



ON THE GENERALIZED BRUNNIAN CONJECTURE

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 4.2 et Proposition 4.4)

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 4.2 and Proposition 4.4).

Keywords. Brunnian Conjecture, finite fields, finite groups, linear groups, matrix groups, primitive polynomials.

Mathematics Subject Classification (2010). 12Y05, 20H30.

1. Introduction

The goal of this paper is to give a partial proof of the Conjecture $B(n, p, P)$ ([1, Conjecture 3.6 p. 62]). We shall refer to it as the “Brunnian Conjecture” from now on. Our strategy consists in using Nick Gill’s proof of the Conjecture $A(n, p, P)$ ([1, Conjecture 3.4 p. 62]) given in [3, Theorem 2 p. 230], corrected by the paper of Joel Brewster Lewis, see ([6, Theorem 7 p. 6 and Correction 3.3 p. 10]).

Our main result is:

Theorem 1.1. *Let p a prime number, and $n \geq 3$ an integer, and*

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

a primitive polynomial of degree n . Let $C = C_f$ denote the companion matrix of f , namely:

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

Let G denote the companion matrix of the polynomial $X^n - 1$, and let:

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

Then, if $p \geq 5$ and n is not divisible by $p-1$, then

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

2. Background and strategy

This story started with René Guitart’s works on Klein’s group (defined as the automorphisms group of the Klein’s quartic with 168 elements), described as a borromean objet ([4, section 3 p. 148]), which is nothing else that $\mathrm{GL}_3(\mathbb{F}_2)$. In [1], we extended René Guitart’s notion of borromean group

by introducing the notions of n -cyclable groups ([1, Definition 1.1 p. 58]) and n -brunnian groups ([1, Definition 1.2 and Definition 1.3 p. 58]). The so-called “Brunnian conjecture” refers to the following statement: if p is a prime number, and $n \geq 2$, then the group $\mathrm{GL}_n(\mathbb{F}_p)$ can be generated by the companion matrix of a primitive polynomial $P(X) \in \mathbb{F}_p[X]$ of degree n , and the conjugates by G^k for $1 \leq k \leq n-1$ of the companion matrix of polynomial $X^n - 1$. This conjecture is correlated to this other one: the group $\mathrm{GL}_n(\mathbb{F}_p)$ can be generated by the companion matrix of a primitive polynomial $P(X) \in \mathbb{F}_p[X]$ of degree n , denoted by C , and the companion matrix of the polynomial $X^n - 1$, denoted by G . Thus:

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

Then, Nick Gill, using the classification of finite simple groups, gave a proof of the latter statement, as a consequence of the following slightly more general result ([3, Theorem 2 p. 230]): if $\mathbb{F}$ is a finite field of order q and f, g are distinct polynomials of degree n such that f is primitive, and if the constant term of g is non-zero, then:

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

Consequently, we can infer from Nick Gill’s theroem a quite simple way to prove the Brunnian conjecture: it sufficient to build a companion matrix K (of a polynomial g of degree n) with the following properties:

- $K \in \langle G_1, G_2, \dots, G_n \rangle$;
- $g(0) \neq 0$;
- $K \neq G_1$.

Thus, as $\langle G_1, K \rangle \subset \langle G_1, G_2, \dots, G_n \rangle \subset \mathrm{GL}_n(\mathbb{F}_p)$, whenever $\langle G_1, K \rangle = \mathrm{GL}_n(\mathbb{F}_p)$, we are done!

In this paper, our main contribution is to build such a matrix K in a generic way... Our machinery works whenever $-a_0 \neq 1$ and $(-a_0)^n \neq 1$, which is guaranteed by the assumptions $p \geq 5$ and n not divisible par $p-1$. Moreover, we must assume that $n \geq 3$, as Joel Brewster Lewis pointed it out.

