

Discrete

Mathematics - P57

注意扩展欧几里得算法，还有一种递归地利用矩阵乘法的形式。

注意到对于矩阵 $(Y_k) = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} (Y_{k-1})$ 其中 $Y_{k-1} > 0$,

$(Y_k > 0, Y_{k+1} \geq 0)$ 且 $q = Y_{k-1} \text{ div } Y_k$

则如果有，则 $(Y_n) = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} (Y_0)$

又矩阵乘法可结合

又 n 个 2×2 矩阵的积也是 2×2 矩阵 $= \left(\prod_{k=1}^n \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \right) (Y_0) = (S_n, t_n)(a)$

如果对正整数 a, b, c , 有 $\gcd(a, b) = 1$ 且 $a \mid bc$, 则有 $a \mid c$

即有对于 $a, b, c \in \mathbb{Z}^+$, $(\gcd(a, b) = 1 \wedge a \mid bc) \rightarrow a \mid c$. 注意可推广至 $a, b, c \in \mathbb{Z}$ 的情形

证明过程有对于 $a, b \in \mathbb{Z}^+$, 又 $\gcd(a, b) = 1$

则存在 $s, t \in \mathbb{Z}$, 使得 $sa + tb = 1$

又 $c \in \mathbb{Z}^+$, 则 $sac + tbc = c$

又 $a \mid sac$ 且 $a \mid tbc$,

于是有 $a \mid sac + tbc$, 即 $a \mid c$

注意：虽然有析取三段论 $(alb) \vee (alc)$

对于 $a, b, c \in \mathbb{Z}^+$ $\neg(alb)$

其中 $\gcd(a, b) = 1 \therefore a \mid c$ 成立

但是从 $a \mid bc$ 无法得到 $(alb) \vee (alc)$ 的结论。

即如存在 $m, n \in \mathbb{Z}^+$, 且 $\gcd(m, n) = 1$, 令 $a = mn$, $b = m$, $c = n$.

则 $a \mid bc \equiv T$ 但 $(alb) \vee (alc) \equiv F$

所以不能以此证明上述引理

如果对整数 a_1, a_2, \dots, a_n 和素数 p , 有 $p \mid a_1, a_2, \dots, a_n$, 则 $\exists 1 \leq i \leq n \ p \mid a_i$

证明过程有，对于任意给定的素数 p . $P(n)$ 表示在 n 个整数的情形下的上述命题

基础步骤：对于 $P(1)$, 即有 $a_1 \in \mathbb{Z}$,

则如果有 $p \mid a_1$, 那么 $\exists 1 \leq i \leq 1 \ p \mid a_i$ 平凡地为真

递归步骤：假设对于 $\forall n \in \mathbb{Z}^+, P(n)$ 为真, 则考虑 $P(n+1)$

对于 $P(n+1)$, 即有 $a_1, a_2, \dots, a_n, a_{n+1} \in \mathbb{Z}$, 且 $p \mid a_1, a_2, \dots, a_n, a_{n+1}$

令 $c = a_1, a_2, \dots, a_n$, 于是有 $p \mid c, a_{n+1}$

如果 $p \mid c$, 则 $\exists 1 \leq i \leq n \ p \mid a_i$ (IH) $\rightarrow \exists 1 \leq i \leq n+1 \ p \mid a_i$

如果 $p \nmid c$, 则有 $p \mid a_{n+1}$, 于是 $\exists 1 \leq i \leq n+1 \ p \mid a_i$ 为真

注意：这是一个非构造性的存在性证明。

Discrete

Mathematics - P58

算术基本定理 对于定理中的一部分的证明，即正整数素因子分解式的唯一性

每个大于1的正整数最多只有一种写成非递减序素数的乘积的方式

即有 $\forall n \in \mathbb{Z}^+ (n > 1 \rightarrow \exists! (p_1, p_2, \dots, p_k) (p_1 \leq p_2 \leq \dots \leq p_k \wedge k \in \mathbb{Z}^+ \wedge n = p_1 p_2 \dots p_k))$

证明过程为反证法。

假设对某一个正整数 n ，存在两个不同的非递减的素数序列。

即 p_1, p_2, \dots, p_s 为素数，且 $p_1 \leq p_2 \leq \dots \leq p_s$ ，使得 $n = p_1 p_2 \dots p_s$

又有 q_1, q_2, \dots, q_t 为素数，且 $q_1 \leq q_2 \leq \dots \leq q_t$ ，使得 $n = q_1 q_2 \dots q_t$

如果去掉 $p_1 p_2 \dots p_s$ 和 $q_1 q_2 \dots q_t$ 中相同的素数。

令剩余部分为 p_s, p_{s+1}, \dots, p_u 和 q_t, q_{t+1}, \dots, q_v

则可知 $\forall i, j \in \mathbb{Z}^+ (1 \leq i \leq u \wedge 1 \leq j \leq v \rightarrow p_s \neq q_{t+j})$

又因为去掉的是相同的素数，于是有 $p_s, p_{s+1}, \dots, p_u = q_t, q_{t+1}, \dots, q_v$

考虑 p_s ，有 $p_s | q_{t+1}, q_{t+2}, \dots, q_v$

又 $p_s, q_{t+1}, q_{t+2}, \dots, q_v \in \mathbb{Z}^+$ ，则应有 $\exists 1 \leq j \leq v \ p_s | q_{t+j}$

但是由于 $p_s, q_{t+1}, q_{t+2}, \dots, q_v$ 都是素数，且 $\forall 1 \leq j \leq v \ p_s \neq q_{t+j}$

