Projet d'Initiation à la Recherche
Propriétés Arithmétiques des Périodes des Suites Récurrentes Linéaires D'Ordre Deux et Trois

Adil AMZAZ, Rémi GASC, Elohim NEULAT

12 mai 2017

Dans cet exposé, K désignera un corps de caractéristique différente de 2, et p un nombre premier impair.
L'acronyme SRL signifiera Suite Récurrente Linéaire.

Lorsqu'on créée une suite pseudo-aléatoire avec des LFSR, la connaissance de la période de la SRL associée est indispensable : celle-ci détermine la longueur maximale de la suite. En effet, la longueur de la suite pseudo-aléatoire créée est au maximum égal à la période de la SRL utilisée pour sa génération. Notons qu'une suite récurrente à valeur dans un corps fini est nécessairement périodique à partir d'un certain rang.
Nous allons, dans cet exposé, étudier d'un point de vue arithmétique la période d'une SRL d'ordre deux ou trois : Nous verrons qu'en fonction des propriétés générales du polynôme caractéristique associé, on sera en mesure de déterminer un multiple de la période de la SRL, voir directement de la calculer.

Nous commencerons par énoncer quelques définitions et théorèmes nécéssaires à la bonne compréhension de l'exposé.
Dans un second temps, nous ferons une étude générale de la période des SRL d'ordre 2. Nous traiterons l'exemple de Fibonacci à valeur dans $\mathbb{F}_p$, que nous illustrerons dans le cas où $p = 5$.
Enfin, nous ferons une étude générale de la période d'une SRL d'ordre 3 à valeur dans un corps fini.

1 Quelques définitions et théorèmes sur les Discriminants et Résultants

Les notions de discriminant et résultant étant prépondérantes dans ce rapport, nous énonçons dans cette partie quelques définitions, théorèmes et démonstrations à ce sujet.

Définition 1 (Résultant)**.** *Soient A un anneau intègre et P, Q deux polynômes de $A[X]$, de degrés respectifs n et m. Le résultant des deux polynômes P et Q, noté $R(P,Q)$ est, par définition, le déterminant de leur matrice de Sylvester. Le résultant appartient donc à A.*

Proposition 1. *Soient K un corps et P, Q deux polynômes de $K[X]$. On a : $R(P,Q) = 0 \Leftrightarrow$ le pgcd de P et Q dans $K[X]$ est non constant, ie ces deux polynômes ont au moins une racine commune dans une clôture algébrique de K.*

Définition 2 (Discriminant)**.** *Soient K un corps, et $f(X) = \sum_{k=0}^{n} a_k X^k$ un élément de $K[X]$.*
Le discriminant de f, noté $D(f)$ est définit ainsi :

$$D(f) := a_0^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2$$

Cela généralise la notion de discriminant pour un polynôme P de $K[X]$ de degré quelconque.
Cela permet de déterminer si les racines de P sont simples ou multiples.

Soient R un anneau commutatif intègre de corps de fraction L et

$$A(X) := a_0 + ... + a_p X^p \in R_p[X]$$

et

$$B(X) := b_0 + ... + b_q X^q \in R_q[X]$$

on introduit alors la *matrice de Sylvester* :

$$S_{p,q}(A,B) := \begin{pmatrix} a_0 & 0 & \ddots & 0 & b_0 & 0 & 0 & \cdots & 0 & 0 \\ a_1 & a_0 & \ddots & 0 & b_1 & b0 & 0 & \ddots & 0 & 0 \\ \vdots & a_1 & \ddots & 0 & \vdots & b_1 & b_0 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & a_0 & \ddots & \ddots & b_1 & \ddots & 0 & 0 \\ a_{p-1} & \vdots & \ddots & a_1 & b_q & \vdots & \vdots & \ddots & b_0 & 0 \\ a_p & a_{p-1} & \ddots & \vdots & 0 & b_q & \vdots & \ddots & b_1 & b_0 \\ 0 & a_p & \ddots & \vdots & 0 & 0 & b_q & \ddots & \vdots & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & a_{p-1} & \vdots & \vdots & \vdots & \ddots & b_q & \vdots \\ 0 & 0 & \cdots & a_p & 0 & 0 & 0 & \cdots & 0 & b_q \end{pmatrix} \in M_{p+q}(R).$$

Les q premières colonnes sont formées avec les coefficients de A, les p suivantes avec les coefficients de B.
Nous noterons $Res_{p,q}(A,B) := detS_{p,q}(A,B)$ le déterminant de la matrice de Sylvester.
Exemples : Si $A := a \in R, S_{0,q}(A,B) = aI_q$ et $Res_{0,q}(A,B) = a^q$.
De même, $B = b \in R, S_{p,0}(A,B) = b^p$.

Proposition 2. *Pour que $Res_{p,q}(A,B)$ soit nul, il faut, et il suffit, qu'il existe $P \in R_{q-1} etQ \in R_{p-1}[X]$ non tous deux nuls tels que $AP + BQ = 0$.*

Démonstration. Il revient au même de prendre $P \in R_{q-1}[X]$ et $Q \in R_{p-1}[X]$ ou $P \in R_{q-1}[X]$ et
$Q \in R_{p-1}$. On remarque que $S_{p,q}(A,B)$ est la matrice de la famille $(A, XA, ..., X^{q-1}A, B, XB, ..., X^{p-1}B)$ dans la base canonique du R-espace vectoriel $R_{p+q-1}[X]$.
En conséquence, si $P := \alpha_0 + ... + \alpha_{q-1}X^{q-1} \in R_{q-1}$ et $Q := \beta_0 + ... + \beta_{p-1}X^{p-1} \in R_{p-1}[X]$, alors le vecteur colonne des coordonnées de $AP + BQ$ dans la base canonique de R_{p+q-1} est $S_{p,q}(A,B)\, C_{\alpha,\beta}$, où l'on a noté $C_{\alpha,\beta}$ le vecteur colonne transposé du vecteur ligne $(\alpha_0 ... \alpha_{q-1}\beta_0 ... \beta_{p-1})$. L'affirmation de la proposition en découle.
□

Proposition 3. *Il existe $P \in R_{q-1}[X]$ et $Q \in R_{p-1}[X]$ tels que $AP+BQ = Res_{p,q}(A,B)$.*

Démonstration. Notons $S := S_{p,q}(A,B)$ et $\widetilde{S}$ la transposée de la matrice des cofacteurs de S. D'après les formules de Cramer, $S\widetilde{S} = Res_{p,q}(A,B)\, Ip + q$. Si l'on note $(\alpha_0, ..., \alpha_{q-1}, \beta 0, ..., \beta_{p-1})$ la première colonne de $\widetilde{S}$, alors $Q := \alpha_0, ..., \alpha_{q-1}X^{q-1}$ et $P := \beta 0, ..., \beta_{p-1}X^{p-1}$ conviennent. □

Définition 1.1. Le *résultant* des polynômes $A, B \in R[X]$ de degrés respectifs $p, q \geq 0$ est l'élément $Res(A,B) \in R$.

