arXiv:2512.22645v1 [math.GM] 27 Dec 2025

广义梅森数的整除性

Alex Chan

alexandr13s98765@gmail.com

2025

引言。本文提出一个定理，用于确定两个广义梅森数的整除判据。这两个数分别是在底数为a^m 和a^k的数制下、位数相同的重复数字数。除了一般证明外，我还给出了该定理在一个特殊情形下的另一种证明。

本文中， d、 m、 k、 a 均为正整数， $d > 1$、 $a > 1$。

“广义梅森数”一词有几种不同的解释。

在本文中，我定义广义梅森数 $M_d(x) := \sum_{j=0}^{d-1} x^j$。

致谢。作者感谢 N. Osipov 教授、A. Kalmynin 和 A. Skopenkov 教授在项目不同阶段给予的持续支持。

定理。以下条件等价。
(1) 数 $M_d(a^m)$ 可被数 $M_d(a^k)$ 整除 .
(2) m 可被 k 整除， 且 $\gcd(\frac{m}{k};\, d) = 1$。

证明。定义

$$Q := \frac{M_d(a^m)}{M_d(a^k)}$$

证明 (1) $\Leftarrow$ (2)。设 m 可整除 k， 且 $\frac{m}{k}$ 与 d的最大公约数为 $= 1$。令 $n = \frac{m}{k}$， 使得n与 d的最大公约数为 $= 1$。对应的商可写为

$$Q = \frac{(a^{md} - 1)(a^k - 1)}{(a^m - 1)(a^{kd} - 1)} = \frac{(b^{nd} - 1)(b - 1)}{(b^n - 1)(b^d - 1)}$$

其中 $b = a^k \geq 2$。我们有 $b^n - 1$与 $b^d - 1$的最大公约数为 $= b^{\gcd(n,d)} - 1 = b - 1$。因此，

$$Q = \frac{b^{nd} - 1}{\operatorname{lcm}(b^n - 1, b^d - 1)}$$

且由于 $b^{nd} - 1$ 是 $b^n - 1$ 和 $b^d - 1$ 的公倍数， Q 是整数。

证明 (1) $\Rightarrow$ (2)。设商

$$Q = \frac{(a^{md}-1)(a^k-1)}{(a^m-1)(a^{kd}-1)}$$

为整数。现在我们分别证明 m 可被 k 整除，以及 gcd($\frac{m}{k}$; d) $= 1$。

证明 (1) $\Rightarrow m$ 可被 k整除。利用所谓的 Zsigmondy 定理（见 [Bi, 定理 V] 或原始的 Zsigmondy 的论文 [Zs]），证明 m 可被 k整除。

当 $kd = 2$时的情形。若 $kd = 2$，则 $k = 1$，结论显然成立。

当 $kd = 6$ 且 $a = 2$时的情形。若 $kd = 6$ 且 $a = 2$，则要么 $k = 1$（此时m 可被 k整除），要么 $(k, d) \in \{(2, 3), (3, 2)\}$。在 $(k, d) = (2, 3)$ 的情形下，商

$$Q = \frac{2^{2m}+2^m+1}{21}$$

仅当 $m = 2n$ 为整数且 n 不能被 3 整除时才是整数。在 $(k, d) = (3, 2)$ 的情形下，商

$$Q = \frac{2^m+1}{9}$$

仅当 $m = 3n$ n 为奇数时才是整数。因此，在这两种情况下， m 可被 k整除。

所有其他情况。在其余情况下，根据 Zsigmondy 定理，存在 $a^{kd}-1$ 的一个素因子 p，使得 $\mathrm{ord}_p(a) = kd$。由 $kd > k$ 可知， $a^k \not\equiv 1 \pmod{p}$。由于 Q 是整数，我们得到 $a^{md} \equiv 1 \pmod{p}$。因此，md 可被 kd 整除，或者等价地， m 可被 k整除。

