UNE BORNE INFÉRIEURE POUR LE NOMBRE MAXIMAL DE POINTS RATIONNELS DES COURBES SUR LES CORPS FINIS

ELISA LORENZO GARCÍA

Abstract. En 1985, Jean-Pierre Serre a donné une série de cours à l'université de Harvard sur le nombre de points des courbes sur les corps finis. En se basant sur les notes prises à cette période par F. Q. Gouvêa, nous avons publié une version éditée de ce cours à la SMF. Pour célébrer le lancement de cette publication, nous avons interviewé Jean-Pierre Serre en 2021. Après discussion avec lui, nous avons publié deux papiers avec les premiers progrès substantiels sur une des questions posées il y a 40 ans dans ces notes. Plus précisément, nous montrons que pour tout $g > 0$ et tout $\epsilon > 0$ et pour tout q assez grand, il existe une courbe de genre g sur $\mathbb{F}_q$ avec au moins $q + 1 + (2g - \epsilon)\sqrt{q}$ points, c'est-à-dire, à distance $\epsilon\sqrt{q}$ de la borne de Hasse-Weil.

1. Partie I

On va parler de courbes sur les corps finis, alors on va commencer pour définir qu'est-ce que c'est une courbe pour nous. On va prendre la définition suivante: une courbe projective algébrique lisse et irréductible. Une courbe algébrique est une variété algébrique de dimension 1. Le fait qu'elle soit projective veut dire qu'elle vit dans un espace projectif. Si vous aviez jamais vu l'espace projective, ce n'est pas maintenant le moment de le faire, même si je vous encourage à apprendre de la géométrie projective qui est une discipline vraiment jolie. En pratique, pour nous, on peut penser que nos courbes sont donnes par les zéros des quelques polynômes en n variables de sort que le lieu géométrique a dimension 1. C'est une courbe. Alors si le corps de définition est le réels, on obtient ce qu'on s'imagine pour une courbe, une ligne lisse qui ne se coupe pas, plongée dans un espace. Et si le corps de définition est le complexes, on obtient alors une surface de Riemann. Un invariant topologique des surfaces de Riemann est le genre, c'est-à-dire, le nombre de trous. Ainsi, une sphère a genre 0, mais un donuts ou une tasse à café à genre 1, et un pretzel a genre 3. Bien-sûr, cette définition du genre comme le nombre de trous, c'est très bien pour l'intuition mais ce n'est pas trop formelle et elle n'a pas de sens quand la courbe est définie sur les corps finis. C'est quoi alors la courbe ? en fait, dans se cas là, qui est le cas qui nous intéresse, la courbe est un ensemble finit de points. Imaginons que les polynômes ont n variables et qu'on travaille sur $\mathbb{F}_q$: alors chaque variable peut prendre au plus q valeurs et on a une borne de q^n pour les nombre de points dans la courbe ... bon, cela n'est pas complètement vrai parce qu'on a dit qu'on considère de courbes projectives et alors il faut aussi compter les points à l'infini, cela veut dire qu'on compactifie un peu les espaces. Par exemple, la droite $x = y$ sur $\mathbb{F}_q$ au lieu d'avoir q points, a $q + 1$ parce qu'il faut ajouter le point à l'infini.

Date: 21-22 March 2025.

Mais je reviens maintenant à la définition du genre. C'est un invariant qui mesure d'une certaine façon, la complexité d'une courbe. Il prend comme valeurs des entiers non-négatifs, le nombre des trous, et plus précisément, c'est la dimension de l'espace des différentielles régulières, et alors encore un entier non-négatif !

Alors, les courbes de genre 0 sur $\mathbb{F}_q$ sont toutes isomorphes à la droite projective et elles ont, comme on à déjà vu $q+1$ points. Elles ne sont pas trop intéressantes.

