L'usage des calculatrices est autorisé.

Rappelez-vous tout ce qui a été dit lors de la correction des DS précédents ! N'oubliez pas que le concepteur du sujet est votre ami, mais pas le correcteur ! Lisez donc l'énoncé attentivement, vérifiez la cohérence de vos résultats à l'aide de l'énoncé et rédigez soigneusement sans vouloir tout faire et sans étourderie.

Ce sujet est constitué de quatre problèmes. Il est hors de question de tout faire en 4 heures. Donc choisissez selon vos préférences.

Problème 1 - Arithmétique 1

On veut résoudre l'équation diophantienne $x^2 - 3 \times 2^y = 1$ d'inconnue $(x, y) \in \mathbb{N}^2$.

Question 1)

a) Précisez la parité de 2^y selon les valeurs de y.

b) Montrez que l'équation n'a qu'une seule solution (x, y) telle que x soit pair et précisez-la.

Désormais, on suppose que (x, y) est une solution telle que x est impair.

Question 2) Montrez que $y \notin \{1, 2\}$ et que x est congru à 1 ou à -1 modulo 4.

Dans la suite, et jusqu'à nouvel ordre, on suppose $x \equiv 1\ [4]$. On note donc $x = 4n + 1$ où $n \in \mathbb{N}^*$.

Question 3) Montrez que n et $2n+1$ sont premiers entre eux. Qu'en déduisez-vous à propos de leurs facteurs premiers ?

Question 4) D'après la question 2, on a nécessairement $y \geqslant 3$.

a) Donnez une expression factorisée de $3 \times 2^{y-3}$ en fonction de n. Étudiez le cas $y = 3$.

b) Dans le cas $y > 3$, en utilisant la décomposition en facteurs premiers de $3 \times 2^{y-3}$, justifiez qu'il n'y a que deux valeurs possibles pour n, puis aboutissez à une contradiction.

Question 5) Concluez : quelles sont les solutions (x, y) de l'équation telles que $x \equiv 1\ [4]$?

Dans la question suivante, on suppose désormais $x \equiv -1\ [4]$. On note donc $x = 4n - 1$ où $n \in \mathbb{N}^*$.

Question 6) Y-a-t-il des solutions respectant cette condition ? Si oui, lesquelles ?

Question 7) Concluez ce problème.

Problème 2 - Arithmétique 2

Dans tout le problème, p désigne un nombre premier impair, qu'on écrit $p = 2q + 1$.

Soit $a \in \mathbb{Z}$. On dit que a est inversible modulo p quand il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1$ $[p]$.

On dit que a est un carré modulo p quand il existe $c \in \mathbb{Z}$ tel que $a \equiv c^2$ $[p]$.

Partie 1 - Le th. de Wilson et une conséquence

Question 1)

a) Montrez l'équivalence : a est inversible modulo p si et seulement si a est premier avec p.

b) Exemple : dans cette question, $p = 347$ et $a = 514$, donnez un entier b tel que $514\,b \equiv 1$ $[347]$; la méthode utilisée doit être explicitée, un résultat seul ne sera pas pris en compte.

Question 2) On pose $E = [\![1, p-1]\!]$

a) Montrez que pour tout $a \in E$, il existe un unique $b \in E$ tel que $ab \equiv 1$ $[p]$. L'entier b est noté $\bar{a}$.

b) Justifiez que les seuls entiers $a \in E$ tel que $\bar{a} = a$ sont 1 et $p - 1$.

Question 3)

a) Montrez que $\displaystyle\prod_{k=2}^{p-2} k \equiv 1$ $[p]$: vous pourrez grouper deux par deux les entiers entre 2 et $p - 2$.

b) Déduisez-en le th. de Wilson : si p est un nombre premier impair, alors $(p-1)! \equiv -1$ $[p]$.

Question 4)

a) Montrez que $(p-1)! \equiv (-1)^q (q!)^2$ $[p]$.

b) Déduisez-en que si $p \equiv 1$ $[4]$, alors -1 est un carré modulo p.

La question suivante est consacrée à l'étude de la réciproque.

Question 5) On suppose dans cette question que -1 est un carré modulo p.

a) Rappelez le petit théorème de Fermat.

b) Montrez alors que $(-1)^q \equiv 1$ $[p]$, puis déduisez-en que $p \equiv 1$ $[4]$.

Question 6) On suppose dans cette question que $p \equiv 1$ $[4]$.

