Antoine Hugounet

Idéaux de Carmichael et primalité

travail encadré de recherche
encadré par Alain Kraus (IMJ-PRG)
de janvier à juin 2020

Sorbonne Université

Introduction

Ce mémoire s'applique à étudier les idéaux de Carmichael dans les corps de nombres et évaluer la viabilité de cette jeune théorie pour fournir un test de primalité. Le point de départ est l'article de G.A. Steele *Carmichael numbers in number rings* [1]. Commençons par quelque énoncés.

Le test de primalité non naïf le plus simple est le *test de primalité de Fermat*. Étant donné un entier n dont on veut tester la primalité, ce dernier affirme que s'il existe un entier a vérifiant $a^n \not\equiv a \pmod{n}$, alors n est composé. Il existe cependant des entiers n **composés** vérifiant

$$a^n \equiv a \pmod{n}$$

pour tout entier a. On les appelle *entiers de Carmichael* et le test de Fermat est incapable de prouver leur composition. Pire encore, il existe une infinité de tels entiers. On peut les caractériser ainsi.

Proposition 0.1. *Soit n un entier. Les assertions suivantes sont équivalentes :*

(a) *n est un entier de Carmichael ;*

(b) *n est composé, sans facteur carré et pour tout nombre premier p divisant n, on a*

$$p - 1 \mid n - 1 \ ;$$

(c) *on a*

$$\lambda(n) \mid n - 1,$$

la fonction λ étant l'indicatrice de Carmichael.

L'assertion (b) de la proposition est appelée *critère de Korselt* et est l'outil théorique le plus couramment utilisé pour démontrer qu'un entier donné est de Carmichael. Le lecteur désireux d'une preuve de cette proposition pourra se référer au *cours d'algèbre* de M. Demazure [2] §3.3, p. 89. Dans l'article susnommé [1], la notion d'entier de Carmichael est étendue à la notion d'*idéal de Carmichael* dans l'anneau d'entiers d'un corps de nombres.

Définition 0.2. Soient K un corps de nombres et I un idéal de $\mathcal{O}_K$. On dit que I est un idéal de Carmichael si pour tout entier algébrique $\alpha \in \mathcal{O}_K$, la congruence

$$\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{I} \qquad (*)$$

est vérifiée.

Remarque 0.3. Un entier de Carmichael peut donc être vu comme un idéal de Carmichael du corps de nombres $\mathbb{Q}$.

Cette définition est le point de départ d'un formalisme fructueux. Ce dernier donne naissance à une réciproque au petit théorème de Fermat 1.3 et à plusieurs tests de primalité théoriques. L'auteur de l'article, après quelques énoncés généraux, s'intéresse spécifiquement aux corps quadratiques et aux corps cyclotomiques ; nous suivrons ces traces. Tout en assurant une base solide à sa théorie, l'auteur soulève de nombreuses questions, notamment la question fondamentale suivante.

Question 0.4. Soient n un entier de Carmichael et K un corps de nombre. Dans quel mesure n est-il de Carmichael dans K ?

Nous nous proposons de répondre nous même à une partie de ces questions au fil de ce mémoire.

À noter que l'auteur du présent texte a choisi de ne pas y incorporer toutes les preuves des énoncés de l'article : ne sont données que celles des théorèmes 2.2, 2.3 et 3.6. Les démonstrations de l'auteur de l'article sont claires et nous n'aurions rien d'autre à apporter que de la paraphrase. Nous jugeons plus opportun de commenter ces dernières, ce que nous faisons dans des environnements intitulés *Un mot sur la preuve.*

Donnons dès à présent la liste des vingt-neuf premiers entiers de Carmichael. Nous l'étudierons beaucoup dans la suite de ce mémoire [1].

$$\left\{\begin{array}{c} 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \\ 15841, 29341, 41041, 46657, 52633, 62745, 63973, \\ 75361, 101101, 115921, 126217, 162401, 172081, \\ 188461, 252601, 278545, 294409, 314821, 334153, \\ 340561, 399001, 410041, 449065, 488881, 512461 \end{array}\right\} \qquad (\mathfrak{C})$$

1. C'est l'entrée A002997 de l'encyclopédie en ligne des séquences d'entiers : `https://oeis.org/A002997`.

1 Délices de la théorie

Fort heureusement, certaines propriétés fondamentales des *entiers* de Carmichael restent vraies dans le cadre plus général des *idéaux* de Carmichael. Tout d'abord, le petit théorème de Fermat se généralise aux corps de nombres galoisiens : dans une telle extension, un nombre premier engendre un idéal qui est soit premier, soit de Carmichael. Plus formellement, vient ceci.

