Chers Dudes,

La saison de la chasse au poulpor n'est pas encore ouverte que déjà les candidats se pressent au portilllon.
(Pour les ceusses qui ne seraient pas au parfum : le séminaire poulpor (du nom du regretté Poulpor) se décline en plusieurs fragrances capiteuses à souhait. En voici le règlement :
- art 1 : Le poulpor seminar est un rendez-vous hebdommmadaire au cours duquel un membre de la poulpor mailing list expose à ses collègues un petit sujet qui lui tient à coeur.
- art 2 : En cas d'exposé incompréhensible, l'orateur sera pendu avec son foie.
- art 3 : L'incompréhensibilité d'un exposé se décide à la majorité qualifiée des sous-signés organisateurs du poulpor semiflard (qui sont sensibles à la corruption).
- art 4 : Le présent règlement est susceptible.
- art 5 : Car il peut être modifié à tout moment par les soucis gnés organisateurs.
- art 6 : Toute allusion, même implicite et involontaire, à Assyr Abdulle sera punie.)

L'ouvertüre officielle de la chasse au poulpor coïncide bizarrement avec le début du semestre d'été (et quand on réalise que Jupiter passe au même moment entre la grande Arche, on se dit que ce ne peut être un hasard). L'horaire précis et définitif des scéances poulporesques est écrit sur un parchemin dans un coffre dont la clé est au fond d'un puits dans de la farine animale dont la clé est en plastique (ah non, elle faisait juste semblant d'être en plastique), mais nos équipes devraient le retrouver d'ici là.
Néanmoins, sensibles aux supplications lamentables de Bernhardt Wüütrick (qui perd contenance en pal), les sous-signés organisateurs ont décidé (à la majorité qualifiée) de célébrer sa venue en le claquant au tableau lors d'un poulpor séminaire essepssionnel.
En deux mots comme en deux, nous avons le plaisir (discutable) d'accueillir BERNHARDTDT WÜÜÜTRICKR ce vendredi, qui nous causera (en fransöze approximatif) de :

ÜBER DEN SCHMALZ.

Date: Vendredi 7 décembre 2001
Heure: 13h30
Lieu: 6ème étage
Tenue du conférencier: petit papa.

Du plâtre bienvenu.
Squelettor s'abstenir.

M.Baillif (de la neige au soleil)
D. Cimasoni (des patates dans le sahara)

"Pour savoir la cardinalité de la classe des constellations formées de 70 succès et 30 échecs, il faut se patienter."

F.S.

ÜBER IWASAWATHEORIE

CHRISTIAN "BERNHARDT" WÜTRICH

Je vais commencer par démontrer ce petit

Théorème.
Soit p un nombre premier impair. Il n'existe pas de triple d'entiers x, y et z, tous non divisibles par p, tels que

$$x^p + y^p = z^p\,.$$

Preuve complètement fausse. Par l'absurde, on suppose qu'on a un tel triple. On peut supposer que x, y, z sont premiers entre eux. Soit ζ_p une $p^{\text{ième}}$ racine primitive de l'unité. Comme p est impair, on a

$$\begin{aligned} z^p &= y^p\left(\frac{x^p}{y^p}+1\right) = y^p\left(\frac{x}{y}+1\right)\left(\frac{x}{y}+\zeta_p\right)\cdots\left(\frac{x}{y}+\zeta_p^{p-1}\right) \\ z^p &= (x+y)(x+\zeta_p y)(x+\zeta_p^2 y)\cdots(x+\zeta_p^{p-1}y) \end{aligned} \tag{1}$$

($\star$) Comme on a une $p^{\text{ième}}$ puissance à gauche, chaque facteur à droite est une $p^{\text{ième}}$ puissance, disons

$$x + \zeta_p y = \alpha^p \tag{2}$$

pour $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ avec $a_i \in \mathbb{Z}$ pour tout i. On a alors

$$\begin{aligned} \alpha^p &\equiv a_0^p + (a_1\zeta_p)^p + \cdots + (a_{p-2}\zeta_p^{p-2})^p \pmod p \\ &\equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \pmod p \\ &\equiv \overline{\alpha}^p \pmod p, \end{aligned}$$

où la congruence se comprend comme la congruence modulo p pour chaque coefficient devant les ζ_p et $\overline{\alpha}$ est le complexe conjugué de α. On en déduit une belle contradiction avec l'hypothèse que y ne soit pas divisible par p.

