Winter Cup 4

Rami Zouari Oussema Jeballah Yessine Jallouli

February 3, 2022

Abstract

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

Contents

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 Matrices

2.1 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
$\mathbb{K}$ [1]	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 idendity 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 $(S_n)_{n\in\mathbb{N}}$

2.2 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:

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

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

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

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

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

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:

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

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

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

2.4 Case $2: \chi_B$ 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:

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

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

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

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

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

[2] 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.

2.5 Case $3 : \chi_B$ 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:

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

2.6 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 $(S_{t_1}, \dots, S_{t_m})$, we can estimate the fundamental period $R = \mathtt{EP}(S)$ by finding:

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

2.7 Complexity

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

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

3 Solution using Ring Theory

3.1 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
$\mathbb{K}$ [3]	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 idendity 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 $(S_n)_{n\in\mathbb{N}}$

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

3.2 Analysis of Ψ function

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

Definition & Importance: The Ψ function is by definition:

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

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 $\mathcal{D}$:

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

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:

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

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:

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

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 $n = 1,\ m < p-1$: 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[4]:

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

[4] 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.

3.3 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.

3.4 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.

3.5 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 $\forall n \in \mathbb{N}$

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

3.6 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 $\forall n \in \mathbb{N}$

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

3.7 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:

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

3.8 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, $\texttt{EP}(S) \mid p(p^2 - 1)$
- 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, $\texttt{EP}(S) \mid p^2(p - 1) = 4$
- 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, $\texttt{EP}(S) \mid p(p - 1)$
- 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, $\texttt{EP}(S) \mid p(p - 1)$
- Case 3.1 : $\varphi = 1$ and $p = 2$: $\texttt{EP}(S) \mid p^2 = 4$
- Case 3.2 : $\varphi = 1$ and $p = 3$: $\texttt{EP}(S) \mid p^2 = 9$
- Case 3.3 : $\varphi = 1$ and $p > 3$: $\texttt{EP}(S) \mid p$
- Case 3.4 : $\varphi \neq 1$: $\texttt{EP}(S) \mid p(p - 1)$

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 $R = \texttt{EP}(S)$ by finding:

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

3.9 Complexity

$$\mathcal{O}\left(s \log\left(\max_{i\in\{1,\ldots,s\}}(n_i)\right) + md_0(T)\log N + \sqrt{p}\right)$$

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

4 Solution using Pattern Matching

Part II
Mean Absolute Deviation