现代密码学

Modern Cryptography

张方国

中山大学计算机学院

Office: Room 305, IM School Building

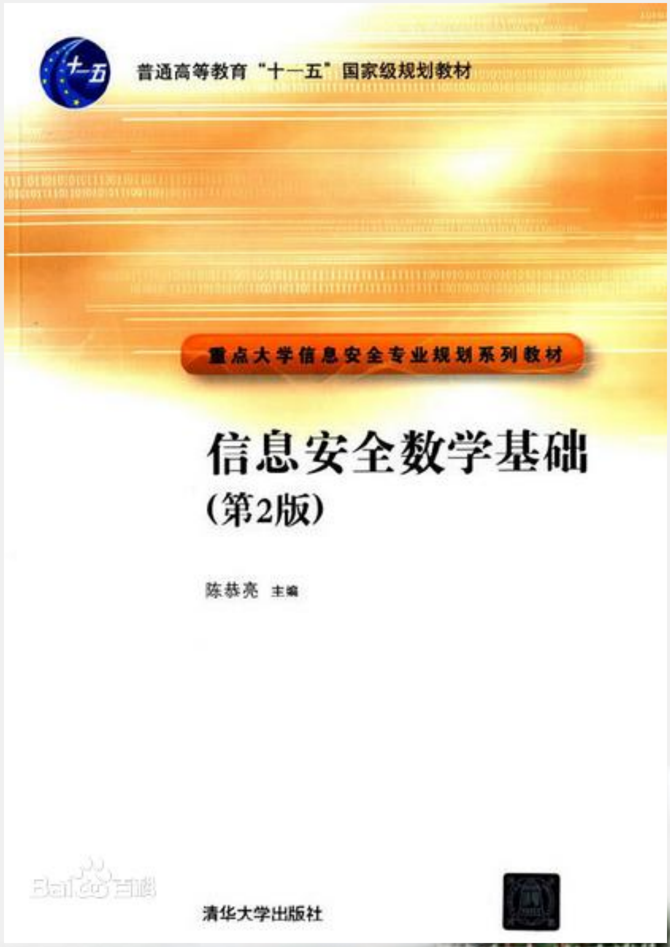
E-mail: isszhfg@mail.sysu.edu.cn

HomePage: https://cse.sysu.edu.cn/content/2460

第四讲 密码的数学基础(复习一)

- 初等数论
  素数，整除，
  同余，原根
  连分式

第1章 整数的可除性
第2章 同余
第3章 同余式
第4章 二次同余式与平方剩余
第5章 原根与指标
第6章 素性检验
第7章 连分数



数论——数学中的皇冠

数论就是指研究整数性质的一门理论。整数的基本元素是素数，所以数论的本质是对素数性质的研 究。

- **初等数论（古典数论）**

  初等数论的大部份内容早在古希腊欧几里德的《几何原本》中就已出现。

- **高等数论（近代数论）**

  代数数论，解析数论，算术代数几何等等

初等数论（elementary number theory）

初等数论部分是以整数的整除性为中心的，包括

- **整除性：** 整除、因数、倍数、质数与合数；唯一分解定理、欧几里德的辗转相除法、算术基本定理、素数个数无限证明等
- **同余式：** 同余、原根、指数、平方剩余、同余方程；二次互反律、欧拉定理、费马小定理、中国剩余定理等
- **不定方程：** 丢番图方程；低次不定方程的求解问题
- **连分数：** 连分数，连分数展开，循环连分数展开、最佳逼近问题、佩尔方程求解
- **数论函数：** 欧拉函数等。

初等数论

- 中国古代对初等数论的研究有着光辉的成就，《周髀算经》、《孙子算经》、《张邱建算经》、《数书九章》等古文献上都有记载。孙子定理比欧洲早500年，西方常称此定理为中国剩余定理，秦九韶的大衍求一术也驰名世界。
- 中国近现代的数论研究：陈景润的哥德巴赫猜想证明
- 初等数论不仅是研究纯数学的基础，也是许多学科的重要工具。它的应用是多方面的，如计算机科学、组合数学、密码学、信息论等。

数论知识

基本概念

整除性

定义 对于整数$a \neq 0$，b。我们说a整除b，如果存在一个整数k使得$b=ka$，我们把a叫做b的因数，b叫做a的倍数，记为$a|b$。如果这个k不存在，我们说a不整除b，记为$a \nmid b$。

