Ch. 2. 初等数论基础

朱彬

中山大学智能工程学院

zhub26@mail.sysu.edu.cn

2024 年 9 月 9 日

References

Lovász, Pelikán, and Vesztergombi, Discrete Mathematics: Elementary and Beyond, Springer, Ch. 6.

Lang, Undergraduate Algebra, third edition, Springer, Ch. I.

Hardy & Wright, An Introduction to the Theory of Numbers, sixth edition, Oxford University Press, selected parts.

集合符号：整数 $\mathbb{Z}$，非负整数（自然数）$\mathbb{N}$，正整数 $\mathbb{N}_+$。

Axiom (良序 (well-ordering))

任何由非负整数组成的非空集合都有一个最小元素。也就是说：若 $S \subset \mathbb{N}$，则存在一个整数 $n \in S$ 使得 $n \leq x$ 对所有 $x \in S$ 都成立。

良序公理的重要推论：数学归纳法 (mathematical induction)

Proposition (归纳法第一形式)

假定对于每个整数 $n \geq 1$，我们都有一个断言 *(assertion)* $A(n)$；而且，我们能够证明以下两个性质：

(1) 断言 $A(1)$ 为真。

(2) 对于每个整数 $n \geq 1$，若 $A(n)$ 为真，则 $A(n+1)$ 也为真。

那么对于所有整数 $n \geq 1$，断言 $A(n)$ 均为真。

证明（归纳法第一形式）：.

令 $S := \{n \in \mathbb{N}_+ : A(n) \text{ 为假}\}$，我们想证明 S 为空集。

假定 S 非空，那么由良序公理可知：S 中存在一个最小元素 n_0。

- 由假设可知，$n_0 \neq 1$，故 $n_0 > 1$。
- 因为 n_0 是 S 中的最小元素，所以 $n_0 - 1 \notin S$；这说明 $A(n_0 - 1)$ 为真。
- 但根据性质 (2)，$A(n_0)$ 必须也为真。

由此产生矛盾，故命题得证。 □

Remark

在归纳法的陈述中，我们可以把所有的 1 替换为 0，此时证明仍然成立。

Proposition (归纳法第二形式)

假定对于每个整数 $n \geq 0$，我们都有一个断言 *(assertion)* $A(n)$；而且，我们能够证明以下两个性质：

(1') 断言 $A(0)$ 为真。

(2') 对于每个整数 $n > 0$，若 $A(k)$ 在 $0 \leq k < n$ 时均为真，则 $A(n)$ 也为真。

那么对于所有整数 $n \geq 0$，断言 $A(n)$ 均为真。

证明.

和归纳法第一形式的证明类似，留作练习题。

□

首先交代一些关于整数的最基本概念。令 a, b 为两个整数，如果存在一个整数 m 使得 $b = am$，则称

- a 整除 b (a divides b)，
- 或 a 是 b 的一个约数 (a is a divisor of b)，
- 或 b 是 a 的一个倍数 (b is a multiple of a)。

用符号表示：$a \mid b$。

如果 a 不是 b 的一个约数，那么我们写 $a \nmid b$。

若 $a \neq 0$，则 $a \mid b$ 表明比值 b/a 是一个整数。

若 $a \nmid b$ 且 $a > 0$，则我们仍可以用 a 除 b，此时带一个余数 (remainder)。

- 除法 $b \div a$ 的余数 r 是一个满足 $0 \leq r < a$ 的整数。
- 若带余除法的商 (quotient) 为 q，则我们有

$$b = aq + r.$$

- 上式也被称为“欧几里得算法”(Euclidean algorithm)，证明见 Lang, p. 4（使用良序公理)。
- 这种对带余除法的思考方式非常有用。

若一个整数 $p > 1$ 除了 $1, -1, p$ 和 $-p$ 以外，不能被任何其他整数整除，则称 p 为一个**素数** (prime)。

- 另一种说法：如果一个整数 $p > 1$ 不能被写成两个更小正整数的乘积，则 p 是一个素数。

若一个整数 $n > 1$ 不是素数，则称它为**合数** (composite)。

我们认为数字 1 既不是素数，也不是合数。

因此 $2, 3, 5, 7, 11$ 是素数，但 $4 = 2 \cdot 2, 6 = 2 \cdot 3$, $8 = 2 \cdot 4, 9 = 3 \cdot 3$, $10 = 2 \cdot 5$ 不是素数。

自从古代以来，素数就使人们着迷。

- 古希腊人已经知道（并证明了）存在无穷多个素数。

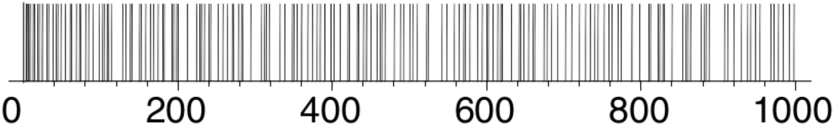

FIGURE 6.1. A bar chart of primes up to 1000.

Lang, Sec. I.3 最大公约数 (greatest common divisor)

令 m, n 为非零整数。若一个整数 $d \neq 0$ 满足 $d \mid m$ 且 $d \mid n$，则称 d 为 m 和 n 的**一个公约数** (common divisor)。

m 和 n 的一个**最大公约数** (greatest common divisor, or gcd) 指的是一个公约数 $d > 0$ 使得：若 e 是 m 和 n 的一个公约数，则 e 整除 d。用符号表示：

$$d = \gcd(m, n) \quad \text{或} \quad d = (m, n).$$

- 我们即将看到 m 和 n 的最大公约数总存在（需要证明!）。
- 容易验证最大公约数（若存在）是唯一确定的（作为练习题）。
- 类似可以定义多个整数的 gcd。

令 J 为整数集 $\mathbb{Z}$ 的子集。若 J 有以下性质：

- 整数 0 在 J 中；
- 若 $m, n \in J$，则 $m + n \in J$；
- 若 $m \in J$ 且 n 是一个任意整数，则 $nm \in J$。

则称 J 是一个**理想** (ideal)。

例

令 $m_1, \ldots, m_r$ 为整数。令 J 为如下集合：

$$\{x_1 m_1 + \cdots + x_r m_r : x_1, \ldots, x_r \in \mathbb{Z}\} \subset \mathbb{Z}.$$

