

# Numbers Related to Bernoulli-Goss Numbers

Mohamed Ould Douh Benough\*

Département de Mathématique-Informatique, Université des Sciences, de Technologie et de Médecine, Nouakchott, Mauritanie  
 \*Corresponding author: mdouh@univ-nkc.mr

Received January 12, 2014; Revised February 12, 2014; Accepted February 20, 2014

**Abstract** In this paper, we generalize a Goss result appeared in ([5], page 325, line 19, for  $i=1$ ), and give a characterization of some numbers of Bernoulli-Goss [5] by introducing the special numbers  $M(d)$ .

**Keywords:** Bernoulli-Goss, Carlitz Module, congruence, irreducible polynomials.

**Cite This Article:** Mohamed Ould Douh Benough, "Numbers Related to Bernoulli-Goss Numbers." *Turkish Journal of Analysis and Number Theory*, vol. 2, no. 1 (2014): 13-18. doi: 10.12691/tjant-2-1-4.

## 1. Introduction

Let  $\mathbb{F}_q$  be a finite field of  $q = p^n$  elements,  $q \geq 3$ ,  $p$  is the characteristic of  $\mathbb{F}_q$ ,  $n > 1$ . Let

$$B(n) = \sum_{a \in \mathbb{F}_q[T], a \text{ monic}} a^n$$

denotes the  $n$ -th Bernoulli-Goss number [5] which is a special value of the zeta function of Goss and is in  $\mathbb{F}_q[T]$ .

In the following we give a characterization of monic irreducible polynomials dividing  $B(q^d - 2)$  by introducing the numbers  $M(d)$ , for  $d = 1, 2, 3$ .

## 2. Definitions and Notations

In this section, we introduce some definitions and notation that will be used throughout the paper.

- $\mathbb{F}_q$  is a finite field of  $q$  elements,  $q$  is a power of a prime  $p$ ,  $q \geq 3$ ;
- $A = \mathbb{F}_q[T]$ ,  $k = \mathbb{F}_q(T)$ ,  $k_\infty = \mathbb{F}_q\left(\frac{1}{T}\right)$ ;
- $A^+ = \{ \text{monic} (in T) \in A \}$ ;
- Let  $P \in A$ , we say that  $P$  is prime if  $P \in A^+$  and  $P$  is irreducible;
- $v_p(\cdot)$  is the  $P$ -adic valuation where  $p$  is a prime;
- $\forall i \geq 1, [i] = T^{q^i} - T$ ;
- $L_0 = 1$ , and  $\forall i \geq 1, L_i = [i].[i-1] \dots [1]$ ;
- $D_0 = 1$ , and  $\forall i \geq 1, D_i = [i].[i-1]^q \dots [1]^{q^{i-1}}$ .

## 3. Carlitz Module

Let  $\rho$  be the Carlitz module which is a morphism of  $\mathbb{F}_q$ -algebras from  $\mathbb{F}_q[T]$  into the  $\mathbb{F}_q$ -endomorphisms of the additive group given by  $\rho_T(X) = T.X + X^q$ , for

$$a = a_n T^n + a_{n-1} T^{n-1} + \dots + a_0 \in A,$$

$$\rho_a(X) = \sum_{i=0}^{i=n} a_i \rho_{T^i}(X) = \sum_{i=0}^{i=n} \begin{bmatrix} a \\ i \end{bmatrix} X^{q^i}, \begin{bmatrix} a \\ i \end{bmatrix} \in A,$$

and

for  $\alpha \in \mathbb{F}_q, \rho_\alpha(X) = \alpha.X$

### 3.1.1. Lemma ([5], Proposition 3.3.10)

Let  $a \in A, n \in \mathbb{N}$ , then  $\begin{bmatrix} a \\ i+1 \end{bmatrix} = \frac{\begin{bmatrix} a \\ i \end{bmatrix}^q - \begin{bmatrix} a \\ i \end{bmatrix}}{[i+1]}$

Where  $[j] = T^{q^j} - T$  for  $j \geq 1$

### 3.1.2. Lemma

Let  $a \in A - \{0\}$  of degree  $n$ , then

- 1).  $\deg \begin{bmatrix} a \\ i \end{bmatrix} = q^i(n-i)$  if  $0 \leq i \leq n$
- 2).  $\begin{bmatrix} a \\ i \end{bmatrix} = 0$  if  $i \geq n+1$

#### Proof

The proof is very easy and can be done with the following

Hints:

- 1). By induction on  $i$
- 2). This is obvious.

