n^2+1 的最大素因子以及关于次指数 ABC 猜想的改进

Hector Pasten

- Received: 27 December 2023
- Accepted: 9 February 2024
- Published online: 26 February 2024

摘要

我们结合超越方法和 ABC 猜想的模方法，证明了 n^2+1 的最大素因子至少为 $\frac{(\log_2 n)^2}{\log_3 n}$，其中 $\log_k$ 是对数函数的第 k 次迭代。这显著改进了现有的最佳估计，此前的估计本质上是 $\log_2 n$ 量级的，最早可追溯到 1934 年乔拉（Chowla）的工作。利用相同的思路，我们在 ABC 猜想的次指数界方面也取得了重大进展，在一种情况下，首次改进了斯图尔特（Stewart）和余（Yu）二十多年前的一个结果。我们方法的核心是作者所建立的志村曲线与 ABC 猜想之间的联系。

Part I

引言

对于非零整数 n，设 $\mathscr{P}(n)$ 为 n 的最大素因子，并规定 $\mathscr{P}(\pm 1)=1$。给 $\mathscr{P}(f(n))$ 确定下界是一个经典问题，其中 f 是整系数非线性多项式。1934 年，乔拉 [1] 证明存在正常数 κ，使得当 n 增大时，有

$$\mathscr{P}\left(n^2+1\right) \geq \kappa \cdot \log_2 n \tag{1.1}$$

这里 $\log_k$ 是对数函数的第 k 次迭代（对于迭代对数，我们总是假设自变量足够大以保证其有定义）。从那以后，这个结果被推广到所有多项式（参见 [9] 及其中的参考文献），但 90 年过去了，乔拉定理仅有一些小的改进：据作者所知，目前最精确的估计是通过对数线性形式理论得到的，其形式为

$$\mathscr{P}\left(n^2+1\right) \geq \kappa \cdot \frac{\log_3 n}{\log_4 n} \cdot \log_2 n,$$

见 [9]。我们证明了 $\mathscr{P}(n^2+1)$ 的一个下界，几乎是之前界的平方：

定理 1.1. *存在常数 $\kappa > 0$，使得当 n 增大时，有*

$$\mathscr{P}\left(n^2+1\right) \geq \kappa \cdot \frac{(\log_2 n)^2}{\log_3 n}$$

对于正整数 n，设 $\mathrm{rad}(n)$ 为其根基，即 n 的最大无平方因子除数。实际上，前面的结果是下一个定理的直接推论：

定理 1.2. *存在常数 $\kappa > 0$，使得当 n 增大时，有*

$$rad\left(n^2+1\right) \geq \exp\left(\kappa \cdot \frac{(\log_2 n)^2}{\log_3 n}\right)$$

上述定理的证明结合了对数线性形式理论，以及作者利用志村曲线理论 [7] 发展的 ABC 猜想的模方法相关结果。特别地，这些方法涉及超越数论和算术几何两个领域。更确切地说，当我们将对数线性形式应用于这个问题时，会把 n^2+1 分解式中指数较大的素数与指数较小的素数分开。然后，对于每个 n，我们构造一条椭圆曲线，并将 [7] 中的结果应用于这条椭圆曲线，从而对 n^2+1 中指数较大的素因子个数给出一个较好的界。在此之后，我们利用这个新的信息，再回到对数线性形式提供的界，进而得出结论。本文所开发的技术并不局限于前面这两个定理。事实上，我们方法的另一个应用是，能够改进 ABC 猜想现有的最精确次指数界。让我们回顾一下这个问题的表述。

猜想 1.3. *（马瑟 - 奥斯特勒 ABC 猜想）设 $\epsilon > 0$，存在仅依赖于 ϵ 的数 $\kappa_\epsilon > 0$，使得以下结论成立：给定互素的正整数 a、b、c，且 $a+b=c$，我们有 $c \leq \kappa_\epsilon \cdot rad(abc)^{1+\epsilon}$ 。*

