

$x \mapsto x^3$ 在 $\mathbb{Z}/n\mathbb{Z}$ 中有多少次是一对一的？

OLIVIER GARET

ABSTRACT. 我们表征了整数 n ，使得 $x \mapsto x^3$ 从集合 $\mathbb{Z}/n\mathbb{Z}$ 到其自身的双射，并确定这些整数的频率。确切地说，用 W 表示这些整数的集合，我们证明一个整数属于 W 当且仅当它是无平方因子并且没有模 3 余 1 的素因子，并且存在 $C > 0$ 使得

$$|W \cap \{1, \dots, n\}| \sim C \frac{n}{\sqrt{\log n}}.$$

这些事实（或等效的事实）在 OEIS[11, A074243] 网站上被陈述但没有证明。我们给出了 C 的具体值，这似乎之前并不为人所知。类似的结论也对那些对素因子同余类有要求的整数族进行了证明。证明基于 Delange 的一个 Tauber 型定理。

1. 介绍

众所周知，映射 $x \mapsto x^3$ 实现在实数线上的双射。自然会想知道在 $\mathbb{Z}/n\mathbb{Z}$ 中的情况如何。通过对几个例子的研究很快表明，具有这种性质的整数 n 相对较多：借助计算机工具，我们可以列出在 1 和 50 之间的它们的列表：1, 2, 3, 5, 6, 10, 11, 15, 17, 22, 23, 29, 30, 33, 34, 41, 46, 47。

此序列在整数序列在线百科全书 (OEIS) [11, A074243] 网站上有引用，该网站列出了许多显著的序列。关于这个序列的一些性质在那里被提及，但没有提供证明。特别指出的是，存在一个常数 c 使得序列的 n 项等价于 $cn\sqrt{\log n}$ 。

事实上，我们将证明以下等价的结果，其陈述似乎更有意义：

记 W 为整数集 n ，使得应用 $x \mapsto x^3$ 实现从 $\mathbb{Z}/n\mathbb{Z}$ 到其自身的双射，存在 $C > 0$ 使得

$$|W \cap \{1, \dots, n\}| \sim C \frac{n}{\sqrt{\log n}},$$

这相当于 OEIS 宣布的结果，带有 $C = \frac{1}{e}$ 。我们给出了 C 的字面值，其接近于 0.664。

这个集合的自然密度因此为零，但这些数比素数分布得更紧密。这并不令人惊讶。根据中国定理，如果 p 和 q 是互质整数，并且 a 对 p 和 q 来说都是立方剩余，那么它也将是对 pq 的立方剩余，反之亦然。因此， W 对于互质元素的乘积保持稳定这一事实机械地产生了一些组合数学。

2000 *Mathematics Subject Classification.* 11B05, 11M06, 11N37.

Key words and phrases. 整数集的密度.

这可能会让人想起另一组整数，也通过互质整数的乘积保持稳定：可以写成两个平方和的整数集 S 。已知

$$|S \cap \{1, \dots, n\}| \sim b \frac{n}{\sqrt{\log n}},$$

其中 b 是 Landau-Ramanujan 常数，接近于 0.764 [11, A064533]。这一结果由 Landau [8] 和 Ramanujan 独立发现，在解析数论的专著中经常被提及（例如，参见 Tenenbaum [13]）。

此备注为我们提供了探索问题的方法：要描述 W 的元素，我们需要确定在什么条件下，当 p 是素数时， p^α 属于 W 。这是第 2 节的主题，我们将证明 $p^\alpha \in W$ 当且仅当 $\alpha = 1$ 和 p 不同余于 1 模 3。

确定小于 x 且其素因子属于与 m 互质的模 m 同余类族的整数个数等价的问题是一个古老问题，该问题在 20 世纪初由 Landau[9] 解决。大约半个世纪多一点后，Wirsing 重新审视了这个问题，旨在将小于 x 且其素因子属于特定素数族的整数个数与这个族的规律性联系起来 [14, 15]。此问题在 Tenenbaum 的专著 [13] 中提及，他提出了一项练习（或更准确地说是一系列练习），依照 Wirsing 的精神，得出不超过 x 且所有素因子都形如 $4m + 3$ 的整数个数的显式等价表达。

关于没有平方因子的整数是否存在自然密度以及如何计算的问题更为人所熟知；这个问题可以在许多数学教科书中作为练习题找到（参见例如 Garet-Kurtzmann [6]）。结果通常归功于 Gegenbauer [7]，但同一年 Cesàro [3] 也证明了这一点。¹

我们的文献研究尚未引导我们找到同时满足这两个条件的情况。

是时候陈述我们的主要结果了。我们从一般定理开始：

定理 1. 令 Q 是无平方因子整数的集合。对于正自然数 m 和 $A \subset \{1, \dots, m\}$ ，令 $I_m(A)$ 是那些没有一个素因数模 m 同余于 A 中元素的正自然数的集合。

