Correction Examen 2nd session 2022-2023

Exercice 1.
1) Les entiers 3 et 4 sont premiers entre eux. On a donc par le théorème des restes chinois que $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/12\mathbb{Z}$. Ainsi, si x_0 est une solution du système $a)$ (resp. $b)$), alors les solutions de ce système sont données par

$$S = \{x_0 + 12k \mid k \in \mathbb{Z}\}$$

L'entier 5 (resp. 7) est une solution particulière du système $a)$ (resp. $b)$), donc les solutions de ce système sont donc exactement les entiers congrus à 5 modulo 12 (resp. à 7 modulo 12).

2) Soit x une solution quelconque du système (S). Il existe par hypothèse deux entiers k, k' tels que

$$\begin{cases} x_0 = 3 + 4k \\ x_0 = 1 + 6k' \end{cases} \Rightarrow 3 + 4k = 1 + 6k' \Leftrightarrow 2 = 2(3k' - 2k) \Leftrightarrow 1 = 3k' - 2k$$

On cherche donc toutes les solutions (k, k') de cette relation de Bézout. Si $3k' - 2k = 1$, on a

$$3 - 2 = 3k' - 2k \Leftrightarrow 3(k' - 1) = 2(k - 1)$$

Comme 3 et 2 sont premiers entre eux, on obtient l'existence d'un entier $p \in \mathbb{Z}$ tel que $k - 1 = 3p$ et $k' - 1 = 2p$. On obtient alors $k = 3p+1$ et $x_0 = 3+4(3p+1) = 7+12p$. Ainsi, les solutions x de (S) sont telles que $x \equiv 7[12]$. Réciproquement, si $x \equiv 7[12]$, alors $x \equiv 7 \equiv 3[4]$ et $x \equiv 7 \equiv 1[6]$, d'où l'implication réciproque et l'équivalence voulue.

Exercice 2.
1) Une fois encore, on effectue l'algorithme d'Euclide :

$$\begin{aligned} 1004 &= 768 \cdot 1 + 236 \\ 768 &= 236 \cdot 3 + 60 \\ 236 &= 60 \cdot 3 + 56 \\ 60 &= 56 \cdot 1 + 4 \\ 56 &= 4 \cdot 14 + 0 \end{aligned}$$

On remonte cet algorithme pour obtenir $1004 \cdot (-13) + 768 \cdot 17 = 4$.

2) En divisant la première ligne de l'algorithme d'Euclide précédent par 768, on obtient

$$\frac{1004}{768} = 1 + \frac{236}{768} = 1 + \frac{1}{\frac{768}{236}} = \left[1, \frac{768}{236}\right]$$

On est donc ramenés à trouver la décomposition de $\frac{768}{236}$ en fraction continue, on regarde donc la deuxième ligne de l'algorithme d'Euclide précédent, pour obtenir :

$$\frac{768}{236} = 3 + \frac{60}{236} = \left[3, \frac{236}{60}\right]$$

On obtient de même avec les deernières lignes :

$$\frac{236}{60} = \left[1, \frac{60}{56}\right], \ \frac{60}{56} = \left[1, \frac{56}{4}\right] = [1, 14]$$

On obtient, en réinjectant successivement :

$$\begin{aligned}\frac{1004}{768} &= \left[1, \frac{768}{236}\right] \\ &= \left[1, 3, \frac{236}{60}\right] \\ &= \left[1, 3, 3, \frac{60}{56}\right] \\ &= [1, 3, 3, 1, 14]\end{aligned}$$

On s'aperçoit d'ailleurs que les coefficients de cette fraction continues sont les quotients successifs de l'algorithme d'Euclide.

3) Pour les nombres irrationnels, hélas plus d'algorithme d'Euclide. Pour racine de 5, on a $2^2 < 5 < 3^2$, donc la partie entière de $\sqrt{5}$ est $\lfloor \sqrt{5} \rfloor = 2$. On a alors

$$\sqrt{5} = 2 + (\sqrt{5} - 2) = \left[2, \frac{1}{\sqrt{5} - 2}\right]$$

Il reste donc à trouver la décomposition en fraction continue de $\frac{1}{\sqrt{5}-2}$. On a

$$\frac{1}{\sqrt{5} - 2} = \frac{\sqrt{5} + 2}{(\sqrt{5} - 2)(\sqrt{5} + 2)} = \frac{\sqrt{5} + 2}{5 - 4} = \sqrt{5} + 2$$

Dont la partie entière est $2 + 2 = 4$. On a alors

$$\sqrt{5} = [2, \sqrt{5} + 2] = \left[2, 4, \frac{1}{\sqrt{5} - 2}\right]$$

On retrouve $\frac{1}{\sqrt{5}-2}$, en appliquant le même calcul, on trouve

$$\sqrt{5} = \left[2, 4, 4, \frac{1}{\sqrt{5} - 2}\right] = [2, \overline{4}]$$

Exercice 3.
1) On cherche les racine du polynôme $X^2 - 1$ dans $\mathbb{Z}/n\mathbb{Z}$. On a $X^2 - 1 = (X - 1)(X + 1)$, donc

$$x^2 \equiv [n] \Leftrightarrow (x - 1)(x + 1) \equiv 0[n]$$

Comme n est premier, $Z/n\mathbb{Z}$ est intègre, donc ceci équivaut à $x - 1 \equiv 0[n]$ ou $x + 1 \equiv 0[n]$. On a donc deux solutions de $x^2 \equiv 1[n]$: $x = 1$ et $x = -1$. Notons que si n n'est pas premier, on peut avoir d'avantage de solutions : $4^2 = 1[15]$ alors que $4 \not\equiv 1, -1[15]$.

