Equations en nombres entiers

Stéphane Fischler
(Université Paris XI - Orsay)

Lycée Michelet (Vanves), 3 mai 2006

Dans le cadre des « Promenades Mathématiques »

Plan

1. Une histoire d'allumettes.
2. Un jeu de construction.
3. Le théorème de Fermat.
4. La conjecture de Catalan.
5. Les nombres 1111…111.

Merci à Emmanuel Peyre !

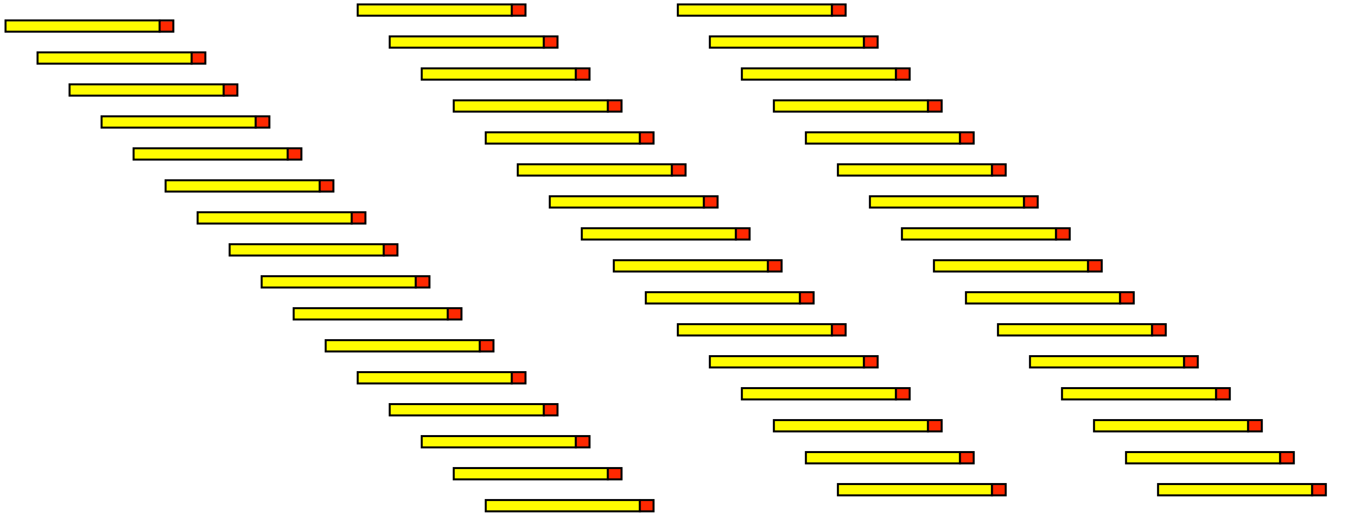
Plan

1. **Une histoire d'allumettes.**
2. *Un jeu de construction.*
3. *Le théorème de Fermat.*
4. *La conjecture de Catalan.*
5. *Les nombres 1111…111.*

Merci à Emmanuel Peyre !

