

# Discrete

## Mathematics - P68

对于素数  $p$ , 对任意正整数  $a$  且  $p \nmid a$ , 有  $a^{p-1} \equiv 1 \pmod{p}$  (根据费马小定理)

如果存在  $b \in \mathbb{Z}^+$  且  $b < p-1$ , 有  $a^b \equiv 1 \pmod{p}$ , 则  $b \mid p-1$ , 即  $p-1 = kb$  (最小的), 即  $\exists b \in \mathbb{Z}^+ (a^b \equiv 1 \pmod{p}) \rightarrow \forall n \in \mathbb{Z}^+ (a^n \equiv 1 \pmod{p} \rightarrow b \mid n)$

梅森数的素因子, 对于奇素数  $p$ , 梅森数  $M_p = 2^p - 1$ , 其每个素因子都形如  $2kp + 1$ , 其中  $k \in \mathbb{N}$

如果存在大于2的素数  $q$ , 使得  $q \mid M_p$ , 即  $q$  是梅森数  $M_p = 2^p - 1$  的素因子  
则  $q \mid 2^p - 1$ , 即  $2^p \equiv 1 \pmod{q}$

又对于素数  $q \geq 2$ , 有  $q \nmid 2$ , 即  $2^{q-1} \equiv 1 \pmod{q}$

于是有  $p \mid q-1$ , 即  $p \mid q = 1 + lp$ ,  $l \in \mathbb{N}$ , ( $p$  是素数, 即不存在  $1 < b < p$ , 使  $b \mid p$ )

又  $q$  为奇数,  $p$  也为奇数, 所以  $l$  为偶数, 即  $p \mid l = 2k$ ,  $k \in \mathbb{N}$

即有梅森数  $M_p$  的素因子都具有  $2kp + 1$  ( $k \in \mathbb{N}$ ) 的形式

### 原根

(primitive root modulo  $p$ ), 对于素数  $p$ , 模  $p$  的原根是  $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$  中的整数  $r$

使得  $\mathbb{Z}_p$  中的每个非零元素  $a$ , 都是  $r$  的一个幂次:

即有  $\forall a \in \mathbb{Z}_p \setminus \{0\} \rightarrow \exists k \in \mathbb{Z}^+ r^k \pmod{p} = a$

对于每个素数  $p$ , 都存在一个模  $p$  的原根,

即有  $\forall p \in \mathbb{Z}^+ (p \text{ 是素数} \rightarrow \exists r \in \mathbb{Z}^+ (1 \leq r \leq p-1 \wedge (\forall a \in \mathbb{Z}_p \setminus \{0\} \rightarrow \exists k \in \mathbb{Z}^+ r^k \pmod{p} = a)))$

对于素数  $p$ ,  $r$  是模  $p$  的原根, 则对于每个  $\mathbb{Z}_p$  中的非零元素  $a$ , 存在唯一  $[1, p-1]$  的幂次  $e$ , 使  $r^e \pmod{p} = a$

即对于素数  $p$  和模  $p$  的原根  $r$ ,  $\forall a \in \mathbb{Z}_p \setminus \{0\} \rightarrow \exists e \in \mathbb{Z}^+ (1 \leq e \leq p-1 \wedge r^e \pmod{p} = a)$

### 离散对数

(discrete logarithm). 对于素数  $p$ ,  $r$  是模  $p$  的一个原根,  $a$  为整数且  $1 \leq a \leq p-1$

如果有  $r^e \pmod{p} = a$  且  $1 \leq e \leq p-1$ , 则称  $e$  为以  $r$  为底  $a$  模  $p$  的离散对数, 记作  $\log_r a = e$

对于奇素数  $p$ ,  $r$  是模  $p$  的原根, 如果  $a$  和  $b$  是  $\mathbb{Z}_p$  中的正整数, 则  $\log_r (ab) \equiv \log_r a + \log_r b \pmod{p-1}$

证明过程有, 对于奇素数  $p > 2$ , 集合  $\{1, 2, \dots, p-1\}$  中共有  $p-1$  个元素.

对于其中任意一个元素  $a$ , 都有正整数  $1 \leq e \leq p-1$ ,  $r^e \equiv a \pmod{p}$

又  $a^{p-1} \equiv 1 \pmod{p}$ , 则对于任意非负整数  $k \in \mathbb{N}$ ,  $r^{e+k(p-1)} \equiv r^{k(p-1)} \cdot r^e \equiv r^e \equiv a \pmod{p}$

即有  $\forall e' \in \mathbb{Z}^+ (e' \equiv e \pmod{p-1}) \rightarrow r^{e'} \equiv r^e \equiv a \pmod{p}$

令有对于  $a, b \in \{1, 2, \dots, p-1\}$ , 存在正整数  $1 \leq e_a, e_b \leq p-1$ , 使得  $r^{e_a} \equiv a \pmod{p}$   
 $r^{e_b} \equiv b \pmod{p}$

即有  $r^{e_a+e_b} \equiv r^{e_a} \cdot r^{e_b} \equiv r^{(e_a+e_b) \pmod{p-1}} \pmod{p}$ , 又  $\log_r a = e_a$ ,  $\log_r b = e_b$

