TESTS DE PRIMALITÉ ET DE PSEUDO-PRIMALITÉ

par

Tony Ezome

Résumé. — Dans cet article, nous présentons quelques algorithmes permettant d'*étudier la primalité* d'un entier n donné, c'est-à-dire déterminer si n est premier ou composé. Les algorithmes les plus élémentaires reposent sur des propriétés de l'anneau $\mathbb{Z}/n\mathbb{Z}$, différentes selon que n est premier ou composé. D'autres algorithmes font intervenir une extension de $\mathbb{Z}/n\mathbb{Z}$.

Abstract. — In this article we describe some algorithms for determining whether a given integer n is prime or composite. The simplest algorithms are based on properties of the ring $\mathbb{Z}/n\mathbb{Z}$. Others involve an extension of $\mathbb{Z}/n\mathbb{Z}$.

À ma mère ...

Introduction

Formalisme. — Étudier la primalité d'un entier n donné est un problème très ancien. Les *Éléments d'Euclide* abordent déjà cette question. Et plus près de nous, le petit théorème de Fermat affirme que pour tout nombre premier n et tout entier x dans l'intervalle $[1, n-1]$, on a $x^{n-1} \equiv 1 \bmod n$. On déduit de ce théorème un *critère de composition* : s'il existe un entier x dans l'intervalle $[1, n-1]$, tel que $x^{n-1} \not\equiv 1 \bmod n$, alors n est composé. Nous verrons que cette congruence peut être vérifiée sans trop de calculs. En général, un critère de composition est une propriété des inversibles d'un anneau S, qui peut-être $\mathbb{Z}/n\mathbb{Z}$ ou une extension. Cette propriété est toujours satisfaite lorsque n est premier. On prouve que n est composé en exhibant un inversible x qui ne satisfait pas la propriété. À l'instar des critères de composition, il existe aussi des *critères de primalité*. On sait par exemple que si n est impair et composé, alors le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ est strictement inférieur à $n-1$. On peut donc prouver que n est premier en exhibant un élément x d'ordre $n-1$ dans $(\mathbb{Z}/n\mathbb{Z})^*$. C'est le principe du *test de Pocklington-Lehmer*. Nous verrons cependant qu'il n'est pas toujours facile de prouver que l'ordre de x est égal à $n-1$.

***Classification mathématique par sujets* (2010).** — 11A51.
Mots clefs. — primalité, pseudo-primalité, extensions d'anneaux.

À partir d'un critère de composition, on construit, pour tout nombre impair n, un ensemble de *témoins* W_n et une application

$$P_n : W_n \to \{\text{premier, composé}\}$$

qui à tout témoin $x \in W_n$ associe une affirmation concernant la primalité de n.
Un *test de composition* est la donnée d'un critère de composition, de l'ensemble des témoins W_n associé à ce critère, et de l'application $P_n : W_n \to \{\text{premier, composé}\}$. Lorsque n est premier, l'image de P_n est $P_n(W_n) = \{\text{premier}\}$. Dans ce cas, il n'y a que de *bons témoins*. Si n est composé, alors les éléments x de W_n tels que $P_n(x) = \text{premier}$ sont appelés *faux témoins*. On dit que n a *validé un test* P_n, si après avoir choisi uniformément un témoin x dans W_n, on a obtenu $P_n(x) = \text{premier}$. Le calcul de $P_n(x)$ se fait à l'aide d'un algorithme permettant de vérifier la propriété énoncée dans le critère de composition. Il est naturel de compter le nombre d'*opérations élémentaires* nécessaires à l'exécution d'un tel algorithme, c'est-à-dire son *temps de calcul*. Les *machines de Turing* à deux bandes sont des modèles formels décrivant l'exécution des algorithmes ([**15**], chapitre 2). Elles permettent de définir rigoureusement la notion de temps de calcul. Dans cet article, nous nous contentons de majorer le nombre d'opérations élémentaires nécessaires pour calculer $P_n(x)$. Cette majoration dépend du nombre de chiffres dans la représentation binaire de n. On rappelle que l'addition de deux entiers, dont la représentation binaire comporte au plus k chiffres, nécessite $O(k)$ opérations élémentaires. D'autre part, multiplier deux nombres binaires de taille k, en utilisant l'algorithme élémentaire, requiert $O(k^2)$ opérations élémentaires. Les algorithmes utilisant des techniques de multiplication rapide nécessitent quant à eux $O(k^{1+\epsilon(k)})$ opérations élémentaires, où $k \mapsto \epsilon(k)$ est une fonction qui tend vers 0 lorsque k tend vers l'infini ([**19**], chapitre 8).

Le test de Fermat. — Le petit théorème de Fermat induit un test de composition dont l'ensemble des témoins W_n est égal à $(\mathbb{Z}/n\mathbb{Z})^*$. L'application P_n associée est définie par :

$$P_n \quad : \quad (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \{\text{premier, composé}\}$$

$$x \longmapsto \begin{cases} \text{premier si } x^{n-1} = 1 \bmod n \\ \text{composé si } x^{n-1} \neq 1 \bmod n \end{cases}$$

L'algorithme d'*exponentiation rapide* ([**8**], section 1.2, page 8) permet de calculer efficacement g^n dans un groupe G, où $g \in G$ et $n \in \mathbb{Z}$. Cet algorithme est très important. Il est utilisé par la plupart des tests que nous présentons dans ce document. Par exemple pour effectuer un test de Fermat, l'exponentiation rapide détermine x^{n-1} en temps $(\log n)^{2+\epsilon(n)}$, où $n \mapsto \epsilon(n)$ est une fonction qui tend vers 0 lorsque n tend vers l'infini.
Un *nombre de Carmichael* est un entier composé n tel que $x^{n-1} \equiv 1$ pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Il existe une infinité de nombre de Carmichael [**2**]. Ces derniers n'admettent que de faux témoins pour le test de Fermat, il faut donc affiner ce test.

Le test de Solovay-Strassen. — Soient n un nombre premier impair, et a un entier. Le *symbole de Legendre* $\left(\frac{a}{n}\right)$ est défini par

$$\left(\frac{a}{n}\right) = \begin{cases} 0 & \text{si 0 est l'unique solution de l'équation } x^2 = a, \text{ dans } \mathbb{Z}/n\mathbb{Z}. \\ 1 & \text{si l'équation } x^2 = a \text{ a deux solutions dans } \mathbb{Z}/n\mathbb{Z}. \\ -1 & \text{si l'équation } x^2 = a \text{ n'a aucune solution dans } \mathbb{Z}/n\mathbb{Z}. \end{cases}$$

Il existe plusieurs règles et propriétés permettant de calculer le symbole de Legendre ([**8**], section 1.4.2, page 27). L'une des propriétés les plus importantes est la loi de réciprocité quadratique ([**8**], section 1.4.2, théorème 1.4.7). Le *symbole de Jacobi* étend le symbole de Legendre à tous les entiers impairs $n \geq 3$. Certaines propriétés, telles que la loi de réciprocité quadratique, s'étendent. Ces propriétés, associées à la division euclidienne, induisent des algorithmes efficaces pour calculer le symbole de Jacobi.
Si n est un nombre premier impair, alors la congruence $x^{n-1} \equiv 1 \bmod n$ du petit théorème de Fermat implique que :
– soit $x^{\frac{n-1}{2}} \equiv 1 \bmod n$, et dans ce cas x est un *résidu quadratique* (*i.e* un carré) modulo n car $(\mathbb{Z}/n\mathbb{Z})^*$ est un groupe cyclique.
– soit $x^{\frac{n-1}{2}} \equiv -1 \bmod n$, dans ce cas x n'est pas un résidu quadratique modulo n.
Dans tous les cas, on a $x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \bmod n$.
Donc pour un entier impair $n \geq 3$ donné, l'existence d'un x dans $(\mathbb{Z}/n\mathbb{Z})^*$ tel que $x^{\frac{n-1}{2}} \not\equiv \left(\frac{x}{n}\right) \bmod n$, implique que n est composé. C'est le principe du test de composition de Solovay-Strassen. L'ensemble des témoins pour ce test est $W_n = (\mathbb{Z}/n\mathbb{Z})^*$ et l'application associée

$$\mathrm{SS}_n \quad : \qquad (\mathbb{Z}/n\mathbb{Z})^* \longrightarrow \{\text{premier, composé}\}$$

est définie par : $\mathrm{SS}_n(x) =$ premier si et seulement si $x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \bmod n$.
On définit une notion importante pour les tests de composition : *la densité de faux témoins*. Il s'agit de la probabilité d'erreur, elle permet d'évaluer la *fiabilité* du test. La situation du test de Solovay-Strassen est précisée par le théorème suivant :