于是有 $\forall 1 \leq j \leq v \ p_s \neq q_{t+j}$ ，从而产生矛盾。

即不存在正整数 n ，它用两个不同的表示为非递减序素数的乘积的方式

如果对于整数 a, b, c 和正整数 m ，有 $ac \equiv bc \pmod{m}$ 且 $\gcd(c, m) = 1$ ，则有 $a \equiv b \pmod{m}$

证明过程由 $ac \equiv bc \pmod{m}$ ，可知 $m | ac - bc$ ，即 $m | (a-b)c$

又 $\gcd(c, m) = 1$ ，即 $m \nmid c$

于是可知 $m | a-b$ ，即 $a \equiv b \pmod{m}$

如果对于大于1的整数 a, m 且 m 为奇数，则 $a^m + 1$ 为合数

证明过程有 $a^m + 1 = a^m - a^{m-1} + a^{m-1} - \dots - a + a + 1$

如果 m 为奇数，则有 $\sum_{k=0}^{m-1} (-1)^{k+m} \cdot a^k$

$$= -1 + a - a^2 + \dots - a^{m-2} + a^{m-1}$$

于是 $a^m + 1 = (a^m - a^{m-1} + a^{m-1} - \dots - a^2 + a) + (a^{m-1} - a^{m-2} + a^{m-3} - \dots - a + 1)$

$= (a+1)(a^{m-1} - a^{m-2} + a^{m-3} - \dots - a + 1)$ ，即 $a^m + 1$ 为合数

由此可以推广为，对于大于1的整数 a, m 且 $m = kt$ ，其中 t 为奇数。

即 $a^m + 1 = a^{kt} + 1 = a^{kt} + a^{kt-1} - a^{kt-1} + \dots + a^k - a^k + 1$

又 $\sum_{i=0}^{t-1} (-1)^i (a^k)^i = 1 - a^k + a^{2k} - \dots - a^{(k(t-1))} + a^{kt}$

于是 $a^m + 1 = a^{kt} - a^{kt-1} + a^{kt-2} - \dots - a^{2k} + a^{k+1} + (a^{kt-1} - a^{kt-2} + \dots + a^{2k} - a^k + 1)$

$= (a^k + 1)(a^{kt-1} - a^{kt-2} + \dots + a^{2k} - a^k + 1)$

其逆否命题有，对于任意整数 a, m ，如果 $a^m + 1$ 为素数，则 m 为偶数 ($m=0$ 时也为真)

Discrete

Mathematics - P59

对于大于1的整数 a, m , 如果 $a^m + 1$ 为素数, 则 m 为偶数。
有更强的命题, 对于大于1的整数 a, m , 如果 $a^m + 1$ 为素数, 则 a 为偶数且 m 为2的幂。

如果 a, b 为正整数, 则有 $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$

其证明过程如, 当 $a=b$ 时, $(2^a - 1) \bmod (2^b - 1) = 0$

$$\text{又 } a \bmod b = 0 \quad 2^{a \bmod b} - 1 = 0 = (2^a - 1) \bmod (2^b - 1)$$

当 $a < b$ 时, $a \bmod b = a$, $2^a - 1 < 2^b - 1$

$$\text{所以有 } (2^a - 1) \bmod (2^b - 1) = 2^a - 1 = 2^{a \bmod b} - 1$$

当 $a > b$ 时, $(2^a - 1) \bmod (2^b - 1) = (2^a - 2^{a-b} + 2^{a-b} - 1) \bmod (2^b - 1)$

$$= [2^{a-b}(2^b - 1) + (2^{a-b} - 1)] \bmod (2^b - 1) \\ = 0 + (2^{a-b} - 1) \bmod (2^b - 1)$$

由于 $a > b$, 所以 $(2^a - 1) \bmod (2^b - 1) = (2^{a-b} - 1) \bmod (2^b - 1)$

$$\text{又 } a-b \leq b, \text{ 则 } (2^a - 1) \bmod (2^b - 1) = (2^{a-b} - 1) \bmod (2^b - 1) = 2^{(a-b) \bmod b} - 1 = 2^{a \bmod b} - 1$$

如果 $a-b > b$, 则重复此步直到 $a-kb \leq b$, 其中 $k \in \mathbb{Z}^+$

所以对于 $a, b \in \mathbb{Z}^+$, 有 $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$

如果 a, b 为正整数, 则 $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$

注意有对于正整数 r, m , 如果有 $2^r - 1 \mid 2^m - 1$, 则有 $r \mid m$

$$(2^m - 1) \bmod (2^r - 1) = 0 = 1 - 1 = 2^{m \bmod r} - 1$$

于是有 $m \bmod r = 0$, 即 $r \mid m$

如果有 $r \mid m$, 则存在整数 n , 使得 $m = rn$

$$\text{即 } 2^m - 1 = 2^{rn} - 1 = (2^r - 1)(2^{r(n-1)} + 2^{r(n-2)} + \dots + 2^r + 1), \text{ 即 } 2^r - 1 \mid 2^m - 1$$

$$\text{令 } r_0 = a, r_1 = b, \gcd(2^{r_0} - 1, 2^{r_1} - 1) = \gcd(2^{r_0} - 1 \bmod r_1, 2^{r_1} - 1) = \gcd(2^{r_0 \bmod r_1} - 1, 2^{r_1} - 1)$$

$$\text{令 } r_{k+1} = r_{k-1} \bmod r_k = \gcd(2^{r_k \bmod r_{k-1}} - 1, 2^{r_k} - 1)$$

则有 $\gcd(2^{r_{k-1}} - 1, 2^{r_k} - 1) = \gcd(2^{r_k} - 1, 2^{r_{k+1}} - 1)$, 直至 $r_{k+1} = 0$,

$$\text{于是有 } \gcd(2^a - 1, 2^b - 1) = \gcd(2^{\gcd(a, b)} - 1, 2^0 - 1) = 2^{\gcd(a, b)} - 1$$

