数学背景

数论知识

除数（因子）的概念：

设a, b为两个任意整数，Z为全体整数构成的集合，若b≠0且使得a = mb，称b整除a。记为b | a，还称b为a的除数(因子)

注:若a = mb + r且0 < r < b,此时b不整除a,记为b ∤ a

性质：1) b | a，a | c，则b | c

2) c | a，c | b，则c | am + bn

3) b | a，则$\left(\frac{a}{b}\right)$ | a

数学背景

素数(质数)的概念:

整数p > 1被称为素数是指p的因子仅有1, -1, p, -p。

算术基本定理:

任何正整数a > 1都可以写成唯一的表达式

$a = P_1^{\alpha 1} P_2^{\alpha 2} \ldots P_t^{\alpha t}$, 这里$P_1 > P_2 > P_3 > \ldots > P_t$是素数，

其中$\alpha_i > 0$

例：$305613 = 11 * 7^3 * 3^4$

数学背景

最大公约数：

若a, b, k∈Z，如果k| a，k| b，称k是a和b的公约数。

正整数c称为a和b的最大公约数，如果它满足

- c是a和b的公约数。
- 对a和b的任何一个公约数k有 k| c 。

注：1、等价的定义形式是：

$$\gcd(a, b) = \max\{k \mid k \mid a, k \mid b\}$$

2、若gcd (a, b) = 1，称a与b是互素的。

例： gcd (323, 221) = 17

数学背景

最小公倍数：

若a, b, k∈Z，如果a｜ k，b｜ k ，称k是a和b的公倍数。

正整数d称为a和b的最小公倍数，如果它满足

- d是a和b的公倍数。
- 对a和b的任何一个公倍数k有d｜ k。

等价的定义形式是：lcm (a, b)＝min { k｜ a｜ k，b｜ k }

例： lcm (56, 34) = 952

数学背景

欧拉函数：

设n>1若φ(n)表示比n小而与n互素的正整数的个数。则φ(n)为欧拉函数。

以n＝24为例，比24小而与24 互素的正整数为：1，5，7，11，13，17，19，23，因此，我们有φ(24)＝8。

性质：1）若p为素数，则φ(p)＝p－1。

2）若p为素数，则$\varphi(p^k)= p^{k-1}(p-1)$

3）若m与n互素，则φ(m*n)＝φ(m)*φ(n)

4）若$n = P_1^{\alpha 1}P_2^{\alpha 2}\ldots P_t^{\alpha t}$，

则$\varphi(n)= n(1-\frac{1}{P_1})(1-\frac{1}{P_2})\ldots(1-\frac{1}{P_t})$

数学背景

带余除法：

$\forall a \in Z > 0$，可找出两个唯一确定的整数q和r，使 $a = qm + r, 0 \le r < m$，q和r这两个数分别称为以m去除a所得到的商数和余数。(若$r = 0$则$m \mid a$）

数学背景

欧几里德算法(Euclid)：

计算最大公约数gcd (a, b)，不需要对a, b分解因式。

方法：假设a>b

$a = b*q_1 + r_1$

$b = r_1*q_2 + r_2$

$r_1 = r_2*q_3 + r_3$

。。。。。。

$r_{n-2} = r_{n-1}*q_n + r_n$

$r_{n-1} = r_n*q_{n+1} + r_{n+1}$ ($r_{n+1}=0$)

于是gcd (a, b)= r_n

数学背景

例：求gcd (1547, 560)

解：1547 = 2*560 + 427

560 = 1*427 + 133

427 = 3*133 + 28

133 = 4*28 + 21

28 = 1*21 + 7

21 = 3*7 + 0

于是 gcd (1547, 560) = 7

数学背景

同余：

设a, b∈Z，若m｜ a－b，则称整数a和b模正整数m同余，并写a≡b (mod m)，m称为同余式的模。

性质：1）自反性：对任意整数a有a≡a (mod m)

2）对称性：如果a≡b (mod m)，则b≡a (mod m)

