Les carrés modulo p ($p \in \mathbb{P}$, $p \geq 3$)

Définition $x \in \mathbb{Z}/p\mathbb{Z}$ est un carré

$\iff \exists y \in \mathbb{Z}/p\mathbb{Z},\ y^2 = x.$

Thm (1) Il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$

(2) x est un carré non nul

$\iff x^{\frac{p-1}{2}} \equiv 1$

(3) -1 est un carré

$\iff p \equiv 1 \ [4]$.

dem (1) $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$

$x \longmapsto x^2$

est un morphisme de groupes.

$\ker \varphi = \{1, -1\}$ donc

$|\mathrm{Im}(\varphi)| = \frac{p-1}{2}$.

$\uparrow$

carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$.

(2) $\mathbb{Z}/p\mathbb{Z}$ est un corps. donc le polynôme $X^{\frac{p-1}{2}} - 1$ possède au plus $\frac{p-1}{2}$ racines. Les carrés non nuls sont racine de $X^{\frac{p-1}{2}} - 1$: $(x^2)^{\frac{p-1}{2}} = x^{p-1}$

$= 1$

(Fermat).

Donc $\{$ racine de $X^{\frac{p-1}{2}} - 1\} = \{$ carrés non nuls $\}$.

(3) -1 est un carré

$\Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2}$ est pair

$\Leftrightarrow p \equiv 1 \ [4]$.

Les cubes modulo p $(p \in \mathbb{P},\ p \geq 3)$

$$\varphi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$
$$x \longmapsto x^3$$

- φ est un morphisme de groupe.
- $\ker \varphi = \{ x \in (\mathbb{Z}/p\mathbb{Z})^* \mid x^3 = 1 \}$.

$|\ker \varphi| \leq 3$.

S'il existe $x \neq 1$ tel que $x^3 = 1$,

alors $\left(\frac{1}{x}\right)^3 = 1$

De plus $x = \frac{1}{x} \iff x^2 = 1$

$\iff x = 1$ ou -1.

Or, $-1 \notin \ker(\varphi)$ DONC $x \neq \frac{1}{x}$

DONC $\ker \varphi = \{1, x, \frac{1}{x}\}$

On a donc $\ker(\varphi) = \{1\}$

ou $|\ker(\varphi)| = 3$.

- Si $\ker \varphi = \{1\}$, $\operatorname{Im} \varphi = (\mathbb{Z}/p\mathbb{Z})^*$

Si $|\ker \varphi| = 3$,

alors $3 \mid p-1$ et $|\operatorname{Im} \varphi| = \frac{p-1}{3}$

• Réciproquement, si $3 \mid p-1$, soit a un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. Posons $b = a^{\frac{p-1}{3}}$

Alors $b \neq 1$ et $b^3 = a^{p-1} = 1$

donc $|\ker \varphi| = 3$.

On a démontré :

Théorème

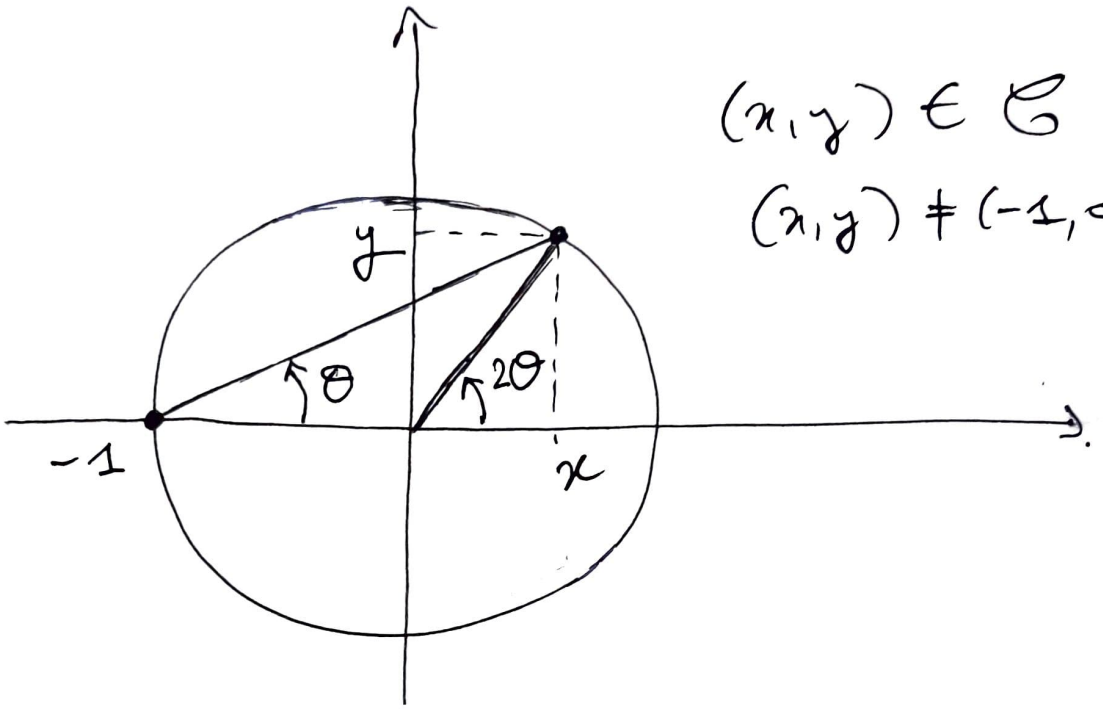
• Si $p \equiv 1 \ [3]$, il y a $\frac{p-1}{3}$ cubes non nuls dans $\mathbb{Z}/p\mathbb{Z}$.

De plus, x est un cube non nul

$$\Leftrightarrow x^{\frac{p-1}{3}} = 1.$$

• Si $p \not\equiv 1 \ [3]$, tout élément de $\mathbb{Z}/p\mathbb{Z}$ est un cube.

Paramétrisation rationnelle du cercle unité



$(x,y) \in \mathcal{C}$

$(x,y) \neq (-1,0)$

Soit $t = \tan(\theta) = \dfrac{y}{x+1}$

$$x = \cos(2\theta) = \frac{\cos^2\theta - \sin^2\theta}{\cos^2\theta + \sin^2\theta} = \frac{1-\tan^2\theta}{1+\tan^2\theta}$$

$$= \frac{1-t^2}{1+t^2}$$

et $$y = \sin(2\theta) = \frac{2\sin\theta\cos\theta}{\cos^2\theta + \sin^2\theta}$$

$$= \frac{2\tan\theta}{1+\tan^2\theta} = \frac{2t}{1+t^2}.$$

Remarque $(x,y) \in \mathcal{C} \cap \mathbb{Q}^2 \iff t \in \mathbb{Q}$.

Tous ces calculs fonctionnent modulo p à condition que $1+t^2 \neq 0$.

Deux cas :

- Si $p \not\equiv 1 \ [4]$, alors -1 n'est pas un carré.

$$\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathcal{C} = \{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 \mid x^2+y^2=1\}$$

$$t \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

$\neq -1$

est injective, à valeurs dans $\mathcal{C} \setminus \{(-1,0)\}$

et $\mathcal{C} \setminus \{(-1,0)\} \longrightarrow \mathbb{Z}/p\mathbb{Z}$

$$(x,y) \longmapsto t = \frac{y}{1+x}$$

est la bijection réciproque.

Conséquence $\operatorname{card} \mathcal{C} = p+1$.

• Si $p \equiv 1 \ [4]$.

Alors -1 est un carré modulo p ; soient α et $-\alpha$ les deux racines carrées de -1.

$$\mathbb{Z}/p\mathbb{Z} \setminus \{-\alpha, \alpha\} \longrightarrow \mathcal{C} \setminus \{(-1,0)\}$$

$$t \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right)$$

est bijective, de bijection réciproque

$$(x,y) \longmapsto t = \frac{y}{x+1}.$$

Et donc :

$$\text{card } \mathcal{C} = p - 1.$$

L'anneau $\mathbb{Z}[i]$.

Rappel $\mathbb{Z}[i] = \{a+ib \mid a,b \in \mathbb{Z}\}$.

$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$ est une

$a+ib \longmapsto a^2+b^2$

application multiplicative :

$$N((a+ib)(\alpha+i\beta)) = N(a+ib)N(\alpha+i\beta)$$

Thm : $\mathbb{Z}[i]$ est un anneau euclidien.

dem si $z_1 \in \mathbb{Z}[i]$, $z_2 \in \mathbb{Z}[i]\setminus\{0\}$

alors $\frac{z_1}{z_2} \in \mathbb{C}$ et il existe

$a+ib \in \mathbb{Z}[i]$ tel que

$$\left| \frac{z_1}{z_2} - (a+ib) \right| \leq \sqrt{2}/2$$

Ecrivons : $z_1 = (a+ib)z_2 + (z_1 - z_2(a+ib))$.

$\in \mathbb{Z}[i]$

et $N(z_1 - z_2(a+ib)) \leq \frac{1}{2} N(z_2)$

$< N(z_2)$ ∎

Conséquence

Dans $\mathbb{Z}[i]$, les éléments irréductibles sont les éléments premiers.

Corollaire. Soit $p \in \mathbb{P}$., $p \geq 3$

Alors $\exists\, a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$

$\Leftrightarrow$ $p \equiv 1 \ [4]$.

dém. • Si $p = a^2 + b^2$, alors

$$a^2 + b^2 \equiv 0 \ [p]$$

$$\left(\frac{a}{b}\right)^2 \equiv -1 \ [p].$$

Donc -1 est un carré

donc $p \equiv 1 \ [4]$

• Si $p \equiv 1 \ [4]$, -1 est un carré modulo p.

Donc $\exists\, x \in \mathbb{Z}$ tel que $p \mid x^2 + 1$

donc $p \mid (x+i)(x-i)$

Or, $p \nmid x+i$ et $p \nmid x-i$

donc p n'est pas premier, donc

p n'est pas irréductible :

$\exists\, z_1, z_2 \in \mathbb{Z}[i]$ tels que

$$p = z_1 \times z_2 \in \mathbb{Z}[i]$$

donc $N(p) = N(z_1)\,N(z_2)$

$$\| \qquad\qquad \|$$

$$p^2 = (a^2+b^2)(c^2+d^2) \in \mathbb{Z}.$$

donc $p = a^2 + b^2$. ∎.