Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Alain Kraus

Correction du partiel du 1er avril 2022

Exercice 1

1) On a $n = 11 \times 23$ et $\varphi(n) = 220$. Déterminons l'inverse de 147 modulo 220. Pour cela, on vérifie avec l'algorithme d'Euclide que l'on a le tableau suivant :

	1	2	73	
220	147	73	1	0
1	0	1	-2	
0	1	-1	3	

On en déduit que l'on a

$$-2 \times 220 + 3 \times 147 = 1.$$

Par suite, 3 est l'inverse cherché. Le message secret que Bob souhaite envoyer à Alice est donc 5^3 mod. 253 i.e. 125 mod. 253.

2.1) On a $n = 3 \times 29$. On a $7 \equiv 1$ mod. 3, donc 7 est un carré modulo 3 et d'après la loi de réciprocité quadratique, on a les égalités des symboles de Legendre

$$\left(\frac{7}{29}\right) = \left(\frac{29}{7}\right) = 1.$$

Parce que 7 est un carré modulo 3 et 29, c'est donc un carré modulo n.

2.2) Soit S l'ensemble des solutions de l'équation $x^2 = 7$ dans $\mathbb{Z}/n\mathbb{Z}$. Les quatre messages décryptés possibles sont les éléments de S. Modulo 3, les racines carrées de 7 sont ± 1. Modulo 29, les racines carrées de 7 sont ± 6. On est ainsi amené à résoudre les deux systèmes de congruences

$$\begin{cases} x \equiv 1 \text{ mod. } 3 \\ x \equiv 6 \text{ mod. } 29 \end{cases} \quad \text{et} \quad \begin{cases} x \equiv 1 \text{ mod. } 3 \\ x \equiv -6 \text{ mod. } 29. \end{cases}$$

On obtient comme solutions particulières respectivement $x = 64$ et $x = 52$. En tenant compte des solutions opposées, on en déduit que l'on a

$$S = \left\{\overline{23}, \overline{35}, \overline{52}, \overline{64}\right\}.$$

Exercice 2

1) Il s'agit du polynôme $1 + X + X^2 \in \mathbb{F}_2[X]$.

2) On vérifie que f n'a pas de racines dans $\mathbb{F}_2$. Par ailleurs, on a

$$f = (X^2 + X + 1)(X^3 + X^2) + 1.$$

(On peut par exemple obtenir cette égalité en remarquant que l'on a $f = X^2(X^3+1)+1$ et que $X^3+1 = (X+1)(X^2+X+1)$.) Ainsi, f n'est pas divisible par l'unique polynôme de degré 2 de $\mathbb{F}_2[X]$, donc f est irréductible sur $\mathbb{F}_2$. Le cardinal de K est $2^5 = 32$.

3) Parce que l'ordre de K^* est 31, tout élément distinct de 1 est un générateur de K^*, en particulier tel est le cas de α.

4.1) On a $\alpha^5 + \alpha^2 = 1$ d'où $\alpha^2(1 + \alpha^3) = 1$. Par suite, on a $1 + \alpha^3 = \alpha^{-2}$. On a $\alpha^{31} = 1$, d'où $\alpha^{-2} = \alpha^{29}$, puis $a = 29$.

4.2) On a $(1 + \alpha)^{32} = 1 + \alpha$. Par ailleurs, on a $(1 + \alpha)^2 = 1 + \alpha^2 = \alpha^5$. On en déduit les égalités $1 + \alpha = \alpha^{80} = \alpha^{18}$, d'où $b = 18$.

4.3) D'après les deux questions précédentes, on a donc $C = \alpha^{522}$. On a $522 \equiv 26$ mod. 31, d'où $n = 26$.

Exercice 3

1) On a $8^{44} = 2^{132}$ et $132 = 11 \times 12$. Par ailleurs, on vérifie que l'on a $2^{12} \equiv 1$ mod. 45. Il en résulte que $8^{44} \equiv 1$ mod. 45. L'entier 45 est composé, d'où le résultat.