完全数

(perfect number), 指对于正整数 n , 其除自身外所有的正因子之和等于其本身

即对于 $n \in \mathbb{Z}^+$, 令集合 $S = \{x \in \mathbb{Z}^+ \mid x \mid n \wedge x \neq n\}$, 则 $\sum_{x \in S} x = n$

注意有, 如果有 $2^p - 1$ 是素数, 则 $2^{p-1}(2^p - 1)$ 是完全数

证明有: $2^{p-1}(2^p - 1)$ 的公因子有: $2^{p-1}, 2^{p-2}, \dots, 2^1, 2^0$

$$2^0(2^p - 1), 2^1(2^p - 1), \dots, 2^{p-2}(2^p - 1), 2^{p-1}(2^p - 1)$$

$$\text{于是有 } \sum_{k=0}^{p-1} 2^k + \sum_{i=0}^{p-2} 2^i(2^p - 1) = (2^p - 1) + (2^{p-1} - 1)(2^p - 1) = 2^{p-1}(2^p - 1)$$

Discrete Mathematics - P60

Part - euclidean

线性同余方程 (linear congruence) 指对于整数变量 x , 形如 $ax \equiv b \pmod{m}$ 的同余式, 其中 $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$
即求方程 $ax = b + km$ 的整数解, 其中 a, b 是给定整数, m 是给定正整数, k 为任意整数
求解线性同余方程需要用到 a 模 m 的逆, 即 $\bar{a} \in \mathbb{Z}$, 使得 $\bar{a}a \equiv 1 \pmod{m}$

a 模 m 的逆 (inverse of a modulo m), 即对于 $a \in \mathbb{Z}$ 和 $m \in \mathbb{Z}^+$, 使得 $\bar{a}a \equiv 1 \pmod{m}$ 成立的整数 \bar{a}

注意: 如果对于整数 a, m , 有 a, m 互素且 $m > 1$, 则 a 模 m 的逆存在

证明过程如: 对于 $a, m \in \mathbb{Z}$ 且 $m > 1$, 如果有 $\gcd(a, m) = 1$

则存在 $s, t \in \mathbb{Z}$, 使得 $sa + tm = \gcd(a, m) = 1$

$sa = 1 - tm$, 即 $sa \pmod{m} = 1$

于是有 $sa \equiv 1 \pmod{m}$

则 s 即为 a 模 m 的逆

另外注意, 虽然如果有 s 是 a 模 m 的逆, 则 $\forall k \in \mathbb{Z}$ $s + km$ 是 a 模 m 的逆

但是仅有 1 个 a 模 m 的逆落在 $(0, m)$ 之内

证明过程有: 假设存在 2 正整数 $s_1, s_2 \in (0, m)$, 且 $s_1 \neq s_2$ 且都是 a 模 m 的逆

则有 $s_1 a \equiv s_2 a \pmod{m}$, 即 $m | (s_1 a - s_2 a) = a(s_1 - s_2)$

~~且 s_1, s_2 互素且 $0 < s_1, s_2 < m$~~ 且 $\gcd(a, m) = 1$, 即应有 $m | (s_1 - s_2)$

而 $s_1 \neq s_2 \wedge 0 < s_1, s_2 < m$, 则 $|s_1 - s_2| < m$

于是 $m \nmid (s_1 - s_2)$, 即产生矛盾

即有 $(0, m)$ 之内的 a 模 m 的逆唯一

于是有 $\forall a \in \mathbb{Z}, m \in \mathbb{Z}^+ (m > 1 \wedge \gcd(a, m) = 1 \rightarrow \exists! \bar{a} \in \mathbb{Z} (0 < \bar{a} < m \wedge \bar{a}a \equiv 1 \pmod{m}))$

注意到 a 模 m 的逆实际上是 a, m 的贝祖系数中 a 的系数,

即可以通过修改扩展欧几里得算法以求 a 模 m 的逆

`inverseMod :: Int -> Int -> Maybe Int`

`inverseMod a m = case extendEuclid a m of`

`(1, s, _) -> Just (s `mod` m)`

如果 $\gcd(a, m) \neq 1$ ($_1, _2, _3$) \rightarrow Nothing

由此可求得线性同余方程的解, 当 $\gcd(a, m) = 1$ 时, $x \equiv \bar{a}b \pmod{m}$

证明: 由 $\gcd(a, m) = 1$ 可知, 存在 \bar{a} 使得 $\bar{a}a \equiv 1 \pmod{m}$

又 $ax \equiv b \pmod{m}$, 则有 $ax \pmod{m} = b \pmod{m}$.

于是 $(\bar{a}a)x \pmod{m} = \bar{a}b \pmod{m}$, 而 $(\bar{a}a)x \pmod{m} = (\bar{a}a \pmod{m})(x \pmod{m}) \pmod{m}$

~~且 $\bar{a}a \pmod{m} = 1 \pmod{m}$~~ $= x \pmod{m}$

即有 $x \pmod{m} = \bar{a}b \pmod{m}$, 即 $x \equiv \bar{a}b \pmod{m}$

Discrete

Mathematics - P61

Chinese remainder theorem
中国剩余定理

中国剩余定理 (Chinese remainder theorem), 数论中关于求解线性同余方程组的定理

令 m_1, m_2, \dots, m_n 为大于 1 的两两互素的正整数, 而 a_1, a_2, \dots, a_n 为任意整数

则线性同余方程组 $\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$

有唯一的模 $M = m_1 m_2 \cdots m_n$ 的解, 且解为小于 M 的非负整数

即对于 m_1, m_2, \dots, m_n 为大于 1 的两两互素的正整数, 而 $a_1, a_2, \dots, a_n \in \mathbb{Z}$

$$\exists! x \in \mathbb{Z} (0 \leq x < M \wedge \bigwedge_{i=1}^n x \equiv a_i \pmod{m_i})$$