性质1 1) 对于任意$a \neq 0, a|0$，$a|a$，对于任意$b, 1|b$。

2) 如果$a|b$，$b|c$，则$a|c$。

3) 如果$a|b$，$a|c$，则$a|(sb+tc)$，这里s和t是任意整数。

定理 设a，b是两个整数，其中$b>0$，则存在两个唯一的整数q及r，使得

$$a = bq + r，0 \leq r < b$$

成立。

素数

定义　一个大于1的正整数，如果它的正因数只有1和它本身，就叫做素数，否则就叫做合数。

定理 素数的个数是无穷的。

证明. 如果素数的个数是有限的可令$p_1 = 2$，$p_2 = 3, \cdots$，p_k是全体素数。再令$p = p_1 p_2 \cdots p_k + 1$，知其必为合数，而$p$不可为$p_1$，$p_2, \cdots$，$p_k$之中任意一个整除，必然存在其它素数，因此，与素数的个数是有限的假设矛盾。

定理3 (素数数量定理) 如果$\pi(x)$表示小于x的所有素数个数，则有$\pi(x)\approx\dfrac{x}{\ln x}$，也就是说当$x\to\infty$时，比率$\pi(x)/(x/\ln x)\to 1$。

在各种密码应用中经常要求使用300位左右的十进制素数，通过**定理3**我们可以估计

$$\pi(10^{300})-\pi(10^{299})\approx\frac{10^{300}}{\ln 10^{300}}-\frac{10^{299}}{\ln 10^{299}}\approx 1.3\times 10^{97},$$

因此，足够使用。

互素

定义 设a_1，$a_2,\cdots$，a_n是n个不全为零的整数。若整数d是它们之中每一个的因数，那么d就叫a_1，$a_2,\cdots$，a_n的一个公因数。整数a_1，$a_2,\cdots$，a_n的公因数中最大的一个叫最大公因数，记作$(a_1, a_2,\cdots, a_n)$，若$(a_1, a_2,\cdots, a_n)=1$，就说a_1，$a_2,\cdots$，a_n互素。

定理4 设a，b，c是任意三个不全为零的整数，且

$$a=bq+c,$$

其中q是整数，则$(a, b)=(b, c)$。

欧几里得算法

Euclidean算法的表述

不失一般性假定任意$a>0$，$b>0$有

$a = bq_1 + r_1, 0 < r_1$

$b = r_1 q_2 + r_2, 0 < r_2$

$r_1 = r_2 q_3 + r_3, 0 < r$

… … …

$r_{n-3} = r_{n-2} q_{n-1} + r_{n-}$

$r_{n-2} = r_{n-1} q_n + r_n, 0$

$r_{n-1} = r_n q_{n+1} + r_{n+1}$， $r_{n+1} = 0$。

INPUT: Two positive integers, a and $b(a > b)$.

OUTPUT: $GCD(a,b)$: the greatest common divisor, d, of a and b.

1. if $b = 0$
2. return a
3. else
4. return $GCD(b, a \mod b)$

定理5 任意$a>0$，$b>0$，则(a, b)就是上述过程中最后一个不等于零的余数，即$(a, b) = r_n$。

定理6 若任给整数$a>0$，$b>0$，则存在两个整数m，n使得

$$(a，b)=ma+nb。$$

例子7 计算$(482,1180)$。

$1180=2\cdot 482+216$

$482=2\cdot 216+50$

$216=4\cdot 50+16$

$50=3\cdot 16+2$

$16=8\cdot 2+0$。

因此,$(482,1180)=2$。

可以看到余数都经历了：剩余$\rightarrow$除数$\rightarrow$被除数$\rightarrow$忽略的过程。

根据**定理5**的证明,我们可以得到递推公式:

