Calculs et expérimentations en théorie des nombres

X.-F. Roblot

Pourquoi des calculs en théorie des nombres ?

- **Parce que c'est possible !**

2. Pour expliciter les objets donnés par la théorie

   Exemple : Extensions de degré donné d'un corps p-adique

3. Pour tester ou établir des conjectures

   Exemple : Conjecture de Brumer-Stark

1. Pour démontrer des résultats

   Exemple : Entiers de la forme $p + 2^k$

`Tous les calculs ont été effectués avec le système PARI/GP`

Entiers de la forme $p + 2^k$ (avec L. Habsieger)

On étudie les entiers impairs de la forme

$$p + 2^k \textbf{ avec } p \textbf{ premier et } k \geq 1$$

Exemples : $125 = 109 + 2^4$ ou $65\,755 = 32\,987 + 2^{15}$

Question. Quelle est la “proportion” des entiers impairs qui s'écrivent sous cette forme ?

Beaucoup ! Jusqu'à 500, seuls 127, 149, 251, 331, 337, 373 ne s'écrivent pas sous cette forme.

Reformulation. Trouver des majorations de

$$d = \lim_{N\to\infty} \frac{\#\left\{n \leq N \text{ avec } n \text{ impair et } n = p + 2^k\right\}}{N/2} \ ?$$

$$\bar{d} = \limsup_{N\to\infty} \frac{\#\left\{n \leq N \textbf{ avec } n \textbf{ impair et } n = p + 2^k\right\}}{N/2}$$

L'idée d'**Erdös** est de trouver un entier M et une classe c modulo M tels que

$$c - 2^k \text{ non inversible modulo } M \text{ pour tout } k \geq 1.$$

En effet, si $n = p + 2^k \equiv c \pmod{M}$, alors

ou $p \nmid M$ et p est inversible modulo M : **impossible**

ou $p \mid M$, mais alors

$$\#\{n = p + 2^k \leq N \text{ avec } p \mid M\} \leq C \times \log N$$

et donc ces entiers ont une **densité nulle**.

Donc, une telle classe fait **diminuer la densité de** $1/M$.

Par exemple, pour $M = (2^{24} - 1)/3$, il y a 48 telles classes et donc

$$\bar{d} \leq 0.9999914161$$

On peut généraliser cette idée : si pour c une classe modulo M, l'ensemble

$$\{c - 2^k \ ; \ k \geq 1\} \cap (\mathbb{Z}/M\mathbb{Z})^\times$$

est **très petit**, alors la proportion d'entiers impairs de la forme $p + 2^k$ congrus à c modulo M est **très faible**.

Plus précisément, si le cardinal de cet ensemble est $L(c)$ alors on a

$$\lim_{N\to\infty} \frac{\#\{n = p + 2^k \leq N \text{ avec } n \equiv c \pmod{M}\}}{N/2} \leq \frac{2\,L(c)}{w \log 2\,\varphi(M)}$$

où w est l'ordre de 2 modulo M

Par un procédé de **"backtracking"**, on trouve M admettant beaucoup de telles classes avec

$$M = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 41 \cdot 73 \cdot 241 \cdot 257$$

Théorème

$$\bar{d} \leq 0.98188186$$

Extensions de degré donné d'un corps p-adique (avec S. Pauli)

Nombres p-adiques. Soit p un nombre premier

$$\mathbb{Z} = \left\{ \pm(a_0 + a_1 p + \cdots + a_k p^k) \text{ avec } k \geq 0 \text{ et } 0 \leq a_i \leq p-1 \right\}$$

$$\mathbb{Z}_p = \left\{ a_0 + a_1 p + \cdots + a_k p^k + \cdots \quad \textbf{avec } 0 \leq a_i \leq p-1 \right\}$$

Exemples :

$$\begin{aligned} -2 &= 1 + 2\cdot 3 + 2\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + \cdots \in \mathbb{Z}_3 \\ -1/3 &= 3 + 5 + 3\cdot 5^2 + 5^3 + 3\cdot 5^4 + 5^5 + \cdots \in \mathbb{Z}_5 \\ \sqrt[4]{17} &= 1 + 2 + 2^4 + 2^6 + 2^9 + 2^{13} + 2^{15} + \cdots \in \mathbb{Z}_2 \end{aligned}$$

$\mathbb{Z}_p$ est la **complétion** de $\mathbb{Z}$ pour la valeur absolue $|x| = p^{-v_p(x)}$, c'est un anneau intègre avec un **seul idéal premier**, engendré par p, dont le corps de fraction est $\mathbb{Q}_p$, le **corps de nombres p-adiques**.