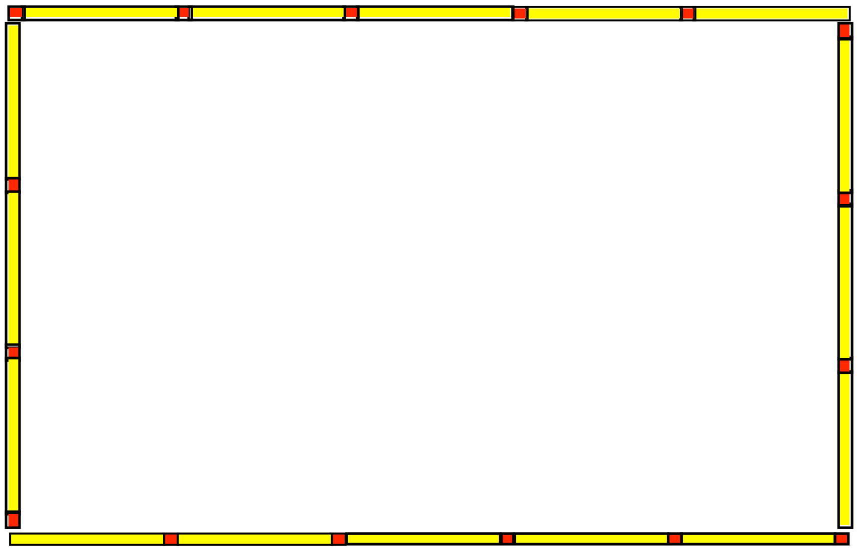
Allumettes

On joue avec des allumettes…



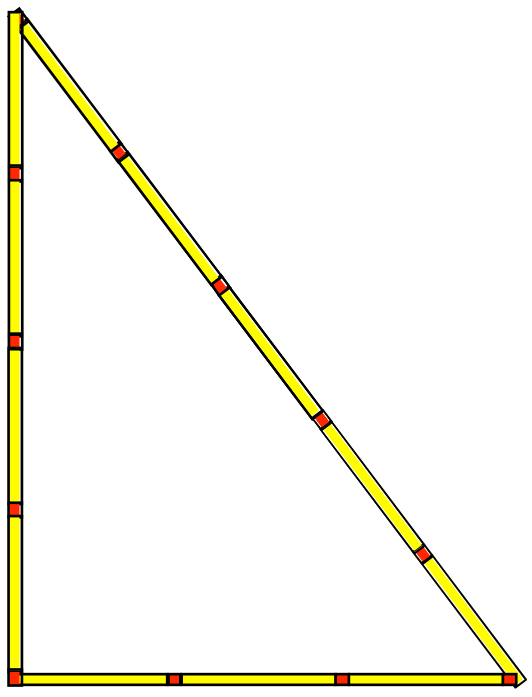
Allumettes

Un rectangle, c’est facile !



