Über die Vermutung von Birch und Swinnerton-Dyer

Jingwei Zhao
jingwei.zhao@math.uni-karlsruhe.de

Fakultät für Mathematik
Institut für Algebra und Geometrie

Universität Karlsruhe

13. Dezember 2008

关于Birch和Swinnerton-Dyer猜想

美国Clay数学研究所于2000年5月宣布了七个“**千禧年数学难题**”,对每个问题悬赏一百万美圆.

BSD猜想为七个悬赏问题之一, 属于数论中的内容, 是关于方程的整数和有理数解的问题.

Hilbert第十问题是不可解的: 不存在一般方法来确定任意一个丢番图方程是否有一个整数解.

当解是一个**阿贝尔簇**的点时, Birch和Swinnerton-Dyer猜想认为, 有理点的群的大小于一个相关的L-函数 在$s = 1$附近的形态有关：**如果 $L(1) = 0$, 那么存在无限多个有理解; 相反, 则只存在有限多个.**

Birch和Swinnerton-Dyer

BSD猜想的证明情况

1977	Coates, Wiles:	证明了BSD猜想在类数为**1**的虚二次数域上和椭圆曲线有复乘的情况下部分成立.
1978	Arthaud:	把CW的证明推广到数域K的**类数**h_K**任意**的情形.
1986	Gross, Zagier:	一条**模椭圆曲线**若在 $s = 1$ 处有一个阶为1的零点, 那么它就有一个无穷阶的有理点.
1989	Kolyvagin:	证明出BSD猜想对模椭圆曲线的L-函数在$s = 1$处的阶为 0或 1 时成立.
1995	Taylor, Wiles:	证明了$\mathbb{Q}$上定义的半稳定椭圆曲线都是模曲线.
1996	加藤和也:	利用**欧拉系统**把CW的证明推广到椭圆曲线**没有复乘**的情形.
2000	Taylor等人:	证明了$\mathbb{Q}$上定义的椭圆曲线都是模曲线.

BSD猜想可以推广到任何一个**整体域**(即$\mathbb{Q}$和函数域$\mathbb{F}_q(t)$的有限扩张)上的阿贝尔簇, Artin, Tate, Kato, Trihan等人对此都有一定的研究.

预备知识

椭圆曲线的定义与性质

椭圆曲线的复乘理论

数域的量特征表: "*Größencharakter*"

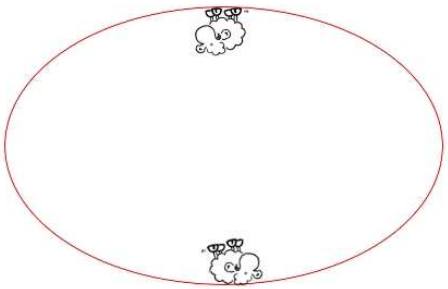
椭圆曲线的L-函数

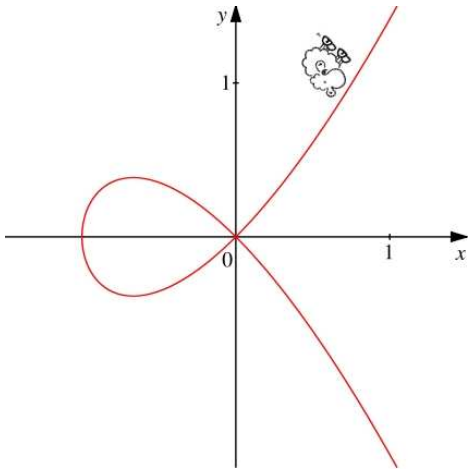
椭圆曲线的定义

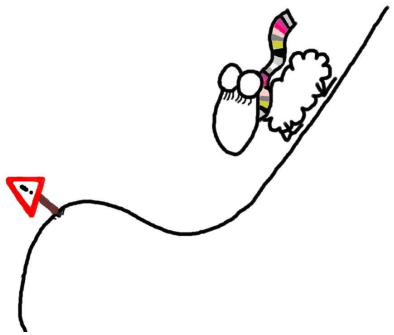
椭圆曲线一词来源于椭圆函数，椭圆函数由椭圆积分产生.

设K为任意一个域.

定义: E是一个亏格为1的正则射影曲线，O为该曲线上一点. 有序对(E, O)叫作一条椭圆曲线. 若E为定义在K上的一条曲线，并且$O \in E(K)$，那么我们称(E, O)是定义在K上的.







