



**HAL**  
open science

## ON THE PADOVAN SEQUENCE

Alain Faisant

► **To cite this version:**

| Alain Faisant. ON THE PADOVAN SEQUENCE. 2019. hal-02131654

**HAL Id: hal-02131654**

**<https://hal.science/hal-02131654>**

Preprint submitted on 16 May 2019

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# ON THE PADOVAN SEQUENCE

ALAIN FAISANT

ABSTRACT. The aim of this article is to give some properties of the so-called Padovan sequence  $(T_n)_{n \geq 0}$  defined by

$$T_{n+3} = T_{n+1} + T_n \quad \text{for all } n \in \mathbf{N}, \quad T_1 = T_2 = T_3 = 1$$

that is divisibility properties, periods, identities.

## 1. INTRODUCTION

Let  $(T_n)_{n \geq 0}$  be the Padovan sequence, recursively defined by

$$T_{n+3} = T_{n+1} + T_n, \quad n \geq 0$$

and the initial values  $T_0 = 0, T_1 = 1, T_2 = 1$ . In this paper we consider a prime  $p$ , and give information on the index  $\omega_p$  of first occurrence of  $p$  as divisor of any  $T_n$  in the sequence. The principal result is that  $\omega_p \leq t_p \leq p^{r_p} - 1$ , where  $t_p$  is the period modulo  $p$  of  $(T_n)_{n \geq 0}$ , and  $r_p = 1, 2, 3$  the degree of the extension  $R_p/\mathbb{F}_p$ ,  $R_p$  being the splitting field of the polynomial  $T(X) = X^3 - X - 1 \pmod{p}$  associated to the Padovan sequence. We give also some technical precisions (using in particular class field theory), examples, and identities relative to the sequence  $(T_n)_{n \geq 0}$ . Many questions remain open.

## 2. DEFINITIONS

We consider the sequences recursively defined by  $x_{n+3} = x_{n+1} + x_n$ ,  $n \geq 0$ .

The choice of  $(x_0, x_1, x_2)$  determines the sequence : usually the Cordonnier-Padovan sequence is determined by the conditions  $x_1 = x_2 = x_3 = 1$ , corresponding to the choice  $x_0 = 0$  denoted here by  $(T_n)_{n \geq 0}$  : the Padovan sequence. It is convenient for us to extend  $T_{-1} = 1, T_{-2} = 0, T_{-3} = 0$ . It appears as sequence A000931 in Sloane's Online Encyclopedia of Integer Sequences [4].

This sequence is also cited in [2] as  $(R_n)_{n \geq 0}$  :  $R_n = T_{n-2}$ .

The other choice  $(3, 0, 2)$  gives the Perrin sequence  $(P_n)_{n \geq 0}$  [1].

---

2010 *Mathematics Subject Classification.* 13A05, 20M13, 11B50.

*Key words and phrases.* Divisibility, Padovan sequence, plastic number, recurrence.

The first few terms of the sequence are

$n$	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$T_n$	0	0	1	0	1	1	1	2	2	3	4	5	7	9	12	16	21	28	37	49	65	86	114	151

The associated generating series is

$$\sum_{n \geq 0} T_n X^n = \frac{1 - X}{1 - X^2 - X^3}$$

Let  $K$  be a field, and consider

$$\mathcal{T}_K = \{(x_n)_{n \geq 0} : x_n \in K, x_{n+3} = x_{n+1} + x_n, \forall n \geq 0\}$$

This is a 3-dimensional  $K$ -vector space, with explicit evident isomorphism :

$$\begin{array}{ccc} K^3 & \xrightarrow{\varphi} & \mathcal{T}_K \\ (x_0, x_1, x_2) & \mapsto & (x_n)_{n \geq 0} \end{array}$$

The  $K^3$ -basis  $\{(0, 1, 0), (1, 0, 1), (0, 1, 1)\}$  gives the  $\mathcal{T}_K$ -basis  $\{(T_{n-2})_{n \geq 0}, (T_{n-1})_{n \geq 0}, (T_n)_{n \geq 0}\}$ .

