arXiv:2305.05522v1 [math.NT] 9 May 2023

幂和与库默尔同余

Samuel Goodman

2023年5月

引言

库默尔同余的最简单形式于1851年由恩斯特·爱德华·库默尔在 [2]中首次证明。它们指出，给定一个素数 p 以及偶正整数 r、 s，满足 r 不是 $p-1$ 的倍数且 $r \equiv s$ 模 $p-1$，则

$$\frac{B_r}{r} \equiv \frac{B_s}{s} \mod p$$

其中， B_n 表示第 n 个伯努利数。这一结果的更强版本最初由沃罗诺伊于 [3] 年利用幂和恒等式得到，后来久保田 - 利奥波德于 [1] 年利用 p- 进 L 函数理论得到：给定素数 p、非负整数 a，以及满足 r 不是 $p-1$ 的倍数且 $r \equiv s$ 模 $p^a(p-1)$ 的偶正整数 r、 s，则

$$(1-p^{r-1})\frac{B_r}{r} \equiv (1-p^{s-1})\frac{B_s}{s} \mod p^{a+1}$$

特别地，久保田-利奥波德从更自然的角度阐释了这一经典结果，因为它实际上成为证明 p-进 ζ 函数连续性的基础。

在本文中，我们发展了一套结构理论，以一种全新的方式重新阐释这一结果：通过一系列关于这些多项式所具有的“伪乘法”结构的新结果，并分析自然乘法作用在所得值集上的稳定子，从而揭示某一特殊类多项式中各元素在模 p 的幂意义下的行为。通过这一方法，我们还推导出了库默尔同余的一种新证明。

我们首先介绍一些文献中广为人知的预备结果：

引理 1

设 $p > 3$ 为素数， a 为正整数，且 r 为正偶整数。则有

$$\sum_{n=1}^{p^a} n^r \equiv p^a B_r \mod p^{2a+v_p(r)+1}$$

引理 2

设 p 为奇素数， a 和 n 为正整数， k 为正整数，且 $k \geq r+a$、 $p^r | k$ 和 $p-1$ 均不整除 k。则有

$$\sum_{n=1}^{p^a} n^k \equiv 0 \mod p^{r+a}$$

引理 3（Adams 定理）

对于任意偶整数 s，若 s 不是 $p-1$ 的倍数，则 $v_p(\frac{B_s}{s}) \geq 0$（特别是，$\frac{B_s}{s}$ 是一个 p-整数）。

我们首先证明，在自然乘法作用下，某些特殊多重集会被非平凡剩余类保持不变。这将首次提示我们，局部信息（即多项式模 p 的幂的各个取值）具有丰富的内在结构，能够解释全局现象，其中之一将成为库默尔同余的先声。

定理 1

设 p 为奇素数， a、t 为非负整数， k 为满足 $p^{2a+1} | k$ 的正整数。设 $d = \frac{p-1}{\gcd(k,p-1)}$， $v = \min(v_p(k) - 2a - 1, t)$，且 g 是模 $p^{3a+t+v+2}$ 的 d 次单位根。此外，设 $\mathfrak{S}$ 为多重集，其中包含 $n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))^{p^t}}$ 在 n 从 1 变化到 p^{a+1} 时所取到的模 $p^{3a+t+v+2}$ 可逆剩余类，并按重数计入。那么 $g\mathfrak{S} = \mathfrak{S}$。

我们证明 $g\mathfrak{S} \subset \mathfrak{S}$，由此可得 $g\mathfrak{S} = \mathfrak{S}$，因为它们是大小相同的多重集。 $\mathfrak{S}$ 中的每个元素 s 都对应某个正整数 n，满足 $1 \leq n < p^{a+1}$，其中 $n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))^{p^t}} \equiv s$按构造模 $p^{3a+t+v+2}$ 成立。对于这个 n，我们找到一个关联的 n'，使得 $n'^{(k+p^a(p-1))p^t} + n'^{(k-p^a(p-1))^{p^t}} \equiv gs$ 模 $p^{3a+t+v+2}$成立。

设 $k = p^r k'$，其中 $p \nmid k'$。首先，我们证明 $x^{k'} \equiv g$模 p^{a+1}有一个解。注意到 $\gcd(k', p-1) = \gcd(k, p-1)$，因此 $x^{k'}$和 $x^{\gcd(k,p-1)}$生成相同的模 p^{a+1}剩余类，所以只需对$x^{\gcd(k,p-1)}$证明结论。设 g' 是模 p^{a+1} 的一个原根，并写作 $g \equiv g'^b$ 模 p^{a+1}，其中 b。由于 $g^d \equiv 1$模 p^{a+1}，我们得出 $p-1 | db$，这意味着 $\frac{p-1}{d} | b$，由此根据定义可得 $\gcd(k, p-1) | b$，进而存在某个 x，使得 $g \equiv x^{\gcd(p-1,k)}$ 模 p^{a+1}。

现在选取一个固定的解 x' to $x^{k'} \equiv g \mod p^{a+1}$。对于每个 n，我们令 n' 为满足 $n' \equiv nx' \mod p^{a+1}$ 的唯一正整数 $\leq p^{a+1}$，并证明在此假设下，$n'^{(k+p^a(p-1))p^t} + n'^{(k-p^a(p-1))^{p^t}} \equiv gs \mod p^{3a+t+v+2}$。注意，这是一个双射，因为 x' 与 p 互素。

首先注意到

$$(nx')^{(k+p^a(p-1))p^t}+(nx')^{(k-p^a(p-1))p^t}=(n'+p^{a+1}c)^{(k+p^a(p-1))p^t}+(n'+p^{a+1}c)^{(k-p^a(p-1))p^t}$$

但根据二项式定理，这就意味着它是

$$n'^{(k+p^a(p-1))p^t}+n'^{(k-p^a(p-1))^{p^t}}+kp^{a+t+1}c(n'^{(k+p^a(p-1)-1)p^t}+n'^{(k-p^a(p-1))^{p^t-1}})\text{ 模 }p^{3a+t+v+2}$$

根据假设，我们有 $p^{2a+1+v}|k$，这意味着

$$kp^{a+t+1}c(n'^{(k+p^a(p-1)-1)p^t}+n'^{(k-p^a(p-1))p^t-1})$$

模 $p^{3a+t+v+2}$ 消失，因此我们得到

$$(nx')^{(k+p^a(p-1))p^t}+(nx')^{(k-p^a(p-1))p^t}\equiv n'^{(k+p^a(p-1))p^t}+n'^{(k-p^a(p-1))p^t}\mod p^{3a+t+v+2}$$

因此，只需证明 国产成人

$$(nx')^{(k+p^a(p-1))p^t}+(nx')^{(k-p^a(p-1))p^t}\equiv g(n^{(k+p^a(p-1))p^t}+n^{(k-p^a(p-1))p^t})\mod p^{3a+t+v+2}$$

我们来分析

$$n^{(k+p^a(p-1))p^t}(x'^{(k+p^a(p-1))p^t}-g)+n^{(k-p^a(p-1))p^t}(x'^{(k-p^a(p-1))p^t}-g)$$