存在非零正常数 $(c_a)_{1 \leq a \leq m}$ ，使得以下结果成立：对于 $A \subset \{1, \dots, m\}$ ，在 $\ell = |\{a \in A; a \wedge m = 1\}| < \phi(m)$ 的条件下，其中 ϕ 表示欧拉函数，则有 $n \rightarrow \infty$ 我们有

$$(1) \quad |I_m(A) \cap \{1, \dots, n\}| \sim \left(\prod_{a \in A} c_a \right) \frac{n}{(\log n)^{\frac{\ell}{\phi(m)}}}$$

¹Gegenbauer 和 Cesàro 的文章发表于 1885 年，然而值得注意的是，关于互质整数对的类似结果在同一时期已经被多位作者证明了 [10, 2]。

和

$$(2) \quad |I_m(A) \cap Q \cap \{1, \dots, n\}| \sim \left(\prod_{a \in A} c_a \right) \prod_{\substack{p \nmid A+m\mathbb{Z} \\ p \text{ prime}}} \left(1 - \frac{1}{p^2} \right) \frac{n}{(\log n)^{\frac{\ell}{\phi(m)}}}.$$

在退化情形中, 其中 $\ell = \phi(m)$, 我们将 B 记为不在 A 中的 m 的素因子集合。 $I_m(A)$ 中的元素是其素因子在 B 中的整数。如果 B 是空集, $I_m(A)$ 被简化为 $\{1\}$, 否则我们有

$$(3) \quad |I_m(A) \cap \{1, \dots, n\}| \sim \frac{(\log n)^{|B|}}{|B|!} \prod_{p \in B} \frac{1}{\log p}.$$

当然, 如果 $\ell = \phi(m)$, $I_m(A) \cap Q$ 是有限的, 带有 $|I_m(A) \cap Q| = 2^{|B|}$ 。

我们可以很容易地推导出所需的结果:

定理 2. 令 W 为整数集 n , 使得 $x \mapsto x^3$ 实现从 $\mathbb{Z}/n\mathbb{Z}$ 到其自身的双射。存在一个常数 $C > 0$, 当趋向无穷时

$$|\{W \cap \{1, \dots, n\}\}| \sim C \frac{n}{(\log n)^{1/2}}.$$

如同 Landau [9] 所示, 我们将使用由 Dirichlet 开创的解析数论技术, 特别是 L-函数的技术。然而, 我们的证明将比 Landau 的更短, 利用了时间磨练了一些经典论证和自那时以来陈述的新结果的优势。特别地, 我们将依赖于 Delange 的一个定理, 这将使我们能够获得一个相当简短的证明, 基本上基于在算术级数定理的证明中出现的经典工具, 例如可以在 Serre [12] 中找到的。这是第 3 节的主题。

最后一节致力于确定常数 C 。它借鉴了 Tenenbaum 前述工作中的一种思想, 即通过与原字符相关的函数 L 的幂来分解自然关联于该问题的 Dirichlet 级数。

定理 3. 在定理 2 的假设下, 我们有

$$C = \frac{4}{\pi} 3^{-3/4} \left(2 \prod_{\substack{p \equiv 2 \pmod{3} \\ p \text{ prime}}} \right)^{1/2} \approx 0.664.$$

可以看出, 对于大部分内容而言, 定理 3 的证明包含了定理 2 的存在性证明, 几乎没有借用定理 1 和 2 的证明材料。然而, 我们想要展示定理 1 的证明, 这似乎对我们来说具有其自身的兴趣。

例如, 定理 1 允许我们精确化布朗的近期结果 [1]。在这篇文章中, 布朗证明了如果 r 和 m 是互质整数, 并且有 $1 \leq r \leq m$, 则 $Q \cap I_m(\{r\})$ 的自然密度

为零，这是我们的更精确结果的直接推论：

$$|I_m(\{r\}) \cap Q \cap \{1, \dots, n\}| \sim c_r \prod_{\substack{p \neq r \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right) \frac{n}{(\log n)^{\frac{1}{\phi(m)}}}.$$

2. 确定 W

我们已经注意到，根据中国剩余定理， $N = \prod_{i=1}^k p_i^{n_i}$ 在 W 中当且仅当对于所有的 i ， $p_i^{n_i}$ 在 W 中。

2.1. W 的元素是无平方因子的. 我们首先证明对于 p 素数，如果每个整数都是模 p^n 的立方，则必然有 $n = 1$ 。确实，如果 $n \geq 2$ 和每个整数都是模 p^n 的立方数，则每个整数也是模 p^2 的立方数，特别是 p 是模 p^2 的立方数。然而，对于 p 素数， p 模 p^2 从不是一个幂。确实，如果 p 与 a^α 模 p^2 同余且有 $\alpha \geq 2$ ，我们将会有一个整数 k ，使得

$$p = a^\alpha + kp^2.$$

因此， a^α 会与 0 模 p 同余，因此 a 也是如此；对于某个整数 b 我们可以写出：

$$p = (pb)^\alpha + kp^2.$$

这将意味着 p^2 整除 p ，这是荒谬的。

2.2. 素数因子的研究. 所有整数都是模 2 的立方，因为 0 和 1 是立方。类似地，所有整数都是模 3 的立方，因为 $0, 1, -1$ 是立方。我们现在假设 p 是一个素数，并且有 $p \geq 5$ 。