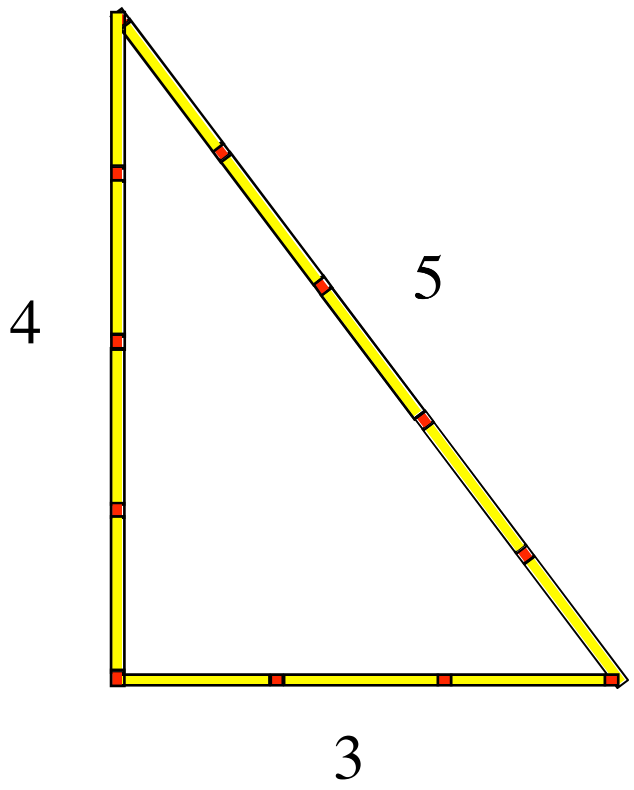
Allumettes

Un triangle rectangle, c'est plus dur



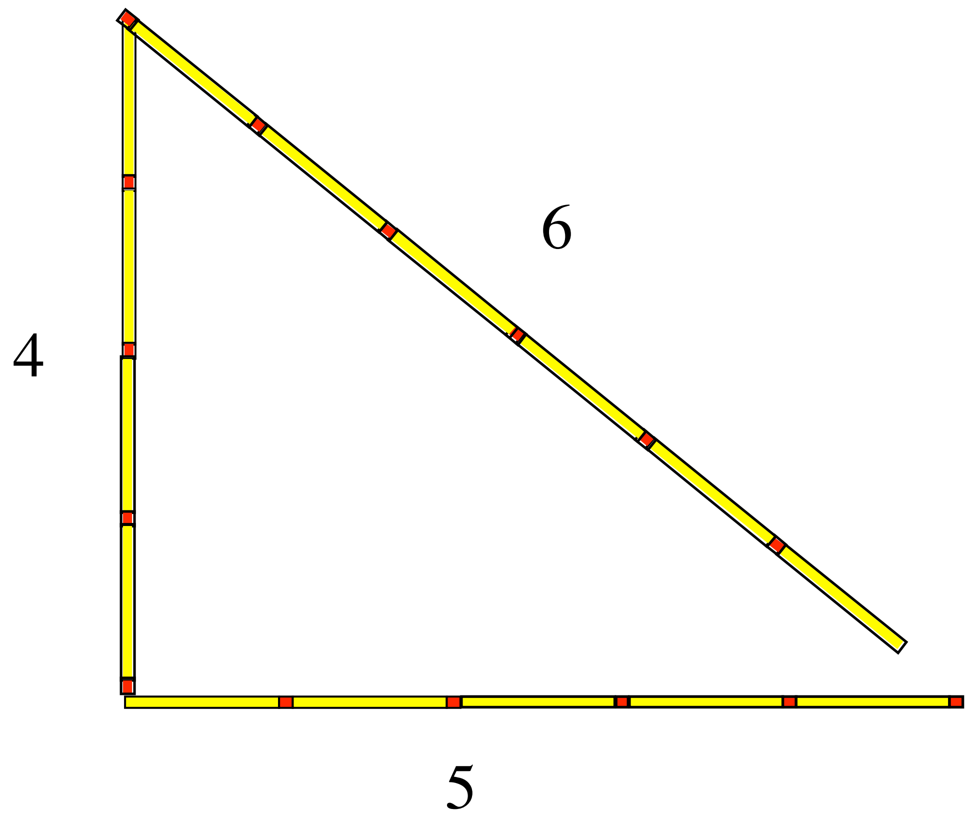
Allumettes

Un triangle rectangle, c'est plus dur



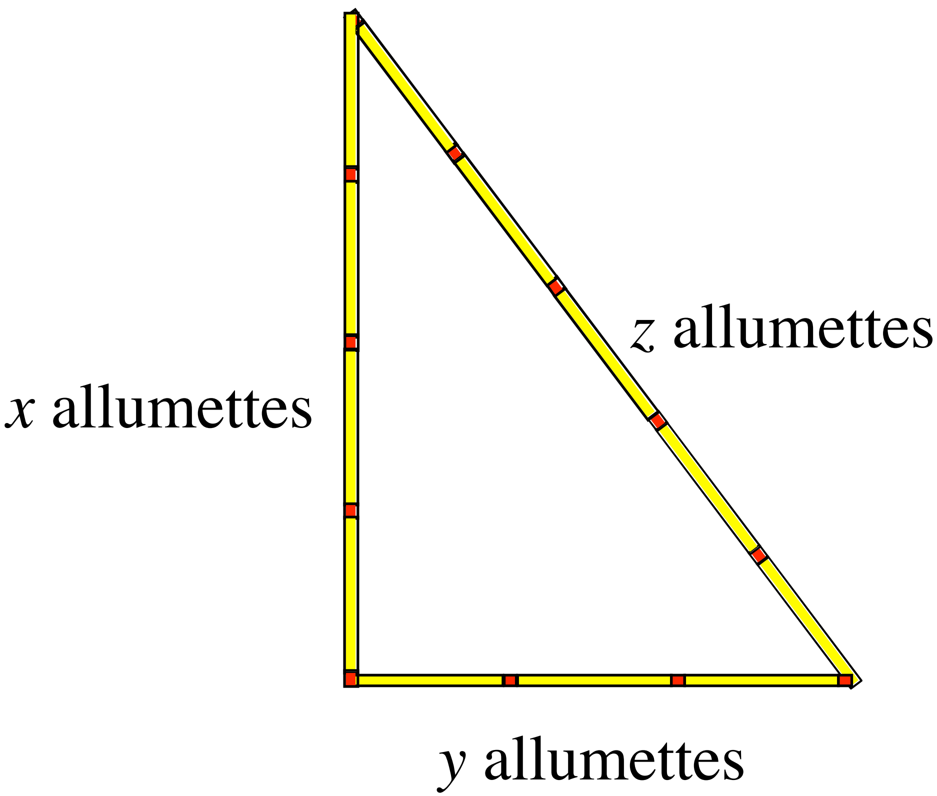
Allumettes

Ça ne marche pas toujours !