欧拉定理意味着 $x'^{(k+p^a(p-1))p^t}\equiv x'^{(k+rp^{3a+v+1}(p-1)+p^a(p-1))p^t}$ 模 $p^{3a+t+v+2}$，对任意 r 均成立，但随后注意到，我们可以选择 r，使得 $k'|rp^{3a+v+1}(p-1)+p^a(p-1)$（因为 p 模 k' 是可逆元）。对于这个 r，我们有 $(k+rp^{3a+v+1}(p-1)+p^a(p-1))p^t\equiv 1$ 模 d。由于 $k'|(p-1)(rp^{3a+v+1}+p^a)p^t$，我们可以将其写为 $k'=k_1k_2$，其中 $k_1|p-1$，且 $k_2|(rp^{3a+v+1}+p^a)p^t$。对于这个 k_1，我们看到$k_1|\gcd(k,p-1)$，因此 $d|\frac{p-1}{k_1}$，这立即意味着 $d|(rp^{3a+v+1}(p-1)+p^a(p-1))p^t$。因此，$(k+rp^{3a+v+1}(p-1)+p^a(p-1))p^t\equiv 1$ 模 d。令 $u=(k+rp^{3a+v+1}(p-1)+p^a(p-1))p^t$，

$$x'^{(k+p^a(p-1))p^t}-g\equiv(x'^{k'}-g)(\sum_{i=0}^{u-1}x'^{k'(u-1-i)}g^i)\mod p^{3a+t+v+2}$$

同样，令 $u'=(k+r'p^{3a+v+1}(p-1)+p^a(p-1))p^t$，其中存在 r' 满足 $k'|(r+r')(p-1)$，我们有

$$x'^{(k-p^a(p-1))p^t}-g\equiv(x'^{k'}-g)(\sum_{i=0}^{u'-1}x'^{k'(u'-1-i)}g^i)\mod p^{3a+t+v+2}$$

因此，接下来只需证明

$$n^{(k+p^a(p-1))p^t}(\sum_{i=0}^{u-1}x'^{k'(u-1-i)}g^i)+n^{(k-p^a(p-1))p^t}(\sum_{i=0}^{u'-1}x'^{k'(u'-1-i)}g^i)\equiv 0\mod p^{2a+t+v+1}$$

现在，由于

$$\sum_{i=0}^{u-1} x'^{k'(u-1-i)} g^i = \frac{x'^{uk'} - g^u}{x'^{k'} - g}$$

提升意味着和模 $p^{v_p(u)} = p^{a+t}$ 为零，因此

$$n^{(k+p^a(p-1))p^t}(\sum_{i=0}^{u-1} x'^{k'(u-1-i)} g^i) \equiv n^{kp^t}(\sum_{i=0}^{u-1} x'^{k'(u-1-i)} g^i) \mod p^{2a+2t+1}$$

根据欧拉定理。 $t \geq v$ 给出了模 $p^{2a+t+1+v}$ 下的这一关系，现在重复这一过程，并

.....

$$n^{(k-p^a(p-1))p^t}(\sum_{i=0}^{u'-1} x'^{k'(u'-1-i)} g^i)$$

这表明只需证明

$$\sum_{i=0}^{u-1} x'^{k'(u-1-i)} g^i + \sum_{i=0}^{u'-1} x'^{k'(u'-1-i)} g^i \equiv 0 \mod p^{2a+t+v+1}$$

将 $u = p^{a+t+v}q + y$ 和 $u' = p^{a+t+v}q' + y'$ 写成 $0 \leq y$、$y' < p^{a+t+v}$。

首先，我们断言我们的表达式恰好是

$$(q+q')\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(p^{a+t+v}-1-i)} g^i + g^q \sum_{i=0}^{y-1} x'^{k'(y-1-i)} g^i + g^{q'} \sum_{i=0}^{y'-1} x'^{k'(y'-1-i)} g^i \mod p^{2a+1+t+v}$$

我们有，对于任意正整数 c,

$$\sum_{i=cp^{a+t+v}}^{(c+1)p^{a+t+v}-1} x'^{k'(u-1-i)} g^i = \sum_{i=0}^{p^{a+t+v}-1} x'^{k'(u-1-cp^{a+t+v}-i)} g^{i+cp^{a+t+v}}$$

通过提升，我们有 $x'^{k'p^{a+t+v}} \equiv g^{p^{a+t+v}} \mod p^{2a+t+v+1}$，因此

$$\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(u'-1-cp^{a+t+v}-i)} g^{i+cp^{a+t+v}} \equiv \sum_{i=0}^{p^{a+t+v}-1} x'^{k'(u-1-i)} g^i \mod p^{2a+t+v+1}$$

然后注意到

$$\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(u-1-i)} g^i - x^{k'(p^{a+t+v}-1-i)} g^i = (x'^{k'(u-p^{a+t+v})} - 1) \sum_{i=0}^{p^{a+t+v}-1} x^{k'(p^{a+t+v}-1-i)} g^i$$

我们有 $v_p(x'^{k'(u-p^{a+t+v})} - 1) \geq a + 1 + a + t$，并且

$$v_p(\sum_{i=0}^{p^{a+t+v}-1} x^{k'(p^{a+t+v}-1-i)} g^i) \geq a + t + v$$

通过提升，因此

$$\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(u-1-i)}g^i - x^{k'(p^{a+t+v}-1-i)}g^i \equiv 0 \mod p^{3a+2t+v+1}$$

表明

$$\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(u-1-i)}g^i \equiv \sum_{i=0}^{p^{a+t+v}-1} x^{k'(p^{a+t+v}-1-i)}g^i \mod p^{2a+t+v+1}$$

总之，我们得到的是

$$\sum_{i=0}^{qp^{a+t+v}-1} x'^{k'(u-1-i)}g^i \equiv q \sum_{i=0}^{p^{a+t+v}-1} x'^{k'(p^{a+t+v}-1-i)}g^i \mod p^{2a+t+v+1}$$

现在我们知道了。

$$\sum_{i=qp^{a+t+v}}^{u-1} x'^{k'(u-1-i)}g^i \equiv g^q \sum_{i=0}^{y-1} x'^{k'(y-1-i)}g^i \mod p^{2a+t+v+1}$$

通过移位，因为

$$\sum_{i=qp^{a+t+v}}^{u-1} x'^{k'(u-1-i)}g^i \equiv \sum_{i=0}^{y-1} x'^{k'(y-1-i)}g^{i+q} \mod p^{2a+t+v+1}$$

对 u' 重复同样的论证并相加，即可完成该断言的证明。

现在我们断言，这不过是

$$\frac{u+u'}{p^{a+t+v}} \sum_{i=0}^{p^{a+t+v}-1} x'^{k'(p^{a+t+v}-1-i)}g^i \mod p^{2a+1+t+v}$$

若 $v = 0$，则由于 $p^{a+t}|u, u'$ ，可立即推出 $y = y' = 0$ 和 $q + q' = \frac{u+u'}{p^{a+t+v}}$，从而证明该断言。现在假设 $v > 0$，这意味着 $p^{a+t+v} \nmid u, u'$。由于 $0 < y+y' < 2p^{a+t+v}$ 且 $p^{a+t+v}|y+y'$，因此可得 $y+y' = p^{a+t+v}$，进而有 $q + q' = \frac{u+u'}{p^{a+t+v}} - 1$。因此，只需证明

$$g^q \sum_{i=0}^{y-1} x'^{k'i}g^{y-1-i} + g^{q'} \sum_{i=0}^{y'-1} x'^{k'i}g^{y'-1-i} - \sum_{i=0}^{p^{a+t+v}-1} x'^{k'i}g^{p^{a+t+v}-1-i} \equiv 0 \mod p^{2a+t+v+1}$$