Théorème 1.1 (petit théorème de Fermat généralisé, 2.3 dans l'article)**.** *Soient p un nombre premier et K un corps de nombre galoisien tel que $p \nmid \mathrm{Disc}(K)$. Alors, pour tout entier algébrique $\alpha \in \mathcal{O}_K$, on a*

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(p)} \equiv \alpha \pmod{p\mathcal{O}_K}.$$

Démonstration. Comme $p \nmid \mathrm{Disc}(K)$, le nombre premier p n'est pas ramifié dans $\mathcal{O}_K$. Comme l'extension $K/\mathbb{Q}$ est galoisienne, les indices de ramifications et degrés résiduels des idéaux de $\mathcal{O}_K$ au dessus de $\mathfrak{p}$ sont égaux. L'idéal $p\mathcal{O}_K$ est donc de la forme

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdot \ldots \mathfrak{p}_r.$$

Soit donc f ce degré résiduel. On a $ef = [K : \mathbb{Q}]$ et surtout que f divise $[K : \mathbb{Q}]$. Ainsi, pour tout indice $1 \leqslant i \leqslant r$, il vient

$$\mathrm{N}(\mathfrak{p}_i) - 1 = p^f - 1 \mid p^{[K:\mathbb{Q}]} - 1 = \mathrm{N}(p\mathcal{O}_K) - 1.$$

L'idéal $\mathcal{O}_K$ vérifie donc le critère de Korselt généralisé 1.4. Il est donc soit premier, soit de Carmichael. □

Fait tout à fait remarquable, l'auteur de l'article fournit une réciproque au petit théorème de Fermat dans ce nouveau cadre des idéaux de Carmichael.

Théorème 1.2 (réciproque du petit théorème de Fermat généralisé, 2.3 dans l'article)**.** *Soit $n > 2$ un entier composé. Alors il existe un corps* quadratique *K vérifiant $n \nmid \mathrm{Disc}(K)$ et un entier algébrique $\alpha \in \mathcal{O}_K$ tels que*

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n)} \not\equiv \alpha \pmod{n\mathcal{O}_K}.$$

Un mot sur la preuve. À l'instar de beaucoup d'autres résultats de l'article, la preuve de cet énoncé jouit à la fois d'une complexité technique raisonnable et d'une grande ingéniosité. Connaissant un diviseur p premier de n, l'auteur construit un corps quadratique $K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ dans lequel n n'est pas de Carmichael. Ce dernier point se démontre avec des techniques de base de la ramification.

Nous pouvons de plus mettre à bout ces deux résultats pour fournir cette délicieuse équivalence.

Théorème 1.3 (petit théorème de Fermat généralisé et sa réciproque)**.** *Soit $n > 2$ un entier. Alors n est premier si, et seulement si, pour tout corps* quadratique *K vérifiant $n \nmid \mathrm{Disc}(K)$ et tout entier algébrique $\alpha \in \mathcal{O}_K$, on a*

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n)} \equiv \alpha \pmod{n\mathcal{O}_K}.$$

Au delà de sa force théorique, cette énoncé semble porter une valeur historique majeure. Le test de primalité de Fermat était le seul test de primalité à ne pas disposer d'une réciproque (pour le test d'Euler par exemple, c'est une équivalence). Cette absence de réciproque semblait bien être le prix à payer pour sa simplicité et son efficacité. Il aura certes fallu aller chercher la réciproque dans les corps de nombres, mais l'énoncé prouve que les corps quadratiques. Ces objets ne sont d'ailleurs pas si loin de l'arithmétique classique : Gauss les étudiait déjà.

Un autre résultat d'importance (démontré avant le petit théorème de Fermat généralisé dans l'article) est la généralisation du critère de Korselt 0.1. C'est ce résultat que l'on utilise en premier lieu pour déterminer si un entier est de Carmichael.

Théorème 1.4 (critère de Korselt généralisé, 2.2 dans l'article)**.** *Soient K un corps de nombres et I un idéal de $\mathcal{O}_K$. On prend garde à supposer que I est composé. Alors I est de Carmichael si, et seulement si, I est sans facteurs carrés et pour tout idéal premier $\mathfrak{P}$ divisant I, on a*

$$\mathrm{N}(\mathfrak{P}) - 1 \mid \mathrm{N}(I) - 1.$$

Démonstration. Commençons par le sens réciproque. Soit $\alpha \in \mathcal{O}_K$ un entier algébrique et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ divisant I. Si $\alpha \notin \mathcal{O}_K$, viennent $\alpha^{\mathrm{N}(\mathfrak{p})-1} \equiv \alpha \pmod{p}$ et donc

