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

1 Délices de la théorie

2 Troublants corps quadratiques

3 Salutaires 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 énoncer ce résultat théorique.

Théorème 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 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 (3.6 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 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 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 4, l'auteur a pu implémenter un algorithme SageMath apportant dans certains cas une réponse à la question centrale de l'article (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 étudions tous les nombres de Carmichael de la liste [2]

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

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 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.

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

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 ([**article**], 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. 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 [3] 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 [4] — 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

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

4. 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 $\mathbb{Q}(\sqrt{95})$.

B Todo

— Enlever les hypothèses $Disc(K)$ premier avec n si Kraus est ok et rajotuer en lemme que c'est bon en introductoin