证明存在性: 令 M_k 为 m_1, m_2, \dots, m_n 中除 m_k 外其他正整数的乘积

$$\text{即 } M_k = m_1 m_2 \cdots m_n / m_k, k = 1, 2, \dots, n$$

$$\text{且 } \forall i, j \in \mathbb{Z} (1 \leq i < j \leq n \rightarrow \gcd(m_i, m_j) = 1)$$

于是有 $(\gcd(M_k, M_k)) = 1$

即存在整数 y_k 为 M_k 模 M_k 的逆, 即 $M_k y_k \equiv 1 \pmod{M_k}$

$$\text{于是有 } a_k M_k y_k \equiv a_k \pmod{m_k}$$

$$\text{则取 } x = \sum_{k=1}^n a_k M_k y_k$$

$$\text{另外, } \forall i (1 \leq i \leq n, i \neq k \rightarrow M_i \pmod{m_k} = 0)$$

$$\text{于是对于 } x \pmod{m_k} = (a_k M_k y_k \pmod{m_k}) + (\sum_{j=1, j \neq k}^n a_j M_j y_j \pmod{m_k}) = a_k + \sum_{j=1, j \neq k}^n (a_j M_j y_j \pmod{m_k}) = a_k$$

可知 $\bigwedge_{k=1}^n (x \equiv a_k \pmod{m_k})$ 为真

即 x 为线性同余方程组的解

且 $x + km$ ($k \in \mathbb{Z}$) 都是线性同余方程组

证明唯一性: 首先对于大于 1 且两两互素的正整数 m_1, m_2, \dots, m_n

有整数 a, b , 使得 $a \equiv b \pmod{m_i}, i = 1, 2, \dots, n$

从 m_1 开始, 有 $m_1 | a - b$, 于是有 $a - b = k_1 m_1, k_1 \in \mathbb{Z}$

又 $m_2 | a - b$, 即 $m_2 | m_1 k_1$, 又 $\gcd(m_1, m_2) = 1$, 有 $m_2 | k_1$,

即 $k_1 = m_2 k_2$, 于是 $a - b = m_1 m_2 k_2$

以此类推, 可知 $a - b = m_1 m_2 \cdots m_n k_n$

即 $m_1 | a - b$, 即 $a \equiv b \pmod{m}$, 其中 $m = m_1 m_2 \cdots m_n$

如果存在两个模 m 不同余的解 x 和 y , 即 $x \not\equiv y \pmod{m}$

又 x, y 都是线性同余方程组的解

即有 $\forall i (1 \leq i \leq n) x \pmod{m_i} = a_i \equiv y \pmod{m_i}$

则 $\bigwedge_{i=1}^n m_i | (x - y)$, 即有 $x \equiv y \pmod{m}$, 其中 $m = m_1 m_2 \cdots m_n$

这是产生矛盾, 即不存在两个模 m 不同余的解 x 和 y

于是可知, 对于线性同余方程组, 有且仅有唯一模 $m = m_1 m_2 \cdots m_n$ 的解

Discrete

Mathematics - P62

求解线性同余方程组，方法一是参考中国剩余定理证明过程中，对解的构造。

即对于输入的大于1且两两互素的正整数 m_1, m_2, \dots, m_n 和任意整数 a_1, a_2, \dots, a_n

求解唯一模 $m = m_1 m_2 \dots m_n$ 的解 x ，使得 $\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$

其中 $M_k = m/m_k$, $M_k y_k \equiv 1 \pmod{m_k}$

则求解方法为依次计算 $a_k M_k y_k$ ($k=1, 2, \dots, n$) 并求和，最后求模 m 的值

`chineseRemainder :: [Int] → [Int] → Int`

chineseRemainder as ms = [] 输入列表 $[a_1, a_2, \dots, a_n]$ 和 $[m_1, m_2, \dots, m_n]$

let m = product ms [] 初始化 $m = m_1 m_2 \dots m_n$

ls = zip as ms [] ls 为 (a_k, m_k) pair 组成的 list

func acc (cak, mk) = [] 对每一个 (cak, m_k) pair

let kM = m `div` mk [] $kM = m/m_k$, $y_k = \text{inverseMod}' kM mk$

in acc + cak * (inverseMod' kM mk) * kM [] acc += $cak * y_k * kM$

in (foldl func 0 ls) `mod` m [] 求和后模 m 的值即为解

如 `chineseRemainder [2, 3, 2] [3, 5, 7] → 23`

方法二为双向替换，即对于输入的 $[a_1, a_2, \dots, a_n]$ 和 $[m_1, m_2, \dots, m_n]$ 的线性同余方程组

先取 $x \equiv a_1 \pmod{m_1}$ 和 $x \equiv a_2 \pmod{m_2}$

设 $x = m_1 t + a_1$, 其中 $t \in \mathbb{Z}$, 可知 x 满足 $x \equiv a_1 \pmod{m_1}$

代入 $x \equiv a_2 \pmod{m_2}$ 有 $m_1 t + a_1 \equiv a_2 \pmod{m_2}$

又 $\gcd(m_1, m_2) = 1$, 所以可以求出 m_1 模 m_2 的逆 \bar{m}_1

即可解出 $t \equiv \bar{m}_1(a_2 - a_1) \pmod{m_2}$, 即可设 $t = m_2 u + \bar{m}_1(a_2 - a_1)$, 其中 $u \in \mathbb{Z}$