$x_1=1,\ x_2=-q_2,\ x_j=-q_jx_{j-1}+x_{j-2}$

$y_1=-q_1,\ y_2=1+q_1q_2,\ y_j=-q_jy_{j-1}+y_{j-2}$

则$ax_n+by_n=(a,b)$。

因此，$x_1=1,\ x_2=-2,\ x_3=-2x_2+x_1=5,$

$x_4=-4x_3+x_2=-22,\ x_5=-3x_4+x_3=71$。

同样有$y_5=-29$，所以$482\cdot 71+1180\cdot(-29)$

$=2=(482,1180)$。

这一过程被称为扩展Euclidean算法。

定理7 若$a\mid bc,(a,b)=1$，则$a\mid c$。

整数唯一分解定理

引理1 设a是任一大于1的整数，则a的除1以外的最小正因数q是素数，并且当a是合数时，

$$q \le \sqrt{a}。$$

引理2 若p是一素数，a是任一整数，则有$p \mid a$或$(p, a) = 1$。

引理3 若p是素数，$p|ab$，则$p \mid a$或$p \mid b$。

定理8 (整数唯一分解定理) 任何大于1的正整数都能分解成素数的乘积,即对于整数$a>1$，有

$$a = p_1 p_2 \cdots p_n,\quad p_1 \le p_2 \le \cdots \le p_n, \tag{I}$$

其中p_1，$p_2,\cdots$，p_n都是素数,并且若

$$a = q_1 q_2 \cdots q_m,\quad q_1 \le q_2 \le \cdots \le q_m, \tag{II}$$

其中q_1，$q_2,\cdots$，q_m都是素数，则$m=n$，$q_i = p_i (i=1,2,\cdots,\ n)$。

证明:首先证明(I)成立，数学归纳法，当$a=2$时(I)显然成立，假定一且小于a的正整数都成立，考虑a如果为素数显然成立，如果为合数则必有分解$a=bc, 1<b\le c<a$,可知b和c都能表示为素数乘积，因此a也能表示为素数乘积，故(I)成立。

其次,证明唯一性。由(I)和(II)知$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$，由引理3可知$p_1 \mid q_j$，$q_1 \mid p_k$，由于$q_j$，$p_k$为素数，所以$p_1 = q_j$，$q_1 = p_k$。同时有$p_1 \ge q_1$和$q_1 \ge p_1$，因此，$p_1 = q_1$。进一步，由$p_2 \cdots p_n = q_2 \cdots q_m$可以得$p_2 = q_2$，以此类推，最后可得，$m=n$，$p_n = q_m$。

几种特殊的素数

- **梅森(Mersenne)素数:**
  2^p-1, p is prime
- 广义梅森素数
  $2^p \pm a$, p is prime。（a是小奇数）
- **费马素数Fn**
  2^2^n+1 (当 n取0、1、2、3、4时，这个式子对应值分别为3、5、17、257、65537，费马发现这五个数都是素数)
- 孪生素数
  p, p+2都是素数

一次不定方程

二元一次不定方程是指

$$a_1x + a_2y = n, \qquad \text{(III)}$$

其中a_1，a_2，n是给定的整数，$a_1a_2 \neq 0$。

定理9 方程(III)有整数解的充分必要条件是

$$(a_1, a_2) \mid n。$$

定理10 设$(a_1, a_2) = 1$，则(III)的全部解可表示为

$$x = x_0 + a_2t, \quad y = y_0 - a_1t,$$

其中x_0，y_0为(III)的一组解，t为任意整数。

同余

定义 15 给定正整数m，如果用m去除两个整数a和b所得的余数相同，我们就说a，b对m同余，记为$a \equiv b \pmod{m}$，如果余数不同，a，b对m就不同余，记为$a \not\equiv b \pmod{m}$。

性质 2 1) 自反性 $a \equiv a \pmod{m}$;

2) 对称性 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$;

3) 传递性$a \equiv b \pmod{m}, b \equiv c \pmod{m}, a \equiv c \pmod{m}$。

定理11 整数a，b对模m同余的充分必要条件是$m \mid a-b$。

定理12 如果$a \equiv b \pmod{m}$，$\alpha \equiv \beta \pmod{m}$,则有

1) $ax+\alpha y \equiv bx+\beta y \pmod{m}$，其中$x$，$y$为任意整数；

2) $a\alpha \equiv b\beta \pmod{m}$;

3) $a^n \equiv b^n \pmod{m}$;

