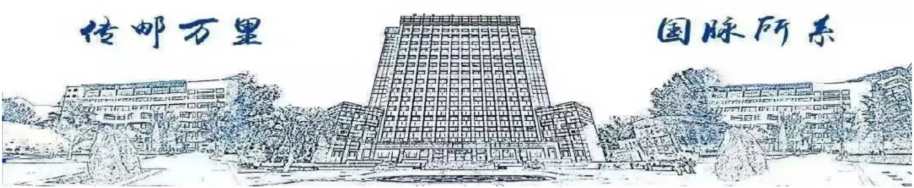
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

—— 同余 (2)

信数课题组

北京邮电大学



上次课回顾

- **同余**
  - **判断(等价条件)**
    - $a \equiv b \bmod m \Leftrightarrow a = b + q \cdot m$
    - a, b 被 m 除的余数相等
  - **基本性质**
    - 同余是等价关系
    - 加法、乘法、方幂的线性组合下保持同余关系
      - 简化计算
      - 十进制整数被 3、9 整除的判定
      - 千进制整数被 7、11、13 整除的判定
    - 同时约除与模互素的因子后保持同余关系
    - 同乘同余整数和模后保持新模下的同余关系
    - 同时约除同余整数和模的公因子后保持新模下的同余关系
    - 仅约除模的因子后保持新模下的同余关系
    - $a \equiv b \mod [m_1, \cdots, m_k]$
    - $a \equiv b \mod m$, 则 $(a, m) = (b, m)$
  - **剩余及剩余类**
    - **完全剩余系**
      - $\{ax+b\}$ 仍是完全剩余系
      - 最小非负完全剩余系
      - 最小正完全剩余系
      - 最大非正完全剩余系
      - 最大负完全剩余系
      - 绝对值最小完全剩余系
      - 两个模的完全剩余系：$m_2 \cdot x_1 + m_1 \cdot x_2$　其中　m_1, m_2　互素

目录

目录

定义 2.2.4

设 m 是一个正整数，则 m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数的个数，记作 $\varphi(m)$，通常叫做 **欧拉** (Euler) **函数**.

定义 2.2.4

设 m 是一个正整数，则 m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数的个数，记作 $\varphi(m)$，通常叫做 **欧拉** (Euler) **函数**.

莱昂哈德 · 欧拉

(Leonhard Euler, 1707.4.15 — 1783.9.18)

瑞士数学家、自然科学家. 18 世纪数学界最杰出的人物之一，是数学史上最多产的数学家，写下了浩如烟海的书籍和论文，其中《无穷小分析引论》、《微分学原理》、《积分学原理》等都是数学界的经典著作. 几乎在每一个数学领域都可以看到欧拉的名字，如初等几何的欧拉线，多面体的欧拉定理，立体解析几何的欧拉变换公式，四次方程的欧拉解法，数论中的欧拉函数，微分方程的欧拉方程，级数论的欧拉常数，变分学的欧拉方程，复变函数的欧拉公式等等. 欧拉还创造了一批数学符号，如 $f(x), \pi, e, \sin, \cos, \mathrm{ty}, \Sigma, \Delta x, i$ 等.

定义 2.2.4

设 m 是一个正整数，则 m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数的个数，记作 $\varphi(m)$，通常叫做 **欧拉** (Euler) **函数**.

莱昂哈德 · 欧拉

(Leonhard Euler, 1707.4.15 — 1783.9.18)

瑞士数学家、自然科学家. 18 世纪数学界最杰出的人物之一，是数学史上最多产的数学家，写下了浩如烟海的书籍和论文，其中《无穷小分析引论》、《微分学原理》、《积分学原理》等都是数学界的经典著作. 几乎在每一个数学领域都可以看到欧拉的名字，如初等几何的欧拉线，多面体的欧拉定理，立体解析几何的欧拉变换公式，四次方程的欧拉解法，数论中的欧拉函数，微分方程的欧拉方程，级数论的欧拉常数，变分学的欧拉方程，复变函数的欧拉公式等等. 欧拉还创造了一批数学符号，如 $f(x)$, π, e, sin, cos, ty, Σ, Δx, i 等.

例 2.2.5　设 $m = p$ 是素数，则 p 个整数 $1, 2, \cdots, p-1$ 中与 p 互素的整数为 $1, 2, \cdots, p-1$，所以 $\varphi(p) = p - 1$.

定理 2.2.5

对于素数幂 $n = p^\alpha$, 有 $\varphi(n) = p^\alpha - p^{\alpha-1}$.

定理 2.2.5

对于素数幂 $n = p^\alpha$, 有 $\varphi(n) = p^\alpha - p^{\alpha-1}$.

证：对于素数幂 $n = p^\alpha$, 从 1 到 n 的 n 个整数的形式为

$$\begin{array}{rcrr}
1, & \cdots, & p-1, & 1\cdot p, \\
p+1, & \cdots, & p+p-1, & 2\cdot p, \\
2\cdot p+1, & \cdots, & 2\cdot p+p-1, & 3\cdot p, \\
& \vdots & & \\
(p^{\alpha-1}-1)\cdot p+1, & \cdots, & (p^{\alpha-1}-1)\cdot p+p-1, & p^{\alpha-1}\cdot p.
\end{array}$$

其中与 n 不互素的整数为 $1\cdot p,\ 2\cdot p,\ \cdots,\ (p^{\alpha-1}-1)\cdot p,\ p^{\alpha-1}\cdot p$, 共有 $p^{\alpha-1}$ 个整数. 因此, n 个整数中与 n 互素的整数个数为 $p^\alpha - p^{\alpha-1}$, 即证.

定理 2.2.5

对于素数幂 $n=p^\alpha$, 有 $\varphi(n)=p^\alpha-p^{\alpha-1}$.

证：对于素数幂 $n=p^\alpha$, 从 1 到 n 的 n 个整数的形式为

$$\begin{array}{rcrr}
1, & \cdots, & p-1, & 1\cdot p, \\
p+1, & \cdots, & p+p-1, & 2\cdot p, \\
2\cdot p+1, & \cdots, & 2\cdot p+p-1, & 3\cdot p, \\
 & \vdots & & \\
(p^{\alpha-1}-1)\cdot p+1, & \cdots, & (p^{\alpha-1}-1)\cdot p+p-1, & p^{\alpha-1}\cdot p.
\end{array}$$

其中与 n 不互素的整数为 $1\cdot p,\ 2\cdot p,\ \cdots,\ (p^{\alpha-1}-1)\cdot p,\ p^{\alpha-1}\cdot p$, 共有 $p^{\alpha-1}$ 个整数. 因此, n 个整数中与 n 互素的整数个数为 $p^\alpha-p^{\alpha-1}$, 即证.

例 2.2.6 设 $m=7^3$, 则 m 的欧拉函数值为 294.

定义 2.2.5

设 m 是一个正整数，如果一个模 m 的剩余类中存在一个与 m 互素的剩余，就称这个模 m 的剩余类为 **简化剩余类**.

定义 2.2.5

设 m 是一个正整数，如果一个模 m 的剩余类中存在一个与 m 互素的剩余，就称这个模 m 的剩余类为 **简化剩余类**.

注：简化剩余类的这个定义与剩余的选取无关.

定理 2.2.6

设 r_1, r_2 是同一模 m 剩余类的两个剩余，则 r_1 与 m 互素的充要条件是 r_2 与 m 互素.

定义 2.2.5

设 m 是一个正整数，如果一个模 m 的剩余类中存在一个与 m 互素的剩余，就称这个模 m 的剩余类为 **简化剩余类**.

注：简化剩余类的这个定义与剩余的选取无关.

