KU LEUVEN

Master Thesis Meeting 1

Yarne Thijs

Faculty of Science
Master Of Mathematics

12/07/2024

Table of Contents

$\mathbb{Z}[X]/(X^N + 1)$ Is a Cyclotomic ring. $\forall$ polynomials $P(X), \exists! Q(X)$ polynomial at most degree $N - 1 : P(X) = Q(X)$ with regards to $\mathcal{R}$

LWE, RLWE, and RGSW Ciphertexts. We defi ne a ciphertext modulus as q and plaintext modulus as t, where $t \ll q$. Let us denote $\Delta = \left\lfloor \frac{q}{t} \right\rceil$ (Rounded?).

- An LWE ciphertext is de
  fined as $\vec{c} := (\vec{a}, b) \in \mathbb{Z}_q^{n+1}$ ($n+1$ times smaller than q).
  where $b = \langle \vec{a}\vec{s} \rangle + \Delta \cdot m + e$ for a message $m \in \mathbb{Z}_t$ and a secret key $\vec{s} \in \mathbb{Z}^n$. $\vec{c}$ is denoted by $\mathrm{LWE}_{n,t,q}(m)$.
- An RLWE ciphertext is de
  ned as $c := (a, b) \in \mathcal{R}_q^2$, where $b = a \cdot s + \Delta \cdot m + e$ for a message polynomial $m \in \mathcal{R}_t$ and a secret key $s \in \mathcal{R}$. c is denoted by $\mathrm{RLWE}_{N,t,q}(m)$.
- Given a base B_g and $l = \mathcal{O}(\log_2 q)$, we defi
  ne a gadget vector $\vec{g} = (1, B_g, \ldots, B_g^{l-1})^t$ t is here transpose?. An RGSW ciphertext is a form of $\vec{C} := (\vec{a}, \vec{b}) \in \mathcal{R}_q^{2l \times 2}$, where $\vec{b} = \vec{Z} + m \cdot \vec{G}$, where each row of $\vec{Z}$ is an RLWE encryption of 0 and $\vec{G}$ is a gadget matrix which is de
  ned by $\vec{G} = I_2 \otimes g \otimes ???$

Table of Contents

The Abel Prize

- Annual math award in commemoration of Niels Henrik Abel
- Norwegian Ministry of Education and Research
- Purpose: reward scientific work, raise status and stimulate interest
- Prize: $\pm$ 650 000 euros

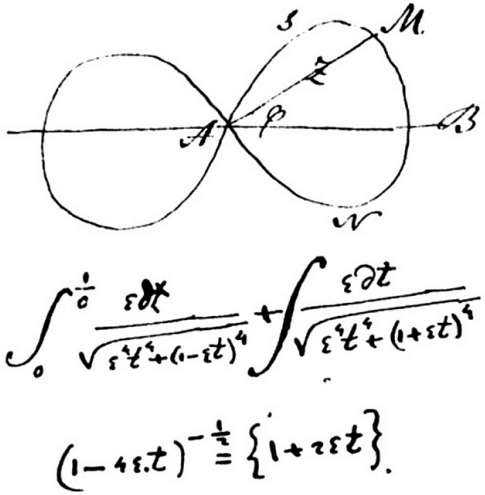

Figure: Niels Henrik Abel (Johan Gørbitz, 1826)

Table of Contents

Partial Differential Equations (PDE's)

Definition

With $u : (\Omega, \mathbb{R}) \to Y : (x, t) \mapsto u(x, t), \Omega \subseteq \mathbb{R}^n$
Now find u, that satisfied certain conditions on it's derivatives.

Example: $\begin{cases} \frac{\partial u}{\partial t} + a\frac{\partial u}{\partial x} = u & \text{for } x \in \mathbb{R},\ t > 0 \\ u(x, 0) = x_0(x) & \text{for } x \in \mathbb{R} \end{cases}$

Parabolic Partial Differential Equation

$$Au_{xx} + 2Bu_{xy} + Cu_{yy} + Du_x + Eu_y + Fu + G = 0$$

$$\text{Parabolic: } B^2 - AC = 0$$

Example (Heat equation): $\frac{\partial u}{\partial t} = \alpha \frac{\partial^2 u}{\partial x^2}$
But more with Fien in the financial application

Elliptic Partial Differential Equation

- 2 dimensions: $\Omega \subset \mathbb{R}^2$

$$Au_{xx} + 2Bu_{xy} + Cu_{yy} + Du_x + Eu_y + Fu + G = 0$$

Elliptic: $B^2 - AC < 0$

$$u_{xx} + u_{yy} + \text{lower orders} = 0$$

Elliptic Partial Differential Equation

- 2 dimensions: $\Omega \subset \mathbb{R}^2$

$$Au_{xx} + 2Bu_{xy} + Cu_{yy} + Du_x + Eu_y + Fu + G = 0$$

Elliptic: $B^2 - AC < 0$

$$u_{xx} + u_{yy} + \text{lower orders} = 0$$

- $2 \leqslant n$ dimensions: $\Omega \subset \mathbb{R}^n$

$$Lu = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} \frac{\partial^2 u}{\partial x_i \partial x_j} + \cdots = 0$$

Elliptic: The eigenvalues are all positive or all negative

An example: Laplace' s Equation

$$\nabla^2 \mathrm{f} = 0 = \Delta \mathrm{f}$$

2 dims, independent, rectangular: $\frac{\partial^2 \mathrm{u}}{\partial \mathrm{x}^2} + \frac{\partial^2 \mathrm{u}}{\partial \mathrm{y}^2} = 0 = \mathrm{u_{xx}} + \mathrm{u_{yy}}$

- Rectangular Coordinates: $\nabla^2 \mathrm{f} = \frac{\partial^2 \mathrm{f}}{\partial \mathrm{x}^2} + \frac{\partial^2 \mathrm{f}}{\partial \mathrm{y}^2} + \frac{\partial^2 \mathrm{f}}{\partial \mathrm{z}^2} = 0$
- Cylindrical Coordinates: $\nabla^2 \mathrm{f} = \frac{1}{\mathrm{r}} \frac{\partial}{\partial \mathrm{r}} \left(\mathrm{r} \frac{\partial \mathrm{f}}{\partial \mathrm{r}} \right) + \frac{1}{\mathrm{r}^2} \frac{\partial^2 \mathrm{f}}{\partial \theta^2} + \frac{\partial^2 \mathrm{f}}{\partial \mathrm{z}^2} = 0$
- Spherical Coordinates:
  $\nabla^2 \mathrm{f} = \frac{1}{\mathrm{r}^2} \frac{\partial}{\partial \mathrm{r}} \left(\mathrm{r}^2 \frac{\partial \mathrm{f}}{\partial \mathrm{r}} \right) + \frac{1}{\mathrm{r}^2 \sin\theta} \frac{\partial}{\partial \theta} \left(\sin\theta \frac{\partial \mathrm{f}}{\partial \theta} \right) + \frac{1}{\mathrm{r}^2 \sin^2\theta} \frac{\partial^2 \mathrm{f}}{\partial \phi^2} = 0$

What is Regularity?

What is Regularity?

Left as exercise to the audience!

What is Regularity?

Left as exercise to the audience!

Wikipedia https://en.wikipedia.org/wiki/Regularity_theory

Regularity is a property of elliptic partial differential equations such as Laplace's equation. Hilbert's nineteenth problem was concerned with this concept

KU LEUVEN

Master Thesis Meeting 1

Yarne Thijs

Faculty of Science
Master Of Mathematics

12/07/2024