



DM 1 · A0. L'HOMME QUI COMPTAIT JUSQU'À 39 CHIFFRES

Des poètes du sanskrit au record d'Édouard Lucas

LE PLAN DE L'ÉDIFICE

PARTIE	NIVEAUX	S'APPUIE SUR
0. Prologue et préliminaires	△	
I. La suite des poètes	△▲	les préliminaires
II. La récurrence à deux pas	▲◆	R1 et la partie I
III. La récurrence forte	▲◆	R2 ; indépendante de II
IV. Le sommet : 1876	▲◆	tout ce qui précède

Facultatif, et pour longtemps. Tout travail sincère, même partiel, est valorisé ; un travail bâclé ne l'est jamais. Ce document peut vous accompagner plusieurs années : certaines questions vous attendront en prépa ou à l'université. Horizon raisonnable : 3 à 4 semaines. Et si vous bloquez, écrivez : dire où l'on bloque et pourquoi est déjà du travail mathématique, souvent le plus formateur. Vérifiez toujours les hypothèses d'un résultat avant de l'utiliser.

△ fondations : accessible avec le cours · ▲ construction : recul et autonomie · ◆ sommet : défis, ou invitations pour plus tard

PROLOGUE

1876 : trente-neuf chiffres, à la main

LE 10 janvier 1876, devant l'Académie des sciences, un professeur de lycée français de trente-trois ans, Édouard Lucas, annonce que le nombre $2^{127} - 1$ est premier. C'est un nombre de trente-neuf chiffres, qu'il faut avoir contemplé une fois en entier :

170 141 183 460 469 231 731 687 303 715 884 105 727

Aucun ordinateur, évidemment ; des années de calculs à la main, commencés dans sa jeunesse, menés avec une arme inattendue : une suite où chaque terme naît des *deux* précédents. Son record tiendra soixante-quinze ans, et reste aujourd'hui encore le plus grand nombre premier jamais prouvé sans machine. Vous connaissez déjà Lucas sans le savoir : les tours de Hanoï de la feuille d'exercices, c'est lui. Ce devoir remonte le fil de son arme secrète.

△ **Q1.** En utilisant $2^{10} \approx 10^3$, justifier que l'écriture décimale de 2^{127} compte environ 39 chiffres.

Notations et outils. Dans tout le document, (F_n) désigne la suite de Fibonacci, définie par :

$$F_0 = 0, \quad F_1 = 1 \quad \text{et} \quad \forall n \in \mathbb{N}, F_{n+2} = F_{n+1} + F_n.$$

On pose $\varphi = \frac{1 + \sqrt{5}}{2}$ (le nombre d'or) et $\psi = \frac{1 - \sqrt{5}}{2}$. Les résultats encadrés R1, R2, R3 peuvent être cités partout.

R1 – PRINCIPE DE RÉCURRENCE DOUBLE

Soit P_n une proposition dépendant de $n \in \mathbb{N}$. Si P_0 et P_1 sont vraies, et si pour tout $n \in \mathbb{N}$, $(P_n \text{ et } P_{n+1})$ implique P_{n+2} , alors P_n est vraie pour tout $n \in \mathbb{N}$. (Admis ici ; démontré à la question Q12.)

R2 – PRINCIPE DE RÉCURRENCE FORTE

Soit P_n une proposition dépendant de $n \in \mathbb{N}$. Si P_0 est vraie, et si pour tout $n \in \mathbb{N}$, $((P_0 \text{ et } P_1 \text{ et } \dots \text{ et } P_n) \text{ implique } P_{n+1})$, alors P_n est vraie pour tout $n \in \mathbb{N}$. (Admis : l'hérédité peut s'appuyer sur TOUS les rangs précédents.)