在 $\mathbb{Z}/p\mathbb{Z}$ 中，方程 $x^3 = 0$ 的唯一解是 $x = 0$ ，所以当且仅当 $x \mapsto x^3$ 是从 $(\mathbb{Z}/p\mathbb{Z})^\times$ 到 $\mathbb{Z}/p\mathbb{Z}^\times$ 满射时， $x \mapsto x^3$ 是从 $\mathbb{Z}/p\mathbb{Z}$ 到 $\mathbb{Z}/p\mathbb{Z}$ 的满射。然而， $\phi : x \mapsto x^3$ 作为从 $(\mathbb{Z}/p\mathbb{Z})^\times$ 到其自身的群同态，它是满射当且仅当它是单射。然而，

$$\ker \phi = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times; x^3 = 1\} = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times; (x-1)(x^2+x+1) = 0\}.$$

由于 1 不是多项式 $x^2 + x + 1$ 的根， ϕ 是单射当且仅当方程 $x^2 + x + 1 = 0$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中没有根。

由于方程 $x^2 + x = 1 = 0$ 的判别式是 $\Delta = 1 - 4 = -3$, 当且仅当 -3 不是模 p 的平方时, 该态射是单射的, 换句话说, 使用勒让德符号:

$$\begin{aligned}
 p \in W &\iff \left(\frac{-3}{p}\right) = -1 \iff \left(\frac{3}{p}\right) \left(\frac{-1}{p}\right) = -1 \\
 &\iff \left(\frac{3}{p}\right) \left(\frac{p}{3}\right) \left(\frac{-1}{p}\right) = -\left(\frac{p}{3}\right) \\
 &\iff (-1)^{\frac{p-1}{2} \frac{3-1}{2}} \left(\frac{-1}{p}\right) = -\left(\frac{p}{3}\right) \text{ with the quadratic reciprocity law} \\
 &\iff 1 = -\left(\frac{p}{3}\right) \\
 &\iff p \equiv 2 \pmod{3} \text{ because the squares modulo 3 are 0 and 1}
 \end{aligned}$$

最后, W 由那些没有一个素数除数对 3 同余于 1 的无平方因子数组成。

3. 频率的研究

回忆一下, 一个函数 $f: \mathbb{N} \rightarrow \mathbb{C}$ 被称为乘性函数如果对于任意互质整数 p 和 q , 等式 $f(pq) = f(p)f(q)$ 成立。如果恒等式在没有任何限制条件下对 p 和 q 成立, 我们说 p 是严格乘性的。

作为中国定理的推论, 集合 W 的指示函数是一个乘法函数。同样适用于其素因子不同余于 1 模 V 的整数集的指标。3

这导致了与这些集合相关的狄利克雷级数的引入:

$$L(s) = \sum_{n=1}^{+\infty} \frac{\mathbb{1}_V(n)}{n^s} \text{ and } \tilde{L}(s) = \sum_{n=1}^{+\infty} \frac{\mathbb{1}_W(n)}{n^s}.$$

为了研究集合 V 和 W 的分布, 我们将使用 Delange 提出的一个定理, 该定理特别适合解决这类问题。Delange 系统化了一种用于研究整数集 [5] 分布的方法, 他将这种方法应用于许多具有算术性质的数字集合。他的定理实际上是对他从 Ikehara 的陶伯型定理 [4] 得到的一个推广的重新表述。

定理 a. 令 A 为一整数集合, ρ 为一个非负整数或零的实数。假设对于 $\operatorname{Re} s > 1$

$$\sum_{n \in A} \frac{1}{n^s} = (s-1)^{-\rho} a(s) + b(s),$$

a 和 b 在 $\operatorname{Re} s \geq 1$ 上是全纯的 $a(1) \neq 0$

然后, 对于 x 趋向于 $+\infty$ 我们有

$$|A \cap [0, x]| \sim \frac{a(1)}{\Gamma(\rho)} x (\log x)^{\rho-1}.$$

这里 $(s-1)^{-\rho}$ 被理解为 $\exp(-\rho \operatorname{Log}(s-1))$, 其中 Log 是对数的主要确定, 定义在 $\mathbb{C} \setminus]-\infty, 0]$ 上。

我们首先介绍一些来自数论分析的经典对象。

3.1. 符号表示法. 我们用 P 表示素数集合。对于自然整数 a 和 m , 我们用 $P_a(m) = P \cap (a + m\mathbb{Z})$ (表示模 m 同余于 a 的素数)。

对于非零自然数 m , 我们记 $\operatorname{Dir}(m)$ 为模 m 的字符集: 这些是从 $(\mathbb{Z}/m\mathbb{Z})^\times$ 到 $\mathbb{C}$ 的乘法同态。对于 $\chi \in \operatorname{Dir}(m)$ 和 n 这样的自然整数, 我们也用 $\chi(n)$ 表示 n 在 $\mathbb{Z}/m\mathbb{Z}$ 中的像, 那些与 m 不互质的整数被映射到 0。这样定义的函数是可乘的。