3. Statements and proofs

Definition 3.1. *With the notations of the main theorem, assuming $n \geq 3$, we define the matrix K by:*

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

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

Proof. We start by showing, thanks to a recurrence-based reasoning, the following result:

$$G_k G_{k-1} \cdots G_1 = G^{k-1} C (G^{-1} C)^{k-1} \text{ for all } 2 \leq k \leq n .$$

Indeed, if $k = 2$, this equality is equivalent to:

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

therefore, it is true because the right hand side equals $GC G^{-1}C = G_2 G_1$. We assume the recurrence hypothesis at rank k , and we show it at rank $k+1$. We have:

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

We then get: $G_n G_{n-1} \cdots G_1 = G^{n-1} C (G^{-1})^{n-1} C$. We conclude that:

$$\begin{aligned} G_1 G_n G_{n-1} \cdots G_1 &= G_1 G^{n-1} C (G^{-1})^{n-1} , \\ &= C G^{-1} C (G^{-1})^{n-1} , \\ &= C (G^{-1} C)^n , \end{aligned}$$

QED. □

Proposition 3.3. *Let E_k denote the k^{th} vector of the canonical basis, for $1 \leq k \leq n$. Then we get:*

1. $G^{-1}C.E_k = E_k$ for $1 \leq k \leq n-1$;
2. $G^{-1}C.E_n = -a_0E_n + \sum_{j=0}^{n-1} -a_jE_j$,

id est :

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

Proof. The first statement is a consequence of the fact that the product of the matrix G (respectively C) by the column vector E_k is equal to the column vector E_{k+1} for $1 \leq k \leq n-1$. Thus, $G^{-1}C.E_k = G^{-1}.CE_k = G^{-1}.E_{k+1} = E_k$.

To show the second statement, we proceed as follows:

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

thanks to the change of variables $j = i - 1$. □

Proposition 3.4. *We assume that $-a_0 \neq 1$. Then be the matrix $G^{-1}C$ can be written as $Q^{-1}G^{-1}CQ = D$, where $Q \in \text{GL}_n(\mathbb{F}_p)$ and D , diagonal*

matrices, express like:

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

We deduce that: $K = G^{n-1}(G^{-1}C)^n = C(QDQ^{-1})^n = CQD^nQ^{-1}$.

Proof. The chacteristic polynomial of the matrix $G^{-1}C$ is $\chi_{G^{-1}C}(X) = (X - 1)^{n-1}(X + a_0)$. Therefore, the eigenvalues are 1, of order $n - 1$ and $-a_0$, or order 1. From Propostion 3.3, (1), page 4, we can infer that Q will satisfy $Q.E_k = E_k$ for $1 \leq k \leq n - 1$. Consequently, we must find a column vector V such that $G^{-1}CV = -a_0V$, as eigenvector associated to the eigenvalue $-a_0$.

Thefore, we write :

$$V := \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}, \text{ hence } G^{-1}CV = \begin{pmatrix} v_1 - a_1v_n \\ v_2 - a_2v_n \\ \vdots \\ v_{n-1} - a_{n-1}v_n \\ -a_0v_n \end{pmatrix}, \text{ and}$$

$$-a_0V = \begin{pmatrix} -a_0v_1 \\ -a_0v_2 \\ \vdots \\ -a_0v_n \end{pmatrix}$$

Solving this Cramer linear system in $v_1, v_2, \dots, v_n$, we get:

1. $v_n \in \mathbb{F}_p$;
2. $v_i = \frac{a_i v_n}{1+a_0}$ for $1 \leq i \leq n - 1$.

We now just have to choose $v_n = 1$ to get the previously announced matrix Q . □

Proposition 3.5. *If $-a_0 \neq 1$ and $(-a_0)^n \neq 1$, the matrix*

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

is a companion matrix, different from C .

Proof. Under the action of Q and D , the column vectors E_k for $1 \leq k \leq n-1$ remain unchanged. We thus have:

$$\begin{aligned} K.E_k &= C Q D^n Q^{-1}.E_k \\ &= C.E_k \\ &= E_{k+1}. \end{aligned}$$

Therefore, we must evaluate $K.E_n = C Q D^n Q^{-1}.E_n$

Let $U := Q^{-1}E_n$. Then $E_n = QU$. To find the value of U , it is sufficient to solve the equation. However, if

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

then

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

enables to get : $u_n = \frac{1}{q_n} = 1$ (because q_n is a notation for the coefficient in row n and column n of Q , which equals 1), and:

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

Thus, we have:

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

Now, let $W := D^n U$. Then:

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

and $CQD^n U = CQW$. Now, the following holds:

