数，我们怎样认识她?

王崧

中国科学院数学与系统科学研究院

June 2, 2010

自然数、整数、有理数

- 自然数: $\mathbb{N} := 0, 1, 2, \ldots$ (加法、乘法)
- 整数: $\mathbb{Z} := 0, \pm 1, \pm 2, \ldots$ (加法、减法、乘法)
- 有理数: $\mathbb{Q} := r/s$ (加、减、乘、除)
  $r, s \in \mathbb{Z}, s \neq 0$

- 解丢番图方程是数论的一个核心课题。

自然数、整数、有理数

- 自然数: $\mathbb{N} := 0, 1, 2, \ldots$ (加法、乘法)
- 整数: $\mathbb{Z} := 0, \pm 1, \pm 2, \ldots$ (加法、减法、乘法)
- 有理数: $\mathbb{Q} := r/s$ (加、减、乘、除)
  $r, s \in \mathbb{Z}, s \neq 0$

- 解丢番图方程是数论的一个核心课题。

自然数、整数、有理数

- 自然数: $\mathbb{N} := 0, 1, 2, \ldots$ (加法、乘法)
- 整数: $\mathbb{Z} := 0, \pm 1, \pm 2, \ldots$ (加法、减法、乘法)
- 有理数: $\mathbb{Q} := r/s$ (加、减、乘、除)
  $r, s \in \mathbb{Z}, s \neq 0$

- 解丢番图方程是数论的一个核心课题。

自然数、整数、有理数

- 自然数: $\mathbb{N} := 0, 1, 2, \ldots$ (加法、乘法)
- 整数: $\mathbb{Z} := 0, \pm 1, \pm 2, \ldots$ (加法、减法、乘法)
- 有理数: $\mathbb{Q} := r/s$ (加、减、乘、除)
  $r, s \in \mathbb{Z}, s \neq 0$

- 解丢番图方程是数论的一个核心课题。

数，我们怎样认识它？

——数的大小

认识数的大小，我们需要尺度–绝对值(absolute values)。

例: 3 和5/2 谁大？

数的大小–绝对值

- 绝对值定义：$|\quad|: \mathbb{Q} \to \mathbb{R}_{\geq 0}$.
  (1). $|x| \geq 0, \forall x \in \mathbb{Q}; |x| = 0 \Leftrightarrow x = 0$.
  (2). $|x \cdot y| = |x| \cdot |y|, \forall x, y \in \mathbb{Q}$.
  (3). 三角不等式: $|x + y| \leq |x| + |y|$.
- 问题：在拓扑等价的意义下，$\mathbb{Q}$ 上有多少中绝对值？

数的大小–绝对值

- 绝对值定义：$|\quad|: \mathbb{Q} \to \mathbb{R}_{\geq 0}$.
  (1). $|x| \geq 0, \forall x \in \mathbb{Q}; |x| = 0 \Leftrightarrow x = 0$.
  (2). $|x \cdot y| = |x| \cdot |y|, \forall x, y \in \mathbb{Q}$.
  (3). 三角不等式: $|x + y| \leq |x| + |y|$.
- 问题：在拓扑等价的意义下，$\mathbb{Q}$ 上有多少中绝对值？

数的大小–绝对值

- $|\quad|_\infty$: ∞-adic 赋值。

$$|x|_\infty = \mathrm{sgn}(x) \cdot x = \begin{cases} x & x \geq 0 \\ -x & x \leq 0 \end{cases}$$

- 例: $|3|_\infty > |5/2|_\infty$。

数的大小–绝对值

- $|\quad|_\infty$: ∞-adic 赋值。

$$|x|_\infty = \mathrm{sgn}(x) \cdot x = \begin{cases} x & x \geq 0 \\ -x & x \leq 0 \end{cases}$$

- 例: $|3|_\infty > |5/2|_\infty$。

数的大小 – – 绝对值

- $|\quad|_p$: p-adic 赋值, 当p为素数时。

$$|x|_p = \begin{cases} |p^n \frac{a}{b}|_p = p^{-n}, a, b \in \mathbb{Z}, p \nmid ab & x \neq 0 \\ 0 & x = 0 \end{cases}$$

- 例: $|3|_3 < |5/2|_3, |3|_2 < |5/2|_2, |3|_5 > |5/2|_5$

数的大小 – – 绝对值

- $|\quad|_p$: p-adic 赋值, 当p为素数时。

$$|x|_p = \begin{cases} |p^n \frac{a}{b}|_p = p^{-n}, a, b \in \mathbb{Z}, p \nmid ab & x \neq 0 \\ 0 & x = 0 \end{cases}$$

- 例: $|3|_3 < |5/2|_3, |3|_2 < |5/2|_2, |3|_5 > |5/2|_5$

数的大小 – – 绝对值

平凡赋值(trivial absolute value):

$$|x|_0 = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$$

例: $|3|_0 = |5/2|_0 = 1$

数的大小 – – 绝对值

- 有理数$\mathbb{Q}$ 的赋值:
  阿基米德绝对值: $|\ \ |_\infty$
  p-adic 绝对值: $|\ \ |_p$
  平凡绝对值: $|\ \ |_0$
- 定理(Ostrowski): 任何$\mathbb{Q}$ 上的绝对值等价于以上几类。

$\{\mathbb{Q}$ 上的非平凡绝对值等价类$\} \longleftrightarrow \{$素数$p\}, \{\infty\}$

数的大小 – – 绝对值

- 有理数$\mathbb{Q}$ 的赋值:
  阿基米德绝对值: $|\ \ |_\infty$
  p-adic 绝对值: $|\ \ |_p$
  平凡绝对值: $|\ \ |_0$
- 定理(Ostrowski): 任何$\mathbb{Q}$ 上的绝对值等价于以上几类。