在接下来的内容中，设 $R=\mathrm{rad}(abc)$，其中 a、b、c 是 ABC 猜想陈述中的三元组，术语“绝对常数”是指与所有参数无关的数。目前，最好的无条件界由斯图尔特 - 余 [12] 给出，其形式为

$$\log c \leq \kappa \cdot R^{1/3} (\log R)^3$$

对于某个绝对常数 κ。也可参见 [5, 10, 11] 中其他的无条件界。虽然所有这些界关于 R 都是指数形式的，但在某些情况下可以得到更好的次指数界：

1.（见作者的 [6]）设 $\epsilon>0$，存在仅依赖于 ϵ 的数 $\kappa_\epsilon>0$，使得如果对于某个 $\eta>0$ 有 $a\le c^{1-\eta}$，那么

$$\log c\le \eta^{-1}\cdot\kappa_\epsilon\cdot\exp\left((1+\epsilon)\cdot\frac{\log_3 R}{\log_2 R}\cdot\log R\right)$$

2.（见斯图尔特和余的 [12]）设 $q=\min\{\mathscr{P}(a),\mathscr{P}(b),\mathscr{P}(c)\}$。那么对于某绝对常数 $\kappa>0$，我们有

$$\log c\le q\cdot\exp\left(\kappa\cdot\frac{\log_3 R}{\log_2 R}\cdot\log R\right)$$

我们的方法对这两个界都有显著改进：

定理 1.4. *设 a、b、c 遍历互素正整数三元组且满足 $a+b=c$，并记 $R=rad(abc)$。那么有以下界：*

1. 存在绝对常数 $\kappa>0$，使得如果对于某个 $\eta>0$ 有 $a\le c^{1-\eta}$，那么

$$\log c\le \eta^{-1}\exp\left(\kappa\cdot\sqrt{(\log R)\log_2 R}\right)$$

2. 设 $q=\min\{\mathscr{P}(a),\mathscr{P}(b),\mathscr{P}(c)\}$。存在绝对常数 $\kappa>0$，使得

$$\log c\le q\cdot\exp\left(\kappa\cdot\sqrt{(\log R)\log_2 R}\right)$$

值得指出的是，前面定理的第 2 项是二十多年来对 [12] 中定理 2 的首次改进。利用定理 1.4 的第 2 项，我们还得到了对 [12] 中界（7）的如下改进：

推论 1.5. *存在绝对常数 $\kappa>0$，使得当 $x<y$ 遍历互素正整数时，我们有*

$$\mathscr{P}(xy(x+y))\ge\kappa\cdot\frac{(\log_2 y)^2}{\log_3 y}$$

而 [12] 中的界（7）为

$$\mathscr{P}(xy(x+y))\ge\kappa\cdot\frac{(\log_2 y)\log_3 y}{\log_4 y}$$

这反过来又是对范德波滕（van der Poorten）、辛泽尔（Schinzel）、肖里（Shorey）和蒂德曼（Tijdeman）[14] 早期界

$$\mathscr{P}(xy(x+y))\ge\kappa\cdot\log_2 y$$

的改进。正如读者将看到的，通过一些整理工作，可以得到定理 1.1、1.2、1.4 以及推论 1.5 中 κ 的显式值，这些值对于足够大的变量值是有效的。我们把这个任务留给感兴趣的读者。

Part II

预备知识

1　对数线性形式的界

我们需要埃弗特斯（Evertse）和焦里（Győry）给出的关于有限生成乘法群逼近的估计（参见 [3] 中的定理 4.2.1），它来自对数线性形式理论和数的几何理论。

首先引入一些符号。设 k 是一个在 $\mathbb{Q}$ 上次数为 d 的数域。如果 v 是 k 的一个阿基米德位，与嵌入 $\sigma: k \to \mathbb{C}$ 相关（它可以是实嵌入，也可以是一对复共轭嵌入之一），我们在 k 上定义 v–adic 范数

$$|x|_v = |\sigma(x)|^{\epsilon_v}$$

其中 $|\cdot|$ 是通常的复数绝对值，并且当 σ 是实嵌入时 $\epsilon_v = 1$，当 σ 是复嵌入时 $\epsilon_v = 2$。另一方面，如果 v 是 k 的一个非阿基米德位，与 O_k 的一个素理想 $\mathfrak{p}$ 相关，我们令 $v_{\mathfrak{p}}$ 是 k 上的 $\mathfrak{p}$–adic 赋值，并定义 v–adic 范数

$$|x|_v = \mathrm{Norm}(\mathfrak{p})^{-v_{\mathfrak{p}}(x)}$$

在 $k = \mathbb{Q}$ 的情况下，当 p 是素数时，我们简单地用 v_p 表示 p–adic 赋值。

k 上的高度定义为

$$h(x) = \frac{1}{d}\sum_v \log\max\{1, |x|_v\}$$

设 Γ 是 k^* 的一个有限生成乘法子群，并且 $\{\xi_1, \ldots, \xi_m\} \subseteq \Gamma$ 是 $\Gamma/\Gamma_{\mathrm{tor}}$ 的一组生成元，其中 $m \geq 1$。在这些符号和假设下，由 [3] 中的定理 4.2.1，我们得到：