Les courbes de genre 1, sont beaucoup plus intéressants ! elles sont les courbes elliptiques. Elles sont des courbes, mais elles sont aussi des groupes ! il y a une jolie loi du groupe donné comme une addition des points. Je vais essayer de la vous montrer : les courbes elliptiques sont données par des équations de la forme : $y^2 = x^3 + ax + b$ (bon, en caractéristique différente de 2 et 3). Sur les réels, le graphe de la fonction $y = \pm\sqrt{x^3 + ax + b}$ est symétrique par rapport à l'axe y, on peut l'imaginer comme une tranche de donuts (courbe sur les complexes), qui donnera 2 ovales, mais un de points est le point à l'infini, et alors sur les réels on ne voit qu'un ovale et un ovale ouvert. On prend maintenant 2 points, comment on les addition ? On prend la droite qui passe par les deux points, cette droite coupe la courbe dans un troisième point (l'équation a degré 3, c'est une conséquence du théorème de Bézout, qui marche bien parce qu'on est dans l'espace projectif !), alors ce troisième point n'est pas la somme, mais son symétrique par rapport à l'axe y. C'est un joli exercice de montrer que cette construction géométrique donne une loi de groupe !

Cela donnerai pour un autre exposé, mais les courbes elliptiques, en plus, d'avoir une très jolie théorie mathématique derrière elles, (par exemple, une pièce clé de la preuve du dernier théorème de Fermat, est les courbes elliptiques), elles sont très pratiques pour la cryptographie ! Par exemple la sécurité de Whatsapp, que vous n'aimez pas beaucoup, est basée sur une courbe elliptique précise sur un corps fini très grand.

Et bon, je reviens à ma question originale. Le nombre des points des courbes. Pour les courbes de genre 0, la réponse était $q+1$, est pour les courbes elliptiques, le nombre de points va être de la forme $q+1-t$ où $t \in [-2\sqrt{q}, 2\sqrt{q}]$. Il faut comprendre ce nombre t comme en terme d'erreur. En fait, cela va être vrai toujours, le nombre de points d'une courbe va être de l'ordre de $q+1$ et après il a un terme d'erreur proportionnel à la racine de q. Cela est un résultat de Hasse et Weil des années 30 et 40 sur lequel je reviendrai plus tard.

Mais comment calculons nous le nombre de points d'une courbe elliptique ? en fait une réponse intelligent de cela n'est pas trivial. On peut penser à l'algorithme naïf, pour chaque valeur d'x, on calcule la valeur de $x^3 + ax + b$ et on regarde si c'est un carré ou pas dans $\mathbb{F}_q$. La complexité de ça est polynomial en q. René Schoof a donné un bel algorithme logarithmique en 1995. Je ne rentrerai pas dans les détails. Mais je reviens à la théorie, d'où il sort la formule $q + 1 - t$? Est-ce que vous connaissez l'endomorphisme de Frobenius ? sur $\overline{\mathbb{F}}_p$, il reviens a prendre un élément α et considérer sa puissance p-ième. Les seuls éléments qui sont fixés par cette endomorphisme sont les éléments de $\mathbb{F}_p$. Les seuls éléments fixés par le Fobenius au carré sont les éléments de $\mathbb{F}_{p^2}$, et en général par la puissance r-ième du Frobenius, sont les éléments de $\mathbb{F}_q$ avec $q = p^r$. Maintenant on va appliquer cette opérations aux points de la courbe elliptique $y^2 = x^3 + ax + b$, on envoie (x, y) à (x^q, y^q), les points définies sur $\mathbb{F}_q$ seront les points fixés par cette transformation, qui est un endomorphisme parce qu'elle respecte la loi du groupe (pas difficile à vérifier

avec du papier et un stylo). Alors, il sont les points dans le noyau du Frobenius à la puissance r moins l'identité. On veut calculer alors la taille du noyau de $\mathrm{Fr}^r - \mathrm{Id}$. On peut voir chacun de ces deux endomorphismes comme de matrices 2×2. Le cardinal du noyau est égal au déterminant de $\mathrm{Fr}^r - \mathrm{Id}$, qui est égale au déterminant de Fr^r plus 1 moins sa trace. Le déterminant est égal à q, donc la formule $q + 1 - t$. Les valeur propres de Fr^r ont norme racine de q est alors sa somme, la trace, en valeur absolue, est plus petite ou égal à 2 fois racine de q.

