Quelques aspects sur une généralisation des suites de Fibonacci

http://alain.pichereau.pages.perso-orange.fr
marc.pichereau@wanadoo.fr

Résumé

Dans [5] (et [6], à la question 10 de l'exercice 1 de P4) il a été vu que pour tout nombre premier $p \geq 5$, $2p$ divise $F_{n+2p} - F_{n+p} - F_n$ où $(F_n)_{n\in N}$ est la suite de Fibonacci initialisée par $F_0 = 0,\ F_1 = 1$.
Dominique Guillaume a alors remarqué que ce résultat devait être vrai pour toute suite $(S) = (S_n)_{n\in N}$ vérifiant $S_{n+2} = AS_{n+1} + BS_n,$ avec A, B deux constantes entières non nulles et $S_0,\ S_1$ entiers. Un des buts de cet article est de justifier cette conjecture et de montrer qu'elle permet de prouver de façon assez rapide les deux résultats classiques suivants :
1) si p est premier ≥ 3 alors $2^{\frac{p-1}{2}} \equiv 1\ (p) \Leftrightarrow p \equiv \pm 1\ (8)$ (en prenant $A = 2, B = -2$)
2) si p est premier ≥ 5 alors $3^{\frac{p-1}{2}} \equiv 1\ (p) \Leftrightarrow p \equiv \pm 1\ (12)$ (en prenant $A = 3, B = -3$)

Par ailleur un exemple sera prétexte à évoquer la périodicité des suites (S) modulo un entier.

D'autres résultats sur les suites de Fibonacci se généralisant aux suites (S) seront donnés, ainsi qu'un lien entre deux suites (S) particulières et les polynômes de Tchebychev.
Enfin, je terminerai par un exemple de suite (S) à éléments dans $\mathbb{Z}[i]$ avec illustration de la généralisation de $p\gcd(F_m, F_n) = F_{p\gcd(m,n)}$.

Notations

Dans ce qui suit $(S) = (S_n)_{n\in N}$ sera la suite de nombres complexes vérifiant pour tout $n \geq 0,\ S_{n+2} = AS_{n+1} + BS_n,$ avec A, B **deux complexes quelconques**.
(S) est une suite récurrente linéaire d'ordre 2, d'équation caractéristique $x^2 - Ax - B = 0$, dont les racines, éventuellement confondues, seront notées r_1, r_2.
Le cas $A = B = 1$ donne évidemment les suites de Fibonacci ; $(F) = (F_n)_{n\in N}$ désignera la suite de Fibonacci initialisée par $F_0 = 0,\ F_1 = 1$ et $(L) = (L_n)_{n\in N}$ désignera la suite de Fibonacci initialisée par $L_0 = 2,\ L_1 = 1,$ suite appelée la suite de Lucas.
Pour n et k entiers naturels quelconques on posera $D_{n,k}(S) = S_{n+2k} - AS_{n+k} - BS_n$.
p désignera toujours un nombre premier.
Enfin, on conviendra que $C_0^0 = 1,\ C_n^k = 0$ si $k < 0$ ou $k > n$ et $0^0 = 1$.

I Préliminaires

1) A et B étant deux complexes quelconques, il existe évidemment une et une seule suite $S = (S_n)_{n\in N}$ telle que pour tout $n \geq 0,\ S_{n+2} = AS_{n+1} + BS_n,$ avec $S_0,\ S_1$ deux nombres complexes donnés.

Donc si deux suites (P) et (Q) vérifient pour tout $n \geq 0$ $P_{n+2} = AP_{n+1} + BP_n$ et $Q_{n+2} = AQ_{n+1} + BQ_n$ avec $P_0 = Q_0$ et $P_1 = Q_1$, alors pour tout $n \geq 0$, $P_n = Q_n$.

2) A et B étant deux complexes quelconques, soit $S = (S_n)_{n \in N}$ la seule suite telle que pour tout $n \geq 0$, $S_{n+2} = AS_{n+1} + BS_n$, avec S_0, S_1 deux nombres complexes donnés :

si $B = 0$, **alors pour tout** $n \geq 1$, $S_n = S_1 A^{n-1}$: (S) **est une suite géométrique de raison** A **à partir du rang** 1, cela même si $A = 0$, puisqu'il a été convenu que $0^0 = 1$.

si $A = 0$, alors pour tout $n \geq 0$, $S_{2n} = S_0 B^n$ et $S_{2n+1} = S_1 B^n$

si $A = B = 0$, alors pour tout $n \geq 2$, $S_n = 0$.

3) **Formules de Binet lorsque** $B \neq 0$.

Le terme général S_n de la suite (S) définie par les quatre nombres complexes $A, B \neq 0, S_0, S_1$ s'obtient par les formules de Binet suivantes :

si $A^2 + 4B \neq 0$, pour tout $n \geq 0$, $S_n = \lambda r_1^n + \mu r_2^n$

avec $\lambda = \frac{-r_2 S_0 + S_1}{r_1 - r_2}$ et $\mu = \frac{r_1 S_0 - S_1}{r_1 - r_2}$

si $A^2 + 4B = 0$, pour tout $n \geq 0$, $S_n = \lambda r_1^n + \mu n r_1^n$

avec $r_1 = \frac{A}{2} \neq 0$ (car $B \neq 0$), $\lambda = S_0$ et $\mu = \frac{S_1}{r_1} - S_0$

Pour le prouver, il suffit d'appliquer le 1), en considérant la suite $X_n = \lambda r_1^n + \mu r_2^n$ pour le premier cas ($X_0 = S_0, X_1 = S_1$ et $\forall\, n \geq 0$, $r_i^{n+2} = A r_i^{n+1} + B r_i^n$ pour $i = 1$ et $i = 2$), et la suite $X_n = \lambda r_1^n + \mu n r_1^n$ pour le deuxième cas ($X_0 = S_0, X_1 = S_1$ et $\forall n \geq 0$, $(n+2) r_1^{n+2} = A(n+1) r_1^{n+1} + B n r_1^n$).

Remarque : si $B = 0$, on a évidemment, d'après le 2) ci-dessus, $S_n = S_1 A^{n-1}$ pour tout $n \geq 1$.

4) Rappelons le **théorème de Fermat** qui sera souvent utilisé dans cette étude :

pour tout a dans Z, pour tout nombre premier p, on a $a^p \equiv a\ (p)$, c'est-à-dire p divise $a^p - a$; si en outre p ne divise pas a, alors $a^{p-1} \equiv 1\ (p)$.

II Sur la divisibilité, pour $n \geq 0$, de $D_{n,p}(S) = S_{n+2p} - AS_{n+p} - BS_n$ par $2p$, dans le cas où A, B, S_0, S_1 sont entiers.

Dans [5], il a été prouvé que pour tout nombre premier $p \geq 5$ et pour tout entier naturel n, $F_{n+2p} - F_{n+p} - F_n$ est divisible par $2p$.
On va montrer ici que ce résultat se généralise à **toute** suite (S) avec A, B, S_0, S_1 entiers (ce qui assure que tous les termes de (S) sont entiers), cela sans chercher à expliciter $D_{n,p}(S)$. On verra au III qu'il est cependant possible d'expliciter $D_{n,p}(S)$ dans certains cas.

Proposition 1

k et n étant des entiers naturels quelconques, $S_{n+2k} = \sum_{j=0}^{k} C_k^j A^{k-j} B^j S_{n+k-j}$ $(C_0^0 = 1,\ 0^0 = 1)$.

Si on change n en $n-k$, on obtient pour $n \geq k \geq 0$, $S_{n+k} = \sum_{j=0}^{k} C_k^j A^{k-j} B^j S_{n-j}$, relation qui redonne pour $A = B = 1$ et $S_0 = 0,\ S_1 = 1$ la proposition 2 de [5].

démonstration :
un raisonnement par récurrence est possible, mais la démonstration ci-dessous, d'après une idée de Claude Morin, présente l'avantage de montrer que le résultat vient d'un résultat général sur suites et polynômes.
lemme préliminaire

On se donne deux polynômes quelconques (à coefficients dans C), $P(X) = \sum_{i=0}^{d_1} a_i X^i$ et $Q(X) = \sum_{j=0}^{d_2} b_j X^j$ et on considère leur produit $R(X) = P(X) \times Q(X) = \sum_{l=0}^{d_1+d_2} c_l X^l$.

Alors, pour toute suite $(u) = (u_n)_{n \in N}$ on a
$\forall n \in N,\ \sum_{l=0}^{d_1+d_2} c_l u_{n+l} = \sum_{j=0}^{d_2} b_j (\sum_{i=0}^{d_1} a_i u_{n+i+j})$.

preuve du lemme :
avec la convention $a_i = 0$ si $i < 0$ ou $i > d_1$, $b_j = 0$ si $j < 0$ ou $j > d_2$, et en notant s le membre de gauche,
$s = \sum_{l=0}^{d_1+d_2} (\sum_{j=0}^{l} a_{l-j} b_j u_{n+l}) = \sum_{l=0}^{d_1+d_2} (\sum_{j=0}^{d_1+d_2} a_{l-j} b_j u_{n+l}) = \sum_{j=0}^{d_1+d_2} (\sum_{l=0}^{d_1+d_2} a_{l-j} b_j u_{n+l}) = \sum_{j=0}^{d_1+d_2} (\sum_{l=j}^{d_1+j} a_{l-j} b_j u_{n+l})$,
d'où $s = \sum_{j=0}^{d_1+d_2} b_j (\sum_{l=j}^{d_1+j} a_{l-j} u_{n+l}) = \sum_{j=0}^{d_2} b_j (\sum_{i=0}^{d_1} a_i u_{n+i+j})$. □

application :

de l'identité $u^m - v^m = (u-v) \sum_{i=0}^{m-1} u^{m-1-i} v^i$, valable dans tout anneau commutatif et pour tout entier naturel m non nul, on déduit que pour tout entier naturel k non nul, il existe, un polynôme Q de degré $2k-2$ tel que $X^{2k} - (AX+B)^k = (X^2 - AX - B)Q(X)$.
En prenant alors $R(X) = X^{2k} - (AX+B)^k$, $P(X) = X^2 - AX - B$, le lemme donne, pour tout n dans N et tout $k \geq 1$,
$S_{n+2k} - \sum_{l=0}^{k} C_k^l A^{k-l} B^l S_{n+k-l} = \sum_{j=0}^{2k-2} b_j (S_{n+2+j} - AS_{n+1+j} - BS_{n+j})$, d'où le résultat annoncé, du moins pour $k \geq 1$, puisque par définition même de la suite (S), tous les termes $S_{n+2+j} - AS_{n+1+j} - BS_{n+j}$ sont nuls. Mais si $k = 0$ le résultat est évidemment vrai aussi

$(C_0^0 A^0 B^0 = 1)$. □

Proposition 2

Pour tout nombre premier p, pour tout $n \geq 0$, p divise $D_{n,p}(S) = S_{n+2p} - AS_{n+p} - BS_n$.

démonstration : d'après la proposition 1, pour tout $n \geq 0$

$S_{n+2p} = \sum_{j=0}^{p} C_p^j A^{p-j} B^j S_{n+p-j} = A^p S_{n+p} + B^p S_n + \sum_{j=1}^{p-1} C_p^j A^{p-j} B^j S_{n+p-j}$.

p étant premier, p divise C_p^j pour $j = 1, 2, \ldots, p-1$ et comme d'après le théorème de Fermat $A^p \equiv A\ (p)$ et $B^p \equiv B\ (p)$, c'est que $S_{n+2p} \equiv AS_{n+p} + BS_n\ (p)$. □

Proposition 3 :

Si A ou B est pair, pour tout p premier et tout $n \geq 0$, 2 divise $D_{n,p}(S)$.

Si A et B sont impairs, pour tout p premier distinct de 3 et tout $n \geq 0$, 2 divise $D_{n,p}(S)$ et 2 divise $D_{n,3}(S)$ si et seulement si S_n est pair ; par exemple, pour la suite de Fibonacci et la suite de Lucas on a $D_{1,3}(F) = F_7 - F_4 - F_1 = 13 - 3 - 1 = 9$ et $D_{1,3}(L) = L_7 - L_4 - L_1 = 29 - 7 - 1 = 21$ qui ne sont pas divisibles par 2.

démonstration :

dans toute cette démonstration, $\equiv$ désignera la congruence modulo 2 et ainsi montrer que 2 divise $D_{n,p}(S)$ équivaut à montrer que $D_{n,p}(S) \equiv 0$.

D'après la proposition 1), pour tout $n \geq 0$, on a $S_{n+2p} = A^p S_{n+p} + B^p S_n + \sum_{j=1}^{p-1} C_p^j A^{p-j} B^j S_{n+p-j}$ et comme pour tout entier $k \geq 1$, $A^k \equiv A$, $B^k \equiv B$ (puisque l'élèvation à une puissance $k \geq 1$ ne change pas la parité) c'est que

$D_{n,p}(S) = S_{n+2p} - AS_{n+p} - BS_n \equiv S_{n+2p} - A^p S_{n+p} - B^p S_n \equiv AB \sum_{j=1}^{p-1} C_p^j S_{n+p-j}$.

Il est alors évident que si A ou B est pair on a $D_{n,p} \equiv 0$: le seul problème est lorsque A et B sont impairs.