### 3. BASIS OF $\mathcal{T}_K$

We want to find a basis of  $\mathcal{T}_K$  of geometrical progressions  $(x^n)_{n \geq 0}$ , i.e.

$$x^{n+3} = x^{n+1} + x^n \quad \forall n \geq 0$$

this is equivalent to  $x^3 = x + 1$  ; so we have to solve the equation  $T(x) = 0$  in  $K$ , where

$$T(X) = X^3 - X - 1 \in K[X]$$

The general case is when  $T$  admits 3 distinct roots  $\alpha, \beta, \gamma \in K$ : there exist  $c_\alpha, c_\beta, c_\gamma \in K$  such that

$$(3.1) \quad T_n = c_\alpha \alpha^n + c_\beta \beta^n + c_\gamma \gamma^n, \quad n \geq 0$$

corresponding to a  $K$ -linear system whose (Van der Monde) determinant is

$$\delta = \begin{vmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{vmatrix} = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$$

and whose solution is

$$(3.2) \quad T_n = \frac{\alpha + 1}{(\alpha - \beta)(\alpha - \gamma)} \alpha^n + \frac{\beta + 1}{(\beta - \alpha)(\beta - \gamma)} \beta^n + \frac{\gamma + 1}{(\gamma - \alpha)(\gamma - \beta)} \gamma^n$$

Since  $1 + \alpha = \alpha^3$  we have the useful equivalent expression

$$(3.3) \quad -\delta T_n = (\beta - \gamma) \alpha^{n+3} + (\gamma - \alpha) \beta^{n+3} + (\alpha - \beta) \gamma^{n+3}$$

**Remark 3.1.** If  $T$  has a double root  $\alpha = \beta$ , a basis of  $\mathcal{T}_K$  is

$$\{(\alpha^n)_{n \geq 0}, (n\alpha^{n-1})_{n \geq 0}, (\gamma^n)_{n \geq 0}\}$$

obtained by derivation of  $\alpha^n$  with respect to the “variable”  $n$  :

$$n\alpha^{n-1} + (n-1)\alpha^{n-2} = n\alpha^{n+1} - \alpha^{n-2} = \alpha^{n+1}(n - \alpha^{-3}) = \alpha^{n+1}(n - (1 - \alpha^{-2})).$$

But  $T'(\alpha) = 3\alpha^2 - 1 = 0$  so  $\alpha^{-2} = 3$  :  $n\alpha^{n-1} + (n-1)\alpha^{n-2} = \alpha^{n+1}(n+2)$  proving that  $(n\alpha^{n-1})_{n \geq 0}$  lies in  $\mathcal{T}_K$ .

**Remark 3.2.** For the Perrin sequence  $(P_n)_{n \geq 0}$  mentioned above we have  $P_n = \alpha^n + \beta^n + \gamma^n$  : if  $p$  is prime we have  $P_p = \alpha^p + \beta^p + \gamma^p = (\alpha + \beta + \gamma)^p = 0$  in the splitting field of  $T \pmod p$  : so that

$$n \text{ prime} \implies n | P_n$$

Perrin [1] observed that, reciprocally, for many, many, non prime  $n$  we have  $n \nmid P_n$  : indeed the first counterexample is the “pseudoprime”  $n = 271441$  :  $n = 521^2$ .

#### 4. CALCULUS OF THE ROOTS $\alpha, \beta, \gamma$ OF $T(X) = X^3 - X - 1$

##### 4.1. Rational case.

If  $K = \mathbb{Q}$ , then  $T$  is irreducible and separable. Its discriminant is  $Disc(T) = -23 < 0$ , so there exists one real root, and two complexes. Cardano’s method gives explicitly the real root :

$$\psi = \sqrt[3]{\frac{1}{2} + \frac{1}{6}\sqrt{\frac{23}{3}}} + \sqrt[3]{\frac{1}{2} - \frac{1}{6}\sqrt{\frac{23}{3}}}$$

Here  $\psi \simeq 1,324718\dots$  is the **plastic number**, a Pisot number (greater than 1, and conjugate less than 1 : here  $\beta = \bar{\gamma}$  and  $\beta\gamma = 1/\psi < 1$ ). Consequently by 3.1  $\lim_{n \rightarrow +\infty} \frac{T_{n+1}}{T_n} = \psi$ .

##### 4.2. Finite case.

Here  $K = \mathbb{F}_p$  is the Galois field with  $p$  elements, and we read modulo  $p$  :

$$T(X) = X^3 - X - 1 \in \mathbb{F}_p[X]$$

We need the following lemma, which expresses two roots rationally from the third and the discriminant.