Écrivez une fonction en langage Python, de paramètre l'entier p, qui permet de calculer un entier $c \geqslant 0$ tel que $c^2 \equiv -1$ $[p]$ le plus petit possible : on rappelle que l'opérateur `%` permet de calculer des restes de division euclidienne (par exemple, `25 % 7 = 4`).

Exemple : pour $p = 53$, donnez la valeur de c.

Problème 3 - Étude de deux suites implicites

Pour $n \in \mathbb{N}^*$, on définit la fonction $f_n : x \mapsto x^3 - 3nx + n$.

Question 1) Montrez que pour tout $n \in \mathbb{N}^*$, l'équation $f_n(x) = 0$ d'inconnue $x \geqslant 0$ a deux solutions, qu'on note a_n et b_n, telles que $a_n < b_n$. Justifiez l'inégalité : $\frac{1}{3} < a_n < 1 < b_n$.

On définit ainsi deux suites a et b.

Partie 1 - Étude de la suite a

Question 1)

a) Pour $n \in \mathbb{N}$, déterminez le signe de $f_{n+1}(a_n)$ pour en déduire la position relative de a_n et a_{n+1}.

b) Justifiez que la suite a converge.

Question 2) Exprimez $3a_n - 1$ à l'aide de a_n^3 et n et montrez que la suite a converge vers $\frac{1}{3}$.

Question 3) On pose $u_n = a_n - \frac{1}{3}$. Donnez un équivalent simple de u_n.

Question 4) Dans cette question, les notations $\alpha(n)$, $\beta(n)$, etc, désignent des expressions qui tendent vers 0 quand n tend vers $+\infty$.

L'équivalence précédente peut se traduire en un développement limité de a_n à l'ordre 1 : $a_n = \frac{1}{3} + \frac{1}{81n} + \frac{1}{n}\alpha(n)$.

a) Vérifiez que $a_n = \frac{1}{3} \times \left(1 + \frac{a_n^3}{n}\right)$.

b) Justifiez alors le dév. limité de a_n à l'ordre 2 : $a_n = \frac{1}{3} + \frac{1}{81n} + \frac{1}{2187n^2} + \frac{1}{n^2}\beta(n)$.

Partie 2 - Étude de la suite b

Question 1) Montrez que la suite b diverge vers $+\infty$.

Question 2) En remarquant que $n(3b_n - 1) = b_n^3$, déduisez-en que $b_n \sim \sqrt{3n}$ quand n tend vers $+\infty$.

Question 3) On pose $v_n = b_n - \sqrt{3n}$. En calculant $b_n(b_n + \sqrt{3n})v_n$, montrez que v_n a une limite réelle ℓ (à préciser) quand n tend vers $+\infty$.

Question 4) Justifiez le développement asymptotique :

$$b_n = \sqrt{3n} + \ell - \frac{1}{24\sqrt{3n}} + o\left(\frac{1}{\sqrt{n}}\right)$$

Problème 4 - Une suite définie par récurrence

On note f la fonction $x \mapsto \dfrac{(x-1)^2}{2}$ sur $\mathbb{R}_+$.

On s'intéresse à une suite (u_n) pour laquelle $u_0 \geqslant 0$ et pour tout $n \in \mathbb{N}$, $u_{n+1} = f(u_n)$.

Note : il est recommandé de s'aider d'un dessin pour émettre des conjectures.

Question 1)

a) Étudiez le signe de la fonction $x \mapsto f(x) - x$ sur $\mathbb{R}_+$ et déterminez les points fixes de f. On notera α et β ces points fixes avec $\alpha < \beta$. Préciser leur position par rapport à 0 et 1.

b) Montrez que les intervalles $[0,1]$, $[0,\beta[$ et $]\beta,+\infty[$ sont stables par f.

On ADMET pour gagner du temps que

— α et β sont les seuls points fixes de $f \circ f$;

— pour tout $x \in [0,\alpha]$, $f \circ f(x) \geqslant x$ et pour tout $x \in [\alpha,1]$, $f \circ f(x) \leqslant x$.

Vous êtes parfaitement capables de prouver ceci grâce à quelques études de fonctions, il ne vous est pas demandé de le faire.

Question 2) Étudiez la nature de la suite (u_n) et sa limite éventuelle dans chacun des cas suivants :

a) $u_0 > \beta$

b) $u_0 \in [0,1]$.