Question. Calculer les extensions totalement ramifiées de degré fixé de $\mathbb{Q}_p$.

Extensions de corps.

E/F est une **extension de corps** si E et F sont deux corps avec $F \subset E$.

E est un F-espace vectoriel et on note $[E : F]$, **le degré** de E sur F, la dimension de cet espace.

E/F est **algébrique** si, pour tout $\alpha \in E$, il existe $A(X) \in F[X]$ tel que $A(\alpha) = 0$. On peut choisir A **unitaire et irréductible**, il est alors **unique**. On note $\mathrm{Irr}_\alpha(X)$.

Résultat. Si $[E : F] < +\infty$, alors E/F est algébrique.
De plus, si $\mathrm{car}(F) = 0$, alors il existe $\alpha \in E$ tel que

$$E = F(\alpha) = \left\{ \frac{P(\alpha)}{Q(\alpha)} \textbf{ avec } P, Q \in F[X],\ Q(\alpha) \neq 0 \right\} \simeq \frac{F[X]}{(\mathrm{Irr}_\alpha(X))}$$

On a alors $[E : F] = \deg \mathrm{Irr}_\alpha(X)$.

Anneaux des entiers et ramification.

Soit $K/\mathbb{Q}_p$ une extension algébrique de degré N, l'ensemble

$$\mathbb{Z}_K = \{\alpha \in K \textbf{ tel que } \mathrm{Irr}_\alpha(X) \in \mathbb{Z}_p[X]\}$$

est un sous-anneau de K, **l'anneau des entiers de K**. L'anneau $\mathbb{Z}_K$ admet un **unique idéal premier** $\mathfrak{p}_K$.

On a $p\mathbb{Z}_K = \mathfrak{p}_K^e$ et $[\mathbb{Z}_K/\mathfrak{p}_K : \mathbb{F}_p] = f$ avec $[K : \mathbb{Q}_p] = N = e \times f$.

L'extension $K/\mathbb{Q}_p$ est **totalement ramifiée** si $f = 1$. Alors, pour π générateur de $\mathfrak{p}_K$, on a $K = \mathbb{Q}_p(\pi)$ et le polynôme $\mathrm{Irr}_\pi(X)$ est un **polynôme d'Eisenstein** en p, c'est-à-dire

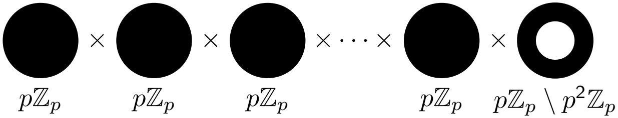
$$\mathrm{Irr}_\pi(X) = X^N + a_{N-1}X^{N-1} + \cdots + a_1 X + a_0$$

avec $a_{N-1}, \ldots, a_0 \in p\mathbb{Z}_p$ **et** $a_0 \notin p^2\mathbb{Z}_p$.

La **réciproque est aussi vraie** : une racine d'un polynôme d'Eisenstein engendre une extension totalement ramifiée.

Polynômes d'Eisenstein et extensions totalement ramifiées.

L'ensemble $\mathbb{E}_N$ des polynômes d'Eisenstein de degré N s'identifie avec



Par le **lemme de Krasner**, si deux polynômes $E_1, E_2 \in \mathbb{E}_N$ sont **très proches** alors les corps qu'ils définissent sont **isomorphes**

$$\mathbb{Q}_p[X]/(E_1) \simeq \mathbb{Q}_p[X]/(E_2)$$

Puisque $\mathbb{E}_N$ est **compact**, on en déduit qu'il suffit d'un **nombre fini de polynômes** pour engendrer toutes les extensions totalement ramifiées de degré N de $\mathbb{Q}_p$, donc ce **nombre d'extensions est fini**.

Par une étude précise, on peut déterminer un tel ensemble fini $\mathcal{S}_N$ de polynômes. **Problème** : il y a **beaucoup trop** de polynômes !