△ Q2. Vérifier que φ et ψ sont les deux solutions de l'équation $x^2 = x + 1$, puis calculer $\varphi + \psi$, $\varphi\psi$ et $\varphi - \psi$. (ce résultat peut être admis pour la suite)

PARTIE I

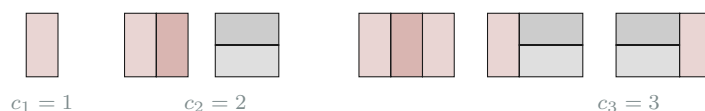
s'appuie sur les préliminaires

La suite des poètes

Un rythme poétique du sanskrit alterne syllabes courtes (durée 1) et longues (durée 2). Combien de rythmes différents ont une durée totale de n ? Le grammairien Pingala pose la question vers 200 avant notre ère ; le savant jaïn Hemachandra, vers 1150, en donne la réponse complète : chaque total s'obtient des deux précédents. Un demi-siècle plus tard, à Pise, Léonard de Pise dit Fibonacci retrouve la même suite en comptant des lapins. Et c'est Édouard Lucas, sept siècles après, qui lui donnera son nom : la suite de Fibonacci.

△ Q3. Calculer $F_2, F_3, \dots, F_{10}$.

Q4. Les dominos d'Hemachandra. Pour $n \in \mathbb{N}^*$, on note c_n le nombre de façons de paver entièrement une bande de 2 cases de haut et n cases de large avec des dominos 2×1 (posés verticalement ou horizontalement).



- △ Dénombrer, en les dessinant, les pavages d'une bande 2×4 , et vérifier $c_4 = 5$.
- ▲ En raisonnant sur la manière dont la dernière colonne est couverte (disjonction des cas), justifier que : $\forall n \in \mathbb{N}^*, c_{n+2} = c_{n+1} + c_n$.
- ▲ En déduire, par récurrence double (R1), que : $\forall n \in \mathbb{N}^*, c_n = F_{n+1}$.

LE RYTHME ET LE DOMINO

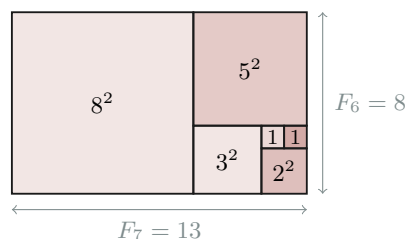
Une syllabe courte est un domino vertical, une longue en vaut deux horizontaux : les rythmes d'Hemachandra et les pavages de dominos sont le même comptage. La suite était née en musique avant de naître en mathématiques.

▲ Q5. Démontrer par récurrence simple que :

$$\forall n \in \mathbb{N}, F_0 + F_1 + \dots + F_n = F_{n+2} - 1.$$

▲ Q6. La spirale des carrés. Démontrer par récurrence simple que :

$$\forall n \in \mathbb{N}^*, \quad F_1^2 + F_2^2 + \dots + F_n^2 = F_n F_{n+1}.$$



Les carrés de côtés 1, 1, 2, 3, 5, 8 remplissent un rectangle 8×13 : c'est l'identité de la question Q6, lue pour $n = 6$.

PARTIE II

s'appuie sur R1 et la partie I

La récurrence à deux pas

La suite est définie par ses deux derniers termes : pour démontrer, il faut donc souvent supposer *deux* rangs à la fois. C'est le principe R1, que cette partie met au travail jusqu'à la formule qui a rendu la suite célèbre.

▲ Q7. Démontrer par récurrence double que : $\forall n \in \mathbb{N}, F_n < 2^n$.

Q8. La formule de Binet. On veut démontrer :

$$\forall n \in \mathbb{N}, \quad F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

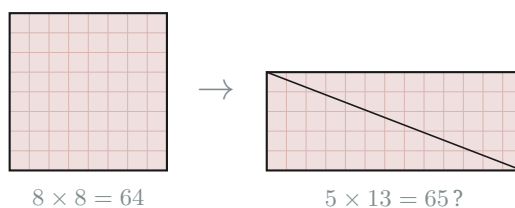
- ▲ Montrer que les suites (φ^n) et (ψ^n) vérifient toutes deux la relation $u_{n+2} = u_{n+1} + u_n$ (on utilisera Q2).
- ▲ Démontrer la formule par récurrence double. (ce résultat peut être admis pour la suite)

À QUI LA FORMULE ?