即有  $\log_r ab \equiv e_a + e_b \equiv \log_r a + \log_r b \pmod{p-1}$

# Discrete

## Mathematics - P69

二次剩余 (quadratic residue) 指对于正整数  $m$  和整数  $a$ , 且有  $\gcd(a, m) = 1$

如果同余式  $x^2 \equiv a \pmod{m}$  有解, 则称整数  $a$  为  $m$  的二次剩余

或者说  $m$  的一个二次剩余是与  $m$  互素的整数且与一个完全平方数模  $m$  同余

即有对于  $m \in \mathbb{Z}^+$ , 且  $a \in \mathbb{Z}$  且  $\gcd(a, m) = 1$

如果  $x^2 \equiv a \pmod{m}$  无解, 则称  $a$  为  $m$  的二次非剩余 (quadratic nonresidue)

即有, 对  $m \in \mathbb{Z}^+$ ,  $a \in \mathbb{Z}$ , 且  $\gcd(a, m) = 1$

$(\exists x \in \mathbb{Z}^+ \ x^2 \equiv a \pmod{m}) \Leftrightarrow a$  是模  $m$  的二次剩余,

$(\forall x \in \mathbb{Z}^+ \ x^2 \not\equiv a \pmod{m}) \Leftrightarrow a$  是模  $m$  的二次非剩余

模  $P$  不同余的解

如果  $P$  是奇素数且  $a$  为不能被  $P$  整除的整数, 则同余式  $x^2 \equiv a \pmod{P}$  要么无解, 要么恰有两个

即有对于奇素数  $P$ ,  $a \in \mathbb{Z}$  且  $P \nmid a$ ; 对于同余式  $x^2 \equiv a \pmod{P}$

$(\forall x \in \mathbb{Z}^+ \ x^2 \not\equiv a \pmod{P}) \oplus (\exists! x_1, x_2 \in \mathbb{Z}^+ (x_1^2 \equiv x_2^2 \equiv a \pmod{P}) \wedge x_1 \neq x_2 \pmod{P})$

证明过程有, 对于奇素数  $P$ ,  $a \in \mathbb{Z}$  且  $P \nmid a$ , 同余式  $x^2 \equiv a \pmod{P}$

则有  $P \mid x^2 - a$ , 于是有  $x^2 = a + kp$ , 其中  $k \in \mathbb{Z}$

由于  $P \nmid a$ , 所以不存在  $k \in \mathbb{Z}$ , 使得  $a + kp = 0$

即  $x^2 = a + kp$  不可能有相等的零根  $x_1 = x_2 = 0$ .

且  $x \not\equiv 0 \pmod{P}$ , 即取  $x \equiv k \pmod{P}$ , 且  $k \in \{1, 2, \dots, P-1\}$

如果  $a$  是  $P$  的二次非剩余, 则  $x^2 \not\equiv a \pmod{P}$  无解

如果  $a$  是  $P$  的二次剩余, 则  $x \equiv k \pmod{P}$ , 且  $k \in \{1, 2, \dots, P-1\}$  存在

且  $k' = P - k$ , 则  $k'^2 \pmod{P} = (P - k)^2 \pmod{P} = k^2 \pmod{P} = a \pmod{P}$

即  $k'$  也是  $x^2 \equiv a \pmod{P}$  的解.

又  $P$  是奇素数, 所以  $P - k' = P - k \neq k$ , 且  $k, k' \in \{1, 2, \dots, P-1\}$

于是有此时  $x^2 \equiv a \pmod{P}$  有且仅有两个模  $P$  同余的解

如果  $P$  是奇素数, 则在  $\{1, 2, \dots, P-1\}$  中恰有  $(P-1)/2$  个模  $P$  的二次剩余

对于奇素数  $P$ , 集合  $\{1, 2, \dots, P-1\}$  中有偶数个元素

对于  $k \in \{1, 2, \dots, (P-1)/2\}$ ,  $P - k \in \{(P+1)/2, \dots, P-2, P-1\}$ ,

且  $(P-k)^2 \pmod{P} = k^2 \pmod{P}$ , 即  $(P-k)^2 \equiv k^2 \equiv l \pmod{P}$ ,  $l \in \{1, 2, \dots, P-1\}$

而对于  $i, j \in \{1, 2, \dots, (P-1)/2\}$  且  $i < j$ ,

则  $j^2 - i^2 = (j-i)(j+i)$ , 又  $0 < j-i, j+i < P$ ,

所以  $i^2 \neq j^2 \pmod{P}$ ,

于是如果  $x^2 \equiv a \pmod{P}$  有解, 则有且仅有两个模  $P$  不同余的根,

且  $\{1, 2, \dots, P-1\}$  有且仅有  $(P-1)/2$  个模  $P$  的二次剩余

# Discrete

## Mathematics - P70

勒让德符号 (Legendre symbol), 用  $(\frac{a}{p})$  表示, 对于奇素数  $p$  和不能被  $p$  整除的整数  $a$ , 如果  $a$  为模  $p$  的二次剩余, 则  $(\frac{a}{p}) = 1$ , 如果  $a$  为模  $p$  的二次非剩余, 则  $(\frac{a}{p}) = -1$ . 另外特别的有, 当  $p \mid a$  时, 定义  $(\frac{a}{p}) = 0$ .

如果  $p$  为奇素数, 而  $a$  和  $b$  为整数, 且有  $a \equiv b \pmod{p}$ , 则有  $(\frac{a}{p}) = (\frac{b}{p})$ .

证明过程有, 对于  $a$  和  $b$  为不能被奇素数  $p$  整除的整数,  $\gcd(a, p) = 1$  且  $\gcd(b, p) = 1$ .

考虑同余式  $x^2 \equiv a \pmod{p}$  的解, 即有  $x^2 \equiv b \pmod{p}$ .

