Réductibilité dans $\mathbb{Z}$

Les congruences suivantes justifient trois tests de réductibilité historiquement importants :

Théorème 1. *Si $N > 2$ est premier et $0 < a < N$, alors les égalités suivantes sont vérifiées dans $\mathbb{Z}/N\mathbb{Z}$:*

(1) $a^{N-1} = 1$,
(2) $a^{(N-1)/2} = \left(\frac{a}{N}\right) \neq 0$,
(3) *Écrivons $N - 1 = 2^e q$, avec q impair et $e \geqslant 1$, et posons $b := a^q$. Alors $b = 1$ ou il existe un unique $0 \leqslant i < e$ tel que $b^{2^i} = -1$ (ou exclusif).*

Preuve. (1) est le petit théorème de Fermat et (2) est une propriété du symbole de Legendre. La condition $\left(\frac{a}{N}\right) \neq 0$ est toujours satisfaite lorsque N est premier, mais nous en aurons besoin pour un N quelconque par la suite. La dernière congruence découle de l'égalité polynomiale suivante, évaluée en $X = b$:

$$X^{2^e} - 1 = (X - 1)(X + 1)(X^2 + 1) \dots (X^{2^{e-1}} + 1)$$

(on la démontre directement ou comme une propriété des polynômes cyclotomiques $X^{2^e} - 1 = \prod_{d|2^e} \Phi_d$). Le membre de gauche est nul d'après Fermat, donc l'un des facteurs du membre de droite est nul puisqu'on a supposé N premier, donc $\mathbb{Z}/N\mathbb{Z}$ intègre. L'indice i est unique : partons du plus petit d'entre eux, les b^{2^j}, $j > i$, s'obtiennent par élévations au carré successives, donc valent tous 1.

Cette dernière idée fournit une preuve plus éclairante : d'après Fermat, $a^{N-1} = 1 = b^{2^e}$. Dans un corps de caractéristique différente de 2, l'équation $X^2 = 1$ a exactement deux solutions, -1 et 1. Comme on obtient 1 à partir de b par une suite d'élévations au carré, soit tous les b^{2^i} valent 1, soit on rencontre -1 en cours de route (une seule fois). □

Ces congruences fournissent trois tests de réductibilité probabilistes : on tire un entier $0 < a < N$ au hasard et l'on vérifie l'une des conditions (1), (2) ou (3) ci-dessus, ce qui donne respectivement les tests de Fermat (1640), de Solovay-Strassen (1977) et de Rabin-Miller (1980). Pour ce dernier, Miller (1976) a conçu un test déterministe conditionnel (dépendant d'une hypothèse de Riemann convenable), que Rabin a modifié en 1980 pour obtenir le test probabiliste ci-dessus. En détail :

Algorithme 1. Test de réductibilité de Solovay-Strassen

Entrées: N un entier impair, $a \in \mathbb{Z}/N\mathbb{Z}$, $a \neq 0$.
Sorties: $SS(a) =$ `Composé` ou `Échec`

1: Si $\left(\frac{a}{N}\right) = a^{(N-1)/2}$ (symbole de Jacobi, on ne sait pas si N est premier), renvoyer `Échec`.
2: Renvoyer `Composé`.

Algorithme 2. Test de réductibilité de Rabin-Miller

Entrées: N un entier impair, $a \in \mathbb{Z}/N\mathbb{Z}$, $a \neq 0$.
Sorties: $RM(a) =$ `Composé` ou `Échec`
1: Écrire $N - 1 = 2^e q$, avec q impair.
2: Calculer $b = a^q$.
3: Si $b = 1$ ou si $b^{2^i} = -1$ pour un certain $i = 0, \ldots, e-1$, renvoyer `Échec`.
4: Renvoyer `Composé`.

Théorème 2. *Les trois tests de réductibilité s'exécutent en temps* $\widetilde{O}(\log N)^2$.