则 $x = m_1 m_2 u + m_1 \bar{m}_1(a_2 - a_1) + a_1$

又 $\gcd(m_3, m_1 m_2) = 1$, 则可继续代入以求得一个形如 $m_1 m_2 m_3 v + a'$ 的解

重复直到有形如 $x = m_1 m_2 \dots m_n b + a$ 的式子，可知 $x \pmod{m}$ 即为解

`inverseReplace :: [Int] → [Int] → [(Int, Int)]`

`inverseReplace as ms = []` 输入列表 $[a_1, a_2, \dots, a_n]$

let ls = zip as ms [] 在第 k 次迭代中，方程为 $x = a_k \pmod{m_k}$

func (kM, tk) (cak, mk) = [] 此时有 $x = M_k u + tk$,

let yk = inverseMod' kM mk [] 其中 $M_k = \prod_{i=1}^{k-1} m_i$, y_k 为 M_k 模 m_k 的逆

tk' = (yk * cak - tk) `mod` mk [] $t' \equiv y_k(cak - tk) \pmod{m_k}$

in (kM * mk, tk' + tk) [] 在第 k 次迭代后有 $x = M_{k+1} u + t_{k+1}$

in (foldl func (1, 0) ls) [] 其中 $t_{k+1} = M_k \cdot t' + tk$

acc 初始值相当于全 $x = 1 \cdot u + 0$, 其中 $M_1 = 1$, $t_1 = 0$

Discrete Mathematics - P63

大整数的算术

中国剩余定理在大整数的计算机算术的应用

即对于大于1的两两互素的正整数 m_1, m_2, \dots, m_n , 任意整数 a_1, a_2, \dots, a_n

有唯一的模 $m = m_1 m_2 \cdots m_n$ 的解

若令 $\mathbb{Z}_k = \{0, 1, \dots, m_k - 1\}$, 可知 \mathbb{Z}_k 为 m_k 的最小剩余系, 且 $|\mathbb{Z}_k| = m_k$

而令 $a_k \in \mathbb{Z}_k$, 则可知 a_k 有 m_k 种不同的取值

含有 n 元组 (a_1, a_2, \dots, a_n) , 则可知 n 元组的所有可能的集合为 $\mathbb{Z}_1 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n$

于是有 $|\mathbb{Z}_1 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n| = m_1 m_2 \cdots m_n = m$

又对于每一个不相等的 n 元组 (a_1, a_2, \dots, a_n) 有唯一模 m 的解 x

而 x 的取值范围为 m 的最小剩余系 $\{0, 1, \dots, m-1\}$

又 $|\mathbb{Z}_m| = m = |\mathbb{Z}_1 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n|$

所以存在 $f: \mathbb{Z}_1 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ 的一一对应关系

即存在整数 $0 \leq x < m$ 和 n 元组 (a_1, a_2, \dots, a_n) 的一一对应

$\forall 1 \leq k \leq n \quad x \equiv a_k \pmod{m_k}$, 即 $x \pmod{m_k} = a_k \pmod{m_k} = a_k \quad (a_k \in \mathbb{Z}_k)$

于是有, 对于大于1的两两互素的正整数 m_1, m_2, \dots, m_n , 有 $m = m_1 m_2 \cdots m_n$

则满足 $0 \leq a < m$ 的正整数 a , 可唯一地表示为 n 元组

$(a \pmod{m_1}, a \pmod{m_2}, \dots, a \pmod{m_n})$, 或写作 (a_1, a_2, \dots, a_n)

而已知 (a_1, a_2, \dots, a_n) 时, 可以通过求解线性同余方程组得到唯一的整数 $0 \leq a < m$

注意这种表示为 n 元组的方法可以将一个模 m 加法或乘法拆为 n 个模 m_k 加法或乘法

即如果对于两两互素且大于1的正整数 m_1, m_2, \dots, m_n , 有 $m = m_1 m_2 \cdots m_n$

且以 (a_1, a_2, \dots, a_n) 和 (b_1, b_2, \dots, b_n) 表示整数 $0 \leq a, b < m$, 且 $a_k, b_k \in \mathbb{Z}_k$, $(k=1, 2, \dots, n)$

则 $a + b$ 的结果 c 可表示为 (c_1, c_2, \dots, c_n) 且 $c_k = a_k + m_k b_k$

$a \cdot b$ 的结果 d 可表示为 (d_1, d_2, \dots, d_n) 且 $d_k = a_k \cdot m_k b_k$

注意: 对于整数 a , 正整数 m, n , 如果有 $n \mid m$, 则 $(a \pmod{m}) \pmod{n} = a \pmod{n}$

于是有如果 $c = (a+b) \pmod{m}$, 则对于 m_k , $k=1, 2, \dots, n$

有 $c \pmod{m_k} = ((a+b) \pmod{m}) \pmod{m_k} = (a+b) \pmod{m_k} = (a_k + b_k) \pmod{m_k}$

同理 $d \pmod{m_k} = ((a \cdot b) \pmod{m}) \pmod{m_k} = (a \cdot b) \pmod{m_k} = (a_k \cdot b_k) \pmod{m_k}$

于是可知, 对于选定的模数, 大整数的算术运算可以通过在 n 元组分量上的运算完成,

优点是可以完成通常在一台计算机上完成的大整数算术

对不同模数的运算可以并行计算, 以提高运算速度

特别的有, 由于对形如 $2^k - 1$ 的整数, 可以方便地通过 $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$ 判断是否互素

可以通过取 $2^{m_k} - 1$ 来快速构造模数的集合

如用 $2^3 - 1, 2^5 - 1, 2^7 - 1, 2^8 - 1, 2^{11} - 1$ 可构造出 $2^{34} - 1$ 以内的模 m 运算

Discrete

Mathematics - P64

8.9 - number theory

对于大于1的正整数m和任意整数a, b, c, 如果有 $ac \equiv bc \pmod{m}$, 则有 $a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$