### 3.1.3. Lemma

Let  $P$  be a prime of degree  $d$  and let  $n \geq 1$ , then

$$v_P \begin{bmatrix} P^n \\ k \end{bmatrix} = n - \left\lfloor \frac{k}{d} \right\rfloor, \text{ if } 0 \leq k \leq n$$

#### Proof

The proof can be done by induction on k. □

### 4. A remarkable Congruence

#### 4.1.1. Definition

Let  $j \in \mathbb{N}, i \in \mathbb{Z}$ , we set

1.  $S_j(i) = \sum_{a \in A^+, \deg_T a=j} a^i$   
 $E_0(X) = X$  and for  $j \geq 1$ ,
2.  $E_j(X) = \prod_{a \in A, \deg_T a < j} (X - a)$

We have :  $E_j(T^j) = D_j$ , and using Carlitz's theorem ([5], Theorem 3.1.5),

$$E_j(X) = \sum_{l=0}^{l=j} (-1)^{j-l} \frac{D_j}{D_l(L_{j-l})^{q^l}} X^{q^l}$$

Now, we present our first theorem which generalizes a result of Goss appeared in [5], page 325, line 19 for  $i=1$ .

#### 4.1.2. Theorem

Let  $1 \leq i \leq q$ , then

$$\forall j \geq 0, S_j(-i) = \frac{(-1)^{ij}}{(L_j)^i}$$

#### Proof

We have

$$E_j(X + T^j) = E_j(X) + D_j = \prod_{a \in A^+, \deg_T a=j} (X + a)$$

On the other hand, we have :

$$\frac{d}{dX} E_j(X + T^j) = (-1)^j \frac{D_j}{L_j}$$

So the logarithmic derivative of  $E_j(X + T^j)$  is:

$$(-1)^j \frac{D_j}{L_j} \frac{1}{E_j(X + T^j)} = \sum_{a \in A^+, \deg_T a=j} \frac{1}{X + a}$$

Thus

$$\frac{1}{X + a} = \frac{1}{a} \cdot \frac{1}{1 + \frac{X}{a}} = \frac{1}{a} \cdot \sum_{n \geq 0} (-1)^n a^{-n} X^n$$

Therefore:

$$\begin{aligned} \sum_{a \in A^+, \deg_T a=j} \frac{1}{X + a} &= \sum_{n \geq 0} (-1)^n X^n \sum_{a \in A^+, \deg_T a=j} a^{-(n+1)} \\ &= \sum_{n \geq 0} (-1)^n X^n S_j(-(n+1)) \end{aligned}$$

On the other hand, we have :

$$\begin{aligned} \frac{1}{E_j(X) + D_j} &= \frac{1}{D_j} \cdot \frac{1}{1 + \frac{E_j(X)}{D_j}} \\ &= \frac{1}{D_j} \cdot \sum_{m \geq 0} (-1)^m \left( \frac{E_j(X)}{D_j} \right)^m \\ &= \frac{1}{D_j} \cdot \sum_{m \geq 0} (-1)^m \cdot D_j^{-m} (E_j(X))^m \end{aligned}$$

Since

$$\begin{aligned} \frac{E_j(X)}{D_j} &= \sum_{m=0}^j (-1)^{j-m} \frac{1}{D_m(L_{j-m})^{q^m}} \cdot X^{q^m} \\ &\equiv \frac{(-1)^j}{L_j} \cdot X \pmod{X^q} \end{aligned}$$

We deduce that

$$\begin{aligned} \frac{(-1)^j D_j}{L_j} \cdot \frac{1}{E_j(X) + D_j} &= \sum_{m=0}^{q-1} \frac{(-1)^{(m+(m+1)j)}}{(L_j)^{m+1}} \cdot X^m \pmod{X^q} \end{aligned}$$

By identification, we obtain:

$$\begin{aligned} (-1)^m S_j(-(m+1)) &= \frac{(-1)^{(m+(m+1)j)}}{(L_j)^{m+1}} \\ \Rightarrow S_j(-(m+1)) &= \frac{(-1)^{(m+1)j}}{(L_j)^{m+1}} \end{aligned}$$