注意到

$$\sum_{i=0}^{y-1} x'^{k'i}g^{p^{a+t+v}-1-i} - g^q x'^{k'i}g^{y-1-i} \equiv -(g^{qp^{a+t+v}+y} - g^{p^{a+t+v}}) \sum_{i=0}^{y-1} x'^{k'i}g^{-1-i} \equiv 0 \mod p^{2a+v+t+1}$$

注意到 $qp^{a+t+v}+y\equiv u\equiv 1$ 模 d 后。此外，由于

$$\sum_{i=y}^{p^{a+t+v}-1} x'^{k'i}g^{p^{a+t+v}-1-i}=\sum_{i=0}^{y'-1} x'^{k'(i+y)}g^{y'-1-i}$$

$$\sum_{i=y}^{p^{a+t+v}-1} x'^{k'i}g^{p^{a+t+v}-1-i}-g^{q'}\sum_{i=0}^{y'-1} x'^{k'i}g^{y'-1-i}$$

仅变为

$$(x'^{k'y}-g^{q'})\sum_{i=0}^{y'-1} x'^{k'i}g^{y'-1-i} \mod p^{2a+t+v+1}$$

现在注意到 $g^{q'}\equiv g^{q'p^{a+t+v}}\equiv x'^{k'q'p^{a+t+v}}\equiv x'^{k'(u'-y')}$ 模 $p^{2a+t+v+1}$，因此只需证明娱乐主管

$$(x'^{k'y}-x'^{k'(u'-y')})\sum_{i=0}^{y'-1} x'^{k'i}g^{y'-1-i}\equiv 0 \mod p^{2a+t+v+1}$$

然而，$v_p(x'^{k'y}-x'^{k'(u'-y')})=v_p(x'^{k'(u'-p^{a+t+v})}-1)\geq a+1+a+t$ 和

$$\sum_{i=0}^{y'-1} x'^{k'i}g^{y'-1-i}\equiv 0 \mod p^{a+t}$$

因此，最后我们得出结论：

$$\sum_{i=y}^{p^{a+t+v}-1} x'^{k'i}g^{p^{a+t+v}-1-i}-g^{q'}\sum_{i=0}^{y'-1} x'^{k'i}g^{y'-1-i}\equiv 0 \mod p^{2a+t+v+1}$$

从而完成该断言的证明。

因此，整个问题归结为证明在线计划。

$$\frac{u+u'}{p^{a+t+v}}\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(p^{a+t+v}-1-i)}g^{i}\equiv 0 \mod p^{2a+1+t+v}$$

注意，$u+u'$的赋值至少为 $2a+1+t+v$，因此 $\frac{u+u'}{p^{a+t+v}}$的赋值至少为 $a+1$，所以只需证明】【。

$$\sum_{i=0}^{p^{a+t+v}-1} x'^{k'(p^{a+t+v}-1-i)}g^{i}\equiv 0 \mod p^{a+t+v}$$

这是提升的直接推论。

推论 1

设 p 为一个奇素数，x 和 $y \bmod p$ 为剩余类，使得对于某个 $x \equiv y\mu \bmod p$，有一个 $\gcd(k, p-1)$ 次单位根 μ。令 $\mathfrak{S}_x$ 表示当 $n \equiv x$ 从 1 变化到 p^{a+1} 时，$n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t}$ $(k, a, t$（如定理 1 所述）所取得的模 $p^{3a+t+v+2}$ 剩余类构成的多重集，并计入其重数；对于 $\mathfrak{S}_y$ 也作类似定义。则 $\mathfrak{S}_x = \mathfrak{S}_y$。

定理 1 的主要内容表明，若 $x'^{k'} \equiv g \bmod p^{a+1}$，则对于任意可逆元 n 和满足 $n' \equiv nx' \bmod p^{a+1}$ 的 n'，

$$n'^{(k+p^a(p-1))p^t} + n'^{(k-p^a(p-1))p^t} \equiv g(n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t}) \text{ 模 } p^{3a+t+v+2}$$

令 $g \equiv 1 \bmod p^{a+1}$，并注意到 $x'^{k'} \equiv 1 \bmod p^{a+1}$ 当且仅当 $x'^{\gcd(p-1,k)} \equiv 1 \bmod p^{a+1}$（因为 $\gcd(p-1, k) = \gcd(p-1, k')$），由此可知，对于任意 $\gcd(p-1, k)$ 次单位根 $x' \bmod p^{a+1}$，

$$n'^{(k+p^a(p-1))p^t} + n'^{(k-p^a(p-1))p^t} \equiv n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t} \mod p^{3a+t+v+2}$$

现在将 $\gcd(p-1, k)$ 次单位根模 p 约化，可知其约化结果是模 p 的 $\gcd(p-1, k)$ 次单位根。此外，若其中两个模 p 同余，设为 y、y'，则由 $y^{\gcd(p-1,k)} - y'^{\gcd(p-1,k)} \equiv 0 \bmod p^{a+1}$ 可知 $y \equiv y' \bmod p^{a+1}$，这是由提升得到的。因此，它们的约化结果恰好各表示一个模 p 的 $\gcd(p-1, k)$ 次单位根。于是令 x' 为满足 $x' \equiv \mu \bmod p$ 的唯一模 p^{a+1} 的 $\gcd(p-1, k)$ 次单位根。接着注意到，将 n 与 n' 配对，在满足 $n \equiv x \bmod p^{a+1}$ 且满足 $n' \equiv y \bmod p^{a+1}$ 的正整数 $\le p^{a+1}$ 之间建立了一个双射，因为该映射是单射且两集合大小相同；然而，由于

$$n'^{(k+p^a(p-1))p^t} + n'^{(k-p^a(p-1))p^t} \equiv n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t} \mod p^{3a+t+v+2}$$

每一对对应项模 $p^{3a+t+v+2}$ 后都得到相同的元素，从而立即得到 $\mathfrak{S}_x = \mathfrak{S}_y$。

现在我们还可以证明一个同余式，它对库默尔同余的“困难”情形很有用。

推论 2

设 a、b、t 为非负整数，且 $p^{a+t} | b$ 和 $p - 1 \nmid b$。那么有

$$\sum_{n=1}^{p^{a+1}} n^b (n^{p^{a+t}(p-1)} - 1)^2 \equiv 0 \mod p^{3a+t+v+2}$$

设 S 为模 $p^{3a+t+v+2}$ 下 $\mathfrak{S}$ 中所有元素的和。由于 $p - 1 \nmid b$，我们可以找到一个模下的本原 d $p^{3a+t+v+2}$ $g\mathfrak{S} =$ 次单位根，使得对于某个。$\mathfrak{S}$ $d > 1$ $n^{(k+p^a\ p-1\ p^t} + n^{(k-p^a\ p-1\ p^t}$ 如果 $())()$ 是不可逆元，那么

取模 p，这意味着 $p|n$；但由于 $2p^{a+t} \geq 3a+2t+2$，我们得到它模 $p^{3a+t+v+2}$ 等于 0，从而推出 $S \equiv gS$ 模 $p^{3a+t+v+2}$。只需证明$g \not\equiv 1$ 模 p。假设这一点成立，并注意到 $p^{3a+t+v+2}|g^d-1=(g-1)(g^{d-1}+\cdots+1)$。我们有 $g^{d-1}+\cdots+1 \equiv d \bmod p$，这意味着第二项与 p 互素，因此 $p^{3a+t+v+2}|g-1$，这与本原性矛盾。因此

$$\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t} \equiv 0 \mod p^{3a+t+v+2}$$

