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

$$\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{I} \tag{1}$$

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 **??** 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].

$$\left\{\begin{array}{c} 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, \\ 15841, 29341, 41041, 46657, 52633, 62745, 63973, \\ 75361, 101101, 115921, 126217, 162401, 172081, \\ 188461, 252601, 278545, 294409, 314821, 334153, \\ 340561, 399001, 410041, 449065, 488881, 512461 \end{array}\right\} \tag{2}$$

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

1 Délices de la théorie

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. □

Nous étendons alors la notion de témoin de Fermat.

Définition 1.2. Soient K un corps de nombres galoisien, I un idéal de $\mathcal{O}_K$ et $\alpha \in \mathcal{O}_K$ un entier algébrique. On dit que α est un K-témoin de Fermat pour I si l'on a

$$\alpha^{\mathrm{N}(I)} \not\equiv \alpha \pmod{n\mathcal{O}_K}.$$

Étant donnés n un entier et K un corps de nombres, nous appellerons K-témoin de Fermat pour n tout K-témoin de Fermat pour l'idéal $n\mathcal{O}_K$. Un nombre premier n'a donc de témoins de Fermat dans aucun corps de nombres Galoisien et un idéal de Carmichael est un idéal n'ayant aucun témoin de Fermat dans l'anneau d'entiers dans lequel il vit. La réciproque du théorème 1.1 s'énonce alors ainsi.

Théorème 1.3. *Soient n un entier et K un corps de nombres galoisien. Si n admet un K-témoin de Fermat, alors n est composé.*

le critère de korselt 0.1 si utile pour l'étude des nombres de carmichael dans $\mathbb{Q}$ trouve une généralisation dans ce nouveau cadre.

Théorème 1.4 (critère de Korselt généralisé, 2.2 dans l'article)**.** *Soient K un corps de nombres et I un idéal (premier ou composé) de $\mathcal{O}_K$. Alors I n'a aucun K-témoin de Fermat 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 $K = \mathbb{Q}$.

On a alors la caractérisation suivante.

Corollaire 1.6. *Soient K un corps de nombres et I un idéal de $\mathcal{O}_K$. Alors I est de Carmichael si, et seulement si, I est composé et I vérifie les hypothèses du critère de Korselt.*

Remarque 1.7. Il faut ici se montrer vigilant avec la nomenclature. Pour montrer qu'un idéal est de Carmichael, montrer qu'il vérifie le critère de Korselt ne suffit pas. Il faut aussi montrer qu'il est composé. Dans la littérature, on dit en général qu'un idéal vérifie le critère de Korselt s'il vérifie les hypothèses du théorème 1.4 et en plus qu'il est composé.

Fait tout à fait remarquable, l'auteur de l'article donne une réciproque au petit théorème de Fermat généralisé 1.1.

Théorème 1.8 (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 $n \nmid \mathrm{Disc}(K)$ dans lequel n admet un K-témoin de Fermat.*

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 1.9 (petit théorème de Fermat généralisé et sa réciproque)**.** *Soit $n > 2$ un entier. Alors n est premier si, et seulement si, il n'a de K-témoin de Fermat dans aucun corps quadratique K vérifiant $n \nmid \mathrm{Disc}(K)$.*

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.

Nous avons déjà des outils suffisamment robustes pour fournir un test de primalité naïf. Comme certains outils de calcul formel sont capables de décomposer un idéal de l'anneau d'entiers d'un corps de nombres en produit d'idéaux premiers dudit anneau [2], il est facile d'implémenter le critère de Korselt. Le petit théorème de Fermat généralisé 1.1 nous permet donc d'écrire le critère de composition suivant, basé sur le critère de Korselt.

Algorithme 1 : Critère de composition de Korselt dans les corps de nombres galoisiens

Entrées : n (entier à tester)
$\mathscr{L}$ (liste de corps de nombres galoisiens)

```
pour chaque K dans 𝓛 faire
    si n et Disc(K) sont premiers entre eux alors
        si nO_K ne vérifie pas le critère de Korselt alors
            retourner nO_K n'est pas de Carmichael et n est composé
            arrêter le programme.
```

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

Lemme 1.10. *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. C'est le cas par exemple de SageMath et PariGP **mettre liens**. L'auteur de ce texte a choisi d'utiliser Sage et s'en servira beaucoup par la suite.