Théorème 1. — *Supposons que n est un entier impair composé et que $\left(\frac{x}{n}\right)$ désigne le symbole de Jacobi. Alors la densité μ_{SS} de faux témoins pour le test de Solovay-Strassen vérifie*

$$\mu_{\mathrm{SS}} = \frac{\{x \in (\mathbb{Z}/n\mathbb{Z})^* |\ x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \bmod n\}}{\varphi(n)} \leq \frac{1}{2},$$

où $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration. — [**15**], théorème 11.2, Page 253. □

Avec le test de Solovay-Strassen, on a donc au moins une chance sur deux de détecter un nombre composé. La probabilité qu'un entier composé valide k tests de Solovay-Strassen indépendants est au plus égale à $(1/2)^k$.

Le test de Miller-Rabin. — Il repose sur une factorisation du polynôme $P(X) = X^{n-1} - 1$ dans $(\mathbb{Z}/n\mathbb{Z})[X]$, comme le précise le théorème suivant :

***Théorème 2* (Critère Miller-Rabin).** — *Soit $n \geq 3$ un entier impair. On pose $n-1 = 2^k m$, où m est un entier impair. Si n est premier alors pour tout x dans $(\mathbb{Z}/n\mathbb{Z})^*$*

$$(1) \qquad x^m = 1, \text{ ou bien il existe un } i \text{ dans } \{0,1,2,\ldots,k-1\} \text{ tel que } x^{m2^i} = -1.$$

Démonstration. — En effet d'après le petit théorème de Fermat, on a : $x^{n-1} - 1 = 0 \bmod n$. En factorisant successivement chacune des différences de deux carrés, on obtient :

$$x^{n-1}-1 = (x^{\frac{n-1}{2}}+1)(x^{\frac{n-1}{2}}-1) = \cdots = (x^{2^{k-1}m}+1)(x^{2^{k-2}m}+1)\cdots(x^{2m}+1)(x^m+1)(x^m-1).$$

Puisque $\mathbb{Z}/n\mathbb{Z}$ est un corps, l'un de ces facteurs est nul. □

L'ensemble des témoins pour le test de Miller-Rabin est $W_n = (\mathbb{Z}/n\mathbb{Z})^*$, et l'application associée $\mathrm{MR}_n : (\mathbb{Z}/n\mathbb{Z})^* \to \{\text{premier, composé}\}$ est définie par :

$$\mathrm{MR}_n(x) = \text{ premier } \iff \begin{cases} x^m = 1 \\ \text{ ou} \\ \text{il existe } i \in \{0,1,2,\ldots,k-1\} \text{ tel que } x^{m2^i} = -1. \end{cases}$$

La fiabilité de ce test est donnée par le théorème suivant.

***Théorème 3*.** — *Soit n un entier impair composé. Alors la densité de faux témoins pour le test Miller-Rabin vérifie*

$$\mu_{\mathrm{MR}} = \frac{\#\{x \in (\mathbb{Z}/n\mathbb{Z})^* |\ \textit{la condition (1) est vérifiée}\}}{\varphi(n)} \leq \frac{1}{2^{t-1}}$$

où $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$ et t est le nombre de diviseurs premiers distincts de n.
De plus si $n \geq 11$, alors $\mu_{\mathrm{MR}} \leq \frac{1}{4}$.

Démonstration. — [**17**], section 2, théorème 2.1. □

Le test de Miller-Rabin est particulièrement fiable lorsque n a beaucoup de diviseurs premiers. Ce test, comme le test de Solovay-Strassen, ne prouve pas qu'un entier est premier, mais apporte une forte conviction. C'est pourquoi on dit aussi que ce sont des tests de *pseudo-primalité*. Les majorations des théorèmes 1 et 3 montrent que le test de Miller-Rabin est plus rassurant que celui de Solovay-Strassen.

Le test de Pocklington-Lehmer. — Si un entier n valide plusieurs tests de Miller-Rabin, il a de fortes chances d'être premier. En pratique on est convaincu de la primalité de n, mais la rigueur mathématique exige une preuve. Les *algorithmes de preuve de primalité* permettent de conclure avec certitude, grâce aux critères de primalité, qu'un entier donné est premier. Un *test de primalité* est la donnée d'un critère de primalité et de l'algorithme de preuve de primalité induit par ce critère. On dit que le test est *probabiliste* si l'une des étapes, de l'algorithme associé, est aléatoire. Lorsque toutes les étapes de l'algorithme sont sans aléa, le test est dit *déterministe*.
Le théorème 4 ci-dessous est dû à Pocklington, l'énoncé original est différent de celui que nous donnons ici.

***Théorème 4* (Pocklington).** — *Soit $n \geq 2$ un entier naturel. Supposons qu'il existe un élément a dans $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre exact s tel que $s \geq \sqrt{n}$. Alors n est un nombre premier.*

Dire que a est d'ordre exact s dans $(\mathbb{Z}/n\mathbb{Z})^*$ signifie que $a^s = 1$ et $a^i - 1$ est inversible modulo n, pour $1 \leq i \leq s-1$. Cela revient à dire que $a^s = 1$ et que $a^{\frac{s}{q}} - 1$ est une unité pour tout diviseur premier q de s. Cette dernière condition est facile à vérifier à l'aide de l'exponentiation rapide, pourvu que l'on connaisse la factorisation de s.

Démonstration du théorème 4. — Soit p un diviseur premier de n. L'élément $a \bmod p$ est d'ordre s dans $(\mathbb{Z}/p\mathbb{Z})^*$. Donc s divise $p-1$. Ainsi $p \geq 1 + s > \sqrt{n}$. Par conséquent tout diviseur premier de n est plus grand que $\sqrt{n}$. Cela n'est possible que si n est premier. □

Le théorème de Pocklington donne lieu à l'algorithme suivant :

***Algorithme* (Pocklington-Lehmer).** — *Soit $n \geq 2$ un entier.*

1. *Déterminer un ensemble Q de petits diviseurs premiers q de $n-1$ tels que le produit $s = \prod_{q \in Q} q^{v_q(n-1)}$ vérifie $s \geq \sqrt{n}$.*
2. *Tirer au hasard (avec distribution uniforme) un b dans $(\mathbb{Z}/n\mathbb{Z})^*$ jusqu'à ce qu'en posant $a = b^{\frac{n-1}{s}}$, on ait :*
   (a) $a^s = 1$;
   (b) $\operatorname{pgcd}(a^{\frac{s}{q}} - 1, n) = 1$ *pour tout* $q \in Q$.

Si l'entier n passe tous les tests, alors il est premier d'après le théorème 4.

***Remarque*.** — 1. Le test de Pocklington-Lehmer est le plus simple des algorithmes de preuve de primalité. Mais l'utilisation de ce test soulève une difficulté, il faut trouver et factoriser un diviseur s de $n-1$, où $s \geq \sqrt{n}$. Cela revient souvent à factoriser l'entier $n-1$, mais la factorisation est un problème très difficile. Le test APRCL que nous présentons dans la section 3 permet de contourner cette difficulté en introduisant un paramètre supplémentaire, le degré d d'une extension de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

2. L'algorithme de Pocklington-Lehmer est probabiliste. La seconde étape de cet algorithme consiste à déterminer un élément a d'ordre exact s dans $(\mathbb{Z}/n\mathbb{Z})^*$. Lorsque n est premier, la probabilité pour que $a = b^{\frac{n-1}{s}}$ soit d'ordre exact s est égale à $\varphi(s)/s$.