因此，引理 2 蕴含

$$\sum_{n=1}^{p^{a+1}} n^{(k-p^a(p-1))p^t}(n^{p^{a+t}(p-1)}-1)^2 \equiv 0 \mod p^{3a+t+v+2}$$

现在，若 $p^{a+t}|b$，则对于某个满足 $p^{2a+1}|k$ 的 k，有 $b \equiv kp^t \bmod p^{a+t}(p-1)$，于是写作 $b=kp^t+lp^{a+t}(p-1)$，其中 v 是某个整数，这意味着我们的和就是

$$\sum_{n=1}^{p^{a+1}} n^{kp^t+lp^{a+t}(p-1)}(n^{p^{a+t}(p-1)}-1)^2 - n^{kp^t-p^{a+t}(p-1)}(n^{p^{a+t}(p-1)}-1)^2 \mod p^{3a+t+v+2}$$

然而，注意到 $n^{|l+1|p^{a+t}(p-1)}-1$ 可被 $n^{p^{a+t}(p-1)}-1$ 整除，和变为

$$\sum_{n=1}^{p^{a+1}} n^{kp^t+\min(l,-1)p^{a+t}(p-1)} f(n)(n^{p^{a+t}(p-1)}-1)^3$$

对于某个属于 $\mathbb{Z}$ 的 $f(n)$，根据欧拉定理，它模 $p^{3a+t+v+2}$ 为零。

由此，我们可以推导出一个线性关系，从而很快推出库默尔同余式。

定理 2

设 k 为不能被 $p-1$ 整除的正整数，且满足 $2p^{2a+1}|k$。那么对于任意非负整数 t 和满足 $k+p^a(p-1)r>0$ 的整数 r，我们有

$$\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1)r)p^t} \equiv r \sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^t} \mod p^{3a+t+v+2}$$

由引理 2 可得

$$\sum_{n=1}^{p^{a+1}} n^{kp^t} \equiv 0 \mod p^{3a+t+v+2}$$

因此，对 $r=0$，结论成立。

现在我们假设它对 $r-1$、r 成立。我们证明它对 $r+1$ 也成立。推论 2 告诉我们

$$\sum_{n=1}^{p^{a+1}} n^{k+p^a(p-1)(r-1)p^t}(n^{p^{a+t}(p-1)}-1)^2 \equiv 0 \mod p^{3a+t+v+2}$$

因此

$$\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1)(r+1))p^t} \equiv \sum_{n=1}^{p^{a+1}} 2n^{(k+p^a(p-1)r)p^t} - n^{(k+p^a(p-1)(r-1))p^t} \mod p^{3a+t+v+2}$$

根据归纳假设，我们得到

$$\sum_{n=1}^{p^{a+1}} 2n^{(k+p^a(p-1)r)p^t} - n^{k+p^a(p-1)(r-1))p^t} \equiv (r+1)\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^t} \mod p^{3a+t+v+2}$$

如所需。类似地，沿相反方向进行论证，可证明所有带有 $k+p^a(p-1)r>0$ 的负 r 都满足该结论，因为 $k+p^a(p-1)r>0$ 意味着 $(k+p^a(p-1)r)p^t \geq 2p^{a+t} \geq 3a+2t+2$。

同余式的证明

为了证明一般情形，我们将其分为三种情况：第一种情况与另外两种无关，而最后再将后两种情况结合起来。在整个证明过程中，我们还假设 $s>r$。

首先，注意到，在假设 $s>r$ 的情况下，证明中总可以排除 $1-p^{s-1}$ 项，因为此时 $s \geq r+p^a(p-1) > 2+2^a > a+2$，这意味着 $1-p^{s-1}$ 总是模 p^{a+1} 为零，因此，由于根据推论 2，$\frac{B_s}{s}$ 是一个 p-整数，我们得出 $(1-p^{s-1})\frac{B_s}{s} \equiv \frac{B_s}{s}$ 模 p^{a+1}。

情况 1：$v_p(r) < a$（这意味着 $v_p(s)=v_p(r)<a$）。

为证明模 p^{a+1} 下的结论，我们假设在此情形下，同余式在模 p^a 下成立，并注意到对于 $a=0$，这种情形为空。

考虑这个和

$$\sum_{n=1}^{p^a} n^r(n^{p^{a-1}(p-1)}-1)^p$$

对于满足 p 不整除 n 的项，欧拉定理表明，每一项都能被 p^{ap} 整除，因此 $p^{2a+v_p(r)+2}$，因为 $ap \geq 3p \geq 2a+v_p(r)+1$。现在

若 $p|n$，则 $p^{p^{a-1}(p-1)}|n^{p^{a-1}(p-1)}$，因此由于 $p^{a-1}(p-1) \geq 4(5^{a-1}) > 3a$，我们得出结论：

$$\sum_{m=1}^{p^{a-1}} (pm)^r ((pm)^{p^{a-1}(p-1)} - 1)^p \equiv -p^r \sum_{m=1}^{p^{a-1}} m^r \mod p^{2a+v_p(r)+1}$$

我们看到，

$$\sum_{m=1}^{p^{a-1}} m^r \equiv p^{a-1} B_r \mod p^{2a-2+v_p(r)+1}$$

根据引理 1，因此

$$-p^r \sum_{m=1}^{p^{a-1}} m^r \equiv -p^{r+a-1} B_r \mod p^{2a+v_p(r)+1}$$

（注明 $r \geq 2$ 后）。

现在和之前一样，和展开为

$$\sum_{n=1}^{p^a} \sum_{i=0}^{p} \binom{p}{i} (-1)^{p-i} n^{r+ip^{a-1}(p-1)}$$

应用引理 1，我们得到

$$\sum_{i=0}^{p} \binom{p}{i} (-1)^{p-i} B_{r+ip^{a-1}(p-1)} \equiv -p^{r-1} B_r \mod p^{a+v_p(r)+1}$$

因此

$$B_{r+p^a(p-1)} - B_r + \sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} B_{r+ip^{a-1}(p-1)} \equiv -p^{r-1} B_r \mod p^{a+v_p(r)+1}$$

现在我们有大小规律

$$(1-p^{r-1}) \frac{B_r}{r} \equiv \frac{B_{r+ip^{a-1}(p-1)}}{r+ip^{a-1}(p-1)} \mod p^a$$

so

$$B_{r+ip^{a-1}(p-1)} \equiv (1-p^{r-1})(r+ip^{a-1}(p-1)) \frac{B_r}{r} \mod p^{a+v_p(r)}$$

由于 $v_p(r+ip^{a-1}(p-1)) \geq v_p(r)$。现在模 $p^{a+v_{p(r)}+1}$，

$$\sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} B_{r+ip^{a-1}(p-1)} \equiv (1-p^{r-1}) \sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} (r+ip^{a-1}(p-1)) \frac{B_r}{r}$$