$$\alpha^{\mathrm{N}(I)-1} \equiv \alpha \pmod{p},$$

car $\mathrm{N}(\mathfrak{p}) - 1 \mid \mathrm{N}(I) - 1$ par hypothèse. Si désormais $\alpha \in \mathfrak{p}$, la dernière congruence est toujours vérifiée. L'idéal I étant de plus sans facteurs carrés (hypothèse), il est de la forme $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, les $\mathfrak{p}_i$ étant des idéaux premiers distincts de $\mathcal{O}_K$. Ces idéaux sont même maximaux (anneau de Dedekind) et donc comaximaux, d'où un isomorphisme d'anneaux

$$\mathcal{O}_K \Big/ (\mathfrak{p}_1 \cdot \cdots \cdot \mathfrak{p}_r) \simeq \mathcal{O}_K \Big/ \mathfrak{p}_1 \times \cdots \times \mathcal{O}_K \Big/ \mathfrak{p}_r$$

et la congruence

$$\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{I}.$$

Démontrons cette fois le sens direct. La preuve se fait en deux temps, on montre les relations de divisibilité puis que I est sans facteur carré. Écrivons $I = \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_r^{e_r}$, les

$\mathfrak{p}_i$ étant des idéaux premiers de $\mathcal{O}_K$ distincts. Pour tout indice $1 \leqslant i \leqslant r$ donnons nous $\alpha_i \in \mathcal{O}_K$ un élément dont la classe modulo $\mathfrak{p}_i$ engendre le groupe quotient $(\mathcal{O}_K/\mathfrak{p}_i)^\times$. Un tel élément existe car $\mathcal{O}_K/\mathfrak{p}_i$ est un corps fini et que le groupe des inversibles d'un corps fini est cyclique. En particulier, α_i n'est *pas* dans $\mathfrak{p}_i$. On a alors

$$\alpha_i^{\mathrm{N}(I)-1} \equiv \alpha_i \pmod{\mathfrak{p}_i}$$

(comme dans le paragraphe précédent) puis que l'ordre de α_i modulo $\mathfrak{p}_i$ divise $\mathrm{N}(I)-1$ (théorème de Lagrange). Cet ordre étant $\mathrm{N}(\mathfrak{p}_i)-1$, on en déduit la division désirée.

Démontrons désormais que I est sans facteurs carrés. Supposons qu'il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ tel que $p^2 \mid \mathcal{O}_K$ et posons

$$H = \left(\mathcal{O}_K \Big/ \mathfrak{p}^2\right)^\times.$$

On a

$$|H| = \mathrm{N}(\mathfrak{p})(\mathrm{N}(\mathfrak{p})-1).$$

Soit $p \in \mathbb{Z}$ l'unique nombre premier tel que $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. L'entier $\mathrm{N}(\mathfrak{p})$ est une puissance de $\mathfrak{p}$, d'où $p \mid \mathrm{N}(\mathfrak{p})$ et

$$p \mid |H|.$$

Le théorème de Cauchy abélien assure alors qu'il existe un élément $\alpha \in H$ d'ordre p. Comme I est de Carmichael par hypothèse et que $\alpha \notin \mathfrak{p}^2$, on a $\alpha^{\mathrm{N}(I)-1} \equiv 1 \pmod{\mathfrak{p}^2}$ puis $\alpha^{\mathrm{N}(I)-1} \equiv 1 \pmod{\mathfrak{p}^2}$ et

$$p \mid \mathrm{N}(I) - 1.$$

Comme $p \mid \mathrm{N}(I)$, cela constitue une contradiction. L'idéal I est donc sans facteur carré. □

Remarque 1.5. Le critère de Korselt que nous connaissons dans le cadre de l'arithmétique se déduit immédiatement du critère de Korselt généralisé en prenant $K = \mathbb{Q}$.

Remarque 1.6. Il faut ici se montrer vigilant avec la nomenclature. Un idéal I est de Carmichael dans un corps de nombres K si I est un idéal **composé** qui *en plus de cela*, vérifie l'identité $*$ pour tout entier algébrique $\alpha \in \mathcal{O}_K$.

Si l'on a un corps de nombres L et un idéal J de $\mathcal{O}_K$, montrer que $\mathrm{N}(\mathfrak{P})-1 \mid \mathrm{N}(J)-1$ pour tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ divisant J ne suffit pas. La preuve du critère de Korselt généralisé 1.4 nous enseigne que si J est premier, J vérifie également cette identité. Il faut donc indépendamment montrer que J est composé si l'on veut montrer que J est un idéal de Carmichael. Là est le cœur du problème. L'auteur de l'article fait lui-même une petite erreur en oubliant cette hypothèse dans l'énoncé du théorème 2.7 : il doit y supposer n composé.

Avant de poursuivre, donnons un lemme qui permettra d'alléger les énoncés de l'article.

