arXiv:2602.05090v1 [math.NT] 4 Feb 2026

几乎所有素数都是部分正则的

Evan Chen[†]、Chris Cummins[*]、Ben Eltschig[*]、Dejan Grubisic[*]、Leopold Haller[*]、Letong Hong[◇]、Andranik Kurghinyan[*]、Kenny Lau[†*]、Hugh Leather[*]、Seewoo Lee[†]、Aram Markosyan[*]、Ken Ono[†]、Manooshree Patel[*]、Gaurang Pendharkar[*]、Vedant Rathi[*]、Alex Schneidman[*]、Volker Seeker[*]、Shubho Sengupta[◇]、Ishan Sinha[*]、Jimmy Xin[*]和 Jujian Zhang[†*]

作者按字母顺序排列。
[†]数学贡献者，[*]工程贡献者，[◇]首席研究员。

Abstract. 对于奇素数 p，令 $K_p := \mathbb{Q}(\zeta_p)$为第 p个分圆域，并令 ω 表示其 Teichm¨uller 特征。对于 $\alpha > 1/2$，如果奇素数 p 满足：在伽罗瓦作用下，$\mathrm{Cl}(K_p)$ 的 p-Sylow 子群的特征子空间对所有满足ω^{p-2k} 的特征都消失，则称其为部分正则

$$2 \le 2k \le \frac{\sqrt{p}}{(\log p)^{\alpha}}. \tag{1}$$

等价地，在整个此范围内，$p \nmid \mathrm{num}(B_{2k})$。我们证明，素数的一个密度为一的子集在此意义下是部分正则的。由 ***Leopoldt***反射，可得一个部分 ***Vandiver*** 定理：对于一个密度为一的素数集合 p，所有满足 (1) 的偶数 $2k$ 对应的偶特征子空间 $A_p(\omega^{2k})$ 均为零。该结果对 Kubota–Leopoldt p-进 L-函数、尖点形式与 Eisenstein级数之间的同余关系，以及代数 K-群中的 p-挠有重要影响。证明几乎所有 p 都具有部分正则性的定理已在 Lean/Mathlib 中完全形式化，并由 AxiomProver 根据该猜想的自然语言表述自动生成。

1. 引言

设 p 为一个奇素数，并令 $\zeta_p := e^{2\pi i/p}$。记 $K_p := \mathbb{Q}(\zeta_p)$，并令 $\mathcal{O}_{K_p} := \mathbb{Z}[\zeta_p]$ 为整数环。令 $\mathrm{Cl}(K_p)$ 表示 $\mathcal{O}_{K_p}$的理想类群。用指数 p 证明费马大定理（FLT）的库默尔方法基于如下分解

$$x^p + y^p = \prod_{a=0}^{p-1} (x + \zeta_p^a y) \qquad \text{in } \mathcal{O}_{K_p},$$

以及由类群所决定的因式分解性质。库默尔经典判据（现代术语称为 p-正则性）断言，若 $p \nmid |\mathrm{Cl}(K_p)|$，则费马大定理

Axiom Math, 124 University Avenue, Palo Alto, CA 94301电子邮箱地址: evan@axiommath.ai, chris@axiommath.ai, ben@axiommath.ai, dejan@axiommath.ai, leo@axiommath.ai, carina@axiommath.ai, andranik@axiommath.ai, kenny@axiommath.ai, hugh@axiommath.ai, seewoo@axiommath.ai, am@axiommath.ai, ken@axiommath.ai, manooshree@axiommath.ai, gaurang@axiommath.ai, vedant@axiommath.ai, alex@axiommath.ai, volker@axiommath.ai, shubho@axiommath.ai, ishan@axiommath.ai, jimmy@axiommath.ai, jujian@axiommath.ai.日期：2026年2月3日。2010 数学主题分类。11Y40, 11R18。关键词和短语。正则素数, 伯努利数，Vandiver猜想。

对指数 p 成立（例如，参见库默尔的原著 [8] 以及现代阐述，如 [19]）。

正则性是一个可以用伯努利数轻易描述的条件。若素数 p满足正则，则对所有偶数 $2k \in \{2, \dots, p-3\}$都有 $p \nmid B_{2k}$。然而，对于非正则素数，我们仍可考察特定指标。以此为动机，结合 Jensen 关于存在无穷多个非正则素数的定理 [5], ，我们研究“部分正则性”。Siegel猜想 [17], 认为非正则素数的渐近密度为 $1 - e^{-1/2} \approx 0.393469\dots$，这进一步引起了人们对这一方向的兴趣。我们要探讨的是，是否存在对几乎所有素数都成立的部分正则性结果。

为此，我们称奇素数 p 是 m-正则的，若对于每个偶整数$2 \le 2k \le \min(m,\ p-3)$，都有 $p \nmid \mathrm{num}(B_{2k})$。本文证明的主要结果是关于$M_\alpha(p)$-正则素数的以下估计，其中对于 $\alpha > 1/2$，我们定义

$$M_\alpha(p) := \left\lfloor \frac{\sqrt{p}}{(\log p)^\alpha} \right\rfloor. \tag{2}$$