3）传递性：如果a≡b (mod m)，b≡c (mod m)

则a≡c (mod m)

4）a (mod m)±b (mod m) ≡(a±b) (mod m)

a (mod m) * b (mod m) ≡ a*b (mod m)

例：通过同余式演算证明$5^{60}-1$是56的倍数。

解：$5^3 = 125 \equiv 13 \pmod{56}$，于是有$5^6 \equiv 169 \equiv 1 \pmod{56}$

对同余式的两边同时升到10次幂，即有56｜ $5^{60}-1$。

数学背景

全体整数集合Z可按模m (m>1)分成一些两两不交的等价类。

整数模m同余类共有m个，它们分别为

$$mk+0, mk+1, mk+2, \ldots, mk+(m-1), \quad k \in Z$$

每个类选这类中的最小非负整数作为其代表元，

于是称[0], [1], [2], … , [m-1]为标准完全剩余系。

Z模12的标准剩余系为：

[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11]

定理1： 设a为整数，若存在整数a′，使$a\,a' \equiv 1 \pmod m$，则称a′为a对模m的数论倒数。

例：设m＝5， a＝7，则a′＝3

定理2： 若(a, m) = 1，则对模m，整数a有数论倒数a′。

数学背景

Format定理：

如果p是素数，a是正整数，a不是p 的倍数，则$a^{p-1}\equiv 1 \pmod p$。

证明：$Z^*_p \equiv \{\alpha \in Z_p \mid (\alpha, p) = 1\}$

易见，$Z^*_p = \{1, 2, 3, \ldots, (p-1)\}$，且由$(a, p)=1$知

$a\,Z^*_p = \{a, 2a, 3a, \ldots, (p-1)a\} = Z^*_p$，原因是$a\,Z^*_p$内的元素两两不同。他们刚好为1, 2, 3, …, (p－1)的一个排列。

所以 $a*2a*3a*\ldots*(p-1)a \equiv 1*2*3*\ldots(p-1) \pmod p$

由$((p-1)!, p)=1$，所以 $a^{p-1}\equiv 1 \pmod p$

易见：对$(a, p)=1$，有$a^p \equiv a \pmod p$

例：$4^6 \pmod 7 = 4096 \pmod 7 = 1$

$4^7 \pmod 7 = 16384 \pmod 7 = 4$

数学背景

Euclid定理：若(a，m)=1，则$a^{\phi(m)} \equiv 1 \pmod m$

证明：设小于m且与m互素的正整数为$r_1, r_2, r_3, \ldots, r_{\varphi(m)}$ (1)

他们是模m两两互不同余的。对每一个定数i来说，由于

a和r_i都与m互素，所以$(ar_i, m) = 1$，

所以ar_i同余于(1)中的某个$r_{i'}$，即

$$ar_i \equiv r_{i'} \pmod m，\ 1 \le i \le \varphi(m)$$

并且当$i \neq j$时，有$ar_i \neq ar_j \pmod m$，

于是，$r_{1'}, r_{2'}, \cdots r_{\varphi(m)'}$ 为 $r_1, r_2, \cdots, r_{\varphi(m)}$ 的置换。

所以有 $a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_{1'} r_{2'} \cdots r_{\varphi(m)'} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod m$

由$(r_i, m)=1$，$(r_1, r_2, \cdots, r_{\varphi(m)}, m) = 1$

所以 $a^{\phi(m)} \equiv 1 \pmod m$

数学背景

同余式解：设$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$为整系数多项式，m为正整数，若存在整数x使同余式$f(x) \equiv 0 \pmod m$成立，则称整数x为同余式的解。

若f(x)为一次方程，则称其为一次同余式

$$ax \equiv b \pmod m$$

定理3：若$(a, m) = 1$，则同余式$ax \equiv b \pmod m$恰有一个解。

定理4：一次同余式$ax \equiv b \pmod m$，$a \not\equiv 0 \pmod m$有解的充要条件是$(a, m) \mid b$，若有解，解的个数为$d = (a, m)$

