Annales Mathématiques Blaise Pascal **Version de travail – 25 octobre 2025**

Sur la conjecture brunnienne (généralisée)

Jean-Yves Degos

Résumé. Nous démontrons la conjecture $B(n, p, P)$ de [1, Conjecture 3.6 p. 62], que nous renommons ici « conjecture brunnienne », dans les cas où $p \geq 5$ et n n'est pas divisible par $p - 1$. Nous introduisons aussi la « conjecture brunnienne généralisée » $B(n, q, P)$ et nous la démontrons dans les cas où $q \geq 4$ et n n'est pas divisible par $q - 1$. En fin d'article, nous montrons aussi, analytiquement, que la stratégie intrinsèque que nous introduisons ici permet de conclure favorablement quant à la véracité de la conjecture dans une proportion significative des cas (voir Proposition 5.2 et Proposition 5.4).

On the (generalized) Brunnian Conjecture

Abstract. We prove the Conjecture $B(n, p, P)$ of [1, Conjecture 3.6 p. 62], which is renamed here as the "Brunnian Conjecture", in the case where $p \geq 5$ and n is not a multiple of $p - 1$. We also introduce, and prove the "Generalized Brunnian Conjecture" $B(n, q, P)$ and prove it in the cases where $q \geq 4$ and n is not divisible by $q - 1$. At the end of the paper, we also show with through an analytical argument that the intrinsic strategy we introduce here leads to a proof of the conjecture in a significant proportion of cases (see Proposition 5.2 and Proposition 5.4).

1. Introduction

Le but de cet article est de donner une démonstration partielle de la Conjecture $B(n, p, P)$ ([1, Conjecture 3.6 p. 62]). Nous nous référerons désormais à celle-ci sous l'appellation « conjecture brunnienne ». Notre stratégie consiste à utiliser la démonstration donnée par Nick Gill de la Conjecture $A(n, p, P)$ ([1, Conjecture 3.4 p. 62]) dans [3, Theorem 2 p. 230], corrigée par l'article de Joel Brewster Lewis, see ([6, Theorem 7 p. 6 et Correction 3.3 p. 10]).

Notre résultat principal est (voir Théorème 3.6 page 8) :

Théorème. *Soit p un nombre premier, $n \geq 3$ un entier, et*

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{F}_p[X]$$

Mots-clés: Polynômes primitifs, Corps finis, Groupes linéaires, Conjecture brunnienne.
Classification math.: 00X99.

un polynôme primitif de degré n. Notons $C = C_P$ la matrice compagnon de P, c'est-à-dire :

$$C = C_P = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{bmatrix}.$$

Notons G la matrice compagnon du polynôme $X^n - 1$, et soit :

$$\begin{aligned} G_1 &:= C\,, \\ G_{k+1} &:= GG_kG^{-1} \text{ pour tout } 1 \leq k \leq n-1. \end{aligned}$$

Alors, si $p \geq 5$ et n n'est pas divible par $p - 1$, nous avons :

$$\langle G_1, G_2, \dots, G_n \rangle = \mathrm{GL}_n(\mathbb{F}_p)\,.$$

2. **Historique et stratégie**

Cette histoire commence avec les travaux de René Guitart sur le groupe (de Klein) d'ordre 168 (défini comme le groupe d'automorphismes de la quartique de Klein), qu'il a été le premier à décrire comme un « objet borroméen » ([4, section 3 p. 148]), qui n'est autre que $\mathrm{GL}_3(\mathbb{F}_2)$. Dans [1], nous avons étendu la notion de groupe borroméen introduite par René Guitart en définissant les notions de groupes n-cyclables ([1, Definition 1.1 p. 58]) et de groupes n-brunniens ([1, Definition 1.2 et Definition 1.3 p. 58]. La ci-nommée « Conjecture brunnienne » renvoie à l'énoncé suivant : si p est un nombre premier, et $n \geq 2$ un entier, alors le groupe $\mathrm{GL}_n(\mathbb{F}_p)$ peut être engendré par la matrice compagnon d'un polynôme primitif $P(X) \in \mathbb{F}_p[X]$ de degré n, et ses conjuguées successives par G^k pour $1 \leq k \leq n-1$ où G la matrice compagnon du polynôme $X^n - 1$. Cette conjecture est reliée à une autre : le groupe $\mathrm{GL}_n(\mathbb{F}_p)$ peut être engendré par la matrice compagnon d'un polynôme primitif $P(X) \in \mathbb{F}_p[X]$ de degré n, notée C, et la matrice compagnon du polynôme $X^n - 1$, notée G. Ainsi :