Lemme 1.7. *Soient n un entier et K un corps de nombres. Si n est de Carmichael dans K, alors n et* $\mathrm{Disc}(K)$ *sont premiers entre eux.*

Démonstration. Si n et $\mathrm{Disc}(K)$ ne sont pas premiers entre eux, n a un facteur premier qui se ramifie dans $\mathcal{O}_K$. L'idéal $n\mathcal{O}_K$ a donc un facteur carré, ce qui l'empêche d'être un idéal de Carmichael d'après le critère de Korselt généralisé 1.4. □

Ces résultats fournissent un début de théorie confortable, qui nous laisse envisager l'avenir avec espoir. Nous pouvons dès à présent nous confronter à une étude plus spécifique, celle des corps quadratiques.

2 Corps quadratiques

2.1 Vers un possible test de primalité

Entrons dès à présent dans le vif du sujet. L'un de nos objectifs principaux de répondre à la question 0.4. Le théorème 2.5 de l'article y apporte de premiers éléments de réponse.

Théorème 2.1 (2.5 dans l'article)**.** *Soit n un entier impair sans facteurs carrés. S'il existe un diviseur premier p de n tel que*

$$p^2 - 1 \nmid n^2 - 1,$$

alors il existe une infinité de corps quadratiques K dans lesquels n n'est pas *de Carmichael.*

Un mot sur la preuve. On présage dès l'énoncé la nature de la preuve : c'est le critère de Korselt généralisé 1.4. On commence par s'assurer que n est sans facteurs carrés de sorte de contrôler la décomposition de $n\mathcal{O}_K$ dans un corps quadratique K donné. Du reste, comme la norme d'un idéal premier au dessus de $n\mathcal{O}_K$ est un nombre premier p divisant n, on sent bien que la condition de non-divisibilité va empêcher être n d'être de Carmichael dans les corps quadratiques [2] bien choisis. La partie réellement inventive de la preuve consiste à trouver les bons corps quadratiques. Cette partie est hautement non triviale et est basée sur la connaissance d'un nombre premier p comme dans les hypothèses du théorème et sur une savante utilisation du théorème chinois. Les techniques de base de la ramification permettent encore une fois de s'assurer que les corps construits vérifient bien ce qu'on leur demande de vérifier.

2. Les carrés ne sont ni plus ni moins que les normes de p et de n dans toute extension quadratique.

Bien que cet énoncé ne semble pas optimal en pratique [3], certains nombres de Carmichael vérifient ces hypothèses. C'est le cas par exemple du nombre de 512461 et de son facteur premier 271. Il existe ainsi une infinité de corps quadratiques dans lequel 512461 n'est pas de Carmichael. Mieux encore, nous avons numériquement exhibé pour chaque entier de Carmichael de la liste $\mathfrak{C}$ une liste de corps quadratiques dans lequel ledit entier n'est pas de Carmichael. **ajouter liste**

Complément. Une liste bien plus dense exhibée par l'auteur de ce mémoire est disponible sur sa page GitHub : `https://github.com/kryzar/ter-carmichael/blob/master/scripts/results_carmichael_not_carmichael_in_quad_field.txt`.

Malgré cela, l'algorithme que nous avons utilisé pour trouver ces corps est sans doute très sous-optimal. Utilisant le critère de Korselt généralisé 1.4, il impose de décomposer l'idéal $n\mathcal{O}_K$ en produit d'idéaux premiers [4]. Dans l'exemple 2.6 de l'article, l'auteur ouvre une voix bien plus intéressante. Il montre que $n = 561$ est composé en exhibant le corps quadratique $K = Q(\sqrt{13})$ puis l'entier algébrique $\alpha = 2 + 1 \cdot \left(\frac{1+\sqrt{13}}{2}\right) \in \mathcal{O}_K$. Comme

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n)} \not\equiv \alpha \pmod{n\mathcal{O}_K}$$

et que n et 13 sont premiers entre eux, cela prouve la composition de n. Le point clé est que l'auteur ne semble pas utiliser le critère de Korselt (il n'a pas donné les détails et nous ne pouvons en conséquence pas en être sûrs). Cette approche nous invite à étudier l'algorithme *probabiliste* suivant. Soit n un entier impair (potentiellement de Carmichael).

3. Il n'y a à ce jour (3 juin 2020) pas d'algorithme efficace pour déterminer si un entier est sans facteurs carrés. Les algorithmes passent souvent par la décomposition en produit de facteurs premiers, ce qui ne nous arrange pas. **sourcer**.