Nombre des extensions totalement ramifiées de degré N.

Soit $\mathcal{K}_N$ l'ensemble des extensions totalement ramifiées de degré N. En étudiant les **fibres** de l'application

$$\begin{array}{ccc} \displaystyle\bigcup_{K\in\mathcal{K}_N} \mathfrak{p}_K \setminus \mathfrak{p}_K^2 & \longrightarrow & \mathbb{E}_N \\ \pi & \longmapsto & \mathsf{Irr}_\pi(X) \end{array}$$

on en déduit le nombre d'éléments de $\mathcal{K}_N$. On peut alors engendrer les éléments de $\mathcal{S}_N$, **les uns après les autres**, jusqu'à obtenir suffisamment de polynômes pour définir tous les éléments de $\mathcal{K}_N$.

Exemple.

Les 9 polynômes suivants engendrent toutes les extensions totalement ramifiées de degré 3 de $\mathbb{Q}_3$

$$\begin{array}{ccc} X^3-2 & X^3+3X-1 & X^3-39X-104 \\ X^3-39X-107 & X^3-39X-116 & X^3+6X-28 \\ X^3-396X-3063 & X^3+81X-234 & X^3-396X-3054 \end{array}$$

Vérification de la Conjecture de Brumer-Stark
(avec C. Greither et B. Tangedal)

Un **corps de nombres** est une extension finie de $\mathbb{Q}$.

Pour K un corps de nombres, il existe $\alpha \in K$ tel que $K = \mathbb{Q}(\alpha)$ et donc

$$\mathbb{Q}(\alpha) \simeq \mathbb{Q}[X]/(\mathrm{Irr}_\alpha(X)) \simeq \mathbb{Q}(\alpha_i)$$

où $\alpha_1, \ldots, \alpha_d$ sont les racines de $\mathrm{Irr}_\alpha(X)$ dans $\mathbb{C}$.

On pose r_1 le nombre de α_i appartenant à $\mathbb{R}$ et $2r_2 = d - r_1$ le nombre de α_i appartenant à $\mathbb{C} \setminus \mathbb{R}$.

K est **totalement réel** si $r_2 = 0$ et **totalement complexe** si $r_1 = 0$.

Un **idéal fractionnaire** de K est de la forme $a^{-1}\mathfrak{a}$ avec $a \in \mathbb{Z}_{\geq 1}$ et $\mathfrak{a}$ un idéal **entier** non nul de $\mathbb{Z}_K$. Les idéaux fractionnaires de K forment un groupe I_K, et les idéaux **principaux** un sous-groupe P_K d'**indice fini**.

Soit K/k une **extension abélienne** de corps de nombres, c'est-à-dire le groupe de Galois $\mathrm{Gal}(K/k)$ de cette extension est un **groupe abélien**.

La **théorie du corps de classes** associe à cette extension un idéal entier $\mathfrak{f}$ de k, la partie finie du **conducteur** de K/k, et un morphisme de groupes

$$\begin{array}{rcl} I_k(\mathfrak{f}) & \longrightarrow & \mathrm{Gal}(K/k) \\ \mathfrak{a} & \longmapsto & \sigma_{\mathfrak{a}} \end{array}$$

où $I_k(\mathfrak{f})$ est le groupe des idéaux (fractionnaires) de k **premiers** avec $\mathfrak{f}$.

Pour $\sigma \in \mathrm{Gal}(K/k)$, on définit une fonction **zêta partielle**

$$\zeta_{K/k}(\sigma, s) = \sum_{\substack{\mathfrak{a} \in I_K(\mathfrak{f}),\ \mathfrak{a} \subset \mathbb{Z}_K \\ \sigma_{\mathfrak{a}} = \sigma}} \mathcal{N}\mathfrak{a}^{-s} \qquad \Re(s) > 1$$

avec $\mathcal{N}\mathfrak{a} \in \mathbb{N}$, la **norme** de l'idéal entier $\mathfrak{a}$.

On suppose K **totalement complexe** et k **totalement réel**.