我们证明，素数中存在一个密度为一的子集，其元素是部分正则的。

定理 1.1. 固定 $\alpha > 1/2$ 并按 (2) 定义 $M_\alpha(p)$ 。那么存在一个常数 $C_\alpha > 0$，使得当 $X \to +\infty$ 时，我们有

$$\#\Big\{ p \le X \text{ prime} : \ p \text{ is not } M_\alpha(p)\text{-regular} \Big\} \ \le \ C_\alpha \, \frac{X}{(\log X)^{2\alpha}}.$$

特别地，几乎所有素数都是 $M_\alpha(p)$-正则的。

注记 1.2. 事实上，结果表明

$$C_\alpha = 10$$

是定理 1.1（以及推论 1.4）中每个 $\alpha > 1/2$ 都适用的一个常数。特别地，该常数可以选取得与 α 无关。

注记 1.3. 素数定理断言，当 $X \to +\infty$，时，

$$\pi(X) := \#\{p \le X \ : \ p \text{ prime}\} \sim \frac{X}{\log X}$$

因此，定理 1.1 指的是素数集合中一个密度为一的子集。这就是我们所说的几乎所有素数。

自然会有人问，定理 1.1 是否对费马大定理相关的数学有所启示。为此，我们重新考察 Kummer判别准则中研究充分的伽罗瓦细化。令 A_p 表示类群 $\mathrm{Cl}(K_p)$ 的 p-部分。伽罗瓦群的作用

$$G_p := \mathrm{Gal}(K_p/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$$

给出了 A_p 按 $\mathbb{Z}_p[G_p]$-模的特征子空间作出的典范分解

$$A_p \cong \bigoplus_{i=0}^{p-2} A_p(\omega^i), \tag{3}$$

其中 $\omega : \ G_p \to \mathbb{Z}_p^\times$是 Teichm¨uller 特征，它将 a 映射为 $\mathbb{Z}_p^\times$中满足 $\omega(a) \equiv a \pmod{p}$ 的唯一 $(p-1)$次单位根。这些特征子空间分为“负部分” A_p^-

（其中 i 为奇数）和“正部分” A_p^+（其中 i 为偶数）。后者对应于最大实子域 $K_p^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ 的类群的 p-部分。

A_p^- 的结构性理解由 Herbrand-Ribet 定理给出。该定理将奇特征子空间的非零性与伯努利数 B_{2k} 的整除性联系起来。对于范围 $2 \le 2k \le p-3$ 内的偶数 $2k$，这表明

$$A_p(\omega^{p-2k}) \neq 0 \iff p \mid B_{2k}. \tag{4}$$

这一结果由 Herbrand [3] 开创，并由 Ribet [15] 运用模形式理论完成。它表明，“负”分量完全由伯努利数以及黎曼ζ函数在负奇整数处的 p-进性质通过欧拉恒等式$\zeta(1-2k) = -B_{2k}/2k$ 所支配（例如，参见 [4]）。

虽然 A_p^- 已得到充分理解，但“正”部分 A_p^+ 是 Vandiver 猜想（也归功于 Kummer）所研究的对象。该猜想断言， p 不整除 K_p^+的类数 h_p^+。用特征子空间来表述，该猜想断言如下。

猜想 (Kummer-Vandiver [7, 21])。 如果 p 是奇素数，那么我们有

$$A_p(\omega^{2k}) = 0 \quad \textit{for all even } 2k \in \{2, 4, \dots, p-3\}.$$

这里我们考虑 Vandiver 猜想的一个较弱形式，它涉及特征子空间初始范围的平凡性。由定理 1.1 可得，几乎对所有素数 p，以下结果都成立。

推论 1.4。 如果 $\alpha > 1/2$，那么存在一个常数 $C_\alpha > 0$，使得当 $X \to +\infty$ 时，我们有 e

$$\#\Big\{ p \le X \textit{ prime}: \ A_p(\omega^{2k}) \neq 0 \textit{ for some } 2 \le 2k \le M_\alpha(p) \Big\} \ \le \ C_\alpha \frac{X}{(\log X)^{2\alpha}}.$$

特别地，几乎对所有素数 p，我们有

$$A_p(\omega^2) \ = \ A_p(\omega^4) \ = \ \dots \ = A_p(\omega^{M_\alpha(p)}) = 0.$$

推论 1.4 由定理 1.1 推出，而定理 1.1 通过 Herbrand-Ribet 定理与奇特征子空间直接相关。类群的两部分 A_p^- 和 A_p^+ 之间的联系由反射原理建立，该原理称为 Leopoldt 的 *Spiegelungssatz* [10]。此定理给出了一个特殊的嵌入

$$A_p(\omega^{2k}) \neq 0 \implies A_p(\omega^{p-2k}) \neq 0.$$

这表明，偶 Vandiver 分量中的任何 p-整除性都会反映为相应奇 Herbrand-Ribet 分量中的 p-整除性。这给出了伯努利数与 Vandiver猜想之间的单向关系，可视为经典 p-正则性概念的局部细化。