On l'appelle « formule de Binet » (1843), mais Abraham de Moivre la connaissait dès 1718, et Euler comme Daniel Bernoulli l'avaient retrouvée au fil du siècle. Les noms des théorèmes récompensent parfois le dernier arrivé : vous voilà prévenus.

Q9. L'identité de Cassini. Pour $n \in \mathbb{N}^*$, on pose $A_n = F_{n-1}F_{n+1} - F_n^2$.

- ▲ Montrer que : $\forall n \in \mathbb{N}^*, A_{n+1} = -A_n$.
- △ En déduire : $\forall n \in \mathbb{N}^*, F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.
- ▲ Un célèbre puzzle découpe un carré 8×8 en quatre pièces qui, réarrangées, semblent former un rectangle 5×13 . Comparer les aires, puis expliquer, à l'aide de l'identité de Cassini pour $n = 6$, d'où vient (et où se cache) la case fantôme.



Le puzzle de la question Q9.c : quatre pièces, deux aires. L'une des deux figures ment.

▲ **Q10. Un encadrement à deux pas.** On considère la suite (a_n) définie par :

$$a_0 = a_1 = 1 \quad \text{et} \quad \forall n \in \mathbb{N}^*, a_{n+1} = a_n + \frac{2}{n+1} a_{n-1}.$$

Démontrer par récurrence double que : $\forall n \in \mathbb{N}^*, 1 \leq a_n \leq n^2$. (Attention au démarrage : la proposition est fausse pour $n = 0$.)

◆ **Q11. Le nombre d'or au bout de la suite.**

- a) Dédurre de la formule de Binet que : $\forall n \in \mathbb{N}, \left| F_n - \frac{\varphi^n}{\sqrt{5}} \right| < \frac{1}{2}$. Que peut-on en conclure sur F_n et le réel $\frac{\varphi^n}{\sqrt{5}}$?
- b) (Ouverture vers le chapitre des suites.) En admettant que ψ^n devient arbitrairement proche de 0 quand n grandit (car $|\psi| < 1$), expliquer pourquoi le quotient $\frac{F_{n+1}}{F_n}$ s'approche de φ . Vérifier sur $\frac{F_{10}}{F_9}$.

◆ **Q12. Pourquoi R1 est légitime.** Démontrer le principe de récurrence double à partir du principe de récurrence simple. (On pourra appliquer la récurrence simple à la proposition Q_n : « P_n et P_{n+1} ».)

PARTIE III

s'appuie sur R2 ; indépendante de la partie II

La récurrence forte

Parfois, même deux pas ne suffisent pas : pour avancer, il faut tout l'édifice déjà construit sous ses pieds. C'est le principe R2, et il ouvre deux portes : l'une donne sur l'arithmétique, l'autre sur une écriture secrète des entiers.

Q13. Le premier théorème de l'arithmétique.

- a) △ On veut démontrer que tout entier $n \geq 2$ admet un diviseur premier. Expliquer pourquoi la récurrence simple est mal adaptée : quel rapport entre les diviseurs de n et ceux de $n+1$?
- b) ▲ Démontrer l'énoncé par récurrence forte (R2) : pour l'hérédité, distinguer selon que $n+1$ est premier ou s'écrit $n+1 = ab$ avec $2 \leq a \leq n$.

▲ **Q14.** Démontrer de même, par récurrence forte, que tout entier $n \geq 2$ s'écrit comme un produit de nombres premiers. (ce résultat peut être admis pour la suite) (L'unicité de cette écriture, plus délicate, vous attend en arithmétique.)

Q15. L'écriture secrète de Zeckendorf. Le théorème de Zeckendorf affirme que tout entier $N \geq 1$ s'écrit de façon unique comme somme de nombres de Fibonacci d'indices ≥ 2 , deux à deux non consécutifs. Par exemple : $30 = 21 + 8 + 1 = F_8 + F_6 + F_2$.

