Le corps $\mathbb{F}_p$.

① Des carrés dans $\mathbb{F}_p$.

Déf: Soit $a \in \mathbb{F}_p$ ou plus généralement à K, un corps.
On dit que a est un carré dans K s'il existe $b \in K$
$a = b^2$, b s'appelle une racine (carrée) de a.
si a n'est pas un carré, a est dit un non-carré.
Les éléments 0 et 1 sont des carrés dans K.

Propriété: Soit p un nombre premier impair, $p \neq 2$.
$a \in \mathbb{F}_p^*$. Si a est un carré, alors a possède deux racines carrés (distinctes), si u est une racine l'autre c'est $-u$.

Preuve: On suppose que $a = u^2$, Soit v une autre racine de a; $a = u^2 = v^2$ ou encore:

$$(u-v)(u+v) = 0 \iff u = v \text{ ou } u = -v.$$

Remarque dans $\mathbb{F}_2$: $u = -u$.

Soit p un nombre premier tq, $p \neq 2$,

et soit $x \in \mathbb{F}_p^*$: $p-1$ est pair, donc

$\frac{p-1}{2}$ est un entier, posons $a = x^{\frac{p-1}{2}}$.

$$a^2 = \left(x^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1. \text{ (Euler).}$$

L'élément a est donc une racine carrée de 1

On conclut donc que $a \in \{-1, 1\}$.

On vient donc de montrer la proposition suivante.

Proposition : p premier, $p \neq 2$; pour tout $x \in \mathbb{F}_p^*$; $x^{\frac{p-1}{2}} = \pm 1$.

Cette proposition va nous permettre de caractériser les carrés et de les compter dans $\mathbb{F}_p$.

Th : Soit p premier, $p \neq 2$.

L'ensemble des carrés dans $\mathbb{F}_p^*$ est un sous-groupe (multiplicatif), qui a $\frac{p-1}{2}$ éléments

dans $\mathbb{F}_p^*$, il y a $\frac{p-1}{2}$ carrés

il y a $\frac{p-1}{2}$ non carrés.

De plus : x est un carré ssi $x^{\frac{p-1}{2}} = 1$

" non carré ssi $x^{\frac{p-1}{2}} = -1$

Remarque : Le produit de deux Carrés (ou de deux non Carrés) est un Carré.

Le produit d'un Carré et d'un non Carré est un non Carré

preuve : On définit l'application $f : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$
$x \longmapsto x^2$

f est un morphisme de groupe multiplicatif [$\mathbb{F}_p^*$ est commutatif]
On note C l'ensemble de carrés de $\mathbb{F}_p^*$.
C est donc égal à $\mathrm{Im} f$, c'est donc un sous-groupe de $\mathbb{F}_p^*$.
$\ker f = \{x,\ x^2 = 1\} = \{-1, 1\}$. Il y a deux éléments
Le nombre de classes d'équivalence de $\mathbb{F}_p^*$ modulo $\ker f$ est égale à $\frac{p-1}{2}$.
Ici on utilise un théorème admis :
$\mathbb{F}_p^*/\ker f$ est isomorphe à $C = \mathrm{Im} f$
On en déduit que ces deux ensembles ont le même Cardinal, donc $|C| = \frac{p-1}{2}$.
Le nombre de ~~nombre~~ non Carré est donc égal à
$$|\mathbb{F}_p^*| - |C| = p-1 - \frac{p-1}{2} = \frac{p-1}{2}$$

Soit $x \in \mathbb{F}_p^*$; si $x \in C$, $\exists u \in \mathbb{F}_p^*$ tel que

$$x = u^2 \; ; \quad x^{\frac{p-1}{2}} = (u^2)^{\frac{p-1}{2}} = u^{p-1} = 1$$

Les éléments de C (les carrés) qui sont en nombre de $\frac{p-1}{2}$ sont les racines du polynôme $X^{\frac{p-1}{2}} - 1$

Ce polynôme est de degré $\frac{p-1}{2}$; il a donc au plus $\frac{p-1}{2}$ racines ; On conclut donc que.