当  $x^2 \equiv a \pmod{p}$  有解时,  $a$  和  $b$  都是模  $p$  的二次剩余,  $(\frac{a}{p}) = (\frac{b}{p}) = 1$ .

当  $x^2 \equiv a \pmod{p}$  无解时,  $a$  和  $b$  都是模  $p$  的二次非剩余,  $(\frac{a}{p}) = (\frac{b}{p}) = -1$ .

欧拉准则 (Euler's criterion), 对于奇素数  $p$  和整数  $a$  且  $p \nmid a$ , 则有  $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

证明过程有, 如果  $a$  是模  $p$  的二次剩余, 则有  $(\frac{a}{p}) = 1$ .

且  $\exists x \in \mathbb{Z}^+ : x^2 \equiv a \pmod{p} \wedge p \nmid x$ .

于是有  $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \equiv (\frac{a}{p}) \pmod{p}$ .

如果  $a$  是模  $p$  的二次非剩余, 则有  $(\frac{a}{p}) = -1$ .

则  $\forall x \in \mathbb{Z}^+ : x^2 \not\equiv a \pmod{p} \wedge p \nmid x$ .

于是有  $a^{\frac{p-1}{2}} \not\equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ .

$x (a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ , 所以  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  或者  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ .

于是有  $a^{\frac{p-1}{2}} \equiv -1 \equiv (\frac{a}{p}) \pmod{p}$ .

如果  $p$  为奇素数, 和不能被  $p$  整除的整数  $a, b$ , 有  $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ .

证明如, 对于奇素数  $p$  和  $a, b \in \mathbb{Z}$  且  $p \nmid a, p \nmid b$ , 则有  $p \nmid ab$ .

$(\frac{ab}{p}) \equiv (cab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \pmod{p}$ .

注意蕴含着, 如果  $a$  和  $b$  都是模  $p$  的二次非剩余, 则  $ab$  是模  $p$  的二次剩余.

取整数  $d$ , 且  $p \nmid d$ , 使得  $d^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ .

取  $r$  为  $p$  的一个原根, 则存在  $i \in \mathbb{Z}^+$ , 使得  $d \equiv r^i \pmod{p}$ .

则  $(\frac{d}{p})^{\frac{p-1}{2}} \equiv d^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ , 又  $r^{p-1} \equiv 1 \pmod{p}$ .

因为  $p-1 \mid (p-1)/2$ , ( $r$  是  $p$  的原根) 则  $i$  是偶数, 有  $i = 2k, k \in \mathbb{Z}^+$ .

取  $x = r^k$ , 则  $x^2 \equiv r^{2k} \equiv r^i \equiv d \pmod{p}$ , 即  $d$  是模  $p$  的二次剩余.

于是有  $(\frac{a}{p}) = -1 \wedge (\frac{b}{p}) = -1, (\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}) = 1$ .

即  $a, b$  是模  $p$  的二次非剩余, 则  $ab$  是模  $p$  的二次剩余.

$$\left( \frac{-1}{p} \right) = \left( \frac{-1}{p} \right) = \begin{cases} 1, & p \equiv 1 \pmod{4}, \\ (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{1+(-1)}{2}} \equiv (-1)^{2k} \equiv 1 \pmod{p}, & \text{其中 } k \in \mathbb{N} \end{cases}$$

$$\text{对于奇素数 } p \equiv 3 \pmod{4}, (-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{4k+3-2}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod{p}$$

# Discrete

## Mathematics - P71

stuvell

欧拉函数  $\varphi(n)$ , 又称欧拉总计函数 (Euler's totient function), 记为  $\varphi(n)$

定义对正整数  $n$ ,  $\varphi(n)$  为小于或等于  $n$  的正整数中与  $n$  互质的数的数目

$\varphi(1)$

$\varphi(1) = 1$ , 由于对于  $a \in \mathbb{Z}^+$  且  $a \leq 1$ , 仅有  $a=1$ , 使得  $\gcd(a, 1) = 1$

$\varphi(p^k)$

对于素数  $p$  的  $k$  次幂 ( $k \in \mathbb{Z}^+$ ),  $\varphi(p^k) = p^{k-1}(p-1)$

由于对于  $a \in \mathbb{Z}^+$  且  $a \leq p^k$ , 有且仅有  $p \mid a$  时,  $\gcd(a, p^k) \neq 1$ , 这样的  $a$  有  $p^{k-1}$  个

$$\text{所以 } \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

$\varphi(mn)$

$\varphi(mn) = \varphi(m)\varphi(n)$ , 其中  $m, n$  为正整数且  $\gcd(m, n) = 1$

注意有  $\forall a \in \mathbb{Z}^+ (\boxed{\gcd(a, mn) = 1} \iff \gcd(a, m) = 1 \wedge \gcd(a, n) = 1)$

又根据中国剩余定理, 存在一个  $f: \{0, 1, \dots, m-1\} \times \{0, 1, \dots, n-1\} \rightarrow \{0, 1, \dots, mn-1\}$  一一对应

则分别从中剔除与  $m, n, mn$  不互素的元素.

