TD Cryptographie

ENSSAT

Exercice 1

Exercice 2

1. Si l'équation (1) admet au moins une solution, il existe $(x, y) \in \mathbb{Z}^2$ tels que

$$ax + by = c$$

Notons $d = \text{PGCD}(a, b)$. d divise a et b, donc divise $ax + by$, c'est-à-dire que d divise c.

2. Réciproquement, si c divise d, et quitte à diviser par d, on obtient l'équation

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

où $a' = \frac{a}{d}, b' = \frac{b}{d}$ et $c' = \frac{c}{d}$ sont des entiers. Par définition du PGCD :

$$\text{PGCD}(a, b) = \text{PGCD}\left(da', db'\right) = d\text{PGCD}(a', b')$$

et donc $\text{PGCD}(a', b') = 1$. Ainsi, on peut supposer que a et b sont premiers entre eux, quitte à diviser l'équation par le PGCD de a et b.
On peut alors obtenir un couple (u, v) vérifiant $au + bv = 1$ (par l'algorithme d'Eculide), et alors

$$a(cu) + b(cv) = c$$

et le coupe (cu, cv) est solution de (1).
Connaissant une solution particulière de (1), qu'on note (x_0, y_0), on en déduit, par soustraction, que (x, y) vérifie (1) si et seulement si

$$a(x - x_0) = b(y_0 - y)$$

Puisqu'on a supposé a et b premiers entre eux, cela indique que a divise $y_0 - y$ (théorème de Gauss) et donc que $y = y_0 - ka$ avec $k \in \mathbb{Z}$. En injectant dans l'équation précédente, on a alors

$$a(x - x_0) = bka \Leftrightarrow x = x_0 + kb$$

Ainsi l'ensemble des solutions est de (1) est

$$\mathscr{S} = \left\{(x_0 - ka, y_0 + kb), \quad k \in \mathbb{Z}\right\}$$

3. Remarquons que $\text{PGCD}(15, 6) = 3$. Ainsi

$$15x - 6y = 9 \Leftrightarrow 5x - 2y = 3$$

5 et 2 sont premiers entre eux. On applique l'algorithme d'Euclide étendue pour une obtenir une solution, ou alors on constate que $(1, 1)$ est une solution particulière évidente. Alors, par soustraction

$$5x - 2y = 3 \Leftrightarrow 5(x - 1) - 2(y - 1) = 0 \Leftrightarrow 5(x - 1) = 2(y - 1)$$

5 et 2 sont premiers entre eux. D'après le théorème de Gauss, on en déduit que 5 divise $y - 1$ et donc qu'il existe $k \in \mathbb{Z}$ tel que $y - 1 = 5k$, c'est-à-dire $y = 1 + 5k$. En injectant dans l'équation précédente, on obtient

$$5(x - 1) = 2 \times 5k \Leftrightarrow x = 1 + 2k$$

Ainsi, l'ensemble des solutions est

$$\mathscr{S} = \{(1 + 2k, 1 + 5k), \quad k \in \mathbb{Z}\}$$

Exercice 3

Remarquons que, en majorant grossièrement :

$$4444^{4444} < 10000^{4444} = 10^{17776}$$

Donc 4444^{4444} possède moins de 17776 chiffres. Donc

$$\begin{aligned} f\left(4444^{4444}\right) &\leqslant f(999\cdots999) = 17776 \times 9 < 160000 \\ \text{puis } f \circ f\left(4444^{4444}\right) &\leqslant f(999999) = 54 \\ \text{et } f \circ f \circ f\left(4444^{4444}\right) &< f(59) = 5+9 = 14 \end{aligned}$$

On doit donc trouver un moyen de trouver l'entier entre 1 et 13 qui est égal $f \circ f \circ f(\mathrm{N})$. Utilisons une propriété usuelle de la division par 9 : un nombre N est congrus à sa somme de chiffre modulo 9. Ainsi

$$f(\mathrm{N}) \equiv f \circ f(\mathrm{N}) \equiv f \circ f \circ f(\mathrm{N}) \equiv \mathrm{N} \mod 9$$

Or $4444 \equiv 7 \mod 9$, donc $4444^3 \equiv 1 \mod 9$. Ainsi

$$4444^{4444} = 4444^{1481\times3} \times 4444 \equiv 1^{1481} \times 7 = 7 \mod 9$$

Ainsi $f \circ f \circ f(\mathrm{N}) \equiv 7 \mod 9$.

Le seul nombre entier congru à 7 modulo 9 dans l'intervalle $[\![1;13]\!]$ étant 7, on en déduit donc que

$$f \circ f \circ f(\mathrm{N}) = 7$$

Exercice 4

Généralités

1. En utilisant les notation du cours, on a l'invariant de boucle :

$$\begin{cases} u_0 a + v_0 b &= r_0 \\ u_1 a + v_1 b &= r_1 \\ r_1 &\geqslant 0 \end{cases}$$

2.

Analyse de l'algorithme d'Euclide

1. (a) D'après l'algorithme d'Euclide, on a, pour $1 \leqslant i \leqslant \mathrm{N}_1$: :

$$r_{i-2} = q_i r_{i-1} + r_i$$

(b)

2. (a) Pour $k = N-1$, alors $\varphi^{N-1-k} = 1$ et on a, par construction, $r_{N-1} \geqslant 1$ (et $r_N = 0$ premier reste nul). Par hérédité, supposons que pour tout $n \leqslant k \leqslant N-1$, $r_k \geqslant \varphi^{N-1-k}$. Montrons que le résultat est vrai pour r_{k-1} :

$$\begin{aligned} r_{k-1} &= q_{k+1} r_k + r_{k+1} \\ &\geqslant q_{k+1} \varphi^{N-1-k} + \varphi^{N-1-(k+1)} \\ &\geqslant \varphi^{N-k-2} \left(\varphi + 1\right) \\ &\geqslant \varphi^{N-k-2)} \varphi^2 \text{ car } \varphi^2 = \varphi + 1 \\ &\geqslant \varphi^{N-k} = \varphi^{(N-1)-(k-1)} \end{aligned}$$

Par récurrence descendante, on a donc bien le résultat.

(b) Puisque $r_0 = b$, on a alors :

$$\begin{aligned} r_0 = b \Rightarrow & \qquad\qquad b \geqslant \varphi^{N_1} \\ \Rightarrow & \ln(b) \geqslant (N-1)\ln(\varphi) \\ \Rightarrow & N \leqslant \log_\varphi(b) + 1 \text{ où } \log_\varphi(b) = \frac{\ln(b)}{\ln(\varphi)} \text{ (car } \ln(\varphi) > 0) \end{aligned}$$

(c) L'algorithme est assez efficace. Par exemple, pour N = 100000, on a $N \leqslant 30$.

(d) Pour Euclide étendu, c'est aussi efficace, parce que le nombre N ne dépend que des divisions euclidiennes successives : on obtient, en plus, u et v vérifiant $au + bv = 1$.