Question 3) On suppose dans cette question que $u_0 \in\ ]1,\beta[$.

a) Montrez par l'absurde qu'il existe $N \in \mathbb{N}$ tel que $u_N \in [0,1]$.

b) Déduisez-en la nature de la suite (u_n) et sa limite éventuelle.

Problème 1

Question 1)

a) Si $y = 0$, alors $2^y = 1$ est impair ; si $y \geqslant 1$, alors $2^y = 2 \times 2^{y-1}$ donc 2^y est pair.

b) Si x est pair, alors $1 + 3 \times 2^y$ est pair donc 2^y est impair donc $y = 0$ d'après a, puis $x^2 = 4$ donc $x = 2$. Réciproquement, le couple $(x, y) = (2, 0)$ est bien solution.
Ceci prouve donc que le couple $(2, 0)$ est la seule solution telle que x soit pair.

Question 2) Si x est impair, alors $y \neq 0$ d'après la question précédente. Il est facile de vérifier qu'il n'y a aucune solution telle que $y = 1$ ou $y = 2$: $1 + 3 \times 2 = 7$ n'est pas un carré, $1 + 3 \times 2^2 = 13$ non plus. Donc $y \geqslant 3$.

De plus tout entier est congru à 0, 1, 2 ou 3 modulo 4, donc comme x est impair, il ne peut être congru à 0 ou à 2 modulo 4. Il reste donc $x \equiv 1$ [4] ou $x \equiv 3 \equiv -1$ [4].

Question 3) Soit d le pgcd de n et $2n + 1$. En particulier, d est un entier positif qui divise n et $2n + 1$ donc qui divise $(2n + 1) - 2 \times n = 1$, donc $d = 1$.

Par conséquent, n et $2n + 1$ n'ont aucun facteur premier commun.

Question 4)

a) $(4n + 1)^2 = 1 + 3 \times 2^y$ donc $16n^2 + 8n = 3 \times 2^y$ donc $n(2n + 1) = 3 \times 2^{y-3}$.
Si $y = 3$, alors on a l'égalité $n(2n + 1) = 3$ donc soit $n = 3$ et $(2n + 1) = 1$, soit $n = 1$ et $(2n + 1) = 3$. Seule la deuxième alternative est possible, donc on a $n = 1$. On a donc montré trouvé un candidat-solution : $(x, y) = (5, 3)$. Or $25 = 1 + 3 \times 8$ donc $(5, 3)$ est une solution telle que $x \equiv 1$ [4].

b) Si $y > 3$, alors il y a deux facteurs premiers dans la décomposition primaire de $3 \times 2^{y-3}$ qui sont 2 et 3. On doit donc les retrouver dans l'un ou l'autre des facteurs n ou $2n + 1$, mais comme n et $2n + 1$ sont premiers entre eux, on ne peut trouver le facteur 2 que dans l'un des deux facteurs. Or $2n+1$ est impair, donc 2^{y-3} divise n. On a donc deux alternatives encore : soit $n = 2^{y-3}$ et $2n + 1 = 3$, soit $n = 2^{y-3} \times 3$ et $2n + 1 = 1$. Les deux sont impossibles : la première donne $n = 1$ et n divisible par 2, la seconde $n = 0 = 3 \times 2^{y-3}$.

Question 5) La seule solution (x, y) de l'équation telle que $x \equiv 1$ [4] est donc $(5, 3)$ (on vérifie directement que c'est effectivement une solution).

Question 6) On fait de même : $n(2n - 1) = 3 \times 2^{y-3}$ et n, $(2n - 1)$ sont premiers entre eux et $2n - 1$ impair, puis

si $y = 3$, on a soit $n = 3$ et $(2n - 1) = 1$, soit $n = 1$ et $(2n - 1) = 3$, ce qui est de toute façon impossible.

si $y > 3$, on a soit $n = 3 \times 2^{y-3}$ et $(2n - 1) = 1$, soit $n = 2^{y-3}$ et $(2n - 1) = 3$ et seule la seconde alternative est possible donc $n = 2$ et $y = 4$.

On a donc montré que le seul candidat-solution (x, y) tel que $x \equiv -1$ [4] est le couple $(x, y) = (7, 4)$. Or $49 = 1 + 3 \times 16$ donc $(7, 4)$ est la seule solution telle que $x \equiv -1$ [4].

Question 7) L'équation proposée a donc finalement trois solutions : $(2, 0)$, $(5, 3)$ et $(7, 4)$.