Le plan. — Dans la section 1, nous étudions les extensions galoisiennes d'un anneau commutatif unitaire arbitraire R. Ensuite nous examinons le cas des anneaux finis $R = \mathbb{Z}/n\mathbb{Z}$ dans la section 2. Cette étude nous permet de décrire deux algorithmes dans la section 3 : le test de primalité APRCL et le *test de Galois*. La section 4 est consacrée au test de primalité AKS et à ses principales variantes.

Remerciements. Je remercie Jean-Marc Couveignes pour ses orientations et conseils.

Convention. Dans cet article, tous les anneaux (et les algèbres) sont supposés unitaires.

1. Extensions galoisiennes d'anneaux

Cette section reprend quelques éléments concernant les extensions galoisiennes d'un anneau commutatif. Seules les définitions et propriétés utiles aux critères de (pseudo-)primalité seront énoncées. Les résultats classiques de la théorie algébrique des nombres (en particulier ceux

de la théorie de Galois sur les corps) sont supposés connus, les ouvrages [**13**] et [**16**] sont de très bonnes références.

1.1. Préliminaires. —

Définition 1.1. — *Soit R un anneau commutatif.*

1. *Une algèbre sur R est la donnée d'un anneau S et d'un morphisme d'anneaux $\varphi : R \to S$ tel que $\varphi(R)$ est contenu dans le centre de S.*
2. *On dit qu'un R-module S est projectif si l'une des conditions équivalentes (*[**13**]*, page 137) suivantes est vérifiée :*
   (a) *Toute suite courte exacte de R-modules*
   $$0 \longrightarrow M' \longrightarrow M'' \longrightarrow S \longrightarrow 0$$
   est scindée, c'est-à-dire que le R-module M'' est isomorphe à la somme directe $M' \oplus S$.
   (b) *Il existe un R-module M tel que la somme $M \oplus S$ est un R-module libre, en d'autres termes S est isomorphe à un facteur direct d'un R-module libre.*

Soient S une algèbre commutative sur un anneau commutatif R, et $\mathcal{G}$ un groupe fini de R-automorphismes de S. Le produit tensoriel $S \otimes_R S$ a une structure de S-algèbre induite par la relation $s(a \otimes b) = (sa) \otimes b$, pour tous $a, b, s \in S$. L'application $\phi : S \otimes_R S \to S^{\#\mathcal{G}}$, définie par $\phi(a \otimes b) = (a\sigma(b))_{\sigma \in \mathcal{G}}$ et $\phi(\sum_{1 \leq i \leq k} a_i \otimes b_i) = \sum_{1 \leq i \leq k} \phi(a_i \otimes b_i)$, est un morphisme de S-algèbres. D'autre part, l'algèbre S a une structure de $S \otimes_R S$-module induite par la relation $(s_1 \otimes s_2)s_3 = s_1 s_2 s_3$. On introduit le morphisme de $S \otimes_R S$-modules

$$\begin{array}{ccc} \mu & : & S \otimes_R S \longrightarrow S \\ & & \sum_i s_i \otimes s_i' \longmapsto \sum_i s_i s_i'. \end{array}$$

Définition 1.2. — *1. Soient R un anneau commutatif et S une R-algèbre commutative. On dit que S est une R-algèbre séparable si le morphisme μ fait de S un $S \otimes_R S$-module projectif.*

2. *Un élément a d'un anneau A est nilpotent s'il existe un entier naturel non nul n tel que $a^n = 0$. L'ensemble des éléments nilpotents d'un anneau A est un idéal : c'est le nilradical* $\mathrm{Nil}(A)$ *de A. Si* $\mathrm{Nil}(A) = \{0\}$*, alors on dit que A est un anneau réduit.*
3. *On dit qu'un module M sur un anneau A est fidèle si tout élément a dans A vérifiant $aM = \{0\}$ est nul, autrement dit l'annulateur de M est trivial.*

Tous les ingrédients sont maintenant réunis pour définir les extensions galoisiennes d'un anneau commutatif.

1.2. Définition et illustration. —

Définition 1.3. — *Soit R un anneau commutatif. Soient $S \supset R$ une R-algèbre commutative fidèle et $\mathcal{G}$ un sous-groupe fini de l'ensemble $\mathrm{Aut}_R(S)$ des R-automorphismes de S. Alors $(S, \mathcal{G})$ est une extension galoisienne de R si l'une des trois conditions équivalentes (*[**12**]*, proposition 1.2, page 80) suivantes est vérifiée :*

1. *(a) La sous-algèbre $S^{\mathcal{G}}$ des éléments de S fixés par $\mathcal{G}$ est égale à R.*
   (b) Pour tout élément idempotent non nul e de S (c'est-à-dire $ee = e$ et $e \neq 0$) et tout couple d'automorphismes distincts $(\sigma, \tau) \in \mathcal{G}^2$, il existe un élément s dans S tel que $\sigma(s)e \neq \tau(s)e$.
   [Lorsque 0 et 1 sont les seuls idempotents de S, cette condition est triviale].
   (c) S est une R-algèbre séparable.
2. *(a) La sous-algèbre $S^{\mathcal{G}}$ des éléments de S fixés par $\mathcal{G}$ est égale à R.*
   (b) L'application $\phi : S \otimes_R S \to S^{\#\mathcal{G}}$, définie à la section 1.1, est un isomorphisme de S-algèbres.
3. *(a) La sous-algèbre $S^{\mathcal{G}}$ des éléments de S fixés par $\mathcal{G}$ est égale à R.*
   (b) Pout tout idéal maximal M de S et pour tout σ dans $\mathcal{G} - \{\mathrm{Id}_S\}$, il existe un élément x dans S tel que $\sigma(x) - x \notin M$.

Proposition 1.4. — *Soit $(S, \mathcal{G})$ une extension galoisienne d'un anneau commutatif R. Alors :*

1. *S est un R-module projectif de type fini.*
2. *Son rang $\mathrm{Rang}_R(S)$ est bien défini, et il est égal à $\#\mathcal{G}$. Cela veut dire que pour tout idéal premier $\mathfrak{p}$ de R, le $R_{\mathfrak{p}}$-module $S \otimes_R R_{\mathfrak{p}}$ est libre de rang $\#\mathcal{G}$.*

Démonstration. — [**12**], page 80, proposition 1.2 pour l'assertion (1). Et [**12**], page 85, corollaire 1.3 pour l'assertion (2). □

On appelle *degré* d'une extension galoisienne $(S, \mathcal{G})$, le rang $\mathrm{Rang}_R(S) = \#\mathcal{G}$ du R-module S. Lorsque le groupe $\mathcal{G} = \langle\sigma\rangle$ est engendré par un R-automorphisme σ, on dit que $(S, \mathcal{G})$ est une *extension cyclique* de R.