例：解同余式$6x \equiv 15 \pmod{33}$

解：$2x \equiv 5 \pmod{11}$，$x = 5*6 \pmod{11} = 8 \pmod{11}$

又x=19，30(mod 11)亦为解

数学背景

中国剩余定理：

例子：（孙子算经）今有物不知其数。三三数之余二；五五数之余三；七七数之余二。问物几何？

答曰：二十三。

$$23 \equiv 2*70+3*21+2*15 \pmod{105}$$

（口诀：三人同行七十稀，五树梅花廿一枝，

七子团圆月正半，除百零五便得知。）

问，70，21，15如何得到的？

原问题为求解同余方程组

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

数学背景

注意：若x_0为上述同余方程组的解，

则$x_0' = x_0 + 105*k\ (k \in Z)$ 也为上述同余方程组的解。

解题口诀提示我们先解下面三个特殊的同余方程组

(1) $\begin{cases} x \equiv 1 (\mathrm{mod}\, 3) \\ x \equiv 0 (\mathrm{mod}\, 5) \\ x \equiv 0 (\mathrm{mod}\, 7) \end{cases}$ (2) $\begin{cases} x \equiv 0 (\mathrm{mod}\, 3) \\ x \equiv 1 (\mathrm{mod}\, 5) \\ x \equiv 0 (\mathrm{mod}\, 7) \end{cases}$ (3) $\begin{cases} x \equiv 0 (\mathrm{mod}\, 3) \\ x \equiv 0 (\mathrm{mod}\, 5) \\ x \equiv 1 (\mathrm{mod}\, 7) \end{cases}$

的特殊解 $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ =? $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ =? $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ =?

以方程(1)为对象，相当于解一个同余方程 35y≡1(mod 3)，

理由是从(1)的模数及条件知，x应是35的倍数，于是

数学背景

可以假设x＝35y，35y≡1(mod 3)相当于2y≡1(mod 3)

解出y = 2(mod 3)，于是x ≡ 35*2 ≡ 70 (mod 105)

类似地得到(2)、(3)方程的模105的解21、15。

于是有 $\begin{pmatrix}1\\0\\0\end{pmatrix} = 70$ $\begin{pmatrix}0\\1\\0\end{pmatrix} = 21$ $\begin{pmatrix}0\\0\\1\end{pmatrix} = 15$

得 $\begin{bmatrix}2\\3\\2\end{bmatrix} = 2\begin{bmatrix}1\\0\\0\end{bmatrix} + 3\begin{bmatrix}0\\1\\0\end{bmatrix} + 2\begin{bmatrix}0\\0\\1\end{bmatrix}$

$= 2*70 + 3*21 + 2*15 \equiv 23 \pmod{105}$

数学背景

中国剩余定理：

设$m_1,m_2,\ldots m_r$两两互素，并记$N=m_1m_{2\ldots}m_r$，则同余方程组

$$\begin{cases} x = b_1 \pmod{m_1} \\ x = b_2 \pmod{m_2} \\ \vdots \\ x = b_r \pmod{m_r} \end{cases}$$

在模N同余的意义下有唯一解。

数学背景

平方剩余：

设a $\in Z_m^*$如果存在x$\in Z_m^*$，使得$x^2 \equiv a \pmod m$有解，

则称a为模m的平方剩余，否则称a为模m的非平方剩余。

例如： $x^2 \equiv a \pmod 7$，

当a＝1，2，4时有解，当a＝3，5，6时无解。

模运算：

$(a*b) \pmod m = ((a \bmod m)*(b \bmod m)) \pmod m$

$(a*b) \equiv (a*c) \pmod m$，则$b \equiv c \pmod m$ 成立的

条件是(a，m)=1

数学背景

抽象代数理论

1、群，环，域

2、有限域

复杂性理论

算法复杂性：时间复杂度、空间复杂性

问题复杂性：

判别标准：一个问题可具体转换为能在多项式时间内解决的形式，即为“易解”问题；反之，只能用指数函数时间解决的问题，认为是“难解”问题。