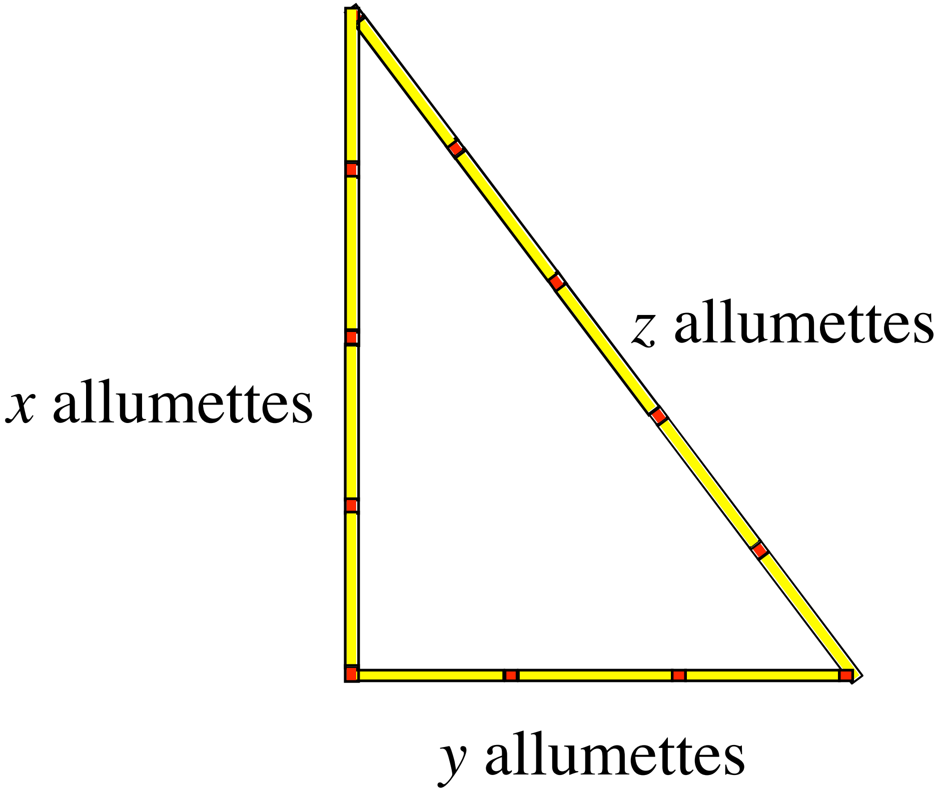
Allumettes

C’est un problème de maths !



Allumettes

Théorème de Pythagore



$$x^2 + y^2 = z^2$$

Traduction du problème

Trouver des entiers x, y et z tels que

$$x^2 + y^2 = z^2$$

(avec $x, y, z \geq 1$)

Solution du problème (1)

Théorème : Il existe une infinité d'entiers x,y,z tels que $x^2 + y^2 = z^2$.

Exemples :

$$3^2 + 4^2 = 5^2$$

$$5^2 + 12^2 = 13^2$$

Solution du problème (2)

Théorème : On a $x^2 + y^2 = z^2$ si, et seulement si :

$x = 2mn$		$x = m^2 - n^2$
$y = m^2 - n^2$	ou	$y = 2mn$
$z = m^2 + n^2$		$z = m^2 + n^2$

avec $m > n \geq 1$.

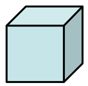
Plan

1. *Une histoire d'allumettes.*
2. **Un jeu de construction.**
3. *Le théorème de Fermat.*
4. *La conjecture de Catalan.*
5. *Les nombres 1111…111.*

Construction

Un jeu de construction

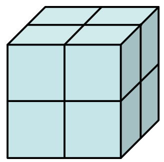
Léa et Léo jouent avec des petits cubes, comme celui-ci :



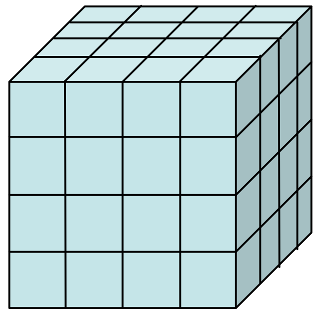
Ils assemblent leurs petits cubes pour faire des gros cubes.

Construction

Chacun le fait de son côté…



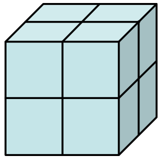
Léa



Léo

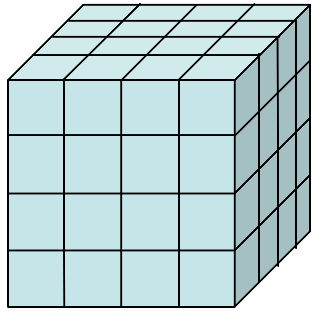
Construction

avec ses propres petits cubes.



Léa

$2 \times 2 \times 2 = 8$ petits cubes



Léo

$4 \times 4 \times 4 = 64$ petits cubes

Puis ils les mettent en commun !

Ensemble, ils ont $8 + 64 = 72$ petits cubes…

Construction

Puis ils les mettent en commun !

Ensemble, ils ont 8 + 64 = 72 petits cubes…

Ils ne peuvent pas faire un gros cube ! Car :

- Gros cube de côté 4 : 64 petits cubes
  donc il en reste !
- Gros cube de côté 5 : 125 petits cubes
  donc il en manque !

Construction

Peuvent-ils parfois réussir ?

Léa a x^3 petits cubes : il en fait un gros cube de côté x.

Léo a y^3 petits cubes : il en fait un gros cube de côté y.

A eux deux ils ont x^3+y^3 petits cubes…

Construction

Peuvent-ils parfois réussir ?

Léa a x^3 petits cubes : il en fait un gros cube de côté x.
Léo a y^3 petits cubes : il en fait un gros cube de côté y.

A eux deux ils ont x^3+y^3 petits cubes : est-ce que ça peut faire z^3 ? On veut :

$$x^3 + y^3 = z^3$$

Non, jamais !

- *Théorème :* Il n'existe pas d'entiers $x,y,z \geq 1$ tels que

$$x^3 + y^3 = z^3$$

- Démontré par Euler (1707 - 1783).
- Donc Léa et Léo ne pourront jamais réunir leurs cubes pour en faire un gros !