那么容易验证 J 是一个理想。事实上，

- 若 $y_1, \ldots, y_r$ 为整数，则

$$\begin{aligned}(x_1 m_1 + \cdots + x_r m_r) + (y_1 m_1 + \cdots + y_r m_r) \\ = (x_1 + y_1) m_1 + \cdots + (x_r + y_r) m_r \in J.\end{aligned}$$

- 若 $n \in \mathbb{Z}$，则

$$n(x_1 m_1 + \cdots + x_r m_r) = n x_1 m_1 + \cdots + n x_r m_r \in J.$$

- 最后，$0 = 0m_1 + \cdots + 0m_r \in J$，因此 J 是一个理想。

我们称 J 由 (is generated by) $m_1, \ldots, m_r$ **生成**，这 r 个整数为 J 的**生成元** (generators)。

注意到 $\{0\}$ 本身是一个理想，叫做**零理想** (zero ideal)；$\mathbb{Z}$ 也是一个理想，叫做**单位理想** (unit ideal)。

所有偶数的集合是一个理想吗？所有奇数的集合呢？

定理 (Lang, Ch. I, Thm. 3.1)

令 J 为 $\mathbb{Z}$ 的一个理想。那么存在一个整数 d 使得它是 J 的一个生成元。若 $J \neq \{0\}$，则我们可以把 d 取为 J 中最小的正整数。

证明.

如果 J 是零理想，则 0 是一个生成元。

假定 $J \neq \{0\}$。若 $n \in J$，则 $-n = (-1)n \in J$，故 J 包含一些正整数。令 d 为 J 中最小的正整数，其存在性由整数的良序公理保证。

我们声称 d 是 J 的一个生成元。为证明此论断，任取 $n \in J$ 并写下 $n = dq + r$，其中 $0 \leq r < d$。

- 然后 $r = n - dq \in J$ (由理想的定义)；但由于 $r < d$，故必有 $r = 0$。
- 由此得到 $n = dq$；由于 n 的任意性，故 d 是一个生成元。

□

以上结果在初等数论和抽象代数中具有基础 (fundamental) 地位，在后续课程中会被多次用到。

定理 (Lang, Ch. I, Thm. 3.2，最大公约数的存在性)

令 m_1, m_2 为正整数，它们生成理想 J。令 d 为 J 的一个正生成元（其存在性由前一个定理保证），则 d 是 m_1 和 m_2 的一个最大公约数。

证明.

由定理假设可知 $J = \{x_1m_1 + x_2m_2 : x_1, x_2 \in \mathbb{Z}\} = \{qd : q \in \mathbb{Z}\}$。由于 $m_1 = 1m_1 + 0m_2$，故 $m_1 \in J$，即存在一个整数 q_1 使得

$$m_1 = q_1d,$$

因此 d 整除 m_1。类似地，d 整除 m_2。

令 e 为 m_1 和 m_2 的一个（非零）公约数，即存在整数 h_1, h_2 使得

$$m_1 = h_1e \quad 且 \quad m_2 = h_2e.$$

由于 $d \in J$，故存在整数 s_1, s_2 使得 $d = s_1m_1 + s_2m_2$。 □

证明（续）.

由此得到

$$d = s_1 h_1 e + s_2 h_2 e = (s_1 h_1 + s_2 h_2)e.$$

故 e 整除 d，证明完成。 □

推论 (裴蜀定理 (Bézout's theorem or Bézout's identity))

令 $d = \gcd(m, n)$，则 d 可以被写为如下形式

$$d = am + bn,$$

其中 a, b 为整数。

证明.

作为练习题。也可参考 Lovász et al., p. 104. □

Remark

上述证明适用于多个整数的情形。例如，若 $m_1, \ldots, m_r$ 为非零整数，它们生成理想 J，令 d 为 J 的一个正生成元，则 d 是 $m_1, \ldots, m_r$ 的一个最大公约数。

若整数 $m_1, \ldots, m_r$ 的最大公约数为 1，则称它们**互素** (relatively prime, or coprime)。在这种情况下，存在整数 $x_1, \ldots, x_r$ 使得

$$x_1 m_1 + \cdots + x_r m_r = 1,$$

因为 1 位于由 $m_1, \ldots, m_r$ 生成的理想中。

定理 (算术基本定理 (Fundamental Theorem of Arithmetic))

每个正整数 $n \geq 2$ 都可以被写作若干个素数（允许重复）的乘积，即

$$n = p_1 \cdots p_r,$$

且这样的分解除去素因数的顺序之外是唯一的。

分解的存在性不难证明（留做练习题）；难点在于唯一性，为此我们需要一个引理。

引理 (Lang, Ch. I, Lem. 4.2; Lovász et al., p. 92, Ex. 6.3.3(a))

令 p 为一个素数，m, n 为非零整数使得 p 整除 mn。则 $p \mid m$ 或 $p \mid n$。

证明（引理）.

假设 $p \nmid m$，此时我们需要证明 $p \mid n$。

由于 p 为素数，故 $\gcd(p, m) = 1$ (Why?)。根据 Bézout 等式，存在整数 a, b 使得

$$1 = ap + bm.$$

两边乘以 n 得到

$$n = nap + bmn.$$

但是 $mn = pc$ 对于某个整数 c 成立，故

$$n = (na + bc)p,$$

即 $p \mid n$，证明完成。 □

我们把上述引理用于 p 整除若干个素数乘积 $q_1 \cdots q_s$ 的情形。

- 此时，p 要么整除 q_1，要么整除 $q_2 \cdots q_s$。
- 若 $p \mid q_1$，则必然有 $p = q_1$ (Why?)；
- 否则，我们可以继续对 $p \mid (q_2 \cdots q_s)$ 做推理，如此进行下去能得出结论：必存在某个 i 使得 $p = q_i$。

证明（素因数分解的唯一性）.

假定我们可以把整数 $n \geq 2$ 写成两种素数之积

$$p_1 \cdots p_r = q_1 \cdots q_s.$$

根据上面的推理，我们可以对素数 $q_1, \ldots, q_s$ 重新编号，然后假设 $p_1 = q_1$。 □

证明（续）.

