Théorie des Nombres

Table des matières

Introduction

Liste des sujets :

- Sujets classiques, entiers
- Sujets classiques, réels
- L'analyse entre les entiers et les polynômes
- Fonctions génératrices

Équations polynomiales sur les entiers

On va étudier les équations polynomiales sur les entiers :

- $x_1^2 + x_2^2 - x_3^2 = 0$ correspond aux triplets pythagoriciens
- $x_1^k + x_2^k - x_3^k = 0$ est nommée l'équation de Fermat de n'a pas de solutions entières pour $k > 2$
- $y = x^3 + ax + b$ représente les courbes elliptiques

Premiers 'atomes'

Les atomes en Théorie des Nombres sont les nombres premiers : 2,3,5,7... Le problème le plus important des maths les concerne : Combien de nombres premiers sont plus petits que x ?

$$\#\{\text{nb de nombres premiers} \leq x\} = \int_2^x \frac{1}{log(t)} dt + err$$

où l'erreur est une Hypothèse de Riemann.

Les nombres réels

On sait que $\pi \notin \mathbb{Q}$, mais est-ce que $\pi + e \in \mathbb{Q}$?

1 Sujets classiques : les entiers

1.1 Divisibilité

Notations

On note $\mathbb{N} = \{1, 2, 3, ...\}$ et $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$. Pour deux nombres $a, b \in \mathbb{N}$, on écrit $a|b$ et lit 'a divise b' si $\exists c$ tel que $b = a \cdot c$

1.2 Algorithme de division

On sait que pour chaque $a, b \in \mathbb{Z}$ et $b > 0$, $\exists q, r \in \mathbb{Z}$ tel que $a = bq + r$ où $0 \leq r < b$.

1.3 Le plus grand diviseur commun (pgcd)

On dit que d est un diviseur commun de a et b si $d|a$ et $d|b$. Ainsi, $pgcd(a, b)$ est le plus grand diviseur commun de a et b.

Proposition

Soit $d = pgcd(a, b)$. Alors d est le nombre minimal positif écrit sous la forme $d = ax + by$, avec $x, y \in \mathbb{Z}$.

Preuve

Si $D = ax + by > 0$, alors $d|D$ et en particulier $d \leq D$.

Supposons que $D = ax + by > 0$ est minimal. On réécrit $a = Dq + r$ (division euclienne par q où $0 \leq r < D$) et on obtient alors $r = a - Dq = a - axq - byq = a(1 - xq) + b(-yq)$. Puisque D est minimal, alors $r = 0$, c'est à dire que $D|d$. Similairement, on obtient aussi $D|b$.

$\implies D \leq d = pgcd(a, b) \implies D = d$ □

Définition : Nombres premiers entre eux

Si $pgcd(a, b) = 1$, on dit que a et b sont premiers entre eux, c'est à dire qu'ils n'ont pas de diviseurs en commun.

1.4 L'algorithme d'Euclide

Le but de l'algorithme d'Euclide est de trouver le $d = pgcd(a, b)$ sans factoriser.

Supposons que $a > b > 0$.

- $a = bq_1 + r_1$ avec $0 \leq r_1 < b$
- $b = r_1q_2 + r_2$ avec $0 \leq r_2 < r_1$
- $r_1 = r_2q_3 + r_3$ etc.
- $r_{k-2} = r_{k-1}q_k + r_k$
- $r_{k-1} = r_kq_{k+1} + r_{k+1}$ avec $r_{k+1} = 0$. $r_{k+1} = 0$ parce que $r_1 > r_2 > \cdots > r_{k+1} = 0$

Affirmation : $pgcd(a, b) = r_k$

Preuve

Notons que $r_k|a$ et $r_k|b$ parce que $r_k|r_{k-1} \implies r_k|r_{k-2} \cdots$
Chaque diviseur d de a et b divise r_k. Donc on a $d \leq r_k$. Donc $d|a$ et $d|b \implies d|r_1$, $d|r_2$ $\square$

Exemple

$$\begin{aligned} 18 &= 15 \cdot 1 + 3 \\ 15 &= 3 \cdot 5 + 0 \\ &\implies 3 \text{ est le pgcd de 15 et 3} \end{aligned}$$

Proposition : Bachet - Bézout

Soient $a, b, D \in \mathbb{Z}$. L'équation $ax + by = D$ a des solutions dans $x, y \in \mathbb{Z}$ si et seulement si D est un multiple de $pgcd(a, b)$.

Corollaire

Si $pgcd(a, b) = 1$, alors il existe une solution pour tout D.

Remarque

Il est clair que $pgcd(a, b)|D$ est nécessaire.

Preuve du Corollaire par méthode

Trouvons la solution $x, y \in \mathbb{Z}$ à l'équation $22x + 37y = 1$.

$$\begin{aligned} 37 &= 22 \cdot 1 + 15 \\ 22 &= 15 \cdot 1 + 7 \\ 15 &= 7 \cdot 2 + 1 \\ 7 &= 1 \cdot 7 + 0 \end{aligned}$$

Il faut maintenant retrouver la solution x, y à partir de cette méthode.
On remonte notre algorithme :

$$\begin{aligned} 1 &= 15 - 7 \cdot 2 \\ &= 15 - (22 - 15 \cdot 1) \cdot 2 \\ &= (37 - 22) \cdot 1 - (22 - (37 - 22) \cdot 1) \cdot 2 \\ &= 37 \cdot 3 + 22 \cdot (-5) \end{aligned}$$

Donc $\begin{cases} x = -5 \\ y = 3 \end{cases}$ est une solution.

Est-ce qu'il y a d'autres solutions ?

$ax + by = 1$ est une équation linéaire, on a donc une infinité de solution réelles. Mais combien de ces solutions sont des solutions entières ?

Construisons les autres solutions :

Soient $22x_p + 37y_p = 1$ et $22x_H + 37y_H = 0$ des solutions de l'équation homogène. Alors $(x_p + x_H, x_p + y_H)$ est aussi une solution.

Alors $x_p + x_H$ est aussi une solution, $x_H = \frac{-37}{22} y_H$, $x_H = 37k$, $y_H = -22k$ avec $k \in \mathbb{Z}$.

Et donc toutes les solutions sont sous la forme $(-5 + 37k, 3 - 22k)$, $k \in \mathbb{Z}$

Et en général, on peut écrire toutes les autres solutions à partir d'une solution particulière (x, y)

$$\left(x + k \cdot \frac{b}{pgcd(a,b)}, y - k \cdot \frac{a}{pgcd(a,b)} \right)$$

1.5 Théorème fondamental de l'algèbre

Définition : nombres premiers

$p \in \mathbb{N}$ est un nombre premier si $p \neq 1$ et ses seuls diviseurs sont p et 1.

Par exemple, les premiers nombres premiers sont $2, 3, 5, 7, 11$.

Lemme

Si p est premier et $p \,|\, ab$, alors soit $p \,|\, a$, soit $p \,|\, b$, soit p divise a et b.

Preuve du Lemme

Supposons que $p \nmid a$, alors $pgcd(p, a) = 1 \implies \exists x, y$ tel que $px + ay = 1$. On multiplie par b et on obtient $pxb + ayb = b$

Observation triviale : $p \,|\, p$ et $p \,|\, ab \implies p \,|\, b$ □

Thèorème 1. *Théorème fondamental des nombres premiers*

On peut écrire chaque $n \in \mathbb{N}$comme produit de nombres premiers de manière unique :

$$n = p_1^{j_i} \cdot p_2^{j_2} \cdots p_k^{j_k}$$

avec $p_1 < p_2 < \cdots < p_k$

Exemple

$90 = 2 \cdot 3^2 \cdot 5$.

Preuve du Théorème

- Existence

  Soit $n > 1$. On prend p_1 le plus petit diviseur > 1 de n. Évidemment, p_1 est premier. On répète ensuite avec $\frac{n}{p_1}$. Si $\frac{n}{p_1} = 1$, on a fini, sinon on continue. On obtient à la fin un nombre de la forme $p_1^{j-1} \cdot p_2^{j_2} \cdots p_k^{j_k}$

- Unicité

  Supposons que $n = p_1^{j_1} \cdots p_2^{j_2} \cdots p_k^{j_k} = q_1^{i_1} \cdot q_2^{i_2} \cdots q_l^{i_l}$

  Donc si $p_i \,|\, q_1^{i_1} \cdot q_2^{i_2} \cdots q_l^{i_l} \implies p_1 \,|\, q_m \implies p_1 = q_m$ car c'est des nombres premiers. On divise ensuite des deux côtés par $p_1 = q_m$ et on continue le même processus.

  On obtient à la fin que $p_m = q_m$, $j_m = i_m \, \forall m \leq k$

□

1.6 Nombres premiers

Combien y a-t-il de nombres premiers ? Un nombre fini, une infinité ?

Thèorème 2. *Euclide Il y a une infinité de nombres premiers.*

Preuve du Théorème

Supposons qu'il n'existe qu'un nombre fini de nombres premiers et SPDG, disons qu'il y a exactement N nombres premiers. Soient $p_1, \cdots, p_N$ la liste de tous ces N nombres premiers.

Prenons $x = 1 + \prod_{k=1}^{N} p_k$. On remarque que $p_k \nmid x \, \forall 1 \leq k \leq N$. Par le Théorème fondamental de l'algèbre, on sait que x a au moins un diviseur premier, donc il existe un nombre premier $q > p_N$.

□

Questions ouvertes

- $\pi(x) = \#\{p \leq x \,|\, p \text{ premier } \} = \int_2^x \frac{1}{log(t)} dt +$ erreur . Quelle est la taille de l'erreur ? L'hypothèse de Riemann dit que ce nombre devrait être $C \cdot x^{1/2} log(x)$

- Les nombres premiers jumeaux. Deux nombres premiers sont jumeaux si $p_{k+1} - p_k = 2$, par exemple $\{3, 5\}$ ou $\{1000000007, 1000000009\}$ Est-ce qu'il en existe une infinité ?

- $p = n^2 + 1$, y a-t-il une infinité de ces nombres premiers ?

- Conjecture de Goldbach pour $n > 4$, est-ce qu'il existe toujours p, q premiers tels que $n = p + q$? Exemple : $32 = 29 + 3$

2 Fonctions arithmétiques

2.1 Fonctions multiplicatives

Soit $f : \mathbb{N} \to \mathbb{C}$ une fonction.

Définition : fonction multiplicative

On dit que f est multiplicative si $\forall n, m$ tels que $pgcd(n, m) = 1$, alors $f(nm) = f(n) \cdot f(m)$.

Exemples

- $\mathbb{1}(n) = 1 \, \forall n$
- $\delta(n) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$
- $Id(n) = n$
- $f_a(n) = pgcd(a, n)$
- $\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^k & \text{si } n = p_1 p_2 \cdots p_k \text{ où tous les } p_i \text{ sont distints} \\ 0 & \text{si } \exists p \text{ tel que } p^2 \mid n \end{cases}$ La fonction de Möbius.

  $\mu(6) = (-1)^2 = 1$, $\mu(18) = 0$
- $\tau(n) = \#$ diviseurs de $n = \sum_{d \mid n} 1$, par exemple $\tau(p) = 2$ si p est premier.
- $\sigma(n) =$ somme des diviseurs de $n = \sum_{d \mid n} d$. Si p est premier, alors $\sigma(p) = p + 1$. Si $\sigma(n) = n$, on dit que n est un nombre parfait. Par exemple $\sigma(6) = 1 + 2 + 3 = 6$ est un nombre parfait.
- L'indicatrice d'Euler $\phi(n) = \#$ nombre $quisontpremiersavecn$, par exemple $\phi(8) = 4 = \#\{1, 2, 4, 8\}$. $|(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$. Ce n'est pas évident que ϕ est multiplicative.

Convolution de Dirichlet

Soient $f, g : \mathbb{N} \to \mathbb{C}$ deux fonctions.

Définition : Convolution de Dirichlet

$(f * g)(n) = \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right)$ est la convolution de Dirichlet.

Remarque

On peut faire un parallèle avec l'analyse complexe : $(F * G)(x) = \int_{\mathbb{R}} F(t)G(x-t)dt$

Proposition

La convolution de Dirichlet est une opération symétrique, $f*g = g*f$ et associative, $(f*g)*h = f*(g*h)$

Preuve de la Proposition

$(f*g)(n) = \sum_{d\,|\,n} f(d)g\left(\frac{n}{d}\right) = \sum_{d\cdot c=n} f(d)g(c) = \sum_{c\,|\,n} f\left(\frac{n}{c}\right)g(c) = (g*f)(n)$

De manière similaire, $f*(g*h) = \cdots = \sum_{d\cdot c\cdot b=n} f(d)g(c)h(b) = \cdots = (f*g)*h$ □

Remarque

Donc $(\{f : \mathbb{N} \to \mathbb{C}\}, +, *)$ est un anneau.

