arXiv:2603.03104v1 [math.NT] 3 Mar 2026

# 关于三个变量的弗罗贝尼乌斯数

´PETER SUHAJDA 和 ANITHA THILLAISUNDARAM

Abstract. 对于没有公因数的正整数 $a$、 $b$ 和 $c$， $a$、 $b$ 和 $c$ 的弗罗贝尼乌斯数定义为不能表示为 $a$、 $b$ 和 $c$ 的非负整数系数线性组合的最大整数。2017 年，Tripathi 给出了三个变量情形下弗罗贝尼乌斯数的算法公式，但该公式存在一些小的不一致之处。本文解决了这些不一致问题。

## 1. Introduction

对于整数 $n \geq 2$， $n$变量的弗罗贝尼乌斯问题 是确定不能表示为给定的 $n$ 个互质正整数的非负整数线性组合的最大正整数。这个最大正整数称为弗罗贝尼乌斯数。更准确地说，给定 $a_1, \ldots, a_n \in \mathbb{N}$，其中 $\gcd(a_1, \ldots, a_n) = 1$，弗罗贝尼乌斯数 $g(a_1, \ldots, a_n)$ 为

$$\max \mathbb{N} \backslash \{a_1 x_1 + \cdots + a_n x_n \mid x_1, \ldots, x_n \in \mathbb{N} \cup \{0\}\}.$$

二元情形，即 $n = 2$，是该问题的起源；这一情形由 Sylvester 于1884年加以考虑，并由 W. J. Curran Sharp 证明了 $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$；参见 [8]。除了考虑 $n$取更高值时的弗罗贝尼乌斯问题之外，如今也研究相关方面，例如伪弗罗贝尼乌斯数（例如参见 [6]），以及计算弗罗贝尼乌斯数的算法方面（例如参见 [4]）。

关于情形 $n = 3$，Curtis [2] 证明了对于 $n = 3$ 不存在弗罗贝尼乌斯数的闭多项式公式，对于 $n$ 的更高取值亦然。尽管如此，对于某些算术数列已经给出了公式；参见 [9] 以了解这些结果的综述。对于 $n = 3$ 的一般情形，Tripathi 在 [9], 中给出了具有算法性质的公式，其中采用了高度技术性的方法。然而，Tripathi 的结果中存在一些细微出入，我们在此予以解决。尽管 [9]的整个框架仍然适用，只需在过程中以及对最后一个陈述作少量调整。

更具体地说， [9]中的第一个不一致之处出现在 [9], 引理5中，涉及某个函数的连续局部极小值的计算。这个引理5被用于一系列逐步导向主要结果的结果中。在大多数情况下，这些其他结果的表述仍然成立，只需对证明进行调整。然而，最终主要结果的一部分表述，即 [9, 定理 5(b)], ，遗憾的是并不一致；这一点从第一作者在隆德大学撰写其学士论文期间获得的弗罗贝尼乌斯数计算数据 [7]中可以看出。调整主要结果证明的一个关键方面依赖于引理 4.14，该引理确立了某个数列各项之间的正确距离。

*Date*: 2026年3月4日。2020 *Mathematics Subject Classification.* 主分类号11D07；次分类号 11D04。*Key words and phrases.* 弗罗贝尼乌斯数，三变量弗罗贝尼乌斯数公式。

在本文中，我们给出所有必要的调整和修正；特别是，关于 [9, 5]引理 5]的修正，参见引理 2.7；关于上述距离的修正，参见引理 4.14。为简洁起见，也为方便读者，我们在此重述了 Tripathi 的许多论证和证明，尽管我们经常对其加以扩展，并提供额外细节以使说明更加清晰。由于算法公式的表述需要大量记号，我们请读者参阅第 4 节中的修正表述，即定理 4.16。不过，我们在此给出这些公式的概要。表 1 假设三个变量两两互素。如果并非如此，我们提醒读者可以使用 Johnson 公式；另见下文定理 2.1。

| **条件** | $g\ (a,\ b,\ c)\ + a$ |
|---|---|
| $\ell \le k$ | $ab - b$ |
| $\ell > k$ & $br < cq$ | $\begin{cases} b\big((\lambda+1)(a-\ell)+r-1\big) & \text{如果 } \lambda \ge \frac{c(q-1)-br}{b(a-\ell)+c}, \\ b(a-\ell-1)+c(q-\lambda-1) & \text{若 } \lambda \le \frac{c(q-1)-br}{b(a-\ell)+c}. \end{cases}$ |
| $\ell > k$ & $br > cq$, $\mu < \lfloor \frac{r}{u} \rfloor$ | 最大值 $\Big\{b(r-\mu u-1)\ b(u-1)\ + c\big(\mu(q+1)\ + q(\lfloor \frac{(a-\ell-r)\mu}{r} \rfloor + 1)\big)\Big\} + cq\lfloor \frac{a-\ell-1}{r} \rfloor$ |
| $\ell > k$ & $br > cq$, $\mu < \lfloor \frac{r}{u} \rfloor$ & $\Lambda > \Delta$ | $\max\big\{b(r-\Delta(a-\ell-r)\ -1)\ b(a-\ell-r-1)\ + c\big(\Delta(q+1)\ + q\big)\big\} + cq$ |
| $\ell > k$ & $br > cq$, $\mu < \lfloor \frac{r}{u} \rfloor$ & $\Delta' > \Lambda'$ | $\max\ \big\{b(r-1)\ b\big((a-\ell-1) \bmod r\big) + cq\big\} + cq\lfloor \frac{a-\ell-1}{r} \rfloor$. |
| $\ell > k$ & $br > cq$, $\mu > \lfloor \frac{r}{u} \rfloor$ | 最大值 $\{b(\widehat{x}-1)\ + cy_w,\quad b(\widehat{x}+u-x_\mu-1)\ + cy_\mu\} + cq\lfloor \frac{a-\ell-1}{r} \rfloor$. |

TABLE 1. 三个变量的所有公式汇总表 $a < b < c$，假设它们两两互素。关于所有记号，特别参见记号2.2、记号2.9、定理3.3、记号 4.5和定理 4.16。

三个变量的弗罗贝尼乌斯数的算法公式分为两个结果， [9], 即 [9, 定理 3] 和 [9, 定理 5]。此外，Tripathi采用略有不同的并行方法，在 [9, 定理 4] 和 [9, 定理 6],中给出了替代的算法公式，其中存在与 [9, 引理 6]类似的不一致。本文仅明确讨论Tripathi的定理3和定理5，因为我们的方法可以相应地调整，从而对 [9, 定理 4], 的证明、 [9, 定理 6] 的证明以及[9, 定理 6(b)]的表述作出必要修正。为求完整，我们在论文末尾给出 [9, 定理 6(b)]的修正版。

组织安排。 在第2节中，我们汇集了一些预备结果，并给出 [9, 引理5和 7]的修正版。随后，我们沿用 [9], 中的方法，根据涉及 $a$、 $b$ 和$c$取值的条件，将主要结果分为两部分，分别置于第3节和第 4 节。特别是，我们在第3节指出， [9, 定理 3] 的表述仍然成立；在第 4 节中，我们看到 [9, 定理5(a)] 是正确的，但 [9, 定理5(b)] 需要作一些小的调整。

## 2. Preliminary results

在全文中，设 $c > b > a \geq 2$ 为两两互素整数，即 $\gcd(a,b) = \gcd(a,c) = \gcd(b,c) = 1$。注意，基于以下 Johnson [3]的结果，我们可以采用更强的假设，即$a, b, c$两两互素，而不只是 $\gcd(a,b,c) = 1$:

**定理 2.1**。 [3, 参见定理 2] 设 $a$、$b$、$c \geq 2$ 满足 最大公因数$(a$、$b$、$c) = 1$。若 最大公因数$(b$、$c) = d$ 且 $b = db'$、$c = dc'$，则

$$g(a,b,c) = d \cdot g(a,b',c') + a(d-1).$$

我们回顾一下 [9] 中的以下记号:

**记号2.2**。 设 $c > b > a \geq 2$ 为两两互素整数。定义

$$k := \left\lfloor \frac{c}{b} \right\rfloor, \qquad \ell := cb^{-1} \pmod{a},$$

在本文中，每当我们将数 $z$ 对 $n$ 取模时，总是假设 $z \in \{0, 1, \ldots, n-1\}$。

**注2.3.** 如 [9, 引理 2] 所示，若 $\ell \leq k$，则 $g(a, b, c) = g(a, b)$；从现在起，我们总是假设 $\ell > k$。

我们先记录一个简单的观察，供后续使用。回顾一下，本文余下部分的基本假设是 $c > b > a \geq 2$ 两两互素。

**引理 2.4.** 设 $\ell > k$。则 $c - b\ell < 0$。

证明。 反设 $c - b\ell \geq 0$。显然，不可能有 $c - b\ell = 0$，因为这样便有 $\ell = k$。因此设 $c - b\ell > 0$。注意到 $c - b < bk \leq c$，所以有 $c > b\ell > bk > c - b$。然而， $c - b$ 与 $c$ 之间不存在能容纳两个不同的 $b$ 倍数的空间。因此结论成立。□

接下来回顾 [9] 中的以下结果。首先，对非负整数 $x$, $y$，定义$\mathbf{v}(x, y) := bx + cy$，并将其称为 $(x, y)$ 的$\mathbf{v}$-值。

**引理 2.5**。 [9, 引理 3] 假设 $\ell > k$。那么

$$g(a,b,c) = \max_{1 \leq x < a} \left\{ \min_{0 \leq t < a} \mathbf{v}\big((x + (a-\ell)t) \bmod a, t\big) \right\} - a.$$

由此得到以下定义 [9]:

定义 2.6。 [9, 定义 1] 设 $x \in \{0, 1, \ldots, a-1\}$。如果 $\mathbf{v}(x, y)$ 是局部极小值，则称之为局部极小值，当且仅当 $\mathbf{v}(x, y) \leq \min\big\{\mathbf{v}\big((x-\ell) \bmod a, y+1\big), \mathbf{v}\big((x+\ell) \bmod a, y-1\big)\big\}$ 当 $y \in \{1, \ldots, a-2\}$，$\mathbf{v}(x, y) \leq \mathbf{v}\big((x-\ell) \bmod a, y+1\big)$ 当 $y = 0$，$\mathbf{v}(x, y) \leq \mathbf{v}\big((x+\ell) \bmod a, y-1\big)$ 当 $y = a-1$.