2 Corps quadratiques

2.1 Théorie

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 [3] 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.

Bien que cet énoncé ne semble pas optimal en pratique [4], certains nombres de Carmichael vérifient ces hypothèses. On vérifie numériquement que c'est même le cas de tous les nombres de Carmichael de la liste 2 ! On peut par exemple prendre l'entier de Carmichael 512461 de son facteur premier 271 : il existe ainsi une infinité de corps quadratiques dans lequel 512461 n'est pas de Carmichael.

Dans l'exemple 2.6 de l'article, l'auteur ouvre une voix intéressante : celle du test de Fermat dans les corps quadratiques. Il montre que $n = 561$ est composé en exhibant le corps quadratique $K = Q(\sqrt{13})$ puis le K-témoin de Fermat $\alpha = 2+1\cdot\left(\frac{1+\sqrt{13}}{2}\right) \in \mathcal{O}_K$, ce qui prouve la composition de n d'après le théorème 1.3. Bien qu'il ne donne pas les détails,

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

4. 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**.

cela laisse penser que plutôt que d'utiliser le critère de Korselt [5], ce dernier a directement cherché un entier algébrique α ne vérifiant pas la congruence 1. Cet algorithme est appelé *test de Fermat dans les corps quadratiques* et est un critère de composition. Étant donné un entier n dont on veut prouver la composition, une version simple du test est la suivante.

Algorithme 2 : Test de Fermat dans un corps quadratique

Entrées : n (entier à tester)
K (corps quadratique)
S_α (ensemble coordonnées α)

```
si n et Disc(K) sont premiers entre eux alors
    θ ← un générateur de O_K
    pour chaque α = x + yθ, x, y ∈ S_α faire
        si α^{n²} ≢ α (mod nO_K) alors
            retourner n n'est pas de Carmichael dans K et est composé
            arrêter le programme
```

Nous discutons plus en détails de cet algorithme dans la section suivante. Il peut enfin être tentant d'utiliser cet algorithme pour déterminer la primalité de n *avec une certitude morale*, dans l'esprit test de primalité de Rabin-Miller (voir [2], §3.3.7, p. 68). 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. Nous allons cependant voir qu'un tel test ne saurait exister.

Nous avons évoqué la réciproque du petit théorème de Fermat (1.9). Il faut bien faire attention au fait que l'on ne peut pas remplacer l'hypothèse « $n \nmid \mathrm{Disc}(K)$ » par l'hypothèse « n et $\mathrm{Disc}(K)$ sont premiers entre eux » [6] ! Le mathématicien E.W. Howe montre en effet le résultat suivant.

Théorème 2.2 (Howe, 2000)**.** *Il existe un entier h qui soit à la fois* composé *et de Carmichael dans tout corps quadratique de discriminant premier avec h.*

En guise de preuve, Howe exhibe un tel nombre, l'entier

$$h = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331 = 443372888629441. \tag{3}$$

Nous l'appellerons dans la suite *entier de Howe*. L'existence de cet entier signifie que — comme dans $\mathbb{Q}$ — le test de Fermat **??** ne peut pas prouver qu'un entier est composé

5. Ce qui nécessiterait de décomposer l'idéal $561\mathcal{O}_{\mathbb{Q}(\sqrt{13})}$.

6. Cela peut être contre intuitif : si n est un entier et K un corps de nombres, le fait que n soit de Carmichael dans K implique que n et $\mathrm{Disc}(K)$ sont premiers entre eux.

simplement parce qu'il n'a pas de témoins de Fermat. Plus généralement, l'auteur de l'article montre le théorème 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.*

L'entier de Howe 3 est donc un nombre de Carmichael rigide d'ordre 2. Ces troublants résultats nous enseignent que les corps quadratiques ne peuvent pas fournir un test de Fermat fiable.

2.2 Simulation

2.2.1 Test de Fermat

Testons ici le test de Fermat dans les corps quadratiques, plus précisément, l'algorithme 2, que l'auteur du présent mémoire a implémenté. Nous le testons pour chaque entier de Carmichael de la liste 2 et choisissons [7] le corps quadratique

$$K = \mathbb{Q}(\sqrt{43})$$

et l'ensemble de coordonnées

$$S_\alpha = [\![-2, +2]\!].$$

Résumons ici les résultats obtenus.