Therefore :  $S_j(-i) = \frac{(-1)^{ij}}{L_j^i}$

This terminates the proof. □

#### 4.1.3. Definition

We define the  $i$ -th Bernoulli-Goss numbers as follows:

$B(0) = 1$

and

$$B(i) = \sum_{j \geq 0} S_j(i) \in A, \text{ if } i \not\equiv 0 \pmod{q-1}$$

$$B(i) = \sum_{j \geq 1} j S_j(i) \in A, \text{ if } i \equiv 0 \pmod{q-1}, i \geq 1,$$

#### 4.1.4. Theorem ([11], Theorem10)

Let  $p$  be a prime of degree  $d$ ,

$0 \leq i \leq d-1$  and  $1 \leq c \leq q-2$ , then

$$B(q^d - 1 - cq^i) \equiv \left( \sum_{j=0}^{d-1} \frac{(-1)^{c \cdot j}}{L_j^c} \right)^{q^i} \pmod{P} \quad \square$$

#### Proof

We have

$$q^d - 1 - cq^i \equiv -cq^i \not\equiv 0 \pmod{q-1}.$$

Therefore

$$B(q^d - 1 - cq^i) = \sum_{m \geq 0} S_m(q^d - 1 - cq^i)$$

For  $i \in \mathbb{N}, i = a_0 + a_1q + \dots + a_nq^n, a_i \in \{0, \dots, q-1\}$ , we denote  $l(i) = a_0 + a_1 + \dots + a_n$ .

According to Sheats ([9]), we have if  $l(i) < j(q-1)$ , therefore  $S_j(i) = 0$ , thus

$$\text{for } j \geq d, S_j(q^d - 1 - cq^i) = 0.$$

Hence, it follows that:

$$\begin{aligned} B(q^d - 1 - cq^i) &= \sum_{j=0}^{d-1} S_j(q^d - 1 - cq^i) \\ &\equiv \sum_{j=0}^{d-1} S_j(-cq^i) \pmod{P} \end{aligned}$$

So according to Theorem 4.1.2, we have :

$$\begin{aligned} B(q^d - 1 - cq^i) &\equiv \sum_{j=0}^{d-1} S_j(-cq^i) \\ &\equiv \left( \sum_{j=0}^{d-1} S_j(-c) \right)^{q^i} \pmod{P} \\ &\equiv \left( \sum_{j=0}^{d-1} \frac{(-1)^{c \cdot j}}{(L_j)^c} \right)^{q^i} \pmod{P} \end{aligned}$$

This terminates the proof.  $\square$

**4.1.5. Lemma**

Let P be a premier of degree d, then

$$\frac{\begin{bmatrix} P \\ k \end{bmatrix}}{P} \equiv \frac{(-1)^k}{L_k} \pmod{P}, \text{ for } 0 \leq k \leq d-1 \quad \square$$

**Proof**

This can be shown by a combination of an induction on k, and lemma 3.1  $\square$

Now, we present the following remarkable congruence:

**4.1.6. Theorem([11], Theorem 11)**

Let P be a premier of degree d, then

$$\rho_{P-1}(1) \equiv 0 \pmod{P^2} \Leftrightarrow B(q^d - 2) \equiv 0 \pmod{P} \quad \square$$

**Proof**

We have

$$\rho_{P-1}(1) = \sum_{k=0}^{d-1} \frac{\begin{bmatrix} P \\ k \end{bmatrix}}{P} = P \times \left( \sum_{k=0}^{d-1} \frac{\begin{bmatrix} P \\ k \end{bmatrix}}{P} \right)$$

$$\begin{aligned} &\equiv P \times \left( \sum_{k=0}^{d-1} \frac{(-1)^k}{L_k} \right) \pmod{P} \\ &\equiv P \times B(q^d - 2) \pmod{P} \end{aligned}$$

Since for  $i = 0, c = 1$ , we have by Theorem 4.1.4

$$B(q^d - 1 - 1 \cdot q^0) = B(q^d - 2), \text{ and}$$

$$B(q^d - 2) \equiv \left( \sum_{j=0}^{d-1} \frac{(-1)^j}{L_j} \right)^{q^0} \equiv \left( \sum_{j=0}^{d-1} \frac{(-1)^j}{L_j} \right) \pmod{P} \quad \square$$

$$\Rightarrow \rho_{P-1}(1) \equiv 0 \pmod{P^2} \Leftrightarrow B(q^d - 2) \equiv 0 \pmod{P}$$