$$\mathrm{GL}_n(\mathbb{F}_p) = \langle C, G \rangle.$$

Ensuite, Nick Gill, en utilisant la classification des groupes finis simples, a donné une preuve de notre conjecture (A, n, p), en démontrant l'énoncé plus général suivant ([3, Theorem 2 p. 230]) : si $\mathbb{F}$ est un corps fini q éléments et si f, g sont des polynômes dictincts de $\mathbb{F}[X]$ de degrés n tels que f est primitif, et le terme constant de g est non nul, alors :

$$\langle C_f, C_g \rangle = \mathrm{GL}_n(\mathbb{F}).$$

Par conséquent, nous pouvons déduire du théorème de Nick Gill une méthode simple pour démontrer (certains cas de) la conjecture brunnienne : il suffit de fabriquer une matrice compagnon K (d'un polynôme g de degré n) avec les propriétés suivantes :

- $K \in \langle G_1, G_2, \ldots, G_n \rangle$;

- $g(0) \neq 0$;

- $K \neq G_1$.

Ainsi, comme $\langle G_1, K \rangle \subset \langle G_1, G_2, \ldots, G_n \rangle \subset \mathrm{GL}_n(\mathbb{F}_p)$, chaque fois que $\langle G_1, K \rangle = \mathrm{GL}_n(\mathbb{F}_p)$, c'est gagné !

Dans cet article, notre principal apport est de construire une telle matrice K de façon *générique*... En effet, notre construction fonctionne chaque fois que $-a_0 \neq 1$ et $(-a_0)^n \neq 1$, ce qui est garanti par les hypothèses $p \geq 5$ et n non divisible par $p - 1$, quand le corps de base est $\mathbb{F}_p$. De plus, nous devons supposer que $n \geq 3$, comme Joel Brewster Lewis l'a signalé.

3. Énoncés et démonstrations

Définition 3.1. Avec les notations de notre théorème principal, nous faisons l'hypothèse que $n \geq 3$ est un entier, et nous définissons la matrice K par :

$$K := G_n G_{n-1} \cdots G_2 G_1 \, .$$

Proposition 3.2. *Nous avons* $K = C(G^{-1}C)^n$.

Démonstration. Nous commençons par démontrer, grâce à un raisonnement par récurrence, le résultat suivant :

$$G_k G_{k-1} \ldots G_1 = G^{k-1} C (G^{-1} C)^{k-1} \text{ pour tous } 2 \leq k \leq n \, .$$

En effet, si $k = 2$, cette égalité est équivalente à :

$$G_2 G_1 = G^{2-1} C (G^{-1} C)^{2-1} \, ;$$

par conséquent, elle est vraie, parce que le membre de droite vaut $GCG^{-1}C = G_2 G_1$. Supposons vraie l'hypothèse de récurrence au rang k, et montrons-là au rang $k + 1$. Nous

avons :

$$\begin{aligned} G_{k+1}G_kG_{k-1}\cdots G_1 &= G_{k+1}\cdot G^{k-1}C(G^{-1}C)^{k-1} \\ &= G^kCG^{-k}\cdot G^{k-1}C(G^{-1}C)^{k-1} \\ &= G^k\cdot C\cdot G^{-k}\cdot G^{k-1}C\cdot(G^{-1}C)^{k-1} \\ &= G^k\cdot C\cdot G^{-1}C\cdot(G^{-1}C)^{k-1} \\ &= G^k\cdot C\cdot(G^{-1}C)^k\,. \end{aligned}$$

Nous avons alors : $G_nG_{n-1}\ldots G_1 = G^{n-1}C\left(G^{-1}\right)^{n-1}C$. Nous pouvons conclure que :

$$\begin{aligned} G_1G_nG_{n-1}\ldots G_1 &= G_1G^{n-1}C(G^{-1})^{n-1}\,, \\ &= CG^{-1}C(G^{-1})^{n-1}\,, \\ &= C(G^{-1}C)^n\,, \end{aligned}$$

ce qu'il fallait démontrer. □

Proposition 3.3. *Notons E_k le k^e vecteur de la base canonique, pour $1 \le k \le n$. Alors :*

(1) $G^{-1}C.E_k = E_k$ *pour* $1 \le k \le n-1$;

(2) $G^{-1}C.E_n = -a_0E_n + \sum_{j=0}^{n-1} -a_jE_j$,

c'est-à-dire :

$$G^{-1}C = \begin{bmatrix} 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \\ 0 & 0 & \ldots & 0 & -a_0 \end{bmatrix}.$$

Démonstration. La première assertion est une conséquence du fait que le produit de la matrice G (respectivement : C) par le vecteur-colonne E_k est égal au vecteur-colonne E_{k+1} pour $1 \le k \le n-1$. Ainsi, $G^{-1}C.E_k = G^{-1}.CE_k = G^{-1}.E_{k+1} = E_k$.