- L'algorithme fournit des K-témoins de Fermat pour 561, 2465, 2821, 8911, 10585, 15841, 29341, 46657, 52633 et 62745.
- L'algorithme ne fournit aucun K-témoin de Fermat pour 1729, 6601 et 41041.
- Dès lors que l'algorithme a trouvé un K-témoin de Fermat pour un certain entier, il en a trouvé plusieurs. Pour l'entier $n = 10585$, l'algorithme fournit par exemple

  $$(-2,-2),\ (-2,-1),\ (-2,1),\ (-1,-1),\ (-1,1),\ (1,1),$$

  où ces éléments sont donnés par leurs coordonnées dans la base canonique $(1, \sqrt{43})$ de $\mathcal{O}_K$. Attention, $(1, 2)$ n'est pas un K-témoin de Fermat pour n.

7. L'entier 43 est le premier nombre premier qui ne soit facteur d'aucun des éléments de la liste 2. Cela assure que chaque entier de ladite liste est premier avec le discriminant de $\mathbb{Q}(\sqrt{43})$.

En choisissant [8] cette désormais le corps

$$K = \mathbb{Q}(\sqrt{-7})$$

, l'algorithme fournit des K-témoins de Fermat pour 6601 (qui n'en avait pas pour $\mathbb{Q}(\sqrt{43})$ mais pas pour 2425 (qui en avait plusieurs pour $\mathbb{Q}(\sqrt{43})$.

L'algorithme souffre néanmoins d'un gros problème de performances. Si les calculs prennent une fraction de secondes pour les premiers entiers, il faut 5 min à l'algorithme pour terminer sur l'entier 15841, 42 min pour 41041 puis 2 h 48 pour 62745, avant de planter pour les entiers suivants. Cela s'explique par les calculs de puissances. Si $\alpha \in \mathcal{O}_K$ est un K-témoin de Fermat potentiel, il faut calculer α^{n^2}. Lorsque n devient grand, le coût de calcul devient prohibitif, dépassant largement les capacités d'un ordinateur personnel standard. Si l'on pose $n = 10848$ et $\alpha = 1 + 1 \cdot \sqrt{43}$, les coordonnées de α^{n^2} sont tout de même des nombres à plusieurs milliers de chiffres. Cet algorithme est donc inutilisable en l'état pour tester la primalité de grands nombres. Si l'on ajoute à cela le fait qu'il n'est pas capable de détecter tous les entiers composés — comme l'entier de Howe — (voir section précédente), son usage semble définitivement à proscrire.

2.2.2 Critère de Korselt

Toujours dans l'objectif de numériquement prouver que les entiers de la liste 2 sont effectivement composés, nous employons cette fois le critère de composition de Korselt dans des corps quadratiques. Pour tout entier n, nous cherchons une liste de corps quadratiques dans lesquels n n'est pas de Carmichael. Pour cela, nous lançons l'algorithme avec les paramètres suivant.

corps testés	corps quadratiques de la forme $\mathbb{Q}(\sqrt{d})$ où d est un entier sans facteur carré dans $[\![-5000, +5000]\!]$ [9]
entiers de Carmichael testés	tous ceux de la liste 2 %

FIGURE 1 – Paramètres des simulations du critère de Korselt pour les corps quadratiques.

Pour ces paramètres, le critère de Korselt est capable de donner pour tout élément n de la liste, plusieurs corps quadratiques de discriminant premier avec n dans lesquels n n'est pas de Carmichael. En fait, il en exhibe des centaines. Il est donc impossible d'énoncer ici tous les résultats, mais citons à titre d'exemple que 561 n'est pas de Carmichael dans $\mathbb{Q}(\sqrt{-4874})$ mais qu'il l'est dans $\mathbb{Q}(\sqrt{4877})$ ou que 172081 n'est pas de Carmichael dans $\mathbb{Q}(\sqrt{766})$ mais qu'il l'est dans $\mathbb{Q}(\sqrt{-1459})$. En fait, pour la plupart des

8. Arbitrairement.

couples (n, K) testés, n n'est pas de Carmichael dans K. Nous avons tiré les statistiques suivantes de nos simulations.

nombre de corps testés	143524
nombre d'idéaux de Carmichael trouvés dans ces corps	34138
proportion d'idéaux de Carmichael trouvés dans ces corps	0,23786 %

FIGURE 2 – Statistiques des simulations du critère de Korselt sur les corps quadratiques pour les paramètres 2.2.2.

