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

Ayant pour point de départ l'article *Carmichael numbers in number rings* [Ste06] de G.A. Steele, ce mémoire s'applique à en redonner les résultats, les tester numériquement, répondre à quelques questions soulevées et essayer d'en tirer un critère de composition.

Le test de primalité non naïf le plus simple est le *test de primalité de Fermat*. Étant donné un entier rationnel n dont on veut tester la primalité, ce dernier affirme que s'il existe un entier rationnel a vérifiant $a^n \not\equiv a \pmod{n}$, alors n est composé. On dit alors que a est un *témoin de Fermat pour* n. Il existe cependant des entiers rationnels n **composés** n'ayant aucun témoin de Fermat. 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 **ref vers [1] de l'article**, que l'on peut caractériser ainsi.

Proposition I.1. *Soit n un entier rationnel. Les assertions suivantes sont équivalentes :*

(a) *l'entier n n'a aucun témoin de Fermat ;*

(b) *l'entier n est sans facteurs carrés et chacun de ses facteurs premiers p vérifie l'identité*
$$p - 1 \mid n - 1 \ .$$

(c) *l'identité*
$$\lambda(n) \mid n - 1$$
est vérifiée, la fonction λ étant l'indicatrice de Carmichael, définie comme la fonction $\mathbb{N}^* \to \mathbb{N}^*$ qui à tout entier n associe l'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

Un entier rationnel n est donc de Carmichael si, et seulement si, **il est composé** et vérifie l'une des assertions de I.1. 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 rationnel donné est de Carmichael. Le lecteur désireux d'une preuve de cette proposition pourra se référer à [Dem08] §3.3, p. 89. Dans l'article susnommé [Ste06], 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 I.2 ([Ste06] déf. 2.1)**.** Soient K un corps de nombres et I un idéal de $\mathcal{O}_K$. On dit que I est un idéal de Carmichael si I **est composé** et pour tout entier $\alpha \in \mathcal{O}_K$, la congruence
$$\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{I}$$
est vérifiée.

Remarque I.3. Un entier de Carmichael peut donc être vu comme un idéal de Carmichael du corps de nombres $\mathbb{Q}$.

Étant donnés n un entier rationnel et K un corps de nombres, nous dirons que n est de Carmichael dans K si l'idéal $n\mathcal{O}_K$ est de Carmichael dans $\mathcal{O}_K$. De tels idéaux existent et cette définition est le point de départ d'un formalisme fructueux. L'auteur de l'article commence par généraliser le critère de Korselt et le petit théorème de Fermat ; il en donne notamment une fameuse réciproque. Il étudie en suite les corps quadratiques, puis cyclotomiques, cadres dans lesquels il démontre plusieurs résultats d'existence et non-existence d'idéaux de Carmichael. De nombreuses questions sont soulevées par l'article, notamment la suivante.

Question I.4. Soient n un entier de Carmichael et K un corps de nombres. Dans quelle mesure n est-il de Carmichael dans K ?

Nous nous proposons de répondre à une partie de cette question au cours de ce mémoire, que nous abordons avec une vision aussi bien théorique que pratique. Au delà des résultats de l'article, l'auteur du présent texte a implémenté plusieurs algorithmes y étant suggérés, et en explique les résultats. Les preuves des énoncés fondamentaux de l'article sont redonnées (voire légèrement modifiées [1] dans ce mémoire. Nous ajoutons quelques corollaires et étendons la notion de *témoin de Fermat*. Enfin certaines preuves non redonnées sont quant à elle commentées dans des environnements dédiés 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 [2].

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

1. Nous ajoutons deux lemmes à la preuve du théorème 3.6 de l'article (4.3).
2. 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. Commençons par un lemme.

Lemme 1.1. *Soient K un corps de nombres, $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\alpha \in \mathcal{O}_K$ un entier. Alors la congruence*

$$\alpha^{\mathrm{N}(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}$$

est vérifiée.

Démonstration. Si $\alpha \equiv 0 \pmod{\mathfrak{p}}$, le résultat est évident. Si ce n'est pas le cas, l'idéal $\mathfrak{p}$ étant un idéal premier d'un anneau de Dedekind, il est maximal. Le quotient $\mathcal{O}_K/\mathfrak{p}$ est donc un corps et $\mathrm{N}(\mathfrak{p})-1$ est le cardinal du groupe des inversibles de $\mathcal{O}_K/\mathfrak{p}$. Le théorème de Lagrange implique donc $\alpha^{\mathrm{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$ puis

$$\alpha^{\mathrm{N}(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}$$

en multipliant par α des deux côtés. □

Nous pouvons dès à présent généraliser le critère de Korselt I.1.

Théorème 1.2 (critère de Korselt généralisé, [Ste06] th. 2.2)**.** *Soient K un corps de nombres et I un idéal (premier ou composé) de $\mathcal{O}_K$. Les assertions suivantes sont équivalentes :*

- *pour tout entier $\alpha \in \mathcal{O}_K$, la congruence*

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

  est vérifiée ;
- *l'idéal I est sans facteurs carrés et chacun de ses facteurs premier $\mathfrak{p}$ vérifie l'identité*

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

Démonstration. Commençons par le sens réciproque. Soit $\alpha \in \mathcal{O}_K$ un entier et $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ divisant I.

