第二章 同余
2015 年03月24 日

# 信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn





# 2.1 同余的概念及基本性质

**思考题**

1. 如何对信息分类? 如何对信息数字化?
2. 什么是等价关系?
3. 什么是等价分类? 整数的等价分类是什么?
4. 如何判断一个整数属于某一个等价类?
5. 如何从整数集合构造一个由有限元素组成的新集合，使得该集合能保持整数集合中的一些运算? 哪些运算性质保持不变? 哪些运算性质会发生变化? 如何变化?
6. 同余是等价关系吗?
7. 设$m$ 为正整数. 对于整数$r,\ 0 \leq r <$, 记余数为$r$ 的所有整数所组成的集合为$C_r$, $\{C_r \mid r,\ 0 \leq r < m\}$ 是整数集合$\mathbf{Z}$ 的等价分类吗? 相对应的等价关系是什么?
8. 由$C_r$ 所组成的新集合$\mathbf{Z}/R = \{C_r \mid r,\ 0 \leq r < m\}$, 如何定义$\mathbf{Z}/R$ 中的加法运算? 如何定义$\mathbf{Z}/R$ 中的乘法运算?

本章主要讲述如下问题:

1. 同余的基本概念
2. 模同余的判断: 等价关系和模运算等
3. 模同余的基本性质
4. 剩余类与完全剩余系
5. 简化剩余类与简化剩余系
6. 模逆元素 乘法表
7. 欧拉函数及其计算
8. 欧拉定理 费马小定理
9. RSA 解密证明
10. 模重复平方法





## 2.1.1 同余的概念

前面讨论了整数的整除性质, 现在讨论整数的同余性质, 以对整数进行恰当的分类. 同余是数论中的一个十分重要的概念, 同余理论在密码学, 特别是公钥密码学中有着非常重要的应用.

生活中常问某月某日是否有空？是否有课？通常的决定过程是看该天是星期几？

设有 26 个英文字符, 将它们作移位变换 (左移 3 位) 有.

| 字符 | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 字符 | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |

## 将符号数字化

| 字符 | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

则相应的移位变换为

| 数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 数字 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 0 | 1 | 2 |

现在, 问能否用一个数学函数来表示上述变换. $a \leftrightarrow a + 3 \bmod 26$

我们还可以构造变换

| 数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 数字 | 0 | 7 | 14 | 21 | 2 | 9 | 16 | 23 | 4 | 11 | 18 | 25 | 6 | 13 | 20 | 1 | 8 | 15 | 22 | 3 | 10 | 17 | 24 | 5 | 12 | 19 |

现在, 问能否用一个数学函数来表示上述变换. $a \leftrightarrow 7 \cdot a \bmod 26$

类似地, 我们可以构造一个数字变换

| 数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 数字 | 1 | 4 | 16 | 11 | 44 | 17 | 15 | 7 | 28 | 6 | 24 | 43 | 13 | 52 | 49 | 37 | 42 | 9 | 36 | 38 | 46 | 25 | 47 | 29 | 10 | 40 |

现在, 问能否用一个数学函数来表示上述变换.

$$a \leftrightarrow 4^a \bmod 53$$

同样, 构造一个数字变换

| 数字 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 数字 | 7 | 28 | 6 | 24 | 43 | 13 | 52 | 49 | 37 | 42 | 9 | 36 | 38 | 46 | 25 | 47 | 29 | 10 | 40 | 1 | 4 | 16 | 11 | 44 | 17 | 15 |

现在, 问能否用一个数学函数来表示上述变换.

$$a \leftrightarrow 7 * 4^a \bmod 53$$

**定义2.1.1** 给定正整数 $m$. 两个整数 $a$, $b$ 叫做模 $m$ **同余**, 如果 $a-b$ 被 $m$ 整除, 或

$$m \mid a-b,$$

记作

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

否则, 叫做模 $m$ **不同余**. 记作

$$a \not\equiv b \pmod{m}.$$

**注** 模 $m$ 是正整数, 在同余性质的讨论中为固定整数.

**例2.1.1** 我们有 $29 \equiv 1 \pmod{7}$, 因为 $7 \mid 29-1$.
同样, $27 \equiv 6 \pmod{7}$ 和 $23 \equiv -5 \pmod{7}$.
同余的概念常常出现于日常生活中. 例如, 时针是模 12 或 24 小时. 分针和秒针是模 60.