证明 (1) $\Rightarrow$ gcd($\frac{m}{k}$; d) $= 1$。再次令 $n = \frac{m}{k}$，得到

$$Q = \frac{M_d(b^n)}{M_d(b)}$$

其中 $b = a^k \geq 2$。假设 Q 是一个整数，我们需要证明 gcd$(n, d) = 1$。

令 gcd$(n, d) = l$ 且 $n_1 = n/l$, $d_1 = d/l$。那么

$$M_d(b^n) \equiv lM_{d_1}(b^l) \pmod{M_d(b)} \tag{1}$$

正如我们稍后将看到的。此外，我们有 $M_d(b) = M_{d_1}(b^l)M_l(b)$，因此

$$0 < lM_{d_1}(b^l) = \frac{l}{M_l(b)}M_d(b) < M_d(b)$$

对于所有 $b \geq 2$ 和 $l > 1$。因此，对于 $l > 1$， $M_d(b^n)$ 不能被 $M_d(b)$ 可整除。因此， $l = 1$。

还需证明 (1)。我们使用以下众所周知的事实：对于任何可被 d 整除的 N，同余式 $b^N \equiv 1 \pmod{M_d(b)}$ 成立。我们有

$$M_d(b^n) = \sum_{i=0}^{d-1} b^{ni} = \sum_{q=0}^{l-1}\sum_{r=0}^{d_1-1} b^{ln_1(d_1q+r)} \equiv \sum_{q=0}^{l-1}\sum_{r=0}^{d_1-1} b^{ln_1r} = l\sum_{r=0}^{d_1-1} b^{ln_1r} =$$

$$= l\sum_{r=0}^{d_1-1} b^{l(j_r+d_1q_r)} \equiv l\sum_{r=0}^{d_1-1} b^{lj_r} = l\sum_{r=0}^{d_1-1} b^{lr} = lM_{d_1}(b^l) \pmod{M_d(b)}.$$

这里 $n_1r = j_r + d_1q_r$ 对于某些整数 j_r, q_r $(0 \le j_r < d_1)$，使得

$$\{j_0, j_1, \ldots, j_{d_1-1}\} = \{0, 1, \ldots, d_1 - 1\}$$

由于最大公约数 $\gcd(n_1, d_1) = 1$。

在环 $\mathbb{Z}[x]$ 中，同余式 (1) 可改写为

$$M_d(x^n) \equiv lM_{d_1}(x^l) \pmod{M_d(x)}$$

也成立（证明方法相同）。 □

备注。1. $M_d(x^m)$ 在多项式环 $\mathbb{Z}[x]$ 中可被 $M_d(x^k)$ 整除，当且仅当 m, k, d 满足相同的条件。命题“若”部分的证明几乎完全沿用了第一部分中的证明。同时，命题“仅当”部分的证明则通过考察多项式的复根及其重数而得到简化，无须使用 Zsigmondy 定理。

2. 证明 (1) $\Rightarrow \gcd(\frac{m}{k}; d) = 1$ 可借助 Zsigmondy 定理和著名的 LTE 引理（见 [LTE]）完成。将 $Q = M_d(b^n)/M_d(b)$ 改写为

$$Q = \frac{(b^{nd}-1)(b-1)}{(b^n-1)(b^d-1)}.$$

假设 Q 是一个整数，且 $\gcd(n, d) > 1$。令 q 为 n 和 d的一个公素因子。令 $n_1 = n/q$ 和 $d_1 = d/q$。

当 $q \ge 3$时的情形。根据 Zsigmondy 定理，存在 $b^q - 1$ 的一个素因子 p，使得 $\mathrm{ord}_p(b) = q$。于是 $b \not\equiv 1 \pmod{p}$。由此可得推论 $p \ne q$和 $p \ne 2$。令 $c = b^q$。我们有

$$\nu_p((b^n-1)(b^d-1)) = \nu_p((c^{n_1}-1)(c^{d_1}-1)) =$$

$$= \nu_p(c^{n_1}-1) + \nu_p(c^{d_1}-1) = 2\nu_p(c-1) + \nu_p(n_1) + \nu_p(d_1).$$

而

$$\nu_p((b^{nd}-1)(b-1)) = \nu_p(b^{nd}-1) = \nu_p(c^{qn_1d_1}-1) =$$

$$= \nu_p(c-1) + \nu_p(qn_1d_1) = \nu_p(c-1) + \nu_p(n_1) + \nu_p(d_1).$$

因此，$\nu_p((b^n-1)(b^d-1)) > \nu_p((b^{nd}-1)(b-1))$，而且 Q 不可能是整数。矛盾。

当 $q=2$ 且 $b+1\neq 2^t$ 时。在这种情况下， $b+1$ 有一个素因子 $p\neq 2$。显然，$b\not\equiv 1$ (模 p)。我们可以用与上面相同的方法得到矛盾。