并注意到

$$\sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} i = -p$$

得到 $-(1-p^{r-1})p^a(p-1)\frac{B_r}{r}$。我们有 $v_p(p^{a+r-1}\frac{B_r}{r}) \geq a+r-1 \geq a+v_p(r)+1$，这里用到了引理 3，并注意到 $r \geq v_p(r)+2$，因此我们得出 $-(1-p^{r-1})p^a(p-1)\frac{B_r}{r} \equiv -p^a(p-1)\frac{B_r}{r}$ 模 $p^{a+v_p(r)+1}$。综合以上结果可得 $B_{r+p^a(p-1)} \equiv (r+p^a(p-1))\frac{B_r}{r} - p^{r-1}B_r$ 模 $p^{a+v_p(r)+1}$。再次应用引理 3 可得 $v_p(p^{a+r-1}B_r) \geq a+r-1+v_p(r)$，因此，由于 $r \geq 2$，我们看到 $p^a(p-1)(p^{r-1}B_r)$ 模 $p^{a+v_p(r)+1}$为零，因此

$$B_{r+p^a(p-1)} \equiv (r+p^a(p-1))\frac{B_r}{r} - (r+p^a(p-1))p^{r-1}\frac{B_r}{r} \mod p^{a+v_p(r)+1}$$

最后，由于 $v_p(r) = v_p(r+p^a(p-1))$，我们得出

$$\frac{B_{r+p^a(p-1)}}{r+p^a(p-1)} \equiv (1-p^{r-1})\frac{B_r}{r} \mod p^{a+1}$$

必要时反复应用这一同余，便完成了这一情形的证明。

要处理下一个情形，我们必须使用定理 2，而不能只用直接归纳法。这是因为，如果我们试图重复处理 $v_p(r) < a$ 这一情形时所用的同一论证，就会遇到这样的问题：二项式系数只能多提供一个 p 的因子，而实际上我们需要两个（一个是为了达到 a，另一个是因为分隔 r 的幂次比和中对应的幂次更大）

注意，从现在起也可以排除 $1-p^{r-1}$，因为 $r \geq 2p^a \geq 2^{a+1} \geq a+2$，且可使用与 s 相同的论证。

Case 2: $v_p(r) = v_p(s) \geq a$.

定理 2 立即推出，模 p^{4a+t+2},

$$(k+p^a(p-1))\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1)b)p^t} \equiv (k+bp^a(p-1))\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^t}$$

现在，由引理 1 可得

$$(k+p^a(p-1))B_{(k+bp^a(p-1))p^t} \equiv (k+bp^a(p-1))B_{(k+p^a(p-1))p^t} \mod p^{3a+t+1}$$

因此，如果 r 不是 p 的倍数，那么立即除以 $p^t(k+p^a(p-1))(k+bp^a(p-1))$（赋值为 $2a+t$）即可得出该定理。

情形 3：分支

现在关键是考察这个对象

$$\sum_{n=1}^{p^{a+1}} n^{kp^t}(n^{p^{a+t-1}(p-1)}-1)^p$$

它模 $p^{p(a+t)}$ 为零，因此也模 p^{3a+t+2}为零。根据二项式定理，这恰好等于

$$\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^t} - n^{kp^t} + \sum_{n=1}^{p^{a+1}} \sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} n^{kp^t + ip^{a+t-1}(p-1)}$$

这个双重求和只是

$$\sum_{i=1}^{p-1} \binom{p}{i} (-1)^{p-i} (\frac{k}{p^a} + i) \sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^{t-1}} \mod p^{3a+t+2}$$

由定理 2 可知，因此整个和就归结为

$$-p \sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^{t-1}} \mod p^{3a+t+2}$$

这意味着

$$\sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^t} \equiv p \sum_{n=1}^{p^{a+1}} n^{(k+p^a(p-1))p^{t-1}} \mod p^{3a+t+2}$$

再次使用引理 1，我们得到

$$B_{(k+p^a(p-1))p^t} \equiv p B_{(k+p^a(p-1)r)p^{t-1}} \mod p^{2a+t+1}$$

最后，立即除以（$k + p^a(p-1))p^t$ （赋值为 $a + t$），即可得到

$$\frac{B_{(k+p^a(p-1))p^t}}{(k+p^a(p-1))p^t} \equiv \frac{B_{(k+p^a(p-1))p^{t-1}}}{(k+p^a(p-1))p^{t-1}} \mod p^{a+1}$$

完成分支步骤，从而完成全部库默尔同余式的证明。

因此，我们通过理解局部行为，并在全局和的背景下对其进行诠释，完成了证明库默尔同余的目标。

注意到集合 $\mathfrak{S}$ 带有一个$(\mathbb{Z}/p^{3a+t+v+2}\mathbb{Z})^*$ 作用，而定理 3 的内容是，在此作用下， d次单位根的子群 μ_d 包含于 Stab($\mathfrak{S}$) 中。现在我们来更全面地分类 Stab($\mathfrak{S}$)。我们需要一些引理。

在开始证明之前，我们先简要说明一下关于 p-进赋值和多项式的问题。对于多项式 $g(x)$，我们称对于剩余类 $s \bmod p^k$，$v_p(g(s)) \geq l$，当且仅当对剩余类$s \bmod p^k$ 中的每个正整数 s'，都有 $g(s') \equiv 0 \bmod p^l$ （一般来说，我们可以说 $v_p(g(s)) = \min_{s' \equiv s \text{ 模 } p^k} v_p(g(s'))$）。

引理 4

令 p 为奇素数，并设 $f(x) = x^{(k+p^a(p-1))p^t} + x^{(k-p^a(p-1))p^t}$ 为多项式。那么对于任意满足 n 与 p互素的正整数 m、n，有 $v_p(f^{(m)}(n)) \geq 2a+t+v$。此外，如果 $m=1$，则有 $v_p(f(m)(n)) \geq 2a+t+1+v$；若 $v<t$，则等号总是成立。对于 $m=2$，如果 $v=t$，则有 $v_p(f(m)(n)) = 2a+2t$；如果 $v<t$，则有 $v_p(f(m)(n) \geq 2a+t+v+1$。最后，对于 $m=3$ 和 $v=t$，除非 $p=3$，否则有 $v_p(f(m)(n)) = 2a+2t$；若 $p=3$，则其值为 $\geq 2a+2t+1$；对于 $v<t$，有 $v_p(f(m)(n)) \geq 2a+t+v+1$。

展开 $f^{(m)}(n)$，我们得到

$$n^{(k+p^a(p-1))p^t-m}\prod_{i=0}^{m-1}((k+p^a(p-1))p^t-i)+n^{(k-p^a(p-1))p^t-m}\prod_{i=0}^{m-1}((k-p^a(p-1))p^t-i)$$

由于 m 是一个正整数，每个乘积的赋值至少为 $a+t$，因此欧拉定理意味着这恰好是

$$n^{kp^t-m}(\prod_{i=0}^{m-1}((k+p^a(p-1))p^t-i)+\prod_{i=0}^{m-1}((k-p^a(p-1))p^t-i)) \mod p^{2a+2t+1}$$

然后注意，乘积之和恰好就是

$$p^{a+t}(p-1)(\prod_{i=1}^{m-1}(p^{a+t}(p-1)-i)+(-1)^m\prod_{i=1}^{m-1}(p^{a+t}(p-1)+i)) \mod p^{2a+t+1+v}$$

代入 $m=1$ 即可立即得到第二个陈述中的不等式。对于等号成立的情形，将 $m=1$ 代入该表达式。

$$n^{kp^t-m}\prod_{i=0}^{m-1}((k+p^a(p-1))p^t-i)+\prod_{i=0}^{m-1}((k-p^a(p-1))p^t-i))$$

给出 $f'(n) \equiv 2n^{kp^t-m}kp^t$ 模 $p^{2a+2t+1}$，且若 $v_p(k) < 2a+1+t$，则$v_p(kp^t) < 2a+2t+1$，因此在此情形下，$f'(n)$ 的赋值恰为 $v_p(k)+t = 2a+t+1+v$。