L'élément neutre pour l'addition est $f \equiv 0$, mais quel est l'élément neutre pour la convolution de Dirichlet ?

$(\delta * f)(n) = \sum_{d\,|\,n} \delta(d) f\left(\frac{n}{d}\right) = \delta(1)f(n) + 0 = f(n)$ car $\delta(d) = 0\,\forall d > 1$

Donc δ est l'élément neutre pour la convolution de Dirichlet.

Exemple

- $\delta * f = f$, OK
- $\tau(n) = \sum_{d\,|\,n} 1 = \mathbb{1} * \mathbb{1}(n)$
- $\sigma(n) = \sum_{d\,|\,n} d = Id * \mathbb{1}(n)$

Remarque

$a(n) \to A(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ séries de Dirichlet.

On a $\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \cdot \sum_{m=1}^{\infty} \frac{b(m)}{m^s} = \sum_{k=1}^{\infty} \frac{(a*b)(k)}{k^s}$

On peut refaire un parallèle à l'analyse complexe : $f(t) \to \hat{F}(w) = \int_{-\infty}^{\infty} f(t)e^{iwt}dt$, $\hat{F}\cdot\hat{G} = \hat{F * G}$

Proposition

Si f et g sont multiplicatives, alors $f * g$ est aussi multiplicative.

Preuve de la Proposition

Soient n, m deux nombres tels que $pgcd(n, m) = 1$. Notons que $c \,|\, nm \implies c = dd'$ avec $d \,|\, n$, $d' \,|\, m$ et $pgcd(d, d') = 1$.

$$\begin{aligned}(f * g)(nm) &= \sum_{c \,|\, mn} f(c) g\left(\frac{mn}{c}\right) \\ &= \sum_{d' \,|\, m} \sum_{d \,|\, n} f(dd') g\left(\frac{nm}{dd'}\right) \\ &= \sum_{d' \,|\, m} \sum_{d \,|\, n} f(d) f(d') g\left(\frac{n}{d}\right) g\left(\frac{m}{d'}\right) \\ &= \sum_{d' \,|\, m} f(d') g\left(\frac{m}{d'}\right) \sum_{d \,|\, n} f(d) g\left(\frac{n}{d}\right) \\ &= (f * g)(m)(f * g)(n)\end{aligned}$$

□

Exemple

$f * \delta = f$, OK

Corollaire

τ et σ sont multiplicatives.

2.2 La fonction de Möbius $\mu(n)$

Exemples

- $\mu(6) = 1$
- $\mu(p) = -1$
- $\mu(4m) = 0$

Proposition

μ est multiplicative.

Preuve de la Proposition

Soit $pgcd(n,m) = 1$
Donc $n = p_1 \cdots p_k$ et $m = q_1 \cdots q_l$ avec $p_i \neq q_j \, \forall i,j$

- Si $a^2|n \implies \mu(n) = 0$
- Si $a^2|mn \implies \mu(m) = 0$
- Si $a^2|mn$, alors soit $a^2|n$, soit $a^2|m \implies \mu(n)$ ou $\mu(m) = 0$. Donc ce $\mu(mn) = 0 = \mu(n)\mu(m)$

Si $a^2 \nmid n \, \forall a$, alors tout p_i et q_j sont distincts. $\mu(n \cdot m) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \mu(n)\mu(m)$

Proposition

$\delta = \mu * \mathbb{1}$

Preuve de la Proposition

$\mu * \mathbb{1}$ est multiplicative d'après notre Proposition précédente. Donc les valeurs de $\mu * \mathbb{1}$ sont déterminées par les valeurs de p^j où p est premier et $j \in \mathbb{N}$. Il suffit donc de vérifier que $\delta(p^j) = (\mu * \mathbb{1})(p^j)$. Mais $\delta(p^j) = 0$ sauf pour $j = 0$. Et on fini par calculer :

$$\begin{aligned}(\mu ast \mathbb{1})(p^j) &= \sum_{p^i \cdot p^{j-i} = p^j} \mu(p^i)\mathbb{1}(p^{j-i}) \\ &= \mu(1) \cdot 1 + \mu(p) \cdot 1 + \mu(p^2) \cdot 1 + \cdots + \mu(p^j) \cdot 1 \\ &= 1 + (-1) + 0 + \cdots + 0 = 0\end{aligned}$$

Donc $\delta = \mu * \mathbb{1}$ □

Thèorème 3. *Formule d'inversion de Möbius Soient* $f : \mathbb{N} \to \mathbb{C}$ *et* $g(n) = \sum_{d \,|\, n} f(d) = f * \mathbb{1}(n)$

Alors $f(n) = \sum_{d \,|\, n} \mu(d) g\left(\frac{n}{d}\right) = (\mu * g)(n)$

Preuve du Théorème

On a $g = f * \mathbb{1}$
Alors $g * \mu = (f * \mathbb{1}) * \mu = f * (\mathbb{1} * \mu) = f * \delta = f$ car $\mathbb{1} * \mu = \delta$

□

2.3 Nombre parfaits

Un exemple de l'usage de $\sigma(n) = \sum_{d \mid n} d$

Définition

On dit que n est parfait si $\sigma(n) = 2n$, autrement dit, $n =$ somme des diviseurs $< n$.

Par exemple, 6, 28 et 496 sont les 3 premiers nombres parfaits.

Pour l'histoire, 6, 28, 496, 8128 étaient déjà connus en 100 après J.C. Euclide a ensuite démontré que tout $2^{p-1}(2^p - 1)$ sont des nombres parfaits quand p et $2^p - 1$ sont premiers.

- $p = 2$, $2^2 - 1 = 3$ et on obtient $2 \cdot 3 = 6$
- $p = 3$, $2^3 - 1 = 7$ et on obtient $2^2 \cdot 7 = 28$
- $p = 5$, $2^5 - 1 = 31$ et on obtient $2^4 \cdot 31 = 496$

Questions ouvertes à propos des nombres parfaits :

- Y a-t-il une infinité de nombres premiers ? On en connait que 51 pour l'instant
- Existe-t-il un nombre parfait impair ?
- On ne sait pas non plus d'il y a une infinité de nombres premiers de Mersenne, donc de la forme $2^p - 1$.

Thèorème 4. *Euclide-Euler*
Soit n pair, alors n est parfait si et seulement si $n = 2^{p-1}(2^p - 1)$ où p et $2^p - 1$ sont premiers.

Preuve du Théorème

[$\Rightarrow$], prouvé par Euclide. Soit $n = 2^{p-1}(2^p - 1)$ et définissons $2^p - 1 = q$ où p et q sont premiers. Alors :

$$\begin{aligned}
\sigma(n) &= 1 + 2 + 4 + \cdots + 2p - 1 + 1 + 2q + 4q + \cdots 2^{p-1}q \\
&= (1 + 2 + \cdots + 2^{p-1})(1 + q) \\
&= \frac{1 - 2^p}{1 - 2}(1 + q) \\
&= (2^p - 1)(1 + q) \\
&= (2^p - 1)(2^p) \\
&= 2 \cdot 2^{p-1}(2^p - 1) = 2n
\end{aligned}$$

[$\Leftarrow$], prouvé par Euler. Soit $n = 2^k \cdot m$ un nombre avec $k > 0$ et m impair. Supposons que $\sigma(n) = 2n$. Donc :

$$\begin{aligned} 2 \cdot 2^k \cdot m &= \sigma(2^k \cdot m) \\ &= \sigma(2^k) \cdot \sigma(m) \\ &= (1 + 2 + 4 + \cdots + 2^k) \cdots \sigma(m) \\ &= (2^{k+1} - 1)\sigma(m) \end{aligned}$$

$\implies (2^{k+1} - 1)\sigma(m) = 2 \cdot 2^k \cdot m \implies \sigma(m) = 2^{k+1} \cdot \dfrac{m}{2^{k+1} - 1}$ $(*)$

$\dfrac{m}{2^{k+1} - 1}$ est forcément entier, notons le l.

- Cas 1 : $l > 1$

  Alors, $1, l$ et m sont des diviseurs distincts et donc $\sigma(m) \leq 1 + l + m$. Mais $l + (2^{k+1} - 1)l = 2^{k+1}l = \sigma(m)$ par $(*)$. Contradiction !

- Cas 2 : $l = 1$

  Alors, $\sigma(m) = 2^{k+1} = (2^{k+1} - 1) + 1 = m + 1$, $\iff m$ est premier de la forme $2^{k+1} - 1$. Donc $n = 2^k(2^{k+1} - 1)$.

  Il faut encore montrer que $k + 1$ doit être premier pour que $2^{k+1} - 1$ soit premier. Montrons que $m \mid n \implies 2^m - 1 \mid 2^n - 1$. Et ça c'est vrai car $(2^{ab} - 1) = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a})$. On prend alors $n = ab$ et $m = a$. Donc $k + 1$ est forcément premier.

3 Congruences

Les congruences sont les calculs avec les restes par un nombre n. On travail alors sur $\mathbb{Z}/n\mathbb{Z}$, qui sont les n différents restes après la division par n.

3.1 Définitions

$m \equiv m' \mod n \iff m - m' = k \cdot n,\ k \in \mathbb{Z}$

Une autre définition est $m \equiv m' \iff [m] = [m']$ dans le groupe $\mathbb{Z}/n\mathbb{Z}$, mais par abus de notation, on écrit juste $m = m'$.

Rappel

$\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n est premier. Les autres corps finis sont $\mathbb{F}_{p^m}$

3.2 Théorème de Fermat et de Euler

Rappelons la fonction indicatrice de Euler : $\phi(n) = \#\{m \leq n \,|\, pgcd(m,n) = 1\}$ = l'ordre du groupe multiplicatif de $\mathbb{Z}/n\mathbb{Z}$, noté $(\mathbb{Z}/n\mathbb{Z})^*$

Thèorème 5. *Petit Théorème de Fermat*

Soit p un premier et $a \in \mathbb{N}$, alors :

$$a^p \equiv a \mod p$$

En particulier, si $pgcd(a,p) = 1$, alors $a^{p-1} \equiv 1 \mod p$

Il y aussi une version plus générale de ce Théorème :

Thèorème 6. *Théorème d'Euler*

Soit $(a,n) = 1$, alors :

$$a^{\phi(n)} \equiv a \mod n$$

Preuve du Théorème d'Euler

$(a,n) = 1 \implies a \in (\mathbb{Z}/n\mathbb{Z})^*$. Par Lagrange, l'ordre de a divise $\phi(n)$, $a^k = 1$ et $\phi(n) = k \cdot l$. Donc $a^{\phi(n)} = (a^k)^l = 1$ □

Le petit Théorème de Fermat est un Corollaire puisque $\phi(p) = p - 1 \implies a^{p-1} \equiv 1 \mod p$ (sauf pour $a \equiv 0 \mod p$).

3.3 Théorème de Wilson

Thèorème 7. *Wilson*

n est premier si et seulement si $(n-1)! \equiv -1 \mod n$

Preuve du Théorème de Wilson

[$\Leftarrow$] Supposons que $n = ab$ avec $1 \leq a < n$, alors $a \in \{1, 2, \cdots, n-1\}$. Donc $a \,|\, (n-1)!$. Puisque $(n-1)! = -1 + k \cdot n$, $k \in \mathbb{Z}$, alors on voit que $a \,|\, -1$ car $a \,|\, n$ (ne pas oublier que $n = ab$). Donc $a = 1 \implies n$ est premier.

[$\Rightarrow$] Pour $n = 2$, $(2-1)! = 1 \equiv 1 \mod 2$ OK

Soit n un nombre premier impair. Alors pour $0 < a < n$, a^{-1} existe.

Notons que $a = a^{-1} \iff a^2 = 1 \iff \begin{cases} a = 1 \mod n \\ a = -1 \mod n \end{cases}$. On peut alors partitionner $\{2, 3, \cdots, n-2\}$ en couples de 2 nombres qui seront l'inverse l'un de l'autre. Alors :

$$\begin{aligned} & 2 \cdot 3 \cdot 4 \cdots 3^{-1} \cdots 2^{-1} \cdots (n-2) \equiv 1 \mod n \\ \implies & (n-1)! \equiv 1 \cdot (2 \cdot 3 \cdots (n-2)) \cdot (n-1) \equiv n-1 \equiv -1 \mod n \end{aligned}$$

□

Question ouverte

Il n'est pas connu pour quels p premier, $(p-1)! \equiv -1 \mod p^2$.

3.4 Équations linéaires mod p

Considérons $ax \equiv b \mod n$, $a, b \in \mathbb{Z}$.