定理 2.1. *（逼近界）存在仅依赖于 d 的数 K_d，使得以下结论成立：*

1. *（阿基米德界）设 v 是 k 的一个阿基米德位。对于每个 $\xi \in \Gamma$ 且 $\xi \neq 1$，我们有*

$$-\log|1-\xi|_v < K_d^m \cdot (\log\max\{e, h(\xi)\}) \prod_{j=1}^{m} h(\xi_j)$$

2. *（非阿基米德界）设 v 是 k 的一个非阿基米德位，与 O_k 的素理想 $\mathfrak{p}$ 相关。对于每个 $\xi \in \Gamma$ 且 $\xi \neq 1$，我们有*

$$-\log|1-\xi|_v < K_d^m \cdot \frac{Norm(\mathfrak{p})}{\log Norm(\mathfrak{p})} (\log\max\{e, Norm(\mathfrak{p})h(\xi)\}) \prod_{j=1}^{m} h(\xi_j)$$

2　经典模方法对斯皮罗猜想的界

在 [5] 中，穆尔蒂（Murty）和作者利用经典模形式给出了斯皮罗猜想的一个无条件部分结果。

定理 2.2. *（斯皮罗型界，[5]）存在绝对常数 $\kappa > 0$，使得对所有定义在 $\mathbb{Q}$ 上的椭圆曲线 E，有*

$$\log\Delta \leq \kappa \cdot N\log N$$

其中 Δ 和 N 分别是 E 的最小判别式和导子。

在 [5] 中，常数 κ 被明确给出，这个结果足够强，在丢番图方程的显式计算中很有用；关于 S–单位方程可参见 [5]，其他应用可参见 [15]。改进内容可参见 [7]。

从前面的定理特别可以得到：

推论 2.3. （最小判别式指数的界）*存在绝对常数 $\kappa > 0$，使得对于所有定义在 $\mathbb{Q}$ 上的椭圆曲线 E 和所有素数 P，有*

$$v_p(\Delta) \le \kappa \cdot N \log N$$

其中 Δ 和 N 分别是 E 的最小判别式和导子。

3 志村曲线的界

在 [7] 中，作者基于椭圆曲线的志村曲线参数化发展了一种理论，以便为 ABC 猜想和斯皮罗猜想获得一种新型的无条件界。下面陈述我们需要的结果。

定理 2.4. （椭圆曲线的界，*[7] 中的推论 16.3*）*设 S 是一个有限素数集，且 $\epsilon > 0$。存在仅依赖于 S 和 ϵ 的数 $\kappa_{S,\epsilon}$，使得以下结论成立：设 E 是定义在 $\mathbb{Q}$ 上且在 S 之外半稳定的椭圆曲线，其最小判别式为 Δ，导子为 N。那么*

$$\prod_{p|N^*} v_p(\Delta) \le \kappa_{S,\epsilon} \cdot N^{11/2+\epsilon}$$

其中 N^* 是所有整除 N 但不在 S 中的素数的乘积。

定理 2.5. （*ABC* 三元组的界，*[7] 中的定理 16.8*）*设 $\epsilon > 0$。存在仅依赖于 ϵ 的数 κ_ϵ，使得以下结论成立：对于所有互素的正整数 a、b、c 且 $a+b=c$，我们有*

$$\prod_{p|abc} v_p(abc) \le \kappa_\epsilon \cdot rad(abc)^{8/3+\epsilon}$$

为方便读者，我们简要概述一下前面两个结果证明中的主要思路。

设 E 是定义在 $\mathbb{Q}$ 上的椭圆曲线。根据模性定理 [1, 13, 16]，存在模参数化 $\varphi : X_0(N) \to E$ 。通过雅克比 - 朗兰兹对应，对于每个可允许的分解 $N = DM$，存在志村曲线参数化 $\varphi_{D,M} : X_0^D(M) \to E$，特别地，$X_0(N) = X_0^1(N)$ 且 $\varphi = \varphi_{1,N}$ 。我们假设这些参数化具有最小次数。

