$$\text{MW} \Longrightarrow \text{弱 MW}$$

$$E(K)\ \text{f.g.} \overset{?}{\Longleftarrow} E(K)/mE(K)\ \text{有限.}$$

1. Fermat 递降法

Fermat 证明 $x^4+y^4=z^4$ 无非平凡解.

Pf 反证法. 若有解 ≠ 非平凡解. $(x,y,z) \in \mathbb{Z}^3$ 不妨设两两互素（否则 $p|x, p|y \Rightarrow p|z$，可约去 p），那么 $x, y, w=z^2$ 是 $x^4+y^4=w^2$ 的（非平凡）解.

仍有 x, y, w 之间两两互素.

无穷递降法的策略：x, y, w 是 (*) $x^4+y^4=w^2$ 的解

设法从 (x,y,w) 开始出发造出一个 w 值更小的解，从而矛盾。

具体构造：(x^2, y^2, w) 是一组勾股数.

于是 $\begin{cases} x^2 = u^2-v^2 \\ y^2 = 2uv \\ w = u^2+v^2 \end{cases}$ $u, v \in \mathbb{Z}$

由 x, y, w 两两互素 $\Rightarrow \gcd(u,v)=1$

且 u 奇 v 偶.

$$\left.\begin{matrix} y^2 = \underset{\text{奇}}{u}\cdot\underset{\text{偶}}{2v} \quad \text{是个平方数} \\ \gcd(u,v)=1 \end{matrix}\right\} \Rightarrow \begin{cases} u = a^2 \\ v = 2b^2 \\ \text{且 } \gcd(a,b)=1 \end{cases}$$

于是 $x^2 = u^2-v^2 = a^4-4b^4 \Rightarrow x^2+(2b^2)^2=(a^2)^2$

故 $(x, 2b^2, a^2)$ 是一组勾股数 且两两互素.

从而 $\begin{cases} x = c^2-d^2 \\ 2b^2 = 2cd \\ a^2 = c^2+d^2 \end{cases}$ 且 $\gcd(c,d)=1$.

$$\left.\begin{matrix} b^2 = cd \\ \gcd(c,d)=1 \end{matrix}\right\} \Rightarrow \begin{cases} c = r^2 \\ d = s^2 \\ \gcd(r,s)=1 \end{cases}$$

$r^4+s^4 = c^2+d^2 = a^2$ 且 r, s, a 两两互素

(r, s, a) 是 (*) 的解

$a \le a^2 = u \le u^2 < w$ 与 w 的最小性矛盾 #

$a \le a^2 = u \le u^2 < w$ 与 w 的最小性矛盾 #

Cor（大炮打蚊子） $\sqrt[4]{2}$ 是无理数 $\quad x^4+y^4=z^6 \quad (1,1,\sqrt[4]{2})$

（同理，Fermat 大定理 $\Rightarrow \forall n \ge 3 \quad \sqrt[n]{2} \notin \mathbb{Q}$）

Rk 无穷递降的证明，用到的关键性质"正整数的大小"这个量不可能一直向下降，总要有限步停下来。

弱 MW $\Longrightarrow$ MW

此时需要在 $E(K)$ 上定义一个用于衡量"大小"的量

Recall. 线性代数中"大小"用范数来衡量，由正定双线性型导出。

$\mathbb{R}$-向量空间 $\rightsquigarrow$ "$\mathbb{Z}$-向量空间" $\mathbb{Z}$-模（= Abel 群）A.

Def 称 $\underset{\text{Abel群}}{q: A} \longrightarrow \mathbb{R}$ 为一个二次型，若 $\forall P, Q \in A$

$$q(P+Q)+q(P-Q)=2q(P)+2q(Q)$$

（$\Longleftrightarrow$ 平行四边形法则 $\|x+y\|^2+\|x-y\|^2=\|x\|^2\times 2+2\|y\|^2$）

- 取 $P=Q=0 \Rightarrow q(0)=0$
- 取 $P=Q \Rightarrow q(2P)=4q(P)$
- 取 $P=-Q \Rightarrow q(-P)=q(P)$
- 取 $Q=2P \Rightarrow q(3P)=9q(P)$
- 归纳 $\Rightarrow q(nP)=n^2 q(P) \quad \forall n \in \mathbb{N}$ ($\mathbb{Z}$)

若 $P \in A$ 是扭元（$\exists n \in \mathbb{N} \quad nP=0$）$\Rightarrow q(P)=0$

Def 称实值函数 f 具有 Northcott 性质 若 $\forall B \in \mathbb{R}$

$\{x \mid f(x) \le B\}$ 是有限集

若二次型 $q: A \to \mathbb{R}$ 还具有 Northcott 性质，则由上述知 $A_{tor}=\{P \in A \mid \exists n \in \mathbb{N} \quad nP=0\}$ 是个有限群。

