INFMDI720
Contrôle de connaissance — Corrigé

Rappels mathématiques pour la cryptographie

22 novembre 2011

Consignes :

Les exercices sont complètement indépendants. Ils pourront être traités dans un ordre quelconque, mais on demande de faire apparaître de façon très visible dans les copies où commence chaque exercice.

Il n'est pas nécessaire de faire des réponses longues.

L'usage de tous les documents (notes de cours manuscrites ou imprimées, livres) est autorisé.

L'usage des calculatrices électroniques est interdit.

Durée : 2h

Exercice 1.

(1a) Rappeler pourquoi, si x n'est pas multiple de 13, alors $x^{12} \equiv 1 \pmod{13}$, et pourquoi, si x n'est pas multiple de 19, alors $x^{18} \equiv 1 \pmod{19}$.

Corrigé. Cela découle, dans les deux cas, du petit théorème de Fermat ($x^{p-1} \equiv 1 \pmod{p}$ si p est premier et x non multiple de p). ✓

(1b) En déduire que, si x n'est pas multiple de 13, alors $x^{36} \equiv 1 \pmod{13}$, et que, si x n'est pas multiple de 19, alors $x^{36} \equiv 1 \pmod{19}$.

Corrigé. On a $36 = 12 \times 3$; donc, si on a $x^{12} \equiv 1 \pmod{13}$ (pour x non multiple de 13), alors en particulier $x^{36} = x^{12\times 3} = (x^{12})^3 \equiv 1 \pmod{13}$. De la même façon, puisque $36 = 18 \times 2$, le fait que $x^{18} \equiv 1 \pmod{19}$ entraîne $x^{36} \equiv 1 \pmod{19}$. ✓

(2) Conclure de la question précédente que si x est premier avec 247, alors $x^{36} \equiv 1 \pmod{247}$ (remarque : $247 = 13 \times 19$).

Corrigé. Dire que x est premier avec $247 = 13\times 19$ signifie que x n'est multiple ni de 13 ni de 19. D'après la question précédente, on a alors $x^{36} \equiv 1$ modulo 13 et modulo 19. Le théorème chinois implique, vu que 13 et 19 sont premiers entre eux, que cette congruence $x^{36} \equiv 1$ vaut encore modulo $13 \times 19 = 247$. (Ou, de façon équivalente, $x^{36} - 1$ est multiple de 13 et de 19, donc de 247.) ✓

(3) Que vaut $\varphi(247)$ (où bien sûr φ désigne l'indicatrice d'Euler) ?

Corrigé. On a $\varphi(13 \times 19) = (13 - 1) \times (19 - 1) = 12 \times 18 = 216$. ✓

(4) En oubliant provisoirement les questions (1) et (2), quel théorème connu permettait d'énoncer le fait que $x^N \equiv 1 \pmod{247}$ si x est premier avec 247, pour un certain N (à préciser) ne dépendant pas de x ? Comparer ce résultat avec celui de la question (2), et commenter (lequel est le plus fort ?).

Corrigé. Le théorème d'Euler assure que $x^{\varphi(247)} \equiv 1 \pmod{247}$ pour tout x premier avec 247, c'est-à-dire $x^{216} \equiv 1 \pmod{247}$ (bref, $N = 216$ convient). La question (2) affirmait la même chose pour $N = 36$. Cette dernière est donc plus forte (comme 36 divise 216, le fait que $x^{36} \equiv 1$ entraîne automatiquement $x^{216} \equiv 1$). ✓

(5) Rappeler pourquoi il existe g_1 (resp. g_2) un élément de $(\mathbb{Z}/13\mathbb{Z})^\times$ (resp. $(\mathbb{Z}/19\mathbb{Z})^\times$) dont l'ordre multiplicatif vaut exactement 12 (resp. 18) : comment appelle-t-on un tel élément ?

Corrigé. Un tel élément s'appelle un élément primitif. Il existe car 13 (resp. 19) est premier. ✓

(6) Rappeler pourquoi il existe $h \in (\mathbb{Z}/247\mathbb{Z})^\times$ tel que $h \equiv g_1 \pmod{13}$ et $h \equiv g_2 \pmod{19}$.