Si $(a, n) = 1$, alors a^{-1} existe dans $\mathbb{Z}/n\mathbb{Z}$ et donc $x = a^{-1}b \mod n$ est l'unique solution.

Proposition

L'équation $ax \equiv b \mod n$, $a, b \in \mathbb{Z}$ a une solution si et seulement si $(a, n) \,|\, b$.

Dans les cas où une solution existe, il y en a exactement (a, n) solutions différentes $\mod n$.

Preuve de la Proposition

[$\Longrightarrow$] Une solution de $ax \equiv b \mod n \implies ax + ny = b$ pour un certain $y \in \mathbb{Z}$.

On observe trivialement alors que $(a, n) \,|\, b$ car $(a, n) \,|\, a$ et $(a, n) \,|\, n$.

[$\Longleftarrow$] Soit $d = (a,n) \,|\, b$. On divise l'équation par d et on obtient $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $n' = \frac{n}{d}$ et $a'x = b' \mod n$

$(a', n') = 1 \implies a'^{-1}$ existe $\implies x = a'^{-1}b'^{-1} \mod n'$

Toute solution à $x = a'^{-1}b'^{-1} + mn'$ pour $m = 0, 1, 2, \cdots$ tel que $m \cdot n' < n$ est une solution à notre équation de base. On a alors (a,n) solutions différentes en tout.

Exemple

$2x \equiv 8 \mod 6$, $(2,6) = 2$

Considérons $x = 4 \mod 3 \implies x = 1 + 3 \cdot m$ pour $m = 0, 1 \mod 6$

Thèorème 8. *Théorème des restes Chinois (trouvé par Suuzi Suanjing, 300 E.C.) Soient $n_1, \cdots, n_k$ nombres premiers entres eux, c'est à dire que $(n_i, n_j) = 1, \forall i \neq j$. Prenons $0 < a_i < n_i \, \forall i$ et définissons $N = \prod_{i=1}^{k} n_i$.*

Alors $\exists! x$, $0 \leq x < N$ tel que :
$$\begin{cases} x \equiv a_1 \mod n_1 \\ x \equiv a_2 \mod n_2 \\ \vdots \\ x \equiv a_k \mod n_k \end{cases}$$

Preuve du Théorème

- Unicité

  Soient x et y deux solutions à notre système. Alors, $x - y \equiv \mod n_i \, \forall i$. Puisque tous les n_i sont premiers entre eux, alors $x - y \equiv 0 \mod N \implies x = y$

- Existence

  Soit $N_j = \frac{N}{n_j}$. On a alors $(N_j, n_j) = 1$. Donc $\exists x_j$ tel que $N_j x_j \equiv a_j \mod n_j$. Prenons alors $x = N_1x_1 + N_2x_2 + \cdots + N_kx_k$ et grâce à $n_j \,|\, N_i \, \forall i \neq j$, on a que $x \equiv N_j x_j \mod n_j \, \forall j$. On a donc créé notre solution.

Remarque

En algèbre, on a vu que si $n = \prod_{i=1}^{k} p_i^{r_i}$, alors $\mathbb{Z}/n\mathbb{Z} \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{r_i}\mathbb{Z}$ comme groupe abélien.

Exemple

Trouver un nombre $x \in \mathbb{Z}$ qui satisfait : $\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 4 \mod 11 \end{cases}$.

On trouve tout d'abord $N = 5 \cdot 7 \cdot 11 = 385$.

$N_1 = 77$,$N_2 = 55$ et $N_3 = 35$. et on veut résoudre $N_1 \equiv 2 \mod 5$, $N_2 \equiv 6 \mod 7$ et $N_3 \equiv 2 \mod 11$,

$$\begin{cases} 2x_1 \equiv 2 \mod 5 & \implies x_1 = 1 \\ 6x_2 \equiv 3 \mod 7 & \implies x_1 = 4 \\ 2x_3 \equiv 4 \mod 11 & \implies x_3 = 2 \end{cases}$$

Et donc en mettant tout ensemble comme dans la preuve de l'existence, on obtient $x = 77 \cdot 1 + 55 \cdot 4 + 35 \cdot 2 = 367 < 385 = N$.

Donc $x = 367$ est une solution de notre système d'équation.

3.5 Équation quadratiques mod p

$$\begin{aligned} x^2 + bx + c &= 0 \\ (x + {}^b\!/_2)^2 &= {}^{b^2}\!/_4 - c \\ x &= -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} - c} \end{aligned}$$

On a la même chose $\mod p$. Pour p premier, ça marche sauf pour $p = 2$. où 2 et 4 n'ont pas d'inverse. Pour les autres nombres premiers, il n'y a que la racine qui pose problème.

Donc on peut réduire le problème à $x^2 \equiv a \mod p$, c'est à dire trouver $\sqrt{a} \in {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$. Comme pour $\mathbb{R}$, cela peut existe ou pas, $\sqrt{2} \in \mathbb{R}$ mais $\sqrt{-2} \notin \mathbb{R}$.

Dans $\mathbb{Z}$, $a \equiv x^2$ si et seulement si $a = p_1^{2n_1} \cdots p_k^{2n_k} = (p_1^{n_1} \cdots p_k^{n_k})^2$. On remarque alors que $\mod p$, c'est plus subtil.

Exemple

Regardons la structure des carrés parfaits modulo 5 :

x	x^2
0	0
1	1
2	4
3	4
4	1

Donc les seuls carrés parfaits $\mod 5$ peuvent être les nombres congrus à 1 ou 4 $\mod 5$. 1 et 4 sont appelés les résidus quadratiques possibles et on note leur ensemble $Q = \{1, 4\}$ (on ne prend par 0) et les non-résidus sont notés $NQ = \{2, 3\}$. On peut alors remarquer que $4 \in Q$ et $\sqrt{4} = 2$ ou $3 = \pm 2$. Mais $2 \in NQ$ et on remarque donc que $\sqrt{2} \notin \mathbb{Z}/5\mathbb{Z}$.

Par contre, si on change de modulo, $\sqrt{3}$ peut existe. Par exemple, $4^2 \equiv 3 \mod 13$ et donc $\sqrt{3}$ existe $\mod 13$.

Thèorème 9. *Théorème de Lagrange*

Soient K un corps et $P(t)$ un polynôme de degré $d \geq 1$. Alors il y a au plus d solutions à $P(t) = 0$.

Exemple

On prend le polynôme $t^2 + 1 \equiv \mod 7$ a 0 solutions. et

- $t^2 + 1 \equiv 0 \mod 7$ a 0 solutions
- $t^2 + 1 \equiv 0 \mod 2$ a 1 solution, 1 et -1 sont le même nombre nombre $\mod 2$.
- $t^2 + 1 \equiv 0 \mod 5$ a 2 solutions, 1 et -1.
- $t^2 + 1 \equiv 0 \mod 8$ a 4 solutions, mais 8 n'est pas premier et donc $\mathbb{Z}/8\mathbb{Z}$ n'est pas un corps et donc, ça ne contredit pas notre théorème.

Symbôle de Legendre

Soit p un nombre premier et $a \in \mathbb{Z}$.

Définition : Symbôle de Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } x^2 \equiv a \mod p \text{ admet une solution} \\ -1 & \text{si } x^2 \equiv a \mod p \text{ n'admet pas de solution} \\ 0 & \text{si } a \equiv 0 \mod p \end{cases}$$

- $\left(\frac{1}{p}\right) = 1$ car $(\pm 1)^2 \equiv 1 \mod p \forall p$
- $\left(\frac{a}{2}\right) = \begin{cases} 1 & \text{si } a \text{ est impair} \\ 0 & \text{si } a \text{ est pair} \end{cases}$

Fait à voir : $a \to \left(\frac{a}{p}\right)$ est une fonction multiplicative.

Thèorème 10. *Réciprocité quadratique de Gauss*
Soient $p \neq q$ deux nombres premiers impairs. Alors :

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

Exemple

Si on nous demande si $x^2 \equiv 3 \mod 97$, c'est long de faire le tableau des congruences de x^2 mod 97. Mais on peut utiliser la réciprocité quadratique.

$$\left(\frac{3}{97}\right)\left(\frac{97}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{97-1}{2}} = (-1)^{48} = 1$$

Donc $\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right)$ et on sait que : $x^2 \equiv 97 \mod 3$ a une solution si et seulement si $x^2 \equiv 3$ mod 97 a une solution.

On voit que $x^2 \equiv 97 \equiv 1 \mod 3$ et donc $x = \pm 1$ est une solution mod 3. Et donc il existe une solution à $x^2 \equiv 3 \mod 97$.

Définition : Résidu quadratique

Si $\left(\frac{a}{p}\right) = +1$, on dit que a est un résidu quadratique mod p. L'ensemble des résidus quadratiques mod p est noté $Q = \left\{a \in \mathbb{Z}/p\mathbb{Z} \mid \left(\frac{a}{p}\right) = +1\right\}$. Le complémentaire, donc les non-résidus mod p sont : $NQ = \left\{a \in \mathbb{Z}/p\mathbb{Z} \mid \left(\frac{a}{p}\right) = -1\right\}$

Donc $\mathbb{Z}/p\mathbb{Z} = Q \cup NQ \cup \{0\}$.

Exemple

$\mathbb{Z}/5\mathbb{Z} = \{1,4\} \cup \{2,3\} \cup \{0\}$.

Exemple

Prenons maintenant $p = 7$. Voici le tableau des carrés :

x	x^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Alors, $Q = \{1, 2, 4\}$ et $NQ = \{3, 5, 6\}$.

Proposition

Pour p premier différent de 2, $|Q| = |NQ| = \frac{p-1}{2}$.

Preuve de la Proposition

Chaque $a \in Q$ a exactement deux racines qui ne se répètent jamais, donc les racines de Q vont prendre au plus toutes les valeurs entre 1 et $p-1$, donc $\pm\sqrt{a} \implies |Q| \leq \frac{p-1}{2}$.

D'autre part, $\phi x \to x^2$ peut prendre la même valeur maximum 2 fois. Donc $|Q| = Im(\phi) \geq \frac{p-1}{2}$. On a toujours au moins $\frac{p-1}{2}$ résultats différents, sinon un résultat serait issu de 3 racines différentes.

$\implies |Q| = |NQ| = \frac{p-1}{2}$.

Proposition

La fonction $n \to \left(\frac{n}{p}\right)$ est une fonction multiplicative, donc $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right)$

Preuve de la Proposition

- Si $a^2 = n$ et $b^2 = m$, alors $(ab)^2 = nm$. Alors $\left(\frac{nm}{p}\right) = +1 = (-1) \cdot (-1) = \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right)$.
- Si $a^{=}n$ et $m \in NQ$ ou inversement. Supposons que $nm = c^2$, alors $m = n^{-1} \cdot c^{-1} = a^{-2}c^2 = (a^{-1}c)^2$. Contradiction, car $m \in NQ$. Donc $mn \in NQ$. Alors, $\left(\frac{nm}{p}\right) = -1 = (+1) \cdot (-1) = \left(\frac{n}{p}\right) \cdot \left(\frac{m}{p}\right)$. Donc $Q \cdot NQ \subset NQ$.
- Rappel : $|Q| = |NQ| = \frac{p-1}{2}$ et $p = 2$ est un cas spécial.

  Si $n \in NQ$. D'après le point précédent, on sait que $n \cdot Q \subset NQ$ Contradiction car $n \cdot Q$ est juste une permutation des éléments de Q. Cela implique que $n \cdot NQ = Q$ car $n \cdot \{1, 2, \cdots, p-1\} = \{1, 2, \cdots, p-1\}$.

Donc $\left(\frac{nm}{p}\right) = 1 = (-1)\cdot(-1) = \left(\frac{n}{p}\right)\cdot\left(\frac{m}{p}\right)$.

□

Le critère d'Euler

Proposition

Soit $p > 2$ premier. $Q = \left\{1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2\right\}$.

Preuve

Ces nombres sont des carrés. La partie qu'il faut vérifier, c'est que deux de ces nombres ne sont pas les mêmes.

On sait que l'on a 2 solutions distinctes à $x^2 = a$ et donc $x = \pm b$ avec $0 < b \leq \frac{p-1}{2}$, alors $-b = p - b \geq p - \frac{p-1}{2} = \frac{p+1}{2} > \frac{p-1}{2}$. Donc pour chaque équation $x^2 = a$, les deux solutions sont dans des moitiés différentes de $0, \cdots, p-1$. Une racine (b) se trouve forcément entre 1^2 et $\left(\frac{p-1}{2}\right)$ et l'autre est forcément entre $\left(\frac{p+1}{2}\right)^2$ et $(p-1)^2$)

Cela nous confirme que $|Q| = \frac{p-1}{2}$.