On suppose donc maintenant que $A \equiv B \equiv 1$.

On a alors, pour tout $n \geq 0$, $S_{n+2} \equiv S_{n+1} + S_n$ (c'est-à-dire, modulo 2, la suite (S) est une suite de Fibonacci) et $D_{n,p}(S) \equiv \sum_{j=1}^{p-1} C_p^j S_{n+p-j}$.

$D_{n,2}(S) \equiv C_2^1 S_{n+1} \equiv 2S_{n+1} \equiv 0$

$D_{n,3}(S) \equiv C_3^1 S_{n+2} + C_3^2 S_{n+1} \equiv S_{n+2} + S_{n+1} \equiv 2S_{n+1} + S_n \equiv S_n$, et donc $D_{n,3}(S) \equiv 0 \Leftrightarrow S_n \equiv 0$.

Examinons maintenant le cas $p \geq 5$.

De $S_{n+2} \equiv S_{n+1} + S_n$, on déduit que pour tout $n \geq 0$, $S_{n+3} \equiv S_{n+2} + S_{n+1} \equiv 2S_{n+1} + S_n \equiv S_n$, c'est à-dire, modulo 2, la suite (S) est périodique, de période 3, à partir du rang 0 (on verra à la fin de l'exemple 4 du IV quelques généralités sur cette notion de périodicité modulo un entier pour les suites (S)).

Donc pour tout $n \geq 0$ et tout entier $k \geq 0$, $S_{n+3k} \equiv S_n$.

En utilisant le fait que $p = 1 + 3k$ ou $p = 2 + 3k$, avec k entier naturel (car p est ici distinct de 3), on peut alors conclure.

$D_{n,p}(S) = S_{n+2p} - AS_{n+p} - BS_n \equiv S_{n+2p} - S_{n+p} - S_n$, d'où

si $p = 1 + 3k$, $D_{n,p}(S) \equiv S_{n+2+6k} - S_{n+1+3k} - S_n \equiv S_{n+2} - S_{n+1} - S_n \equiv 0$ et,

si $p = 2 + 3k$, $D_{n,p}(S) \equiv S_{n+4+6k} - S_{n+2+3k} - S_n \equiv S_{n+1} - S_{n+2} - S_n \equiv S_{n+2} - S_{n+1} - S_n \equiv 0$.

Ainsi, pour tout $p \geq 5,$ pour tout $n \geq 0,$ 2 divise $D_{n,p}(S)$. □

Proposition 4.
Si A ou B est pair, pour tout p premier distinct de 2 et tout $n \geq 0,$ $2p$ divise $D_{n,p}(S)$.
Si A et B sont impairs, pour tout p premier ≥ 5 et tout $n \geq 0,$ $2p$ divise $D_{n,p}(S)$.

démonstration : application immédiate des deux résultats précédents, 2 et p étant premiers entre eux. □

Remarque : vérifions ce résultat lorsque $B = 0$ (donc B est pair) par un calcul explicite de $D_{n,p}(S)$.
On a $D_{n,p}(S) = S_{n+2p} - AS_{n+p},$ d'où, d'après le 2) du I,
si $A = 0$ alors $S_n = 0$ pour $n \geq 2,$ et pour tout $n \geq 0,$ $D_{n,p}(S) = 0,$ divisible par $2p$
si $A \neq 0$ alors $S_n = S_1 A^{n-1}$ pour $n \geq 1,$ et pour tout $n \geq 0,$ $D_{n,p}(S) = S_1 A^{n+p-1}(A^p - A)$;
or $A^p - A$ est divisible par p (Fermat) et par 2 (A^p a même parité que A), donc si p est distinct de 2, $2p$ divise $D_{n,p}(S)$.

Proposition 5 (**dans le cas** $B \neq 0$)
Rien n'empêche de définir une suite (S) pour tout indice n dans Z en posant $S_{n+2} = AS_{n+1} + BS_n$ pour tout $n \in Z,$ la suite étant toujours initialisée par S_0 et S_1.
Pour $n \geq 0,$ il n'y a rien de changé au processus d'obtention des S_n successifs, mais pour $n < 0$ on procéde ainsi :
puisque $B \neq 0,$ $S_n = \frac{1}{B}(S_{n+2} - AS_{n+1}),$ ce qui donne $S_{-1} = \frac{1}{B}(S_1 - AS_0),$
$S_{-2} = \frac{1}{B}(S_0 - AS_{-1}),$ ....
On voit tout de suite que si $B \neq \pm 1,$ il n'y a aucune raison que pour $n < 0,$ $S_n,$ et donc $D_{n,p}(S)$ soient entiers :
par exemple, si $A = 7, B = 3, S_0 = 2, S_1 = 3,$ alors $S_{-1} = \frac{-11}{3}, S_{-2} = \frac{83}{9}$ et
$D_{-2,p} = S_{-2+2p} - 7S_{-2+p} - \frac{83}{3}$ qui n'est pas entier puisque S_{-2+2p} et S_{-2+p} le sont ($p \geq 2$).
Par contre si $B = \pm 1,$ pour $n < 0,$ $S_n,$ et donc $D_{n,p}(S),$ restent évidemment entiers ; par exemple $\forall n \in Z,$ $F_{-n} = (-1)^{n+1} F_n$ et $L_{-n} = (-1)^n L_n$: voir [6].

Lorsque $B \neq 0,$ on a alors les trois résultats suivants :

5.**1**) Les formules de Binet (voir 3) du I) sont vraies pour tout n dans Z.

5.**2**) Les relations de la proposition 1 du II sont vraies pour tout n dans $Z,$ k restant un entier naturel.

5.**3**) **Si** $B = \pm 1,$ les propositions 2,3,4 du II sont vraies pour tout dans Z.

démonstration :
5.**1**) Il suffit d'appliquer le 1) du I qui reste vrai si on remplace tout $n \geq 0$ par tout n dans Z.
Par exemple pour le cas $A^2 + 4B \neq 0,$ on pose, pour n dans Z,
$X_n = \frac{-r_2 S_0 + S_1}{r_1 - r_2} r_1^n + \frac{r_1 S_0 - S_1}{r_1 - r_2} r_2^n$ (voir 3) du I) : la relation $X_{n+2} = AX_{n+1} + BX_n$ est alors vérifiée pour tout n dans Z et comme $X_0 = S_0,$ $X_1 = S_1,$ c'est que pour tout n dans Z, $S_n = X_n$.

5.**2**) k étant un entier naturel quelconque, la première relation de la proposition 1 du II est vraie pour tout $n \geq 0$.

Examinons ce qui se passe pour $n < 0$:
si $n = -1$:
$S_{-1+2k} = \frac{1}{B}(S_{1+2k} - AS_{0+2k})$; comme 1 et 0 sont ≥ 0, on applique la première relation pour $n = 1$ et $n = 0$, soit
$S_{-1+2k} = \frac{1}{B}(\sum_{j=0}^{k} C_k^j A^{k-j} B^j S_{1+k-j} - A\sum_{j=0}^{k} C_k^j A^{k-j} B^j S_{k-j})$
$S_{-1+2k} = \sum_{j=0}^{k} C_k^j A^{k-j} B^j [\frac{1}{B}(S_{1+k-j} - AS_{k-j})] = \sum_{j=0}^{k} C_k^j A^{k-j} B^j S_{-1+k-j}$, et la première relation est vraie pour $n = -1$.
si $n = -2$:
$S_{-2+2k} = \frac{1}{B}(S_{0+2k} - AS_{-1+2k})$; comme 0 et -1 sont ≥ -1, on applique la première relation pour $n = 0$ et $n = -1$, etc.
Ainsi la première relation de la proposition 1 reste vraie pour tout n dans Z (k restant un entier naturel).
En changeant, dans cette première relation, n en $n - k$ (pas besoin d'imposer ici $n - k \geq 0$), la deuxième relation devient vraie aussi pour tout n dans Z.

5.3) puisque $B = \frac{1}{B}$, pour tout j dans Z on $S_j = B(S_{j+2} - AS_{j+1})$, d'où
pour tout n dans Z,
$D_{n,p}(S) = S_{n+2p} - AS_{n+p} - BS_n = B(S_{n+2+2p} - AS_{n+1+2p}) - AB(S_{n+2+p} - AS_{n+1+p}) - B^2(S_{n+2} - AS_{n+1})$, soit
$D_{n,p}(S) = B(D_{n+2,p}(S) - AD_{n+1,p}(S))$.
D'après la proposition 2, $D_{1,p}(S)$ et $D_{0,p}(S)$ sont divisibles par p, donc
$D_{-1,p}(S) = B(D_{1,p}(S) - AD_{0,p}(S))$ est aussi divisible par p,
puis, $D_{0,p}(S)$ et $D_{-1,p}(S)$ sont divisibles par p, donc $D_{-2,p}(S)$ l'est aussi, "etc" : la proposition 2 du II est vraie pour tout n dans Z.
Même raisonnement pour la propositions 3 du II (divisibilité par 2), d'où la proposition 4 du II est encore vraie pour tout n dans Z. □

III Exemples.

Le but est surtout de redémontrer la proposition 4 du II sur trois exemples à partir d'une formule explicite de $D_{n,p}(S)$.

Par contre, pour l'exemple 4, mis ici surtout pour une comparaison avec la suite (F), on ne peut expliciter de façon simple $D_{n,p}(S)$, et on se contente donc de quelques vérifications ; cet exemple est aussi l'occassion de mettre en évidence la périodicité de toute suite (S) lorsqu'on travaille modulo un entier.

p désigne toujours un nombre premier et n toujours un entier naturel.

Exemple 1 : $A, B \neq 0, S_0, S_1$ sont quatre entiers avec $A^2 + 4B = 0$: ceci implique que A est non nul et pair.

L'équation caractéristique a une seule racine $\frac{A}{2}$ (entière, non nulle), donc d'après Binet, pour tout $n \geq 0$ on a $S_n = (S_0 + (\frac{2}{A}S_1 - S_0)n)(\frac{A}{2})^n$.

En posant $\varpi = \frac{2}{A}S_1 - S_0$, et puisque $B = -(\frac{A}{2})^2$,

$D_{n,p}(S) = (\frac{A}{2})^n[(S_0 + \varpi(n+2p))(\frac{A}{2})^{2p} - A(S_0 + \varpi(n+p))(\frac{A}{2})^p + (S_0 + \varpi n)(\frac{A}{2})^2]$

$D_{n,p}(S) = (\frac{A}{2})^n[(S_0 + \varpi n)((\frac{A}{2})^p - \frac{A}{2})^2 + \varpi p(2(\frac{A}{2})^{2p} - A(\frac{A}{2})^p)]$

$D_{n,p}(S) = (\frac{A}{2})^n((\frac{A}{2})^p - \frac{A}{2})[(S_0 + \varpi n)((\frac{A}{2})^p - \frac{A}{2}) + 2\varpi p(\frac{A}{2})^p]$

$D_{n,p}(S) = (\frac{A}{2})^n((\frac{A}{2})^p - \frac{A}{2})[(S_0\frac{A}{2} + n(\varpi\frac{A}{2}))((\frac{A}{2})^{p-1} - 1) + 2p(\varpi\frac{A}{2})(\frac{A}{2})^{p-1}]$

Comme $\varpi\frac{A}{2} = S_1 - S_0\frac{A}{2}$ est entier, $D_{n,p}(S) = \rho((\frac{A}{2})^p - \frac{A}{2})$ avec ρ entier.

$(\frac{A}{2})^p$ et $\frac{A}{2}$ étant de même parité et égaux modulo p (d'après Fermat), pour tout p distinct de 2, pour tout $n \geq 0$, on a bien $2p$ qui divise $D_{n,p}(S)$: c'est la proposition 4, puisque ici A est pair.

Remarque :

si $A = 2$, alors pour tout $n \geq 0$ et tout $p \geq 2$, $S_n = S_0 + (S_1 - S_0)n$, et $D_{n,p}(S) = 0$,

si $A = -2$, alors pour tout $n \geq 0$ et tout $p \geq 3$, $S_n = (S_0 - (S_1 + S_0)n)(-1)^n$ et $D_{n,p}(S) = 0$; par contre $D_{n,2} = 4S_0 - (S_0 + S_1)(4n + 8)$ n'est pas nul en général ; il est cependant divisible par 2×2.

Exemple 2 : A, B, S_0, S_1 sont quatre entiers avec $A^2 + 4B \neq 0$, et une des racines de l'équation caractéristique est $r_1 = \epsilon = \pm 1$.

r_2 étant l'autre racine, on a $r_1 r_2 = -B$ et $r_1 + r_2 = A$, d'où $r_2 = -\epsilon B$ (distincte de r_1, donc $B \neq -1$) et $A = \epsilon(1 - B)$.

Montrons que pour tout $n \geq 0$,

$D_{n,p}(S) = \frac{\epsilon^{n-1}}{B+1}[(\epsilon B S_0 + S_1)(1 - A\epsilon^p - B) + (\epsilon S_0 - S_1)(-B)^n(B^{2p} - A(-\epsilon B)^p - B)]$.