Preuve. C'est évident pour Fermat et facile pour Rabin-Miller (il faut $O(\log q + e) = O(\log N)$ multiplications dans $\mathbb{Z}/N\mathbb{Z}$). C'est plus délicat pour Solovay-Strassen : la partie exponentiation est de nouveau facile, mais il faut adapter la preuve de complexité de l'algorithme d'Euclide au calcul du symbole de Jacobi $\left(\frac{a}{N}\right)$ à l'aide de la loi de réciprocité quadratique. □

Définition 3. Un a tel que $SS(a)$ ou $RM(a)$ renvoie `Composé` est appelé un *témoin* (de réductibilité, pour le test en question). Si N est composé, un a tel que ces tests renvoient `Échec` est appelé un *menteur*.

Notons qu'un témoin atteste que N est composé, mais fournit une preuve indirecte : aucun facteur explicite n'est exhibé.

Théorème 4. *Soit $N > 2$ un entier impair, et $0 < a < N$ un entier. Considérons à nouveau les congruences du théorème 1. Alors (3) implique (2), qui implique (1).*

Preuve. (1) découle de (2) élevée au carré : puisque l'on impose $\left(\frac{a}{N}\right) \neq 0$ dans (2), le symbole de Jacobi vaut ± 1. Montrons maintenant (3) $\Rightarrow$ (2), qui est étonnamment délicat. Dans la suite p désigne toujours un diviseur premier de N. Les propriétés des groupes multiplicatifs $(\mathbb{Z}/N\mathbb{Z})^*$ et $(\mathbb{Z}/p\mathbb{Z})^*$ ainsi que de leurs 2-Sylow vont être la clé de la démonstration. Pour k entier, on note ord_k l'ordre dans le groupe multiplicatif $(\mathbb{Z}/k\mathbb{Z})^*$. Pour tout $p \mid N$ premier, écrivons $p - 1 = 2^{e_p} q_p$, avec q_p impair.

Notons que (3) $\Rightarrow$ (1) est de nouveau évident par élévations au carré, ce qui implique déjà $a \in (\mathbb{Z}/N\mathbb{Z})^*$ et $\left(\frac{a}{N}\right) = \pm 1$. Comme $b^{2^e} = 1$ dans $(\mathbb{Z}/N\mathbb{Z})^*$ ainsi que dans les $(\mathbb{Z}/p\mathbb{Z})^*$, l'ordre de b divise 2^e dans tous ces groupes ; il est caractérisé par sa valuation 2-adique.

★ Étude des valuations :

Lemme 5. *Pour tout $p \mid N$, $ord_p(a)$ et $ord_p(b)$ ont la même valuation 2-adique.*

Preuve. Écrivons $\mathrm{ord}_p(a) = 2^{\alpha_p} m_p$ avec m_p impair. Comme q est impair, $\gcd(\mathrm{ord}_p(a), q) = \gcd(m_p, q)$, d'où

$$\mathrm{ord}_p(b) = \frac{\mathrm{ord}_p(a)}{\mathrm{pgcd}(\mathrm{ord}_p(a), q)} = 2^{\alpha_p} \cdot \frac{m_p}{\mathrm{pgcd}(m_p, q)},$$

et le second facteur est impair. □

Lemme 6. *La condition (3) implique que les $\mathrm{ord}_p(b)$ sont tous égaux à un même 2^s, avec $s \leqslant e$. Dans ces conditions, on a égalité $s = e$ si et seulement si $a^{(N-1)/2} = b^{2^{e-1}} = -1$.*

Preuve. Remarquons que, si $b = 1$, on a $\mathrm{ord}_p(b) = 1$ et $s = 0 \leqslant e$. Sinon $b^{2^i} \equiv -1 \pmod p$ dit que $\mathrm{ord}_p(b) = 2^{i+1}$ (car $p \neq 2$) et $s = i + 1 \leqslant e$. Comme $e > 0$, l'égalite $s = e$ ne peut se produire que dans le deuxième cas, avec $i = e - 1$ ce qui est équivalent à $b^{2^{e-1}} \equiv -1 \pmod N$ par définition de i dans l'algorithme de Miller-Rabin. □