Pour démontrer la seconde assertion, nous procédons comme suit :

$$\begin{aligned}
G^{-1}C.E_n &= G^{-1}.\left(\sum_{i=1}^{n} -a_{i-1}E_i\right) \\
&= \sum_{i=1}^{n} -a_{i-1}G^{-1}.E_i \\
&= \sum_{i=1}^{n} -a_{i-1}\begin{cases} E_{i-1} & \text{si} \quad 2 \leq i \leq n \\ E_n & \text{si} \quad i = 1 \end{cases} \\
&= -a_0G^{-1}E_1 + \sum_{i=2}^{n} -a_{i-1}G^{-1}E_i \\
&= -a_0E_n + \sum_{i=2}^{n} -a_{i-1}E_{i-1} \\
&= -a_0E_n + \sum_{j=1}^{n} -a_jE_j
\end{aligned}$$

grâce au changement de variable $j = i - 1$. □

Proposition 3.4. *Suppons que $-a_0 \neq 1$. Alors la matrice $G^{-1}C$ peut s'écrire comme $Q^{-1}G^{-1}CQ = D$, où $Q \in \mathrm{GL}_n(\mathbb{F}_p)$ et D, matrice diagonale, s'expriment ainsi :*

$$Q = \begin{bmatrix} 1 & 0 & \dots & 0 & \frac{a_1}{1+a_0} \\ 0 & 1 & \dots & 0 & \frac{a_2}{1+a_0} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \frac{a_{n-1}}{1+a_0} \\ 0 & 0 & \dots & 0 & 1 \end{bmatrix} \text{ et } D = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & -a_0 \end{bmatrix},$$

Nous en déduisons que : $K = G^{n-1}(G^{-1}C)^n = C(QDQ^{-1})^n = CQD^nQ^{-1}$.

Démonstration. Le polynôme caractéristique de la matrice $G^{-1}C$ est $\chi_{G^{-1}C}(X) = (X - 1)^{n-1}(X + a_0)$. Par conséquent, les valeurs propres sont 1, d'ordre $n - 1$ et $-a_0$, d'ordre 1. D'après la Propostion 3.3, (1), page 4, nous pouvons en déduire que Q satisfera les égalités $Q.E_k = E_k$ pour $1 \leq k \leq n-1$. Conséquemment, nous devons trouver un vecteur-colonne V tel que $G^{-1}CV = -a_0V$, comme vecteur propre associé à la valeur propre $-a_0$.

Par conséquent, nous écrivons :

$$V := \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \text{ d'où } G^{-1}CV = \begin{pmatrix} v_1 - a_1 v_n \\ v_2 - a_2 v_n \\ \vdots \\ v_{n-1} - a_{n-1} v_n \\ -a_0 v_n \end{pmatrix}, \text{ and}$$

$$-a_0 V = \begin{pmatrix} -a_0 v_1 \\ -a_0 v_2 \\ \vdots \\ -a_0 v_n \end{pmatrix}$$

En résolvant ce système de Cramer en $v_1, v_2, \ldots, v_n$, nous obtenons :

(1) $v_n \in \mathbb{F}_p$;

(2) $v_i = \frac{a_i v_n}{1+a_0}$ pour $1 \leq i \leq n-1$.

Maintenant, il nous suffit de choisir $v_n = 1$ pour obtenir la matrice précédemment annoncée Q. □

Proposition 3.5. *Si $-a_0 \neq 1$ et $(-a_0)^n \neq 1$, la matrice*

$$K := G_n G_{n-1} \cdots G_2 G_1$$

est une matrice compagnon, distincte de C.

Démonstration. Sous l'action de Q et D, les vecteurs-colonnes E_k pour $1 \leq k \leq n-1$ sont fixes. Nous avons donc :

$$\begin{aligned} K.E_k &= CQD^nQ^{-1}.E_k \\ &= C.E_k \\ &= E_{k+1} . \end{aligned}$$

Par conséquent, nous devons évaluer $K.E_n = CQD^nQ^{-1}.E_n$.

