# Construction de nombres pseudo-premiers de Perrin

Lionel Fourquaux

1er février 2017

## 1 Les nombres de Perrin

La suite de Perrin est définie par :

$$u_0 = 3 \quad u_1 = 0 \quad u_2 = 2$$
$$u_n = u_{n-2} + u_{n-3} \qquad (\forall n \geqslant 3).$$

Ses termes sont appelés les *nombres de Perrin*. Ce sont des entiers positifs, et $u_n \underset{n\to+\infty}{=} \rho^n + o(1)$, où $\rho = 1.32471795724...$ est l'unique racine réelle de $X^3 - X - 1$, appelée le *nombre plastique*.
Les premiers termes de la suite de Perrin sont :

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $u_n$ | 3 | 0 | 2 | 3 | 2 | 5 | 5 | 7 | 10 | 12 | 17 | 22 | 29 | 39 | 51 | 68 | 90 | 119 |

On remarque que pour $2 \leqslant n \leqslant 17$, l'entier $u_n$ est multiple de $n$ si et seulement si $n$ est premier.
On a en fait le théorème suivant.

**Théorème 1.1.** *Si $p$ est un nombre premier, alors $p \mid u_p$.*

*Démonstration.* Soit $k$ une extension de $\mathbb{F}_p$ où le polynôme $X^3 - X - 1$ est scindé. Soient $\alpha, \beta, \gamma \in k$ (pas forcément distincts) ses racines. Une récurrence facile montre que $u_n = \alpha^n + \beta^n + \gamma^n$ (dans $k$). On en déduit $u_p = u_1^p = 0$, i.e. $p \mid u_p$. □

La réciproque est en revanche fausse : pour $n = 271441 = 521^2$, on a $n \mid u_n$. Ce contre-exemple a été proposé par William Adams et Daniel Shanks en 1982 (doi:10.2307/2007637).

Un tel entier $n \geqslant 2$ non premier mais qui vérifie $n \mid u_n$ est appelé un *pseudo-premier de Perrin*. Une recherche exhaustive montre que les pseudo-premiers de Perrin compris entre 2 et $2^{30}$ sont :
271441, 904631, 16532714, 24658561, 27422714, 27664033, 46672291, 102690901, 130944133, 196075949, 214038533, 517697641, 545670533, 801123451, 855073301, 903136901, 970355431.

En 2010, Jon Grantham (doi:10.1016/j.jnt.2009.11.008) a montré qu'il existe une infinité de nombres pseudo-premiers de Perrin.

## 2 Un test de non-primalité

Bien qu'il ne soit pas possible d'utiliser cette propriété pour prouver qu'un nombre est premier, le théorème 1.1 permet de s'en servir comme test de non-primalité (qui ne permet pas de différentier les nombres premiers des pseudo-premiers de Perrin). Pour cela, il faut tester efficacement si $n \mid u_n$ pour un entier $n$ donné. Bien sûr, la croissance exponentielle des $u_n$ fait qu'il n'est pas question de calculer l'entier $u_n$ lui-même quand $n$ est grand. En revanche, il est relativement aisé de calculer l'image de $u_n$ dans $\mathbb{Z}/n\mathbb{Z}$.

Une première possibilité serait de calculer les termes de la suite de proche en proche, à l'aide de la relation de récurrence qui la définit. Le nombre d'additions modulaires croît alors linéairement en $n$, donc exponentiellement en la taille des données.

Un procédé considérablement plus efficace consiste à écrire la relation de récurrence sous forme matricielle, et à utiliser un algorithme d'exponentiation rapide pour calculer les puissances de matrices.

Une variante de cette dernière idée consiste à calculer $X^n$ dans l'anneau $(\mathbb{Z}/n\mathbb{Z})[X]/(X^3 - X - 1)$, par exponentiation rapide. On trouve alors une relation $X^n \equiv aX^2 + bX + c \pmod{X^3 - X - 1}$. Si $\alpha, \beta, \gamma$ sont les éléments du corps $k$ définis dans la preuve du théorème 1.1, alors on a :

$$\begin{aligned}\alpha^n &= a\alpha^2 + b\alpha + c\\ \beta^n &= a\beta^2 + b\beta + c\\ \gamma^n &= a\gamma^2 + b\gamma + c,\end{aligned}$$

donc, en sommant :

$$\begin{aligned}u_n &= au_2 + bu_1 + cu_0\\ &= 2a + 3c.\end{aligned}$$

Cette fois-ci, le temps de calcul est polynomial en la taille des données.

