L3 Alg. effective. Corrigé de l'échauffement du 15 octobre 2019

Ex1 $n = 315 = 5 \times 63 = 5 \times 7 \times 9 \rightsquigarrow \varphi(n) = \underbrace{\varphi(5)}_{4} \times \underbrace{\varphi(7)}_{6} \times \underbrace{\varphi(9)}_{9-3} = 4 \times 6^2 = 144$

dans $\mathbb{Z}/315\mathbb{Z}$ 4 est inversible car $4 \wedge 315 = 1$ et alors $4^{\varphi(315)} = 1$, $4^{\varphi(315)+1} = 4$

5 n'est pas inversible dans $\mathbb{Z}/315\mathbb{Z}$. Avec le lemme chinois $\phi : \mathbb{Z}/315\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ isomorphisme d'anneaux

$x \longmapsto (x \bmod 5, x \bmod 7, x \bmod 9)$

$5^{145} \mapsto (\bar{5}^{145}, \bar{5}^{145}, \bar{5}^{145})$

On a $5 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$ donc $5^{145} = 5^{145} \times 0 = 0 = 5$ dans $\mathbb{Z}/5\mathbb{Z}$

Dans $\mathbb{Z}/7\mathbb{Z}$ 5 est inversible donc $5^6 = 1$ puis $5^{144} = (5^6)^{144/6} = 1$ puis $5^{145} = 5^{144} \times 5 = 5$

De même dans $\mathbb{Z}/9\mathbb{Z}$ 5 est inversible donc $5^{\underbrace{\varphi(9)}_{6}} = 1$ puis $5^{144} = 1$ enfin $5^{145} = 5$

On obtient $\phi(5^{145} - 5) = (0,0,0) \in \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/9$ et comme ϕ est bijective, $5^{145} - 5 = 0$ dans $\mathbb{Z}/315\mathbb{Z}$

On a vu $\phi(5^{144}) = (0,1,1)$ de $\mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/9 \simeq \mathbb{Z}/5 \times \mathbb{Z}/63$ donc $5^{144} = 5k$ pour un $k \in \mathbb{Z}$ avec $5k = 1 \bmod 63$

On cherche k inverse de 5 dans $\mathbb{Z}/63\mathbb{Z}$. Algorithme d'Euclide : $63 = 12 \times 5 + 3$ $\rightsquigarrow 1 = 3 \times 2 - 5 = (63 - 12 \times 5) \times 2 - 5$

$5 = 3 + 2 = 3 \times 2 - 1$ $= 63 \times 2 - 25 \times 5$

$\rightsquigarrow k = -25$ convient puis $5^{144} = 5 \times (-25) = -125$ dans $\mathbb{Z}/5\mathbb{Z}$ et dans $\mathbb{Z}/63\mathbb{Z}$ donc dans $\mathbb{Z}/315\mathbb{Z}$

Ex2 $5 \wedge 144 = 1$ donc $\exists x \in \mathbb{Z}$, $5x = 1 \bmod 144$

$144 = 2 \times 72 = 2 \times 8 \times 9 = 16 \times 9$ $\rightsquigarrow \mathbb{Z}/144\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. Dans $\mathbb{Z}/16\mathbb{Z}$ $5 \times 3 = 15 = -1$ donc $x = -3 \bmod 16$

dans $\mathbb{Z}/9\mathbb{Z}$ $5 \times 2 = 1$ donc $x = 2 \bmod 9$

On écrit $x = -3 + 16k$ et alors $x - 2 = -5 + 16k = 0 \bmod 9$ donc $16k = 5 \bmod 9$

$= 9k + 7k \equiv 7k \bmod 9 = -2k \bmod 9$

On observe $k = 2$ convient. Alternative : $(-2)(-4) = -1 \bmod 9$ donc $(-2)(-4)(-5) = 5 \bmod 9$. $k = 20$ convient

Finalement $x = -3 + 16k = 29$

Avec l'algorithme d'Euclide : $144 = 145 - 1 = 5 \times 29 - 1$ donc $5 \times 29 = 1 \bmod 144$ c'est bien plus rapide.

Ex3 $y^5 = 79 \bmod 315$. ~~$79^5 x \wedge 315 = 1$~~ donc $\exists x$, $79^5 x = 1 \bmod 315$ et alors $y\, y^4 x = 1 \bmod 315$: $y^4 x$ est inverse de y dans $\mathbb{Z}/315\mathbb{Z}$

inversement s'il existe x tq $yx = 1$ dans $\mathbb{Z}/315\mathbb{Z}$ alors $(yx)^5 = y^5 x^5 = 1$ donc x^5 est inverse de y^5.

$79 = -1 \bmod 5$ donc $79^{29} = (-1)^{29} = -1 \bmod 5$

$79 = 77 + 2 = 2 \bmod 7$ donc $79^{29} = 2^{29} \bmod 7$ On $2 \in (\mathbb{Z}/7\mathbb{Z})^\times$ donc $2^6 = 1 \bmod 7$ puis $2^{29} = 2^{30-1} = 2^{-1} = 4 \bmod 7$

$79 = 81 - 2 = -2 \bmod 9$ donc $79^{29} = (-2)^{29} = ((-2)^3)^9 (-2)^2 = 1^9 (-2)^2 = 4 \bmod 9$

$\phi : \mathbb{Z}/315\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/5 \times \mathbb{Z}/7 \times \mathbb{Z}/9$ $\phi(79^{29}) = (-1, 4, 4) = (4, 4, 4)$ donc $\phi(79^{29} - 4) = 0$ donc $79^{29} = 4 \bmod 315$

D'où $(y^5)^{29} = y^{145} = 4 \bmod 315$. Comme dans l'ex. 1 $y^{145} = y \bmod 315$ car y est inversible. Conclusion $y = 4 \bmod 315$