Exemple 1.5. — Soient R un anneau commutatif et $d \geq 3$ un entier naturel non nul. On note S l'anneau produit R^d. Nous identifions R à un sous-anneau de S par le monomorphisme

$$R \longrightarrow S$$

$$r \longmapsto (r, r, \ldots, r).$$

Toute permutation α de $\{1, 2, \ldots, d\}$ induit un R-automorphisme de S (que nous notons également α) défini par $\alpha(x_1, \ldots, x_d) = (x_{\alpha^{(-1)}(1)}, \ldots, x_{\alpha^{(-1)}(d)})$. Soit σ le R-automorphisme d'ordre d de S défini par $\sigma(x_1, \ldots, x_d) = (x_2, x_3, \ldots, x_d, x_1)$. Alors la sous-algèbre S^σ des éléments de S fixés par σ est $S^\sigma = R$. De plus le morphisme de S-algèbres $\phi : S \otimes_R S \to S^d$ défini par $\phi(a \otimes b) = (a\sigma^k(b))_{k \in \mathbb{Z}/d\mathbb{Z}}$ est un isomorphisme. Donc $(S, \langle\sigma\rangle)$ est une extension galoisienne de R de degré d. Mais (S, S_d) n'est pas une extension galoisienne de R, bien que la

sous-algèbre des éléments de S fixés par le groupe symétrique soit $S^{\mathrm{S}_d} = R$. En effet, notons τ le R-automorphisme de S induit par la transposition $\tau = (1\ 2)$, et soit M un idéal maximal de R. Alors $\mathfrak{M} = R \times R \times M \times R \times \cdots \times R$ est un idéal maximal de S. Et pour tout x dans S, $\tau(x) - x$ appartient à $\mathfrak{M}$. Cela est contraire à la condition $3(b)$ de la définition 1.3.

On voit sur cet exemple que la notion d'extension galoisienne est étroitement liée au groupe d'automorphismes considéré.
On rappelle qu'une algèbre S sur un corps $\mathbf{K}$ est *classiquement séparable* sur $\mathbf{K}$ si pour toute extension de corps $\mathbf{L}/\mathbf{K}$, l'anneau $\mathbf{L} \otimes_{\mathbf{K}} S$ est réduit. D'après [**12**], page 50, théorème 2.5, une $\mathbf{K}$-algèbre S est séparable au sens de la définition 1.2, si et seulement si

1. S est une $\mathbf{K}$-algèbre classiquement séparable,
2. Et S est un $\mathbf{K}$-espace vectoriel de dimension finie.

Remarque 1.6. — 1. Un élément algébrique sur un corps $\mathbf{K}$ est classiquement séparable si son polynôme minimal n'a que des racines simples.
Une extension $\mathbf{L}$ de $\mathbf{K}$ de degré fini est classiquement séparable sur $\mathbf{K}$ si et seulement si tout élément de $\mathbf{L}$ est classiquement séparable sur $\mathbf{K}$ ([**13**], théorème 4.3, page 241).

2. Si R et S sont deux corps, et $\mathcal{G}$ un groupe fini tel que $(S, \mathcal{G})$ est une extension galoisienne de R au sens de la définition 1.3, alors $(S, \mathcal{G})$ est une extension galoisienne de R au sens de la théorie de Galois classique sur les corps. En effet :
   (a) On a vu que la condition $1.(c)$ de la définition 1.3 implique que S est une extension de degré fini classiquement séparable sur R.
   (b) Dans ce cas, la condition $1.(a)$ signifie que S est une extension normale de R.
3. Réciproquement, supposons que R et S sont deux corps, et que $\mathcal{G}$ est un groupe fini tel que $(S, \mathcal{G})$ est une extension galoisienne de R au sens de la théorie de Galois classique sur les corps. Alors S est une algèbre classiquement séparable normale de degré fini sur R et $S^{\mathcal{G}} = R$. Puisque les seuls éléments idempotents dans un corps sont 0 et 1, on conclut que $(S, \mathcal{G})$ est une extension galoisienne de R au sens de la définition 1.3.

1.3. Deux résultats intéressants. — Dans cette section nous donnons deux propositions utiles pour la suite.

Proposition 1.7. — *Soient $(S, \mathcal{G})$ une extension galoisienne de R, et $\mathfrak{p}$ un idéal premier de R. Alors :*

1. *L'application*

$$R/\mathfrak{p} \times S \longrightarrow S/\mathfrak{p}S$$

$$(r \bmod \mathfrak{p}, s) \longmapsto rs \bmod \mathfrak{p}S$$

   est R-bilinéaire et induit un isomorphisme de $R/\mathfrak{p} \otimes_R S$ sur $S/\mathfrak{p}S$.

2. *De plus, $(S/\mathfrak{p}S, \mathcal{G})$ est une extension galoisienne de $R/\mathfrak{p}$.*

Démonstration. — [**13**], chapitre XVI paragraphe 2, Proposition 2.7 pour l'assertion (1). Et [**12**], page 85, Corollaire 1.3 pour l'assertion (2). □

Soient $n > 1$ un entier naturel et $(S, \mathcal{G})$ une extension galoisienne de $R = \mathbb{Z}/n\mathbb{Z}$. Si p est un diviseur premier de n, alors la proposition 1.7 implique que $(S/pS, \mathcal{G})$ est une extension galoisienne de $\mathbf{F}_p$. Dans la section 2, nous étudions les propriétés de la $\mathbf{F}_p$-algèbre S/pS.

Définition 1.8. — *Soient R un anneau commutatif, et $(S, \mathcal{G})$ une extension galoisienne de R. Soit ω un élément de S. Si $(\sigma(\omega))_{\sigma\in\mathcal{G}}$ est une R-base de S, alors on dit que c'est une R-base normale de S.*

Proposition 1.9. — *Soit R un anneau commutatif semi-local (i.e n'ayant qu'un nombre fini d'idéaux maximaux). Soit $(S, \mathcal{G})$ une extension galoisienne de R. Alors :*

1. *S est un R-module libre de rang* $\mathrm{Rang}_R(S) = \#\mathcal{G}$.
2. *S est isomorphe à $R[\mathcal{G}]$, pour la structure de $R[\mathcal{G}]$-module sur S induite par $(r\sigma)s = r\sigma(s)$, où $(r, \sigma) \in R \times \mathcal{G}$. Cela signifie que S possède une R-base normale.*

Démonstration. — L'assertion (1) est obtenue en combinant la proposition 1.4 du présent article et la proposition 5 de [**5**], chapitre II, paragraphe 5, numéro 3. L'assertion (2) vient de [**7**], théorème 4.2. □

2. Le cas des anneaux finis $\mathbb{Z}/n\mathbb{Z}$

Soit $n > 1$ un entier naturel, on pose $R = \mathbb{Z}/n\mathbb{Z}$. D'après la proposition 1.9, toute extension galoisienne $(S, \mathcal{G})$ de R est une R-algèbre libre de rang fini. L'objectif dans cette section est d'étudier les propriétés de l'anneau S, et d'examiner l'action de $\mathcal{G}$ sur les quotients S/pS où p est diviseur premier de n. Lorsque le groupe $\mathcal{G}$ est engendré par un R-automorphisme σ, nous préciserons la relation entre σ et l'automorphisme de Frobenius de S/pS.

2.1. Rappels sur les anneaux artiniens. —

Définition 2.1. — *Soit A un anneau commutatif.*

1. *On dit que A est noethérien si et seulement si tout sous A-module (i.e tout idéal) de A est un A-module de type fini.*
2. *Une chaine d'idéaux premiers de A est une suite strictement croissante d'idéaux premiers $\mathfrak{p}_0 \subset \mathfrak{p}_1 \cdots \subset \mathfrak{p}_r$. La longueur de la chaine est r. La dimension $dim(A)$ de A est la borne supérieure de l'ensemble des longueurs de toutes les chaines d'idéaux premiers de A.*
3. *Le spectre* $\mathrm{Spec}(A)$ *de A est l'ensemble de ses idéaux premiers.*
4. *On dit que A est artinien (on dit aussi anneau d'Artin) si et seulement si A est noethérien et $dim(A) = 0$ (c'est-à-dire tout idéal premier de A est maximal).*

Exemple 2.2. — 1. Tout corps commutatif $\mathbf{K}$ est évidemment un anneau artinien.

2. L'anneau $\mathbb{Z}$ des entiers relatifs est principal, et donc noethérien.
3. Si $n > 1$ est un entier naturel, alors $R = \mathbb{Z}/n\mathbb{Z}$ est un anneau noethérien ([**3**], proposition 7.1). D'autre part, les idéaux premiers de R sont les quotients des idéaux premiers de $\mathbb{Z}$ contenant $n\mathbb{Z}$. Or tout idéal premier non nul de $\mathbb{Z}$ est maximal. Donc $dim(R) = 0$, et par conséquent R est un anneau artinien.