$$x \in C \iff x^{\frac{p-1}{2}} = 1 \; \#.$$

Si x est un non carré ; $x \in \mathbb{F}_p^* - C$;

$x^{\frac{p-1}{2}} = -1$ car $x^{\frac{p-1}{2}} = \pm 1$ pour tout $x \in \mathbb{F}_p^*$,

. si a un carré, b un carré ; $a^{\frac{p-1}{2}} = 1$, $b^{\frac{p-1}{2}} = 1$

donc $(ab)^{\frac{p-1}{2}} = 1$, le reste de la démonstration se fait de cette manière.

Corollaire : Soit p un nombre premier tel que $p \equiv 3 [4]$; Soit $x \in \mathbb{F}_p^*$ un carré,

alors : $x^{\frac{p+1}{4}}$ est une racine carré de x.

Preuve : $\left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p+1}{2}}$

$= x^{\left(1 + \frac{p-1}{2}\right)} = x \cdot \underbrace{x^{\frac{p-1}{2}}}_{=1} = x$

Exemple $p = 19$
$x = 4 = 2^2$
$4^{\frac{5}{4}} = 17 = -2$
racine carré de 4

Exemple : $\mathbb{F}_3$; le groupe des carré ≠ {1}.

• $\mathbb{F}_{13}$, il y a 6 carrés ; $C = \{1, 4, 9, 3, 12, 10\}$.

prenons 4 par exemple ; on devait avoir

$$4^{\frac{13-1}{2}} = 1 :$$

$4^2 = 3$; $4^4 = 9$; $4^6 = 27 = 1\ [13]$.

4 ≠ d'ordre 6. , 4 le groupe C ≠ de cardinal 6 ; donc C ≠ cyclique et 4 ≠ un générateur de ce groupe.

Remarque : pour tout l'ordre de 4 : $\omega(4) \mid 6$

$4 \neq 1$ donc $\omega(4) \in \{2, 3, 6\}$.

$4^2 \neq 1$ $4^2 = 3 \neq 1$, $4^3 = -1 \neq 1$ donc $\omega(4) = 6$.

Théorème : soit p un nombre premier, $p \neq 2$.

-1 ≠ un carré ssi $p \equiv 1\ [4]$

preuve : (-1) ≠ un carré ssi $(-1)^{\frac{p-1}{2}} = 1$

Cette condition signifie que l'entier $\frac{p-1}{2}$ ≠ pair [$p \neq 2$; donc $1 \neq -1$].

$\frac{p-1}{2} = 2k \Rightarrow p = 4k+1$

ou encore. $p \equiv 1\ [4]$.

(15.)

Exemple : $\mathbb{F}_{13}^*$: on a déjà vu que

$C = \{1, 4, 9, 3, 12, 10\}$, $12 = -1 \in C$

et $13 = 4 \times 3 + 1$; $13 \equiv 1 [4]$.

$\mathbb{F}_{11}^*$; -1 n'est pas un carré ; $(-1)^{\frac{11-1}{2}} = (-1)^5 = -1 \neq 1$

Application : on voudrait résoudre une équation du Second degré dans $\mathbb{Z}/p\mathbb{Z}$.

Soit par exemple : $X^2 + 4X - 1 = 0$.

Commençons par résoudre cette équation dans $\mathbb{R}$.

$$X^2 + 4X - 1 = X^2 + 2 \cdot 2X - 1 = X^2 + 2 \cdot 2X + 4 - 4 - 1$$
$$= (X+2)^2 - 5$$

On a utilisé jusqu'à présent que les opérations $+, \times$ et la structure de corps. donc cette méthode peut être utilisée aussi dans $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

On continue dans $\mathbb{R}$.

$$X^2 + 4X - 1 = (X+2)^2 - (\sqrt{5})^2$$
$$= (X + 2 - \sqrt{5})(X + 2 + \sqrt{5}) = 0$$

A qui donne $X = \sqrt{5} - 2$ ou $X = -2 - \sqrt{5}$.