由定理 1.1 推导推论 1.4。 根据 Herbrand–Ribet 定理与 Leopoldt 反射原理，推论 1.4 是定理 1.1 的直接推论。

$$A_p(\omega^{2k}) \neq 0 \implies A_p(\omega^{p-2k}) \neq 0. \qquad \square$$

推论 1.4 关于特征子空间 $A_p(\omega^{2k})$ 平凡性的结果，对 p-进解析理论有直接影响。为陈述这一点，我们回顾一下 *Kubota-Leopoldt* p-进L-函数 $L_p(s, \chi)$，它在 p-进意义下插值狄利克雷 L-函数的值。根据 Mazur 和 Wiles 证明的“岩泽理论主猜想” [13]以及下文所述的 Leopoldt 反射原理

代数特征子空间 $A_p(\omega^{2k})$ 的消失等价于相应的 p-进 L-函数是岩泽代数 $\Lambda = \mathbb{Z}_p[[T]]$ 中的单位（当 $p \nmid B_{2k}$ 时）。因此，推论 1.4 得出如下关于 p-进 L-函数的解析非消失定理，它断言 $\mathbb{Z}_p$ 是一个无零区域。

推论1.5。 如果 $\alpha > 1/2$ 和 $M_\alpha(p)$ 如 (2)中所定义，那么对于几乎所有素数 p，*Kubota-Leopoldt* p进 L函数满足

$$\left|L_p(s,\omega^{2k})\right|_p = 1 \quad for\ all\ s \in \mathbb{Z}_p,$$

对于所有偶整数 数 $2 \le 2k \le M_\alpha(p)$。特别是，这些函数在 $\mathbb{Z}_p$ 上没有零点 .

注1.6。 需要注意的是，推论1.5在定性上（以及在 p进意义上）与经典黎曼猜想的复分析框架中所得出的无零点结论截然不同，而且强得多。广义黎曼猜想（GRH）预言， $L(s,\chi)$ 的所有非平凡零点都位于临界线 $\mathrm{Re}(s) = 1/2$ 上，而上述 p进结果则断言，在域 $\mathbb{Z}_p$内根本没有零点。从复分析的角度看，这一现象令人瞩目，但在 p进分析中却很常见。这对应于岩泽理论中特征多项式为单位（次数为 0）的情形。这反映出人们预期“多数”素数都是正则的（或满足 Vandiver 猜想）；在这种情况下，相应的算术对象是平凡的，解析函数则是可逆单位。

推论*1.5*的证明。 根据圆分岩泽理论中的标准控制定理， K_∞/K 上的非分歧岩泽模的 ω^{p-2k}-特征子空间，其 Γ-余不变量与 $A_p(\omega^{p-2k})$ 有典范同构（例如参见 Washington [19, 第 13] 章）。因此， $A_p(\omega^{p-2k}) = 0$ 由中山引理迫使该特征子空间为零。根据 Mazur–Wiles [13], ，圆分主猜想将该特征子空间的特征理想与由附属于 ω^{2k} （等价地，附属于 $\omega^{1-(p-2k)}$）的 Kubota–Leopoldt p-进 L-函数生成的主理想相对应，因此，模为零等价于该 p-进 L-函数是 Λ 的单位。因此，它在 $\mathbb{Z}_p$ 上的取值都是p-进单位，即 $|L_p(s,\ \omega^{2k})|_p = 1$ 对所有 $s \in \mathbb{Z}_p$ 均成立。□

我们记录定理 1.1 通过伯努利数无处不在的特性，支配数论和算术几何中各种现象的若干其他方式。传统上，伯努利数最初通过法乌尔哈伯公式出现在整数幂和的公式中（见 [4] 第 15 章），但它们更深层的意义则体现在它们出现在L函数的特殊值中。特别地，黎曼ζ函数在负奇整数处的取值为

$$\zeta(1-2k) = -\frac{B_{2k}}{2k},$$

因此，伯努利数分子的整除性质蕴含了关于这些特殊值的微妙信息。这种联系在代数数论中发挥着核心作用，尤其是在岩泽理论以及对前文提及的分圆域的研究中（另见 [19, 第 5]章）。

伯努利数在模形式理论中第二次引人注目地出现。Eisenstein级数与尖点海克特征形式之间的某些同余关系，恰恰由伯努利数的整除性所决定。最著名的例子是拉马努金 τ 函数的同余关系

$$\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691},$$

它将权 12 尖点形式 $\Delta(q)$ 的傅里叶系数与 Eisenstein级数$E_{12}(q)$ 的傅里叶系数联系起来。这一同余关系反映了这样一个事实：

$$B_{12} = -\frac{691}{2730},$$

因此素数 691 整除 B_{12}的分子。更一般地，正如 Swinnerton-Dyer [18], 所阐明的，整除伯努利数分子的素数会导致偶权 Eisenstein级数与尖点特征形式之间出现同余关系，揭示特殊值L-函数、有理挠点椭圆曲线以及海克代数结构之间的深刻联系（见 [2, 12, 14]）。