$\{\mathbb{Q}$ 上的非平凡绝对值等价类$\} \longleftrightarrow \{$素数$p\}, \{\infty\}$

数的大小 – – 绝对值

- 阿基米德公理：$\forall a, b \in \mathbb{Q}, a, b \neq 0$, 存在正整数$n$ 使得

$$|na|_\infty > |b|_\infty$$

- (3') 强三角不等式(当p为素数时):

$$|x + y|_p \leq \max(|x|_p, |y|_p)$$

$$|x + y|_p = \max(|x|_p, |y|_p), \quad \text{if } |x|_p \neq |y|_p$$

- $\mathbb{Q}$ 在$|\quad|_0$ 上的拓扑是离散拓扑。

数的大小 – – 绝对值

- 阿基米德公理：$\forall a, b \in \mathbb{Q}, a, b \neq 0$, 存在正整数$n$ 使得

$$|na|_\infty > |b|_\infty$$

- (3') 强三角不等式(当p为素数时):

$$|x + y|_p \leq \max(|x|_p, |y|_p)$$

$$|x + y|_p = \max(|x|_p, |y|_p), \quad \text{if } |x|_p \neq |y|_p$$

- $\mathbb{Q}$ 在$|\quad|_0$ 上的拓扑是离散拓扑。

数的大小 – – 绝对值

- 阿基米德公理：$\forall a, b \in \mathbb{Q}, a, b \neq 0$, 存在正整数$n$ 使得

$$|na|_\infty > |b|_\infty$$

- (3') 强三角不等式(当p为素数时):

$$|x + y|_p \leq \max(|x|_p, |y|_p)$$

$$|x + y|_p = \max(|x|_p, |y|_p), \quad \text{if } |x|_p \neq |y|_p$$

- $\mathbb{Q}$ 在$|\quad|_0$ 上的拓扑是离散拓扑。

数的大小 – – 绝对值

- 对所有非平凡绝对值$|\quad|$，$(\mathbb{Q},|\quad|)$ 成为一个赋值域，但是不是完备的。
- 完备化:

$$(\mathbb{Q},|\quad|_\infty)\longrightarrow\mathbb{R}=\mathbb{Q}_\infty\qquad(\mathbb{R},|\quad|_\infty)$$
$$(\mathbb{Q},|\quad|_p)\longrightarrow\mathbb{Q}_p\qquad(\mathbb{Q}_p,|\quad|_p)$$
$$(\mathbb{Q},|\quad|_0)\longrightarrow\mathbb{Q}\qquad(\mathbb{Q},\text{离散拓扑})$$

$\mathbb{R}$, $\mathbb{Q}_p$, $(\mathbb{Q},$ 离散拓扑$)$ 均为局部紧的Hausdorff拓扑域。

数的大小 – – 绝对值

- 对所有非平凡绝对值$|\quad|$，$(\mathbb{Q}, |\quad|)$ 成为一个赋值域，但是不是完备的。
- 完备化:

$$
\begin{array}{lll}
(\mathbb{Q}, |\quad|_\infty) \longrightarrow \mathbb{R} = \mathbb{Q}_\infty & & (\mathbb{R}, |\quad|_\infty) \\
(\mathbb{Q}, |\quad|_p) \longrightarrow \mathbb{Q}_p & & (\mathbb{Q}_p, |\quad|_p) \\
(\mathbb{Q}, |\quad|_0) \longrightarrow \mathbb{Q} & & (\mathbb{Q}, \text{离散拓扑})
\end{array}
$$

$\mathbb{R}$, $\mathbb{Q}_p$, $(\mathbb{Q}, \text{离散拓扑})$ 均为局部紧的Hausdorff拓扑域。

数的大小－－绝对值

$\Sigma = \mathbb{Q}$ 上的非平凡绝对值等价类的集合$= \{\infty, 2, 3, 5, \ldots, \quad p$素数.$, \ldots\}$

$\mathbb{Z}_p := \mathbb{Q}_p$ 上的单位球：$\{x, |x|_p \leq 1\}$，我们称为p-adic 整数环。

数的大小 – – 绝对值

- 问题：这些绝对值之间的关系（依赖性和独立性）
- 定理1 (乘积公式)：$\forall x \in \mathbb{Q}^\times, \prod_{v\in\Sigma} |x|_v = 1.$
- 定理2 (中国剩余定理 – – 强逼近定理I)
  对任意$\mathbb{Q}$ 上绝对值的有限非空集合$S \subset \Sigma$，下面的对角嵌入

$$\mathbb{Q} \hookrightarrow \prod_{v\in S} \mathbb{Q}_v$$

$$\mathbb{Q}^\times \hookrightarrow \prod_{v\in S} \mathbb{Q}_v^\times$$

  均是稠密的。

数的大小 – – 绝对值

- 问题：这些绝对值之间的关系（依赖性和独立性）
- 定理1 (乘积公式)：$\forall x \in \mathbb{Q}^\times, \prod_{v\in\Sigma} |x|_v = 1.$
- 定理2 (中国剩余定理 – – 强逼近定理I)
  对任意$\mathbb{Q}$ 上绝对值的有限非空集合$S \subset \Sigma$，下面的对角嵌入

$$\mathbb{Q} \hookrightarrow \prod_{v\in S} \mathbb{Q}_v$$

$$\mathbb{Q}^\times \hookrightarrow \prod_{v\in S} \mathbb{Q}_v^\times$$

  均是稠密的。

数的大小 – – 绝对值

- 问题：这些绝对值之间的关系（依赖性和独立性）
- 定理1 (乘积公式)：$\forall x \in \mathbb{Q}^\times, \prod_{v\in\Sigma} |x|_v = 1.$
- 定理2 (中国剩余定理 – – 强逼近定理I)
  对任意$\mathbb{Q}$ 上绝对值的有限非空集合$S \subset \Sigma$，下面的对角嵌入

$$\mathbb{Q} \hookrightarrow \prod_{v\in S} \mathbb{Q}_v$$

$$\mathbb{Q}^\times \hookrightarrow \prod_{v\in S} \mathbb{Q}_v^\times$$

  均是稠密的。

数的大小 – – 绝对值

- 数论中的一个重要课题是丢番图方程，即对给定整系数(或有理系数) 的多项式方程组求其整数解(或有理数解)。
- 局部整体原则：方程有$\mathbb{Q}$解$\Longrightarrow$ 对所有v 方程有$\mathbb{Q}_v$ 解
- 例：$x^2+5=0$ 在$\mathbb{Q}$ 中无解，因为它在$\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_5$ 中无解; $x^2-3=0$ 在$\mathbb{Q}$ 中无解，因为它在$\mathbb{Q}_2, \mathbb{Q}_3$ 中无解。