Si l'on cherche donc à s'assurer de la composition d'un entier n pour lequel il existe au moins un corps quadratique de discriminant premier avec n dans lequel n n'est pas de Carmichael, ces résultats semblent indiquer qu'on a de bonnes chances d'en trouver un rapidement. Bien sûr, ces sommaires statistiques ne prouvent rien et on ne sait pas déterminer a priori s'il existe un tel corps quadratique.

Quant aux performances, les calculs sont extrêmement rapides dans tous les corps et semblent homogènes. On a par exemple les données suivantes.

corps cyclotomique	temps de calcul
$\mathbb{Q}(\sqrt{-4957})$	0.00303 s
$\mathbb{Q}(\sqrt{-2426})$	0.00211 s
$\mathbb{Q}(\sqrt{-2})$	0.0024 s
$\mathbb{Q}(\sqrt{+2})$	0.0024 s
$\mathbb{Q}(\sqrt{+2426})$	0.0031 s
$\mathbb{Q}(\sqrt{+4957})$	0.0031 s

FIGURE 3 – Temps de calcul du critère Korselt dans les corps quadratiques donnés pour l'entier $n = 512461$.

3 Corps cyclotomiques

3.1 Théorie

Dans cette section, nous nous intéressons aux corps cyclotomiques de la forme $\mathbb{Q}(\zeta_q)$, q étant un nombre 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 *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 et l'auteur y 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. Pour ce théorème, la construction des corps se fait avec la correspondance de Galois et la vérification et la vérification qu'ils vérifient les bonnes propriétés nécessite 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 (n°3.3 chez nous).

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, n n'admet aucun K-témoin de Fermat.*

Le résultat le plus à même d'aboutir à un test de primalité est le crucial théorème suivant. Il nous enseigne qu'il faut aller chercher du côté des corps cyclotomiques. Nous en donnons la démonstration.

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.

Démonstration. **placeholder** □

Un nombre de Carmichael ayant toujours au moins trois diviseurs premiers distincts (voir [2], Proposition 3.35, p. 90), il vérifiera toujours les hypothèses du théorème. Ce résultat est donc en théorie bien plus puissant que le théorème 2.1 (2.5 dans l'article),

puisque nous avons vu que le test de primalité naïf qui en découlait ne détectait pas tous les entiers de Carmichael, comme par exemple l'entier de Howe 3. Nous avons par ailleurs le corollaire suivant, qui montre lui aussi la supériorité des corps cyclotomiques pour détecter des corps dans lesquels un entier de Carmichael n'est pas de Carmichael.

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.*

Démonstration. Distinguons trois cas.

- Si n a un unique facteur premier, étant composé, il a un facteur carré et ne sera jamais de Carmichael, d'après le critère de Korselt généralisé 1.4.
- Si n a deux uniques facteurs premiers distincts, il n'est pas de Carmichael dans $\mathbb{Q}$, le corps cyclotomique $\mathbb{Q}(\zeta_2)$ (voir [2], Proposition 3.35, p. 90).
- Si n a au moins trois facteurs premiers distincts, nous appliquons le théorème précédent.

□

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, n n'admet aucun K-témoin de Fermat.*

Remarque 3.6. Dans les deux réciproques que nous venons de donner, l'hypothèse sur le discriminants est que n et K doivent être premiers entre eux. C'est une hypothèse bien plus forte que de demander à ce que n ne divise pas le discriminant de K comme dans les corps quadratiques (1.9). Cela permet de tester beaucoup moins de corps.

Passons désormais aux simulations numériques.

3.2 Simulation

3.2.1 Test de Fermat

Revenons au théorème 3.3, duquel nous voulons tirer un critère de primalité. Étant donné un entier de Carmichael n, la version « cyclotomique » du test de Fermat serait la suivante.

