CRYPTOGRAPHIE ALGÉBRIQUE **4M035** **Feuille 4**
P. V. Koseleff

Exercice 4.1. — p désigne un nombre premier impair.

1. (a) Montrer que le polynôme X^2-1 a deux racines dans $\mathbf{F}_p$.
   (b) En déduire que pour $x \in \mathbf{F}_p^*$, on a $x^{\frac{p-1}{2}} = \pm 1$.
2. Soit $S : \mathbf{F}_p^* \to \mathbf{F}_p^*$, $x \mapsto x^2$.
   (a) Montrer que S est un morphisme de groupe.
   (b) Montrer que $x \in \mathbf{F}_p^*$ est un carré si et seulement si $x^{\frac{p-1}{2}} = 1$.
   (c) Montrer qu'il existe un seul morphisme de groupe non trivial de $\mathbf{F}_p^*$ dans $\{-1,1\}$.

Solution 4.1. —

1. (a) $X^2-1 = (X-1)(X+1)$ donc 1 et -1 sont deux racines distinctes car $p \neq 2$.
   (b) Soit $x \in \mathbf{F}_p^*$, et posons $y = x^{\frac{p-1}{2}}$. Alors $y^2 = x^{p-1} = 1$ d'après le théorème de Lagrange dans $\mathbf{F}_p^*$ et $y = \pm 1$ d'après la question précédente.
2. (a) On a clairement $S(xy^{-1}) = x^2y^{-2} = S(x)S(y)^{-1}$.
   (b) L'ensemble des carrés de $\mathbf{F}_p^*$ est exactement $S(\mathbf{F}_p^*)$, isomorphe à $\mathbf{F}_p^*/\{\pm 1\}$, donc de cardinal $(p-1)/2$. Si $x = y^2$ alors $x^{\frac{p-1}{2}} = y^{p-1} = 1$. Mais dans le corps $\mathbf{F}_p$, il y a au plus $(p-1)/2$ racines $(p-1)/2$-èmes de 1 : c'est $S(\mathbf{F}_p^*)$.
   (c) Soit g un générateur de $\mathbf{F}_p^*$ cyclique. Si $\varphi(g) = 1$ alors φ est trivial, sinon $\varphi(g) = -1$ et φ est uniquement déterminé.

Exercice 4.2. — Dans toute la suite p désigne un nombre premier.

1. Montrer que pour tout $a \in \mathbf{Z}$, on a $a^p = a \pmod p$.
2. En déduire que dans $\mathbf{Z}/p\mathbf{Z}[X]$, on a $X^p - X = \prod_{\alpha \in \mathbf{Z}/p\mathbf{Z}} (X-\alpha)$.
3. En déduire (en considérant la transformation $u \mapsto u-1$) que $(X+1)^p - (X+1) \equiv X^p - X \pmod p$.
4. En déduire le théorème de Wilson : $(p-1)! \equiv -1 \pmod p$.
5. En déduire que pour tout $k \in \mathbf{N}$, on a $(X+1)^{p^k} - (X+1) \equiv X^{p^k} - X \pmod p$.
6. En déduire que si $q = p^n$ alors $p \mid \binom{q}{m}$ si $1 \leq m \leq q-1$.

Solution 4.2. —

1. Lorsque p est premier et si p ne divise pas a, a est inversible modulo p donc $a^{p-1} \equiv 1 \pmod p$ et $a^p \equiv a \pmod p$. Lorsque $p \mid a$ alors $a^p \equiv a \equiv 0 \pmod p$.
2. Tous les éléments de $\mathbf{Z}/p\mathbf{Z}$ sont racines de $X^p - X$ et on déduit la factorisation $X^p - X = \prod_{\alpha \in \mathbf{Z}/p\mathbf{Z}} (X-\alpha)$.
3. L'application $u \mapsto u-1$ est une bijection de $\mathbf{Z}/p\mathbf{Z}$. Donc

$$X^p - X = \prod_{\alpha \in \mathbf{Z}/p\mathbf{Z}} (X-\alpha) = \prod_{\alpha \in \mathbf{Z}/p\mathbf{Z}} (X+1-\alpha) = (X+1)^p - (X+1)$$

   Mais alors par la formule du binôme, on a $(X+1)^p = \sum_{m=0}^{p} \binom{p}{m} X^m = X^p + 1$, soit $\binom{p}{m} \equiv 0 \pmod p$, pour $1 \leq m \leq p-1$.