Soit $U := Q^{-1}E_n$. Alors $E_n = QU$. Pour trouver la valeur de U, il suffit de résoudre l'équation. Cependant, si

$$Q = \begin{bmatrix} 1 & 0 & \ldots & 0 & q_1 \\ 0 & 1 & \ldots & 0 & q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & q_{n-1} \\ 0 & 0 & \ldots & 0 & q_n \end{bmatrix} \text{ et } U = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{n-1} \\ u_n \end{bmatrix},$$

alors

$$QU = \begin{bmatrix} u_1 + q_1 u_n \\ u_2 + q_2 u_n \\ \vdots \\ u_{n-1} + q_{n-1} u_n \\ q_n u_n \end{bmatrix} \text{ est égale à } E_n = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

ce qui permet d'obtenir : $u_n = \frac{1}{q_n} = 1$ (parce que q_n est une notation pour le coefficient de la rangée n et de la colonne n de Q, lequel vaut 1), et :

$$u_k = -q_k u_n = -q_k = \frac{-a_k}{1 + a_0}\,.$$

Ainsi, nous avons :

$$U = \begin{bmatrix} \frac{-a_1}{1+a_0} \\ \frac{-a_2}{1+a_0} \\ \vdots \\ \frac{-a_{n-1}}{1+a_0} \\ 1 \end{bmatrix}.$$

Maintenant, soit $W := D^n U$. Alors :

$$W = \begin{bmatrix} \frac{-a_1}{1+a_0} \\ \frac{-a_2}{1+a_0} \\ \vdots \\ \frac{-a_{n-1}}{1+a_0} \\ (-a_0)^n \end{bmatrix},$$

et $CQD^n U = CQW$. Maintenant, nous avons :

$$QW = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ (-a_0)^n \end{bmatrix},$$

En résumé, nous avons :

$$\begin{aligned} K.E_n &= CQD^nQ^{-1}.E_n \\ &= CQD^nU \\ &= CQWW \\ &= C(-a_0)^nE_n \\ &= (-a_0)^nCE_n \\ &= \sum_{i=1}^{n} -a_{i-1}(-a_0)^nE_i \,. \end{aligned}$$

Par conséquent, la matrice K est une matrice compagnon, distincte de C, parce que nous avons supposé que $(-a_0)^n \neq 1$. □

Théorème 3.6 (Résultat principal)**.** *Soit $p \geq 5$ un nombre premier. Alors $-a_0 \neq 1$. De plus, si n n'est pas divisible par $p-1$ alors $(-a_0)^n \neq 1$. Dans ce cas, la conjecture brunnienne $B(n,p,P)$ est vraie, où*

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{F}_p[X]$$

est un polynôme primitif de degré n sur $\mathbb{F}_p[X]$. C'est-à-dire :

$$\langle G_1, G_2, \ldots, G_n \rangle = \mathrm{GL}_n(\mathbb{F}_p) \,.$$

Démonstration. Comme le polynôme $P(X)$ est primitif, $(-1)^na_0$ engendre le groupe multiplicatif $\mathbb{F}_p^\times$, donc si $p \geq 5$, l'égalité $-a_0 = 1$ ne peut pas avoir lieu. En effet, si l'on avait $-a_0 = 1$, on aurait $a_0 = -1$, et alors $(-1)^na_0 = (-1)^{n+1}$ serait égal à -1 ou 1, qui ne sont jamais des générateurs de $\mathbb{F}_p^\times$ lorsque $p \geq 5$.

Si n n'est pas divisible par $p-1$, supposons que $(-a_0)^n = 1$ dans $\mathbb{F}_p^\times$. Nous pouvons écrire $n = (p-1)q + r$, où $1 \leq r < p-1$ est un entier. Alors $(-a_0)^r = 1$, parce que d'après notre hypothèse, $1 = (-a_0)^n = (-a_0)^{(p-1)q}(-a_0)^r$ et $(-a_0)^{p-1} = 1$ (puisque $-a_0 \in \mathbb{F}_p^\times$). Maintenant, il est clair que $(-1)^na_0 = (-1)^{r-1}(-a_0)$ a un ordre qui divise $r < p-1$. C'est une contradiction avec le fait que $(-1)^na_0$ est un générateur de $\mathbb{F}_p^\times$, dont l'ordre est $p-1$. Par conséquent, si n n'est pas divisible par $p-1$, alors $(-a_0)^n \neq 1$. □

En fait, ce résultat peut être généralisé dans le cas d'un corps de base de cardinal $q = p^r, r \geq 1$. Nous obtenons alors le résultat suivant.