Soit w_K le nombre de **racines de l'unité** dans K, l'**élément de Brumer** est défini par

$$\Theta_{K/k} = w_K \sum_{\sigma \in \mathrm{Gal}(K/k)} \zeta_{K/k}(\sigma, 0) \cdot \sigma^{-1} \in \mathbb{Z}[\mathrm{Gal}(K/k)].$$

Soit $\mathfrak{A}$ un idéal fractionnaire de K. On dit que $BS(\mathfrak{A})$ est vérifié si

1. L'idéal $\mathfrak{A}^{\Theta_{K/k}}$ est un idéal **principal**

et admet un générateur $\alpha(\mathfrak{A})$ tel que

2. $\alpha(\mathfrak{A})$ est une **anti-unité**, *i.e.* $|\sigma(\alpha(\mathfrak{A}))| = 1$, $\forall \sigma \in \mathrm{Gal}(K/k)$.
3. $\alpha(\mathfrak{A})$ est w_K**-abélien** pour K/k, *i.e.* $\forall \lambda \in \mathbb{C}$ avec $\lambda^{w_K} = \alpha(\mathfrak{A})$, l'extension $K(\lambda)/k$ est abélienne.

Conjecture de Brumer-Stark.

$BS(\mathfrak{A})$ est vérifiée pour tout idéal fractionnaire $\mathfrak{A}$ de K.

Question. Comment vérifier cette conjecture ?

L'ensemble

$$\{\mathfrak{A} \in I_K \text{ tel que } BS(\mathfrak{A}) \text{ est vérifiée}\}$$

est un sous-groupe de I_K, stable sous l'action de Gal(K/k), et contenant les idéaux principaux de K. Ainsi la vérification de la conjecture de Brumer-Stark se ramène à un **nombre fini** de vérifications $BS(\mathfrak{A}_i)$, $i = 1, .., s$ avec

$$\langle \mathfrak{A}_1, \cdots, \mathfrak{A}_s \rangle_{\mathbb{Z}[\mathrm{Gal}(K/k)]} \cdot P_K = I_K.$$

Soit $\mathfrak{A}$ idéal fractionnaire de K, comment vérifier $BS(\mathfrak{A})$?

On commence par déterminer $\Theta_{K/k}$. Pour cela, on calcule des **valeurs approchées** des fonctions $\zeta_{K/k}(\sigma, 0)$, on remplace dans la formule et on **arrondit** aux entiers les plus proches.

Puis, on calcule

$$\mathfrak{A}^{\Theta_{K/k}}$$

et on vérifie que c'est bien un **idéal principal**.

On trouve un **générateur** $\alpha(\mathfrak{A})$. Pour vérifier si c'est une **anti-unité**, on utilise le critère suivant

α est une anti-unité ssi $\alpha^{1+c} = 1$, $\forall c$ conjugaison complexe de K.

Si ce n'est pas le cas, on **réduit** $\alpha(\mathfrak{A})$ modulo le groupe U_K des **unités** de K, pour obtenir une anti-unité. Mais, en fait c'est **toujours** le cas !

Pour tester si $\alpha(\mathfrak{A})$ est **w_K-abélien pour K/k**, on utilise le critère suivant

Soient $\sigma_1, \ldots, \sigma_t$ un système de générateurs de $\mathrm{Gal}(K/k)$, et des entiers N_i avec $\sigma_i(\omega) = \omega^{N_i}$ pour toutes racines de l'unité $\omega \in K$.

Alors, α est w_K-abélien ssi $\exists \beta_i \in K$ tels que

$$\alpha^{\sigma_i - N_i} = \beta_i^{w_K}, \ \forall i$$

$$\beta_i^{\sigma_j - N_j} = \beta_j^{\sigma_i - N_i}, \forall i \neq j.$$

Toutes ces tests se font sur des objets **exacts**, ainsi chaque vérification pour une extension K/k fournit une **preuve de la validité** de la conjecture.

Vérification

La conjecture de Brumer-Stark est démontrée par cette méthode pour 379 extensions K/k de groupe C_4 avec k quadratique réel, 534 extensions K/k de groupe C_6 avec k quadratique réel, et 259 extensions K/k de groupe C_6 avec k cubique réel.

Ces calculs ont aussi permis de remarquer un phénomène sur la 2-**partie** dans les exemples du **premier cas**. Dans toutes ces exemples, une part de la 2-partie peut être **supprimée** sans affecter la validité de la conjecture.

Merci de votre attention !