La question maintenant est de savoir si toute les valeurs de t dans cet intervalle sont obtenus par des courbes elliptiques sur $\mathbb{F}_q$. Et c'est Deuring qui a montré que oui, si t n'est pas un multiple de q. Bon, la caractérisation est beaucoup lus précise, mais cela nous serve pour montrer c'est qu'on veut montrer:

Théorème 1.1. *(Deuring) Pour tout q, il existe une courbe de genre 1 (elliptique) sur $\mathbb{F}_q$ a distance plus petite ou égal à 1 de la borne de Hasse-Weil.*

La preuve de Deuring utilise la théorie de la multiplication complexe. Elle est encore une très belle théorie que je ne pourrais pas expliquer aujourd'hui.

2. Partie II

On passe maintenant au genre 2. Je vous donne directement le résultat :

Théorème 2.1. *(Serre) Pour tout q, il existe une courbe de genre 2 sur $\mathbb{F}_q$ a distance plus petite ou égal à 3 de la borne de Hasse-Weil.*

Quelque rappels ici. Les courbes de genre 2 son données par des équations $y^2 = f(x)$ avec f de degré 5 ou 6. Pour le genre plus large, ce n'est pas vrai en général que les courbes soient données par des équations $y^2 =$ un polynôme. Mais pour genre 2, c'est encore le cas. Cela est un peu spécial parce qu'en particulier cela dit que la courbe admet un automorphisme non-trivial. Le fait que les courbes de genre 2 soient données par des équations comme ça, n'est pas difficile mais un peu techniques, si vous êtes intéressés je vous envoie aux notes du course sur le courbes algébriques de mon collaborateur, ici présent, Christophe Ritzenthaler.

La borne de Hasse-Weil(-Serre) est $\mid t \mid \leq g\lfloor 2\sqrt{q} \rfloor$ où t est la trace du Frobenius et le nombre de points est encore donné par la formule $q + 1 - t$. L'idée cette fois là est très semblable au cas des courbes elliptiques : les courbes de genre g ne sont pas en général de groupes, mais on peut les associe des variétés de dimension g qui sont en plus des groupes (la jacobienne), maintenant on utilise la même idée qu'avec les courbes elliptiques mais cette fois là le Frobenius et la identité sont vues comme des matrices taille $2g \times 2g$, on a alors $2g$ valeurs propres de norme racine de q et la trace en valeur absolue est donc bornée par $2g\sqrt{q}$. Bien-sûr, j'ai simplifié un peu les choses, tout ça fait partie des conjectures de Weil, et plus particulièrement cette affirmation sur les valeurs propres du Frobenius et le nombre de points est ce qui est connu comme la hypothèse de Riemann sur les corps finis ...

Mais comment il a montré, Serre, ce résultat ?

Bon, pour commencer, pour ceux qui ne le savent pas, Jean-Pierre Serre avaient gagné la médaille Fields avec 28 ans en raison de ses contributions exceptionnelles à la topologie, à la géométrie algébrique et à la théorie des nombres. Et après il a gagné le prix Abel dans sa toute première édition. Il a maintenant 98 ans et il continue à faire de maths ...

En 1985, même avant que j'étais née, il était à Harvard pour faire un course sur le sujet dont on parle aujourd'hui. C'était deux fois par semaine, les mardis et les

jeudis. Les mardis il parlait des courbes de genre petit avec beaucoup de points rationnels et en particulière il a montré le cas pour genre 2 que je viens de vous énoncer et les jeudi il fixait q est envoyait g à l'infini.

La preuve pour le cas de genre 2 n'a pas été publié jusqu'à récemment, on avaient seulement les notes manuscrites de Fernando Gouvêa scannées sur internet. Et on lui remercie, énormément pour avoir laissé trace de ces notes, mais son écriture étaient horrible ... j'ai passé un bons temps pendant ma thèse à essayer de comprend ce qu'il avait écrit.

C'est pour cela qu'en 2017 avec Alp Bassa, Christophe Ritzenthaler et René Schoof, nous avons décidé d'éditer ces notes. Plus de 300 pages à la main qu'avec des appendices et des révisions par Serre, on a finalement publié chez la SMF en 2021.