$$\begin{aligned} x + \zeta_p y = \alpha^p \equiv \overline{\alpha}^p = x + \zeta_p^{-1} y \pmod p \\ \zeta_p y \equiv \zeta_p^{-1} y \pmod p \\ \zeta_p^2 y \equiv y \pmod p \\ y \equiv 0 \pmod p \end{aligned}$$

$\square$

La question au public de trouver les fautes dans cette démonstration fut répondu par le très cher Cimasoni David, Grand-Organisateur et Bienfaiteur du Séminaire Poulpor©: "C'est pas quelque chose avec la factorisation...". Bravo David !

Faute 1 : Il se pourrait que l'anneau

$$\mathcal{O} = \mathbb{Z}(\zeta_p) = \mathbb{Z} \oplus \mathbb{Z}\zeta_p \oplus \cdots \oplus \mathbb{Z}\zeta_p^{p-2} \cong \mathbb{Z}[X]/(1 + X + \cdots + X^{p-1})$$

n'est pas factoriel. L'argument ($\star$) ne marche plus, car la factorisation pourrait ne pas être unique.

Faute 2 : De toute façon, l'argument ($\star$) était seulement juste si les facteurs à droite sont premiers entre eux.

Faute 3 : Les unités ne sont pas nécessairement des $p^{\text{ième}}$ puissances. Par exemple $4 = (-2)(-2)$ est un carré qui se factorise en deux non carrés.

En ce qui concerne la *faute 3*, on peut remplacer l'équation (2) par

$$x + \zeta_p y = \varepsilon \cdot \alpha^p \tag{2'}$$

où ε est une unité de l'anneau $\mathbb{Z}(\zeta_p)$. On peut montrer qu'il existe une autre unité ε' telle que $\varepsilon = \zeta_p^r \cdot \varepsilon'$ et $\overline{\varepsilon'} = \varepsilon'$. On peut alors terminer la démonstration de la façon suivante:

$$\begin{aligned} x + \zeta_p y = \zeta_p^r \varepsilon' \alpha^p \equiv \zeta_p^r \varepsilon' \overline{\alpha}^p \equiv \zeta_p^{2r} \cdot \overline{\zeta_p^r \varepsilon' \alpha^p} \equiv \zeta_p^{2r} \cdot \overline{x + \zeta_p y} \\ x + \zeta_p y \equiv \zeta_p^{2r} \cdot (x + \zeta_p^{-1} y) \pmod p \end{aligned}$$

et un peu plus de travail pour distinguer les différents cas pour r, on arrive quand même à une contradiction.

La *faute 2* va être comblée par le lemme. On aurait alors réussi à démontrer le théorème pour les premiers pour lesquelles $\mathbb{Z}(\zeta_p)$ est un anneau factoriel. Malheureusement, il y en a pas tant: c'est seulement le cas pour $p \leqslant 19$ (Montgomery et Uchida).

Considérons maintenant la *faute 1*; mais d'abord - eh oui, ne ralez pas - un peu de théorie. $\mathcal{O} = \mathbb{Z}(\zeta_p)$ est l'anneau des entiers du corps $\mathbb{Q}(\zeta_p)$, une extension finie de $\mathbb{Q}$. Un tel anneau n'a pas forcément une factorisation en premiers comme les entiers rationnels $\mathbb{Z}$. Mais chaque idéal se factorise d'une manière unique en produit d'idéaux premiers.

Le défaut d'être factoriel pour l'anneau $\mathcal{O}$ est mesuré dans le groupe $\mathrm{Cl}\,\mathcal{O}$, le groupe des classes des idéaux modulo les idéaux principaux. Ce groupe est toujours fini, son ordre $h_{\mathcal{O}}$ est appelé le nombre de classe de $\mathcal{O}$.

Nous pouvons maintenant montrer le

THÉORÈME.
Soit $p \geqslant 5$ un premier. On suppose que le nombre de classe $h_{\mathcal{O}}$ n'est pas divisible par p. Alors il n'y a pas un triple d'entiers x, y et z, tous non divisibles par p, tels que

$$x^p + y^p = z^p \, .$$

Preuve. Si $x \equiv y \equiv -z \pmod p$, alors $-2z^p \equiv z^p$ et $p \mid 3z$, ce qui n'est pas possible si $p \geqslant 5$. (Le cas $p = 3$ se résout d'ailleurs facilement en regardant l'équation modulo 9.) Quitte à permuter si nécessaire $(x^p + (-z)^p = (-y)^p)$, on peut supposer que $x \not\equiv y \pmod p$.