4. On alors $X^{p-1}-1=\prod_{\alpha\in\mathbf{F}_p^*}(X-\alpha)$. En $X=0$, on trouve l'égalité demandée :

$$-1=\prod_{\alpha=1}^{p-1}(-\alpha)=(-1)^{p-1}(p-1)!=(p-1)!$$

5. Par récurrence sur k. La formule est vrai pour $k=0,1$. Supposons la vrai pour k, alors

$$(X+1)^{p^{k+1}}-(X+1)^p=\Big((X+1)^{p^k}-(X+1)\Big)^p=\Big(X^{p^k}-X\Big)^p=X^{p^{k+1}}-X^p,$$

d'où

$$(X+1)^{p^{k+1}}-(X+1)=X^{p^{k+1}}-X+\Big((X+1)^p-(X+1)-(X^p-X)\Big)=X^{p^{k+1}}-X.$$

6. On alors, en posant $q=p^n$, dans $\mathbf{F}_p[X]$, $(X+1)^q=\sum_{m=0}^{q}\binom{q}{m}X^m=X^q+1$, d'où le résultat.

Exercice 4.3. — Racines de 2.
p désigne ici un nombre premier impair.

1. (a) Montrer que $(p-1)!\equiv -1\pmod p$. (Théorème de Wilson).
   (b) En déduire que $\left(\frac{p-1}{2}!\right)^2\equiv(-1)^{(p+1)/2}\pmod p$.
2. (a) Montrer que -1 est un carré de $\mathbf{F}_p^*$ si et seulement si $p\equiv 1\pmod 4$.
   (b) En déduire que dans ce cas là : $a=\frac{p-1}{2}!$ vérifie $a^2=-1$.
3. (a) Montrer que
$$\left(\frac{2}{p}\right)\left(\frac{p-1}{2}!\right)\equiv 2\times 4\times\cdots(p-1)\pmod p$$
   (b) Montrer que
$$2\times 4\times\cdots(p-1)\pmod p\equiv(-1)\times 2\times(-3)\times 4\times\cdots(-\tfrac{p-3}{2})^{\frac{p-1}{2}}\pmod p$$
   (c) En déduire que
$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}.$$
   (d) À quelle condition 2 est-il un carré dans $\mathbf{F}_p^*$?
   (e) Montrer que si $p\equiv -1\pmod 8$, alors $4^{\frac{p+1}{8}}$ est une racine carrée de 2.

Solution 4.3. —

1. (a) On a $(p-1)!=1\times(-1)\times\prod_{i=2}^{p-2}i=-1$ car dans le produit $\prod_{i=2}^{p-2}i$ chaque élément apparaît avec son inverse distinct. On peut aussi utiliser l'exercice précédent.
   (b) On écrit $p-i\equiv -i$ pour $i\le(p-1)/2$, ainsi $(p-1)!=\left(\frac{p-1}{2}!\right)^2(-1)^{(p-1)/2}=-1$.
2. (a) -1 est un carré ssi $(-1)^{(p-1)/2}=1$, ie $p\equiv 1\pmod 4$.
   (b) On a $a^2=(-1)^{(p+1)/2}=-1$.
3. (a) On a
$$\left(\frac{2}{p}\right)\left(\frac{p-1}{2}!\right)\equiv 2^{(p-1)/2}\Big(\prod_{i=1}^{(p-1)/2}i\Big)\equiv\prod_{i=1}^{(p-1)/2}(2i)=2\times 4\times\cdots(p-1)\pmod p$$
   (b) Dans ce produit, on remplace $p-i$ par $-i$ lorsque i est impair et inférieur à $(p-3)/2$. On obtient
$$(-1)\times 2\times(-3)\times 4\times\cdots(-\tfrac{p-3}{2})^{\frac{p-1}{2}}\pmod p$$

(c) Mais

$$\begin{aligned}(-1)\times 2\times(-3)\times 4\times\cdots(-\tfrac{p-3}{2})\tfrac{p-1}{2} &= \prod_{i=1}^{(p-1)/2}(-1)^i\cdot i\\ &= \Big(\frac{p-1}{2}!\Big)(-1)^{1+2+\cdots+(p-1)/2}\\ &= (-1)^{\frac{p^2-1}{8}}\Big(\frac{p-1}{2}!\Big).\end{aligned}$$

On obtient donc

$$\Big(\frac{2}{p}\Big)\Big(\frac{p-1}{2}!\Big)\equiv(-1)^{\frac{p^2-1}{8}}\Big(\frac{p-1}{2}!\Big)\,(\mathrm{mod}\ p)$$

et le résultat car $a=\Big(\frac{p-1}{2}!\Big)$ vérifie $a^2\equiv -1\,(\mathrm{mod}\ p)$.

(d) $(4^{\frac{p+1}{8}})^2=2^{\frac{p+1}{2}}=2^{\frac{p-1}{2}}\cdot 2=2$.

Exercice 4.4. — Solutions de $a^2+b^2=p$
Soit $p>2$ un nombre premier impair.