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

To summarize, we get:

$$\begin{aligned} K.E_n &= CQD^n Q^{-1}.E_n \\ &= CQD^n U \\ &= CQWW \\ &= C(-a_0)^n E_n \\ &= (-a_0)^n C E_n \\ &= \sum_{i=1}^n -a_{i-1} (-a_0)^n E_i. \end{aligned}$$

Therefore, the matrix K is a companion matrix, different from C , because we assumed that $(-a_0)^n \neq 1$. $\square$

Theorem 3.6 (Main result). *Let $p \geq 5$ a prime number. Then $-a_0 \neq 1$. Moreover, if n is not divisible by $p-1$ then $(-a_0)^n \neq 1$. In this case, the Brunnian conjecture $B(n, p, P)$ is true.*

Proof. As the polynomial f is primitive, $(-1)^n a_0$ generates the multiplicative group $\mathbb{F}_p^\times$, so if $p \geq 5$, the equality $-a_0 = 1$ can not occur. Indeed, if $-a_0 = 1$ held, we would have $a_0 = -1$, then $(-1)^n a_0 = (-1)^{n+1}$ would be equal to -1 or 1 , which is never a generator of $\mathbb{F}_p^\times$ when $p \geq 5$.

If n is not divisible by $p-1$, let us assume that $(-a_0)^n = 1$ in $\mathbb{F}_p^\times$. We can write $n = (p-1)q + r$, where $1 \leq r < p-1$ is an integer. Then $(-a_0)^r = 1$, because according to our assumption, $1 = (-a_0)^n = (-a_0)^{(p-1)q}(-a_0)^r$ and $(-a_0)^{p-1} = 1$ (because $-a_0 \in \mathbb{F}_p^\times$). Now, it turns out that $(-1)^n a_0 = (-1)^{r-1}(-a_0)$ has an order which divides $r < p-1$. This is a contradiction with the fact that $(-1)^n a_0$ is a generator of $\mathbb{F}_p^\times$, the order of which is $p-1$. Consequently, if n is not divisible by $p-1$, then $(-a_0)^n \neq 1$. $\square$

4. Further remarks

In [1], we gave some “experimental checkings”, and we were unable to conclude whether the conjecture was true for certain couples (n, p) , due to a lack of power of computations and/or high complexity of calculus. Thanks to our new method, some answers can be given. We sum up them in the following tables. If “(False)” is written in last column, it means that the conjecture can be true, but it is not a consequence of the main result of this paper.

Primitive polynomials over $\mathbb{F}_5$

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

Primitive polynomials over $\mathbb{F}_7$

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

Primitive polynomials over $\mathbb{F}_{11}$

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

Primitive polynomials over $\mathbb{F}_{13}$

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

Primitive polynomials over $\mathbb{F}_{17}$

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

Primitive polynomials over $\mathbb{F}_{19}$

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

Primitive polynomials over $\mathbb{F}_{23}$

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

Primitive polynomials over $\mathbb{F}_{29}$

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

Primitive polynomials over $\mathbb{F}_{31}$

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

Primitive polynomials over $\mathbb{F}_{37}$

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

Primitive polynomials over $\mathbb{F}_{41}$

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

Primitive polynomials over $\mathbb{F}_{43}$

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

Primitive polynomials over $\mathbb{F}_{47}$

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

Primitive polynomials over $\mathbb{F}_{53}$

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

Primitive polynomials over $\mathbb{F}_{59}$

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

Primitive polynomials over $\mathbb{F}_{61}$

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

Primitive polynomials over $\mathbb{F}_{67}$

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

Primitive polynomials over $\mathbb{F}_{71}$

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

Primitive polynomials over $\mathbb{F}_{73}$

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

Primitive polynomials over $\mathbb{F}_{79}$

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

Primitive polynomials over $\mathbb{F}_{83}$

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

Primitive polynomials over $\mathbb{F}_{89}$

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

Primitive polynomials over $\mathbb{F}_{97}$

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

We shall conclude this paper by giving to results which enable to see that our results cover a large part of the cases.