最后，伯努利数也支配着代数 K-理论中的挠现象。代数K-群提供了一种系统的方法，用来衡量唯一分解及环中相关结构性质的失效，并将单位群和类群等经典不变量加以推广。对于整数 $\mathbb{Z}$，Lichtenbaum 和 Quillen 提出的深刻猜想经 Borel 等人的工作得以证明；这些猜想将高阶 K-群 $K_{4k-2}(\mathbb{Z})$中的 p-挠与伯努利数的整除性联系起来。因此，正如在分圆类群和模形式中一样，整除伯努利数分子的素数控制着 K-理论中的微妙挠现象。关于这些思想的通俗入门介绍，请参阅 [20,第 18] 章。

我们记录一个便于使用的四部分推论，以说明定理 1.1 的直接结论。

推论 1.7。 固定 $\alpha > 1/2$ ，并令 $M_\alpha(p)$ 如 (2) 中所述。那么对于几乎所有素数 p，以下结论对每个整数 $1 \le 2k \le M_\alpha(p)$同时成立：

(1) 同余式

$$\sum_{a=1}^{p-1} a^{2k} \equiv B_{2k}\, p \pmod{p^2}$$

在 $\mathbb{Z}/p^2\mathbb{Z}$ 中成立（将 B_{2k} 解释为其模 p^2 的约化）。

(2) 我们有 $\zeta \qquad (1-2k)$ 是一个 p-进单位。

(3) 不存在满足下列条件的归一化尖点海克特征形式 $f(q)$：其层为1，权为 $2k$，且其傅里叶展开满足

$$f(q) \equiv \sum_{n=1}^{\infty} \sum_{d \mid n} d^{2k-1} q^n \pmod{p}.$$

(4) 群 $K_{4k-2}(\mathbb{Z})$没有 p-挠。

注 1.8（广义伯努利数）。 设 χ 是模 N 的狄利克雷特征。广义伯努利数 $B_{m,\,\chi}$ 定义为

$$\sum_{a=1}^{N} \chi(a)\, \frac{te^{at}}{e^{Nt}-1} = \sum_{m=0}^{\infty} B_{m,\chi}\, \frac{t^m}{m!},$$

并且满足 $L(1-m,\ \chi) = -B_{m,\,\chi}/m$ 其中 $m \ge 1$ （参见 [19, 第 4] 章）。定理 1.1 的一个相应版本可以证明适用于适当范围内 $B_{m,\,\chi}$ 的分子的 p-整除性，从而得到相应的“几乎所有素数”推论，涉及带 Nebentypus 特征的尖点形式的同余关系、 p-进 L-函数的特殊值，以及整数环的 K-群中的挠。

注 1.9（自主证明与 Lean验证）。 本文是对正在开发的人工智能工具 AxiomProver 的案例研究和测试案例。我们要求该系统证明定理 1.1，它生成了一份 Lean/Mathlib 陈述和一份经过全面验证的证明。以这项形式化开发为参照，我们为正文准备了面向

数学读者的阐述，旨在补充背景和动机，并给出一份精简的推导，使读者无需阅读 Lean 代码也能独立理解。

本文结构如下。在第2节中，我们回顾关于伯努利数的经典事实，并在第3节中证明定理 1.1。在第4节中，我们讨论定理 1.1 之证明的形式化与Lean验证，包括代码和产物的网页链接。

Acknowledgements

作者感谢Ken Ribet、Ashvin Swaminathan和Ila Varma对本文较早版本提出的意见。

2. Nuts and Bolts

我们首先回顾证明定理 1.1 所需的相关预备知识。全文中，我们固定$\alpha > 1/2$ 并令 $M_\alpha(p) = \lfloor \sqrt{p}/(\log p)^\alpha \rfloor$。对于整数 $m \geq 1$，我们定义

$$P_m := \prod_{k=1}^{m} \left|\mathrm{num}(B_{2k})\right| \in \mathbb{Z}^+. \tag{5}$$

设 $\omega_{\mathrm{pf}}(n)$ 表示正整数 n 的不同素因子个数：

$$\omega_{\mathrm{pf}}(n) := \#\{\ell \text{ prime} : \ell \mid n\}.$$

下一个引理bo 界定了 m-正则素数的个数，其中 m是一个固定的正整数。

引理 2.1. 设 $p \geq 5$ 为素数且 $m \geq 1$。若 p 不是 m-正则的，则 $p \mid P_m$。特别地，我们有

$$\#\{p \leq X \text{ prime} : p \text{ is not } m\text{-regular}\} \leq \omega_{\mathrm{pf}}(P_m).$$

证明。若 p 不是 m-正则的，则存在 $2 \leq 2k \leq \min(m, p-3)$，使得 $p \mid \mathrm{num}(B_{2k})$。由 P_m的定义，因子 $|\mathrm{num}(B_{2k})|$ 出现在该乘积中，因此 $p \mid P_m$。计数不等式成立，是因为整除 P_m 的互异素数 $p \leq X$ 构成整除 P_m的所有互异素数之集的一个子集，该集合的基数为 $\omega_{\mathrm{pf}}(P_m)$。□