等式两边消去 q_1，得到

$$p_2 \cdots p_r = q_2 \cdots q_s.$$

然后，我们可以继续进行有限次类似推理并得出结论：在对 $q_1, \ldots, q_s$ 做重新编号之后，我们有 $r = s$ 且 $p_i = q_i$ 对所有 i 成立。如此唯一性结论得证。 □

另一种 (?) 证明见 Lovász et al., pp. 90–91。注：数论中很多结论的证明方法不唯一。

在把一个整数表达为若干个素数之积时，我们通常把相同的因子放到一起：令 n 为大于 1 的整数，$p_1, \ldots, p_r$ 为能整除 n 的**不同**素数。那么存在唯一一组整数 $m_1, \ldots, m_r > 0$ 使得

$$n = p_1^{m_1} \cdots p_r^{m_r}.$$

Lovász et al., Sec. 6.5 费马小定理 (Fermat's "Little" Theorem)

素数的重要性在于：它们可以合成 (compose) 任意（≥ 2）整数；但它们还有许多令人惊讶的性质。

定理 (费马定理)

若 p 是一个素数且 a 是一个整数，则 $p \mid a^p - a$。

定理的等价说法（证明利用前一条引理，作为练习题）：若 p 是一个素数，a 是一个不能被 p 整除的整数，则有

$$p \mid a^{p-1} - 1.$$

定理的证明需要一条引理，也是关于素数的整除性（相对容易证明）。

引理

若 p 是一个素数且 $0 < k < p$，则 $p \mid \binom{p}{k}$。

证明.

我们知道二项式系数

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}.$$

此处 p 能整除分子而不能整除分母，因为分母中的所有因子均小于 p:

- 根据 Lang, Ch. I，引理 4.2，若一个素数 p 不能整除任何一个因子，则 p 不能整除它们之积。
- 再根据 Lovász et al., p. 92, Ex. 6.3.3(b):

设 a 和 b 为整数且 $a \mid b$，再设 p 为一个素数且 $p \mid b$ 但 $p \nmid a$。证明：p 是比值 b/a 的一个约数。

我们得知 p 是 $\binom{p}{k}$ 的一个约数。

证明（费马定理）.

我们对 a 做归纳进行证明。若 $a = 0$，结论显然成立。

令 $a > 0$，我们把它写作 $a = b + 1$。则有

$$
\begin{aligned}
a^p - a &= (b+1)^p - (b+1) \\
&= b^p + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b + 1 - b - 1 \\
&= (b^p - b) + \binom{p}{1} b^{p-1} + \cdots + \binom{p}{p-1} b.
\end{aligned}
$$

此处由归纳假设可知 $b^p - b$ 能被 p 整除；而根据上一条引理，其他每一项都能被 p 整除。因此 $a^p - a$ 也能被 p 整除，归纳完成。 $\square$

费马最有名的是他的“最后”定理 (Fermat’s “Last” Theorem)：

若整数 $n > 2$，则以下丢番图方程 (Diophantine equation)

$$a^n + b^n = c^n$$

没有正整数解 (a, b, c)。

其中假设 $n > 2$ 是必要的：当 $n = 2$ 时，方程有很多正整数解，称为毕达哥拉斯三元组 (Pythagorean triples，中文也叫做“勾股数”)，见 Lovász et al., Ex. 6.6.7 about Euclid’s formula。

费马在一个杂志的边栏声称证明了该“定理”($\sim$1637)，但从未写下证明；这或许是数学中最有名的未决问题，直到 1995 年才被英国数学家 Andrew Wiles 解决。

Lovász et al., Sec. 6.6 辗转相除法计算 gcd (also called “Euclidean algorithm”)

关于两个整数的最大公约数的计算，最直接的思路是利用它们的素因数分解：查看分解中的公共素因数，然后取对应的两个指数中的较小值，乘方，再取这些素数乘方之积。

- 例如，$900 = 2^2 \cdot 3^2 \cdot 5^2$，$54 = 2 \cdot 3^3$，因此 $\gcd(900, 54) = 2 \cdot 3^2 = 18$。

但麻烦的是，找到大整数的素因数分解是非常困难的——我们需要更聪明的算法。

- 本节讨论的辗转相除法不需要计算素因数分解，且能更快地计算 $\gcd(a, b)$。
- 该算法在几乎所有其他涉及整数计算的算法中扮演重要角色。
- 其发明人为古希腊数学家欧几里得。

欧几里得算法基于如下两个基本事实，见习题 6.6.1 和 6.6.2:

Ex. 6.6.1 证明：若 a 和 b 为正整数且 $a \mid b$，则 $\gcd(a,b)=a$。

Ex. 6.6.2 (a) 证明：$\gcd(a,b)=\gcd(a,b-a)$。
(b) 令 r 为 b 除以 a 的余数，则 $\gcd(a,b)=\gcd(a,r)$。

给定两个正整数 a,b，目标是找到 $\gcd(a,b)$。算法步骤如下：

1. **If** $a>b$, **then** 交换 a 和 b。
2. **If** $a>0$, 计算 $b\div a$ 得到余数 r。用 r 替换 b 并返回步骤 1。
3. **Else** (**if** $a=0$), **return** b 为 gcd，停机。

当我们用纸和笔执行该算法时，我们当然无需在 $a > b$ 时交换 a, b 的值：

- 我们只需要用大数除以小数得到余数；
- 若余数不为零，再用它去替换大数。

例

$$
\begin{aligned}
\gcd(300,18) &= \gcd(12,18) = \gcd(12,6) = 6.\\
\gcd(101,100) &= \gcd(1,100) = 1.\\
\gcd(89,55) &= \gcd(34,55) = \gcd(34,21) = \gcd(13,21) = \gcd(13,8)\\
&= \gcd(5,8) = \gcd(5,3) = \gcd(2,3) = \gcd(2,1) = 1.
\end{aligned}
$$

Ex. 在每种情况，使用素因数分解验证所得结果确实是 gcd。

在描述一个算法时，第一个问题是算法是否能够在有限步之后停止(terminates)。

- 对于辗转相除法，其中的数字单调减小：步骤 2 执行之后，其中一个数字（严格）减小但仍为非负；故算法不可能无限进行下去。

其次，我们当然需要保证算法返回想要的结果。

- 步骤 1（交换两个数字）显然不会改变 gcd。
- 根据 Ex. 6.6.2(b)，步骤 2（用除法所得的余数替换大数）也不会改变 gcd。
- 当我们在步骤 3 停机时，所返回的数字确实是当前 a, b 的 gcd (Ex. 6.6.1)。

第三个更为微妙的问题：算法需要多长时间（执行多少步骤）才能停机？

从有限停机的论断中，我们可以给出执行步数的一个上限：

- 每执行一次步骤 1、2 组成的循环，a, b 之一必然减小，因此算法必然在 $a+b$ 次循环之内停机。
- 但这个上界几乎无用：若对两个 100 位数字执行辗转相除法，则上界 $a+b$ 说我们最多需要执行 $2 \cdot 10^{100}$ 次循环。
- 幸运的是，这只是一个悲观的上界；之前的例子似乎说明算法的终止远快于此。

但那些例子也表明：辗转相除法的执行长度（时间）可以极为不同，这依赖于具体的数字。

问题的关键在于如下引理：

引理

在辗转相除法执行一次循环（步骤 1、2）之后，当前两个数字之积至少减小为原来的 $1/2$。

证明.