4. **Si possible, donner un mot sur la complexité de l'algo de décomposition dans un extension**

Entrées : b (borne coordonnées α)
pour chaque $d \in \mathbb{N}$ *sans facteurs carrés* **faire**
  $K \leftarrow \mathbb{Q}(\sqrt{d})$
  $\theta \leftarrow$ un générateur de $\mathcal{O}_K$
  si d *et* n *sont premiers entre eux* **alors**
    pour chaque $\alpha = x + y\theta$, $x, y \in [\![1, b]\!]$ **faire**
      si $\alpha^{n^2} \not\equiv \alpha \pmod{n\mathcal{O}_K}$ **alors**
        retourner n *est composé*
        fin du programme
      fin
    fin
  fin
fin

Pour que cet algorithme soit viable en pratique, il conviendra de définir la notion de *témoin de Carmichael* et d'étudier finement leur répartition, à la manière du test de primalité de Rabin-Miller (voir § 2.3.7, p.69 de [2]). L'auteur de ce présent mémoire est pleinement conscient du travail à accomplir. Par ailleurs, il n'y aucune preuve que l'algorithme termine en l'état.

Il peut en outre être tentant d'utiliser cet algorithme pour déterminer la primalité de n avec une certitude morale, toujours dans l'esprit test de primalité de Rabin-Miller. L'idée serait que si n vérifie la congruence $\alpha^{\mathrm{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}} \equiv \alpha \pmod{n\mathcal{O}_K}$ pour un nombre suffisamment grand de corps quadratiques $K = \mathbb{Q}(\sqrt{d})$ de discriminant premier avec n et d'entiers algébriques $\alpha \in \mathcal{O}_K$, nous aurions une certitude morale de la primalité de n. Mais l'existence d'entiers h qui sont de Carmichael *dans tout corps quadratique de discriminant premier avec* h est un problème majeur qui empêche de considérer cette voie. C'est le propos de la prochaine sous-section.

2.2 Un pas en arrière

Revenons un pas en arrière. Nous avons évoqué la réciproque du petit théorème de Fermat (1.3). Il faut bien faire attention au fait que l'énoncé suivant est faux !

Énoncé faux 2.2 (réciproque eronnée du petit théorème de Fermat généralisé)**.** *Soit* $n > 2$ *un entier. Alors* n *est premier si, et seulement si, pour tout corps* quadratique K *vérifiant* $\mathrm{pgcd}(n, \mathrm{Disc}(K)) = 1$ *et tout entier algébrique* $\alpha \in \mathcal{O}_K$*, on a*

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n)} \equiv \alpha \pmod{n\mathcal{O}_K}.$$

Si l'on veut prouver qu'un entier $n > 2$ est premier, montrer que la congruence précédente est vérifiée pour tous les corps quadratiques de discriminant premier avec

n ne suffit pas. Il faut s'assurer pour tous les corps quadratiques de discriminant non divisé par n. Même si ces notions sont les mêmes lorsque n est effectivement premier, cette condition est beaucoup plus forte ! Il est même facile de démontrer le résultat suivant.

Théorème 2.3 (2.7 dans l'article)**.** *Soient n un entier composé sans facteur carré et $d \geqslant 1$ un entier. Si pour tout diviseur p de n et tout enter $1 \leqslant i \leqslant d$ la division*

$$p^i - 1 \mid n^d - 1$$

est vérifiée, alors n est de Carmichael dans $\mathbb{Q}$ et tout corps de nombres de degré d de discriminant premier avec n.

Définition 2.4. Un entier n vérifiant les hypothèses du théorème 2.3 pour un certain entier $d \geqslant 1$ est appelé *nombre de Carmichael rigide d'ordre d.*

Chose troublante, de tels nombres existent.

Théorème 2.5 (Howe, 2000)**.** *Il existe un couple (n, d) d'entiers tel que n soit un entier de Carmichael rigide d'ordre d.*

En guise de preuve, E. W. Howe exhibe un entier de Carmichael rigide d'ordre 2. Il est donné par

$$h = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$$

et est appelé *entier de Howe.*

À la lumière de ces troublants résultats, si l'on veut pouvoir trouver un test de primalité *alla* Rabin-Miller comme évoqué dans la sous-section précédente, il faudra modifier l'algorithme (2) en la version suivante.

Entrées : I (intervalle d'entiers d sans facteurs carrés), b (borne coordonnées α)
pour chaque $d \in \mathbb{N}$ *sans facteurs carrés dans* I **faire**
  $K \leftarrow \mathbb{Q}(\sqrt{d})$
  $\theta \leftarrow$ un générateur de $\mathcal{O}_K$
  si n *et* $\mathrm{Disc}(K)$ *sont premiers entre eux* **alors**
    pour chaque $\alpha = x + y\theta$, $x, y \in [\![1, b]\!]$ **faire**
      si $\alpha^{n^2} \not\equiv \alpha \pmod{n\mathcal{O}_K}$ **alors**
        retourner n *est composé*
        fin du programme
      fin
    fin
  fin
fin
retourner n *a une certitude morale d'être premier*

Il y a de nouveau un travail substantiel à faire pour s'assurer de la viabilité de cette direction. Il ne faut pas non plus négliger d'autres pistes, c'est pourquoi nous partons explorer le royaume des corps cyclotomiques.