数的大小 – – 绝对值

- 数论中的一个重要课题是丢番图方程，即对给定整系数(或有理系数) 的多项式方程组求其整数解(或有理数解)。
- 局部整体原则：方程有$\mathbb{Q}$解$\Longrightarrow$ 对所有v 方程有$\mathbb{Q}_v$ 解
- 例：$x^2+5=0$ 在$\mathbb{Q}$ 中无解，因为它在$\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_5$ 中无解; $x^2-3=0$ 在$\mathbb{Q}$ 中无解，因为它在$\mathbb{Q}_2, \mathbb{Q}_3$ 中无解。

数的大小 – – 绝对值

- 数论中的一个重要课题是丢番图方程，即对给定整系数(或有理系数) 的多项式方程组求其整数解(或有理数解)。
- 局部整体原则：方程有$\mathbb{Q}$解$\Longrightarrow$ 对所有v 方程有$\mathbb{Q}_v$ 解
- 例：$x^2+5=0$ 在$\mathbb{Q}$ 中无解，因为它在$\mathbb{R}, \mathbb{Q}_2, \mathbb{Q}_5$ 中无解; $x^2-3=0$ 在$\mathbb{Q}$ 中无解，因为它在$\mathbb{Q}_2, \mathbb{Q}_3$ 中无解。

数的大小 – – 绝对值

- **Hasse-Minkowski 原则:**
  一个有理系数二次方程有有理解，当且仅当它在每个$\mathbb{Q}_v$中均有解。

- 例：$3x^3 + 4y^4 + 5z^5 = 0$在每一个$\mathbb{Q}_v$中有非零解。但是方程在 $\mathbb{Q}$ 中无非零解。

数的大小 – – 绝对值

Catalan 猜想 – – Mihailesku 定理 设p, q 为不小于2 的整数，则$x^p - y^q = 1$ 只有如下的非平凡解：$(\pm 3)^2 - 2^3 = 1$。

证明需对$\mathbb{Q}_\infty$, $\mathbb{Q}_p$ 和$\mathbb{Q}_q$ 的研究。

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- 我们追求一个能够包含所有局部域$\mathbb{Q}_v$信息的对象。
  候选者: $\prod_v \mathbb{Q}_v$
- 失败理由：没有好的分析性质。事实上，每个 $\mathbb{Q}_v$ 都是局部紧的，从而有积分理论(Haar 、测度)。但是该乘积不是局部紧致的拓扑群。紧集的乘积空间是紧的，但局部紧集的乘积空间一般不是局部紧的。

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- 我们追求一个能够包含所有局部域$\mathbb{Q}_v$信息的对象。
  候选者: $\prod_v \mathbb{Q}_v$
- 失败理由：没有好的分析性质。事实上，每个 $\mathbb{Q}_v$都是局部紧的，从而有积分理论(Haar 、测度)。但是该乘积不是局部紧致的拓扑群。紧集的乘积空间是紧的，但局部紧集的乘积空间一般不是局部紧的。

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- $$\mathbb{A}_{\mathbb{Q}} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p \text{ for almost all}$$

$$\mathbb{A}_{\mathbb{Q}}^{\times} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p^{\times} \text{ for almost all}$$

- $\mathbb{A}_{\mathbb{Q}}$ 和 $\mathbb{A}_{\mathbb{Q}}^{\times}$ 在限制乘积拓扑下是局部紧的，从而有整体局部调和分析理论。
- 选取 Haar 测度dx on $\mathbb{A}_{\mathbb{Q}}$, Haar 测度 dx_v on $\mathbb{Q}_v$, $v \in \Sigma$

$$dx = \otimes_v dx_v$$

- 同样对 $\mathbb{A}_{\mathbb{Q}}^{\times}$,

$$d^{\times}x = \otimes d^{\times}x_v$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- $$\mathbb{A}_{\mathbb{Q}} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p \text{ for almost all}$$

  $$\mathbb{A}_{\mathbb{Q}}^{\times} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p^{\times} \text{ for almost all}$$

- $\mathbb{A}_{\mathbb{Q}}$ 和 $\mathbb{A}_{\mathbb{Q}}^{\times}$ 在限制乘积拓扑下是局部紧的，从而有整体局部调和分析理论。
- 选取 Haar 测度dx on $\mathbb{A}_{\mathbb{Q}}$, Haar 测度 dx_v on $\mathbb{Q}_v$, $v \in \Sigma$

  $$dx = \otimes_v dx_v$$

- 同样对 $\mathbb{A}_{\mathbb{Q}}^{\times}$,

  $$d^{\times}x = \otimes d^{\times}x_v$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- $$\mathbb{A}_{\mathbb{Q}} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p \text{ for almost all}$$

$$\mathbb{A}_{\mathbb{Q}}^{\times} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p^{\times} \text{ for almost all}$$

- $\mathbb{A}_{\mathbb{Q}}$ 和 $\mathbb{A}_{\mathbb{Q}}^{\times}$ 在限制乘积拓扑下是局部紧的，从而有整体局部调和分析理论。
- 选取 Haar 测度dx on $\mathbb{A}_{\mathbb{Q}}$, Haar 测度 dx_v on $\mathbb{Q}_v$, $v \in \Sigma$

$$dx = \otimes_v dx_v$$

- 同样对 $\mathbb{A}_{\mathbb{Q}}^{\times}$,

$$d^{\times}x = \otimes d^{\times}x_v$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- $$\mathbb{A}_{\mathbb{Q}} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p \text{ for almost all}$$

$$\mathbb{A}_{\mathbb{Q}}^{\times} = \prod_v{}' \mathbb{Q}_v = \{x = (x_\infty, x_p), x_p \in \mathbb{Z}_p^{\times} \text{ for almost all}$$