定理 2.2.6

设 r_1, r_2 是同一模 m 剩余类的两个剩余，则 r_1 与 m 互素的充要条件是 r_2 与 m 互素.

证：依题设，存在整数 k，使得 $r_1 = r_2 + k \cdot m$. 根据定理 1.2.2, $(r_1, m) = (r_2, m)$. 故 $(r_1, m) = 1$ 的充要条件是 $(r_2, m) = 1$.

定义 2.2.5

设 m 是一个正整数，如果一个模 m 的剩余类中存在一个与 m 互素的剩余，就称这个模 m 的剩余类为 **简化剩余类**.

注：简化剩余类的这个定义与剩余的选取无关.

定理 2.2.6

设 r_1, r_2 是同一模 m 剩余类的两个剩余，则 r_1 与 m 互素的充要条件是 r_2 与 m 互素.

证：依题设，存在整数 k，使得 $r_1 = r_2 + k \cdot m$. 根据定理 1.2.2, $(r_1, m) = (r_2, m)$. 故 $(r_1, m) = 1$ 的充要条件是 $(r_2, m) = 1$.

定义 2.2.6

设 m 是一个正整数，在模 m 的所有不同简化剩余类中，从每个类任取一个数组成的整数的集合，叫做模 m 的一个**简化剩余系**.

定义 2.2.5

设 m 是一个正整数，如果一个模 m 的剩余类中存在一个与 m 互素的剩余，就称这个模 m 的剩余类为 **简化剩余类**.

注：简化剩余类的这个定义与剩余的选取无关.

定理 2.2.6

设 r_1, r_2 是同一模 m 剩余类的两个剩余，则 r_1 与 m 互素的充要条件是 r_2 与 m 互素.

证：依题设，存在整数 k，使得 $r_1 = r_2 + k \cdot m$. 根据定理 1.2.2, $(r_1, m) = (r_2, m)$. 故 $(r_1, m) = 1$ 的充要条件是 $(r_2, m) = 1$.

定义 2.2.6

设 m 是一个正整数，在模 m 的所有不同简化剩余类中，从每个类任取一个数组成的整数的集合，叫做模 m 的一个**简化剩余系**.

注：由定义可知，模 m 的一个简化剩余系的元素个数为 $\varphi(m)$.

定义 2.2.7

设 m 是一个正整数，则

(i) m 个整数 $0, 1, \cdots, m-1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小非负简化剩余系**.

定义 2.2.7

设 m 是一个正整数，则

(i) m 个整数 $0, 1, \cdots, m-1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小非负简化剩余系**.

(ii) m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小正简化剩余系**.

定义 2.2.7

设 m 是一个正整数，则

(i) m 个整数 $0, 1, \cdots, m-1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小非负简化剩余系**.

(ii) m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小正简化剩余系**.

(iii) m 个整数 $-(m-1), \cdots, -1, 0$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最大非正简化剩余系**.

定义 2.2.7

设 m 是一个正整数，则

(i) m 个整数 $0, 1, \cdots, m-1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小非负简化剩余系**.

(ii) m 个整数 $1, \cdots, m-1, m$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小正简化剩余系**.

(iii) m 个整数 $-(m-1), \cdots, -1, 0$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最大非正简化剩余系**.

(iv) m 个整数 $-m, -(m-1), \cdots, -1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最大负简化剩余系**.

定义 2.2.7 (续)

(v) 当 m 为偶数时, m 个整数

$$-\frac{m}{2}, -\frac{m-2}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-2}{2}$$

或 m 个整数

$$-\frac{m-2}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-2}{2}, \frac{m}{2}$$

中与 m 互素的整数全体组成模 m 的一个简化剩余系;

当 m 为奇数时, m 个整数

$$-\frac{m-1}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-1}{2}$$

中与 m 互素的整数全体组成模 m 的一个简化剩余系.

上述两个简化剩余系统称为模 m 的一个**绝对值最小简化剩余系**.

例 2.2.7 $1, 7, 11, 13, 17, 19, 23, 29$ 是模 30 的简化剩余系, $\varphi(30) = 8$.

例 2.2.7 　$1, 7, 11, 13, 17, 19, 23, 29$ 是模 30 的简化剩余系, $\varphi(30) = 8$.

例 2.2.8 　$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ 是模 13 的简化剩余系, $\varphi(13) = 12$.

注：当 $m = p$ 是素数时, $1, 2, \cdots, p-1$ 是模 p 的简化剩余系, 所以 $\varphi(p) = p - 1$.

例 2.2.7 $1, 7, 11, 13, 17, 19, 23, 29$ 是模 30 的简化剩余系, $\varphi(30) = 8$.

例 2.2.8 $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ 是模 13 的简化剩余系, $\varphi(13) = 12$.

注：当 $m = p$ 是素数时, $1, 2, \cdots, p-1$ 是模 p 的简化剩余系, 所以 $\varphi(p) = p - 1$.

定理 2.2.7

设 m 是一个正整数, 若 $r_1, \cdots, r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数, 并且两两模 m 不同余, 则 $r_1, \cdots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

例 2.2.7 $1, 7, 11, 13, 17, 19, 23, 29$ 是模 30 的简化剩余系, $\varphi(30) = 8$.

例 2.2.8 $1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$ 是模 13 的简化剩余系, $\varphi(13) = 12$.

注：当 $m = p$ 是素数时, $1, 2, \cdots, p-1$ 是模 p 的简化剩余系, 所以 $\varphi(p) = p - 1$.

定理 2.2.7

设 m 是一个正整数, 若 $r_1, \cdots, r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数, 并且两两模 m 不同余, 则 $r_1, \cdots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

证：根据题设及定理 2.2.1 知, $\varphi(m)$ 个整数 $r_1, \cdots, r_{\varphi(m)}$ 是模 m 的所有不同简化剩余类的剩余. 因此, $r_1, \cdots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

定理 2.2.8

设 m 是一个正整数，a 是满足 $(a,m)=1$ 的整数．如果 x 遍历模 m 的一个简化剩余系，则 $a\cdot x$ 也遍历模 m 的一个简化剩余系．

定理 2.2.8

设 m 是一个正整数, a 是满足 $(a, m) = 1$ 的整数. 如果 x 遍历模 m 的一个简化剩余系, 则 $a \cdot x$ 也遍历模 m 的一个简化剩余系.

证：因为 $(a, m) = 1, (x, m) = 1$, 根据推论 1.2.1, 有 $(a \cdot x, m) = 1$. 这说明 $a \cdot x$ 是简化剩余类的剩余.

又 $a \cdot x_1 \equiv a \cdot x_2 \pmod m$ 时, 有 $x_1 \equiv x_2 \pmod m$.

因此, x 遍历模 m 的一个简化剩余系时, $a \cdot x$ 遍历 $\varphi(m)$ 个数, 且它们两两模 m 不同余. 根据定理 2.2.7, $a \cdot x$ 遍历模 m 的一个简化剩余系.

定理 2.2.8

设 m 是一个正整数, a 是满足 $(a,m)=1$ 的整数. 如果 x 遍历模 m 的一个简化剩余系, 则 $a\cdot x$ 也遍历模 m 的一个简化剩余系.

证：因为 $(a,m)=1,(x,m)=1$, 根据推论 1.2.1, 有 $(a\cdot x,m)=1$. 这说明 $a\cdot x$ 是简化剩余类的剩余.

又 $a\cdot x_1\equiv a\cdot x_2 \mod m$ 时, 有 $x_1\equiv x_2 \mod m$.

因此, x 遍历模 m 的一个简化剩余系时, $a\cdot x$ 遍历 $\varphi(m)$ 个数, 且它们两两模 m 不同余. 根据定理 2.2.7, $a\cdot x$ 遍历模 m 的一个简化剩余系.