- a) △ Donner l'écriture de Zeckendorf de 50, puis de 100.
- b) ▲ *Existence.* Démontrer par récurrence forte que tout entier $N \geq 1$ admet une telle écriture. (Prendre le plus grand $F_m \leq N$ avec $m \geq 2$, et montrer que $N - F_m < F_{m-1}$: la suite de l'écriture ne pourra pas utiliser F_{m-1} .)
- c) ◆ *Unicité.* On admet le lemme suivant : une somme de nombres de Fibonacci d'indices ≥ 2 , deux à deux non consécutifs, dont le plus grand est F_m , est strictement inférieure à F_{m+1} . En déduire l'unicité de l'écriture de Zeckendorf.

MILES, KILOMÈTRES ET NOMBRE D'OR

Un mile vaut 1,609 km, et $\varphi \approx 1,618$: presque la même chose. Conséquence amusante : décaler d'un cran chaque indice de l'écriture de Zeckendorf convertit approximativement les miles en kilomètres. Ainsi $50 = F_9 + F_7 + F_4$ devient $F_{10} + F_8 + F_5 = 55 + 21 + 5 = 81$, et 50 miles font bien 80,5 km. Vérifiez sur votre écriture de 100.

PARTIE IV

s'appuie sur tout ce qui précède

Le sommet : 1876

Revenons à Lucas. Pour prouver que $2^{127} - 1$ est premier, pas question d'essayer les diviseurs : même à un milliard d'essais par seconde, l'Univers n'y suffirait pas. L'idée de Lucas : fabriquer une suite dont le comportement *modulo* $2^p - 1$ trahit la primalité. Sa version, polie plus tard par Derrick Lehmer (1930), tient en trois lignes ; la voici, appliquée d'abord à sa propre suite fétiche.

Q16. La suite de Lucas. On définit (L_n) par :

$$L_0 = 2, \quad L_1 = 1 \quad \text{et} \quad \forall n \in \mathbb{N}, \quad L_{n+2} = L_{n+1} + L_n.$$

- a) $\triangle$ Calculer $L_2, L_3, \dots, L_8$.
- b) $\blacktriangle$ Démontrer par récurrence double que : $\forall n \in \mathbb{N}^*, \quad L_n = F_{n-1} + F_{n+1}$.

◆ **Q17.** Démontrer que : $\forall n \in \mathbb{N}, \quad L_n = \varphi^n + \psi^n$. (Imiter la stratégie de la question Q8.)

R3 – TEST DE LUCAS-LEHMER

Soit p un nombre premier impair et $M_p = 2^p - 1$. On définit la suite (s_k) par $s_0 = 4$ et $\forall k \in \mathbb{N}, \quad s_{k+1} = s_k^2 - 2$. Alors M_p est premier si et seulement si s_{p-2} est divisible par M_p . De plus, on peut remplacer à chaque étape s_k par son reste dans la division par M_p sans changer le verdict. (*Admis : la démonstration utilise précisément les suites de Lucas.*)

Q18. Refaire Lucas, en petit puis en grand.

- a) $\triangle$ Calculer s_1, s_2 et s_3 (sans réduction).
- b) $\blacktriangle$ Dérouler le test pour $p = 7$, c'est-à-dire $M_7 = 127$, en réduisant à chaque étape modulo 127 : recopier et compléter le tableau, puis conclure sur la primalité de 127.

k	0	1	2	3	4	5
reste de s_k par 127	4	14	67	...	...	...

- c) ◆ Pour $p = 127$, le test demande 125 étapes, et chaque étape élève au carré un nombre d'environ 39 chiffres. En estimant le nombre de produits de chiffres que demande un tel carré posé à la main, donner un ordre de grandeur du nombre d'opérations élémentaires du calcul complet. Une étape par jour vous paraît-elle un rythme réaliste ?