Algorithme 3 : Test de Fermat dans un corps cyclotomique

Entrées : n (entier à tester)
K (corps cyclotomique de la forme $\mathbb{Q}(\zeta)$)
S_α (ensemble coordonnées α)

si n *et* $\mathrm{Disc}(K)$ *sont premiers entre eux* **alors**
  pour chaque $\alpha = x_0 + x_1\zeta + \cdots + x_{p-1}\zeta^{p-1}$, $x_0, \ldots, x_{p-1} \in S_\alpha$ **faire**
    si $\alpha^{n^2} \not\equiv \alpha \pmod{n\mathcal{O}_K}$ **alors**
      retourner n *n'est pas de Carmichael dans* $\mathbb{Q}(\sqrt{d})$ *et est composé*
      arrêter le programme

L'auteur du présent texte a — comme pour les corps quadratiques — implémenté et testé cet algorithme. Force est de constater que cet algorithme s'est montré extrêmement lent et semble inutilisable. En posant $n = 561$, $K = \mathbb{Q}(\zeta_5)$ et $S_\alpha = \{-1, 0, +1\}$, l'algorithme n'a toujours pas terminé après avoir tourné pendant une heure sur l'ordinateur personnel de l'auteur. Ce n'est finalement pas si étonnant. On aura

$$\mathrm{N}(n\mathcal{O}_K) = 561^4 = 99049307841$$

et si l'on prend par exemple l'entier algébrique de coordonnées $(1, 1, 0, 0)$

$$\alpha = 1 + \zeta,$$

l'ordinateur portable de l'auteur n'a toujours pas su calculer $alpha^{\mathrm{N}(n\mathcal{O}_K)}$ après trente minutes de calculs [10]. Les coordonnées ont pourtant été choisies pour être les plus petites possibles, mais le coût du calcul de $\alpha^{\mathrm{N}(n\mathcal{O}_K)}$ est prohibitif. Plus généralement, si n est un nombre dont on veut prouver la composition avec le test de Fermat cyclotomique et q un nombre premier, on a

$$\mathrm{N}(n\mathcal{O}_{\mathbb{Q}(\zeta_q)}) = n^{q-1},$$

un nombre qui sort rapidement des capacités d'un ordinateur personnel standard.

3.2.2 Critère de Korselt

Comme dans la section sur les corps quadratiques, nous cherchons ici — pour tout entier n de la liste 2 — un corps cyclotomique de la forme $\mathbb{Q}(\zeta_q)$, q étant premier, dans lequel il n'est pas de Carmichael. Nous reprenons donc l'algorithme 2.2.2 et l'utilisons avec les paramètres suivants.

Pour ces paramètres, le critère de Korselt est capable de donner pour tout élément n de la liste, plusieurs corps cyclotomiques de discriminant premier avec n dans lesquels n n'est pas de Carmichael. Voici les résultats pour l'entier $n = 561$.

10. Wolfram alpha n'a pas fait mieux.

corps testés	corps cyclotomiques de la forme $\mathbb{Q}(\zeta_q)$ où q est un nombre premier dans $[\![3, 300]\!]$ [11]
entiers de Carmichael testés	tous ceux de la liste 2 %

FIGURE 4 – Paramètres des simulations du critère de Korselt pour les corps cyclotomiques.