2) On a $n \equiv 1$ mod. 4 et $n \equiv 2$ mod. 3. D'après la loi de réciprocité quadratique, on en déduit que l'on a

$$\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) = -1.$$

Parce que n est pseudo-premier d'Euler en base 3, on a donc

$$3^{\frac{n-1}{2}} \equiv -1 \text{ mod. } n.$$

Par ailleurs, on a $n - 1 \equiv 0$ mod. 4, donc il existe $s \geq 2$ et un entier t impair tels que $n - 1 = 2^s t$. On obtient

$$3^{2^{s-1}t} \equiv -1 \text{ mod. } n,$$

ce qui montre que n est pseudo-premier fort en base 3 (Définition 2.6).

3) On a $2^4 \equiv 1$ mod. 5. On a $n \geq 2$ d'où $2^{2^n} \equiv 1$ mod. 5, puis $F_n \equiv 2$ mod. 5. D'après la loi de réciprocité quadratique, on a donc les égalités des symboles de Jacobi

$$\left(\frac{5}{F_n}\right) = \left(\frac{F_n}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

En utilisant par exemple le corollaire 2.4, avec $h = 1$, $N = 2^n$ et $a = 5$, on en déduit l'équivalence annoncée. On peut aussi utiliser le corollaire 2.3 d'où l'on avait déduit le test de Pepin.

4) Supposons $p \geq 3$ et que 2 soit un générateur de $\mathbb{F}_{M_p}^*$. On a $M_p - 1 = 2^p - 2$ d'où $\frac{M_p-1}{2} = 2^{p-1} - 1$. On a $2^{p-1} \equiv 1$ mod. p, d'où la congruence (qui a été établie dans la démonstration du lemme 2.5 concernant les entiers pseudo-premiers)

$$2^{\frac{M_p-1}{2}} \equiv 1 \text{ mod. } M_p.$$

On en déduit que l'on a $\frac{M_p-1}{2} = M_p - 1$ i.e. $M_p = 1$, d'où une contradiction. Par ailleurs, 2 est un générateur de $\mathbb{F}_3^*$. L'ensemble cherché est donc le singleton $\{2\}$.

Exercice 4

1.1) On a $284^2 - 123^2 = 161 \times 407 \equiv 0$ mod. N. On vérifie que $\text{pgcd}(N, 161) = 23$ d'où l'on déduit que $N = 23 \times 37$.

1.2) L'exposant du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est $\lambda(n)$ où λ est la fonction de Carmichael (voir le chapitre I page 7). D'après la question précédente, on obtient (Lemme 1.3 ou la formule (5) page 8)

$$\lambda(n) = \text{ppcm}(22, 36) = 396.$$

2) On utilise l'algorithme $p - 1$ de Pollard qui se trouve à la page 4 du chapitre III, avec l'entier $B = 3$. On a $B! = 6$ et $\text{pgcd}(2^6 - 1, 77) = 7$, d'où $77 = 7 \times 11$ comme attendu.

3) Calculons les premiers termes de la suite $(x_i)_{i\in\mathbb{N}}$ définie par $x_0 = 3$ et par l'égalité $x_{i+1} = f(x_i)$ mod. 1339. On a

$$x_0 = 3, \quad x_1 = 10, \quad x_2 = 101.$$

On a $\text{pgcd}(x_2 - x_1, 1339) = 13$ d'où $1339 = 13 \times 103$. Par ailleurs, 103 est un premier, car il n'est pas divisible par un nombre premier plus petit que 10, c'est donc la décomposition cherchée.

4) Posons $p = 191$. L'entier p est un nombre premier, car il n'est pas divisible par un nombre premier plus petit que 14. On a $p \equiv 3$ mod. 4 et $2p + 1 = 383$, qui n'est pas divisible par un nombre premier plus petit que 20, est aussi un nombre premier. D'après la question 2 de l'exercice 6 du chapitre II, l'entier $2^{191} - 1$ est donc divisible par 383.