**5. The Numbers M(d)**

We note that :

$$\sum_{k=0}^{d-1} \frac{(-1)^k}{L_k} = \frac{1}{L_{d-1}} \cdot \sum_{k=0}^{d-1} \frac{L_{d-1}(-1)^k}{L_k}$$

**5.1. Definition**

For  $d \geq 1$ , we set

$$M(d) = \sum_{k=0}^{d-1} \frac{(-1)^k L_{d-1}}{L_k}, M(1) = 1$$

$$M(d) \in A^+ \text{ and } \deg_T M(d) = \frac{q^d - q}{q - 1} \quad \square$$

According to theorem 4.1.6 if P is a prime of degree d, then

$$\begin{aligned} \rho_{P-1}(1) \equiv 0 \pmod{P^2} &\Leftrightarrow M(d) \equiv 0 \pmod{P} \\ &\Leftrightarrow B(q^d - 2) \equiv 0 \pmod{P} \end{aligned}$$

**5.2. The Number M(2)**

**5.2.1. Lemma**

**M(2)** is the product of  $\frac{q}{p}$  distinct monic irreducible polynomials (prime) of A of degree p.

These polynomials are the divisors of the  $(q^2 - 2)$ -th Bernoulli-Goss number  $B(q^2 - 2)$ .  $\square$

**Proof**

$$\text{We have: } \frac{d}{dT}(T^q - T - 1) = -1$$

Let  $F(T)$  be a irreductible of degree d such that  $F(T)$  divides  $T^q - T - 1, d \geq 1$

Let  $\alpha \in \overline{\mathbb{F}}_q, F(\alpha) = 0, \mathbb{F}_{q^d} = \mathbb{F}_q(\alpha), d$  is the smallest integer  $k \geq 1$  such that  $\alpha^{q^k} = \alpha$

$$\begin{aligned} \alpha^q &= \alpha + 1 \neq \alpha \\ \alpha^{q^2} &= (\alpha + 1)^q = \alpha^q + 1 = \alpha + 2 \neq \alpha \\ &\vdots \\ \alpha^{q^{p-1}} &= (\alpha + 1)^q = \alpha + p - 1 \neq \alpha \\ \alpha^{q^p} &= \alpha \\ \Rightarrow d &= p. \end{aligned}$$

Because

$$\alpha^{q^p} = \alpha \Rightarrow \alpha \text{ be a root of } T^{q^p} - T$$

This proves that : P divides  $T^{q^p} - T$

$$\Rightarrow \deg_T P = 1 \text{ or } \deg_T P = p$$

But  $\alpha \notin \mathbb{F}_q \Rightarrow \deg_T P = p$ . □

The previous lemma answers the question: What are the primes of degree 2 dividing the  $q^2 - 2$ -th Bernoulli-Goss number  $B(q^2 - 2)$ ?

i. e

$$\begin{aligned} \rho_P(1) \equiv 1 \pmod{P^2} &\Leftrightarrow M(2) \equiv 0 \pmod{P} \\ &\Leftrightarrow B(q^2 - 2) \equiv 0 \pmod{P} \end{aligned}$$

**Conclusion**

- If  $p = 2$ , there is exactly  $\frac{q}{2}$  primes of degree 2 satisfying the equation
- If  $p \neq 2$ , there is no prime of degree 2 satisfying the equation.

**5.3. Number M(3)**

Let P be a prime of degree 3 which divides M(3), P is a divisor of the  $q^3 - 2$ -th Bernoulli-Goss number  $B(q^3 - 2)$

$$\begin{aligned} M(3) &= [2]M(2) + (-1)^2 \\ &= \left(T^{q^2} - T\right)\left(T^q - T - 1\right) + 1 \end{aligned}$$

Let  $\alpha \in \overline{\mathbb{F}}_q, P(\alpha) = 0, \mathbb{F}_3 = \mathbb{F}_q(\alpha)$ , and

$$M(3)(\alpha) = 0 \Rightarrow (\alpha^{q^2} - \alpha)(\alpha^q - \alpha - 1) + 1 = 0$$