Exemple

Prenons $p = 5$: $\mathbb{Z}/5\mathbb{Z}$. Alors $\frac{5-1}{2} = 2$. Alors $Q = \{1^2, 2^2\} = \{1, 4\}$.

Proposition : Critère d'Euler

Soit $p > 2$ premier. Alors $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \mod p$.

Preuve de la Proposition

i) Si $a = 0 \mod p$, alors on a 0 des deux côtés.

ii) Si $\left(\frac{a}{p}\right) = 1$, alors $\exists x_a$ tel que $x_a^2 = a$. Alors $a^{\frac{p-1}{2}} = (x_a^2)^{\frac{p-1}{2}} = x_a^{p-1} \equiv 1 \mod p$ d'après le Petit Théorème de Fermat. OK

iii) En général, $a^{p-1} - 1 \equiv 0 \mod p \iff \left(a^{\frac{p-1}{2}} - 1\right)\cdot\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p$ pour p impair.

Donc soit $a^{\frac{p-1}{2}} = 1$, soit $a^{\frac{p-1}{2}} = -1$. Ces équations ont au plus $\frac{p-1}{2}$ solutions d'après le Théorème de Lagrange. Donc par ii) et le fait que $|Q| = \frac{p-1}{2}$, $a^{\frac{p-1}{2}} = 1 \iff a \in Q$.

Donc $a \in NQ \iff a^{\frac{p-1}{2}} = -1 \iff \left(\frac{a}{p}\right) = -1$

□

Corollaire

Pour $a, b \in \mathbb{N}$:

i) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

ii) $\left(\frac{1}{p}\right) = 1$

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

Preuve du Corollaire

i) $\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

ii) évident par la dernière Proposition.

iii) évident par la dernière Proposition.

Lemme de Gauss

Soit $p > 2$ premier. Soit $S = \{1, 2, \cdots, \frac{p-1}{2}\}$. Si $s \in S$ et $a \in \mathbb{Z}/p\mathbb{Z}\backslash\{0\}$, alors on peut écrire $a \cdot s = e_s(a) \cdot s_a$ avec $e_s(a) = \pm 1$ et $s_a \in S$. On peut voir $e_s(a)$ comme la fonction qui associe 1 à a quand $a < \frac{p-1}{2}$ et -1 si a est dans la deuxième partie.

Donc $(\mathbb{Z}/p\mathbb{Z})^* = S \cup (-S)$

Lemme de Gauss (autre)

Pour un nombre premier p impair, on a :

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a)$$

Preuve

$$\begin{aligned} a^{\frac{p-1}{2}} \cdot \prod_{s\in S} s &= \prod_{s\in S} as \\ &= \prod_{s\in S} e_s(a) \cdot s_a \\ &= \left(\prod_{s\in S} e_s(a)\right) \cdot \left(\prod_{s\in S} s_a\right) \\ &= \left(\prod_{s\in S} e_s(a)\right) \cdot \left(\prod_{s\in S} s\right) \end{aligned}$$

La dernière égalité est obtenue parce que les s et s_a sont en bijection et donc on fait le produit sur tout le monde dans les 2 cas.

Donc $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \prod_{s\in S} e_s(a)$. □

Corollaire

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Preuve en exercices.

Preuve de la réciprocité quadratique

Soit $f(m) = sin\left(\frac{2\pi m}{p}\right)$. $f : \mathbb{Z} \to \mathbb{R}$ et même, $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{R}$ car $f(kp+r) = sin\left(\frac{2\pi \cdot (kp+r)}{p}\right) = sin\left(\frac{2\pi r}{p}\right)$.

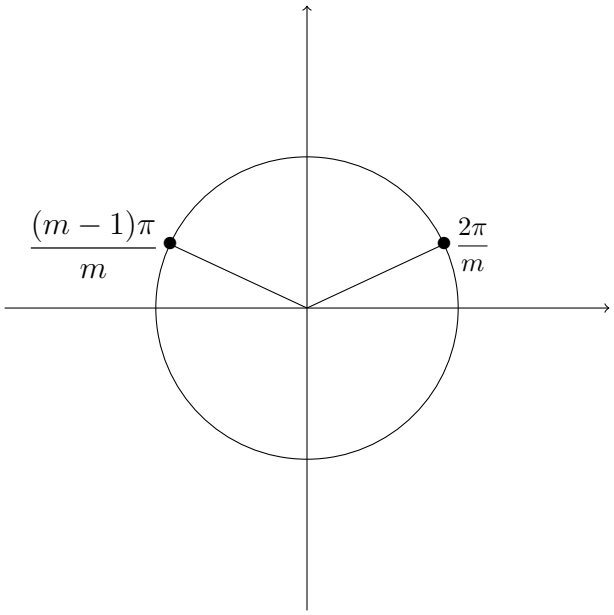
Lemme

Soit $m > 0$ un nombre premier impair. Alors :

$$\frac{sin(mx)}{sin(x)} = (-4)^{\frac{m-1}{2}} \cdot \prod_{1\leq j\leq \frac{m-1}{2}} \left(sin^2(x) - sin^2\left(\frac{2\pi 1}{m}\right)\right)$$

Preuve

On a que $\frac{sin(mx)}{sin(x)} = 0$ quand $x = \frac{2\pi j}{m}$, $1 \leq j \leq \frac{m-1}{2}$. La partie du haut de la fraction sera toujours 0 et le dénominateur sera toujours différent de 0 parce que $sin(x)$ prendra des valeurs > 0 tout le temps parce que x ne passera jamais de l'autre côté du cercle puisque $x < \pi \, \forall j$:



D'autre part,

$$\begin{aligned} sin(mx) &= e^{imx} - e^{-imx}2i \\ &= \frac{1}{2i}\left((cos(x) + i \cdot sin(x))^m - (cos(x) - i \cdot sin(x))\right) \\ &= \sum_{\substack{k=0 \\ k \text{ pair}}}^{m-1} a_k cos(x)^k sin(x)^{m-k} \end{aligned}$$

On peut écrire $cos(x)^k = (1 - sin^2(x))^{\frac{k}{2}}$ car k est pair.

Donc $\frac{sin(mx)}{sin(x)} = \sum_{j=0}^{\frac{m-1}{2}} b_j sin(x)^{2j}$, donc $\frac{sin(mx)}{sin(x)}$ est un polynôme de degré $\frac{m-1}{2}$ en $t = sin^2(x)$.

On a déjà trouvé $\frac{m-1}{2}$ racines distinctes t_j, donc :

$$\implies \frac{sin(mx)}{sin(x)} = c \cdot \prod_{1 \leq j \leq \frac{m-1}{2}} \left(sin^2(x) - sin^2\left(\frac{2\pi j}{m}\right)\right)$$

Pour la constante c :
D'une part, $\frac{sin(mx)}{sin(x)} = \frac{e^{imx} - e^{-imx}}{e^{ix} - e^{-ix}} = \frac{e^{imx} - e^{imx}}{e^{ix}} \cdot \frac{1}{1 - e^{e^{-2ix}}}$

$$= \left(e^{i(m-1)x} - e^{-i(m-1)x}\right)\left(1 + e^{-2ix} + \cdots\right)$$

D'autre part :

$$c \cdot \prod_{1 \leq j \leq \frac{m-1}{2}} \left(\frac{(e^{ix} - e^{-ix})^2}{(2i)^2} - sin^2\left(\frac{2\pi j}{m}\right) \right)$$

$$= x \cdot \left(\frac{e^{2ix \cdot \frac{m-1}{2}}}{(2i)^{2 \cdot \frac{m-1}{2}}} + \cdots \right)$$

$$= \frac{e^{i(m-1)x}}{(-4)^{\frac{m-1}{2}}} \implies c = (-4)^{\frac{m-1}{2}}$$

□

Théorème de Gauss

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

3.6 Preuve du Théorème

$q \cdot s = e_s(q)s_q$.
$sin\left(\frac{2\pi}{p}qs\right) = \frac{2\pi}{p}qs - \frac{1}{3!}\left(\frac{2\pi}{p}\right)^3 (qs)^3 + \frac{1}{5!}\left(\frac{2\pi}{p}\right)^5 (qs)^5 + \cdots = e_s(q) \cdot sin\left(\frac{2\pi}{p}s_q\right)$
Notons que $e_s(q)^n = e_s(q)$ car n est toujours impair.
Par Gauss, on sait que :

$$\left(\frac{q}{p}\right) = \prod_{s \in S} e_s(q)$$

$$= \frac{\prod_{s \in S} sin\left(\frac{2\pi}{p}qs\right)}{\prod_{s \in S} sin\left(\frac{2\pi}{p}s_q\right)}$$

Par bijection, on a :

$$= \frac{\prod_{s \in S} sin\left(\frac{2\pi}{p}qs\right)}{\prod_{s \in S} sin\left(\frac{2\pi}{p}s\right)}$$

Par le Lemme, on continue :

$$= \prod_{s\in S}(-4)^{\frac{q-1}{2}} \prod_{1\leq j\frac{q-1}{2}} \left(sin^2\left(\frac{2\pi}{p}s\right) - sin^2\left(\frac{2\pi j}{q}\right)\right)$$

$$= (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \prod_{\substack{s\in S=\{1,2,\cdots,\frac{p-1}{2}\}\\ t\in T=\{1,2,\cdots,\frac{q-1}{2}\}}} \left(sin^2\left(\frac{2\pi}{p}s\right) - sin^2\left(\frac{2\pi}{q}t\right)\right)$$

On fait le même calcul de l'autre côté avec $\left(\frac{p}{q}\right)$: y a juste les s et les t qui ont changé de place, du coup faut compter les (-1).

$$\left(\frac{p}{q}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \prod_{\substack{s\in S=\{1,2,\cdots,\frac{p-1}{2}\}\\ t\in T=\{1,2,\cdots,\frac{q-1}{2}\}}} \left(sin^2\left(\frac{2\pi}{q}t\right) - sin^2\left(\frac{2\pi}{p}s\right)\right)$$

$$= (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \cdot \prod_{\substack{s\in S=\{1,2,\cdots,\frac{p-1}{2}\}\\ t\in T=\{1,2,\cdots,\frac{q-1}{2}\}}} \left(sin^2\left(\frac{2\pi}{p}s\right) - sin^2\left(\frac{2\pi}{q}t\right)\right)$$

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

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

□

4 Les nombres réels, suite

4.1 Le Théorème de Dirichlet

Par définition de $\mathbb{R}$, chaque $\theta \in \mathbb{R}$ peut être approximé par des rationnels, c'est à dire que θ est dense dans $\mathbb{R}$. Comment 'bien' approximer θ ? On veut $\theta \approx \frac{p}{q}$ avec $pgcd(p,q) = 1$.

Si q est grand, alors c'est facile à faire. $\left|\theta - \frac{p}{q}\right|$ est petit. On dit que q est le coût de notre approximation.

Exemple

$\pi = \frac{25}{8} = 3,125$, mais aussi $\pi \approx \frac{31415}{10000}$.

Méthode efficace par rapport au coût

4.2 Fractions continues

Une fraction continue ressemble à :

$$\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} := [a_0,\, a_1,\, a_2,\, \cdots]$$

Une fraction continue peut avoir un nombre de termes fini ou infini et tous les $a_i \in \mathbb{Z}$.
$x_0 = \theta = \lfloor\theta\rfloor + \{\theta\}$. $x_{j+1} = \frac{1}{x_j - \lfloor x_j\rfloor} = \frac{1}{\{x_j\}}$, $a_j = \lfloor x_j\rfloor$.

Exemple

$\theta = 3,14 = 3 + 0,14 = x_0 \implies a_0 = \lfloor x_0\rfloor = 3$
$x_1 = \frac{1}{\{x_0\}} = \frac{1}{0,14} = \frac{100}{14} = 7,1428 \implies a_1 = \lfloor x_1\rfloor = 7$
$x_2 = \frac{1}{0,1428} = 7 \implies a_2 = 7.$
Alors, $3,14 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}} = 3 + \cfrac{1}{7 + \frac{1}{7}} = 3 + \cfrac{1}{\frac{49+1}{7}} = 3 + \frac{7}{50} = \frac{157}{50} = 3,14$. On a même vérifié que notre fraction continue nous donne le bon résultat.

Proposition

θ rationnel $\iff$ sa représentation par une fraction continue est finie.