- $\mathbb{A}_{\mathbb{Q}}$ 和 $\mathbb{A}_{\mathbb{Q}}^{\times}$ 在限制乘积拓扑下是局部紧的，从而有整体局部调和分析理论。
- 选取 Haar 测度dx on $\mathbb{A}_{\mathbb{Q}}$, Haar 测度 dx_v on $\mathbb{Q}_v$, $v \in \Sigma$

$$dx = \otimes_v dx_v$$

- 同样对 $\mathbb{A}_{\mathbb{Q}}^{\times}$,

$$d^{\times}x = \otimes d^{\times}x_v$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- 定义：Riemann-Zeta 函数 $\zeta(s) = \sum_{n=1}^{\infty}$，$\mathrm{Re}(s) > 1$。
- 定理：$\zeta(s)$, 可以解析延拓为复平面$\mathbb{C}$ 上的半纯函数，仅在$s = 1$ 处有一单极点，留数为1。同时，满足函数方程:

$$\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \Lambda(1-s)$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- 定义：Riemann-Zeta 函数 $\zeta(s) = \sum_{n=1}^{\infty}$，$\mathrm{Re}(s) > 1$。
- **定理：** $\zeta(s)$, 可以解析延拓为复平面$\mathbb{C}$ 上的半纯函数，仅在$s = 1$ 处有一单极点，留数为1。同时，满足函数方程：

$$\Lambda(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \Lambda(1-s)$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- *Proof*: 回忆我们有积分理论。选取在$\mathbb{A}_{\mathbb{Q}}$ 上的Haar测度$dx = \otimes dx_v$, 及在 $\mathbb{A}_{\mathbb{Q}}^{\times}$ 上的 Haar测度$d^{\times}x = \otimes d^{\times}x_v$。考察以下一个好的分析空间 $\mathcal{S}(\mathbb{R})$, $\mathbb{R}$ 上的Schwartz 函数空间集合，因为它的元素有着很好收敛性，同时在它上可以做Fourier 分析。定义Fourier 变换如下:

$$\mathcal{S}(\mathbb{R}) \to \mathcal{S}(\mathbb{R})$$

$$f(x) \mapsto \hat{f}(x) = \int_{\mathbb{R}} f(y) \exp(-2\pi i x y)\, dx$$

- Fact (Multiplicity One): $\mathbb{R}^{\times}$ 在 $\mathcal{S}(\mathbb{R})$ 上作用，从而在 $\mathcal{S}'(\mathbb{R})$，$\mathcal{S}(\mathbb{R})$ 上的连续线性泛函即分布(distribution)的集合上作用。在$\mathbb{R}^{\times}$ 作用下保持不变的分布组成的空间是 1 维的。

Adele 环$\mathbb{A}_{\mathbb{Q}}$

- *Proof*: 回忆我们有积分理论。选取在$\mathbb{A}_{\mathbb{Q}}$ 上的Haar测度$dx = \otimes dx_v$, 及在 $\mathbb{A}_{\mathbb{Q}}^{\times}$ 上的 Haar测度$d^{\times}x = \otimes d^{\times}x_v$。考察以下一个好的分析空间 $\mathcal{S}(\mathbb{R})$, $\mathbb{R}$ 上的Schwartz 函数空间集合，因为它的元素有着很好收敛性，同时在它上可以做Fourier 分析。定义Fourier 变换如下:

$$\mathcal{S}(\mathbb{R}) \to \mathcal{S}(\mathbb{R})$$

$$f(x) \mapsto \hat{f}(x) = \int_{\mathbb{R}} f(y) \exp(-2\pi i x y)\, dx$$

- Fact (Multiplicity One): $\mathbb{R}^{\times}$ 在 $\mathcal{S}(\mathbb{R})$ 上作用，从而在 $\mathcal{S}'(\mathbb{R})$，$\mathcal{S}(\mathbb{R})$ 上的连续线性泛函即分布(distribution)的集合上作用。在$\mathbb{R}^{\times}$ 作用下保持不变的分布组成的空间是 1 维的。

- 作为分布，

$$Z := \phi \mapsto \frac{\int_{\mathbb{R}^\times} \phi(x)|x|^s \, d^\times x}{\pi^{-s/2}\Gamma(s/2)} \Big|_{s=0}$$

$$Z' := \phi \mapsto \frac{\int_{\mathbb{R}^\times} \hat{\phi}(x)|x|^{1-s} \, d^\times x}{\pi^{(1-s)/2}\Gamma((1-s)/2)} \Big|_{s=0}$$

同属于在$\mathbb{R}^\times$作用下保持不变的分布，因此它们相差一个常数因子。

- 实际上，

$$\frac{\int_{\mathbb{Q}_v^\times} \hat{\phi}(x)|x|^{1-s} \, d^\times x}{\zeta_v(1-s)} = \epsilon_v(s) \frac{\int_{\mathbb{Q}_v^\times} \phi(x)|x|^s}{\zeta_v(s)}$$

$$\zeta_v(s) = \begin{cases} (1-p^{-s})^{-1} & v = p < \infty \\ \pi^{-s/2}\Gamma(s/2) & v = \infty \end{cases}$$

Adele 环$\mathbb{A}_{\mathbb{Q}}$

事实上，固定一个$\mathbb{Q}\backslash\mathbb{A}_{\mathbb{Q}}$上的非平凡加法特征$\Psi$，选取任意$\phi=\otimes\phi_v$，由 Poisson 求和，

$$\int_{\mathbb{A}_{\mathbb{Q}}^{\times}}\phi(x)|x|^{s}\,d^{\times}x=\int_{\mathbb{A}_{\mathbb{Q}}^{\times}}\hat{\phi}(x)|x|^{1-s}\,d^{\times}x$$

$$\Rightarrow\Lambda(s)=\prod_{v\in\Sigma}\zeta_v(s)=\Lambda(1-s)$$

代数方面

- 数我们应该怎样认识她:
  ——-代数方面
  有一位年青的数学家创造出伟大的理论
  他的生命流星般的消失
  但是他的贡献影响延伸永远
- $\Longrightarrow$ Galois

代数方面

- 数我们应该怎样认识她:
  ——代数方面
  有一位年青的数学家创造出伟大的理论
  他的生命流星般的消失
  但是他的贡献影响延伸永远
- $\Longrightarrow$ **Galois**

代数方面

- **题目：** $y^2 = x^3 - 5 \quad (*)$

$$\Rightarrow (y + \sqrt{-5})(y - \sqrt{-5}) = x^3$$

- 我们可以在数域$\mathbb{Q}[\sqrt{-5}]$ 及其整数环 $\mathbb{Z}[\sqrt{-5}]$ 中解(*), 然后研究其在$\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q})$ 下的作用 $\Longrightarrow$ 无解
- 事实上，我们需要关于$\mathbb{Z}[\sqrt{-5}]$ 的两个基本事实：(1)任何一个理想的平方均可由单个元素生成，(2)它的单位群为 $\{\pm 1\}$