1. Montrer que si $p\equiv 3 \mod 4$, il n'y a pas de solution dans $\mathbf{Z}^2$ à l'équation $x^2+y^2=p$.
2. On suppose désormais $p\equiv 1\,(\mathrm{mod}\ 4)$.
   (a) Montrer qu'il existe $a\in(\mathbf{Z}/p\mathbf{Z})^\times$ tel que $a^{(p-1)/2}\neq 1$. En déduire qu'il existe $b\in(\mathbf{Z}/p\mathbf{Z})^\times$ tel que $b^2=-1$.
   (b) Montrer que l'on peut trouver x et y entiers naturels tels que $x^2+y^2=mp$, avec $m<p/2$.
   (c) Supposons que $m>1$ et posons $x'\equiv x\,(\mathrm{mod}\ m)$ et $y'\equiv y\,(\mathrm{mod}\ m)$, avec $|x'|\leq m/2$ et $|y'|\leq m/2$. Montrer que
   $$X=\frac{xx'+yy'}{m}\quad\text{et}\quad Y=\frac{xy'-yx'}{m}$$
   sont des entiers et que l'on a $X^2+Y^2=pm'$, avec $m'\leq m/2$.
   (d) En déduire qu'il existe deux entiers naturels a et b tels que $a^2+b^2=p$.

Exercice 4.5. — Racines carrées dans $\mathbf{F}_p$
Soit $p\geq 3$ un nombre premier et a un élément de $\mathbf{F}_p^*$ qui soit un carré dans $\mathbf{F}_p$. Cet exercice concerne la détermination d'une racine carrée x de a dans $\mathbf{F}_p$. On pourra utiliser le critère d'Euler : *$a\in\mathbf{F}_q^*$ est un carré si et seulement si* $a^{(q-1)/2}=1$.

1. Si $p\equiv 3\,(\mathrm{mod}\ 4)$, montrer que l'on a $x=\pm\, a^{\frac{p+1}{4}}$.
2. Supposons $p\equiv 5\,(\mathrm{mod}\ 8)$. On admettra ici que 2 n'est pas un carré de $\mathbf{F}_p^*$.
   (a) Justifier l'égalité $a^{\frac{p-1}{4}}=\pm 1$.
   (b) Montrer que l'on a $x=\pm a^{\frac{p+3}{8}}$ si $a^{\frac{p-1}{4}}=1$.
   (c) Montrer que l'on a $x=\pm\, 2a\cdot(4a)^{\frac{p-5}{8}}$ sinon.
3. Le cas où $p\equiv 1\,(\mathrm{mod}\ 8)$ est moins simple.
   (a) Montrer que l'on a $p-1=2^e m$ où m est impair. Soit G le 2-sous-groupe $\mathbf{F}_p^*$ formé des solutions de l'équation $x^{2^e}=1$. C'est un groupe cyclique d'ordre 2^e. Soit z l'un de ses générateurs.
   (b) Montrer que a^m appartient à G et que a^m est un carré dans G.
   (c) Montrer qu'il existe un entier pair k tel que $a^m z^k=1$ avec $0\leq k<2^e$.
   (d) En déduire que $x=a^{\frac{m+1}{2}}z^{\frac{k}{2}}$ est une racine carrée de a dans $\mathbf{F}_p$.

Solution 4.5. —

1. D'après le critère d'Euler on a dans $\mathbf{F}_p^*$ l'égalité $a^{\frac{p-1}{2}} = 1$. Il en résulte que l'on a
$$\left(a^{\frac{p+1}{4}}\right)^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a = a.$$
2. (a) Parce que $\mathbf{F}_p$ est un corps, l'égalité $a^{\frac{p-1}{2}} = 1$ entraîne $a^{\frac{p-1}{4}} = \pm 1$ (p est congru à 1 modulo 4).
   (b) Si l'on a $a^{\frac{p-1}{4}} = 1$, en posant $x = \pm a^{\frac{p+3}{8}}$, on obtient $x^2 = a^{\frac{p+3}{4}} = a$.
   (c) Supposons $a^{\frac{p-1}{4}} = -1$. D'après la congruence $p \equiv 5 \mod 8$, on a l'égalité $2^{\frac{p-1}{2}} = -1$. Posons $x = \pm 2a.(4a)^{\frac{p-5}{8}}$. On vérifie alors que l'on a
$$x^2 = 4a^2.(4a)^{\frac{p-5}{4}} = a^{\frac{p+3}{4}} 2^{\frac{p-1}{2}} = -a^{\frac{p+3}{4}} = -a^{\frac{p-1}{4}} a = a.$$
3. (a) Parce que $\mathbf{F}_p^*$ est cyclique, G est l'unique sous-groupe de $\mathbf{F}_p^*$ d'ordre 2^e et il est formé des éléments $x \in \mathbf{F}_p^*$ tels que $x^{2^e} = 1$. On a
$$a^{p-1} = \left(a^m\right)^{2^e} = 1,$$
   donc a^m est dans G.
   Notons G^2 l'ensemble des carrés de G. C'est l'unique sous-groupe de G d'ordre 2^{e-1} (considérer le morphisme $G \to G$ qui à x associe x^2, dont le noyau est d'ordre 2). Ainsi, pour tout $x \in G$, x est dans G^2 si et seulement si $x^{2^{e-1}} = 1$. L'élément a étant un carré dans $\mathbf{F}_p$, on a
$$a^{\frac{p-1}{2}} = \left(a^q\right)^{2^{e-1}} = 1,$$
   donc a^q appartient à G^2.
   (b) D'après la question précédente, il existe un entier pair u tel que l'on ait $a^q = z^u$ avec $0 \leq u < 2^e$, ce qui entraîne l'assertion (si $u = 0$ on prend $k = 0$, sinon on prend $k = 2^e - u$). On obtient ainsi les égalités $x^2 = a^{q+1} z^k = a(a^q z^k) = a$.