Fichier 561_cyclotomic.txt

```
561 is Carmichael in Q(zeta5): False, 561 and 5 are coprime
561 is Carmichael in Q(zeta7): False, 561 and 7 are coprime
561 is Carmichael in Q(zeta13): False, 561 and 13 are coprime
561 is Carmichael in Q(zeta19): False, 561 and 19 are coprime
561 is Carmichael in Q(zeta23): False, 561 and 23 are coprime
561 is Carmichael in Q(zeta29): False, 561 and 29 are coprime
561 is Carmichael in Q(zeta31): False, 561 and 31 are coprime
561 is Carmichael in Q(zeta37): False, 561 and 37 are coprime
561 is Carmichael in Q(zeta41): False, 561 and 41 are coprime
561 is Carmichael in Q(zeta43): False, 561 and 43 are coprime
561 is Carmichael in Q(zeta47): False, 561 and 47 are coprime
561 is Carmichael in Q(zeta53): False, 561 and 53 are coprime
561 is Carmichael in Q(zeta59): False, 561 and 59 are coprime
561 is Carmichael in Q(zeta61): False, 561 and 61 are coprime
561 is Carmichael in Q(zeta67): False, 561 and 67 are coprime
561 is Carmichael in Q(zeta71): False, 561 and 71 are coprime
561 is Carmichael in Q(zeta73): False, 561 and 73 are coprime
561 is Carmichael in Q(zeta79): False, 561 and 79 are coprime
561 is Carmichael in Q(zeta83): False, 561 and 83 are coprime
561 is Carmichael in Q(zeta89): False, 561 and 89 are coprime
561 is Carmichael in Q(zeta97): False, 561 and 97 are coprime
561 is Carmichael in Q(zeta101): False, 561 and 101 are coprime
561 is Carmichael in Q(zeta103): False, 561 and 103 are coprime
561 is Carmichael in Q(zeta107): False, 561 and 107 are coprime
561 is Carmichael in Q(zeta109): False, 561 and 109 are coprime
561 is Carmichael in Q(zeta113): False, 561 and 113 are coprime
561 is Carmichael in Q(zeta127): False, 561 and 127 are coprime
561 is Carmichael in Q(zeta131): False, 561 and 131 are coprime
561 is Carmichael in Q(zeta137): False, 561 and 137 are coprime
561 is Carmichael in Q(zeta139): False, 561 and 139 are coprime
561 is Carmichael in Q(zeta149): False, 561 and 149 are coprime
561 is Carmichael in Q(zeta151): False, 561 and 151 are coprime
561 is Carmichael in Q(zeta157): False, 561 and 157 are coprime
561 is Carmichael in Q(zeta163): False, 561 and 163 are coprime
561 is Carmichael in Q(zeta167): False, 561 and 167 are coprime
561 is Carmichael in Q(zeta173): False, 561 and 173 are coprime
561 is Carmichael in Q(zeta179): False, 561 and 179 are coprime
561 is Carmichael in Q(zeta181): False, 561 and 181 are coprime
```

```
561 is Carmichael in Q(zeta191): False, 561 and 191 are coprime
561 is Carmichael in Q(zeta193): False, 561 and 193 are coprime
561 is Carmichael in Q(zeta197): False, 561 and 197 are coprime
561 is Carmichael in Q(zeta199): False, 561 and 199 are coprime
561 is Carmichael in Q(zeta211): False, 561 and 211 are coprime
561 is Carmichael in Q(zeta223): False, 561 and 223 are coprime
561 is Carmichael in Q(zeta227): False, 561 and 227 are coprime
561 is Carmichael in Q(zeta229): False, 561 and 229 are coprime
561 is Carmichael in Q(zeta233): False, 561 and 233 are coprime
561 is Carmichael in Q(zeta239): False, 561 and 239 are coprime
561 is Carmichael in Q(zeta241): False, 561 and 241 are coprime
561 is Carmichael in Q(zeta251): False, 561 and 251 are coprime
561 is Carmichael in Q(zeta257): False, 561 and 257 are coprime
561 is Carmichael in Q(zeta263): False, 561 and 263 are coprime
561 is Carmichael in Q(zeta269): False, 561 and 269 are coprime
561 is Carmichael in Q(zeta271): False, 561 and 271 are coprime
561 is Carmichael in Q(zeta277): False, 561 and 277 are coprime
561 is Carmichael in Q(zeta281): False, 561 and 281 are coprime
561 is Carmichael in Q(zeta283): False, 561 and 283 are coprime
561 is Carmichael in Q(zeta293): False, 561 and 293 are coprime
```

Il n'y a qu'un seul corps cyclotomique pour lequel 561 reste de Carmchael : c'est $\mathbb{Q}(\zeta_3)$! Il n'est de Carmichael dans aucun autre corps testé. Le fichier présenté ici correspond au fichier `561_cyclotomic.txt`, disponible à **url**. Cet algorithme permet aussi de prouver que l'entier de Howe 3 est composé ! Nous trouvons qu'il est de Carmichael dans $\mathbb{Q}(\zeta_3)$ mais dans aucun autre corps testé [12] En fait, nous avons trouvé très peu de couples (n, K) où n est un entier de Carmichael de la liste et K un corps cyclotomique dans lequel n est de Carmichael. La liste exhaustive de tels couples est la suivante.