对于 $m=2$ 的情况，我们有表达式为 $2p^{2a+2t}(p-1) \mod p^{2a+t+v+1}$.
如果 $t=v$，那么我们得到 $2p^{2a+2t}(p-1) \mod p^{2a+2t+1}$，因此 $v_p(f''(n)) = 2a+2t$。如果 $v<t$，注意到 $2a+2t \geq 2a+t+v+1$，因此 $2p^{2a+2t}(p-1) \equiv 0 \mod p^{2a+t+v+1}$，如所需。

代入 $m=3$, $p^{a+t}(p-1)((p^{a+t}(p-1)-1)(p^{a+t}(p-1)-2)-(p^{a+t}(p-1)+1)(p^{a+t}(p-1)+2)) \equiv -6p^{2(a+t)}(p-1)^2$ 模 $p^{2a+t+v+1}$。若 $v=t$，则可得 $f'''(n)$ 的赋值为 $2a+2t$（当 $p \neq 3$ 时），且模 $p^{2a+2t+1}$（当 $p=3$ 时）为零。若 $v<t$，则 $f'''(n)$ 再次自动模 $p^{2a+t+v+1}$ 为零。

对于第一种情况，只需证明

$$\prod_{i=1}^{m-1}(p^{a+t}(p-1)-i)+(-1)^m\prod_{i=1}^{m-1}(p^{a+t}(p-1)+i)\equiv 0 \mod p^{a+v}$$

模 p^{a+v} 约化后得到

$$(-1)^{m-1}(m-1)!+(-1)^m(m-1)!\equiv 0 \mod p^{a+v}$$

如所求。

推论 3

设 r 为非负整数，$k\geq r$ 为正整数。那么，对于任意与 p互素的整数 s，$f(s+p^kx)\equiv f(s)+f'(s)p^kx$模 $p^{2a+t+v+2k}$。此外，若 $v<t$，则有更强的 $f(s+p^kx)\equiv f(s)+f'(s)p^kx$模 $p^{2a+t+v+2k+1}$

设 $\deg(f)=w$。对于任意正整数 k，有

$$f(s+p^kx)=\sum_{n=0}^{w}f^{(n)}(s)\frac{(p^kx)^n}{n!}$$

由引理 4 可知 $f^{(n)}(s)\geq 2a+t+v$，因此对于 $n>1$，我们有$v_p(f^{(n)}(s)(p^kx)^n/n!)\geq 2a+t+v+2k$，因此

$$f(s+p^kx)\equiv f(s)+f'(s)p^kx \mod p^{2a+t+v+2k}$$

现在假设 $v<t$。那么我们断言，对于所有 $n\geq 2$，$v_p(f^{(n)}(s)(p^kx)^n/n!)\geq 2a+t+v+2k+1$。对于 $n=2$ 或 3，引理 4 表明 $v_p(f^{(n)}(s))\geq 2a+t+v+1$，因此 $v_p(f^{(n)}(s)(p^kx)^n/n!)\geq 2a+t+v+1+2k$，当 $n=2$ 时成立；而当 $n=3$ 时，$2a+t+v+1+3k-1\geq 2a+t+v+1+2k$，从而证明了这些情形下的断言。对于 $n>3$，我们有 $v_p(f^{(n)}(s)(p^kx)^n/n!)\geq 2a+t+v+4k-1\geq 2a+t+v+2k+1$，这就完成了所有情形的证明，并得出情形 $v<t$。

引理 5

假设 $v=t$。那么对于每个满足 $0\leq s\leq a$ 的非负整数 s，恰好存在 $p^{a-s}(p-1)$ 个满足 u 且与 p 互素的正整数 $u\leq p^{a+1}$，以及 $v_p(f'(u))\geq 2a+2t+s+1$。

我们通过归纳法证明，对于任意非负整数 s，$f'(x)\equiv 0 \mod p^{2a+2t+s+1}$ 有 $p-1$ 个模 p^{s+1} 的解 u。$s=0$ 的基例可由引理 4 立即得出。假设该命题对 $s-1$ 成立，并令u' 为 $f'(x)\equiv 0 \mod p^{2a+2t+s}$的一个解。我们证明 u' 可以提升到

u 模 p^{s+1}，且 $f'(u) \equiv 0$ 模 $p^{2a+2t+s+1}$。通过泰勒级数展开，我们得到：

$$f'(u' + p^s x) = \sum_{n=0}^{w-1} f^{(n+1)}(u') \frac{(p^s x)^n}{n!}$$

去掉前两项后得到

$$f'(u') + f''(u') p^s x + \sum_{n=2}^{w-1} f^{(n+1)}(u') \frac{(p^s x)^n}{n!}$$

由引理 4 可知，对于任意 n，$f^{(n+1)}(u')$ 被 p^{2a+2t} 整除；并且由于对于 $n > 1$，我们有 $v_p(\frac{(p^s x)^n}{n!}) \geq 2s \geq s+1$，~~因为根据假设，~~ $s \geq 1$，
$f^{(n+1)}\ u'\ \frac{p^s x\ ^n}{n}$ $p^{2a+2t+s+1}$ $f'\ u' + p^s x \equiv f'\ u'\ + ( )\ ()!$被
$f''\ u'\ p^s x$ $p^{2a+2t+s+1}$
整除。因此，( ) ( ) ( ) mod，这立即意味着 u' 有唯一的提升。此外，对于任意满足 $f'(u') \not\equiv 0 \bmod p^{2a+2t+s}$ 的 $u' \bmod p^s$，我们有

$$f'(u' + p^s x) \equiv f'(u') + f''(u') p^s x \mod p^{2a+2t+s+1}$$

但此时 $v_p(f'(u')) < v_p(f''(u')p^s)$，因此不存在能在此处给出一个解的提升，这意味着模 p^{s+1} 的所有解都是模 p^s 的解的提升。证明这一点后，注意到有 $p^{a-s}(p-1)$ 个满足 $k \equiv u \bmod p^{a+1}$ 的正整数 $k \leq p^{a+1}$，证毕。

定理 3

在定理 1 的条件下，Stab(𝔖) $= \mu_n$ 当且仅当 $n = dp^a$；若 $v < t$，且$n = d$ 当且仅当 $v = t$。

由于 Stab(𝔖) 由 $(\mathbb{Z}/p^{3a+t+v+2}\mathbb{Z})^*$ 对 $\mathfrak{S}$ 的群作用定义，因此 Stab(𝔖) 是 $(\mathbb{Z}/p^{3a+t+v+2}\mathbb{Z})^*$ 的子群，故特别是循环的。令 P 为 Stab(𝔖) 的 p-Sylow 子群，则可将 Stab(𝔖) 写为 $= PG$，其中 G 是一个阶与 p 互素的阿贝尔群（这里的乘积同构于直积）。因此，G 由所有阶与 p 互素的元素组成，故其阶整除 $p-1$。

由于 p 是奇数，这类元素构成的子群必然是 μ_{p-1}，因为 $(\mathbb{Z}/p^{3a+t+v+2}\mathbb{Z})^*$ 是循环的。现在注意，若 $g \in$ 属于 Stab(𝔖)，则其模 p 的约化 g' 自动属于 Stab(𝔖′)，其中 S' 是 S 模 p 定义的。我们有

$$n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t} \equiv 2n^{k'} \mod p$$