Preuve de la Proposition

[$\Longleftarrow$] OK. Si la fraction continue est fini, on va forcément trouver un nombre rationnel à la fin.
[$\Longrightarrow$]

Pour $\theta = \frac{a}{b}$, on applique l'algorithme d'Euclide :

$$\begin{aligned} a = q_1 b + r_1 &\implies \frac{a}{b} = q_1 + \frac{r_1}{b} \\ b = q_2 r_1 + r_2 &\implies \frac{b}{r_1} = q_2 + \frac{r_2}{r_1} \\ r_1 = q_3 r_2 + r_3 &\implies \frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2} \\ &\text{etc.} \end{aligned}$$

$a_j := q_{j+1}$, $\theta = [a_0, a_1, \cdots, a_l]$

Pour $j = l + 1$, $a_j = q_{j+1} + 0$. Il ne nous reste plus de reste, la fraction continue est donc terminée. □

Pour calculer la fraction continue d'un nombre irrationnel, on va appliquer la même méthode, mais celle-ci ne va jamais s'arrêter. La fraction continue sera infinie.

Exemple

- $\frac{1+\sqrt{5}}{2} = [1, 1, 1, 1, \cdots]$ est la fraction continue du nombre d'or.
- $\pi = [3, 7, 15, 1, 242, 1, 1, 2, 1, \cdots]$
- $e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \cdots]$

Erreur de notre approximation

$$\frac{1}{k_n(k_{n+1} + k_n)} < \left|\theta - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}} \text{ où } \frac{h_n}{k_n} = [a_0, a_1, \cdots]$$

Exemple

$\pi \approx [3, 7, 15, 1] = 3 + \dfrac{1}{7 + \dfrac{1}{15 + 1}} = \dfrac{355}{113} \approx 3,1415929$, cela nous donne les 6 premières décimales.

Le principe que l'on veut remarquer est :

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$

En allant vers la droite, c'est relativement facile à approximer, mais revenir vers la gauche, c'est plus dûr.

Thèorème 11. *(Dirichlet 1847)*
Dans ce Théorème, Q est appelé le budget.

Pour tout $\theta \in \mathbb{R}$ et $Q > 1$, il existe $p, q \in \mathbb{Z}$ avec $0 < q < Q$ tel que $|q\theta - p| \leq \frac{1}{Q}$, ce qui est équivalent à $\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q \cdot Q}$

Exemples

- $\theta = 2$ et $Q = 5$. On trouve que $|1 \cdot Q - 2| = 0$
- Si on prend une autre approximation de 2 avec $Q = 5$, on peut prendre $2 \approx \frac{4}{5} \implies |5 \cdot 2 - 11| = 1 > \frac{1}{5}$. C'est une mauvaise approximation.
- $|10000\pi - 31415| \geq 0,9 > \frac{1}{10000}$ C'est une mauvaise approximation.
- Par contre $|113\pi - 355| \approx 0,00001 < \frac{1}{113} < \frac{1}{114}$. On a trouvé une bonne approximation de π.

Preuve du Théorème

On va utiliser le Principe des Tiroirs.

Les tiroirs sont les $\left[\frac{i}{Q}, \frac{i+1}{Q}\right]$ pour $i = 0, \cdots, Q-1$. On a donc Q tiroirs.

On veut placer les nombres $0, 1, \{Q\}, \{2Q\}, \cdots, \{(Q-1)Q\}$ dans $[0, 1]$, ce qui fait $Q+1$ nombres à placer.

Par le principe des tiroirs, $\exists m_1$ et m_2 distincts tels que $|\{m_1\theta\} - \{m_2\theta\}| \leq \frac{1}{Q} \implies n_1$ et n_2 (partie fractionnaire de $m_1 Q$ et $m_2 Q$) tels que $|(n_1 + m_1 Q) - (n_2 + m_2 Q)| \leq \frac{1}{Q}$ que l'on peut réécrire en $|(m_1 - m_2)Q - (n_2 - n_1)| \leq \frac{1}{Q}$.

On note maintenant $q = m_1 - m_2$ et $p = n_2 - n_1$. On remarque que $0 < q < Q$. □

Remarquons que si $\theta \in \mathbb{Z} \implies p\theta - q \in \mathbb{Z}$. Donc soit $q\theta - p = 0$ et on a une approximation exacte, soit $|q\theta - p| \geq 1$ et on a donc une approximation mauvaise.

Corollaire

θ est rationnel $\iff \left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}$ possède un nombre fini de solutions (p, q) avec $pgcd(p, q) = 1$.

θ est irrationnel $\iff \left|\theta - \frac{p}{q}\right| < \frac{1}{q^2}$ possède une infinité de solutions (p, q) avec $pgcd(p, q) = 1$.

Preuve

Soient $\theta = \frac{a}{b}$ et $\frac{p}{q} \neq Q$. Alors $\left|\theta - \frac{p}{q}\right| = \left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|qa - pb|}{bq} \geq \frac{1}{bq} > \frac{1}{q^2}$ en supposant que $q > b$.

On a donc un nombre fini de solutions et plus exactement 0 avec $q > b$. Donc il ne reste plus que les solutions avec $q \leq b$, ce qui donne un nombre fini de solutions.

Soit θ irrationnel, alors $0 < |q_1\theta - p_1| < \frac{1}{Q} \leq \frac{1}{q_1}$ et donc $|q_1\theta - p_1| < \frac{1}{p_1}$. Ces p_1 et q_1 existent par Dirichlet.

Choisissons $Q_2 > \frac{1}{|q_1\theta - p_1|}$. On applique encore Dirichlet et on trouve $p_2, q_2 < Q_2$ tels que $|q_2\theta - p_2| < \frac{1}{Q_2} < |q_1\theta - p_1|$. On remarque qu'on va jamais retrouver une même solution, $(p_2, q_2) \neq (p_1, q_1)$.

Et on peut continuer jusqu'à l'infini : $Q_3 = \frac{1}{|q_2\theta - p_2|}$...

5 Théorème de Liouville

Rappel

Dirichlet $\alpha \in \mathbb{R}\backslash\mathbb{Q} \implies \exists inf\, \frac{p}{q} \in \mathbb{Q}$ tel que $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^2}$

Thèorème 12. *Liouville 1844*
Soit $\alpha \in \mathbb{R}$ un nombre algébrique de degré $d \geq 2$. Alors $\exists$ une constante $C = C(\alpha)$ telle que pour tous les p, q, on a $\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^d}$.

En d'autres termes, si α est algébrique, alors il n'est pas très bien approximable par $\frac{p}{q}$.

Corollaire

$\theta = \sum_{n=1}^{\infty} 10^{-n!} = 0,1100010\ldots010\ldots$ est un nombre transcendant.

Preuve du Corollaire

Soit $p_j = 10^{j!}(10^{-1!} + \cdots + 10^{-j!}) \in \mathbb{Z}$ et $q_j = 10^{j!} \in \mathbb{Z}$. Alors :

$$\begin{aligned}
\left|\theta - \frac{p_j}{q_j}\right| &= 10^{-(j+1)!} + 10^{-(j+2)!} + \cdots \\
&\leq 10^{-(j+1)!}(1 + 10^{-1} + 10^{-2} + \cdots) \\
&= 10^{-(j+1)!}\frac{1}{1 - \frac{1}{10}} \\
&= \frac{10}{9}(10^{-j!})^{j+1} \\
&\leq (10^{-j!})^{j} \\
&= (q_j^{-1})^j = \frac{1}{q_j^j} << \frac{1}{q_j^d}
\end{aligned}$$

Donc Liouville dit que pour tout C et d, θ ne peut pas être algébrique de degré d. Donc θ est forcément transcendant.

Preuve du Théorème

Soit $P(\alpha) \in \mathbb{Z}[\alpha]$ le polynôme minimal de α. Notons $deg(P) = d$. On peut donc écrire $P(\alpha)$ comme : $P(\alpha) = a_d x^d + \cdots a_1 x + a_0$ et $pgcd($ tous les $a_i) = 1$.

Notons que pour $\frac{p}{q} \in \mathbb{Q}$, $P\left(\frac{p}{q}\right) \neq 0$ car P est minimal. Si $\frac{p}{q}$ était une racine de P, alors on pourrait le factoriser par $x - \frac{p}{q}$ et on trouverait un autre polynôme dont le degré serait plus petit. Montrons cela de manière un peu plus concrète :

Supposons que $P\left(\frac{p}{q}\right) = 0$ et notons $\tilde{P}(x) = q^{-d}a_d x^d + \cdots + q^{-1}x + a_0$. Donc $\tilde{P}(p) = P\left(\frac{p}{q}\right) = 0$. Soit $Q(x) = \frac{\tilde{P}(x)}{x-p}$, alors $deg(Q) < deg(P)$ et $Q(q\alpha) =$ car $P(\alpha) = 0$. En plus, $q^d Q \in \mathbb{Z}[\alpha]$ et $q^d Q(q\alpha) = 0 \implies \tilde{Q}(\alpha) = 0$ où $\tilde{Q}(\alpha) = q^d Q(qx)$. Il ne faut pas oublier que $deg(\tilde{Q}) < d$. C'est OK.

Alors $q^d P\left(\frac{p}{q}\right) \in \mathbb{Z}\backslash\{0\}$, donc $\left|q^d P\left(\frac{p}{q}\right)\right| \geq 1$, c'est à dire que $\left|P\left(\frac{p}{q}\right)\right| \geq q^{-d}$.

D'autre part, $\exists \xi \in [\alpha, \frac{p}{q}]$ (ou bien $[\frac{p}{q}, \alpha]$) tel que $P(\alpha) - P\left(\frac{p}{q}\right) = P'(\xi)\left(\alpha - \frac{p}{q}\right)$ par le Théorème des accroissements finis.

$P(\alpha) = 0 \implies \left|P\left(\frac{p}{q}\right)\right| = |P'(\xi)| \cdot \left|\alpha - \frac{p}{q}\right| \leq \underset{\alpha-1 \leq x \leq \alpha+1}{max} |P'(\alpha)| \cdot \left|\alpha - \frac{p}{q}\right|$.

$\implies q^{-d} \leq \left|P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot D \implies \left|\alpha - \frac{p}{q}\right| \geq \frac{D^{-1}}{q^d}$ où $C(\alpha) = D^{-1}$.

□

6 π est transcendant

Rappels d'Algèbre II

- Les nombres algébriques forment un sous-anneau de $\mathbb{C}$.
- Le polynôme $P(x_1, x_2, \cdots, x_n)$ est symétrique si $P(x_1, x_2, \cdots, x_n) = P(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)})$.
- Les polynômes symétriques élémentaires sont : $\prod_{i=1}^{n}(\lambda - x_i) = \lambda^n - e_1(x_1, x_2, \cdots, x_n)\lambda^{n-1} + \cdots + (-1)^n e_n(x_1, x_2, \cdots, x_n)$ où les e_i sont des polynômes symétriques où en particulier $e_n = x_1 x_2 \cdots x_n$ et $e_1 = x_1 + x_2 + \cdots + x_n$.
- Théorème fondamental. Si P est un polynôme symétrique, alors $\exists Q \in \mathbb{Z}[t_1, \cdots, t_n]$ tel que $P(x_1, \cdots, x_n) = Q(e_1(x_1, \cdots, x_n), \cdots, e_n(x_1, \cdots, x_n))$. Voici un exemple :

  $P(x_1, x_2) = x_1^2 + x_2^2$. On a $n = 2$ et P est bien symétrique. On remarque que $P(x_1, x_2) = (x_1 + x_2)^2 - 2x_1x_2 = t_1^2 - 2t_2 = Q(t_1, t_2)$ pour $Q(t_1, t_2) = t_1^2 - 2t_2$.

Lemme

Soient $f(x) = a_m x^m + \cdots + a_0$ avec $a_m \neq 0$ et $deg(f) = m$. Soit $I(t) = \int_0^t e^{t-x} f(x)dx = int_{[0,t]} e^{t-x} f(x)dx$. Alors :

i) $I(t))e^t \sum_{j=0}^{m} f^(j)(0) - \sum_{j=0}^{m} f^{(j)}(t)$

ii) $|I(t)| \leq |t| e^{|t|} \underset{x\in[0,t]}{max} |f(x)|$

Preuve du Lemme

i)

$$I(t) = \int_0^t e^{t-x} f(x)dx$$

On intègre par parties

$$\begin{aligned} &= e^t \left(\left[\frac{e^{-x}}{-1} f(x) \right]_0^t - \int_0^t \frac{e^{-x}}{-1} f'(x)dx \right) \\ &= -f(t) + e^t f(0) - \int_0^t e^{t-x} f'(x)dx \qquad = \cdots \\ &= e^t \left(\sum_{j=0}^{m} f^{(j)}(0) \right) - \sum_{j=0}^{m} f^{(j)}(t) \end{aligned}$$

ii)

$$\begin{aligned}[I(t)] &\leq |t| \max_{x\in[0,t]} |e^{t-x}| \cdot |f(x)| \\ &\leq |t| e^{|t|} \max_{x\in[0,t]} |f(x)|\end{aligned}$$

□

Thèorème 13. *Lindeman 1882*

π est transcendant.