Corrigé. Un tel h existe d'après le théorème chinois, qui garantit que la donnée d'une congruence quelconque modulo 13 et d'une congruence quelconque modulo 19 peut toujours s'écrire comme une unique congruence modulo $13\times19 = 247$ (de nouveau, parce que 13 et 19 sont premiers entre eux). ✓

(7) Montrer que l'ordre multiplicatif (modulo 247) d'un tel h vaut exactement 36. Quel est l'ordre multiplicatif maximal possible d'un élément de $(\mathbb{Z}/247\mathbb{Z})^\times$?

Corrigé. Supposons que $h^s \equiv 1 \pmod{247}$ pour un certain entier s. Alors, en réduisant modulo 13, puisque $h \equiv g_1 \pmod{13}$, on a $g_1^s \equiv 1 \pmod{13}$, ce qui, vu que g_1 est d'ordre exactement 12, entraîne que s est multiple de 12. De même, $g_2^s \equiv 1 \pmod{19}$, ce qui entraîne que s est multiple de 18. On en conclut que s est multiple de $\mathrm{ppcm}(12, 18) = 36$.

On a vu en (2) que l'ordre multiplicatif de tout élément de $(\mathbb{Z}/247\mathbb{Z})^\times$ divise 36, on vient de voir qu'il existe des éléments d'ordre 36, donc l'ordre maximal possible est 36. ✓

(8) Dresser la table des puissances de 2 modulo 13 puis modulo 19.

Corrigé. Modulo 13, on calcule (de proche en proche) :

s	0	1	2	3	4	5	6	7	8	9	10	11
2^s	1	2	4	8	3	6	12	11	9	5	10	7

Ces douze puissances sont distinctes (après quoi on retombe sur 1), donc 2 est primitif modulo 13.

Modulo 19, on calcule (de proche en proche) :

s	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2^s	1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10

Ces dix-huit puissances sont distinctes (après quoi on retombe sur 1), donc 2 est primitif modulo 19. ✓

(9) Montrer que 2 est d'ordre multiplicatif 36 modulo 247.

Corrigé. On vient de voir que $g_1 = 2$ est primitif modulo 13 et que $g_2 = 2$ l'est modulo 19, donc $h = 2$ est d'ordre 36 modulo $13 \times 19 = 247$ d'après la question (7). ✓

(10) Montrer que l'élément $\bar{3} \in (\mathbb{Z}/247\mathbb{Z})^\times$ ***n'est pas*** une puissance de 2 (on justifiera la réponse).

Corrigé. Si $2^s \equiv 3 \pmod{247}$, on a $2^s \equiv 3 \pmod{13}$ et $2^s \equiv 3 \pmod{19}$. La première partie donne $s \equiv 4 \pmod{12}$ d'après la table des puissances de 2 modulo 13 qu'on a calculée. La seconde condition donne $s \equiv 13 \pmod{18}$ d'après la table des puissances de 2 modulo 18. Ces deux conditions ne sont pas compatibles (la première implique que s est pair, la seconde, que s est impair) :

la prémisse est donc absurde, c'est-à-dire que 3 n'est pas une puissance de 2 modulo 247. ✓

Exercice 2.

Soit p un nombre premier tel que $p \equiv 3 \pmod 4$.

(1) Montrer que $(p-1)/2$ est impair. Que vaut $(-1)^{(p-1)/2}$?

Corrigé. On peut écrire $p = 3 + 4k$ avec $k \in \mathbb{Z}$, donc $p - 1 = 2 + 4k$ donc $(p-1)/2 = 1+2k$, ce qui montre que $(p-1)/2$ est impair (i.e., $p \equiv 1 \pmod 2$). On a donc $(-1)^{(p-1)/2} = -1$. ✓

(2) Si $z \in \mathbb{F}_p^\times$, que vaut $(z^2)^{(p-1)/2}$? En déduire qu'il n'existe pas de $z \in \mathbb{F}_p$ tel que $z^2 = -1$.