Lucas a tenu ce rythme, avec ses variantes du test, pendant des années. Son record de 1876 ne sera dépassé qu'en 1951, à l'aube des premiers calculateurs électroniques ; aujourd'hui, le projet collaboratif GIMPS traque les nombres premiers de Mersenne avec des centaines de milliers de machines, en utilisant toujours le test de Lucas-Lehmer. Le plus grand nombre premier connu est un $2^p - 1$. La suite à deux pas des poètes du sanskrit compte toujours.

ANNEXE • COUPS DE POUCE

À consulter librement : un coup de pouce n'est pas une solution, et y recourir n'enlève rien à la valeur du travail.

Q1. $2^{127} = 2^7 \times (2^{10})^{12}$.

Q4b. La dernière colonne est couverte soit par un domino vertical, soit par les extrémités de deux dominos horizontaux superposés. Compter les pavages de chaque sorte.

Q5. Au rang $n + 1$, isoler la somme au rang n , puis utiliser la relation de récurrence de la suite.

Q6. $F_n F_{n+1} + F_{n+1}^2 = F_{n+1} (F_n + F_{n+1})$: c'est le rectangle qui grandit d'un carré.

Q7. $2^{n+1} + 2^n < 2^{n+1} + 2^{n+1}$.

Q8b. Dans l'hérédité, appliquer la question a) : $\varphi^{n+2} = \varphi^{n+1} + \varphi^n$, et de même pour ψ .

Q9a. Remplacer F_{n+2} par $F_{n+1} + F_n$, développer, puis faire réapparaître A_n en utilisant $F_{n+1} - F_n = F_{n-1}$.

Q10. Initialiser aux rangs 1 et 2 (calculer a_2 directement). Pour l'hérédité, majorer $\frac{2}{n+1}(n-1)^2$ par $2n+1$ revient à une inégalité polynomiale simple.

Q11a. $F_n - \frac{\varphi^n}{\sqrt{5}} = -\frac{\psi^n}{\sqrt{5}}$, et $|\psi| < 1$ donc $|\psi|^n \leq 1$.

Q12. Si Q_n est vraie pour tout n , alors en particulier P_n est vraie pour tout n . Vérifier que (Q_n) satisfait bien les deux hypothèses de la récurrence simple.

Q13b. Si $n + 1 = ab$ avec $2 \leq a \leq n$, alors l'hypothèse de récurrence forte s'applique à a .

Q15b. $N < F_{m+1} = F_m + F_{m-1}$, donc $N - F_m < F_{m-1}$. Appliquer l'hypothèse de récurrence forte à $N - F_m$ (s'il est non nul).

Q15c. Supposer deux écritures distinctes, comparer leurs plus grands termes à l'aide du lemme, et conclure par l'absurde.

Q16b. Initialiser aux rangs 1 et 2 ; l'hérédité est purement additive.

Q18c. Le carré d'un nombre de 39 chiffres posé à la main demande environ 39×39 produits de chiffres, plus les retenues et les additions.

ANNEXE • LE LABORATOIRE PYTHON

Pour explorer, vérifier vos calculs, et refaire en une seconde ce qui demanda dix-neuf ans.

```

1 def fibo(n):
2     a, b = 0, 1
3     for _ in range(n):
4         a, b = b, a + b
5     return a
6
7 def zeckendorf(N):
8     termes = []
9     while N > 0:
10        a, b = 1, 1
11        while b <= N:
12            a, b = b, a + b
13            termes.append(a)
14            N = N - a
15    return termes

```

```
16
17 def lucas_lehmer(p):
18     M = 2**p - 1
19     s = 4
20     for _ in range(p - 2):
21         s = (s * s - 2) % M
22     return s == 0
23
24 print(lucas_lehmer(127))    # le record de 1876, en une seconde
```

LA SUITE SUR LE COMPAGNON NUMÉRIQUE

L'idée de la démonstration du test de Lucas-Lehmer, l'histoire complète du record et le palmarès actuel de GIMPS vous attendent sur le compagnon numérique.

DM A0.1 · ANNÉE 2026-2027