我们首先回顾关于伯努利数的两个标准事实。

引理 2.2 （欧拉公式：$\zeta(2k)$）。对每个整数 $k \geq 1$，我们有

$$\zeta(2k) = (-1)^{k+1} \frac{(2\pi)^{2k}}{2(2k)!} B_{2k} \qquad \text{and} \qquad \zeta(1-2k) = -\frac{B_{2k}}{2k}.$$

证明。这是经典结果；参见 [1, 第12章，定理12.17]。 □

引理 2.3 (冯·施陶特–克劳森)。对于每个整数 $k \geq 1$，我们有

$$B_{2k} + \sum_{\substack{\ell \text{ prime} \\ (\ell-1) \mid 2k}} \frac{1}{\ell} \in \mathbb{Z}.$$

特别地，我们有

$$\mathrm{den}(B_{2k}) = \prod_{\substack{\ell \text{ prime} \\ (\ell-1) \mid 2k}} \ell,$$

这意味着

$$\operatorname{den}(B_{2k}) \le \prod_{\ell \le 2k+1} \ell. \tag{6}$$

证明。 证明见 [1, 第 12 章，习题 12]。若 $(\ell-1) \mid 2k$，则 $\ell \le 2k+1$，因此得出所述上界。□

我们利用这个引理，推导出伯努利数以最简形式表示时分子的一个上界。

引理 2.4。 存在一个绝对常数 $C_1 > 0$，使得对每个整数 $k \ge 1$，都有

$$\log\bigl|\operatorname{num}(B_{2k})\bigr| \;\le\; C_1\, k \log(2k).$$

因此，存在一个绝对常数 $C_2 > 0$，使得对所有 $m \ge 2$，

$$\log P_m \;\le\; C_2\, m^2 \log m.$$

证明。 固定 $k \ge 1$。由引理 2.2，得

$$|B_{2k}| = \frac{2(2k)!\,\zeta(2k)}{(2\pi)^{2k}} \le \frac{2(2k)!\,\zeta(2)}{(2\pi)^{2k}} < \frac{4(2k)!}{(2\pi)^{2k}},$$

因为 $\zeta(2) = \pi^2/6 < 2$。根据引理 2.3，伯努利数的分母无平方因子，并且满足

$$\operatorname{den}(B_{2k}) \le (2k+1)!.$$

将 $B_{2k} = \operatorname{num}(B_{2k})/\operatorname{den}(B_{2k})$ 写成最简形式，得到 $|\operatorname{num}(B_{2k})| = |B_{2k}|\operatorname{den}(B_{2k})$，因此

$$|\operatorname{num}(B_{2k})| \le \left(\frac{4(2k)!}{(2\pi)^{2k}}\right)(2k+1)!.$$

取对数，并利用 $-2k\log(2\pi) < 0$，我们可以舍去负项，得到

$$\log\bigl|\operatorname{num}(B_{2k})\bigr| \le \log 4 + \log\bigl((2k)!\bigr) + \log\bigl((2k+1)!\bigr).$$

利用初等界 $\log(n!) = \sum_{j=1}^{n} \log\, j \le n\log\, n$，得到

$$\log\bigl((2k)!\bigr) \le 2k\log(2k) \quad \text{and} \quad \log\bigl((2k+1)!\bigr) \le (2k+1)\log(2k+1).$$

此外，由于 $2k+1 \le 4k$，我们有 $\log(2k+1) \le \log(4k) = \log(2k) + \log\, 2 \le 2\log(2k)$，并且 $2k+1 \le 3k$ for $k \ge 1$。因此

$$\log\bigl((2k+1)!\bigr) \le (2k+1)\log(2k+1) \le (2k+1)\log(4k) \le 3k \cdot 2\log(2k) = 6k\log(2k).$$

综合这些估计可得

$$\log\bigl|\operatorname{num}(B_{2k})\bigr| \le \log 4 + 2k\log(2k) + 6k\log(2k) \le C_1\, k\log(2k)$$

其中 $C_1 > 0$ 是适当的绝对常数。

对于 第二个结论，对 $1 \le k \le m$ 求和，并利用 $\log(2k) \le \log(2m)$，可得 s

$$\log P_m = \sum_{k=1}^{m} \log\bigl|\operatorname{num}(B_{2k})\bigr| \le C_1 \log(2m) \sum_{k=1}^{m} k = \frac{C_1}{2} m(m+1)\log(2m) \le C_2\, m^2 \log m$$