Corrigé. Si $z \in \mathbb{F}_p^\times$, on a $(z^2)^{(p-1)/2} = z^{p-1} = 1$ dans $\mathbb{F}_p$ d'après le petit théorème de Fermat. Il n'existe donc pas de $z \in \mathbb{F}_p^\times$ tel que $z^2 = -1$ (car on vient de voir que $(-1)^{(p-1)/2} = -1 \neq 1$) ; par ailleurs, si $z = 0$ on a $z^2 = 0 \neq -1$ donc il n'existe pas de $z \in \mathbb{F}_p$ tel que $z^2 = -1$. ✓

(3) Déduire de la question précédente que le polynôme $t^2 + 1 \in \mathbb{F}_p[t]$ est irréductible.

Corrigé. Le polynôme $t^2 + 1$ étant de degré 2, la seule façon dont il pourrait être réductible serait qu'il le fût comme produit de deux facteurs de degré 1, c'est-à-dire qu'il eût deux racines. Or la question précédente signifie précisément que $t^2 + 1$ n'a pas de racine dans $\mathbb{F}_p$. ✓

On pose maintenant $E = \mathbb{F}_p[t]/(t^2 + 1)$.

(4) Combien d'éléments a E ? Que peut-on dire de sa structure algébrique (est-ce un anneau, un corps...) ? Quel autre nom (à part « E ») pourrait-on lui donner ? Quelle est la forme générale d'un élément de E ?

Corrigé. Les éléments de E sont au nombre de $p^{\deg(t^2+1)} = p^2$ et se voient comme des polynômes de degré < 2, c'est-à-dire ≤ 1, à coefficients dans $\mathbb{F}_p$, autrement dit de la forme $u + v\bar{t}$ avec $u, v \in \mathbb{F}_p$ (uniquement déterminés). Par ailleurs, comme $t^2 + 1$ est irréductible, on peut dire que E est un corps, et il mériterait de se noter $\mathbb{F}_{p^2}$ (c'est *le* corps fini à p^2 éléments). ✓

On notera « $\sqrt{-1}$ » l'élément $\bar{t}$ de E, c'est-à-dire, la classe modulo $t^2 + 1$ de l'indéterminée t. (On ne cherchera pas à donner un sens à la notation $\sqrt{\ }$, encore moins à faire un lien avec les nombres réels ou complexes : on se contentera de prendre $\sqrt{-1}$ comme une notation pour $\bar{t}$.)

(5) Que vaut le carré $(\sqrt{-1})^2$ de l'élément qu'on vient de décrire ?

Corrigé. Modulo $t^2 + 1$, on a $t^2 = -1$, c'est-à-dire que $(\sqrt{-1})^2 = -1$ dans E. ✓

(6) Quelles sont toutes les solutions de l'équation $z^2 = -1$ dans E ? En déduire quelle est la factorisation du polynôme $t^2 + 1$ vu, cette fois, comme un élément de $E[t]$.

Corrigé. On vient de voir que $(\sqrt{-1})^2 = -1$. On en déduit $(-\sqrt{-1})^2 = -1$. On a donc trouvé deux solutions, $\sqrt{-1}$ et $-\sqrt{-1}$, de l'équation $z^2 = -1$, c'est-à-dire deux racines du polynôme $t^2+1 \in E[t]$. Comme il s'agit d'un polynôme (non nul) de degré 2, il ne peut pas admettre strictement plus que deux racines, donc on a bien toutes les racines : les solutions de $z^2 = -1$ sont exactement $\sqrt{-1}$ et $-\sqrt{-1}$, et la factorisation de t^2+1 dans $E[t]$ s'écrit : $t^2+1 = (t-\sqrt{-1})(t+\sqrt{-1})$. ✓

(7) Expliquer pourquoi tout élément de E s'écrit de la forme $u + v\sqrt{-1}$ avec u, v deux éléments de $\mathbb{F}_p$ (uniquement déterminés). Donner des formules permettant de calculer la somme $(u_1 + v_1\sqrt{-1}) + (u_2 + v_2\sqrt{-1})$ et le produit $(u_1 + v_1\sqrt{-1}) \cdot (u_2 + v_2\sqrt{-1})$ de deux éléments de E, en les mettant sous la forme $u + v\sqrt{-1}$ (on demande donc de calculer u et v de la somme et du produit en fonction de u_1, v_1, u_2, v_2).

