DS7 - Arithmétique

I A) $51x - 26y = 1$

1) 26 se décompose en facteurs premiers : $26 = 2 \times 13$
et on a $51 = 3 \times 17$
il apparaît donc que $26 \wedge 51 = 1$
et donc d'après le th de Bezout, il existe $(u,v) \in \mathbb{Z}^2$ tels que

$$51u + 26v = 1$$

On a donc des solutions pour $51x - 26y = 1$ (avec $u = x$ et $y = -v$)

2a) $(-1,-2)$ est solution évidente de cette équation car $51 \times (-1) - 26(-2) = 52 - 51 = 1$

2b) $\left.\begin{array}{l} 51x - 26y = 1 \\ 51(-1) - 26(-2) = 1 \end{array}\right\}$ par différence $\Longrightarrow$ $51(x+1) - 26(y+2) = 0$

$\Rightarrow$ $51(x+1) = 26(y+2)$ (*)

$\Rightarrow$ $51 \mid 26(y+2)$

Or $51 \wedge 26 = 1$ donc d'après le th de Gauss $51 \mid y+2$

$\Rightarrow$ il existe $k \in \mathbb{Z}$ tel que $y + 2 = 51k$

En reprenant (*) on a alors $(x+1) = 26k$.

Finalement $x = 26k - 1$ et $y = 51k - 2$; $k \in \mathbb{Z}$

Réciproquement si x, y définis comme précédemment, on a

$$\begin{aligned} 51x - 26y &= 51(26k-1) - 26(51k-2) \\ &= 51(-1) - 26(-2) \\ &= 1 \end{aligned}$$

Ainsi les solutions de l'équation sont $\mathcal{S} = \{(26k-1 ; 51k-2) ; k \in \mathbb{Z}\}$

II B) 1) à N correspond la valeur $x = 13$

et $51x + 2 = 51 \times 13 + 2 \equiv -13 + 2 \equiv -11 \equiv 15 \ (26)$
donc $f(13) = 15$ c'est-à-dire que la lettre N est codée par P.

② On cherche $0 \leq a \leq 25$ et $51a \equiv 1 \ (26)$

$51a \equiv 1 \ (26) \iff 51a = 1 + 26q \ ; \ q \in \mathbb{Z}$

$\iff 51a - 26q = 1$

$\iff (a, q)$ solution de l'équation de la partie A

$\iff \exists k \in \mathbb{Z}$ tel que $a = 26k - 1$ et $q = 51k - 2$

On veut de plus $0 \leq a \leq 25$

$\iff 0 \leq 26k - 1 \leq 25 \iff 1 \leq 26k \leq 26$

$\iff k = 1$ car $k \in \mathbb{Z}$

Ainsi $a = 26 - 1 = 25$ est l'unique solution à $0 \leq a \leq 25$ et $51a \equiv 1 \ (26)$

③ l'entier x est codé par y

$\Rightarrow 51x + 2 \equiv y \ (26)$

$\Rightarrow 51x \equiv y - 2 \ (26)$

$\Rightarrow \underbrace{25 \cdot 51}_{\equiv 1} x \equiv 25(y-2) \ (26)$

$\Rightarrow x \equiv 25y - 50 \ (26) \Rightarrow x \equiv 25y + 2 \ (26)$

qui est bien le résultat attendu car $a = 25$

④ Une lettre est codée par N (valeur 13)

Nous cherchons donc x tel que $f(x) = 13$ (y vaut 15)

d'après la question ③ x satisfait $x \equiv 25 \times y + 2 \ (26)$

$\equiv 25 \cdot 13 + 2 \ (26)$

$\equiv -13 + 2 \ (26)$

$\equiv 15 \ (26)$

La lettre de départ est donc la lettre P (qui une fois encodée donne N)

⑤ On code la valeur x une fois par f :

On a $y = f(x) \equiv 51x + 2 \equiv -x + 2 \ (26)$

On recode cette valeur une 2ème fois et on a $y' = f(y) \equiv 51(-x+2) + 2 \ (26)$

$\equiv -(-x+2) + 2 \ (26)$

$\equiv x \ (26)$

Ainsi quand on applique 2 fois la fonction f à une valeur x, on retrouve la valeur x. Donc en appliquant 100 fois la fonction f, cela revient à appliquer 50 fois "2 fois la fct f" et donc on retrouve x. Ça ne change pas la lettre !

III A 1) $p_1, p_2, \dots p_n$ sont premiers donc tous supérieurs à 2 (ou égal)

donc $p_1 p_2 \dots p_n \geq 2$ et ainsi $E \geq 3 > 2$.

On a alors $E - p_1 \times p_2 \times \dots \times p_n = 1$

qui est une équation de Bezout qui montre clairement $E \wedge p_i = 1 \quad \forall i = 1 \dots n$

2) Par l'absurde comme E admet un diviseur premier il existe $i_0 \in \{1, \dots n\}$ tel que $p_{i_0} \mid E$ mais ceci est une contradiction avec le fait que $p_{i_0} \wedge E = 1$

Donc il ne peut pas y avoir un nombre fini de nombres premiers.

B 1a) Voir tableau

1b) 2 premier $\Rightarrow H_2 = 3$ premier
3 premier $\Rightarrow H_3 = 7$ premier
5 premier $\Rightarrow H_5 = 31$ premier
7 premier $\Rightarrow H_7 = 127$ premier (127 premier car il n'est divisible ni par 2, 3, 5, 7, ni par 11)

On peut donc conjecturer k premier alors H_k premier.

2a) Par la somme des suites géométriques, si $q \neq 1$ on a $1 + q + \dots q^{n-1} = \frac{1-q^n}{1-q}$

Donc si $p \geq 1$ $\quad 1 + 2^p + (2^p)^2 + \dots + (2^p)^{q-1} = \frac{1-(2^p)^q}{1-2^p} = \frac{(2^p)^q - 1}{2^p - 1}$.

b) On déduit de ce qui précède que

$$\circledast \quad 2^{pq} - 1 = \underbrace{\left(1 + 2^p + \dots + (2^p)^{q-1}\right)}_{\in \mathbb{N}} (2^p - 1) \quad \text{et en particulier } 2^p - 1 \text{ divise } 2^{pq} - 1$$

c) Si k n'est pas premier alors $k = p \times q$ avec $p \geq 2$; $q \geq 2$

et d'après 2b) $2^p - 1 \mid 2^{pq} - 1$ c'est-à-dire que

$2^p - 1 \mid H_k$ avec $2^p - 1 \geq 3$ et $2^p - 1 \neq H_k$ donc H_k non premier.

Remarque : avec l'égalité $\circledast$ on voit directement que H_k est composé

(3a) $H_{11} = 2047$

$\sqrt{H_{11}} \approx 45$

Nous allons ~~tester~~ la divisibilité de H_{11} par les nombres premiers p inférieurs à 45

On remarque que $2047 = 23 \times 89$ donc H_{11} n'est pas premier.

(3b) La conjecture de (15) est donc fausse.

On n'a pas # la premier $\Rightarrow H_k$ premier

Partie C :

(1) $u_0 = 4$; $u_{n+1} = u_n^2 - 2$.

on a $u_1 = 16 - 2 = 14$.

$u_2 = 14^2 - 2 = 194$

$u_3 = 194^2 - 2$

et $H_5 = 31$

Nous avons $H_3 = 194^2 - 2 \equiv 8^2 - 2 \quad (31)$

$\equiv 62 \quad (31)$

$\equiv 0 \quad (31)$

Ainsi $u_3 \equiv 0\ (H_5)$ donc d'après le th de Lucas-Lehmer H_5 est premier.