Problème 2

Partie 1

Question 1)

a) Si a est inversible modulo p, alors il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1$ $[p]$, donc il existe aussi $v \in \mathbb{Z}$ tel que $ab = 1 + pv$, ou encore $ab - pv = 1$: d'après le th. de Bézout, on en déduit que a et p sont premiers entre eux.
Réciproquement, si a est premier avec p, alors toujours d'après le th. de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + pv = 1$ donc $au \equiv 1$ $[p]$, donc a est inversible modulo p.

b) On applique l'algorithme d'Euclide pour trouver deux coefficients de Bézout pour 514 et 347.
$514 = 1 \times 347 + 167$, puis $347 = 2 \times 167 + 13$, puis $167 = 12 \times 13 + 11$, puis $13 = 1 \times 11 + 2$ et enfin $11 = 5 \times 2 + 1$ et 1 divise 2, donc 514 et 347 sont premiers entre eux.
En remontant les calculs, on a $1 = 11 - 5 \times 2 = 11 - 5 \times (13 - 11) = 6 \times 11 - 5 \times 13$
puis $1 = 6 \times (167 - 12 \times 13) - 5 \times 13 = 6 \times 167 - 77 \times 13$
puis $1 = 6 \times 167 - 77 \times (347 - 2 \times 167) = 160 \times 167 - 77 \times 347$
puis $1 = 160 \times (514 - 347) - 77 \times 347 = 160 \times 514 - 237 \times 347$
L'entier $b = 160$ convient donc, car $514 \times 160 \equiv 1$ [347].

Question 2)

a) Si $a \in E$, alors $a < p$ et a non nul, donc a n'est pas divisible par p. Puisque p est premier, a et p sont premiers entre eux, donc il existe $b' \in \mathbb{Z}$ tel que $ab' \equiv 1$ $[p]$. Soit b le reste de la division euclidienne de b' par p : b' est premier avec p donc $b \neq 0$ et $b < p$, donc $b \in E$. De plus, $b \equiv b'$ $[p]$ donc $ab \equiv ab'$ $[p]$ donc $ab \equiv 1$ $[p]$.

Si b et c sont deux éléments de E tels que $ab \equiv 1$ $[p]$ et $ac \equiv 1$ $[p]$, alors $a(b-c) \equiv 0$ $[p]$ autrement dit p divise $a(b-c)$, mais a et p sont premiers entre eux donc d'après le th. de Gauss, p divise $b-c$. Mais comme $|b-c| < p$, on a comme seule solution $b - c = 0$ donc $b = c$.

b) Si $a = 1$ ou $a = p-1$, alors $a^2 \equiv 1$ $[p]$ donc dans ces deux cas, $a = \bar{a}$.

Réciproquement, si $\bar{a} = a$, alors $a^2 \equiv 1$ $[p]$ donc p divise $a^2 - 1 = (a-1)(a+1)$. Comme p est premier, il divise donc $a-1$ ou $a+1$. Sachant que $a \in E$, le premier cas donne $a = 1$, le second donne $a = p-1$.

Question 3)

a) Dans le produit $\displaystyle\prod_{k=2}^{p-2} k$, chaque facteur k est dans E et est différent de 1 et $p-1$, donc $\bar{k}$ est aussi dans E et il est différent de k. Autrement dit pour chaque facteur du produit $\displaystyle\prod_{k=2}^{p-2} k$, $\bar{k}$ est aussi dans le produit. Donc si on les regroupe par deux, le produit est un produit de nombres tous congrus à 1 modulo p, donc $\displaystyle\prod_{k=2}^{p-2} k \equiv 1$ $[p]$.

b) $(p-1)! = \displaystyle\prod_{k=2}^{p-2} k \times (p-1)$ donc $(p-1)! \equiv p-1$ $[p]$, ou encore $(p-1)! \equiv -1$ $[p]$.

Question 4)

a) On écrit différemment le produit $(p-1)!$: $(p-1)! = \displaystyle\prod_{k=1}^{p-1} k = \prod_{k=1}^{q} k \times \prod_{k=q+1}^{2q} k$.

Or pour tout $k \in [\![q+1, 2q]\!]$, $k \equiv k - p$ $[p]$ donc $k \equiv -(p-k)$ $[p]$: quand k varie de $q+1$ à $2q$, $p - k = 2q + 1 - k$ varie de 1 à q, donc les produits $\displaystyle\prod_{k=q+1}^{2q} k$ et $\displaystyle\prod_{j=1}^{q} -j$ sont congrus modulo p.