12. Nous sommes en réalité allés plus loin pour l'entier de Howe et avons testé tous les corps cyclotomiques de la forme $\mathbb{Q}(\zeta_q)$ où q est un nombre premier compris entre 3 et 600.

Find_Carmichael_in_Results_files_cyclotomic.txt

```
15841 is Carmichael in Q(zeta3): True, 15841 and 3 are coprime
46657 is Carmichael in Q(zeta3): True, 46657 and 3 are coprime
115921 is Carmichael in Q(zeta3): True, 115921 and 3 are coprime
294409 is Carmichael in Q(zeta3): True, 294409 and 3 are coprime
252601 is Carmichael in Q(zeta5): True, 252601 and 5 are coprime
63973 is Carmichael in Q(zeta3): True, 63973 and 3 are coprime
512461 is Carmichael in Q(zeta3): True, 512461 and 3 are coprime
512461 is Carmichael in Q(zeta5): True, 512461 and 5 are coprime
188461 is Carmichael in Q(zeta3): True, 188461 and 3 are coprime
172081 is Carmichael in Q(zeta3): True, 172081 and 3 are coprime
8911 is Carmichael in Q(zeta3): True, 8911 and 3 are coprime
1729 is Carmichael in Q(zeta3): True, 1729 and 3 are coprime
52633 is Carmichael in Q(zeta3): True, 52633 and 3 are coprime
29341 is Carmichael in Q(zeta3): True, 29341 and 3 are coprime
488881 is Carmichael in Q(zeta3): True, 488881 and 3 are coprime
443372888629441 is Carmichael in Q(zeta3): True, 443372888629441 and 3 are coprime
2821 is Carmichael in Q(zeta3): True, 2821 and 3 are coprime
126217 is Carmichael in Q(zeta3): True, 126217 and 3 are coprime
```

Voici les faits remarquables à retenir de ces simulations.

— Nous n'avons trouvé aucun corps cyclotomique parmi ceux testés dans lequel les entiers suivants sont de Carmichael : 561, 1105, 2465, 6601, 1085, 41041, 62745, 101101, 449065.

— Les autres entiers sont de Carmichael dans $\mathbb{Q}(\zeta_3)$ ou $\mathbb{Q}(\zeta_5)$, mais dans aucun autre corps testé.

— Les deux seuls entiers de Carmichael de la liste de Carmichael dans $\mathbb{Q}(\zeta_5)$ sont 252601 et 512461. Nous remarquons que leurs facteurs premiers sont congrus à 1 modulo 5 [13].

— L'entier 512461 est l'unique entier testé qui soit de Carmichael dans deux corps cyclotomiques à la fois.

— L'entier de Howe est de Carmichael dans $\mathbb{Q}(\zeta_3)$ mais dans aucun autre corps testé.

Donnons aussi quelques statistiques.

Quant aux performances, les calculs sont cependant significativement plus longs dans le cas des corps cyclotomiques que dans le cas des corps quadratiques.

Les temps de calcul pour l'entier de Howe sont sensiblement similaires.

13. **on a trouvé des Carmichael dont les facteurs premiers n'étaient pas 1 mod. 5.**

nombre de corps testés	1857
nombre d'idéaux de Carmichael trouvés dans ces corps	18
proportion d'idéaux de Carmichael trouvés dans ces corps	0,00969 %

FIGURE 5 – Statistiques des simulations du critère de Korselt sur les corps cyclotomiques pour les paramètres 3.2.2.

corps cyclotomique	temps de calcul
$\mathbb{Q}(\zeta_7)$	0.005 s
$\mathbb{Q}(\zeta_{101})$	1.626 s
$\mathbb{Q}(\zeta_{199})$	18.9 s
$\mathbb{Q}(\zeta_{293})$	38.4 s

FIGURE 6 – Temps de calcul du critère Korselt dans les corps cyclotomiques donnés pour l'entier $n = 512461$.

Conclusion

A De la simulation

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

— label les énoncés de l'introduction avec des lettres et non des 0.x
— refaire annexe
— conclusion
— "un regard à la fois théorique et pratique"
— dire plus ce que l'on fait dans l'intro et mettre l'accent sur l'implémentation
— temps calcul cyclo
— on ne sait pas si Korselt est efficace
— résultats mentionnés par A. Kraus par mail et dans les notes