Exercice 4.6. — Polynômes irréductibles

1. Montrer que le nombre de polynômes irréductibles unitaires de degré 2 dans $\mathbf{F}_p[X]$ est $\frac{p(p-1)}{2}$
2. Déterminer tous les polynômes polynômes irréductibles de degré inférieur à 4 dans $\mathbf{F}_2[X]$.

Solution 4.6. —

1. Le nombre $m_n(p)$ de polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ de degré n, vérifie
$$\sum_{d|n} d m_d(n) = p^n.$$
   On en déduit en particulier que $n m_n(p) < p^n$ puis
$$n m_n(p) \geq p^n - \sum_{d=1}^{n-1} d m_d(n) \geq p^n - \frac{p^n - p}{p-1} = \frac{p}{p-1} + p^n \frac{p-1}{p-1} \geq 1.$$
   Pour $n = 2$, on trouve $m_2(p) = \binom{p}{2}$. On peut retrouver ce résultat en remarquant que les polynômes de degré 2 qui ne sont pas irréductibles sont donc scindés. Il convient de choisir 2 racines (avec répétition) parmi les p éléments de $\mathbf{F}_p$, soit $\binom{p+1}{2}$. Il reste donc $p^2 - \binom{p+2}{2} = \binom{p}{2}$ polynômes irréductibles.
2. On a $m_4(p) = \frac{1}{4}(p^4 - p^2)$. Pour $p = 2$, on trouve $m_2(4) = 3$. Un polynôme de degré 4 est irréductible si il n'a pas de racine ou si il n'est pas divisible par un polynôme irréductible de degré 2. Le seul polynôme irréductible de degré 2 est $X^2 + X + 1 = \Phi_3$. On doit donc chercher $P = X^4 + aX^3 + bX^2 + cX + d$ avec $d = 1$ et $1 + a + b + c + d = 1$, soit $d = 1$ et $a + b + c = 1$. On doit aussi avoir $P \neq (X^2 + X + 1)^2 = X^4 + X^2 + 1$. Restent donc
$$P_1 = X^4 + X^3 + 1, P_2 = X^4 + X + 1, P_3 = X^4 + X^3 + X^2 + X + 1 = \Phi_5.$$
   Remarquons que $X^{16} - X = X(X-1)\Phi_3\Phi_5 P_1 P_2 \in \mathbf{F}_2[X]$ mais également $X^{16} - X = X(X^{15} - 1) = X\Phi_1\Phi_3\Phi_5\Phi_{15}$. On déduit alors que $\Phi_{15} = P_1 \cdot P_2$ dans $\mathbf{F}_2[X]$.

Exercice 4.7. — Algorithme de Cipolla

Voici un autre procédé pour extraire des racines carrées dans $\mathbf{F}_p$ qui est dû à Cippola. Soit a un carré de $\mathbf{F}_p^*$.

1. Montrer qu'il y a exactement $\frac{p-1}{2}$ éléments $t \in \mathbf{F}_p$ tels que $t^2 - 4a$ ne soit pas un carré dans $\mathbf{F}_p$.
2. Soit t un tel élément de $\mathbf{F}_p$. Considérons l'anneau

$$\mathbf{F}_p[X]/(X^2 - tX + a).$$

   C'est un corps de cardinal p^2. Soit α la classe de X modulo l'idéal $(X^2 - tX + a)$. (On peut aussi prendre pour α une racine carrée de $t^2 - 4a$ dans $\mathbf{F}_{p^2}$.)
   Montrer que l'on a

$$\left(\alpha^{\frac{p+1}{2}}\right)^2 = a.$$

   En particulier, $\alpha^{\frac{p+1}{2}}$ est une racine carrée de a dans $\mathbf{F}_p$.
3. Application : montrer que 5 est un carré dans $\mathbf{F}_{29}$ et déterminer ses racines carrées. On pourra utiliser les deux méthodes précédentes.