进一步地，如果不存在满足 $y < \widetilde{y} < y'$ 的局部极小值 $\mathbf{v}(\widetilde{x}, \widetilde{y})$，则称两个局部极小值 $\mathbf{v}(x, y)$ 和 $\mathbf{v}(x', y')$ 是相邻的 。

显然，根据引理 2.5，我们只需研究$\mathbf{v}$值中的局部极小值，这正如 [9, 引理 5]中所做的那样。不过， [9, 引理 5] 中的陈述并不完全正确，因此我们在下文给出修正后的版本，并补充一些信息:

**引理 2.7**。 设 $\ell > k$，并令$\mathbf{v}(x, y)$ 和$\mathbf{v}(x', y')$ 为连续局部极小值。则$x, x' < \min\{a - \ell, \ell\}$。

此外，令 $\rho_x \in \{0, 1, \ldots, a - \ell - 1\}$ 满足 $\rho_x \equiv x - \ell$ 模（$a - \ell$），则有

$$\mathbf{v}(x', y') - \mathbf{v}(x, y) = \mathbf{v}\left((\rho_x \bmod \ell) - x, \left\lceil \frac{\ell - x}{a - \ell} \right\rceil + \left\lfloor \frac{\ell + \rho_x}{\ell} \right\rfloor\right).$$

证明。 我们沿用 [7, 引理 5.11] 中的设定。从 $\mathbf{v}(x, y)$ 出发，注意到随着我们依次考察连续的 $\mathbf{v}$ 值， $x$ 分量每次增加 $a - \ell$（模 $a$），而 $y$ 分量增加 1。为方便起见，我们记

$$x_i = x + i(a - \ell) \pmod a$$

为 $\mathbf{v}(x, y)$ 之后第 $i$ 个 $\mathbf{v}$ 值的 $x$ 分量。注意，这些连续的 $\mathbf{v}$ 值始终递增，直到 $x$ 分量首次大于或等于 $\ell$，此后 $\mathbf{v}$ 值便会减小。事实上，回想 $\ell > k$，尤其是由引理 2.4 可知 $b\ell > c$；若假设 $x$ 分量首次大于或等于 $\ell$ 的时刻为 $x_\iota$，则

$$\mathbf{v}(x_{\iota+1}, y + \iota + 1) - \mathbf{v}(x_\iota, y + \iota) = -b\ell + c < 0.$$

我们还注意到，由于 $\ell \le x_\iota \le a - 1$，可得 $0 \le x_{\iota+1} \le a - \ell - 1$。因此，第一个陈述得证。

我们计算得，从 $\mathbf{v}(x, y)$ 开始，连续递增的$\mathbf{v}$值的个数为

$$\iota = \left\lceil \frac{\ell - x}{a - \ell} \right\rceil.$$

若 $x_{\iota+1} \ge \ell$，则 $\mathbf{v}(x_{\iota+2}, y + \iota + 2)$ 同样严格小于 $\mathbf{v}(x_{\iota+1}, y + \iota + 1)$。由此可得，从 $\mathbf{v}(x_\iota, y + \iota)$ 开始连续递减次数等于

$$\left\lfloor \frac{x_\iota}{\ell} \right\rfloor.$$

根据 $\rho_x$ 的定义，我们有

$$\ell - x = \left\lceil \frac{\ell - x}{a - \ell} \right\rceil (a - \ell) - \rho_x$$

因此，由于 $x_\iota = x + \underline{\left\lceil \frac{\ell - x}{a - \ell} \right\rceil} (a - \ell)$，我们得到

$$x_\iota = \ell - x + \rho_x + x = \ell + \rho_x = \left\lfloor \frac{\ell + \rho_x}{\ell} \right\rfloor \ell + (\rho_x \bmod \ell).$$

因此，从 $\mathbf{v}(x_\iota, y + \iota)$ 开始连续递减次数为

$$\left\lfloor \frac{\ell + \rho_x}{\ell} \right\rfloor.$$

因此，为证明最后一个陈述，若下一个局部极小值位于$\mathbf{v}(x', y')$处，我们首先注意到

$$y' - y = \left\lceil \frac{\ell - x}{a - \ell} \right\rceil + \left\lfloor \frac{\ell + \rho_x}{\ell} \right\rfloor.$$

同样地，根据上述内容，我们计算出 t 为

$$\begin{aligned} x' - x &= \left\lceil \frac{\ell - x}{a - \ell} \right\rceil (a - \ell) - \left\lfloor \frac{\ell + \rho_x}{\ell} \right\rfloor \ell \\ &= \ell - x + \rho_x + (\rho_x \bmod \ell) - \ell - \rho_x \\ &= (\rho_x \bmod \ell) - x, \end{aligned}$$

如所要求的。 □

我们指出， [7, 引理5.11] 中的陈述与上面的引理不同，因为[7, 引理5.11] 仍存在一些需要处理的小的不一致之处。

**注 2.8.** 由 [9, 引理 4] 以及 $b\ell \equiv c$ （模 $a$），可知相邻的$\mathbf{v}$值之差是 $a$的非零倍数。因此，从 $\mathbf{v}(x,0)$开始并包括该值在内，所有相邻的$\mathbf{v}$值都属于 $[bx]$，即模 $a$的 $bx$同余类。

这里我们回顾 [9]的引理 7。尽管该引理的证明引用了 [9], 中错误的引理5，但其陈述仍然成立。为完整起见，我们给出修订后的证明，并首先回顾 [9]中的一些记号。

**记号 2.9.** 对于 $x \in \mathbb{N}$，我们记

$$\mathbf{m}(x) = \min\{z \in \mathbb{N} \mid z = bn_1 + cn_2 \text{ for some } n_1, n_2 \in \mathbb{N} \cup \{0\} \quad \text{and} \quad z \equiv x \pmod{a}\}.$$

Also

$$q := \left\lfloor \frac{a}{a-\ell} \right\rfloor, \quad r := a - q(a-\ell).$$

**注 2.10.** 还要注意， $r \equiv a$ 模（$a-\ell$）且 $r \equiv \ell$ 模（$a-\ell$）；事实上，这可由等式 $a = \ell + a - \ell$ 推出。此外， $r \leq \ell$。

我们也可以假设 $r > 0$，因为情形 $r = 0$ 等价于 $\ell = a - 1$，而 Brauer 和 Shockley 已解决了这一情形 [1, 第 220], 页，正如 [9, 注 2]中所述。不过，本文中的证明对情形 $r = 0$也同样适用，因此无需排除这一情形。

**引理 2.11.** [9, 引理 7] 设 $\ell > k$。对于 $x \in \{1, \ldots, a-1\}$,

$$\mathbf{m}(bx) = \min\{bx, \mathbf{m}(bx') + cy'\},$$

其中

$$(x', y') = \begin{cases} \left(x \bmod (a-\ell) - r + a - \ell,\ q - \lfloor \frac{x}{a-\ell} \rfloor + 1\right) & \text{if } 0 \leq x \bmod (a-\ell) \leq r-1; \\ \left(x \bmod (a-\ell) - r,\ q - \lfloor \frac{x}{a-\ell} \rfloor\right) & \text{if } r \leq x \bmod (a-\ell) \leq a-\ell. \end{cases}$$

证明。正如前一个结果的证明中所观察到的，从 $\mathbf{v}(x, 0)$ 开始，$\mathbf{v}$ 值的首次下降发生在 $\mathbf{v}(x', y')$ 处，其中（ $x', y'$ ）如上文所述。因此，从 $\mathbf{v}(x, 0)$ 开始的连续 $\mathbf{v}$ 值的最小值，要么是 $\mathbf{v}(x, 0)$，要么是从 $\mathbf{v}(x', y')$ 开始的所有连续 $\mathbf{v}$值中的最小值。由于从 $\mathbf{v}(x', y')$ 开始的所有连续 $\mathbf{v}$值也都可以分别表示为 $cy'$ 与从 $\mathbf{v}(x', 0)$ 开始的所有连续 $\mathbf{v}$值之和，注意到从 $\mathbf{v}(x', 0)$ 开始的所有连续 $\mathbf{v}$值中的最小值记为 $\mathbf{m}(bx')$，结论即得。□

当然，借助引理 2.7，即 [9, 引理 5], 的修正版本，我们也可以通过将（$x', y'$）替换为$\mathbf{v}$（$x$,0）之后下一个局部极小值的坐标，来加强前一个引理。然而，这对于证明主要结果而言并非必要。

接下来，我们现在分成两种情形：首先当 $br < cq$ （第3节），其次当$br > cq$ （第 4 节）。注意 $br \neq cq$，正如 [9, 第3.5]小节中所指出的那样。事实上，我们有$\gcd(b, c) = 1$ 和 $r < a - \ell < a < c$。

## 3. The case $br < cq$

我们首先记录一个有用的结果。

**引理 3.1**。 设 $\mathbf{v}(x,y)$ 和 $\mathbf{v}(x',y')$ 为连续局部极小值，且满足 $y < y'$。若 $\ell > k$ 且$br < cq$，则 $a-\ell \leq \ell$ 且 $\mathbf{v}(x',y') > \mathbf{v}(x,y)$。

证明。 首先注意到，假设 $br < cq$ 会迫使 $r < \ell$。事实上，由于 $r \leq \ell$，如果 $r = \ell$ ，那么$q = 1$ ，从而 $br = b\ell < c$，这与引理 2.4 矛盾。然后，由于 $r \equiv \ell$ 模 $(a-\ell)$，可推出 $r \leq \ell - (a-\ell)$。特别地，这意味着 $a - \ell \leq \ell$。事实上，如果 $\ell < a - \ell$，由于$r \equiv \ell$ 模 $(a-\ell)$且 $r < a-\ell$，那么我们将有 $r = \ell$，这与上述结论矛盾。

按照引理 2.7 的证明中的记号，注意从 $\mathbf{v}(x,y)$ 开始，递增的 $\mathbf{v}$ 值的个数要么是 $q$，要么是 $q-1$，即

$$\iota = \left\lceil \frac{\ell - x}{a-\ell} \right\rceil = \begin{cases} q & \text{if } x < r, \\ q-1 & \text{if } x \geq r. \end{cases}$$

此后，在达到局部极小值 $\mathbf{v}(x',y')$ 之前，递减的 $\mathbf{v}$ 值的个数为

$$\left\lfloor \frac{\ell + \rho_x}{\ell} \right\rfloor,$$

其中 $\rho_x \equiv x - \ell$ 对 $(a-\ell)$ 取模。回忆

$$\ell - x = \left\lceil \frac{\ell - x}{a-\ell} \right\rceil (a-\ell) - \rho_x$$

因此

$$\ell + \rho_x = \begin{cases} q(a-\ell) + x & \text{if } x < r, \\ (q-1)(a-\ell) + x & \text{if } x \geq r. \end{cases}$$

还要注意

$$(q-1)(a-\ell) \leq \ell < q(a-\ell) \leq 2\ell;$$

事实上，若 $q(a-\ell) \leq \ell$，则 $(q+1)(a-\ell) \leq a$，这与 $q$ 的定义矛盾。因此，对于情形 $x \geq r$，显然有

$$\left\lfloor \frac{(q-1)(a-\ell) + x}{\ell} \right\rfloor = 1$$

因为 $x < a - \ell$ 根据引理 2.7。对于 $x < r$ 的情形，我们断言 $q(a-\ell) + r \leq 2\ell$。事实上，若$a = q(a-\ell) + r > 2\ell$，则 $a - \ell > \ell$，这与我们上面已证明的结论矛盾。因此，

$$\begin{aligned} \mathbf{v}(x',y') - \mathbf{v}(x,y) &= \begin{cases} bq(a-\ell) - b\ell + c(q+1) & \text{if } x < r, \\ b(q-1)(a-\ell) - b\ell + cq & \text{if } x \geq r, \end{cases} \\ &= \begin{cases} b(a-r) - b\ell + c(q+1) & \text{if } x < r, \\ b(a-r-a+\ell) - b\ell + cq & \text{if } x \geq r, \end{cases} \\ &= \begin{cases} b(a-\ell) + c - br + cq & \text{if } x < r, \\ -br + cq & \text{if } x \geq r, \end{cases} \\ &> 0, \end{aligned}$$