##### Lemma 4.1.

Let  $\alpha, \beta, \gamma \in \overline{\mathbb{F}_p}$  be the roots of  $T(X) = X^3 - X - 1$

i)  $\delta = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$  verifies  $\delta^2 = Disc(T) = -23 \pmod p$ ,

ii)

- if  $p \neq 2, 23$  :

$$(4.1) \quad \beta, \gamma = \frac{1}{2}[-\alpha \pm \frac{\alpha}{2\alpha + 3}\delta]$$

- if  $p = 2$  :  $\beta = \alpha^2, \gamma = \alpha^2 + \alpha$ ,

- if  $p = 23$  :  $\alpha = 3, \beta = \gamma = 10$ .

*Proof.*

i) Classically  $Disc(X^3 + pX + q) = [(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]^2 = \delta^2 = -4p^3 - 27q^2$ .

ii) For  $p = 2, 23$  : direct calculation. Else one uses the relations

$$(4.2) \quad \begin{aligned} \alpha + \beta + \gamma &= 0 \\ \alpha\beta + \beta\gamma + \gamma\alpha &= -1 \\ \alpha\beta\gamma &= 1 \\ \alpha^3 &= \alpha + 1 \end{aligned}$$

On the one hand  $\beta + \gamma = -\alpha$ , on the other hand  $\delta \neq 0$ , so  $\beta - \gamma = \frac{\delta}{(\alpha - \beta)(\gamma - \alpha)} = \dots = \frac{-\delta}{2\alpha + 3}$  ; since  $p \neq 2, \beta = \frac{1}{2}[(\beta + \gamma) + (\beta - \gamma)]$  and the formula follows.  $\square$

Define  $R_p = \mathbb{F}_p(\alpha, \beta, \gamma)$  as the splitting field of  $T$  over  $\mathbb{F}_p$ , and  $r_p = [R_p : \mathbb{F}_p]$  his degree. There exist three cases :

• if  $T$  has a root  $\alpha \in \mathbb{F}_p$

1. either  $-23$  is a square in  $\mathbb{F}_p$  :  $\delta \in \mathbb{F}_p$ , and by the lemma 4.1  $\beta, \gamma \in \mathbb{F}_p$  :  $R_p = \mathbb{F}_p$  and  $r_p = 1$  **CASE 1** (examples  $p = 23, 59, 101, 173, 211$ )

2. or  $-23$  is not a square : by the lemma 4.1  $\beta, \gamma \in \mathbb{F}_p(\delta) = \mathbb{F}_{p^2}$  ;  $R_p = \mathbb{F}_{p^2}$  and  $r_p = 2$  **CASE 2** (examples  $p = 5, 7, 11, 17$ )

• if  $T$  is irreducible in  $\mathbb{F}_p[X]$

let  $\alpha \in \overline{\mathbb{F}_p}$  be a root of  $T$ , then  $R_p = \mathbb{F}_p(\alpha) = \mathbb{F}_{p^3}$  and  $r_p = 3$  : indeed  $\mathbb{F}_p(\beta), \mathbb{F}_p(\gamma)$  are cubic extensions of  $\mathbb{F}_p$ , so are equal, to  $\mathbb{F}_{p^3}$  ; moreover in this case  $-23$  is a square in  $\mathbb{F}_p$  :  $-23 = \delta^2$  is a square in  $\mathbb{F}_{p^3}$ , so in  $\mathbb{F}_p$  :

**CASE 3** (examples :  $p = 2, 3, 13, 29, 31$ ).

By quadratique reciprocity  $-23$  is a square in  $\mathbb{F}_p$  if and only if  $p$  is a square mod 23, that is

$$p \equiv 0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \pmod{23}$$

In short

$$\begin{array}{l} \text{if } -23 \text{ square mod } p \\ \text{if } -23 \text{ not square mod } p \end{array} \quad \begin{array}{l} \swarrow \\ \searrow \end{array} \quad \begin{array}{l} \alpha \in \mathbb{F}_p \quad R_p = \mathbb{F}_p \quad r_p = 1 \\ T \text{ irreducible} \quad R_p = \mathbb{F}_{p^3} \quad r_p = 3 \\ \alpha \in \mathbb{F}_p \quad R_p = \mathbb{F}_{p^2} \quad r_p = 2 \end{array}$$

## 5. PRIME DIVISORS IN THE SEQUENCE $(T_n)_{n \geq 0}$

We are interested in the first occurrence of the prime  $p$  in the Padovan sequence. In the case of the Fibonacci sequence  $(F_n)_{n \geq 0}$ , the answer is easy, linked with the order of  $\Phi/\overline{\Phi}$  mod  $p$  (where  $\Phi$  is the golden ratio,  $\overline{\Phi}$  the conjugate of  $\Phi$ ) : this is a divisor of  $p - 1$  or  $p + 1$  according to

$p \equiv \pm 1, p \equiv \pm 2 \pmod{5}$ . Here it is much more complicated.