因此，$\mathfrak{S}'$ 由形如 $2n^{\gcd(k,p-1)}$的元素组成，而这构成了 μ'_d的一个陪集。因此，Stab(𝔖′) $= \mu'_d$，这意味着 $g' \in \mu'_d$。然而，由于 ord$_p(g)$|ord$_{p^{3a+t+v+2}}(g)$，且 ord$_{p^{3a+t+v+2}}(g)$与 p互素，根据提升可知，ord$_p(g)$ =ord$_{p^{3a+t+v+2}}(g)$，从而 $g \in \mu_d$。定理 2 随即推出 $\mu_d \subset$Stab(𝔖)，特别地，$\mu_d \subset G$，因此我们得出结论：$G = \mu_d$。

接下来需要分析 P。首先，我们找出 P 的阶为$\leq p^r$ 的某个非负整数 r时的一个刻画。回顾其为循环的，这一条件等价于不存在阶为 p^{r+1}的元素。如果 g 是某个阶为 p^{r+1}的元素，那么它必然满足模 $p^{3a+t+v+1-r}$同余于 1，因此对于任意元素 $s \in \mathfrak{S}$， s 在由 g 生成的子群作用下的轨道，将是由满足模 $p^{3a+t+v+2}$ 同余于 $s+p^{3a+1+t+v-r}x$ 的 $0 \leq x \leq p^{r+1}-1$所组成的集合。因此，每个满足模 $p^{3a+1+t+v-r}$ 同余于 $s' \equiv s$ 的元素 s'，都必须在 $\mathfrak{S}$中出现相同的次数。

现在我们引入一些术语。给定非负整数 $i \geq k$ 以及一个特定的模 p^k剩余类 s，我们将 p^{i-k} 个 s 模 p^i 的提升上 $g(s) \bmod p^{2a+t+1+v+i}$的取值称为 $g(s)$的第 i层分支。此外，我们将此类 s 的第 i层 i 定义为所有第 i层分支（模 $p^{2a+t+1+v+i}$取值）构成的多重集。对于 $t > j$，如果一个多重集 $\mathfrak{T} \bmod p^t$ j满足：对任意元素 $s \in \mathfrak{T}$，其模 p^{t-j} 约化的 p^j 个提升在 $\mathfrak{T}$中出现次数相同，则称该多重集是均衡的。此外，如果一个多重集的 j-特征是 j-均衡的，则称其为良好；否则称为不良。注意，删除一个良好的多重子集，绝不会改变该多重集的 j-特征。

根据这些定义， P的大小为 $\leq p^r$ 当且仅当 $\mathfrak{S}$ 不是 $r+1$-均衡的。现在注意到，$\mathfrak{S}$ 是 $\mathfrak{S}_x$ 的互不相交并，其中 x 遍历模 p的可逆剩余类。设 $s_1, ..., s_d$ 是 $\mu_{\gcd(p-1,k)}$ 在$(\mathbb{Z}/p\mathbb{Z})^*$ 中的一组陪集代表元。根据推论 3， $\mathfrak{S}$ 恰好是多重集 $\coprod_{i=1}^{d} \mathfrak{S}_{s_i}$的$\gcd(p-1,k)$个副本。令 $\mathfrak{V} = \coprod_{i=1}^{d} \mathfrak{S}_{s_i}$。由此立即可得， $\mathfrak{V}$ 是 $r+1$-均衡的当且仅当 $\mathfrak{S}$ 是。再次注意到

$$n^{(k+p^a(p-1))p^t} + n^{(k-p^a(p-1))p^t} \equiv 2n^{k'} \mod p$$

如果 $x \neq y\mu$ 模 p 同余于某个 $p-1$、k 互素的单位根 μ，则可知即使将范围限制在模 p 的情形下， $\mathfrak{S}_x$ 和 $\mathfrak{S}_y$ 仍然是不相交的。因此，对于任意 $s \in \mathfrak{S}_x$， $\mathfrak{S}_y$ 中都不可能出现满足 $s' \equiv s$ 模 $p^{3a+1+t-r}$ 的元素 s'。由此， $\mathfrak{V}$ 是 $r+1$-平衡的，当且仅当对于每个 x 和 $s \in \mathfrak{S}_x$，所有 s' 在 $\mathfrak{S}_x$ 中出现的次数都相同，而这恰好等价于对每个 x， $\mathfrak{S}_x$ 都是 $r+1$-平衡的。最后，注意到如果 $\mathfrak{S}_x$ 是 $r+1$-平衡的，那么 $\mathfrak{S}'_x$ 就是 $r+1-q$-平衡的，其中 $\mathfrak{S}'_x$ 是 $\mathfrak{S}_x$ 模 $p^{3a+t+v+2-q}$ 的约化。

情况 1： $v < t$

在这种情况下，我们证明 P 是阶为 p^a 的循环群。为了证明 P 的大小为 p^a，我们证明每个 $\mathfrak{S}_x$ 都是 1-平衡的，但不是 $a+1$-平衡的。为了证明 $\mathfrak{S}_x$ 不是 $a+1$-平衡的，注意在推论 3 中取 $k=1$，可得 $f(s+px) \equiv f(s) + f'(s)px \equiv f(s)$ 模 $p^{2a+t+v+2}$，因此 $\mathfrak{S}_x$ 模 $p^{2a+t+v+2}$ 的约化不是 1-平衡的，这意味着对每个 x， $\mathfrak{S}_x$ 都不是 $a+1$-平衡的。

现在我们证明每个 $\mathfrak{S}_x$ 都是 a-平衡的。考虑由 $a_n = \lceil \frac{a+1}{2^n} \rceil$ 给出的正整数数列，其中 $n \geq 0$ 取遍所有值。注意到 $2\lceil x \rceil \geq \lceil 2x \rceil$，可知 $2a_n \geq a_{n-1}$，因此根据推论 3 的加强版，对每个正整数 n，都有 $f(s + p^{a_n}x) \equiv f(s) + f'(s)p^{a_n}x$ 模 $p^{2a+t+v+a_{n-1}+1}$。现在我们证明，对每个正整数 k，$\mathfrak{S}_x$ 都是 $a_0 - a_k = a + 1 - a_k$-平衡的。取一个模 p^{a_k} 的剩余类 s，并计算 s 的 $a+1$ 层中，固定的提升 u（它是 $f(s)$ 模 $p^{2a+t+v+a_k+1}$ 的一个提升）出现的次数。为此，只需找出满足 $s' \equiv s$ 模 p^{a_k} 且 $f(s') \equiv u$ 模 p^{3a+t+2} 的模 p^{a+1} 的 s' 的个数。我们用归纳法证明，对所有 $0 \leq r \leq n$，存在唯一一个 s 模 p^{a_r} 的提升 s'，使得 $u \equiv f(s')$ 模 $p^{2a+t+v+a_r+1}$。$r = k$ 的基例显然成立。现在假设结论对 n 成立，并证明它对 $n-1$ 也成立。令 s_n 为 s 模 p^{a_n} 的唯一提升，满足 $u \equiv f(s_n)$ 模 $p^{2a+t+v+a_n+1}$。于是有 $f(s_n + p^{a_n}x) \equiv f(s_n) + f'(s_n)p^{a_n}x$ 模 $p^{2a+t+v+a_{n-1}+1}$。由于 $v_p(f'(s_n)p^{a_n}) = 2a + t + v + a_n + 1$，这唯一确定了模 $p^{a_{n-1}-a_n}$ 的 x，从而唯一确定了 s_{n-1}。因此，模 p^{a+1} 的 s_0 被唯一确定，这说明对于给定的 u，恰有一个 s 模 p^{a+1} 的提升与之对应。因此，$\mathfrak{S}_x$ 是 $a_0 - a_k = a + 1 - a_k$-平衡的。取足够大的 k，即可推出 $\mathfrak{S}_x$ 是 a-平衡的。

