2022-2023学年秋季学期

课程名称: 信息安全数学基础

英文名称: Mathematical Foundations for Information Security

授课团队：胡磊、许军、王丽萍

助　　教：郭一

信息安全数学基础

Mathematical Foundations for Information Security

[第 3 次课]　同余与模幂运算

授课教师：胡磊

授课时间：2022年9月7、14日

概 要

- 同余的概念及其性质
- 剩余类及完全剩余类
- 简化剩余系与欧拉函数
- 欧拉定理和费马小定理
- 重复平方—乘法法及其变型（一般模幂运算）
- Montgomery模幂运算

同余的概念及基本性质

定义： 对**m**作带余除法（余数范围固定），如果整数 ***a*** ，***b***被***m***除的余数相同，则称***a, b***模***m*** 同余，记作***a≡b* (mod*m*),** 否则叫做模**m**不同余，记作

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

定理：两个整数***a, b***叫做模***m***同余$\Longleftrightarrow$ ***m|a-b***

$\Longleftrightarrow$ ***a=b+km，k*** $\in$***Z***

a=mq + r,　0 ≤ r < m,

b=mq’ + r’,　0 ≤ r’ < m,

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

定理： 如果 $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, 则

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

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

证

$$a_1 = b_1 + k_1 m,\ a_2 = b_2 + k_2 m,$$

$$a_1 + a_2 = b_1 + b_2 + (k_1 + k_2)m$$

$$a_1 a_2 = b_1 b_2 + (k_1 b_2 + k_2 b_2 + k_1 k_2 m)m$$

- 同余保持加、减、乘运算。

定理 5 若 $x \equiv y \pmod{m}$, $a_i \equiv b_i \pmod{m}$, $0 \le i \le k$, 则

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

定理 6 设 $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0,\ 0 \le a_i < 10.$

则 $3|n \Leftrightarrow 3|a_k + \cdots + a_0$; 而 $9|n \Leftrightarrow 9|a_k + \cdots + a_0.$

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

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 7 设 $n = 5874192$, 则 $3|n,\ 9|n.$

解 $a_k + \cdots + a_0 = 5+8+7+4+1+9+2 = 36$, 又 $3|36,\ 9|36$, 故 $3|n,\ 9|n.$

例 8 设 $n = 637693$, 则 n 被 3 整除, 但不被 9 整除.

解 $a_k + \cdots + a_0 = 6+3+7+6+9+3 = 30 = 3 \cdot 10$, 又 $3|3 \cdot 10,\ 9 \nmid 3 \cdot 10$, 故 $3|n,\ 9 \nmid n.$

定理 7 设 $n = a_k 1000^k + \cdots + a_1 1000 + a_0, \qquad 0 \le a_i < 1000.$

则 7或11,或13$|n \Leftrightarrow$ 7或11,或13$|(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$.

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

$1000 \equiv 1000^3 \equiv \cdots \equiv -1 \pmod 7, \quad 1000^2 \equiv 1000^4 \equiv \cdots \equiv 1 \pmod 7.$ 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, $7|n \Leftrightarrow 7 \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$.

即结论对于 $m = 7$ 成立. 同理, 结论对于 $m = 11$ 或 13 也成立.

例 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 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.

* **定理** 8 设 $ad \equiv bd \pmod{m}$. 若 $(d, m) = 1$, 则 $a \equiv b \pmod{m}$.

证 因为$ad \equiv bd \bmod m$, 则 $m \mid ad - bd$

$$m \mid (a - b)d$$

$m \mid (a - b)$, 故 $a \equiv b \bmod m$

* **定理** 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 $d|(a, b, m)$, 则 $a = da', \quad b = db', \quad m = dm'$.

又 $a \equiv b \pmod{m}$, 有 $a = b + mk$, 即 $da' = db' + dm'k$.

故 $a' = b' + m'k$. 或 $a' \equiv b' \pmod{m'}$ 或者 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

* **定理 11** 设 $a \equiv b \pmod{m}$. 如果 $d|m$, 则 $a \equiv b \pmod{d}$.

* **定理 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 $m_i | a - b$. 进而 $[m_1, \ldots, m_k] \mid a - b$. 即 $a \equiv b \pmod{[m_1, \ldots, m_k]}$.