Remarque 7. Nous n'en aurons pas besoin mais, si on suppose de plus $a^{N-1} = 1$, alors la réciproque est vraie : la condition de Rabin-Miller devient *équivalente* à « les $v_2(\mathrm{ord}_p(b))$ sont tous égaux ». En effet, la condition $a^{N-1} = b^{2^e} = 1$ impose que les $\mathrm{ord}_{p^{f_p}}(b)$ divisent 2^e. Comme le noyau de la projection $(\mathbb{Z}/p^f\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ est un p-groupe, on a $\mathrm{ord}_{p^{f_p}}(b) = \mathrm{ord}_p(b)$ pour tout $p \mid N$. Ils sont tous égaux à 2^s par hypothèse et on conclut par lemme chinois que $b^{2^{s-1}} = -1$. Si on ne suppose plus $a^{N-1} = 1$, la réciproque devient fausse, par exemple $N = 9$, $a = b = 4$: il n'y a qu'un premier divisant N donc la condition sur les $\mathrm{ord}_p(b)$ est automatique, mais a n'est pas un menteur.

★ Intéressons nous maintenant aux symboles de Jacobi :

Lemme 8. *On a $\left(\frac{a}{N}\right) = \left(\frac{b}{N}\right)$. Si $a^{N-1} = 1$, on a $\left(\frac{b}{p}\right) = -1$ si et seulement si $\mathrm{ord}_p(b) = 2^{e_p}$.*

Preuve. Comme q est impair, on a $\left(\frac{a}{N}\right) = \left(\frac{a}{N}\right)^q = \left(\frac{b}{N}\right)$ par multiplicativité du symbole de Jacobi. On sait déjà que $\mathrm{ord}_p(b) \mid 2^{e_p}$ donc $b^{2^{e_p-1}} \equiv \pm 1 \pmod p$. Ainsi $\left(\frac{b}{p}\right) \equiv b^{2^{e_p-1}q_p} \equiv b^{2^{e_p-1}} \pmod p$ car q_p est impair. Finalement $\left(\frac{b}{p}\right) = -1$ si et seulement si $\mathrm{ord}_p(b) = 2^{e_p}$. □

Il suit des deux derniers lemmes que, si (3) est vraie (donc $a^{N-1} = 1$), alors $\left(\frac{b}{p}\right) = -1$ si et seulement si $e_p = s$. Finalement, $\left(\frac{a}{N}\right) = \left(\frac{b}{N}\right) = -1$ si et seulement si $\#\{p\colon e_p = s\}$ est impair (les p sont répétés avec leur multiplicité dans N).

★ Il reste à comprendre cette dernière condition. On écrit $N = \prod_p p$ où chaque p est répété selon sa multiplicité. On développe, en utilisant $s \leqslant e_p$:

$$\begin{aligned} N = \prod_p (1 + 2^{e_p} q_p) &\equiv 1 + 2^s \sum_{p\colon e_p = s} q_p \pmod{2^{s+1}} \\ &\equiv 1 + 2^s \#\{p\colon e_p = s\} \pmod{2^{s+1}}. \end{aligned}$$

Il en résulte que $s \leqslant e$ (ce qu'on savait déjà), avec égalité si et seulement si le terme $\#\{p\colon e_p = s\}$ est impair.

★ Finalement, $a^{(N-1)/2}$ et $\left(\frac{a}{N}\right)$, qui valent tous deux ± 1, sont égaux à -1 exactement si $s = e$. Ils sont donc égaux. □

Autrement dit, le test de Rabin-Miller est plus fort que celui de Solovay-Strassen, lui-même plus fort que celui de Fermat. Il est facile de trouver des contre-exemples explicites montrant que les implications réciproques ne sont pas vraies en général. Pour savoir si nos

tests sont bons, il nous faut maintenant démontrer que, pour tout N impair composé, il existe suffisamment de $0 < a < N$ qui ne vérifient pas (1), (2) ou (3).