代数方面

- **题目：** $y^2 = x^3 - 5 \quad (*)$

$$\Rightarrow (y + \sqrt{-5})(y - \sqrt{-5}) = x^3$$

- 我们可以在数域$\mathbb{Q}[\sqrt{-5}]$ 及其整数环 $\mathbb{Z}[\sqrt{-5}]$ 中解(*), 然后研究其在$\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q})$ 下的作用
$\Longrightarrow$ 无解
- 事实上，我们需要关于$\mathbb{Z}[\sqrt{-5}]$ 的两个基本事实：(1)任何一个理想的平方均可由单个元素生成，(2)它的单位群为 $\{\pm 1\}$

代数方面

- **题目：** $y^2 = x^3 - 5 \quad (*)$

$$\Rightarrow (y + \sqrt{-5})(y - \sqrt{-5}) = x^3$$

- 我们可以在数域$\mathbb{Q}[\sqrt{-5}]$ 及其整数环 $\mathbb{Z}[\sqrt{-5}]$ 中解(*), 然后研究其在$\mathrm{Gal}(\mathbb{Q}(\sqrt{-5})/\mathbb{Q})$ 下的作用
  $\Longrightarrow$ 无解
- 事实上，我们需要关于$\mathbb{Z}[\sqrt{-5}]$ 的两个基本事实：(1)任何一个理想的平方均可由单个元素生成，(2)它的单位群为 $\{\pm 1\}$

代数方面

- *Proof*:

$$(y+\sqrt{-5})(y-\sqrt{-5})=x^3$$

由前两点，以及理想的唯一分解定理可知

$$y+\sqrt{-5}=(a+b\sqrt{-5})^3=(a^3-15ab^2)+(3a^2b-5b^3)$$

取Galois共轭，有

$$y-\sqrt{-5}=(a-b\sqrt{-5})^3=(a^3-15ab^2)-(3a^2b-5b^3)$$

- 于是，两个方程相减并约掉$2\sqrt{-5}$，有

$$1=3a^2b-5b^3=b(3a^2-5b^2)$$

$$\Rightarrow b=\pm 1,\quad 3a^2-5=\pm 1\Rightarrow 3a^2=4,6$$

无解。

代数方面

- *Proof*:

$$(y+\sqrt{-5})(y-\sqrt{-5})=x^3$$

由前两点，以及理想的唯一分解定理可知

$$y+\sqrt{-5}=(a+b\sqrt{-5})^3=(a^3-15ab^2)+(3a^2b-5b^3)$$

取Galois共轭，有

$$y-\sqrt{-5}=(a-b\sqrt{-5})^3=(a^3-15ab^2)-(3a^2b-5b^3)$$

- 于是，两个方程相减并约掉$2\sqrt{-5}$，有

$$1=3a^2b-5b^3=b(3a^2-5b^2)$$

$$\Rightarrow b=\pm 1,\quad 3a^2-5=\pm 1\Rightarrow 3a^2=4,6$$

无解。

Galois 群

问题：能否找到一个好的对象，包含所有的有限代数扩张的信息？
定义$\bar{\mathbb{Q}}$ 为$\mathbb{Q}$ 的代数闭包

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{K/\mathbb{Q}} \mathrm{Gal}(K/\mathbb{Q})$$

其中，$K/\mathbb{Q}$ 跑遍所有的代数扩张；它的表示，已经成为当今数论的核心问题。

代数方面

例：Catalan 猜想。若 p, q 为奇数且 $x^p - y^q = 1$ 有非平凡解 (x, y)，通过对$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 在 μ_q 的表示的研究。则该解对应着 Selmer同调群

$$H^1_{Sel_q^p}(\mathbb{Q}(\zeta_p), \mu_q)$$

中的一个元素。而上面关于$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 模μ_q 的上同调群定义由在$v = p, q$的特殊局部条件和其它v处的非分歧条件给出。Catalan猜想的解决转化为对该同调群的研究。

多姿多彩

数，我们应该怎样认识她？

——多姿多彩　　代数几何、代数流形

数的几何

- 考察整边直角三角形的三边 $(a,b,c), a^2+b^2=c^2$的求解。该问题等价于

$$x^2+y^2=1, xy \in \mathbb{Q}$$

我们可以通过单位圆$x^2+y^2=1$ 和所有通过 $(0,1)$ 的有理斜率的直线的交点来获得该单位圆上的所有有理点。

-

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

$$\Rightarrow (a,b,c)=k\left((s-t)^2, 2st, (s+t)^2\right)$$

数的几何

- 考察整边直角三角形的三边 $(a,b,c), a^2+b^2=c^2$的求解。该问题等价于

$$x^2+y^2=1, xy \in \mathbb{Q}$$

我们可以通过单位圆$x^2+y^2=1$ 和所有通过 $(0,1)$ 的有理斜率的直线的交点来获得该单位圆上的所有有理点。

-

$$(x,y)=(\frac{t^2-1}{t^2+1},\frac{2t}{t^2+1})$$

$$\Rightarrow (a,b,c)=k((s-t)^2,2st,(s+t)^2)$$

数的几何

- **Congruent number** 问题：n 是任意的整数，是否存在有理直角三角形C，使得它的面积为n?
  设直角三角形的直角边为a, b，斜边为c，则有
-

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{1}{2}ab = n \end{cases} \tag{0.1}$$

$$(a, b, c) \in \mathbb{Q}^3 \tag{0.2}$$

数的几何

- **Congruent number 问题**：n 是任意的整数，是否存在有理直角三角形C，使得它的面积为n?
  设直角三角形的直角边为a, b，斜边为c，则有
-

$$\begin{cases} a^2 + b^2 = c^2 \\ \dfrac{1}{2}ab = n \end{cases} \tag{0.1}$$

$$(a, b, c) \in \mathbb{Q}^3 \tag{0.2}$$

数的几何

- **等价命题** $E_{(n)}$ 是定义在 $\mathbb{Q}$ 上的椭圆曲线 (elliptic curve). 在上面有着极其丰富的理论. 其中，包括无穷远点，它上面所有的$\mathbb{Q}$点集合组成一个有限生成的Abel 群。关于其证明，则需研究Galois 群$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$在

$$T_p(E) = \varprojlim E[p^n]$$

这个2维$\mathbb{Z}_p$上的自由模上的作用. 特别的, n 为一个congruent number 当且仅当$E_{(n)}(\mathbb{Q})$ 有一个$\mathbb{Q}$点$(x, y \neq 0)$.