对于实数 a , 我们用 H_a 表示实部严格大于 a 的复数集合。

我们将对数的主值表示为 Log 。我们回忆一下, $(H_0, \times)$ 是一个群, 并且 $\forall a, b \in H_0, \operatorname{Log}(ab) = \operatorname{Log}(a) + \operatorname{Log}(b)$ 。对于 $\alpha \in \mathbb{R}$ 和 $z \in H_0$, z^α 表示 $\exp(\alpha \operatorname{Log}(z))$, 而对于 $\alpha, \beta \in \mathbb{R}$ 和 $z \in H_0$, 我们有 $\exp \operatorname{Log} z = z$ 和 $(z^\alpha)^\beta = z^{\alpha\beta}$ 。

在以下内容中, 我们将表示 $E = I_m(A)$, $F = E \cap Q$, 然后

$$\forall s \in H_1 \quad L(s) = \sum_{n=1}^{+\infty} \frac{\mathbb{1}_E(n)}{n^s} \text{ and } \tilde{L}(s) = \sum_{n=1}^{+\infty} \frac{\mathbb{1}_F(n)}{n^s}.$$

3.2. 计算 L 和 $\tilde{L}$. 为了计算 L 和 $\tilde{L}$, 我们引入了一种概率形式主义, 我们认为这种形式主义对某些性质给出了相当令人愉快的解释, 这些性质也可以从与乘法函数相关的 L 函数的因子分解公式中推导出来。

对于 $s > 1$, 我们考虑一个在 $\mathbb{N}^*$ 上的概率测度, 称为参数为 s 的 Zeta 分布, 我们用 μ_s 表示, 并由 $\mu_s(k) = \zeta(s)^{-1} k^{-s}$ 定义。

因此我们有 $\mu_s(E) = \frac{L(s)}{\zeta(s)}$ 。

如果随机变量 X 遵循 μ_s 定律, 很容易看出对于任何非零自然整数 n , $\mathbb{P}(n|X) = n^{-s}$ 。如果 ν_p 表示 p 进赋值, 我们有

$$\begin{aligned} \mathbb{P}(\nu_{p_1}(X) \geq a_1, \dots, \nu_{p_r}(X) \geq a_r) &= \mathbb{P}\left(\prod_{i=1}^r p_i^{a_i} | X\right) \\ &= \left(\prod_i p_i^{a_i}\right)^{-s} = \prod_i \mathbb{P}(\nu_{p_i}(X) \geq a_i), \end{aligned}$$

因此, 变量 $\nu_p(X)$ 是具有移位几何分布的独立变量, 与 $1 + \nu_p(X) \sim \mathcal{G}(1 - p^{-s})$ 相关, 换句话说, 对于 $k \in \mathbb{N}$, 我们有

$$\mathbb{P}(\nu_p(X) = k) = (1 - p^{-s})p^{-sk}.$$

然后我们观察到 $\{X \in E\} = \bigcap_{\substack{p \text{ prime} \\ p \in A+m\mathbb{Z}}} \{\nu_p(X) = 0\}$ 和

$$\{X \in F\} = \bigcap_{\substack{p \text{ prime} \\ p \in A+m\mathbb{Z}}} \{\nu_p(X) = 0\} \cap \bigcap_{\substack{p \text{ prime} \\ p \notin A+m\mathbb{Z}}} \{\nu_p(X) \leq 1\}.$$

。由于 $\nu_p(X)$ 是独立变量，我们得到

$$\mu_s(F) = \prod_{\substack{p \text{ prime} \\ p \in A+m\mathbb{Z}}} (1 - p^{-s}) \prod_{\substack{p \text{ prime} \\ p \notin A+m\mathbb{Z}}} (1 - p^{-2s}) \text{ and } \mu_s(E) = \prod_{\substack{p \text{ prime} \\ p \in A+m\mathbb{Z}}} (1 - p^{-s}).$$

类似地，相关的狄利克雷级数由恒等式联系在一起

$$\tilde{L}(s) = L(s) \prod_{p \in P \setminus I_m(A)} (1 - p^{-2s}).$$

在后续部分，我们仍将记 $\mu_s(E)$ 表示商 $\frac{L(s)}{\zeta(s)}$ 对于 $s \in H_1$ 。根据解析延拓原理，在 $s \in]1, +\infty[$ 上已经证明的恒等式在整个集合 H_1 上仍然成立。

3.3. 证明. 我们的策略是应用 Delange 定理 a 与 $b(s) = 0$ 。

由于 $s \mapsto \prod_{p \in P \setminus I_m(A)} (1 - p^{-2s})$ 定义了一个在 $H_{1/2}$ 上不消失的全纯函数，因此使用 L 或 $\tilde{L}$ （即使用 E 或 F ）是等价的。