Soit $n > 1$ un entier naturel, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Soit $S \supset R$ une R-algèbre commutative libre de rang fini. Puisque R est noethérien, l'anneau S est noethérien ([**3**], proposition 7.2). Si $\mathfrak{p}$ est un idéal premier de S, alors l'intersection $\mathfrak{p} \cap R$ est un idéal premier de R. En fait $\mathfrak{p} \cap R$ est un idéal maximal, car R est un anneau artinien. Donc $\mathfrak{p}$ est un idéal maximal de S ([**6**], chapitre V, paragraphe 2, numéro 1, proposition 1). On en déduit que la dimension de S est nulle. Ainsi toute algèbre commutative libre de rang fini (et particulièrement toute extension galoisienne) sur un anneau fini $\mathbb{Z}/n\mathbb{Z}$ est un anneau artinien.

2.2. Rappels sur les actions de groupes. — Nous développons ici quelques notions, sur les actions de groupes, utiles pour la suite de notre étude.

Définition 2.3. — *Soient S un anneau commutatif, et $\mathcal{G}$ un groupe agissant sur S. Soit $\mathfrak{p}$ un idéal premier de S.*

1. *Le groupe de décomposition de $\mathfrak{p}$ est le sous-groupe des éléments $\sigma \in \mathcal{G}$ tels que $\sigma.\mathfrak{p} = \mathfrak{p}$, on le note $\mathcal{G}^{\mathrm{Z}}(\mathfrak{p})$.*
2. *Le groupe d'inertie de $\mathfrak{p}$, noté $\mathcal{G}^{\mathrm{T}}(\mathfrak{p})$, est le sous-groupe de $\mathcal{G}^{\mathrm{Z}}(\mathfrak{p})$ formé par les σ tels que l'endomorphisme*

$$S/\mathfrak{p} \longrightarrow S/\mathfrak{p}$$

$$x \bmod \mathfrak{p} \longmapsto \sigma(x) \bmod \mathfrak{p}$$

est égal à l'identité.

Par exemple si $n > 1$ est un entier naturel, alors le groupe symétrique S_3 agit sur l'anneau produit $(\mathbb{Z}/n\mathbb{Z})^3$ de la façon suivante :

$$\sigma(x_1, x_2, x_3) = (x_{\sigma^{(-1)}(1)}, x_{\sigma^{(-1)}(2)}, x_{\sigma^{(-1)}(3)}) \text{ pour tout } (\sigma, x_1, x_2, x_3) \in \mathrm{S}_3 \times (\mathbb{Z}/n\mathbb{Z})^3.$$

Tout diviseur premier p de n est tel que le groupe de décomposition de l'idéal premier $\mathfrak{p} = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times p\mathbb{Z}/n\mathbb{Z}$ est $\mathcal{G}^{\mathrm{Z}}(\mathfrak{p}) = \langle (1\ 2) \rangle$ engendré par la transposition (1 2). On vérifie également que le groupe d'inertie de $\mathfrak{p}$ est $\mathcal{G}^{\mathrm{T}}(\mathfrak{p}) = \langle (1\ 2) \rangle$.

Proposition 2.4. — *1. Soient S un anneau commutatif et $\mathcal{G}$ un groupe fini agissant sur S. Alors S est entier sur son sous-anneau $S^{\mathcal{G}}$ des éléments invariants par $\mathcal{G}$.*

2. *Soient S un anneau commutatif et $\mathcal{G}$ un groupe fini agissant sur S. Soit $\mathfrak{p}$ un idéal premier de l'anneau $S^{\mathcal{G}}$ des invariants de S par $\mathcal{G}$. On note $\mathcal{E}_{\mathfrak{p}}$ l'ensemble des idéaux premiers $\mathfrak{P}$ de S tels que $\mathfrak{P} \cap S^{\mathcal{G}} = \mathfrak{p}$. Alors $\mathcal{G}$ agit transitivement sur $\mathcal{E}_{\mathfrak{p}}$, autrement dit pour tout couple d'idéaux premiers $(\mathfrak{P}, \mathfrak{Q}) \in \mathcal{E}_{\mathfrak{p}}^2$ il exite un élément $\sigma \in \mathcal{G}$ tel que $\mathfrak{P} = \sigma.\mathfrak{Q}$.*
3. *Soient $(S, \mathcal{G})$ une extension galoisienne d'un anneau commutatif R, et $\mathfrak{p}$ un idéal premier de R. Alors le groupe d'inertie $\mathcal{G}^{\mathrm{T}}(\mathfrak{p})$ est trivial.*

Démonstration. — [**6**], chapitre V, paragraphe 1, numéro 9, proposition 22 pour l'assertion (1). L'assertion (2) vient de [**6**], chapitre V, paragraphe 2, numéro 2, théorème 2. L'assertion (3) est une appplication immédiate de l'assertion 3(b) de la définition 1.3. □

2.3. Extensions cycliques de $\mathbb{Z}/n\mathbb{Z}$. — Soient $n > 1$ un entier naturel et p un diviseur premier de n. Soit $(S, \langle\sigma\rangle)$ une extension galoisienne de $R = \mathbb{Z}/n\mathbb{Z}$ de degré d. Le R-automorphisme $\sigma : S \to S$ induit un $\mathbf{F}_p$-automorphisme de $\mathbf{L} = S/pS$ que nous notons également σ. On pose $\mathcal{G} = \langle\sigma\rangle$. D'après l'assertion (2) de la propostion 1.7, $(\mathbf{L}, \mathcal{G})$ est une extension galoisienne de $\mathbf{F}_p$. Donc la $\mathbf{F}_p$-algèbre $\mathbf{L}^{\mathcal{G}}$ des éléments de $\mathbf{L}$ invariants par l'action de σ est égale à $\mathbf{F}_p$. D'après la proposition 2.4, l'anneau $\mathbf{L}$ est entier sur $\mathbf{F}_p$ et l'automorphisme σ agit transitivement sur $\mathrm{Spec}(\mathbf{L})$. L'anneau $\mathbf{L}$ est artinien (voir l'étude faite à la fin de la section 2.1). Il admet donc un nombre fini m d'idéaux premiers ([**3**], Proposition 8.3). Ces idéaux premiers ont un groupe de décomposition commun que nous notons $\mathcal{G}^{\mathrm{Z}}$. Soit $\mathcal{G}^{\mathrm{T}}$ leur groupe d'inertie commun, on note f l'ordre du quotient $\mathcal{G}^{\mathrm{Z}}/\mathcal{G}^{\mathrm{T}}$. La dimension d du $\mathbf{F}_p$-espace vectoriel $\mathbf{L}$ vérifie $d = fm$, car le groupe d'inertie $\mathcal{G}^{\mathrm{T}}$ est trivial. Soient $\mathfrak{p}_0, \mathfrak{p}_1 \ldots, \mathfrak{p}_{m-1}$ les idéaux premiers de $\mathbf{L}$. Pour $i \in \{0, 1, \ldots, m-1\}$, le groupe des $\mathbf{F}_p$-automorphismes du corps résiduel $\mathbf{M}_i = \mathbf{L}/\mathfrak{p}_i$ est isomorphe au quotient $\mathcal{G}^{\mathrm{Z}}/\mathcal{G}^{\mathrm{T}}$ ([**6**], chapitre V, paragraphe 2, numéro 2, théorème 2). Les extensions $\mathbf{M}_i$ de $\mathbf{F}_p$ sont galoisiennes de degré f. L'automorphisme de Frobenius de $\mathbf{M}_i$ défini par

$$\begin{aligned} \mathrm{Frob}_p \quad : \qquad & \mathbf{M}_i \longrightarrow \mathbf{M}_i \\ & x \longmapsto x^p \end{aligned}$$

est la réduction modulo $\mathfrak{p}_i$ d'un générateur de $\mathcal{G}^Z$, c'est-à-dire une puissance $\sigma^{z_i m}$ de σ telle que z_i est un entier premier à f. En particulier pour $i = 0$, on a

$$\sigma^{z_0 m}(a) = a^p \bmod \mathfrak{p}_0 \tag{2}$$

pour tout élément a de $\mathbf{L}$. En faisant agir σ sur l'équation (2), on obtient $z_0 = z_1 = \cdots = z_{m-1}$, car σ agit transitivement sur le spectre de $\mathbf{L}$. Donc il existe un entier z premier à f tel que pour tout x de $\mathbf{L}$, on a $x^p = \sigma^{zm}(x)$.