4) $f(a) \equiv f(b) \pmod{m}$，$f(x)$为任意给定整系数多项式。

剩余类和完全剩余类

定义16 设m是一个给定整数，$C_r\,(r=0,1,\cdots,\ m-1)$表示所有形如$qm+r$的整数组成的集合，其中$q=0,\pm1,\cdots$，则$C_0$，$C_1,\cdots$，$C_{m-1}$叫做模$m$的剩余类。

定理14 设$m>0$，C_0，$C_1,\cdots$，C_{m-1}是模m剩余类，则有

1) 每个整数都包含在某一个剩余类C_j中，这里$0\le j\le m-1$;

2) 两个整数x，y属于同一类的充分必要条件是

$$x\equiv y\ (\bmod m)\ 。$$

定义17 在模m的剩余类C_0，$C_1,\cdots$，C_{m-1}中各取一个数$a_j\in C_j$，$j=0,1,\cdots$，$m-1$，此m个数a_0，$a_1,\cdots$，a_{m-1}称为模m的一组完全剩余系。

由定义立即得到：

定理15 m个整数成为模m的完系的充要条件为两两对模m不同余。

#常用的完全剩余系$0,1,\cdots$，$m-1$，称为模m的非负最小完全剩余系。

缩 系

定义18 如果一个模m的剩余类里的数与m互素(显然一个互素全部互素)，就把它叫做一个与模m互素的剩余类，在其中各取一个数组成的集叫模m的一组缩系。

定义19 欧拉函数$\varphi(n)$是一个定义在整数上的函数，$\varphi(n)$的值为序列$0,1,\cdots$，$n-1$中与n互素的数的个数。显然p是素数时$\varphi(p)=p-1$。

定理16 模m的一组缩系含有$\varphi(m)$个数。

定理17 若$a_1,\cdots$，$a_{\varphi(m)}$是$\varphi(m)$个与m互素的整数，则$a_1,\cdots$，$a_{\varphi(m)}$为缩系的充要条件为它们两两模m不同余。

定理18 若$(a$，$m)=1$，x是通过模m的缩系则ax也是模m的缩系。

定理19(欧拉定理）设$m>1, (a, m)=1$，则

$$a^{\varphi(m)} \equiv 1 \pmod m。$$

由**定理19**立刻可得：

定理20（费马小定理）若p是素数，则

$$a^{p} \equiv a \pmod p。$$

定理21 设$m_1>0$，$m_2>0$,$(m_1，m_2)=1$，而x_1，x_2分别通过模m_1，m_2的缩系，则$m_2x_1+m_1x_2$通过模m_1m_2的缩系。

由**定理21**立得

推论1 若$(m_1，m_2)=1$，则$\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$。

定理22 设n的标准分解$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)。$$

一次同余式

定义 20 设$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots a_1 x+a_0$，其中$n>0$，$a_i(i=0,1,\cdots,n)$是整数，又设$m>0$，则

$$f(x)\equiv 0(\mathrm{mod}\, m)$$

叫模m的同余式。若$a_n\not\equiv 0(\mathrm{mod}\, m)$，则$n$叫次数。如果$x_0$满足$f(x_0)\equiv 0(\mathrm{mod}\, m)$，则$x\equiv x_0(\mathrm{mod}\, m)$叫同余式的解。不同的解是指互不同余的解。

定理23 设$(a, m)=1$，$m>0$，则同余式

$$ax\equiv b(\mathrm{mod}\, m)$$

恰有一个解，这个解就是$x\equiv ba^{\varphi(m)-1}(\mathrm{mod}\, m)$。特别地，我们将$ax\equiv 1(\mathrm{mod}\, m)$的解$a^{\varphi(m)-1}$称为$a$的逆元，记为$a^{-1}$。

定理24 (Lagrange定理) 设p是素数，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0$，$n>0$，$a_n\not\equiv 0(\bmod p)$，是一个整系数多项式，则同余式