We adopt the following notations

- $t_p =$  period of the sequence  $(T_n)_{n \geq 0}$
- $\Omega_p = \{n \geq 1 : p \text{ divide } T_n\}$
- $\omega_p = \min \Omega_p$  : index of first occurrence of  $p$  in the sequence  $(T_n)_{n \geq 1}$
- $A_p = \Omega_p \cap \{1, 2, \dots, t_p\}$
- $a = o(\alpha), b = o(\beta), c = o(\gamma)$  (orders in  $R_p^\times$  : divisors of  $p^{r_p} - 1$ )

### 5.1. Principal results.

#### Theorem 5.1.

Let  $R_p = \mathbb{F}_p(\alpha, \beta, \gamma), r_p = [R_p : \mathbb{F}_p], r_p = 1, 2, 3$

1) for all  $p : t_p - 3, t_p - 2, t_p \in A_p$ , hence  $\omega_p \leq t_p - 3$

2)  $\Omega_p = A_p + \mathbf{N}t_p$

3) if  $p \neq 23 : t_p = \text{LCM}\{a, b, c\}$ , and it divides  $p^{r_p} - 1$

4) if  $p = 23 : t_{23} = 506 = p(p - 1)$ , and  $r_p = 1$

5) moreover :

- ♣  $r_p = 1$  if and only if  $p = x^2 + 23y^2$
- ♣ if  $r_p = 2$  :
  - $\alpha \in \mathbb{F}_p$ , and  $t_p = b = c$
  - $b$  divide  $(p + 1)a$
  - $\omega_p \leq (p + 1)o(\alpha^3) - 3$
- ♣ if  $r_p = 3$  :  $t_p = a = b = c$  divide  $\frac{p^3 - 1}{p - 1} = p^2 + p + 1$ .

**Corollary 5.2.** For every prime  $p$  there exists  $n \geq 1$  such that  $p$  divides  $T_n$ , and the index  $\omega_p$  verifies :  $\omega_p \leq p^3 - 4$ .

*Proof.* By definition  $t_p = \min\{n \geq 1 : T_n \equiv 0, T_{n+1} \equiv 1, T_{n+2} \equiv 1 \pmod{p}\}$ . Along the proof we denote  $t_p = t$ .

1) Since  $T_t = 0, T_{t+1} = 1, T_{t+2} = 1$ , by ‘‘redshift’’ we deduce  $T_{t-1} = 1, T_{t-2} = 0, T_{t-3} = 0$ .

2) Let  $n \in \Omega_p : n = ut + v, 0 \leq v \leq t - 1$  ; we have  $T_t = T_0, T_{t+1} = T_1, T_{t+2} = T_2$ , so induction gives  $T_{t+m} = T_m$ , then (induction on  $u$ )  $T_{ut+m} = T_m$  ; so here  $T_n = T_v$  ;  $n \in \Omega_p \Rightarrow T_n = 0$ , so  $T_v = 0$  and  $v \in \Omega_p \cap \{1, \dots, t\} = A_p$ .

3) Let  $s = \text{LCM}\{a, b, c\}$  ;  $p \neq 23 \Rightarrow \delta \neq 0$ . Apply 3.3 :  $-\delta T_{s-3} = \beta - \gamma + \gamma - \alpha + \alpha - \beta = 0$ , so  $T_{s-3} = 0$ .

Similarly  $-\delta T_{s-2} = (\beta - \gamma)\alpha + (\gamma - \alpha)\beta + (\alpha - \beta)\gamma = 0$ , so  $T_{s-2} = 0$ , and  $T_s = T_{s-2} + T_{s-3} = 0$ .

3.3:  $-\delta T_{s-1} = (\beta - \gamma)\alpha^2 + (\gamma - \alpha)\beta^2 + (\alpha - \beta)\gamma^2 = -\delta$ , so  $T_{s-1} = 1$ . Hence

$$T_s = 0, T_{s+1} = 0, T_{s+2} = 1 \Rightarrow t \leq s$$

On the other hand, following 3.1

$$\begin{aligned} T_t &= c_\alpha \alpha^t &+& c_\beta \beta^t &+& c_\gamma \gamma^t &= 0 \\ T_{t+1} &= c_\alpha \alpha^{t+1} &+& c_\beta \beta^{t+1} &+& c_\gamma \gamma^{t+1} &= 1 \\ T_{t+2} &= c_\alpha \alpha^{t+2} &+& c_\beta \beta^{t+2} &+& c_\gamma \gamma^{t+2} &= 1 \end{aligned}$$

