Isogénies de Mazur, "switch 3-5" de Wiles et 15-isogénies : le récit le plus simple gemini pour Denise Vella-Chemla, 10 novembre 2026

1. Le décor, en n'utilisant que $\mathbb{Z}/p\mathbb{Z}$

Une courbe elliptique E sur $\mathbb{Q}$ est une équation du type $y^2 = x^3 + ax + b$ à coefficients entiers.

Fixons un nombre premier p. Dans les nombres complexes, il y a exactement p^2 points P de la courbe tels que $pP = 0$ (pour la loi d'addition des points) : ce sont les *points de p-torsion*, notés $E[p]$.

Ils forment un "plan" sur le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: un espace de dimension 2, avec p^2 éléments, donc $p + 1$ droites.

Les coefficients de la courbe sont rationnels, donc le groupe de Galois de $\mathbb{Q}$ permute ces p^2 points, et le fait de façon *linéaire*.

Chaque élément de Galois devient une matrice 2×2 inversible à coefficients dans $\mathbb{F}_p$.

On obtient ainsi une représentation

$$\overline{\rho}_{E,p} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Pour un premier $\ell \neq p$ où la courbe est "bonne", le Frobenius en ℓ est une matrice de trace $a_\ell \bmod p$ (où $\ell + 1 - a_\ell$ est le nombre de points de la courbe modulo ℓ) et de déterminant $\ell \bmod p$.

Réductible veut dire : il existe une droite du plan $E[p]$ que *toutes* ces matrices laissent stable (un vecteur propre commun). En changeant de base, toutes les matrices deviennent triangulaires supérieures.

Cela équivaut à l'existence d'une *isogénie rationnelle de degré p* : si l'on quotiente E par cette droite, on obtient une autre courbe E', encore définie sur $\mathbb{Q}$, avec une application de E vers E' de degré p.

2. Le théorème de Mazur (1977)

Question : pour quels p existe-t-il une courbe elliptique sur $\mathbb{Q}$ avec une p-isogénie ?

Réponse : exactement pour

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

Pour tout autre p, aucune courbe sur $\mathbb{Q}$ n'a de droite stable dans $E[p]$.

2.1. Comment raconter cela ?

Les droites stables par Galois dans $E[p]$ sont les *points rationnels* d'une courbe $X_0(p)$ (la courbe modulaire), qui paramètre les couples (E, droite).

Le nombre de points rationnels dépend du *genre* de $X_0(p)$ (le nombre de "trous").

- pour le genre 0 : $p = 2, 3, 5, 7, 13$. La courbe $X_0(p)$ est une droite projective : elle a une infinité de points rationnels, donc une infinité de courbes avec une p-isogénie.
- pour le genre ≥ 1 : il n'y a plus qu'un nombre fini de points rationnels (Faltings le dit en genre ≥ 2, mais Mazur fait bien mieux : il les trouve *tous*, et montre qu'il n'y en a aucun pour les autres p).
- parmi les p restants, $19, 43, 67, 163$ viennent des courbes à multiplication complexe par $\mathbb{Q}(\sqrt{-p})$, corps dont le nombre de classes est 1. Les cas 11, 17, 37 sont des accidents particuliers.

L'outil de Mazur est l'*idéal d'Eisenstein* dans l'algèbre de Hecke de $J_0(p)$: une congruence modulo le numérateur de $\dfrac{p-1}{12}$ entre une série d'Eisenstein et des formes paraboliques.

C'est le cœur du travail, et c'est cela qui est formalisé dans les fichiers "quotient d'Eisenstein" et "étape 3 de Mazur" du dépôt Lean.

3. Pourquoi Wiles a besoin de 3 et de 5

Pour prouver la modularité de la courbe de Frey E (semistable), Wiles utilise un "théorème de relèvement" : si $\overline{\rho}_{E,p}$ est *irréductible* et *modulaire* (c'est-à-dire qu'elle provient d'une forme modulaire), alors E est modulaire.

Il lui faut donc un p pour lequel on sait que $\overline{\rho}_{E,p}$ est modulaire.