3 Corps cyclotomiques

3.1 Horizon

L'étude des idéaux de Carmichael dans les corps cyclotomiques est porteuse d'espoir et fournit de beaux résultats susceptibles d'être à la base de tests de primalité, notamment le théorème 3.6. Notons que les seuls corps qui nous intéressent ici sont les corps cyclotomiques engendrés par des racines primitive p-ième de l'unité, où p est premier. Commençons par un résultat théorique.

Théorème 3.1 (3.1 dans l'article)**.** *Pour tout entier naturel n composé, il existe une infinité de corps de nombres* abéliens *K de discriminant premier avec n dans lesquels n* n'est pas de Carmichael.

Un mot sur la preuve. Les preuves des énoncés sur les corps cyclotomiques sont autrement plus sophistiquées que celles sur les corps quadratiques ; l'auteur utilise à volonté des résultats de théorie analytique des nombres. Ces derniers assurent de l'existence d'objets mais ne les construisent pas, à l'image des lemmes 3.3 et 3.4 de l'article. La construction des corps se fait avec la correspondance de Galois et la vérification que ces corps fonctionnent nécessitent des arguments sophistiqués de ramification (groupes de décomposition et d'inertie, Frobenius d'un élément). Nous verrons ces arguments plus en détails dans la preuve du théorème 3.6 de l'article 3.3.

Un nombre de Carmichael étant composé, il vérifie les hypothèses du théorème. Cela fournit une nouvelle réciproque au petit théorème de Fermat, plus contraignante que la précédente.

Théorème 3.2 (deuxième réciproque)**.** *Soit n un entier. Alors n est premier si, et seulement si, pour tout corps de nombres* abélien *K de discriminant premier avec n et tout entier algébrique $\alpha \in \mathcal{O}_K$, on a*

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n\mathcal{O}_K)} \equiv \alpha \pmod{n\mathcal{O}_K}.$$

Le résultat le plus à même d'aboutir à un test de primalité est le théorème suivant.

Théorème 3.3 (3.6 dans l'article)**.** *Soit n un entier composé ayant au moins trois facteurs premiers distincts. Alors il existe une infinité de corps cyclotomiques K de la forme $K = \mathbb{Q}(\zeta_q)$, q étant premier, tels que* $\mathrm{Disc}(K)$ *est premier avec n et n* n'est pas de Carmichael dans K.

Un nombre de Carmichael ayant toujours au moins trois diviseurs premiers distincts, il est aisé d'aboutir à ce corollaire.

Corollaire 3.4 (3.7 dans l'article)**.** *Soit n un entier composé. Il existe au moins un corps cyclotomique de la forme $\mathbb{Q}(\zeta_q)$, q étant premier, de discriminant premier avec n dans lequel n n'est pas de Carmichael.*

Ce corollaire a bien entendu droit à sa réciproque du théorème de Fermat.

Théorème 3.5 (troisième réciproque)**.** *Soit n un entier. Alors n est premier si, et seulement si, pour tout corps cyclotomique K de la forme $K = \mathbb{Q}(\zeta_q)$, q étant premier, et tout entier algébrique $\alpha \in \mathcal{O}_K$, on a*

$$\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n\mathcal{O}_K)} \equiv \alpha \pmod{n\mathcal{O}_K}.$$

Remarque 3.6. Dans ces deux réciproques, l'hypothèse sur les discriminants n'est plus que n ne doit pas diviser $\mathrm{Disc}(K)$ comme dans **??** mais bien que $\mathrm{Disc}(n)$ et $\mathrm{Disc}(K)$ soient premiers entre eux.

3.2 Pratique

Armé du corollaire 3.4, l'auteur a pu implémenter un algorithme SageMath apportant dans certains cas une réponse à la question centrale de l'article (0.4). Ici, nous nous donnons des nombres de Carmichael n et cherchons des corps cyclotomiques K de la forme $K = \mathbb{Q}(\zeta_q)$, q étant premier, dans lesquels n *n'est pas de Carmichael*. Nous testons les entiers de Carmichael de la liste $\mathfrak{C}$ **ajouter référence** avec l'algorithme suivant.

Entrées : borne_q
pour chaque *n dans liste_entiers_Carmichael* **faire**
  pour chaque *q nombre premier dans* $[\![3, \text{borne\_q}]\!]$ **faire**
    $K = \mathbb{Q}(\zeta_q)$;
    si $\mathrm{pgcd}(q, n) = 1$ **alors**
      si *n n'est pas de Carmichael dans K* **alors**
        exporter le couple (n, q) dans un fichier texte ;
      fin
    fin
  fin
fin

Remarque 3.7. Pour tester si un nombre est de Carmichael dans un corps de nombres de donné, nous implémentons le critère de Korselt dans une fonction dédiée. Pour plus de détails sur l'implémentation de ces algorithmes, nous invitons le lecteur à se référer à l'annexe A.