可知  $f: \{0 < a \leq m | \gcd(a, m) = 1\} \times \{0 < a \leq n | \gcd(a, n) = 1\} \rightarrow \{0 < a \leq mn | \gcd(a, mn) = 1\}$

存在一个一一对应的  $f: A \times B \rightarrow C$ , 于是有  $|A| \times |B| = |C|$

即有  $\varphi(m) \times \varphi(n) = |A| \times |B| = |C| = \varphi(mn)$

$\varphi(n)$

对于正整数  $n$ , 如果  $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ , 其中  $k \in \mathbb{N}$ ,  $p_1, \dots, p_k$  为不同的素数

则有  $\varphi(n) = \varphi(p_1^{e_1}) \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) = \prod_{i=1}^k p_i^{e_i-1}(p_i-1)$

$= \prod_{i=1}^k p_i^{d_p-1}(p-1)$ , 其中  $p$  为素数,  $d_p$  为正整数, 使得  $p^{d_p} \mid n \wedge p^{d_p+1} \nmid n$

$$= \prod_{i=1}^k p_i^{d_p}(p-1)/p = \prod_{i=1}^k p_i^{d_p} \cdot \prod_{i=1}^k (1 - \frac{1}{p}) = n \cdot \prod_{i=1}^k (1 - \frac{1}{p})$$

积性函数 (multiplicative function), 指定义在正整数上的算术函数 (arithmetic function)  $f(n)$ ,  $n \in \mathbb{Z}^+$

有  $f(1) = 1$ , 且对于互素的正整数  $a, b$ , 有  $f(ab) = f(a)f(b)$

可见欧拉函数  $\varphi(n)$  是积性函数, 有  $\varphi(1) = 1$ , 且对于  $m, n \in \mathbb{Z}^+$ ,  $\gcd(m, n) = 1 \rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

另有完全积性函数 (completely multiplicative) 指  $f(ab) = f(a)f(b)$  对任意  $a, b \in \mathbb{Z}^+$  成立

欧拉定理 (Euler's theorem), 指对于正整数  $a, n$ , 有  $\gcd(a, n) = 1$ , 则有  $a^{\varphi(n)} \equiv 1 \pmod{n}$

一般化 费马小定理: 对于素数  $p$ ,  $\forall a \in \mathbb{Z}^+ \setminus \{p\}$ , 有  $a^p \equiv a \pmod{p}$

高斯版本 欧拉定理: 对于互素的正整数  $a, n$ , 有  $a^{\varphi(n)} \equiv 1 \pmod{n}$

如果  $p$  是素数, 且  $p \nmid a \in \mathbb{Z}^+$ , 则  $a^{\varphi(p)} \equiv 1 \equiv a^{p-1} \pmod{p}$

eulerTotient  $n =$  (eulerTotient :: Int → Int)

let func acc rest lst = based on  $\varphi(n) = n \cdot \prod_{p \mid n} (1 - \frac{1}{p})$

  | null lst = acc \* rest    $= n \cdot \prod_{p \mid n} (p-1) / \prod_{p \mid n} p$

  | otherwise w = let p = head lst   | l = filter (\x → x `mod` p /= 0) lst

  | in if (rest `mod` p /= 0) then func acc rest l

  | else func (acc \* (p-1)) (rest `div` p) l

in func 1 n [2..n]

# Discrete

## Mathematics - P72

STRUCTURE

离散对数问题

输入: 素数  $P$ , 模  $P$  的原根  $r$ , 正整数  $a \in \mathbb{Z}_P$   
输出: 以  $r$  为底  $a$  模  $P$  的离散对数

特别注意: 实际上没有已知的多项式时间算法求解离散对数问题

散列函数 (hash function), map data of arbitrary size to data of a fixed size

使用键 (key), 返回散列值 (hash value)

当多个 key 映射到同一个 hash value 时, 称出现了冲突 (collision)

消解冲突的方法之一是使用散列函数分配已占用地址后边的第一个未占用的地址  
线性探测函数 (linear probing), 即  $h(k, i) = \boxed{\text{hash}}(k) + i \pmod m$ , 其中  $0 \leq i \leq m-1$   
 $(h(k) + i)$

伪随机数 (pseudorandom number), 由系统方法生成的数并非真正随机, 所以为伪随机数

线性同余方法 (linear congruential generator), 是最常用的产生伪随机数的过程

模数  $m \in \mathbb{Z}^+$ , 为生成伪随机数范围, 即有  $\{0, 1, \dots, m-1\}$

倍数  $a$ ,  $2 \leq a < m$  用于生成连续地生成伪随机序列  $\{x_n\}$  的下一项

增量  $c$ ,  $0 \leq c < m$

种子  $x_0$ , 作为伪随机数序列  $\{x_n\}$  的第一项,  $0 \leq x_0 < m$

递归函数: 对于任意  $n \in \mathbb{N}$ , 有  $0 \leq x_n < m$ , 有  $x_{n+1} = (ax_n + c) \pmod m$

如, 取  $x_0 = 3$ ,  $x_{n+1} = (7x_n + 4) \pmod 9$

则有  $x_1 = 7 \rightarrow 8 \rightarrow 6 \rightarrow 1 \rightarrow 2 \rightarrow 0 \rightarrow 4 \rightarrow 5 \rightarrow 3 \rightarrow 7 \rightarrow \dots$

纯倍式生成器, 指使用增量  $c=0$  的线性同余生成器

特别注意: 由此生成的伪随机数序列不具有真正的随机数具有的重要统计特性

奇偶校验位 (parity bit), 将位串子的数字信息划分成指定大小的块, 并在块结尾添加一个额外位

如对于位串  $x_1 x_2 \dots x_n$ , 定义奇偶校验位为

$$x_{n+1} = (x_1 + x_2 + \dots + x_n) \pmod 2$$

注意: 奇偶校验位可以检测块中奇数个错误, 但无法检测偶数个错误

通用产品代码 (Universal Product Code, UPC), 由1位产品种类, 5位制造商, 5位特定产品, 最后一位校检位

$$\text{校验式: } 3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$$

国际标准书号 (International Standard Book Number, ISBN-10), 为10位数代码, 最后一位为校验码

$$\text{使得满足 } x_{10} = (\sum_{i=1}^9 ix_i) \pmod{11}, \text{ 即有 } \sum_{i=1}^9 ix_i \equiv 0 \pmod{11}$$

$$11x_{10} \equiv (\sum_{i=1}^9 ix_i) + 10x_{10} \pmod{11}, \text{ 即 } \sum_{i=1}^9 ix_i \equiv 0 \pmod{11}$$