En notation développée, $\displaystyle\prod_{k=q+1}^{2q} k = (q+1)(q+2)\ldots(2q) \equiv (-q)(-q+1)\ldots(-1) \equiv (-1)^q q!$ $[p]$.

Donc $(p-1)! = \displaystyle\prod_{k=1}^{q} k \times \prod_{k=q+1}^{2q} k \equiv q! \times (-1)^q q!$ $[p]$, c'est-à-dire $(p-1)! \equiv (-1)^q (q!)^2$ $[p]$.

b) Si $p \equiv 1$ $[4]$, alors q est pair donc $(p-1)! \equiv (q!)^2$ $[p]$, or on sait que $(p-1)! \equiv -1$ $[p]$, donc $-1 \equiv (q!)^2$ $[p]$. En posant $c = (q!)$, on a donc $c^2 \equiv -1$ $[p]$.

Question 5)

a) Si a est premier avec p et p est un nombre premier, alors $a^{p-1} \equiv 1$ $[p]$.

b) Soit c une racine carrée modulo p de -1. Il a déjà été signalé que c est non divisible par p, ce qui revient à dire c premier avec p. Donc $c^{p-1} \equiv 1$ $[p]$. Or $c^2 \equiv -1$ $[p]$, donc $(c^2)^q \equiv (-1)^q$ $[p]$, ce qui revient à $c^{2q} \equiv (-1)^q$ $[p]$, c'est-à-dire $c^{p-1} \equiv (-1)^q$ $[p]$. Finalement, on a $(-1)^q \equiv 1$ $[p]$.

Comme $(-1)^q$ vaut soit 1, soit -1, la seule solution est que $(-1)^q = 1$ donc que q soit pair, donc $p \equiv 1$ $[4]$.

Question 6)

```
def racine(p):
  q = (p - 1) // 2
  for c in range(1,q+1):
    if (c * c + 1) % p == 0:
      return c
```

On applique l'algorithme précédent pour $p = 53$, on trouve $c = 23$.

Problème 3

Question 1) La fonction f_n est dérivable sur $[0, +\infty[$ (polynôme) et pour tout $x \geqslant 0$, $f_n'(x) = 3x^2 - 3n$. Sur $[0, +\infty[$, la dérivée s'annule en $\sqrt{n}$, elle est strictement négative avant et strictement positive après.

$f_n(0) = n > 0$ et $f_n(\sqrt{n}) = n(1-2\sqrt{n}) < 0$, donc sur $\left[0, \sqrt{n}\right]$, f_n est continue et strictement décroissante et a des valeurs aux extrémités de l'intervalle de signes contraires, donc d'après le th. de la valeur intermédiaire, l'équation $f_n(x) = 0$ a une unique solution a_n dans $\left[0, \sqrt{n}\right]$.

De même sur $\left[\sqrt{n}, +\infty\right[$, f_n est continue et strictement croissante et passe d'une valeur strictement négative à la limite $+\infty$, donc le même th. permet d'affirmer l'existence de b_n.

Puis $f_n\left(\dfrac{1}{3}\right) = \dfrac{1}{27} > 0$, $f_n(1) = 1 - 2n < 0$ et $1 \in \left[0, \sqrt{n}\right]$, on a aussi $0 \leqslant \dfrac{1}{3} < a_n < 1$. De plus, $1 \leqslant \sqrt{n} < b_n$.

Partie 1

Question 1)

a) $f_{n+1}(a_n) = a_n^3 - 3(n+1)a_n + (n+1)$, or $f_n(a_n) = 0$, donc $f_{n+1}(a_n) = 1 - 3a_n < 0$.
On a donc $f_{n+1}(a_n) < 0 = f_{n+1}(a_{n+1})$ et a_n, a_{n+1} sont dans $[0, 1]$ et f_{n+1} est strictement décroissante sur $[0, 1]$, donc $a_{n+1} < a_n$.

b) D'après ce qui précède, la suite a est décroissante et minorée par $\dfrac{1}{3}$, donc elle converge d'après le th. de la limite monotone.

Question 2) $3a_n - 1 = \dfrac{a_n^3}{n}$: comme a converge vers un réel k, alors (a_n^3) converge vers k^3, donc d'après les th. d'opérations sur les limites, $(3a_n - 1)$ converge vers 0, autrement dit, a_n converge vers $\dfrac{1}{3}$.

Question 3) $u_n = \dfrac{a_n^3}{3n} \underset{n\to+\infty}{\sim} \dfrac{\frac{1}{3^3}}{3n} \underset{n\to+\infty}{\sim} \dfrac{1}{81n}$.

Question 4)

a) Simple calcul.

b) a_n a un d.l. à l'ordre 1, donc a_n^3 aussi : $a_n^2 = \dfrac{1}{27} + \dfrac{1}{243n} + \dfrac{1}{n}\gamma(n)$
en divisant par n, on a un d.l. à l'ordre 2 : $\dfrac{a_n^3}{n} = \dfrac{1}{27n} + \dfrac{1}{243n^2} + \dfrac{1}{n^2}\delta(n)$ donc $a_n = \dfrac{1}{3} \times \left(1 + \dfrac{1}{27n} + \dfrac{1}{243n^2} + \dfrac{1}{n^2}\delta(n)\right)$
$a_n = \dfrac{1}{3} + \dfrac{1}{81n} + \dfrac{1}{729n^2} + \dfrac{1}{n^2}\beta(n)$

Partie 2

Question 1) On a montré que $b_n \geqslant \sqrt{n}$, donc le th. d'encadrement permet de conclure : b diverge vers $+\infty$.

Question 2) b diverge vers $+\infty$, donc $3b_n - 1 \sim 3b_n$, donc de l'égalité vérifiée, on tire : $3nb_n \sim b_n^3$, donc $3n \sim b_n^2$, donc $b_n \sim \sqrt{3n}$.

Question 3) $b_n(b_n + \sqrt{3n})v_n = b_n^3 - 3nb_n = n$.

Or grâce au cas favorable d'addition des équivalents, $b_n + \sqrt{3n} \sim 2\sqrt{3n}$.

Donc $v_n \sim \dfrac{n}{b_n(b_n + \sqrt{3n})} \sim \dfrac{n}{\sqrt{3n} \times 2\sqrt{3n}} \sim \dfrac{n}{6n} \sim \dfrac{1}{6}$.

Donc v_n tend vers $\dfrac{1}{6}$.

Question 4) $v_n = \dfrac{n}{b_n(b_n + \sqrt{3n})}$ donc $v_n - \dfrac{1}{6} = \dfrac{6n - b_n(b_n + \sqrt{3n})}{6b_n(b_n + \sqrt{3n})}$.

Puis on réécrit le numérateur en faisant apparaître et compensant :

$6n - b_n(b_n + \sqrt{3n}) = \sqrt{3n} \times 2\sqrt{3n} - b_n(b_n + \sqrt{3n}) = (\sqrt{3n} - b_n) \times 2\sqrt{3n} + 2b_n\sqrt{3n} - b_n(b_n + \sqrt{3n})$

$= -v_n \times 2\sqrt{3n} + b_n(\sqrt{3n} - b_n) = -v_n \times (2\sqrt{3n} + b_n)$

On applique alors encore le même résultat :

pour le numérateur, on a : $6n - b_n(b_n + \sqrt{3n}) \sim -\dfrac{1}{6} \times 3\sqrt{3n}$

pour le dénominateur : $6b_n(b_n + \sqrt{3n}) \sim 6 \times \sqrt{3n} \times 2\sqrt{3n}$

donc finalement, on a $v_n - \dfrac{1}{6} \sim \dfrac{-\frac{1}{6} \times 3\sqrt{3n}}{6 \times \sqrt{3n} \times 2\sqrt{3n}} \sim \dfrac{-1}{24\sqrt{3n}}$,

ce qui justifie le développement asymptotique attendu.

Problème 4

Question 1)

a) $f(x) - x = \dfrac{1}{2}(x^2 - 4x + 1)$: ce polynôme du second degré a deux racines $\alpha = 2 - \sqrt{3}$ et $\beta = 2 + \sqrt{3}$, il est positif sur $[0, \alpha]$ et sur $[\beta, +\infty[$, négatif sur $[\alpha, \beta]$. De plus, $0 < \alpha < 1 < \beta$.

b) La fonction f est décroissante et continue sur $[0,1]$ donc $f([0,1]) = [f(1), f(0)] = [0, 1/2] \subset [0,1]$, donc $[0,1]$ est stable par f.