椭圆曲线的Weierstrass方程

椭圆曲线是一个Weierstrass方程在$\mathbb{P}^2(K)$中全部解的集合:

$$E: \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

$$a_1, ..., a_6 \in K, \quad O = [0:1:0]\text{为}E\text{的基点}.$$

可用非齐次坐标的形式表示椭圆曲线的Weierstrass方程:

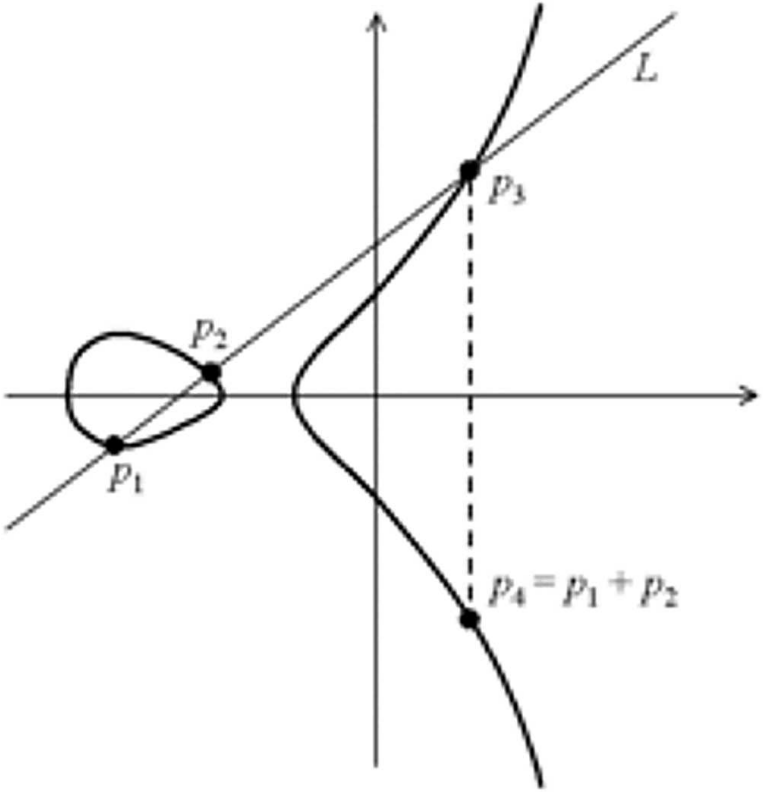
$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \qquad (1)$$

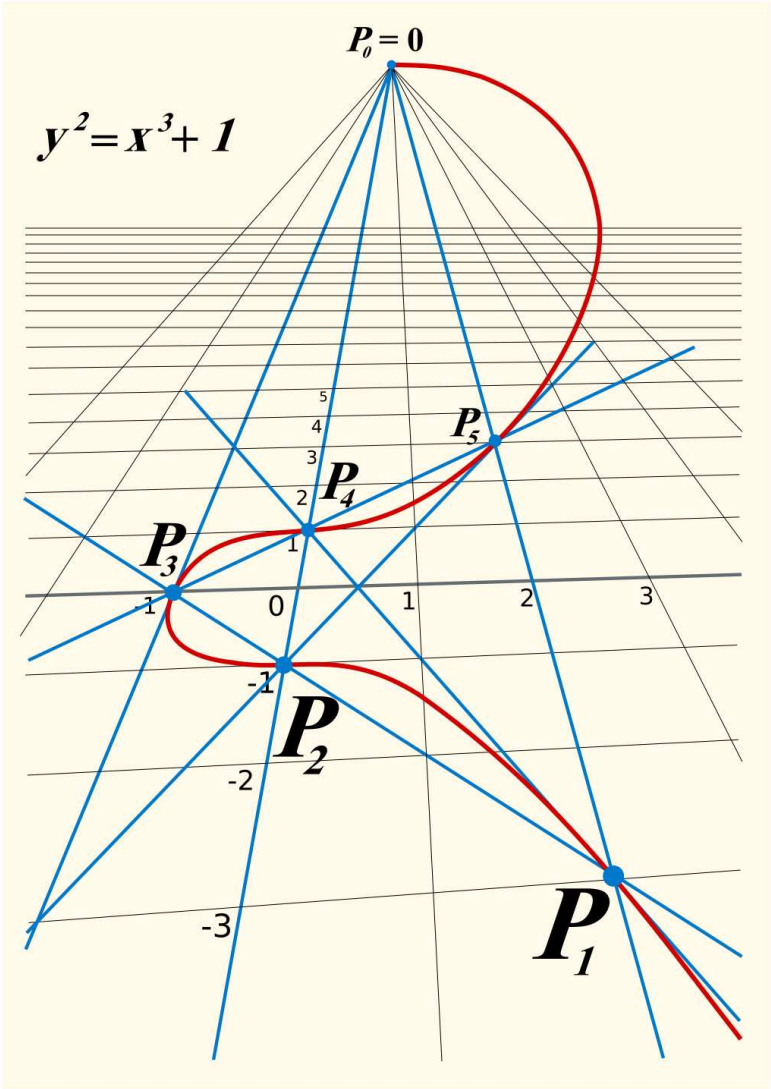
此时, 椭圆曲线就是方程(1)在射影平面$\mathbb{A}^2(K)$上的**全部解**外加上一个无穷远点O组成的集合.

当$char(K) \neq 2, 3$时, 通常采用以下简化形式的方程:

$$E: \quad y^2 = x^3 + ax + b, \quad a, b \in K\text{.这里有}4a^3 + 27b^2 \neq 0.$$

椭圆曲线的判别式 $\Delta := -16(4a^3 + 27b^2)$


L
P_3
P_2
P_1
$P_4 = P_1 + P_2$


$P_0 = 0$
$y^2 = x^3 + 1$
P_5
P_4
P_3
P_2
P_1
5
4
3
2
1
-1
0
1
2
3
-1
-2
-3

椭圆曲线的性质

基本的性质: E是一个阿贝尔群簇, 群的加法和取逆元都是代数映射

定义运算$\oplus$:
(a) $P \oplus O = P \quad \forall P \in E(K)$
(b) $P \oplus Q = Q \oplus P \quad \forall P, Q \in E(K)$
(c) $\forall P \in E(K)\ \exists (\ominus P) \in E(K): \quad P \oplus (\ominus P) = O$
(d) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R) \quad \forall P, Q, R \in E(K)$

运算$\oplus$由O唯一决定, 其可交换性也从中自动推导出.

$$E : y^2 = x^3 + ax^2 + b \quad (\mathrm{char}(K) \neq 2, 3)$$

回忆: 椭圆曲线的判别式 $\Delta := -16(4a^3 + 27b^2)$

椭圆曲线的j-不变量 $j := -1728(4a)^3/\Delta$
j-不变量唯一决定了椭圆曲线在$\overline{K}$上的同构类

定义在复域$\mathbb{C}$上的椭圆曲线

设 $E/\mathbb{C}: \ y^2 = 4x^3 - g_2x - g_3$ 为一条椭圆曲线.

$E/\mathbb{C}$为一个**复李群**, 一种特殊的具有群结构的复流形.

存在格$\mathcal{L} \subset \mathbb{C}$以及复李群之间的**解析同构** $\xi : \mathbb{C}/\mathcal{L} \xrightarrow{\sim} E(\mathbb{C})$

$$z + \mathcal{L} \longmapsto \begin{cases} (\wp(z), \wp'(z), 1) & \text{falls } z \notin \mathcal{L} \\ (0, 1, 0) & \text{falls } z \in \mathcal{L}. \end{cases}$$

这里$\wp$为格$\mathcal{L}$的Weierstrass $\wp$-函数:

$$\wp(z, \mathcal{L}) = \frac{1}{z^2} + \sum_{\omega \in \mathcal{L}, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

定义在复域$\mathbb{C}$上的椭圆曲线

一般的有以下**一一对应**关系:

$$\{\mathbb{C}\text{上的椭圆曲线}\}/\mathbb{C}\text{-同构} \xleftrightarrow{1:1} \{\mathbb{C}\text{中格}\Lambda\}/\mathbb{C}^{\times}.$$

设$E/\mathbb{C}$对应格$\mathcal{L}$. 存在以下**同构关系**:

$$\mathrm{End}_{\mathbb{C}}(E) \xrightarrow{\sim} \{\alpha \in \mathbb{C} : \alpha\mathcal{L} \subset \mathcal{L}\}.$$

对任一满足$\mathrm{char}(K) = 0$的域K总有:

$$\mathrm{End}_K(E) \cong \mathbb{Z} \text{ 或者 } \mathrm{End}_K(E) \cong \text{一个}\textbf{虚二次域}\text{的 Ordnung}\mathcal{O}.$$

在第二种情况下我们,我们称E/K有复乘$\mathcal{O}$。

Mordell-Weil定理

对于定义在代数数域K(可以嵌入复域$\mathbb{C}$)的椭圆曲线E上的K-有理点, 我们有

Mordell-Weil定理: 已知数域K以及定义其上的椭圆曲线E/K。上所有K-有理点构成一个群(Mordell-Weil群),并且该群满足以下性质:

$$E(K) \cong E_{\mathrm{tors}}(K) \times \mathbb{Z}^r.$$

我们称r为$E(K)$的秩。

有复乘的椭圆曲线对应的量特征标

设K为一个代数数域.
代数数域: 有理域$\mathbb{Q}$的**有限扩域**

对于K的一个赋值$\mathfrak{P}$, $K_{\mathfrak{P}}$为K对此赋值的**完备化**.
$\rightsquigarrow$ $K_{\mathfrak{P}}$为一个局部域, 并且满足:

$$\begin{aligned} K_{\mathfrak{P}} &= p\text{-进制域}\mathbb{Q}_p\text{的有限扩域, 若}\mathfrak{P}\text{为有限赋值;} \\ &= \mathbb{R}\text{或者}\mathbb{C}\text{,若}\mathfrak{P}\text{为无限赋值.} \end{aligned}$$

数域上的Adel环和Idel群分别定义为一个**限制积**:

$$\begin{aligned} &\text{整体域Adel环:} && \mathbb{A}_K := \prod_{\mathfrak{P}} K_{\mathfrak{P}} \\ &\text{整体域Idel群:} && \mathbb{A}_K^{\times} := \prod_{\mathfrak{P}} K_{\mathfrak{P}}^{\times} \end{aligned}$$

有复乘的椭圆曲线对应的量特征标

数域K上的**量特征标(Größencharakter)**即为一个具有某性质的连续的同态映射$\chi\colon \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$.

设K为一虚二次域, E/K为一有复乘的椭圆曲线.

$\rightsquigarrow$ 可以利用谷山丰和志村五郎建立的复乘的主定理 (Hauptsatz der komplexen Multiplikation)构造出一个量特征标ψ_K.

量特征标ψ_K主要可用来构造一个Hecke-L-函数$L(\psi_K, s)$.

数论中各种L-函数

最著名的L-函数　　**黎曼 Zeta 函数**: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$

数论里其它的L-函数　　**Dirichtlet** L-函数
Dedekind Zeta-序列
Hecke L-序列
Artin L-序列
$\vdots$
$\vdots$

椭圆曲线的L-函数

设K为一个数域, E/K一条椭圆曲线.

E作为阿贝尔簇, 可对应一个**Hasse-Weil-Zeta-函数** $L(E/K, s)$:

$$L(E/K, s) := \prod_{\mathfrak{P}} L_{\mathfrak{P}}(E/K, q_{\mathfrak{P}}^{-s})^{-1}, \quad \mathrm{Re}(s) > \frac{3}{2}.$$

这里$L_{\mathfrak{P}}(E/K, T)$为对应每个素理想$\mathfrak{P}$(即K的有限赋值)的局部L-**函数**, 由曲线在$\mathfrak{P}$处**约化映射**的性质决定。

当E有复乘时, 我们还有对应量特征标ψ_K的L-函数:

$$L(\psi_K, s) = \prod_{\mathfrak{P}} (1 - \psi_K(\mathfrak{P}) q_{\mathfrak{P}}^{-s})^{-1}.$$

椭圆曲线的L-函数

Hasse-Weil-Zeta-函数$L(E/K,s)$与ψ_F的Hecke-L-函数$L(\psi_K,s)$的性质和相互之间的关系:

Hecke:	$L(\psi_K,s)$可以解析开拓到全部复域$\mathbb{C}$上
Deuring:	$L(E/K,s)=L(\psi_K,s)\cdot L(\overline{\psi}_K,s)$
$\rightsquigarrow$	$L(E/K,s)$亦可解析开拓到全部复域$\mathbb{C}$上

Birch和Swinnerton-Dyer猜想

Mordell-Weil定理: $E(K) \cong E_{\mathrm{tors}}(K) \times \mathbb{Z}^r$.
r 为$E(K)$的秩。

BSD猜想: 假设E的Hasse-Weil-Zeta-函数 $L(E/K, s)$ 可开拓成$\mathbb{C}$上的解析函数,那么$L(E/K, s)$在$s = 1$处零点的阶恰好为$E(K)$的秩 r。

Coates-Wiles定理

Coates-Wiles定理: 设K为一个类数(即K的理想类群的元素个数)为1的虚二次域, E/K为一条有复乘$\mathcal{O}_K$的椭圆曲线. 那么当E的秩$r \geq 1$时, E的Hasse-Weil-Zeta函数$L(E/K, s)$在$s = 1$处取值为0.

证明中主要用到的数学工具: 形式群与形式模, Lubin-Tate理论
椭圆单位元
整体类域论

形式群理论

“没有具体群元素的群的运算法则”

一个代数群可以配一个形式群，通过研究该形式群研来研究代数群的性质

形式群理论的应用: 椭圆曲线理论

代数数域中的**局部类域论**(针对局部域的)

(一维)形式群

设 $\mathcal{O}$ 为一个含1元素的交换环。

定义: 一个$\mathcal{O}$上的一维形式群$\mathcal{F}$就是一个满足以下性质的形式幂级数$\mathcal{F}(X,Y) \in \mathcal{O}[[X,Y]]$:

(i) $\mathcal{F}(X,Y) \equiv X+Y \mod \deg 2$

(ii) $\mathcal{F}(X,\mathcal{F}(Y,Z)) = \mathcal{F}(\mathcal{F}(X,Y),Z)$. **结合律**

如果还有以下性质(iii)成立,则称 $\mathcal{F}$ 为一个可交换的形式群:

(iii) $\mathcal{F}(X,Y) = \mathcal{F}(Y,X)$. **交换律**

例: (i) 加法形式群 $\mathbb{G}_a(X,Y) = X+Y$.
(ii)乘法形式群 $\mathbb{G}_m(X,Y) = X+Y+XY$.

我们把环$\mathcal{O}$上形式群$\mathcal{F}$, $\mathcal{G}$的同态映射与同构映射定义为满足某些性质的**幂级数**$f(X) \in \mathcal{O}[[X]]$.

(一维)形式模

定义: 一个一维形式$\mathcal{O}$模就是$\mathcal{O}$上一个形式群$\mathcal{F}$和一个环同态:

$$\mathcal{O} \longrightarrow \mathrm{End}_{\mathcal{O}}(\mathcal{F}), \quad \alpha \longmapsto [\alpha]_{\mathcal{F}}(X),$$

并且该同态要满足条件

$$[\alpha]_{\mathcal{F}}(X) \equiv \alpha X \mod \deg 2.$$

代数数论中重要的形式模: 对应赋值环$\mathcal{O}$中某一素元素π的 **Lubin-Tate-形式$\mathcal{O}$-模**

- 所有对π的Lubin-Tate形式$\mathcal{O}$-模都同构
- 特别地, 我们有对π的特殊Lubin-Tate形式$\mathcal{O}$-模

应用: 椭圆曲线理论, 如CW对BSD猜想的证明; 局部类域论.

从一个形式模出发可以构造一个普通模.

椭圆曲线与形式群，形式模

定义在商域的特征不为2的无零因子环$\mathcal{O}$上的椭圆曲线$E/\mathcal{O}$可以对应一个形式群 $\widehat{E}$: 利用参数变换

$$(x, y) \longmapsto -\frac{2x}{y}.$$

特别的，对某些具有特殊性质的椭圆曲线E，其对应的 $\widehat{E}$ 可以成为一个对应素元素$\psi_K(\mathfrak{P})$的Lubin-Tate模。

椭圆单位元

来源于复乘理论

为椭圆模函数在特殊点处的取值

椭圆单位元构成虚二次域上有限阿贝尔扩域的代数整数环单位群的一个子群

大量应用在CW对BSD猜想的证明中

椭圆单位元的构造

设K为一个虚二次域.设$\mathcal{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ 为$\mathbb{C}$中一个格，E/K为对应格$\mathcal{L}$并且**有复乘**的的椭圆曲线。

定义格$\mathcal{L}$的Theta函数:

$$\theta(z, \mathcal{L}) := \Delta(\mathcal{L}) e^{-6\eta(z,\mathcal{L})z} \sigma(z, \mathcal{L})^{12}.$$

其中 $\sigma(z, \mathcal{L}) = z \prod'_{\omega \in \mathcal{L}} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2}$ Weierstrass σ-函数

$\Delta(\mathcal{L}) = g_2^3(\mathcal{L}) - 27 g_3^2(\mathcal{L})$ $\mathcal{L}$的判别式函数

利用Theta函数构造函数$\Theta(z, A, \mathcal{N})$; A为一理想集，$\mathcal{N}$为一下标集.