# Discrete

## Mathematics - P73

STORY

7.9 - 2019.9.10



单错

指校检码中仅有一位数字的错误，是最常见的一类错误

换位错

指校检码中两位数字颠倒的错误，是另一类常见错误

双散列函数(secondary re-hashing), 或 double hashing). 指使用两个散列函数取得散列值

即先使用一个初始散列函数  $h(k)$ , 再使用第二个散列函数  $g(k)$

如果发生冲突，则使用一个探测序列(probing sequence)

即有  $h(k, i) = (h(k) + i \cdot g(k)) \bmod p$ , 其中  $0 \leq i < p$

如取素数  $p$ , 初始散列函数  $h(k) = k \bmod p$ , 第二个散列函数  $g(k) = (k+1) \bmod (p-2)$

平方取中法(middle-square method), 指从正整数  $a$  生成伪随机数序列

方法为, 先取  $a$  的平方, 并在  $a^2$  前添加 0 以保证为  $2n$  位的整数

然后取中间的  $n$  位数字作为下一个伪随机数

即有伪随机数序列  $\{x_n\}$ , 其中  $x_0 = a$ ,

对于  $n \in \mathbb{N}^+$ ,  $x_n = (x_{n-1}^2 \bmod 10^{2n})$

middleSquare :: Int → Int → [Int]

middleSquare  $x_0$  n  $k_0$  =

let func x k lst

|  $k == 0$  = lst

| otherwise = let

$x' = (x * x) \bmod 10^{2k}$

    in func  $x'$  (k-1) (lst ++ [x'])

  in func  $x_0$  k0 [x0]

如: middleSquare 2357 4 5 → [2357, 5554, 8469, 7239, 4031]

middleSquare 3792 4 5 → [3792, 3792, 3792, 3792, 3792]

幂次生成器

为一种生成伪随机数序列, 取素数  $P$  和不能被  $P$  整除的正整数  $d$ , 以及种子  $x_0$ 。

并有对于  $n \in \mathbb{N}^+$ , 递归定义  $x_n = x_{n-1}^{d^n} \bmod p$

expIter p d x0 k0 = (expIter :: Int → Int → Int → Int → [Int])

let func x k lst

|  $k == 0$  = reverse lst ] 由于生成的是双向序列, 所以输出前需要反转

| otherwise = let x' = myPowerMod x d p ]  $x' = x^d \bmod p$

  in func  $x'$  (k-1) (x': lst)

  in func  $x_0$  k0 [x0]

# Discrete

## C Mathematics - P74

美国邮政署 (The United States Postal Service, USPS) 汇票标识码，由 11 位数字  $x_1, x_2, \dots, x_{10}$  标识汇票，前 10 位为标识码，校检码  $x_{11} = (x_1 + x_2 + \dots + x_{10}) \bmod 9$

国际标准连续出版物号 (International Standard Serial Number, ISSN)，若两组 4 位数字构成

第二组的最后一位为校检码，有  $d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}$

当  $d_8 \equiv 10 \pmod{11}$  时，用字母 X 表示  $d_8$

加密

(Encryption)：指使消息成为秘密的过程

解密

(Decryption)：指将秘密消息还原到原始形式的过程

加密密钥

(Encryption key)：指确定的选用加密函数系列的一个值

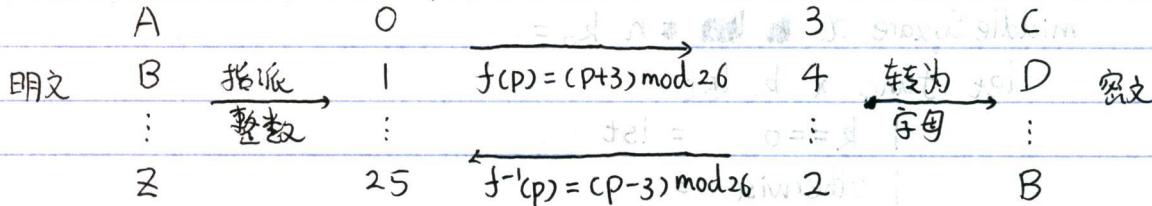
移位密码 (Shift cipher)，指将明文字母  $p$  加密为  $f(p) \bmod m$  的密码，密钥  $k$  为整数

而解密过程则为  $f^{-1}(p) = (p - k) \bmod m$

如恺撒密码 (Caesar cipher)，首先为字母 A~Z 指派整数  $\{0, 1, \dots, 25\}$

然后有加密函数  $f(p) = (p + 3) \bmod 26$

解密函数  $f^{-1}(p) = (p - 3) \bmod 26$



`char caesar_cipher const char &C){`

`return char(cc - 'a' + 3) % 26 + 'a');`

`char caesar_decrypt const char &C){`

`return char(cc - 'a' + 23) % 26 + 'a');`

仿射密码 (Affine cipher)，将明文字母  $p$  加密成  $(ap + b) \bmod m$  的密码，其中  $a, b$  为整数且有  $\gcd(a, m) = 1$