Théorème 3.7 (Résultat principal généralisé)**.** *Soit $q = p^r$ une puissance d'un nombre premier, avec $q \geq 4$. Alors $-a_0 \neq 1$. De plus, si n n'est pas divisible par $q-1$ alors $(-a_0)^n \neq 1$. Dans ce cas, la Conjecture brunnienne généralisée $B(n,q,P)$ est vraie, où*

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{F}_q[X]$$

est un polynôme primitif de degré n sur $\mathbb{F}_q[X]$. *C'est-à-dire :*

$$\langle G_1, G_2, \ldots, G_n \rangle = \mathrm{GL}_n(\mathbb{F}_q)\,.$$

Démonstration. Nous pouvons définir les mêmes objets que dans le Théorème 3.6 (c'est-à-dire la matrice compagnon $C = C_P$, la matrice compagnon G et $G_1, \ldots G_n$) par rapport qu polynôme primitif $P(X)$. Alors $(-1)^n a_0$ engendre le groupe multiplicatif $\mathbb{F}_q^\times$, donc si $q \geq 4$, l'égalité $-a_0 = 1$ ne peut avoir lieu. En effet, si l'on avait $-a_0 = 1$, on aurait $a_0 = -1$, et $(-1)^n a_0 = (-1)^{n+1}$ serait égal à -1 ou 1, qui ne sont jamais des générateurs de $\mathbb{F}_q^\times$ lorsque $q \geq 4$.

Si n n'est pas divisible par $q-1$, supposons que $(-a_0)^n = 1$ in $\mathbb{F}_q^\times$. Nous pouvons écrire $n = (q-1)k + s$, où $1 \leq s < q-1$ est un entier. Alors $(-a_0)^s = 1$, à cause de notre hypothèse, $1 = (-a_0)^n = (-a_0)^{(q-1)k}(-a_0)^s$ et $(-a_0)^{q-1} = 1$ (parce que $-a_0 \in \mathbb{F}_q^\times$). Maintenant, il est clair que $(-1)^n a_0 = (-1)^{s-1}(-a_0)$ a un ordre qui divise $s < q-1$. C'est une contradiction avec le fait que $(-1)^n a_0$ est un générateur de $\mathbb{F}_q^\times$, dont l'ordre est $q-1$. Par conséquent, si n n'est pas divisible par $q-1$, alors $(-a_0)^n \neq 1$. □

4. **Remarques complémentaires**

Dans [1], nous avions effectué des « vérifications expérimentales », reposant sur une liste de polynômes primitifs établie par Philippe Langevin[1], et nous n'avions pas été capable de conclure quant à la véracité de la conjecture pour certains couples (n, p), à cause d'un manque de puissance de calcul et/ou de la complexité de ces calculs. Grâce à la méthode développée ici, nous pouvons maintenant donner des réponses aux cas laissés en suspens. Nous les résumons dans les tableaux suivants. Si « (False) » est écrit dans la dernière colonne, cela signifie que la conjecture peut être vraie, mais cela n'est pas une conséquence des deux résultats principaux de cet article.

Polynômes primitifs sur $\mathbb{F}_5$

n	p	$P(x)$	$B(n,p,P)$
7	5	$x^7 + x^6 + 2$	True
8	5	$x^8 + x^5 + x^3 + 3$	(False)
9	5	$x^9 + x^7 + x^6 + 3$	True
10	5	$x^{10} + x^9 + x^7 + 3$	True
11	5	$x^{11} + x^{10} + 2$	True
12	5	$x^{12} + x^7 + x^4 + 3$	(False)
13	5	$x^{13} + 4x^2 + 3x + 3$	True
14	5	$x^{14} + x^7 + 4x^5 + 4x^4 + 2x^3 + 3x^2 + x + 2$	True
15	5	$x^{15} + 2x^5 + 4x^5 + 3x^3 + 3x^2 + 4x + 3$	True
16	5	$x^{16} + x^7 + 4x^6 + 4x^5 + 4x^4 + 4x^3 + 4x^2 + x + 2$	(False)
17	5	$x^{17} + 3x^2 + 2x + 3$	True
18	5	$x^{18} + x^{12} + x^{11} + x^{10} + x^9 + 2x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 2$	True

[1] Elle peut être téléchargée ici : https ://langevin.univ-tln.fr/project/apc/primitif.data.