Quelques mots sur la preuve pour le genre 2 : on sait construire des courbes elliptiques avec un nombre de points donné, sauf si la trace nécessaire est un multiple de p. On va essayer de coller 2 telles courbes elliptiques pour obtenir la variété de dimension 2 associée à une courbe de genre 2. Il y a plusieurs cas à considérer et des stratégies différentes pour les coller. Mais Serre est arrivé à le faire. En plus, en caractéristique différente de 2, la distance à la borne de Hasse-Weil est au plus de 2 pas de 3. Il caractérise minutieusement la distance exacte pour chaque q. En fait, cela est quelque chose que j'apprécie beaucoup de lui, il est, je dirai le mathématiciens le plus fort de nos temps, il fait de mathématiques très abstraites et compliquées, mais au même temps, il arrive, et il s'intéresse !, par des mathématiques très effectives, s'il énonce un théorème d'existence, il donne aussi d'habitude la construction ! Et il n'a pas peur de faire de calculs longues comme ceux-ci ! Je pense que beaucoup de mathématiciens très forts, auront quitté cette entreprise pour le genre 2 assez tôt ... Ce sont des calculs délicats avec beaucoup de cas et chacun nécessitant de nouvelles astuces.

Ok, on a la réponse pour le genre 0, 1 et 2 depuis 1985. Qu'est-ce qu'on peut dire pour le genre 3 ? On a toujours des courbes de genre 3 à distance 3, 4, 5 de la borne de Hasse-Weil ? et bien, on ne sait pas. Et ce n'est pas parce qu'il n'y a pas eu des mathématiciennes et mathématiciens qui ont travaillé sur le sujet ... En fait il y en a eu beaucoup. Je vais citer seulement quelqu'uns : Fieker, van der Geer, Howe, Ibukiyama, Kawakita, Lauter, Mestre, Niederreiter, Ritzenthaler, Stichtenoth, Top, van der Vlugt, Voloch, ... Et on ne connaît pas encore la réponse. C'est un peu surprenant. Lauter avait montré en utilisant la même estratégie que Serre pour le cas de genre 2 qu'il existe toujours une courbe de genre 3 a une distance d'au plus 3 du maximum ou de minimum, mais on ne peut pas distinguer à priori si on a beaucoup de points ou tout le contraire. Cela est dû au fait que les courbes de genre 3 ne sont pas toujours de la forme $y^2 = f(x)$, il n'y a pas nécessairement d'automorphisme d'ordre 2 qui nous permettra de conclure. Après il y a des gens qu'on essayé de produire des constructions des familles particulières avec beaucoup de points. Une page web que s'appelle `manypoint.org` contient une base de données qui est régulièrement misse à jour avec les nouveaux records de courbes avec beaucoup de points. Et par exemple, déjà pour $q = 89$ et $g = 4$ ou pour $q = 3$ et $g = 8$, on ne sais pas quel est le nombre de points maximal d'une telle courbe.

En général, la question posée par Serre dans ce cours est la suivante :

Question 2.1. *(Serre'85) C'est vrai que pour tout q, il existe une constante $c(g)$ qui ne dépend que de g, telle qu'il existe une courbe de genre g sur $\mathbb{F}_q$ à distance $c(g)$ de la borne supérieure de Hasse-Weil ?*

Comme on a vu, la réponse est oui pour $g = 0, 1$ et 2. Dans ces cas, on a des courbes avec au moins $q + 1 + g\lfloor 2\sqrt{q}\rfloor - c(g)$. Avec $c(0) = 0$, $c(1) = 1$ et $c(2) = 3$.

Après le lancement de notes de Serre qu'on a publié chez la SMF, nous avons organisé une conférence pour le fêter. C'était en 2021 et alors la conférence a été en ligne. Et parce qu'on voulait faire de toute façon quelque chose un peu spécial, avec Ritzenthaler, on a interview Serre à Neuchâtel, où je travaille. En ce moment là, il habité à Lausanne et un Suisse il n'y avait pas de confinement. C'était un vrai honneur. L'interview est en ligne sur Youtube, et il a déjà plus de 27 mille reproductions. Cela me flatte, mais au même temps me stresse un peu.

Comme personne arrivait à répondre à sa question originale, après l'interview, il nous a proposé une version plus faible de la question :

Question 2.2. *(Serre'21) Fixons $g \geq 0$. C'est vrai que pour tout $\epsilon > 0$ et q assez grand, il existe une courbe de genre g sur $\mathbb{F}_q$ à distance $\epsilon\sqrt{q}$ de la borne supérieure de Hasse-Weil ?*

3. Partie III

Et maintenant, avec mes collaborateurs, Bergström, Howe et Ritzenthaler, on est arrivés à répondre et la réponse est oui, il existe une telle courbe !