情形 2：$t = v$

由推论 3 可知，给定 $v_p(f'(s)) = 2a + 2t + 1 + u$ 对某个非负整数 u，对于所有满足 $k \geq u + 1$ 的 k，$f(s + p^k x) \equiv f(s)$ 模 $p^{2a+2t+k+u+1}$，这表明对于 s'，s 模 p^k 的约化在其 $k + u$ 个分支上对于这样的 k 是常数。然而，我们还有 $f(s + p^k x) \equiv f(s) + f'(s)p^k x$ 模 $p^{2a+2t+k+u+2}$ 对于 $k \geq u + 2$ 成立，因此对于这样的 k，给定 $f(s')$ 的一个 $k + u$ 分支，其 $f(s')$ 的 $k + u + 1$ 个分支是常数，而不同 $k+u$ 分支的 $k + u + 1$ 个分支彼此不同；因此，它们恰好各一次构成 $f(s')$ 的 $k + u$ 分支模 $p^{2a+k+u+1}$ 的所有提升，这意味着 s' 的 $k + u + 1$ 层是 1-平衡的。

现在假设对于某个正整数 $u \leq \lfloor \frac{a}{2} \rfloor$，存在一个 s 模 p^{u+1}，满足 $v_p(f'(s)) < 2a + 2t + u + 1$。那么第一条条件和引理 5 的证明表明，对于 s 的任意提升 s' 模 p^k，都有 $v_p(f'(s')) = v_p(f'(s))$。令 $v_p(f'(s)) = 2a + 2t + 1 + w$，则 $w < u$ 推出 $w \leq \lfloor \frac{a}{2} \rfloor - 1$。特别地，取 $k = 3a + 2t + 1 - v_p(f'(s'))$，关于 w 的不等式推出 $k = a - w \geq w + 2$，因此上述结论适用，故位于 s' 模 p^k 上方的 $a+1$ 层是 1- 平衡的。注意到 $v_p(f'(s)) = v_p(f'(s'))$，所以 s 的 $a+1$ 层（它是其模 p^k 的提升的 $a+1$ 层的不相交并）也平衡。逐一考察每个 $\mathfrak{S}_x$，引理 5 现在允许我们移除除模 $p^{\lfloor \frac{a}{2} \rfloor + 1}$ 下的一个元素之外所有元素上方的 $a+1$ 层，而不改变 $\mathfrak{S}$ 的 1-质量，因此只需证明模 $p^{\lfloor \frac{a}{2} \rfloor + 1}$ 下任意（尽管我们会逐一证明）例外元素上方的 $a+1$ 层并非 1-平衡。由推论 3 可知，对于任意这样的例外 s，$f(s + p^{\lfloor \frac{a}{2} \rfloor + 1}x) \equiv f(s) + f'(s)p^{\lfloor \frac{a}{2} \rfloor + 1}x$模 $p^{2a+2t+2\lfloor \frac{a}{2} \rfloor + 2}$；但由于 $f'(s) \equiv 0$模 $p^{2a+2t+\lfloor \frac{a}{2} \rfloor + 1}$，我们得到$f(s + p^{\lfloor \frac{a}{2} \rfloor + 1}x) \equiv f(s)$ 模 $p^{2a+2t+2\lfloor \frac{a}{2} \rfloor + 2}$。

如果 a 为偶数，$2a+2t+2\lfloor\frac{a}{2}\rfloor+2=3a+2t+2$，因此每个例外 s 的全部 $a+1$ 分支都相同，这立即意味着没有 $\mathfrak{S}_x$ 是 1-平衡的。

剩下需要处理 a 为奇数的情况。取一个模 $p^{\frac{a+1}{2}}$ 的例外元素 s，再次只需证明其 $a+1$ 层不是 1-平衡的。根据引理 5 的证明，我们可以选取一个正整数 s'，其模 $p^{\frac{a+1}{2}}$ 的约化为 s，使得 $f'(s')\equiv 0$ 模 $p^{\frac{5a+3}{2}+2t}$。由泰勒级数展开可得

$$f(s'+p^{\frac{a+1}{2}}x)=\sum_{n=0}^{w}f^{(n)}(s')\frac{(p^{\frac{a+1}{2}}x)^n}{n!}$$

对于 $n>2$，我们断言 $v_p(f^{(n)}(s')(p^{\frac{a+1}{2}}x)^n/n!)\geq 3a+2t+2$。对于 $n>3$，注意到由于引理 4 蕴含 $v_p(f^{(n)}(s'))\geq 2a+2t$，因此 $v_p(f^{(n)}(s')(p^{\frac{a+1}{2}}x)^n/n!)\geq 4a+2t+1\geq 3a+2t+2$，因为 $a\geq 1$。对于 $n=3$ 和 ~~$p>3$~~，不等式 $v_p(f^{(n)}(s'))\geq 2a+2t$ 再次给出 $v_p(f^{(n)}(s')(p^{\frac{a+1}{2}}x)^n/n!)\geq 2a+2t+3(\frac{a+1}{2})\geq 3a+2t+2$。最后，~~对于 $n=3$~~、$p=3$，引理 4 蕴含 $v_p(f^{(n)}(s'))\geq 2a+2t+1$，因此我们仍可得到 $v_p(f^{(n)}(s')(p^{\frac{a+1}{2}}x)^n/n!)\geq 2a+2t+3(\frac{a+1}{2})\geq 3a+2t+2$，~~从~~而证明了这一断言。

因此我们得出结论：

$$f(s'+p^{\frac{a+1}{2}}x)=f(s')+f'(s')p^{\frac{a+1}{2}}x+f''(s')\frac{p^{a+1}x^2}{2}\mod p^{3a+2t+2}$$

根据 s'，$v_p(f'(s')p^{\frac{a+1}{2}}x)\geq\frac{5a+3}{2}+2t+\frac{a+1}{2}=3a+2t+2$ 的构造，因此

$$f(s'+p^{\frac{a+1}{2}}x)=f(s')+f''(s')\frac{p^{a+1}x^2}{2}\mod p^{3a+2t+2}$$

只需证明 $f''(s')\frac{p^{a+1}x^2}{2}$ 无法取遍所有形如 $p^{3a+2t+1}k$ mod $p^{3a+2t+2}$ 的剩余类，这直接由映射 x^2 mod p 不是满射这一事实得出，从而完成证明。

参考文献

[1] Kubota, Tomio；Leopoldt, Heinrich-Wolfgang（1964），《ζ 值的 p 进理论。I. p 进狄利克雷 L 函数的引入》，《纯粹与应用数学杂志》，214/215：328–339

[2] 库默尔，恩斯特·爱德华（1851年），《关于某一类解析函数的有理展开系数的一般性质》，《纯粹与应用数学杂志》，41：368–372。

[3] G.F. 沃罗诺伊，关于伯努利数，哈尔科夫数学学会通讯 2（1890年）

129–148（俄语）

数学系，加州理工学院，美国加利福尼亚州帕萨迪纳，邮编 91125电子邮箱：
sgoodman@caltech.edu