Plan

1. *Une histoire d'allumettes.*
2. *Un jeu de construction.*
3. ***Le théorème de Fermat.***
4. *La conjecture de Catalan.*
5. *Les nombres 1111…111.*

Résumé

Allumettes : $x^2 + y^2 = z^2$

Construction : $x^3 + y^3 = z^3$

Généralisation : $x^n + y^n = z^n$

avec un entier $n \geq 2$.

Théorème de Fermat

Théorème : Si $n \geq 3$, il n'existe pas d'entiers $x,y,z \geq 1$ tels que

$$x^n + y^n = z^n$$

Conjecturé par Fermat vers 1636…

… démontré par Wiles en 1994 !

Enoncé par Fermat (1636)

Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere.

Rappels de 1ère …

Pour un polynôme de degré 2 :

$$a\,X^2 + b\,X + c \quad \text{avec} \quad a = 1$$

Racines : $(-b-\sqrt{\Delta})/2$ et $(-b+\sqrt{\Delta})/2$.

Distance entre les racines : $\sqrt{\Delta}$.

Donc *le discriminant est le carré de la distance entre les deux racines*.

Stratégie de preuve (1)

Si $x^n + y^n = z^n$, on considère le polynôme

$$B\ (B - x^n)\ (B + y^n)$$

Racines : 0, x^n et $-y^n$.

Distances entre les racines : x^n, y^n et $x^n + y^n = z^n$.

Discriminant : $\Delta = (xyz)^{2n}$

(c'est le carré du produit des distances entre les racines)

Stratégie de preuve (2)

Ce polynôme incite à étudier l'équation

$$A^2 = B\,(B - x^n)\,(B + y^n)$$

qui est celle d'une

« courbe elliptique »

dont le discriminant Δ est une puissance $2n$-ième…

Fermat

Stratégie de preuve (3)

Cette courbe elliptique est tellement particulière qu'elle ne peut pas être *modulaire* (si $n \geq 3$).

Synthèse : Si $x^n + y^n = z^n$ avec $n \geq 3$ alors on a construit une courbe elliptique *qui n'est pas modulaire*.

Stratégie de preuve (4)

Conjecture (Taniyama - Weil) : Une telle courbe elliptique non modulaire ne peut pas exister.

Wiles a démontré cette conjecture, donc le théorème de Fermat.

Et après Fermat ?

Théorème : L'équation

$$x^n + y^n = 2z^n \qquad \text{avec } n \geq 3$$

n'a que des solutions triviales $x,y,z \geq 1$.

Solutions triviales : telles que $x = y = z$.

Démontré par Darmon et Merel (1997).

Plan

1. *Une histoire d'allumettes.*
2. *Un jeu de construction.*
3. *Le théorème de Fermat.*
4. **La conjecture de Catalan.**
5. *Les nombres 1111…111.*

Puissances pures

- Carrés : $1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16,$
  $5^2 = 25, \quad 6^2 = 36, \quad 7^2 = 49, \dots$
- Cubes : $1^3 = 1, \quad 2^3 = 8, \quad 3^3 = 27, \quad 4^3 = 64,$
  $5^3 = 125, \quad 6^3 = 216, \quad 7^3 = 343, \dots$
- Puissances quatrièmes : $1^4 = 1, \quad 2^4 = 16, \dots$
- Puissances cinquièmes : $1^5 = 1, \quad 2^5 = 32, \dots$
- etc.

Catalan

Dans l’ordre croissant

1 4 8 9 16 25 27 32 36 49 64 …

On voit que 8 et 9 sont consécutifs.

Est-ce que ce sont les seules puissances pures consécutives ?

Conjecture de Catalan

- *Théorème :* Les seules puissances pures consécutives sont 8 et 9.

- Conjecturé par Catalan en 1844.
- Démontré par Mihailescu en 2002.

Autre formulation

- *Conjecture de Catalan :* L'équation

$$x^a = y^b + 1$$

admet une seule solution x,a,y,b avec $a,b \geq 2$:

$$(x,a,y,b) = (3,2,2,3).$$

- Tijdeman, 1976 : les solutions sont en nombre fini.

Plan

1. *Une histoire d'allumettes.*
2. *Un jeu de construction.*
3. *Le théorème de Fermat.*
4. *La conjecture de Catalan.*
5. **Les nombres 1111…111.**

Nombres formés de 1

- 11 n’est pas une puissance pure.
- 111 n’est pas une puissance pure car :

$10^2 = 100 < 111 < 121 = 11^2$

$4^3 = 64 < 111 < 125 = 5^3$

$3^4 = 81 < 111 < 256 = 4^4$

$2^5 = 32 < 111 < 243 = 3^5$

Nombres formés de 1

- 1111 n'est pas une puissance pure car :

  $33^2 = 1089 < 1111 < 1156 = 34^2$

  $10^3 = 1000 < 1111 < 1331 = 11^3$

  $5^4 = 625 < 1111 < 1296 = 6^4$

  $4^5 = 1024 < 1111 < 3125 = 5^5$

  $3^6 = 729 < 1111 < 4096 = 4^6$

  $2^7 = 128 < 1111 < 2187 = 3^7$

De même…

- 11111 n’est pas une puissance pure.
- 111111 n’est pas une puissance pure.
- 1111111 n’est pas une puissance pure.
- etc.