起点是证明里贝特 - 高桥公式 [8] 的一个推广，以得到公式

$$\prod_{p|D} v_p(\Delta) = \gamma_{D,M} \cdot \frac{\deg \varphi}{\deg \varphi_{D,M}}$$

其中有一个高度可控的误差因子 $\gamma_{D,M}$（在最坏的情况下，对于任何 $\epsilon > 0$ ，只要 N 足够大，就有 $h(\gamma_{D,M}) \le (1+\epsilon)\log D$ ），这里 Δ 是 E 的最小判别式。这个公式的重要之处在于它是全局性的：考虑了每个素数的贡献。

如果 $h(E)$ 表示 E 的法尔廷斯高度，c 是 φ 的马宁常数，那么通过 E 的参数化拉回 E 的一个奈龙微分，可以推出

$$\frac{\deg \varphi}{\deg \varphi_{D,M}} = \frac{c^2 \|f\|^2 e^{2h(E)}}{\|f_{D,M}\|_2^2 e^{2h(E)}} = \frac{c^2 \|f\|^2}{\|f_{D,M}\|_2^2}$$

其中 $\|\cdot\|_2$ 是彼得松范数，f 是与 E 相关联的傅里叶正规化新形式，$f_{D,M}$ 是定义在 $X_0^D(M)$ 的整模型上的四元数模形式，它是与 f 相关的雅克比 - 朗兰兹对应形式。

工作的一个重要部分是证明马宁常数 c 的一致上界（固定加法约化的素数集）。另一方面，已知 $\|f\|_2^2 \ll_\epsilon N^{1+\epsilon}$ [4]。由于 $f_{D,M}$ 可以延拓到 $X_0^D(M)$ 的整模型上，所以可以使用阿拉克洛夫理论给出

$\|f_{D,M}\|_2^2 \gg_\epsilon N^{-(5/3+\epsilon)}M^{-1}$ 的多项式下界。为此，至关重要的是根据 L 函数得到黑格纳点的阿拉克洛夫高度的界（这是袁 - 张在科尔梅兹猜想背景下对乔拉 - 塞尔伯格公式的推广 [17]），以及相关 L 函数合适的无零点区域。将所有这些结合起来，最终得到

$$\prod_{p|D} v_p(\Delta) \ll_\epsilon N^{8/3+\epsilon} DM = N^{11/3+\epsilon}$$

通过改变 M 的选择得到定理 2.4。通过选择 E 为弗雷 - 赫勒高奇椭圆曲线得到定理 2.5，在这种情况下可以证明更强的界 $h(\gamma_{D,M}) \le \epsilon \log D$ 。

Part III

n^2+1 的最大素因子

下面这个简单的观察结果会被多次用到。

引理 3.1. *考虑一个数 $A>e$。实函数 $t\mapsto t\log(A/t)$ 在 $1\le t\le A/e$ 这个区间内是单调递增的。*

下一个引理给出的界并非该方法所能得到的最佳界，但对我们的目的来说已经足够。

引理 3.2. *存在一个绝对常数 $K>0$，使得对于所有正整数 n，我们有*

$$\prod_{p|n^2+1} v_p\left(n^2+1\right)\le K\cdot rad\left(n^2+1\right)^8$$

证明. 设 n 是一个正整数，考虑椭圆曲线

$$E: y^2=x^3+3x+2n$$

设 Δ 和 N 分别是 E 的最小判别式和导子。这个魏尔斯特拉斯方程除了可能在 2 和 3 处之外都是极小的，并且它有（不一定是最小的）判别式

$$-16\left(4\cdot 3^3+27(2n)^2\right)=-1728\left(n^2+1\right)$$

可以验证 E 在 2 和 3 之外有乘法约化（因此，除了 2 和 3 的有界次幂之外，N 是无平方因子的），并且最小判别式是

$$\Delta=-2^s\cdot 3^t\cdot\left(n^2+1\right)$$

其中 s 和 t 是绝对值有界的整数。

根据推论 2.3，存在一个绝对常数 $\kappa>0$，使得

$$v_2\left(n^2+1\right)v_3\left(n^2+1\right)\le\kappa\cdot N^2(\log N)^2$$

令 $\epsilon>0$，并选择 $S=\{2,3\}$，应用定理 2.4，我们得到一个仅依赖于 S 和 ϵ 的数 $\kappa_{S,\epsilon}$，使得

$$\prod_{p|N^*} v_p\left(n^2+1\right)\le\kappa_{S,\epsilon}\cdot N^{11/2+\epsilon}$$