Proposition 2.5. — *Soit $n > 1$ un entier naturel. Soit $(S, \langle\sigma\rangle)$ une extension galoisienne de $\mathbb{Z}/n\mathbb{Z}$. Soit p un diviseur premier de n. On pose $\mathbf{L} = S/pS$ et on note encore σ le $\mathbf{F}_p$-automorphisme de $\mathbf{L}$ induit par σ. Alors il existe un entier naturel z premier au degré résiduel f tel que pour tout x dans $\mathbf{L}$, on a : $x^p = \sigma^{zm}(x)$.*

3. Primalité et pseudo-primalité avec les extensions galoisiennes

Dans cette section nous décrivons un test de primalité et un test de pseudo-primalité qui utilisent chacun une extension cyclique de l'anneau $\mathbb{Z}/n\mathbb{Z}$, où n est l'entier dont on veut étudier la primalité.

3.1. Le test de primalité APRCL. —

3.1.1. Le critère. — Au début des années 80 Adleman, Pomerance, Rumely ont publié le test de primalité APR qui a ensuite été amélioré par Cohen et Lenstra. Cela a donné lieu au test APRCL. C'est l'un des tests de primalité les plus puissants utilisés en pratique. Voici une formulation du critère APRCL qui fait intervenir les extensions galoisiennes.

***Théorème 5* (Critère APRCL).** — *Soit $n \geq 3$ un entier impair, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Soit $(S, \langle\sigma\rangle)$ une extension galoisienne de degré d de R. Supposons qu'il existe une unité $a \in S^*$ d'ordre exact $s \geq \sqrt{n}+1$ telle que $\sigma(a) = a^n$. On pose $r_i = n^i \bmod s$ pour tout $0 \leq i < d$, où $0 < r_i < s$. Si*

$$\text{pour tout } 0 \leq i < d, \text{ on a } r_i = n \text{ ou } \gcd(r_i, n) = 1, \tag{3}$$

alors n est un nombre premier.

Démonstration. — Supposons que n est un entier composé. Alors il admet un diviseur premier p tel que $p \leq \sqrt{n} < s$. D'après la proposition 2.5, il exite un entier $u \in [0, d[$ tel que $a^p = \sigma^u(a) = a^{n^u} \in (S/pS)^*$. Donc

$$p \equiv n^u \bmod s, \tag{4}$$

car la classe de a dans $(S/pS)^*$ est d'ordre s. Puisque σ est d'ordre d, on a $n^d \equiv 1 \bmod s$. Donc l'ordre du sous-groupe de $(\mathbb{Z}/s\mathbb{Z})^*$ engendré par n divise d. L'entier u vérifie $0 \leq u < d$. De plus $p < s$. Donc l'équation (4) implique que p est égal à l'un des r_i. La condition (3) du théorème mène à une contradiction. □

Cette version du critère APRCL exige de construire une extension galoisienne de $R = \mathbb{Z}/n\mathbb{Z}$ telle qu'il existe un élément inversible $a \in S^*$ d'ordre exact $s \geq \sqrt{n}+1$. C'est une situation semblable à celle du test de Pocklington-Lehmer, mais ici il y a un avantage : on a le choix du degré d de S sur R. Il faut chercher d tel que $n^d - 1$ ait un diviseur $s \geq \sqrt{n}+1$ facilement factorisable. Le théorème suivant montre qu'un tel entier d existe.

***Théorème 6* (Pomerance et Odlyzko).** — *Il existe une constante positive Θ telle que pour tout entier $n \geq \Theta$, il existe un entier $d \leq (\log n)^{\Theta \log\log\log n}$ tel que $n^d - 1$ a un facteur $s > \sqrt{n}$ dont les diviseurs premiers q vérifient $q \leq d+1$.*

Démonstration. — Pour tout entier naturel x, on note $f(x)$ le plus petit entier strictement positif sans facteur carré tel que le produit des nombres premiers q, pour lesquels $q-1$ divise $f(x)$, est strictement plus grand que $\sqrt{x}$. D'après ([**1**], page 196, théorème 3), il existe une constante absolue $c_4 > 0$ telle que pour tout $x > 100$, on a :

$$f(x) < (\log x)^{c_4 \log\log\log x}.$$

Donc $f(n^4) < (4\log n)^{c_4 \log\log(4\log n)} \leq (\log n)^{c_5 \log\log\log n}$, pourvu que n soit assez grand. Ainsi il existe une constante Θ telle que pour tout $n \geq \Theta$, on a $f(n^4) < (\log n)^{\Theta \log\log\log n}$. On rappelle que le produit des nombres premiers q divisant n est au plus égal à n. Donc si $d = f(n^4)$, alors le produit des nombres premiers q, tels que $q-1$ divise d et $\operatorname{pgcd}(n,q) = 1$, est strictement plus grand que $\frac{\sqrt{n^4}}{n} > \sqrt{n}$. Mais $\operatorname{pgcd}(n,q) = 1$ signifie que la classe de n est inversible dans $\mathbb{Z}/q\mathbb{Z}$, c'est-à-dire que $n^{q-1} \equiv 1 \bmod q$. Donc le produit des nombres premiers q, tels que $q-1$ divise d et $\operatorname{pgcd}(n,q) = 1$, est un diviseur de $n^d - 1$ plus grand que $\sqrt{n}$. □

3.1.2. L'algorithme. — Soit $n \geq 3$ un entier impair. On peut décrire une version simple de l'algorithme APRCL en quatre étapes :

1. Construire une extension galoisienne $(S, \langle\sigma\rangle)$ de rang d sur $R = \mathbb{Z}/n\mathbb{Z}$. L'entier n a validé plusieurs tests Miller-Rabin, il est très certainement premier. On peut donc utiliser les algorithmes de construction des extensions de corps finis.

   (a) On commence par chercher un petit entier d tel que $n^d - 1$ ait plusieurs petits diviseurs. Cela permet de choisir l'ordre $s > \sqrt{n}$ de l'unité $a \in S^*$ qu'il faudra trouver à l'étape (3). D'après le théorème 6, on peut toujours trouver un petit entier d convenable.

   (b) Déterminer un polynôme $f(x)$ (irréductible si n est premier) unitaire de degré d tel que $x^{n^i} - x$ est une unité dans $S = R[x]/f(x)$ pour $1 \leq i \leq \frac{d}{2}$.

   (c) Ensuite on considère l'endomorphisme de R-modules $\sigma : S \to S$ défini par $\sigma(x^i) = x^{ni} \bmod f(x)$, pour $0 \leq i \leq d-1$. Soit M la matrice de σ dans la R-base $(1, x, \ldots, x^{d-1})$ de S. On s'assure que σ est un endomorphisme d'algèbres, en vérifiant que $\sigma(x^i \bmod f(x)) = x^{ni} \bmod f(x)$ pour $d \leq i \leq 2d-2$. Ensuite on vérifie que σ est d'ordre d en examinant l'égalité $x^{n^d} - x = 0$ dans S. On vérifie également que $S^\sigma = R$, en utilisant la matrice M.