## 3 Nombres de Carmichael et pseudo-premiers de Perrin

Comme mentionné ci-dessus, on peut trouver des pseudo-premiers de Perrin par recherche exhaustive : pour tous les entiers $n$ de 2 à une certaine borne, on applique le test précédent, et si $n \mid u_n$, alors on teste s'il est premier (par exemple par essais de division par les entiers 2, ..., $\lfloor\sqrt{n}\rfloor$, puisque $n$ n'est pas très grand).

Si l'on cherche seulement à construire des pseudo-premiers, sans se préoccuper de leur taille ou de les trouver tous, on peut être plus astucieux en utilisant les nombres de Carmichael. Rappelons le résultat suivant (critère de Korselt).

**Théorème 3.1.** *Soit $n \geqslant 2$ un entier non premier. Les deux propriétés suivantes sont équivalentes :*

*(i) pour tout entier $a$ premier à $n$, on a $a^{n-1} \equiv 1 \pmod{n}$ ;*
*(ii) l'entier $n$ est sans facteur carré, et pour tout diviseur premier $p$ de $n$ on a $(p-1) \mid (n-1)$.*

*Démonstration.* Si $n$ vérifie la seconde propriété, alors la première découle du petit théorème de Fermat et du théorème chinois.

Supposons que $n$ vérifie la première propriété. Soit $p$ un diviseur premier de $n$.

Si $p^2 \mid n$, posons $m = \frac{n}{p}$. Alors en développant $(1+m)^p$ par la formule du binôme, on trouve $(1+m)^p \equiv 1 \pmod{n}$, donc $a = 1 + m$ est premier à $n$ et il est d'ordre $p$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Par hypothèse, on a $a^{n-1} \equiv 1$

$(\mathrm{mod}\ n)$, donc $p \mid (n-1)$, or $p \mid n$ : contradiction. Ceci étant vrai pour tous les diviseurs premier de $n$, celui-ci est sans facteur carré.

Prenons maintenant $a$ qui relève un générateur de $\mathbb{F}_p^\times$ et qui est premier à $n$ (le théorème chinois montre que c'est possible). Alors on a $a^{n-1} \equiv 1 \pmod{p}$, donc $(p-1) \mid (n-1)$. □

Les entiers qui vérifient les propriétés du théorème 3.1 sont appelés des nombres de Carmichael. En 1994, Alford, Granville et Pomerance (doi:10.2307/2118576) ont montré qu'il y en a une infinité.

En choisissant bien les facteurs premiers de nombres de Carmichael, on peut fabriquer des pseudo-premiers de Perrin. En effet, on montre facilement la proposition suivante.

**Proposition 3.2.** *Soit $n = p_1 \dots p_m$ un entier naturel sans facteur carré. Si :*

*(i) $n$ est un nombre de Carmichael (i.e. $(p_i - 1) \mid (n-1)$ pour tout i) ;*
*(ii) pour tout i, le polynôme $X^3 - X - 1$ est scindé sur $\mathbb{F}_{p_i}$ ;*

*alors $n$ est un pseudo-premier de Perrin.*

Les nombres premiers $p$ tels que $X^3 - X - 1$ est scindé à racines simples sur $\mathbb{F}_p$ sont faciles à reconnaître : ce sont ceux pour lesquels $X^p \equiv X \pmod{X^3 - X - 1}$, et ce calcul peut se faire par exponentiation rapide comme dans la partie précédente.

Le seul nombre premier pour lequel $X^3 - X - 1$ n'est pas sans facteur carré sur $\mathbb{F}_p$ est 23. En effet, c'est le seul diviseur premier du résultant de $X^3 - X - 1$ et de sa dérivée[1]. Sur le corps $\mathbb{F}_{23}$, on a $X^3 - X - 1 = (X+3)(X-10)^2$, donc le polynôme est scindé dans ce cas aussi.

Une optimisation utile s'appuie sur la condition nécessaire suivante.

**Proposition 3.3.** *Si le polynôme $X^3 - X - 1$ est scindé sur $\mathbb{F}_p$, alors $p$ est un carré modulo 23.*

On peut donc construire une table des carrés de $\mathbb{F}_{23}$, et commencer par tester si $p \pmod{23}$ est dans la table.

*Démonstration.* Si $X^3 - X - 1 = (X-\alpha)(X-\beta)(X-\gamma)$, on considère le *discriminant* du polynôme : $\Delta = \big[(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\big]^2$.