例 2.2.9　$1,7,11,13,17,19,23,29$ 是模 30 的简化剩余系, $(7,30)=1$, 则

$$\begin{aligned}
&7\cdot 1\equiv 7, && 7\cdot 7\equiv 49\equiv 19, && 7\cdot 11\equiv 77\equiv 17\\
&7\cdot 13\equiv 91\equiv 1, && 7\cdot 17\equiv 119\equiv 29, && 7\cdot 19\equiv 133\equiv 13\\
&7\cdot 23\equiv 161\equiv 11, && 7\cdot 29\equiv 203\equiv 23 \mod 30.
\end{aligned}$$

故 $7\cdot 1,7\cdot 7,7\cdot 11,7\cdot 13,7\cdot 17,7\cdot 19,7\cdot 23,7\cdot 29$ 是模 30 的简化剩余系.

例 2.2.9 设 $m=7$, a 表示第一列数, 为与 m 互素的给定数. x 表示第一行数, 遍历模 m 的简化剩余系. a 所在行与 x 所在列的交叉位置表示 ax 模 m 最小非负剩余. 则我们得到如下的列表：

ax \ x / a	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

其中 a 所在行的数表示 ax 随 x 遍历模 m 的简化剩余系.

定理 2.2.9

设 m 是一个正整数，a 是满足 $(a,m)=1$ 的整数，则存在唯一的整数 a'，$1 \leqslant a' < m$ 使得 $a \cdot a' \equiv 1 \mod m$.

定理 2.2.9

设 m 是一个正整数，a 是满足 $(a, m) = 1$ 的整数，则存在唯一的整数 a'，$1 \leqslant a' < m$ 使得 $a \cdot a' \equiv 1 \mod m$.

证一：(存在性证明).

因为 $(a, m) = 1$，根据定理 2.2.8，x 遍历模 m 的一个简化剩余系时，$a \cdot x$ 也遍历模 m 的一个简化剩余系.

因此，存在整数 $x = a'$，$1 \leqslant a' < m$ 使得 $a \cdot a'$ 属于 1 的剩余类，即 $a \cdot a' \equiv 1 \mod m$.

定理 2.2.9

设 m 是一个正整数，a 是满足 $(a,m)=1$ 的整数，则存在唯一的整数 a'，$1\leqslant a'<m$ 使得 $a\cdot a'\equiv 1 \mod m$.

证一：(存在性证明).

因为 $(a,m)=1$，根据定理 2.2.8，x 遍历模 m 的一个简化剩余系时，$a\cdot x$ 也遍历模 m 的一个简化剩余系.

因此，存在整数 $x=a'$，$1\leqslant a'<m$ 使得 $a\cdot a'$ 属于 1 的剩余类，即 $a\cdot a'\equiv 1 \mod m$.

证二：(构造性证明).

因为 $(a,m)=1$，运用广义欧几里得除法，可找到整数 s,t 使得

$$s\cdot a+t\cdot m=(a,m)=1.$$

因此，整数 $a'=s \mod m$ 即为所求.

例 2.2.11　设 $m=7$, a 表示与 m 互素的整数. 根据定理 2.2.9, 得到:

$$1\cdot 1\equiv 1,\ \ 2\cdot 4\equiv 1,\ \ 3\cdot 5\equiv 1 \mod 7,$$

$$4\cdot 2\equiv 1,\ \ 5\cdot 3\equiv 1,\ \ 6\cdot 6\equiv 1 \mod 7.$$

例 2.2.11 设 $m = 7$, a 表示与 m 互素的整数. 根据定理 2.2.9, 得到:

$$1 \cdot 1 \equiv 1,\ \ 2 \cdot 4 \equiv 1,\ \ 3 \cdot 5 \equiv 1 \mod 7,$$

$$4 \cdot 2 \equiv 1,\ \ 5 \cdot 3 \equiv 1,\ \ 6 \cdot 6 \equiv 1 \mod 7.$$

例 2.2.12 设 $m = 65521, a = 32749$.

由广义欧几里德除法, 可找到整数 $s = 11391, t = -22790$ 使得 $11391 \cdot 65521 - 22790 \cdot 32749 = 1$.

因此, $a' = -22790 \equiv 42731 \mod 65521$ 使得 $42731 \cdot 32749 \equiv 1 \mod 65521$.

定理 2.3.6

设 m_1, m_2 是互素的两个正整数. 如果 x_1, x_2 分别遍历模 m_1 和模 m_2 的简化剩余系，则 $m_2 \cdot x_1 + m_1 \cdot x_2$ 遍历模 $m_1 \cdot m_2$ 的简化剩余系.

定理 2.3.6

设 m_1, m_2 是互素的两个正整数. 如果 x_1, x_2 分别遍历模 m_1 和模 m_2 的简化剩余系, 则 $m_2 \cdot x_1 + m_1 \cdot x_2$ 遍历模 $m_1 \cdot m_2$ 的简化剩余系.

证：首先证明 $(x_1, m_1) = 1, (x_2, m_2) = 1$ 时,

$$(m_2 \cdot x_1 + m_1 \cdot x_2, m_1 \cdot m_2) = 1.$$

定理 2.3.6

设 m_1, m_2 是互素的两个正整数. 如果 x_1, x_2 分别遍历模 m_1 和模 m_2 的简化剩余系, 则 $m_2 \cdot x_1 + m_1 \cdot x_2$ 遍历模 $m_1 \cdot m_2$ 的简化剩余系.

证：首先证明 $(x_1, m_1) = 1, (x_2, m_2) = 1$ 时,

$$(m_2 \cdot x_1 + m_1 \cdot x_2, m_1 \cdot m_2) = 1.$$

事实上, 因为 $(m_1, m_2) = 1$, 根据定理 1.2.2 和定理 1.2.8, 有

$$(m_2 \cdot x_1 + m_1 \cdot x_2, m_1) = (m_2 \cdot x_1, m_1) = (x_1, m_1) = 1,$$

$$(m_2 \cdot x_1 + m_1 \cdot x_2, m_2) = (m_1 \cdot x_2, m_2) = (x_2, m_2) = 1.$$

因此, 再根据推论 1.2.1, 可得到

$$(m_2 \cdot x_1 + m_1 \cdot x_2, m_1 \cdot m_2) = 1.$$

其次, 证明模 $m_1 \cdot m_2$ 的任一简化剩余可表示为

$$m_2 \cdot x_1 + m_1 \cdot x_2,$$

其中 $(x_1, m_1) = 1, (x_2, m_2) = 1.$

其次, 证明模 $m_1 \cdot m_2$ 的任一简化剩余可表示为

$$m_2 \cdot x_1 + m_1 \cdot x_2,$$

其中 $(x_1, m_1) = 1, (x_2, m_2) = 1$.

事实上, 根据定理 2.2.4, 模 $m_1 \cdot m_2$ 的任一剩余可以表示为 $m_2 \cdot x_1 + m_1 \cdot x_2$.

而当 $(m_2 \cdot x_1 + m_1 \cdot x_2, m_1 \cdot m_2) = 1$ 时, 有

$$(x_1, m_1) = (m_2 \cdot x_1, m_1) = (m_2 \cdot x_1 + m_1 \cdot x_2, m_1) = 1.$$

同理, $(x_2, m_2) = 1$.

故结论成立.

从定理 2.2.10 我们可以推出欧拉函数 φ 的性质（即 φ 是所谓的乘性函数）.

定理 2.2.11

设 m, n 是互素的两个正整数，则 $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

从定理 2.2.10 我们可以推出欧拉函数 φ 的性质（即 φ 是所谓的乘性函数）.