此时还必有 q 是半正定的（$\forall x \in A \quad q(x) \ge 0$）

（否则 $\exists x_0 \in A$，$q(x_0)<0$，$\neq 0$ $\quad x_0$ 不是扭元 $\forall n \in \mathbb{N} \quad q(nx_0)=n^2 q(x_0)<0$

(否则 $\exists\, x_0\in A$, $g(x_0)\underset{\neq 0}{<}0$, x_0 不是挠元 $\forall n\in\mathbb{N}$ $g(nx_0)=n^2g(x_0)<0$
这与 Northcott 性质矛盾).

于是 $|x|:=\sqrt{g(x)}\in\mathbb{R}_{\geq 0}$

直接考虑 $g(\cdot)$ 或 $|\cdot|$, "挠元" $\mapsto 0$, 只需考虑 "A/A_{tor}": 自由Abel群
自由 $\mathbb{Z}$-模

"$\mathbb{Z}$-线性组合 $\rightsquigarrow$ $\mathbb{Q}$-线性组合" $\rightsquigarrow$ $\mathbb{Q}$-向量空间.

交换代数中, $(A/A_{tor})\otimes_{\mathbb{Z}}\mathbb{Q}\cong A\otimes_{\mathbb{Z}}\mathbb{Q}$.

即允许 $\frac{n}{m}P$ 这种元素 ($\frac{n}{m}\in\mathbb{Q}$, $P\in A$)

此时定义 $g(\frac{n}{m}P)=\frac{n^2}{m^2}g(P)$ 则把 g 从在 A 上定义延拓到 $A\otimes_{\mathbb{Z}}\mathbb{Q}$ 上定义.

※. 这时是 $\mathbb{Q}$-向量空间 $A\otimes_{\mathbb{Z}}\mathbb{Q}$ 上经典的二次型 (即是正定的)

利用极化恒等式, 令 $f(P,Q)=\frac{1}{4}\big(g(P+Q)-g(P-Q)\big)$ 则 $f(P,P)=g(P)$

是 $A\otimes_{\mathbb{Z}}\mathbb{Q}$ 上的对称双线性型, 且是半正定的. ($|P|=\sqrt{g(P)}$)

仍有 Cauchy-Schwarz 不等式 $|f(P,Q)|\leq|P|\cdot|Q|$
(但 "=" 条件并不一定是 P,Q 成比例)

由 C-S $\Rightarrow$ 三角不等式 $|P+Q|\leq|P|+|Q|$

以下引理说明 "弱MW" $\Rightarrow$ "MW"

<u>Lem</u> A: Abel群, 若存在一个二次型 $g: A\to\mathbb{R}$ 满足 <u>Northcott 性质</u>.
若 $A/2A$ 有限, 则 A 有限生成。

若记 S 为 $A/2A$ 一组代表元, 令 $B_0=\max\limits_{x\in S}g(x)$ (≥ 1, 否则以 $B_0=0$ 替换)

那么 $\{x\in A\mid g(x)\leq B_0\}$ 生成 A.
有限集

Pf. 令 $x\in A$ 且 $\overset{|x|>\sqrt{B_0}}{g(x)>B_0}$, 我们将定义一个序列 $(x_n)_{n\geq 0}$.

$x_0=x$ 可写成 $x_0=y_1+2x_1$ 其中 $y_1\in S$ $x_1\in A$
再把 x_1 写成 $x_1=y_2+2x_2$ 其中 $y_2\in S$, $x_2\in A$ . . .

再把 x_1 写成 $x_1 = y_2 + 2x_2$ 其中 $y_2 \in S$，$x_2 \in A$ ...

于是 $|x_1| = \frac{1}{2}|x_0 - y_1| \le \frac{1}{2}(|x_0| + |y_1|) \le \frac{1}{2}(|x_0| + \sqrt{B_0}) < |x_0|$

同理：只要 $|x_n| > \sqrt{B_0}$ 则 $|x_n| < |x_{n-1}| < \cdots < |x_1| < |x_0|$

由 Northcott 性质，这无法一直持续下去，从而有限步之后必有 $|x_n| \le \sqrt{B_0}$

此时 $x = x_0$ 是 $y_i \in S$ 以及 x_n 的 $\mathbb{Z}$-线性组合，

即 $\{x \in A \mid q(x) \le B_0\}$ 生成了 A. #.