Corrigé. On a déjà expliqué en réponse à la question (4) que tout élément de E s'écrit de la forme $u + v\bar{t}$ avec $u, v \in \mathbb{F}_p$ (uniquement déterminés), et on a choisi de noter $\bar{t}$ comme $\sqrt{-1}$.

Pour la somme, on a $(u_1+v_1\sqrt{-1})+(u_2+v_2\sqrt{-1}) = (u_1+u_2)+(v_1+v_2)\sqrt{-1}$ en factorisant, c'est-à-dire qu'elle vaut $u+v\sqrt{-1}$ avec $u = u_1+u_2$ et $v = v_1+v_2$.

Pour le produit, on a $(u_1 + v_1\sqrt{-1}) \cdot (u_2 + v_2\sqrt{-1}) = u_1u_2 + u_1v_2\sqrt{-1} + v_1u_2\sqrt{-1}+v_1v_2(\sqrt{-1})^2$ en développant, soit $(u_1u_2-v_1v_2)+(u_1v_2+v_1u_2)\sqrt{-1}$ en utilisant $(\sqrt{-1})^2 = -1$ et en factorisant, c'est-à-dire que ce produit vaut $u+v\sqrt{-1}$ avec $u = u_1u_2 - v_1v_2$ et $v = u_1v_2 + v_1u_2$. ✓

(8) Que vaut $(\sqrt{-1})^4$? Déterminer $(\sqrt{-1})^r$ en discutant suivant la valeur de l'entier r modulo 4.

Corrigé. On a $(\sqrt{-1})^4 = (-1)^2 = 1$: si on veut, l'élément $\sqrt{-1}$ de $E^\times$ est d'ordre (multiplicatif) 4. Par conséquent, la valeur de $(\sqrt{-1})^r$ ne dépend que de la classe de r modulo 4. Selon que r est congru à 0, 1, 2 ou 3 modulo 4, la valeur en question est respectivement $(\sqrt{-1})^0 = 1$, $(\sqrt{-1})^1 = \sqrt{-1}$, $(\sqrt{-1})^2 = -1$, ou $(\sqrt{-1})^3 = -\sqrt{-1}$. ✓

On rappelle que $\mathrm{Frob}\colon E \to E$ désigne l'application $x \mapsto x^p$.

(9) D'après la question précédente, que vaut $\mathrm{Frob}(\sqrt{-1})$?

Corrigé. On a $p \equiv 3 \pmod 4$ par hypothèse, donc $\mathrm{Frob}(\sqrt{-1}) = (\sqrt{-1})^p = -\sqrt{-1}$ d'après la question (8). ✓

On rappelle pour la question suivante que $\mathrm{Frob}(x + y) = \mathrm{Frob}(x) + \mathrm{Frob}(y)$

et $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$ pour tous $x, y \in E$ (« le Frobenius est un morphisme de corps »), et aussi que $\mathrm{Frob}(a) = a$ si et seulement si $a \in \mathbb{F}_p$ (petit théorème de Fermat).

(10) Que vaut $\mathrm{Frob}(u + v\sqrt{-1})$ si $u, v \in \mathbb{F}_p$?

Corrigé. On vient de voir que $\mathrm{Frob}(\sqrt{-1}) = -\sqrt{-1}$, et par ailleurs $\mathrm{Frob}(u) = u$ et $\mathrm{Frob}(v) = v$ puisque $u, v \in \mathbb{F}_p$. En utilisant les propriétés rappelées, on a donc $\mathrm{Frob}(u + v\sqrt{-1}) = u - v\sqrt{-1}$. ✓

(11) En utilisant notamment la question précédente, montrer que l'on a : $(u + v\sqrt{-1})^{p+1} = u^2 + v^2$ pour tous $u, v \in \mathbb{F}_p$.