椭圆单位元群$\mathcal{C}_n$为$\Theta(z, A, \mathcal{N})$在格$\mathcal{L}$一本原分割点处取值之集合.

类域论

为代数数论的一个分支.

主要定理为数域的阿贝尔扩域的**Artin**互反律.


Hilbert


Furtwängler


Weber


高木贞治


Artin

类域论

类域论的发展情况:

- 1898 Hilbert类域论, 对**Gauss二次互乎反律**的自然推广.
  Hilbert提出猜想: 对任一数域K 存在一个阿贝尔扩域H使得
  (1) 伽罗华群$G(H/K)$与理想类群Cl_K同构
  (2) H/K不分歧 (对所有素理想)
  (3) $\mathfrak{p}$的惯性度f恰好为$\mathfrak{p}$在Cl_K中的剩余类次数
  (4) K的理想到H里均为主理想
- 1907 Furtwängler证明出前三条
- 1908 Weber引入广义理想类群,作出一般的类域论的猜想
- 1920 高木贞治证明了一般类域的存在
- 1927 Artin大体上完成了类域论
- 1930 Furtwängler证明出第四条

整体类域论

整体类域论的主定理: 设K为任一数域。那么所有**有限阿贝尔扩域**L/K与K的**射群**(Strahlgruppe)一一对应。

典范映射 $r_{L/K}$: $G(L/K) \xrightarrow{\sim} C_K/N_{L/K}C_L$.

存在一个**满**同态映射"**范数剩余符号**":

$$[\ ,L/K]: \quad \mathbb{A}_K^\times \longrightarrow G(L/K).$$

CW对BSD猜想的大体证明步骤

Coates-Wiles定理: 设K为一个类数(即K的理想类群的元素个数)为1的虚二次域, E/K为一条有复乘$\mathcal{O}_K$的椭圆曲线. 那么当E的秩$r \geq 1$时, E的Hasse-Weil-Zeta函数$L(E/K, s)$在$s = 1$处取值为0.

取一个满足某给定性质(*)的素数p,
定义一个由椭圆曲线E/K决定的, 以$k(k=0,\ldots,p-1)$为参数的量λ_k.

记G_0为扩域$K(E_\pi)/K$的伽罗华群. 对每一个非负整数n, 利用椭圆单位元素群$\mathcal{C}_n$构造一个群代数$\mathbb{Z}_p[G_0]$的模M_n,
把M_n典范分解为一个子模的直和: $M=\bigoplus_{k=0}^{p-1} M_n^{(k)}$.

利用形式模的Lubin-Tate理论证明λ_k可被K中每一个p上的素理想$\mathfrak{p}$整除.

证明等价关系: (a) λ_k可被$K(E_\pi)$中所有$\mathfrak{p}$上的素理想$\mathfrak{q}$整除.
(b) $\exists n\in\mathbb{N}_0$, 使得 $1\le k\le p-2$ 都有$M_n^{(k)}\neq 1$成立.

证明存在$n\in\mathbb{N}_0$使得$M_n^{(1)}\neq 1 \rightsquigarrow \lambda_1 =$非零常数$\cdot L_K(\overline{\psi}_K,1)\equiv 0 \bmod \mathfrak{q}$.

利用Čebotarev密度定理证明存在无穷多个符合性质(*)的素数p
$\rightsquigarrow \lambda_1$可被$K(E_\pi)$中无穷多个素理想$\mathfrak{q}$整除 $\rightsquigarrow L_K(\overline{\psi}_K,1)=0$.

最后利用Deuring乘积式推出:

$$L(E/K,1)=L_K(\psi_K,1)\cdot L_K(\overline{\psi}_K,1)\cdot \text{有限多个Euler乘积}=0 \qquad \square$$

How to get rich?