* **例 16** 设 p, q 是不同素数. 若 a, b 满足 $a \equiv b \pmod{p}, a \equiv b \pmod{q}$, 则 $a \equiv b \pmod{pq}$.

定理 13 设 $a \equiv b \pmod{m}$, 则 $(a, m) = (b, m)$.

证 设 $a \equiv b \pmod{m}$, 则存在整数 k 使得 $a = b + mk$. 根据 §1.3 定理 3, 我们有 $(a, m) = (b, m)$.

剩余类及完全剩余系

对任意整数 a, 令 $\quad C_a = \{c \mid c \in \mathbf{Z},\ a \equiv c \pmod m\}.$

定理 1 i) 任一整数必包含在一个 C_r 中, $\quad 0 \le r \le m-1.$

ii) $C_a = C_b \Leftrightarrow a \equiv b \pmod m.$ $\qquad (1)$

iii) $C_a \cap C_b = \emptyset \Leftrightarrow a \not\equiv b \pmod m.$

定义 1 C_a 叫做模 m 的 a 的 **剩余类**. 一个剩余类中的任一数叫做该类的 **剩余** 或 **代表元**. 若 $r_0, r_1, \ldots, r_{m-1}$ 是 m 个整数, 并且其中任何两个数都不在同一个剩余类里, 则 $r_0, \ldots, r_{m-1}$ 叫做模 m 的一个 **完全剩余系**. 模 m 的剩余类有 m 个

$$C_0, C_1, \ldots, C_{m-1}.$$

例 1 对任意整数 a, $C_a = \{a + 10k \mid k \in \mathbf{Z}\}$ 是模 $m = 10$ 的剩余类.

$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ 为模 10 的一个完全剩余系.

定理 2 m 个整数 $r_0, r_1, \ldots, r_{m-1}$ 为模 m 的一个完全剩余系的充分必要条件是它们模 m 两两不同余.

例 2 设 m 是一个正整数. 则

i) $0, 1, \ldots, m-1$ 是模 m 的一个完全剩余系, 叫做模 m 的 **最小非负完全剩余系**;

ii) $1, \ldots, m-1, m$ 是模 m 的一个完全剩余系, 叫做模 m 的 **最小正完全剩余系**;

iii) $-(m-1),\ \ldots,\ -1,\ 0$ 是模 m 的一个完全剩余系，叫做模 m 的**最大非正完全剩余系**;

iv) $-m,\ -(m-1),\ \ldots,\ -1$ 是模 m 的一个完全剩余系，叫做模 m 的**最大负完全剩余系**;

v) 当 m 分别为偶数时，$-m/2,\ -(m-2)/2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ (m-2)/2$，或 $-(m-2)/2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ (m-2)/2,\ m/2$，是模 m 的一个完全剩余系;

当 m 分别为奇数时，

$$-(m-1)/2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ (m-1)/2$$

是模 m 的一个完全剩余系，上述两个完全剩余系统称为模 m 的一个**绝对值最小完全剩余系**.

定理 3 设 $(a,m)=1$, b 是任意整数. 若 x 遍历模 m 的一个完全剩余系, 则 $ax+b$ 也遍历模 m 的一个完全剩余系.

证 根据定理 2, 只需证明: 当 $a_0, a_1, \ldots, a_{m-1}$ 是模 m 的一个完全剩余系时, m 个整数 $aa_0+b, aa_1+b, \ldots, aa_{m-1}+b$ 模 m 两两不同余. 事实上, 若存在 a_i 和 $a_j\ (i\neq j)$ 使得

$$aa_i+b\equiv aa_j+b \pmod m,$$

则 $m|a(a_i-a_j)$. 因为 $(a,m)=1$

$$m|a_i-a_j$$

这说明 a_i 与 a_j 模 m 同余, 与假设矛盾.

因此, $ax+b$ 也遍历模 m 的一个完全剩余系.

定理 4 设 $(m_1, m_2) = 1$. 若 x_1, x_2 分别遍历模 m_1, m_2 的完全剩余系，则 $m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的完全剩余系.

