

Courbes elliptiques sur des corps finis

Origine historique

Les courbes elliptiques sont apparues dans le calcul de longueurs d'arc d'ellipses du fait que les points de la courbe $y^2 = x^3 + ax + b$ sont paramétrés par l'intégrale :

$$\int \frac{dx}{\sqrt{x^3 + ax + b}}$$

Géométrie algébrique

La géométrie algébrique relie équations polynomiales et formes géométriques.

Géométrie arithmétique

La géométrie arithmétique utilise la géométrie pour étudier des problèmes d'arithmétique.

Les courbes elliptiques et isogénies

Ce sont des courbes définies par $y^2 = x^3 + ax + b$ munies d'une structure de groupe, et les isogénies sont les morphismes qui préservent cette structure.

Grand théorème de Fermat

Il n'existe pas d'entiers naturels x, y et z , tous non nuls, tels que $x^n + y^n = z^n$ pour n un entier strictement supérieur à 2.

Par quel moyen ?

Par la construction d'isogénies de degré premier, puis l'étude des extensions associées au noyau.

Sujet de thèse

Construction d'extensions de corps via les courbes elliptiques et l'étude de l'action galoisienne sur les points rationnels.

Formule de Vélu

Soit $\phi : E \rightarrow E'$ une isogénie de noyau $G = \langle P \rangle$. Alors, pour tout point $P = (X, Y) \in E$, on a :

$$\phi(X, Y) = \left(\frac{\Phi_G(X)}{\Psi_G(X)^2}, \frac{Y\Omega_G(X)}{\Psi_G(X)^3} \right)$$

Quelles mathématiques ?

Algèbre

L'algèbre étudie les structures et les relations dans leur ensemble, plutôt que les objets pris isolément.

Théorie de Galois

La théorie de Galois relie les équations polynomiales aux groupes d'automorphismes de leurs corps de décomposition, révélant la structure arithmétique cachée.

Le groupe de Galois d'une extension de corps K/k est l'ensemble des automorphismes de K laissant k invariant, c'est l'ensemble $\text{Gal}(K/k) = \{\sigma \in \text{Aut}(K) / \forall x \in k, \sigma(x) = x\}$.

Objectifs

Au sein des mathématiques

Meilleure compréhension des liens entre l'arithmétique et la géométrie.

Vers l'industrie

Base théorique des protocoles de cryptographie post-quantique.