Proposition 4. *Soit $A = QB + A_1$ une division euclidienne, avec $A_1 \neq 0$. Alors, avec les mêmes notations que précédemment $Res(A,B) = b_p^{degA_degA_1} Res(A_1,B)$.*

Démonstration. Pour $0 \leq k \leq q_p = degB - degA$, remplacer A par $A - cX^kB$ revient à effectuer les opérations élémentaires suivantes sur les colonnes de $S_{p,q}(A,B)$: $C_i \leftarrow C_i - cC_{p+i+k}$, pour toute i, vérifiant $1 \leq i \leq p$ (et dans un ordre quelconque). Ces opérations ne changent pas le déterminant, d'où l'égalité $Res_{p,q}(A,B) = Res_{p,q}(A_1,B)$. Il suffit alors d'appliquer les règles déjà énoncées. □

Lemme 1. *Si $B = (X - \alpha)C$, alors $Res(A,B) = A(\alpha)\, Res(A,C)$.*

Démonstration. On note :

$$A := a_0 + ... + a_{p-1}X^{p-1}, B := b_0 + ... + b_qX^q, C := c_0 + ... + c_{q-1}X^{q-1}.$$

On a donc :
$b_i = c_{i-1} - \alpha c_i$ pour $i \in \{0, ..., q\}$, en convenant que $c_{-1} = c_q := 0$.
On effectue sur $S_{p,q}(A,B)$ les opérations élémentaires suivantes sur les lignes : $L_i \leftarrow$

$L_i + \alpha L_{i+1}$, pour i de $p+q-1$ à 1 (dans cet ordre). Dans la matrice obtenue, chaque a_i a été remplacé par $A_i(\alpha)$, où $A_i := \sum_{k=1}^{p} a_k X^{k-i}$ (de sorte que $A_0 = A$, $A_p = a_p$ et $A_i = a_i + XA_{i+1}$).
De même, chaque b_j a été remplacé par c_{j-1}. On effectue ensuite sur la matrice obtenue les opérations élémentaires suivantes sur les colonnes :$C_j \leftarrow C_j - \alpha C_{j-1}$ pour j de q à 2 (dans cet ordre). Les c_j restent en place et les $A_i(\alpha)$ redeviennent des a_i, sauf ceux de la première colonne, qui ne sont pas affectés.
Sur la matrice finale, les coefficients de la première ligne sont nuls. sauf le premier, qui vaut $A(\alpha)$, le mineur correspondant est $S_{p,q-1}(A,C)$. La formule annoncée en découle. □

Théorème 1. *Si $A := a(X-\alpha_1)...(X-\alpha_p)$ et $B := b(X-\beta_1)...(X-\beta_q)$, alors :*

$$\begin{aligned} Res(A,B) &= b^q A(\beta_1)...A(\beta_q) \\ &= b^p a^q \prod_{\substack{1\le j\le q \\ 1\le i\le p}} (\beta_j - \alpha_i) \\ &= (-1)^{pq} a^q B(\alpha_1)...B(\alpha_p). \end{aligned}$$

Démonstration. La première formule s'obtient en itérant le lemme. La seconde découle alors de l'égalité $A(\beta) = a\prod_{1\le i\le p}(\beta-\alpha)$. La dernière se découle de la seconde □

Corollaire 1. *Supposons le corps L algébriquement clos.alors $Res(A,B) = 0$ si, et seulement si, les polynômes A et B ont une racine commune.*

Définition 1.2. Le *discriminant* de A est défini par la formule :

$$Dis(A) := \frac{(-1)^{\frac{p(p-1)}{2}}}{a_p} Res(A, A')$$

.

Proposition 5. *Pour que $Res(A,B) = 0$, il faut, et il suffit, que A et B aient un facteur commun non constant dans $L[X]$*

Démonstration. si Δ est le *pgcd* de A et B et qu'il est non trivial, en posant $P = \frac{B}{\Delta}$ et $Q = -\frac{A}{\Delta}$, on déduit de la proposition 1 que le résultant est nul. Si $\Delta = 1$, l'égalité $AP + BQ = 0$ entraîne $A|BQ$ donc $A|Q$ (lemme de Gausse) ; si $degQ \le p-1$, on a donc $Q = 0$. D'après la même proposition, le résultant est donc non nul. □

Corollaire 2. *Si l'anneau R est factoriel, pour que $Res(A,B)$ s'annule, il faut, et il suffit, que A et B aient un facteur commun non constant dans $R[X]$.*

Théorème 2. *Soit K un corps algébrique cols. et $A(X) = a_n\prod_{k=1}^{n}(X-\alpha_i)$, $B(X) = b_m\prod_{k=1}^{m}(X-\beta_j)$ et $C(X) = c_t\prod_{k=1}^{t}(X-\gamma_k)$, alors*

$$Res(AB,C) = Res(A,C)\,Res(B,C)$$

Démonstration. On a $(AB)(X) = a_n b_m \prod_{i=1}^{n} \prod_{j=1}^{m} (X - \alpha_i)(X - \beta_j)$ donc le polynôme AB a pour zéros les α_i et β_j. Si on note $\zeta_i = \alpha i$ pour $1 \leq i \leq n$ et $\zeta_{n+j} = \beta_j$ pour $1 \leq j \leq m$, donc :

$$\begin{aligned} Res(AB, C) &= (a_n b_m)^t c_t^{n+m} \prod_{AB(\zeta_i)=0, C(\gamma_k=0)} (\zeta_i - \gamma_k) \\ &= a_n^t c_t^n \prod_{C(\gamma_k=0), i=1}^{n} (\alpha_i - \gamma_k) b_m^t c_t^m \prod_{C(\gamma_k)=0, j=1}^{m} (\beta_j - \gamma_k) \\ &= Res(A, C) Res(B, C) \end{aligned}$$

□

Lemme 2. *Si A et B sont deux polynômes unitaires à coefficients dans un corps, alors leur discriminant vérifie la formule*

$$D(A, B) = \pm Res^2(A, B) Dis(A) Dis(B)$$

Démonstration.