定理 2.2.11

设 m, n 是互素的两个正整数, 则 $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

证：根据定理 2.2.10, 当 x 遍历模 m 的简化剩余系, 共 $\varphi(m)$ 个整数, 以及 y 遍历模 n 的简化剩余系, 共 $\varphi(n)$ 个整数时, $n \cdot x + m \cdot y$ 遍历模 $m \cdot n$ 的简化剩余系, 其整数个数为 $\varphi(m) \cdot \varphi(n)$. 但模 $m \cdot n$ 的简化剩余系的元素个数又为 $\varphi(m \cdot n)$, 故 $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

从定理 2.2.10 我们可以推出欧拉函数 φ 的性质（即 φ 是所谓的乘性函数）.

定理 2.2.11

设 m, n 是互素的两个正整数, 则 $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

证：根据定理 2.2.10, 当 x 遍历模 m 的简化剩余系, 共 $\varphi(m)$ 个整数, 以及 y 遍历模 n 的简化剩余系, 共 $\varphi(n)$ 个整数时, $n \cdot x + m \cdot y$ 遍历模 $m \cdot n$ 的简化剩余系, 其整数个数为 $\varphi(m) \cdot \varphi(n)$. 但模 $m \cdot n$ 的简化剩余系的元素个数又为 $\varphi(m \cdot n)$, 故 $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

例 2.2.13 $\varphi(143) = \varphi(11)\varphi(13) = 10 \cdot 12 = 120.$

$\varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 2 \cdot 4 \cdot 6 = 48.$

下面给出欧拉函数的计算公式.

定理 2.2.12

设正整数 n 的标准因数分解式

$$n = \prod_{p \mid m} p^{\alpha} = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

则

$$\varphi(n) = n \prod_{p \mid m} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

下面给出欧拉函数的计算公式.

定理 2.2.12

设正整数 n 的标准因数分解式

$$n = \prod_{p \mid m} p^{\alpha} = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

则

$$\varphi(n) = n \prod_{p \mid m} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

证：由欧拉函数的可乘性, 有

$$\begin{aligned}\varphi(n) &= \prod_{p \mid n} \varphi(p^{\alpha}) = \prod_{p \mid n} (p^{\alpha} - p^{\alpha-1}) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

下面给出欧拉函数的计算公式.

定理 2.2.12

设正整数 n 的标准因数分解式

$$n = \prod_{p \mid m} p^{\alpha} = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

则

$$\varphi(n) = n \prod_{p \mid m} \left(1 - \frac{1}{p}\right) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

证：由欧拉函数的可乘性, 有

$$\begin{aligned}\varphi(n) &= \prod_{p \mid n} \varphi(p^{\alpha}) = \prod_{p \mid n} (p^{\alpha} - p^{\alpha-1}) \\ &= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

注 1：设 p, q 是不同的素数, 则 $\varphi(p \cdot q) = p \cdot q - p - q + 1$.

注 1：设 p, q 是不同的素数, 则 $\varphi(p \cdot q) = p \cdot q - p - q + 1$.

注 2：当 n 为合数, 且不知道 n 的因数分解式时, 通常很难求出 n 的欧拉函数值 $\varphi(n)$.

注 1：设 p, q 是不同的素数, 则 $\varphi(p \cdot q) = p \cdot q - p - q + 1$.

注 2：当 n 为合数, 且不知道 n 的因数分解式时, 通常很难求出 n 的欧拉函数值 $\varphi(n)$.

例 2.2.14　设正整数 n 是两个不同素数的乘积. 如果知道 n 和欧拉函数值 $\varphi(n)$, 则可以求出 n 的因数分解式.

注 1：设 p, q 是不同的素数，则 $\varphi(p \cdot q) = p \cdot q - p - q + 1$.

注 2：当 n 为合数，且不知道 n 的因数分解式时，通常很难求出 n 的欧拉函数值 $\varphi(n)$.

例 2.2.14　设正整数 n 是两个不同素数的乘积. 如果知道 n 和欧拉函数值 $\varphi(n)$，则可以求出 n 的因数分解式.

证：考虑未知数 p, q 的方程组

$$\begin{cases} p + q = n + 1 + \varphi(n) \\ p \cdot q = n \end{cases}$$

根据多项式的根与系数之间的关系，我们可以从二次方程

$$z^2 - (n + 1 - \varphi(n))z + n = 0$$

求出 n 的因数 p, q.

目录

在实际应用中, 经常要考虑模幂运算, 即 $a^k \mod m$.

例 2.2.15 设 $m = 7, a = 2$. 有 $(2,7) = 1, \varphi(7) = 6$. 考虑模 7 的最小非负简化剩余系 $x = 1,2,3,4,5,6$, 我们有 $2x =$

$$2 \cdot 1 \equiv 2, \quad 2 \cdot 2 \equiv 4, \quad 2 \cdot 3 \equiv 6,$$

$$2 \cdot 4 \equiv 1, \quad 2 \cdot 5 \equiv 3, \quad 2 \cdot 6 \equiv 5 \mod 7.$$

在实际应用中, 经常要考虑模幂运算, 即 $a^k \mod m$.

例 2.2.15 设 $m = 7, a = 2$. 有 $(2,7) = 1, \varphi(7) = 6$. 考虑模 7 的最小非负简化剩余系 $x = 1,2,3,4,5,6$, 我们有 $2x =$

$$2\cdot 1 \equiv 2,\quad 2\cdot 2 \equiv 4,\quad 2\cdot 3 \equiv 6,$$

$$2\cdot 4 \equiv 1,\quad 2\cdot 5 \equiv 3,\quad 2\cdot 6 \equiv 5 \mod 7.$$

上述式子左右对应相乘, 得到

$$(2\cdot 1)(2\cdot 2)(2\cdot 3)(2\cdot 4)(2\cdot 5)(2\cdot 6) \equiv 2\cdot 4\cdot 6\cdot 1\cdot 3\cdot 5 \pmod 7$$

或

$$2^6\cdot 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \pmod 7.$$

注意到 $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \equiv (1\cdot 6)(2\cdot 4)(3\cdot 5) \equiv (-1)\cdot 1\cdot 1 \equiv -1 \mod 7$, 故 $2^6 \equiv 1 \mod 7$.

例 2.2.16 设 $m=30, a=7$. 有 $(7,30)=1, \varphi(30)=8$. 考虑模 30 的最小非负简化剩余系 $x=1,7,11,13,17,19,23,29$, 我们有 $7x=$

$$
\begin{aligned}
&7\cdot 1\equiv 7, && 7\cdot 7\equiv 49\equiv 19, && 7\cdot 11\equiv 77\equiv 17,\\
&7\cdot 13\equiv 91\equiv 1, && 7\cdot 17\equiv 119\equiv 29, && 7\cdot 19\equiv 133\equiv 13,\\
&7\cdot 23\equiv 161\equiv 11, && 7\cdot 29\equiv 203\equiv 23 \mod 30.
\end{aligned}
$$

例 2.2.16　设 $m = 30, a = 7$. 有 $(7, 30) = 1, \varphi(30) = 8$. 考虑模 30 的最小非负简化剩余系 $x = 1, 7, 11, 13, 17, 19, 23, 29$, 我们有 $7x =$

$$\begin{aligned} 7\cdot 1 &\equiv 7, & 7\cdot 7 &\equiv 49 \equiv 19, & 7\cdot 11 &\equiv 77 \equiv 17, \\ 7\cdot 13 &\equiv 91 \equiv 1, & 7\cdot 17 &\equiv 119 \equiv 29, & 7\cdot 19 &\equiv 133 \equiv 13, \\ 7\cdot 23 &\equiv 161 \equiv 11, & 7\cdot 29 &\equiv 203 \equiv 23 \pmod{30}. \end{aligned}$$

上述式子左右对应相乘, 得到

$$(7\cdot 1)(7\cdot 7)(7\cdot 11)(7\cdot 13)(7\cdot 17)(7\cdot 19\cdot 23\cdot 29) \equiv 7\cdot 19\cdot 17\cdot 1\cdot 29\cdot 13\cdot 11\cdot 23 \pmod{30}$$

或

$$7^8\cdot 1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29 \equiv 1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29 \pmod{30}.$$

注意到 $(1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29, 30) = 1$, 故 $7^8 \equiv 1 \pmod{30}$.