2) Comme n est premier, tous les entiers de $\{1, \ldots, n - 1\}$ admettent un unique inverse modulo $\mathbb{Z}/n\mathbb{Z}$. On sait d'ailleurs que 1 et $n - 1$ sont leurs propres inverses modulo n (car $1^2 \equiv 1[n]$ et $(n - 1)^2 \equiv (-1)^2 \equiv 1[n]$). Un entier $k \in \{2, \ldots, n - 2\}$ admet donc un unique inverse modulo n dans $\{2, \ldots, n - 2\}$, en effet, l'inverse de k ne peut être 1 où $n - 1$ car k n'est pas égal ni à 1, ni à $n - 1$.

En réordonnant le produit $2 \ldots n - 2$, on peut donc l'écrire comme des produits d'éléments de $\{2, \ldots, k\}$ et de leurs inverses. Le produit est alors égal à 1 modulo n. On a alors $(n - 1)! \equiv 1 \cdot (n - 1)[n] \equiv -1[n]$

3) Supposons que n est non premier, et soit p le plus petit diviseur de n non égal à 1. On pose $n = pq$.

- Si $p < q$, alors les entiers p et q apparaissent dans le produit $(n - 1)!$, donc n divise $(n - 1)!$ et $(n - 1)! = 0$.
- Si $p = q$, alors $n = p^2$. Si $p = 2$, alors $n = 4$, et il est clair que $3! = 6 \equiv 2[4]$. Si $p > 2$ alors $p^2 = n > 2p$. Donc p et $2p$ sont deux entiers plus petit que $n - 1$, qui apparaissent donc dans le produit $(n - 1)!$. Donc $2p^2 = 2n$ divise $(n - 1)!$ et $(n - 1)! \equiv 0[n]$.

4) On a montré à la question (b) que si n est premier, alors $(n-1)! \equiv -1[n]$. Et on a montré à la question (c) que si n n'est pas premier, alors $(n-1)! \not\equiv -1[n]$.

Exercice 4.

1) On a premièrement 51447-17=51430. Ensuite, comme $3 \cdot 17 = 51$, on a $51430 - 3000 \cdot 17 = 430$. Enfin, comme $430 - 25 \cdot 17 = 5$, on a le résultat voulu.

2) On a $12 = 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 0 \cdot 1$, la décomposition en binaire de 12 est donc 1100. 3) Pour $i \in \mathbb{N}$, on sait que $5^{2^{i+1}} = 5^{2 \cdot 2^i} = (5^{2^i})^2$. Ceci est aussi vrai modulo 17. On a

- $5^0 = 1 \equiv 1[17]$ et $5^1 \equiv 5[17]$.
- $5^2 = 25 \equiv 8[17]$.
- $5^4 \equiv 8^2 \equiv 64 \equiv 13[17]$.
- $5^8 \equiv 13^2 \equiv (-4)^2 \equiv 16 \equiv -1[17]$.

4) On a
$$51447^{12} \equiv 5^{12} = 5^8 \cdot 5^4 \equiv -1 \cdot 13 \equiv 4[17]$$

5) L'exponentiation naïve requiert m multiplications de n avec lui même, d'où une complexité en $O(m)$. Pour l'exponentiation rapide, on calcule n^{2^i} pour $i \leqslant L(m)$, soit $L(m)$ multiplications (où $L(m)$ désigne la longueur en base 10, elle appartient à $O(\ln(m))$. On fait ensuite le produit des n^{2^i}, soit au plus $L(m)$ multiplications, soit une complexité totale en $O(2L(m)) \subset O(2\ln(m))$ comme annoncé.

Exercice 5.

1) Comme $35 = 7 \cdot 5$ et que 7 et 5 sont premiers entre eux, on a $\varphi(35) = \varphi(7)\varphi(5)$. Comme 7 et 5 sont des nombres premiers, on a $\varphi(5) = 4$ et $\varphi(7) = 6$, d'où $\varphi(35) = 24$.

2) Comme $5^2 = 25$, on a $5^2 \equiv 1[24]$, donc 5 est son propre inverso modulo $\varphi(n)$.

3) La clé publique est $(35, 5)$. Soit M le message original (décodé). Par définition du chiffrement RSA, on a $M^5 = C$. Le décodage doit être fait en calculant $C^n[35]$ où n est l'inverse de 5 modulo $\varphi(35)$. Par la question précédente, on calcule
$$10^5 = 10^4 \cdot 10 = 100^2 \cdot 10 \equiv (-5)^2 \cdot 10 \equiv 25 \cdot 10 \equiv -100 \equiv 5[35]$$

Pour réencoder le message, il suffit de faire $5^5 = 10[35]$ et on retrouve le message codé C.