证 因为 x_1, x_2 分别遍历 m_1, m_2 个数时， $m_2x_1 + m_1x_2$ 遍历 m_1m_2 个整数，所以只需证明这 m_1m_2 个整数模 m_1m_2 两两不同余. 事实上，若整数 x_1, x_2 和 y_1, y_2 满足

$$m_2x_1 + m_1x_2 \equiv m_2y_1 + m_1y_2 \pmod{m_1m_2},$$

则 $m_2x_1 + m_1x_2 \equiv m_2y_1 + m_1y_2 \pmod{m_1}$

$m_2x_1 \equiv m_2y_1 \pmod{m_1}$ 所以 $m_1 | x_1 - y_1$

故 x_1 与 y_1 模 m_1 同余.

同理， x_2 与 y_2 模 m_2 同余. 因此，定理是成立的.

例 3 设 $p,\ q$ 是不同的素数， $n = pq$. 则对任意整数 c, 存在惟一的一对整数 $x,\ y$ 满足 $qx + py \equiv c \pmod{n}, \quad 0 \leq x < p,\ 0 \leq y < q.$

证 因为 $p,\ q$ 是两个不同的素数，所以 $p,\ q$ 是互素的. 根据定理 4 及其证明，知 $x,\ y$ 分别遍历模 $p,\ q$ 的完全剩余系时， $qx + py$ 遍历模 $n = pq$ 的完全剩余系. 因此，存在惟一的一对整数 $x,\ y$ 满足

$$qx + py \equiv c \pmod{n}, \qquad 0 \leq x < p,\ 0 \leq y < q.$$

简化剩余类及欧拉函数

定义 1 设 m 是一个正整数. 则 m 个整数 $0,\ 1,\ \ldots,\ m-1$ 中与 m 互素的整数的个数，记作 $\varphi(m)$, 通常叫做 **欧拉** (Euler) **函数**.

例 1 设 $m = 10$. 则 10 个整数 $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9$ 中与 10 互素的整数为 $1,\ 3,\ 7,\ 9$, 所以 $\varphi(10) = 4$.

定义 2 一个模 m 的剩余类叫做 **简化剩余类**, 如果该类中存在一个与 m 互素的剩余.

定理 1 设 $r_1,\ r_2$ 是同一模 m 剩余类的两个剩余，则 r_1 与 m 互素的充分必要条件是 r_2 与 m 互素.

证 依题设, 有 $r_1 = r_2 + km$. 进而 $(r_1, m) = (r_2, m)$. 因此, $(r_1, m) = 1 \Leftrightarrow (r_2, m) = 1$.

定义 3 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**.

模 m 的简化剩余系的元素个数为 $\varphi(m)$.

例 3 $1,\ 3,\ 7,\ 9$ 是模 10 的简化剩余系，$\varphi(10)=4$.

例 4 $1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$ 是模 30 的简化剩余系，$\varphi(30)=8$.

例 5 $1,\ 2,\ 3,\ 4,\ 5,\ 6$ 是模 7 的简化剩余系，$\varphi(7)=6$.

例 6 当 $m=p$ 为素数时，$1,\ 2,\ \ldots,\ p-1$ 是模 p 的简化剩余系，所以 $\varphi(p)=p-1$.

定理 2 若 $r_1,\ \ldots,\ r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数，并且两两模 m 不同余，则 $r_1,\ \ldots,\ r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

定理 3 设 $(a,m)=1$. 如果 x 遍历模 m 的一个简化剩余系, 则 ax 也遍历模 m 的一个简化剩余系.

证 因为 $(a,m)=1$, $(x,m)=1$, 所以 $(ax,m)=1$. 这说明 ax 是简化剩余类的剩余. 又 $ax_1 \equiv ax_2 \pmod m$ 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, ax 遍历 $\varphi(m)$ 个数, 且它们两两模 m 不同余. 根据定理 2, ax 遍历模 m 的一个简化剩余系.

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

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

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

例 8 设 $m = 7$.

$a \setminus x$	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

定理 4 设 $(a,m)=1$. 则存在整数 a', $1 \le a' < m$ 使得

$$aa' \equiv 1 \pmod{m}.$$

证一 (存在性证明). 因为 $(a,m)=1$, 根据定理 3, x 遍历模 m 的一个最小简化剩余系时, ax 也遍历模 m 的一个简化剩余系. 因此, 存在整数 $x=a'$, $1 \le a' < m$ 使得 aa' 属于 1 的剩余类, 即 $aa' \equiv 1 \pmod{m}$. 证毕.