对所有 $m \ge 2$ 均成立，其中 $C_2 > 0$ 是适当的绝对常数。 □

在下面的引理中，我们应用素数定理。这是素数阶乘渐近增长的一个标准推论。

引理 2.5。 存在绝对常数 $C_3 > 0$和 $N_0 \geq 3$ ，使得对于每个整数$n \geq N_0$，都有

$$\omega_{\mathrm{pf}}(n) \leq C_3 \frac{\log n}{\log\log n}.$$

证明。 令 $t = \omega_{\mathrm{pf}}(n)$，并按递增顺序列出 n 的不同素因子： $q_1 < q_2 < \cdots < q_t$。那么

$$n \geq q_1 q_2 \cdots q_t \geq 2 \cdot 3 \cdot 5 \cdots p_t,$$

其中 p_t 是第 t 个素数，最后一个乘积是第 t 个素数阶乘 $p_t^{\#} := \prod_{j=1}^{t} p_j$。取对数得

$$\log n \geq \log(p_t^{\#}) = \vartheta(p_t),$$

其中 $\vartheta(x) = \sum_{p \leq x} \log p$ 是切比雪夫 θ-函数。

素数定理等价于 $\vartheta(x) \sim x$ ，当 $x \to \infty$ 时成立（见 [1, 第 4] 章）。特别地，存在 $x_0 \geq 2$ ，使得对所有 $x \geq x_0$,

$$\vartheta(x) \geq \frac{x}{2}. \tag{7}$$

同样，素数定理意味着 $\pi(x) \sim x/\log x$，因此存在 $x_1 \geq 3$，使得对所有 $x \geq x_1$，我们有

$$\pi(x) \leq 2\frac{x}{\log x}. \tag{8}$$

固定 t_0 ，使得对所有 $t \geq t_0$， $p_t \geq \max(x_0, x_1)$。

现在假设 $t \geq t_0$。在 $x = p_t$处应用 (8)，得到 $t = \pi(p_t) \leq 2p_t/\log p_t$，因此 $p_t \geq \frac{t}{2}\log p_t \geq \frac{t}{2}\log t$ （因为 $p_t \geq t+1$）。在 $x = p_t$ 处应用 (7)，得到

$$\vartheta(p_t) \geq \frac{p_t}{2} \geq \frac{t}{4}\log t.$$

因此，对于 $t \geq t_0$，我们有

$$\log n \geq \vartheta(p_t) \geq \frac{t}{4}\log t.$$

记 $L = \log n$。当 n 充分大时（等价地，当 L 充分大时），不等式 $L \geq \frac{t}{4}\log t$推出 $t \leq 8L/\log L$（这是对 $t\log t \ll L$的标准反演）。具体而言：取足够大的 L_0，使得对所有 $L \geq L_0$，$\log(8L/\log L) \geq \frac{1}{2}\log L$。若 $t > 8L/\log L$且 $L \geq L_0$，则 $\log t \geq (8L/\log L) \cdot (\frac{1}{2}\log L) = 4L$，这与 $t\log t \leq 4L$矛盾。因此，对所有 $L \geq L_0$， $t \leq 8L/\log L$。

最后，将有限多个满足 $\log n < L_0$ 的整数 n 吸收到常数中。也就是说，定义$N_0 = \lceil e^{L_0} \rceil$ 并取

$$C_3 := \max\left(8, \max_{3 \leq n < N_0} \omega_{\mathrm{pf}}(n)\frac{\log\log n}{\log n}\right),$$

这是有限的。因此，对所有 $n \geq N_0$, $\omega_{\mathrm{pf}}(n) \leq C_3 \log n \log\log n$成立。 □

3. Proof of Theorem 1.1

固定 $\alpha > 1/2$。令 $X \geq 3$，并设

$$m_X := \left\lfloor \frac{\sqrt{X}}{(\log X)^\alpha} \right\rfloor.$$

我们首先将变化的范围 $M_\alpha(p)$ 缩减到统一范围 m_X。考虑函数

$$f(t) = \frac{\sqrt{t}}{(\log t)^\alpha}$$

对于 $t > 1$。直接计算可得

$$f'(t) = \frac{1}{t^{1/2}(\log t)^\alpha}\left(\frac{1}{2} - \frac{\alpha}{\log t}\right),$$

因此，f 对所有 $t > e^{2\alpha}$ 都是递增的。于是，对于每个满足 $e^{2\alpha} \leq p \leq X$ 的素数 p，有

$$M_\alpha(p) = \lfloor f(p) \rfloor \;\leq\; \lfloor f(X) \rfloor = m_X.$$

因此，如果这样的素数 p 不是 $M_\alpha(p)$-正则的，那么它也不是 m_X-正则的。其余素数$p < e^{2\alpha}$ 构成一个仅依赖于 α 的有限集；我们将它们的贡献并入最终常数。剩下的工作是估计不是 m_X-正则的素数 $p \leq X$ 的数量。由引理 2.1,

$$\#\{p \leq X : \; p \text{ not } m_X\text{-regular}\} \;\leq\; \omega_{\mathrm{pf}}(P_{m_X}).$$

当 X 足够大时，我们有 $P_{m_X} \geq N_0$ （其中 N_0 来自引理 2.5），因此由引理 2.5 和引理 2.4 可得

$$\omega_{\mathrm{pf}}(P_{m_X}) \leq C_3 \frac{\log P_{m_X}}{\log\log P_{m_X}} \leq C_3 \frac{C_2\, m_X^2 \log m_X}{\log\log P_{m_X}}.$$

现在我们给出一个具体的下界，用 $\log m_X$ 表示 $\log\log P_{m_X}$。对于任意整数 $m \geq 1$，我们有

$$P_m = \prod_{k=1}^{m} |\operatorname{num}(B_{2k})| \;\geq\; |\operatorname{num}(B_{2m})| \;\geq\; |B_{2m}|,$$