## 2.1.2 同余的判断

如何判断两个整数 $a,\ b$ 模 $m$ 同余呢?

直接运用同余的定义, 就必须作欧几里得除法, 即计算 $a-b$ 被模 $m$ 除的余数. 但这是一项冗长的工作. 因此, 我们引进一些等价的判别法, 以便更快捷地判断两个整数 $a,\ b$ 模 $m$ 是否同余.

首先, 通过整数 $a,\ b$ 的表达形式来判断整数 $a,\ b$ 模 $m$ 是否同余. 通过整数 $a,\ b$ 之间的关系式 $a=b+q\cdot m$ 来判断它们模 $m$ 是否同余.

# 由整数表达式来判断同余

**定理2.1.1** 设 $m$ 是正整数, 设 $a$, $b$ 是整数, 则 $a \equiv b \pmod{m}$ 的充要条件是存在一个整数 $q$ 使得

$$a = b + q \cdot m.$$

**证** 如果 $a \equiv b \pmod{m}$, 则根据同余的定义, 有 $m \mid a - b$. 又根据整除的定义, 存在整数 $q$ 使得 $a - b = q \cdot m$. 故

$$a = b + q \cdot m.$$

反过来, 如果存在整数 $q$ 使得 $a = b + q \cdot m$, 则有

$$a - b = q \cdot m.$$

根据整除的定义, 有 $m \mid a - b$. 再根据同余的定义, 得到 $a \equiv b \pmod{m}$.

**例2.1.2** 我们有 $39 \equiv 4 \pmod{7}$, 因为 $39 = 5 \cdot 7 + 4$.

# 由等价关系来判断同余

其次, 模同余具有一种叫做**等价关系** 的性质.

**定理2.1.2** 设 $m$ 是一个正整数, 则模 $m$ 同余是等价关系, 即

i). (自反性) 对任一整数 $a$, $a \equiv a \pmod{m}$;

ii). (对称性) 若 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$;

iii). (传递性) 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$,

则 $a \equiv c \pmod{m}$.

**证** 运用定理2.1.1 来给出证明.

1. (自反性) 对任一整数 $a$, 有 $a = a + 0 \cdot m$, 所以

$$a \equiv a \pmod{m};$$

2. (对称性) 若 $a \equiv b \pmod{m}$, 则存在整数 $q$ 使得

$$a = b + q \cdot m,$$

从而有 $b = a + (-q)m$. 因此, $b \equiv a \pmod{m}$;

3. (传递性) 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则分别存在整数 $q_1$, $q_2$ 使得

$$a = b + q_1 m, \qquad b = c + q_2 m,$$

从而

$$a = c + (q_1 + q_2)m.$$

因为 $q_1 + q_2$ 是整数, 所以$a \equiv c \pmod{m}$.

**例2.1.3** 因为 $39 \equiv 32 \pmod{7}$, $32 \equiv 25 \pmod{7}$, 所以

$39 \equiv 25 \pmod{7}$. 传递性

同时, 我们有

$39 \equiv 39 \pmod{7}$, $25 \equiv 25 \pmod{7}$, 自反性

以及

$32 \equiv 39 \pmod{7}$, $25 \equiv 32 \pmod{7}$. 对称性

第三, 运用整数 $a$, $b$ 模 $m$ 的余数, 可以判断 $a$, $b$ 模 $m$ 是否同余.

# 由最小非负余数来判断同余

**定理2.1.3** 设 $m$ 是一个正整数, 则整数 $a$, $b$ 模 $m$ 同余的充分必要条件是 $a$, $b$ 被 $m$ 除的余数相同.

**证** 根据欧几里得除法, 分别存在整数 $q$, $r$ 和 $q'$, $r'$ 使得

$$a = q \cdot m + r, \quad b = q' \cdot m + r', \quad 0 \leq r,\ r' < m.$$

两式相减, 得到 $a - b = (q - q')m + (r - r')$,

或者 $(r - r') = a - b - (q - q') \cdot m.$

因此, $m|a - b$ 的充分必要条件是 $m \mid r - r'$. 但因为

$$0 \leq |r - r'| < m,$$

且 $m \mid r - r'$ 的充分必要条件是 $r - r' = 0$, 所以 $m \mid a - b$ 的充分必要条件是 $r - r' = 0$. 这就是定理的结论, 证毕.