小结：想要证明 Mordell-Weil 定理

① 要构造出一个满足 Northcott 性质的二次型 $q: E(K) \to \mathbb{R}$

(事实上得到的还是正定的)

② 证明弱 MW：$E(K)/mE(K)$ 有限

① ⟶ 引入"高度"来衡量"有理点的大小" —— 算术复杂度。

② ⟶ 引入 Galois 上同调理论，用代数数论得出某上同调的有限性

从而控制 $E(K)/mE(K)$ 的大小。

2. 高度

从最简单的情况开始 $K = \mathbb{Q}$. $\mathbb{P}^n$ 上.

$\forall P \in \mathbb{P}^n(\mathbb{Q})$ $\quad P = (x_0 : \cdots : x_n)$

不妨前设 $x_i \in \mathbb{Z}$ 且 $\gcd(x_0, \cdots, x_n) = 1$

此时定义 P 的高度/对数高度为

$$H_{\mathbb{Q}}(P) = \max(|x_0|, \cdots, |x_n|) \qquad \& \quad h_{\mathbb{Q}} = \log H(P)$$

乘法记号 $\qquad$ 加法记号

Rk

Rk "$H_{\mathbb{Q}}$ 良好定义"，这是依赖于 $\mathbb{Z}$ 中有唯一分解，于是无法简单直接推广到一般代数数域 K 上（$\mathcal{O}_K$ 不一定是 UFD）

例. 也可定义 $\underset{x}{\mathbb{Q}} = \mathbb{A}^1(\mathbb{Q}) \subset \mathbb{P}^1(\mathbb{Q})$ $\qquad H_{\mathbb{Q}}(x) := H_{\mathbb{Q}}(x:1)$

例如 π 的近似值 $\pi_1 = \frac{22}{7}$ 与 $\pi_2 = \frac{355}{113}$ 更复杂

$H(\pi_1) = H_{\mathbb{Q}}(\frac{22}{7}:1) = H_{\mathbb{Q}}(22:7) = |22| = 22$

例如 π 的近似值 $\pi_1 = \frac{22}{7}$ 与 $\pi_2 = \frac{355}{113}$

$$H_{\mathbb{Q}}(\pi_1) = H_{\mathbb{Q}}\left(\tfrac{22}{7} : 1\right) = H_{\mathbb{Q}}(22 : 7) = |22| = 22$$

$$H_{\mathbb{Q}}(\pi_2) = 355.$$

Prop $P \in \mathbb{P}^n(\mathbb{Q})$ 任取齐次坐标 $P = (x_0 : x_1 : \cdots : x_n)$ 则有

$$H_{\mathbb{Q}}(P) = \prod_{v \in \Omega_{\mathbb{Q}}} \max(|x_0|_v, \cdots, |x_n|_v)$$

$\Omega_{\mathbb{Q}} = \{p\} \cup \{\infty\}$ （平凡赋值为有限 $\prod$，$p|$ 某个分母或分子 才有 p-adic $|\ |_p \neq 1$）

Pf. 首先由乘积 $\prod_{v \in \Omega_{\mathbb{Q}}} |x|_v = 1$ 可知上述右式不依赖于 P 的齐次坐标的选取。于是不妨取为 $x_i \in \mathbb{Z}$ 且 $\gcd(x_0, \cdots, x_n) = 1$.

这时，对于 $v = p$ 为素数，则有 $\max(|x_0|_p, \cdots, |x_n|_p) = 1$

右式只剩 $v = \infty$ 一项. $\max(|x_0|_\infty, \cdots, |x_n|_\infty)$ 即 $H_{\mathbb{Q}}(P)$. #

Rk. 右式可直接推广到数域 K 上：（只依赖于 $\prod_{v \in \Omega_K} |x|_v = 1$ $(\forall x \in K^*)$）

$\forall P \in \mathbb{P}^n(K)$

$$H_K(P) := \prod_{v \in \Omega_K} \max(|x_0|_v, \cdots, |x_n|_v)$$

良好定义，不依赖于 P 的齐次坐标选取.

$$N\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$$

$v = \mathfrak{p}$ 素理想 $|x|_{\mathfrak{p}} = (N\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$

$v = \sigma : K \hookrightarrow \mathbb{R}$ 或 $\mathbb{C}$ 则取

$$|x|_\sigma = \begin{cases} |x| & \text{实嵌入} \\ |x|^2 & \text{复嵌入} \end{cases}$$

由代数数论的知识：

Lem. K'/K 为数域的有限扩张，则 $\forall P \in \mathbb{P}^n(K) \subset \mathbb{P}^n(K')$

$$H_{K'}(P) = H_K(P)^{[K':K]}$$

$$H_{K'}(P) = H_K(P)^{[K':K]}$$

由此可定义 $\mathbb{P}^n(\overline{\mathbb{Q}})$ 上的点的高度

Def $\forall P \in \mathbb{P}^n(\overline{\mathbb{Q}})$ 取数域 K 使 $P \in \mathbb{P}^n(K)$