考虑数对 (a, b)——其中 $a < b$——被替换为 (r, a) 的步骤，其中 r 为 $b \div a$ 的余数。

- 我们有 $r < a$ 和 $a + r \leq b$，后者由 $b = qa + r$ 和 $(a < b \implies q \geq 1)$ 得出。
- 于是 $b \geq a + r > 2r$，因此 $ar < \frac{1}{2}ab$。

□

定理

辗转相除法应用于两个正整数 a 和 b 的步骤数最多为 $\log_2 a + \log_2 b$。

证明.

假设算法进行 k 步之后仍未停机，这表明当前 a 和 b 之积仍不为零。

- 上一条引理说明：当前两个数字之积最多为 $ab/2^k$。
- 该乘积是一个正整数，故至少为 1，由此得到

$$ab \geq 2^k,$$

故

$$k \leq \log_2(ab) = \log_2 a + \log_2 b.$$

定理得证。

□

我们把之前算法执行次数的悲观估计 $a+b$ 替换为 $\log_2 a + \log_2 b$，这是一个显著的提高！

- 例如，在计算两个 300 位整数的 gcd 时，循环次数不超过 $2\log_2 10^{300} = 600\log_2 10 < 2000$；这比 $2\cdot 10^{300}$ 小得多。
- 注意到 $\log_2 a$ 小于 a 的二进制表示包含的位数 (bits)，因此我们可以说：辗转相除法进行的循环次数不超过 a 和 b 的二进制表示包含的位数之和。

上述定理只给出了算法执行步数的一个上限；有时候我们可以更幸运——算法停止更早。

- 例如，辗转相除法运用于两个连续整数时，只需要一步。
- 但另一些时候，我们无法做得更好，见 Lovász et al., pp. 102–103，特别是习题 6.6.9 和 6.6.10（关于把算法用于两个连续的斐波那契数）。

推论 (Bézout again)

令 $d = \gcd(a, b)$，则 d 可以被写为如下形式

$$d = am + bn,$$

其中 m, n 为整数。

辗转相除法提供了计算上述表达式的方法。

例

回顾

$$\gcd(300, 18) = \gcd(12, 18) = \gcd(12, 6) = 6.$$

此处 12 为 $300 \div 18$ 的余数，故 $12 = 300 - 16 \cdot 18$，由此把第一个等式改写为

$$\gcd(300, 18) = \gcd(300 - 16 \cdot 18, 18).$$

下一步，余数 $6 = 18 - 12$，我们可以维持 $(300$ 的倍数$) + (18$ 的倍数$)$ 的形式

$$\gcd(300 - 16 \cdot 18, 18) = \gcd(300 - 16 \cdot 18, 17 \cdot 18 - 300).$$

由此得 $\gcd = 6$ 可以被写为

$$6 = 17 \cdot 18 - 300.$$

以上例子说明：算法中途产生在数字都能被写成 $am + bn$ 的形式，证明（采用归纳法）见 Lovász et al., p. 104。

这里我们把 Lovász et al., Sec. 6.6 中提到的用素因数分解计算 gcd 的说法表述为定理。

- 我们采用备选记号 (a, b) 表示 $\gcd(a, b)$。

定理 (50)

若

$$a = \prod_p p^{\alpha} \quad (\alpha \geq 0),$$

且

$$b = \prod_p p^{\beta} \quad (\beta \geq 0),$$

则

$$(a, b) = \prod_p p^{\min(\alpha, \beta)}.$$

关于定理中符号的解释：无穷乘积

$$\prod_p f(p) = f(2)\cdot f(3)\cdot f(5)\cdots f(p)\cdots$$

中的变量 p 可能的取值为所有素数。类似地，乘积

$$\prod_{p|m} f(p)$$

中 p 可能的取值为 m 所有的（不同）素因数，故为有限项。

在定理的第一个公式

$$a = \prod_p p^{\alpha} \quad (\alpha \geq 0)$$

中，若 $p \nmid a$，则相应的指数 $\alpha = 0$；故该乘积实际只包含有限项。我们可以把它等价地写成

$$a = \prod_{p|a} p^{\alpha},$$

此时每个 α 都是**正整数**。

两个整数 a 和 b 的**最小公倍数** (least common multiple, lcm) 是同时能被 a 和 b 整除的正数（公倍数）中最小的那个，用 $\{a,b\}$ 或 $\mathrm{lcm}(a,b)$ 来表示，故

$$a \mid \{a,b\}, \quad b \mid \{a,b\},$$

且 $\{a,b\}$ 是具有该性质的最小整数。

定理 (51)

采用定理 50 的记号，

$$\{a,b\} = \prod_p p^{\max(\alpha,\beta)}.$$

从定理 50 和 51，我们推导出：

定理 (52)

$$\{a, b\} = \frac{ab}{(a, b)}.$$

- 若 a, b 互素，即 $(a, b) = 1$，则 $\{a, b\} = ab$。
- 补充定义：若整数 $a, b, c, \ldots, k$ 两两互素，则称它们**互素** (coprime)。
  - 该条件比
    $$(a, b, c, \ldots, k) = 1$$
    强得多，后者只是说除了 1 以外，没有其他数可以整除所有的 $a, b, c, \ldots, k$。

我们有时候说 “a 和 b 没有公因子”，意思是它们没有大于 1 的公因子，即两者互素。

Hardy & Wright, Sec. 5.2 同余和残数类 (congruences and classes of residues)