**例2.1.4** 我们有 $39 \equiv 25 \pmod 7$, 因为$39 = 5 \cdot 7 + 4, \quad 25 = 3 \cdot 7 + 4.$

# 由加法和乘法运算来判断同余

第四, 因为模同余是等价关系, 所以有整数 $a$, $b$ 模 $m$ 的加法运算和乘法运算性质, 并可运用这个性质来判断 $a$, $b$ 模 $m$ 是否同余.

**定理2.1.4** 设 $m$ 是正整数, 设 $a_1$, $a_2$, $b_1$, $b_2$ 是整数. 如果

$$a_1 \equiv b_1 \pmod{m}, \qquad a_2 \equiv b_2 \pmod{m},$$

则 (i) $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$;

(ii) $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$.

**证** 依题设, 根据定理2.1.1 , 分别存在整数 $q_1$, $q_2$ 使得

$$a_1 = b_1 + q_1 \cdot m, \quad a_2 = b_2 + q_2 \cdot m,$$

(i) 我们有 $a_1 + a_2 = b_1 + b_2 + (q_1 + q_2) \cdot m$. 因为 $q_1 + q_2$ 是整数, 所以有

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}.$$





(ii) 我们有

$$\begin{aligned} a_1 \cdot a_2 &= (b_1 + q_1 \cdot m)(b_2 + q_2 \cdot m) \\ &= b_1 \cdot b_2 + q_1 \cdot m \cdot b_2 + b_1 \cdot q_2 \cdot m + q_1 \cdot m \cdot q_2 \cdot m \\ &= b_1 \cdot b_2 + q_1 \cdot b_2 \cdot m + b_1 \cdot q_2 \cdot m + q_1 \cdot m \cdot q_2 \cdot m \\ &= b_1 \cdot b_2 + (q_1 \cdot b_2 + b_1 \cdot q_2 + q_1 \cdot m \cdot q_2)m \qquad (\text{交换性}) \end{aligned}$$

因为 $q_1 \cdot b_2 + b_1 \cdot q_2 + q_1 \cdot m \cdot q_2$ 是整数, 所以有

$$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

即定理成立.

**例2.1.5** 已知 $39 \equiv 4 \pmod 7$, $22 \equiv 1 \pmod 7$, 所以

$$\begin{aligned} 61 &= 39 + 22 \equiv 4 + 1 \equiv 5 \pmod 7, \\ 17 &= 39 - 22 \equiv 4 - 1 \equiv 3 \pmod 7, \\ 858 &= 39 \cdot 22 \equiv 4 \cdot 1 \equiv 4 \pmod 7, \\ 1521 &= 39^2 \equiv 4^2 \equiv 2 \pmod 7, \\ 484 &= 22^2 \equiv 1^2 \equiv 1 \pmod 7. \end{aligned}$$

**例2.1.6** 2003 年 5 月 9 日是星期五, 问第 $2^{2003}$ 天是星期几?

**解** 因为 $2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 = 8 \equiv 1 \pmod 7$,

又 $2003 = 667 \cdot 3 + 2$. 所以

$$2^{2003} = (2^3)^{667} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod 7.$$

故第 $2^{2003}$ 天是星期二.

**例2.1.6'** 2014 年05 月05日是星期一, 问第 $2^{20140505}$ 天是星期几?

**解** 因为 $2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 = 8 \equiv 1 \pmod 7$,

又 $20140505 = 6713501 \cdot 3 + 2$. 所以

$$2^{20140505} = (2^3)^{6713501} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4 \pmod 7.$$

故第 $2^{20140505}$ 天是星期五.

**定理2.1.5** 若 $x \equiv y \pmod{m}$, $a_i \equiv b_i \pmod{m}$, $0 \le i \le k$, 则

$$a_0 + a_1 x + \cdots + a_k x^k \equiv b_0 + b_1 y + \cdots + b_k y^k \pmod{m}.$$

**证** 设 $x \equiv y \pmod{m}$, 由定理2.1.4, 有

$$x^i \equiv y^i \pmod{m}, \quad 0 \le i \le k.$$

又 $a_i \equiv b_i \pmod{m}$, 有

$$a_i x^i \equiv b_i y^i \pmod{m}.$$

最后, 得到

$$a_0 + a_1 x + \cdots + a_k x^k \equiv b_0 + b_1 y + \cdots + b_k y^k \pmod{m}.$$