$$\begin{aligned} Dis(AB) &= \pm Res(AB, (AB)') = \pm Res(AB, AB' + A'B) \\ &= \pm Res(A, AB' + A'B) Res(B, AB' + A'B)(thorme2) \\ &= \pm Res(A, A'B) Res(B, AB')(proposition3) \\ &= \pm Res(A, A') Res(A, B) Res(B, A) Res(B, B') \end{aligned}$$

d'où le résultat. □

Lemme 3. *Si $Q = (X - a)P$ est un polynôme cubique à coefficients dans un corps K de caractéristique différente de deux, avec P irréductible sur K, et $a \in K$, alors le discriminant de Q n'est pas un carré dans le corps K.*

Démonstration. Si β et γ sont les racines de P dans une extension convenable du corps K alors :

$$\begin{aligned} Dis(Q) &= (a - \beta)^2 (a - \gamma)^2 (\beta - \gamma)^2 \\ &= R^2(a) Dis(P) \end{aligned}$$

et D(P) n'est pas un carré dans K (sinon P serait réductible)

□

2 Étude de la période d'une SRL d'ordre 2

Cas général :
Soit $(u_n)_{n\in n}$ une suite récurrente linéaire d'ordre 2, à coefficients dans K, définie par ses deux premiers termes et la relation de récurrence :

$$u_{n+2} = bu_{n+1} + cu_n,\ (b,c) \in K \times K^* \tag{1}$$

Notons $\mathbb{U}$ l'espace vectoriel des suites vérifiant (1).
Soit $P(X) = X^2 - bX - c$ le polynôme caractéristique associé à (1). On note Δ le discriminant de $P(X)$.
Un polynôme du second degré a une racine dans K si et seulement si son discriminant est un carré dans K. Cela résulte de la forme canonique :

$$X^2 + bX + c = (X + 2^{-1}b)^2 - 4^{-1}(b^2 - 4ac) = (X + 2^{-1}b)^2 - (2^{-1})^2\Delta$$

En effet, lorsque Δ est un carré dans $\mathbb{F}_p$, alors d'après l'égalité ci-dessus :

$$X^2 + bX + c = (X + 2^{-1}b - (2^{-1})^2\sqrt{\Delta})(X + 2^{-1}b + (2^{-1})^2\sqrt{\Delta})$$

.

— Cas où Δ est un carré dans $\mathbb{F}_p$ ($i.e$ $(\Delta/p) = 1$) :
Le polynôme P a donc deux racines distinctes dans le corps $\mathbb{F}_p$:

$$r_1 = \frac{b - \sqrt{\Delta}}{2} \text{ et } r_2 = \frac{b + \sqrt{\Delta}}{2}$$

. Il existe α et β dans $\mathbb{F}_p$ tels que $u_n = \alpha r_1^n + \beta r_2^n$.
On initialise la suite (u_n) à $u_0 = 0$ et u_1. On a :

$$\begin{cases} u_0 = 0 = \alpha + \beta \\ \\ u_1 = 1 = \alpha r_1 + \beta r_2 \end{cases}$$

On trouve les valeurs de α et β en résolvant le système ci-dessus.

Calcul de la période :

La période s de (u_n divise $ppcm(ord(r_1), ord(r_2))$. En effet : $\alpha r_1^{n+s} + \beta r_2^{n+s} = \alpha r_1^n + \beta r_2^n$

— Cas où $\Delta = 0 = p$, $i.e$ $(\frac{\Delta}{p}) = 0$:
Dans ce cas, P a racine de multiplicité 2 dans $\mathbb{F}_p$. On a :
$u_n = (\alpha n + \beta) r_0^n$.
On a : $s = pgcd(ord(r_0), \alpha^{-1})$ La période divise donc s.

— Cas où Δ n'est pas un carré dans $\mathbb{F}_p$ ($i.e$ $(\frac{\Delta}{p}) = -1$) :
Considérons l'anneau abélien fini

$$A := \frac{\mathbb{F}_p[X]}{< X^2 + bX + c >}$$

Puisque P est de degré 2, il est irréductible dans $\mathbb{F}_p[X]$ si et seulement si il n'a pas de racine dans $\mathbb{F}_p$. Mais comme $\Delta < 0$, alors P n'a pas de racine dans $\mathbb{F}_p$, donc est irréductible dans $\mathbb{F}_p[X]$. L'anneau A est donc un corps.
Notons α la classe de X dans A. Comme α est différent de 0, il appartient au groupe des inversibles de A. Regardons l'ordre de α :
Il existe un diviseur s de p^2-1 tel que $\alpha^s = 1$, donc $X^s - 1 \in < X^2 + bX + c >$, donc $X^2 + bX + c$ divise $X^s - 1$.
Il existe donc $g(X) \in \mathbb{F}_p[X]$ tel que

$$X^s - 1 = (X^2 + bX + c)g(X)$$

. Considérons l'application "$shift$" $X : E \to E$, $(u_n) \mapsto (un + 1)$.
On a :

$$u_{n+s} - u_n = (\underbrace{u_{n+2} + bu_{n+1} + cu_n}_{=0})g(X) = 0$$

Donc la période de (u_n) divise s.

3 Étude de cas : La période de la suite de fibonnacci dans $\mathbb{F}_p$

3.1 La suite de Fibonacci dans $\mathbb{F}_p$:

Soit E l'espace vectoriel des suites récurrentes linéaires (un) vérifiants :

$$u_{n+2} = u_{n+1} + u_n$$

.
On notera $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci, avec $F_0 = 0$ et $F_1 = 1$.
Appliquons l'application shift X à (Fn) :
On a $X^2(F_n) = X(F_n) + id_E(F_n)$, donc $(F_n)(X^2 - X - id_E) = 0$ (suite nulle).
On a, par une analogie, un polynôme de $\mathbb{F}_p[X]$: $P(X) := X^2 - X - 1$, que l'on appelle polynôme caractéristique de (u_n). Une étude de ce polynome nous fournira des informations sur la période de (F_n) dans $\mathbb{F}_p[X]$.
exemple : Dans $\mathbb{F}_3$: période $= 9$ (initialisation a $uo = 0$, $u_1 = 1$)
On sait que si α est une racine de $X^2 - X - 1$, alors $\mathbb{F}_p[X]/(X^2 - X - 1)$ est isomorphe à $\mathbb{F}_p[\alpha]$. Lorsque $X^2 - X - 1$ est irréductible dans $\mathbb{F}_p[X]$, alors $Fp[X]/(X^2 - X - 1)$ est un corps à p^2 éléments, et est isomorphe à $\mathbb{F}_p[\alpha] = \mathbb{F}_p(\alpha)$.