Théorème 9. *Si $N > 1$ est composé, alors*

$$\left\{0 < a < N \colon a^{N-1} \equiv 1 \pmod{N}\right\}$$

est un sous-groupe de $(\mathbb{Z}/N\mathbb{Z})^*$. Il est égal au groupe $(\mathbb{Z}/N\mathbb{Z})^*$ tout entier si et seulement si N est sans facteur carré et $p \mid N \Rightarrow p-1 \mid N-1$ pour tout diviseur premier p de N.

Preuve. C'est clairement un sous-groupe. Supposons maintenant que $a^{N-1} \equiv 1 \pmod{N}$ pour tout a premier à N, et cette congruence vaut modulo tout diviseur premier p de N. Donc l'ordre de tout a dans $(\mathbb{Z}/p\mathbb{Z})^*$ divise $N-1$. En choisissant pour a une racine primitive (d'ordre $p-1$) dans $\mathbb{F}_p^*$, on obtient $p-1 \mid N-1$. Si de plus $p^2 \mid N$, alors en prenant a d'ordre $p(p-1)$ dans le groupe cyclique $(\mathbb{Z}/p^2\mathbb{Z})^*$, on obtient $p(p-1) \mid N-1$. Ceci contredit $p \mid N$ puisque $\operatorname{pgcd}(N, N-1) = 1$.

Pour la réciproque, la divisibilité implique $a^{N-1} \equiv 1 \pmod{p}$ pour $a \in (\mathbb{Z}/N\mathbb{Z})^*$ et tout premier $p \mid N$ (Fermat), et le lemme chinois montre la congruence modulo N (car N est sans facteur carré). □

Un composé N désagréable comme ci-dessus, qui ruine complètement le test de Fermat, est appelé un nombre de Carmichael. Ces nombres avaient en fait été définis et étudiés auparavant par Korselt (1899), qui ne mentionne aucun exemple. En 1910, Carmichael énonce un critère voisin et donne quatre tels nombres, dont les deux plus petits (561 et 1105). Remarquons que le critère de Korselt a une formulation plus générale : si un entier N sans facteur carré vérifie $p-1 \mid N-1$ pour chacun de ses diviseurs premiers, alors $a^N \equiv a \pmod{N}$ pour *tout* entier a (lemme chinois, le résultat étant évident si $p \mid a$).

Il n'y a pas d'équivalent des nombres de Carmichael pour le test de Solovay-Strassen, ni pour le test plus fort de Rabin-Miller :

Théorème 10. *Si $N > 1$ est impair et composé, alors*

$$\left\{0 < a < N \colon a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \neq 0 \pmod{N}\right\}$$

est un sous-groupe propre de $(\mathbb{Z}/N\mathbb{Z})^*$.

Preuve. C'est de nouveau clairement un sous-groupe par multiplicativité du symbole de Jacobi, et il faut prouver que ce n'est pas le groupe tout entier. Comme c'est un sous-groupe de celui considéré au théorème précédent, on peut supposer que N est un nombre de Carmichael (sinon le sous-groupe du théorème précédent est déjà propre), et il faut trouver un a n'appartenant pas à l'ensemble donné.

Si $p \mid N$ est un nombre premier impair, prenons a non carré modulo p et $a \equiv 1 \pmod{N/p}$, ce qui existe d'après le lemme chinois : comme N est sans facteur carré, on a $\operatorname{pgcd}(p, N/p) = 1$. Cela implique $\left(\frac{a}{N}\right) = -1$, mais $a^{(N-1)/2} \equiv -1 \pmod{N}$ est impossible puisque c'est faux modulo N/p. □

Corollaire 11. *Si N est un entier composé impair, un entier $0 < a < N$ choisi uniformément au hasard est un témoin pour Solovay-Strassen avec probabilité $\geqslant 1/2$.*