Let:  $\beta = \alpha^q - \alpha$ , we have :

$$\begin{aligned} \beta^q + \beta &= (\alpha^q - \alpha)^q + (\alpha^q - \alpha) \\ &= \alpha^{q^2} - \alpha^q + \alpha^q - \alpha = \alpha^{q^2} - \alpha. \end{aligned}$$

**There is two possible cases:**

**Case 1** if  $\beta \in \mathbb{F}_q^*$ , then

$\mathbb{F}_q(\beta) = \mathbb{F}_q \Rightarrow \beta^q = \beta$  therefore  $\alpha$  is a root of the polynomial  $(T^q - T - \beta)$ , with  $\beta \in \mathbb{F}_q^*$ . We have

$$\begin{aligned} \alpha^q &= \alpha + \beta \Rightarrow (\alpha^q)^q = (\alpha + \beta)^q = \\ \alpha^{q^2} + \beta &= \alpha + \beta + \beta = \alpha + 2\beta \Rightarrow \alpha^{q^2} = \alpha + 2\beta \end{aligned}$$

Then

$$\begin{aligned} \alpha^{q^3} &= (\alpha + 2\beta)^q = \alpha^q + 2\beta = \alpha + \beta + 2\beta \\ \alpha^{q^3} &= \alpha \Rightarrow 3\beta = 0 \Rightarrow p = 3 \end{aligned}$$

Moreover :

$$(\beta^q + \beta)(\beta - 1) + 1 = 2\beta(\beta - 1) + 1 \Rightarrow \beta^2 - \beta - 1 = 0$$

if

$$\begin{aligned} \Delta &= 1 + 4 = 5 \in (\mathbb{F}_q^*)^2 \\ \Leftrightarrow q &= 3^s, s \equiv 0 \pmod{2}. \end{aligned}$$

Since

$$5 \in (\mathbb{F}_q^*)^2, 5 \notin (\mathbb{F}_3^*)^2$$

Let F an irreducible of degree d which divides  $(T^q - T - \beta) \Rightarrow F$  is of degree 3, because if  $\delta$  is a root of F, then

$$\begin{aligned} \delta^q - \delta - \beta &= 0 \Rightarrow \delta^{q^2} = (\delta + \beta)^q = \delta^q + \beta = \delta + 2\beta \\ \Rightarrow \delta^{q^3} &= \delta + 3\beta = \delta \Rightarrow \delta^{q^3} = \delta \\ \Rightarrow \delta &\text{ is a root of } T^{q^3} - T \end{aligned}$$

This proves that: F divide  $T^{q^3} - T$   
 $\Rightarrow \deg_T F = 1$  or  $\deg_T F = 3$

But  $\delta \notin \mathbb{F}_q \Rightarrow \deg_T F = 3$ . □

Therefore there is  $\frac{q}{3}$  irreducible polynomial of degree 3 which divides  $(T^q - T - \beta)$  and if F divide  $(T^q - T - \beta) \Rightarrow F$  divide  $M(3)$ .

**Conclusion:**

For  $q = p^s, s \equiv 0 \pmod{2}$ ,

there is :  $2 \cdot (\frac{q}{3})$  irreducible polynomials of degree 3 dividing M(3)

Indeed, in this case,  $5 \in (\mathbb{F}_q^*)^2$  and therefore the equation

$$X^2 - X - 1 = 0 \tag{1}$$

has two solutions in  $\mathbb{F}_q, \beta_1, \beta_2$

For each  $\beta_i, i = 1, 2$ , there is  $\frac{q}{3}$  irreducible polynomials of degree 3 which divide  $(T^q - T - \beta_i)$ , and thus divide  $(M)3$ .

Thus, if P is an irreducible of degree d which divides  $(T^q - T - \beta)$ ,  $\alpha$  is a root of P, then  $P(\alpha) = 0$ .

Therefore

$$\alpha^q - \alpha - \beta_i = 0 \Rightarrow \alpha^q - \alpha = \beta_i$$

But:

$$\begin{aligned} M(3)(\alpha) &= (\alpha^{q^2} - \alpha)(\alpha^q - \alpha - 1) + 1 \\ &= (\beta_i^q + \beta_i)(\beta_i - 1) + 1, i = 1, 2 \\ &= 2\beta_i(\beta_i - 1) + 1 = 2\beta_i^2 - 2\beta_i + 1 \\ &= \beta_i^2 - \beta_i - 1 = 0 \end{aligned}$$

Since  $\beta_i^q = \beta_i, p = 3, \beta_i$  is a root of (1).