我们可以进一步分解

$$\mu_s(E) = \prod_{\substack{p \in P \cap (A+m\mathbb{Z}) \\ p|m}} (1 - p^{-s}) \prod_{\substack{a \in A \\ a \wedge m = 1}} \prod_{p \in P_a(m)} (1 - p^{-s})$$

第一个产品 $\prod_{\substack{p \in P \cap (A+m\mathbb{Z}) \\ p|m}} (1 - p^{-s})$ 具有有限数量的项，并定义了 H_0 上的

全纯函数。最显著的部分由形式为 $\prod_{p \in P_a(m)} (1 - p^{-s})$ 的乘积给出。

这些产品的研究重现了狄利克雷算术级数定理的证明过程。

我们从一些复分析的经典引理开始。

引理 1. 存在一个在 H_0 上的全纯函数 h_0 ，使得 $h_0(1) = 0$ 成立。

$$\forall s \in H_1 \quad -\operatorname{Log} \zeta(s) = \operatorname{Log}(s-1) + h_0(s).$$

Proof. 众所周知，存在一个在 H_0 上的全纯函数 ϕ ，在 H_1 上恒等式为 $\zeta(s) = \frac{1}{s-1} + \phi(s)$ 。函数 $\psi : s \mapsto 1 + (s-1)\phi(s)$ 当然也是全纯的，并且在 1 处等于

1. 在半平面 H_1 上, 函数 ζ 取值于 H_0 。由此我们推断出恒等式 $-\operatorname{Log} \zeta(s) = \operatorname{Log}(s-1) + \operatorname{Log} \psi(s)$ 。恒等式 $\zeta(s) = \frac{\psi(s)}{s-1}$ 扩展到 $H_0 \setminus \{1\}$; 正弦函数 ζ 在 H_0 上不消失, ψ 也是如此, 这使得在 H_0 上定义一个 ψ 的对数成为可能, 该对数扩展了 $\operatorname{Log} \psi$; 这就是 h_0 所需的函数。 $\square$

备注 1. 作为这个引理的结果, 我们看到在 *Delange* 定理 a 的假设中, 我们可以用 $\zeta(s)^\rho$ 替换 $(s-1)^{-\rho}$, 因为有一个恒等式

$$\zeta(s)^\rho = \exp(-\rho \operatorname{Log}(s-1) - \rho h_0(s)) = (s-1)^{-\rho} \exp(-\rho h_0(s)).$$

引理 2. 设 (a_n) 是一族模小于或等于 1 的复数。我们设定 $F(s) = \prod_{p \in P} (1 - \frac{a_p}{p^s})$ 。对于 $s \in H_1$, 乘积 $F(s)$ 绝对收敛。存在一个在 $H_{1/2}$ 上的全纯函数 h , 使得

$$\forall s \in H_1 \quad -\operatorname{Log} F(z) = \sum_{p \in P} \frac{a_p}{p^s} + h(s).$$

Proof. 证明是标准的; 它以简写形式给出: 对于 $\operatorname{Re} s > 1$, 我们写作 $-\operatorname{Log}(1 - \frac{a_p}{p^s}) = \frac{a_p}{p^s} + r(\frac{a_p}{p^s})$, 其中 $r(z) = \sum_{n \geq 2} \frac{z^n}{n}$ 。对于 $\operatorname{Re} s \geq s_0 > 1/2$, 我们有 $|r(\frac{a_p}{p^s})| \leq r(p^{-s_0})$; 一般项级数 $r(p^{-s_0})$ 收敛, 这确保了 $h(s) = \sum_p r(\frac{a_p}{p^s})$ 在 $H_{1/2}$ 上的全纯性。 $\square$

推论 1. 定义在 H_1 上由 $s \mapsto \sum_{p \in P} \frac{1}{p^s}$ 给出的函数扩展为 $\overline{H_1}$ 的一个邻域上的全纯函数, 其中去掉了 1。存在一个在 $\overline{H_1}$ 的邻域上的全纯函数 h , 对于 $s \in H_1$ 成立。

$$\sum_{p \in P} \frac{1}{p^s} = \operatorname{Log} \frac{1}{s-1} + h(s).$$

Proof. 根据引理 2 以及将 ζ 以欧拉乘积形式的表示, 存在一个在 $H_{1/2}$ 上的全纯函数 h , 使得对于所有 $s \in H_1$

$$\operatorname{Log} \zeta(s) = \sum_{p \in P} \frac{1}{p^s} + h(s).$$

成立。因此, 为了扩展 $\sum_{p \in P} \frac{1}{p^s}$, 只需要注意到在 $H_0 \setminus \{1\}$ 上全纯的 ζ 函数不在 H_1 (其中乘积绝对收敛) 以及除去 1 的直线 $\operatorname{Re} s = 1$ 上不为零 (参见例如 Colmez, 定理 A.4.3 第 317 页)。这允许取对数扩展到线 $\operatorname{Re} s = 1$ 减去 1。我们以引理 1 结论。 $\square$