Preuve. L'indice d'un sous-groupe propre est au moins 2. □

Le résultat reste vrai pour Rabin-Miller puisque les menteurs pour ce test le sont aussi pour Solovay-Strassen. Cet argument rapide dit que les témoins sont relativement abondants. On a un résultat plus précis :

Théorème 12. (1) *Si $N = \prod p^{f_p}$, posons $\omega = \#\{p \mid N\}$,*

$$e_p = v_2(p-1), \quad E = \min_{p|N} e_p.$$

Alors le nombre de a tels que $RM(a)$ renvoie **`Échec`** *est exactement*

$$\prod_{p|N} \operatorname{pgcd}(q, p-1) \cdot \left(1 + \frac{2^{E\omega}-1}{2^\omega - 1}\right).$$

(2) *Si N est composé, un entier $0 < a < N$ choisi uniformément au hasard est un témoin avec probabilité $\geqslant 3/4$.*

Preuve. Un a tel que $RM(a)$ échoue appartient à $(\mathbb{Z}/N\mathbb{Z})^*$. D'après le lemme chinois, le groupe $(\mathbb{Z}/N\mathbb{Z})^*$ est isomorphe à $\prod_{p|N}(\mathbb{Z}/p^{f_p}\mathbb{Z})^*$. Chaque facteur est cyclique, de générateur g_p, et isomorphe à $(\mathbb{Z}/\varphi(p^{f_p})\mathbb{Z}, +)$, ce qui permet de linéariser les équations en recherchant a sous la forme $(g_p^{a_p})_{p|N}$. Rappelons que l'équation linéaire $ax \equiv b \pmod c$ n'a pas de solution si $\operatorname{pgcd}(a,c) \nmid b$ et en a $\operatorname{pgcd}(a,c)$ sinon.

Comptons donc les (a_p) dans le produit $\prod_{p|N} \mathbb{Z}/\varphi(p^{f_p})\mathbb{Z}$ tels que $RM(a)$ renvoie `Échec` :

$$\#\{(a_p) : qa_p = 0\} + \sum_{i=0}^{e-1} \#\left\{(a_p) : q2^i a_p = \varphi(p^{f_p})/2\right\};$$

ces ensembles sont disjoints et on a utilisé $-1 = g_p^{\varphi(p^{f_p})/2}$.

La congruence $qa_p = 0$ a $\operatorname{pgcd}(q, \varphi(p^{f_p})) = \operatorname{pgcd}(q, p-1)$ solutions. La congruence $q2^i a_p = (p-1)p^{f_p-1}/2$ n'a de solution que si $2^i \mid (p-1)/2$, c'est-à-dire $i \leqslant e_p - 1$, et elle en a $2^i \operatorname{pgcd}(q, p-1)$ dans ce cas. Le produit sur les $p \mid N$ donne

$$\#\{(a_p) : qa_p = 0\} = \prod_p \operatorname{pgcd}(q, p-1)$$

ainsi que, quand $i < e_p$ pour tout p c'est-à-dire $i < E$,

$$\#\left\{(a_p) : q2^i a_p = \varphi(p^{f_p})/2\right\} = 2^{i\omega} \prod_p \operatorname{pgcd}(q, p-1)$$

mais il vaut 0 si $i \geqslant E$. On remarque maintenant $E \leqslant e$ (un produit d'entiers $p \equiv 1 \pmod{2^E}$ est $\equiv 1 \pmod{2^E}$) et on obtient finalement

$$\left(1 + \sum_{i=0}^{E-1} 2^{i\omega}\right) \prod_p \operatorname{pgcd}(q, p-1) = \left(1 + \frac{2^{\omega E}-1}{2^\omega - 1}\right) \prod_p \operatorname{pgcd}(q, p-1)$$

et le premier résultat en découle. Le cas particulier $N = p$ (donc $\omega = 1$ et $E = e$), redémontre le point (3) du théorème 1 puisqu'on obtient $N - 1$ témoins. Mais nous en avons déjà vu deux preuves plus éclairantes.