即有仿射变换  $f(p) = (ap + b) \bmod m$ ，注意  $f(p)$  必须为一个双射函数

其解密函数  $f^{-1}(p) = \bar{a}(b-p) \bmod m$ ，其中  $\bar{a}$  为  $a$  模  $m$  的逆元

字符密码 (Character cipher)，逐个字符加密的密码，或称单码密码

注意这种加密方法面对基于密文中字频率分析的破译是脆弱的

英文字母频率 E 13% > T 9% > A 8% > O 8% > I 7% > N 7% > S 7%

# Discrete

## Mathematics - P75

换位密码 是一种简单的分组密码，密钥为定义在  $\{1, 2, \dots, m\}$  上的 $1-1$  对应关系，其中  $m \in \mathbb{Z}^+$ 。  
 即密钥为一个置换  $\sigma: \{1, \dots, m\} \rightarrow \{1, \dots, m\}$ ,  $\sigma$  为 $1-1$  对应函数。  
 方法是，将明文分成大小为  $m$  的块，如果不能被  $m$  整除，可在结尾加入随机字符。  
 对于每一个  $m$  位的分组  $P_1, P_2, \dots, P_m$ ，加密为  $C_1, C_2, \dots, C_m$ 。  
 使得  $C_1, C_2, \dots, C_m = P_{\sigma(1)}, P_{\sigma(2)}, \dots, P_{\sigma(m)}$ 。  
 而当解密  $C_1, C_2, \dots, C_m$  时，取  $P_1, P_2, \dots, P_m = C_{\sigma^{-1}(1)}, C_{\sigma^{-1}(2)}, \dots, C_{\sigma^{-1}(m)}$ 。  
 由于  $\sigma(i)$  为 $1-1$  对应函数，则可知  $P_{\sigma(1)}, P_{\sigma(2)}, \dots, P_{\sigma(m)}$  为  $P_1, P_2, \dots, P_m$  的一个排列。

同理  $(C_{\sigma^{-1}(1)}, C_{\sigma^{-1}(2)}, \dots, C_{\sigma^{-1}(m)})$  是  $(C_1, C_2, \dots, C_m)$  的一个排列。

如 取  $\sigma: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$       P I R A I T E A T I T A C K  
 $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2$       I A P R | E T T A | A K T C

分组密码 (block cipher)，按等长字符串分组加密的密码，通过用一组字母替换另一组字母。

密码分析 (cryptanalysis)，指在没有加密方法的信息或者有加密方法但没有密钥时，试图从密文恢复出明文的过程。

密码系统 (cryptosystem)，为一个五元组  $(P, C, K, E, D)$ ，形式化地定义一系列新的密码。

其中， $P$  为明文串的集合， $C$  为密文串的集合， $K$  是所有可能的密钥的集合。

$E$  为加密函数的集合， $D$  为解密函数的集合。

取  $E_k$  为  $E$  中应用密钥  $k$  的加密函数，即  $C = E_k(p)$ 。

$D_k$  为  $D$  中应用密钥  $k$  的解密函数，即  $p = D_k(C)$ 。

于是有  $\forall p \in P \quad p = D_k(E_k(p))$ 。

如对于多位密码，可有形式化的定义为：首先有字表  $I = \{a, b, \dots, z\}$ 。

则有明文串集合  $P$  和密文串集合  $C$ ， $I^* = \{a, b, \dots, z\}^*$ 。

密钥集合  $K = \{k \in \mathbb{Z}^+ \mid k < m\}$ ，其中  $m = |I| = 26$ 。

加密函数集合  $E = \{E_k(p) = (p + k) \bmod m \mid p \in I, k \in K\}$ 。

解密函数集合  $D = \{D_k(c) = (c - k) \bmod m \mid c \in C, k \in K\}$ 。

如恺撒密码有加密函数  $E_3(p) = (p + 3) \bmod 26$ 。

取密钥  $k = 3$ ，解密函数  $D_3(c) = (c - 3) \bmod 26$ 。

而对于仿射密码，可像修改多位密码那样定义得到。

密钥集合  $K = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}, \gcd(a, 26) = 1\}$ 。

加密函数集合  $E = \{E_{(a,b)}(p) = (ap + b) \bmod 26 \mid p \in I, (a, b) \in K\}$ 。

解密函数集合  $D = \{D_{(a,b)}(c) = \bar{a}(c - b) \bmod 26 \mid c \in C, (a, b) \in K, \bar{a}a \equiv 1 \pmod{26}\}$ 。

# Discrete

## Mathematics - P76

私钥加密系统(private key cryptosystem)，指加密密钥和解密密钥均需保密的加密方法。由于秘密通信双方必须共享一个密钥且任伺人只要知道密钥即可轻易完成加密和解密，所以通信双方也需要安全地交换密钥。

维吉尼亞密碼(Vigenère cipher)，为一种分组密码，又称为不可破译的密码(le chiffre indéchiffrable)

密钥为一个字母串  $k_1, k_2, \dots, k_m$ ，其中  $k_i \in \mathbb{Z}_{26}$ ,  $i = 1, 2, \dots, m$

将明文拆分成长度为  $m$  的块，对于每一个块  $P_1, P_2, \dots, P_m$  应用密钥加密与解密

加密函数  $f(P_i) = (P_i + k_i) \bmod 26$ , 其中  $P_i, k_i \in \mathbb{Z}_{26}$ ,  $i = 1, 2, \dots, m$