Un nombre formé de 1 peut-il être une puissance pure ?

111…11

- *Théorème :* Un nombre formé de n fois le chiffre 1 ne peut jamais être une puissance pure (si $n \geq 2$).

- Démontré par Bugeaud et Mignotte (1999).

Comment généraliser ?

- $11111 = 99999 / 9$
- $99999 = 100000 - 1 = 10^5 - 1$
- $$\underbrace{111....111}_{n \text{ chiffres}} = \frac{10^n - 1}{10 - 1}$$
- Puissance pure : y^q avec $q \geq 2$.

Théorème de Bugeaud-Mignotte

Théorème : L'équation

$$\frac{10^n - 1}{10 - 1} = y^q$$

n'a aucune solution $n, y, q \geq 2$.

Généralisation

Conjecture : L'équation

$$\frac{x^n - 1}{x - 1} = y^q$$

admet exactement trois solutions (x,n,y,q)

avec $x,y,q \geq 2$ et $n \geq 3$.

111…11

Les trois solutions

$$\frac{3^5 - 1}{3 - 1} = 11^2$$

$3^5 = 243$

$$\frac{7^4 - 1}{7 - 1} = 20^2$$

$7^4 = 2401$

$$\frac{18^3 - 1}{18 - 1} = 7^3$$

$18^3 = 5832$ et $7^3 = 343$

On en est loin…

On ne sait pas démontrer que l'équation

$$\frac{x^n - 1}{x - 1} = y^q$$

n'admet qu'un nombre fini de solutions

avec $x,y,q \geq 2$ et $n \geq 3$.

Seuls certains cas particuliers sont connus.

Méthodes de démonstration

- Théorie algébrique des nombres :

  Cas particuliers de Fermat ; Mihailescu.
- Modularité des courbes elliptiques :

  Wiles ; Merel-Darmon.
- Formes linéaires de logarithmes :

  Tijdeman ; Bugeaud-Mignotte.
- Et il y en a d'autres !

Merci pour votre attention !

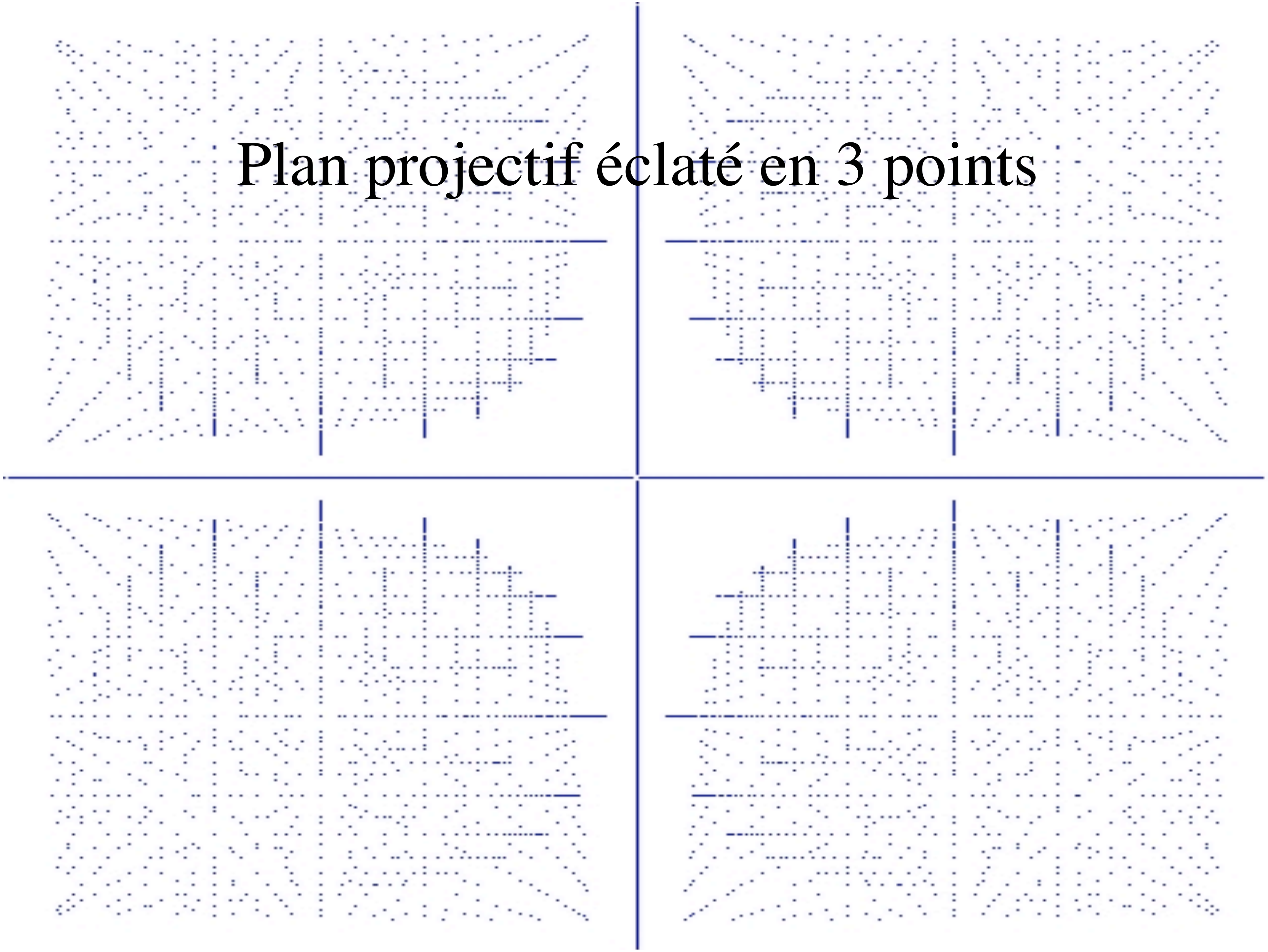
Sur le même thème :