若 m 是 $x-a$ 的一个约数，我们称 x **和** a **对模** m **同余** (x is congruent to a modulo m)，写做

$$x \equiv a \pmod{m}.$$

- 这个定义（发明人为 Gauss）没有引入任何新的思想，因为 $x \equiv a \pmod{m}$ 的意思和 $m \mid x-a$ 一样。
- 但每种记号都有其优势，这个同余式看起来像等式——实际上也有许多和等式类似的性质。
- “同余”如其字面意思：若 x 和 a 分别除以 m，则余数相同。（证明作为练习题）

$x \not\equiv a \pmod{m}$ 表示 x 和 a 对模 m 不同余。

若 $x \equiv a \pmod m$，则 a 叫做 x 模 m 的**一个残数** (residue)。

- 若 $0 \leq a \leq m-1$，则称 a 为**最小（非负）残数** (least residue)。
- 因此两个模 m 同余的数 a, b 具有相同的模 m 残数。

一个模 m 残数类 (a class of residues $(\bmod\, m)$) 是一个集合，其中包含所有和给定残数模 m 同余的数，每一个这样的数都叫做该残数类的一个**代表** (representative)。

- 显然，总共有 m 个残数类，它们的代表分别为

$$0, 1, 2, \ldots, m-1.$$

- 这 m 个数，或以任何其他方式从每一类中选取一个得到的 m 个数，构成了一个模 m **不同余残数的完整系统** (a complete system of incongruent residues modulo m)，或简称为模 m **完整系统** (a complete system $(\bmod\, m)$)。

同余在日常生活中极其重要。

- 例如，“今天是周六”说的是自从某个固定的日期（例如创世）开始经过天数的一个 $\pmod 7$ 同余性质——该性质通常比实际经过的天数重要得多。
- 大学排课、火车排班也反映了同余性质；和前者相关的模是 $365, 7$ 和 24。

为了找到一周中特定事件会发生的某一天，我们需要在“模 7 算术” (arithmetic $\pmod 7$) 中求解一个问题。

- 在这样一种算术中，同余数是**等价的** (equivalent)，因此这类算术是严格的有限科学，其中的所有问题可以通过试错 (by trial) 解决。

例

假定一门课程每两天（包括周日）上一次课，某个周一上第一节课。问：第一次在周二上的课是第几节？

解：假设第 $x+1$ 节课第一次在周二上，则有

$$2x \equiv 1 \pmod 7;$$

于是我们通过试错可以找到方程的**最小正整数解**为

$$x = 4.$$

故第五节课在周二上，且这是该课程第一次在周二上。

类似地，我们通过试错发现：同余方程

$$x^2 \equiv 1 \pmod 8$$

只有四个解，即

$$x \equiv 1, 3, 5, 7 \pmod 8.$$

固定模 m 时，显然同余具有如下性质：

1. （对称性）$a \equiv b \implies b \equiv a$；
2. （传递性）若 $a \equiv b$ 且 $b \equiv c$，则 $a \equiv c$；
3. （两边相加）若 $a \equiv a'$ 且 $b \equiv b'$，则 $a + b \equiv a' + b'$。

此外，若 $a \equiv a'$，$b \equiv b', \dots$，则有

4. （线性组合）$ka + \ell b + \cdots \equiv ka' + \ell b' + \cdots$；特别地，有 $a - b \equiv a' - b'$（两边相减）。
5. $a^2 \equiv a'^2$，$a^3 \equiv a'^3$ 等。

最后，若 $\phi(a, b, \dots)$ 是任意**整系数**多项式，我们有

6. $\phi(a, b, \dots) \equiv \phi(a', b', \dots)$；特别地，有 $ab \equiv a'b'$（两边相乘）。

定理 (53)

若 $a \equiv b \pmod{m}$ 且 $a \equiv b \pmod{n}$，则

$$a \equiv b \pmod{\{m, n\}}.$$

特别地，若 $(m, n) = 1$，则

$$a \equiv b \pmod{mn}.$$

证明.

结论由定理 51 导出：若 p^c 是素数 p 能整除 $\{m, n\}$ 的最高次幂，则 $p^c \mid m$ 或 $p^c \mid n$，因此 $p^c \mid (a-b)$。上述推理对 $\{m, n\}$ 的每个素因数都成立，因此

$$a \equiv b \pmod{\{m, n\}}.$$

□

显然，该定理能被推广到任意数量的同余式。

Lang, Sec. I.5 等价关系和同余 (Equivalence relations and congruences)

等价关系是数学（尤其是在本课程）中一个非常重要的概念。

令 S 为一个集合。S 中的一个**关系** (relation) R 是 $S \times S$ 的一个子集；若 $(x, y) \in R$，则称 x, y 满足关系 R，写作 xRy。

- 由于 $S \times S$ 表示 S 中的**有序**元素对，故 $xRy \not\Rightarrow yRx$。

S 中的一个**等价关系** (equivalence relation) 是一个关系——满足该关系的元素对写为 $x \sim y$（读作 "x 等价于 y"）——且满足如下条件：

1. （自反性，reflexivity）对所有 $x \in S$，有 $x \sim x$；
2. （传递性，transitivity）若 $x \sim y$ 且 $y \sim z$，则 $x \sim z$；
3. （对称性，symmetry）若 $x \sim y$，则 $y \sim x$。

假定 S 中有这样一个等价关系。给定一个元素 $x \in S$，令集合 C_x 包含 S 中所有和 x 等价的元素。

- 那么由等价关系的三条性质可知，C_x 中的所有元素都互相等价。(验证这一点！)
- 进一步，容易验证：若 x, y 为 S 中的元素，则要么 $C_x = C_y$，要么 C_x, C_y 没有公共元素（不相交)。

每个 C_x 都叫做一个**等价类** (equivalence class)。

- 上两条结论表明：S 上的等价关系确定了 S 的一个不相交等价类分解 (a decomposition of S into disjoint equivalence classes，更准确而言，应叫做“划分”)。
- 一个等价类的任一元素叫做该类的一个**代表** (representative)。

等价关系的第一个例子就是同余的概念：

$$a \equiv b \pmod{m},$$

其中模 m 为正整数，a, b 为整数。

根据前面**同余的基本性质**，可知这是一个等价关系；此处的等价类为**模 m 残数类**，共 m 个，它们构成了整数集 $\mathbb{Z}$ 的一个划分。

我们定义**偶数** (even integers) 为和 0 对模 2 同余的数，

- 故 n 为偶数当且仅当存在整数 m 使得 $n = 2m$。

再定义**奇数** (odd integers) 为不是偶数的其他整数，

- 则容易证明：一个奇数 n 可以被写作 $2m + 1$ 的形式，其中 m 为某个整数。

同余的基本性质看起来和代数方程一样，但很快我们就发现一个不同点——关于除法（消去律）：一般而言，

$$ka \equiv ka' \;\not\Rightarrow\; a \equiv a'.$$

例如

$$2 \cdot 2 \equiv 2 \cdot 4 \pmod 4,$$

但是

$$2 \not\equiv 4 \pmod 4.$$

下面我们给出正确的消去律。

定理 (54)

若 $(k, m) = d$，则

$$ka \equiv ka' \pmod{m} \implies a \equiv a' \left(\bmod \frac{m}{d}\right),$$

反之亦成立。

证明.