3.2 Illustration : Étude de la période de la suite de Fibonacci dans $\mathbb{F}_5$:

Calculons le discriminant de $P(X)$: $\Delta = 5 = 0$.
On a : $(\frac{\Delta}{5}) = 0$. D'après les résultats vus dans la section précédente, le polynôme caractéristique P de F_n a une racine double $r_0 \in \mathbb{F}_5$. On voit rapidement que $r_0 = 3$. On a donc :

$$\exists\ \alpha, \beta \in \mathbb{F}_5 \text{ tels que : } \forall n \in \mathbb{N},\ F_n = (\alpha n + \beta) \cdot 3^n$$

Déterminons α et β :

$$\begin{cases} F_0 &= (\alpha \cdot 0 + \beta) \cdot 3^0 = 0 \text{ , donc } \beta{=}0 \\ F_1 &= (\alpha \cdot 1 + \beta) \cdot 3^1 = 1 \text{ , donc } \alpha{=}2 \end{cases}$$

Le terme général de (F_n) est donc :

$$F_n = 2 \cdot n \cdot 3^n$$

Calcul de la période t_5 : :

On sait qu'elle divise $5 \cdot (5-1) = 20$.
Les valeurs possibles pour t_5 sont donc : $2, 4, 5, 10, 20$.
On a :

- $F_2 = 1 \neq 0$, donc $t_5 \neq 2$.
- $F_4 = 3 \neq 0$, donc $t_5 \neq 4$.
- $F_5 = 0$ mais $F_6 = -2 \neq 1$, donc $t_5 \neq 5$.
- $F_{10} = 0$ mais $F_{11} = -1 \neq 1$, donc $t_5 \neq 10$.

On en déduit que $t_5 = 20$.

4 Propriétés arithmétique de la période des suites récurrentes linéaires d'ordre 3 à valeur dans un corps fini

Lemme 4. *Soit $Q \in K[X]$ $(car(K) \neq 2)$ un polynôme unitaire cubique de la forme $Q = (X-a)R$, avec $a \in K$ et R irréductible sur K.*
Soit Δ le discriminant de Q.
Alors Δ n'est pas un carré dans K.

Démonstration. Notons α et β les racines de R (dans une certaine extension de K). On a alors :

$$\begin{aligned} \Delta &= \prod_{1 \leq i < j \leq 3} (\alpha_i - \alpha_j)^2, \textit{ avec } \quad \alpha_1 = a, \alpha_2 = \beta, \alpha_3 = \alpha \\ &= (\alpha_1 - \alpha 2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2 \\ &= (a-\beta)^2 (a-\alpha)^2 (\beta - \alpha)^2 \\ &= R(a)^2 D(R) \end{aligned}$$

Pour que Δ soit un carré dans K, il faut donc que $D(R)$ soit aussi un carré dans K.
Or R est irréductible, son discriminant ne peut donc pas être un carré dans K.
Donc Δ n'est pas un carré dans K. □

Proposition 6. *Soit q une puissance d'un nombre premier, et $f(x) \in F_q[X]$ un polynôme irréductible de degré d.*
Soit α une racine de $f(x)$ dans F_{q^d} (une extension de F_q de degré d).
Les racines de f sont :
$\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$.

La preuve de cette dernière proposition est simple.

Considérons maintenant $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire d'ordre 3, définie par la relation de récurrence :

$$u_{n+3} = au_{n+2} + bu_{n+1} + cu_n \text{ , avec } a, b \in K \text{ et } c \in K^\times.$$

On pose : $P(X) := X^3 - aX^2 - bX - c \in Z[X]$ le polynôme caractéristique de (u_n), et α, β, γ les racines de P.

Proposition 7. *Si P est irréductible et $u_n = \lambda\alpha^n + \mu\beta^n + \nu\gamma^n$, alors $t_p | e(p^2+p+1)$, où e est l'ordre de $-c$ dans le corps F_{p^3}.*

Démonstration. On a :
$P(\alpha) = \alpha^3 - a\alpha^2 - b\alpha - c = 0$, donc :

$$\begin{aligned} P(\alpha^p) &= ((\alpha^p)^3 - a(\alpha^p)^2 - b\alpha^p - c) \\ &= ((\alpha^3)^p - a^p(\alpha^2)^p - b^p\alpha^p - c^p) \\ &= (\alpha^3 - a\alpha^2 - b\alpha - c)^p \\ &= P(\alpha)^p \\ &= 0^p = 0 \end{aligned}$$

On a donc :

$$\alpha^p = \alpha \text{ ou } \alpha^p = \beta \text{ ou } \alpha^p = \gamma$$

Puisque P est irréductible sur $\mathbb{F}_p$, on a :

$$\alpha^p = \beta \text{ ou } \alpha^p = \gamma$$

Supposons $\alpha^p = \beta$, alors :

$$P(\beta) \ = \ 0 \ = \ \beta^3 - a\beta^2 - b\beta - c$$

Donc :

$$(\beta^3 - a\beta^2 - b\beta - c)^p \ = \ 0 \ = \ (\beta^p)^3 - a(\beta^p)^2 - b\beta^p - c$$

Par ailleurs, on a $\beta^p \neq \beta$ pour la même raison que $\alpha^p \neq \alpha$.
Donc :

$$\beta^p = \gamma = (\alpha^p)^p = \alpha^{p^2}$$

On a par ailleurs :

$$\alpha\beta\gamma = -c = \alpha\alpha^p\alpha^{p^2} = \alpha^{1+p+p^2}$$

On a :

$$(-c)^e = 1 = \alpha^{e(1+p+p^2)}$$

Puisque $t_p = ord(\alpha)$ (dans K'), on a donc :

$$t_p | e(1+p+p^2)$$

□

Remarques :

(1) Pour la suite de Tribonacci : $u_{n+3} = u_{n+2} + u_{n+1} + u_n$, si le polynôme caractéristique $P \in K[X]$ est irréductible sur $K \neq \mathbb{F}_2$ et : $u_n = \lambda\alpha^n + \mu\beta^n + \nu\gamma^n$, alors $t_p | 2(p^2+p+1)$ puisque -$c = -1$ est d'ordre 2 dans tout corps $K \neq F_2$.
(2) On a :

$$\forall p \geq 3,\ 2(p^2+p+1) \leq p^3 - 1$$

Pour la suite de Tribonacci, on peut donc améliorer la borne $p^3 - 1$ en $2(p^2+p+1)$