其中 N^* 是除了 2 和 3 之外整除 N 的素数的乘积。对于 $p\ne 2,3$ 的素数，p 整除 N 当且仅当它整除 Δ，进而当且仅当它整除 n^2+1。由此可得

$$\prod_{p|n^2+1} v_p\left(n^2+1\right)\le\kappa\cdot\kappa_{S,\epsilon}\cdot N^{15/2+\epsilon}$$

因为 S 是固定的，我们可以选择 $\epsilon=1/2$，从而得到

$$\prod_{p|n^2+1} v_p\left(n^2+1\right)\le K\cdot\mathrm{rad}\left(n^2+1\right)^8$$

对于某个绝对常数 $K>0$，这是因为 $\mathrm{rad}(n^2+1)$ 和 N 除了可能相差 2 和 3 的有界次幂之外是一致的（这是由于在 $p\ne 2,3$ 的素数处的半稳定约化）。 □

定理 1.2 的证明. 设 n 是一个足够大的正整数，并且记 $i=\sqrt{-1}\in\mathbb{C}$ 。我们考虑 $\mathbb{Z}[i]$ 中的方程

$$(n+i)-(n-i)=2i$$

这给出了在二次数域 $k=\mathbb{Q}(i)$ 中的方程

$$1-\frac{n-i}{n+i}=\frac{2i}{n+i}$$

考虑 $n+i=u\cdot\gamma_1^{e_1}\cdots\gamma_r^{e_r}$ 的分解，其中 γ_j 是 $\mathbb{Z}[i]$ 中互不相伴的不可约元素，$u\in\{\pm1,\pm i\}$ 。那么我们有 $n-i=\overline{u}\cdot\overline{\gamma}_1^{e_1}\cdots\overline{\gamma}_r^{e_r}$，这里上划线表示复共轭。

设

$$B=\exp\left(\sqrt{(\log R)\log_2 R}\right)$$

其中 $R=\mathrm{rad}(n^2+1)$ 。在接下来的内容中，我们将使用 R 随着 n 增大而增大这个事实（例如，根据乔拉的结果），尽管我们不需要精确的增长速率。

定义 $J=\{1,\ldots,r\}$，并且设 $I\subseteq J$ 是满足 $e_j>B$ 的指标集。设 $\xi_j=\overline{\gamma}_j/\gamma_j$ 对于 $j\in J$，并且设 $\xi_0=\prod_{j\in J-I}\xi_j^{e_j}$ 。设 $w=\overline{u}/u$ 。那么我们有

$$\frac{n-i}{n+i}=w\cdot\xi_0\cdot\prod_{j\in I}\xi_j^{e_j}$$

设 $I_0=I\cup\{0\}$，并且设 Γ 是由 w 和 $j\in I_0$ 的 ξ_j 生成的 $k^\times$ 的子群。设 $m=1+\#I=\#I_0$ 。那么 $j\in I_0$ 的 ξ_j 生成 $\Gamma/\Gamma_{\mathrm{tor}}$，并且我们可以写成

$$\frac{2i}{n+i}=1-\xi$$

其中 $\frac{n-i}{n+i}=\xi=w\cdot\xi_0\cdot\prod_{j\in I}\xi_j^{e_j}\in\Gamma$ 。定理 2.1 的第 1 项（取 $d=2$ ）给出一个绝对常数 K，使得

$$\log n\le-2\log\frac{2}{|n+i|}=-\log|1-\xi|^2\le K^m\cdot(\log\max\{e,h(\xi)\})\prod_{j\in I_0}h(\xi_j)\tag{3.1}$$