如所要求。 □

**备注3.2**。 如上面的证明所示，由于所考察的连续**v**值中只有一个下降步，因此在这种情况下 [9, Lem. 5] 成立 $br < cq$。因此， [9, Lem. 5]仅在 $br > cq$ 的情况下不一致。事实上， [9, Lem. 5] 的原始表述如下：对于 $\mathbf{v}(x,y)$ 和 $\mathbf{v}(x',y')$ 连续局部极小值，且 $0 \le x, x' < a - \ell$（并满足 $y < y'$），

$$\mathbf{v}(x',y') - \mathbf{v}(x,y) = \begin{cases} \mathbf{v}(a-\ell-r, q+1) & \text{if } 0 \le x < r, \\ \mathbf{v}(-r, q) & \text{if } r \le x < a-\ell. \end{cases}$$

如在 [7, 例 5.13], 中所述，取 $a = 11$、 $b = 15$ 和 $c = 16$时，我们有 $q = 1$和 $\ell = r = 4$。因此， [9, 引理 5] 中的陈述表明，$\mathbf{v}(1,0) = 15$之后的下一个局部极小值应为$\mathbf{v}(4,2) = 92$；然而，$\mathbf{v}(4,2)$之后的**v**值，也就是$\mathbf{v}(0,3) = 48$，才是真正的局部极小值。如前所述，我们在此确认 $br = 60 > cq = 16$。

与 [9, 引理 7], 的情形一样， [9, 定理 3] 中的陈述仍然成立。证明与 [9],中的相同，只需将对 [9, 引理 5] 的引用替换为引理 3.1。为方便起见，我们在此给出完整证明，并补充了一些说明，使论述更加清晰。

**定理3.3**。 [9, 定理。 3] 若 $\ell > k$ 且 $br < cq$，则记作 $\lambda := \left\lfloor \frac{cq-br}{b\,a-\ell\,()+c} \right\rfloor$，

$$g(a,b,c) + a = \begin{cases} b\big((\lambda+1)(a-\ell)+r-1\big) & \text{if } \lambda \ge \frac{c(q-1)-br}{b(a-\ell)+c}; \\ b(a-\ell-1) + c(q-\lambda-1) & \text{if } \lambda \le \frac{c(q-1)-br}{b(a-\ell)+c}. \end{cases}$$

证明。 由引理 3.1 可知，$\mathbf{m}(bx) = bx$ 对 $x \in \{1, \dots, a-1\}$成立。然后由引理 2.11，并采用其中的记号，可得 $\mathbf{m}(bx) = \min\{bx, bx' + cy'\}$ 对 $x \in \{1, \dots, a-1\}$成立。

我们固定某个 $x \in \{1, \dots, a-1\}$，并记 $m := \lfloor \frac{x}{a-\ell} \rfloor$ 和 $s := x$ 模 $(a-\ell)$。根据 $s \ge r$ 或 $s < r$，分别令 $\epsilon$ 为 0 或 1。由引理 2.11 可推出$\mathbf{m}(bx) = bx$ 当且仅当

$$\begin{aligned} & b\big(m(a-\ell)+s\big) = bx \le bx' + cy' = b\big(s - r + \epsilon(a-\ell)\big) + c\big(q - (m-\epsilon)\big) \\ \iff \quad & b\big((m-\epsilon)(a-\ell)+r\big) \le c\big(q-(m-\epsilon)\big) \\ \iff \quad & (m-\epsilon)\big(b(a-\ell)+c\big) \le cq - br \\ \iff \quad & m \le \lambda + \epsilon. \end{aligned} \tag{3.1}$$

因此，对于固定的 $s \in \{0, 1, \dots, a-\ell-1\}$，我们断言

$$\max_m \mathbf{m}(bx) = \max\left\{ b\big((\lambda+\epsilon)(a-\ell)+s\big),\, b\big(\epsilon(a-\ell)+s-r\big) + c(q-\lambda-1) \right\}.$$

事实上，对于 $m \in \{0, 1, \dots, \lambda+\epsilon\}$，上述等价关系表明 $\mathbf{m}(bx) = bx$，而这些值的最大值出现在 $m = \lambda + \epsilon$ 时。对于 $m \ge \lambda + \epsilon + 1$，我们有 $\mathbf{m}(bx) = bx' + cy'$。由于 $x'$ 不依赖于 $m$，并且由于 $y' = q - (m-\epsilon)$，我们看到随着 $m$ 增大，相应的值 $bx' + cy'$ 减小。因此，这些值的最大值出现在 $m - \epsilon = \lambda + 1$ 时。

现在注意到上述两项之差，

$$\begin{aligned} & \big[b\big(\epsilon(a-\ell)+s-r\big) + c(q-\lambda-1)\big] - b\big((\lambda+\epsilon)(a-\ell)+s\big) \\ & \qquad = c(q-1) - br - \lambda\big(b(a-\ell)+c\big), \end{aligned} \tag{3.2}$$

与 $s$和 $\epsilon$无关。还要注意，

$$b\big(\lambda(a-\ell)+a-\ell-1\big) \le b\big((\lambda+1)(a-\ell)+r-1\big).$$

因此，我们断言，若 (3.2) 中的差值非正，即若 $\lambda \ge \frac{c}{b\ a-\ell\ +c}\!\!\!

若 (3.2) 中的差值非负，即若 $\lambda \le \frac{c}{b}\,{}_{a-\ell+c}(q-1-br)()$，则

$$\max_{s}\left\{\max_{m}\mathbf{m}(bx)\right\} = b(a-\ell-1)+c(q-\lambda-1);$$

事实上，$b\big(a-\ell+s-r\big)$ 在 $s<r$ 中的最大值出现在 $s=r-1$时，而 $b\big(s-r\big)$ 在 $s\ge r\ge 0$ 中的最大值出现在 $s-r=a-\ell-1$时。

最后，注意到 $b\big((\lambda+1)(a-\ell)+r-1\big) = b(a-\ell-1)+c(q-\lambda-1)$ 当且仅当$\lambda\big(b(a-\ell)+c\big) = c(q-1)-br$，因此定理中对 $\lambda$ 的限制是有依据的。□

如前所述 在引言中，[9] 的定理 4 可以通过类似的调整来证明 .

## 4. The case $br > cq$

接下来我们来看 [9] 的引理 9。证明与 [9], 中的相同，只是我们需要稍微改写对 [9, Lem. 5] 的引用。为方便起见，和之前一样，我们在此给出完整证明，并对某些断言提供更多论证。还要注意，考虑连续的 $\mathbf{v}$ 值，等价于从坐标 $(x,y)$ 变为 $(x+a-\ell,y+1)$。这种坐标变化称为大小为 1 的 步 。

为简洁起见，我们还将记作

$$u := (a-\ell) \bmod r.$$

特别要注意，$r>0$，因为 $br>cq$。

**引理 4.1.** [9, Lem. 9] 若 $\ell > k$ 且 $br > cq$，则

$$\max_{0\le x<a}\mathbf{m}(bx) = \max\left\{\max_{0\le x<u}\mathbf{m}(bx)+cq,\ \max_{u\le x<r}\mathbf{m}(bx)\right\}+cq\left\lfloor\frac{a-\ell-1}{r}\right\rfloor.$$

证明. 对于 $1\le x<a$，为简洁起见，我们再次记 $m := \lfloor \frac{x}{a-\ell}\rfloor$ 以及 $s := x$，模 $(a-\ell)$。注意，当我们令 $m$ 和 $s$ 在表达式 $m(a-\ell)+s$ 中变化时，集合 $\{1,\dots,a-1\}$ 中的每个元素都会被覆盖。

由于 $br>cq$，参照定理3.3中的记号，我们有 $\lambda<0$。因此，若 $m\ge 1$，则必然有 $m>\lambda+1$。故参照 (3.1) 与引理 2.11，我们有 $\mathbf{m}(bx) = \mathbf{m}(bx')+cy'$；此处 $x',y'$ 如引理 2.11 中所述。

因此我们首先考虑

$$\begin{aligned}
&\max_{m\ge1}\left\{\max_{r\le s<a-\ell}\mathbf{m}\big(b(s-r)\big)+c(q-m),\ \max_{0\le s<r}\mathbf{m}\big(b(s+a-\ell-r)\big)+c(q-m+1)\right\}\\
&\quad=\max_{m\ge1}\left\{\max_{0\le s<a-\ell-r}\mathbf{m}(bs)+c(q-m),\ \max_{a-\ell-r\le s<a-\ell}\mathbf{m}(bs)+c(q-m+1)\right\} \qquad (4.1)\\
&\quad=\max\left\{\max_{0\le x<a-\ell-r}\mathbf{m}(bx)+c(q-1),\ \max_{a-\ell-r\le x<a-\ell}\mathbf{m}(bx)+cq\right\}.
\end{aligned}$$

接下来，我们将上述结果与 $m=0$ 时 $\mathbf{m}(bx)$ 的最大值进行比较。这归结为将上述表达式与

$$\max_{0\le x<a-\ell}\mathbf{m}(bx).$$

因为由 (4.1) 的最后一行可得

$$\max\left\{\max_{0\le x<a-\ell}\mathbf{m}(bx),\ \max\left\{\max_{0\le x<a-\ell-r}\mathbf{m}(bx)+c(q-1),\ \max_{a-\ell-r\le x<a-\ell}\mathbf{m}(bx)+cq\right\}\right\}$$
$$=\max\left\{\max_{0\le x<a-\ell-r}\mathbf{m}(bx)+c(q-1),\ \max_{a-\ell-r\le x<a-\ell}\mathbf{m}(bx)+cq\right\},$$

因此，利用引理 2.11，我们还可得到

$$\max_{0\le x<a}\mathbf{m}(bx)=\max\left\{\max_{0\le x<a-\ell-r}\mathbf{m}(bx)+c(q-1),\ \max_{a-\ell-r\le x<a-\ell}\mathbf{m}(bx)+cq\right\}.$$