Polynômes primitifs sur $\mathbb{F}_7$

n	p	$P(x)$	$B(n,p,P)$
6	7	$x^6+x^5+x^4+3$	(False)
7	7	x^7+x^5+4	True
8	7	x^8+x^7+3	True
9	7	$x^9+x^8+x^3+2$	True
10	7	$x^{10}+x^9+x^8+3$	True

Polynômes primitifs sur $\mathbb{F}_{11}$

n	p	$P(x)$	$B(n,p,P)$
5	11	$x^5+x^4+x^3+3$	True
6	11	x^6+x^5+x+7	True
7	11	x^7+x^6+4	True
8	11	$x^8+x^7+x^6+7$	True

Polynômes primitifs sur $\mathbb{F}_{13}$

n	p	$P(x)$	$B(n,p,P)$
5	13	$x^5+x^4+x^3+6$	True
6	13	$x^6+x^5+x^3+6$	True
7	13	x^7+x^4+2	True
8	13	$x^8+x^7+x^6+11$	True

Polynômes primitifs sur $\mathbb{F}_{17}$

n	p	$P(x)$	$B(n,p,P)$
4	17	x^4+x^3+5	True
5	17	x^5+x^4+5	True
6	17	x^6+x^5+3	True
7	17	x^7+x^6+7	True

Polynômes primitifs sur $\mathbb{F}_{19}$

n	p	$P(x)$	$B(n,p,P)$
4	19	x^4+x^3+2	True
5	19	x^5+x^4+5	True
6	19	x^6+x^5+15	True
7	19	x^7+x^6+5	True

Polynômes primitifs sur $\mathbb{F}_{23}$

n	p	$P(x)$	$B(n,p,P)$
4	23	x^4+x^3+20	True
5	23	x^5+x^4+6	True
6	23	x^6+x^5+7	True

Polynômes primitifs sur $\mathbb{F}_{29}$

n	p	$P(x)$	$B(n,p,P)$
4	29	x^4+x^3+2	True
5	29	x^5+x^4+2	True
6	29	x^6+x^5+11	True

Polynômes primitifs sur $\mathbb{F}_{31}$

n	p	$P(x)$	$B(n,p,P)$
4	31	x^4+x^3+13	True
5	31	x^5+x^4+10	True
6	31	x^6+x^5+12	True

Polynômes primitifs sur $\mathbb{F}_{37}$

n	p	$P(x)$	$B(n,p,P)$
3	37	x^3+x^2+17	True
4	37	x^4+x^3+22	True
5	37	x^5+x^4+2	True

Polynômes primitifs sur $\mathbb{F}_{41}$

n	p	$P(x)$	$B(n,p,P)$
3	41	x^3+x^2+11	True
4	41	x^4+x^3+26	True
5	41	x^5+x^4+11	True

Polynômes primitifs sur $\mathbb{F}_{43}$

n	p	$P(x)$	$B(n,p,P)$
3	43	x^3+x^2+9	True
4	43	x^4+x+20	True
5	43	x^5+x^4+9	True

Polynômes primitifs sur $\mathbb{F}_{47}$

n	p	$P(x)$	$B(n,p,P)$
3	47	x^3+x^2+2	True
4	47	x^4+x^3+5	True
5	47	x^5+x^4+6	True

Polynômes primitifs sur $\mathbb{F}_{53}$

n	p	$P(x)$	$B(n,p,P)$
3	53	x^3+x^2+2	True
4	53	x^4+x^3+2	True
5	53	x^5+x^4+12	True

Polynômes primitifs sur $\mathbb{F}_{59}$

n	p	$P(x)$	$B(n,p,P)$
3	59	x^3+x^2+9	True
4	59	x^4+x^3+18	True
5	59	x^5+x^4+4	True

Polynômes primitifs sur $\mathbb{F}_{61}$

n	p	$P(x)$	$B(n,p,P)$
3	61	x^3+x^2+6	True
4	61	x^4+x^3+17	True
5	61	x^5+x^4+55	True

Polynômes primitifs sur $\mathbb{F}_{67}$

n	p	$P(x)$	$B(n,p,P)$
3	67	x^3+x^2+6	True
4	67	x^4+x^3+12	True

Polynômes primitifs sur $\mathbb{F}_{71}$

n	p	$P(x)$	$B(n,p,P)$
3	71	x^3+x^2+8	True
4	71	x^4+x^3+13	True

Polynômes primitifs sur $\mathbb{F}_{73}$

n	p	$P(x)$	$B(n,p,P)$
3	73	x^3+x^2+5	True
4	73	x^4+x^3+33	True

Polynômes primitifs sur $\mathbb{F}_{79}$

n	p	$P(x)$	$B(n,p,P)$
3	79	x^3+x^2+2	True
4	79	x^4+x^3+7	True

Polynômes primitifs sur $\mathbb{F}_{83}$

n	p	$P(x)$	$B(n,p,P)$
3	83	x^3+x^2+11	True
4	83	x^4+x^3+24	True

Polynômes primitifs sur $\mathbb{F}_{89}$

n	p	$P(x)$	$B(n,p,P)$
3	89	x^3+x^2+6	True
4	89	x^4+x^3+14	True

Polynômes primitifs sur $\mathbb{F}_{97}$

n	p	$P(x)$	$B(n,p,P)$
3	97	x^3+x^2+5	True
4	97	x^4+x^3+15	True

5. **Conclusion**

Nous conclurons cet article en donnant des résultats qui permettent de voir que nos résultats couvrent une bonne partie des cas.