由于 $\operatorname{den}(B_{2m}) \geq 1$。由欧拉公式（即引理 2.2）和显然的不等式 $\zeta(2m) > 1$，我们有

$$|B_{2m}| = \frac{2(2m)!\,\zeta(2m)}{(2\pi)^{2m}} \;\geq\; \frac{2(2m)!}{(2\pi)^{2m}}.$$

取对数 并使用初等的斯特林下界（例如，参见 [16]）

$$(2m)! \geq (2m/e)^{2m},$$

我们得到

$\log P_m \geq \log |B_{2m}| \geq \log 2 + \log((2m)!) - 2m\log(2\pi) \geq \log 2 + 2m\log(2m) - 2m - 2m\log(2\pi)$。特别地，存在一个绝对常数整数 $m_0 \geq 2$，使得对所有 $m \geq m_0$，我们都有

$$\log P_m \geq m \log m,$$

从而

$$\log\log P_m \geq \log(m\log m) \geq \log m.$$

由于 $m_X \to \infty$ 与 X，对于所有充分大的 X，我们都有 $m_X \geq m_0$，因此

$$\log\log P_{m_X} \geq \log m_X.$$

将其代入前一个界中，对于所有充分大的 X，可得

$$\omega_{\mathrm{pf}}(P_{m_X}) \le C_3 \frac{C_2\, m_X^2 \log m_X}{\log\log P_{m_X}} \le C_2 C_3\, m_X^2.$$

最后，$m_X^2 \le X/(\log X)^{2\alpha}$，因此对所有充分大的 X，我们有

$$\#\{p \le X:\ p \text{ not } M_\alpha(p)\text{-regular}\} \ \le\ \omega_{\mathrm{pf}}(P_{m_X}) \le (C_2C_3)\,\frac{X}{(\log X)^{2\alpha}}.$$

将常数增大，以涵盖有限多个例外素数 $p < e^{2\alpha}$ 以及有限多个剩余的 X 值，即可证明该定理。□

4. AxiomProver's autonomous proof and Lean verification

这里，我们介绍本项目的背景，以及形式化和 Lean验证所采用的流程。

4.1. 一个案例研究。 据我们所知，定理 1.1 和推论 1.4 都是新的。对于解析数论领域的专家而言，所用方法都是标准的（即伯努利数同余、关于 $\zeta(1-2k)$ 的欧拉公式以及筛法）。我们询问了目前仍在开发中的人工智能工具 AxiomProver，能否仅根据一个解析数论估计的陈述，自主推导出正确的证明。

我们学到了什么？仅凭命题的自然语言表述，AxiomProver 就成功地自主证明了本文的核心引擎——定理 1.1，并由 Lean 验证通过。整个过程没有任何人工协助。

乍看之下，AxiomProver 找到的证明与本文呈现的叙述并不相似。将 Lean 文件转化为人类可读的证明可能很困难，因为 Lean 是面向类型检查器编写的代码，而不是供读者阅读的解释。它会把所有"显而易见"的细节都明确写出（重写步骤、类型转换、附加条件、分类讨论），而且往往会采用对库而言最方便的引理和由策略驱动的路径，而非最能阐明概念的路径。

人类数学家通常可以大幅精简这些内容，因为他们可以依赖共同的历史背景[1], 标准论证，以及 Lean 无法想当然接受的非正式认同。因此，根据 Lean 文件撰写论文并非只是重新排版。作者必须消化形式化脚本，重构其背后的思想，再将代码转化为一种叙述：突出关键洞见，同时谨慎省略 Lean 不得不详尽写出的常规细节。

备注 4.1。 为了准确界定本文的范围，我们强调，人工智能系统并未被要求重新证明分圆下降或 Herbrand–Ribet 定理等深奥的外部定理。这些定理均引自已有文献。本案例研究聚焦于定理 1.1 的证明。

4.2. AxiomProver 协议。 这里介绍我们使用 AxiomProver 自主证明并验证 Lean 中的定理 1.1 所采用的协议（见 [9, 11]）。除我们引用并采用的 Euler 、 Kummer 、 Herbrand 、 Leopoldt、Mazur-Wiles 和 Ribet 的奠基性工作外，AxiomProver 是本文的主要引擎。定理 1.1 形式化所需的全部数学内容均在第 2 节和第 3 节中给出。

[1]例如，solution.lean 包含 ~ 3500 行代码，其中超过 1000 行用于确立引理 2.3 的结论 (6)，即经典的冯·施陶特-克劳森定理。在本文的叙述中，我们仅引用这一经典结果。

流程。 本文提供的形式化证明使用 Lean4.26.0开发并验证。由于 Lean 4 编译器及其核心库不断演进，无法保证与更早或更晚版本的兼容性。相关文件均已发布在以下代码仓库中：