狄利克雷特征发挥作用。

推论 2. 令 $\chi \in \operatorname{Dir}(m)$ 。我们注意到 $L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}$ 。然后,

(1) 存在一个在 $H_{1/2}$ 上的全纯函数 h , 使得

$$\forall s \in H_1 \quad \text{Log } L(\chi, s) = \sum_{p \in P} \frac{\chi(p)}{p^s} + h(s).$$

(2) 对于 $\chi \neq \chi_0$, 函数 $s \mapsto \sum_{p \in P} \frac{\chi(p)}{p^s}$ 扩展为 $\overline{H_1}$ 邻域上的全纯函数。

(3) 对于 $\chi = \chi_0$, 函数 $s \mapsto \sum_{p \in P} \frac{\chi_0(p)}{p^s}$ 扩展为在去掉 1 的 $\overline{H_1}$ 邻域上的全纯函数。存在一个在 $\overline{H_1}$ 的邻域上的全纯函数 h , 对于 $s \in H_1$:

$$\sum_{p \in P} \frac{\chi_0(p)}{p^s} = \text{Log } \frac{1}{s-1} + h(s).$$

Proof. 根据引理 2, 第一个点是立即将其写成欧拉乘积形式 $L(\chi, s) = \prod_{p \in P} (1 - \frac{\chi(p)}{p^s})^{-1}$ 的直接结果。同之前一样, 为了扩展 $\sum_{p \in P} \frac{\chi(p)}{p^s}$, 只需注意到函数 $L(\chi, s)$ 在 H_0 上是全纯的, 并且在 H_1 (其中乘积绝对收敛) 以及直线 $\text{Re } s = 1$ 上不消失 (例如参见 Colmez, 练习 A.4.4 第 318 页), 这使得我们可以取对数以扩展到除去 1 的直线 $\text{Re } s = 1$ 上。我们以引理 1 结束。最后一点源自于级数 $\sum_{p \in P} \frac{\chi_0(p)}{p^s}$ 和 $\sum_{p \in P} \frac{1}{p^s}$ 只相差有限数量的项, 这些项在 H_0 上是全纯的。 $\square$

引理 3. 令 a, m 是互质的非零自然数。则存在一个在 $\overline{H_1} \setminus \{1\}$ 每一点上全纯的函数 h_a , 使得对于每一个 $s \in H_1$

$$-\text{Log } \prod_{p \in P_a(m)} (1 - p^{-s}) = \frac{1}{\phi(m)} \text{Log } \frac{1}{s-1} + h_a(s).$$

Proof. 给定引理 2, 我们只需要研究

$$\sum_{p \in P_a(m)} \frac{1}{p^s} = \sum_{p \in P} \mathbb{1}_{a+m\mathbb{Z}}(p) \frac{1}{p^s}.$$

现在, 应用在交换群 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中的特征理论告诉我们, 对于 a 和 x 在 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中, 有

$$\frac{1}{\phi(m)} \sum_{\chi \in \text{Dir}(m)} \chi(x) = \delta_0(x) \text{ then } \frac{1}{\phi(m)} \sum_{\chi \in \text{Dir}(m)} \chi(a^{-1}x) = \delta_0(a^{-1}x) = \delta_a(x)$$

通过转换为整数, 我们得到

$$\mathbb{1}_{a+m\mathbb{Z}}(p) = \frac{1}{\phi(m)} \sum_{\chi \in \text{Dir}(m)} \overline{\chi(a)} \chi(p)$$

和

$$\sum_{p \in P_a(m)} \frac{1}{p^s} = \frac{1}{\phi(m)} \sum_{\chi \in \text{Dir}(m)} \overline{\chi(a)} \sum_{p \in P} \frac{\chi(p)}{p^s}.$$

然后, 该引理立即从推论 2 跟进。 $\square$

我们现在可以证明定理 1。

Proof. 令 $s \in H_1$ 成立。 $M(s) = \zeta(s) \prod_{\substack{a \in A \\ a \wedge m = 1}} \prod_{\substack{p \in P \\ p \equiv a}} (1 - p^{-s})$ 导致

$$\forall s \in H_1 \quad \text{Log } M(s) = \text{Log } \zeta(s) + \sum_{\substack{a \in A \\ a \wedge m = 1}} \text{Log} \prod_{p \in P_a(m)} (1 - p^{-s}).$$

通过将引理 1 和引理 3 结合起来，我们得到 $s \in H_1$

$$\text{Log } M(s) = (-1 + \frac{\ell}{\phi(m)}) \text{Log}(s-1) - \left(h_0(s) + \sum_{\substack{a \in A \\ a \wedge m = 1}} h_a(s) \right), \text{ then}$$

$$M(s) = (s-1)^{-1+\ell/\phi(m)} e^{-h(s)} \text{ where } h(s) = h_0(s) + \sum_{\substack{a \in A \\ a \wedge m = 1}} h_a(s), \text{ and}$$

$$L(s) = \zeta(s) \mu_s(E) = \prod_{\substack{p \in P \cap (A+m\mathbb{Z}) \\ p|m}} (1-p^{-s}) M(s) = (s-1)^{-1+\ell/\phi(m)} e^{-h(s)} \prod_{\substack{p \in P \cap (A+m\mathbb{Z}) \\ p|m}} (1-p^{-s}).$$