其中 $|\cdot|$ 是 $\mathbb{C}$ 上通常的绝对值。我们来估计（3.1）右边的项。首先我们有

$$h(\xi)=h\left(\frac{n-i}{n+i}\right)\le\frac{1}{2}\log|n+i|^2=\log|n+i|$$

所以

$$K^m\cdot(\log\max\{e,h(\xi)\})\le(2K)^m\log_2 n.\tag{3.2}$$

另一方面，对于每个 $j\in J-I$ 有 $e_j\le B$，并且由于 γ_j 是互不相伴的不可约元素，我们得到

$$h(\xi_0)\le B\cdot h\left(\prod_{j\in J-I}\gamma_j\right)\le\frac{B}{2}\log\prod_{j\in J}\mathrm{Norm}(\gamma_j)\le B\log\prod_{p\mid n^2+1}p$$

这就给出

$$h(\xi_0)\le B\cdot\log R.\tag{3.3}$$

此时我们注意到，如果 $m=1$（即 $I=\varnothing$ ），那么由（3.1）、（3.2）和（3.3）可得

$$\sqrt{\log n}\le\frac{\log n}{\log_2 n}\le 2KB\log R<\exp\left(K'\cdot\sqrt{(\log R)\log_2 R}\right)$$

对于一个合适的绝对常数 $K'>0$，此时结论得证。所以我们可以假设 $m\ge2$ 。

设 p_j 是 γ_j 下方的素数。注意到对于 $j\in I$，我们有 $h(\xi_j)\le\log p_j$，所以

$$\prod_{j\in I}h(\xi_j)\le\prod_{j\in I}\log p_j\le\left(\frac{\log R}{m-1}\right)^{m-1}$$

这里我们使用了算术 - 几何平均不等式。将其与（3.1）、（3.2）和（3.3）结合起来，我们推断出

$$\sqrt{\log n} \le \frac{\log n}{\log_2 n} \le (2K)^m B(\log R)\left(\frac{\log R}{m-1}\right)^{m-1}$$
$$= 2KB(\log R)\left(\frac{2K\cdot\log R}{m-1}\right)^{m-1}$$

接下来，我们注意到

$$e_j = v_{(\gamma_j)}(n+i) \le 2v_{p_j}\left(n^2+1\right)$$

因此 $e_j > B$ 这个条件意味着 $v_{p_j}(n^2+1) > B/2$，满足前一个条件的指标 j 的个数是 $m-1=\#I$ 。这就给出

$$\prod_{j\in I} v_{p_j}\left(n^2+1\right) > (B/2)^{m-1}$$

另一方面，根据引理 3.2，我们有

$$\prod_{p\mid n^2+1} v_p\left(n^2+1\right) \le \kappa\cdot R^8$$

对于某个绝对常数 κ。由此可得

$$m-1 < \frac{8\log R+\log\kappa}{\log(B/2)} < \kappa'\cdot\frac{\log R}{\sqrt{(\log R)\log_2 R}} = \kappa'\cdot\sqrt{\frac{\log R}{\log_2 R}}$$

对于一个合适的绝对常数 κ' 。

使用引理 3.1，取 $A = 2K\log R$，并且由于对于足够大的 R 有

$$\kappa'\cdot\sqrt{\frac{\log R}{\log_2 R}} < \frac{2K}{e}\log R$$

我们推断出

$$\left(\frac{2K\cdot\log R}{m-1}\right)^{m-1} \le \left(\frac{2K}{\kappa'}\sqrt{(\log R)\log_2 R}\right)^{\kappa'\sqrt{(\log R)/\log_2 R}}$$
$$\le \exp\left(K''\cdot\sqrt{(\log R)\log_2 R}\right)$$

对于一个合适的绝对常数 K'' 。将其代入（3.4），我们得到

$$\sqrt{\log n} \le 2KB(\log R)B^{K''}$$

因此，对于一个合适的绝对常数 $M>0$，我们得到

$$\log n \le \exp\left(M\cdot\sqrt{(\log R)\log_2 R}\right)$$

结论得证。 □

定理 1.1 的证明. 记 $R = \mathrm{rad}(n^2+1)$ 。根据定理 1.2，我们有

$$R \ge \exp\left(\kappa\cdot\frac{(\log_2 n)^2}{\log_3 n}\right)$$

记 $P = \mathscr{P}(n^2+1)$ 。根据 $\theta(x) = \sum_{p\le x}\log p$ 的切比雪夫界，我们有

$$R \le \prod_{p\le P} p \le \exp(4P)$$

由此结论得证。 □

Part IV

次指数 ABC 猜想，情形 1

定理 1.4 第 1 项的证明. 我们保持陈述中的符号，并且假设 c 足够大。注意到 R 随着 c 增大而增大（例如，根据 $S-$ 单位方程解的有限性）。我们可以写成

