si*

$$a|bc$$

et pgcd$(a,b) = 1$ *(a, b premier entre eux) alors* $a|c$

Donc on obtient $a^2 - a + 1 | a$.

Il faut que $a^2 - a + 1 \leq a$ donc $a^2 - 2a + 1 \leq 0$ donc $(a-1)^2 \leq 0$ donc $a = 1$.

Conclusion : les solutions sont $(a = 1, b = 2)$ et $a = b = 2$ et $a = b = 3$. (et les symmétrie en échangeant a et b).

Exercice 6. Trouver tous les entiers x, y tels que $15x^2 - 7y^2 = 9$.

Solution 6. 15 et 9 sont multiple de 3 donc $3|7y^2$ donc $3|y$. On écrit $y = 3y'$.

$$15x^2 - 7 \times 9 \times (y')^2 = 9$$

donc

$$5x^2 - 7 \times 3 \times (y')^2 = 3$$

Même chose on a $3|5x^2$ donc $3|x$. On écrit $x = 3x'$. Alors

$$5 \times 9 \times (x')^2 - 7 \times 3 \times (y')^2 = 3$$

donc

$$15 \times (x')^2 - 7 \times (y')^2 = 1$$

On regarde l'équation modulo 3

$$-(y')^2 = 1[3] \Rightarrow (y')^2 = 2[3]$$

Or les carrés modulo 3 sont seulement 0 ou 1

x	0	1	2
x^2	0	1	1

Absurde.

Exercice 7. Trouver les deux derniers chiffres de 1032^{1032}.

Solution 7. Traduction : Calculer $1032^{1032}[100]$. Par le Lemme des restes chinois

$$\Leftrightarrow \text{Calculer} \begin{cases} 1032^{1032}[4] \\ 1032^{1032}[25] \end{cases}$$

($100 = 4 \times 25$ et 4 et 25 sont premiers entre eux.) On a

$$1032^{1032}[4] = 0[4]$$

On a aussi

$$1032^{1032} = 7^{1032}[25]$$

$$7^2 = 49 = -1[25]$$

Donc

$$7^{1032} = (-1)^{516}[25] = 1[25]$$

Il suffit donc de trouver un $0 \leq x < 100$ tel que

$$\begin{cases} x = 0[4] \\ x = 1[25] \end{cases}$$

$x = 1[25] \Rightarrow x \in \{1, 26, 51, 76\}$. Ici 76 fonctionne. Conclusion : la solution est 76.

Exercice 8. Soit p un nombre premier. Montrer que tout diviseur premier de $2^p - 1$ est strictement plus grand que p.

(Indice : ordre et petit Théorème de Fermat.)

Solution 8. Soit q un diviseur premier de $2^p - 1$. Donc

$$2^p - 1 = 0[q]$$
$$2^p = 1[q]$$

Lemme 4. $x^a = 1[q] \Leftrightarrow$ *ordre*(x) *divise* a.

L'ordre de 2 (dans $\mathbb{Z}/q\mathbb{Z}^*$) divise p. Donc ordre$(2) = 1$ soit p car p est premier. Comme $2 \neq 1[q]$ on a ordre$(2) = p$.

Par le petit théorème de Fermat

$$2^{q-1} = 1[q]$$

Par le même argument on a ordre(2) divise $q - 1$. Donc $p | q - 1$ en particulier $p \leq q - 1$ donc $p < q$.

Exercice 9. Montrer que quel que soit $n > 1$, $n^5 + 7$ n'est pas un carré.

Indice : puissance $= 5$. p tel que $5 | p - 1$?

Ici choisir $p = 11$ va fonctionner

Exercice 10. Montrer que 19^{19} ne peut pas s'écrire comme somme d'un cube et d'une puissance quatrième.

Indice : puissances $= 3$ et 4. p tel que $3|p-1$ et $4|p-1$?

Ici choisir $p = 13$ va fonctionner

Exercice 11. Trouver tous les entiers $x, y \geq 1$ tels que $x^3 - y^3 = xy + 61$.

Exercice 12. Trouver tous les couples d'entiers (m, n) tels que $m^5 - n^5 = 16mn$.