LEMME. *Les idéaux $(x+y)\mathcal{O}$, $(x+\zeta_p y)\mathcal{O}$, ... $(x+\zeta_p^{p-1}y)\mathcal{O}$ sont premier deux à deux.*

Preuve. D'après une enquête auprès du public, ces détails ne valaient pas l'ennui qu'ils auraient causé. Voir [3], Lemma 1.7, page 5. □

L'équation (1) s'écrit maintenant comme

$$(z\mathcal{O})^p = (x+y)\mathcal{O} \cdot (x+\zeta_p y)\mathcal{O} \cdots (x+\zeta_p^{p-1}y)\mathcal{O} \tag{1'}$$

$(\star')$ Comme les idéaux à droite sont premiers entre eux, chacun est une $p^{\text{ième}}$ puissance d'un idéal, disons

$$(x+\zeta_p y)\mathcal{O} = I^p \tag{2''}$$

I est alors un idéal dont la $p^{\text{ième}}$ puissance est un idéal principal, c.-a-d. p divise son ordre dans le groupe des classes $\mathrm{Cl}\,\mathcal{O}$ de $\mathcal{O}$. Comme $h_{\mathcal{O}}$ n'est pas divisible par p, le groupe $\mathrm{Cl}\,\mathcal{O}$ ne contient pas d'élément d'ordre p. Ainsi on a montré que I est principal, disons $I = (\alpha)$ pour un $\alpha \in \mathcal{O}$. On retombe sur l'équation (2'). □

Les premiers p tels que $p \mid h_{\mathcal{O}}$ sont appelés des premiers irréguliers. Malheureusement, il en existe une infinité, commençant par

$$p = 37,\ 59,\ 67,\ 101,\ 103,\ 131,\ 149,\ 157\ \ldots$$

Par contre, on ne sait pas encore s'il existe une infinité de nombres premiers réguliers. Mais des méthodes probabilistes prédisent que 60,65% des nombres premiers devraient être réguliers.

Soit p un nombre premier impair. On appelle

$$i(p) = \#\{n \mid p \text{ divise } B_n \text{ pour } i \leqslant 2 \leqslant p-3\}$$

l'irrégularité de p. Ici B_n est le $n^{\text{ième}}$ nombre de Bernoulli définit par

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

On a par exempe $B_1 = \frac{-1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = \frac{-1}{30}$, $B_6 = \frac{1}{42}$, ... Les nombres de Bernoulli sont des nombres rationnels. On dit que $p \mid B_n$ si $B_n = p^r \cdot \frac{a}{b}$ avec $\operatorname{pgcd}(a,b,p) = 1$ et $r \geqslant 1$.

Théorème (Eichler – Brückner – Iwasawa – Skula).
Si $i(p) < \sqrt{p} - 2$, alors l'équation $x^p + y^p = z^p$ n'a pas de solution avec $p \nmid xyz$.

Preuve. Voir [3], theorem 6.23, page 107. □

- Un nombre est régulier si son irrégularité est 0.
- Pour un grand nombre des nombres irréguliers, l'irrégularité vaut 1. Par exemple $i(37) = 1$, $i(59) = 1$, ... Le plus petit premier qui a irrégularité 2, c'est 157.
- Pour $p < 4'000'000$ l'irrégularité ne dépasse jamais 7.
- À l'aide de ce théorème, le grand théorème de Fermat a pu être vérifié pour $p < 6 \cdot 10^9$ et pour les p plus grand la probabilité que la condition du théorème précédent ne soit pas satisfaite est plus petite que $10^{-300'000}$.

Je suppose que je devrais indiquer pourquoi, tout à coup, les nombres de Bernoulli interviennent. En gros, c'est parce que la fonction $\zeta_{\mathbb{Q}(\zeta_p)}(s)$ du corps $\mathbb{Q}(\zeta_p)$ (analogue de la fonction $\zeta(s)$ de Riemann pour $\mathbb{Q}$) prend aux nombres négatifs des valeurs qui s'expriment à l'aide de nombres de Bernoulli. D'autre part, le résidu de cette même fonction en $s = 1$ est lié à $h_{\mathbb{Q}(\zeta_p)}$.