**定理2.1.6** 设 $n = a_k 10^k + \cdots + a_1 10 + a_0,\ 0 \le a_i < 10$. 则

$$3 \mid n \Leftrightarrow 3 \mid a_k + \cdots + a_0;$$

$$9 \mid n \Leftrightarrow 9 \mid a_k + \cdots + a_0.$$

**证** 因为 $10 \equiv 1 \pmod 3$, 又 $1^i = 1, \quad 0 \le i \le k$. 所以,

$$a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv a_k + \cdots + a_0 \pmod 3.$$

因此,

$$a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv 0 \pmod 3$$

的充分必要条件是

$$a_k + \cdots + a_0 \equiv 0 \pmod 3.$$

结论对于 $m = 3$ 成立.

**例2.1.7** 设 $n = 5874192$, 则 $3 \mid n,\ 9 \mid n$.

**解** 因为

$$a_k + \cdots + a_0 = 5 + 8 + 7 + 4 + 1 + 9 + 2 = 36,$$

又 $3 \mid 36,\ 9 \mid 36$, 故 $3 \mid n,\ 9 \mid n$.

**例2.1.8** 设 $n = 637693$, 则 $n$ 被 3 整除, 但不被 9 整除.

**解** 因为

$$a_k + \cdots + a_0 = 6 + 3 + 7 + 6 + 9 + 3 = 30 = 3 \cdot 10,$$

又 $3 \mid 3 \cdot 10,\ 9 \nmid 3 \cdot 10$, 故 $3 \mid n,\ 9 \nmid n$.

**定理2.1.7** 设 $n = a_k 1000^k + \cdots + a_1 1000 + a_0,\ \ 0 \le a_i < 1000.$ 则

$$7 \mid n \Leftrightarrow 7 \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$$

$$11 \mid n \Leftrightarrow 11 \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$$

$$13 \mid n \Leftrightarrow 13 \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$$

**证** 因为 $1000 = 7 \cdot 11 \cdot 13 - 1 \equiv -1 \pmod 7$, 所以有

$1000 \equiv 1000^3 \equiv \cdots \equiv -1 \pmod 7,$

$1000^2 \equiv 1000^4 \equiv \cdots \equiv 1 \pmod 7.$

进而,

$a_k 1000^k + a_{k-1} 1000^{k-1} + \cdots + a_1 1000 + a_0$

$\equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \pmod 7.$

因此, $7 \mid n \Leftrightarrow 7 \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$

即结论对于 $m = 7$ 成立.

同理, 结论对于 $m = 11$ 或 $m = 13$ 也成立.

**例2.1.9** 设 $n = 637693$, 则 $n$ 被 7 整除, 但不被 11, 13 整除.

**解** 因为 $n = 637 \cdot 1000 + 693$, 又

$$(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) = 693 - 637 = 56 = 7 \cdot 8.$$

所以 $n$ 被 7 整除, 但不被 11, 13 整除.

**例2.1.10** 设 $n = 75312289$, 则 $n$ 被 13 整除, 但不被 7, 11 整除.

**解** 因为 $n = 75 \cdot 1000^2 + 312 \cdot 1000 + 289$, 又

$$(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) = (289 + 75) - 312 = 52 = 13 \cdot 4.$$

所以 $n$ 被 13 整除, 但不被 7, 11 整除.

## 2.1.3 同余的性质

下面, 我们进一步讨论同余的性质.

**定理2.1.8** 设 $d \cdot a \equiv d \cdot b \pmod{m}$. 若 $(d, m) = 1$, 则

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

**证** 若 $d \cdot a \equiv d \cdot b \pmod{m}$, 则

$m \mid d \cdot a - d \cdot b$, 或 $m \mid d \cdot (a - b)$.

因为 $(d, m) = 1$, 所以 $m \mid a - b$. 结论成立. 证毕.