因此，由上面的推导可知，只需考虑 $0\le x<a-\ell$。如引理 3.1 的证明中所述，若 $x\ge r$，从 $\mathbf{v}(x,y)$ 开始，$\mathbf{v}$ 值首次下降发生在 $q$步之后，并导致坐标从 $(x,y)$ 变为 $(x-r,y+q)$。由于 $br>cq$，我们注意到 $\mathbf{v}(x-r,y+q)<\mathbf{v}(x,y)$。因此，对于每个 $x'\in\{0,1,\dots,r-1\}$，都存在一个数$x\in\{r,r+1,\dots,2r-1\}$，即 $x'+r$，使得 $bx=\mathbf{v}(x,0)>\mathbf{v}(x',q)=bx'+cq$。注意，$x'$在此对应于引理 2.11 中的 $x'$，而在那里 $y'=q$。因此，由引理 2.11 可推得 $\mathbf{m}(bx)=\mathbf{m}(bx')+cq>\mathbf{m}(bx')$。因此

$$\max_{0\le x<a}\mathbf{m}(bx)=\max\left\{\max_{r\le x<a-\ell-r}\mathbf{m}(bx)+c(q-1),\ \max_{a-\ell-r\le x<a-\ell}\mathbf{m}(bx)+cq\right\}.$$

对每个 $x'\in\{r,r+1,\dots,2r-1\}$ 等重复这一考察可知，为了求得上文所示的最大值，我们可以将范围限制为$a-\ell-r\le x<a-\ell$。

现在，若 $nr$是满足 $a-\ell-r\le nr<a-\ell$的 $r$的唯一倍数，则对于那些 $x<nr$，可以像上面那样进行 $n-1$步、每步大小为 $q$；而对于范围 $a-\ell-r\le x<a-\ell$内的 $x\ge nr$，可以进行 $n$步、每步大小为 $q$。因此，由上文可得，

$$\max_{0\le x<a}\mathbf{m}(bx)=\max_{a-\ell-r\le x<a-\ell}\mathbf{m}(bx)+cq$$
$$=\max\left\{\max_{0\le x<u}\mathbf{m}(bx)+cq,\ \max_{u\le x<r}\mathbf{m}(bx)\right\}+cq\left\lfloor\frac{a-\ell-1}{r}\right\rfloor,$$

如所需。 □

接下来，我们回顾 [9], 中的以下定义，它将在下文中发挥重要作用。

**定义 4.2**。 [9, 定义 3] 设 $\ell>k$ 和 $br>cq$。我们定义

$$\mathcal{X}:=\{x\in\{1,\dots,r\}\mid\mathbf{m}(bx)\equiv 0\bmod c\}.$$

我们回顾 [9],中的以下观察，并在此补上下面引理中第一个陈述的证明里一个小小的缺漏；另见注 4.4:

**引理 4.3.** [9, 注。 6] 假设 $\ell>k$ 且 $br>cq$。那么 $r\in\mathcal{X}$ 且

$$\min\mathcal{X}=\min\{x\in\{1,\dots,r\}\mid\mathbf{m}(bx)\ne bx\}.$$

证明。 我们断言 $\mathbf{m}(br)=cq$，由此即可得到第一个陈述。由于 $a=q(a-\ell)+r$，我们得到从$\mathbf{v}(r,0)$开始的前$\mathbf{v}$个连续值之间的以下不等式:

$$\mathbf{v}(r,0)<\mathbf{v}(a-\ell+r,1)<\cdots<\mathbf{v}((q-1)(a-\ell)+r,q-1)>\mathbf{v}(0,q)$$

因此，$\mathbf{v}(r,0)$ 和 $\mathbf{v}(0,q)$ 是连续局部极小值。由于 $br>cq$，我们得到

$$\min\{\mathbf{v}(r,0),\mathbf{v}(0,q)\}=\mathbf{v}(0,q).$$

现在注意，任何满足 $y' > q$ 的局部极小值 $\mathbf{v}(x, y)$，即出现在 $\mathbf{v}(0, q)$ 之后的局部极小值，都将满足 $\mathbf{v}(x, y) > \mathbf{v}(0, q)$。因此断言得证。

对于最后一个结论，写作 $\widehat{x} := \min \mathcal{X}$ 和 $x = \min\{x \in \{1, \ldots, r\} \mid \mathbf{m}(bx) \neq bx\}$。注意，$\mathbf{m}(bx) = bx_0 + cy_0$，其中某个 $x_0 \geq 0$ 和 $y_0 \geq 1$。因此

$$bx_0 < bx_0 + cy_0 < b\overline{x},$$

因此 $x_0 < x$。现在我们还有 $cy_0 \in [b(x - x_0)]$，且 $cy_0 < b(x - x_0)$，由此可得 $\mathbf{m}(b(x - x_0)) < b(x - x_0)$。若 $x_0 > 0$，则这与将 $x$ 选为集合 $\{x \in \{1, \ldots, r\} \mid \mathbf{m}(bx) \neq bx\}$ 中最小元素的做法矛盾。因此必有 $x_0 = 0$。于是 $\mathbf{m}(bx) = cy_0$，从而 $x \in \mathcal{X}$。由于 $\mathcal{X} \subseteq \{x \in \{1, \ldots, r\} \mid \mathbf{m}(bx) \neq bx\}$，可知 $x = \widehat{x}$，正如所需。□

**注 4.4.** 在 [9, Rmk. 6] 中曾声称，类 $[br]$ 中的局部极小值只有 $\mathbf{v}(r, 0)$ 和 $\mathbf{v}(0, q)$。如上文证明的第一部分所示，在 $\mathbf{v}(0, q)$ 之后，类 $[br]$ 中还可能存在局部极小值，而且不难找到这样的例子。[9] 中很可能想表达的是，在 $br$ 和 $cq$ 之间没有其他局部极小值，因为从 $\mathbf{v}(r, 0)$ 到 $\mathbf{v}(0, q)$ 只需一步 $\downarrow$。

接下来，我们回顾 [9, Def. 4] 中的一些记号；不过，我们对其中一个定义作了修改（参见下文注 4.6）：

**记号 4.5.** 设 $A := br - cq$, $B := b(a - \ell - r) + c(q + 1)$，并且

$$\Lambda := \left\lfloor \frac{r}{a - \ell - r} \right\rfloor, \qquad \Delta := \left\lfloor \frac{A}{B} \right\rfloor, \qquad \Lambda' := \left\lfloor \frac{a - \ell - r}{r} \right\rfloor, \qquad \Delta' := \left\lfloor \frac{B}{A} \right\rfloor.$$

另设

$$\mu := \min \left\{ i \in \mathbb{Z}_{\geq 0} \,\middle|\, \left\lfloor \frac{(i+1)B}{A} \right\rfloor \neq \left\lfloor \frac{(i+1)(a - \ell - r)}{r} \right\rfloor \right\},$$

并回忆一下，$u \equiv (a - m)^{-1} \bmod r$。

**Rem备注 4.6**。在 [9, 引理 11],中，量 $\mu$ 在 [9], 中记作 $\mu'$，其定义却是 as

$$\mu := \max \left\{ i \in \mathbb{Z}_{\geq 0} \,\middle|\, \left\lfloor \frac{iB}{A} \right\rfloor = \left\lfloor \frac{i(a - \ell - r)}{r} \right\rfloor \right\}.$$

我们猜想，我们对 $\mu$ 的定义才是 Tripathi 原本的意思，因为 $\mu$ 在 [9, 例子 5], 中被指出等于 4，而该例子采用的是我们的定义；相比之下，Tripathi 的定义应给出 $\mu \geq 9$。将例子中的数值代入 $i = 9$，并注意到以下事实，即可看出这一点:

$$\left\lfloor \frac{9 \cdot 2500}{3800} \right\rfloor = 5 = \left\lfloor \frac{9 \cdot 22}{39} \right\rfloor.$$

为了给出一个更 详尽的例子来说明这两种定义之间的差异，参见 [7, 例 5。18] .

在继续之前，我们先记录一个有用的观察结果。

**引理 4.7**。假设 $\ell > k$ 且 $br > cq$。那么，参照记号 *4.5*，我们有 $A \neq B$。

证明。反设 $A = B$，因此 $br - cq = b(a - \ell - r) + c(q + 1)$。重新整理可得

$$b(2r - a + \ell) = c(2q + 1).$$

由于 $\gcd(b, c) = 1$，特别地，$b$ 整除 $2q+1$。因此 $a \leq 2q$。由 $a = q(a-\ell)+r$可知，$a - \ell < 2$。也就是说，我们有 $a - \ell = 1$。正如引理 2.11之前所述，这等价于情形 $r = 0$；当 $br > cq$时不可能出现这种情形。□

[9, 引理 11] 的相应结论仍然成立，只需根据 $\mu$的新定义对证明作 minor 调整；此外，这是因为引用 [9, 引理 5] 仅用于确定在两个特定形式的局部极小值 $\mathbf{v}(x,0)$ 和 $\mathbf{v}(0,y)$之间需要经过多少步，而不论还需要经过多少个其他（伪）局部极小值。由于这些局部极小值 $\mathbf{v}(x,0)$ 和 $\mathbf{v}(0,y)$始终是真正的局部极小值，因此 [9, 引理 11]的证明在这一方面不存在问题。事实上，这里使用 [9, 引理 5] 只涉及可能经过一些伪局部极小值。具体而言，要从一个伪局部极小值到达下一个真正的局部极小值，就必须实施更多的 $\downarrow$步；按照 [9]的记号（见 [9, 引理 5]之后的注释），$\downarrow$步是坐标中 $\mathbf{v}$ 值从 $(x,y)\mapsto(x-r,y+q)$ 的变化，这会使 $\mathbf{v}$ 值减少 $A$（参见记号 4.5）。类似地，$\uparrow$步是从 $(x,y)\mapsto(x+a-\ell-r,y+q+1)$ 的变化，这会使 $\mathbf{v}$ 值增加 $B$。特别地，我们注意到以下事实，它进一步说明了伪局部极小值何时出现（另见注 4.9）：

**引理 4.8**。 设 $\ell>k$ 和 $br>cq$，并令 $\mathbf{v}(x,y)$ 和 $\mathbf{v}(x',y')$ 为连续局部极小值。则要么

$$y'-y=\begin{cases}q+1 & \text{if } 0\le x<r,\\ q & \text{if } r\le x<a-\ell,\end{cases}\quad \text{and then}\quad x'-x=\begin{cases}a-\ell-r & \text{if } 0\le x<r,\\ -r & \text{if } r\le x<a-\ell,\end{cases}$$

*or*

$$y'-y>\begin{cases}q+1 & \text{if } 0\le x<r,\\ q & \text{if } r\le x<a-\ell,\end{cases}$$

并且在这种情况下 $q=1$ 和 $r=\ell$。

证明。 如引理 2.7 的证明中所述，在从$\mathbf{v}(x,y)$开始经历若干次连续的$\mathbf{v}$值增加后，在达到下一个局部极小值$\mathbf{v}(x',y')$之前，递减的$\mathbf{v}$值的数量为

$$\left\lfloor\frac{\ell+\rho_x}{\ell}\right\rfloor,$$

其中 $\rho_x\equiv x-\ell$ 模 $(a-\ell)$，并且

$$\ell+\rho_x=\begin{cases}q(a-\ell)+x & \text{if } x<r,\\ (q-1)(a-\ell)+x & \text{if } x\ge r.\end{cases}$$