令 $H(P) := H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$ （良定义，不依赖 K 的选取）

同理定义 $\alpha \in \overline{\mathbb{Q}} = \mathbb{A}(\overline{\mathbb{Q}}) \subset \mathbb{P}^1(\overline{\mathbb{Q}})$ $\quad H(\alpha) := H(\alpha : 1)$

$$\alpha \longmapsto (\alpha : 1)$$

目标：希望建立 H 的 Northcott 性质：高度有界的点只有有限个.

需若干引理.

Recall Gauss 引理，$f, g \in \mathbb{Z}[x]$

$c(f)$ = 容量 = f 的系数的最大公约数.

$c(fg) = c(f) \cdot c(g)$

$f = \sum a_n X^n$

$g = \sum b_n X^n$

$f \cdot g = \sum c_n X^n$

$c_n = \sum_k a_{n-k} b_k$

Lem (Gauss) K 数域，$v \in \Omega_K$ 非阿基米德赋值（即 $v = v_{\mathfrak{p}}$，$\mathfrak{p} \subset \mathcal{O}_K$）

令 $P, Q \in K[x]$，记 $\|P\|_v$ = P 的系数的 $|\cdot|_v$ 值的最大值.

那么 $\|PQ\|_v = \|P\|_v \cdot \|Q\|_v$

Lem 令 α 为代数数 $\alpha \in \overline{\mathbb{Q}}$，$K = \mathbb{Q}(\alpha)$

α 在 $\mathbb{Z}[x]$ 中极小多项式（系数 $\gcd = 1$）记为

$$P(x) = a_0(x - \alpha_1) \cdots (x - \alpha_d) = a_0 x^d + \cdots$$

那么 $H_K(\alpha) = |a_0| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$ （其中 $|\cdot|$ 是 $\mathbb{C}$ 中模长）

Pf 加入 α 的所有共轭元得到域 $L = \mathbb{Q}(\alpha_1, \cdots, \alpha_d)$.

$$\Omega_L = \Omega_L^f \sqcup \Omega_L^\infty$$

$$(*) \quad H_K(\alpha)^{[L:K]} = H_L(\alpha) = \prod_{\mathfrak{q} \in \Omega_L^f} \max(1, |\alpha|_{\mathfrak{q}}) \cdot \prod_{w \in \Omega_L^\infty} \max(1, |\alpha|_w)$$

$\mathfrak{q}\in\Omega_L$

对于无穷位，有：

$$\prod_{w\in\Omega_L^\infty}\max(1,|\alpha|_w)=\prod_{v\in\Omega_K^\infty}\max(1,|\alpha|_v)^{[L:K]}=\left(\prod_{i=1}^{d}\max\{1,|\alpha_i|\}\right)^{[L:Q]}$$

对于有限位，有L上用关于 $\mathfrak{q}\in\Omega_L^f$ 用 Gauss 引理，对于 $P(x)$ 的分解有：

$$1=\|P\|_{\mathfrak{q}}=|a_0|_{\mathfrak{q}}\cdot\prod_{i=1}^{d}\max(1,|\alpha_i|_{\mathfrak{q}})$$

对 $\mathfrak{q}\in\Omega_L^f$ 求积

$$1=\underbrace{\prod_{\mathfrak{q}\in\Omega_L^f}|a_0|_{\mathfrak{q}}}\prod_{i=1}^{d}\prod_{\mathfrak{q}\in\Omega_L^f}\max(1,|\alpha_i|_{\mathfrak{q}})$$

共轭元的 $\mathfrak{q}$-adic $|\cdot|_{\mathfrak{q}}$ 一样大

L上积公式 $\prod_{w\in\Omega_L}|x|_w=1$

$$=|a_0|^{-[L:Q]}\left(\prod_{\mathfrak{q}\in\Omega_L^f}\max(1,|\alpha|_{\mathfrak{q}})\right)^{d}$$

上述代入两式整理得

$$H_K(\alpha)^{[L:K]}=|a_0|^{[L:Q]/d}\cdot\prod_{i=1}^{d}\max(1,|\alpha_i|)^{[L:K]}$$

同时开 $[L:K]$ 次方得 $\qquad [L:K]\cdot[K:Q]=[L:Q]$

$$H_K(\alpha)=|a_0|\cdot\prod_{i=1}^{d}\max(1,|\alpha_i|).$$

#