证明过程有, 当 $c=0$ 时, 可知 $ac \equiv bc \pmod{m}$ 对任意 $a, b \in \mathbb{Z}$ 为真

而 $\gcd(c, m) = m$, 于是 $\frac{m}{\gcd(c, m)} = 1$, 而 $a \pmod{1} = b \pmod{1} = 0$ 平凡地为真

当 $c \neq 0$ 时, 可知 $m | c(a-b)$, 即 $c(a-b) = km$, $k \in \mathbb{Z}$

令 $n = \gcd(c, m)$, 则有 $\gcd(c/n, m/n) = 1$

而 $(c/n)(a-b) = km/n$, 即 $m/n | (c/n)(a-b)$

于是有 $\frac{m}{n} | a-b$, 即 $a \equiv b \pmod{\frac{m}{\gcd(c, m)}}$

Euclid's lemma 如果 p 为素数, 则 $x^2 \equiv 1 \pmod{p}$ 仅有解为满足 $x \equiv 1 \pmod{p}$ 或 $x \equiv -1 \pmod{p}$ 的整数 x

证明过程有: 对于素数 p , 对任意整数 x , 存在唯一的整数 $d, 0 \leq r < p$, 使得 $x = dp+r$

则 $x^2 = (dp+r)^2 = Mp + r^2$, 其中 $M \in \mathbb{Z}$

是 $r^2 \equiv x^2 \equiv 1 \pmod{p}$, 即 $p | r^2 - 1 = (r+1)(r-1)$

又 $0 \leq r < p$, 则 $r=1$ 或者 $r=p-1$

于是 $x \pmod{p} = r$, 即 $x \equiv 1 \pmod{p}$ 或 $x \equiv -1 \pmod{p}$

如果 p 为素数, 则对于小于 p 的正整数, 除了 1 和 $p-1$ 之外, 可以分割成成对的整数, 使得互为模 p 的逆

证明过程有: 对于 $p=2$ 和 $p=3$, 除了 1 和 $p-1$ 之外, 集合 $M_p = \{2, \dots, p-2\}$ 为空, 结论平凡地为真

对于大于3的素数 p , 首先 p 为奇数, 于是集合 $M_p = \{2, 3, \dots, p-2\}$ 非空且有偶数个元素

对于任意 $r \in M_p$, 可知 $\gcd(r, p) = 1$,

于是必然存在整数 $0 \leq s \leq p-1$, 使得 $sr \equiv 1 \pmod{p}$, 即 s 为 r 模 p 的逆

又 $r \neq 1$ 且 $r \neq p-1$, 所以 $s \neq 1 \wedge s \neq p-1 \wedge s \neq r$

则可知 s 为 M_p 中唯一的不同于 r 的元素,

且对于 s , 元素 r 也是唯一的,

于是可知 $M_p = \{2, 3, \dots, p-2\}$ 可记作 $M_p = \{a_1, b_1, \dots, a_k, b_k\}$ 其中 $k = \frac{(p-3)}{2}$

使得 $\forall 1 \leq i \leq k, a_i b_i \equiv 1 \pmod{p}$

威尔逊定理 (Wilson's theorem), 指如果 p 为素数, 则 $(p-1)! \equiv -1 \pmod{p}$

证明过程有: 对于 $p=2$ 和 $p=3$, 有 $(2-1)! \equiv -1 \pmod{2}$, $(3-2)! \equiv -1 \pmod{3}$

对于大于3的素数 p , 可知集合 $M_p = \{2, 3, \dots, p-2\}$ 非空

且 M_p 可分割为 $\{a_1, b_1, \dots, a_k, b_k\}$, 使得 $\forall 1 \leq i \leq k, a_i b_i \equiv 1 \pmod{p}$, 其中 $k = \frac{(p-3)}{2}$

则 $(p-1)! \pmod{p} = [1 \times (p-1) \times \prod_{i=1}^k (a_i b_i)] \pmod{p} = 1 \times (p-1) \pmod{p} \times \prod_{i=1}^k (a_i b_i) \pmod{p}$

$= 1 \times (-1) \times 1 \pmod{p}$, 即 $(p-1)! \equiv -1 \pmod{p}$

同时可知其逆否命题, 如果正整数 n 有 $(n-1)! \not\equiv -1 \pmod{n}$, 则 n 不是素数

Discrete

Mathematics - P65

费马小定理 (Fermat's little theorem) 指对于素数 p , a 为不能被 p 整除的整数, 则有 $a^{p-1} \equiv 1 \pmod{p}$

即有对于 $\forall a \in \mathbb{Z}, p \neq 2$ (p 是素数 $\wedge p \nmid a \rightarrow a^{p-1} \equiv 1 \pmod{p}$)

另外 $\forall a \in \mathbb{Z}$ (p 是素数 $\rightarrow a^p \equiv a \pmod{p}$)

注意当 $p \mid a$ 时 $a^p \equiv 0 \equiv a \pmod{p}$

证明过程有: 对于素数 p , 和不能被 p 整除的整数 a , 那么

令有整数 $1 \cdot a, 2 \cdot a, \dots, (p-1)a$ 共 $(p-1)$ 个整数,

使 $1 \leq r_1 < r_2 \leq p-1$, 可知 $r_1 a, r_2 a$ 为 $1 \cdot a, 2 \cdot a, \dots, (p-1)a$ 中任意两项

考虑 $r_2 a - r_1 a = (r_2 - r_1)a$. 有 $0 < r_2 - r_1 < p$, 且 $p \nmid (r_2 - r_1)$

又 $p \nmid a$, 于是有 $p \nmid (r_2 - r_1)a$, 即 $r_2 a \not\equiv r_1 a \pmod{p}$

即可知 $1 \cdot a, 2 \cdot a, \dots, (p-1)a$ 中任何两个模 p 不同余.