由于 $(k, m) = d$，我们有

$$k = k_1 d, \quad m = m_1 d, \quad (k_1, m_1) = 1,$$

故

$$\frac{ka - ka'}{m} = \frac{k_1(a - a')}{m_1}.$$

因为 $(k_1, m_1) = 1$，所以

$$m \mid ka - ka' \iff m_1 \mid a - a'.$$

上述定理的一个特殊情形为：

定理（55（消去律））

若 $(k, m) = 1$，则

$$ka \equiv ka' \pmod{m} \implies a \equiv a' \pmod{m},$$

反之亦成立。

定理 (56)

若 $a_1, a_2, \ldots, a_m$ 是一个模 m 不同余残数的完整系统，且 $(k, m) = 1$，则 $ka_1, ka_2, \ldots, ka_m$ 也是一个模 m 完整系统。

证明.

若 $ka_i - ka_j \equiv 0 \pmod{m}$，则根据定理 55，有 $a_i - a_j \equiv 0 \pmod{m}$；由定理假设，除非 $i = j$，否则该同余式不可能成立。 $\square$

更一般地，若 $(k, m) = 1$，则

$$ka_r + \ell \quad (r = 1, 2, \ldots, m)$$

是一个模 m 不同余残数的完整系统。

定理 (57)

考虑同余（方程）

$$kx \equiv \ell \pmod{m},$$

其中 x 为未知整数。若 $(k, m) = d$，则当且仅当 $d \mid \ell$ 时，该同余才有解；此时它有 d 个（不同余）解。

- 特别地，若 $(k, m) = 1$，则该同余有且只有一个解。

证明.

该同余方程等价于

$$kx - my = \ell,$$

其中 x, y 为未知量；此方程具有 Bézout 等式的形式，因此其有解的判定条件 $d \mid \ell$ 由 Lang, Ch. I, Thm. 3.1 直接导出。

- 当我们说该同余“只有 d 个”解时，（模 m）同余的解自然被看成是同一个。

$\square$

证明（续）.

若 $d = 1$，则定理 57(的特例) 是定理 56 的一个推论 (Why?)。

若 $d > 1$ 且 $d \mid \ell$，则同余式 $kx \equiv \ell \pmod{m}$ 有解。此时令

$$m = dm', \quad k = dk', \quad \ell = d\ell',$$

则定理中的同余等价于（Ex. 检查！）

$$k'x \equiv \ell' \pmod{m'}.$$

由于 $(k', m') = 1$，根据定理的特例，上述同余式只有一个解；设其为

$$x \equiv t \pmod{m'},$$

则

$$x = t + ym';$$

然后通过赋予 y 所有可能的值使得 $t + ym'$ 的值模 m 不同余，我们就能找到原同余式的完整解集。 □

证明（续）.

由于

$$t + ym' \equiv t + zm' \pmod{m} \iff m \mid m'(y-z) \iff d \mid (y-z),$$

故总共只有 d 个解，它们的代表为

$$t,\ t+m',\ t+2m',\ \ldots,\ t+(d-1)m'.$$

由此证明完成。 $\square$

Hardy & Wright, Sec. 5.5 欧拉函数 $\phi(m)$ (Euler's function)

给定正整数 m，我们用 $\phi(m)$ 表示不超过 m 且和 m 互素的正整数个数，也就是说，符合如下条件的整数 n 的个数：

$$0 < n \leq m, \quad (n, m) = 1.$$

注意，只有当 $m = 1$ 时，n 才能等于 m；故 $\phi(1) = 1$。

若 a 和 m 互素，则根据 Lovász et al., Ex. 6.6.2(a)，任意和 a 模 m 同余的数 x 也和 m 互素，即（Ex. 证明此结论！）

$$(a, m) = 1 \implies (\underbrace{a + km}_{x}, m) = 1.$$

因此共有 $\phi(m)$ 个和 m 互素的残数类；从每一类中任意挑一个数——共 $\phi(m)$ 个残数构成的集合叫做**一个和 m 互素的残数的完整集合** (a complete set of residues prime to m)。

- 一个这样的完整集合由不超过 m 且和 m 互素的 $\phi(m)$ 个数构成。

定理 (58)

若 $a_1, a_2, \ldots, a_{\phi(m)}$ 是一个和 m 互素的残数的完整集合，且 $(k, m) = 1$，则

$$ka_1, ka_2, \ldots, ka_{\phi(m)}$$

也是这样一个集合。

证明.

第二个集合中的每个数都和 m 互素，即

$$(k, m) = 1 \text{ 且 } (a_i, m) = 1 \implies (ka_i, m) = 1 \quad (i = 1, \ldots, \phi(m)).$$

(Ex. 证明以上结论。)

并且，类似于定理 56 的证明，若 $i \neq j$，则 ka_i 和 ka_j 不同余 $\pmod m$。 □

定理 (59)

假定 $(m, m') = 1$，a 取遍一个模 m 完整系统中的数，a' 取遍一个模 m' 完整系统中的数。则 $a'm + am'$ 取遍一个模 mm' 完整系统中的数。

证明.

形如 $a'm + am'$ 的数共有 mm' 个。若

$$a_1'm + a_1m' \equiv a_2'm + a_2m' \pmod{mm'},$$

则 (Why?)

$$a_1m' \equiv a_2m' \pmod{m},$$

故

$$a_1 \equiv a_2 \pmod{m};$$

类似有

$$a_1' \equiv a_2' \pmod{m'}.$$

因此这 mm' 个数都模 mm' 不同余，构成一个（模 mm'）完整系统。 □

定义

一个函数 $f(m)$ 若满足如下性质:

$$(m, m') = 1 \implies f(mm') = f(m)f(m'),$$

则称它为**乘性的** (multiplicative)。

定理 (60)

$\phi(m)$ 是乘性的。

证明.