- Si $\alpha \notin \mathfrak{p}$, vient $\alpha^{\mathrm{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$ d'après le lemme 1.1. L'entier $\mathrm{N}(\mathfrak{p})-1$ divisant $\mathrm{N}(I)-1$ par hypothèse, cela entraîne $\alpha^{\mathrm{N}(I)-1} \equiv 1 \pmod{\mathfrak{p}}$ et donc

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

- Si $\alpha \in \mathfrak{p}$, la dernière congruence est toujours vérifiée.

L'idéal I étant de plus sans facteurs carrés (hypothèse), il est de la forme $I = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, où les $\mathfrak{p}_i$ sont des idéaux premiers distincts de $\mathcal{O}_K$. Ces idéaux sont même maximaux (anneau de Dedekind) et donc comaximaux. Le théorème chinois affirme alors que l'application canonique

$$\begin{array}{ccc} \mathcal{O}_K\big/I & \longrightarrow & \mathcal{O}_K\big/\mathfrak{p}_1 \times \cdots \times \mathcal{O}_K\big/\mathfrak{p}_r \\ a \pmod{I} & \longmapsto & (a \pmod{\mathfrak{p}_1}, \ldots, a \pmod{\mathfrak{p}_r}), \end{array}$$

est un isomorphisme d'anneaux. Comme nous avons montré $\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{\mathfrak{p}_i}$ pour tout $1 \leqslant i \leqslant r$, l'isomorphisme évoqué entraîne la congruence

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

Démontrons cette fois le sens direct. La preuve se fait en deux temps. 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

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

en reprenant le raisonnement précédent. D'après le théorème de Lagrange, l'ordre de α_i modulo $\mathfrak{p}_i$ divise $\mathrm{N}(I) - 1$. 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 $\mathfrak{p}^2 \mid I$ 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, on a $\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{I}$ puis $\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{\mathfrak{p}^2}$, car $\mathfrak{p}^2 \mid I$. Comme en outre $\alpha \notin \mathfrak{p}^2$, on en déduit $\alpha^{\mathrm{N}(I)-1} \equiv 1 \pmod{\mathfrak{p}^2}$ puis

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

d'après le théorème de Lagrange. Comme $p \mid \mathrm{N}(I)$, cela constitue une contradiction. L'idéal I est donc sans facteurs carrés. □

Remarque 1.3. 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 (fondamentale) caractérisation suivante.

Corollaire 1.4. *Soient K un corps de nombres et I un idéal de $\mathcal{O}_K$. Alors l'idéal I est de Carmichael si, et seulement si, il est composé et vérifie les hypothèses du critère de Korselt généralisé 1.2.*

Remarque 1.5. Il faut être vigilant avec la nomenclature. Pour établir qu'un idéal est de Carmichael, il faut montrer qu'il est composé, indépendamment du critère de Korselt.

Ce critère permet de généraliser le petit théorème de Fermat. Dans une extension galoisienne K de Q de degré fini, un nombre premier est soit inerte, soit de Carmichael dans K. Plus précisément.

Théorème 1.6 (petit théorème de Fermat généralisé, [Ste06] th. 2.2)**.** *Soient p un nombre premier et $K/\mathbb{Q}$ une extension galoisienne de degré fini tels que $p \nmid \mathrm{Disc}(K)$. Alors, pour tout entier $\alpha \in \mathcal{O}_K$, 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 de degré fini, 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 $rf = [K : \mathbb{Q}]$ 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 1.2, d'où le résultat. □

Nous étendons alors la notion de témoin de Fermat.

Définition 1.7. Soient n un entier rationnel, $K/\mathbb{Q}$ une extension galoisienne de degré fini et $\alpha \in \mathcal{O}_K$ un entier. On dit que α est un K-témoin de Fermat pour n si l'on a

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

Un nombre premier n'a donc de témoins de Fermat dans aucun corps de nombres galoisien et un idéal de Carmichael est un idéal **composé** n'ayant aucun témoin de Fermat dans l'anneau d'entiers dans lequel il vit. Cette généralisation de la notion de témoin de Fermat apparaît naturellement dans la contraposée du théorème 1.6. Fait tout à fait remarquable, l'auteur de l'article donne une réciproque au petit théorème de Fermat généralisé 1.6.

Théorème 1.8 (réciproque du petit théorème de Fermat généralisé, [Ste06] th. 2.4)**.** *Soit $n > 2$ un entier rationnel composé. Alors n admet un témoin de Fermat dans les corps quadratique de la forme*

$$K = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$$

où p est un facteur premier impair de n.

Démonstration. Soit K un corps quadratique comme dans l'énoncé. Le nombre premier p se ramifie dans K et $n\mathcal{O}_K$ a un facteur carré. Il n'est donc pas de Carmichael d'après le critère de Korselt généralisé 1.2 et la caractérisation 1.4. □

Vient alors l'équivalence suivante.

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

Démonstration. Le sens direct correspond à 1.6 et le sens réciproque s'obtient avec l'énoncé précédent en constatant que $\mathrm{Disc}(K) = p$ et $n \nmid p$. □

Remarque 1.10. Au delà de sa force théorique, cette énoncé semble porter une valeur historique notable. Le test de primalité de Fermat était le seul test de primalité classique 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 suffisent. 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 [3], il est facile d'implémenter le critère de Korselt 1.2. La contraposée du petit théorème de Fermat généralisé 1.9 nous permet en suite d'écrire le critère de composition suivant.

3. 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.

Algorithme 1 : Critère de composition de Korselt dans les extensions galoisiennes de degré fini de $\mathbb{Q}$

Entrées : n (entier rationnel à tester), $\mathscr{K}$ (liste d'extensions galoisiennes de degré fini de $\mathbb{Q}$)

```
pour chaque K dans 𝒦 faire
    si n ∤ Disc(K) 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 1.11. *Soient n un entier rationnel 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 les entiers n et $\mathrm{Disc}(K)$ ne sont pas premiers entre eux, n a un facteur premier qui divise $\mathrm{Disc}(K)$ et 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 1.2 et la caractérisation 1.4. □

Ces résultats fournissent un début de théorie confortable. Nous pouvons dès à présent nous confronter à une étude plus spécifique, celle des corps quadratiques.

2 Corps quadratiques

2.1 Théorie

Entrons dès à présent dans le vif du sujet.

Théorème 2.1 ([Ste06] th. 2.5)**.** *Soit n un entier rationnel impair sans facteurs carrés. S'il existe un diviseur premier p de n vérifiant*

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

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 1.2 et la caractérisation 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. La partie la plus difficile de la preuve consiste à trouver les bons corps quadratiques. Elle 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 : c'est même le cas de tous les nombres de Carmichael de la liste $\mathfrak{C}$. Il existe donc pour chacun d'eux une infinité de corps quadratiques dans lesquels ils ne sont pas de Carmichael, prouvant qu'ils sont composés (énoncé 1.9).

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 $K = \mathbb{Q}(\sqrt{13})$ puis le K-témoin de Fermat $\alpha = 2 + 1 \cdot \left(\frac{1+\sqrt{13}}{2}\right) \in \mathcal{O}_K$: c'est le test de Fermat dans les corps quadratiques. Cet algorithme est appelé *test de Fermat dans les corps quadratiques* et est un critère de composition. Étant donné un entier rationnel n dont on veut prouver la composition, une version simple du test est la suivante.

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

Algorithme 2 : Test de Fermat dans un corps quadratique

Entrées : n (entier rationnel à tester), K (corps quadratique), S_α (ensemble de coordonnées pour α)

si n *et* $\mathrm{Disc}(K)$ *sont premiers entre eux* **alors**
  $(1, \theta) \leftarrow$ une base intégrale de $\mathcal{O}_K$ [a]
  pour chaque $\alpha = x + y\theta$, $x, y \in S_\alpha$ **faire**
    si $\alpha^{n^2} \not\equiv \alpha \pmod{n\mathcal{O}_K}$ **alors**
      retourner n *n'est pas de Carmichael dans* K *et est composé*
      arrêter le programme

a. Dans les faits, si $K = \mathbb{Q}(\sqrt{d})$ où d est un entier rationnel sans facteurs carrés, θ vaudra $\sqrt{d}$ si $d \equiv 2$ ou $3 \pmod 4$, $\frac{1+\sqrt{d}}{2}$ sinon. Voir [Sam71] ch. 2 §5.

Nous discutons plus en détails de cet algorithme dans la section suivante.

Il par ailleurs tentant d'utiliser ce test pour déterminer la primalité de n *avec une certitude morale*, dans l'esprit du test de primalité de Rabin-Miller (voir [Dem08], §3.3.7, p. 68). L'idée serait que si n vérifie la congruence $\alpha^{\mathrm{N}(n\mathcal{O}_K)} \equiv \alpha \pmod{n\mathcal{O}_K}$ pour un nombre « suffisamment grand » de corps quadratiques $K = \mathbb{Q}(\sqrt{d})$ de discriminant premier avec n et d'entiers $\alpha \in \mathcal{O}_K$, 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 » [5] ! Le mathématicien E.W. Howe montre en effet le résultat suivant.

Théorème 2.2 (Howe, 2000)**.** *Il existe un entier rationnel 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, défini par

$$h = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331 = 443372888629441. \tag{1}$$

Nous l'appellerons dans la suite *entier de Howe*. Il est même de Carmichael dans $\mathbb{Q}$. L'existence de cet entier rationnel signifie que — comme dans $\mathbb{Q}$ — le test de Fermat 3 ne peut pas prouver qu'un entier rationnel est composé simplement parce qu'il n'a de K-témoins de Fermat dans aucun corps quadratique K dont le discriminant lui est premier. Plus généralement, l'auteur de l'article montre le théorème suivant.

5. Cela peut être contre intuitif : si n est un entier rationnel 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.

Théorème 2.3 ([Ste06] th. 2.7)**.** *Soient n un entier rationnel composé sans facteurs carrés et $d \geqslant 1$ un entier rationnel. 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 tout corps de nombres de degré d de discriminant premier avec n.

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

L'entier de Howe est donc un nombre de Carmichael rigide d'ordre 2. Ces résultats nous enseignent que les corps quadratiques — à l'instar de $\mathbb{Q}$ — ne peuvent pas détecter tous les entiers de Carmichael à l'aide avec le test de Fermat. Terminons avec un énoncé proche de l'arithmétique classique.

Corollaire 2.5. *Soit n un entier rationnel. Si n est sans facteurs carrés et composé, alors les propositions suivantes sont équivalentes :*

- *l'entier n est de Carmichael dans tout corps quadratique de discriminant premier avec n ;*
- *l'identité*

  $$p^2 - 1 \mid n^2 - 1$$

  est vérifiée pour tout diviseur premier p de n.

Démonstration. Si n est de Carmichael dans tout corps quadratique de discriminant premier avec n, le théorème 2.1 assure que l'identité

$$p^2 - 1 \mid n^2 - 1$$

est vérifiée pour tout diviseur premier p de n. Pour le sens réciproque, soit p un facteur premier de n. On a $p - 1 \mid (p-1)(p+1) = p^2 - 1$ et $p^2 - 1 \mid n^2 - 1$ par hypothèse. La division

$$p^i - 1 \mid n^2 - 1$$

est donc vérifiée pour toute puissance $1 \leqslant i \leqslant 2$. Le théorème 2.3 permet alors de conclure. □

Remarque 2.6. L'énoncé est faux si n n'est pas composé. Sous cette hypothèse, notons $p = n$. Soit K un corps quadratique dans lequel p est inerte. Un idéal de Carmichael étant composé, p n'est pas de Carmichael dans K. L'identité $p^2 - 1 | n^2 - 1 = p^2 - 1$ est cependant vérifiée.

Passons désormais aux simulations numériques.

2.2 Simulations

2.2.1 Test de Fermat

Nous étudions ici le test de Fermat dans les corps quadratiques, plus précisément, l'algorithme 3, implémenté par l'auteur de ce mémoire. Nous le testons pour chaque entier de Carmichael de la liste $\mathfrak{C}$ et choisissons [6] pour paramètres de simulation 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 rationnel, il en a trouvé plusieurs. Pour 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 10585.

Changeons de corps quadratique. En choisissant [7] 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 **trouver mieux** pour les entiers suivants. Cela s'explique par les calculs intermédiaires 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 des nombres à plusieurs milliers de chiffres.

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

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 rationnels composés — comme l'entier de Howe — (voir section précédente), son usage semble définitivement à proscrire.

2.2.2 Critère de Korselt

Nous étudions ici le critère de composition de Korselt dans des corps quadratiques. Pour tout entier rationnel 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 suivants.

paramètre	valeur
corps testés	corps quadratiques de la forme $\mathbb{Q}(\sqrt{d})$ où d est un entier rationnel sans facteurs carrés dans $[\![-5000, +5000]\!]$ [8]
entiers de Carmichael testés	tous ceux de la liste $\mathfrak{C}$

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

Avec ces paramètres, le critère de Korselt a donné pour chaque 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 $\mathbb{Q}(\sqrt{-1459})$. Pour la plupart des couples (n, K) testés, n n'est pas de Carmichael dans K. Nous avons tiré les statistiques suivantes de nos simulations.

donnée évaluée	statistique
nombre de corps testés	143524
nombre d'idéaux de Carmichael trouvés dans ces corps	34138
proportion d'idéaux de Carmichael trouvés dans ces corps	23,8 %

TABLE 2 – Statistiques des simulations du critère de Korselt sur les corps quadratiques pour les paramètres 2.2.2 **renvoyer vers le bon truc**.

S'il s'avère que l'entier rationnel n que nous testons n'est pas comme l'entier de Howe et admet bien un K-témoin de Fermat dans un certains corps quadratique K dont le

discriminant lui est premier, ces résultats laissent penser qu'on a de bonnes chances de le trouver. Bien sûr, ces sommaires statistiques ne prouvent rien et on ne sait pas déterminer a priori s'il existe ou non un tel témoin. Pour les performances, les calculs sont extrêmement rapides dans tous les corps. D'après nos tests, ils sont sensiblement proches pour tout entier rationnel et tout corps quadratique testé.

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

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

3 Interlude : idéaux de Carmichael et extensions de corps

Donnons nous

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

une tour de corps de nombres, $I \subset \mathcal{O}_K$ un idéal de Carmichael de K et $J \subset \mathcal{O}_L$ un idéal de Carmichael de L.

Question 3.1. 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 ?

L'auteur de l'article a déjà répondu à la première partie de la question dans l'exemple 2.6 de l'article, en utilisant le test de Fermat dans les corps quadratiques.

Proposition 3.2. *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.*

Démonstration. L'exemple 2.6 de l'article montre que l'entier de Carmichael 561 n'est pas de Carmichael dans $\mathbb{Q}(\sqrt{13})$. On a alors l'énoncé en prenant $K = \mathbb{Q}$, $I = 561\mathcal{O}_K$ et $L = \mathbb{Q}(\sqrt{13})$. □

L'algorithme de Korselt 2.2.2 dans les corps quadratiques permet de répondre à la deuxième partie de la question.

Proposition 3.3. *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.*

Pour y répondre, l'auteur du présent mémoire a implémenté l'algorithme Suivant.

Algorithme 3 : trouver un entier rationnel n et un corps quadratique K tels que n ne soit pas de Carmichael dans K

Entrées : $\mathscr{N}$ (liste d'entiers qui ne sont *pas* de Carmichael), $\mathscr{K}$ (liste de corps quadratiques)
Sorties : couples (n, K) où K est un corps quadratique de $\mathscr{K}$ et n est est un entier rationnel de $\mathscr{N}$ de Carmichael dans K mais pas dans $\mathbb{Q}$

```
1 pour chaque n dans 𝒩 faire
2     pour chaque K dans 𝒦 faire
3         si n est de Carmichael dans K (critère de Korselt) alors
4             retourner n n'est pas de Carmichael mais nO_K l'est
5             arrêter le programme
```

Cette algorithme retourne de nombreux résultats. Par exemple 35 est de Carmichael dans $\mathbb{Q}(\sqrt{11})$ et 8029 est de Carmichael dans $\mathbb{Q}(\sqrt{-73})$; aucun de ces deux nombres n'est de Carmichael dans $\mathbb{Q}$. **lien vers résultats complets** Nous avons tiré les statistiques suivantes.

donnée évaluée	statistique
nombre de couples testés	5723
nombre d'entiers rationnels qui sont de Carmichael dans un corps testé	2930
proportion d'entiers rationnels qui sont de Carmichael dans un corps testé	51,2 %

TABLE 4 – Statistiques des simulations du critère de Korselt sur les corps quadratiques pour les paramètres 2.2.2.

Remarque 3.4. L'entier $n = 8029$ a la particularité d'être le produit de trois nombres premiers distincts :

$$n = 8029 = 7 \cdot 31 \cdot 37.$$

Le fait qu'il existe un corps quadratique dans lequel n n'est pas de Carmichael peut se traduire dans le cadre de l'arithmétique classique grâce au critère de Korselt : existe-t-il un tripler de nombres premiers distincts p, q et r pour lesquels

$$(pqr)^2 - 1$$

est divisible à la fois par $p-1$, $q-1$ et $r-1$? Les diviseurs premiers de 8029 sont un tel triplet.

Face à la généralité de l'énoncé de la question posée, il était tentant d'aller chercher une réponse ou bien théorique, ou bien dans des corps de nombres beaucoup plus compliqués. En fin de compte, les corps quadratiques auront suffit. Nous avons vu à la section précédente que sur les entiers de Carmichael et les corps quadratiques testés, ceux-ci restaient de Carmichael dans environ 24 % des cas. Ici, nous avons montré que sur les entiers n'étant pas de Carmichael et les corps quadratiques testés, ceux-ci engendraient un entier de Carmichael dans plus de 50 % des cas. Ces statistiques sont symptomatiques du fait que nous sommes a priori largement ignorants sur le comportement d'un idéal de Carmichael lorsqu'on l'étend ou le restreint, et ce même en restant dans le cadre des corps quadratiques, corps de nombres a priori parmi les moins compliqués.

4 Corps cyclotomiques

4.1 Théorie

Dans cette section, nous nous intéressons aux corps cyclotomiques de la forme $\mathbb{Q}(\zeta_q)$ où q est un nombre premier. Commençons par un résultat théorique.

Théorème 4.1 ([Ste06] th. 3.1)**.** *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 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°4.3 chez nous).

Un nombre de Carmichael étant composé, il vérifie les hypothèses du théorème 4.1. Cela fournit une nouvelle réciproque au petit théorème de Fermat, plus contraignante que la précédente.

Théorème 4.2 (deuxième réciproque)**.** *Soit n un entier rationnel. Alors n est premier si, et seulement si, pour tout corps de nombres* abéliens *K de discriminant premier avec n, n n'admet aucun K-témoin de Fermat.*

Démonstration. Supposons que n est premier. Dans ce cas, d'après le théorème 1.6 et la définition 1.7, de K-témoin de Fermat dans aucun corps de nombres abélien K de discriminant premier avec n. L'application réciproque résulte directement du théorème 4.1. □

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 4.3 ([Ste06] th. 3.6)**.** *Soit n un entier rationnel 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*.*

Nous avons de quelques résultats préliminaires.

Lemme 4.4 ([Ste06] lemme 3.3)**.** *Soit n un entier rationnel. Si n n'est pas la puissance d'un nombre premier, alors pour tout diviseur premier p de n, il existe un rang d_0 tel que l'identité*

$$p^d - 1 \nmid n^d - 1$$

pour tout entier rationnel $d > d_0$.

Démonstration. **référence vers l'article** □

Lemme 4.5 (théorème de Heath-Brown, [Ste06] th. 3.5)**.** *Tous les nombres premiers — à l'exception d'au plus deux d'entre eux — sont des racines primitives modulo q pour une infinité de nombres premiers q.*

Démonstration. **référence vers l'article** □

Lemme 4.6. *Soient $K/\mathbb{Q}$ une extension* abélienne *de degré fini et p un nombre premier non ramifié. S'il existe un groupe* cyclique *H et un isomorphisme de groupes*

$$\mathrm{Gal}(K/\mathbb{Q}) \to H$$

qui envoie la substitution de Frobenius de p en $K/\mathbb{Q}$[9] *sur un générateur de H, alors p est inerte dans K.*

Démonstration. Dans cette preuve, nous utilisons les résultats de [Kra00], ch. 3, § 4 et 5. Soient $f : \mathrm{Gal}(K/\mathbb{Q}) \to H$ un isomorphisme de groupes, s_p la substitution de Frobenius de p en $K/\mathbb{Q}$ et h un générateur de H vérifiant $f(s_p) = h$. L'extension étant non ramifiée en p, tout ceci a bien un sens. Comme h engendre H, que s_p engendre le sous-groupe de décomposition de p[10] et que f est un isomorphisme entre $\mathrm{Gal}(K/\mathbb{Q})$ et H, le Frobenius s_p est générateur de $\mathrm{Gal}(K/\mathbb{Q})$. On a donc l'égalité