Définition 5.1. Pour un entier $N \geq 5$:

(1) nous noterons $\mathcal{P}(N)$ l'ensemble des nombres premiers p pour lesquels les inégalités suivantes sont satisfaites : $5 \leq p \leq N$;

(2) nous noterons $\mathcal{Q}(N)$ l'ensemble des nombres primaires q tels qu'il existe un nombre premier $5 \leq p \leq N$ et un entier $r \geq 1$ tel que $q = p^r$. Ainsi $q \geq 4$.

Si $n \geq 3$, $N \geq 5$, et $p \in \mathcal{P}(N)$, nous voudrions évaluer la probabilité que n ne soit pas divisible par $p-1$, sachant que nous espérons qu'elle soit le plus élevé possible. Le résultat est donné par la proposition suivante.

Proposition 5.2. *Pour $N \geq 5$, soit :*

$$\mathcal{E}_N = \{(p,n) \mid p \in \mathcal{P}(N), 3 \leq n \leq N\};$$

$$\mathcal{D}_N = \{(p,n) \mid p \in \mathcal{P}, 3 \leq n \leq N, n \in (p-1)\mathbb{Z}\}.$$

Alors :

(1) $\#\mathcal{E}_N = (\pi(N)-2)(N-2)$ *et* $\#\mathcal{D}_N = \sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor$ *;*

(2) $\frac{\#\mathcal{D}_N}{\#\mathcal{E}_N} \leq \frac{\sqrt{N}}{N-2}$ *et* $\frac{\#\overline{\mathcal{D}}_N}{\#\mathcal{E}_N} \geq 1 - \frac{\sqrt{N}}{N-2}$.

Démonstration. En effet, le nombre d'éléments dans $\mathcal{P}(N)$ est le nombre $\pi(N)$ de nombres premiers inférieurs à N, exceptés 2 et 3. Par conséquent :

$$\#\mathcal{E}_N = (\pi(N)-2)(N-2).$$

Aussi :

$$\begin{aligned}\#\mathcal{D}_N &= \left\{(p, k(p-1)) \mid p \in \mathcal{P}(N), \frac{3}{p-1} \leq k \leq \frac{N}{p-1}\right\}, \\ &= \sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor.\end{aligned}$$

Alors le premier point est démontré. Maintenant, par récurrence sur $N \geq 5$, nous pouvons démontrer (voir the Lemme 5.3 ci-dessous) que :

$$\#\mathcal{D}(N) \leq \sqrt{N}(\pi(N)-2)$$

.

En divisant par $\#\mathcal{E}(N)$, nous obtenons les deux inégalités du second point. □

Lemme 5.3. *Soit $p \geq 5$ un nombre premier avec $p \leq N$ pour un entier $N \geq 5$. Alors :*

$$\sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor \leq \sum_{p\in P(N)} \sqrt{N}.$$

Démonstration. Étape d'initialisation : si $N = 5$, alors $\mathcal{P}(N) = \{5\}$. Par conséquent :

$$\sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor = \left\lfloor \frac{5}{4} \right\rfloor = 1,25 \leq \sqrt{5} = \sum_{p\in P(N)} \sqrt{N}.$$

Étape de récurrence : nous devons prouver que si la propriété est vraie pour un entier $N \geq 5$, elle est également vraie pour l'entier $N+1$. Nous devons pour cela justifier que :

$$\sum_{p\in\mathcal{P}(N+1)} \left\lfloor \frac{N+1}{p-1} \right\rfloor \leq \sum_{p\in P(N+1)} \sqrt{N+1}.$$

Soit $N+1$ n'est pas premier, soit il l'est.

Commençons par traiter le cas où $N+1$ n'est pas premier. Alors $\mathcal{P}(N+1) = \mathcal{P}(N)$, et nous obtenons :

$$\begin{aligned}\sum_{p\in\mathcal{P}(N+1)} \left\lfloor \frac{N+1}{p-1} \right\rfloor &= \sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N+1}{p-1} \right\rfloor \\ &= \sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor \\ &\leq \sum_{p\in\mathcal{P}(N)} \sqrt{N} \text{ (récurrence)} \\ &= \sum_{p\in\mathcal{P}(N+1)} \sqrt{N} \\ &< \sum_{p\in\mathcal{P}(N+1)} \sqrt{N+1}.\end{aligned}$$

CQFD.