如上例题可推广为一般的结论，即欧拉（Euler）定理.

定理 2.2.13 (欧拉定理)

设 m 是大于 1 的整数. 如果 a 是满足 $(a,m)=1$ 的整数，则

$$a^{\varphi(m)} \equiv 1 \mod m.$$

如上例题可推广为一般的结论, 即欧拉（Euler）定理.

定理 2.2.13 (欧拉定理)

设 m 是大于 1 的整数. 如果 a 是满足 $(a, m) = 1$ 的整数, 则

$$a^{\varphi(m)} \equiv 1 \mod m.$$

证：取 $r_1, \cdots, r_{\varphi(m)}$ 为模 m 的一个最小正简化剩余系, 则当 a 是满足 $(a, m) = 1$ 的整数时, 根据定理 2.2.8, $a \cdot r_1, \cdots, a \cdot r_{\varphi(m)}$ 也为模 m 的一个最小正简化剩余系. 这就是说, $a \cdot r_1, \cdots, a \cdot r_{\varphi(m)}$ 模 m 的最小正剩余是 $r_1, \cdots, r_{\varphi(m)}$ 的一个排列. 故 $(a \cdot r_1)(a \cdot r_2) \cdots (a \cdot r_{\varphi(m)})$ 模 m 的最小正剩余和 $r_1 r_2 \cdots r_{\varphi(m)}$ 模 m 的最小正剩余相等. 根据定理 2.1.2, 有

$$(a \cdot r_1) \cdots (a \cdot r_{\varphi(m)}) \equiv r_1 \cdots r_{\varphi(m)} \mod m.$$

因此, $r_1 \cdots r_{\varphi(m)}(a^{\varphi(m)} - 1) \equiv 0 \mod m$. 又由
$(r_1, m) = 1, \cdots, (r_{\varphi(m)}, m) = 1$ 及推论 1.2.1, 可推出 $(r_1 \cdots r_{\varphi(m)}, m) = 1$.
从而, 根据性质 2.1.3, 得到 $a^{\varphi(m)} \equiv 1 \mod m$.

例 2.2.17

设 $m = 19, a = 3$, 有 $(3, 19) = 1, \varphi(19) = 18$, 故 $3^{18} \equiv 1 \mod 19$.

设 $m = 31, a = 2$, 有 $(2, 31) = 1, \varphi(31) = 30$, 故 $2^{30} \equiv 1 \mod 31$.

例 2.2.17

设 $m=19, a=3$, 有 $(3,19)=1, \varphi(19)=18$, 故 $3^{18}\equiv 1 \mod 19$.
设 $m=31, a=2$, 有 $(2,31)=1, \varphi(31)=30$, 故 $2^{30}\equiv 1 \mod 31$.

应用欧拉定理, 当 m 是素数时, 给出费马（Fermat）小定理与 Wilson 定理.

定理 2.2.14 (费马小定理)

设 p 是一个素数, 则对任意整数 a, 有

$$a^p \equiv a \mod p.$$

例 2.2.17

设 $m = 19, a = 3$, 有 $(3, 19) = 1, \varphi(19) = 18$, 故 $3^{18} \equiv 1 \mod 19$.

设 $m = 31, a = 2$, 有 $(2, 31) = 1, \varphi(31) = 30$, 故 $2^{30} \equiv 1 \mod 31$.

应用欧拉定理, 当 m 是素数时, 给出费马（Fermat）小定理与 Wilson 定理.

定理 2.2.14 (费马小定理)

设 p 是一个素数, 则对任意整数 a, 有

$$a^p \equiv a \mod p.$$

证：分两种情形考虑.

(i) 若 a 被 p 整除, 则同时有 $a \equiv 0 \mod p$ 和 $a^p \equiv 0 \mod p$. 故 $a^p \equiv a \mod p$.

例 2.2.17

设 $m = 19, a = 3$，有 $(3, 19) = 1, \varphi(19) = 18$，故 $3^{18} \equiv 1 \mod 19$.

设 $m = 31, a = 2$，有 $(2, 31) = 1, \varphi(31) = 30$，故 $2^{30} \equiv 1 \mod 31$.

应用欧拉定理，当 m 是素数时，给出费马（Fermat）小定理与 Wilson 定理.

定理 2.2.14 (费马小定理)

设 p 是一个素数，则对任意整数 a，有

$$a^p \equiv a \mod p.$$

证：分两种情形考虑.

(i) 若 a 被 p 整除，则同时有 $a \equiv 0 \mod p$ 和 $a^p \equiv 0 \mod p$. 故 $a^p \equiv a \mod p$.

(ii) 若 a 不能被 p 整除，则 $(a, p) = 1$ (见例 1.2.5). 根据定理 2.2.13 知，$a^{p-1} \equiv 1 \mod p$. 两端同时乘以 a 得，$a^p \equiv a \mod p$.

例 2.2.18 应用欧拉定理可以证明 RSA 公钥密码算法的正确性. Ron Rivest 和 Adi Shamir 以及 Leonard Adleman 于 1978 年提出的 RSA 公钥密码体制至今仍被公认为是一个安全性能良好的密码体制. RSA 公钥密码体制的描述如下：

1) 选取两个大素数 p, q.

2) 计算 $n = pq, \varphi(n) = (p-1)(q-1)$.

3) 随机选取正整数 $e, 1 < e < \varphi(n)$, 满足 $(e, \varphi(n)) = 1$.

4) 计算 d, 满足 $de \equiv 1 \mod \varphi(n)$. $p, q, \varphi(n), d$ 是保密的；n, e 是公开的.

5) 加密变换：对于明文 $m, 1 < m < n$, 加密后的密文为 $c \equiv m^e \mod n$.

6) 解密变换：对于密文 $c, 1 < c < n$, 解密后的明文为 $m = c^d \mod n$.

这个解密变换能正确恢复出明文.

证：由于 $de \equiv 1 \mod \varphi(n)$, 所以存在正整数 t, 使得 $de = 1 + t\varphi(n)$.

对任意明文 $m, 1 < m < n$,

当 $(m, n) = 1$ 时, 根据欧拉定理得

$$c^d \equiv (m^e)^d \equiv (m^{\varphi(n)})^t m \equiv 1^t m \equiv m \mod n. \tag{2.2.2}$$

当 $(m, n) \neq 1$ 时, 因为 $n = pq$ 且 p, q 是两个素数, 所以 $\varphi(n) = (p-1)(q-1)$, $(m, n) = p$ 或 q. 不妨设 $(m, n) = p$, 则 $p \mid m$. 设 $m = bp, 1 \leq b < q$. 另一方面, 由欧拉定理得 $m^{q-1} \equiv 1 \mod q$, 从而 $m^{t\varphi(n)} = (m^{q-1})^{t(p-1)} \equiv 1 \mod q$, 于是存在一个整数 s, 使得 $m^{t\varphi(n)} = 1 + sq$. 此式两端用 $m = bp$ 同乘, 就得到

$$m^{t\varphi(n)+1} = m + bsn, \tag{2.2.3}$$

从而由（2.2.2）与（2.2.3）有, $c^d \equiv m^{t\varphi(n)+1} \equiv m \mod n$.

