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

Racines carrées. Corps finis

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 $\{-1,1\}$.

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 $1 \le m \le q-1$.

Exercice 4.3. — Racines de 2
p désigne 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
$$2 \times 4 \times \cdots (p-1) \pmod p \equiv (-1) \times 2 \times (-3) \times 4 \times \cdots (-\tfrac{p-3}{2}) \tfrac{p-1}{2} \pmod p$$
   (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.

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 $p\equiv 1 \pmod 4$.
   (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 $x'\equiv x \pmod m$ et $y'\equiv y \pmod m$, 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 $p\equiv 3 \mod 4$, montrer que l'on a $x=\pm\, a^{\frac{p+1}{4}}$.
2. Supposons $p\equiv 5 \mod 8$. 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 $x=\pm\, 2a.(4a)^{\frac{p-5}{8}}$ sinon.
3. Le cas où $p\equiv 1 \mod 8$ 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 $\mathbf{F}_p$.

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 $\mathbf{F}_2[X]$.

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.