对于 a 在 1 和 m 之间，我们最终设定

$$c_a = \begin{cases} e^{-h_a(1)} & \text{if } a \wedge m = 1 \\ 1 - a^{-1} & \text{if } a \wedge m \neq 1 \text{ and } a \in P \\ 1 & \text{if } a \wedge m \neq 1 \text{ and } a \notin P \end{cases}$$

请注意, (c_a) 不依赖于集合 A 。可以看出如果 $p \in P$, 则条件 $p|m$ 和 $p \wedge m \neq 1$ 是等价的。然后可以验证

$$e^{-h(1)} \prod_{\substack{p \in P \cap (A+m\mathbb{Z}) \\ p|m}} (1 - p^{-1}) = \prod_{a \in A} c_a.$$

当 $\ell < \phi(m)$ 时，我们得出 Delange 定理。

假设 $\ell = \phi(m)$, 令 $a \in \{1, \dots, m\} \setminus A$ 。由于 $\ell = \phi(m)$, 我们有 $a \wedge m \neq 1$ 。现在令 p 是一个模 m 同余于 a 的素数。 p 与 a 模 $\text{ulom} \wedge a$ 同余, 并且 a 与 0 模 $\text{ulom} \wedge a$ 同余, 因此 p 与 0 模 $\text{ulom} \wedge a$ 同余, 从而得到 $p = m \wedge a$ 。但我们知道 p 与 a 模 m 同余, 所以 $m \wedge a$ 与 a 模 m 同余, 这给出了我们 $a = m \wedge a = p$ 。最后, p 是一个素数, 它是 m 的除数, 并且是授权同余类的一个代表。因此, 如果我们用 $(p_1, \dots, p_k)$ 表示这样的素数组成的集合, 则 $I_m(A)$ 由可以写成 $\prod_{i=1}^k p_i^{x_i}$ 形式的整数组成, 其中 x_i 是一个自然数。 $I_m(A) \cap \{1, \dots, n\}$ 因此具有与由方

程确定的单形中整数坐标点集相同的势

$$\begin{cases} \forall i \in \{1, \dots, k\} & x_i \geq 0 \\ \sum_{i=1}^k x_i \log(p_i) \leq \log n \end{cases}$$

换句话说, $|I_m(A) \cap \{1, \dots, n\}| = |(\log n)V \cap \mathbb{Z}^d|$, 带有

$$V = \left\{ x \in [0, +\infty[^k; \sum_{i=1}^k x_i \log(p_i) \leq 1 \right\},$$

这导致 $|I_m(A) \cap \{1, \dots, n\}| \sim (\log n)^k \lambda(V) = (\log n)^k \frac{1}{k!} \prod_{i=1}^k \frac{1}{\log p_i}$. $\square$

我们可以继续证明定理 2。

Proof. 由于 $W = Q \cap I_3(\{1\})$, 根据定理 1 的第二点得出。我们有 $A = \{1\}$, $m = 3$, $\ell = 1 < 2 = \phi(m)$. $\square$

4. 常数的计算 C

我们引入模 3 的本原迪利克雷特征, 记作 χ_1 : 它定义为

$$\chi_1(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{3}, \\ -1 & \text{if } n \equiv 2 \pmod{3}, \\ 0 & \text{if } n \equiv 0 \pmod{3}. \end{cases}$$

这个字符使我们能够根据其模 3 同余性来分离素数。

我们知道, 如果一个函数 ϕ 是严格乘性的且模数有界于 1, 则我们有

$$\sum_{n \geq 1} \frac{\phi(n)}{n^s} = \prod_{p \in P} \left(1 - \frac{\phi(p)}{p^s} \right)^{-1}.$$

特别是, 通过根据模 3 的同余分离, 我们得到

$$\sum_{n \geq 1} \frac{\phi(n)}{n^s} = \left(1 - \frac{\phi(3)}{3^s} \right)^{-1} \prod_{p \in P_1(3)} \left(1 - \frac{\phi(p)}{p^s} \right)^{-1} \prod_{p \in P_2(3)} \left(1 - \frac{\phi(p)}{p^s} \right)^{-1}.$$

将这应用于字符 χ_1 , 我们对于函数 $L_{\chi_1}(s) = \sum_{n \geq 1} \frac{\chi_1(s)}{n^s}$ 得到

$$L_{\chi_1}(s) = \prod_{p \in P_1(3)} \left(1 - \frac{1}{p^s} \right)^{-1} \cdot \prod_{p \in P_2(3)} \left(1 + \frac{1}{p^s} \right)^{-1},$$