En utilisant de l'analyse p-adique, on montre que

$$p \mid h \Leftrightarrow p \text{ divise un } B_j \text{ pour } j = 2, 4, \ldots, p-3$$

Par exemple $p = 37$ divise

$$B_{32} = \frac{106783830147866529886385444979142647942017}{510}$$

et $p = 157$ divise B_{62} et B_{110}.

Pour le théorème d'Eichler on a besoin, en plus, d'un théorème de Stickelberger: Une analyse très fine de la structure de $\operatorname{Cl}\mathcal{O}$.

La théorie d'Iwasawa

Soit p^{e_n} la plus grande puissance de p qui divise le nombre de classes h de $K_n = \mathbb{Q}(\zeta_{p^n})$.

Théorème (Iwasawa).
Il existe des entiers $\lambda \geqslant 0$, $\mu \geqslant 0$ et ν tels que

$$e_n = \lambda n + \mu p^n + \nu$$

pour presque tout n.

Preuve. Voir [3], theorem 13.13, page 277. □

Le théorème est valable pour beaucoup plus de tours d'extensions. Dans notre cas on a en plus que $\mu = 0$. Je vais vite parler un peu des idées derrière cette théorie:

Soit $K_\infty = \bigcup_{n \geqslant 1} K_n$, c'est une extension infinie de $K_1 = \mathbb{Q}(\zeta_p)$ de groupe de Galois $\Gamma = \mathrm{Gal}(K_\infty : K_1) \cong \mathbb{Z}_p$, l'anneau des entiers p-adiques, avec sa topologie habituelle. La théorie des classes de corps montre que, pour tout $n \geqslant 1$, il existe une extension $L_n : K_n$ telle que son groupe de Galois soit isomorphes au p-Sylow X_n du groupe de classes de K_n, on a donc $|X_n| = p^{e_n}$. On obtient un groupe $X = \mathrm{Gal}(L_\infty = \bigcup_{n \geqslant 1} L_n : K_\infty)$. On peut mettre une action de Γ sur X par conjugaison et X devient un $\mathbb{Z}_p[[\Gamma]]$-module. Ici, $\Lambda = \mathbb{Z}_p[[\Gamma]]$ n'est rien d'autre que $\mathbb{Z}_p[[T]]$, les séries formelles à coefficients dans $\mathbb{Z}_p$. On peut montrer que X est un Λ-module de type fini et pour ceux-là, il existe une décomposition qui ressemble à la décomposition des groupes abéliens de type fini:

$$X \sim \Lambda^r \oplus \bigoplus_{i=1}^{M} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{N} \Lambda/(f_j(T)^{m_j})$$

pour certains polynômes $f_j(T)$. Ici, $\sim$ veut dire qu'il existe un morphisme de noyau et de conoyau fini. Les constantes λ et μ peuvent maintenant se lire directement dans cette décomposition.

"Ce que je vais faire", vous avez demandé? Eh ben, je ne sais pas, mais on m'a raconté ça: on prend une courbe elliptique E sur $\mathbb{Q}$ sans multiplication complexe. Serre a montré que l'on a une représentation

$$\rho\colon\ \mathrm{Gal}(\overline{\mathbb{Q}} : \mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$$

dont l'image G est un sous-groupe ouvert. On forme

$$\Lambda = \varprojlim \mathbb{Z}_p[G/U]$$

où U parcourt les sous-groupes ouverts normales de G. Λ n'est plus abélien. Coates–Sujatha–Schneider ont trouvé un théorème de décomposition pour les Λ-module de type fini. On espère avancer vers la conjecture de Birch–Swinnerton-Dyers en analysant des Λ-module X provenant des groupes de Selmer de E.

References

[1] John Coltrane, *Transcendence*, mcps, 1998.

[2] Jean-Pierre Serre, *Abelian ℓ-Adic Representations and Elliptic Curves*, W. A. Benjamin, 1968.

[3] Lewrence C. Washington, *Introduction to Cyclotomic Fields*, second ed., Springer Verlag, 1996.

Remerciement

Je tiens à remercier de tout mon coeur mon amie Sylvia Guibert, ainsi que Gianluigi Sechi pour son part three essay.