考虑 p 的完全剩余系 $\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$, $|Z_p| = p$

而 $a, 2a, \dots, (p-1)a$ 任何两个模 p 不同余.

且 $\forall 1 \leq r \leq p-1$, $ra \not\equiv 0 \pmod{p}$, 即 p 任何一个模 p 不余 0.

则集合 $M_p = \{0 \cdot a, 1 \cdot a, \dots, (p-1)a\}$ 也是 p 的完全剩余系, $|M_p| = p$

于是存在一个一一对应 $f: M_p \rightarrow \mathbb{Z}_p$ 使得 $f(xa) = x \pmod{p}$.

又不论 a 取任何不能被 p 整除的整数, 都有 $f(a \cdot 0) = 0$.

即 $\forall 1 \leq r \leq p-1$, $f(ra) \neq 0$.

于是 $(\prod_{r=1}^{p-1} ra) \pmod{p} = (\prod_{r=1}^{p-1} (ra \pmod{p})) \pmod{p} = (p-1)! \pmod{p}$

即 $(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$

又 $\forall k \in \mathbb{Z}$ ($1 \leq k \leq p-1 \rightarrow \gcd(k, p) = 1$), 于是有 $\gcd((p-1)!, p) = 1$

于是有 $a^{p-1} \equiv 1 \pmod{p}$, 同时有 $p \nmid a$ 情况下的 $a^p \equiv a \pmod{p}$

推论 对于素数 p , a 为满足 $p \nmid a$ 的整数, 则 a^{p-2} 为 a 模 p 的逆

即有对于素数 p , $\forall a \in \mathbb{Z}$ ($p \nmid a \rightarrow a$ 模 p 的逆 $\bar{a} = a^{p-2}$)

证明过程有, 根据费马定理有 $a^{p-2} \cdot a \equiv a^{p-1} \equiv 1 \pmod{p}$

对于素数 p , a 为整数且 $p \nmid a$, 则对任意 n , $a^n \pmod{p} = a^{n \pmod{p-1}} \pmod{p}$

即对于素数 p 和 $a \in \mathbb{Z}$ 且 $p \nmid a$, 则 $a^n \pmod{p} = a^{n \pmod{p-1}} \pmod{p}$

证明过程有, 对于任意非负整数 n , 都存在 $d \in \mathbb{Z}$, $r \in \mathbb{Z}$ 且 $0 \leq r < p-1$, 使得 $n = d(p-1) + r$

于是 $a^n \pmod{p} = a^{d(p-1)+r} \pmod{p} = [a^{p-1} \pmod{p}]^d \cdot [a^r \pmod{p}] \pmod{p}$

又根据费马定理有 $a^{p-1} \pmod{p} = 1$, 于是有 $a^n \pmod{p} = a^r \pmod{p}$

又 $r = n \pmod{p-1}$, 则 $a^n \pmod{p} = a^{n \pmod{p-1}} \pmod{p}$

从而 $a^n \pmod{p} = a^{n \pmod{p-1}} \pmod{p}$

Discrete

Mathematics - P66

以b为基数的强伪素数(pseudoprime to the base b), 对于正整数b, 使 $b^{n-1} \equiv 1 \pmod{n}$ 成立的合数n。

■ 基于对费马定理的反命题的证明

即对正整数n, $\forall b \in \mathbb{Z}^+ (\gcd(b, n) = 1 \rightarrow b^{n-1} \equiv 1 \pmod{n}) \rightarrow n$ 是素数. $\equiv F$

注意当p为素数时, 对于整数a, $\forall p | a \rightarrow \gcd(a, p) = 1$

卡米切字数(Carmichael number), 指合数n对于所有满足 $\gcd(b, n) = 1$ 的正整数b, $b^{n-1} \equiv 1 \pmod{n}$ 成立

即如果正合数n为卡米切字数, 则 $\forall b \in \mathbb{Z}^+ (\gcd(b, n) = 1 \rightarrow b^{n-1} \equiv 1 \pmod{n})$

又称绝对费马伪素数(absolute Fermat pseudoprime)

等价定义(Korselt's criterion, Korselt判别法), 指一个正合数n为卡米切字数当且仅当

1. square-free, 即n中没有素数的平方因子, 即 $\forall p \in \mathbb{P}$ 是素数 $\wedge p | n \rightarrow p^2 \nmid n$

2. 对于n的每个素因子p, 都有 $(p-1) | (n-1)$, 即 $\forall p (\text{p是素数} \wedge p | n \rightarrow (p-1) | (n-1))$

注意由条件2可以直接得到卡米切字数是奇数的结论。

证明充分性, 如果对于正合数n, 如果满足n是square-free的

则可知 $n = p_1 p_2 \cdots p_k$, 其中 p_1, p_2, \dots, p_k 是不相同的素数, $k \in \mathbb{Z}$ 且 $k \geq 2$

则对于正整数a, 如果 $\gcd(a, n) = 1$,

则有 $\forall 1 \leq i \leq k \ \gcd(a, p_i) = 1$, 即对每个素因子 p_i 都有 $a^{p_i-1} \equiv 1 \pmod{p_i}$

又 $\forall 1 \leq i \leq k \ p_i-1 | n-1$, 于是对每个素因子 p_i 都有 $a^{n-1} \equiv a^{d_i(p_i-1)} \equiv 1 \pmod{p_i}$