This proves that  $(c_\alpha \alpha^t, c_\beta \beta^t, c_\gamma \gamma^t)$  is solution of the system

$$\begin{cases} x + y + z = 0 \\ \alpha x + \beta y + \gamma z = 1 \\ \alpha^2 x + \beta^2 y + \gamma^2 z = 1 \end{cases}$$

Its determinant is  $(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = \delta \neq 0$  and its unique solution is  $(c_\alpha, c_\beta, c_\gamma)$ ; so necessarily

$$\begin{aligned} c_\alpha \alpha^t &= c_\alpha \\ c_\beta \beta^t &= c_\beta \\ c_\gamma \gamma^t &= c_\gamma \end{aligned}$$

$c_\alpha \neq 0$  since  $\alpha \neq -1 : T(-1) = -1 \neq 0$ ; we conclude that  $\alpha^t = \beta^t = \gamma^t = 1$ , and  $s = LCM\{o(\alpha), o(\beta), o(\gamma)\}$  divides  $t$ , and finally  $s = t = t_p$ .

4) The case  $p = 23$  is different (cf 3.1) : here  $3T_n = 4.3^n - 4.10^n + 8.n.10^{n-1}$ ; we have to solve the equation  $(-2)^n = 9n + 1$  giving  $n = 503$  and  $t_{23} = 506 = 22 \times 23$ .

5)

♣  $r_p = 1 \Leftrightarrow p = x^2 + 23y^2$  see below 5.3

♣  $r_p = 2$  :  $\alpha \in \mathbb{F}_p, \beta, \gamma = \frac{1}{2}[-\alpha \pm \frac{\alpha}{2\alpha+3}\sqrt{-23}]$  are conjugate in  $\mathbb{F}_p(\sqrt{-23})$  hence have same order  $b = c$ ; moreover  $\alpha = \frac{1}{\beta\gamma} \Rightarrow \alpha^b = 1 : a|b$  and  $t_p = b = c$ .

The Frobenius  $x \mapsto x^p$  coincides with the conjugation :  $\beta^p = \gamma, \beta^{p+1} = \beta\gamma = \frac{1}{\alpha}$ , and  $\beta^{(p+1)a} = 1 : b|(p+1)a$ .

Let  $m \geq 1$  :  $\alpha^{m(p+1)} = \alpha^{2m}(\alpha^{p-1} = 1); \beta^{m(p+1)} = \alpha^{-m}, \gamma^{m(p+1)} = \alpha^{-m}$ ; by 3.3 :

$-\delta T_{m(p+1)-3} = (\beta - \gamma)\alpha^{2m} + (\gamma - \alpha)\alpha^{-m} + (\alpha - \beta)\alpha^{-m} = (\beta - \gamma)\alpha^{-m}(\alpha^{3m} - 1)$ . The choice  $m = o(\alpha^3)$  gives  $m(p+1) - 3 \in \Omega_p$ . Example :  $p=7, \alpha = 5, \alpha^3 = -1$ , hence  $2(7+1) - 3 = 13 \in \Omega_p$ .

♣  $r_p = 3$  :  $\alpha, \beta, \gamma$  are conjugate so  $a = b = c$ ; by Frobenius  $x \mapsto x^p$  :  $\alpha^p = \beta$  or  $\gamma, \alpha^{p^2} = \gamma$  or  $\beta$ , and  $\alpha\beta\gamma = 1 = \alpha\alpha^p\alpha^{p^2} : a = b = c|1 + p + p^2$ .  $\square$

**Remark 5.3.** The analog of the theorem may be done for the Tribonacci sequence :  $\omega_p \leq p^3 - 2; r_p = 1$  for  $p = 47, 53, 269, \dots$ ;  $r_p = 2$  for  $p = 13, 17, 19, \dots$ ;  $r_p = 3$  for  $p = 3, 5, 23 \dots$

It may happen that two consecutive terms are divisible by  $p$ .

**Proposition 5.4.** *If  $p \neq 23$ , the following assertions are equivalent :*

- i)  $\alpha^n = \beta^n = \gamma^n$
- ii)  $p|T_{n-3}$  and  $p|T_{n-2}$ .

