Antoine Hugounet

placeholder Titre

travail encadré de recherche
encadré par Alain Kraus[1] (IMJ-PRG)
de janvier à juin 2020

Sorbonne Université

1. https://webusers.imj-prg.fr/~alain.kraus/

Introduction

Question 0.1. Soient n un entier de Carmichael et K un corps de nombre. Dans quel mesure n est-il de Carmichael dans K ?

$$\alpha^{\mathrm{N}(I)} \equiv \alpha \pmod{I}, \quad \forall \alpha \in \mathcal{O}_K. \tag{1}$$

Nous étudions tous les nombres de Carmichael de la liste [2]

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

1 Délices de la théorie

Fort heureusement, certaines propriétés fondamentales des *entiers* de Carmichael sont transportées au cadre plus général des *idéaux* de Carmichael. Tout d'abord, dans une extension *galoisienne*, un idéal premier est soit premier, soit de Carmichael. Plus formellement, vient ceci.

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

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

Vu autrement, on retrouve le petit théorème de Fermat dans les extensions finies abéliennes de $\mathbb{Q}$. Fait tout à fait remarquable, G. A. Steele fournit — dans ce nouveau cadre des idéaux de Carmichael — une réciproque au petit théorème de Fermat.

Théorème 1.2 (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*

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

Ainsi, vient l'équivalence suivante.

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*

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

2. La liste des premiers entiers de Carmichael est disponible à `https://oeis.org/A002997`.

Au delà de sa force théorique, cette énoncé semble porter une valeur historique majeure. Le test de Fermat était le seul à ne pas disposer d'une réciproque (pour le test d'Euler par exemple, c'est une équivalence). Il aura certes fallu la chercher dans les corps de nombres, mais les corps quadratiques suffisent. Ces objets ne sont d'ailleurs pas si loin de l'arithmétique classique : Gauss les étudiait déjà. Quant à la preuve, elle repose — comme la plupart des énoncés de la section 2 de l'article — sur des outils classiques de théorie algébrique des nombres. Son apparente complexité technique raisonnable dissimule un réel savoir-faire. Il semble indispensable de louer la créativité de l'auteur pour l'élaboration de son formalisme, ainsi que la conception de ses preuves.

Un autre résultat d'importance (démontré avant le petit théorème de Fermat généralisé dans l'article) est la généralisation du critère de Korselt. 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*

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

Remarque 1.5. 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 1. Si l'on a un corps de nombres L et un idéal J de $\mathcal{O}_K$, montrer que $\mathrm{N}(\mathfrak{P})-1 \mid \mathrm{N}(J)-1,\ \forall \mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_K) : \mathfrak{P} \mid J$ ne suffit pas. La preuve du critère de Korselt généralisé nous enseigne que si J est premier, J vérifie également cette identité. Il faut donc indépendamment montrer que J est composé, 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 1.6. *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 reste de donner une réponse à la question 0.1. Le théorème 2.5 de l'article 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.*

Remarque 2.2. On présage dès l'énoncé la nature de la preuve : c'est le critère de Korselt. On demande déjà que n soit sans facteurs carrés et comme la norme d'un idéal premier au dessus de $n\mathcal{O}_K$ est un nombre premier p divisant n, la partie réellement inventive de la preuve consiste à trouver les bons corps quadratiques. Cette partie est non triviale et est basée sur une savante utilisation du théorème chinois et la connaissance d'un nombre premier p comme dans les hypothèses du théorème.

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 $n = 512461$ et de son facteur premier $p = 271$: il existe 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 **ajouter référence** une liste de corps quadratiques dans lequel ledit entier n'est pas de Carmichael. **ajouter liste**

L'algorithme que nous avons utilisé pour trouver ces corps n'est cependant probablement pas utilisable en pratique, puisqu'il utilise le critère de Korselt généralisé et 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 trouvant le corps quadratique $K = \mathbb{Q}(\sqrt{13})$ et l'élément $\alpha = 2 + 1 \cdot \left(\frac{1+\sqrt{13}}{2}\right) \in \mathcal{O}_K$. 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 composition de n. Le point clé est que l'auteur ne semble pas utiliser le critère de Korselt. Il aurait besoin pour cela d'exhiber une

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**

décomposition en produit d'idéaux premiers de $n\mathcal{O}_K$, ce qui est certainement prohibitif. Au lieu de cela, il exhibe un élément $\alpha \in \mathcal{O}_K$ tel que $\alpha^{\mathrm{N}_{K/\mathbb{Q}}(n)} \not\equiv \alpha \pmod{n\mathcal{O}_K}$. Étant donné un entier impair (potentiellement de Carmichael) dont on veut tester la primalité, cela donne envie d'étudier l'algorithme *probabiliste* suivant.

Entrées : I (intervalle d'entiers sans facteurs carrés), b (borne coordonnées)
pour chaque d *sans facteurs carrés dans* I **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
retourner n *est probablement premier*

Ce potentiel algorithme est dans le même esprit que le test de primalité de Rabin-Miller. L'idée est 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 aurons une certitude morale de la primalité de n. Bien entendu, la « certitude morale » est finement quantifiée dans le test de Rabin-Miller (voir § 2.3.7, p. 69 de [2]). Pour que l'algorithme décrit ici soit viable, il conviendrait de définir une notion de *témoin de Carmichael* et d'étudier finement la répartition ou la répartition de tels témoins. La réciproque du théorème de Fermat (1.3) nous assure toutefois de leur existence.

2.2 Problèmes

Il ne faut toutefois pas se réjouir trop vite. Revenons un peu 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 2.3 (mauvaise réciproque 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*

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

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. 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 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*

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

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 (0.1). 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 **?? 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 $\text{pgcd}(q, n) = 1$ **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 3.6. 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`.

3.3 Technique

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*. deuxième édition. 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

- **Rajouter des liens vers les fonctions implémentées depuis les algorithmes.**
- **ajouter des titres aux algorithmes**
- **ajouter intro à table des matières et ornement**