于是有唯一的模n的解, $n = p_1 p_2 \cdots p_k$. p_1, p_2, \dots, p_k 两两互素

令 $b = 1 + kn$, 可知 $\forall 1 \leq i \leq n \ b \pmod{p_i} = 1$

于是可知 $a^{n-1} \equiv b \equiv 1 \pmod{n}$

由于对于正合数n, $\forall a \in \mathbb{Z}^+ (\gcd(a, n) = 1 \rightarrow a^{n-1} \equiv 1 \pmod{n})$

可知正合数n为卡米切字数。

证明必要性, 如果正合数n是卡米切字数, 即 $\forall a \in \mathbb{Z}^+ (\gcd(a, n) = 1 \rightarrow a^{n-1} \equiv 1 \pmod{n})$

假设存在素数p, ~~是n的素因子~~ 是n的素因子, 且有 $p^k | n \wedge p^{k+1} \nmid n$, $k \in \mathbb{Z}^+$

则有 $a^{n-1} \equiv 1 \pmod{p^k}$, 如果有 $a \equiv ap \pmod{p^k}$, $a^{p-1} \equiv 1 \pmod{p^k}$

又 $\gcd(a, n) = 1$, 即 $\gcd(a, p^k) = 1$, 于是有 $\gcd(ap, p^k) = 1$ ($ap \equiv a \pmod{p^k}$)

根据欧拉定理, $a^{p-1} \equiv 1 \pmod{p^k}$, 即 $a^{p^{k+1}(p-1)} \equiv 1 \pmod{p^k}$

于是有 $p^{k+1}(p-1) | (n-1)$, 如果 $k > 1$, 则必有 $p | (n-1)$, 产生矛盾,

即n中没有素数的平方因子, 即n是square-free。

同时, 由于 $k=1$, 所以必然有 $(p-1) | (n-1)$.

即对于n中的每个素因子p, 有 $(p-1) | (n-1)$

奇数 如果卡米切字数n是偶数, 则除了素数2, 必然有奇数因子p, 又 $p-1$ 为偶数, $n-1$ 为奇数

则与 $(p-1) | (n-1)$ 矛盾, 所以卡米切字数必定是奇数

Discrete

Mathematics - P67

米勒-拉宾素性测试 (Miller-Rabin primality test)，为一种素数判定法则，利用随机化算法判断是否素数。

对于正整数 n ，如果对正整数 b 且 $n \neq b$ ，进行以 b 为底的米勒素性测试

如果正整数 n 通过以 b 为底的米勒素性测试，则称 b 为 n 是素数的强伪证 (strong liar)

如果 n 没有通过，则称 b 为 n 是合数的凭证 (witness)

如果正合数 n 通过以 b 为底的米勒素性测试，则称正合数 n 是以 b 为底的强伪素数 (strong pseudoprime base b)

原理

首先，如果 p 为素数且 $p > 2$ 时，则考虑方程 $x^2 \equiv 1 \pmod{p}$ 的整数解。

可知 p 为大于 2 的素数，仅有平凡平方根 (trivial square root), $x \equiv \pm 1 \pmod{p}$

且没有非平凡平方根 (no trivial square root). 即 $x \equiv r \pmod{p}$, $r \in \mathbb{Z}^*$ 且 $1 < r < p-1$

假设 n 是大于 2 的素数，则 n 为奇数， $n-1$ 为偶数，并且存在 $s \in \mathbb{Z}^*$, $d \in \mathbb{Z}^*$, 有 d 为奇数且 $n-1 = 2^s \cdot d$

于是 对于正整数 b 且 $n \neq b$,

如果 $b^{n-1} \not\equiv 1 \pmod{n}$, 则 n 必定是合数，否则有 $(b^{2^{s-1} \cdot d})^2 \equiv 1 \pmod{n}$

则 $b^{2^{s-1} \cdot d} \equiv \pm 1 \pmod{n}$, 所以如果 $b^{2^{s-1} \cdot d}$ 有非平凡平方根，则 n 必定是合数

如果 $b^{2^{s-1} \cdot d} \equiv -1 \pmod{n}$, 由于对根没有限制，则视为通过以 b 为底的素性测试

如果 $b^{2^{s-1} \cdot d} \equiv 1 \pmod{n}$, 如果此时 $s=1=0$, 即 $b^d \equiv 1 \pmod{n}$

且 d 是奇数，则对根没有限制，则视为通过以 b 为底的素性测试

如果 $s > 0$, 则重复以上步骤，直到得出结论

myPowerMod :: Int → Int → Int → Int // 计算 $a^n \pmod{m_0}$

myPowerMod a n m₀ = let n = b_k * 2^k + b_{k-1} * 2^{k-1} + ... + b₁ * 2 + b₀

let func acc x n = a^{b_k * 2^k} * a^{b_{k-1} * 2^{k-1}} * ... * a^{b₁ * 2} * a^{b₀}

| n == 0 = acc = aⁿ mod m = (($\prod_{i=0}^k$ a^{b_i * 2ⁱ mod m)) mod m}

| otherwise =

let acc0 = if even n then acc else ((acc * x) `mod` m₀)

in func acc0 ((x * x) `mod` m₀) (n `div` 2)

in func 1 a n.

millerTest :: Int → Int → Bool

millerTest n b =

let func b d = case (myPowerMod b d n) of

对于 $a^{2^r d} \pmod{n}$, $a^{2^r d} \equiv 1 \pmod{n}$ 时，通过测试 -1 → True

其中 $0 < r \leq s$

且 $d \in \mathbb{Z}^*$ 且为奇数 出现非平凡平方根，则未通过 -1 → False

且 $n-1 = 2^s \cdot d$ in func b (n-1) → if odd d then True else func b (d `div` 2)

且 $n-1 = 2^s \cdot d$ in func b (n-1) → if odd d then True else func b (d `div` 2)