Pour chacun des nombres n de la liste $\mathfrak{C}$, cet algorithme a pu exhiber de nombreux corps cyclotomiques dans lesquels n n'est pas de Carmichael, prouvant que n est composé ! Par exemple,

— 561 n'est pas de Carmichael dans $\mathbb{Q}(\zeta_5)$;

— 1729 n'est pas de Carmichael dans $\mathbb{Q}(\zeta_{17})$;

— 512461 n'est pas de Carmichael dans $\mathbb{Q}(\zeta_{83})$.

Nombre d'autres résultats sont disponibles sur la page GitHub de l'auteur : `https://github.com/kryzar/TER-Carmichael/blob/master/Scripts/Results_Corollary_3-7.txt`.

Cet algorithme permet aussi de prouver que l'entier de Howe est composé ! Notons h cet entier. Mentionné après le théorème 2.7 de l'article, h vaut

$$h = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331$$

et est de Carmichael non seulement dans $\mathbb{Q}$, mais aussi dans tout corps quadratique dont le discriminant est premier avec h (on dit que h est un nombre de Carmichael *rigide d'ordre 2*). Notre algorithme exhibe toutefois de nombreux corps cyclotomiques dans lesquels h n'est pas de Carmichael, comme $\mathbb{Q}(\zeta_{199})$. La liste complète des résultats trouvés est cette fois disponible à `https://github.com/kryzar/TER-Carmichael/blob/master/Scripts/Results_Howe_cyclotomic.txt`.

4 Idéaux, extensions, simulation

Dans toute cette sous-section, nous nous donnons

$$\mathbb{Q} \subset K \subset L$$

une tour de corps de nombres et

— $I \subset \mathcal{O}_K$ un idéal de Carmichael de K ;

— $J \subset \mathcal{O}_L$ un idéal de Carmichael de L.

Question 4.1. L'idéal étendu $I\mathcal{O}_L$ est-il de Carmichael dans L et l'idéal restreint $J \cap \mathcal{O}_K$ est-il de Carmichael dans K ?

Nous avons déjà montré la première partie de la question sans la sous-section précédente ! En prenant $K = \mathbb{Q}$ et un corps quadratique pour L, nous avons établi que pour tout entier n de Carmichael de la liste $\mathfrak{C}$, il existait plusieurs corps quadratiques dans lesquels n n'est pas de Carmichael.

Proposition 4.2. *Il existe des tours de corps de nombres $\mathbb{Q} \subset K \subset L$ et des idéaux de Carmichael I de K pour lesquels l'idéal étendu $I\mathcal{O}_L$ qui ne sont pas de Carmichael dans L.*

Intéressons nous à la deuxième partie de la question.

Proposition 4.3. *Il existe des tours de corps de nombres $\mathbb{Q} \subset K \subset L$ et des idéaux de Carmichael J de L pour lesquels l'idéal restreint $J \cap \mathcal{O}_K$ n'est pas de Carmichael dans K.*

Avant de se lancer dans cette étude, il convient d'aller explorer le royaume des corps cyclotomiques, ce qui s'avérera porteur d'espoir pour l'élaboration d'un test de primalité.

Il n'aura pas fallu aller chercher bien loin pour trouver des exemples de tels corps et idéaux. Prendre $K = \mathbb{Q}$ et un corps quadratique pour L aura suffi. Si l'on dispose d'un idéal de Carmichael dans un corps de nombres donné et d'une extension finie de ce corps de nombres, il s'avère difficile de déterminer si l'idéal reste de Carmichael dans le grand corps de nombres.

Conclusion

A Produire des contre-exemples

Question : soient $\mathbb{Q} \subset K \subset L$ une tour de corps de nombres et $n \in \mathbb{Z}$ un entier, si n est de Carmichael dans $\mathcal{O}_L$, l'est-il dans $\mathcal{O}_K$? Nous affirmons que cette assertion est fausse en exhibant un contre exemple à l'aide du critère de Korselt généralisé ([1], théorème 2.2). Ce critère impose une condition sur les facteurs de $n\mathcal{O}_K$ ($n\mathcal{O}_K$ doit être sans facteurs carrés) et une condition sur les normes des diviseurs premiers de $n\mathcal{O}_K$ ($\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) - 1$ doit diviser $\mathrm{N}_{K/\mathbb{Q}}(n\mathcal{O}_K) - 1$ pour tout idéal premier de $\mathcal{O}_L$ divisant $n\mathcal{O}_K$). L'enjeu est de comprendre si ces propriétés vraies dans $\mathcal{O}_L$ sont transmises à $n\mathcal{O}_K$.