   (d) Enfin, on choisit arbitrairement un élément u dans S et on vérifie que $\sigma^i(u) - u$ est une unité pour $1 \leq i \leq d-1$. Si n premier, la densité de tels u dans $S = \mathbf{F}_{n^d}$ est au moins égale à $\frac{1}{2}$. En effet, dire que $\sigma^i(u) - u$ n'est pas inversible dans $\mathbf{F}_{n^d}$ (pour au moins un i) signifie que u appartient à un sous-corps strict de $\mathbf{F}_{n^d}$. Donc tout générateur u de $\mathbf{F}_{n^d}$ est tel que $\sigma^i(u) - u$ est inversible dans $\mathbf{F}_{n^d}$. D'après [**11**], section 7, page 17, lemme 4, la densité de générateurs dans $\mathbf{F}_{n^d}$ est au moins égale à $\frac{1}{2}$.

2. Déterminer une unité a de S d'ordre exact s, en utilisant la méthode de l'étape (2) de l'algorithme de Pocklington-Lehmer que nous avons décrit dans l'introduction. Puis vérifier que $\sigma(a) = a^n$.

3. Pour $0 \leq i < d$, poser $r_i = n^i \bmod s$. Vérifier que $r_i = n$ ou $\gcd(r_i, n) = 1$.

Si n valide toutes les étapes, alors on conclut qu'il est premier d'après le théorème 5.

Remarque 3.1. —
1. Puisque d est petit, le nombre de $\gcd(n, r_i)$ à calculer est négligeable.
2. La version du test APRCL utilisée en pratique est probabiliste ([**8**], algorithme 9.1.28). Elle est très efficace ([**9**], sections 25.2.2 et 25.2.4). Son temps de calcul est $O((\log n)^{c \log\log\log n})$ opérations élémentaires, où c est une constante réelle positive.

3.1.3. Un exemple. — Nous montrons que $n = 1801$ est premier en utilisant l'algorithme APRCL.
Une recherche rapide du degré d, parmi les petits entiers k tels que les facteurs premiers d'un diviseur s de $n^k - 1$ soient petits, nous donne $d = 4$ et $s = 2^4 \times 3 \times 5$. En effet $n^4 - 1 = s \times 43837281030$.

Le polynôme $f(x) = x^4+x+1$ est tel que x^n-x et $x^{n^2}-x$ sont inversibles dans $S = R[x]/f(x)$. Soit $\sigma : S \to S$ l'endomorphisme de R-modules défini par

$$\sigma(x^i) = x^{ni} \bmod f(x) \text{ pour } i \in \{0,1,2,3\}.$$

On vérifie que

$$\sigma(x^i) = x^{ni} \bmod f(x) \text{ pour } i \in \{4,5,6\}.$$

Donc σ est un morphisme de R-algèbres. On vérifie aussi que $x^{n^d} = x$. Donc σ est d'ordre d. La matrice

$$M = \begin{pmatrix} 0 & 428 & 893 & 138 \\ 0 & 622 & 986 & 1664 \\ 0 & 1396 & 529 & 1558 \\ 0 & 1171 & 1791 & 640 \end{pmatrix}$$

du R-endomorphisme $\sigma - \mathrm{Id}_S$ dans la base $(1, x, x^2, x^3)$ est de rang 3. Donc $\mathrm{Ker}(\sigma - \mathrm{Id}_S) = R$, c'est-à-dire que $S^{\mathcal{G}} = R$.
On a vu au début de l'exemple que $x^n - x$ et $x^{n^2} - x$ sont inversibles dans S. Il en est de même pour $x^{n^3} - x$. Donc les $\sigma^i(x) - x$ sont inversibles dans S pour $1 \leq i \leq 3$.
L'élément $a = (7+x)^{\frac{n^d-1}{s}} \in S$ est d'ordre exact s, car $a^s = 1$, $a^{\frac{s}{2}} - 1 = -2$, $a^{\frac{s}{3}} - 1 = 1726$, $a^{\frac{s}{5}} - 1 = 349$ et les classes de -2, 1726, 349 sont inversibles modulo n. On détermine les éléments $r_i = n^i \bmod s$ du sous-groupe de $(\mathbb{Z}/s\mathbb{Z})^*$ engendré par la classe de n. Cela donne

$$r_0 = 1 \bmod s,\ r_1 = 121 \bmod s,\ r_2 = 1 \bmod s, \quad \text{et} \quad r_3 = 121 \bmod s.$$

On vérifie que $\gcd(r_i, n) = 1$ pour tout i. D'après le théorème 5, l'entier n est premier.
Notons que le test APRCL est utilisé en pratique pour étudier la primalité d'entiers beaucoup plus intéressants que $n = 1801$. L'option $flag = 2$ de la fonction **`isprime`** du système de calcul formel PARI/GP utilise une implémentation du test APRCL ([**18**], page 83). On a la confirmation que l'entier $n = 2^{1024} + 643$ est premier en moins de 4 secondes (3,228 secondes pour être précis) sur une architecture Intel Core i7 à 2.90 GHz.

3.2. Le test de Galois. — C'est un test de pseudo-primalité ([**10**], sections 1 et 2) qui repose sur la généralisation du petit théorème de Fermat suivante :

Théorème 7. — *Soit $n \geq 2$ un entier, on pose $R = \mathbb{Z}/n\mathbb{Z}$. Soit $S \supset R$ une R-algèbre commutative fidèle libre de rang fini. Soit σ un R-endomorphisme de S. Soit $\Omega \subset S$ un sous-ensemble de S tel que la plus petite sous R-algèbre de S contenant Ω et stable par σ est encore S. Supposons que $\sigma(\omega) = \omega^n$ pour tout $\omega \in \Omega$. Si n est premier, alors pour tout x dans S on a : $\sigma(x) = x^n$.*

Démonstration. — Soit T l'ensemble des solutions dans S de l'équation $x^n = \sigma(x)$. Le sous-ensemble Ω de S est contenu dans T, et $\sigma(T) \subset T$. Si n est premier, alors T est stable par addition et multiplication, et R est contenu dans T. Donc $T = S$. □

En pratique l'algèbre S est telle que $(S, \langle\sigma\rangle)$ est une extension galoisienne de l'anneau $R = \mathbb{Z}/n\mathbb{Z}$ (l'étape 1 de l'algorithme décrit à la section 3.1.2 explique comment construire une telle

extension). L'ensemble des témoins pour le test de Galois est égal au groupe S^* des unités de l'anneau S. L'application associée

$$P_n : S^* \longrightarrow \{\text{premier, composé}\}$$

est définie par : $P_n(x) =$ premier si et seulement si $\sigma(x) = x^n$. Si n est premier, alors il n'y a que de bons témoins conformément au théorème 7. Lorsque n est composé, les mauvais témoins sont les inversibles $x \in S^*$ tels que $\sigma(x) = x^n$. Le test de Galois coûte $d^{1+\epsilon(d)}$ fois plus cher qu'un test de Miller-Rabin (d est le degré de S sur R). Dans certains cas, ce test apporte la même sécurité que $O(\log n)$ tests Miller-Rabin. Le résultat suivant donne une majoration de la proportion de faux témoins.