Corrigé. On vient de voir que $\mathrm{Frob}(u + v\sqrt{-1}) = u - v\sqrt{-1}$. On a $(u+v\sqrt{-1})^{p+1} = (u+v\sqrt{-1})\,(u+v\sqrt{-1})^p = (u+v\sqrt{-1})\,\mathrm{Frob}(u+v\sqrt{-1}) = (u+v\sqrt{-1})\,(u-v\sqrt{-1}) = u^2+v^2$ (en utilisant les formules de la question (7)). ✓

(12) Rappeler pourquoi il existe un élément g de $E^\times$ d'ordre multiplicatif $p^2 - 1$ (on ne demande pas de démontrer ce fait, mais de citer un théorème qui l'affirme) ; comment appelle-t-on un tel élément ?

Corrigé. Un tel élément s'appelle un élément primitif. Il existe car le groupe multiplicatif $E^\times$ des éléments non nuls de E, d'ordre p^2-1, est cyclique (comme l'est le groupe multiplicatif pour n'importe quel corps fini). ✓

Pour r entier, on définit u_r, v_r, éléments de $\mathbb{F}_p$, par la formule : $u_r + v_r\sqrt{-1} = g^{r(p-1)}$, où g est un élément comme dans la question précédente.

(13) Que vaut $u_r^2 + v_r^2$? Expliquer pourquoi les (u_r, v_r) avec $0 \leq r \leq p$ sont deux-à-deux distincts.

Corrigé. D'après (11), on a $u_r^2 + v_r^2 = (g^{r(p-1)})^{p+1} = g^{r(p^2-1)}$. Mais $g^{p^2-1} = 1$ puisque $g \in E^\times$. On a donc $u_r^2 + v_r^2 = 1$.

Si $0 \leq r \leq p$, c'est-à-dire $0 \leq r < p+1$, alors $0 \leq r(p-1) < p^2-1$. Puisque g est d'ordre exactement $p^2 - 1$, les g^s pour $0 \leq s < p^2 - 1$ sont deux-à-deux distincts, et en particulier les $g^{r(p-1)}$ pour $0 \leq r < p+1$ le sont. Comme par ailleurs u_r et v_r déterminent complètement $u_r + v_r\sqrt{-1}$, les couples (u_r, v_r) avec $0 \leq r \leq p$ sont eux-mêmes deux-à-deux distincts. ✓

(14) Réciproquement, si u, v dans $\mathbb{F}_p$ vérifient $u^2 + v^2 = 1$, montrer que $u + v\sqrt{-1}$ peut s'écrire sous la forme $g^{r(p-1)}$ (on a donc $(u, v) = (u_r, v_r)$) pour un certain r qu'on peut trouver vérifiant $0 \leq r \leq p$. (On pourra commencer par écrire $u + v\sqrt{-1} = g^s$ pour un certain s, puis montrer que celui-ci est un multiple de $p - 1$ en utilisant $u^2 + v^2 = 1$.)

Corrigé. Comme g est primitif, on peut écrire $u+v\sqrt{-1} = g^s$ pour un certain s vérifiant $0 \leq s < p^2-1$. L'hypothèse $u^2+v^2 = 1$ assure que $(u+v\sqrt{-1})^{p+1} = 1$

(d'après (11)), c'est-à-dire $g^{s(p+1)} = 1$. Autrement dit, $s(p+1)$ est multiple de $p^2 - 1$. Quitte à diviser par $p+1$, on voit donc que s est multiple de $p-1$, c'est-à-dire qu'on peut écrire $s = r(p-1)$, et on a alors bien $u + v\sqrt{-1} = g^{r(p-1)}$ avec $0 \leq r < p+1$ (puiqsue $r = \frac{s}{p-1}$). ✓

(15) Des questions précédentes, déduire le nombre de solutions (u, v) dans $\mathbb{F}_p$ de l'équation $u^2 + v^2 = 1$.

Corrigé. On a montré que ces solutions étaient les (u_r, v_r) avec $0 \leq r \leq p$, qui sont distinctes. Il y en a donc $p+1$. ✓