En plus, dans le premier papier qu'on à écrit sur ce sujet, on donne 3 preuves de ce résultat. La première est très courte, elle est presque une conséquence direct de la théorie profonde de Katz-Sarnak. Et voici en exemple qui montre que parfois la partie difficile d'une recherche, n'est pas la preuve en elle-même, mais de savoir poser les bonnes questions ! Le problème avec ce rapprochement est qu'il n'est pas du tout effectif. Je vais revenir après un peu plus sur lui. La deuxième stratégie avait était suggéré par Serre quand il nous a proposé cette nouvelle version de la question : on étudie la moyenne des puissances, alors les moments, de la trace du Frobenius dans l'espace de modules de courbes de genre g sur $\mathbb{F}_q$. Un espace de module est simplement un espace qui paramétrise des objets. Dans ce cas, nos courbes. Il faut faire gaffe parce que si une courbe a des automorphisme supplémentaires, elle admets de courbes tordues et la trace n'est pas bien définie a priori pour la classe d'isomorphisme. On calcule ces moyennes d'une façon différent en utilisant de résultats de Bergström de la cohomologie de système locaux sur des espace de modules de courbes, et on arrive à conclure qu'il doit y avoir des courbes avec beaucoup de points parce que sinon les moments ne pourrait pas être si grands. Finalement, la troisième preuve est complètement explicite, elle, nous permet de donner des équations de courbes de genre g (toutes elles hyperelliptiques, cette à dire avec ce célèbre automorphisme d'ordre 2) avec au moins $1 + q + 4\sqrt{q} - 32$ points sur $\mathbb{F}_q$. L'idée est la suivante : on commence avec une courbe de genre 2 ou 3 sur $\mathbb{F}_q$ avec plus de nombre de points, après on donne une construction pour à partir d'une courbe hyperelliptique de genre g construire une autre avec au moins le même nombre de points en genre $2g$ et $2g + 1$. Avec ça, on arrive à construire de telles courbes pour toutes les genres. Pouvez vous vous convaincre de ça ?

Je reviens maintenant vers la première stratégie, même si pas effective, c'est la seule qu'on pense pouvoir pousser dans le futur pour répondre à la question originale de Serre.

On regarde le espace de modules de courbes de genre g et ses points sur $\mathbb{F}_q$, et on regarde aux traces de ces courbes, qui sont de nombres entiers dans l'intervalle $[-2g\sqrt{q}, 2g\sqrt{q}]$. Parce que l'intervalle dépend de q et on va faire q aller vers l'infini (s'il y a seulement un nombre fini de q, on pourrait prendre le maximum des distances à la borne de Hasse-Weil comme la constante qu'on cherche), on va travailler avec la trace normalisée, on divise alors la trace par $\sqrt{q}$ et alors la trace normalisée est dans l'intervalle $[-2g, 2g]$. Notons que une trace normalisée à distance au plus une constante de $2g$ est une trace sans normaliser à distance au plus cette constante fois $\sqrt{q}$ et qu'une trace sans normaliser à distance au plus une constante de la borne de Hasse-Weil est une trace normalisée à distance au plus cette constante divisée par $\sqrt{q}$ de $2g$, alors à une distance très petite, de l'ordre de $1/\sqrt{q}$. Cela on n'arrive à le montrer, cela serait la question original de Serre, mais on arrive a montrer que la trace normalisée est à distance au plus une constante (qu'on peut prendre tout le petit qu'on veut) de $2g$. Comment on fait ça ? Bon, comme j'avais déjà annoncé, on prendre la théorie de Katz-Sarnak qui dit que, quand q va vers l'infini, la distribution de cette trace normalisée dans l'intervalle $[-2g, 2g]$ est une fonction gaussienne et le terme d'erreur est de l'ordre de $O(1/\sqrt{q})$. Visualisez cette fonction gaussienne sur l'intervalle $[-2g, 2g]$, on se met à distance ϵ de $2g$, et on regarde l'air sur $[2g-\epsilon, 2g]$ cette aire est très petite, mais pas 0, le nombre de courbes de genre g sur $\mathbb{F}_q$ est plus au moins q^{3g-3}, alors pour q assez grand, $1/q^{3g-3}$ est plus grand que cette aire et il existe alors une courbe avec trace normalisée plus grande que $2g-\epsilon$.