Le résultant de $X^3 - X - 1$ et de sa dérivée est égal à $-\Delta$, et se calcule facilement : $-\Delta = 23$. (On peut aussi calculer $\Delta$ en l'exprimant à partir des polynômes symétriques élémentaires). D'autre part, si $\alpha, \beta, \gamma \in \mathbb{F}_p$, alors $\Delta$ est un carré dans $\mathbb{F}_p$.

On conclut en remarquant que $-23$ est un carré dans $\mathbb{F}_p$ si et seulement si $p$ est un carré dans $\mathbb{F}_{23}$, par réciprocité quadratique. □

# 4 Construction de nombres de Carmichael

Pour construire des nombres de Carmichael, on considère ici ceux qui ont trois facteurs premiers, dont le plus petit (noté $p$) est connu. D'après la proposition 3.1, ce sont les entiers $n = pqr$, avec $p < q < r$ premiers tels que

$$(p-1) \mid (n-1), \quad (q-1) \mid (n-1), \quad (r-1) \mid (n-1),$$

1. Au signe près, ce résultant est ce qu'on appelle le *discriminant* du polynôme. On pourra comparer avec la définition alternative donnée un peu plus loin.

ou de manière équivalente

$$\begin{aligned} qr &\equiv 1 \pmod{p-1} \\ pr &\equiv 1 \pmod{q-1} \\ pq &\equiv 1 \pmod{r-1}. \end{aligned}$$

Notons que $p \geqslant 3$ puisque $n-1$ est forcément pair, et on a donc $p+2 \leqslant q \leqslant r-2$.

Posons $a = \frac{pq-1}{r-1}$. On a alors $0 < a \leqslant \frac{p(r-2)-1}{r-1} = p - \frac{p+1}{r-1}$, donc $1 \leqslant a \leqslant p-1$ puisque $a$ est entier.

Si $a = 1$, on aurait $r = pq$, ce qui est exclus puisque $r$ est premier. On a donc $2 \leqslant a \leqslant p-1$.

Si $a$ est connu, on a $pq - 1 = a(r-1)$, donc $ar = pq + a - 1$.

Comme $pr \equiv 1 \pmod{q-1}$, on a :

$$\begin{aligned} 0 &\equiv a(pr-1) \pmod{q-1} \\ &\equiv p(pq+a-1) - a \pmod{q-1} \\ &\equiv p(p+a-1) - a \pmod{q-1} \\ &\equiv p(p+a) - (p+a) \pmod{q-1} \\ &\equiv (p-1)(p+a) \pmod{q-1}, \end{aligned}$$

donc $(q-1) \mid ((p-1)(p+a))$, ce qui ne laisse qu'un nombre fini de possibilités pour $q$, donc pour $r = \frac{pq-1}{a} + 1$, et donc aussi pour $n$.

L'algorithme suivant permet donc d'énumérer tous les nombres de Carmichael de la forme $n = pqr$ avec $p < q < r$ premiers, pour un $p$ donné.

```
Données : p≥3 premier

factoriser p-1
pour a de 2 à p-1 :
  factoriser p+a
  en déduire les diviseurs de (p-1)(p+a)
  pour tous les diviseurs d trouvés :
    si d ≤ p passer au diviseur suivant
    q ← d+1
    si pq ≠ 1 (mod a) passer au diviseur suivant
    r ← (pq-1)/a + 1
    si pr ≠ 1 (mod d) passer au diviseur suivant
    si qr ≠ 1 (mod p-1) passer au diviseur suivant
    si q n'est pas premier passer au diviseur suivant
    si r n'est pas premier passer au diviseur suivant
    renvoyer n=pqr et continuer
```

Les entiers considérés ici n'étant pas très grands, on peut par exemple faire les factorisations et les tests de primalités par essais de divisions.

| $p$ | nombres de Carmichael |
|---|---|
| 3 | 561 = 3 × 11 × 17 |
| 5 | 10585 = 5 × 29 × 73<br>2465 = 5 × 17 × 29<br>1105 = 5 × 13 × 17 |
| 7 | 8911 = 7 × 19 × 67<br>2821 = 7 × 13 × 31<br>15841 = 7 × 31 × 73<br>6601 = 7 × 23 × 41<br>1729 = 7 × 13 × 19<br>52633 = 7 × 73 × 103 |

Pour fabriquer des pseudo-premiers de Perrin, on modifie l'algorithme de la manière suivante :

- on le place à l'intérieur d'une boucle sur les nombres premiers $p \geqslant 3$ tels que $X^3 - X - 1$ soit scindé sur $\mathbb{F}_p$, et inférieurs à une borne donnée ;
- pour les nombres premiers $q$ et $r$ trouvés, on teste si $X^3 - X - 1$ est scindé sur $\mathbb{F}_q$ (respectivement $\mathbb{F}_r$), et on ne garde que ceux pour lesquels le polynôme est scindé.