En effet,

soit $B \neq 0$ et la formule de Binet donne, pour tout $n \geq 0$,

$D_{n,p}(S) = \frac{-r_2 S_0 + S_1}{r_1 - r_2} r_1^n(r_1^{2p} - A r_1^p - B) + \frac{r_1 S_0 - S_1}{r_1 - r_2} r_2^n(r_2^{2p} - A r_2^p - B)$ et puisque $r_1 - r_2 = \epsilon(B+1)$, on obtient le résultat annoncé,

soit $B = 0$ et alors pour tout $n \geq 1$, $S_n = S_1 A^{n-1}$ (voir le 2) du I), d'où, pour tout $n \geq 0$, puisque $n + 2p$ et $n + p$ sont ≥ 1 et compte-tenu du fait qu'ici $A = \epsilon = \pm 1$,

$D_{n,p}(S) = S_1 A^{n+2p-1} - A S_1 A^{n+p-1} = S_1 A^{n-1}(1 - A^{p+1})$, ce que donne le résultat annoncé en y faisant $B = 0$.

Pour $p \geq 3$, p est impair, donc

$\epsilon^p = \epsilon,\ 1 - A\epsilon^p - B = 1 - A\epsilon - B = 0,$
$B^{2p} - A(-\epsilon B)^p - B = B^{2p} + \epsilon AB^p - B = B^{2p} + (1-B)B^p - B = (B^p+1)(B^p - B).$

Et, pour tout $n \geq 0,\ D_{n,p}(S) = \rho(B^p - B)$ avec $\rho = \dfrac{\epsilon^{n-1}(\epsilon S_0 - S_1)(-B)^n(B^p+1)}{B+1}$; mais p étant impair, $B+1$ divise B^p+1 (si a et b sont des entiers distincts et m un entier naturel, alors $a-b$ divise $a^m - b^m$) et ρ est ainsi un entier.

D'après Fermat, p divise alors $B^p - B$ et 2 divisant $B^p - B$ (car B^p et B ont même parité), c'est que pour tout $p \geq 3$ et tout $n \geq 0,\ 2p$ divise $\rho(B^p - B) = D_{n,p}(S)$: c'est la proposition 4, compte-tenu que A ou B est pair puisque A et B sont de parités contraires, d'après $A = \epsilon(1-B)$.

Remarque 1

Pour $p \geq 3,$ si $B = 0$ ou si $S_1 = \epsilon S_0$ alors pour tout $n \geq 0,$ on a $D_{n,p}(S) = 0.$

Remarque 2

Dans le cas particulier $A = 3, B = -2$ (les racines de l'équation caractéristique sont 1 et 2),

en prenant $S_0 = 2, S_1 = 3$ on obtient $S_n = 2^n + 1$: la suite (S) contient tous les nombres de Fermat, c'est-à-dire les nombres de la forme $2^{2^n} + 1,$

en prenant $S_0 = 0, S_1 = 1,$ on obtient $S_n = 2^n - 1,$ c'est-à-dire la suite (S) est constituée de tous les nombres de Mersenne (quoique certains auteurs appellent $2^n - 1$ un nombre de Mersenne uniquement s'il est premier).

Au sujet des nombres de Mersenne, notons que si on prend $A = 4, B = -1, S_0 = 2, S_1 = 4$ alors on obtient $S_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n$ et en posant, pour $n \geq 0,\ T_n = S_{2^n}$ on a $T_{n+1} = T_n^2 - 2.$

Cette suite (T) est à la base du test de Lucas-Lehmer sur la primalité des nombres de Mersenne (voir [2]) :

si p est premier $\geq 3,$ alors $2^p - 1$ est premier $\Leftrightarrow 2^p - 1$ divise $T_{p-2}.$

Exemple 3 : $A = -B = 1,\ S_0 = 2, S_1 = 1.$

L'équation caractéristique $x^2 - x + 1 = 0$ a pour racines $-j = e^{-\frac{\pi}{3}}$ et $-j^2 = e^{\frac{\pi}{3}}$ $(j^2 + j + 1 = 0),$ d'où (Binet) pour tout $n \geq 0,\ S_n = (e^{-\frac{\pi}{3}})^n + (e^{\frac{\pi}{3}})^n = 2\cos\dfrac{n\pi}{3}.$

On constate que $S_{n+3} = -S_n$ et $S_{n+6} = S_n$ et S_n ne prend que les quatre valeurs ± 1 et $\pm 2.$

De $D_{n,p}(S) = S_{n+2p} - S_{n+p} + S_n,$ on tire $|D_{n,p}(S)| \leq 6$ et, puisque pour p premier $\geq 5,\ 2p$ doit diviser $D_{n,p}(S),$ c'est que pour p premier ≥ 5 et tout $n \geq 0$ on doit avoir $D_{n,p}(S) = 0.$ Et même, d'après la proposition 5 du II, ceci doit être vrai pour tout n dans $Z.$

Vérifions le.

En fait, pour tout n et tout r dans $Z,\ D_{n,r}(S) = 2\cos\dfrac{(n+2r)\pi}{3} - 2\cos\dfrac{(n+r)\pi}{3} + 2\cos\dfrac{n\pi}{3}$ a la propriété suivante :

si $r \equiv 1$ ou $5\ (6)$ alors $D_{n,r}(S) = 0$

si $r \equiv 0$ ou 2 ou 3 ou $4\ (6)$ alors $D_{n,r}(S) \neq 0.$

Pour cela on remarque que $D_{n,r}(S) = 2\,\mathrm{Re}(e^{i\frac{n\pi}{3}}\varpi_r)$ avec $\varpi_r = (e^{i\frac{r\pi}{3}})^2 - e^{i\frac{r\pi}{3}} + 1,$ et on envisage les six cas possibles :

si $r = 6q,\ e^{i\frac{r\pi}{3}} = 1$ et $\varpi_r = 1,\ D_{n,r}(S) = 2\cos\dfrac{n\pi}{3} \neq 0$

si $r = 6q+3,\ e^{i\frac{r\pi}{3}} = -1$ et $\varpi_r = 3,\ D_{n,r}(S) = 6\cos\dfrac{n\pi}{3} \neq 0$

si $r = 6q+2$, $e^{i\frac{r\pi}{3}} = j$ et $\varpi_r = -2j = 1 - i\sqrt{3}$, $D_{n,r}(S) = 2(\cos\frac{n\pi}{3} + \sqrt{3}\sin\frac{n\pi}{3}) \neq 0$, car $-\sqrt{3}\sin\frac{n\pi}{3} = 0$ ou $\pm\frac{3}{2}$, valeurs que ne peut prendre $\cos\frac{n\pi}{3}$

si $r = 6q+4$, $e^{i\frac{r\pi}{3}} = j^2$ et $\varpi_r = -2j^2 = 1 + i\sqrt{3}$, $D_{n,r}(S) = 2(\cos\frac{n\pi}{3} - \sqrt{3}\sin\frac{n\pi}{3}) \neq 0$

si $r = 6q+1$, $e^{i\frac{r\pi}{3}} = -j^2$ et $\varpi_r = 0$, $D_{n,r}(S) = 0$

si $r = 6q+5$, $e^{i\frac{r\pi}{3}} = -j$ et $\varpi_r = 0$, $D_{n,r}(S) = 0$.

Remarque : en fait $\forall\ S_0$ et S_1 (entiers ou pas), pour p premier ≥ 5, on a $D_{n,p} = 0$.

On part de $S_{n+2} = S_{n+1} - S_n$ qui permet dire (peu importe S_0 et S_1) que $S_{n+3} = S_{n+2} - S_{n+1} = S_{n+1} - S_n - S_{n+1} = -S_n$, d'où $S_{n+6} = S_n$; on en déduit que les valeurs prises par S_n sont $\pm S_0, \pm S_1, \pm(S_0 - S_1)$, puisque par ailleurs $S_2 = S_1 - S_0$.

Pour montrer que pour tout $n \geq 0$, $D_{n,p}(S) = S_{n+2p} - S_{n+p} + S_n$ est nul, on n'utilise pas ici le fait que pour p premier ≥ 5, $2p$ doit diviser $D_{n,p}(S)$ (ce qui exige S_0 et S_1 entiers ce qui n'est pas forcément le cas ici) mais on exploite, outre la périodicité 6 de (S), le fait que p étant premier ≥ 5, $p = 6q \pm 1$:

si $p = 6p+1$, $D_{n,p} = S_{n+12q+2} - S_{n+6q+1} + S_n = S_{n+2} - S_{n+1} + S_n = 0$

si $p = 6q-1$, $D_{n,p} = S_{n+12q-2} - S_{n+6q-1} + S_n = S_{n+4} - S_{n+5} + S_{n+6} = S_{n+6} - S_{n+5} + S_{n+4} = 0$

A noter que $D_{n,p}$ n'est pas forcément nul si $p = 2$ ou 3 :

$D_{0,2} = S_4 - S_2 + S_0 = -S_1 - (S_1 - S_0) + S_0 = 2(S_0 - S_1)$

$D_{0,3} = S_6 - S_3 + S_0 = 3S_0$.

Exemple 4 : $A = B = 3$

Les racines de l'équation caractéristiques $x^2 - 3x - 3 = 0$ sont $\frac{3+\sqrt{21}}{2}$ et $\frac{3-\sqrt{21}}{2,}$, ce qui donne, en prenant $S_0 = S_1 = 1$,

$S_n = \frac{1}{2^{n+1}\sqrt{21}}((-1+\sqrt{21})(3+\sqrt{21})^n + (1+\sqrt{21})(3-\sqrt{21})^n)$ pour tout $n \geq 0$.

Compte-tenu que pour la suite de Fibonacci (F), la formule de Binet ne permet pas d'obtenir une formule "simple" pour F_n, je pense (?) qu'il en est de même pour cette suite (S).

Il me semble donc difficile de trouver une forme explicite de $D_{n,p}$ permettant d'en déduire que pour tout p premier ≥ 5, $2p$ divise $D_{n,p}$.

On peut cependant faire quelques vérifications.

En utilisant la relation $S_{n+2} = 3(S_{n+1} + S_n)$, pour calculer les premiers termes de cette suite on trouve

$D_{1,3}(S) = S_7 - 3S_4 - 3S_1 = 4401 - 3 \times 81 - 3 \times 1$ qui est impair donc 2×3 ne divise pas $D_{1,3}$ (c'est parceque ici A, B, S_1 sont impairs : voir proposition 3), mais 3 divise $D_{1,3}$ (proposition 2).

$D_{1,5}(S) = S_{11} - 3S_6 - 3S_1$ est-il effectivement divisible par $2 \times 5 = 10$?

Pour éviter de calculer S_{11}, calculons modulo 10 les douze premiers termes de la suite (S) : pour cela on remarque que si on note $S_n^{(10)}$ la valeur de S_n modulo 10, valeur choisie dans $\{0;1;\ldots;9\}$, on a $S_{n+2}^{(10)} \equiv 3(S_{n+1}^{(10)} + S_n^{(10)})$ (10).

A partir de cette relation modulo 10 on obtient facilement les douze premières valeurs de $S_n^{(10)}$: 1/1/6/1/1/6/$S_6^{(10)} = 1/1/6/1/1/S_{11}^{(10)} = 6$/...

Donc $D_{1,5}(S) = S_{11} - 3S_6 - 3S_1 \equiv 6 - 3 \times 1 - 3 \times 1 = 0$ (10) et 2×5 divise effectivement $D_{1,5}(S)$.

De la même façon, on montre que 2×7 divise $D_{3,7}(S) = S_{17} - 3S_{10} - 3S_3$.

En effet les dix-huit premières valeurs de la suite $S_n^{(14)}$sont

$1/1/6/S_3^{(14)} = 7/11/12/13/5/12/9/S_{10}^{(14)} = 7/6/11/9/4/11/3/S_{17}^{(14)} = 0/\ldots$, d'où
$D_{3,7}(S) \equiv 0 - 3 \times 7 - 3 \times 7 \equiv 0\ (14)$.

Quelques observations sur la périodicité des suites (S) modulo m : pour la suite (S) considérée dans cet exemple, on constate que la suite des valeurs de S_n modulo 10 est périodique à partir du rang 0 (puisque $S_9 = S_0$ et $S_{10} = S_1$), par contre pour modulo 14, le calcul ci-dessus jusqu'à $S_{17}^{(14)} = 0$ n'est pas suffisant pour conclure : il faut poursuivre ces calculs modulo 14 pour trouver $S_{42}^{(14)} = S_{43}^{(14)} = 1$ et ainsi conclure à la périodicité de la suite $S_n^{(14)}$ à partir du rang 0.

On remarque aussi que la valeur 0 n'apparaît pas dans la suite $S_n^{(10)}$, mais apparaît dans la suite $S_n^{(14)}$.

On sait que la suite $F_n^{(m)}$, c'est-à-dire la suite de Fibonacci modulo m (m entier ≥ 2 ; $F_n^{(m)} \in \{0;1;\ldots;m-1\}$) est toujours périodique, à partir du rang 0 : on verra dans [6], outre la preuve de la périodicité de la suite $F_n^{(m)}$ à partir du rang 0, un lien entre la période de cette suite et la période d'apparition de 0 dans cette suite.

La référence [4] complète ces résultats par une majoration $(6m)$ de la longueur de la période de la suite $F^{(m)}$, et une majoration $(2m)$ de la période d'apparition de 0 dans cette suite. Les deux majorants sont effectivement atteints.