定理 2.2.15 (Wilson 定理)

设 p 是一个素数，则

$$(p-1)! \equiv -1 \mod p.$$

定理 2.2.15 (Wilson 定理)

设 p 是一个素数，则

$$(p-1)! \equiv -1 \mod p.$$

证：若 $p=2$，则结论显然成立.

若 $p \geqslant 3$，根据定理 2.2.9，对于每个整数 $a, 1 \leqslant a \leqslant p-1$，存在唯一的整数 $a', 1 \leqslant a' \leqslant p-1$，使得 $a \cdot a' \equiv 1 \mod p$.

而 $a' = a$ 的充要条件是 a 满足 $a^2 \equiv 1 \mod p$. 这时，$a=1$ 或 $a=p-1$. 故将 $2, \cdots, p-2$ 中的 a 与 a' 配对，得到

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot (p-2) \cdot (p-1) &\equiv 1 \cdot (p-1) \prod_a a \cdot a' \\ &\equiv 1 \cdot (p-1) \\ &\equiv -1 \mod p. \end{aligned}$$

因此，结论成立.

例 2.2.19　设 $p = 13$. 有

$$\begin{aligned} 2\cdot 7 = 14 &\equiv 1 \mod 13, & 3\cdot 9 = 27 &\equiv 1 \mod 13, \\ 4\cdot 10 = 40 &\equiv 1 \mod 13, & 5\cdot 8 = 40 &\equiv 1 \mod 13, \\ 6\cdot 11 = 66 &\equiv 1 \mod 13, & 1\cdot 12 = 12 &\equiv -1 \mod 13. \end{aligned}$$

因此,

$$\begin{aligned} & 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10\cdot 11 \\ = \;& (1\cdot 12)(2\cdot 7)(3\cdot 9)(4\cdot 10)(5\cdot 8)(6\cdot 11) \\ \equiv \;& (-1)\cdot 1\cdot 1\cdot 1\cdot 1\cdot 1 \\ \equiv \;& -1 \mod 13. \end{aligned}$$

在模算术计算中, 常常需要进行大整数的方幂模运算, 即对大整数模 m 和大整数 n, 计算 $b^n \mod m$.

在模算术计算中, 常常需要进行大整数的方幂模运算, 即对大整数模 m 和大整数 n, 计算 $b^n \mod m$.

当然, 可以递归地计算 $b^n \equiv (b^{n-1} \mod m) \cdot b \mod m$. 但这种计算方式较为耗时, 须作 $n-1$ 次乘法.

在模算术计算中，常常需要进行大整数的方幂模运算，即对大整数模 m 和大整数 n，计算 $b^n \mod m$.

当然，可以递归地计算 $b^n \equiv (b^{n-1} \mod m) \cdot b \mod m$. 但这种计算方式较为耗时，须作 $n-1$ 次乘法.

注意到以下计算特性：

$$b^{16} \equiv \left(\left(\left(b^2\right)^2\right)^2\right)^2 \mod m,\ b^{128} \equiv \left(\left(\left(\left(\left(\left(b^2\right)^2\right)^2\right)^2\right)^2\right)^2\right)^2 \mod m.$$

则可以优化方幂模 m 运算.

在模算术计算中，常常需要进行大整数的方幂模运算，即对大整数模 m 和大整数 n，计算 $b^n \mod m$.

当然，可以递归地计算 $b^n \equiv (b^{n-1} \mod m) \cdot b \mod m$. 但这种计算方式较为耗时，须作 $n-1$ 次乘法.

注意到以下计算特性：

$$b^{16} \equiv \left(\left(\left(b^2\right)^2\right)^2\right)^2 \mod m, \ b^{128} \equiv \left(\left(\left(\left(\left(\left(b^2\right)^2\right)^2\right)^2\right)^2\right)^2\right)^2 \mod m.$$

则可以优化方幂模 m 运算.

将 n 写成二进制，即

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}, \ n_i \in \{0, 1\}, \ i = 0, 1, \cdots, k-1.$$

则 $b^n \mod m$ 的计算可归纳为

$$b^n \equiv \underbrace{\underbrace{\underbrace{\underbrace{\underbrace{b^{n_0}}_{a_0}(\underbrace{b^2}_{b_1})^{n_1}}_{a_1}\cdots}_{a_{k-3}}(\underbrace{b^{2^{k-2}}}_{b_{k-2}})^{n_{k-2}}}_{a_{k-2}}(\underbrace{b^{2^{k-1}}}_{b_{k-1}})^{n_{k-1}}}_{a_{k-1}} \mod m.$$

$$b^n \equiv \underbrace{\underbrace{\underbrace{\underbrace{\underbrace{b^{n_0}}_{a_0}(\underbrace{b^2}_{b_1})^{n_1}}_{a_1}\cdots}_{a_{k-3}}(\underbrace{b^{2^{k-2}}}_{b_{k-2}})^{n_{k-2}}}_{a_{k-2}}(\underbrace{b^{2^{k-1}}}_{b_{k-1}})^{n_{k-1}}}_{a_{k-1}} \mod m.$$

或

$$a_0 = b^{n_0},\ b_0 = b,\ b_i = b_{i-1}^2,\ a_i = a_{i-1} \cdot b_i,\ i = 1, \cdots, k-1.$$

$$b^n \equiv \underbrace{\underbrace{\underbrace{\underbrace{\underbrace{b^{n_0}}_{a_0}(\underbrace{b^2}_{b_1})^{n_1}}_{a_1}\cdots}_{a_{k-3}}(\underbrace{b^{2^{k-2}}}_{b_{k-2}})^{n_{k-2}}}_{a_{k-2}}(\underbrace{b^{2^{k-1}}}_{b_{k-1}})^{n_{k-1}}}_{a_{k-1}} \mod m.$$

或

$$a_0 = b^{n_0},\ b_0 = b,\ b_i = b_{i-1}^2,\ a_i = a_{i-1} \cdot b_i,\ i = 1, \cdots, k-1.$$

从“低位”到“高位”(从右到左) 的顺序进行递归.

$$b^n \equiv \underbrace{\underbrace{\underbrace{\underbrace{\underbrace{b^{n_0}}_{a_0}(\underbrace{b^2}_{b_1})^{n_1}}_{a_1}\cdots}_{a_{k-3}}(\underbrace{b^{2^{k-2}}}_{b_{k-2}})^{n_{k-2}}}_{a_{k-2}}(\underbrace{b^{2^{k-1}}}_{b_{k-1}})^{n_{k-1}}}_{a_{k-1}} \mod m.$$

或

$$a_0 = b^{n_0},\ b_0 = b,\ b_i = b_{i-1}^2,\ a_i = a_{i-1} \cdot b_i,\ i = 1, \cdots, k-1.$$

从“低位”到“高位”(从右到左) 的顺序进行递归.

因此, 最多作 $2[\log_2 n]$ 次乘法. 该计算方法叫做“**模重复平方计算法**”.

具体算法如下:

令 $a=1$, 并将 n 写成二进制

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0,1\}$, $i = 0, 1, \cdots, k-1$.

令 $a=1$, 并将 n 写成二进制

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0,1\}$, $i = 0, 1, \cdots, k-1$.

(1) 如果 $n_0 = 1$, 则计算 $a_0 \equiv a \cdot b \mod m$; 否则, 取 $a_0 = a$, 即计算 $a_0 \equiv a \cdot b^{n_0} \mod m$. 再计算 $b_1 \equiv b^2 \mod m$.

