

Démonstration Maths.

+ Exercice

$p \equiv 1 [4]$ est somme de deux carrés.

On veut montrer qu'il existe x entier tel que $x^2 \equiv -1 [p]$.

Quand on divise p par 4, le reste est 1.

Il existe un entier k tel que $p = 4k + 1$.

On distingue les nombres premiers sous deux formes modulo 4.

+ modulo $p \Rightarrow$ un système arithmétique

où deux nombres sont considérés égaux

ont le même reste lorsque on les divise par p .

$a \equiv b [m]$ signifie $a - b$ est divisible par m .

$x^2 + 1 \equiv 0 [p]$ ou encore $p | (x^2 + 1)$

Donc -1 est un résidu quadratique

modulo p .

résidu quadratique : soit p un

nombre premier. Un entier a est un

résidu quadratique ssi a est premier

avec p et qu'il existe x tel que

$x^2 \equiv a [p]$

Formule d'Euler

pour calculer le

symbole de Legendre

Crétore d'Euler :

Pour un nombre premier impair p , le

symbole de Legendre $\left(\frac{a}{p}\right)$ vaut :

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

indique si a est un

carré modulo p ou non

1/4

+1 si a est un résidu quadratique modulo p

-1 sinon

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

Si $p \equiv 1 [4]$, alors $\frac{p-1}{2}$ est pair, donc

Si $p \equiv 3 [4]$, alors $\frac{p-1}{2}$ est impair, donc

Donc si $p \equiv 1 [4]$, -1 est un résidu quadratique modulo p donc il existe x tel que $x^2 \equiv -1 [p]$

Réseau

Un réseau dans $\mathbb{R}^2$ est un ensemble de points de la forme $au + bv$, où u, v sont deux vecteurs linéairement indépendants et $a, b \in \mathbb{Z}$.

Ici on considère le réseau Λ des points $(a, b) \in \mathbb{Z}^2$ tels que :

$$a \equiv 0 [p]$$

2/4

Autrement dit, $a = xp + by$ pour un certain $b \in \mathbb{Z}$

Base du réseau :

On peut montrer que Λ est engendré par les vecteurs :

$$u = (p, 0) \text{ et } v = (0, 1)$$

En effet, tout point $(a, b) \in \Lambda$ s'écrit

$$(a, b) = b(ax, 1) + bp, 0 = (bp + bax, b)$$

avec $b \in \mathbb{Z}$

Volume fondamental

Le volume fondamental du réseau est

$$\det(u, v) = p \times 1 - 0 \times 0 = p$$

Le lemme de Minkowski :

Soit Λ un réseau de $\mathbb{R}^n$ de volume fondamental V , et S un domaine symétrique convexe centré à l'origine.

Si le volume de S est supérieur à $2^n V$, alors S contient un point non nul du réseau.

$S \subset \mathbb{R}^n$ est dit convexe si le segment reliant deux points de S est entièrement contenu dans S .

On prend $S =$ le disque de rayon $\sqrt{2p}$ centré à l'origine.

son aire est $\pi (\sqrt{2p})^2 = 2\pi p$

Le volume fondamental de Λ est p

Comme $2\pi p > 4p$ (car $\pi > 2$), le lemme de Minkowski garantit l'existence d'un point non nul

$(a, b) \in \Lambda$ tel que :

$$a^2 + b^2 < 2p$$

Il existe donc des entiers a, b avec $a \equiv 0 [p]$ et $a^2 + b^2 < 2p$

Calcul modulo p

Puisque $(a, b) \in \Lambda$, on a $a \equiv 0 [p]$ donc :

$$a^2 + b^2 \equiv (0)^2 + b^2 = b^2 (x^2 + 1) \equiv b^2 (1 + 1) \equiv 2b^2 [p]$$

Donc p divise $a^2 + b^2$

On a $0 < a^2 + b^2 < 2p$, et $a^2 + b^2$ est un multiple de p . Le seul multiple de p dans cet intervalle est p lui-même.

Donc $a^2 + b^2 = p$

4/4