Le lecteur qui veut approfondir cet aspect périodicité pour les suites (S) modulo m (à valeurs dans $\{0;1;\ldots;m-1\}$) pourra, en s'inspirant des méthodes utilisées pour la suite (F), montrer que

a) toute suite (S) modulo m est périodique, mais pas forcément à partir du rang 0 (exemple : prendre la suite (S) ci-dessus et $m = 6$ ou $m = 9$)

b) toute suite (S) modulo m avec m premier avec B est périodique à partir du rang 0

Bien sûr, l'apparition de 0 dans une suite (S) modulo m, signifie qu'un terme de cette suite (S) est divisible par m.

Par exemple, toute suite de Fibonacci est, modulo $m \geq 2$, périodique à partir du rang 0 , puisque tout $m \geq 2$ est premier avec $B = 1$.

Pour la suite (F), puisque $F_0 = 0$, il y a toujours apparition de 0 dans la suite modulo m.

Par contre pour la suite (L), il n'y a pas toujours apparition de 0 dans la suite modulo m :

si $m = 4$, puisque $L_3 = 4$, il y a apparition de 0 ; les premiers termes de $L_n^{(4)}$ sont d'ailleurs $2/1/3/0/3/3/2/1/\ldots$, et donc on en déduit que 4 divise L_{3+6k} pour tout k dans N.

si $m = 5$, les premiers termes de $L_n^{(5)}$ sont $2/1/3/4/2/1/\ldots$ et donc il n'y a pas apparition de 0, c'est-à-dire il n'y a aucun terme de la suite (L) qui soit divisible par 5.

IV Deux applications du II.

1) si p est premier ≥ 3 alors $2^{\frac{p-1}{2}} \equiv 1\ (p) \Leftrightarrow p \equiv \pm 1\ (8)$

2) si p est premier ≥ 5 alors $3^{\frac{p-1}{2}} \equiv 1\ (p) \Leftrightarrow p \equiv \pm 1\ (12)$

Remarque : d'après Fermat, si p premier ne divise pas a, alors p divise $a^{p-1}-1$, donc si en outre $p \geq 3$ alors $p-1$ est pair et p divise $(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1)$, donc p divise $a^{\frac{p-1}{2}}-1$ ou $a^{\frac{p-1}{2}}+1$. Mais lequel de ces facteurs p divise-t-il? Le résultat ci-dessus donne la réponse pour $a=2$ et $a=3$.

Ce résultat est en général prouvé dans le cadre des résidus quadratiques ; il sera démontré ici en utilisant uniquement la proposition 4 du II.

démonstration :

1) On considère la suite (S) définie par $A=2, B=-2, S_0=S_1=1$.

Les racines de l'équation caractéristique X^2-2X+2 sont $1 \pm i = \sqrt{2}\, e^{\pm i\frac{\pi}{4}}$ et Binet donne $S_n = \sqrt{2}^{\,n}\cos\frac{n\pi}{4}$ pour tout $n \geq 0$.

On constate alors que pour tout $n \geq 0$, $S_{n+4} = -4S_n$, d'où pour tout $n \geq 0$, $k \geq 0$, $S_{n+4k} = (-4)^k S_n$.

Considérons, puisque $S_2 = 0$, $D_{2,p} = S_{2+2p} - 2S_{2+p}$.

p étant premier ≥ 3, soit $p = 4q+1$, soit $p = 4q-1$:

si $p = 4q+1$

$D_{2,p} = S_{8q+4} - 2S_{4q+3} = (-4)^{2q+1}S_0 - 2(-4)^q S_3 = (-4)^{2q+1} + 4(-4)^q = 2^{2q+2}((-1)^q - 2^{\frac{p-1}{2}})$

si $p = 4q-1$

$D_{2,p} = S_{8q} - 2S_{4q+1} = (-4)^{2q}S_0 - 2(-4)^q S_1 = (-4)^{2q} - 2(-4)^q = 2^{2q+1}(2^{\frac{p-1}{2}} - (-1)^q)$.

Or d'après la proposition 4 du II, A et B étant pairs et p étant premier ≥ 3, $2p$ divise $D_{2,p}$ (ce qui est d'ailleurs encore vrai ici pour $p=2$ puisque $D_{2,2}=8$), donc pour p premier ≥ 3, $p = 4q \pm 1$ divise toujours $2^{\frac{p-1}{2}} - (-1)^q$.

On prouve maintenant le résulat annoncé pour p premier ≥ 3 :

si $p \equiv \pm 1\ (8)$, alors $p = 8k \pm 1$, donc $p = 4q \pm 1$ avec $q = 2k$ pair, et comme p divise $2^{\frac{p-1}{2}} - (-1)^q$, c'est que p divise $2^{\frac{p-1}{2}} - 1$,

et réciproquement, si p divise $2^{\frac{p-1}{2}} - 1$, comme $p = 4q \pm 1$ divise $2^{\frac{p-1}{2}} - (-1)^q$, par différence on voit que p divise $-1 + (-1)^q$, donc q est pair (sinon p diviserait 2) et $p \equiv \pm 1\ (8)$. □

2) Cette fois on considère la suite (S) définie par $A=3$, $B=-3$ et $S_0 = 2, S_1 = 3$.

Les racines de l'équation caractéristique X^2-3X+3 sont $\frac{3 \pm i\sqrt{3}}{2} = \sqrt{3}\, e^{\pm i\frac{\pi}{6}}$ et Binet donne $S_n = 2(\sqrt{3})^n \cos\frac{n\pi}{6}$.

On en déduit

$S_{6k} = (-1)^k \times 2 \times 3^{3k}$ $S_{6k+1} = (-1)^k \times 3^{3k+1}$ $S_{6k+2} = (-1)^k \times 3^{3k+1}$

$S_{6k+3} = 0$ $S_{6k+4} = (-1)^{k+1} \times 3^{3k+2}$ $S_{6k+5} = (-1)^{k+1} \times 3^{3k+3}$

Bien sûr, comme ci-dessus, on a l'aspect pseudo-périodique : pour tout $n \geq 0$, $S_{n+6} = -27S_{n,}$ et pour tout $n \geq 0,\ k \geq 0,\ S_{n+6k} = (-27)^k S_n$.

Puisque $S_3 = 0,$ on considérera $D_{3,p} = S_{3+2p} - 3S_{3+p}$.

p étant premier ≥ 5, p est de la forme $6q + 1$ ou $6q - 1$:

si $p = 6q + 1$,

$D_{3,6q+1}(S) = S_{12q+5} - 3S_{6q+4} = (-1)^{2q+1}3^{6q+3} - 3(-1)^{q+1}3^{3q+2} = 3^{3q+3}((-1)^q - 3^{\frac{p-1}{2}})$

si $p = 6q - 1$,

$D_{3,6q-1}(S) = S_{12q+1} - 3S_{6q+2} = (-1)^{2q}3^{6q+1} - 3(-1)^q 3^{3q+1} = 3^{3q+2}(3^{\frac{p-1}{2}} - (-1)^q)$.

D'après la proposition 4 du II, pour tout nombre premier $p \geq 5$ et pour tout $n \geq 0,\ 2p$ divise $D_{n,p}(S)$. On ne retiendra là aussi que l'aspect p divise $D_{n,p}(S)$.

Donc si $p = 6q \pm 1$ est premier ≥ 5, p divise toujours $3^{\frac{p-1}{2}} - (-1)^q$.

On peut maintenant montrer le résultat annoncé :

si $p \equiv \pm 1\ (12),$ alors $p = 6q \pm 1$ avec q pair et ainsi p divise $3^{\frac{p-1}{2}} - (-1)^q = 3^{\frac{p-1}{2}} - 1,$

et réciproquement si p divise $3^{\frac{p-1}{2}} - 1,$ comme $p = 6q \pm 1$ divise $3^{\frac{p-1}{2}} - (-1)^q,$ alors p divise $-1 + (-1)^q$ et donc q est pair et $p \equiv \pm 1\ (12)$. □

Remarque : le lecteur aura remarqué que les deux suites (S) utilisées ci-dessus correspondent à $A = -B,$ avec $A = 2$ et $A = 3$ d'où $A^2 + 4B = A(A - 4) < 0$; le cas $A = -B = 1$ donne aussi $A^2 + 4B < 0,$ mais il conduit simplement à $D_{n,p} = 0$ (voir l'exemple 3 du III).

V Sur deux suites (S) particulières généralisant les suites (F) et (L) : les suites (U) et (V).

A et B sont deux complexes quelconques, **pas nécessairement entiers**.

1) On définit les deux suites (S) particulières suivantes :

la suite (U) définie par $U_0 = 0, U_1 = 1$: si $B \neq 0, A^2 + 4B \neq 0, \forall\, n \geq 0$ $U_n = \frac{r_1^n - r_2^n}{r_1 - r_2}$

si $B \neq 0, A^2 + 4B = 0, \forall\, n \geq 0$ $U_n = n(\frac{A}{2})^{n-1}$

si $B = 0, \forall\, n \geq 1$ $U_n = A^{n-1}$

la suite (V) définie par $V_0 = 2, V_1 = A$: si $B \neq 0, A^2 + 4B \neq 0, \forall\, n \geq 0$ $V_n = r_1^n + r_2^n$

si $B \neq 0, A^2 + 4B = 0, \forall\, n \geq 0$ $V_n = 2(\frac{A}{2})^n$

si $B = 0, \forall n \geq 1$ $V_n = A^n$

La suite (V) est appelée la suite compagnon de la suite (U).

Si $A = B = 1$, les suites (U) et (V) deviennent respectivement les suites (F) et (L).

On **notera** aussi que pour tout $n \geq 0$,
$A = 2, B = -1 \Rightarrow U_n = n$; $A = -1, B = 1 \Rightarrow U_n = (-1)^{n+1} F_n$; $A = 3, B = -1 \Rightarrow U_n = F_{2n}$.

2) Pour toute suite (S) on a

2.1) pour tout $n \geq 1$, $S_n = S_1 U_n + S_0 B U_{n-1}$ si $B \neq 0$ la relation est vraie pour $n = 0$ avec $U_{-1} = \frac{1}{B}$

ce qui généralise $g_n = g_1 F_n + g_0 F_{n-1}$ où (g) est une suite de Fibonacci quelconque — vraie pour $n = 0$ avec $F_{-1} = 1$

2.2) pour tout $n \geq 1$, $V_n = AU_n + 2BU_{n-1} = U_{n+1} + BU_{n-1}$ si $B \neq 0$ la relation est vraie pour $n = 0$ avec $U_{-1} = \frac{1}{B}$

ce qui généralise $L_n = F_n + 2F_{n-1} = F_{n+1} + F_{n-1}$

2.3) pour tout $n \geq 0$, $S_n = (S_1 - \frac{S_0 A}{2})U_n + \frac{S_0}{2} V_n$ par exemple si $S_0 = S_1 = 1$ $S_n = (1 - \frac{A}{2})U_n + \frac{1}{2} V_n$

ce qui généralise $g_n = (g_1 - \frac{g_0}{2})F_n + \frac{g_0}{2} L_n$ où (g) est une suite de Fibonacci quelconque

3) Voici d'autres relations sur les suites (U) et (V) qui généralisent des relations sur les suites (F) et (L) :

p est toujours un nombre premier,
A, B sont des complexes quelconques sauf pour F7 et F8 où ils sont entiers,
la colonne de droite se déduit de la colonne centrale en faisant $A = B = 1$.

F1 : $n \geq 1$	$U_n = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n-1}{2}} C_n^{2k+1} A^{n-2k-1} (A^2+4B)^k$	$F_n = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n-1}{2}} 5^k C_n^{2k+1}$
F2 : $n \geq 1$	$V_n = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n}{2}} C_n^{2k} A^{n-2k} (A^2+4B)^k$	$L_n = \frac{1}{2^{n-1}} \sum_{0 \leq k \leq \frac{n}{2}} 5^k C_n^{2k}$
F3 : $n \geq 0$	$U_{2n} = U_n V_n$	$F_{2n} = F_n L_n$
F4 : $n \geq 0$	$V_n^2 - (A^2+4B) U_n^2 = 4(-B)^n$	$L_n^2 - 5F_n^2 = 4(-1)^n$
F5 : $n \geq 0$	$V_{2n} = V_n^2 - 2(-B)^n$	$L_{2n} = L_n^2 - 2(-1)^n$
F6 : $n \geq 1$	$U_n^2 - U_{n-1} U_{n+1} = (-B)^{n-1}$	$F_n^2 - F_{n-1} F_{n+1} = (-1)^{n-1}$
$n \geq 0, m \geq 1$	$U_{n+m} = U_{n+1} U_m + B U_n U_{m-1}$	↑ Formule de Cassini ↑
F7 : A, B entiers, p impair	$U_p \equiv (A^2+4B)^{\frac{p-1}{2}} \ (p)$	$F_p \equiv 5^{\frac{p-1}{2}} \ (p)$
F8 : A, B entiers	$V_p \equiv A \ (p)$ $V_{2p} \equiv A^2 + 2B \ (p)$	$L_p \equiv 1 \ (p)$ $L_{2p} \equiv 3 \ (p)$

4) Sur $p\gcd$ et suite (U), lorsque $A \in \mathbb{Z}$ et $B \in \mathbb{Z}$:

4.1) pour tout $n \geq 1$, U_n et U_{n-1} sont premiers entre eux $\Leftrightarrow$ A et B premiers entre eux

4.2) pour tout $n \geq 0$, tout $m \geq 0$, (pas tous les deux nuls)
$p\gcd(U_n, U_m) = |U_{p\gcd(n,m)}| \Leftrightarrow$ A et B premiers entre eux

Remarque 1 : dans $\mathbb{Z}$, l'usage est de choisir comme $p\gcd$ de deux nombres (pas nuls tous les deux nuls) leur plus grand diviseur positif.
Remarque 2: la propriété est encore vraie si on remplace $\mathbb{Z}$ par $\mathbb{Z}[i]$ (définition rappelée au VII).