**例2.1.11** 因为 $95 \equiv 25 \pmod{7}$, $(5, 7) = 1$, 所以

$$19 \equiv 5 \pmod{7}.$$

**定理2.1.9** 设$m$ 是一个正整数, 设$a \equiv b \pmod{m},\ d > 0$, 则

$$d \cdot a \equiv d \cdot b \pmod{d \cdot m}.$$

**证** 设$a \equiv b \pmod{m}$, 由定理2.1.1, 存在整数$q$, 使得

$$a = b + q \cdot m$$

进而,

$$d \cdot a = d \cdot b + q \cdot (d \cdot m)$$

因此,

$$d \cdot a \equiv d \cdot b \pmod{d \cdot m}.$$

证毕

**例2.1.12** 因为$19 \equiv 5 \pmod{7},\ d = 4 > 0$, 所以$76 \equiv 20 \pmod{28}$.

**定理2.1.10** 设 $a \equiv b \pmod{m}$. 若 $d \mid (a, b, m)$, 则

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

**证** 设 $d \mid (a, b, m)$, 则 $a = a' \cdot d, \quad b = b' \cdot d, \quad m = m' \cdot d.$

又 $a \equiv b \pmod{m}$, 有整数$q$ 使得 $a = b + q \cdot m$, 即

$$a' \cdot d = b' \cdot d + q \cdot m' \cdot d.$$

故 $a' = b' + q \cdot m'$. 或 $a' \equiv b' \pmod{m'}$ 或者

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

**例2.1.13** 因为 $190 \equiv 50 \pmod{70}$, 所以取 $d = 10$, 得到

$$19 \equiv 5 \pmod{7}.$$

**定理2.1.11** 设 $a \equiv b \pmod{m}$. 如果 $d \mid m$, 则

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

**证** 因为$d \mid m$, 所以存在整数$q_1$ 使得 $m = q_1 \cdot d$.
又因为$a \equiv b \pmod{m}$, 所以存在整数$q_2$ 使得

$$a = b + q_2 \cdot m.$$

该式又可写成

$$a = b + (q_2 \cdot q_1) \cdot d.$$

故

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

**例2.1.14** 因为$190 \equiv 50 \pmod{70}$, 所以取$d = 7$, 得到

$$190 \equiv 50 \pmod{7}.$$

**定理2.1.12** 设 $a \equiv b \pmod{m_i},\ i = 1, \ldots, k$, 则

$$a \equiv b \pmod{[m_1, \ldots, m_k]}.$$

**证** 设 $a \equiv b \pmod{m_i}$, 则

$$m_i \mid a - b.$$

进而

$$[m_1, \ldots, m_k] \mid a - b.$$

即

$$a \equiv b \pmod{[m_1, \ldots, m_k]}.$$

**例2.1.15** 因 $190 \equiv 50 \pmod{7},\ 190 \equiv 50 \pmod{10}$ , 故

$$190 \equiv 50 \pmod{70}.$$

**例2.1.16** 设 $p, q$ 是不同素数. 若 $a, b$ 满足 $\begin{cases} a \equiv b \pmod{p}, \\ a \equiv b \pmod{q}, \end{cases}$

则 $a \equiv b \pmod{p \cdot q}$.

**证** 设

$$\begin{cases} a \equiv b \pmod{p}, \\ a \equiv b \pmod{q}, \end{cases}$$

则 $p \mid a-b, \quad q \mid a-b$. 因此,

$$[p, q] \mid a-b.$$

因为 $p,\ q$ 是不同的素数, 所以 $p \cdot q \mid a-b$. 即 $a \equiv b \pmod{p \cdot q}$.

**定理2.1.13** 设 $a \equiv b \pmod{m}$, 则

$$(a, m) = (b, m).$$

**证** 设 $a \equiv b \pmod{m}$, 则存在整数 $q$ 使得

$$a = b + q \cdot m.$$

根据定理1.3.3, 我们有 $(a, m) = (b, m)$.

**例2.1.17** 设 $m,\ n,\ a$ 都是正整数. 如果

$$n^a \not\equiv 0, 1 \pmod{m},$$

则存在 $n$ 的一个素因数 $p$ 使得

$$p^a \not\equiv 0, 1 \pmod{m},$$

**证** 反证法. 如果存在 $n$ 的一个素因数 $p$, 使得 $p^a \equiv 0 \pmod{m}$, 则 $m \mid p^a$. 但 $p^a \mid n^a$, 故 $m \mid n^a$. 即 $n^a \equiv 0 \pmod{m}$. 这与假设矛盾. 如果对 $n$ 的每个素因数 $p$, 都有

$$p^a \equiv 1 \pmod{m}.$$

根据定理2.1.4 ii), 我们有

$$n^a \equiv 1 \pmod{m}.$$

这也与假设矛盾. 因此, 结论成立. 证毕