$$D_p = \mathrm{Gal}(K/\mathbb{Q}).$$

La sous-extension de $K/\mathbb{Q}$ correspondant D_p dans la correspondance de Galois est donc $\mathbb{Q}$. D'après le lemme 3.9 de [Kra00], cela induit

$$g_p = 1.$$

L'idéal p est donc l'unique idéal premier de $\mathcal{O}_K$ au dessus de p, et comme p ne se ramifie pas dans K, cela prouve l'inertie de p.

□

9. Bien définie dans le cas abélien.
10. Bien défini dans le cas abélien.

Lemme 4.7. *Soient $n \leqslant 1$ un entier rationnel et ζ_n une racine primitive n-ième de l'unité. L'application*

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \longmapsto & \overline{a}, \end{array}$$

où a est un entier rationnel tel que $\sigma(\zeta_n) = \zeta_n^a$, est un isomorphisme de groupes bien défini.

Démonstration. Commençons par montrer que cette application est bien définie et que c'est un morphisme de groupes. Notons la φ. Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Cet automorphisme envoie ζ_n sur une autre racine primitive de l'unité. La racine ζ_n étant primitive, on a

$$\sigma(\zeta_n) = \zeta_n^a$$

avec a premier avec n. Si désormais a et b sont deux entiers rationnels tels que $\zeta_n^a = \zeta_n^b$, on a alors $\zeta_n^{a-b} = 1$. Comme ζ_n est primitive, cela implique

$$\overline{a} = \overline{b}.$$

Enfin, cette application est un morphisme de groupes, soient $\sigma_1, \sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ dont les images respectives par φ sont a_1 et a_2. On a

$$\sigma_1 \circ \sigma_2(\zeta_n) = \sigma_1(\zeta_n^{a_2}) = (\sigma_1(\zeta_n))^{a_2} = \zeta^{a_1 a_2}$$

et donc

$$\varphi(\sigma_1 \circ \sigma_2) = a_1 a_2 = \varphi(\sigma_1)\varphi(\sigma_2).$$

L'application φ est donc un morphisme de groupes bien défini.

Montrons que c'est un isomorphisme. Comme les ensembles de départ et d'arrivée sont finis, il suffit de montrer l'injectivité. Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ un automorphisme d'image $\overline{1}$. On a alors

$$\sigma(\zeta_n) = \zeta_n$$

et σ étant bijectif, l'égalité

$$\sigma = \mathrm{Id}\,.$$

Cela termine la démonstration. □

Démontrons le théorème 4.3.

Démonstration (du théorème 4.3). L'entier n a par hypothèse au moins trois facteurs premiers distincts. D'après le théorème Heath-Brown 4.5, l'un d'entre eux, que nous

notons p, est donc racine primitive modulo q pour une infinité de nombres premiers q. Soit d_0 le rang à partir duquel on a

$$p^d - 1 \nmid n^d - 1$$

pour tout entier $d > d_0$, donné par le lemme 4.4. On en déduit l'existence d'une infinité de nombres premiers q (premiers avec n) pour lesquels p est une racine primitive et vérifiant $q > d_0$. Fixons un tel nombre q et

$$K = \mathbb{Q}(\zeta_q).$$

Soit φ l'isomorphisme

$$\begin{array}{rccc} \varphi : & \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) & \longrightarrow & \mathbb{F}_q^* \\ & \sigma & \longmapsto & \overline{a}, \end{array}$$

où a est un entier rationnel tel que $\sigma(\zeta_q) = \zeta_q^a$, donné par le lemme 4.7 pour $n = q$. D'après l'identité (23), p. 45 de [Kra00], φ envoie le Frobenius de p sur la classe de p modulo q. Comme p est une racine primitive modulo q, le lemme 4.6 appliqué à $K/\mathbb{Q}$ et φ prouve que p est inerte dans K. En particulier, l'idéal $p\mathcal{O}_K$ est un idéal premier de $\mathcal{O}_K$ divisant $n\mathcal{O}_K$. On peut supposer $d_0 > q - 1$. On a alors

$$\mathrm{N}(p\mathcal{O}_K) - 1 = \mathrm{N}_{K/Q}(p) - 1 = p^{q-1} - 1 \nmid n^{q-1} - 1 = \mathrm{N}_{K/\mathbb{Q}}(n) - 1 = \mathrm{N}(n\mathcal{O}_K) - 1.$$

Le critère de Korselt généralisé 1.2 et la caractérisation **??** permettent d'affirmer que n n'est pas de Carmichael dans K, terminant la démonstration.

□

Un nombre de Carmichael ayant toujours au moins trois diviseurs premiers distincts (voir [Dem08], 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 ([Ste06] th. 2.5), 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 1.

Corollaire 4.8 ([Ste06] cor. 3.7)**.** *Soit n un entier rationnel 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 1.2.
- 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 [Dem08], 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 4.9 (troisième réciproque)**.** *Soit n un entier rationnel. 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.*

Démonstration. C'est la conjonction du théorème 1.6 et du corollaire 4.8. □

Remarque 4.10. Dans les deux réciproques (théorèmes 4.2 et 4.9) 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 (1.8)et cela permet de tester beaucoup moins de corps.

Passons désormais aux simulations numériques.

4.2 Simulations

4.2.1 Test de Fermat

Étant donné un entier de Carmichael n, la version « cyclotomique » du test de Fermat serait la suivante.

Algorithme 4 : Test de Fermat dans un corps cyclotomique

Entrées : n (entier rationnels à tester), K (corps cyclotomique de la forme $\mathbb{Q}(\zeta_q)$ où q est premier), S_α (ensemble coordonnées α)

```
si n et Disc(K) sont premiers entre eux alors
    ζ ← une racine primitive q-ième de l'unité engendrant K, q étant premier
    pour chaque α = x_0 + x_1 ζ + ··· + x_{p-1} ζ^{p-1}, x_0, ..., x_{p-1} ∈ S_α faire
        si α^{n^{p-1}} ≢ α (mod nO_K) alors
            retourner n n'est pas de Carmichael dans K et est composé
            arrêter le programme
```

Cet algorithme s'est montré encore moins performant que sa version quadratique. 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 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 [11]. 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 : chaque coordonnée a plusieurs milliers de chiffres. Plus généralement, le calcul de $\alpha^{\mathrm{N}(n\mathcal{O}_K)} = \alpha^{n^{q-1}}$ sort rapidement des capacités d'un ordinateur personnel standard.

4.2.2 Critère de Korselt

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

paramètre	valeur
corps testés	corps cyclotomiques de la forme $\mathbb{Q}(\zeta_q)$ où q est un nombre premier dans $[\![3, 300]\!]$ [12]
entiers de Carmichael testés	tous ceux de la liste $\mathfrak{C}$

TABLE 5 – Paramètres des simulations du critère de Korselt pour les corps cyclotomiques.

Avec ces paramètres, le critère de Korselt a donné pour chaque élément n de la liste, plusieurs corps cyclotomiques de discriminant premier avec n dans lesquels n n'est pas de Carmichael. Pour l'entier $n = 561$, nous trouvons par exemple qu'il est de Carmichael dans $\mathbb{Q}(\zeta_3)$ mais dans aucun autre corps testé. Cet algorithme permet aussi de prouver que l'entier de Howe 1 est composé ! Nous trouvons qu'il est de Carmichael dans $\mathbb{Q}(\zeta_3)$ mais dans aucun autre corps testé [13] 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.

11. Wolfram alpha n'a pas fait mieux.

13. 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.

entier de Carmichael	corps cyclotomique dans lequel il est de Carmichael
561	$\mathbb{Q}(\zeta_3)$
2821	$\mathbb{Q}(\zeta_3)$
1729	$\mathbb{Q}(\zeta_3)$
8911	$\mathbb{Q}(\zeta_3)$
15841	$\mathbb{Q}(\zeta_3)$
29341	$\mathbb{Q}(\zeta_3)$
46657	$\mathbb{Q}(\zeta_3)$
52633	$\mathbb{Q}(\zeta_3)$
63973	$\mathbb{Q}(\zeta_3)$
115921	$\mathbb{Q}(\zeta_3)$
126217	$\mathbb{Q}(\zeta_3)$
172081	$\mathbb{Q}(\zeta_3)$
115921	$\mathbb{Q}(\zeta_3)$
188461	$\mathbb{Q}(\zeta_3)$
252601	$\mathbb{Q}(\zeta_5)$
294409	$\mathbb{Q}(\zeta_3)$
488881	$\mathbb{Q}(\zeta_3)$
512461	$\mathbb{Q}(\zeta_3)$ et $\mathbb{Q}(\zeta_5)$
entier de Howe	$\mathbb{Q}(\zeta_3)$

TABLE 6 – Liste exhaustive des couples trouvés (n, K) où n est un entier de Carmichael et K un corps cyclotomique dans lequel n reste de Carmichael, pour les paramètres 4.2.2.

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. Leurs facteurs premiers sont congrus à 1 modulo 5. À noter que nous avons exhibé des entiers rationnels qui ne sont pas de Carmichael, dont tous les facteurs premiers ne sont pas congrus à 1 modulo 5 et qui sont de Carmichael dans $\mathbb{Q}(\zeta_5)$. C'est par exemple le cas de 2047 (qui n'est même pas congru à 1 modulo 5). **lien vers liste complète**

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

— L'entier de Howe est de Carmichael dans $\mathbb{Q}(\zeta_3)$ (qui est égal au corps quadratique $\mathbb{Q}(\sqrt{-3})$) mais dans aucun autre corps testé.

Donnons aussi quelques statistiques.

nombre de corps testés	1857
nombre d'idéaux de Carmichael trouvés dans ces corps	18
proportion d'idéaux de Carmichael trouvés dans ces corps	0,9 %

TABLE 7 – Statistiques des simulations du critère de Korselt sur les corps cyclotomiques pour les paramètres 4.2.2.