当 $q=2$ 且 $b=2^t-1$，其中 $t\geqslant 2$ 时。这里，我们有 $n=2n_1$、$d=2d_1$。于是

$$\nu_2(b^n-1)=\nu_2(b^2-1)-1+\nu_2(n)=t+\nu_2(n)=t+1+\nu_2(n_1)$$

类似地

$$\nu_2(b^d-1)=t+1+\nu_2(d_1),\quad \nu_2(b^{nd}-1)=t+2+\nu_2(n_1)+\nu_2(d_1).$$

因此，我们得到

$$\nu_2((b^n-1)(b^d-1))=2t+2+\nu_2(n_1)+\nu_2(d_1)>$$
$$>t+3+\nu_2(n_1)+\nu_2(d_1)=\nu_2((b^{nd}-1)(b-1))$$

并且 Q 不可能再次是整数。矛盾。

因此，$\gcd(n,d)=1$。

(1) $\Rightarrow$ (2) 的证明来自一位匿名审稿人。证明 (1) $\Rightarrow$ m 可被 k 整除。假设商

$$Q'=\frac{(a^{md}-1)(a^k-1)}{a^{kd}-1}$$

是一个整数。因此， m 必须可被 k 整除。确实，令

$$D=\gcd(a^{md}-1,a^{kd}-1)=a^{d\gcd(m,k)}-1,$$
$$a^{md}-1=DA',\quad a^{kd}-1=DA''$$

对于某些 A' 和 A''，使得 $\gcd(A',A'')=1$。那么 $DA'(a^k-1)=DA''Q'$。因此，

$$A'(a^k-1)=A''Q'.$$

那么 $A'(a^k-1)$ 可被 A'' 整除。因此， A'' 是 a^k-1 的因数，因为 $\gcd(A',A'')=1$。由此， DA'' 是 $D(a^k-1)$ 的因数，即 $a^{kd}-1$ 是 $(a^{d\gcd(m,k)}-1)(a^k-1)$ 的因数。特别地，

$$a^{kd}-1\leqslant(a^{d\gcd(m,k)}-1)(a^k-1)<a^{d\gcd(m,k)+k}-1$$

这意味着 $kd<d\gcd(m,k)+k$，或者

$$\frac{k}{\gcd(m,k)}<\frac{d}{d-1}\leqslant 2$$

(回想一下 $d\geqslant 2$)。那么 $k=\gcd(m,k)$，因此 m 可被 k 整除。

证明 (1) $\Rightarrow\gcd(\frac{m}{k};\,d)=1$。设 $n=m/k$，并假设该数

$$\frac{(b^{nd}-1)(b-1)}{(b^n-1)(b^d-1)}=\frac{b^{nd}-1}{b^n-1}:\frac{b^d-1}{b-1}=\frac{b^{nd}-1}{b^d-1}:\frac{b^n-1}{b-1}$$

to 是一个整数（其中 $b = a^k \geqslant 2$）。我们来考 roduce

$$M := \frac{b^{\gcd(n,d)} - 1}{b - 1}.$$

显然，我们有

$$\frac{b^d - 1}{b - 1} \equiv \frac{b^n - 1}{b - 1} \equiv 0 \pmod{M}.$$

作为我们假设的推论，我们得到

$$0 \equiv \frac{b^{nd} - 1}{b^n - 1} = 1 + b^n + \ldots + b^{n(d-1)} \equiv d \pmod{M},$$
$$0 \equiv \frac{b^{nd} - 1}{b^d - 1} = 1 + b^d + \ldots + b^{d(n-1)} \equiv n \pmod{M}.$$