然后, 乘以 $\zeta(s)$ 的展开式, 我们依次得到

$$\begin{aligned}
\zeta(s)L_{\chi_1}(s) &= \left(1 - \frac{1}{3^s}\right)^{-1} \prod_{p \in P_1(3)} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \in P_2(3)} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \\
\mu_s(E)^2 &= \zeta(s)^{-1} L_{\chi_1}(s)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \prod_{p \in P_2(3)} \left(1 - \frac{1}{p^{2s}}\right)^{-1}, \\
\mu_s(E) &= \zeta(s)^{-1/2} L_{\chi_1}(s)^{-1/2} \left(1 - \frac{1}{3^s}\right)^{-1/2} \prod_{p \in P_2(3)} \left(1 - \frac{1}{p^{2s}}\right)^{-1/2},
\end{aligned}$$

并且最后

$$L(s) = \zeta(s)^{1/2} L_{\chi_1}(s)^{-1/2} \left(1 - \frac{1}{3^s}\right)^{-1/2} \prod_{p \in P_2(3)} \left(1 - \frac{1}{p^{2s}}\right)^{-1/2}.$$

并且

$$\begin{aligned}
\tilde{L}(s) &= \prod_{p \in P \setminus I_3(\{1\})} (1 - p^{-2s}) L(s) \\
&= \zeta(s)^{1/2} L_{\chi_1}(s)^{-1/2} \left(1 - \frac{1}{3^s}\right)^{-1/2} (1 - 9^{-s}) \prod_{p \in P_2(3)} \left(1 - \frac{1}{p^{2s}}\right)^{1/2}.
\end{aligned}$$

应用 Delange 定理和备注 1, 我们得到

$$c = \frac{1}{\sqrt{\pi}} L_{\chi_1}(1)^{-1/2} (2/3)^{-1/2} \frac{8}{9} \sqrt{p_2}, \text{ with } p_2 = \prod_{p \in P_2(3)} \left(1 - \frac{1}{p^2}\right).$$

$L_{\chi_1}(1)$ 的值很容易计算: 我们有

$$\begin{aligned}
L_{\chi_1}(1) &= \sum_{n \geq 0} \left(\frac{1}{3n+1} - \frac{1}{3n+2} \right) = \sum_{n \geq 0} \int_0^1 (x^{3n} - x^{3n+1}) dx = \int_0^1 \frac{dx}{x^2 + x + 1} \\
&= \left[\frac{2}{\sqrt{3}} \arctan \left(\frac{1+2x}{\sqrt{3}} \right) \right]_0^1 = \frac{2}{\sqrt{3}} \left(\frac{\pi}{3} - \frac{\pi}{6} \right) = \frac{\pi}{3\sqrt{3}}
\end{aligned}$$

最后得到 $C = \frac{4}{\pi} 3^{-3/4} \sqrt{2p_2} \approx 0.664$.

REFERENCES

- [1] Ron Brown. The natural density of some sets of square-free numbers. *Integers*, 21:paper a81, 9, 2021.
- [2] Ernest Césaro. Sur diverses questions d'arithmétique. Liège Mém. (2) X. 1-360 (1883)., 1883.
- [3] Ernest Cesàro. Le plus grand diviseur carré. *Annali di Matematica Pura ed Applicata*, 13:251-268, 1885.
- [4] Hubert Delange. Généralisation du théorème de Ikehara. *Ann. Sci. Éc. Norm. Supér. (3)*, 71:213-242, 1954.

- [5] Hubert Delange. Sur la distribution des entiers ayant certaines propriétés. *Ann. Sci. Éc. Norm. Supér. (3)*, 73:15–74, 1956.
- [6] Olivier Garet and Aline Kurtzmann. *De l'intégration aux probabilités*. Ref. Sci. Paris: Ellipses, 2nd corrected edition edition, 2019.
- [7] Leopold Gegenbauer. Asymptotic laws of number theory. *Wien. Denkschr.*, 49:37–80, 1885.
- [8] Edmund Landau. On the partition of positive integers in four classes according to the minimal number of squares needed to their additive composition. *Arch. der Math. u. Phys. (3)*, 13:305–312, 1908.
- [9] Edmund Landau. Solution of Lehmer's problem. *Am. J. Math.*, 31:86–102, 1909.
- [10] Franz Mertens. On some asymptotic laws in number theory. *J. Reine Angew. Math.*, 77:289–339, 1873.
- [11] OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences, 2025. Published electronically at <http://oeis.org>.
- [12] Jean-Pierre Serre. Cours d'arithmétique. 2me ed. Le Mathématicien. Paris: Presses Universitaires de France. 188 p. (1977)., 1977.
- [13] Gérald Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*, volume 1 of *Cours Spéc. (Paris)*. Paris: Société Mathématique de France, 2ème éd. edition, 1995.
- [14] Eduard Wirsing. Über die Zahlen, deren Primteiler einer gegebenen Menge angehören. *Arch. Math.*, 7:263–272, 1956.
- [15] Eduard Wirsing. Das asymptotische Verhalten von Summen über multiplikative Funktionen. *Math. Ann.*, 143:75–102, 1961.