Exemples :

1) $A = a+1, B = -a$ avec $a \in \mathbb{Z} - \{1\} \Rightarrow U_n = \frac{a^n - 1}{a-1}$ et on retrouve le résultat $p\gcd(a^n - 1, a^m - 1) = |a^{p\gcd(n,m)} - 1|$:
pour $a = -2$, $U_4 = -5, U_8 = -85, U_{12} = -1365$ et
$p\gcd(U_8, U_{12}) = p\gcd(85, 1365) = 5 = |U_4| = |U_{p\gcd(4,8)}|$

2) $A = 4, B = 9 \Rightarrow U_n = \frac{(2+\sqrt{13})^n - (2-\sqrt{13})^n}{2\sqrt{13}}$:
$p\gcd(U_6, U_9) = p\gcd(4300, 757825) = 25 = U_3 = U_{p\gcd(6,9)}$.

3) On verra au chapitre VII un exemple de suite (U) dont les éléments ne sont pas tous dans $\mathbb{Z}$, mais tous dans $\mathbb{Z}[i]$, et on vérifiera que cette propriété sur le $p\gcd$ est bien vraie dans $\mathbb{Z}[i]$.

Demonstration :

1) Cas U_n : dans le cas $B \neq 0, A^2+4B \neq 0,$ pour toute suite $(S),$ la formule de Binet (voir 3) du I) s'écrit, en groupant les deux termes en S_1 et les deux termes en S_2,
$S_n = S_1\frac{r_1^n - r_2^n}{r_1 - r_2} + S_0 r_1 r_2 \frac{r_2^{n-1} - r_1^{n-1}}{r_1 - r_2}$ pour tout $n \geq 0$, d'où si $S_0 = 0$ et $S_1 = 1$ on obtient, pour $n \geq 0,\ S_n = \frac{r_1^n - r_2^n}{r_1 - r_2} = U_n,$ ce qui prouve que (U) est bien une suite (S).
Je laisse le lecteur vérifier que dans le cas $B \neq 0, A^2+4B = 0,\ S_0 = 0,\ S_1 = 1,$ la formule de Binet donne $S_n = n(\frac{A}{2})^{n-1} = U_n$.

Et si $B = 0,$ pour $n \geq 1\ S_n = S_1 A^{n-1},$ (voir 2) du I), donc en imposant $S_0 = 0,\ S_1 = 1,$ on obtient $S_n = A^{n-1}$ pour $n \geq 1$ (si $A = 0$, pour $n = 1$ cela reste vrai puisque $0^0 = 1$).

Cas V_n : lorsque $B \neq 0, A^2+4B \neq 0,$ on remarque tout de suite $(a^2 - b^2 = (a-b)(a+b))$ que $U_{2n} = U_n V_n$ avec $V_n = r_1^n + r_2^n$, d'où l'idée de considérer cette suite (V). De façon évidente $V_{n+2} = AV_{n+1} + BV_n$ pour tout $n \geq 0$ (puisque les r_i vérifient cette relation de récurrence), donc (voir le 1) du I) la suite (V) est la suite (S) initialisée par $V_0 = 2$ et $V_1 = r_1 + r_2 = A$.
Je laisse là aussi le lecteur vérifier, à l'aide de Binet, que dans le cas $B \neq 0, A^2+4B = 0,$ $S_0 = 2,\ S_1 = A$ on a (c'est immédiat) $S_n = 2(\frac{A}{2})^n = V_n$ pour tout $n \geq 0$.

Et si $B = 0,$ pour $n \geq 1\ S_n = S_1 A^{n-1},$ (voir 2) du I), donc en imposant $S_0 = 2,\ S_1 = A,$ on obtient $S_n = A^n = V_n$ pour $n \geq 1$.

Prouvons les trois cas particuliers :
si $A = 2, B = -1$ une récurrence évidente à partir de $U_{n+2} = 2U_{n+1} - U_n$ donne $U_n = n,$ résultat qui se retrouve aussi par Binet, car l'équation caractéristique est $x^2 - 2x + 1 = 0$ qui a pour racine double 1 et $U_n = \lambda \times 1^n + \mu \times n \times 1^n = \lambda + \mu n$ et $U_0 = 0, U_1 = 1$ donnent $\lambda = 0$ et $\mu = 1,$ soit $U_n = n$;

si $A = -1, B = 1,$ l'équation caractéristique $x^2 + x - 1 = 0$ a pour racines $\frac{-1 \pm \sqrt{5}}{2}$, c'est-à-dire les opposées des racines r_i de $x^2 - x - 1 = 0$ (l'équation caractéristique de la suite (F)), et Binet donne $U_n = \frac{(-r_1)^n - (-r_2)^n}{(-r_1) - (-r_2)} = \frac{(-1)^n}{(-1)} \times \frac{(r_1)^n - (r_2)^n}{(r_1) - (r_2)} = \frac{(-1)^n}{(-1)} F_n$;

si $A = 3, B = -1,$ l'équation caractéristique $x^2 - 3x + 1 = 0$ a pour racines $\frac{3 \pm \sqrt{5}}{2} = (\frac{1 \pm \sqrt{5}}{2})^2,$ c'est-à-dire les carrés des racines r_i de $x^2 - x - 1 = 0,$ et Binet donne $U_n = \frac{(r_1^2)^n - (r_2^2)^n}{r_1^2 - r_2^2}$ et comme $r_1^2 - r_2^2 = (r_1 - r_2)(r_1 + r_2) = r_1 - r_2,\ U_n = F_{2n}$.□

2) La relation 2.1 est une application immédiate de la formule de Binet et de la définition de (U) :
dans le cas $B \neq 0, A^2+4B \neq 0$, le début de la preuve du 1) ci-dessus donne le résultat (puisque par ailleurs $r_1 r_2 = -B$),
et si $B \neq 0, A^2+4B = 0,$ comme $r_1 = \frac{A}{2},$ Binet donne
$S_n = (S_0(1-n) + n\frac{2S_1}{A})(\frac{A}{2})^n = -S_0(n-1)(\frac{A}{2})^{n-2}(\frac{A}{2})^2 + S_1 n(\frac{A}{2})^{n-1},$ soit
$S_n = S_0 B U_{n-1} + S_1 U_n,$ puisque $B = -\frac{A^2}{4}$.
Quant au cas $B = 0,$ pour $n \geq 1,\ S_1 U_n + S_0 B U_{n-1} = S_1 U_n = S_1 A^{n-1} = S_n$ (voir 2) du I).
En prenant pour (S) la suite $(V),$ 2.1 donne 2.2.
Quant à la relation 2.3, elle s'obtient en tirant BU_{n-1} de 2.2 et en reportant dans 2.1. □

3) F1 et F2 :
si $B \neq 0, A^2+4B \neq 0,$ on applique deux fois la formule du binôme pour développer r_1^n et r_2^n, en écrivant $r_i = \frac{A \pm r}{2}$ avec r une racine deuxième de A^2+4B.
si $B \neq 0, A^2+4B = 0,$ le membre de droite se réduit au seul terme correspondant à $k = 0$ et on retrouve bien U_n ou V_n.
si $B = 0,$ on peut factoriser le membre de droite par A^{n-1} ou A^n et on obtient U_n ou V_n car $\sum_{0 \leq k \leq \frac{n}{2}} C_n^{2k} = \sum_{0 \leq k \leq \frac{n-1}{2}} C_n^{2k+1} = 2^{n-1}$.
F3, F4, F5, F6 (1ière relation) : dans chacun des trois cas, $B \neq 0$ et $A^2+4B \neq 0$ ou $B \neq 0$ et $A^2+4B = 0$ ou $B = 0$ la vérification est immédiate à partir des valeurs de U_n et V_n (ne pas oublier que $B^0 = 1$ même si $B = 0$).
Pour la 2ième relation de F6 :
soit $g_m = U_{n+m}$ et $d_m = U_{n+1}U_m + BU_nU_{m-1}$: $g_1 = d_1 = U_{n+1}$ et $g_2 = U_{n+2} = AU_{n+1} + BU_n = d_2$ et par ailleurs il est facile de vérfier que les suites (g) et (d) vérifient la même relation de récurrence puisque $g_{n+2} = Ag_{n+1} + Bg_{n+1}$ et $d_{n+2} = dg_{n+1} + dg_{n+1},$ donc ces suites sont égales.

Cette formule généralise évidemment la relation $F_{n+m} = F_{n+1}F_m + F_nF_{m-1},$ laquelle vient de $u_{n+m} = u_{n+1}F_m + u_nF_{m-1}$ où (u) est une suite de Fibonacci quelconque.

F7 :
si $B \neq 0, A^2+4B \neq 0,$ puisque pour tout p premier et pour tout j tel que $1 \leq j \leq p-1,$ p divise $C_p^j,$ la formule sommatoire F1 donne, pour $p \geq 3,$ $2^{p-1}U_p \equiv (A^2+4B)^{\frac{p-1}{2}}\ (p),$ puisque par ailleurs $2k+1$ ne peut prendre la valeur $0,$ mais prend la valeur p pour $k = \frac{p-1}{2}$.
Comme p ne divise pas $2,$ $2^{p-1} \equiv 1\ (p)$ et $U_p \equiv (A^2+4B)^{\frac{p-1}{2}}\ (p)$; par exemple $U_3 = A^2+B \equiv (A^2+4B)^{\frac{3-1}{2}}\ (3)$.
si $B \neq 0, A^2+4B = 0,$ $U_p = p(\frac{A}{2})^{p-1},$ et donc $U_p \equiv 0\ (p)$ (cela est vrai même pour $p = 2$) et ainsi on a bien $U_p \equiv (A^2+4B)^{\frac{p-1}{2}}\ (p)$ pour p impair.
si $B = 0,$ $U_p = A^{p-1} = (A^2+4B)^{\frac{p-1}{2}}$.

F8 :
si $B \neq 0, A^2+4B \neq 0,$ pour $p \geq 3,$ la formule sommatoire F2 donne $2^{p-1}V_p \equiv A^p \equiv A\ (p),$ puisque $2k$ peut prendre la valeur 0 mais pas la valeur p ; d'où, puisque $2^{p-1} \equiv 1\ (p),$ $V_p \equiv A\ (p)$; et si $p = 2,$ $V_2 = A^2+2B \equiv A^2 \equiv A\ (2)$;
si $B \neq 0, A^2+4B = 0,$ pour tout $n \geq 0,$ $V_n = \frac{1}{2^{n-1}}A^n,$ donc tout pour p premier $2^{p-1}V_p = A^p,$ et on poursuit comme ci-dessus pour obtenir $V_p \equiv A\ (p)$;
si $B = 0,$ $V_p = A^p \equiv A\ (p)$.

Quant à la relation $V_{2p} \equiv A^2+2B\ (p),$ on part de F5 et on applique $V_p \equiv A\ (p),$ d'où $V_{2p} \equiv A^2-2(-B)^p\ (p)$ et Fermat donne $V_{2p} \equiv A^2-2(-B) \equiv A^2+2B\ (p).$ Ce qui donne d'ailleurs $V_4 \equiv A\ (2)$.

4)

Preuve 4.1) :

si U_n et U_{n-1} sont premiers entre eux pour tout $n \geq 1$, alors $U_2 = A$ et $U_3 = A^2 + B$ sont premiers entre eux, donc $p\gcd(A, A^2 + B) = 1$, mais $p\gcd(A, A^2 + B) = p\gcd(A, B)$, puisque les deux couples de nombres ont mêmes diviseurs, donc on a bien $p\gcd(A, B) = 1$.

Supposons maintenant que $p\gcd(A, B) = 1$.

On va montrer par récurrence que U_n et U_{n-1} sont premiers entre eux pour tout $n \geq 1$.

C'est vrai pour $n = 1$ car $U_1 = 1$ et $U_0 = 0$ sont premiers entre eux.

Supposons que pour $n \geq 1$, U_n et U_{n-1} soient premiers entre eux.

Si U_{n+1} et U_n ne sont pas premiers entre eux, c'est qu'il existe un nombre $d > 1$ (ou d différent d'un inversible pour le cas $\mathbb{Z}[i]$) les divisant.

Ce d est obigatoirement premier avec U_{n-1}, sinon d et U_{n-1} auraient un diviseur commun $d' > 1$ (ou d' différent d'un inversible pour le cas $\mathbb{Z}[i]$), et d' diviserait alors U_n et U_{n-1}, ce qui est contraire à l'hypothèse de récurrence.

Or d divise aussi $BU_{n-1} = U_{n+1} - AU_n$, et comme il est premier avec U_{n-1}, d divise B (raisonnement valable dans le cas $\mathbb{Z}[i]$).