解密函数  $f^{-1}(C_i) = (C_i - k_i) \bmod 26$ , 其中  $C_i, k_i \in \mathbb{Z}_{26}$ ,  $i = 1, 2, \dots, m$

如使用 GOD 作为密钥串：

M A N I F E S T O O F T H E C O M M U N I S T P A R T Y  
S O Q I O T H I Y H R I U T W N S F U A P A B L Y H S I G F W E

自动密钥密码(autokey cipher), 或称 autoclave cipher). 与维吉尼亞密码类似，但使用不同方法生成密钥串

key is generated from the message in some automated fashion

通常有两类生成密钥串(keystream)的方法

key-autocipher uses the previous members of the keystream

即使用密钥串之前的元素作为密钥串之后的元素

text-autocipher uses the previous message text

即使用明文串/密文串的部分作为密钥串

第一种是，密钥串为密钥种子后跟隨明文串，对于密钥种子  $k_1, k_2, \dots, k_m$

即对于明文串  $P_1, P_2, \dots, P_n$ ，则生成密钥串  $k_1, k_2, \dots, k_m, P_1, P_2, \dots, P_{n-m}$

如 NOW IS THE TIME TO DECIDE 明文串

X N O W I S T H E T I M E T O D E C I D 密钥串

K B K E A L A L X B U Q X H R H G K L H 密文串

第二种是，密钥串为密钥种子后每一位密钥为前一位生成的密文

如 NOW IS THE TIME TO DECIDE plaintext

13 14 22 08 18 19 07 04 19 08 12 04 19 14 03 04 02 08 03 04 plaintext as numbers

X K Y U C U N U Y R Z L P I W Z D F N Q keystream

23 10 24 20 02 20 13 20 24 17 25 11 15 08 22 25 03 05 13 16 keystream as number

10 24 20 02 20 13 20 24 17 25 11 15 08 22 25 03 05 13 16 20 ciphertext as number

K Y U C N U Y R Z L P I W Z D F N Q U ciphertext

# Discrete

## Mathematics - P77

高级加密标准 (Advanced Encryption Standard, AES), 公钥密码学的美国政府标准  
标准非常复杂, 并被认为能很好地抵抗密码分析, 且具有共享安全通信密钥的特性

公钥密码系统 (public key cryptosystem), 加密密钥公开, 而解密密钥保密的加密方法

即知道如何发送加密消息并不能解密其加密的消息, 而只有接收者能解密消息

在系统中, 各方都有一个众所周知的加密密钥, 而有一个保密的解密密钥

RSA 密码系统 (RSA cryptosystem), 指一种公钥密码系统, 其形式化的定义为

明文集合  $P$  与密文集合  $C$  都是  $\mathbb{Z}_{26}^* = \{0, 1, \dots, 25\}^*$ , 对应字母表  $\{A, B, \dots, Z\}^*$

密钥集合  $K = \{(n, e) \mid n = pq, e \in \mathbb{Z}^+ \wedge \gcd(e, (p-1)(q-1)) = 1, p, q \text{ 为素数}\}$

加密函数集合  $E = \{E_{(n, e)}(p) = p^e \pmod{n} \mid (n, e) \in K, p \in P\}$

解密函数集合  $D = \{D_{(n, e)}(c) = c^d \pmod{n} \mid (n, e) \in K, c \in C, d \text{ 为 } e \pmod{(p-1)(q-1)} \text{ 的逆}\}$

对于明文消息  $M$ , 先按照  $N$  位的长度拆分为块,

将一位字母转换为两位整数, 如  $A \mapsto 00, B \mapsto 01, \dots, Z \mapsto 25$ ,

则  $N$  位字符串可转换为  $2N$  位整数, 则  $m \leq 2525 \dots 25$ , ( $2N$  位整数)

取素数  $p, q$ , 使  $n = pq > 2525 \dots 25$ , 及  $e \in \mathbb{Z}^+$  且  $\gcd(e, (p-1)(q-1)) = 1$

则对每一块明文  $m$ , 取密文  $c = m^e \pmod{n}$ , 然后拼接  $c$  而形成密文串  $C$

则证明 解密函数  $D_{(n, e)}(c) = c^d \pmod{n} = m$  正确

对于素数  $p, q$ , 有  $n = pq > m$ , 及正整数  $e$  使得  $\gcd(e, (p-1)(q-1)) = 1$

且  $c = m^e \pmod{n}$ , 而  $d$  为  $e \pmod{(p-1)(q-1)}$  的逆

即  $P$  有  $de \equiv 1 \pmod{(p-1)(q-1)}$ , 即  $P$   $de = 1 + k(p-1)(q-1)$ , 其中  $k \in \mathbb{Z}^+$

则  $c^d = (m^e)^d = m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot m^{k(p-1)(q-1)}$

考虑  $\gcd(m, pq) = 1$ , 即  $\gcd(m, p) = 1 \wedge \gcd(m, q) = 1$  时

有  $m \cdot m^{k(p-1)(q-1)} \equiv m \cdot (m^{(p-1)})^{k(q-1)} \equiv m \cdot \dots \equiv m \pmod{p}$

$m \cdot m^{k(p-1)(q-1)} \equiv m \cdot (m^{(q-1)})^{k(p-1)} \equiv m \cdot \dots \equiv m \pmod{q}$