Quant aux performances, les calculs sont cependant significativement plus longs dans le cas des corps cyclotomiques que dans le cas des corps quadratiques. On retrouve néanmoins le fait que lesdits temps restent sensiblement proches pour tout entier rationnel (y compris l'entier de Howe) et tout corps cyclotomique testé. **expliquer mieux le tableau, pareil pour quadratiques**

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

TABLE 8 – Temps de calcul du critère Korselt dans les corps cyclotomiques donnés pour l'entier $n = 512461$.

Conclusion

L'article de G.A. Steele propose une extension de la notion d'entier de Carmichael. Nous y retrouvons le petit théorème de Fermat, le critère de Korselt et exposons de précieuses clés pour la détection des entiers de Carmichael. Le théorème, 2.1 tout d'abord, force à faire la distinction entre les nombres de Carmichael et les nombres de Carmichael *rigides* comme l'entier de Howe. Ce dernier indique toutefois que, comme $\mathbb{Q}$, les corps quadratiques ne peuvent pas détecter tous les entiers de Carmichael à l'aide du théorème de Fermat. C'est en revanche le cas des corps cyclotomiques : pour tout nombre de Carmichael n, il existe une infinité de corps cyclotomiques, de discriminant premier avec n, dans lesquels n n'est pas de Carmichael ; c'est le théorème 4.3. Ces énoncés d'existence n'indiquent cependant pas comment trouver de tels corps ou des témoins de Fermat.

Nos simulations numériques ont mis en valeur des tendances allant dans le sens de ces résultats. Les entiers de Carmichael (dans $\mathbb{Q}$) testés restèrent de Carmichael dans environ 24 % des corps quadratiques **ref** contre moins de 1 % des corps cyclotomiques **ref**. Le test de Fermat et les corps quadratiques exclus, le critère de Korselt dans les corps cyclotomiques **ref** est l'alternative la plus crédible à fournir un critère de composition inspiré de ces résultats. Ses performances se sont montrées très correctes et il semble avoir besoin de peu de corps pour prouver la composition d'un entier de Carmichael. L'auteur de ce texte reste conscient de la modeste portée de ces statistiques et de la petitesse de l'échantillon.

Enfin, les résultats de la section 3 témoignent de notre ignorance actuelle quant au comportement des idéaux de Carmichael et des extensions de corps dans lesquelles ces derniers conservent cette propriété. G.A. Steele a par ailleurs concentré son étude sur des corps bien connus : les corps quadratiques et cyclotomiques. Il y utilise à volonté des outils de théorie algébrique des nombres : ramification, discriminant, et de théorie analytique des nombres : lemmes 3.3 et 3.4 de l'article, théorème de Heath-Brown. Le critère de Korselt est le seul outil propre à la théorie. L'expansion de celle-ci dans une plus grande généralité, pour lui fournir des outils souples et adaptés, semble cruciale son développement.

Références

[Dem08] Michel Demazure. *Cours d'algèbre*. 2e éd. Cassini, 2008.

[Kra00] Alain Kraus. *Corps locaux et applications. Cours accéléré de DEA, Université Pierre et Marie Curie*. Sept. 2000.

[Sam71] Pierre Samuel. *Théorie algébrique des nombres*. 2e éd. Hermann Paris, oct. 1971.

[Ste06] G. A. Steele. « Carmichael numbers in number rings ». In : *Journal of Number Theory* 128 (2006), p. 910-917. url : `https://core.ac.uk/download/pdf/82709152.pdf`.

Todo

— refaire annexe
— liens vers les résultats
— temps calcul cyclo
— quid de l'efficacité de Korselt dans un corps cyclotomique ?
— références entre crochets
— rajouter sorties sur les algorithmes
— remarque norme impaire