$$\frac{a}{c} = 1 - \xi$$

其中 $\xi = \frac{b}{c}$。设 $\xi_1, \ldots, \xi_r$ 是 bc 不同的素因子，并且设 $e_j = v_{\xi_j}(b/c)$（可能为负）。设

$$B = \exp\left(\sqrt{(\log R)\log_2 R}\right)$$

并且定义 $J = \{1, 2, \ldots, r\}$ 和 $I = \{j \in J : |e_j| > B\}$。设 $\xi_0 = \prod_{j \in J-I} \xi_j^{e_j}$，设 $I_0 = I \cup \{0\}$，并且设 $m = \#I_0$。设 Γ 是由 $j \in I_0$ 的 ξ_j 生成的 $\mathbb{Q}^\times$ 的子群；特别地，$\xi = \frac{b}{c} \in \Gamma$。

根据定理 2.1 的第 1 项，我们有

$$\eta \cdot \log c \le \log(c/a) = -\log|1-\xi| \le K^m \cdot (\log \max\{e, h(\xi)\}) \prod_{j \in I_0} h(\xi_j)$$

其中 $|\cdot|$ 是 $\mathbb{Q}$ 上的阿基米德绝对值，K 是一个绝对常数。

我们有 $h(\xi) = h(b/c) = \log c \le R^{K'}$，对于某个绝对常数 K'（例如利用 [10] 中给出的 ABC 猜想的指数界，可得 $K' = 15$）。另一方面，我们有 $h(\xi_0) \le B \log R$，所以我们得到

$$\eta \cdot \log c \le K' \cdot K^m B (\log R)^2 \prod_{j \in I} h(\xi_j) \tag{4.1}$$

如果 $m = 1$，我们有 $I = \varnothing$，从而得到

$$\eta \cdot \log c \le K' K B (\log R)^2 \le \exp\left(2\sqrt{(\log R)\log_2 R}\right)$$

结果得证。所以我们可以假设 $m \ge 2$。由 (4.1) 式我们得到

$$\begin{aligned} \eta \cdot \log c &\le K' \cdot K^m B (\log R)^2 \left(\frac{1}{m-1} \log R\right)^{m-1} \\ &\le K' K B^2 \left(\frac{K}{m-1} \log R\right)^{m-1} \end{aligned} \tag{4.2}$$

这里应用了算术 - 几何平均不等式。

现在来界定 m。固定一个小的 $\epsilon > 0$，由定理 2.5 我们得到

$$B^{m-1} \le \prod_{j \in I} |e_j| \le \prod_{p | R} v_p(abc) \le R^3$$

由此可得

$$m - 1 \le \frac{3 \log R}{\log B} = 3\sqrt{\frac{\log R}{\log_2 R}}$$

由引理 3.1 我们推断

$$\left(\frac{K}{m-1} \log R\right)^{m-1} \le \left(\frac{K}{3}\sqrt{(\log R)\log_2 R}\right)^{3\sqrt{(\log R)/\log_2 R}} \le B^{K''}$$

对于某个绝对常数 K''。将其与 (4.2) 式结合，我们得到

$$\eta \cdot \log c \leq K' K B^{2+K''}$$

由 B 的定义，结果得证。 □

Part V

次指数 ABC 猜想，情形 2

定理 1.4 第 2 项的证明. 由定理 1.4 第 1 项，我们只需假设 $c^{1/2} \leq a < b < c$。为了使问题的表述更对称，设 $x, y, z \in \mathbb{Z}$ 是 a, b, c 经过符号调整和顺序排列后的数，使得 $x + y + z = 0$。我们可以假设 q 整除 x，并且将方程 $x + y + z = 0$ 写成

$$-\frac{x}{z} = 1 - \xi$$

其中 $\xi = -\frac{y}{z}$。设 p_0 是 x 的一个素因子（特别地，$p_0 \leq q$），使得 $v_{p_0}(x)$ 在 x 的所有素因子中最大。那么，由于 $c^{1/2} \leq a < b < c$，我们有

$$\frac{\log c}{2 \log R} \leq v_{p_0}(x) \leq 2 v_{p_0}(x) \log p_0 \leq -2 \log |1 - \xi|_{p_0}$$