Preuve du Théorème de Lindeman

Supposons par l'absurde que π n'est pas transcendant. C'est donc un nombre algébrique et donc $i\pi$ est un nombre algébrique aussi. Soit g le polynôme minimal de $i\pi$ que l'on note $g(x) = \sum_{j=0}^{d} a_j x^j$ avec $a_j \in \mathbb{Z}$.

Soit $\theta_1 = i\pi$.

Soient $\theta_2, \theta_3, \cdots, \theta_d$ les autres racines. Ces racines sont distinctes (car g est irréductible et que l'on travaille dans $\mathbb{C}$).

Notons que $P := (1+e^{i\theta_1})(1+e^{i\theta_2})\cdots(1+e^{i\theta_d}) = 0$ car $(1+e^{\theta_1}) = (1+e^{i\pi}) = 0$ par la définition de π.

$P = \sum_{\text{tous les choix}} e^{\varepsilon_1\theta_1+\varepsilon_2\theta_2+\cdots+\varepsilon_d\theta_d}$ où $\varepsilon_i = 0$ ou 1, ce qui nous fait 2^d choix au total.

Soient $\alpha_1, \cdots, \alpha_n$ les choix tels que $\sum \varepsilon_i\theta_i \neq 0$.

Puisque $\varepsilon_i = 0\,\forall i$ est un choix possible, alors $n < 2^d$. Donc $P = \left(2^d - n\right)e^0 + e^{\alpha_1} + \cdots + e^{\alpha_n}$

Soit $f(x) = a_j^{np} x^{p-1}(x-a_1)^p \cdots (x-a_n)^p$ où p est un nombre premier assez grand (que l'on peut choisir). $m := deg(f) = (n+1)p - 1$.

Définissons $I(\alpha_i) = \int_0^{\alpha_i} e^{\alpha_i - x} f(x)dx =$ intégration par parties $= e^{\alpha_i - x}\sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(\alpha_i)$.

Alors :

$$\begin{aligned}J &:= I(\alpha_1) + \cdots + I(\alpha_n) \\ &= \sum_{k=1}^{n} e^{\alpha_k} \sum_{j=0}^{m} f^{(j)}(0) - \sum_{k=1}^{n}\sum_{j=0}^{m} f^{(j)}(\alpha_k) \\ &= (n-2^d)\sum_{j=0}^{m} f^{(j)}(0)\end{aligned}$$

$\sum_{k=1}^{n}\sum_{j=0}^{m} f^{(j)}(\alpha_k)$ est un polynôme symétrique en $\alpha_1, \cdots, \alpha_n$ et aussi en $a_d^{\alpha_1}, \cdots, a_d^{\alpha_d}$ car f, et donc $f^{(j)}$ sont tous des polynômes symétriques

Donc $\sum_{k,j} f^{(j)}(\alpha_k) = Q(e_1, \cdots, e_d)$ à coefficients dans $\mathbb{Z}$ et e_i est le i-ème polynôme symétrique élémentaire dans $a_d^{\alpha_1}, \cdots, a_d^{\alpha_d}$. Ces polynômes sont aussi symétriques en $\theta_1, \cdots, \theta_d$ donc ça peut aussi être exprimé en polynômes symétriques élémentaires en θ_i avec coefficients dans $\mathbb{Z}$, mais les polynômes symétriques élémentaires en θ_i sont aussi les coefficients de g, donc des nombres entiers !

$\implies \sum_{k,j} f^{(j)}(\alpha_k) \in \mathbb{Z}$ où on rappelle que $f(x) = a_d^{np} x^{p-1}(x-\alpha_1)^p \cdots (x-\alpha_n)^p$ et donc $J \in \mathbb{Z}$.

Si $j < p$, alors $f^{(j)}(\alpha_k) = 0$ (quand on remplace par α_k dans $f(x)$, alors il restera un facteur 0) et si $j \geq p$, alors $f^{(j)}(\alpha_k)$ est un nombre entier divisible par p !, on ce sera débarrassé de tous les facteurs $(x - \alpha_k)$.

Si $j \geq p$, alors $f^{(j)}(0)$ est un multiple de p.

Si $j < p-1$, alors $f^{(j)}(0) = 0$ parce que l'on aura toujours un facteur x dans f.

Si $j \geq p-1$, alors $f^{(p-1)}(0) = (p-1)!(a_d)^{np}(-1)^{np}(\alpha_1 \cdots \alpha_n)^p$ et il n'est pas p si $p > a_d\alpha_1 \cdots \alpha_n$, il suffit alors de prendre $p > 2^d - n$.

Notons que $p \nmid J$ parce que tous les termes de J sauf 1 sont divisibles par p. $\implies J \neq 0$ et en plus $(p-1)! \mid J$ par notre disjonction de cas d'avant. $\implies |J| \geq (p-1)!$.

D'autre part :

Petit Lemme que l'on va utiliser :

$$\begin{aligned} |I(\alpha_i)| &\leq \int_0^{\alpha_i} \left|e^{\alpha_i - x} f(x)\right| dx \\ &\leq |\alpha_i| \max_x \{e^{\alpha_i - x} f(x)\} \\ &\leq \max_x \left|e^{\alpha_i - x}\right| \max_x |f(x)| \end{aligned}$$

Et $\max_{0 \leq x \leq \alpha_i} |f(x)| \leq \sum_{k=0}^{np-1} |b_k|$ ALLER CHERCHER CETTE LIGNE

$|J| \leq |\alpha_1| \cdot e^{|\alpha_1|} \cdot \underbrace{|f(|\alpha_1|)|}_{\text{de degré } np-1} + \cdots + |\alpha_n| \cdot e^{|\alpha_n|} \cdot |f(|\alpha_n|)|$

Puisque $\{\alpha_1, \cdots, \alpha_n\}$ est fini, $\exists D$ tel que $|f(|\alpha_1|)| \leq D^{np-1}\, \forall i$ et $\exists C$ tel que $\max_i |\alpha_i| e^{|\alpha_1|}$

Et donc $|J| \leq C \cdot D^{np-1}$. En mettant les deux inégalités que l'on a trouvé :

$$(p-1)! \leq |J| \leq C \cdot D^{np-1}\, \forall p \text{ premier, mais } C \text{ et } D \text{ sont finis}$$

Et donc $|J|$ est à la fois borné par $C \cdot D^{np-1}$, mais doit être plus grand que $(p-1)!$, donc quand $p \to \infty$, on a une contradiction.

Donc $i\pi$ est transcendant et donc π aussi. $\square$

7 Applications aux équations diophantiennes

Exemple 1

$x^2 + y^2 = z^2$ a une infinité de solutions. Par exemple tous les triplets de la forme $x = m^2 - n^2$, $y = 2mn$ et $z = m^2 + n^2$ satisfont la première équation.

Exemple 2

$y^2 = x^3 + ax + b$ est l'équation d'une courbe élliptique. C'est utile en cryptographie.

Exemple 3

Thèorème 14. *Grand Théorème de Fermat*

$x^n + y^n = z^n$ *n'a pas de solutions pour* $n \geq 3$. *La preuve a été terminée par Wiles en 1994.*

Quand Anders Karlsson s'est fait contrôlé à la douane, pour justifier qu'il est bien mathématicien on lui a demandé s'il connait le Grand Théorème de Fermat.

Par contre, il n'est pas connu si $x^n + y^k = z^m$ pour $k, n, m \geq 3$ a des solutions ou pas. Ce problème a été posé par Beal.

Exemple 4

Thèorème 15. *Équation de Pell*
$x^2 - dy^2 = 1$, $d \in \mathbb{N}$ *et* $d \neq n^2$ *a une infinité de solutions. On montre cela avec des fractions continues, en particulier la fraction continue de* $\sqrt{d}$.

On va étudier les équations de la forme $x^3 - by^3 = m$. Pour cela, on aura besoin une version plus forte du Théorème de Liouville.

Thèorème 16. *Rath 1955 Soit* $\alpha \in \mathbb{R}$ *un nombre algébrique.*
Alors $\forall \varepsilon > 0$, $\exists C = C(\alpha, \varepsilon)$ *tel que* $\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^{2+\varepsilon}}$ *(on a 2 eu lieu de* α*).*

On ne va pas démontrer ce Théorème.

Exemple 5

C'est un type de problème qui pourrait tomber à l'examen.

Soit l'équation $x^3 - by^3 = m$ avec $m, b \in \mathbb{N}$. Est-ce qu'il y a des solutions $(x, y) \in \mathbb{N}^2$? Et est-ce qu'il y a une infinité de solutions ?

Remarquons que $(a - c)(a^2 + ac + c^2) = a^3 + a^2c - a^2c + ac^2 - ac^2 - c^3 = a^3 - c^3$

$$x^3 - by^3 = m \iff \frac{x^3}{y^3} - b = \frac{m}{y^3}$$
$$\iff \left(\frac{x}{y} - b^{\frac{1}{3}}\right)\left(\frac{x^2}{y^2} + \frac{x}{y}b^{\frac{1}{3}} + b^{\frac{2}{3}}\right) = \frac{m}{y^3}$$

Toute solution (x, y) satisfait $\left|\frac{x}{y} - b^{\frac{1}{3}}\right| \leq \frac{m}{b^{\frac{2}{3}}} \cdot \frac{1}{y^3}$

Mais selon Roth, $\alpha = \sqrt[3]{b}$ et $\varepsilon = \frac{1}{2}$ par exemple on a : $\left|\frac{x}{y} - \sqrt[3]{b}\right| \geq \frac{C}{y^{2+1/2}}$

Et quand $y \to \infty$, on obtient une contradiction puisque $\frac{1}{y^{2+1/2}} \geq \frac{1}{y^3}$. Donc l'équation n'admet que un nombre fini de solutions. □

8 L'analogie entre les entiers et les polynômes

8.1 Introduction

Les entiers sont représentés par $\mathbb{N}$ et $\mathbb{Z}$ et on les opérations $+, -, \times$ et la division Euclidienne : $p = gb + r$. L'équivalent dans les polynômes est $\mathbb{C}[i]$ avec les opérations $+, -, \times$ et la division polynômiale.

Dans les entiers, on a la factorisation en nombres premiers : $p = \prod_{i=1}^{n} p_i^{a_i}$ et de même, on peut factoriser chaque polynôme en de la manière suivante : $P(x) = C \cdot \prod_{i=1}^{n} (x - r_i)^{a_i}$

Toutes ces choses sont assez simples, mais on peut aller bien plus loin dans l'analyse.

8.2 Grand Théorème de Fermat

Thèorème 17. *$x^p + y^p = z^p$ et $p \geq 3$ n'a pas de solutions dans $\mathbb{Z}\backslash\{0\}$*

Quelle analogie peut-on trouver dans les polynômes ?

Pour $p = 1$, on peut prendre $X(t) = t^2+1$, $Y(t) = 5$ et $Z(t) = t^2+6$ et on a $X(t)+Y(t) = Z(t)$. De même pour $p = 2$, on a $(t^2 - 1)^2 + (2t)^2 = (t^2 + 1)^2$

Pour $p \geq 3$, soient $x = x(t)$, $y = y(t)$ et $z = z(t)$ des polynômes qui ne sont pas constants et tous premiers entre eux tels que $x^p + y^p = z^p$.

Comme on utilise les polynômes, on peut utiliser un outil qui n'existe pas dans les entiers : la dérivation. Et en dérivant, on obtient : $p \cdot x^{p-1}x' + p \cdot y^{p-1}y' = p \cdot z^{p-1}z' \implies x^{p-1}x' + y^{p-1}y' = z^{p-1}z'$

$$\begin{aligned} x^p + y^p &= z^p \\ p \cdot x^{p-1}x' + p \cdot y^{p-1}y' &= p \cdot z^{p-1}z' \\ x^{p-1}x' + y^{p-1}y' &= z^{p-1}z' \end{aligned} \tag{1}$$

On prend maintenant $y' \cdot (1) - y \cdot (2)$:

$$\begin{aligned} x^p y' + y^p y' - y x^{p-1}x' - y^p y' &= z^p y' - y z^{p-1} z' \\ x^{p-1}\left(xy' - yx'\right) &= z^{p-1}(zy' - yz') \end{aligned} \tag{2}$$

Puisque $pgcd(x, z) = 1$, alors $x^{p-1} \mid zy' - yz'$.

Soit $zy' = yz'$, soit x^p divise 'vraiment' $zy' - yz'$

- Cas 1 : $zy' = yz'$

  Ce cas là n'est pas possible. Comparons $\left(\frac{y}{z}\right)' = \frac{y'z - z'y}{y^2} = 0$ donc $\frac{y}{z}$ est une constante ce qui contredit $pgcd(y, z) = 1$.