Remarque 1.1. Si n est premier, il peut très bien être de Carmichael dans un anneau d'entiers, mais ne le sera jamais dans l'anneau $\mathbb{Z}$, car un nombre de Carmichael est composé. Nous pouvons donc supposer n composé.

Se convainquant rapidement que les hypothèses demandées sont trop fortes pour être transmises, nous décidons d'écrire un algorithme naïf pour chercher ledit contre-exemple dans des corps quadratiques. L'idée est simple : passer en revue une liste d'entiers d sans facteur carré qui engendrent ces corps et pour chaque tel d, tester parmi une liste arbitraire d'entiers naturels, lesquels engendrent un idéal de Carmichael sans être un nombre de Carmichael.

Il est facile avec un outil de calcul formel de déterminer si un entier n est de Carmichael dans un corps quadratique $\mathbb{Q}(\sqrt{d})$, d étant sans facteurs carrés. Posons $K = \mathbb{Q}(\sqrt{d})$ et $I = \mathcal{O}_K$. Le logiciel SageMath [5] est capable de donner la décomposition de I en produit d'idéaux premiers de $\mathcal{O}_K$ et calculer des normes d'idéaux. Pour tester si I est de Carmichael, on demande à SageMath sa décomposition, on regarde s'il est sans facteurs carrés et si c'est le cas on teste si $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{p}) - 1$ divise $\mathrm{N}_{K/\mathbb{Q}}(I) - 1$ pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant I. Comme l'extension considérée est quadratique, I a au plus deux facteurs premiers. La norme $\mathrm{N}_{K/\mathbb{Q}}(I)$ est quant à elle donnée par n^2.

Il reste à déterminer si n est un entier de Carmichael. Comme nous n'allons pas chercher bien loin [6] — plutôt que d'effectuer des calculs couteux et inutiles avec le critère de Korselt — il est préférable de regarder si n est dans la (maigre) liste des entiers de Carmichael inférieurs à 10000 :

$$\{561, 1105, 1729, 2465, 2821, 6601, 8911\}.$$

Pour l'implémentation, nous écrivons séparément une fonction testant si I est de Carmichael et l'invoquons pour tout couple (d, n). L'algorithme est donc le suivant ; son

5. Voir `https://www.sagemath.org` et plus particulièrement `http://doc.sagemath.org/html/en/reference/number_fields/sage/rings/number_field/number_field.html`.

6. Nous nous sommes limités à $d \in [\![-100, 100]\!]$ et $n \in [\![2, 10000]\!]$.

implémentation est disponible sur le compte GitHub de l'auteur (`https://github.com/kryzar/TER-Carmichael/blob/master/Script/Script.sage`).

Entrées : a, b, c
pour chaque $d \in [\![a, b]\!]$ *et d est sans facteur carré* **faire**
  $K = \mathbb{Q}(\sqrt{d})$;
  pour chaque $n \in [\![2, c]\!]$ **faire**
    si *n n'est pas de Carmichael* **et** $n\mathcal{O}_K$ *est un idéal de Carmichael* **alors**
      exporter (d, n) dans un fichier texte ;
    fin
  fin
fin

Nous avons pu exhiber de nombreux contre-exemples, comme le couple

$$(d, n) = (11, 35).$$

L'entier 35 n'est pas de Carmichael, mais il engendre un idéal de Carmichael dans $\mathbb{Q}(\sqrt{11})$. Le couple

$$(d, n) = (95, 8029)$$

est un autre contre-exemple, avec la particularité que $8029 = 7 \cdot 31 \cdot 37$ est le produit de trois nombres premiers (on rappelle qu'un nombre de Carmichael a au moins trois facteurs premiers). De même, 8029 n'est pas un entier de Carmichael, mais il engendre un idéal de Carmichael dans $\mathbb{Q}(\sqrt{95})$.

Références

[1] G. Ander Seele. « Carmichael numbers in number rings ». In : *Journal of Number Theory* 128 (2008), p. 910-917. URL : `https://core.ac.uk/download/pdf/82709152.pdf`.

[2] Michel Demazure. *Cours d'algèbre*. 2e éd. Cassini, 2008.

[3] Alain Kraus. *Corps locaux et applications. Cours accéléré de DEA, Université Pierre et Marie Curie*. Sept. 2000.

[4] Pierre Samuel. *Théorie algébrique des nombres*. 2e éd. Hermann Paris, oct. 1971.

Todo

— ajouter des titres aux algorithmes
— label les énoncés de l'introduction avec des lettres et non des 0.x
— numéro de page de titre
— refaire annexe
— dissocier composé / pas composé dans les critères de Korselt
— conclusion