Théorème 8. — *Soient $A > 2$ et $B \geq 3$ deux nombres réels. Soit $n \geq 3$ un entier. Supposons que tout diviseur premier de n est plus grand ou égal à B. On pose $R = \mathbb{Z}/n\mathbb{Z}$. Supposons que n n'est pas une puissance d'un nombre premier. Soit $(S, \langle\sigma\rangle)$ une extension galoisienne de R de rang d. Supposons que p est un nombre premier tel que p^v divise n et*

$$v \log p > \frac{A \log n}{d}. \tag{5}$$

Alors la densité

$$\mu_S = \frac{\#\{x \in S^* | \sigma(x) = x^n\}}{\#S^*}$$

de faux témoins parmi les unités de S est telle que

$$\mu_S \leq p^{-\frac{vd}{2}(1-\frac{2}{A}-\frac{4}{B})} \leq n^{-\frac{A}{2}(1-\frac{2}{A}-\frac{4}{B})}.$$

Démonstration. — [**10**], section 2.4. □

Le test de Galois est donc fiable lorsqu'il existe un nombre premier p et un entier naturel v tels que p^v est un grand diviseur de n. Le temps de calcul de l'exponentiation x^n est $d^{1+\epsilon(d)}(\log n)^{2+\epsilon(n)}$ opérations élémentaires. D'autre part, un entier n ayant beaucoup de diviseurs premiers sera rapidement détecté par une série raisonnable de tests de Miller-Rabin. En effet, la probabilité que n valide k tests de Miller-Rabin indépendants est au plus égale à $2^{-k(t-1)}$, où t est le nombre de diviseurs premiers de n. Le temps de calcul des k tests de Miller-Rabin est $k(\log n)^{2+\epsilon(n)}$.
Un test de pseudo-primalité très efficace, qui combine un test de Galois avec une série raisonnable de tests de Miller-Rabin, et qui exploite chacune des situations que nous venons de décrire est construit à la section 3 de [**10**]. Une implémentation de ce test, sur MAGMA V2.18-2, est disponible sur la page internet de Reynald Lercier.

4. L'algorithme AKS et ses variantes

Dans cette section, nous présentons le test de primalité déterministe AKS proposé par Agrawal, Kayal et Saxena en août 2002. Ces trois auteurs utilisent une $\mathbb{Z}/n\mathbb{Z}$-algèbre commutative libre S de rang fini obtenue en ajoutant une racine de l'unité. Lenstra et Pomerance d'une part, Berrizbeitia et Bernstein d'autre part ont introduit deux variantes galoisiennes de cet algorithme, l'une déterministe, l'autre probabiliste.

4.1. Le test AKS. — Pour tout nombre premier r, on note

$$\Phi_r(X) = X^{r-1} + X^{r-2} + \ldots + X + 1$$

le r-ième polynôme cyclotomique.

***Théorème 9* (Critère AKS).** — *Soient n un entier naturel impair et r un nombre premier. On pose $R = \mathbb{Z}/n\mathbb{Z}$. Supposons que*

1. *Aucun des nombres premiers $q \leq r$ ne divise n ;*
2. *Pour tout $1 \leq i \leq (\log n/\log 2)^2$, r ne divise pas $n^i - 1$;*
3. *Pour tout $0 \leq j < r$, on a $(X+j)^n = X^n + j$, dans $A = R[X]/\Phi_r(X)$.*

Alors n est une puissance d'un nombre premier.

Démonstration. — Section 3 de [**17**]. □

Le théorème 9 donne lieu à l'algorithme suivant :

***Algorithme 4.1* (Agrawal, Kayal et Saxena).** — *Soit $n \geq 3$ un entier naturel. On pose $R = \mathbb{Z}/n\mathbb{Z}$.*

1. *Vérifier que n n'est pas une puissance propre d'un entier.*
2. *a. Déterminer le plus petit nombre premier r ne divisant pas n ni aucun des $n^i - 1$ pour $0 \leq i \leq (\log n/\log 2)^2$.*
   b. Puis vérifier que n n'est divisible par aucun des nombres premiers $q \leq r$.
3. *Vérifier que $(X+j)^n = X^n + j$ dans $A = R[X]/\Phi_r(X)$, pour $0 \leq j \leq r-1$.*

Si n ne passe pas les tests, il est composé. Et s'il les passe tous, il est premier.

***Remarque 4.2*.** —
1. D'après la condition (ii) du théorème 9, le nombre premier r est tel que $r \geq (\log n/\log 2)^2$. Une étude attentive ([**17**], section 3) nous dit que la taille maximale de r est $= O((\log n)^5)$.
2. L'algorithme AKS requiert $(\log n)^{12+\epsilon(n)}$ opérations élémentaires. L'étape 3 est la plus coûteuse. Il s'agit de vérifier un nombre important de congruences dans le gros anneau $A = R[X]/\Phi_r(X)$ (c'est un R-module libre de rang $O((\log n)^5)$).
3. L'algorithme AKS est lent en pratique.

4.2. Les variantes. — Pour améliorer le test AKS, Lenstra et Pomerance proposent dans [**14**] de remplacer $A = R[X]/\Phi_r(X)$ par un anneau plus petit $S = R[X]/f(X)$, où $f(X)$ est un polynôme unitaire de degré $d = O((\log n)^2)$. Ils obtiennent le meilleur algorithme déterministe de preuve de primalité, avec un temps de calcul égal à $O((\log n)^{6+\epsilon(n)})$ opérations élémentaires.
L'idée de Berrizbeitia, reprise et généralisée par Bernstein, est de réduire la quantité de calcul en faisant agir un groupe $\mathcal{G}$ de R-automorphismes de S sur les identités $(X+j)^n = X^n + j$. Ainsi, la vérification d'une seule de ces identités en valide $\#\mathcal{G}$ d'un coup. L'extension S utilisée par Berrizbeitia et Bernstein est de type Kummer. Malheureusement la construction d'une telle extension est probabiliste : on cherche un générateur d'un quotient donné de R^*.
Notons enfin qu'il existe d'autres méthodes pour étudier la primalité d'un entier. Le test ECPP (Elliptic Curve Primality Proving) d'Atkin-Morin [**4**] repose sur un critère similaire

au théorème de Pocklington. L'unité $a \in S^*$ est remplacée par une section d'une courbe elliptique sur R.

Références

[1] L. M. Adleman, C. Pomerance et R. S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math. (2)*, 117(1) :173–206, 1983.

[2] W. R. Alford, A. Granville et C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3) :703–722, 1994.

[3] M. F. Atiyah et I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[4] A. O. L. Atkin et F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203) :29–68, 1993.

[5] N. Bourbaki. *Éléments de mathématique. Fascicule XXVII. Algèbre commutative. Chapitre 1 : Modules plats. Chapitre 2 : Localisation*. Actualités Scientifiques et Industrielles, No. 1290. Herman, Paris, 1961.

[6] N. Bourbaki. *Éléments de mathématique. Fasc. XXX. Algèbre commutative. Chapitre 5 : Entiers. Chapitre 6 : Valuations*. Actualités Scientifiques et Industrielles, No. 1308. Hermann, Paris, 1964.

[7] S. U. Chase, D. K. Harrison et A. Rosenberg. Galois theory and Galois cohomology of commutative rings. *Mem. Amer. Math. Soc. No.*, 52 :15–33, 1965.

[8] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[9] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen et F. Vercauteren, éditeurs. *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[10] J. -M. Couveignes, T. Ezome et R. Lercier. A faster pseudo-primality test. *Rend. Circ. Mat. Palermo (2)*, 61(2) :261–278, 2012.

[11] J. M Couveignes et R. Lercier. Fast construction of irreducible polynomials over finite fields. *To appear in Israel J. Math.* Available from `http://arxiv.org/abs/0905.1642`.

[12] F. DeMeyer et E. Ingraham. *Separable algebras over commutative rings*. Lecture Notes in Mathematics, Vol. 181. Springer-Verlag, Berlin, 1971.

[13] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[14] H. W. Lenstra et C. Pomerance. Primality testing with gaussian periods. Available from `http://math.dartmouth.edu/~carlp/PDF/complexity12.pdf`.

[15] C. H. Papadimitriou. *Computational complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.

[16] P. Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[17] R. Schoof. Four primality testing algorithms. In *Algorithmic number theory : lattices, number fields, curves and cryptography*, Math. Sci. Res. Inst. Publ., pages 101–126. Cambridge Univ. Press, Cambridge, 2008.

[18] The PARI Group, Bordeaux. *PARI/GP, Version 2.3.3*, 2006. Available from `http://pari.math.u-bordeaux.fr/`.

[19] J. von zur Gathen et J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.

---

30 décembre 2012

Tony Ezome, Université des Sciences et Techniques de Masuku, Faculté des Sciences, Département de mathématiques et informatique, BP 943 Franceville, Gabon • *E-mail :* latonyo2000@yahoo.fr