$$f(x)\equiv 0(\bmod p)$$

最多有n个解。

原根

定义 21 设$m>0,(m,a)=1$，l是使

$$a^{l}\equiv 1(\mathrm{mod}\, m)$$

成立的最小正整数，则l叫做a对模m的次数。

定理25 设a对模m的次数为l，如有$a^{n}\equiv 1(\mathrm{mod}\, m)$，$n>0$，则$l\mid n$。

推论 2 设a对模m的次数为l，则$l\mid \varphi(m)$。

定理26 设a对模m的次数为l，则

$$1,\ a,\ a^2, \cdots,\ a^{l-1}$$

对模m两两互不同余。

定理27 设a对模m的次数是l，$\lambda > 0$，a^λ对模m的次数为l_1，则$l_1 = \dfrac{l}{(\lambda,\ l)}$。

推论3 设a对模m的次数是l，则$\varphi(l)$个数

$$a^\lambda,\ (\lambda,\ l) = 1,\ 0 < \lambda \le l,$$

对模m的次数均为l。

定理28 设p是一个素数，如果存在整数a，它对模p的次数为l，则恰有$\varphi(l)$个对模p两两不同余的整数，它们对模p的次数都为l。

定义 22 设整数$m>0, (g, m)=1$，如果整数g对m的次数为$\varphi(m)$，则g叫模m的一个原根。

定理29 设$(g, m)=1$，$m>0$，则g是m的一个原根的充分必要条件是

$$g, g^2, \cdots, g^{\varphi(m)}$$

组成模m的一组缩系。

定理30 $m=2, 4, p^l, 2p^l (l\geq 1, p$为奇素数)时，$m$有原根。

定理31 设$m>2$，$\varphi(m)$的所有不同素因子是q_1，$q_2,\cdots$，q_s,$(g，m)=1$，则g是m的一个原根的充分必要条件是

$$g^{\frac{\varphi(m)}{q_i}} \not\equiv 1 \pmod{m} \qquad (i=1,2,\cdots, s)。$$

例子8 12是41的一个原根。

设$m=41$，$\varphi(41)=40=2^3 5$，$q_1=2$，$q_2=5$，

$12^{20}\equiv 40\not\equiv 1 \pmod{41}$,$12^8\equiv 18\not\equiv 1 \pmod{41}$，故

由**定理31**知12是41的一个原根。

中国剩余定理

孙子问题（Sun Zi's problem）记载于中国古代约公元3世纪成书的《孙子算经》内面，是原书卷下第26题："今有物不知其数，三三数之剩二；五五数之剩三；七七数之剩二，问物几何？答曰：二十三"。用现代符号表示为 $N\equiv2\pmod{3}\equiv3\pmod{5}\equiv2\pmod{7}$，其最小正数解是23。《孙子算经》中给出了其中关键的步骤是："凡三三数之剩一，则置七十；五五数之剩一，则置二十一；七七数之剩一，则置十五"。因此可设 $N=70\times2+21\times3+15\times2-2\times105=23$。原题及其解法中的3、5、7后来叫"定母"，70、21、15叫"乘数"。但在《孙子算经》中并没有说明求乘数的方法，直到1247年宋代数学家秦九韶在《数书九章》中才给出具体求法。70是5与7最小公倍的2倍，21、15分别是3与7、3与5最小公倍数的1倍。秦九韶称这2、1、1的倍数为"乘率"，求出乘率，就可知乘数。

「三人同行七十稀，五树梅花廿一枝，七子团圆整半月，除百零五便得知。」

中国剩余（孙子）定理

$k \geq 2, m_1, m_2, \ldots, m_k$ 两两互素，

$m = m_1 m_2 \ldots m_k, m = m_i M_i, i = 1,2,\ldots k$

则一次同余式组

$$x \equiv b_1 (\mathrm{mod}\, m_1), x \equiv b_2 (\mathrm{mod}\, m_2), \ldots x \equiv b_k (\mathrm{mod}\, m_k)$$

的解为 $x \equiv M_1 M_1' b_1 + M_2 M_2' b_2 + \ldots M_k M_k' b_k (\mathrm{mod}\, m),$

其中 $M_i M_i' \equiv 1 (\mathrm{mod}\, m_i), i = 1,2,\ldots k.$

二次剩余

定义： $x^2=a \bmod n$ 有解，则a 称为mod n 的一个二次剩余，否则称为mod n 的一个二次非剩余。

定理：令p是一个素数

1）$QR_p=\{x^2 \bmod p \mid 0<x<=(p-1)/2\}$

2) 二次剩余和二次非剩余各有(p-1)/2个。

Euler 准则

令p是一个素数，那么对任意的x \in Z_p^*, x是mod p 的二次剩余的充分必要条件是：

$$x^{(p-1)/2} = 1 \bmod p$$

连分式（数）

表达式

$$b_0 + \cfrac{a_0}{b_1 + \cfrac{a_1}{b_2 + \cdots + \cfrac{a_{k-1}}{b_k + \cdots}}} \qquad (9.1.3)$$