- *Observation*: 非常容易观察到，若存在面积为n 的有理三角形，设边长为a, b, c, 且$a > b$,
则$(x = \frac{c^2}{4}, y = \frac{c(a^2-b^2)}{8} \neq 0)$ 是$E_{(n)}$ 上的有理点。

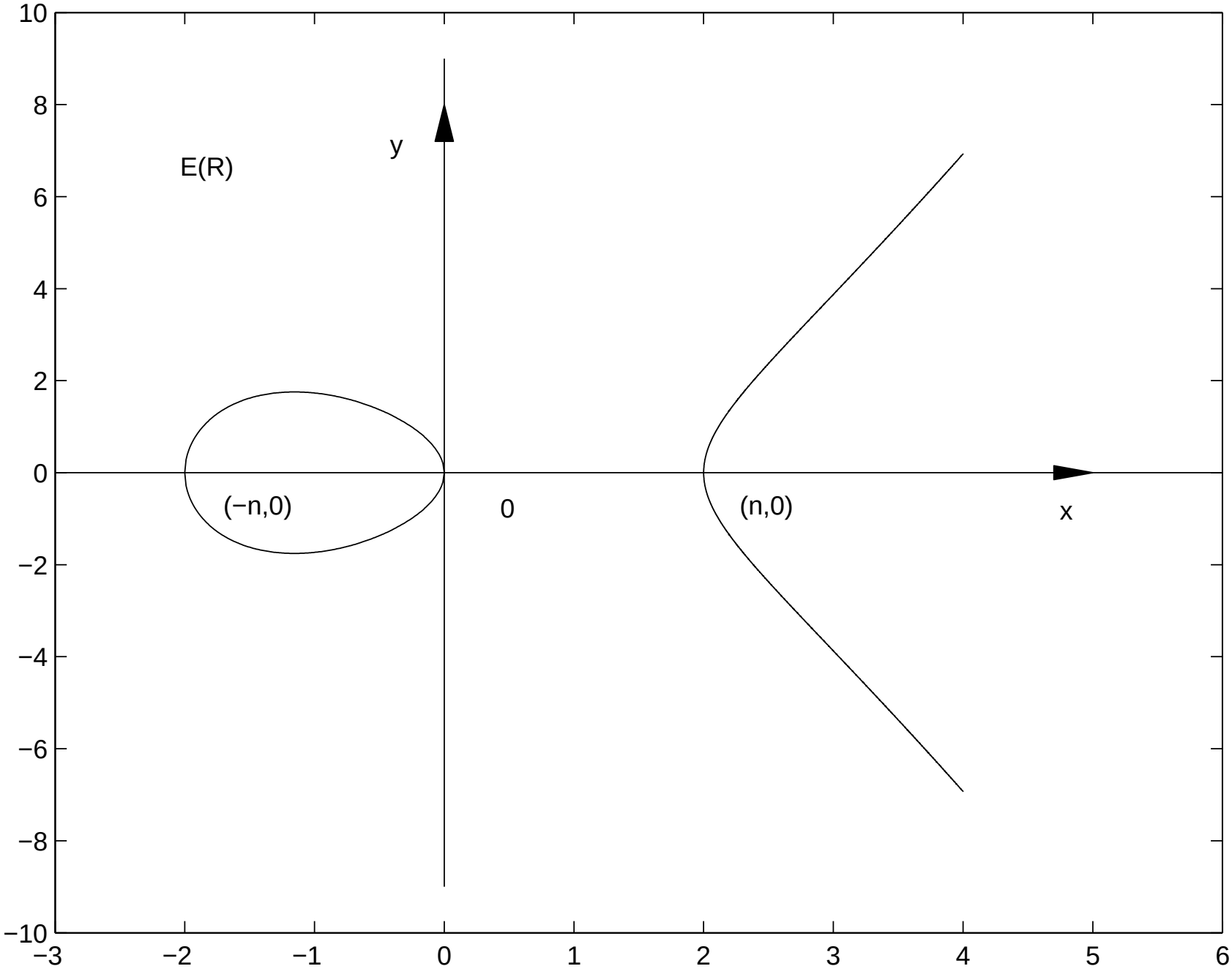
数的几何

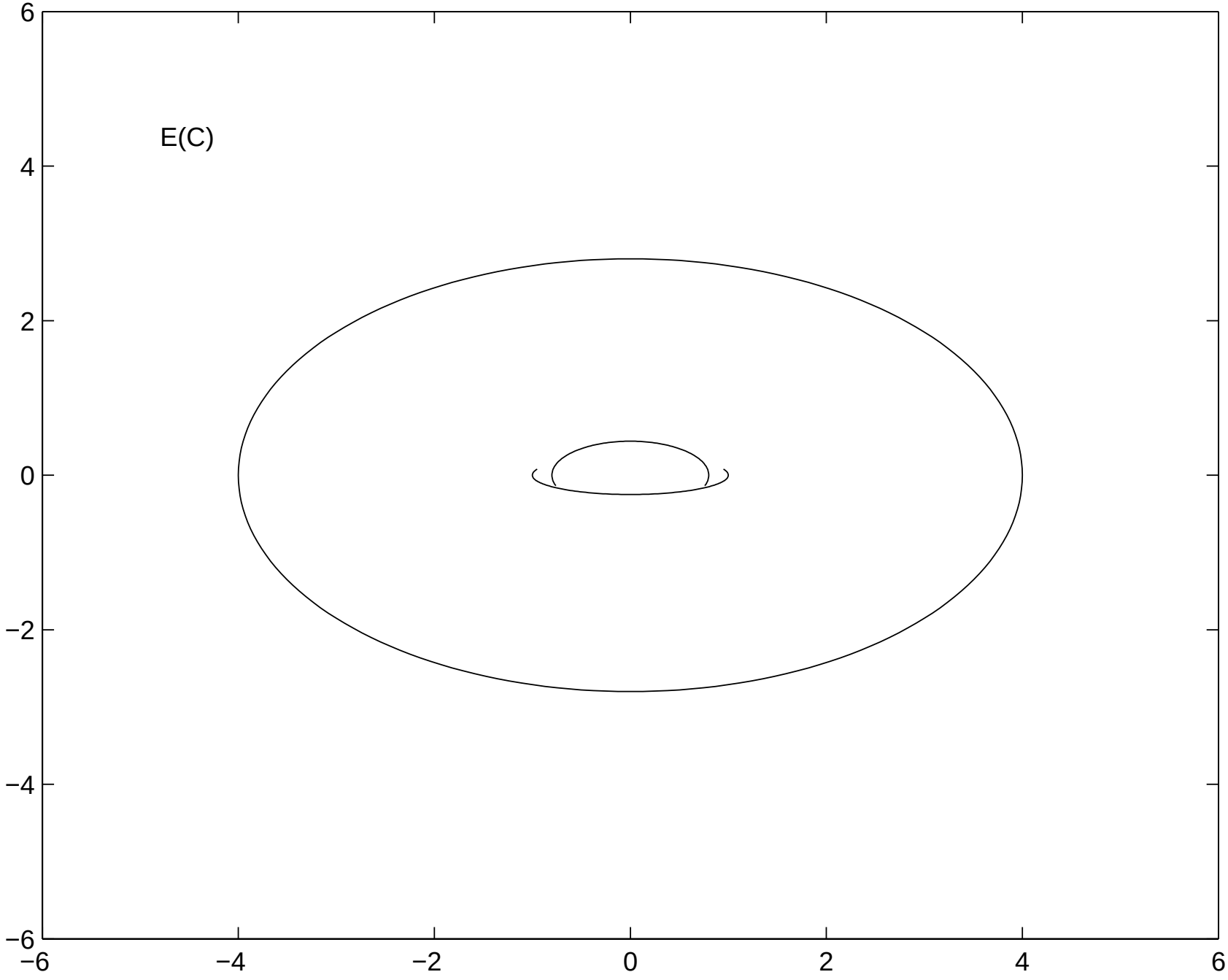
- **等价命题** $E_{(n)}$ 是定义在 $\mathbb{Q}$ 上的椭圆曲线 (elliptic curve). 在上面有着极其丰富的理论. 其中，包括无穷远点，它上面所有的$\mathbb{Q}$点集合组成一个有限生成的Abel 群。关于其证明，则需研究Galois 群$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$在