Pour prouver le second point, notons que la proportion de témoins est

$$\frac{\prod_{p|N} \operatorname{pgcd}(q, p-1)}{N-1} \cdot \left(1 + \frac{2^{\omega E} - 1}{2^\omega - 1}\right).$$

Traitons d'abord le cas $\omega = 1 : N = p^f$, $f > 1$. Comme $\operatorname{pgcd}(q, p-1) \leqslant (p-1)/2^E$, cette proportion est majorée par

$$(p-1)/(p^f - 1) \leqslant 1/(p+1) \leqslant 1/4\,,$$

et le résultat suit. Supposons maintenant $\omega > 1$. Pour tout p, on a

$$\operatorname{pgcd}(q, p-1) \mid (p-1)/2^{e_p} \mid (p-1)/2^E$$

puis $\prod_p (p-1) \leqslant N - 1$: la proportion est donc inférieure à

$$2^{-\omega E}\left(1 + \frac{2^{\omega E} - 1}{2^\omega - 1}\right).$$

Pour ω fixé, c'est une fonction décroissante de E, qui vaut $2^{1-\omega}$ pour $E = 1$. D'où le résultat, sauf si $\omega = 2$, auquel cas on obtient seulement $1/2\ldots$

Revenons sur nos deux divisibilités initiales : si l'une d'entre elles est stricte, notre majoration peut être divisée par au moins 2 et on a gagné. On gagne aussi si N n'est pas sans facteur carré, cette fois à cause de $(\ell - 1)\prod_p (p-1) \leqslant N - 1$ si $\ell^2 \mid N$ (le premier ℓ se retrouve aussi parmi les p), et on gagne de nouveau un facteur $\ell - 1 \geqslant 2$.

Le seul mauvais cas restant est donc $\operatorname{pgcd}(q, p-1) = (p-1)/2^E$ pour chaque p (et les e_p égaux) soit $p - 1 \mid N - 1$ et N sans facteur carré : on retrouve la condition de Carmichael. Mais ce cas est impossible avec $\omega = 2$ car un nombre de Carmichael a au moins trois facteurs premiers distincts. En effet supposons $N = p_1 p_2$ de Carmichael avec $p_1 < p_2$: $N - 1$ est divisible par $p_2 - 1$ et congru à $p_1 - 1$ modulo $p_2 - 1$. Donc $p_2 - 1 \mid p_1 - 1$, en contradiction avec $p_1 < p_2$. □

Si N est un nombre de Carmichael dont les diviseurs premiers sont $\equiv 3 \pmod 4$, il y a exactement $\varphi(N)2^{1-\omega}$ menteurs, et on ne peut pas obtenir mieux que $1/4$ puisqu'on a égalité pour $\omega = 3$; c'est par exemple le cas pour 8911. En général, c'est très pessimiste : pour un grand N aléatoire, on s'attend à ce que $\operatorname{pgcd}(q, p-1)$ soit petit pour $p \mid N$; la proportion de menteurs est alors essentiellement majorée par $2^{(\omega-1)e}/q$, qui est petit. Plus précisément, on dispose du résultat *en moyenne* très fort suivant :

Théorème 13 (Burthe)**.** *Soit $t(N)$ le plus petit témoin de la réductibilité de N, c'est-à-dire le plus petit a tel que $RM(a)$ renvoie* `Composé` *; pour N premier, on pose $t(N) = 0$. La valeur moyenne de $t(N)$ sur les entiers impairs vaut 2 :*

$$\sum_{N<X,\ 2\nmid N} t(N) \sim 2 \sum_{N<X,\ 2\nmid N} 1 \sim X\,, \quad X \to +\infty.$$

Ce qui signifie que 2 est presque toujours un témoin fiable. Notons que, d'après le théorème des nombres premiers, la contribution des premiers au membre de droite est $O(X/\log X)$, donc négligeable. D'autre part, Alford-Granville-Pomerance (1994) ont montré qu'il existe une infinité de nombres de Carmichael et que $\limsup_{N\to\infty} t(N) = +\infty$.