*Proof.*

i)  $\Rightarrow$  ii) : by 3.3.

ii)  $\Rightarrow$  i) : by hypothesis and 3.3 :

$$(5.1) \quad (\alpha - \beta)\gamma^n = (\gamma - \beta)\alpha^n + (\alpha - \gamma)\beta^n \text{ and}$$

$$(5.2) \quad (\alpha - \beta)\gamma^{n+1} = (\gamma - \beta)\alpha^{n+1} + (\alpha - \gamma)\beta^{n+1}$$

5.1  $\Rightarrow$   $(\alpha - \beta)\gamma^{n+1} = (\gamma - \beta)\alpha^n\gamma + (\alpha - \gamma)\beta^n\gamma = (\text{by 5.2})(\gamma - \beta)\alpha^{n+1} + (\alpha - \gamma)\beta^{n+1}$ ; so  $(\gamma - \beta)\alpha^n(\alpha - \gamma) + (\alpha - \gamma)\beta^n(\beta - \gamma) = 0$ , and  $(\gamma - \beta)(\alpha - \gamma)(\alpha^n - \beta^n) = 0$ ;  $p \neq 23 \Rightarrow \alpha^n = \beta^n$ . In the same way  $\beta^n = \gamma^n$ .  $\square$

For example if  $p = 7$  we have  $\alpha^{16} = \beta^{16} = \gamma^{16} = 2$ , so  $7|T_{13}$  and  $7|T_{14}$ .

**5.2. Examples.**

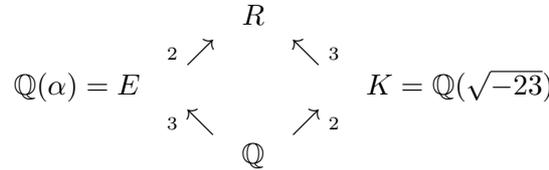
$p$	roots and orders	$t_p$	$\omega_p$	$A_p$	$\sqrt{-23}$	$r_p$
3	$\alpha$ <span style="float:right"><math>a = 13</math></span>	13	6	6, 10, 11, 13	$\pm 1$	3
	$\beta = \alpha + 1$ <span style="float:right"><math>b = 13</math></span>					
	$\gamma = \alpha - 1$ <span style="float:right"><math>c = 13</math></span>					
7	$\alpha = 5$ <span style="float:right"><math>a = 6</math></span>	48	9	9, 13, 14, 16, 25, 29 30, 32, 41, 45, 46, 48	$\pm\sqrt{-2}$	2
	$\beta = 1 + 2\sqrt{-2}$ <span style="float:right"><math>b = 48</math></span>					
	$\gamma = 1 - 2\sqrt{-2}$ <span style="float:right"><math>c = 48</math></span>					
11	$\alpha = 6$ <span style="float:right"><math>a = 10</math></span>	120	25	25, 35, 43, 64, 87, 98 104, 113, 117, 118, 120	$\pm\sqrt{-1}$	2
	$\beta = -3 + 2\sqrt{-1}$ <span style="float:right"><math>b = 120</math></span>					
	$\gamma = -3 - 2\sqrt{-1}$ <span style="float:right"><math>c = 120</math></span>					
59	$\alpha = 4$ <span style="float:right"><math>a = 29</math></span>	58	42	42, 51, 55, 56, 58	$\pm 6$	1
	$\beta = 13$ <span style="float:right"><math>b = 58</math></span>					
	$\gamma = 42$ <span style="float:right"><math>c = 58</math></span>					

The last three elements of  $A_p$  are predicted by the theorem.

**5.3. The sequence  $(T_n)_{n \geq 0}$  and class field theory.**

We refer to the text [3] which gives similar results for the Tribonacci sequence.

Here  $K = \mathbb{Q}(\sqrt{-23})$  : the class number is  $h_K = 3$ , the ring of integers is  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-23}]$ . Denote by  $R = \mathbb{Q}(X^3 - X - 1) \subset \mathbb{C}$  the splitting field of  $T(X) = X^3 - X - 1$ , and  $\alpha \in \mathbb{C}$  a root of  $T$ .



1-  $\mathcal{O}_E = \mathbb{Z}[\alpha]$  : indeed  $Disc(\alpha) = Disc(T) = -23$  is squarefree.

2- Every  $p \neq 23$  is unramified in  $R/\mathbb{Q}$  : by Kummer–Dedekind theorem ( $\mathcal{O}_E = \mathbb{Z}[\alpha]$ )  $p$  in unramified in  $E$ , also in the Galois closure  $R$  of  $E$ .