Mais $U_{n+1} = A^n + B \times W(A, B)$ avec W polynôme à coefficients entiers (voir le VI), et comme d divise U_{n+1} et B, d divise A^n (avec $n \geq 1$) et finalement d divise A^n et B, ce qui est en contradiction avec $p\gcd(A^n, B) = p\gcd(A, B) = 1$ (raisonnement valable dans $\mathbb{Z}[i]$).

Donc on ne peut supposer l'existence de $d > 1$ (ou d différent d'un inversible pour le cas $\mathbb{Z}[i]$) divisant U_{n+1} et U_n et ainsi U_{n+1} et U_n sont bien premiers entre eux : la récurrence est prouvée.

Preuve 4.2) :

si $p\gcd(U_n, U_m) = |U_{p\gcd(n,m)}|$ pour n et m entiers naturels pas tous les deux nuls, en faisant $n = 2, m = 3$ on obtient encore $p\gcd(A, A^2 + B) = |U_1|$, soit $p\gcd(A, B) = 1$.

Supposons maintenant que $p\gcd(A, B) = 1$.

On va montrer que $p\gcd(U_n, U_m) = U_{p\gcd(n,m)}$ pour n et m entiers naturels pas tous les deux nuls en utilisant la même méthode que celle utilisée pour la suite de Fibonacci (F).

Si un seul des indices est nul, par exemple $m = 0$, on a $p\gcd(U_n, U_0) = |U_n| = |U_{p\gcd(n,0)}|$.

On suppose maintenant que n et m sont ≥ 1.

La 2ième relation de F6 donne $p\gcd(U_{n+m}, U_n) = p\gcd(U_{n+1}U_m, U_n)$, les deux couples de nombres ayant les mêmes diviseurs.

Or si d divise U_n, d est premier avec U_{n+1}, sinon il existe $d' > 1$ (ou d' différent d'un inversible pour le cas $\mathbb{Z}[i]$) divisant d et U_{n+1}, et ainsi d' divise U_n et U_{n+1} ce qui est contraire au fait que U_n et U_{n+1} sont premiers entre eux,

d'après l'hypothèse $p\gcd(A, B) = 1$ et le 4.1 ; donc si d divise U_n et $U_{n+1}U_m$, d divise U_n et U_m ; la réciproque étant évidemment vraie, $p\gcd(U_{n+1}U_m, U_n) = p\gcd(U_m, U_n)$ et ainsi $p\gcd(U_{n+m}, U_n) = p\gcd(U_m, U_n)$.

Mais cette dernière relation est vraie pour tout $n \geq 1$ et $m \geq 1$, donc en échangeant n et m on a $p\gcd(U_{n+m}, U_m) = p\gcd(U_n, U_m)$ et donc pour tout $n \geq 1$ et $m \geq 1$, $p\gcd(U_n, U_m) = p\gcd(U_{n+m}, U_{n \text{ ou } m})$.

En supposant $m \geq n$ (sinon on les échange), on a $m = qn + r$ avec $0 \leq r < n$ et

$p\gcd(U_n, U_r) = p\gcd(U_n, U_{n+r}) = p\gcd(U_n, U_{2n+r}) = \ldots = p\gcd(U_n, U_{qn+r}) = p\gcd(U_n, U_m)$

C'est-à-dire

$p\gcd(U_n, U_m) = p\gcd(U_n, U_r)$ avec r reste de la division de m par n, et donc

$p\gcd(U_n, U_r) = p\gcd(U_r, U_{r_1})$ avec r_1 reste de la division de n par r (licite car $n > r$)

$p\gcd(U_r, U_{r_1}) = p\gcd(U_{r_1}, U_{r_2})$ avec r_2 reste de la division de r par r_1 (licite car $r > r_1$)

etc jusqu'à arriver à un dernier reste $r_{k-1} \neq 0$ (et $r_k = 0$), cad

$p\gcd(U_n, U_m) = p\gcd(U_{r_{k-1}}, U_{r_k}) = |U_{r_{k-1}}|$.
Mais $r_{k-1} = p\gcd(n,m)$ (d'après l'algorithme d'Euclide), ce qui prouve le résultat.

Pour les exemples, il suffit de chercher les racines de l'équation caractéristique (a et 1 pour le premier exemple, $2 \pm \sqrt{13}$ pour le second) et appliquer Binet.
Pour le premier exemple, rappelons que, dans $\mathbb{Z}$, $p\gcd(\rho\lambda, \rho\mu) = |\rho| p\gcd(\lambda, \mu)$.□

VI Ecriture, en fonction de A et B, du terme général des suites (V) et (U) et lien avec les polynômes de Tchebychev.

A et B sont deux complexes quelconques, **pas nécessairement entiers**.

Premières valeurs de U_n et V_n :

n	U_n	V_n
0	0	2
1	1	A
2	A	A^2+2B
3	A^2+B	A^3+3AB
4	A^3+2AB	$A^4+4A^2B+2B^2$
5	$A^4+3A^2B+B^2$	$A^5+5A^3B+5AB^2$
6	$A^5+4A^3B+3AB^2$	$A^6+6A^4B+9A^2B^2+2B^3$

Remarque : c'est à partir de ces tableaux que Dominique Guillaume a conjecturé les propositions 2,3,4 du II.

1) Par une récurrence facile on vérifie que pour tout $n \geq 0$, U_n et V_n sont deux polynômes à deux variables A et B, à coefficients entiers, polynômes qui sont précisés ci-dessous.

1.1) pour tout $n \geq 1$, $U_n = \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^{k} A^{n-1-2k} B^k$: considéré comme un polynôme en A, ce polynôme est de degré $n-1$, unitaire et a la parité contraire de n.

Applications : $\forall\, n \geq 1$,

$$F_n = \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^{k}$$

$$\sum_{0 \leq k \leq \frac{n-1}{2}} (-1)^k \frac{C_{n-1-k}^{k}}{4^k} = \frac{n}{2^{n-1}}$$

$$\sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^{k} 2^k = \frac{2^n + (-1)^{n-1}}{3}.$$

1.2) pour tout $n \geq 1$, $V_n = \sum_{0 \leq k \leq \frac{n}{2}} (C_{n-1-k}^{k} + 2C_{n-1-k}^{k-1}) A^{n-2k} B^k = \sum_{0 \leq k \leq \frac{n}{2}} \frac{nC_{n-k}^{k}}{n-k} A^{n-2k} B^k$:

considéré comme un polynôme en A, ce polynôme est de degré n, unitaire et a la parité de n.

Tous les coefficients des $A^{n-2k}B^k$ sont bien des entiers et, **si n est premier** ils sont tous divisibles par n (excepté celui de A^n), et on retrouve le F8 du 3) du V lorsque A et B sont entiers : $V_n \equiv A^n \equiv A\ (n)$.

Remarque : pour $n \geq 3, 1 \leq k \leq \frac{n-1}{2}$, on a $\frac{C_{n-k}^{k}}{n-k} = \frac{C_{n-1-k}^{k-1}}{k} = \frac{C_{n-1-k}^{k}}{n-2k}$.

Applications : $\forall n \geq 1$,

$L_n = 1 + n \sum_{1 \leq k \leq \frac{n}{2}} \frac{C_{n-k}^k}{n-k}$; cette formule me semble apparaître moins souvent dans la littérature que celle donnée au 1.1 pour F_n.

Par exemple $L_6 = 1 + 6(\frac{C_5^1}{5} + \frac{C_4^2}{4} + \frac{C_3^3}{3}) = 18$.

$$\sum_{0 \leq k \leq \frac{n}{2}} (-1)^k \frac{C_{n-k}^k}{(n-k) \times 4^k} = \frac{1}{n 2^{n-1}}$$

$$\sum_{0 \leq k \leq \frac{n}{2}} \frac{C_{n-k}^k}{n-k} 2^k = \frac{1}{n}(2^n + (-1)^n).$$

1.3) pour tout $n \geq 0$, V_n, considéré comme un polynôme en A, a pour polynôme dérivé nU_n.

2) **Lien entre lien entre les suites** (U), (V) **et les polynômes de Tchebychev** ([**3**]), **lorsque** $B \neq 0$.

Pour $n \geq 0$, il ya deux sortes de polynômes de Tchebychev :
ceux de première espèce, T_n, et ceux de deuxième espèce, Z_n.
T_n est le seul polynôme de degré n tel que pour tout θ dans R, $T_n(\cos\theta) = \cos(n\theta)$:
$T_0(X) = 1$, $T_1(X) = X$, $T_2(X) = 2X^2 - 1$, $T_3(X) = 4X^3 - 3X$,
et pour tout $n \geq 0$, $T_{n+2}(X) = 2XT_{n+1}(X) - T_n(X)$.

Quant à Z_n, pour tout $\theta \neq k\pi$, on a $Z_n(\cos\theta) = \frac{\sin((n+1)\theta)}{\sin\theta}$, et
$Z_0(X) = 1$, $Z_1(X) = 2X$, $Z_2(X) = 4X^2 - 1$, $Z_3(X) = 8X^3 - 4X$,
et pour tout $n \geq 0$, $Z_{n+2}(X) = 2XZ_{n+1}(X) - Z_n(X)$.

On remarque que ces deux suites de polynômes vérifient la même relation de récurrence, laquelle est analogue à celle vérifiée par toute suite (S), ce qui explique les résultats ci-dessous, mais l'initialisation n'est pas la même puisque $Z_1(X) \neq T_1(X)$.

On a alors les résultats suivants :

ξ étant une racine deuxième de $-B$,

$$\forall n \geq 1 \; U_n = \xi^{n-1} Z_{n-1}(\frac{A}{2\xi})$$

$$\forall n \geq 0 \; V_n = 2\xi^n T_n(\frac{A}{2\xi})$$

Cas particuliers :

$B = -1$ donne $\forall n \geq 1 \; U_n = Z_{n-1}(\frac{A}{2})$ et $\forall n \geq 0 \; V_n = 2T_n(\frac{A}{2})$

$A = B = 1$ donne : $\forall\, n \geq 1$, $F_n = i^{n-1} Z_{n-1}(\frac{-i}{2})$ et $\forall n \geq 0$, $L_n = 2i^n T_n(\frac{-i}{2})$ (par exemple $L_3 = 2i^3(4(\frac{-i}{2})^3 - 3(\frac{-i}{2})) \; = 4$).

Application à une factorisation de U_n :

$A, B \neq 0$ étant quelconques, $\forall\, n \geq 2$, $U_n = \prod_{k=1}^{n-1}(A - 2\xi\cos(\frac{k\pi}{n}))$.

Si B est réel négatif, on peut prendre $\xi = \sqrt{-B}$, et cette formule factorise U_n en un produit de réels, par contre si B est réel positif, ξ n'est pas réel ($\xi = \pm i\sqrt{B}$), mais en passant d'abord au module, on obtient aussi une factorisation de U_n en un produit de

réels.
On déduit de cette factorisation, pour tout $n \geq 2$,
si n est pair, $\prod_{k=1}^{\frac{n}{2}-1} \sin^2(\frac{k\pi}{n}) = \frac{n}{2^{n-1}}$ et si n est impair, $\prod_{k=1}^{\frac{n-1}{2}} \sin^2(\frac{k\pi}{n}) = \frac{n}{2^{n-1}}$.
Voir [1] pour plus de résultats sur cette factorisation de U_n et l'application au cas $A = B = 1$ (cas qui est aussi dans [6]).

démonstration :

1.**1**)

Si on observe bien les coefficients des premiers U_n, par exemple $U_6 = A^5 + 4A^3B + 3AB^2$, le coefficient de A^5 est $1 = C_6^0$ ou $...C_5^0$, mais celui de A^3B est 4 qui est ni un C_6^i, ni un C_5^i, par contre c'est C_4^1 et le coefficient de AB^2 est 3 qui n'est pas un C_4^i mais c'est C_3^2 : donc les coefficients de U_6 sont C_{5-k}^k, d'où l'idée de conjecturer que les coefficients de U_n sont $C_{(n-1)-k}^k$.
On va le prouver en utilisant le 1) du I.
Pour $n \geq 1$, posons $X_n = \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^k A^{n-1-2k} B^k$.
On a $X_1 = C_0^0 A^0 B^0 = 1 = U_1$ et $X_2 = A = U_2$.
$AX_{n+1} + BX_n = \sum_{0 \leq k \leq \frac{n}{2}} C_{n-k}^k A^{n+1-2k} B^k + \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^k A^{n-1-2k} B^{k+1}$, et en changeant k en $k-1$ dans le deuxième sigma, on obtient
$AX_{n+1} + BX_n = \sum_{0 \leq k \leq \frac{n}{2}} C_{n-k}^k A^{n+1-2k} B^k + \sum_{1 \leq k \leq \frac{n+1}{2}} C_{n-k}^{k-1} A^{n+1-2k} B^k$, ce qui s'écrit
$AX_{n+1} + BX_n = \sum_{0 \leq k \leq \frac{n+1}{2}} C_{n-k}^k A^{n+1-2k} B^k + \sum_{0 \leq k \leq \frac{n+1}{2}} C_{n-k}^{k-1} A^{n+1-2k} B^k$, car pour le premier sigma, si $k = \frac{n+1}{2}$ (éventualité possible que si n est impair), $C_{\frac{n-1}{2}}^{\frac{n+1}{2}} = 0$ et pour le deuxième sigma, si $k = 0$, $C_n^{-1} = 0$.
On a alors $AX_{n+1} + BX_n = \sum_{0 \leq k \leq \frac{n+1}{2}} s_k A^{n+1-2k} B^k$ avec $s_k = C_{n-k}^k + C_{n-k}^{k-1}$.
Pour $1 \leq k \leq n-k$, soit $1 \leq k \leq \frac{n}{2}$, on a évidemment (triangle de Pascal) $s_k = C_{n+1-k}^k$; mais si $k = 0$, $s_k = C_n^0 + 0 = C_{n+1}^0$ et si $k = \frac{n+1}{2}$ (exige n impair),
$s_k = 0 + C_{n-\frac{n+1}{2}}^{\frac{n+1}{2}-1} = 1 = C_{n+1-\frac{n+1}{2}}^{\frac{n+1}{2}}$.
Finalement, pour tout $n \geq 1$, $AX_{n+1} + BX_n = \sum_{0 \leq k \leq \frac{n+1}{2}} C_{n+1-k}^k A^{n+1-2k} B^k = X_{n+2}$ et donc d'après le 1) du I, pour tout $n \geq 1$, $X_n = U_n$.
Quant aux applications, elles correspondent aux trois cas suivants :1) $A = B = 1$, 2) $B = -\frac{A^2}{4} \neq 0$, U_n étant alors égal à $n(\frac{A}{2})^{n-1}$, 3) $A = -1, B = 2$.