证二 (构造性证明). 因为 $(a,m)=1$, 根据 §1.3 定理 5, 运用广义欧几里得除法, 可找到整数 s, t 使得 $sa+tm=(a,m)=1$. 因此, 整数 $a'=s \pmod{m}$ 满足 $aa' \equiv 1 \pmod{m}$.

定理 5 设 $(m_1, m_2) = 1$. 如果 x_1, x_2 分别遍历模 m_1 和模 m_2 的简化剩余系，则 $m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的简化剩余系.

证 先证明：$(x_1, m_1) = 1, (x_2, m_2) = 1$ 时，$(m_2x_1 + m_1x_2, m_1m_2) = 1$.

事实上，因为 $(m_1, m_2) = 1$

$$(m_2x_1 + m_1x_2, m_1) = (m_2x_1, m_1) = (x_1, m_1) = 1,$$

$$(m_2x_1 + m_1x_2, m_2) = (m_1x_2, m_2) = (x_2, m_2) = 1.$$

得到 $(m_2x_1 + m_1x_2, m_1m_2) = 1$

其次，证明模 m_1m_2 的任一简化剩余可表示为 $m_2x_1 + m_1x_2$,

其中 $(x_1, m_1) = 1, (x_2, m_2) = 1$

模 m_1m_2 的任一剩余可以表示为 $m_2x_1 + m_1x_2$

因此，当 $(m_2x_1 + m_1x_2, m_1m_2) = 1$ 时

$$(x_1, m_1) = (m_2x_1, m_1) = (m_2x_1 + m_1x_2, m_1) = 1$$

同理，$(x_2, m_2) = 1$. 结论成立.

定理 6 设 m, n 是互素的两个正整数. 则 $\varphi(mn) = \varphi(m)\varphi(n)$

证 根据定理 5, 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 $\varphi(m)$ 个整数时, $ym + xn$ 遍历模 mn 的简化剩余系, 其整数个数为 $\varphi(m)\varphi(n)$. 但模 mn 的简化剩余系的元素个数又为 $\varphi(mn)$. 因此, 所以 $\varphi(mn) = \varphi(m)\varphi(n)$.

例 11 $\varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60.$

例 12 $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = 1 \cdot 2 \cdot 4 = 8$

定理 7 设 n 有标准因数分解式为 $n = \Pi_{p|n} p^{\alpha} = p_1^{\alpha_1} \cdots p_k^{\alpha_s}$. 则

$$\varphi(n) = n\,\Pi_{p|n}(1-\frac{1}{p}) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$$

证 当 $n = p^{\alpha}$ 为素数幂时，模 n 的完全剩余系为

$$0,\ 1,\ \ldots,\ p-1,\ldots \qquad p(p^{\alpha-1}-1),\ p(p^{\alpha-1}-1)+1,\ \ldots,\ p^{\alpha}-1$$

共有 $n = p^{\alpha}$ 个整数，其中与 n 不互素的整数为

$$p\cdot 0,\ \ p\cdot 1,\ \ \ldots,\ \ p(p^{\alpha-1}-1),$$

共有 $p^{\alpha-1}$ 个整数. 因此，模 $n = p^{\alpha}$ 的简化剩余系的元素个数为 $p^{\alpha} - p^{\alpha-1}$. 即 $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$. 根据定理 6, 我们有

$$\varphi(n) = \prod_{p|n} \varphi(p^{\alpha}) = \prod_{p|n} (p^{\alpha} - p^{\alpha-1}) = n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})$$

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

证明 由定理 7, 有 $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = pq-p-q+1.$

例 13 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.