正如引理 3.1 的证明中所论证的，

$$(q-1)(a-\ell)\le\ell<q(a-\ell).$$

若 $q(a-\ell)+r\le 2\ell$，则要经过的连续下降的$\mathbf{v}$值的个数只有一个，才能到达局部极小值$\mathbf{v}(x',y')$。在这种情况下，如[9, 引理 5] 的证明中所述，我们得到第一个陈述。反之，设 $q(a-\ell)+r>2\ell$，等价地，$a-\ell>\ell$，因此，要经过至少两个连续下降的$\mathbf{v}$值才能到达局部极小值$\mathbf{v}(x',y')$。由于 $(q-1)(a-\ell)\le\ell$，由此可得 $q=1$，进而得到 $r=\ell$。□

**注 4.9**。 接续备注3.2，由上文可知，当 [9, 引理 5]不成立时，可得 $q=1$ 且 $r=\ell$。因此，当我们需要经过多个下降步才能到达下一个局部极小值时，每个下降步实际上都是一个 $\downarrow$-步。

**注4.10**。 事实上，上述注记的逆命题成立，即如果 $q=1$ 和 $r=\ell$，那么[9, 引理 5] 不成立。事实上，考虑 $x_0=\ell-1$。经过一次上升步得到 $x_1=a-1$，经过一次下降步得到 $x_2=a-\ell-1$。回想 $r=\ell<a-\ell$，我们可知至少还可以再进行一次下降步。

下面我们使用 $\mu$ 的新定义陈述 [9, 引理 11]，并给出修订后的证明，同时对原证明中的若干断言提供更多论证。为方便起见，我们先单独提出一个小结果，它将在证明 [9, 引理 11]时用到。

**引理 4.11.** 若 $br > cq$，则 $r$ 不能被 $a-\ell-r$整除。

证明。反设 $r \equiv 0 \bmod (a-\ell-r)$。这只有在以下两种情况下才可能发生：要么$r=0$，但根据假设这已被排除；要么 $r$ 是 $a-\ell-r$的某个正整数倍。因此假设后一种情况，并令 $r=\eta(a-\ell-r)$，其中 $\eta \in \mathbb{N}$. 由 $r$的定义可得

$$\begin{aligned} a &= r + q(a-\ell) \\ &= \eta(a-\ell-r) + q(a-\ell) \\ &= \eta(a-\ell-r) + q(a-\ell-r+r) \\ &= \eta(a-\ell-r) + q\big(a-\ell-r+\eta(a-\ell-r)\big) \\ &= (\eta+q+q\eta)(a-\ell-r). \end{aligned}$$

因此 $a$ 也是 $a-\ell-r$的倍数。类似地，

$$\begin{aligned} \ell &= a-r-(a-\ell-r) \\ &= (\eta+q+q\eta)(a-\ell-r) - \eta(a-\ell-r) - (a-\ell-r) \\ &= (q+q\eta-1)(a-\ell-r). \end{aligned}$$

这意味着 $\gcd(a,\ell)$ 可被 $a-\ell-r$整除，这与 $a,b,c$ 两两互素这一既定假设矛盾。事实上，回想一下，$\ell \equiv cb^{-1} \bmod a$，因此$b\ell = c+\kappa a$，其中某个整数为 $\kappa \neq 0$。再结合 $\gcd(a,\ell)$ 可被 $a-\ell-r$整除这一事实，可得 $c$可被 $a-\ell-r$整除，进而 $\gcd(a,c)$ 可被 $a-\ell-r$整除，矛盾。□

**引理 4. 12.** [9, 引理 11] 设 $\ell > k$ 且 $br > cq$。那么，参照记号 *4.5*，

$$\begin{aligned} \mathcal{X} &= \left\{ r\left( \left\lfloor \tfrac{(a-\ell-r)t}{r} \right\rfloor + 1 \right) - (a-\ell-r)t \mid 0 \le t \le \mu \right\} \\ &= \left\{ \big(r-(a-\ell-r)t\big) \bmod r \mid 0 \le t \le \mu \right\}. \end{aligned}$$

此外，若 $\mu < \lfloor \frac{r}{u} \rfloor$，则

$$\mathcal{X} = \{ r - ut \mid 0 \le t \le \mu \}.$$

特别地，若 $\Lambda > \Delta$ 或 $\Delta' > \Lambda'$，则

$$\mathcal{X} = \{ r - (a-\ell-r)t \mid 0 \le t \le \Delta \}.$$

证明。根据引理 4.8，我们注意到，从一个局部极小值转到下一个局部极小值时，有三种选择：要么在 $0 \le x \le r-1$ 时采取 $\uparrow$-步（$x$，$y$）$\mapsto$（$x+a-\ell-r$，$y+q+1$）；要么在 $r \le x < a-\ell$ 时采取 $\downarrow$-步（$x$，$y$）$\mapsto$（$x-r$，$y+q$）；或者，最多采取一次 $\uparrow$-步，随后采取若干次 $\downarrow$-步（回想一下，在这种最后的选择中，我们有 $q=1$ 且 $r=\ell$）。注意，$\uparrow$-步会使$\mathbf{v}$值增加 $B$，而 $\downarrow$-步会使$\mathbf{v}$值减少 $A$。

由引理 4.3，我们有 $r \in \mathcal{X}$。现在考虑 $x \in \mathcal{X}\backslash\{r\}$。我们观察到，此时$\mathbf{m}(bx) = cy$对某个 $y \in \mathbb{N}$。由于 $\mathbf{v}(x,0)$ 与 $\mathbf{v}(0,y)$ 均为同余类 $[bx]$ 中的局部极小值，我们可以从 $\mathbf{v}(x,0)$ 出发，经由由 $t_1$ $\downarrow$-步与 $t_2$$\uparrow$-步组成的数列，对某个 $t_1,t_2 \in \mathbb{N}$，到达 $\mathbf{v}(0,y)$。事实上，由于 $0<x<r$，$t_1$ 与 $t_2$ 都必须为正。因此

$$x = rt_1 - (a-\ell-r)t_2 \qquad \text{and} \qquad y = qt_1 + (q+1)t_2,$$

从而不等式 $0 < x < r$ 给出

$$\frac{r}{a-\ell-r}(t_1-1) < t_2 < \frac{r}{a-\ell-r}t_1. \tag{4.2}$$

设 $x = rt_1 - (a-\ell-r)t_2$，其中 $t_1,\ t_2 \in \mathbb{N}$ 满足 (4.2)。我们进一步断言，$x \in \mathfrak{X}\backslash\{r\}$ 当且仅当 $t_2 \le \mu$。首先注意，对于这样的 $x$，不等式

$$\mathbf{v}(x,0) = bx > cy = \mathbf{v}(0,y),$$

其中 $y = qt_1 + (q+1)t_2$ 如上所述，重新整理后得到 $At_1 > Bt_2$。

现在证明该断言。我们先假设 $1 \le t_2 \le \mu$。考虑类 $[bx]$ 中任意一个局部极小值$\mathbf{v}(x',\ y')$，使得 $(x',\ y') \neq (0,\ y)$，其中 $x' \ge 0$ 且 $0 \le y' < y$。假设我们经过 $s_1 \downarrow$ 步和 $s_2 \uparrow$ 步，从 $\mathbf{v}(x',\ y')$ 到达$\mathbf{v}(0,\ y)$。那么，我们得到 $x' = rs_1 - (a-\ell-r)s_2 > 0$，因此

$$s_1 > \frac{(a-\ell-r)s_2}{r}.$$

根据 $\mu$ 的定义以及 $s_2 \le t_2 \le \mu$ 这一事实，我们有

$$\left\lfloor \frac{(a-\ell-r)s_2}{r} \right\rfloor = \left\lfloor \frac{Bs_2}{A} \right\rfloor$$

因此，由于

$$\frac{(a-\ell-r)s_2}{r} < \frac{Bs_2}{A},$$

可得 $\frac{Bs_2}{A} \notin \mathbb{Z}$，并且

$$s_1 \ge \left\lceil \frac{Bs_2}{A} \right\rceil > \frac{Bs_2}{A}.$$

现在我们得到

$$\mathbf{v}(x',y') - \mathbf{v}(0,y) = As_1 - Bs_2 = A\left(s_1 - \frac{Bs_2}{A}\right) > 0.$$

因此，当 $t_2 \le \mu$ 且 $0 < x < r$ 具有上述形式时，$\mathbf{m}(bx) = cy$，从而 $x \in \mathfrak{X}$。事实上，请回想，任何满足 $y' > y$ 的局部极小值 $\mathbf{v}(x',y')$，也就是出现在 $\mathbf{v}(0,y)$ 之后的局部极小值，总满足 $\mathbf{v}(x',y') > \mathbf{v}(0,y)$。

接下来，为证明逆向结论，假设 $t_2 > \mu$。由 (4.2) 可知

$$t_1 - 1 < \frac{(a-\ell-r)t_2}{r} < t_1,$$

因此特别地$\frac{(a-\ell-r)t_2}{r} \notin \mathbb{Z}$。然后，由 $\mu$的定义，我们有

$$\begin{aligned}
t_1 &< 1 + \frac{(a-\ell-r)t_2}{r} \\
&= 1 + \frac{(a-\ell-r)(\mu+1)}{r} + \frac{(a-\ell-r)(t_2-\mu-1)}{r} \\
&\le 1 + \left\lfloor \frac{(a-\ell-r)(\mu+1)}{r} \right\rfloor + \frac{(a-\ell-r)(t_2-\mu-1)}{r} \\
&= \left\lfloor \frac{B(\mu+1)}{A} \right\rfloor + \frac{(a-\ell-r)(t_2-\mu-1)}{r} \\
&< \frac{B(\mu+1)}{A} + \frac{B(t_2-\mu-1)}{A}
\end{aligned}$$

因此我们看到

$$t_1 < \frac{Bt_2}{A}.$$

因此，正如上文所见，不等式 $At_1 < Bt_2$ 等价于$\mathbf{v}(x,\ 0) < \mathbf{v}(0,\ y)$。由此 $x \notin \mathcal{X}$，证毕。断言现已得到证明。

最后，为完成第一个陈述的证明，注意到

$$x = rt_1 - (a-\ell-r)t_2 = r - (a-\ell-r)t_2 + r(t_1-1).$$

由于 $\mathcal{X} \subseteq \{1,\dots,r\}$，我们有 $x = \big(r-(a-\ell-r)t_2\big)$ 模 $r$，对所有 $x \in \mathcal{X}$ 均成立。利用方程，第一个陈述中的方程现可得出

$$(a-\ell-r)t_2 = r\left\lfloor \frac{(a-\ell-r)t_2}{r} \right\rfloor + \big((a-\ell-r)t_2\big) \bmod r.$$

接下来，若 $\mu < \lfloor \frac{r}{u} \rfloor$，则对于 $0 \le t \le \mu$ 有 $0 \le ut < r$。由于 $(a-\ell-r)t \equiv ut$ 模 $r$，可知在这种情况下$\mathcal{X} = \{r - ut \mid 0 \le t \le \mu\}$。

对于最后一个陈述，假设 $\Lambda > \Delta$ 或 $\Delta' > \Lambda'$，只需证明以下两个断言：

(i) $\mu = \Delta$;