1.**2**)

Pour obtenir la forme polynomiale de V_n on part de $V_n = AU_n + 2BU_{n-1}$ (voir 2.2 du V) et on remplace U_n et U_{n-1} par leurs formes polynomiales trouvées au 1.1).

Pour $n \geq 2$, $V_n = \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^{k} A^{n-2k} B^k + 2 \sum_{0 \leq k \leq \frac{n-2}{2}} C_{n-2-k}^{k} A^{n-2-2k} B^{k+1}$, puis

$V_n = \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^{k} A^{n-2k} B^k + 2 \sum_{1 \leq k \leq \frac{n}{2}} C_{n-1-k}^{k-1} A^{n-2k} B^k$, ce qui s'écrit

$V_n = \sum_{0 \leq k \leq \frac{n}{2}} C_{n-1-k}^{k} A^{n-2k} B^k + 2 \sum_{0 \leq k \leq \frac{n}{2}} C_{n-1-k}^{k-1} A^{n-2k} B^k$, car pour le premier sigma, si $k = \frac{n}{2}$ (ce qui exige n pair) on a $C_{\frac{n}{2}-1}^{\frac{n}{2}} = 0$ et pour le deuxième sigma, si $k = 0$ on a $C_{n-1}^{-1} = 0$.

Finalement $V_n = \sum_{0 \leq k \leq \frac{n}{2}} (C_{n-1-k}^{k} + 2C_{n-1-k}^{k-1}) A^{n-2k} B^k$.

Pour $n \geq 3$ et $1 \leq k \leq \frac{n-1}{2}$ simplifions $s_k = C_{n-1-k}^{k} + 2C_{n-1-k}^{k-1}$:

$s_k = \frac{(n-1-k)(n-2-k)\ldots(n-2k)}{k!} + 2\frac{(n-1-k)(n-2-k)..(n-2k+1)}{(k-1)!}$,

$s_k = \frac{(n-1-k)(n-2-k)\ldots(n-2k+1)(n-2k+2k)}{k!} = \frac{nC_{n-1-k}^{k-1}}{k}$

$s_k = \frac{(n-k)(n-1-k)(n-2-k)\ldots(n-2k+1)(n)}{(n-k)k!} = \frac{nC_{n-k}^{k}}{n-k}$

$s_k = \frac{(n-1-k)(n-2-k)\ldots(n-2k+1)(n-2k)(n)}{(n-2k)k!} = \frac{nC_{n-1-k}^{k}}{n-2k}$.

Mais si $k = 0$, $s_0 = C_{n-1}^{0} = 1$ et $\frac{nC_{n-k}^{k}}{n-k} = 1$ et si $k = \frac{n}{2}$ (lorsque n est pair)

$s_{\frac{n}{2}} = 0 + 2 \times 1 = 2$ et $\frac{nC_{n-k}^{k}}{n-k} = \frac{n}{\frac{n}{2}} = 2$.

Finalement pour $n \geq 3$, $V_n = \sum_{0 \leq k \leq \frac{n}{2}} (C_{n-1-k}^{k} + 2C_{n-1-k}^{k-1}) A^{n-2k} B^k = \sum_{0 \leq k \leq \frac{n}{2}} \frac{nC_{n-k}^{k}}{n-k} A^{n-2k} B^k$; mais on vérifie que pour $n = 1$ les deux sommes donnent bien A qui est V_1 et pour $n = 2$ elles donnent $A^2 + 2B$ qui est V_2.

Donc pour tout $n \geq 1$, $V_n = \sum_{0 \leq k \leq \frac{n}{2}} (C_{n-1-k}^{k} + 2C_{n-1-k}^{k-1}) A^{n-2k} B^k = \sum_{0 \leq k \leq \frac{n}{2}} \frac{nC_{n-k}^{k}}{n-k} A^{n-2k} B^k$.

La première formule montre que les coefficients des $A^{n-2k}B^k$ sont tous entiers, ce qui bien sûr, d'après la relation de récurrence vérifiée par (V), et le fait que $V_0 = 2$, $V_1 = A$, était prévisible.

Donc pour $n \geq 2$, et $1 \leq k \leq \frac{n}{2}$, $n-k$ divise nC_{n-k}^{k}, d'où si n est un nombre premier, comme $0 < n-k < n$, $n-k$ est premier avec n, c'est que $n-k$ divise C_{n-k}^{k}, ce qui prouve que $\frac{nC_{n-k}^{k}}{n-k}$ est divisible par n.

Quant aux applications, elles correspondent aux trois cas suivants :1) $A = B = 1$, 2) $B = -\frac{A^2}{4} \neq 0$, soit $V_n = 2(\frac{A}{2})^n$, 3) $A = -1, B = 2$, soit $V_n = 1 + (-2)^n$.

1.3) V_n étant considéré comme un polynôme en A, on note $\frac{\partial V_n}{\partial A}$ son polynôme dérivé : montrons que $\frac{\partial V_n}{\partial A} = nU_n$.

Bien entendu ce résultat est évident lorsque $B = 0$ puisque dans ce cas, pour $n \geq 1$ on a $U_n = A^{n-1}$ et $V_n = A^n$.

Montrons le pour B quelconque.

On vérifie facilement que le résultat est vrai pour $n = 0$.

Pour $n \geq 1$, d'après le 1.2), $V_n = \sum_{0 \leq k \leq \frac{n}{2}} \frac{nC_{n-k}^k}{n-k} A^{n-2k} B^k$,

donc $\frac{\partial V_n}{\partial A} = \sum_{0 \leq k < \frac{n}{2}} \frac{nC_{n-k}^k}{n-k} \times (n-2k) A^{n-2k-1} B^k$, car lorsque n est pair, pour $k = \frac{n}{2}$, on a $A^{n-2k} B^k = B^{\frac{n}{2}}$ dont la dérivée par rapport à A est nulle.

Mais $0 \leq k < \frac{n}{2} \Leftrightarrow 0 \leq k \leq \frac{n-1}{2}$; en effet le membre de droite entraîne évidemment le membre de gauche et si on a $0 \leq k < \frac{n}{2}$, soit $n = 2l$ et $k < \frac{2l}{2}$ implique $k \leq l - 1 = \frac{n-2}{2} < \frac{n-1}{2}$, soit $n = 2l+1$ et $k < \frac{2l+1}{2}$ implique $k \leq l = \frac{n-1}{2}$.

Donc $\frac{\partial V_n}{\partial A} = \sum_{0 \leq k \leq \frac{n-1}{2}} \frac{nC_{n-k}^k}{n-k} \times (n-2k) A^{n-2k-1} B^k$.

Mais au 1.2) il a été vu que pour $n \geq 3$ et $1 \leq k \leq \frac{n-1}{2}$ on a $\frac{C_{n-k}^k}{n-k} = \frac{C_{n-1-k}^k}{n-2k}$, égalité qui reste vraie pour $k = 0$, et pour $n = 1$ ou $n = 2$ (k ne pouvant alors être que 0).

Finalement, pour tout $n \geq 1$, $\frac{\partial V_n}{\partial A} = n \sum_{0 \leq k \leq \frac{n-1}{2}} C_{n-1-k}^k A^{n-2k-1} B^k = nU_n$.

Voici une autre façon de prouver $\frac{\partial V_n}{\partial A} = nU_n$ sans utiliser les développements polynômiaux obtenus aux 1.1 et 1.2.

On procéde par récurrence :

le résultat est évidement vrai pour $n = 0$ et $n = 1$

supposons le vrai jusqu'au rang $n \geq 1$:

$\frac{\partial V_{n+1}}{\partial A} = \frac{\partial (AV_n + BV_{n-1})}{\partial A} = V_n + A\frac{\partial V_n}{\partial A} + B\frac{\partial V_{n-1}}{\partial A} = V_n + nAU_n + (n-1)BU_{n-1}$

$\frac{\partial V_{n+1}}{\partial A} = V_n - BU_{n-1} + n(AU_n + BU_{n-1})$, soit, d'après le 2.2 du V,

$\frac{\partial V_{n+1}}{\partial A} = U_{n+1} + nU_{n+1} = (n+1)U_{n+1}$, et la propriété est vraie au rang $n+1$. □

2) Dans la démonstration du IV, on remarque que les deux suites (S) considérées correspondent à $A \neq 0, B \neq 0$ réels, $A^2 + 4B < 0$ et pour chacune S_n est de la forme $ka^n \cos n\theta$.

Examinons de façon générale le cas $A, B \neq 0$ réels, $\Delta = A^2 + 4B < 0$ (donc $B < 0$) : les racines de l'équation caractéristique sont alors $r_i = \frac{A \pm i\sqrt{-\Delta}}{2} = \sqrt{-B}\, e^{\pm i\theta}$ avec

$\cos\theta = \frac{A}{2\sqrt{-B}}$, $\sin\theta = \frac{\sqrt{-\Delta}}{2\sqrt{-B}} > 0$.

On obtient alors, pour tout $n \geq 0$,

$V_n = r_1^n + r_2^n = 2(\sqrt{-B})^n \cos(n\theta) = 2(\sqrt{-B})^n T_n(\cos\theta) = 2(\sqrt{-B})^n T_n(\frac{A}{2\sqrt{-B}})$.

Quant à $U_n = \frac{r_1^n - r_2^n}{r_1 - r_2}$, on obtient, pour $n \geq 1$,
$U_n = (\sqrt{-B})^{n-1} \frac{\sin n\theta}{\sin\theta} = (\sqrt{-B})^{n-1} Z_{n-1}(\cos\theta) = (\sqrt{-B})^{n-1} Z_{n-1}(\frac{A}{2\sqrt{-B}})$, puisque $\sin\theta \neq 0$.

Ces formules sont obtenues pour $A, B \neq 0$ réels, $\Delta = A^2 + 4B < 0$: en fait leur domaine de validité s'étend à tous complexes A et $B \neq 0$ en remplacant le $\sqrt{-B}$ ci-dessus par une racine deuxième ξ, quelconque, de $-B$:

cas U_n :

posons pour $n \geq 1$, $Y_n = \xi^{n-1} Z_{n-1}(\frac{A}{2\xi})$: puisque $Z_{n+1}(\frac{A}{2\xi}) = \frac{A}{\xi} Z_n(\frac{A}{2\xi}) - Z_{n-1}(\frac{A}{2\xi})$, en multipliant les deux membres par ξ^{n+1} on obtient, pour $n \geq 1$, $Y_{n+2} = AY_{n+1} + BY_n$; comme $Y_1 = 1 = U_1$, $Y_2 = \xi \times 2\frac{A}{2\xi} = A = U_2$, c'est que pour tout $n \geq 1$, $U_n = Y_n = \xi^{n-1} Z_{n-1}(\frac{A}{2\xi})$, d'après le 1) du I.

cas V_n :

posons pour $n \geq 0$, $Y_n = 2\xi^n T_n(\frac{A}{2\xi})$: puisque $T_{n+2}(\frac{A}{2\xi}) = \frac{A}{\xi} T_{n+1}(\frac{A}{2\xi}) - T_n(\frac{A}{2\xi})$, en multipliant les deux membres par $2\xi^{n+2}$ on obtient, pour $n \geq 0$, $Y_{n+2} = AY_{n+1} + BY_n$; comme $Y_0 = 2 = V_0$, $Y_1 = 2\xi\frac{A}{2\xi} = A = V_1$, c'est que pour tout $n \geq 0$,
$V_n = Y_n = 2\xi^n T_n(\frac{A}{2\xi})$.

Dans le cas particulier $B = -1$, on a $\xi = 1$, d'où $\forall n \geq 1$, $U_n = Z_{n-1}(\frac{A}{2})$ et $\forall n \geq 0$,
$V_n = 2T_n(\frac{A}{2})$.

Application à la factorisation de U_n :

puisque $U_n = \xi^{n-1} Z_{n-1}(\frac{A}{2\xi})$ pour $n \geq 1$, il suffit de factoriser Z_{n-1} pour obtenir une factorisation de U_n.