exposé d’Eva Bayer à la BNF,

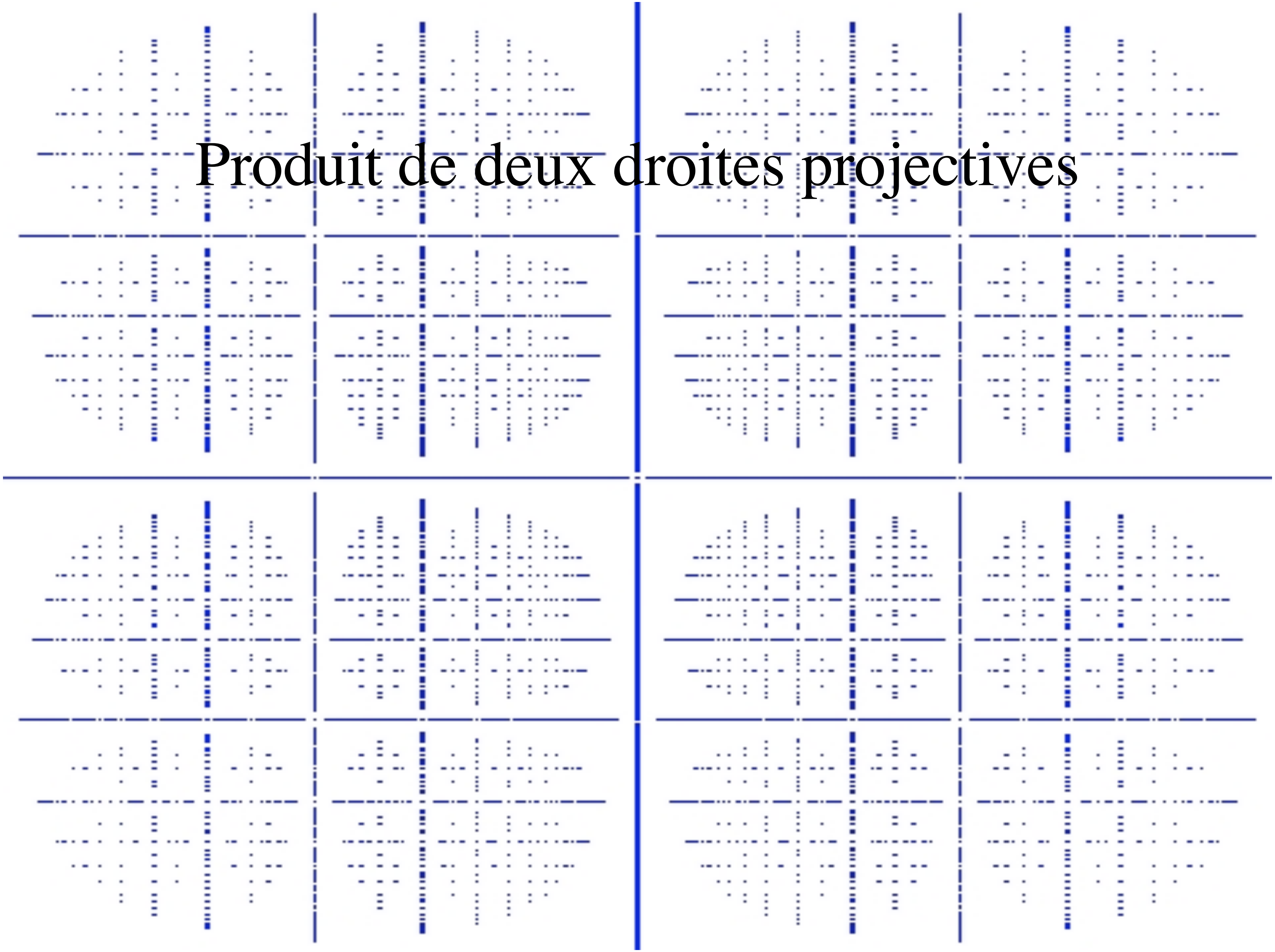
le 10 mai à 18h30

Hermann Minkowski, grand prix de l'Académie des sciences à 18 ans

