Loi de réciprocité quadratique :

leçons 101 150
121 170
123 190

Théorème :

Soit $p \neq q$ de nombres premiers > 2. Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

où $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \text{ est un carré de } \mathbb{F}_p^* \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$

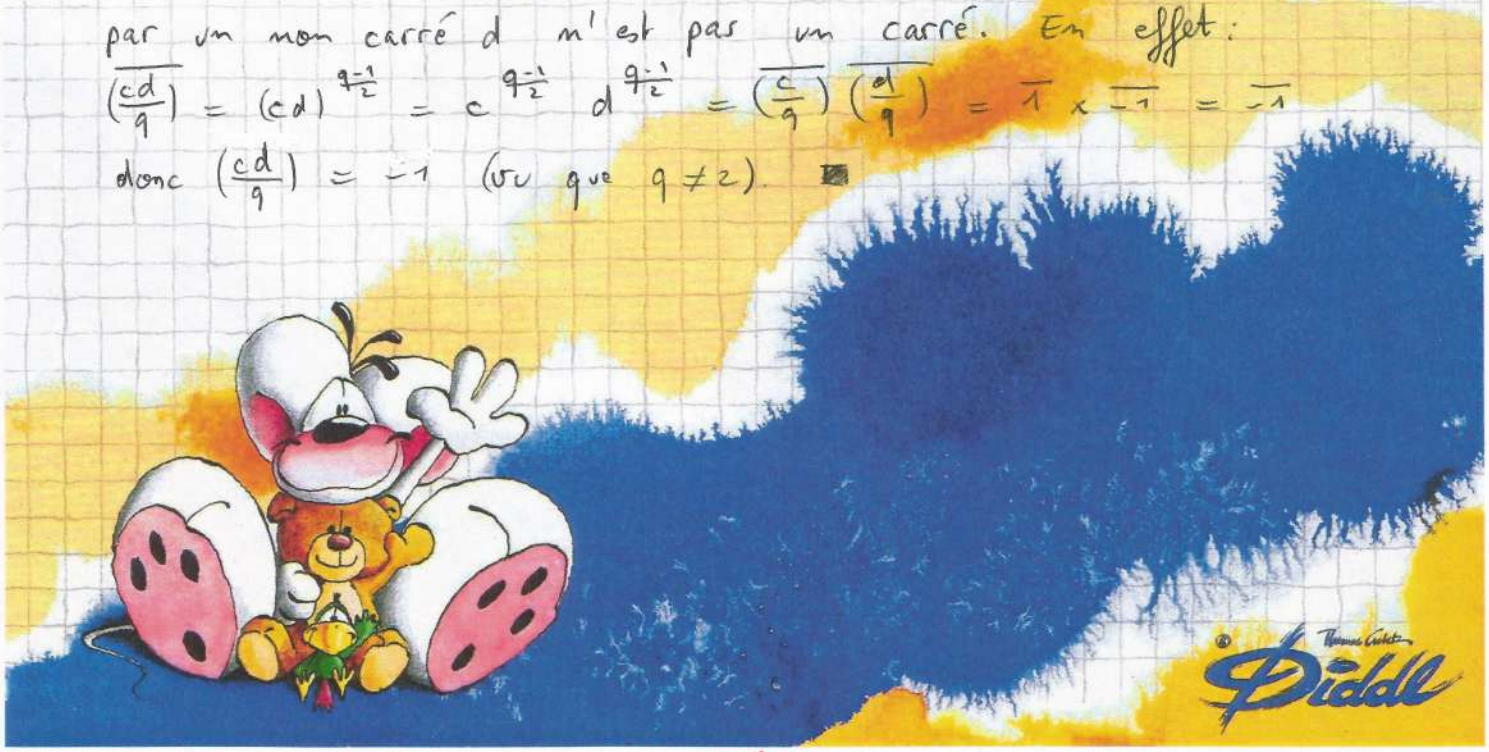
Preuve :

Soit p, q premiers et > 2. Montrons tout d'abord le lemme :

Lemme : Pour $a \in \mathbb{F}_q^*$, on a $\overline{\left(\frac{a}{q}\right)} = a^{\frac{q-1}{2}}$ dans $\mathbb{F}_q^*$
et $\#\{x \in \mathbb{F}_q^* ; ax^2 = 1\} = 1 + \left(\frac{a}{q}\right)$.

Preuve lemme :

- Si a est un carré, $a = b^2$ donc $a^{\frac{q-1}{2}} = b^{q-1} = \overline{1} = \overline{\left(\frac{a}{q}\right)}$
Sinon, comme on a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_p^*$ (en effet, en étudiant $\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*$, $a \mapsto a^2$ qui est un morphisme, de noyau $\{\pm 1\}$, d'image $\mathbb{F}_q^*$. On applique le premier théorème d'isomorphisme donnant $|\mathrm{Im}\,\varphi| = \frac{q-1}{2}$) et que $X^{\frac{q-1}{2}} - 1$ possède $\frac{q-1}{2}$ solutions dans $\mathbb{F}_q^*$, on en déduit que si a n'est pas un carré, alors $a^{\frac{q-1}{2}} = \overline{-1} = \overline{\left(\frac{a}{q}\right)}$.
- Si a est un carré, $a = b^2$ donc $ax^2 = 1 \iff (bx)^2 = 1 \iff x = \pm b^{-1}$ et vu que $q \neq 2$, on a bien deux solutions. Si a n'est pas un carré, il n'y a pas de solution car le produit d'un carré c par un non carré d n'est pas un carré. En effet :
$\overline{\left(\frac{cd}{q}\right)} = (cd)^{\frac{q-1}{2}} = c^{\frac{q-1}{2}} d^{\frac{q-1}{2}} = \overline{\left(\frac{c}{q}\right)}\overline{\left(\frac{d}{q}\right)} = \overline{1} \times \overline{-1} = \overline{-1}$
donc $\left(\frac{cd}{q}\right) = -1$ (vu que $q \neq 2$). ∎



Soit maintenant $X := \{ x = (x_1, \dots, x_p) \in \mathbb{F}_q^p \; ; \; \sum_{i=1}^{p} x_i^2 = 1 \}$. On va dénombrer X de deux manières différentes, modulo p :

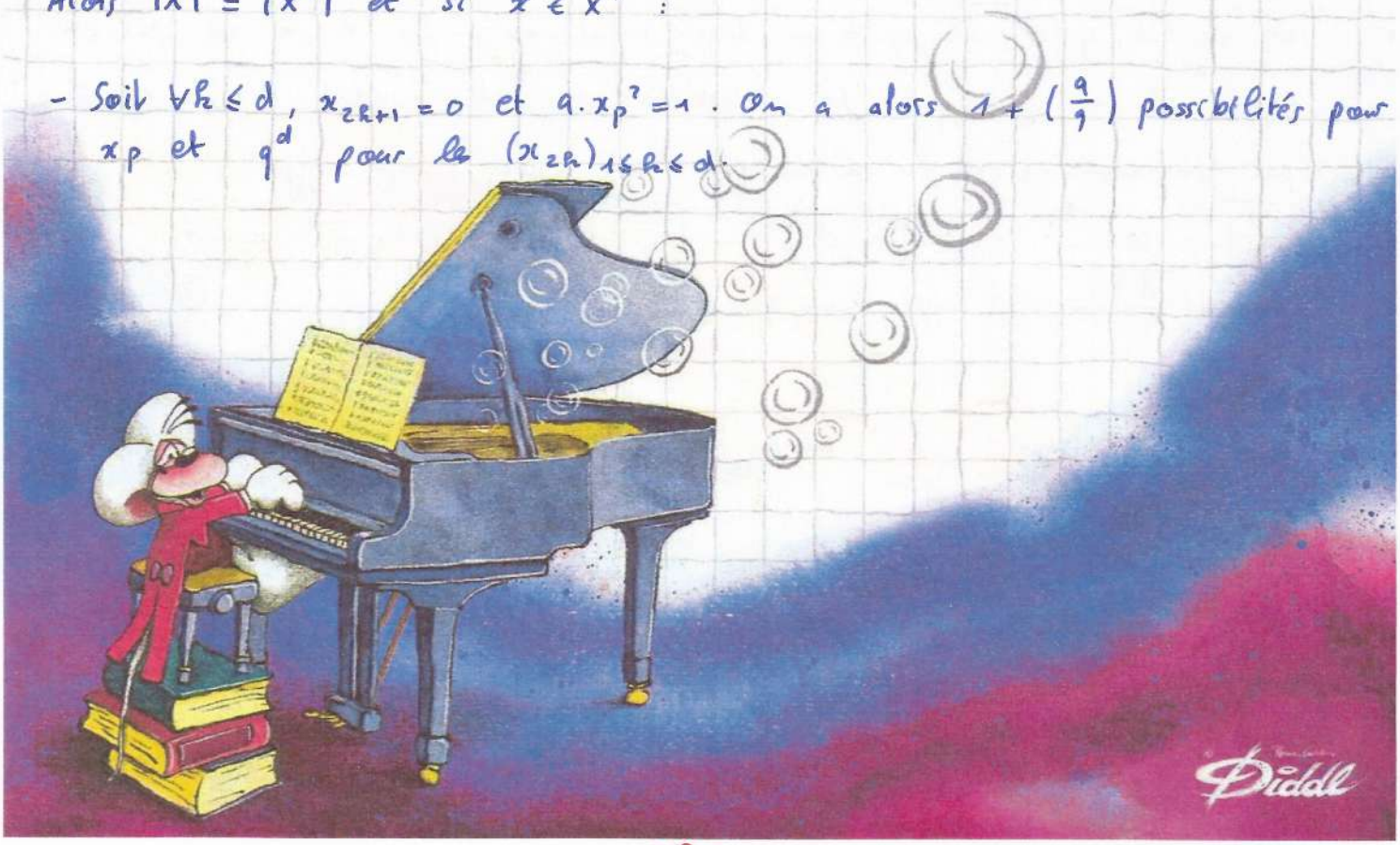
* Considérons d'abord l'action de $\mathbb{F}_p$ sur X définie par $\overline{k} \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$ où les indices sont pris modulo p. Le cardinal de l'orbite d'un élément divise $|\mathbb{F}_p| = p$, donc vaut 1 ou p. En passant modulo p, on a donc
$$|X| \equiv \text{"nombre d'orbites de card 1"} \; [p].$$
Or, l'orbite de x est réduit à lui-même ssi $x_1 = \dots = x_p$. Le nombre de tels x dans X est le nombre de solutions de $p.x_1^2 = 1$, c'est à dire $1 + \left(\frac{p}{q}\right)$ par le lemme. Ainsi, $\boxed{|X| \equiv 1 + \left(\frac{p}{q}\right) \; [p]}$.

* On a $X = \{ x \in \mathbb{F}_q^p \; ; \; f(x) = 1 \}$ où f est la forme quadratique associée à Id_p dans la base canonique. Notons $d = \frac{p-1}{2}$.

Soit $M = \mathrm{diag}(\underbrace{J, \dots, J}_{d \text{ fois}}, a)$ où $J = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ et $a = (-1)^d$
On a $\mathrm{rg}(M) = p$ et $\det(M) = a.(\det J)^d = (-1)^d.(-1)^d = 1$.
La forme quadratique associée à M dans la base canonique est donc non dégénérée, et par classification des formes quadratiques sur $\mathbb{F}_q$, on a f et g congruentes.

Soit $X' = \{ x \in \mathbb{F}_q^p \; ; \; g(x) = 1 \} = \{ x \in \mathbb{F}_q^p \; ; \; 2.\sum_{k=1}^{d} x_{2k} x_{2k-1} + a x_p^2 = 1 \}$
Alors $|X| = |X'|$ et si $x \in X'$:

- Soit $\forall k \leq d$, $x_{2k+1} = 0$ et $a.x_p^2 = 1$. On a alors $1 + \left(\frac{a}{q}\right)$ possibilités pour x_p et q^d pour les $(x_{2k})_{1 \leq k \leq d}$.



- Soit il existe $x_{2k+1} \neq 0$: On choisit les $(x_{2k+1})_{1\leq k\leq d}$ et x_p avec $q\cdot(q^d-1)$ possibilités, puis on choisit les $(x_{2k})_{1\leq k\leq d}$ satisfaisant $2\cdot\sum_{k=1}^{d} x_{2k-1}\cdot x_{2k} = 1 - a\cdot x_p^2$, équation d'un hyperplan affine de cardinal q^{d-1}.

Finalement, $|X| = q^d\left(1+\left(\frac{q}{q}\right)\right) + q^d(q^d-1)$

$= q^d\left(\left(\frac{q}{q}\right) + q^d\right)$

Ainsi par le lemme :

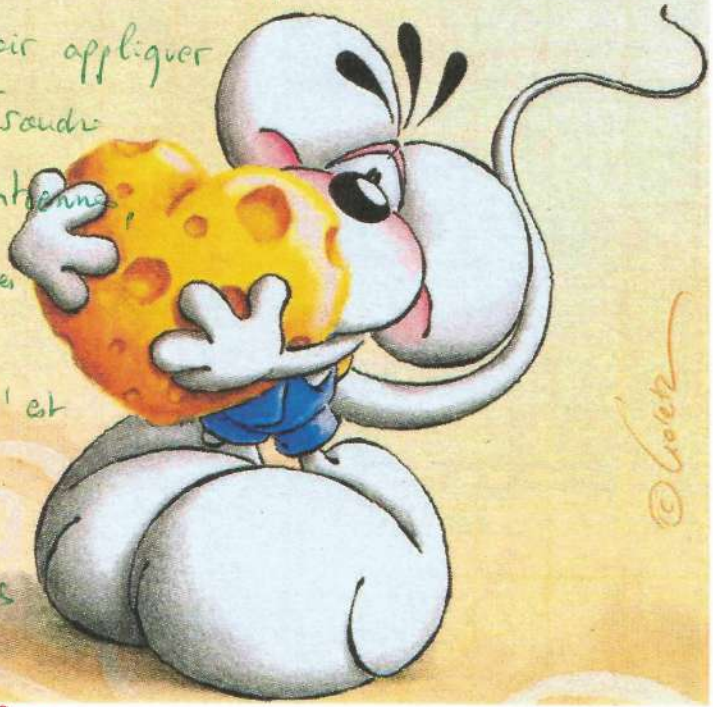
$$1+\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)\left(\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)+\left(\frac{q}{p}\right)\right) \mod p$$

$$\Leftrightarrow \left(\frac{q}{p}\right)+\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right)+\left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}} \mod p$$

$$\Leftrightarrow \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \equiv (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} \mod p$$

p étant >2, on obtient le résultat. ■

Remarque : Connaître le cas où $p=2$. (voir notes).
Il faut aussi savoir appliquer ce théorème pour résoudre des équations diophantiennes, de classifier des formes quadratiques (calcul du déterminant, et voir si c'est un carré). Il faut aussi maîtriser la classification des formes quadratique.



Réciprocité quadratique :

① Introduction : l'utilité des carrés :

On connaît les carrés de $\mathbb{R}$ (ex $x \in \mathbb{R}^+$) ou ceux de $\mathbb{C}$ ($\mathbb{C}$ entier). Mais à quoi cela sert-il ? Un premier thm (thm d'Artin) annonce qu'un corps est ordonnable ssi -1 n'est pas somme de carrés. Sacré Artin.

- **Formes quadratiques :** Le discriminant d'une FQ est définie modulo les carrés (utile pour la classification)

——— k corps commutatif ———

- **Théorie des groupes :** L'étude du groupe quotient $\frac{k^*}{k^{*2}}$ intervient dans l'étude du groupe linéaire comme quotient de $\frac{PGL_2(k)}{PSL_2(k)}$.

- **Groupe orthogonaux :** Soit $\Omega(q)$ le groupe des commutateurs de $O^+(q)$.
  - $\frac{O^+(q)}{\Omega(q)} \simeq \frac{k^*}{k^{*2}}$
  - $-Id \in \Omega(q)$ ssi le discriminant de q est un carré

——— k corps commutatif fini ———

- **En arithmétique :**
  - ax^2+by^2+c, $(a,b,c) \in \mathbb{Z}^3$: On réduit modulo a : $by^2 = c \ [a]$ c'à d $\frac{c}{b}$ carré modulo a.
  - $p = x^2 + dy^2$: d carré modulo p : condition nécessaire

② Généralités sur les carrés de $\mathbb{F}_q$:

1 : $\mathbb{F}_q$ cyclique : **Lemme :** $n = \sum_{d|n} \varphi(d)$

Preuve : On écrit chaque fraction $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$ sous forme irréductible $\frac{k}{d}$ où $d|n$ et $k \wedge d = 1$. Ainsi $\forall d|n$, il y a $\varphi(d)$ fractions. ∎

Thm Tout sous groupe fini de $k^\times$ est cyclique.

Preuve : Soit H sous groupe fini de $k^\times$. H d'ordre n. Soit $x \in H$, $d \mid n$ son ordre.
Alors $\langle x \rangle \cong \mathbb{Z}/d\mathbb{Z}$, et tout élément de $\langle x \rangle$ est d'ordre $\mid d$ donc $y^d = 1$ $\forall y \in \langle x \rangle$. Ainsi $\langle x \rangle$ inclus dans l'ensemble des $x^d - 1 \in k[x]$ (diviseurs).
Par cardinalité, les éléments de $\langle x \rangle$ sont les racines de $X^d - 1$.
Ainsi tous les éléments de H d'ordre d sont dans $\langle x \rangle$.

Ainsi les éléments d'ordre d de H sont $\langle x \rangle$, $\langle x \rangle \cong \mathbb{Z}/d\mathbb{Z}$
donc par le lemme, il y a $\varphi(d)$ éléments d'ordre d dans H.

On a $\sum_{d \mid n} \varphi(d) = n$ et pour $n = \operatorname{card} H$, on a forcément l'existence d'éléments de H tq d'ordre n : il y en a $\varphi(n)$. ∎

2 : Le cas $p = 2$:

- $x \mapsto x^2$ homomorphisme de corps (cas particulier de Frobenius) ★
donc injectif, donc surjectif car $\mathbb{F}_q$ fini, et tout élément de $\mathbb{F}_q$ est un carré (pour $q = 2^n$)

(tout morphisme de corps est injectif : en effet le noyau est un idéal donc trivial)

Frobenius : Soit $\mathbb{F}_p$ le corps à p éléments
- $1^p = 1$
- $(xy)^p = x^p y^p \quad \forall x, y \in A$
- $(x+y)^p =$ binôme de Newton et on est mod p
$= x^p + y^p$

Frobenius $\mathbb{F}_{p^n}$: Soit $\mathbb{F}_q = \mathbb{F}_{p^n}$ de caractéristique $q = p^n$.

$F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ est bien itéré de Frobenius, et aussi
$x \mapsto x^q$ un morphisme de corps !

3: La première suite exacte :

$$1 \to \{\pm 1\} \hookrightarrow \mathbb{F}_q^* \xrightarrow{\gamma} \mathbb{F}_q^{*2} \to 1$$

où γ désigne l'élévation au carré $x \mapsto x^2$.

Alors $\mathbb{F}_q^{*2}$ de card $\frac{q-1}{2}$ et il y a $\frac{q+1}{2}$ carré dans $\mathbb{F}_q$.

4: La deuxième suite exacte :

$$1 \to \mathbb{F}_q^{*2} \hookrightarrow \mathbb{F}_q^* \xrightarrow{\Theta} \{\pm 1\} \to 1$$

où $\Theta(x) = x^{\frac{q-1}{2}}$

Alors si $x \in \mathbb{F}_q^*$, x carré ssi $x^{\frac{q-1}{2}} = 1$

(on peut aussi raisonner de cette manière : $X^{\frac{q-1}{2}} - 1 = 0$ possède max $\frac{q-1}{2}$ racines sur $\mathbb{F}_q$ corps. Par (3), ce sont les carrés. Donc tout non carré x' est par tq $x^{\frac{q-1}{2}} = 1$. Inversement, a carré $\Rightarrow a = b^2 \Rightarrow a^{\frac{q-1}{2}} = b^{q-1} = 1$.

5 : -1 carré dans $\mathbb{F}_q$?

ssi $q \equiv 1 \ [4]$ (réf : Perrin)

6 : 2 carré dans $\mathbb{F}_q$?

ssi, ssi $q \equiv \pm 1 \ [8]$

Preuve :

Lemme : Soit k corps de car $\neq 2$.
Soit ζ racine primitive huitième de l'unité. Alors $(\zeta + \zeta^{-1})^2 = 2$

$(\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2$. On a, $\zeta^8 = 1$ mais $\zeta^4 \neq 1$ donc $\zeta^4 = -1$ i.e. $\zeta^2 = \zeta^{-2}$ (mult par ζ^2). ☐

Conséquence :
2 carré dans k ssi $\zeta + \zeta^{-1} \in k$

Dans notre cas, on pose ζ racine $8^{ième}$ de $\mathbb{F}_{q^2}$: $\zeta \in \mathbb{F}_{q^2}$

[en effet, q impair donc $(q-1)(q+1) = q^2 - 1$ produit de deux pairs consécutifs donc multiple de 8. Comme $\mathbb{F}_{q^2}^*$ cyclique, il contient un élément d'ordre 8, donc ζ.]

Soit $F : x \mapsto x^q$ morphisme de Frobenius.

- Si $q \equiv \pm 1 \ [8]$, $F(\zeta + \zeta^{-1}) = \zeta^q + \zeta^{-q} = \zeta + \zeta^{-1}$. $\zeta + \zeta^{-1}$ fixé par F donc $\in \mathbb{F}_q$. Donc 2 carré
- Si $q \equiv \pm 3 \ [8]$: $F(\zeta + \zeta^{-1}) = \zeta^q + \zeta^{-q} = \zeta^3 + \zeta^{-3}$.
  Si $\zeta^3 + \zeta^{-3} = \zeta + \zeta^{-1}$ alors $\zeta^4 + \zeta^{-2} = \zeta^2 + 1$ $\Rightarrow \zeta$ racine $4^{ième}$ ($\zeta^4 = -1$, $\zeta^{-2} = -\zeta^2$) sauf.

7: Cas spécial $p = q$: Le symbole de Legendre

→ voir des Lois de réciprocité quadratique

Notons que $x \mapsto \left(\frac{x}{p}\right)$ est un morphisme de $\mathbb{F}_p^*$ dans $\{\pm 1\}$

(3) Le (fabuleux) théorème de réciprocité quadratique ♡

Thm: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ (omg !!!)

Autrement dit :

- si p ou q est congru à $1 \bmod 4$, on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$
- si p et q congru à $-1 \bmod 4$, on a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$

exemple de calcul :

$pq = 37$ (premiers tous les deux)

$p = 1987$

$37 \equiv 1 [4]$ donc $\left(\frac{37}{1987}\right) = \left(\frac{1987}{37}\right)$ dans $\mathbb{F}_{37}$, $\overline{1987} = \overline{26}$

$\left(\frac{26}{37}\right)$ ($26 = 2 \times 13$, la multiplicativité se marre par le bonne du bas)

$= \left(\frac{2}{37}\right) \times \left(\frac{13}{37}\right)$

$= (-1) \times \left(\frac{13}{37}\right)$ (2 non carré dans $\mathbb{F}_{37}$ car $37 \equiv -3 [8]$)

$= -\left(\frac{37}{13}\right)$ ($13 \equiv 1 [4]$)

$= -\left(\frac{-2}{13}\right)$

$= -\left(\frac{2}{13}\right)\left(\frac{-1}{13}\right)$

$= -\left(\frac{2}{13}\right)$ (-1 car $13 \equiv 1 [4]$)

et $13 \equiv -3 [8]$ donc $\left(\frac{2}{13}\right) = -1$

donc $\left(\frac{2}{13}\right) = 1$.

Ainsi 37 est un carré modulo 1987. Mais duquel ?

algo bourrin pour la réponse : $632^2 \equiv 37 [1987]$

Application aux équations diophantiennes :

On cherche $p \in \mathbb{P}$ tq $x^2 + 5y^2 = p$.

① Une condition nécessaire est que -5 carré [mod p].

i.e. $\left(\frac{-5}{p}\right) = 1$.

Ainsi on calcule ce symbole :

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{5}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{p}{5}\right)$$

et la condition devient $\left\{p \equiv 1\ [4] \text{ et } p \equiv \pm 1\ [5]\right\}$ ou $\left\{p \equiv -1\ [4] \text{ et } p \equiv \pm 2\ [5]\right\}$

(car les carrés de $\mathbb{Z}/5\mathbb{Z}$ sont : 0 1 2 −2 −2 ; 0 1 −1 −1 −1)

Exercice :

Mq $\left(\frac{101}{641}\right) = -1$

$$\left(\frac{101}{641}\right) = \left(\frac{641}{101}\right) = \left(\frac{35}{101}\right) = \left(\frac{5}{101}\right)\cdot\left(\frac{7}{101}\right)$$

$101 \equiv 1\ [4]$

$$= \left(\frac{101}{5}\right)\cdot\left(\frac{101}{7}\right)$$

$$= \left(\frac{1}{5}\right)\cdot\left(\frac{3}{7}\right) = 1\cdot(-1)$$

$$= -1$$

table carré de 5 : $-2\ -1\ 0\ 1\ 2$; $-1\ 1\ 0\ 1\ -1$

table carré de 7 : $-3\ -2\ -1\ 0\ 1\ 2\ 3$

Exercice

Pour quel nbre premier p la classe de l'entier 7 modulo p est elle un carré ?

- Si $p=2$, 7 carré modulo 2
- Si $p=7$, 7 carré modulo 7
- Soit p premier impair : $\left(\frac{p}{7}\right)\cdot\left(\frac{7}{p}\right) = (-1)^{\frac{p-1}{2}\cdot 3} = (-1)^{\frac{p-1}{2}}$

Ainsi $\left(\frac{7}{p}\right) = 1$ ssi $\begin{cases} \left(\frac{p}{7}\right) = 1 \text{ et } p \equiv 1\ [4] \\ \text{ou} \\ \left(\frac{p}{7}\right) = -1 \text{ et } p \equiv 3\ [4] \end{cases}$ ssi $\begin{cases} p \equiv 1,2,4\ [7] \text{ et } p \equiv 1\ [4] \\ \text{ou} \\ p \equiv 0;3;5;6\ [7] \text{ et } p \equiv 3\ [4] \end{cases}$

carré de $\mathbb{Z}/7\mathbb{Z}$:

0	1	2	3	4	5	6
0	1	4	2	2	4	1

Par le lemme chinois, $\varphi : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \xrightarrow{\simeq} \mathbb{Z}/28\mathbb{Z}$

$$(\bar{a}, \bar{b}) \longmapsto \overline{8a - 7b}$$

Ainsi les conditions précédentes se traduisent par :

$\left(\frac{7}{p}\right) = 1$ ssi $\begin{cases} p \equiv 1, 9, 25 \ [28] \\ \text{ou} \\ p \equiv 3, 19, 27 \ [28] \end{cases}$

ssi $p \equiv 1, 2, 3, 7, 9, 13, 25, 27 \ [28]$

ref: Perrin

Développement: Classification de forme quadratique sur $\mathbb{F}_q$:

Théorème:

Soit $\mathbb{K} = \mathbb{F}_q$ un corps fini tq $\#\mathbb{K} \neq 2$, E un $\mathbb{K}$ ev de dim n. Soit $\alpha \in \mathbb{F}_q^*$ non carré. Il y a deux classes d'équivalence de formes quadratiques non dégénérée sur E, de matrice

$$Q_1 = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \quad \text{et} \quad Q_2 = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \alpha \end{bmatrix}$$

Une forme quadratique Q est de l'un ou l'autre type en fct que son discriminant $\delta(Q)$ soit un carré ou non de $\mathbb{F}_q^*$

Lemme 1:

Il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$

Preuve:

On considère le morphisme $\varphi : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$, $x \longmapsto x^2$

Son image est $\mathbb{F}_q^{*2}$ et son noyau est $\{-1, +1\}$. Ainsi $|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q^*|}{2} = \frac{q-1}{2}$. En particulier, il y a $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ carrés dans $\mathbb{F}_q$. (↑ 0 zéro)

Lemme 2:

L'équation en x et y : $ax^2 + by^2 = 1$ avec $a, b \in \mathbb{F}_q^*$ a des solutions dans $\mathbb{F}_q$

Preuve: On vient de voir qu'il y a $\frac{q+1}{2}$ carrés dans $\mathbb{F}_q$. $\frac{1 - by^2}{a}$ prend donc $\frac{q+1}{2}$ valeurs quand y parcourt $\mathbb{F}_q$, et comme

$$\frac{q+1}{2} + \frac{q+1}{2} > q$$

l'une de ces valeurs est forcément un carré.

Preuve du théorème :

sur $n = \dim E$

On va montrer par récurrence que toute forme quadratique Q sur E a une matrice du type annoncé :

* initialisation :

$n=1$. Soit $e \in \mathbb{F}_q^*$, $Q(e) \neq 0$ puisque Q non dégénérée. On distingue deux cas :

→ si $Q(e) \in \mathbb{F}_q^{*2}$, $\exists \lambda \in \mathbb{F}_q^*$ tq $Q(e) = \lambda^2$, alors $e_1 = \frac{e}{\lambda}$ convient :

$$Q(e_1) = 1$$

→ sinon, alors $Q(e) \notin \mathbb{F}_q^{*2}$. Alors $\exists \lambda \in \mathbb{F}_q^*$ tq $Q(e) = \alpha \lambda^2$ (car $\mathbb{F}_q^{*2}$ d'indice 2 dans $\mathbb{F}_q^*$) et donc $e_1 = \frac{e}{\lambda}$ convient :

$$Q(e_1) = \alpha.$$

* hérédité :

On suppose le résultat vrai au rang n. Montrons le au rang $n+1$. Soit $\{e_1, \dots, e_{n+1}\}$ une base Q-orthogonale de E. Notons $H = \mathrm{Vect}(e_1, e_2)$

$\exists (a,b) \in \mathbb{F}_q^*$ tq $Q_{|H} = \langle a, b \rangle$.

Par le lemme, $ax^2 + by^2 = 1$ admet des solutions dans $\mathbb{F}_q$. Ainsi $\exists \varepsilon_1 \in H$ tq $Q(\varepsilon_1) = 1$. On applique l'hypothèse de récurrence à $H^\perp$: ce qui prouve la récurrence.

Comme α n'est pas un carré, les deux FQ précédentes ne sont pas équivalentes car leurs discriminants ne sont pas égaux modulo les carrés. Donc il y a bien deux classes d'équivalences sur $\mathbb{F}_q$.

Théorème : (Classification générale).

Une forme quadratique Q est caractérisée par son rang et par le discriminant réduit $\overline{\delta(Q)}$ qui est le discriminant de la FQ obtenue en prolongeant E par $\ker(Q)$.

Preuve

Soit Q une forme quadratique sur E de rang n. On note $\overline{\delta(Q)}$ $\varepsilon \in \{1, \alpha\}$

Soit $(e_1, \dots, e_{n-r})$ une base de $\ker(Q)$, soit U un supplémentaire de $\ker(Q)$ dans E. Alors $Q_{|U}$ est non dégénérée et il existe une base B_U de U t.q. $\mathrm{Mat}_{B_U}(Q_{|U}) = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & \varepsilon \end{bmatrix}$.

On obtient la réduite en collant les bases.