Théorème 3.1. *(Bergström, Howe, Lorenzo García, Ritzenthaler'24) Soit $g \in \mathbb{N}$. Pour tout $\epsilon > 0$, et q assez grand, il existe une courbe de genre g sur $\mathbb{F}_q$ avec au moins $q + 1 + (2g-\epsilon)\sqrt{q}$ points.*

Ok, très bien, et comment on essaye de pousser ce résultat pour répondre à la question originale.

En fait, ce qu'il faudrait faire est de mieux comprendre le terme d'erreur $O(1/\sqrt{q})$. Encore, avec les mêmes collaborateurs, et parce qu'on n'avait pas d'idée magique, ce qu'on a essayé de faire est d'expériences numériques. On a voulu étudier la variable aléatoire donné par la trace normalisée moins la distributions prévue par Katz-Sarnak multiplié par $\sqrt{q}$ et maintenant on fait q aller vers l'infini. La façon d'étudier une telle variable aléatoire est en calculant ses moments (espérance de ses puissances). On calcule les moments et on conjecture quelle la fonction de densité correspondent quand q va vers l'infini. Malheureusement, on n'arrive pas à montrer cette convergence de fonctions de densité. Et même ce résultat tout seul ne donnerai pas encore une réponse à la question de Serre. Par contre on produit des graphiques très jolies qui soutient nos conjectures sur le terme d'erreur de la distribution du nombre de points et on observe clairement pour la première fois le folklore sur le déséquilibre à droite du terme d'erreur de cette distribution. Ce-à-dire, même si à la limite la distribution es symétrique, pour un q fixé, il y a, en général, plus de courbes avec beaucoup de points qu'avec peu de points.

Je vais aussi mentionner ici, que la réalisation de ces expériences n'est pas trivial, parce qu'il faut considérer des premiers grands, disons $p = 83$, mais alors l'espace de module de courbes de genre 3 a dimension 6 et 83^6 courbe sont beaucoup de courbes, et après il faut calculer le nombre de points de chacune de ces courbes. D'abord il faut bien paramétriser les courbes, par exemple les courbes de genre 3 génériques sont des quartiques planes et alors à 14 coefficients et il faudrait tester

quand elles sont isomorphes. Et après il y a l'histoire du comptage des points qui n'est pas trivial comme on a déjà commenté pour le cas de courbes elliptiques.

Je vais finir un peu pour un motivation de pourquoi on s'intéresse aux courbes avec beaucoup de points et pas aux courbes avec pas beaucoup de points ou avec un nombre de points intermédiaire. Pour moi, le fait qu'après 40 ans la question est encore ouverte et déjà un bon signe pour la considérer intéressante, mais quelle était la motivation originale ? bon, même Serre la mentionne au début de son cours à Harvard. Elle vient de la théorie de codes. Chambert-Loir vous avez parlé de la théorie de codes dans la descente 8-ème, alors je ne vais pas revenir sur ça. Je dirai seulement que les codes correcteurs d'erreurs linéaires qui sont de utilité dans la théorie de l'information, pour corriger des erreurs dans la transmission de l'information peuvent être construits à partir des courbes sur les corps finis, et le plus grand le nombre de points de la courbe, le mieux sont les paramètres du code au niveau de redondance versus capacité de correction.

Et voilà, avec ça et encore avec une question ouverte sur laquelle je vous invite à y réflechir, je finis mon exposé.

Il y a plus des questions ouvertes dans les proceedings de la conférence pour le lancement des notes de Serre ci-dessous qu'on a publié aussi avec la SMF.

4. Références

- https://smf.emath.fr/publications/rational-points-curves-over-finite-fields
- https://www.youtube.com/watch?v=hPm7_x0DP8Q
- https://smf.emath.fr/publications/courbes-sur-les-corps-finis-passe-present-et-avenir
- https://arxiv.org/abs/2204.08551
- https://arxiv.org/abs/2303.17825

Elisa Lorenzo García, Institut de Mathématiques, Université de Neuchâtel, rue Emile-Argand 11, 2000, Neuchâtel, Switzerland & Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France.

Email address: elisa.lorenzo@unine.ch