以及 (ii) $\mu < \lfloor \frac{r}{u} \rfloor$。

对于 (i)，我们首先注意到 $\lfloor \frac{\Delta B}{A} \rfloor = 0$。事实上，否则我们将有 $\lfloor \frac{\Delta B}{A} \rfloor = 1$，特别是 $\eta := \frac{A}{B} \ge 2$ 是一个正整数；另请参见引理 4.7。因此$\Delta' = 0$，且不可能有 $\Delta' > \Lambda'$。于是，根据假设 $\Lambda > \Delta = \eta$，由此得到$\Lambda = \lfloor \frac{r}{a-\ell-r} \rfloor \ge \eta + 1$。因此 $r \ge (\eta+1)(a-\ell-r)$。回到 $\eta := \frac{A}{B}$，我们得到

$$br - cq = \eta[b(a-\ell-r) + c(q+1)],$$

等价地，

$$b[\eta(a-\ell-r) - r] + c[\eta(q+1) + q] = 0.$$

因此 $c$ 整除 $r - \eta(a-\ell-r)$。另一方面，由于

$$r \ge (\eta+1)(a-\ell-r) > \eta(a-\ell-r) > 0,$$

我们有

$$0 < r - \eta(a-\ell-r) < r < a-\ell < c.$$

这给出 这就得到了所需的矛盾： $c$ 整除 $r - \eta(a-\ell-r)$。因此 $\lfloor \frac{\Delta B}{A} \rfloor = 0$ 并且

$$\lfloor \tfrac{iB}{A} \rfloor = 0 = \lfloor \tfrac{i(a-\ell-r)}{r} \rfloor$$

for $0 \le i \le \Delta$，因为 $\frac{B}{A} > \frac{a-\ell-r}{r} > 0$。所以，为了证明 $\mu = \Delta$，我们需要证明

$$\left\lfloor \frac{(\Delta+1)B}{A} \right\rfloor \ne \left\lfloor \frac{(\Delta+1)(a-\ell-r)}{r} \right\rfloor.$$

我们首先注意到 $\lfloor \frac{(\Delta+1)B}{A} \rfloor \ge 1$。接着先假设 $\Delta' > \Lambda'$。根据定义，这里有 $\mu = 0$，并且由于 $\Delta' > \Lambda'$ 意味着 $\Delta' > 0$，结合引理 4.7，我们得到在这种情况下的 $\Delta = 0 = \mu$。

接下来，如果 $\Lambda > \Delta$，那么

$$\left\lfloor \frac{(\Delta+1)(a-\ell-r)}{r} \right\rfloor \le \left\lfloor \frac{\Lambda(a-\ell-r)}{r} \right\rfloor.$$

我们同样断言 $\left\lfloor \frac{\Lambda(a-\ell-r)}{r} \right\rfloor = 0$。事实上，由于 $\Lambda = \left\lfloor \frac{r}{a-\ell-r} \right\rfloor$，我们有

$$\begin{aligned}\left\lfloor \frac{\Lambda(a-\ell-r)}{r} \right\rfloor &= \left\lfloor \frac{\left\lfloor \frac{r}{a-\ell-r} \right\rfloor (a-\ell-r)}{r} \right\rfloor \\ &= \left\lfloor \frac{r - \big(r \bmod (a-\ell-r)\big)}{r} \right\rfloor \\ &= 1 - \left\lceil \frac{r \bmod (a-\ell-r)}{r} \right\rceil,\end{aligned}$$

但根据引理 4.11，最后一个表达式小于 1，因为 $r \not\equiv 0 \bmod (a-\ell-r)$。因此 $\left\lfloor \frac{\Lambda(a-\ell-r)}{r} \right\rfloor = 0$，这正是所需的结果，所以在第二种情况下，$\mu = \Delta$ 也成立。

最后，我们证明 (ii)，从而完成证明。对于 $\Lambda > \Delta$ 的情况，注意到 $\Lambda' = 0$，因为 $\Lambda > 0$，且 $r \not\equiv 0 \bmod (a-\ell-r)$。因此 $u = a-\ell-r-\Lambda' r = a-\ell-r$ 且 $\mu = \Delta < \Lambda = \left\lfloor \frac{r}{a-\ell-r} \right\rfloor = \left\lfloor \frac{r}{u} \right\rfloor$。对于 $\Delta' > \Lambda'$ 的情况，我们回想起 $\mu = \Delta = 0$。此外，我们有

$$u = a-\ell-r-\Lambda' r < r \tag{4.3}$$

因为 $\frac{a-\ell-r}{r} < \Lambda' + 1$。我们得到 $\left\lfloor \frac{r}{u} \right\rfloor > 0$；因为如果 $\left\lfloor \frac{r}{u} \right\rfloor = 0$，那么

$$\left\lfloor \frac{r}{a-\ell-(1+\Lambda')r} \right\rfloor = 0$$

这给出 $(1+\Lambda')r < a-\ell-r$，根据 (4.3)，这是不可能的。因此 $\mu = \Delta = 0 < \left\lfloor \frac{r}{u} \right\rfloor$，如所需。□

在上述 $\Delta' > \Lambda'$ 情形中，由证明可知 $\mu = \Delta = 0$，因此这里有 $\mathcal{X} = \{r\}$。

接下来我们回顾一下 [9] 中的一些有用的备注。

**引理 4.13**。 [9, 注。 8] 假设 $\ell > k$ 且 $br > cq$。参见记号 *4.5*，设 $\mu > \left\lfloor \frac{r}{u} \right\rfloor$。那么 $\Lambda' = \Delta' = 0$、$u = a-\ell-r$ 和 $\left\lfloor \frac{r}{u} \right\rfloor = \Lambda = \Delta$。

最后，我们给出 [9, 定理 5], 的修正版，其中只需修改 (b) 的陈述。为求完整起见，我们也给出 (a) 部分的证明；尽管 $\mu$ 的定义有所改变，该部分仍然成立。事实证明，只要替换一个错误的数值，[9, 定理 5(b)] 的证明便仍然有效；参见注 4.15。和其他情况一样，为使论证更清楚，我们在 (a) 和 (b) 两部分的证明中都补充了一些说明。此外，我们先证明一个辅助结果，它将是 (b) 部分修正后证明的关键。

**引理 4.14.** 设 $\ell > k$ 和 $br > cq$。参照记号 *4.5*、引理 *4.12* 和引理 *4.13*，记

$$\mathcal{X} = \{x_i := r\left(\left\lfloor \tfrac{ui}{r} \right\rfloor + 1\right) - ui \mid 0 \le i \le \mu\}$$

并假设 $\mu > \left\lfloor \frac{r}{u} \right\rfloor$。那么 $x_\mu$ 是 $\mathcal{X}$ 中大于 $u$ 的最小元素。此外，将 $\mathcal{X}$ 中的元素按递增顺序排列后，$\mathcal{X}$ 中任意两个相邻元素之差为 $\widehat{x} :=$ 最小值 $\mathcal{X}$ 或 $\widehat{x} + u - x_\mu$。

证明。 我们首先证明 $x_\mu > u$。为此，回顾一下

$$x_\mu = r\left(\left\lfloor \frac{\mu u}{r} \right\rfloor + 1\right) - \mu u = r\left(\left\lfloor \frac{\mu B}{A} \right\rfloor + 1\right) - \mu u.$$

还要回顾 $\frac{u}{r} < \frac{B}{A}$，因此根据 $\mu$ 的定义，我们有

$$\mu u = \left\lfloor \frac{\mu u}{r} \right\rfloor r + \delta$$
$$\mu B = \left\lfloor \frac{\mu u}{r} \right\rfloor A + \varepsilon$$

对于某些 $0 \le \delta < r$ 和 $0 \le \varepsilon < A$，并且

$$(\mu+1)u = \left\lfloor \frac{\mu u}{r} \right\rfloor r + (\delta + u)$$
$$(\mu+1)B = \left\lfloor \frac{\mu u}{r} \right\rfloor A + \varepsilon + B = \left(\left\lfloor \frac{\mu u}{r} \right\rfloor + 1\right) A + (\varepsilon + B - A)$$

其中 $\delta + u < r$ 和 $0 \le \varepsilon + B - A < A$。因此，由于 $u = \left\lfloor \frac{\mu u}{r} \right\rfloor r - \mu u + (\delta + u)$ 且 $\delta + u < r$，我们得到

$$x_\mu = \left\lfloor \frac{\mu u}{r} \right\rfloor r - \mu u + r > u.$$

还需证明 $x_\mu$ 是 $\mathcal{X}$中大于 $u$的最小元素。回想一下，表达式 $r - ui$ 关于 $i$是线性的，因此 $(r - ui) \bmod r$ 满足相应的周期线性。于是，如果我们将 $\mathcal{X}$中元素的分布以图形方式表示为 $\mathbb{R}^2$中的点（$i$, $x_i$），其中 $i \in \{0, 1, \ldots, \mu\}$，就会发现分布模式在图的纵轴方向上的区间 $[0, u]$, $[u, 2u]$, $\ldots$, $[(\lfloor \frac{r}{u} \rfloor - 1)u, \lfloor \frac{r}{u} \rfloor u]$ 内呈周期性，最后一个区间 $[\lfloor \frac{r}{u} \rfloor u, r]$ 内也相应如此。实际上，对于每个满足 $x_j < u$的 $x_j \in \mathcal{X}$，都有 $u < x_{j-1} = x_j + u < 2u$, $2u < x_{j-2} = x_j + 2u < 3u$，依此类推。

若 $m \in \{0, 1, \ldots, \mu - 1\}$ 满足 $x_m = \widehat{x} = \min \mathcal{X}$，则这种线性关系立即表明，$\mathcal{X}$中连续递增元素之间只有两种距离：$x_m$ 与其在 $\mathcal{X}$元素有序列表中的下一项之间的常数距离 $d_1$，以及有限等差数列 $x_m$、$x_m + d_1$、$\ldots$ 的最后一项与 $\mathcal{X}$ 中紧随其后的项之间的距离 $d_2$。从图形上看，可以将 $\mathcal{X}$ 中元素的分布视为位于若干有限长斜线上的点，这些斜线具有相同的负斜率或正斜率；第一条斜线分别终止于 $x_m$ 或始于 $x_m$，而下一条这样的斜线的最低点（在 $\mathcal{X}$ 中）与前一条斜线的最高点（在 $\mathcal{X}$ 中）相距 $d_2$。图 1 和图 2 给出了一些示例。