On voit ici qu'on a utilisé dans $\mathbb{R}$: 5 est un carré !

Donc dans $\mathbb{Z}/p\mathbb{Z}$; $X^2 + 4X - 1 = 0$ aura des deux racines si 5 est un carré modulo p ; et 0 racines dans le cas contraire

prenons $p = 11$,

Est-ce que 5 est un carré ? $5^{\frac{p-1}{2}}$

5 est un carré ssi $5^{\frac{p-1}{2}} = 1$ ou encore.

$5^5 = 1$; or $5^2 = 3$; $5^4 = 9 = -2$

$5^5 = -10 = 1$

5 est donc un carré ; il va falloir chercher une racine carrée de 5 modulo 11 :

On calcule les carrés modulo 11 et on trouve :

$4^2 \equiv 16 \equiv 5 \{11\}$.

$x^2 + 4x - 1 = (x+2)^2 - 5 = (x+2)^2 - 4^2$

$= (x+2-4)(x+2+4)$

$= (x-2)(x+6)$.

Les racines sont donc : $x_1 = 2$ et $x_2 = -6 = 5$

dans $\mathbb{Z}/11\mathbb{Z}$.

plus généralement : $x^2 + bx + c$ dans $\mathbb{Z}/p\mathbb{Z}$.

on applique la même méthode :

$x^2 + bx$ correspond au début d'une identité remarquable $(x^2 + 2ax)$ où $a = \frac{b}{2}$: on fait

$a = b\,2^{-1}$

il faut donc trouver l'inverse de 2^{-1} dans $\mathbb{Z}/p\mathbb{Z}$

$i \quad \frac{\sigma}{1+\sigma} = 1 - \sigma$

$$X^2+bX+c = (X+2^{-1}b)^2 - (2^{-1})^2 b^2 + c$$

$$= (X+2^{-1}b)^2 - 4^{-1}(b^2-4c).$$

$$= (X+2^{-1}b)^2 - (2^{-1})^2 \underbrace{(b^2-4c)}_{\Delta}.$$

Remarque dans $\mathbb{R}$; si $\Delta > 0$, on a deux racines, correspond à : Δ est un carré !

si on prend X^2+3X-1 dans $\mathbb{Z}/11\mathbb{Z}$.

$$\Delta = 3^2 - 4(-1) = +2.$$

on veut que 2 n'est pas un carré dans $\mathbb{Z}/11\mathbb{Z}$.

($2^5 = -1$ dans $\mathbb{Z}/11\mathbb{Z}$).

le polynôme X^2+3X-1 n'a pas de solutions dans $\mathbb{Z}/11\mathbb{Z}$.

On va maintenant voir ~~comment on résout une équation du second degré dans $\mathbb{Z}/n\mathbb{Z}$ avec n un premier~~ (sur un exemple). Ce qui se passe dans $\mathbb{Z}/n\mathbb{Z}$ quand n n'est pas premier.

Soit l'équation X^2-4X+3 dans $\mathbb{Z}/6\mathbb{Z}$.

$$X^2-4X+3 = (X-2)^2 - 4 + 3 = (X-2)^2 - 1$$

$= (X-2-1)(X-2+1)$

$= (X-3)(X-1)$.

dnc : $X^2 - 4X + 3 = 0 \iff (X-3)(X-1) = 0$

or : $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre, on ne peut pas dire que $X-3=0$ ou $X-1=0$, il y a peut-être d'autres solutions

il faut dnc chercher les diviseurs de 0 i.e.

$a, b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab=0$ et $a \neq 0$ et $b \neq 0$

ou se ramener à l'equation $(X-2)^2 = 1$; et chercher les $a \in \mathbb{Z}/6\mathbb{Z}$ tel que $a^2 = 1$;

a	0	1	2	3	4	5
a^2	0	1	4	2	4	1

on trouve dnc : $X-2=1$ et $X-2=-1$

ou encore $X=3$ et $X=1$

pour $n=6$, on a deux solutions, en fait on peut avoir plus de racins comme le montre l'exemple $n=12$.

[Ex à faire en TD].