La fonction f est continue et strictement croissante sur $]\beta, +\infty[$, donc $f(]\beta, +\infty[) =]f(\beta), \lim_{+\infty} f[=]\beta, +\infty[$, donc $]\beta, +\infty[$ est stable par f.

La fonction f est continue et strictement croissante sur $[1, \beta[$, donc $f([1,\beta[) = [f(1), f(\beta)[= [0, \beta[$, donc $f([0,\beta[) = f([0,1] \cup [1,\beta[) = f([0,1]) \cup f([1,\beta[) = [0,\beta[$, donc $[0,\beta[$ est stable par f.

Question 2)

a) Si $u_0 > \beta$, alors comme l'intervalle $]\beta, +\infty[$ est stable par f, on en déduit que pour tout $n \in \mathbb{N}$, $u_n \in]\beta, +\infty[$. Or sur cet intervalle, on a montré que la fonction $x \mapsto f(x) - x$ est à valeurs strictement positives, donc en particulier, pour tout $n \in \mathbb{N}$, $f(u_n) - u_n > 0$, c'est-à-dire $u_{n+1} > u_n$.

La suite u est donc strictement croissante et donc d'après le th. de la limite monotone, elle diverge vers $+\infty$ ou converge vers un réel. Mais comme f est continue sur $\mathbb{R}$, ce réel ne peut être qu'une borne de l'intervalle $]\beta, +\infty[$ ou un point fixe (qui n'existe pas dans cet intervalle ouvert). Si la suite converge, elle converge vers β en étant strictement croissante et au-dessus de β : absurde.

Donc la suite u diverge vers $+\infty$.

b) Si $u_0 \in [0,1]$, alors par stabilité du segment $[0,1]$, on en déduit que pour tout $n \in \mathbb{N}$, $u_n \in [0,1]$. Or f est décroissante sur $[0,1]$, donc d'après le cours, les deux suites (u_{2n}) et (u_{2n+1}) sont monotones de sens contraire. Et comme elles sont bornées, elles convergent donc d'après le th. de la limite monotone. Encore une fois, comme $f \circ f$ est continue, leurs limites ne peuvent être que les bornes de $[0,1]$ ou un point fixe de $f \circ f$ dans $[0,1]$: on a donc trois possibilités qui sont 0, 1 et α.

Si par exemple (u_{2n}) converge vers 0, alors $(u_{2n+1}) = (f(u_{2n}))$ converge vers $f(0) = 1/2$ par continuité de f, ce qui contredit les trois possibilités ci-dessus.

De même, si (u_{2n}) converge vers 1, alors $(u_{2n+1}) = (f(u_{2n}))$ converge vers $f(1) = 0$ par continuité de f, mais alors $(u_{2n+2}) = (f(u_{2n+1}))$ converge vers $f(0) = 1/2$, ce qui contredit encore les trois possibilités ci-dessus.

Donc (u_{2n}) converge vers α et de même, (u_{2n+1}) converge aussi vers α. D'après un th. du cours (quasi-réciproque du th. des suites extraites), la suite u converge vers α.

Question 3)

a) Si $u_0 \in]1, \beta[$, alors $u_0 \in [0, \beta[$, intervalle stable par f, donc pour tout $n \in \mathbb{N}$, $u_n \in [0, \beta[$.

On suppose qu'il n'existe pas de rang N tel que $u_N \in [0,1]$. Alors pour tout $n \in \mathbb{N}$, $u_n \in]1, \beta[$. Or la fonction $x \mapsto f(x) - x$ est à valeurs strictement négatives sur $]1, \beta[$, donc en particulier, pour tout $n \in \mathbb{N}$, $f(u_n) - u_n < 0$, c'est-à-dire $u_{n+1} < u_n$. La suite u est donc décroissante et minorée par 1 donc elle converge. Comme f est continue, sa limite est une borne ou un point fixe de f dans $]1, \beta[$, donc sa limite est 1 ou β. Mais comme la suite est strictement décroissante, c'est forcément 1.

Alors $(u_{n+1}) = (f(u_n))$ converge vers $f(1) = 0$ par continuité de f, ce qui est contradictoire avec le th. des suites extraites.

Donc il existe $N \in \mathbb{N}$ tel que $u_N \in [0,1]$.

b) Dès lors, à partir du rang N, la suite u est à termes dans $[0,1]$ par stabilité de l'intervalle par f, donc on est ramené àla question 2.b. à partir du rang N : la suite u converge vers α.