Proposition 8. *Soit $(u_n)_{n\in N}$ une SRL d'ordre 3, définie par la relation de récurrence :*

$$\forall n \in \mathbb{N},\ u_{n+3} = au_{n+2} + bu_{n+1} + cu_n\ ,\ avec\ a, b \in K\ et\ c \in K^\times (K = \mathbb{F})$$

On note $P(X)$ le polynôme caractéristique de (u_n) :

$$P(X) = X^3 - aX^2 - bX - c (\in Z[X])$$

On pose : $\Delta := Dis(P)$, et t_p la période de (u_n)

Quatre cas possibles :

(i) P a une racine double ou triple dans $\mathbb{F}_p \Leftrightarrow \Delta \equiv 0[p]$:

$$t_p | p(p-1)$$

(ii) P a une seule racine dans le corps de base $\mathbb{F}_p \Leftrightarrow (\frac{\Delta}{p} = -1)$:

$$t_p | (p^2-1)$$

(iii) P a trois racines distinctes dans $\mathbb{F}_p \Leftrightarrow (\frac{\Delta}{p} = 1)$ et P est non irréductible :

$$t_p | (p-1)$$

(iv) P est irréductible dans $F_p[X] \Leftrightarrow (\frac{\Delta}{p}) = 1$ et le corps de rupture n'est pas le corps de base :

$$t_p | (p^3-1)$$

Démonstration. **Premier cas :** On a donc $\Delta \equiv 0[p]$. C'est le seul cas où $\Delta = 0$, puisqu'on est dans un anneau intègre.
Il existe α, β et γ dans $\mathbb{F}_p$ tels que :

$$u_n = \alpha r_1^n + (\beta n + \gamma) r_2^n$$

On pose $k = p(p-1)$. Il suffit de remarquer la chose suivante :

$$u_{n+k} = \alpha (r_1^{np})^{p-1} + (\beta n + p(p-1) + \gamma)(r_2^n)^{p-1}$$

Puisque r_1^n et r_2^n sont des suites à valeur dans $\mathbb{F}_p$, on a, d'après le petit théorème de Fermat :

$$(r_1^{np})^{p-1} = (r_1^{np})^{p-1} = 1$$

De plus, puisque $p \equiv 0$, on a : $\beta n + p + \gamma = \beta n + \gamma$.
On a donc :

$$u_{n+k} = \alpha r_1^n + (\beta n + \gamma) r_2^n = u_n$$

Donc :

$$t_p | p(p-1)$$

Le cas où P a une racine triple est similaire.

Deuxième cas : P a une racine (simple) dans le corps $\mathbb{F}_p$, et les deux autres racines α et β n'y sont pas.
On a $P(X) = (X-a)R(X)$, avec $R(X)$ de degré 2, et irréductible sur $\mathbb{F}_p$.
D'après le lemme 3 (page 4), cela équivaut à :

$$\Delta = (a-\beta)^2(a-\gamma)^2(\beta-\gamma) = R^2(a)D(R)$$

Ou encore à : $(\frac{\Delta}{p}) = -1$, puisque $D(R)$ n'est pas un carré dans $\mathbb{F}_p$, car sinon R ne serait pas irréductible sur $\mathbb{F}_p$.

Troisième cas : P a trois racines distinctes r_1, r_2 et r_3, toutes dans le corps $\mathbb{F}_p$:
Dans ce cas : $\Delta = [(r_1-r_2)(r_1-r_3)(r_2-r_3)]^2$ est un carré dans $\mathbb{F}_p$: $(\frac{\Delta}{p}) = 1$
Il existe donc α, β et γ dans $\mathbb{F}_p$ tels que :

$$u_n = \alpha r_1^n + \beta r_2^n + \gamma r_3^n$$

. On a donc $t_p | p-1$, puisque $r_i^{n+(p-1)} = (r_i^n)^{p-1} = 1$, toujours d'après le petit théorème de Fermat.

Quatrième cas : Les trois racines de P n'appartiennent pas au corps de base :
P est donc irréductible sur $\mathbb{F}_p$. Soit α une racine de P. Les autres racines sont donc : α^p et α^{p^2}.
On a donc :

$$\begin{aligned}\Delta &= (\alpha - \alpha^p)^2(a - \alpha^{p^2})^2(\alpha^p - \alpha^{p^2}) \\ &= (\alpha^{p+2} - \alpha^{p^2+2} + \alpha^{2p^2+1} - \alpha^{2p+1} + \alpha^{p^2+2p} - \alpha^{2p^2+p})^2\end{aligned}$$

Posons :

$$\gamma = \alpha^{p+2} - \alpha^{p^2+2} + \alpha^{2p^2+1} - \alpha^{2p+1} + \alpha^{p^2+2p} - \alpha^{2p^2+p}$$

On a :

$$\begin{aligned}\gamma^p &= \alpha^{p^2+2p} - \alpha^{2p+1} + \alpha^{p+2} - \alpha^{2p^2+p} + \alpha^{2p^2+1} - \alpha^{p^2+2} \\ &= \gamma\end{aligned}$$

On a donc $\gamma \in \mathbb{F}_p$, et $\Delta = \gamma^2$, donc $(\frac{\Delta}{p}) = 1$.

Remarques :

(1) On remarque qu'en dimension 3, le discriminant ne joue plus son rôle puisqu'il ne discrimine plus les racines du polynôme.

(2) Le cas où P a deux racines dans $\mathbb{F}_p$ et une racine qui n'y est pas est impossible, puisque dans ce cas P ne serait pas à coefficients dans $\mathbb{F}_p$.

(3) On peut diminuer la borne pour le point (iv) : D'après la proposition 7, si $(\frac{\Delta}{p}) = 1$ et P est irréductible, alors $t_p | e(p^2 + p + 1)$, avec $e = ord(-c)$.

□

5 Travail de recherche et étude algorithmique

Nous allons dans cette partie tenter de découvrir des propriétés que vérifient les périodes des SRL de $\mathbb{F}_p^{\mathbb{N}}$.
Nous allons travailler avec deux programmes que nous avons conçu, trop volumineux pour être insérés ici, et qui ont été envoyés en pièces jointes.
Le fonctionnement des programmes sera détaillé lors de la soutenance, et des exemples seront donnés.