考虑有限等差数列 $x_m$、$x_m + d_1$、$\ldots$。如果经过该数列的斜线斜率为负，那么根据前述区间 $[0, u]$、$[u, 2u]$ 等内部的周期性，我们可推知 $x_\mu$ 是在竖直区间 $[u, 2u]$ 内经过最低斜线的最后一个点（在 $\mathcal{X}$ 中）。特别是，如上所述，对于每个满足 $u < x_j < 2u$ 的 $x_\mu \ne x_j \in \mathcal{X}$，都有 $0 < x_{j+1} = x_j - u < u$。因此，所有位于终止于 $x_\mu$ 的斜线正下方那条斜线上的 $\mathcal{X}$ 中的元素都严格小于 $u$；这些元素也与经过 $x_m$ 的最低斜线上的 $\mathcal{X}$ 中的元素一一对应。反之，如果经过有限等差数列 $x_m$、$x_m + d_1$、$\ldots$ 的斜线斜率为正，那么 $x_\mu$ 就是 $\mathcal{X}$ 中经过最高斜线的最后一个点，该斜线始于区间 $[0, u]$。同样，位于终止于 $x_\mu$ 的斜线上的 $\mathcal{X}$ 中的所有元素，除 $x_\mu$ 本身外，都严格小于 $u$；这些元素也与经过 $x_m$ 的最低斜线上的 $\mathcal{X}$ 中的元素一一对应。因此可知，$x_\mu$ 是 $\mathcal{X}$ 中大于 $u$ 的最小元素。

对于最后一个陈述，将 0 和 $r$ 视为相同后，由斜率的周期性可知，这些距离中有一个是 0 与 $x_m = \widehat{x}$ 之间的距离；根据上文，另一个距离为 $x_{m-1} - x_\mu = \widehat{x} + u - x_\mu$，正如所需。□

**注 4.15**。从 [9, 定理 5(b)]的证明来看，似乎误以为 $m = \lfloor \frac{r}{u} \rfloor$（上方的图 1 和图 2 也表明事实并非如此），并且误以为 $x_\mu = x_{2\lfloor \frac{r}{u} \rfloor}$。

因此，在 [9, 定理 5(b) 的证明], 中，这两个差值被表述为 $x_m$ 和 $\lceil \frac{r}{u} \rceil u - r$。关于 $\mathcal{X}$ 中连续递增元素之间距离的错误断言，是 [9,定理 5(b)]证明中唯一的疏漏。

**定理 4.16** （参见 [9,定理 5]）。使用上述记号，有如下结论：

(a) *If* $\mu < \lfloor \frac{r}{u} \rfloor$, *then*

$$g(a,b,c) + a = \max\Big\{b(r-\mu u-1), b(u-1) + c\big(\mu(q+1) + (\lfloor \tfrac{(a-\ell-r)\mu}{r} \rfloor + 1)q\big)\Big\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor.$$

*Furthermore, if* $\Lambda > \Delta$, *then*

$$g(a,b,c) + a = \max\big\{b(r-\Delta(a-\ell-r)-1), b(a-\ell-r-1) + c\big(\Delta(q+1)+q\big)\big\} + cq$$

*and if* $\Delta' > \Lambda'$, *then*

$$g(a,b,c) + a = \max\big\{b(r-1), b\big((a-\ell-1) \bmod r\big) + cq\big\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor.$$

(b) 若 $\mu > \lfloor \frac{r}{u} \rfloor$，回顾引理 *4.12* 可知 $\mathcal{X} = \{x_i \mid i \in \{0,1,\ldots,\mu\}\}$，其中 $e$

$$x_i = r\left(\left\lfloor \tfrac{(a-\ell-r)i}{r} \right\rfloor + 1\right) - (a-\ell-r)i,$$

并令

$$y_i = q\left(\left\lfloor \tfrac{(a-\ell-r)i}{r} \right\rfloor + 1\right) + (q+1)i$$

对于 $i \in \{0,1,\ldots,\mu\}$。设 $m \in \{0,1,\ldots,\mu\}$ 满足 $x_m :=$ 最小值 $\mathcal{X}$，并令 $w \in \{0,1,\ldots,\mu\}$ 为满足 $x_w + x_m \in \mathcal{X}$ 的最大值。那么

$$g(a,b,c) + a = \max\{b(x_m-1) + cy_w,\, b(x_{m-1} - x_\mu - 1) + cy_\mu\} + cq\lfloor \tfrac{a-\ell-1}{r} \rfloor.$$

证明。 (a) 若 $\mu < \lfloor \frac{r}{u} \rfloor$，则由引理 4.12 可得 $\mathcal{X} = \{r - ui \mid i \in \{0,1,\ldots,\mu\}\}$。因此对于 $i \in \{0,1,\ldots,\mu\}$,

$$x_i = r - ui = r\left(\left\lfloor \tfrac{(a-\ell-r)i}{r} \right\rfloor + 1\right) - (a-\ell-r)i \in \mathcal{X}$$

以及 $\mathbf{m}(bx_i) = cy_i$，其中

$$y_i = (q+1)i + q\left(\left\lfloor \tfrac{(a-\ell-r)i}{r} \right\rfloor + 1\right)$$

因为我们需要进行 $i \uparrow$ 步和 $\left(\left\lfloor \frac{(a-\ell-r)i}{r} \right\rfloor + 1\right) \downarrow$ 步，才能从 $\mathbf{v}(x_i, 0)$ 到达 $\mathbf{v}(0, y_i)$。显然，注意到 $\max\{cy_i \mid i \in \{0,1,\ldots,\mu\}\} = cy_\mu$。

现在，若 $x < \widehat{x} := \min \mathcal{X} = x_\mu = r - \mu u$，则由定义 4.2 和引理 4.3 可得 $\mathbf{m}(bx) = bx$。接下来注意，任意满足 $\widehat{x} < x < r$ 的整数 $x \notin \mathcal{X}$，都可写成 $x_i + z_i$，其中 $1 \le i \le \mu$ 且 $0 < z_i < u$。从 $(x, 0)$ 出发，然后进行 $i \uparrow$ 步和 $(\lfloor \frac{(a-\ell-r)i}{r} \rfloor + 1) \downarrow$ 步（顺序与从 $\mathbf{v}(x_i,0)$ 到 $\mathbf{v}(0,y_i)$ 时相同），即可到达局部极小值 $\mathbf{v}(z_i, y_i)$。事实上，由于 $\mathbf{v}(x_i,0)$ 和 $\mathbf{v}(0,y_i)$ 都是局部极小值，将它们的第一个坐标平移 $z_i$ 并不会改变其局部极小值的性质。特别是，由于 $0 < z_i < u$ 且 $x_{i-1} = x_i + u$，我们观察到

$$\mathbf{v}\big((x_i + j(a-\ell)) \bmod a, j\big) < \mathbf{v}\big((x_i + z_i + j(a-\ell)) \bmod a, j\big) < \mathbf{v}\big((x_{i-1} + j(a-\ell)) \bmod a, j\big)$$

对所有 $0 \le j \le y_i$，除了当 $(x_{i-1} + j(a-\ell)) \bmod a < u$ 时。由 $x_{i-1}$ 的定义以及由 $\mathbf{v}$-值的定义，由于 $r \not\equiv 0 \bmod u$，我们看到 $(x_{i-1} + j(a-\ell)) \bmod a < u$ 只发生一次，即当 $(x_{i-1} + j(a-\ell)) \bmod a = 0$ 时。在这种情况下，$j = y_{i-1}$ 并且我们仍然有

$$\mathbf{v}\big((x_i + y_{i-1}(a-\ell)) \bmod a, y_{i-1}\big) < \mathbf{v}\big((x_i + z_i + y_{i-1}(a-\ell)) \bmod a, y_{i-1}\big).$$

因此，我们的断言成立。

现在注意到$\mathbf{v}(0, y_i)$是同余类 $[bx_i]$中的最小$\mathbf{v}$值。因此，按照上面的推理，将所有$\mathbf{v}$值平移 $bz_i$ 后可得，$\mathbf{v}(z_i, y_i)$是同余类 $[bx]$中最小的$\mathbf{m}(bx)$，其中 $x = x_i + z_i$。还要注意， $u \le \widehat{x} = r - \mu u$，因为$\mu + 1 \le \frac{r}{u}$。所以

$$\max_{0\le x<u} \mathbf{m}(bx) + cq = b(u-1) + cq,$$

并且 si 因此，根据上述讨论，我们有$\mathbf{m}(\widehat{x} + u - 1) = \mathbf{v}(u-1, y_\mu)$，由此可知，

$$\max\left\{\max_{0\le x<u} \mathbf{m}(bx) + cq,\ \max_{u\le x<r} \mathbf{m}(bx)\right\} = \max_{u\le x<r} \mathbf{m}(bx)$$
$$= \begin{cases} \mathbf{v}(u-1, y_\mu) & \text{if } u = \widehat{x}, \\ \max\{\mathbf{v}(\widehat{x}-1, 0),\ \mathbf{v}(u-1, y_\mu)\} & \text{if } u < \widehat{x}. \end{cases}$$

因此，根据引理 4.1以及引理 2.5，由上述考量可得

$$\begin{aligned} g(a,b,c) + a &= \max\left\{\max_{0\le x<u} \mathbf{m}(bx) + cq,\ \max_{u\le x<r} \mathbf{m}(bx)\right\} + cq\left\lfloor \tfrac{a-\ell-1}{r}\right\rfloor \\ &= \max\{\mathbf{v}(\widehat{x}-1, 0),\ \mathbf{v}(u-1, y_\mu)\} + cq\left\lfloor \tfrac{a-\ell-1}{r}\right\rfloor \\ &= \max\Big\{b(r-\mu u-1),\ b(u-1) + c\big((q+1)\mu + q(\left\lfloor \tfrac{(a-\ell-r)\mu}{r}\right\rfloor + 1)\big)\Big\} \\ &\quad + cq\left\lfloor \tfrac{a-\ell-1}{r}\right\rfloor. \end{aligned}$$

因此，第一个陈述。

对于接下来的结论，请注意，根据引理 4.12 的证明，若 $\Lambda > \Delta$ 或若 $\Delta' > \Lambda'$，则有 $\Delta = \mu < \frac{r}{u}$。当 $\Lambda > \Delta$ 时，根据引理 4.12 的证明可知 $u = a - \ell - r$。由此可得 $\lfloor \frac{a-\ell-1}{r} \rfloor = 1$。事实上，由于 $u < r$，我们有 $a - \ell - r < r$，因而$a - \ell - r + (r-1) < 2r - 1$，这就得到了 $\lfloor \frac{a-\ell-1}{r} \rfloor < 2$。根据 $r \le \overline{a-\ell} - 1$ 这一事实，$\lfloor \frac{a-\ell-1}{r} \rfloor \ge 1$，从而得证。最后，当 $\Delta' > \Lambda'$ 时，有 $\Delta = 0$，相应的结果也就成立。

(b) 回忆一下，根据引理 4.3，对所有 $x < \widehat{x} := \min \mathcal{X}$，都有 $\mathbf{m}(bx) = bx$；根据定义 4.2，对 $x \in \mathcal{X}$，有 $\mathbf{m}(bx) = cy$。对于满足 $x > \widehat{x}$ 的 $x \notin \mathcal{X}$，与之前一样，选取满足 $x_j < x$ 的最大元素 $x_j \in \mathcal{X}$，并写作 $x = x_j + z$，其中某个 $z > 0$。注意，这样的元素 $x_j$ 确实存在，因为 $\mathcal{X}$ 非空，且 $\mu \ne 0$。另外，回忆上文还可知 $\mathbf{m}(bx_j) = cy_j$。接下来，我们考察从 $(x_j, 0)$ 到 $(0, y_j)$ 的 $\uparrow$-步和 $\downarrow$-步数列，并将该数列应用于 $(x, 0)$，得到 $(z, y_j)$。因此，正如 (a) 部分所论证的，

$$\mathbf{m}(bx) = \mathbf{m}(bx_j) + b(x - x_j) = b(x - x_j) + cy_j. \tag{4.4}$$