称为连分式。其中

$\frac{a_{k-1}}{b_k}$ 称为连分式(9.1.3)的第k节，

a_{k-1}与b_k称为连分式第k节的两个项。

a_0，a_1，a_2，…称为连分式的部分分子；

b_0称为连分式的常数项，

b_1，b_2，…称为连分式的部分分母。

节数无限的连分式称为无限连分式，记作

$$b_0+\cfrac{a_0}{b_1+\cfrac{a_1}{b_2+\cdots+\cfrac{a_{k-1}}{b_k+\cdots}}}\quad，k=1，2，\cdots \qquad (9.1.4)$$

节数有限的连分式称为有限连分式，记作

$$b_0+\cfrac{a_0}{b_1+\cfrac{a_1}{b_2+\cdots+\cfrac{a_{k-1}}{b_k}}}\quad，k=1，2，\cdots，m \qquad (9.1.5)$$

有限连分式(9.1.5)也称为 k 节连分式。

如果把 k 节连分式(9.1.5)记成

$$\frac{P_k}{Q_k}=b_0+\cfrac{a_0}{b_1+\cfrac{a_1}{b_2+\cdots+\cfrac{a_{k-1}}{b_k}}} \qquad (9.1.6)$$

则称$\dfrac{P_k}{Q_k}$为连分式(9.1.3)的第 k 个渐近分式。

一个(有限)连分数是一个非负整数的 m 组，即

$$[q_1, \cdots, q_m]$$

它是下面表达式的简写形式：

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_m}}}$$

- 连分数展开： a/b=[q1,q2,...,qm]
- 对任意1<=j<=m, 由[q1,q2,...,qj]定义的分数成为a/b的第j个收敛子。

例 5.16 我们计算 34/99 的连续分数展开。用 Euclidean 算法进行如下计算：

$$\begin{aligned} 34 &= 0 \times 99 + 34 \\ 99 &= 2 \times 34 + 31 \\ 34 &= 1 \times 31 + 3 \\ 31 &= 10 \times 3 + 1 \\ 1 &= 3 \times 1 \end{aligned}$$

因此，34/99 的连续分数展开为[0,2,1,10,3]，即

$$\frac{34}{99} = 0 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{10 + \cfrac{1}{3}}}}$$

这个连分数的收敛子如下：

$$\begin{aligned} [0] &= 0 \\ [0,2] &= 1/2 \\ [0,2,1] &= 1/3 \\ [0,2,1,10] &= 11/32 \\ [0,2,1,10,3] &= 34/99 \end{aligned}$$

Suppose the continued fraction of rational $\frac{Z}{M}$ is determined by integers $[a_0, a_1, \cdots, a_t]$ with

$$\frac{Z}{M} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\begin{matrix} \cdots & & \cdots \\ \cdots & + & \cfrac{1}{a_{t-1} + \frac{1}{a_t}} \end{matrix}}}.$$

Let $\frac{p_v}{q_v}$ be the rational determined by integers $[a_0, a_1, \cdots, a_v]$ with

$$\frac{p_v}{q_v} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\begin{matrix} \cdots & & \cdots \\ \cdots & + & \cfrac{1}{a_{v-1} + \frac{1}{a_v}} \end{matrix}}}. \tag{2}$$

Then $\{\frac{p_0}{q_0}, \frac{p_1}{q_1}, \cdots, \frac{p_t}{q_t}\}$ is the convergent sequence of continued fraction expansion of $\frac{Z}{M}$.

Theorem 1 *[5] Let α be a real number, and let r/s be a rational with $gcd(r, s) = 1$ and $|\alpha - r/s| < 1/2s^2$. Then r/s is a convergent of the continued fraction expansion of α.*

定理 5.14 假定 $\gcd(a, b) = \gcd(c, d) = 1$ 且

$$\left| \frac{a}{b} - \frac{c}{d} \right| < \frac{1}{2d^2}$$

那么，c/d 是 a/b 连分数展开的一个收敛子。