

Recherche en théorie des nombres

Siva Nair

Université de Montréal

4 Mars

SAMARI 2024

Théorie des Nombres – c'est quoi?

- Propriétés des entiers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3\dots\},$$

les rationnels

$$\mathbb{Q} = \left\{ \frac{1}{2}, -\frac{3}{4}, \frac{98453}{2024}, \dots \right\},$$

et leurs généralisations.

- **Théorème fondamental de l'arithmétique:** Tout nombre entier s'écrit de façon unique comme un produit de nombres premiers

$$2, 3, 5, 7, 11, \dots$$

Théorie des Nombres – c'est quoi?

- **Théorie des nombres algébrique**
- **Théorie des nombres analytique**
- Autres branches:
 - ▶ Théorie probabiliste des nombres
 - ▶ Géométrie arithmétique
 - ▶ Théorie algorithmique des nombres
 - ▶ Combinatoire additive
- On veut trouver des solutions entières (ou rationnelles) à certaines équations.

Trouvez les solutions en entiers à l'équation

$$x^2 + y^2 = z^2, \quad x^3 + y^3 = z^3, \quad x^n + y^n = z^n, \quad n \geq 3$$

Théorème (grand théorème de Fermat, posé par lui en 1637, résolu par Wiles en 1995)

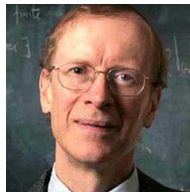
Il n'existe pas de nombres entiers $x, y, z > 0$ tels que

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

dès que $n \geq 3$.

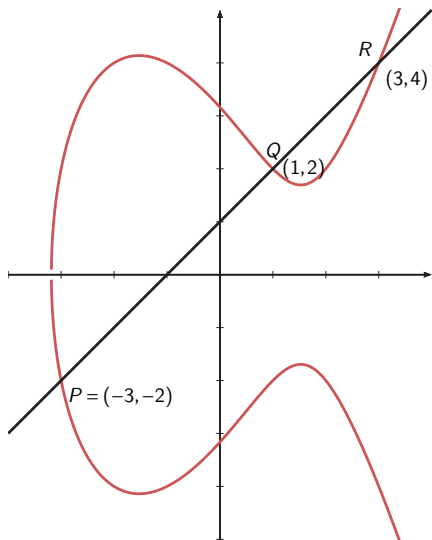


Pierre de Fermat



Andrew Wiles

Courbes elliptiques



Courbe elliptique E , définie par l'équation

$$E : y^2 = x^3 - 7x + 10.$$

Trouvez des points sur E tel que x et y sont rationnels.

Un opérateur d'addition:

$$P \oplus Q = R.$$

Cela donne une structure de groupe à la courbe E !

Courbes elliptiques:applications

- Démonstration du grand théorème de Fermat!
- Cryptographie sur les courbes elliptiques:

$$n \cdot P = \underbrace{P \oplus P \oplus \dots \oplus P}_{n \text{ fois}}.$$

Étant donné les points P et $n \cdot P$, c'est très difficile de trouver n .

Recherche en théorie des nombres

- Un domaine de recherche très intéressant et très populaire!
- Théorie des nombres à Montréal:



Matilde Lalín



Andrew Granville



Dimitris Koukoulopoulos

- Deux problèmes du prix du millénaire posés par l'Institut de mathématiques Clay - **Hypothèse de Riemann** et **Conjecture de Birch et Swinnerton-Dyer**. Million dollars pour chacun!

**C'EST TOUT!
MERCII!**