令 $a=1$, 并将 n 写成二进制

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0,1\}$, $i = 0, 1, \cdots, k-1$.

(1) 如果 $n_0 = 1$, 则计算 $a_0 \equiv a \cdot b \mod m$; 否则, 取 $a_0 = a$, 即计算 $a_0 \equiv a \cdot b^{n_0} \mod m$. 再计算 $b_1 \equiv b^2 \mod m$.

(2) 如果 $n_1 = 1$, 则计算 $a_1 \equiv a_0 \cdot b_1 \mod m$; 否则, 取 $a_1 = a_0$, 即计算 $a_1 \equiv a_0 \cdot b_1^{n_1} \mod m$. 再计算 $b_2 \equiv b_1^2 \mod m$.

$\vdots$

令 $a=1$, 并将 n 写成二进制

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0,1\}$, $i=0,1,\cdots,k-1$.

(1) 如果 $n_0=1$, 则计算 $a_0 \equiv a \cdot b \mod m$; 否则, 取 $a_0 = a$, 即计算 $a_0 \equiv a \cdot b^{n_0} \mod m$. 再计算 $b_1 \equiv b^2 \mod m$.

(2) 如果 $n_1=1$, 则计算 $a_1 \equiv a_0 \cdot b_1 \mod m$; 否则, 取 $a_1 = a_0$, 即计算 $a_1 \equiv a_0 \cdot b_1^{n_1} \mod m$. 再计算 $b_2 \equiv b_1^2 \mod m$.

$\vdots$

(k-1) 如果 $n_{k-2}=1$, 则计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2} \mod m$; 否则, 取 $a_{k-2} = a_{k-3}$, 即计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \mod m$. 再计算 $b_{k-1} \equiv b_{k-2}^2 \mod m$.

令 $a=1$, 并将 n 写成二进制

$$n=n_0+n_1 2+\cdots+n_{k-1}2^{k-1},$$

其中 $n_i\in\{0,1\}$, $i=0,1,\cdots,k-1$.

(1) 如果 $n_0=1$, 则计算 $a_0\equiv a\cdot b \mod m$; 否则, 取 $a_0=a$, 即计算 $a_0\equiv a\cdot b^{n_0} \mod m$. 再计算 $b_1\equiv b^2 \mod m$.

(2) 如果 $n_1=1$, 则计算 $a_1\equiv a_0\cdot b_1 \mod m$; 否则, 取 $a_1=a_0$, 即计算 $a_1\equiv a_0\cdot b_1^{n_1} \mod m$. 再计算 $b_2\equiv b_1^2 \mod m$.

⋮

(k-1) 如果 $n_{k-2}=1$, 则计算 $a_{k-2}\equiv a_{k-3}\cdot b_{k-2} \mod m$; 否则, 取 $a_{k-2}=a_{k-3}$, 即计算 $a_{k-2}\equiv a_{k-3}\cdot b_{k-2}^{n_{k-2}} \mod m$. 再计算 $b_{k-1}\equiv b_{k-2}^2 \mod m$.

(k) 如果 $n_{k-1}=1$, 则计算 $a_{k-1}\equiv a_{k-2}\cdot b_{k-1} \mod m$; 否则, 取 $a_{k-1}=a_{k-2}$, 即计算 $a_{k-1}\equiv a_{k-2}\cdot b_{k-1}^{n_{k-1}} \mod m$.

令 $a=1$, 并将 n 写成二进制

$$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1},$$

其中 $n_i \in \{0,1\}$, $i=0,1,\cdots,k-1$.

(1) 如果 $n_0=1$, 则计算 $a_0 \equiv a \cdot b \mod m$; 否则, 取 $a_0 = a$, 即计算 $a_0 \equiv a \cdot b^{n_0} \mod m$. 再计算 $b_1 \equiv b^2 \mod m$.

(2) 如果 $n_1=1$, 则计算 $a_1 \equiv a_0 \cdot b_1 \mod m$; 否则, 取 $a_1 = a_0$, 即计算 $a_1 \equiv a_0 \cdot b_1^{n_1} \mod m$. 再计算 $b_2 \equiv b_1^2 \mod m$.

$\vdots$

(k-1) 如果 $n_{k-2}=1$, 则计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2} \mod m$; 否则, 取 $a_{k-2} = a_{k-3}$, 即计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \mod m$. 再计算 $b_{k-1} \equiv b_{k-2}^2 \mod m$.

(k) 如果 $n_{k-1}=1$, 则计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1} \mod m$; 否则, 取 $a_{k-1} = a_{k-2}$, 即计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \mod m$.

最后, a_{k-1} 就是要求的 $b^n \mod m$.

例 2.3.1 计算 $7^{29} \mod 31$.

例 2.3.1　计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,

$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$.

例 2.3.1　计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,

$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$. 运用模重复平方法, 依次计算如下：

例 2.3.1 计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,
$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$. 运用模重复平方法, 依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = a \cdot b \equiv 7 \mod 31, \quad b_1 \equiv b^2 \equiv 18 \mod 31.$$

例 2.3.1 计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,

$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$. 运用模重复平方法, 依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = a \cdot b \equiv 7 \mod 31, \quad b_1 \equiv b^2 \equiv 18 \mod 31.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 7 \mod 31, \quad b_2 \equiv b_1^2 \equiv 14 \mod 31.$$

例 2.3.1 计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,

$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$. 运用模重复平方法, 依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = a \cdot b \equiv 7 \mod 31, \quad b_1 \equiv b^2 \equiv 18 \mod 31.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 7 \mod 31, \quad b_2 \equiv b_1^2 \equiv 14 \mod 31.$$

(3) $n_2 = 1$, 计算

$$a_2 = a_1 \cdot b_2 \equiv 5 \mod 31, \quad b_3 \equiv b_2^2 \equiv 10 \mod 31.$$

例 2.3.1 计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,

$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$. 运用模重复平方法, 依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = a \cdot b \equiv 7 \mod 31, \quad b_1 \equiv b^2 \equiv 18 \mod 31.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 7 \mod 31, \quad b_2 \equiv b_1^2 \equiv 14 \mod 31.$$

(3) $n_2 = 1$, 计算

$$a_2 = a_1 \cdot b_2 \equiv 5 \mod 31, \quad b_3 \equiv b_2^2 \equiv 10 \mod 31.$$

(4) $n_3 = 1$, 计算

$$a_3 = a_2 \cdot b_3 \equiv 19 \mod 31, \quad b_4 \equiv b_3^2 \equiv 7 \mod 31.$$

例 2.3.1 计算 $7^{29} \mod 31$.

解：设 $m = 31, b = 7$. 令 $a = 1$. 将 29 写成二进制,

$29 = 1 + 2^2 + 2^3 + 2^4 = (11101)_2$. 运用模重复平方法, 依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = a \cdot b \equiv 7 \mod 31, \quad b_1 \equiv b^2 \equiv 18 \mod 31.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 7 \mod 31, \quad b_2 \equiv b_1^2 \equiv 14 \mod 31.$$

(3) $n_2 = 1$, 计算

$$a_2 = a_1 \cdot b_2 \equiv 5 \mod 31, \quad b_3 \equiv b_2^2 \equiv 10 \mod 31.$$

(4) $n_3 = 1$, 计算

$$a_3 = a_2 \cdot b_3 \equiv 19 \mod 31, \quad b_4 \equiv b_3^2 \equiv 7 \mod 31.$$

(5) $n_4 = 1$, 计算 $a_4 = a_3 \cdot b_4 \equiv 9 \mod 31$.

例 2.3.1 计算 $7^{29} \mod 31$.