$$T_p(E) = \varprojlim E[p^n]$$

这个2维$\mathbb{Z}_p$上的自由模上的作用. 特别的, n 为一个congruent number 当且仅当$E_{(n)}(\mathbb{Q})$ 有一个$\mathbb{Q}$点$(x, y \neq 0)$.

- *Observation*: 非常容易观察到，若存在面积为n 的有理三角形，设边长为a, b, c, 且$a > b$,
则$\left(x = \frac{c^2}{4}, y = \frac{c(a^2-b^2)}{8} \neq 0\right)$ 是$E_{(n)}$ 上的有理点。


E(R)
y
x
(−n,0)
0
(n,0)
10
8
6
4
2
0
−2
−4
−6
−8
−10
−3
−2
−1
0
1
2
3
4
5
6


E(C)
6
4
2
0
−2
−4
−6
−6
−4
−2
0
2
4
6

数的几何

$$a^2 + b^2 = c^2 \qquad ab = 2n$$

$$(a \pm b)^2 = c^2 \pm 4n$$

$$(a^2 - b^2)^2 = c^4 - 16n^2$$

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c^2}{4}\right)^2 - n^2$$

$$\left(\frac{c(a^2 - b^2)}{8}\right)^2 = \left(\frac{c^2}{4}\right)^3 - n^2\left(\frac{c^2}{4}\right)$$

反过来，设(x,y)是$E_{(n)}$: $y^2=x^3-n^2x$中满足$y\neq 0$的一个有理点，则

$$a=\left|\frac{x^2-n^2}{y}\right| \quad b=\left|\frac{2xn}{y}\right| \quad c=\left|\frac{x^2+n^2}{y}\right|$$

就是一个面积为n的有理三角形的三个边。

核心：数论

数，我们应该怎样认识她？

应当从分析、代数、几何三方面来充分认识数。

核心：数论

分析方面：

- $\mathbb{A}_{\mathbb{Q}}$, $\mathbb{A}_{\mathbb{Q}}^{\times}$.
- 对一般的连通约化群G, 考虑$G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}})$上的自守形式和自守表示
- $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}}), \omega)$ 上有 $G(\mathbb{A}_{\mathbb{Q}})$ 作用，它的谱分解是自守形式分析的基础.

核心：数论

分析方面：

- $\mathbb{A}_{\mathbb{Q}}$, $\mathbb{A}_{\mathbb{Q}}^{\times}$.
- 对一般的连通约化群G, 考虑$G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}})$上的自守形式和自守表示
- $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}}),\omega)$ 上有 $G(\mathbb{A}_{\mathbb{Q}})$ 作用，它的谱分解是自守形式分析的基础.

核心：数论

分析方面：

- $\mathbb{A}_{\mathbb{Q}}$, $\mathbb{A}_{\mathbb{Q}}^{\times}$.
- 对一般的连通约化群G, 考虑$G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}})$上的自守形式和自守表示
- $L^2(G(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}}), \omega)$ 上有 $G(\mathbb{A}_{\mathbb{Q}})$ 作用，它的谱分解是自守形式分析的基础.

核心：数论

代数方面：

- $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$
- Galois 群及其子商的表示

核心：数论

几何方面：

- 代数簇over Spec$\mathbb{Q}$、概形over Spec$\mathbb{Z}$。
- 椭圆曲线，Shimura 簇等

核心：数论

几何方面：

- 代数簇over $\mathrm{Spec}\mathbb{Q}$、概形over $\mathrm{Spec}\mathbb{Z}$。
- 椭圆曲线，Shimura 簇等

核心：数论

- 对一个自守表示，Galois 表示和一个代数簇，我们可以定义L-函数或zeta-函数.
- 例如，Riemann-Zeta 函数 $\zeta(s)$, 对应着GL_1的平凡一维自守表示，$G_{\mathbb{Q}}$ 的一维平凡表示，以及 $\mathrm{Spec}(\mathbb{Z})$ zeta 函数.

核心：数论

- 对一个自守表示，Galois 表示和一个代数簇，我们可以定义L-函数或zeta-函数.
- 例如，Riemann-Zeta 函数 $\zeta(s)$, 对应着GL_1的平凡一维自守表示，$G_{\mathbb{Q}}$ 的一维平凡表示，以及 $\mathrm{Spec}(\mathbb{Z})$ zeta 函数.