若 $(m, m') = 1$，则根据定理 59，当 a 和 a' 分别取遍模 m 和模 m' 完整系统中的数时，$a'm + am'$ 取遍一个模 mm' 完整系统中的数。

(下一页继续)

$\square$

证明（续）.

此外，

$$
\begin{aligned}
(a'm+am', mm')=1 &\iff (a'm+am', m)=1 \text{ 且 } (a'm+am', m')=1 \\
&\iff (am', m)=1 \text{ 且 } (a'm, m')=1 \\
&\iff (a, m)=1 \text{ 且 } (a', m')=1.
\end{aligned}
$$

所以，$\phi(mm')$ 个小于 mm' 且与之互素的数正是 $\phi(m)\phi(m')$ 个 $a'm+am'$ 的值所代表的残数类中的最小正残数，其中 a 和 m 互素，a' 和 m' 互素；因此，

$$\phi(mm')=\phi(m)\phi(m').$$

□

上述的证明的一个次要结果为:

定理

若 $(m, m') = 1$，a 遍历一个和 m 互素的残数的完整集合，a' 遍历一个和 m' 互素的残数的完整集合，则 $am' + a'm$ 遍历一个和 mm' 互素的残数的完整集合。

我们现在可以对任意 m 找到它的函数值 $\phi(m)$，即写下其表达式。

定理 (62)

若 $m = \prod p^c$，则

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right).$$

证明（定理 62）.

根据定理 60，我们有 (Why?)

$$\phi(m) = \prod \phi(p^c),$$

因此我们只需计算 $\phi(m)$ 在 m 为素数幂 (prime power) 时的值:

- 小于 p^c 的正整数有 $p^c - 1$ 个，
- 其中 p 的倍数有 $p^{c-1} - 1$ 个 (Why?)，其余数均和 p 互素。
- (换而言之，和 p^c 不互素的数必然是 p 的倍数。)

因此

$$\phi(p^c) = p^c - 1 - (p^{c-1} - 1) = p^c \left(1 - \frac{1}{p}\right);$$

由此可以得到定理中一般情形 $\phi(m)$ 的表达式。 $\square$

定理 (63)

$$\sum_{d|m} \phi(d) = m,$$

其中求和变量 d 为 m 的正约数。

证明.

若 $m = \prod p^c$，则 m 的约数具有形式 $d = \prod p^{c'}$，其中对每个素因数 p 有 $0 \le c' \le c$；（Ex. 共有多少个正约数？）

接着，

$$\begin{aligned}\Phi(m) := \sum_{d|m} \phi(d) &= \sum_{c'} \prod_{p} \phi(p^{c'}) \\ &= \prod_{p} \left[1 + \phi(p) + \phi(p^2) + \cdots + \phi(p^c)\right],\end{aligned}$$

其中第二个等式用到了 $\phi(m)$ 的乘性性质，第三个等式为乘法的基本代数性质。 □

证明（续）.

注意到 (Why?)

$$1+\phi(p)+\cdots+\phi(p^c) = 1+(p-1)+p(p-1)+\cdots \\ +p^{c-1}(p-1) = p^c,$$

因此，

$$\Phi(m) = \prod_p p^c = m.$$

$\square$

本节主要阐述求解线性同余方程组的**中国剩余定理** (Chinese remainder theorem, 也称孙子定理)。

一些历史:

- 同余方程组最早见于中国南北朝时期（公元 5 世纪）的数学著作《孙子算经》中的“物不知数”问题，其理论在南宋（13 世纪）秦九韶的《数书九章》中发展完善，称为“大衍求一术”;
- 基督教士在 19 世纪把该解法引入欧洲，后发现该解法和高斯 1801 年的著作“Disquisitiones Arithmeticae”中的论述完全一致；此定理的英文名称由此而来。

我们首先回顾 Sec. 5.4 中单个线性同余的解法。

考虑一般的线性同余

$$ax \equiv b \pmod{m},$$

- 则它可解的条件（判据）为

$$d = (a, m) \mid b.$$

- 若该条件被满足，则原同余式只有 d 个解，分别是

$$\xi,\ \xi + \frac{m}{d},\ \xi + 2\frac{m}{d},\ \ldots,\ \xi + (d-1)\frac{m}{d},$$

其中 ξ 是同余

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\bmod \frac{m}{d}\right)$$

的唯一解。

下面考虑线性同余方程组

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{m_k} \end{aligned},$$

其中模 $m_1, m_2, \ldots, m_k$ 是（两两）互素的；

- 则方程组有解的条件为 $(a_i, m_i) \mid b_i$ 对每个 i 都成立。
- 若该条件被满足，我们可以对每个同余式分别求解；于是问题化简为对如下同余方程组的求解：

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}$$

- 注意此处的 m_i 和原方程组中不同，但仍然两两互素 (Why?)；事实上，它们对应原方程组的 $m_i/(a_i, m_i)$。

定理 (121)

考虑同余方程组

$$x \equiv c_1 \pmod{m_1}, \quad x \equiv c_2 \pmod{m_2}, \quad \ldots, \quad x \equiv c_k \pmod{m_k}.$$

若 $m_1, m_2, \ldots, m_k$ 是互素的，则该方程组有模 m 唯一解

$$x = M_1 n_1 c_1 + M_2 n_2 c_2 + \cdots + M_k n_k c_k,$$

其中

- $m := m_1 m_2 \cdots m_k = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k$;
- n_i 为同余

  $$M_i n_i \equiv 1 \pmod{m_i}$$

  的（模 m_i）唯一解。

证明.

