159	Algorithme d'Euclide dans $\mathbb{Z}$. Calcul de Pgcd et de coefficients de Bézout. Applications.	Chiffrement affine	Terracher TS

(Wikipedia) Jules César utilisait un chiffrement affine avec f(x)=x+3, appelé depuis "Chiffre de César". Il était assez facile à déchiffrer, par exemple en étudiant la fréquence des lettres utilisées.

On assimile les lettres de l'alphabet A, B, ...Z aux nombres 0,1,...,25, et on code ces nombres par la fonction de "hachage":
$f : \begin{cases} \{0,1,...,25\} \to \{0,1,...,25\} \\ x \mapsto f(x) \equiv 17x+22\,[26] \end{cases}$.
f(x) est le reste de la division Euclidienne de (17x+22) par 26
Jules César utilisait un chiffrement affine f(x)=1x+3.

I. Outils:

- Congruences
- Théorème de Bézout
- Algorithme d'Euclide étendu.

II. Un exemple de chiffrement.

Pour voir fonctionner ce chiffrement, nous allons coder le mot "huit":
Les lettres H, U, I, T correspondent aux nombres 7, 20, 8 et 19.

Or $17\times 7+22=141$, et $\begin{array}{r|l} 141 & 26 \\ 11 & 2 \end{array}$. Donc $f(7)=11$.

De même, $f(20)=24$; $f(8)=2$; et $f(19)=7$.

Or les lettres correspondant respectivement à 11; 24; 2; et 7 sont: L; Y; C et H.
Donc le mot chiffré est: "LYCH".

III. Expression d'une fonction de déchiffrage.

A. Déterminons un entier *u* tel que $17u \equiv 1\,[26]$.

***L'idée**: on a $y \equiv 17x+22\,[26]$, et on cherche u t.q. $17u \equiv 1\,[26]$, pour pouvoir remplacer $y \equiv 17x+22\,[26]$ par $17u.y \equiv 17x+22\,[26]$, et pouvoir diviser par 17 afin de récupérer x au lieu de $17x$.*

On a $17u \equiv 1\,[26]$ équivaut à: Il existe $v \in \mathbb{Z}$ tel que:
$17u-26v=1$. (E_1)
Comme 17 et 26 sont premiers entre eux, le théorème de Bézout assure que des solutions existent.
On cherche une solution particulière en "remontant" l'algorithme d'Euclide:

Algo. d'Euclide (26;17):
$26=17\times 1+9$
$17=9\times 1+8$
$9=8\times 1+1$

Elimination des restes:
$1=9-\underline{8}\times 1$
$1=9-(\underline{17-9})$
$1=\underline{9}\times 2-17$
$1=(\underline{26-17})\times 2-17$
$1=26\times 2-17\times 3$

Finalement une solution particulière de (E_1) est:
$17\times(-3)-26\times(-2)=1$, i.e. $(u;v)=(-3;-2)$.
La solution générale est de la forme:
$u=-3+26k,\quad v=-2+17k,\quad (k\in\mathbb{Z})$.
Un seule valeur vérifie $0\le u\le 25$, c'est ***u*=23**.
Donc $17\times 23\equiv 1\,[26]$

B. Déterminons une fonction de déchiffrage.

Il s'agit de déduire de ce qui précède l'expression d'une fonction de déchiffrage g, de $\{0;1;...25\}$ dans lui-même, telle que:
$y = f(x)[26] \Leftrightarrow x = g(y)[26]$.

On a $17 \times 23 \equiv 1[26]$

Il vient:
$y \equiv 17x + 22[26]$ (en multipliant par $u = 23$:)
$\Leftrightarrow 23y \equiv 23 \times 17x + 506[26]$
$\Leftrightarrow 23y - 506 \equiv x[26]$ Or $-506 = -19 \times 26 - 12$
$\Leftrightarrow 23y + 14 \equiv x[26]$ i.e. $-506 = -20 \times 26 + 14$
Finalement, la fonction de déchiffrage est:
$g : y \mapsto 23y + 14[26]$.

C. Exemple de déchiffrement.

Déchiffrons par exemple le mot "QWXA".
Le mot "QWXA" correspond à la séquence 16; 22; 23; 0.
$23 \times 16 + 14 = 382$ or $382 = 26 \times 14 + 18$;
Ainsi: $g(16) = 18$; $g(22) = 0$; $g(23) = 23$; $g(0) = 14$;
La séquence "déchiffrée" est donc "SAXO".