`https://github.com/AxiomMath/partial-regularity`

输入文件包括

- `problem.tex`，自然语言的问题陈述
- 一个配置文件 `.environment`，其中包含单独一行*lean-4.26.0*，用于指定 AxiomProver 应使用哪个版本的 Lean。

Gi给定这两个输入文件，AxiomProver 自主提供了以下 输出文件 ：

- `problem.lean`，问题陈述的 Lean 4.26.0 形式化；以及
- `solution.lean`，证明的完整 Lean 4.26.0 形式化。

AxiomProver 生成解答后，人类作者撰写了这篇论文（未使用人工智能），供人类读者阅读。事实上，如上所述，研究论文是一种旨在向人类传达思想的叙述，而 Lean 文件则旨在满足计算机内核的要求。值得一提的是，在这次运行中，AxiomProver 独立推导出了冯·施陶特-克劳森定理。

另一份关于注记 1.2 的 Lean 证明。在上面介绍的主要运行中，AxiomProver 没有收到任何“提示”，而是被要求端到端地完成整个证明。

不过，除了上述端到端运行之外，我们还进行了内部实验，在实验中为 AxiomProver 提供了额外资源，例如 Alex Kontorovich 维护的素数定理形式化 [6]（尽管 AxiomProver 最终并未需要这项能力）。在其中一次实验中，AxiomProver 发现，实际上，定理 1.1 中的 $C_\alpha = 10$ 对所有 $\alpha > 1/2$ 都成立；这促使我们在论文中加入注记 1.2。此外，我们发现这次运行并未使用冯·施陶特-克劳森定理；相反，它独立推导出了式（6），并用其证明定理 1.1。

因此，我们在上述代码仓库中提供了相应的 Lean 文件，作为由计算机生成的证明，以证实注记 1.2 确实成立。

References

[1] T. M. Apostol, 《解析数论导论》, Springer, 1976年。[2] F. Diamond 和 J. Shurman, 《模形式入门》, 《数学研究生教材》第228卷, Springer, 2005年。[3] J. Herbrand, 《循环域的单位》, 巴黎科学院院刊, 194（1932年）, 250-252。[4] K. Ireland 和 M. Rosen, 《现代数论经典导论》, 《数学研究生教材》第84卷, Springer-Verlag, 纽约, 第2版, 1990年。[5] K. L. Jensen, 《伯努利数的数论性质》, 《数学新期刊》B辑, 26（1915年）, 73–83。[6]Kontorovich, Alex 和 Tao, Terence。《素数定理及其他》。https://github.com/ AlexKontorovich/PrimeNumberTheoremAnd, 2024年。[7] E. Kummer, 《致 Leopold Kronecker 的信, 1849年12月28日》, 载于《论文集》第I卷, Springer-Verlag, 柏林, 1975年, 第123–124页。[8] E. Kummer, 《费马定理的一般证明：方程 $x^n + y^n = z^n$ 除非 $n = 2$ 或 3 是整数，否则不能由整数¨解出》, 《纯粹与应用数学杂志》**40**（1850年）, 130–138。

[9] L. de Moura、S. Kong、J. Avigad、F. van Doorn 和 J. von Raumer，《Lean 定理证明器》（系统描述），载于《自动演绎——CADE-25》，《计算机科学讲义》第9195卷，Springer，2015年，378–388。[10] H. W. Leopoldt，《伽罗瓦数域的 l-类群结构》，《纯粹与应用数学杂志》199（1958年），165-174。[11] mathlib 社区，《Lean 数学库》，载于第9届 ACM SIGPLAN 认证程序与证明国际会议论文集（CPP 2020），ACM，2020年。[12] B. Mazur，《模曲线与艾森斯坦理想》，Publ. Math. IH´ES 47（1977年），33–186。[13] B. Mazur 和 A. Wiles，《 $\mathbb{Q}$的阿贝尔扩张的类域》，《数学发明》76（1984年），第2期，179–330。[14] K. Ono，《模性之网：模形式系数的算术及 q-级数》，CBMS 数学区域会议丛书第102卷，美国数学学会，普罗维登斯，罗得岛州，2004年。[15] K. A. Ribet，《 $\mathbb{Q}(\mu_p)$的非分歧 p-扩张的一种模构造》，《数学发明》34（1976年），151–162。[16] H. Robbins，《关于斯特林公式的一条评论》，《美国数学月刊》62（1955年），26–29。[17] C. L. Siegel，《关于库默尔的两条评论》（德文），Nachr. Akad. Wiss. G¨ottingen Math.-Phys. Kl. II（1964年），51-57。[18] H. P. F. Swinnerton-Dyer，《关于 ℓ-进表示及模形式系数的同余关系》，载于《单变量模函数 III》，《数学讲义》第350卷，Springer-Verlag，柏林-海德堡-纽约，1973年，第1-55页。[19] L. C. Washington，《圆分域导论》，第2版，《数学研究生教材》第83卷，Springer，1997年。[20] C. A. Weibel，《 K书：代数 K理论导论》，《数学研究生学习丛书》第145卷，美国数学学会，2013年。[21] H. S. Vandiver，《论费马大定理》，《美国数学会汇刊》31（1929年），第4期，613–642。