Definition 4.1. *For an integer $N \geq 5$:*

1. *we denote by $\mathcal{P}(N)$ the set of prime numbers p for which the following inequalities holds: $5 \leq p \leq N$;*
2. *we denote by $\mathcal{Q}(N)$ the set of primary numbers q such that there exists a prime number $5 \leq p \leq N$ and an integer $r \geq 1$ such that $q = p^r$. Then $q \geq 4$.*

If $n \geq 3$, $N \geq 5$, and $p \in \mathcal{P}(N)$, we aim to evaluate the probability for n to is not divisible by $p - 1$, and we hope that this probability is sufficiently large. The result is given by the following proposition.

Proposition 4.2. *For $N \geq 5$, let:*

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

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

Then:

1. $\#\mathcal{E}_N = (\pi(N) - 2)(N - 2)$ and $\#\mathcal{D}_N = \sum_{p \in \mathcal{P}(N)} \left\lfloor \frac{N}{p-1} \right\rfloor$;
2. $\frac{\#\mathcal{D}_N}{\#\mathcal{E}_N} \leq \frac{\sqrt{N}}{N-2}$ and $\frac{\#\overline{\mathcal{D}}_N}{\#\mathcal{E}_N} \geq 1 - \frac{\sqrt{N}}{N-2}$.

Proof. Indeed, the number of elements in $\mathcal{P}(N)$ is the number of prime numbers less than N , except 2 and 3. Therefore:

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

Also:

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

Then the first point is proved. Now, by recurrence on $N \geq 5$, we can prove (see the Lemma 4.3 below) that:

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

.

Dividing by $\#\mathcal{E}(N)$, we get the two inequalities of the second point. $\square$

Lemma 4.3. (i) Let $p \geq 5$ a prime number with $p \leq N$ for an integer $N \geq 5$. Then:

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

Proof. Initialisation step: if $N = 5$, then $\mathcal{P}(N) = \{5\}$. Consequently :

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

Recurrence step: we must prove the if the property is true for an integer $N \geq 5$, it is also true for the integer $N + 1$. We have to justify that:

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

Either $N + 1$ is not prime, or it is.

Let us start by the case where $N + 1$ is not prime. Then $\mathcal{P}(N + 1) = \mathcal{P}(N)$, and we get:

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

QED.

Let us now manage with the case where $N + 1$ is prime. Then $\mathcal{P}(N + 1) = \mathcal{P}(N) \cup \{N + 1\}$, and we get:

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

Thanks to a property of integer part:

$$\left\lfloor \frac{k+1}{k} \right\rfloor = 1 \text{ for all non-zero integer } k,$$

we can infer that:

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

and:

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

QED. □

Proposition 4.4. *For $N \geq 5$, let:*

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

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

Then:

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

Proof. The proof is almost the same. □

Thus:

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

If $n \geq 3$ and $p \geq 5$, the Brunnian Conjecture $B(n, p, P)$ (respectively the Generalized Brunnian Conjecture $B(n, q, P)$) is “almost always true” when $p \geq 5$ and n is not divisible by $p-1$ (respectively when $q = p^r \geq 4$ and n is not divisible by $q-1$).

Acknowledgements

We thank René Guitart for our long hours of discussions on the “borromean” things.

References

- [1] [Degos J.-Y.] – Linear groups and primitive polynomial over $\mathbb{F}_p$, *Cah. Top. Géo. Diff. Cat.*, **LIV-1** (2013) 286–295.
- [2] [Degos J.-Y.] – On the Brunnian Conjecture, <https://arxiv.org/abs/2410.16931>, (2024) 1–12.
- [3] [Gill N.] – On a conjecture of Degos, *Cah. Top. Géo. Diff. Cat.*, **LVII-3** (2016) 229–237.

- [4] [Guitart R.] – Klein’s group as a borromean object, *Cah. Top. Géo. Diff. Cat.*, **L-2**, (2009) 144–155.
- [5] [Langevin P.] – Quelques polynômes primitifs,
<https://langevin.univ-tln.fr/project/apc/primitif.data>.
- [6] [Lewis J. B.] – $\mathrm{GL}_n(\mathbb{F}_q)$ -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, versions 10.6, <https://www.sagemath.org>, (2025).

Jean-Yves Degos
Insee — Établissement de Metz
5, rue Henry Maret
CS 90403
57008 Metz Cedex 1 (France)
jean-yves.degos@insee.fr