- pour $p = 3$: le groupe $\mathrm{GL}_2(\mathbb{F}_3)$ est *résoluble*. Le théorème de Langlands-Tunnell dit alors qu'une $\overline{\rho}_{E,3}$ irréductible est automatiquement modulaire (elle provient d'une forme de poids 1). On n'a rien à vérifier.
- mais $\overline{\rho}_{E,3}$ peut être réductible : c'est exactement une 3-isogénie rationnelle. Il y a une infinité de telles courbes, puisque $X_0(3)$ est de genre 0.

3.1. Le switch

Supposons $\overline{\rho}_{E,3}$ réductible.

1. $\overline{\rho}_{E,5}$ *est alors irréductible.* Sinon E aurait une 3-isogénie et une 5-isogénie, donc une isogénie de degré 15. Or $X_0(15)$ n'a qu'un nombre fini de points rationnels non "à l'infini" : *quatre*, c'est la classification des 15-isogénies (en termes de l'invariant j, ou du quotient c_4^3/Δ comme dans le Lean). Ces courbes (à ma connaissance de conducteur 50, à vérifier dans le fichier Lean) ne sont pas semistables : elles ne peuvent pas être une courbe de Frey. L'exception est donc exclue.

2. *on cherche une courbe auxiliaire* F qui a *la même* représentation modulo 5 que E ($\overline{\rho}_{F,5} \cong \overline{\rho}_{E,5}$), mais telle que $\overline{\rho}_{F,3}$ soit *irréductible*. Les courbes ayant une représentation mod 5 donnée forment une courbe de genre 0 (la courbe $X(5)$ tordue), qui a un point rationnel, donc une infinité de points. Un argument d'irréductibilité de Hilbert permet d'y trouver un F dont la représentation mod 3 est irréductible, avec de bonnes conditions locales.
3. *on enchaîne* : $\overline{\rho}_{F,3}$ irréductible $\Rightarrow$ (Langlands-Tunnell) modulaire $\Rightarrow$ (relèvement en 3) F modulaire $\Rightarrow \overline{\rho}_{F,5} = \overline{\rho}_{E,5}$ modulaire $\Rightarrow$ (relèvement en 5, car $\overline{\rho}_{E,5}$ est irréductible) E modulaire.

Les rôles des nombres sont donc : 3 donne la modularité gratuite (Langlands-Tunnell), 5 donne la liberté de changer de courbe (genre 0), et les quatre 15-isogénies sont la seule exception, qu'on écarte à la main.

4. Est-ce utilisable pour Goldbach ?

Non : rien n'irait vers une démonstration de la conjecture de Goldbach en empruntant ces voies-là. Raisons :

- **obstruction de parité.** Elle vient de ce que les cribles ne distinguent pas un nombre ayant un nombre pair de facteurs premiers d'un nombre en ayant un nombre impair. Rien dans la théorie ci-dessus ne s'attaque à cela : elle compte des traces de Frobenius $a_\ell \bmod p$, pas des solutions de $p + q = n$.
- **pas d'objet géométrique.** Dans le théorème de Mazur, l'énoncé arithmétique (existence d'une isogénie) est un énoncé sur les points rationnels d'une courbe. Pour Goldbach, l'équation $x + y = n$ est linéaire, donc de genre nul ; la difficulté est de demander que x et y soient premiers, condition qui n'est pas algébrique.
- **l'idéal d'Eisenstein** est une congruence modulo des numérateurs de $\dfrac{p-1}{12}$: elle parle de $p - 1$, pas de sommes de deux premiers.
- **le switch 3-5** ressemble à un criblage à deux modules (si ça échoue mod 3, on passe mod 5, et l'échec simultané est une liste finie). Mais cela repose entièrement sur le fait que l'échec simultané est un ensemble fini de points rationnels : pour Goldbach il n'y a pas d'analogue de $X_0(15)$.

En résumé, ces théorèmes sont des outils d'une richesse extraordinaire pour les courbes elliptiques, mais aucun ne contient de prise sur les décomposants de Goldbach, ni sur la parité.