Traitons maintenant le cas où $N+1$ est premier. Alors $\mathcal{P}(N+1) = \mathcal{P}(N) \cup \{N+1\}$, et nous obtenons :

$$\sum_{p\in\mathcal{P}(N+1)} \left\lfloor \frac{k+1}{p-1} \right\rfloor = \sum_{p\in\mathcal{P}(N+1)} \left\lfloor \frac{k+1}{p-1} \right\rfloor + \left\lfloor \frac{k+1}{k} \right\rfloor.$$

Grâce à une propriété de la partie entière :

$$\left\lfloor \frac{k+1}{k} \right\rfloor = 1 \text{ pour tout entier non nul } k,$$

Nous pouvons en déduire que :

$$\sum_{p\in\mathcal{P}(N+1)} \left\lfloor \frac{N+1}{p-1} \right\rfloor \leq \sum_{p\in\mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor + 1 < \sum_{p\in\mathcal{P}(N)} \sqrt{N} + 1$$

et :

$$\sum_{p\in\mathcal{P}(N)} \sqrt{N} + 1 \leq \sum_{p\in\mathcal{P}(N+1)} \sqrt{N+1},$$

CQFD. □

Proposition 5.4. *Pour $N \geq 5$, soit :*

$$\mathcal{E}^*{}_N = \{(q,n) \mid q \in Q(N), 3 \leq n \leq N\};$$

$$\mathcal{D}^*{}_N = \{(q,n) \mid q \in Q(N), 3 \leq n \leq N, n \in (q-1)\mathbb{Z}\}.$$

Alors :

(1) $\#\mathcal{E}^*{}_N = (\pi(N)-2)(N-2)$ *et* $\#\mathcal{D}^*{}_N = \sum_{q\in Q(N)} \left\lfloor \frac{N}{q-1} \right\rfloor$ *;*

(2) $\frac{\#\mathcal{D}^*{}_N}{\#\mathcal{E}^*{}_N} \leq \frac{\sqrt{N}}{N-2}$ *et* $\frac{\#\overline{\mathcal{D}^*}_N}{\#\mathcal{E}^*{}_N} \geq 1 - \frac{\sqrt{N}}{N-2}$.

Démonstration. La démonstration est quasiment la même. □

Ainsi :

$$\lim_{N\to+\infty} \frac{\overline{\mathcal{D}}_N}{\mathcal{E}_N} = 1 \text{ et } \lim_{N\to+\infty} \frac{\overline{\mathcal{D}^*}_N}{\mathcal{E}^*{}_N} = 1.$$

Si $n \geq 3$ et $p \geq 5$, la conjecture brunnienne $B(n, p, P)$ (respectivement : la conjecture brunienne généralisée $B(n, q, P)$) est « presque toujours vraie » lorsque $p \geq 5$ et n n'est pas divisible par $p - 1$ (respectivement : lorsque $q = p^r \geq 4$ et n n'est pas divisible par $q - 1$).

En résumé :

- les cas pour lesquels la conjecture brunnienne n'est pas encore établie complètement sont : $p = 2$, $p = 3$, $p \geq 5$ et n divisible par $p - 1$;

- les cas pour lesqueles la conjecture brunnienne généralisée n'est pas encore établie complètement sont : $q = 2$, $q = 3$, $q \geq 4$ et n divisible par $q - 1$.

Références

[1] Jean-Yves Degos, *Linear groups and primitive polynomial over* $\mathbb{F}_p$, Cah. Top. Géo. Diff. Cat. **LIV** (2013), no. 1, 286–295.

[2] ———, *On the Brunnian Conjecture*, https://arxiv.org/abs/2410.16931 (2024), 1–12.

[3] Nick Gill, *On a conjecture of Degos*, Cah. Top. Géo. Diff. Cat. **LVII** (2016), no. 3, 229–237.

[4] René Guitart, *Klein's group as a Borromean Objet*, Cah. Top. Géo. Diff. Cat. **L** (2009), no. 2, 144–155.

[5] Philippe Langevin, *Quelques polynômes primitifs*, https://langevin.univ-tln.fr/project/apc/primitif.data.

[6] Joel Brewster Lewis, *$GL_n(\mathbb{F}_q)$-analogues of some properties of n-cycles in $\mathfrak{S}_n$*, https://arxiv.org/abs/2407.20347 (2024), 1–12.

[7] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 10.6)*, 2025, https://www.sagemath.org.

Jean-Yves Degos
Direction générale de l'Insee Grand Est
Établissement de Metz
5, rue Henry Maret
F-57070 METZ
FRANCE
jean-yves.degos@insee.fr