Le programme $PIR - PeriodeModP.py$: Il prend en entrée les coefficients d'un polynôme, ceux d'un polynôme caractéristique d'une SRL d'ordre 3, et N un entier.
Il calcule la période de cette SRL pour tous les nombres premiers plus petits que N.
Ensuite, il trace ces périodes en fonction de ces nombres, on peut même rajouter les graphes des fonctions des majorants trouvés à la fin de la partie précédente :
$(p^2 - 1, p(p-1)...)$.

Le programme $PIR - Polynome.py$: Il prend en entrée un nombre premier p.
Il créé tous les polynômes unitaires de degré 3 modulo p, puis calcule la période des SRL modulo p correspondantes à chacun des polynômes.

Le fonctionnement des programmes sera détaillé lors de la soutenance, et des exemples seront donnés.

Les cas possibles illustrés :

Premier cas : P a une racine double ou triple : on a vu que tp divise $p(p-1)$.
Existe t'il des cas ou $tp = p(p-1)$?
Il est évident que si l'une des racines est d'ordre multiplicatif p-1, alors la SRL associée a pour période p-1.
exemple (Figure 1 page 14) : $p = 149$, $P(X) = X^3 - 7X^2 + 16X - 12$
On a en bleu le graphe des valeurs de $p(p-1)$, et en vert les valeurs de t_p

Deuxième cas : P a seule racine dans le corps de base : on sait que t_p divise $p^2 - 1$.
Existe t 'il des cas ou $t_p = p^2 - 1$?
Il est évident que si une racine du polynôme irréductible de degré 2 est une racine primitive de $\mathbb{F}_{p^2}$, alors $t_p = p^2 - 1$.
exemple (Figure 2 page 15) : $P(X) = X^3 - 7X^2 - 9X + 5$ pour $p = 11$ a pour période $120 = 11^2 - 1$.
On a en bleu le graphe des valeurs de $p^2 - 1$, et en vert les valeurs de t_p

Troisième cas : P a trois racines distinctes. Si l'une des racines est d'ordre multiplicatif $p - 1$, alors $t_p = p - 1$.
exemple (Figure 3 de page 16) : $p = 149$ et $P(X) = X^3 - 13X^2 + 146X - 48$: $t_p = 148$.
On a en bleu le graphe des valeurs de $p^2 - 1$, et en vert les valeurs de t_p

Quatrième cas : P est irréductible sur $\mathbb{F}_p$.
Existe t'il des cas où $t_p = p^3 - 1$?
Il est évident que si l'une des racines de P est une racine primitive de $\mathbb{F}_p^3$, alors $t_p = p^3 - 1$
exemple (Figure 4 de page 17) : $p = 17$, $P(X) = X^3 - 3X^2 - 7X - 10$:
On a : $tp = 4912 = 17^3 - 1$.

Remarques :

(1) En réalité, pour les cas 2 et 4, la période est le *ppcm* de l'ordre des racines du polynome irréductible.

(2) On peut se servir du programme *PIR.polynome.py* pour trouver les périodes des polynomes et ainsi determiner ou se situent leurs racines.
En effet, si t_p divise $p^3 - 1$ et pas $p^2 - 1$ ou $p(p-1)$, alors le polynôme est irréductible sur $\mathbb{F}_p$. On peut faire de même pour les autres bornes.
Ainsi, on peut déterminer, pour presque tous les polynômes, ou se situent leur racines.
On peut même aller plus loin : pour trouver les racines primitives de $\mathbb{F}_{p^3}$, il nous suffit de regarder dans les polynômes dont la suite associée est de période $p^3 - 1$, ce qui réduit grandement la recherche plutot que de regarder tous les polynomes irréductibles.