定理 8 设 n 是一个正整数. 则 $\Sigma_{d|n}\varphi(d)=n.$

证 对于正整数 $d|n$, 记

$$C_d=\{m \mid 1\le m\le n,\ (m,n)=d\}.$$

因为 $(m,n)=d$ 的充要条件是 $(\frac{m}{d},\frac{n}{d})=1$, 所以 C_d 中元素 m 的形式为

$$C_d=\{m=dk \mid \quad 1\le k\le \frac{n}{d},\quad (k,\frac{n}{d})=1\ \}$$

因此, C_d 中的元素个数为 $\varphi(\frac{n}{d})$. 因为整数 $1,\ldots,n$ 中的每个整数属于且仅属于一个类 C_d, 所以

$$\#(C)=\sum_{d|n}\#(C_d) \quad 或 \quad n=\sum_{d|n}\varphi(\frac{n}{d})$$

$$故 \quad n=\sum_{d|n}\varphi(\frac{n}{d})=\sum_{d|n}\varphi(d)$$

例 14 设整数 $n = 50$. 则 n 的正因数为 $d = 1,\ 2,\ 5,\ 10,\ 25,\ 50.$ 这时，定理 8 的分类为：

$$C_1 = \{1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19,\ 21,\ 23,\ 27,\ 29,\ 31,\ 33,\ 37,\ 39,\ 41,\ 43,\ 47,\ 49\};$$

$$C_2 = \{2,\ 4,\ 6,\ 8,\ 12,\ 14,\ 16,\ 18,\ 22,\ 24,\ 26,\ 28,\ 32,\ 34,\ 36,\ 38,\ 42,\ 44,\ 46,\ 48\};$$

$$C_5 = \{5,\ 15,\ 35,\ 45\}; \quad c_{10} = \{10,\ 20,\ 30,\ 40\};$$

$$C_{25} = \{25,\}; \qquad C_{50} = \{50\}.$$

$$\#(C_1) = \varphi(50) = 20, \quad \#(C_2) = \varphi(25) = 20,$$

$$\#(C_5) = \varphi(10) = 4, \quad \#(C_{10}) = \varphi(5) = 4,$$

$$\#(C_{25}) = \varphi(2) = 1, \quad \#(C_{50}) = \varphi(1) = 1.$$

$$50 = \varphi(50) + \varphi(25) + \varphi(10) + \varphi(5) + \varphi(2) + \varphi(1) = \sum_{d|50} \varphi(d).$$

欧拉定理　费马小定理

定理 1 (Euler) 如果 $(a, m) = 1$, 则 $a^{\varphi(m)} \equiv 1 \pmod{m}$.

证 取 $r_1, \ldots, r_{\varphi(m)}$ 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， $ar_1, \ldots, ar_{\varphi(m)}$ 也为模 m 的一个简化剩余系， 这就是说， $ar_1, \ldots, ar_{\varphi(m)}$ 模 m 的最小正剩余是 $r_1, \ldots, r_{\varphi(m)}$ 的一个排列.

$$(ar_1) \cdots (ar_{\varphi(m)}) \equiv r_1 \cdots r_{\varphi(m)} \pmod{m}.$$

$$r_1 \cdots r_{\varphi(m)} (a^{\varphi(m)} - 1) \equiv 0 \pmod{m}.$$

因为 $(r_1 \cdots r_{\varphi(m)}, m) = 1$

$$a^{\varphi(m)} - 1 \equiv 0 \pmod{m}.$$

例 3 设 $m = 11, a = 2.$ 则 $(2, 11) = 1, \varphi(11) = 10.$ 故 $2^{10} \equiv 1 \pmod{11}$.

定理 2 (Fermat) 设 p 是一个素数. 则对任意整数 a, 我们有

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

证 i) 若 a 被 p 整数, 则同时有 $a \equiv 0 \pmod{p}$ 和 $a^p \equiv 0 \pmod{p}$. 因此, $a^p \equiv a \pmod{p}$.

ii) 若 a 不被 p 整数, 则 $(a, p) = 1$ (见 §1.3 例 4). 根据定理 1,

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

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

RSA的CRT解密运算使用约减的指数

例 5 设 p, q 是两个不同的奇素数，$n = pq$, a 是与 pq 互素的整数. 如果整数 e 满足 $1 < e < \varphi(n)$, $(e, \varphi(n)) = 1$, 那么存在整数 d, $1 \leq d < \varphi(n)$, 使得

$$ed \equiv 1 \pmod{\varphi(n)}.$$

而且，对于整数 $a^e \equiv c \pmod{n}$, $1 \leq c < n$, 有 $c^d \equiv a \pmod{n}$.