根据定理假设，显然有 $(m_i, M_i) = 1$，因此同余（式中右端的 1 对应秦九韶"大衍求一术"中的"一"）

$$M_i n_i \equiv 1 \pmod{m_i}$$

有模 m_i 唯一解 n_i。

再者，定理构造的 x 显然对每个 i 满足 $x \equiv M_i n_i c_i \equiv c_i \pmod{m_i}$，故 x 是同余方程组的解。

最后需要证明 x 的模 m 唯一性。为此，若 y 也是方程组的解，则对每个 i 有

$$y \equiv c_i \equiv x \pmod{m_i}$$

由于 m_i 互素，故由定理 53 知 $y \equiv x \pmod{m}$。由此唯一性得证。 □

例（《孙子算经》卷下第 26 题“物不知数”）

今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰：二十三（模 105）。

过程：本题求的是如下同余方程组的解：

$$x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7.$$

数字比较简单，直接凑也不难。

这里的三个模显然互素，按照前述定理，

$$\begin{aligned} m_1 &= 3, & m_2 &= 5, & m_3 &= 7; \\ M_1 &= 35, & M_2 &= 21, & M_3 &= 15; \\ n_1 &= 2, & n_2 &= 1, & n_3 &= 1; \\ c_1 &= 2, & c_2 &= 3, & c_3 &= 2. \end{aligned}$$

故

$$x = M_1 n_1 c_1 + M_2 n_2 c_2 + M_3 n_3 c_3 = 233 \equiv 23 \pmod{105}.$$

当模 $m_1, \ldots, m_k$ 不互素时，问题变得更为复杂。一个有趣的例子见 Hardy & Wright, pp. 121–122.

Hardy & Wright, Ch. 16（部分）算术函数 (arithmetical functions)

算术函数指的是正整数 n 的函数，它们表达了 n 的一些算术性质。

例如我们已经见过的 $\phi(n)$，它定义为小于 n 且和 n 互素的正整数个数，其中 $n > 1$；定理 62 表明：

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

该公式也是“容斥原理”(the inclusion-exclusion principle) 的直接推论，见 Hardy & Wright, Sec. 16.1, pp. 302–303.

我们会在课程的第二部分回到这里 (also some lines on pp. 304, 306)。

Möbius 函数 $\mu(n)$ 定义如下：

(i) $\mu(1) = 1$；

(ii) 若 n 包含一个平方因数，即 n 的素因数分解中包含 p^α 且 $\alpha \geq 2$，则 $\mu(n) = 0$；

(iii) $\mu(p_1 p_2 \cdots p_k) = (-1)^k$，其中 $p_1, p_2, \ldots, p_k$ 为不同的素数。

因此，$\mu(2) = -1$，$\mu(4) = 0$，$\mu(6) = 1$。

定理 (262)

$\mu(n)$ 是乘性的，意思是：若 $(m, m') = 1$，则 $\mu(mm') = \mu(m)\mu(m')$。

证明.

作为练习题：由 $\mu(n)$ 的定义直接得出。□

下面我们证明 $\mu(n)$ 的几个其他性质。

定理 (263)

$$\sum_{d|n}\mu(d)=1 \quad (n=1), \quad \sum_{d|n}\mu(d)=0 \quad (n>1).$$

证明.

第一个等式是平凡的。

若 $n>1$，令 $n=p_1^{a_1}\cdots p_k^{a_k}$，其约数的形式为 $d=p_1^{a_1'}\cdots p_k^{a_k'}$，其中 $0\le a_i'\le a_i$。但注意到，若要使得 $\mu(d)\neq 0$，则所有指数需满足 $0\le a_i'\le 1$；因此，

$$\begin{aligned}\sum_{d|n}\mu(d) &= 1+\sum_{i}\mu(p_i)+\sum_{ij}\mu(p_ip_j)+\cdots \\ &= 1-k+\binom{k}{2}-\binom{k}{3}+\cdots=(1-1)^k=0.\end{aligned}$$

$\square$

定理 (264)

若 $n > 1$ 且 k 为 n 不同素因数的个数，则

$$\sum_{d|n} |\mu(d)| = 2^k.$$

证明.

和定理 263 的证明类似。 $\square$

定理 263 还有另一个证明，它依赖于下一个重要的一般结论。

定理 (265)

若 $f(n)$ 是一个 n 的乘性函数，则

$$g(n) = \sum_{d|n} f(d).$$

也是一个乘性函数。

证明.

不难证明（作为练习题）：若 $(n, n') = 1$，$d \mid n$，$d' \mid n'$，则 $(d, d') = 1$，且 $c = dd'$ 能取遍 nn' 所有的约数。

因此，

$$\begin{aligned} g(nn') = \sum_{c|nn'} f(c) &= \sum_{d|n,\ d'|n'} f(dd') \\ &= \sum_{d|n} f(d) \sum_{d'|n'} f(d') = g(n)g(n'). \end{aligned}$$

□

定理 263 的另一个证明.

我们把定理 265 中的 $f(n)$ 取为 $\mu(n)$，得到

$$g(n)=\sum_{d|n}\mu(d).$$

接着，$g(1)=1$；当 $m\geq 1$ 时，

$$g(p^m)=1+\mu(p)=0.$$

因此，若 $n=p_1^{a_1}\cdots p_k^{a_k}>1$，则

$$g(n)=g(p_1^{a_1})g(p_2^{a_2})\cdots=0.$$

□

下面我们会经常用到一个一般的“反演”（求逆）公式，它首先被 Möbius 证明。

定理 (266)

若

$$g(n) = \sum_{d|n} f(d),$$

则

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

证明.

事实上，

$$\sum_{d|n}\mu(d)g\left(\frac{n}{d}\right)=\sum_{d|n}\mu(d)\sum_{c|\frac{n}{d}}f(c)=\sum_{cd|n}\mu(d)f(c)$$
$$=\sum_{c|n}f(c)\sum_{d|\frac{n}{c}}\mu(d).$$

若 $n/c=1$ 即 $c=n$，则此处内部的求和等于 1；否则根据定理 263，$\sum_{d|\frac{n}{c}}\mu(d)$ 为零。因此，上述二重求和最终等于 $f(n)$。 □

定理 266 的逆命题也成立，表述如下：

定理 (267)

$$f(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)g(d)\implies g(n)=\sum_{d|n}f(d).$$

证明.

类似定理 266 的证明，我们有

$$\begin{aligned}\sum_{d|n}f(d)&=\sum_{d|n}f\left(\frac{n}{d}\right)=\sum_{d|n}\sum_{c|\frac{n}{d}}\mu\left(\frac{n}{cd}\right)g(c)\\&=\sum_{cd|n}\mu\left(\frac{n}{cd}\right)g(c)=\sum_{c|n}g(c)\sum_{d|\frac{n}{c}}\mu\left(\frac{n}{cd}\right)=g(n).\end{aligned}$$

□

The End