6 Les graphes

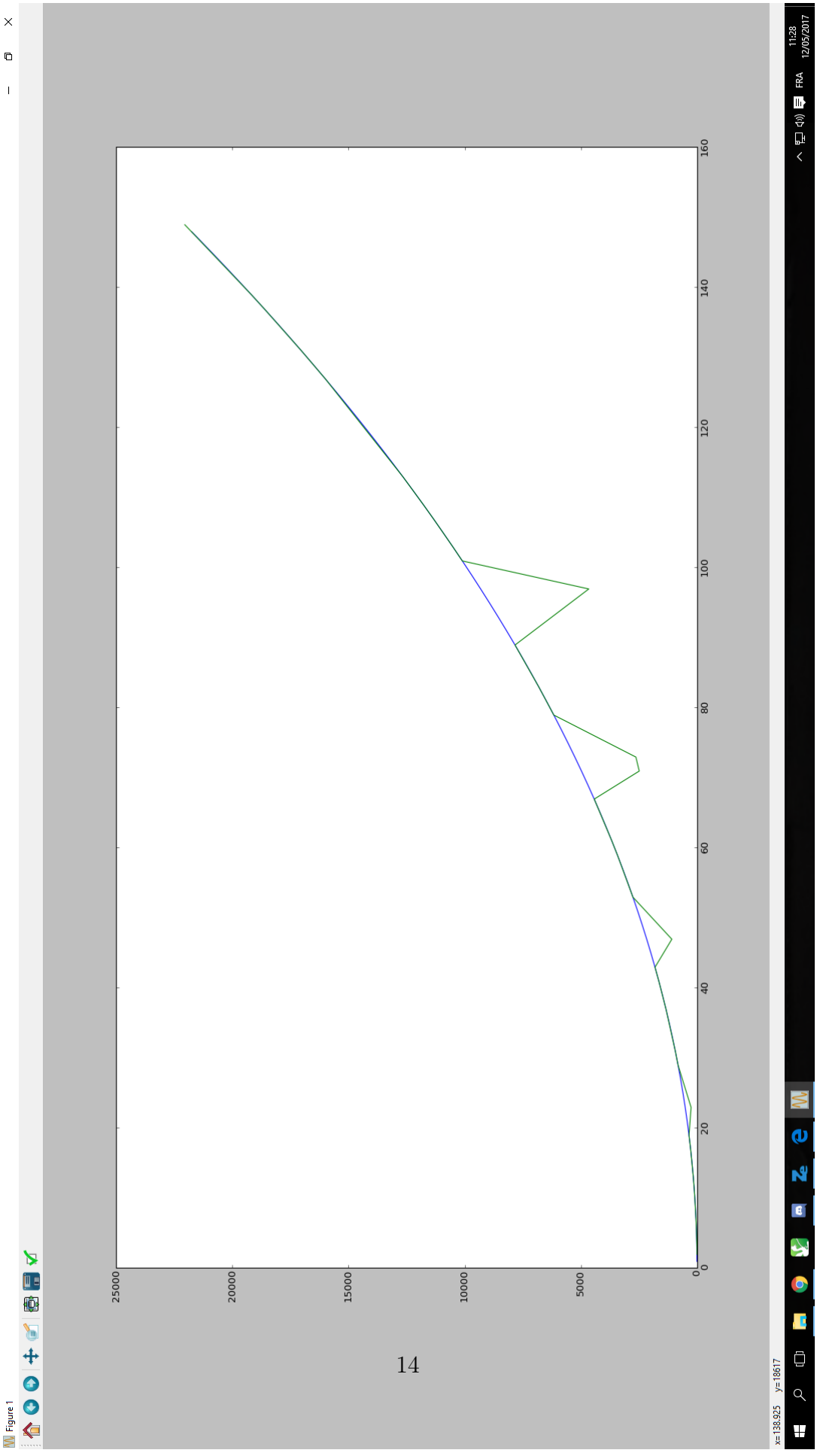

FIGURE 1 – Ici $p = 149$, et $P(X) = X^3 - 7X^2 + 16X - 12$

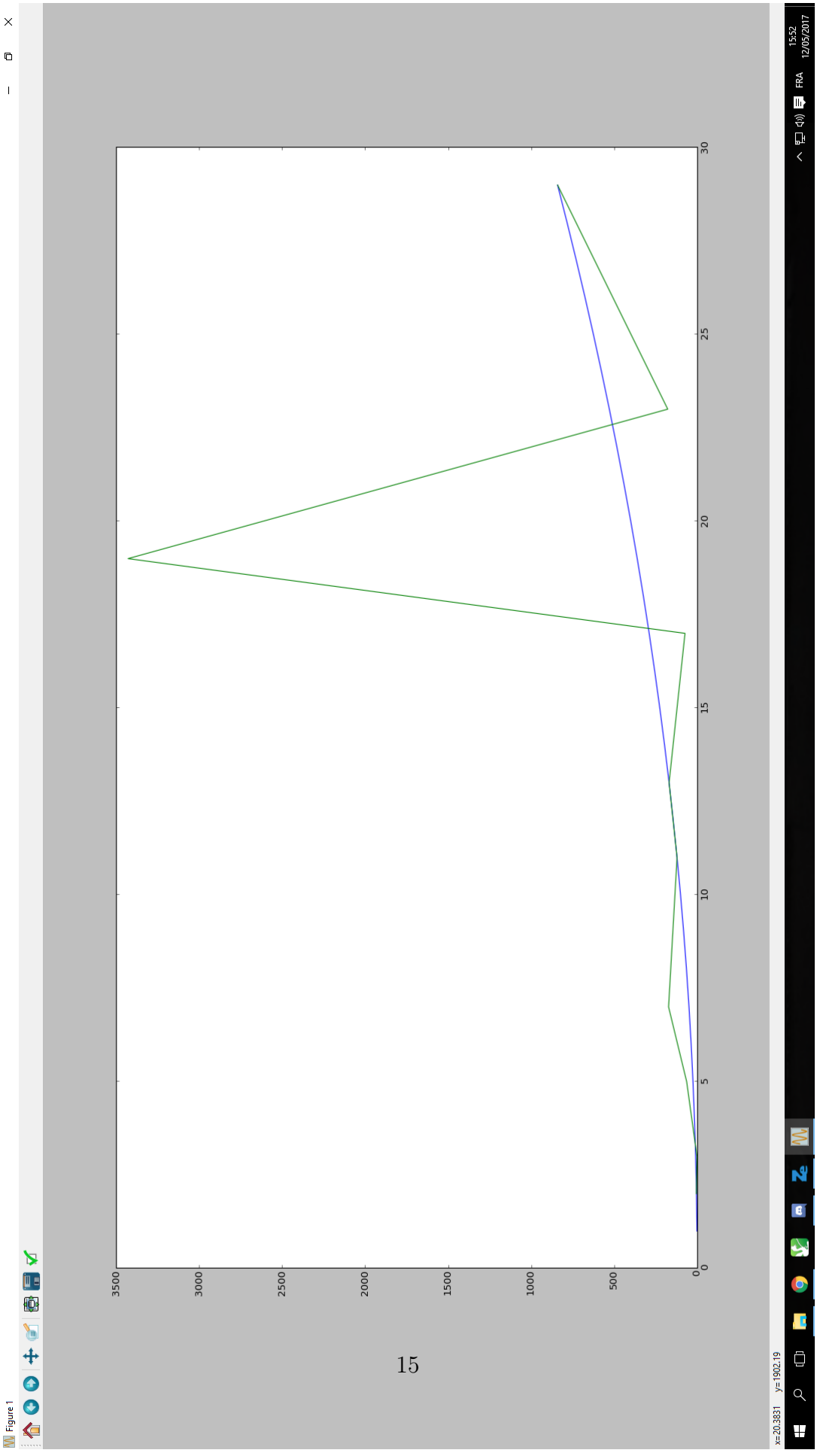

FIGURE 2 – Ici $p = 11$, et $P(X) = X^3 - 7X^2 - 9X + 5$