3-  $P_{23} = \sqrt{-23}\mathcal{O}_K$  is unramified in  $R/K$ : we have  $T \pmod{23} = (X - 3)(X - 10)^2$  ; By Kummer–Dedekind  $23\mathcal{O}_E = P_1P_2^2$  with  $3 = e_1f_1 + e_2f_2$ , so  $e = 1 = f_1 = 1, e_2 = 2, f_2 = 1$ .

$R/K$  is Galois; we have  $P_{23}\mathcal{O}_R = (\mathfrak{Q}_1 \dots \mathfrak{Q}_g)^e, efg = 3$  ; then  $e = 1$  : else  $e = 3$  ; let  $\mathfrak{P}|P_{23}$  in  $R$  :

$$e_{R/\mathbb{Q}}(\mathfrak{P}) = e_{R/K}(\mathfrak{P}).e_{K/\mathbb{Q}}(P_{23}) = 3 \times 2 = 6, \text{ and}$$

$$e_{R/\mathbb{Q}}(\mathfrak{P}) = e_{R/E}(\mathfrak{P}).e_{E/\mathbb{Q}}(P_1 \text{ or } P_2) = [1 \text{ or } 2] \times [\leq 3]$$

necessarily  $e_{R/E}(\mathfrak{P}) = 2$ , and  $e_{E/\mathbb{Q}}(P_i) = 3(i = 1, 2)$ , but  $e_{E/\mathbb{Q}}(P_i) = 1$  or  $2$  : contradiction.

4-  $K$  being imaginary,  $R/K$  is unramified at infinity : so  $R/K$  is abelian unramified and  $[R : K] = 3 = h_K$  ; we conclude that  $R$  is the Hilbert class field of  $K$ .

5- Application :

- if  $p \neq 23$  with  $r_p = 1$  we have  $T \bmod p = (X - \alpha)(X - \beta)(X - \gamma) \in \mathbb{F}_p[X]$  : Kummer-Dedekind shows that  $p\mathcal{O}_E = P_1P_2P_3$  :  $p$  is totally decomposed in  $E$ , and idem in the Galois closure  $R$  of  $E$ , a fortiori in  $K$  :  $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ , and  $\mathfrak{P}_1, \mathfrak{P}_2$  are totally decomposed in the Hilbert class field  $R$  ; by the Artin reciprocity law  $\mathfrak{P}_1$  is a principal ideal :  $\mathfrak{P}_1 = (x + y\sqrt{-23})\mathcal{O}_K$  ; norm :  $p = x^2 + 23y^2$ .
- Reciprocally if  $p = x^2 + 23y^2$  we have  $p\mathcal{O}_K = (x + y\sqrt{-23})\mathcal{O}_K.(x - y\sqrt{-23})\mathcal{O}_K$  :  $p$  is totally decomposed in  $K$ . By Artin reciprocity law ,  $(x + y\sqrt{-23})\mathcal{O}_K$  being principal, we conclude it is totally decomposed in  $R$ , and also in  $E$  :  $p\mathcal{O}_E = P_1P_2P_3$  and Kummer-Dedekind show that  $r_p = 1$ .

We have proved

**Theorem 5.5.**  $r_p = 1 \iff p = x^2 + 23y^2$

Clearly  $p = 23$  is not a problem for the assertion!

## 6. SOME IDENTITIES FOR $(T_n)_{n \geq 0}$

### 6.1.

For all  $m$   $(T_{m+n})_{n \geq 0} \in \mathcal{T}_K$ , so there exist  $u, v, w \in K$  such that  $T_{m+n} = uT_n + vT_{n-1} + wT_{n-2}$ . Applying this for  $n = 0, n = 1, n = 2$ , we obtain the system

$$\begin{cases} v & = & T_m \\ u + w & = & T_{m+1} \\ u + v & = & T_{m+2} \end{cases}$$

Easy calculations give :

$$(6.1) \quad T_{m+n} = T_{m-1}.T_n + T_m.T_{n-1} + (T_{m+1} - T_{m-1}).T_{n-2}$$

As application let  $m = n$  :

$$T_{2n} = 2T_{n-1}T_n + (T_{n+1} - T_{n-1})T_{n-2}$$

if  $p|T_{n-2}$  and  $p|T_{n-1}$  also  $p|T_{2n}$ . On can verify that  $p = 7|T_{13}$  and  $p|T_{14}$ , so  $p|T_{30}$ .

### 6.2.

The well-know formula related to the Fibonacci sequence  $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$  ("Fibonacci-puzzle") can be proved like this : one prove first that  $\Phi^n = F_n\Phi + F_{n-1}$ , and the analog with  $\bar{\Phi}$  conjugate of  $\Phi$  ; since  $\Phi.\bar{\Phi} = -1$ , one has  $(\Phi.\bar{\Phi})^n = (-1)^n = (F_n\Phi + F_{n-1})(F_n\bar{\Phi} + F_{n-1})$  and the identity follows. We use here the same idea.

As  $(\alpha^n)_{n \geq 0} \in \mathcal{T}_K$ , there exist  $u, v, w \in K$  such that  $\alpha^n = uT_n + vT_{n-1} + wT_{n-2}$  : easy calculations give

$$(6.2) \quad \alpha^n = (\alpha^2 - 1)T_n + T_{n-1} + (1 + \alpha - \alpha^2)T_{n-2}$$

and the analog for  $\beta^n, \gamma^n$ . Write now  $\alpha^n\beta^n\gamma^n = 1$ :

$$[(\alpha^2 - 1)T_n + T_{n-1} + (1 + \alpha - \alpha^2)T_{n-2}] \dots$$

$$\dots [(\beta^2 - 1)T_n + T_{n-1} + (1 + \beta - \beta^2)T_{n-2}] \cdot [(\gamma^2 - 1)T_n + T_{n-1} + (1 + \gamma - \gamma^2)T_{n-2}] = 1$$

The left member is a polynomial  $P(T_n, T_{n-1}, T_{n-2}) = \sum_{(a,b,c)} c_{abc} T_n^a T_{n-1}^b T_{n-2}^c$  homogeneous of degree 3 :  $a + b + c = 3$ , and the  $c_{abc}$  are symmetric polynomials in  $\alpha, \beta, \gamma$ , so polynomials in the elementary symmetric functions  $s_1 = \alpha + \beta + \gamma = 0$ ,  $s_2 = \alpha\beta + \beta\gamma + \gamma\alpha = -1$ ,  $s_3 = \alpha\beta\gamma = 1$ . After long calculations we find

$$(6.3) \quad T_n^3 + T_{n-1}^3 + T_{n-2}^3 - T_n T_{n-1}^2 - T_n^2 T_{n-2} + T_{n-1}^2 T_{n-2} + 2T_{n-1} T_{n-2}^2 - 3T_n T_{n-1} T_{n-2} = 1$$

## 7. QUESTIONS

We have many questions !

$Q_1$ – In the case  $r_p = 1$  it seems that  $b = c = 2a$  : is it true ?

$Q_2$ – In the case  $r_p = 2$  it seems that  $b = c = (p + 1)a$  : is it true ?

$Q_3$ – When  $r_p = 3$  :  $a = b = c$  ; some examples show that  $a = 1 + p + p^2$  : is it true ?

$Q_4$ – What is the exact arithmetical nature of  $\omega_p$ , of  $A_p$  ?

$Q_5$ – Primitive divisors : the computations give many exceptions :

$$n = 5, 7, 10, 11, 12, 13, 14, 16, 21, 23, 32, 33, 45, \dots$$

Are there finitely many ?

$Q_6$ –  $T_n$  is prime for

$$n = 4, 5, 6, 8, 9, 15, 20, 31, 38, \dots$$

Are there infinitely many ?

$Q_7$ – We find the following square in  $(T_n)_{n \geq 0}$  :

$$T_{10} = 9, T_{12} = 16, T_{16} = 49$$

Are there finitely many squares ?

Observe that  $\sqrt{9} = 3 = T_6$ ,  $\sqrt{16} = 4 = T_7$ ,  $\sqrt{49} = 7 = T_9$  : is it a coincidence ?

Finally the author thanks F. Nuccio for his (im)pertinent galoisian observations !



## REFERENCES

- [1] R.Perrin *Question 1484*  
L'intermédiaire des mathématicques **6** (1899) 76-77.
- [2] A.G. Shannon, P.G. Anderson, A.F. Horadam, *Properties of Cordonnier, Perrin and Van der Laan numbers*  
International Journal of Mathematical Education in Science and Technology, **37**, n 7, (2006), 825-831.
- [3] T. Evink, P.A. Helminck *Tribonacci numbers and primes of the form  $p = x^2 + 11y^2$*   
Math Slovaca **69** no 3 (2019), to appear.
- [4] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*  
Notices Amer. Math. Soc. **50** (8) (2003), 912-915.
- [5] I. Stewart, *Tales of a Neglected Number*  
Sci. Amer. **274** (1996), 102-103.