Avec la borne $p < 2^{12}$, on trouve les pseudo-premiers de Perrin suivants.

7279379941 = 211 × 3571 × 9661
43234580143 = 223 × 5107 × 37963
254302215553 = 307 × 3673 × 225523
1023698879695801 = 463 × 218527 × 10117801
1295971290159001 = 599 × 120199 × 17999801
144940461540661 = 691 × 69691 × 3009781
7045248121 = 821 × 1231 × 6971
118805562613 = 829 × 9109 × 15733
238168709563051 = 883 × 507151 × 531847
7729741408201 = 1151 × 4831 × 1390121
144377609419 = 1319 × 9227 × 11863
2268102525107329 = 1697 × 62753 × 21298369
588909469501 = 1871 × 16831 × 18701
157529730393001 = 2647 × 44983 × 1323001
996481854292467817 = 3359 × 594367 × 499119689
652270080001 = 3361 × 9241 × 21001
1905099549370921 = 3571 × 255511 × 2087941
66355877639521 = 3637 × 54541 × 334513

On trouve ainsi rapidement beaucoup de pseudo-premiers de Perrin. En revanche, ceux qu'on trouve par cette méthode sont relativement grands.

Il est assez facile de généraliser l'algorithme précédent pour chercher des produits de $m > 3$ facteurs premiers (on fixe $p_1$, ..., $p_{m-2}$, et on détermine $p_{m-1}$ et $p_m$ tels que le produit soit un nombre de Carmichael).

On peut aussi ne chercher que des nombres de Carmichael d'une forme particulière. Par exemple, si $6u + 1$, $12u + 1$ et $18u + 1$ sont premiers, alors leur produit est un nombre de Carmichael. Pour que $X^3 - X - 1$ soit scindé modulo ces trois nombres, il faut que $u \equiv 0, 4, 14$ ou $22 \pmod{23}$, et on vérifie que $u = 8441 = 23 \times 367$ convient (c'est le plus petit).

# 5 Suggestions

1 Pouvez-vous donner des exemples de pseudo-premiers pour différents tests de non-primalité ?
2 On pourra démontrer que si $6u+1$, $12u+1$ et $18u+1$ sont premiers, alors leur produit est un nombre de Carmichael, et construire des pseudo-premiers de Perrin de cette forme.
3 Connaissez-vous un test de primalité (i.e. un test qui démontre vraiment que le nombre est premier) ? Décrivez-le. Quelle est sa complexité ?
4 Montrer que si $p$ est un nombre premier qui vérifie $p \equiv -1 \pmod 8$, alors 2 est d'ordre impair dans $\mathbb{F}_p^\times$. En déduire que si un nombre de Carmichael est produit de tels facteurs premiers, alors c'est un pseudo-premier pour le test de Rabin-Miller en base 2. Construire des pseudo-premiers de cette forme en adaptant la méthode présentée ici.
5 Pourquoi les nombres premiers $p$ tels que $X^3 - X - 1$ est scindé à racines simples sur $\mathbb{F}_p$ sont-ils ceux pour lesquels $X^p \equiv X \pmod{X^3 - X - 1}$ ?
6 Faire le lien entre les deux définitions alternatives données pour le discriminant d'un polynôme unitaire.
7 Généraliser la construction présentée ici au cas de plus de 3 facteurs premiers.
8 La méthode de construction de nombres de Carmichael présentée ici est loin d'être la plus efficace. Une autre méthode[2], due à Erdős, consiste à fixer d'abord un entier $\Lambda$ qui a beaucoup de diviseurs (typiquement un produit de petits nombres premiers, avec des exposants bien choisis), en déduire (avec un test de primalité) les nombres premiers $p_i$ tels que $p_i - 1 \mid \Lambda$, puis à trouver des produits $\prod_{i\in I} p_i \equiv 1 \pmod \Lambda$ d'un certain nombre de tels premiers (c'est l'étape la plus difficile, où il peut être intéressant de procéder de manière plus astucieuse que d'énumérer les très nombreux produits possibles).

2. Cette méthode est en fait l'argument clé de la preuve d'Alford, Granville et Pomerance.