则有  $c^d \equiv m \cdot m^{k(p-1)(q-1)} \equiv m \pmod{pq}$

考虑  $\gcd(m, pq) > 1$  时, 如果有  $\gcd(m, p) > 1 \wedge \gcd(m, q) > 1$

且  $m \neq 0$ , 则有  $m \equiv 0 \pmod{p}$ , 于是有  $c \equiv m^e \equiv 0 \equiv m \pmod{n}$

如果  $\gcd(m, p) > 1 \oplus \gcd(m, q) > 1$ , 则考虑  $\gcd(m, p) > 1$  的情形, 即有  $p \mid m \wedge q \nmid m$

又  $m < pq$ , 即  $m/p < q$ , 且  $c^d \equiv m \cdot (m^{(q-1)})^{k(p-1)} \equiv m \pmod{q}$

$\equiv m^e \pmod{p}$  又  $c \equiv m^e \pmod{pq}$ , 则同时  $c \equiv m^e \pmod{p}$ , 又  $\gcd(pq, p^e) = p$ ,  $\bar{p}$  为  $p$  模  $q$  的逆

$c^d \equiv 0 \pmod{p}$  有  $c \cdot \bar{p}^e \equiv m^e \pmod{pq}$ ,  $c \cdot \bar{p}^e \equiv m^e \pmod{pq}$

$(c \cdot \bar{p}^e)^d \equiv (m^e \cdot \bar{p}^e)^d \equiv m^e \cdot \bar{p}^d \pmod{q}$ , 有  $(cd - m) \cdot \bar{p}^d = k \pmod{q}, k \in \mathbb{Z}$

根据中国剩余定理  $(d \equiv m \pmod{pq}) \wedge \gcd(ped, q) = 1$ , 于是有  $(pq \mid cd - m)$ , 即  $p \mid c^d \equiv m \pmod{pq}$

# Discrete

## Mathematics - P78

对于 RSA 密码系统，如果知道  $(p-1)(q-1)$  的值，则可以很容易地对  $n = pq$  进行因式分解  
则可知  $p+q = pq - (p-1)(q-1) + 1 = n - (p-1)(q-1) + 1$   
 $\sqrt{p+q} = \sqrt{(p+q)^2 - 4pq} = \sqrt{(p+q)^2 - 4n}$ ，即可以将  $n$  分解为素数  $p$  和  $q$

密码协议 (cryptographic protocol)，这是双方或多方为了达到一个特定的安全目标而进行的信息交换  
特别是如何在不安全的通信通道上交换密钥

密钥交换协议 (key exchange protocol)，指用来为双方生成共享密钥的协议

特别是在双方以前没有共享过任何信息的情况下在不安全的通信通道上交换密钥  
如迪菲-赫尔曼密钥协商协议 (Diffie-Hellman key agreement protocol)

对于希望共享密钥的 A 与 B，选择一个双方共用的素数  $p$  与  $p$  的一个原根  $a$  在  $\mathbb{Z}_p^*$  上进行计算

A 选择一个秘密整数  $k_A$ ，计算  $a^{k_A} \bmod p$  并发送给 B

B 选择一个秘密整数  $k_B$ ，计算  $a^{k_B} \bmod p$  并发送给 A

A 计算  $(a^{k_B})^{k_A} \bmod p$  得到密钥  $k$

B 计算  $(a^{k_A})^{k_B} \bmod p$  得到密钥  $k'$

又由于  $(a^{k_B})^{k_A} \equiv (a^{k_A})^{k_B} \pmod{p}$ ，于是有  $k = k'$ ，即  $k$  为 A 和 B 的共享密钥

注意到即使  $p, a, a^{k_A} \bmod p$  和  $a^{k_B} \bmod p$  为公开信息

当  $p$  和  $a$  足够大时，也无法在合理的时间内求解  $a^{k_A} \bmod p$  和  $a^{k_B} \bmod p$  的离散对数问题

数字签名 (digital signature)，指接收者用于判定消息声称的发送者确实发送了该消息的方法

如可以使用 RSA 密码系统完成发送方与接收方的数字签名

对于发送方 A，有公开的 RSA 公钥  $(n_A, e_A)$ ，且有私钥  $d_A$  为  $e_A$  模  $(p_A-1)(q_A-1)$  的逆

接收方 B，有 RSA 公钥  $(n_B, e_B)$ ，且有私钥  $d_B$  为  $e_B$  模  $(p_B-1)(q_B-1)$  的逆

则对于信息  $M$ ，先进行私有解密函数  $D_{(n_A, d_A)}(M) = M^{d_A} \bmod n_A = C_A$

再进行 B 的公有加密函数  $E_{(n_B, e_B)}(C_A) = (M^{d_A} \bmod n_A)^{e_B} \bmod n_B = C$

对于接收方，先进行私有解密函数

$D_{(n_B, d_B)}(C) = (M^{d_A} \bmod n_A)^{e_B d_B} \bmod n_B = M^{d_A} \bmod n_A = C_A$

再进行发送方 A 的公有加密函数

$E_{(n_A, e_A)}(C_A) = M^{d_A e_A} \bmod n_A = M^{d_A} \bmod n_A$

于是对于发送方 A 与接收方 B 可以相互确认

发送方 A： $M \xrightarrow{D_{(n_A, d_A)}} M^{d_A} \bmod n_A \xrightarrow{E_{(n_B, e_B)}} (M^{d_A} \bmod n_A)^{e_B} \bmod n_B$

↓ 发送信

接收方 B： $M \xleftarrow{E_{(n_A, e_A)}} M^{d_A} \bmod n_A \xleftarrow{D_{(n_B, d_B)}} (M^{d_A} \bmod n_A)^{e_B} \bmod n_B$