解：设 $m=31, b=7$. 令 $a=1$. 将 29 写成二进制,

$29=1+2^2+2^3+2^4=(11101)_2$. 运用模重复平方法, 依次计算如下：

(1) $n_0=1$, 计算

$$a_0=a\cdot b\equiv 7 \mod 31,\quad b_1\equiv b^2\equiv 18 \mod 31.$$

(2) $n_1=0$, 计算

$$a_1=a_0\equiv 7 \mod 31,\quad b_2\equiv b_1^2\equiv 14 \mod 31.$$

(3) $n_2=1$, 计算

$$a_2=a_1\cdot b_2\equiv 5 \mod 31,\quad b_3\equiv b_2^2\equiv 10 \mod 31.$$

(4) $n_3=1$, 计算

$$a_3=a_2\cdot b_3\equiv 19 \mod 31,\quad b_4\equiv b_3^2\equiv 7 \mod 31.$$

(5) $n_4=1$, 计算 $a_4=a_3\cdot b_4\equiv 9 \mod 31$.

最后, 计算得出 $7^{29}\equiv 9 \mod 31$.

例 2.3.2　计算 $32760^{365} \mod 65521$.

例 2.3.2 计算 $32760^{365} \mod 65521$.

解：设 $m = 65521, b = 32760$. 令 $a = 1$. 将 365 写成二进制,

$365 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^8 = (101101101)_2$.

例 2.3.2 计算 $32760^{365} \mod 65521$.

解：设 $m = 65521, b = 32760$. 令 $a = 1$. 将 365 写成二进制,

$365 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^8 = (101101101)_2$.可以依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = ab \equiv 32760 \mod 65521, \quad b_1 \equiv b^2 \equiv 49141 \mod 65521.$$

例 2.3.2 计算 $32760^{365} \mod 65521$.

解：设 $m = 65521, b = 32760$. 令 $a = 1$. 将 365 写成二进制，

$365 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^8 = (101101101)_2$.可以依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = ab \equiv 32760 \mod 65521, \quad b_1 \equiv b^2 \equiv 49141 \mod 65521.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 32760 \mod 65521, \quad b_2 \equiv b_1^2 \equiv 61426 \mod 65521.$$

例 2.3.2 计算 $32760^{365} \mod 65521$.

解：设 $m=65521, b=32760$. 令 $a=1$. 将 365 写成二进制，

$365=1+2^2+2^3+2^5+2^6+2^8=(101101101)_2$.可以依次计算如下：

(1) $n_0=1$, 计算

$$a_0=ab\equiv 32760 \mod 65521,\quad b_1\equiv b^2\equiv 49141 \mod 65521.$$

(2) $n_1=0$, 计算

$$a_1=a_0\equiv 32760 \mod 65521,\quad b_2\equiv b_1^2\equiv 61426 \mod 65521.$$

(3) $n_2=1$, 计算

$$a_2=a_1\cdot b_2\equiv 34808 \mod 65521,\quad b_3\equiv b_2^2\equiv 61170 \mod 65521.$$

例 2.3.2 计算 $32760^{365} \mod 65521$.

解：设 $m = 65521, b = 32760$. 令 $a = 1$. 将 365 写成二进制,

$365 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^8 = (101101101)_2$.可以依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = ab \equiv 32760 \mod 65521, \quad b_1 \equiv b^2 \equiv 49141 \mod 65521.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 32760 \mod 65521, \quad b_2 \equiv b_1^2 \equiv 61426 \mod 65521.$$

(3) $n_2 = 1$, 计算

$$a_2 = a_1 \cdot b_2 \equiv 34808 \mod 65521, \quad b_3 \equiv b_2^2 \equiv 61170 \mod 65521.$$

(4) $n_3 = 1$, 计算

$$a_3 = a_2 \cdot b_3 \equiv 34944 \mod 65521, \quad b_4 \equiv b_3^2 \equiv 61153 \mod 65521.$$

例 2.3.2 计算 $32760^{365} \mod 65521$.

解：设 $m = 65521, b = 32760$. 令 $a = 1$. 将 365 写成二进制,
$365 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^8 = (101101101)_2$.可以依次计算如下：

(1) $n_0 = 1$, 计算

$$a_0 = ab \equiv 32760 \mod 65521, \quad b_1 \equiv b^2 \equiv 49141 \mod 65521.$$

(2) $n_1 = 0$, 计算

$$a_1 = a_0 \equiv 32760 \mod 65521, \quad b_2 \equiv b_1^2 \equiv 61426 \mod 65521.$$

(3) $n_2 = 1$, 计算

$$a_2 = a_1 \cdot b_2 \equiv 34808 \mod 65521, \quad b_3 \equiv b_2^2 \equiv 61170 \mod 65521.$$

(4) $n_3 = 1$, 计算

$$a_3 = a_2 \cdot b_3 \equiv 34944 \mod 65521, \quad b_4 \equiv b_3^2 \equiv 61153 \mod 65521.$$

(5) $n_4 = 0$, 计算

$$a_4 = a_3 \equiv 34944 \mod 65521, \quad b_5 \equiv b_4^2 \equiv 12813 \mod 65521.$$

(6) $n_5 = 1$, 计算

$$a_5 = a_4 \cdot b_5 \equiv 32479 \mod 65521, \quad b_6 \equiv b_5^2 \equiv 42864 \mod 65521.$$

(6) $n_5 = 1$, 计算

$$a_5 = a_4 \cdot b_5 \equiv 32479 \mod 65521, \quad b_6 \equiv b_5^2 \equiv 42864 \mod 65521.$$

(7) $n_6 = 1$, 计算

$$a_6 = a_5 \cdot b_6 \equiv 55169 \mod 65521, \quad b_7 \equiv b_6^2 \equiv 48135 \mod 65521.$$

(6) $n_5 = 1$, 计算

$$a_5 = a_4 \cdot b_5 \equiv 32479 \mod 65521, \quad b_6 \equiv b_5^2 \equiv 42864 \mod 65521.$$

(7) $n_6 = 1$, 计算

$$a_6 = a_5 \cdot b_6 \equiv 55169 \mod 65521, \quad b_7 \equiv b_6^2 \equiv 48135 \mod 65521.$$

(8) $n_7 = 0$, 计算

$$a_7 = a_6 \equiv 55169 \mod 65521, \quad b_8 \equiv b_7^2 \equiv 24623 \mod 65521.$$

(6) $n_5 = 1$, 计算

$$a_5 = a_4 \cdot b_5 \equiv 32479 \mod 65521, \quad b_6 \equiv b_5^2 \equiv 42864 \mod 65521.$$

(7) $n_6 = 1$, 计算

$$a_6 = a_5 \cdot b_6 \equiv 55169 \mod 65521, \quad b_7 \equiv b_6^2 \equiv 48135 \mod 65521.$$

(8) $n_7 = 0$, 计算

$$a_7 = a_6 \equiv 55169 \mod 65521, \quad b_8 \equiv b_7^2 \equiv 24623 \mod 65521.$$

(9) $n_8 = 1$, 计算

$$a_8 = a_7 \cdot b_8 \equiv 44915 \mod 65521.$$

最后, 计算得出 $32760^{365} \equiv 44915 \mod 65521$.

本课作业

1. 证明：若 p 为奇素数, 且 $2^m \not\equiv 1 \mod p$, 则
$$1^m + 2^m + \cdots + (p-1)^m \equiv 0 \mod p.$$
2. 求 $\varphi(2024)$.
3. 证明: 如果 m 是正整数, a 是与 m 互素的整数, 且 $(a-1, m) = 1$,
$$\text{则 } 1 + a + a^2 + \cdots + a^{(\varphi(m)-1)} \equiv 0 \mod m.$$
4. 利用模重复平方算法计算 $21^{39} \mod 100$.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn