Nombre de points des courbes modulaires sur un corps fini, d'après Ihara-Langlands.

Soit N un entier, la courbe modulaire $Y_1(N)$ est le quotient du demi-plan de Poincaré par le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ des éléments unipotents supérieurs modulo N. C'est une surface de Riemann avec un nombre fini de pointes, donc une courbe algébrique complexe, qui se trouve être définie sur $\mathbb{Q}$. Mieux, $Y_1(N)$ admet pour $N > 4$ un modèle canonique lisse sur $\mathbb{Z}[1/N]$ dont les points paramètrent les courbes elliptiques munies d'un point d'ordre N. L'objectif du groupe de travail serait de comprendre le calcul du nombre de points de $Y_1(N)(k)$ quand k est un corps fini de caractéristique $p \not| N$, dû initialement à Eichler et Shimura, en suivant la méthode d'Ihara-Langlands (développée ultérieurement par Kottwitz, Milne). Le résultat final est une expression de la fonction zêta de $Y_1(N)$ sur $\mathbb{Q}$ (du moins des facteurs eulériens hors de N) en terme des fonctions L des formes modulaires propres de poids 2 et niveau N, ce qui est donc une version explicite des conjectures de Weil dans ce cas, prouvant en particulier l'équation fonctionnelle globale attendue.

Par exemple, il se trouve que la courbe algébrique $Y_1(11)$ est de genre 1, isomorphe sur $\mathbb{Q}$ à un ouvert de la courbe elliptique d'équation plane $E : y^2 + y = x^3 - x^2$, et nous montrerons alors que $|E(\mathbb{Z}/p\mathbb{Z})| = p + 1 - a_p$ si p est premier différent de 11, où a_p est le p-ième coefficient de la série formelle

$$f = q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2.$$

À l'inverse, cela démontre aussi que $|a_p| \leq 2\sqrt{p}$ (conjecture de Ramanujan-Peterson pour f).

Le groupe de travail pourrait ensuite se poursuivre par l'étude des facteurs eulériens manquant (aux p divisant N) de la fonction zêta de $Y_1(N)$ (Deligne, Langlands, Carayol), ou encore la démonstration par Taylor-Wiles du théorème de modularité des courbes elliptiques semi-stables sur $\mathbb{Q}$.

En ce qui concerne la preuve, il s'agit donc de dénombrer les courbes elliptiques, munies d'un point d'ordre N, sur un corps fini k donné. La théorie de Deuring-Tate-Honda permet un décompte des classes d'isogénie en terme de certains nombres de Weil, puis le théorème des isogénies de Tate sur les variétés abéliennes sur les corps fini permet de dénombrer les classes d'isomorphie dans une classe d'isogénie. Cela nécessitera aussi d'étudier les groupes p-divisibles des courbes elliptiques sur corps de caractéristique p, afin de prendre en compte les p-isogénies. Le cardinal de $Y_1(N)(k)$ se réécrira alors comme une somme indexée par certaines classes de conjugaison d'éléments semisimples de $\mathrm{GL}_2(\mathbb{Q})$ et un peu de travail la fait apparaître comme la partie principale du côté géométrique de la formule des traces de Selberg appliquée à une fonction bien choisie. Parmi les outils à comprendre pour cela : formule des traces de Selberg, pseudo-coefficients de séries discrètes de $\mathrm{SL}_2(\mathbb{R})$, paramètres de Satake, "intégrales orbitales = nombre de réseaux", lemme fondamental pour le changement de base non ramifié, etc... Pour une esquisse de la preuve, voir le séminaire Bourbaki de Clozel (1992-1993, no 766, chap. 1 à 3), et dans un cadre légèrement différent l'article de Casselman (PSPM 33, vol 2, "Automorphic forms, representations, and L-functions"). Des réfénces plus précises viendront ensuite.