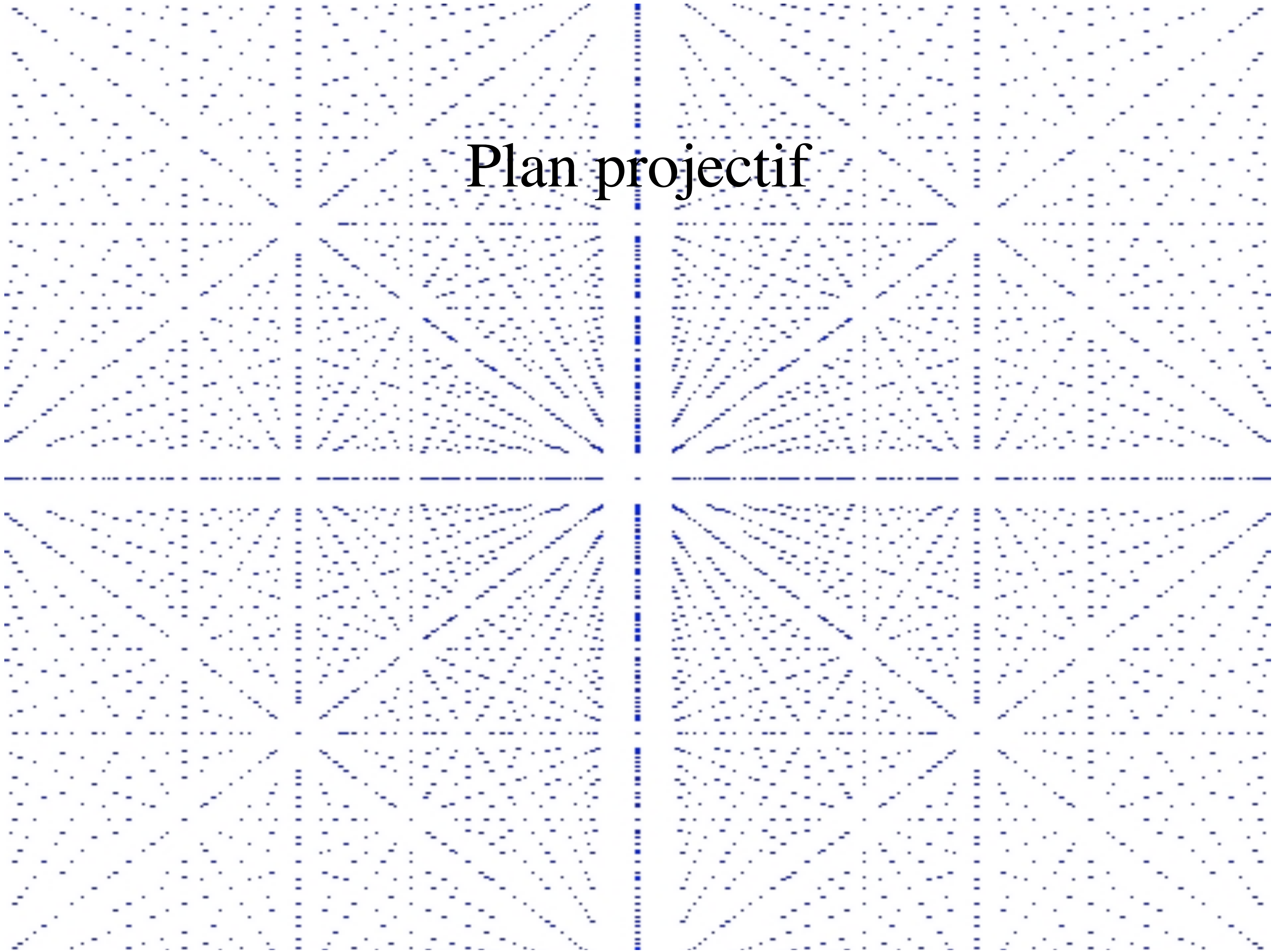
Plan projectif éclaté en 3 points



Produit de deux droites projectives



Plan projectif



Droite projective sur $\mathbf{Q}(i)$