- Cas 2 : x^p divise 'vraiment' $zy' - yz'$

  Alors $(p-1) \cdot deg(x) = deg\,(x^{p-1}) \leq deg(z'y - yz') \leq deg(z) + deg(y) - 1$ et en ajoutant $deg(x)$ de chaque côté, on obtient $p \cdot deg(x) \leq deg(x) + deg(y) + deg(z) - 1$ et notons $A = deg(x) + deg(y) + deg(z)$

  Par symétrie des rôles de x, y et z, on peut juste les permuter et obtenir de la même manière $p \cdot deg(y) \leq A - 1$ et $p \cdot deg(z) \leq A - 1$. En combinant maintenant les 3 inégalités, on obtient $p(deg(x) + deg(y) + deg(z)) \leq 3A - 3 \implies pA \leq 3A - 3 \implies p \leq 2$.

On a donc démontré le Grand Théorème de Fermat pour les polynômes qui s'intitule de la manière suivante :

Thèorème 18. *Pour $p \geq 3$, il n'y a pas de polynômes $x, y, z \in \mathbb{C}[i]$ non-constants et premiers entre eux tels que $x^p + y^p = z^p$.*

8.3 Théorème ABC pour $\mathbb{C}[t]$

La technique de preuve semble être plus générale. Essayons. Soient a, b, c des polynômes dans $\mathbb{C}[t]$ non constants et premiers entre eux tels que $a + b = c$. En prenant la dérivée, on a que $a' + b' = c'$ est vrai aussi. On a alors :

$$\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} c & c' \end{pmatrix} \neq 0_2$$

$Ax = b \iff x = A^{-1}b$. On essaye $\Delta(t) := \begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = \begin{vmatrix} a & c \\ a' & c' \end{vmatrix} = \begin{vmatrix} c & b \\ c' & b' \end{vmatrix}$. On a aussi $\begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = ab' - a'b \neq 0$ car $pgcd(a, b) = 1$.

Supposons que $(t - \alpha)^e \,|\, a$ où e est maximal. Alors :

$$\begin{aligned} &\implies (t-\alpha)^e \,|\, a' \\ &\implies (t-\alpha)^{e-1} \,|\, \Delta(t) \\ &\implies (t-\alpha)^e \,|\, \Delta(t)(t-\alpha) \\ &\implies a(t) \,|\, \Delta(t) \prod_{\substack{\alpha \text{ tel que} \\ a(\alpha)=0}} (t-\alpha) \end{aligned}$$

De même pour b et c

$$\implies a(t)b(t)c(t) \,|\, \Delta(t) \prod_{\substack{\alpha \text{ tel que} \\ abc(\alpha)=0}} (t-\alpha) \,(*)$$

Noter que par les formules de Δ (le Wronksien) :

$$deg(\Delta) = \begin{cases} deg(a) + deg(b) - 1 \\ deg(a) + deg(c) - 1 \\ deg(b) + deg(c) - 1 \end{cases}$$

Donc par $(*)$:

$$deg(abc) \leq deg(\Delta) + \underbrace{deg\left(\prod_{\substack{\alpha \text{ tel que} \\ abc(\alpha)=0}} (t-\alpha)\right)}_{\eta_0(abc)=\#\text{ racines distinctes de } abc}$$

$$\implies deg(a) + deg(b) + deg(c) \leq deg(a) + deg(b) - 1 + \eta_0(abc)$$

$$\implies deg(c) \leq \eta_0(abc) - 1$$

On fait la même chose pour $deg(b)$ et $deg(a)$:

$$\implies deg(b) \leq \eta_0(abc) - 1$$

$$\implies deg(a) \leq \eta_0(abc) - 1$$

On vient alors de démontrer le Théorème suivant :

Thèorème 19. *Mason Statters* $\sim$ 1980

Soient $a, b, c \in \mathbb{C}[t]$ *des polynômes non constants premiers entre eux tels que* $a + b = c$. *Alors :*

$$max\{deg(a), deg(b), deg(c)\} \leq \eta_0(abc) - 1$$

Remarque

C'est assez étonnant puisque $\eta_0(p) \leq deg(p)$. Par exemple, $deg\left((t-2)^{1000}\right) = 1000$ mais $\eta_0\left((t-2)^{1000}\right) = 1$.

Exemples

1) $(t^2-1)^2 + (2t)^2 = (t^2+1)^2$.

   $max(deg) = 4$ et # racines $= 2 + 1 + 2 = 5$. OK

2) $t^n + 1 = t^n + 1$

   $max(deg) = n$ et $\eta_0)1 + 0 + n = n + 1$. OK

3) $16t + (t+1)^3(t-3) = (t+3)(t-1)^3$

$max(deg) = 4$ et $\eta_0 = 1 + 2 + 2 = 5$. OK

Considérons $\underbrace{Ax^k}_{a} + \underbrace{By^m}_{b} = \underbrace{Cz^n}_{c}$ avec $A, B, C \in \mathbb{C}$ et $x, y, z \in \mathbb{C}[t]$ des polynômes non constants premiers entre eux. Alors a, b, c sont aussi non constants et premiers entre eux. Alors :

$$\text{Théorème ABC} \implies \begin{cases} deg\left(Ax^k\right) \leq \eta_0\left(ABCx^k y^m z^n\right) - 1 \\ deg\left(By^m\right) \leq \eta_0\left(ABCx^k y^m z^n\right) - 1 \\ deg\left(Cz^n\right) \leq \eta_0\left(ABCx^k y^m z^n\right) - 1 \end{cases}$$

Notons que :

$$deg(Ax^k) = deg(x)$$
$$\eta_0(Ax^k) = \eta_0(x) \leq deg(x)$$
$$\eta_0(x^k y^m z^n) = \eta_0(x) + \eta_0(y) + \eta_0(z)$$

Car x, y, z sont premiers entre eux et donc :

$$\implies \begin{cases} kdeg(x) \leq deg(x) + deg(y) + deg(z) - 1 \\ mdeg(y) \leq deg(x) + deg(y) + deg(z) - 1 \\ ndeg(z) \leq deg(x) + deg(y) + deg(z) - 1 \end{cases}$$

La somme des inégalités nous donne alors :

$$kdeg(x) + mdeg(y) + ndeg(z) \leq 3\left(deg(x) + deg(y) + deg(z)\right) - 3$$
$$\implies (k-3)deg(x) + (m-3)deg(y) + (n-3)deg(z) \leq -3$$

Puisque $deg(x)$, $deg(y)$, $deg(z) \geq 1$, alors au moins un des $k, m, n \geq 2$.

Corollaire

L'équation $Ax^k + By^m = Cz^n$ avec $A, B, C \in \mathbb{C}$ et $k, m, n \geq 3$ n'a aucune solution dans $\mathbb{C}[t]$ avec x, y, z non constants premiers entre eux.

Remarque

Pour $x, y, z \in \mathbb{Z}\backslash\{0\}$, $x^k + y^m = z^n$ et $k, m, n \geq 3$. Est-ce qu'il y a des solutions ? On ne le sait pas. C'est une question qui donne le prix Beal et $1M\$$

ABC pour les entiers

Le problème pour les entiers, c'est qu'il n'y a pas de dérivée.
Essayons $\frac{d}{dp}(mp^k) = kmp^{k-1}$. Mais ce n'est pas linéaire.

9 L'idée de fonctions génératrices

Le concept de fonctions génératrices en Théorie des nombres et une idée importante.

Fonctions génératrices

On veut étudier les suites de nombres $\{a_n\}_{n=0}^{\infty}$, par exemple les nombres premiers ou les solutions dans $\mathbb{F}_{p^n}$.

Il y a plusieurs manières de définir les fonctions génératrices :

- La manière standard, sous la forme de séries entières : $\sum_{n=0}^{\infty} a_n t^n$
- Fonction génératrice exponentielle : $\sum_{n=0}^{\infty} a_n \frac{t^n}{n!}$
- Séries de Dirichlet : $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$
- Séries génératrices de Dirichlet : $\sum_{n=0}^{\infty} \frac{1}{a_n^s}$
- Séries theta : $\sum_{n=0}^{\infty} e^{-a_n t}$

On étudie cette fonction et grâce à ça on comprend mieux la suite $\{a_n\}$.

Exemple de série importante

$a_n = 1\ \forall n$. Alors $f(t) = \sum_{n=0}^{\infty} 1 \cdot t^n = 1 + t + t^2 + \cdots = \frac{1}{1-t}$ qui est défini pour tout $t \in \mathbb{C}\backslash\{1\}$.

On dit que $\frac{1}{1-t}$ est le prolongement analytique de f, et il est unique !

Pour calculer $f(2)$, on prend juste le prolongement analytique et donc $f(2) = \frac{1}{1-2} = -1$.

Analogie entre le monde discret et les fonctions.

- $\{a_n\} \to f : \mathbb{R} \to \mathbb{R}$
- $a : \mathbb{N}to\mathbb{R}$ avec $a_m = 0$ pour $m < 0$. On associe alors $A(T) = \sum_{n=0}^{\infty} a_n T^n$ et donc le monde des fonctions, cela correspond à $F(w) = \int_{-\infty}^{\infty} f(k) e^{-wt} dt$

- $$\begin{aligned} a_{n-k} \to \sum_{n=0}^{\infty} a_{n-k}T^k &= \sum_{n=k}^{\infty} a_{n-k}T^k \\ &= \sum_{m=0}^{\infty} a_m T^m \\ &= T^k A(T) \end{aligned}$$

  Avec cela, on peut transformer une équation différentielle en une équation algébrique.

  Dans les fonctions, cela correspond à $\frac{d^k}{dt^k}f(t) \to (iw)^k F(w)$. Et comme ça, on transforme une équation algébrique en une équation différentielle.

Exemple de fonction génératrice

Les nombres de Fibonacci sont définis par $\begin{cases} F_0 = 0,\ F_1 = 1 \\ F_n = F_{n-1} + F_{n-2},\ n \geq 2 \end{cases}$. Les premiers nombres de Fibonacci sont $0, 1, 1, 2, 3, 5, 8, 13, 23, \ldots$

Prenons $a_n = F_n$, alors $F(x) = \sum_{n=0}^{\infty} F_n x^n$:

$$\begin{aligned} F(x) &= F_0 + F_1 x + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2})\, T^n \\ &= x + xF + x^2 F \\ \implies F(x) &= \frac{1}{1 - x - x^2} \\ &= \frac{x}{(1-\alpha_1 x)(1-\alpha_2 x)} \end{aligned}$$

avec $\alpha = \frac{1 \pm \sqrt{5}}{2}$

$$\begin{aligned} &= \frac{\frac{1}{\alpha_1 - \alpha_2}}{1 - \alpha_1 x} + \frac{\frac{1}{\alpha_2 - \alpha_1}}{1 - \alpha_2 x} \\ &= \frac{1}{\alpha_1 - \alpha_2} \sum_{n=0}^{\infty} \alpha_1^n x^n + \frac{1}{\alpha_2 - \alpha_1} \sum_{n=0}^{\infty} \alpha_2^n x^n \\ \implies F_n &= \frac{\alpha_1^n}{\alpha_1 - \alpha_2} + \frac{\alpha_2^n}{\alpha_2 - \alpha_1} \\ &= \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n \end{aligned}$$

9.1 Partitions

Soit $n \in \mathbb{N}$ et soit $p(n)$ = nombre de manières d'écrire n comme une somme (pas forcément ordonnée).

Exemple

- $p(0) = 0$
- $p(1) = 1$
- $p(2) = 2 : 2 = 1 + 1$
- $p(3) = 3 : 3 = 2 + 1 = 1 + 1 + 1$
- $p(4) = 5 : 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$
- $p(12) = 77$
- $p(22) = 1002$

Proposition

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty} \frac{1}{1-x^k}$$

Preuve

$$\begin{aligned}\prod_{k=1}^{\infty} \frac{1}{1-x^k} &= \frac{1}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^3} \cdots \\ &= (1 + x + x^2 + \cdots) \cdot (1 + x^2 + x^4 + \cdots) \cdot (1 + x^3 + x^6 + \cdots) \cdots \\ &= 1 + 1 \cdot x + 2 \cdot x^2 + 3 \cdot x^3 + \cdots + p(n)x^n + \cdots\end{aligned}$$

□

Soit $A \subset \mathbb{N}$. Soit $p_A(n) =$ nombre de façons d'écrire n comme somme d'éléments de A.