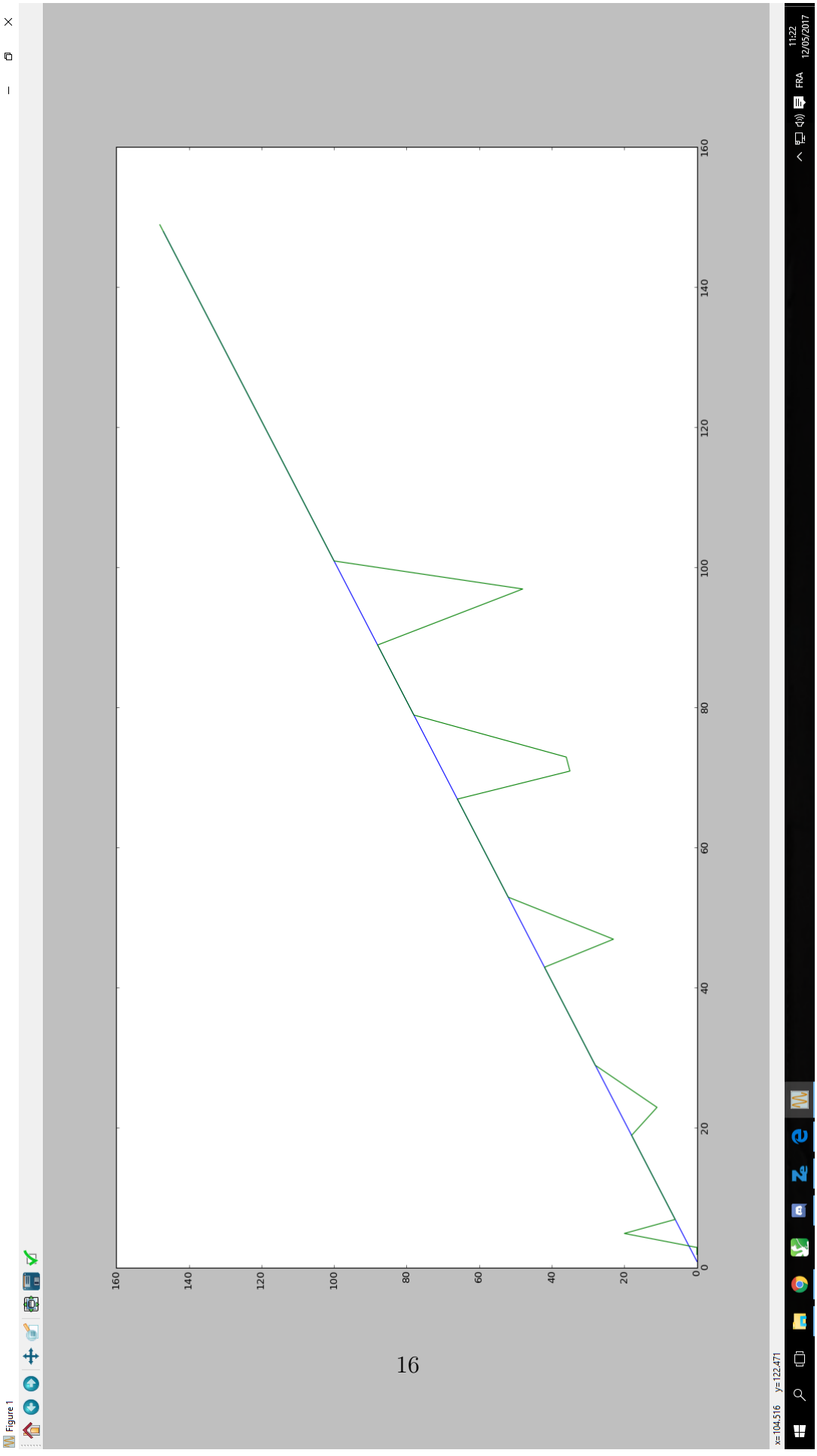

FIGURE 3 – Ici $p = 149$, et $P(X) = X^3 - 13X^2 + 146X - 48$

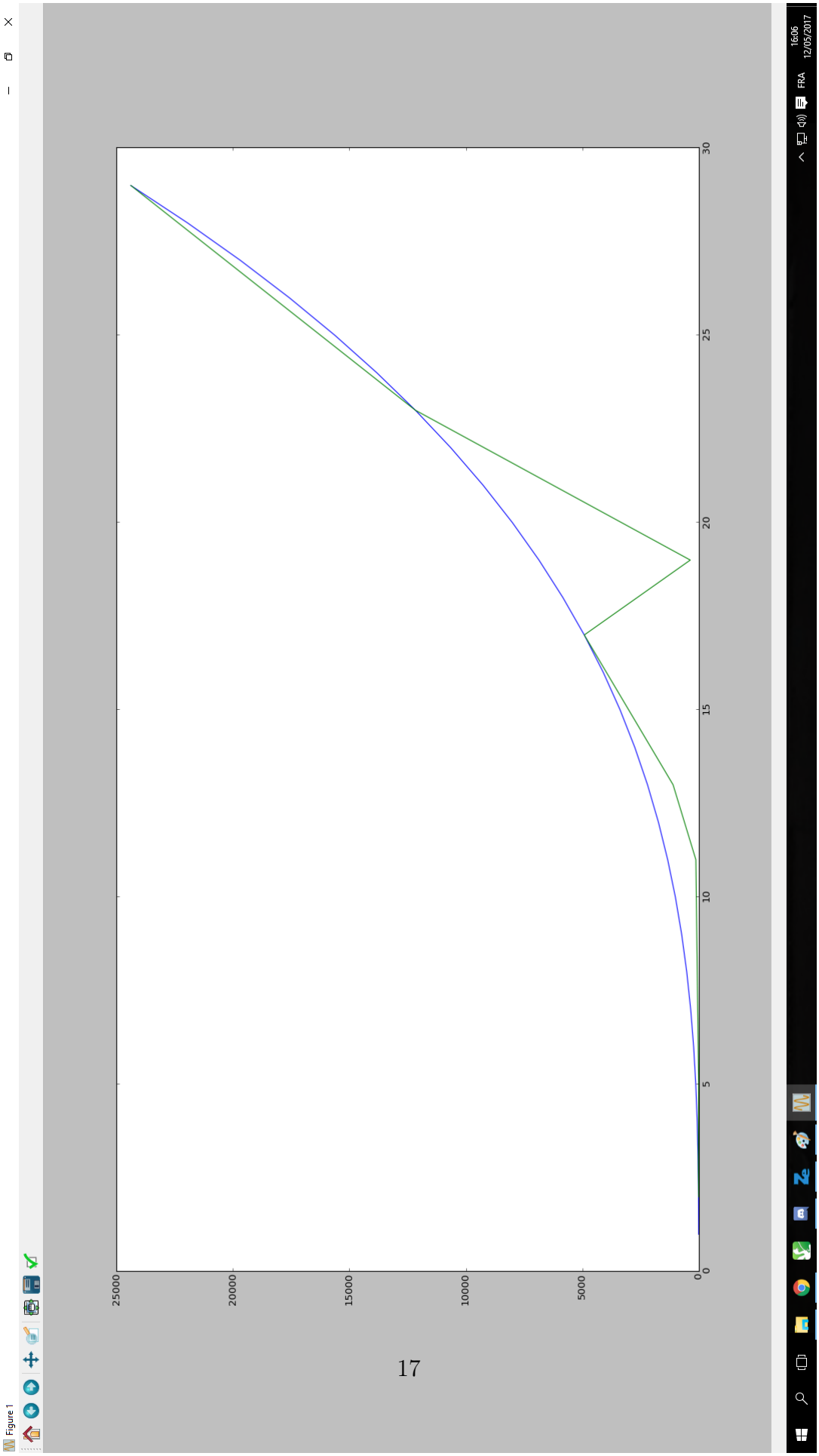

FIGURE 4 – Ici $p = 17$, et $P(X) = X^3 - 3X^2 - 7X - 10$