因此，根据引理 4.1，

$$\max_{0\le x<a} \mathbf{m}(bx) = \max\left\{\max_{0<x<u,\, x\in\mathcal{X}} \mathbf{m}(b(x-1)) + cq,\ \max_{u\le x<r,\, x\in\mathcal{X}} \mathbf{m}(b(x-1))\right\} + cq\left\lfloor \tfrac{a-\ell-1}{r}\right\rfloor.$$

事实上，由上文可知，所有 $x \notin \mathcal{X}$ 中都能达到最大值；而其中，当 $z$ 尽可能大时，最大值便会出现，因此 $x$ 会尽可能远离最近的 $x_j$。

回顾引理 4.14， $\mathcal{X}$ 中相邻递增元素之间恰好有两种差，我们将这两种差记为 $d_1 = x_{m-1} - x_\mu$ 和 $d_2 = \widehat{x}$。因此，结合 (4.4)，并回顾引理 4.14 中的 $x_\mu > u$，可得

$$\max_{0\le x<a} \mathbf{m}(bx) = \left(\max_{u\le x<r,\, x\in\mathcal{X}} \mathbf{m}(b(x-1))\right) + cq\left\lfloor \tfrac{a-\ell-1}{r}\right\rfloor. \tag{4.5}$$

同样由 (4.4) 可知，要确定上述最大值，只需考虑对于 $i \in \{1,2\}$，满足 $x_{j_i} + d_i$ 属于 $\mathcal{X}$ 的最大 $j_i \in \{1,\dots,\mu\}$。回顾一下， $w$ 是最大的，且 $x_w + d_2 = x_w + x_m = x_w + \widehat{x}$ 属于 $\mathcal{X}$。由引理 4.14 可知 $x_{m-1} = x_\mu + d_1 \in \mathcal{X}$。结合 (4.5) 和 (4.4)，即可得出结论。□

正如引言中所承诺的，这里给出与 [9, Thm. 5(b)]平行的结果 [9, Thm. 6(b)]经类似修正后的陈述。我们首先从 [9] 回忆

$$\overline{q} := \left\lfloor \frac{a}{\ell} \right\rfloor, \qquad \overline{r} := a - \overline{q}\ell.$$

and

$$\overline{\mathcal{X}} := \{x \in \{0,1,\dots,\ell-\overline{r}\} \mid \mathbf{m}(bx) \equiv 0 \bmod c\}.$$

此外

$$\overline{A} := b(\ell-\overline{r}) - c(\overline{q}+1), \qquad \overline{B} := b\overline{r} + c\overline{q}, \qquad \overline{u} = \overline{r} \bmod (\ell-\overline{r}),$$

and

$$\overline{\mu} := \min\left\{ i \in \mathbb{Z}_{\geq 0} \,\middle|\, \left\lfloor \frac{(i+1)\overline{B}}{\overline{A}} \right\rfloor \neq \left\lfloor \frac{(i+1)\overline{r}}{\ell-\overline{r}} \right\rfloor \right\}.$$

至于 $\mu$，此处的 $\mu$ 与 [9]中的定义相比，是以类似的不同方式定义的。

**定理 4.17** （参见 [9, 定理 6(b)]）。 设 $\mu > \lfloor \frac{\ell-r}{u} \rfloor$。参照 [9, 引理 12], 记 $\overline{\mathcal{X}} = \{x_i \mid i \in \{0,1,\dots,\overline{\mu}\}\}$，其中

$$x_i = (\ell-\overline{r})\left(\left\lfloor \frac{\overline{r}i}{\ell-\overline{r}} \right\rfloor + 1\right) - \overline{r}i,$$

并令

$$y_i = (\overline{q}+1)\left(\left\lfloor \frac{\overline{r}i}{\ell-\overline{r}} \right\rfloor + 1\right) + \overline{q}i$$

对于 $i \in \{0,1,\dots,\overline{\mu}\}$。假设 $m \in \{0,1,\dots,\mu\}$ 满足 $x_m :=$ 最小 $\mathcal{X}$，并令 $w \in \{0,1,\dots,\mu\}$ 为满足 $x_w + x_m \in \mathcal{X}$的最大值。那么

$$g(a,b,c) + a = \max\{b(x_m-1) + cy_w,\, b(x_{m-1} - x_{\bar{\mu}} - 1) + cy_{\bar{\mu}}\} + c\left((\overline{q}+1)\left\lfloor \frac{\ell-1}{\ell-\overline{r}} \right\rfloor - 2\right).$$

## References


[1] A. Brauer 和 J. E. Shockley，论弗罗贝尼乌斯问题， *J. Reine Angew. Math.* **211** (1962)，215–220。[2] F. Curtis，关于数值半群弗罗贝尼乌斯数公式的研究， *Math. Scand.* **67 (2)** (1990)，190–192。[3] S. M. Johnson，线性丢番图问题， *Canad. J. Math.* **12** (1960)，390–398。[4] J. L. Ram´ırez Alfons´ın, *The Diophantine Frobenius Problem*，牛津大学出版社，2005。[5] A. M. Robles-P´erez 和 J. C. Rosales，三个连续斐波那契数平方所对应的弗罗贝尼乌斯数：三种算法过程的比较，arXiv 预印本：2507.01898。[6] J. C. Rosales 和 M. B. Branco，可表示为对称数值半群的交的数值半群， *J. Pure Appl. Algebra* **171** (2002)，303–314。[7] P. Suhajda， *The Frobenius number; exploring the world of non-representable integers*，学士论文，隆德大学，2024。[8] J. J. Sylvester，问题

7382 *Edu-* 载于: *cational Times* **41**，1884，21

W. J. C. Miller（编），《数学问题及其解答》，( )，第 页。[9] A. Tripathi，三个变量的弗罗贝尼乌斯数公式， *J. Number Theory* **170** (2017)，368–389。

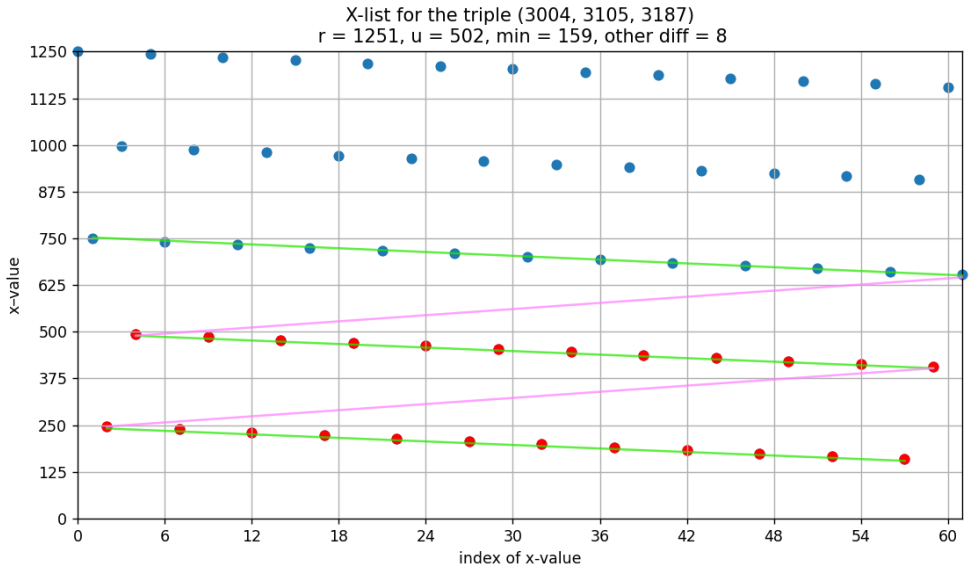



FIGURE 1. 在 $\mathcal{X}$ 中的数值图示示例，其中经过最低点的斜率（以绿色线条表示）为负斜率。红点表示小于 $u$的 $x$值。

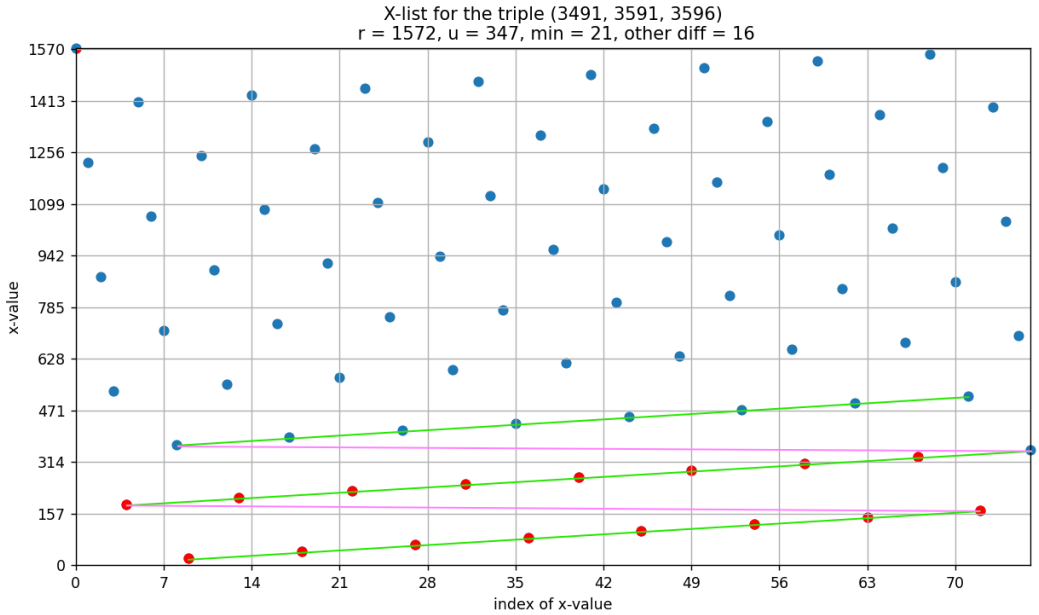



FIGURE 2. 在 $\mathcal{X}$ 中的数值图示示例，其中经过最低点的斜率（见绿色线条）为正斜率。绿色线条和粉色线条的高度分别表示距离 $d_1 = \widehat{x}$ 和 $d_2 = \widehat{x} + u - x_\mu$。

PÉTER SUHAJDA: KTH ROYAL INSTITUTE OF TECHNOLOGY, 114 28 STOCKHOLM, SWEDEN
STOCKHOLM UNIVERSITY, 114 19 STOCKHOLM, SWEDEN*Email address*: suhajda@kth.se

ANITHA THILLAISUNDARAM: CENTRE FOR MATHEMATICAL SCIENCES, LUND UNIVERSITY, 223 62 LUND,SWEDEN*Email address*: anitha.thillaisundaram@math.lu.se