设

$$B = \exp\left(\sqrt{(\log R) \log_2 R}\right)$$

与定理 1.4 第 1 项的证明类似，我们可以使用定理 2.5 来界定 xz 中指数大于 B 的素因子的个数。然后，使用与定理 1.4 第 1 项证明中非常相似的论证，但应用定理 2.1 的第 2 项（取 $v = p_0$ ）而非第 1 项，我们推断存在某个绝对常数 K，使得

$$-\log |1 - \xi|_{p_0} \leq p_0 \cdot B^K \leq q \cdot B^K$$

结果得证。 □

推论 1.5 的证明. 我们取 $a = x$，$b = y$，$c = x + y$。由于 $c < 2b = 2y$，我们可以用 c 来表示 $\mathscr{P}(xy(x+y))$ 所需的下界。

我们可以假设 $q < \frac{(\log_2 c)^2}{\log_3 c}$，否则结论直接成立。由定理 1.4 的第 2 项，对于某个绝对常数 $K > 0$，我们有

$$\log c \leq \exp\left(K \cdot \sqrt{(\log R) \log_2 R}\right)$$

其中 $R = \mathrm{rad}(abc)$。这给出

$$\log R \geq K' \cdot \frac{(\log_2 c)^2}{\log_3 c}$$

对于某个绝对常数 K'。根据切比雪夫界，$\exp(4\mathscr{P}(abc)) \geq R$，结论得证。 □

Part VI

参考文献

[1] Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3 -adic exercises. J. Am. Math. Soc. **14**(4), 843–939 (2001)

[2] Chowla, S.: The greatest prime factor of x^2+1. J. Lond. Math. Soc. **10**(2), 117–120 (1935)

[3] Evertse, J.-H., Győry, K.: Unit Equations in Diophantine Number Theory. Cambridge Studies in Advanced Mathematics, vol. 146. Cambridge University Press, Cambridge (2015)

[4] Murty, M.R.: Bounds for congruence primes. In: Automorphic Forms, Automorphic Representations, and Arithmetic (Fort Worth, TX, 1996). Proc. Sympos. Pure Math., Part 1, vol. 66, pp. 177–192. Am. Math. Soc., Providence (1999)

[5] Murty, M.R., Pasten, H.: Modular forms and effective Diophantine approximation. J. Number Theory **133**(11), 3739–3754 (2013)

[6] Pasten, H.: On the arithmetic case of Vojta’s conjecture with truncated counting functions. Preprint (2022). arXiv:2205.07841

[7] Pasten, H.: Shimura curves and the abc conjecture. J. Number Theory **254**, 214–335 (2024)

[8] Ribet, K., Takahashi, S.: Parametrizations of elliptic curves by Shimura curves and by classical modular curves. Proc. Natl. Acad. Sci. USA **94**(21), 11110–11114 (1997)

[9] Shorey, T., Tijdeman, R.: On the greatest prime factors of polynomials at integer points. Compos. Math. **33**(2), 187–195 (1976)

[10] Stewart, C., Tijdeman, R.: On the Oesterlé - Masser conjecture. Monatshefte Math. **102**(3), 251–257 (1986)

[11] Stewart, C., Yu, K.: On the *abc* conjecture. Math. Ann. **291**(2), 225–230 (1991)

[12] Stewart, C., Yu, K.: On the *abc* conjecture. II. Duke Math. J. **108**(1), 169–181 (2001)

[13] Taylor, R., Wiles, A.: Ring - theoretic properties of certain Hecke algebras. Ann. Math. (2) **141**(3), 553–572 (1995)

[14] van der Poorten, A., Schinzel, A., Shorey, T., Tijdeman, R.: Applications of the Gel’fond - Baker Method to Diophantine Equations. Transcendence Theory: Advances and Applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), pp. 59–77. Academic Press, London (1977)

[15] von Känel, R., Matschke, B.: Solving S - unit, Mordell, Thue, Thue - Mahler and generalized Ramanujan - Nagell equations via the Shimura - Taniyama conjecture. Mem. Am. Math. Soc. **286**, 1419 (2023)

[16] Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. Math. (2) **141**(3), 443–551 (1995)

[17] Yuan, X., Zhang, S.-W.: On the averaged Colmez conjecture. Ann. Math. (2) **187**(2), 533–638 (2018)