This proves that :  $P$  divides  $M(3)$

**Case 2** if  $\beta \notin \mathbb{F}_q^*$ , then  $\mathbb{F}_q(\beta) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^3}$

$$\begin{aligned} (\beta^q + \beta)(\beta - 1) + 1 &= 0 \\ \Rightarrow (\alpha^{q^2} - \alpha)(\alpha^q - \alpha - 1) + 1 &= 0 \end{aligned}$$

Therefore:

$$\begin{aligned} \beta^q + \beta &= -\frac{1}{\beta - 1} \Rightarrow \beta^q + \beta - 2\beta = -\frac{1}{\beta - 1} - 2\beta \\ \Rightarrow \beta^q - \beta &= -\frac{1}{\beta - 1} - 2\beta \\ \Rightarrow \text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q} \left( -\frac{1}{\beta - 1} - 2\beta \right) &= 0 \end{aligned}$$

We set  $\gamma = -\frac{1}{\beta - 1} - 2\beta$

$$\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\gamma) = 0 \Rightarrow \text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q} \left( -\frac{1}{\beta - 1} \right) = 0$$

Since  $\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta) = 0, \beta = \alpha^q - \alpha$  and  $\text{Tr}$  is linear,

then

$$\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta) = 0 \Rightarrow \text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q} \left( -\frac{1}{\alpha^q - \alpha - 1} \right) = 0$$

Because:  $\alpha^q - \alpha \notin \mathbb{F}_q$ .

So we have:

$$M(3) \equiv 0 \pmod{P} \Rightarrow \text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q} \left( -\frac{1}{\alpha^q - \alpha - 1} \right) = 0$$

From :  $\mathbb{F}_q(\beta) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^3}$

Let  $Q(T) = \text{Irr}(\beta, \mathbb{F}_q, T), Q(T)$ , has degree 3

and  $Q(T) = T^3 + aT + b$ , because

$$\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\beta) = 0 \Rightarrow Q(\beta) = \beta^3 + a\beta + b = 0$$

Now we are looking for ,  $\text{Irr} \left( \frac{-1}{\beta - 1}, \mathbb{F}_q, T \right)$ ?

We look for  $F(T)$  of degree 3 such that

$$F \left( \frac{-1}{\beta - 1} \right) = 0,$$

We have :

$$\beta = \frac{1}{\beta - 1} + 1$$

And then

$$\left( \frac{1}{\beta - 1} + 1 \right)^3 + a \left( \frac{1}{\beta - 1} + 1 \right) + b = 0$$

We set

$$F_1(T) = \left( \frac{1}{T} + 1 \right)^3 + a \left( \frac{1}{T} + 1 \right) + b \Rightarrow F_1 \left( \frac{1}{\beta - 1} \right) = 0$$

and we want to get  $F \in \mathbb{F}_q[T]$

we have

$$\begin{aligned} F_1(T) &= \frac{(T+1)^3}{T^3} + a \frac{T+1}{T} + b \\ \Rightarrow F_1(T) &= \frac{(T+1)^3 + a(T+1)T^2 + bT^3}{T^3} \\ \Rightarrow F_1(T) &= \frac{F(T)}{T^3} \Rightarrow F \left( \frac{1}{\beta - 1} \right) = 0 \end{aligned}$$

So we set

$$\begin{aligned} F(T) &= T^3 F_1(T) = T^3 \left( \frac{(T+1)^3}{T^3} + a \frac{T+1}{T} + b \right) \\ &= (T+1)^3 + a(T+1)T^2 + bT^3 \\ \Rightarrow F(T) &= (1+a+b)T^3 + (3+a)T^2 + 3T + 1 \\ \text{Tr} \left( \frac{1}{\beta - 1} \right) &= 0 \Rightarrow 3+a=0 \Rightarrow a = -3 \end{aligned}$$

Therefore the polynomial is as follows

$$Q(T) = T^3 - 3T + b$$

Thus  $Q(T)$  is an irreducible of degree 3 with constant term  $b \neq 2$ , because we have  $\frac{1}{\beta - 1} \in \mathbb{F}_q$  in the other case.