核心：数论

三个方面之间的交汇:
Langlands 纲领是代数和分析的交汇、但是其问题起源、证明、扩展离不开几何。

- 分析$\longleftrightarrow$ 代数: Langlands 纲领。
- 分析$\longrightarrow$ 几何: Eichler-Shimura 理论。
- 分析$\longleftarrow$ 几何: Shimura 簇。
- 代数$\longrightarrow$ 几何: Fontain-Mazur 理论。
- 代数$\longleftarrow$ 几何: Grothendieck etale 上同调。

核心：数论

三个方面之间的交汇:
Langlands 纲领是代数和分析的交汇、但是其问题起源、证明、扩展离不开几何。

- 分析$\longleftrightarrow$ 代数: Langlands 纲领。
- 分析$\longrightarrow$ 几何: Eichler-Shimura 理论。
- 分析$\longleftarrow$ 几何: Shimura 簇。
- 代数$\longrightarrow$ 几何: Fontain-Mazur 理论。
- 代数$\longleftarrow$ 几何: Grothendieck etale 上同调。

核心：数论

三个方面之间的交汇:
Langlands 纲领是代数和分析的交汇、但是其问题起源、证明、扩展离不开几何。

- 分析$\longleftrightarrow$ 代数: Langlands 纲领。
- 分析$\longrightarrow$ 几何: Eichler-Shimura 理论。
- 分析$\longleftarrow$ 几何: Shimura 簇。
- 代数$\longrightarrow$ 几何: Fontain-Mazur 理论。
- 代数$\longleftarrow$ 几何: Grothendieck etale 上同调。

核心：数论

三个方面之间的交汇:
Langlands 纲领是代数和分析的交汇、但是其问题起源、证明、扩展离不开几何。

- 分析$\longleftrightarrow$ 代数: Langlands 纲领。
- 分析$\longrightarrow$ 几何: Eichler-Shimura 理论。
- 分析$\longleftarrow$ 几何: Shimura 簇。
- 代数$\longrightarrow$ 几何: Fontain-Mazur 理论。
- 代数$\longleftarrow$ 几何: Grothendieck etale 上同调。

核心：数论

三个方面之间的交汇:
Langlands 纲领是代数和分析的交汇、但是其问题起源、证明、扩展离不开几何。

- 分析$\longleftrightarrow$ 代数: Langlands 纲领。
- 分析$\longrightarrow$ 几何: Eichler-Shimura 理论。
- 分析$\longleftarrow$ 几何: Shimura 簇。
- 代数$\longrightarrow$ 几何: Fontain-Mazur 理论。
- 代数$\longleftarrow$ 几何: Grothendieck etale 上同调。

核心：数论

在这个对应下，L-函数应当本质上相同，因此它们有着相同的解析延拓，函数方程，Weil 猜想命题. 函数的特殊值有着个方面的算术意义.

核心：数论

- 例子：

$$E : y^2 = x^3 - n^2 x, \quad K = \mathbb{Q}(i)$$

$\rightsquigarrow \pi \in \mathcal{A}_0(\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}}))$ 尖点形式

$\rightsquigarrow \rho : \quad G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_p E)$

Langlands 对应

核心：数论

- **BSD猜想的特殊形式**
  在E上的描述
  n奇数，无平方因子，令：

$$\begin{aligned} a_n &= \#\{2x^2+y^2+8z^2=n|\ 2|z\} - \\ &\quad \#\{2x^2+y^2+8z^2=n|\ 2\not|z\} \end{aligned}$$

  则：

- (1):有理三角形C的面积为$n \Leftrightarrow\ a_n = 0$
- (2):若 $a_n \neq 0$,

$$a_n^2 = 4\sigma_0(n)\#Ш$$

  $Ш = \{$亏格为1的光滑射影曲线C，满足$\mathrm{Jac}(C) = E,\quad C(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset\}$
  $\sigma_0(n)$ 为 n 中不同的素因子个数.

核心：数论

- **BSD猜想的特殊形式**
  在E上的描述
  n奇数，无平方因子，令:

$$\begin{aligned} a_n &= \#\{2x^2+y^2+8z^2=n|\ 2|z\} - \\ &\quad \#\{2x^2+y^2+8z^2=n|\ 2\not|z\} \end{aligned}$$

  则:
- (1):有理三角形C的面积为$n \Leftrightarrow\ a_n = 0$
- (2):若 $a_n \neq 0$,

$$a_n^2 = 4\sigma_0(n)\#Ш$$

  $Ш = \{$亏格为1的光滑射影曲线C，满足$\mathrm{Jac}(C) = E,\quad C(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset\}$
  $\sigma_0(n)$ 为 n 中不同的素因子个数.

核心：数论

- **BSD猜想的特殊形式**
  在E上的描述
  n奇数，无平方因子，令:

$$\begin{aligned} a_n &= \#\{2x^2+y^2+8z^2=n|\ 2|z\} - \\ &\quad \#\{2x^2+y^2+8z^2=n|\ 2\not|z\} \end{aligned}$$

  则:
- (1):有理三角形C的面积为$n \Leftrightarrow\ a_n = 0$
- (2):若 $a_n \neq 0$,

$$a_n^2 = 4\sigma_0(n)\#Ш$$

  $Ш = \{$亏格为1的光滑射影曲线C，满足$\mathrm{Jac}(C) = E,\quad C(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset\}$
  $\sigma_0(n)$ 为 n 中不同的素因子个数.

核心：数论

定理:

n 是congurent 数，则$a_n = 0$

特别的，理解$L-$函数的特殊值，非常重要

Zeta函数特殊值

在数论中，一个**正则素数** $p > 2$ 是一个奇素数，它不整除$\mathbb{Q}(\sqrt[p]{1})$ 的类数。
正则素数很重要，是因为Kummer在推广经典Fermat的经典证明时，用理想代替数，证明$x^p + y^p = z^p$ 无非平凡的解，当p 为正则素数时。

Zeta函数特殊值

Herbrant-Ribet:

p 是正则$\Leftrightarrow p \not| \zeta(1-k), k = 2, 4 \cdots, p-3$

Fact:

$$\zeta(2n) = (-1)^{n+1} \frac{B_{2n}(2\pi)^{2n}}{n(2n)!}$$

$$\zeta(1-n) = -\frac{B_n}{n}$$

其中B_n为:

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n t^n$$

谢谢大家！