证

$$ed = 1 + k\varphi(n)$$

$$c^d = a^{ed} = a^{1+k\varphi(n)} = a(a^{\varphi(n)})^k = a \cdot 1^k = a \pmod{n}$$

模重复平方计算法

$b^n \pmod m$ $\qquad$ $b^n \equiv (b^{n-1} \pmod m) \cdot b \pmod m$

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

其中 $n_i \in \{0, 1\},\ i = 0, 1, \ldots, k-1$. 则 $b^n \pmod m$ 的计算可归纳为

$$b^n \equiv \underbrace{\underbrace{b^{n_0}(b^2)^{n_1}}_{} \cdot \cdots \cdot (b^{2^{k-2}})^{n_{k-2}}}_{} \cdot (b^{2^{k-1}})^{n_{k-1}} \pmod m.$$

我们最多作 $2[\log_2 n]$ 次乘法. 这个计算方法叫做 "**模重复平方计算**

具体算法如下：

$$b^n \equiv \underbrace{b^{n_0}(b^2)^{n_1} \cdot \cdots \cdot (b^{2^{k-2}})^{n_{k-2}} \cdot (b^{2^{k-1}})^{n_{k-1}}}_{\text{}} \pmod{m}.$$

具体算法如下：

0). 令 $a = 1$, 并将 n 写成二进制： $n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}$

1). 计算 $a_0 \equiv a \cdot b^{n_0} \pmod{m}$. 再计算 $b_1 \equiv b^2 \pmod{m}$.

2). 计算 $a_1 \equiv a_0 \cdot b_1^{n_1} \pmod{m}$. 再计算 $b_2 \equiv b_1^2 \pmod{m}$. ……

k-1). 计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod{m}$. $b_{k-1} \equiv b_{k-2}^2 \pmod{m}$.

k). 计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod{m}$.

最后， a_{k-1} 就是 $b^n \pmod{m}$.

- RSA加解密运算使用重复平方法
- 上述重复平方法是从低位到高位进行计算
- 重复平方法还有从高位到低位计算的次序
  计算复杂度相同，但存储略有不同（从高位到低位略好）
- 其他进制表示法：预计算 + 从低位到高位

NAJ表达式

- 重复平方法对任意群适用
- 如果群里求逆无需代价（如椭圆曲线），则可用带负号二进制表达式

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

其中，系数为1，0，-1

- 任意n总有一个NAJ表达式：相邻两个系数有一个为0
- NAJ表达式的平均重量为log_2(n)/3
- 常规二进制表达式的平均重量为log_2(n)/2

带负号二进制算法

- 对于某些群，如椭圆曲线的点群，群元素的逆可能非常容易求得，这时可以将的二进制表示改变为 $a=\sum a_i 2^i, a_i \in \{-1,0,1\}$

  则 $g^a=(\prod_{a_i=1} g^{2^i})\cdot(\prod_{a_i=-1}(g^{2^i})^{-1})$

- $2^{i-1}+2^{i-2}+\cdots+2+1=2^i-1$

  $a=(11010111110001011101)_2$

  $a=(10-101-1000-10010-100-101)_2$

Shamir's trick

- 计算$g^a h^b$ 的快速算法
- 在DSA数字签名标准算法中出现
- 双基链：$k = \sum s_i 2^{ai} 3^{bi}$, 其中$s_i$为±1或0，$\{a_i\}$单调递增，$a_i - a_{i-1}$ 小，$\{b_i\}$单调递增，$b_i - b_{i-1}$ 小，2P和3P容易计算
- 多基链

例：计算$g^{37}h^{20}$如下

$37=$	$(1$	0	0	1	0	$1)_2$
$20=$	$(0$	1	0	1	0	$0)_2$
$\wedge 2$	1	g^2	g^4h^2	g^8h^4	$g^{18}h^{10}$	$g^{36}h^{20}$
$\cdot g$	g					$g^{37}h^{20}$
$\cdot h$		g^2h				
$\cdot gh$				g^9g^5		

Montgomery Form

- Consider to compute ab (mod N)
- Instead of a and b, we work with fast computing abR (mod N) from
  a′ = aR (mod N) and b′ = bR (mod N)
- The numbers a′ and b′ are said to be in **Montgomery form**
- Where we take R := 2^k > N and gcd(R,N) = 1 for free mod R and div R operations
- Also, find R′ and N′ so that RR′ – NN′ = 1 with 0<N′<R, 0<R′<N<R,

The Idea

- Have $a' = aR \pmod N$ and $b' = bR \pmod N$
- $abR = a'b'R^{-1} \pmod N$
- Let $X = a' \cdot b'$. Then $abR = XR^{-1} \pmod N$
- We try to find an integer $X+mN$, s.t. it is a multiple of R. Then $XR^{-1} = (X+mN)/R \pmod N$
- **What is m?**

  $X + mN = 0 \pmod R$

  $XN' + mNN' = 0 \pmod R$

  $XN' + m(RR'-1) = 0 \pmod R$

  $XN' = m \pmod R$
- **Further,** $(X+mN)/R$ can be not far away **from N**

Key Step

- Compute $x = XR^{-1} \pmod N$ from $0 < X < N^2$
- **Montgomery reduction**

  $m = ((X \bmod R) \cdot N') \bmod R$ (1 integer mul)

  $x = (X + m \cdot N)/R$ (1 integer mul)

  if $x \geq N$ then (Claim: $0 < x < 2N$)

  x = x – N // extra reduction

  end if
- return x
- Claim: $0 < x < N$ and $x = XR^{-1} \pmod N$

Proof

- $X+mN$ is a multiple of R.

$$XN' = m \pmod R$$
$$XN' + m(RR'-1) = 0 \pmod R$$
$$XN' + mNN' = 0 \pmod R$$
$$X + mN = 0 \pmod R$$

- It is clear that $x = a'b'R^{-1} \pmod N$ since

$$x = (X + m \cdot N)/R$$

- $0<x<2N$?

$$X<N^2,\ \ m<N,\ N<R,$$
$$(X + m \cdot N)/R < (N^2 + N \cdot N)/N = 2N$$

Montgomery Reduction

- Have $0 < a' < N$ and $0 < b' < N$
- Compute $X = a' \cdot b'$ (1 integer multiplication)
- **Montgomery reduction**

  $m = ((X \bmod R) \cdot N') \bmod R$ (1 integer mul)

  $x = (X + m \cdot N)/R$ (1 integer mul)

  if $x \geq N$ then (Claim: $0 < x < 2N$)

  $x = x - N$ // extra reduction

  end if
- return x
- Claim: $0 < x < N$ and $x = a'b'R^{-1} \pmod N$

Montgomery Exponentiation mod *N*

- Given odd number N, index e, and 0<a<N, to compute $a^e \pmod N$
- Take $R = 2^k > N$, find $0<N'<R$ s.t. $NN' = -1 \pmod R$

  (a precomputation for *N*)
- Compute $a' = aR \pmod N$ (an extra operation)
- Compute $y=a^eR \pmod N$ according to Montgomery multiplication in any repeated-squaring-and-multiplication way

  (In each iteration, 3 multiplications of integers are involved, no mod N operations)
- Compute $a^e = yR^{-1} \pmod N$ (2 muls of integers)

Example

- Montgomery operator: $a' \bigstar b' = a'b'R^{-1} \pmod N$

  $(aR) \bigstar (bR) = (ab)R \pmod N$

  Write $(a')^{\bigstar 2} = a' \bigstar a'$
- $e=13=8+4+1=(1101)_2$,

  $a^{13} = (((a)^2 a)^2 \cdot 1)^2 a \pmod N$
- Compute $a' = aR \pmod N$ (an extra operation)
- Compute $a^{13}R = (((a')^{\bigstar 2} \bigstar a')^{\bigstar 2} \bigstar R)^{\bigstar 2} \bigstar a' \pmod N$

  (Note: $a' \bigstar R = a'$, do nothing)
- Compute $a^{13} = (a^{13}R) \cdot R' \pmod N$ (another extra operation)

Montgomery 模幂运算

- 模多项式的Montgomery 模幂运算完全类似

Q&A