Winter Cup 4

Rami Zouari Oussema Jeballah Yessine Jallouli

February 12, 2022

Abstract

In this article, we will cite the official Winter Cup 4 problems with their solutions.

Contents

I Rami's Scheme **3**

1 Problem Statement **3**

2 Solution using Pattern Matching **4**

3 Solution using Linear Algebra **5**
3.1 Notes . . . 5
3.2 Definitions . . . 5
3.3 Strategy . . . 6
3.4 Recurrence Relation . . . 6
3.5 Period Estimation . . . 7
3.5.1 Case 1 : $b \neq 0$ . . . 7
3.5.2 Case 2 : $b = 0,\ \&\ a \neq 0$ . . . 7
3.5.3 Case 3 : $a = b = 0:$ . . . 8
3.6 Limitations . . . 8

4 Solution using Linear Search **9**
4.1 Notes . . . 9
4.2 Strategy . . . 9
4.3 Complexity . . . 9

5 Solution using Matrices **10**
5.1 Definitions . . . 10
5.2 Strategy . . . 10
5.3 Case 1 : $B \in \mathtt{GL}_2(\mathbb{F}_p)$ . . . 11
5.4 Case 2 : χ_B has a simple root 0 . . . 11
5.5 Case 3 : χ_B has a double root 0 . . . 13

5.6 Period Estimation 15
5.7 Complexity 15

6 Solution using Ring Theory **16**
6.1 Definitions 16
6.2 Analysis of Ψ function 17
6.3 Strategy 21
6.4 Solving $\chi_A(x) = 0$ over $\mathbb{F}_p$ 21
6.5 Case 1 : χ_A is irreducible over $\mathbb{F}_p$ 22
6.6 Case 2 : χ_A has simple roots 23
6.7 Case 3 : χ_A has a double root φ 24
6.8 Period Estimation 27
6.8.1 Probabilistic Method 27
6.8.2 Deterministic Method 27
6.9 Complexity 27

II Mean Absolute Deviation **28**

Part I
Rami's Scheme

1 Problem Statement

Rami always was fond of random numbers, he always wonders how randomness arises from the deterministic nature of mathematics.

Wanting to impress his friends, he created a new pseudo-random number generation scheme, that he proudly called Rami Scheme

a **Rami scheme** consists of the following steps:

1. choose 4 integer parameters: m, a, b such that $0 \leq a, b, < m$ with m prime
2. choose 2 seeds $0 \leq u_0, u_1 < m$
3. for $k > 1$, u_k will be generated with the following rule:

$$u_k = (au_{k-1} + bu_{k-2}) \bmod m$$

4. using the rule above, he will calculate many such numbers and use them to generate the following random numbers $(v_k)_{k\in\mathbb{N}}$:

$$v_k = \left(\sum_{i=0}^{k} iu_i\right) \bmod m$$

5. Finally, after calculating many terms $v_0, \ldots, v_{10^{18}}$, he will choose s numbers $v_{n_1}, \ldots, v_{n_s}$. those final numbers will be the chosen random numbers

Rami wants you to test his scheme, so he asks you for help.

- First of all, he wants you to measure the robustness index R of this scheme, which is defined as the eventual fundamental period of the sequence $(v_k)_{k\in\mathbb{N}}$. In other words,he wants the smallest strictly positive integer R such that:

$$\exists N \in \mathbb{N} / \quad \forall k \in \mathbb{N}_{\geq N}, v_{k+R} = v_k$$

- After that, he knows that he cannot calculate all terms of the sequence $(v_k)_{k\in\mathbb{N}}$, and he only needs s terms $v_{n_1}, \ldots, v_{n_s}$ of the sequence. So he asks your help for it

2 Solution using Pattern Matching

3 Solution using Linear Algebra

3.1 Notes

This solution is not powerful enough to give an estimation about the fundamental period. So to use it, we shall extract the initial guess of the fundamental period from another solution.
Still, It won't be accepted due to time constraints despite having the same complexity as the accepted ones.

3.2 Definitions

Term	Definition
$\mathbb{N}$	Set of natural numbers: $\{0, 1, \dots\}$
$\mathbb{P}$	Set of prime numbers
p	the prime number used for the Scheme
$\mathbb{F}_p$ or $\mathbb{Z}/p\mathbb{Z}$	the cyclic field of order p
$\mathbb{K}$ [1]	a field
$\mathcal{R}$	a commutative ring
$\mathcal{R}[x]$	the ring of polynomials over $\mathcal{R}$
$\mathtt{M}_m(\mathbb{K})$	The associative algebra of $m \times m$ matrices over $\mathbb{K}$
$\mathtt{GL}_m(\mathbb{K})$	The group of $m \times m$ invertible matrices over $\mathbb{K}$
I_m	the identity matrix of $\mathtt{M}_m(\mathbb{K})$
$\langle M \rangle$	$= \left\{M^0, M^1, M^2, \dots\right\}$
a, b	parameters of the scheme
u_0, u_1	seeds
$(w_n)_{n\in\mathbb{N}}$	a sequence in $\mathbb{F}_p^{\mathbb{N}}$
Δ	forward difference operator
$\Phi(w)$	$= (w_{n+2} - aw_{n+1} - bw_n)_{n\in\mathbb{N}}$
$\mathtt{EP}(S)$	eventual fundamental period of a sequence $(S_n)_{n\in\mathbb{N}}$

[1] Note that $\mathbb{K}$ in this solution is a field with characteristic p. More precisely, it is either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$

3.3 Strategy

The sequence $(u_n)_{n\in\mathbb{N}}$ satisfies second order linear homogeneous recurrence relation.
We will show that $(v_n)_{n\in\mathbb{N}}$ will also satisfies a linear homogeneous recurrence relation of a higher order r.

Let $(V_n)_{n\in\mathbb{N}} \in \left(\mathbb{F}_p^r\right)^{\mathbb{N}}, M \in \mathtt{M}_r(\mathbb{F}_p)$ such that:

$$\begin{cases} V_0 &= \begin{pmatrix} v_0 \\ \vdots \\ v_{r-1} \end{pmatrix} \\ V_n &= MV_{n-1} \end{cases}$$

Assuming we can quickly find r and M, the problem is thus reduced to the calculation of:

$$\boxed{V_n = M^n V_0 \quad \forall n \in \{n_1, \ldots, n_s\}}$$

The multiplicative order of $(v_n)_{n\in\mathbb{N}}$ is equal to that of $(V_n)_{n\in\mathbb{N}}$, which is a divisor of the cardinality of the biggest group $G \subset \langle M \rangle$.
To be more precise:

$$|G| = \mathtt{EP}\left((M^n)_{n\in\mathbb{N}}\right)$$

3.4 Recurrence Relation

Recurrence relation of Δv : We have:

$$\begin{aligned} \forall n \in \mathbb{N}, \quad \Phi(\Delta v)_n &= \Delta v_{n+2} - a\Delta v_{n+1} - b\Delta v_n \\ &= (n+2)u_{n+2} - a(n+1)u_{n+1} - bnu_n \\ &= 2u_{n+2} - au_{n+1} \end{aligned}$$

As a consequence, we have then:

$$\boxed{\Phi^2(\Delta v) = 0}$$

Recurrence relation of v : The relation above can also be seen as a recurrence relation of (v_n). It can be unpacked to:

$$\begin{aligned} \forall n \in \mathbb{N}, \quad \Phi^2(\Delta v)_n &= \Delta v_{n+4} - a\Delta v_{n+3} - b\Delta v_{n+2} - a\Delta v_{n+3} + a^2\Delta v_{n+2} + ab\Delta v_{n+1} \\ &\quad - b\Delta v_{n+2} + ab\Delta v_{n+1} + b^2\Delta v_n \\ &= \Delta v_{n+4} - 2a\Delta v_{n+3} + (a^2 - 2b)\Delta v_{n+2} + 2ab\Delta v_{n+1} + b^2\Delta v_n \\ &= v_{n+5} - (1+2a)v_{n+4} + (a^2 - 2b + 2a)v_{n+3} + (2ab - a^2 + 2b)v_{n+2} \\ &\quad + (b^2 - 2ab)v_{n+1} - b^2 v_n \\ &= 0 \end{aligned}$$

As a conclusion, we have $r = 5$, and:

$$\boxed{\begin{aligned}\forall n \in \mathbb{N} \quad v_{n+5} = {} & (1+2a)v_{n+4} - (a^2 - 2b + 2a)v_{n+3} \\ & - (2ab - a^2 + 2b)v_{n+2} - (b^2 - 2ab)v_{n+1} + b^2 v_n\end{aligned}}$$

Finding the matrix M : It is the companion matrix of this linear homogeneous recurrence relation. It is equal to:

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ b^2 & b(2a-b) & a^2 - 2b - 2ab & 2a + 2b - a^2 & 1 + 2a \end{pmatrix}$$

3.5 Period Estimation

It is clear that $\det M = b^2$.

3.5.1 Case 1 : $b \neq 0$

We have then $M \in \mathtt{GL}_5(\mathbb{F}_{,})$, and thus $\langle M \rangle$ is a subgroup of $\mathtt{GL}_5(\mathbb{F}_p)$. By Lagrange's theorem:

$$|\langle M \rangle| \text{ divides } |\mathtt{GL}_5(\mathbb{F}_p)|$$

As a conclusion:

$$\mathtt{EP}(v) \mid |\mathtt{GL}_5(\mathbb{F}_p)| = \prod_{i=0}^{4}(p^5 - p^i)$$

3.5.2 Case 2 : $b = 0,\ \&\ a \neq 0$

Let $\Lambda(w) = (w_{n+1} - aw_n)_{n \in \mathbb{N}}$.
We have then

$$\begin{aligned}\forall n \in \mathbb{N}^*, \Lambda^2(\Delta v) &= \Lambda(\Delta v)_{n+1} - a\Lambda(\Delta v)_n \\ &= \Lambda((n+1)u)_{n+1} - a\Lambda(nu)_n \\ &= \Lambda(u)_n \\ &= 0 \\ &= \Delta v_{n+2} - 2a\Delta v_{n+1} + a^2\Lambda(\Delta v)_n \\ &= v_{n+3} - (1+2a)v_{n+2} + a(a-2)v_{n+1} - a^2 v_n\end{aligned}$$

Let $V'_n = \begin{pmatrix} v_n \\ v_{n+1} \\ v_{n+2} \end{pmatrix}$. We have:

$$\forall n \in \mathbb{N}^*, V'_n = M_*^{n-1} V'_1$$

With

$$M_* = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a^2 & a(2-a) & 1+2a \end{pmatrix}$$

So essentially, $\texttt{EP}(v)$ is a divisor of:

$$\texttt{EP}(v) \mid \ |\texttt{GL}_3(\mathbb{F}_p)| = \prod_{i=0}^{2}(p^3 - p^i) = p^3(p-1)^3(p+1)(p^2+p+1)$$

3.5.3 Case $3: \quad a = b = 0:$

In this case, we have:

$$\texttt{EP}(v) = 1$$

3.6 Limitations

This method gives an expression for $(v_n)_{n\in\mathbb{N}}$. But is does not give a practical period.
If we use the result that $\texttt{EP}(v) \mid p(p^2-1)(p^2-p)$, this method will be more practical, but it is still slow due to the size of the matrix.

4 Solution using Linear Search

4.1 Notes

This is only a solution of the easy version of the problem.
It is dependent of the fact that $(v_n)_{n\in\mathbb{N}}$ satisfies a linear homogeneous recurrence relation of order 5, which is proven in the previous solution.

4.2 Strategy

As $(v_n)_{n\in\mathbb{N}}$ satisfies a linear homogeneous recurrence relation, it is a function of the last 5 terms.
Let K be the offset from which the sequence will become periodic, we have :

$$\boxed{R = \min_{t\in\mathbb{N}^*} \{t \;/\quad v_{N+i} = v_i \;\forall i \in \{0, 1, 2, 3, 4\}\}}$$

Which can be calculated by bruteforce.
Furthermore, as $N \leq 10^6$ in the easy version, we can calculate directly the desired terms.

4.3 Complexity

$$\mathcal{O}(N \log(K + 1) + N + s)$$

We will later prove that $K \leq 1$

5 Solution using Matrices

5.1 Definitions

Term	Definition
$\mathbb{N}$	Set of natural numbers: $\{0, 1, \ldots\}$
$\mathbb{P}$	Set of prime numbers
p	the prime number used for the Scheme
$\mathbb{F}_p$ or $\mathbb{Z}/p\mathbb{Z}$	the cyclic field of order p
$\mathbb{K}$ [2]	a field
$\mathtt{M}_m(\mathbb{K})$	The associative algebra of $m \times m$ matrices over $\mathbb{K}$
$\mathtt{GL}_m(\mathbb{K})$	The group of $m \times m$ invertible matrices over $\mathbb{K}$
I_n	the identity matrix of $\mathtt{M}_m(\mathbb{K})$
a, b	parameters of the scheme
u_0, u_1	seeds
A	$= \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}$
B	$= A - I_m$
S_n	$= \sum_{k=0}^{n} A^k$
χ_M	characteristic polynomial of a matrix M
$\mathtt{EP}(S)$	eventual fundamental period of a sequence $(S_n)_{n\in\mathbb{N}}$

5.2 Strategy

The sequence $(u_n)_{n\in\mathbb{N}}$ satisfies second order linear homogeneous recurrent relation.

Let $(U_n)_{n\in\mathbb{N}}, (V_n)_{n\in\mathbb{N}} \in \mathbb{F}_p^2$ with:

$$U_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$$

$$V_n = \begin{pmatrix} v_n \\ v_{n+1} \end{pmatrix}$$

We can prove that:

[2] Note that $\mathbb{K}$ in this solution is $\mathbb{F}_p$

$$\forall n \in \mathbb{N}, U_n = A^n U_0$$

$$\forall n \in \mathbb{N}, V_n = \sum_{k=0}^{n} k A^k U_0$$

Thus, the problem of calculating $u_{n_1}, \ldots, u_{n_s}$ is reduced to the calculation of:

$$\boxed{S_n = \sum_{k=0}^{n} k A^k, \quad n \in \{n_1, \ldots, n_s\}} \tag{1}$$

Now, the first problem, the eventual period of (v_n) is equal to the eventual period of (S_n). We will show that solving (1) can lead to a probabilistic approach for this problem.

We shall attack the problem (1), we will consider 3 cases:

5.3 Case 1 : $B \in \mathtt{GL}_2(\mathbb{F}_p)$

B^{-1} commutes with A, and we have:

$$\boxed{\sum_{k=0}^{n} k A^k = \frac{nA^{n+2} - (n+1)A^{n+1} + A}{(A - I_2)^2} = B^{-2}\left(nA^{n+2} - (n+1)A^{n+1} + A\right)}$$

5.4 Case 2 : χ_B has a simple root 0

$\chi_B \in \mathbb{F}_p[x]$ has a simple root 0, and it is of degree 2.
So necessarily, it must have another root $\alpha \neq 0$, and we have:

$$\chi_B = x(x - \alpha) = x^2 - \alpha x$$

As we have $\chi_B(B) = 0$, we can conclude that:

$$B^2 = \alpha B$$

Relation between α and a : we have $B = A - I_2$, which implies that $\chi_A(x) = \chi_B(x-1) = (x-1)(x-1-\alpha) = x^2 - (2+\alpha)x + 1 + \alpha$. So

$$a = \alpha + 2$$

Calculating A^n : Let $n \in \mathbb{N}$, we have:

$$\begin{aligned}
A^n &= (B + I_2)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} B^k \\
&= \sum_{k=1}^{n} \binom{n}{k} B^k + I_2 \\
&= \sum_{k=1}^{n} \binom{n}{k} \alpha^{k-1} B + I_2 \\
&= \sum_{k=0}^{n} \binom{n}{k} \alpha^{k-1} B + I_2 - \alpha^{-1} B \\
&= \sum_{k=0}^{n} \binom{n}{k} \alpha^{k} \alpha^{-1} B + I_2 - \alpha^{-1} B \\
&= \alpha^{-1}(\alpha+1)^n B - \alpha^{-1} B + I_2
\end{aligned}$$

So we can conclude that:

$$\begin{aligned}
\sum_{k=0}^{n} k A^k &= \sum_{k=0}^{n} k \alpha^{-1}(\alpha+1)^k B - \alpha^{-1} B + I_2 \\
&= \frac{n(\alpha+1)^{n+2} - (n+1)(\alpha+1)^{n+1} + \alpha + 1}{\alpha^3} B + \sum_{k=0}^{n} k(I_2 - \alpha^{-1} B)
\end{aligned}$$

For $p = 2$: we have, $\sum_{k=0}^{n} k = n + 1 - \lceil \frac{n+1}{2} \rceil$,[3].
We have also $\alpha = 1$, which implies:

$$\begin{aligned}
\forall n \in \mathbb{N}, \quad S_n &= \frac{n(\alpha+1)^{n+2} - (n+1)(\alpha+1)^{n+1} + \alpha + 1}{\alpha^3} B + \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right)(I_2 - \alpha^{-1} B) \\
&= \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right)(I_2 - B) \\
&= \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right)(I_2 + B) \\
&= \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right) A
\end{aligned}$$

As a conclusion:

$$\boxed{\forall n \in \mathbb{N}, \quad S_n = \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right) A}$$

[3] As an exception, the term $\frac{n+1}{2}$ inside the ceil function is interpreted as an Euclidean division between two natural numbers, and not modular division between two cyclic elements.

For $p > 2$**:** we have, $\sum_{k=0}^{n} k \frac{n(n+1)}{2}$, which implies:

$$\boxed{\forall n \in \mathbb{N}, \quad S_n = \frac{n(\alpha+1)^{n+2} - (n+1)(\alpha+1)^{n+1} + \alpha + 1}{\alpha^3} B + \frac{n(n+1)}{2} \left(I_2 - \alpha^{-1} B\right)}$$

5.5 Case 3 : χ_B has a double root 0

In this case, we have:

$$\begin{aligned}
\forall n \in \mathbb{N}^*, \quad A^n &= (B + I_2)^n \\
&= \sum_{k=0}^{n} \binom{n}{k} B^k \\
&= \sum_{k=0}^{1} \binom{n}{k} B^k \\
&= I_2 + nB
\end{aligned}$$

and by extension:

$$\forall n \in \mathbb{N}, \quad A^n = I_2 + nB$$

So we have:

$$\boxed{\forall n \in \mathbb{N}, \quad S_n = \sum_{k=0}^{n} k^2 B + k I_2}$$

If $p = 2$ we have:

$$\sum_{k=0}^{n} k^2 = \sum_{k=0}^{n} k = n + 1 - \left\lceil \frac{n+1}{2} \right\rceil$$

So, as a consequence:

$$\boxed{\forall n \in \mathbb{N}, \quad S_n = \sum_{k=0}^{n} k^2 B + k I_2 = \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right) (B + I_2) = \left(n + 1 - \left\lceil \frac{n+1}{2} \right\rceil\right) A}$$

If $p = 3:$ we have:

$$\sum_{k=0}^{n} k^2 = \sum_{k=0}^{n} k = n + 1 - \left\lceil \frac{n+1}{3} \right\rceil$$

So, as a consequence:

$$\boxed{\forall n \in \mathbb{N}, \quad S_n = \sum_{k=0}^{n} k^2 B + k I_2 = \left(n + 1 - \left\lceil \frac{n+1}{3} \right\rceil\right) B + \frac{n(n+1)}{2} I_2}$$

Otherwise, if $p > 3$: we have:

$$\boxed{\forall n \in \mathbb{N} \quad S_n = \frac{n(n+1)(2n+1)}{6} B + \frac{n(n+1)}{2} I_2}$$

5.6 Period Estimation

This analysis will be case-specific:

- Case 1.1 : $B \in \mathtt{GL}_2(\mathbb{F}_p)$ and $A \in \mathtt{GL}_2(\mathbb{F}_p)$. By Lagrange's theorem, $\operatorname{ord} A \mid |\mathtt{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$.

  So we have $\mathtt{EP}(S) \mid p(p^2-1)(p^2-p)$
- Case 1.2 : $B \in \mathtt{GL}_2(\mathbb{F}_p)$ and $A \notin \mathtt{GL}_2(\mathbb{F}_p)$. We have then $A^2 = \alpha' A$ for some α'. And as a consequence $\forall n \in \mathbb{N}, A^n = \alpha'^{n-1} A$.

  So we may conclude that $\operatorname{ord} A = \operatorname{ord} \alpha' \mid |\mathbb{F}_p^*| = p-1$

  The result above can also be verified for $\alpha' = 0$

  Finally, we have $\mathtt{EP}(S) \mid p(p-1)$
- Case 2.1 : $B^2 = \alpha B,\ \alpha \neq 0$ and $p = 2$. We have then $\operatorname{ord} \alpha \mid p-1$ So, we have $\mathtt{EP}(S) \mid p^2(p-1) = 4$
- Case 2.2 : $B^2 = \alpha B,\ \alpha \neq 0$ and $p > 2$. We have then $\operatorname{ord} \alpha \mid p-1$

  So, we have $\mathtt{EP}(S) \mid p(p-1)$
- Case 3.1 : $B^2 = 0$ and $p = 2$: $\quad \mathtt{EP}(S) = p^2 = 4$
- Case 3.2 : $B^2 = 0$ and $p = 3$: $\quad \mathtt{EP}(S) = p^2 = 9$
- Case 3.3 : $B^2 = 0$ and $p > 3$: $\quad \mathtt{EP}(S) = p$

Now, let T be a strict multiple of the period. By sampling $(S_n)_{n\in\mathbb{N}}$ on m random points $(S_{t_1}, \ldots, S_{t_m})$, we can estimate the fundamental period $R = \mathtt{EP}(S)$ by finding:

$$\boxed{R \approx \arg\min_{d|T} \{d/ \quad S_{t_i} = S_{t_i+d} \quad \forall i \in \{1, \ldots, m\}\}} \tag{2}$$

5.7 Complexity

$$\mathcal{O}\left(s \log \left(\max_{i\in\{1,\ldots,s\}} (n_i)\right) + m d_0(T) \log N + \sqrt{p}\right)$$

Where d_0 is the count divisors function, and T the initial guess of the period.

6 Solution using Ring Theory

6.1 Definitions

Term	Definition
$\mathbb{N}$	Set of natural numbers: $\{0, 1, \dots\}$
$\mathbb{P}$	Set of prime numbers
p	the prime number used for the Scheme
$\mathbb{F}_p$ or $\mathbb{Z}/p\mathbb{Z}$	the cyclic field of order p
$\mathbb{K}$ [4]	a field
$\mathcal{R}$	a commutative ring
$\mathcal{R}[x]$	the ring of polynomials over $\mathcal{R}$
$\mathbb{K}(x)$	the field of rational functions over $\mathbb{K}$
$\mathcal{D}$	Formal Derivative operator
$\frac{\partial}{\partial x}$	Formal Derivative with respect to x operator
$\mathcal{R}/h$ where $h \in \mathcal{R}[x]$ is monic	ring extension of $\mathcal{R}$ by a root of h
$\mathtt{M}_m(\mathbb{K})$	The associative algebra of $m \times m$ matrices over $\mathbb{K}$
$\mathtt{GL}_m(\mathbb{K})$	The group of $m \times m$ invertible matrices over $\mathbb{K}$
I_m	the identity matrix of $\mathtt{M}_m(\mathbb{K})$
a, b	parameters of the scheme
u_0, u_1	seeds
A	$= \begin{pmatrix} 0 & 1 \\ b & a \end{pmatrix}$
S_n	$= \sum_{k=0}^{n} A^k$
$\Psi(x, n, m)$	$= \sum_{k=0}^{n} k^m x^k$
χ_M	characteristic polynomial of a matrix M
$\mathtt{EP}(S)$	eventual fundamental period of a sequence $(S_n)_{n\in\mathbb{N}}$

[4]Note that $\mathbb{K}$ in this solution is a field with characteristic p. More precisely, it is either $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$

6.2 Analysis of Ψ function

Here, we will denote by $\mathbb{K}$ a field with characteristic p.

Definition & Importance: The Ψ function is by definition:

$$\begin{aligned}\Psi : \mathbb{K} \times \mathbb{N} \times \mathbb{N} &\to \mathbb{K} \\ (x, n, m) &\to \sum_{k=0}^{n} k^m x^k\end{aligned}$$

Solutions of the (1) will be expressed with this function. So we will formally build closed form expression for this function on each case.
First of all, we may view this function as a parameterized rational:

As a Rational Function

$$\forall n, m \in \mathbb{N}, \Psi(\cdot, n, m) \in \mathbb{K}(x)$$

Now, we will formally build a working definition of formal derivation that will help us to express Ψ in a closed form:

Formal Derivative $\mathcal{D}$ over $\mathbb{K}[x]$: Let $\mathcal{D}$:

$$\begin{aligned}\mathbb{K}[x] &\to \mathbb{K}[x] \\ \sum_{k=0}^{n} a_k x^k &\to \sum_{k=1}^{n} k a_k x^{k-1}\end{aligned}$$

The operator $\mathcal{D}$ is called the formal derivative.

Formal Derivative $\mathcal{D}$ over $\mathbb{K}(x)$: Using the definition over $\mathbb{K}[x]$, we extend it to $\mathbb{K}(x)$ with:

$$\begin{aligned}\mathbb{K}(x) &\to \mathbb{K}(x) \\ \frac{f}{g} &\to \frac{\mathcal{D}(f)g - f\mathcal{D}(g)}{g^2}\end{aligned}$$

Now, viewing Ψ as a parameterized rational function, we will build a working definition of partial derivation with respect to x, that will 'fix' n, m. and derive the rational:

Formal Partial Derivative $\frac{\partial}{\partial x}$: Let $f \in \mathcal{F}(\mathbb{K} \times \mathbb{N} \times \mathbb{N}, \mathbb{K})$ such that $\forall n, m \in \mathbb{N}, f(\cdot, n, m) \in \mathbb{K}(x)$. By definition, the formal partial derivative of f with respect to x denoted by $\frac{\partial f}{\partial x}$ is the function:

$$\begin{aligned}\mathbb{K} \times \mathbb{N} \times \mathbb{N} &\to \mathbb{K} \\ (x, n, m) &\to \mathcal{D}(f(\cdot, n, m))(x)\end{aligned}$$

Finally, with all these definitions, we are ready to evaluate Ψ

Calculating $\Psi(x,n,0)$:

$$\boxed{\Psi(x,n,0) = \begin{cases} \frac{1-x^{n+1}}{1-x} & x \neq 1 \\ n+1 & x = 1 \end{cases}}$$

Relation between Ψ **and** $\frac{\partial \Psi}{\partial x}$: for $x \neq 0$, we have:

$$\begin{aligned} \Psi(x,n,m) &= \sum_{i=0}^{n} i^m x^i \\ \frac{\partial \Psi}{\partial x}(x,n,m) &= \sum_{i=0}^{n} i^{m+1} x^{i-1} \\ &= \frac{1}{x}\Psi(x,n,m+1) \\ \implies \Psi(x,n,m+1) &= x\frac{\partial \Psi}{\partial x}(x,n,m) \end{aligned}$$

This relation can be trivially extended to the case $x = 0$
As a conclusion:

$$\boxed{\forall x \in \mathbb{K}, \forall n,m \in \mathbb{N}, \quad \Psi(x,n,m+1) = x\frac{\partial \Psi}{\partial x}(x,n,m)}$$

Recurrence relation for Ψ : for $x \neq 0$, we have:

$$\begin{aligned} \frac{\partial \Psi}{\partial x}(x,n,m) &= \sum_{i=1}^{n} i^{m+1} x^{i-1} \\ &= \sum_{i=0}^{n-1} (i+1)^{m+1} x^i \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{m+1} \binom{m+1}{j} i^j x^i \\ \implies \Psi(x,n,m+1) &= x\frac{\partial \Psi}{\partial x}(x,n,m) \end{aligned}$$

This relation can be trivially extended to the case $x = 0$
As a conclusion:

$$\boxed{\forall x \in \mathbb{K}, \forall n,m \in \mathbb{N}, \quad \Psi(x,n,m+1) = x\frac{\partial \Psi}{\partial x}(x,n,m)}$$

Recurrence relation for $n = 1, \ m < p-1:$ Let $n, m \in \mathbb{N}$ with $m < p-1$.
We have:

$$\begin{aligned}
\sum_{i=0}^{n} (i+1)^{m+1} - i^{m+1} &= (n+1)^{m+1} \\
&= \sum_{i=0}^{n} \sum_{j=0}^{m} \binom{m+1}{j} i^j \\
&= \sum_{j=0}^{m} \sum_{i=0}^{n} \binom{m+1}{j} i^j \\
&= \sum_{j=0}^{m} \binom{m+1}{j} \sum_{i=0}^{n} i^j \\
&= \sum_{j=0}^{m} \binom{m+1}{j} \Psi(1, n, j)
\end{aligned}$$

We can conclude that:

$$\boxed{\forall n, m \in \mathbb{N} \ / \ m < p-1, \quad \Psi(1, n, m) = \frac{1}{m+1} \left((n+1)^{m+1} - \sum_{i=0}^{m-1} \binom{m+1}{i} \Psi(1, n, i) \right)}$$

Evaluating $\Psi(1, n, p-1):$ we have

$$\begin{aligned}
\Psi(1, n, p-1) &= \sum_{i=0}^{n} i^{p-1} \\
&= \sum_{p \nmid i, 0 \le i \le n} 1 \\
\sum_{i=0}^{n} i^{p-1} + \sum_{p | i, \ 0 \le i \le n} 1 &= \sum_{p \nmid i, 0 \le i \le n} 1 + \sum_{p | i, \ 0 \le i \le n} 1 \\
&= \sum_{0 \le i \le n} 1 \\
&= n + 1 \\
\sum_{p | i, \ 0 \le i \le n} 1 &= \left\lceil \frac{n+1}{p} \right\rceil
\end{aligned}$$

As a conclusion[5]:

$$\boxed{\forall n \in \mathbb{N}, \quad \Psi(1,n,p-1) = n+1-\left\lceil \frac{n+1}{p} \right\rceil}$$

Table of values: the following table has the values of Ψ.

Range	Value
$x \neq 1, n, m \in \mathbb{N}$	$x\frac{\partial \Psi}{\partial x}(x,n,m)$
$x = 1, n \in \mathbb{N}, m < p-1$	$\frac{1}{m+1}\left((n+1)^{m+1} - \sum_{i=0}^{m-1}\binom{m+1}{i}\Psi(1,n,i)\right)$
$x = 1, n \in \mathbb{N}, m = p-1$	$n+1-\left\lceil \frac{n+1}{p} \right\rceil$

Table of important values: the following table has the important values of Ψ.

Term	Value
$\Psi(x,n,1), \quad x \neq 1$	$\frac{nx^{n+2}-(n+1)x^{n+1}+x}{(1-x)^2}$
$\Psi(1,n,1), \quad p > 2$	$\frac{n(n+1)}{2}$
$\Psi(1,n,1), \quad p = 2$	$n+1-\left\lceil \frac{n+1}{2} \right\rceil = \left\lfloor \frac{n+1}{2} \right\rfloor$
$\Psi(x,n,2) \quad x \neq 1$	$\frac{-n^2x^{n+3}+(2n^2+2n-1)x^{n+2}-(n+1)^2x^{n+1}+x^2+x}{(1-x)^3}$
$\Psi(1,n,2) \quad p > 3$	$\frac{n(n+1)(2n+1)}{6}$
$\Psi(1,n,2) \quad p \in \{2,3\}$	$n+1-\left\lceil \frac{n+1}{p} \right\rceil$
$\frac{\partial \Psi}{\partial x}(x,n,2) \quad x \neq 1$	$\frac{-n^2x^{n+2}+(2n^2+2n-1)x^{n+1}-(n+1)^2x^{n}+x+1}{(1-x)^3}$
$\frac{\partial \Psi}{\partial x}(1,n,2) = \quad p > 3$	$\frac{n(n+1)(2n+1)}{6}$
$\frac{\partial \Psi}{\partial x}(1,n,2) \quad p \in \{2,3\}$	$n+1-\left\lceil \frac{n+1}{p} \right\rceil$

[5] As an exception, the term $\frac{n+1}{p}$ inside the ceil function is interpreted as an Euclidean division between two natural numbers, and not modular division between two cyclic elements.

6.3 Strategy

The sequence $(u_n)_{n\in\mathbb{N}}$ satisfies second order linear homogeneous recurrent relation.

Let $(U_n)_{n\in\mathbb{N}}, (V_n)_{n\in\mathbb{N}} \in \mathbb{F}_p^2$ with:

$$U_n = \begin{pmatrix} u_n \\ u_{n+1} \end{pmatrix}$$
$$V_n = \begin{pmatrix} v_n \\ v_{n+1} \end{pmatrix}$$

We can prove that:

$$\forall n \in \mathbb{N}, U_n = A^n U_0$$
$$\forall n \in \mathbb{N}, V_n = \sum_{k=0}^{n} kA^k U_0$$

Thus, the problem of calculating $u_{n_1}, \dots, u_{n_s}$ is reduced to the calculation of:

$$\boxed{S_n = \sum_{k=0}^{n} kA^k, \quad n \in \{n_1, \dots, n_s\}} \tag{1}$$

Now, this is the same problem of the matrix approach, but here we will reduce it further by diagonalising A, or at least putting it in a jordan normal form.

Now, for the first problem, the eventual period of (v_n) is equal to the eventual period of (S_n). We will show that solving (1) can lead to a probabilistic approach for this problem.

6.4 Solving $\chi_A(x) = 0$ over $\mathbb{F}_p$

If $p = 2:$ then χ_A is irreducible if and only if $a = b = 1$. Otherwise, the roots can be easily found with inspection.

If $p > 2:$ Let $\Delta = a^2 + 4b$.

If Δ is a quadratic residue, then $\chi_A = 0$ has two solutions

$$\varphi_{1/2} = \frac{1 \pm \sqrt{\Delta}}{2}$$

Where $\sqrt{\Delta}$ is any solution of $x^2 = \Delta$

Otherwise, if Δ is a quadratic non-residue, then $\chi_A = 0$ has no solution.

6.5 Case 1 : χ_A is irreducible over $\mathbb{F}_p$

In this case, we will extend $\mathbb{F}_p$ by adjoining a root of χ_A.

Let $\mathcal{R} = \mathbb{F}_p[x]/\chi_A$ be that extension. clearly, $\mathcal{R}$ is a commutative ring. Furthermore, it is a field thanks to the irreducibility of χ_A over $\mathbb{F}_p$. So we will denote it by $\mathbb{K} = \mathcal{R}$

Let $\varphi \in \mathbb{K}$ a root of χ_A. We have $\deg \chi_A = 2$, so necessarily, χ_A has another root $\bar{\varphi} \in \mathbb{K}$.

Proof that $\bar{\varphi} \neq \varphi$: assume otherwise, we have:

$$\begin{aligned}\chi_A &= (x-\varphi)^2 \\ &= x^2 - 2\varphi x + \phi^2 && = x^2 - 2ax + b \\ \implies \varphi &= a \in \mathbb{F}_p \text{ which is a contradiction}\end{aligned}$$

Proof that $\bar{\varphi} = \varphi^p$:

$$\begin{aligned}(\varphi\bar{\varphi})^p &= (-b)^p \\ &= -b \quad \text{because } (-b) \in \mathbb{F}_p \\ &= \varphi^p \bar{\varphi}^p \\ (\varphi + \bar{\varphi})^p &= a^p \\ &= a \text{ because } a \in \mathbb{F}_p \\ &= \varphi^p + \bar{\varphi}^p \quad \text{(Frobenius Automorphism)}\end{aligned}$$

So $\varphi^p, \bar{\varphi}^p$ are also two roots of χ_A. If $\varphi^p = \varphi$, then φ is a root of $x^p - x$ which implies that $\varphi \in \mathbb{F}_p$. a contradiction.
So, necessarily, $\varphi^p = \bar{\varphi}$ $\square$.

Multiplicative order of φ : we have $\varphi \in \mathbb{K}^*$ and $\mathbb{K}$ is a field with order p^2. Then, by Lagrange's theorem:

$$\operatorname{ord} \varphi \mid |\mathbb{K}^\times| = |\mathbb{K}^*| = p^2 - 1$$

Proof that A is diagonalisable: we have $A \in \mathtt{M}_2(\mathbb{K})$, and we have $\chi_A \in \mathbb{K}[x]$ is reducible over $\mathbb{K}$ with simple roots $\varphi, \bar{\varphi}$. So A is necessarily diagonalisable over $\mathtt{M}_2(\mathbb{K})$

Eigenvectors of A Let $e = \begin{pmatrix} 1 \\ \varphi \end{pmatrix}, \bar{e} = \begin{pmatrix} 1 \\ \bar{\varphi} \end{pmatrix}$. we have:

$$\begin{aligned} Ae &= \begin{pmatrix} \varphi \\ b + a\varphi \end{pmatrix} \\ &= \begin{pmatrix} \varphi \\ \varphi^2 \end{pmatrix} \\ &= \varphi \begin{pmatrix} 1 \\ \varphi \end{pmatrix} \\ &= \varphi e \\ \text{Also, } A\bar{e} &= \bar{\varphi}\bar{e} \end{aligned}$$

So $\mathscr{B} = (e, \bar{e})$ is an eigenbasis of A

Eigendecomposition of A :

$$\begin{aligned} A &= \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix} \begin{pmatrix} \varphi & 0 \\ 0 & \bar{\varphi} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix}^{-1} \\ &= PDP^{-1} \end{aligned} \tag{3.a}$$

S_n as a function of φ and $\bar{\varphi}$: we have $\forall n \in \mathbb{N}$

$$\begin{aligned} A^n &= PD^nP^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix} \begin{pmatrix} \varphi^n & 0 \\ 0 & \bar{\varphi}^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix}^{-1} \\ S_n &= \sum_{k=0}^{n} kA^k \\ &= P\left(\sum_{k=0}^{n} kD^k\right)P^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix} \begin{pmatrix} \sum_{k=0}^{n} k\varphi^k & 0 \\ 0 & \sum_{k=0}^{n} k\bar{\varphi}^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix} \begin{pmatrix} \Psi(\varphi, n, 1) & 0 \\ 0 & \Psi(\bar{\varphi}, n, 1) \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi & \bar{\varphi} \end{pmatrix}^{-1} \\ \text{with } \Psi(x, n, 1) &= \sum_{k=0}^{n} kx^k \\ &= \frac{nx^{n+2} - (n+1)x^{n+1} + x}{(1-x)^2} \quad \text{for } x \neq 1 \end{aligned}$$

6.6 Case 2 : χ_A has simple roots

Let $\varphi_1, \varphi_2 \in \mathbb{F}_p$ the distinct eigenvalues of A. It is evident that A is diagonalisable.

Furthermore, $e_1 = \begin{pmatrix} 1 \\ \varphi_1 \end{pmatrix}, e_2 = \begin{pmatrix} 1 \\ \varphi_2 \end{pmatrix}$ are the associated eigenvectors of A.

Eigendecomposition of A : We have:

$$\begin{aligned} A &= PDP^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix} \begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix}^{-1} \end{aligned}$$

S_n as a function of φ and $\bar{\varphi}$: we have $\forall n \in \mathbb{N}$

$$\begin{aligned} A^n &= PD^nP^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix} \begin{pmatrix} \varphi_1^n & 0 \\ 0 & \varphi_2^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix}^{-1} \\ S_n &= \sum_{k=0}^{n} kA^k \\ &= P\left(\sum_{k=0}^{n} kD^k\right)P^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix} \begin{pmatrix} \sum_{k=0}^n k\varphi_1^k & 0 \\ 0 & \sum_{k=0}^n k\varphi_2^k \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix} \begin{pmatrix} \Psi(\varphi_1, n, 1) & 0 \\ 0 & \Psi(\varphi_2, n, 1) \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi_1 & \varphi_2 \end{pmatrix}^{-1} \\ \text{with } \Psi(x, n, 1) &= \sum_{k=0}^{n} kx^k \\ &= \begin{cases} \frac{nx^{n+2}-(n+1)x^{n+1}+x}{(1-x)^2} & \text{for } x \neq 1 \\ \frac{n(n+1)}{2} & \text{for } x = 1 \ \& \ p > 2 \\ n+1-\left\lceil \frac{n+1}{2} \right\rceil & \text{for } x = 1 \ \& \ p = 2 \end{cases} \end{aligned}$$

6.7 Case 3 : χ_A has a double root φ

In this case $\chi_A = (x-\varphi)^2 = x^2 - 2\varphi x + \varphi^2 = x^2 - a - b$.
So we have:

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2\varphi \\ -\varphi^2 \end{pmatrix}$$

Proof that A is defective: let $e_1 = \begin{pmatrix} 1 \\ \varphi \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, we have:

$$\begin{aligned}
Ae_1 &= \varphi e_1 \\
Ae_2 &= \begin{pmatrix} 1 \\ a \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ 2\varphi \end{pmatrix} \\
&= \begin{pmatrix} 1 \\ \varphi \end{pmatrix} + \begin{pmatrix} 0 \\ \varphi \end{pmatrix} \\
&= e_1 + \varphi e_2 \\
\implies (A - \varphi I_2)e_2 &= e_1 \\
\text{and } (A - \varphi I_2)^2 e_2 &= 0
\end{aligned}$$

So A is defective. But it still has a Jordan Normal Form.

Jordan Normal Form of A: We have:

$$\begin{aligned}
A &= PJP^{-1} \\
&= \begin{pmatrix} 1 & 0 \\ \varphi & 1 \end{pmatrix} \begin{pmatrix} \varphi & 1 \\ 0 & \varphi \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \varphi & 1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & 0 \\ \varphi & 1 \end{pmatrix} \begin{pmatrix} \varphi & 1 \\ 0 & \varphi \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\varphi & 1 \end{pmatrix}
\end{aligned}$$

S_n as a function of φ : we have $\forall n \in \mathbb{N}$

$$\begin{aligned}
A^n &= PJ^nP^{-1} \\
&= \begin{pmatrix} 1 & 0 \\ \varphi & 1 \end{pmatrix} \begin{pmatrix} \varphi^n & n\varphi^{n-1} \\ 0 & \varphi^n \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\varphi & 1 \end{pmatrix} \\
S_n &= \sum_{k=0}^{n} kA^k \\
&= P \left(\sum_{k=0}^{n} kJ^k \right) P^{-1} \\
&= \begin{pmatrix} 1 & 0 \\ \varphi & 1 \end{pmatrix} \begin{pmatrix} \sum_{k=0}^n k\varphi_1^k & \sum_{k=0}^n k^2\varphi^{k-1} \\ 0 & \sum_{k=0}^n k\varphi^k \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\varphi & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ \varphi & 1 \end{pmatrix} \begin{pmatrix} \Psi(\varphi, n, 1) & \frac{\partial \Psi}{\partial x}(\varphi, n, 1) \\ 0 & \Psi(\varphi, n, 1) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -\varphi & 1 \end{pmatrix}
\end{aligned}$$

With:

$$
\begin{aligned}
\Psi(x,n,1) &= \sum_{k=0}^{n} kx^k \\
&= \begin{cases} \frac{nx^{n+2}-(n+1)x^{n+1}+x}{(1-x)^2} & \text{for } x \neq 1 \\ \frac{n(n+1)}{2} & \text{for } x = 1 \text{ \& } p > 2 \\ n+1-\lceil\frac{n+1}{2}\rceil & \text{for } x = 1 \text{ \& } p = 2 \end{cases} \\
\frac{\partial \Psi}{\partial x}(x,n,1) &= \frac{\partial}{\partial x}\sum_{k=0}^{n} kx^k \\
&= \sum_{k=0}^{n} k\frac{\partial}{\partial x}x^k \\
&= \sum_{k=0}^{n} k^2x^{k-1} \\
&= \begin{cases} \frac{-n^2x^{n+2}+(2n^2+2n-1)x^{n+1}-(n+1)^2x^{n+1}+x+1}{(1-x)^3} & x \neq 1 \\ \frac{n(n+1)(2n+1)}{6} & x = 1 \text{ \& } p > 3 \\ n+1-\lceil\frac{n+1}{3}\rceil & x = 1 \text{ \& } p = 3 \\ n+1-\lceil\frac{n+1}{2}\rceil & x = 1 \text{ \& } p = 2 \end{cases}
\end{aligned}
$$

6.8 Period Estimation

This analysis will be case-specific:

- Case 1 : χ_A is irreducible. We have: $\operatorname{ord}\bar{\varphi}, \operatorname{ord}\varphi \mid p^2 - 1$.
  So necessarily, $\mathtt{EP}(S) \mid p(p^2 - 1)$
- Case 2.1 : $\chi_A(1) = 0$ and $p = 2$: Let x be the other root.
  we have $\operatorname{ord} x \mid p - 1$. So necessarily, $\mathtt{EP}(S) \mid p^2(p-1) = 4$
- Case 2.2 : $\chi_A(1) = 0$ and $p > 2$: Let x be the other root.
  we have $\operatorname{ord} x \mid p - 1$. So necessarily, $\mathtt{EP}(S) \mid p(p-1)$
- Case 2.3 : $\chi_A(1) \neq 0$: Let $\varphi_1, \varphi_2 \in \mathbb{F}_p$ be the distinct roots.
  we have $\operatorname{ord}\varphi_1, \operatorname{ord}\varphi_2 \mid p - 1$. So necessarily, $\mathtt{EP}(S) \mid p(p-1)$
- Case 3.1 : $\varphi = 1$ and $p = 2$: $\mathtt{EP}(S) \mid p^2 = 4$
- Case 3.2 : $\varphi = 1$ and $p = 3$: $\mathtt{EP}(S) \mid p^2 = 9$
- Case 3.3 : $\varphi = 1$ and $p > 3$: $\mathtt{EP}(S) \mid p$
- Case 3.4 : $\varphi \neq 1$: $\mathtt{EP}(S) \mid p(p-1)$

6.8.1 Probabilistic Method

Now, let T be a period. By sampling $(S_n)_{n\in\mathbb{N}}$ on m random points $(S_{t_1}, \ldots, S_{t_m})$, we can estimate the fundamental period $R = \mathtt{EP}(S)$ by finding:

$$\boxed{R \approx \arg\min_{d \mid T} \{d / \quad v_{t_i} = v_{t_i+d} \quad \forall i \in \{1, \ldots, m\}\}} \tag{2.1}$$

6.8.2 Deterministic Method

From 3.3, we can prove that v_n is a function of its previous 5 terms.
Knowing that the offset $K \leq 1$, we have then:

$$\boxed{R = \arg\min_{d \mid T} \{d / \quad v_i = v_{i+R} \quad \forall i \in \{1, \ldots, 5\}\}} \tag{2.2}$$

6.9 Complexity

$$\mathcal{O}\left(s \log\left(\max_{i\in\{1,\ldots,s\}}(n_i)\right) + m d_0(T) \log N + \sqrt{p}\right)$$

Where d_0 is the count divisors function, and T the initial guess of the period.

Part II
Mean Absolute Deviation