□

Before concluding we will answer the following question: for  $q \geq 3$  is there infinitely many primes

$P \in \mathbb{F}_q[T]$  such that :

$$\rho_{P-1}(1) \not\equiv 0 \pmod{P^2} \tag{2}$$

**5.3.1. Proposition**

Let  $d \geq 1$ , there is at least one prime  $P \in \mathbb{F}_q[T]$  of degree  $d$  such that

$$\rho_{P-1}(1) \not\equiv 0 \pmod{P^2}$$

**Proof**

We can assume  $d \geq 2$ .

$$\deg_T M(d) = \frac{q^d - q}{q-1} < \frac{q^d}{q-1}$$

According to ([7], Proposition 5.5), we have :

$$q^d - q^{\frac{d}{l}} < dN_q(d) < q^d$$

where  $N_q(d)$  is the number of irreducible polynomials of degree  $d \in \mathbb{F}_q[T]$ ,  $l$  is the smallest prime factor of  $d$   
Therefore

$$dN_q(d) > q^d - q^{\frac{d}{2}} > q^d - \frac{q}{q-1}(q^{\frac{d}{2}} - 1)$$

If we had

$$M(d) \equiv 0 \pmod{(\prod_{P \text{ premier, } \deg_T P=d} P)}$$

we would have :

$$\begin{aligned} \deg_T M(d) &\geq q^d - \frac{q}{q-1} \left( q^{\frac{d}{2}} - 1 \right) \\ &\Rightarrow \frac{q^d}{q-1} > q^d - \frac{q}{q-1} \left( q^{\frac{d}{2}} - 1 \right) \end{aligned}$$

i.e

$$(q-2)q^d < q \left( q^{\frac{d}{2}} - 1 \right)$$

which is impossible if  $d \geq 2$ .

On the other hand:

$$dN_q(d) > q^d - \frac{q}{q-1}(q^{\frac{d}{2}} - 1)$$

Therefore

$$dN_q(d) - \deg_T M(d) > \frac{(q-2)q^d}{q-1} - \frac{q}{q-1}(q^{\frac{d}{2}} - 1)$$

Thus, there is at least

$$\frac{(q-2)q^d}{q-1} - \frac{q}{q-1}(q^{\frac{d}{2}} - 1)$$

prime of degree  $d$  which satisfy

$$\rho_{P-1}(1) \not\equiv 0 \pmod{P^2}$$

**Conclusion**

In this paper, we showed that there are infinitely many primes  $P \in \mathbb{F}_q[T]$  such that

$$\rho_{P-1}(1) \not\equiv 0 \pmod{P^2} \quad \square$$

**References**

- [1] G. Anderson. Log-Algebraicity of Twisted A-Harmonic Series and Special Values of L-series in Characteristic  $p$ , J.Number Theory 60(1996), 165-209.
- [2] B. Anglès and L. Taelman. On a Problem à la Kummer-Vandiver for function fields, to appear in J.Number Theory (2012).
- [3] L. Carlitz. An analogue of the Bernoulli polynomials. Duke Math. J.,8:405-412, 1941.
- [4] Ernst-Ulrich Gekeler. On power sums of polynomials over finite fields, J.Number Theory 30(1988), 11-26.
- [5] D. Goss. Basic Structures of Function Field Arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol.35, Springer,Berlin, 1996.
- [6] Ireland K, Rosen M I. A classical introduction to modern number theory. New York: Springer, 1982.
- [7] M. Mignotte. Algèbre Concrete, Cours et exercices.
- [8] M. Rosen. Number theory in function fields}. Springer-Verlag, New York, 2002.
- [9] J. T. Sheats. On the Riemann hypothesis for the Goss Zeta function for  $\mathbb{F}_q[T]$ , J Number Theory 71(1); (1998), 121-157.
- [10] D. Thakur. Zeta measure associated to,  $\mathbb{F}_q[T]$  J.Number Theory 35(1990), 1-17.
- [11] Mohamed Ould Douh Benough. Corps de Fonctions Cyclotomiques, Thèse Doctorat de l'Université de Caen, France (2012).