Z_0 est une constante, mais pour $n \geq 1$, Z_n est de degré n et son coefficient de tête est 2^n, une récurrence immédiate, à partir de $Z_{n+2}(X) = 2XZ_{n+1}(X) - Z_n(X))$, le prouvant (autre façon : pour tout $n \geq 0$, $Z_n(\frac{A}{2}) = U_{n+1}$, la suite (U) correspondant à $B = -1$, et d'après le 1.1 du VI, U_{n+1} est un polynôme en A de degré n et unitaire).

Quant à ses racines, puisque $Z_n(\cos\theta) = \frac{\sin((n+1)\theta)}{\sin\theta}$, on voit que pour $n \geq 1$, $\cos(\frac{k\pi}{n+1})$ pour $k = 1, \ldots, n$ sont n racines distinctes de Z_n, donc ce sont ses n racines puisqu'il est de degré n.

Ainsi pour $n \geq 1$, $Z_n(X) = 2^n \prod_{k=1}^{n} (X - \cos(\frac{k\pi}{n+1}))$ et pour $n \geq 2$,
$U_n = \xi^{n-1} 2^{n-1} \prod_{k=1}^{n-1} (\frac{A}{2\xi} - \cos(\frac{k\pi}{n})) = \prod_{k=1}^{n-1} (A - 2\xi\cos(\frac{k\pi}{n}))$.

Vérifions : $U_2 = A - 2\xi\cos\frac{\pi}{2} = A$,
$U_3 = (A - 2\xi\cos\frac{\pi}{3})(A - 2\xi\cos\frac{2\pi}{3}) = (A - \xi)(A + \xi) = A^2 - \xi^2 = A^2 + B$.

Application de cette factorisation de U_n au cas $A^2 + 4B = 0$, $A \neq 0$:

puisque $B = -(\frac{A}{2})^2$, on a $\xi = \frac{A}{2}$ ou $-\frac{A}{2}$ et comme $U_n = n(\frac{A}{2})^{n-1}$, on obtient, ϵ étant toujours égal à 1 ou toujours à -1, $n(\frac{A}{2})^{n-1} = \prod_{k=1}^{n-1} (A - \epsilon A\cos(\frac{k\pi}{n}))$, ce qui donne
$\prod_{k=1}^{n-1} (1 - \cos\frac{k\pi}{n}) = \prod_{k=1}^{n-1} (1 + \cos\frac{k\pi}{n}) = \frac{n}{2^{n-1}}$ pour tout $n \geq 2$.

Le fait que $\prod_{k=1}^{n-1}(1-\cos(\frac{k\pi}{n})) = \prod_{k=1}^{n-1}(1+\cos(\frac{k\pi}{n}))$ n'est pas vraiment une surprise car $\cos(\frac{k\pi}{n}) = -\cos(\frac{(n-k)\pi}{n})$, et donc en regroupant les termes de la forme $1-\cos\theta$ et $1+\cos\theta$, on voit que pour $n \geq 3$, la valeur commune de ces deux factorisations est soit $\prod_{k=1}^{\frac{n}{2}-1} \sin^2(\frac{k\pi}{n})$ si n est pair, soit $\prod_{k=1}^{\frac{n-1}{2}} \sin^2(\frac{k\pi}{n})$ si n est impair.

Par exemple, $\prod_{k=1}^{2}\sin^2(\frac{k\pi}{6}) = \frac{6}{2^5}$, $\prod_{k=1}^{3}\sin^2(\frac{k\pi}{7}) = \frac{7}{2^6}$.

Cette identité peut se retrouver en considérant les n racines de $(z+1)^n - 1$, le produit des $n-1$ racines non nulles étant $(-1)^{n-1}n$. □

VII Sur $p\gcd$ et suites (U) à éléments dans $\mathbb{Z}[i]$.

1) Rappels sur $Z[i]$ et $p\gcd$ dans $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ est l'ensemble des nombres $a+bi$ avec a et b dans $\mathbb{Z}$ et i tel que $i^2=-1$; il est appelé l'ensemble des entiers de Gauss.

C'est un anneau euclidien, donc principal et factoriel.

Il posséde exactement quatre inversibles : ± 1 et $\pm i$.

u et v étant dans $\mathbb{Z}[i]$

$d\in\mathbb{Z}[i]$ est un $p\gcd$ de u et v signifie d divise u et v et si $d'\in\mathbb{Z}[i]$ divise u et v alors d' divise d

tous les générateurs de l'idéal (principal) $u\mathbb{Z}[i]+v\mathbb{Z}[i]$ sont les $p\gcd$ de u et v : si d est l'un d'entre eux les autres sont $-d, id, -id$; cad si d et d' sont deux $p\gcd$ de u et v, $d'=\pm d$ ou $d'=\pm id$

d est un $p\gcd$ de u et $v\Rightarrow$ il existe x et y dans $\mathbb{Z}[i]$ tels que $d=xu+yv$

u et v sont premiers entre eux signifie que 1 est un de leur $p\gcd$, cad $1=u\mathbb{Z}[i]+v\mathbb{Z}[i]$

u et v sont premiers entre eux$\Leftrightarrow$il existe x et y dans $\mathbb{Z}[i]$ tels que $1=xu+yv$

pour tout k et k' dans N^*, si u et v sont premiers entre eux, alors u^k et $v^{k'}$ sont aussi premiers entre eux

(on élève $1=xu+yv$ à la puissance k, ce qui donne $1=x^ku^k+y'v$, égalité qu'on élève à la puissance k')

si $d\in\mathbb{Z}[i]$ divise uv et si d est premier avec u, alors d divise v

($1=xd+yu$, donc $v=xdv+yuv$)

Comment trouver un $p\gcd$ dans $\mathbb{Z}[i]$?

Voici un exemple : $u=-7220-1000i$ et $v=-136+208i$.

étape 1 : $\frac{u}{v}\simeq 12.531+26.518i$; on prend $q_1=m+in$ avec m et n dans $\mathbb{Z}$ tels que $|12.531-m|\leq\frac{1}{2}$ et $|26.518-n|\leq\frac{1}{2}$,

soit $q_1=13+27i$ et $u=q_1v+r_1$ avec $r_1=u-vq_1=164-32i$; donc $p\gcd(u,v)=p\gcd(v,r_1)$, les deux couples de nombres ayant mêmes diviseurs.

étape 2 : $\frac{v}{r_1}=\frac{-136+208i}{164-32i}\simeq -1.03+1.063$ et on prend $q_1=m+in$ avec m et n dans $\mathbb{Z}$ tels que $|-1.03-m|\leq\frac{1}{2}$ et $|1.063-n|\leq\frac{1}{2}$,

soit $q_2=-1+i$ et $v=q_2r_1+r_2$ avec $r_2=v-q_2r_1=-4+12i$; donc $p\gcd(v,r_1)=p\gcd(r_1,r_2)$

étape 3 : $\frac{r_1}{r_2}=-6.5-11.5i$ et on prend $q_3=m+in$ avec m et n dans $\mathbb{Z}$ tels que $|-6.5-m|\leq\frac{1}{2}$ et $|-11.5-n|\leq\frac{1}{2}$

soit $q_3=-6-11i$ (on aurait pu prendre $-7-12i$) et $r_1=q_3r_2+r_3$ avec $r_3=r_1-q_3r_2=8-4i$; donc $p\gcd(r_1,r_2)=p\gcd(r_2,r_3)$

étape 4 : $\frac{r_2}{r_3}=-1+i$ et cette fois $q_4=-1+i$ (puisque m et n sont nuls), et $r_2=q_4r_3+r_4$ avec $r_4=0$: cela veut dire évidemment que r_3 divise r_2, donc un $p\gcd$ de r_2 et r_3 est r_3, et donc un $p\gcd$ de u et v est $r_3=8-4i$, cad le dernier reste non nul, et les autres $p\gcd$ sont $-8+4i, 4+8i, -4-8i$.

Remarque 1 : $\frac{u}{8-4i}=-672-461i$, $\frac{v}{8-4i}=-24+14i$: donc $-672-461i$ et $-24+14i$ sont premiers entre eux.

Remarque 2 : si à l'étape 1 ci-dessus on avait considéré le quatient $\frac{v}{u}$, on aurait trouvé

$q_1 = 0$ soit un reste $r_1 = v$: $v = 0 \times u + v$ et à l'étape 2 il fallait considérer le quotient $\frac{u}{v}$.

2) **Suites** (U) **à éléments dans** $\mathbb{Z}[i]$.

2.1) Cas $A = 1 + i, B = 3$.
Donc $\forall n \geq 0,\ U_{n+2} = (1+i)U_{n+1} + 3U_n$ avec $U_0 = 0, U_1 = 1$.
On peut évidemment déduire de cette relation de récurrence les premiers termes de cette suite, mais si on dispose d'un logiciel on peut aller plus vite, sans erreur, en appliquant la formule de Binet :
$U_n = \frac{r_1^n - r_2^n}{r_1 - r_2}$ avec $r_1$et r_2 les racines de $x^2 - (1+i)x - 3 = 0$.
Le discriminant de cette équation caractéristique est $(1+i)^2 + 12 = 12 + 2i = (\alpha + i\beta)^2$ et les relations $\alpha^2 - \beta^2 = 12, 2\alpha\beta = 2, \alpha^2 + \beta^2 = \sqrt{4 + 144} = 2\sqrt{37}$ premettent d'en trouver les racines carrées.
Ce qui donne
$r_1 = \frac{1 + \sqrt{6 + \sqrt{37}} + (1 + \sqrt{-6 + \sqrt{37}})i}{2}$ et $r_2 = \frac{1 - \sqrt{6 + \sqrt{37}} + (1 - \sqrt{-6 + \sqrt{37}})i}{2}$.

n	U_n
0	0
1	1
2	$1 + i$
3	$3 + 2i$
4	$4 + 8i$
5	$5 + 18i$
6	$-1 + 47i$
7	$-33 + 100i$
8	$-136 + 208i$
9	$-443 + 372i$
10	$-1223 + 553i$
11	$-3105 + 446i$
12	$-7220 - 1000i$

La propriété du 4) du V (où on s'est placé dans $\mathbb{Z}$) s'applique en fait aussi au cas $\mathbb{Z}[i]$, la démonstration étant la même (à quelques adaptations près, comme le fait que là le $p\gcd$ est défini à un inversible multiplicatif près).
Mais pour pouvoir l'appliquer il faut d'abord s'assurer que $A = 1 + i$ et $B = 3$ sont effectivement premiers entre eux, ce qui est bien le cas car $1 = -(1-i)A + B$.
Donc on doit avoir $p\gcd(U_8, U_{12}) = U_{p\gcd(8,12)}$, cad un $p\gcd$ de U_8 et U_{12} doit être $U_4 = 4 + 8i$: c'est bien ce qui vient d'être prouvé au 1) par la méthode "habituelle" de recherche d'un $p\gcd$ dans $\mathbb{Z}[i]$.

On vérifie aussi qu'un $p\gcd(U_3, U_6)$ est bien $U_{p\gcd(3,6)} = U_3$ car U_3 divise bien U_6 :
$\frac{U_6}{U_3} = \frac{-1 + 47i}{3 + 2i} = 7 + 11i \in \mathbb{Z}[i]$

2.2) Cas $A = 2i, B = 2$

$\forall n \geq 0,\ U_{n+2} = 2iU_{n+1} + 2U_n$ et

Binet donne $U_n = \dfrac{(1+i)^n - (-1+i)^n}{2}$.

On en déduit que pour tout $k \geq 0$

$U_{4k} = \dfrac{((1+i)^4)^k - ((-1+i)^4)^k}{2} = 0$, puisque $(1+i)^4 = (-1+i)^4 = -4$

$U_{4k+1} = \dfrac{(-4)^k(1+i) - (-4)^k(-1+i)}{2} = (-1)^k 4^k$

$U_{4k+2} = 2i \times U_{4k+1} + 2U_{4k} = (-1)^k \times 2 \times 4^k i$

$U_{4k+3} = 2i \times (-1)^k \times 2 \times 4^k i + 2 \times (-1)^k 4^k = -(-1)^k \times 2 \times 4^k = -2U_{4k+1}$

Mais ici, $A = 2i$ et $B = 2$ ne sont pas premiers entre eux, un $p\gcd$ étant $2,$ donc la propriété 4) du V n'est pas vérifiée :

par exemple, $p\gcd(U_4, U_6) = p\gcd(0, -8i) = -8i$ qui n'est pas (à un inversible multiplicatif près) $U_{p\gcd(4,6)} = U_2 = 2i$.

Références

[1] article de recherche de N.Garnier et O.Ramaré n°39 intitulé Fibonacci Numbers and trigonometric identities à math.univ-lille1.fr

[2] article de John H.Jaroma intitulé Note on the Lucas-Lehmer Test dans le bulletin 54 de Irish Mathematical Society à www.maths.tcd.ie/pub/ims/bull54/index.php

[3] P.J Laurent Approximation et optimisation Edition Hermann ou tout autre ouvrage sur les polynômes orthogonaux

[4] Quadrature n° 101 :article Périodes de la suite de Fibonacci réduite

[5] Quadrature n° 97 : article Toujours le démon de Fibonacci

[6] alain.pichereau.pagesperso-orange.fr/ (rubrique 9).