因此，gcd (n, d) 可被 M 整除。在 gcd $(n, d) > 1$ 的情况下，我们得到

$$\gcd(n, d) < 2^{\gcd(n,d)} - 1 \leqslant M$$

这与假设矛盾。因此，gcd$(n, d) = 1$，正如所要证明的。
另一种证明：(1) $\Rightarrow m$ 可被 k 整除。定义 $g = \mathrm{ord}_{M_d(a^k)}(a)$。现在我们证明 $g = kd$。事实上，$a^{kd} - 1$ 可被 $M_d(a^k)$ 整除，因此 kd 可被 g 整除。另一方面，$M_d(a^k) > a^{k(d-1)}$，所以 $g > k(d - 1)$。因此，$g = kd$。于是，(1) $\Rightarrow a^{md} - 1$ 可被 $M_d(a^k)$ $\Rightarrow m$ 整除，而 k可被整除。
定理的特殊情形。命题。以下条件等价。

(1) 对任意整数 n，数 $M_d(n^m)$ 可被数 $M_d(n^k)$整除。(2) m 可被 k 整除，且 gcd$(\frac{m}{k}; d) = 1$。

这个结果可能早已为人所知。我是从 [Sy] 得知的。I. Syukrin 提出了一个利用数的典范分解进行技术性证明的思路。这里我给出一个利用多项式的根的简单证明。

(3) 多项式 $M_d(x^m)$ 在 $\mathbb{Z}[x]$ 中可被多项式 $M_d(x$整除 $^k)$.
(3) 与 (1) 等价，这可由 [Sk，问题 3.4.2.b] 得出（其中假设 P 没有根是多余的）。

现在我们证明，(3) 和 (2) 都等价于以下命题。
(4) 多项式 $(x^{md} - 1)(x^k - 1)$ 可被 $\mathbb{Z}[x]$ 中的多项式 $(x^m - 1)(x^{kd} - 1)$ 整除。

我们证明这些等价关系

$$(2) \Leftrightarrow (4) \Leftrightarrow (3).$$

(3) 与 (4) 等价，这一点显而易见。

证明 (2) $\Rightarrow$ (4)。此论断的证明与定理中 (1) $\Leftarrow$ (2) 的证明相同。

证明 (2) $\Leftarrow$ (4)。由于 $(x^{md} - 1)(x^k - 1)$ 可被 $\mathbb{Z}[x]$ 中的多项式 $(x^m - 1)(x^{kd} - 1)$ 整除，且 $(x^m - 1)(x^{kd} - 1)$ 对于 $x_1 := e^{2\pi i/kd}$ 的值为

0， $e^{2\pi i/kd}$ 是分子和分母的一个根。因此，$(x_1^{md}-1) = 0$，因为 $(x_1^k - 1) \neq 0$。所以， md 可被 kd 整除。于是， m 可被 k 整除。

若 $\gcd(u,d) > 1$，则 $g(y) := (y^u - 1)(y^d - 1)$ 有除 1 以外的重根，而 $f(y) := (y^{ud} - 1)(y - 1)$ 没有这样的根。因此， $f(y)$ 在 $\mathbb{Z}[y]$ 中不能被 $g(y)$ 整除。于是，根据以下众所周知的断言， $f(x^k)$ 不能被 $g(x^k)$ 整除。因此，$\gcd(u,d) = 1$。

所以 (2) 成立。

断言。设 k 是一个整数，且 $f(y)\ g(y) \in \mathbb{Z}[y]$。如果 $f(x^k)$ 在 $\mathbb{Z}[x]$ 中可被 $g(x^k)$ 整除，那么 $f(y)$ 在 $\mathbb{Z}[y]$ 中可被 $g(y)$ 整除。

参考文献

[Sk] A. Skopenkov，《Mathematics Via Problems: Algebra》。https://old. mccme.ru//circles//oim/algebra_eng.pdf[Sy] I. Syukrin，《广义梅森数的整除性》。https://old.mccme.ru//circles//oim/mmks/works2024/syukrini5.pdf.[Bi] G. D. Birkhoff 和 H. S. Vandiver，论 $a^n - b^n$ 的整数因子，《数学年刊》5 (1904)，173–180。[Zs] K. Zsigmondy，《关于幂剩余理论》，《数学与物理月刊》3 (1892)，265–284。[LTE] ´E. Lucas，《Th´eorie des Fonctions Num´eriques Simplement P´eriodiques. [Continued]》，《美国数学杂志》，第 1 卷（1878），第 197–240 页。https://www.jstor.org/stable/2369308[AOP] https://planetmath.org/AllOnePolynomial[Re] https://mathworld.wolfram.com/Repunit.html