Exemples

- $A = \{2, 3\}$, alors $p_A(4) = 1$ car $4 = 2 + 2$
- $A = \{$ impairs$\} = \{1, 3, 5, \ldots\}$ $p_{\text{impaire}}(5) = 3$ car $5 = 5 = 3+1+1 = 1+1+1+1+1$ Même preuve : $\sum_{n=0}^{\infty} p_A(k)x^n = \prod_{a \in A} \frac{1}{1-x^a}$

Interprétation :

$$\prod_{k=1}^{\infty}(1 + x^k) = \sum_{n=0}^{\infty} a_n x^n$$

Mais quelle série est-ce que l'on obtient ? Regardons les premiers termes de cette série :

$$\begin{aligned}\prod_{k=1}^{\infty}(1+x^k) &= (1+x)\cdot(1+x^2)\cdot(1+x^3)\cdots \\ &= 1+x+x^2+2x^3+2x^4+3x^5+\cdots\end{aligned}$$

On remarque que l'on ne peut utiliser chaque puissance qu'une seule fois. Alors ici, $a_n = p^{\text{diff}}(n)$ = nombre de manières d'écrire n comme somme de nombres distincts.

Thèorème 20.

$$p^{diff}(n) = p_{impair}(n)\,\forall n$$

Preuve du Théorème

On veut montrer que $\prod_{n=1}^{\infty}\frac{1}{1-x^{2n-1}} = \prod_{n=1}^{\infty}(1+x)^n$

D'une part :

$$\begin{aligned}\prod_{n=1}^{\infty}(1+x^n)\prod_{n=1}^{\infty}(1-x^n) &= \prod_{n=1}^{\infty}(1+x^n)\cdot(1-x^n) \\ &= \prod_{n=1}^{\infty}(1-x^{2n})\end{aligned}$$

D'autre part :

$$\begin{aligned}\prod_{n=1}^{\infty}(1-x^{2n})\prod_{n=1}^{\infty}(1-x^{2n-1}) &= (1-x)(1-x^2)(1-x^3)\cdots \\ &= \prod_{n=1}^{\infty}(1-x^n)\end{aligned}$$

Combinons maintenant ces deux égalités que l'on a obtenu :

$$\begin{aligned}\prod_{n=1}^{\infty}(1-x^{2n}) &= \prod_{n=1}^{\infty}(1+x^n)\prod_{n=1}^{\infty}(1-x^n)\\ &= \prod_{n=1}^{\infty}(1+x^n)\prod_{n=1}^{\infty}(1-x^{2n})\prod_{n=1}^{\infty}(1-x^{2n-1})\\ \Longrightarrow \prod_{n=1}^{\infty}(1+x^n)\prod_{n=1}^{\infty}(1-x^{2n-1}) &= 1\\ \Longrightarrow \prod_{n=1}^{\infty}(1+x^n) &= \frac{1}{\prod_{n=1}^{\infty}(1-x^{2n-1})}\\ &= \prod_{n=1}^{\infty}\frac{1}{1-x^{2n-1}}\end{aligned}$$

□

Un Théorème un peu plus profond :

Thèorème 21. *Théorème d'Euler*

$$\prod_{n=1}^{\infty}(1-x^n) = \sum_{k=-\infty}^{\infty}(-1)^k x^{\frac{k(3k+1)}{2}}$$

Pour remarque cette égalité, Euler a du calculer 50 termes du produit de gauche.

Remarque

On chercher toujours une formule pour $\left(\prod_{n=1}^{\infty}(1-x^n)\right)^k$ pour $k \geq 1$.
Regardons ce que ça donne pour différents k :

- $k = -1$ c'est ce que l'on vient de faire, c'est égal à $\sum_{n=0}^{\infty} p(n)x^n$
- $k = 1$ Euler a trouvé que c'est les nombres pentagonaux
- $k = 3$ Jacobi
- $k = 10$ Winquist
- $k = 24$ Ramanujan

La dimension du groupe de Lie simple

10 Fonctions génératrices

10.1 Formule de sommation de Poisson

Thèorème 22. *Soit $f \in C^2(\mathbb{R})$ telle que $|f(x)|$, $|f'(x)|$ et $|f''(x)| \leq \frac{C}{1+|x|^2}$ pour une certaine constante C. Alors :*

$$\sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} \hat{f}(n) e^{2\pi i n x}$$

et en particulier pour $x = 0$: $\sum_{n=-\infty}^{\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n)$ *où* $\hat{f}(\omega) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i \omega x} dx$

10.2 Preuve du Théorème

Soit $F(x) = \sum_{n=-\infty}^{\infty} f(x+n)$ la périodification. $F(x)$ converge absolument et uniformément grâce aux hypothèses sur f, et donc F est aussi $C^2(\mathbb{R})$. Notons que :

$$F(x+1) = \sum_{n=-\infty}^{\infty} f(x+1+n) = \sum_{m=-\infty}^{\infty} f(x+m) = F(x)$$

donc on peut développer F avec les séries de Fourier, donc $F(x) = \sum_{n=-\infty}^{\infty} \hat{F}(m) e^{2\pi i m x}$ où $\hat{F}(m) = \int_0^1 - \sum_{-\infty}^{\infty} f(x+n) e^{-2\pi i m x} dx$. Regardons plus précisément ce que vaut $\hat{F}(m)$:

$$\begin{aligned}
\hat{F}(m) &= \int_0^1 - \sum_{-\infty}^{\infty} f(x+n) e^{-2\pi i m x} dx \\
&= \sum_{n=-\infty}^{\infty} \int_0^1 f(x+n) e^{-2\pi i m x} dx \\
&= \sum_{n=-\infty}^{\infty} \int_n^{n+1} f(y) e^{-2\pi i m (y-n)} dy \\
&= \sum_{n=-\infty}^{\infty} \int_n^{n+1} f(y) e^{-2\pi i m y} \underbrace{e^{2\pi i m n}}_{1} dy \\
&= \sum_{n=-\infty}^{\infty} \int_n^{n+1} f(y) e^{-2\pi i m y} dy \\
&= \int_{-\infty}^{\infty} f(y) e^{-2\pi i m y} dy = \hat{f}(m)
\end{aligned}$$

Donc $\sum_{n=-\infty}^{\infty} f(x+n) = F(x) = \sum_{m=-\infty}^{\infty} \hat{f}(m) e^{2\pi i m x}$ et si $x = 0$, alors $\sum_{n=-\infty}^{\infty} f(n) = \sum_{m=-\infty}^{\infty} \hat{f}(m)$.

Exemple

$f(x) = \frac{1}{\sqrt{4\pi t}} e^{\frac{-x^2}{4t}}$. On appelle cette fonction la loi Gaussienne, la loi normale ou encore le noyau de chaleur sur $\mathbb{R}$.

Le Théorème de Poissons nous dit que :

$$\frac{1}{\sqrt{4\pi t}} \sum_{n=-\infty}^{\infty} e^{\frac{-n^2}{4t}} = \sum_{n=-\infty}^{\infty} \underbrace{e^{-4\pi^2 n^2 t}}_{(*)}$$

On fait le changement $g(y) = e^{-\pi y^2} \implies \hat{g}(\omega) = e^{-\pi\omega^2}$.
Soit $\Theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi k t^2}$, alors $(*) = \frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right) = \Theta(t)$.

- $(*) \implies \zeta(1-s) \sim \zeta(s)$.
- $(*) \implies$ la loi de réciprocité quadratique. On applique $(*)$ à $t = \varepsilon + i\frac{p}{q}$ et quand $\varepsilon\tau 0$, alors $\frac{1}{t} = \frac{1}{\varepsilon + i\frac{p}{q}} \approx -i\frac{p}{q}$

10.3 La fonction Θ

Soit $\Theta(z,\tau) = \sum_{n=-\infty}^{\infty} e^{2\pi i n^2 \tau} \cdot e^{2\pi i n z}$ avec $z \in \mathbb{C}$ et $\tau \in \mathbb{H} = \{z \in \mathbb{C} \,|\, Im(z) > 0\}$.

Θ est convergente car si $Im(\tau) = t_0 > 0$, alors on remarque que $\left|e^{\pi i n^2 \tau}\right| = e^{\pi n^2 Re(i\tau)} = e^{-\pi n^2 t_0} \tau 0$ très vite.

Proposition

On a :

a) $\Theta(z+1,\tau) = \Theta(z,\tau)$

b) $\Theta(z+\tau,\tau) = \Theta(z,\tau)e^{-\pi i\tau} \cdot e^{-2\pi i z}$

c) Si $z = \frac{1}{2} + \frac{\tau}{2} + n + m\tau$ avec $n, m \in \mathbb{Z}$, alors $\Theta(z,\tau) = 0$

Preuve de la Proposition

a) C'est clair puisque $e^{2\pi i n(z+1)} = e^{2\pi i n z} \cdot \underbrace{e^{2\pi i n}}_{} 1 = e^{2\pi i n z}$

b)

$$\begin{aligned}
\Theta(z+\tau,\tau) &= \sum_{n=-\infty}^{\infty} e^{piin^2 z} \cdot e^{2\pi i n(z+\tau)} \\
&= \sum_{n=-\infty}^{\infty} e^{\pi i(n^2+2n)\tau} \cdot e^{2\pi i n z} \\
&= \sum_{n=-\infty}^{\infty} \left(e^{\pi i(n+1)^2\tau} e^{-\pi i\tau}\right) \cdot \left(e^{2\pi i(n+1)z} e^{-2\pi i z}\right) \\
&\underset{m=n+1}{=} \sum_{n=-\infty}^{\infty} e^{\pi i m^2\tau} e^{2\pi i m z} e^{-\pi i\tau} e^{-2\pi i z} \\
&= \Theta(z,\tau) \cdot e^{-\pi i\tau} e^{-2\pi i z}
\end{aligned}$$

c) En connaissant les propriétés a) et b), il suffit de vérifier que $\Theta\left(\frac{1}{2}+\frac{\tau}{2},\tau\right) = 0$:

$$\Theta\left(\frac{1}{2}+\frac{\tau}{2},\tau\right) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2\tau} e^{2\pi i n\left(\frac{1}{2}+\frac{\tau}{2}\right)}$$

On a que $e^{\pi i} = -1$ et on sépare le n^2 en deux parties

$$= \sum_{n=-\infty}^{\infty} (-1)^n e^{\pi i(n^2+n)\tau}$$

Pour $n \geq 0$ on a $(-1)^n e^{\pi i(n^2+n)\tau}$, $n = 0,1,2,3,\cdots$ Pour $n < 0$, on change de variable : $n = -m-1$ avec $m \geq 0$. Et donc quand $m = 0,1,2,3,\cdots$, alors $n = -1,-2,-3,-4,\cdots$. Regardons ce que ça donne avec m :

$$\begin{aligned}
(-1)^{m-1} e^{\pi i\left((-m-1)^2-m-1\right)\tau} &= -(-1)^m \cdot e^{\pi i\left(m^2+2m+1-m-1\right)\tau} \\
&= -(-1)^m \cdot e^{\pi i\left(m^2+m\right)\tau}
\end{aligned}$$

Donc ces termes d'annulent deux à deux et donc la somme $\Theta\left(\frac{1}{2}+\frac{\tau}{2},\tau\right) = 0$

□

Encore une utilité de Θ

Soit $\theta(q) = \sum_{n=-\infty}^{\infty} q^{n^2}$. Regardons $(\theta(q))^2$:

$$\begin{aligned}(\theta(q))^2 &= \sum_{n_1=-\infty}^{\infty} q^{n_1^2} \cdot \sum_{n_2=-\infty}^{\infty} q^{n_2^2} \\ &= \sum_{n_1,n_2} q^{n_1^2+n_2^2} \\ &\underset{m=n_1^2+n_2^2}{=} \sum_{m=0}^{\infty} r_2(m) q^m\end{aligned}$$

où $r_2(m)$ est le nombre de façons d'écrire n comme somme de deux carrés, $r_2(5) = (\pm 1)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 1)^2$

De même, on peut écrire $(\theta(q))^d = \sum_{m=0}^{\infty} r_d(n) q^n$. Soit $q = e^{\pi i \tau}$ avec $\tau \in \mathbb{H}$. Alors $\theta(q) = \Theta(0, \tau)$ par définition.

Poisson nous dit que $\Theta\left(z, -\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}} e^{\pi i \tau z^2} \Theta(z\tau, \tau)$. On a une symétrie par rapport à θ.

$\implies r_2(n) = 4(d_1(n) - d_3(n))$ où $d_1(n)$ est le nombre de diviseurs de n de la forme $4k+1$ et $d_3(n)$ est le nombre de diviseurs de n de la forme $4k+3$.

Exemple

$n = 5$, les seuls diviseurs de 5 sont 1 et 5, alors $d_1(5) = 2$ et $d_3(5) = 0$. Et donc $r_2(5) = 4 \cdot 2 = 8$.

$n = 6$, on trouve que $d_1(6) = 1$ et $d_3(6) = 1$. Alors $r_2(6) = 4 \cdot (1 - 1) = 0$. Donc on voit bien qu'il y a en effet aucun moyen d'écrire 6 comme somme de deux carrés.