

数论进入了应用学科*

孙 琦

(四川大学)

一、引 言

长期以来,数论被认为是脱离实际的.于是,产生了两种极端的观点,一种为数论的无用而洋洋得意,典型的例了是Hardy^[1]在《一个数学家的自白》中所称颂的,认为数论是“洁身自好,出污泥而不染”.另一种为数论无用而悲叹,如Gamow^[2]所著《从一到无穷大》中的一段话:“……,迄今为止,数学还有一个大分支没有找到什么用途(除了智力体操的作用外)……”.实际上,这些观点都是陈旧的.近几十年来,数论,特别是初等数论(包括代数数论的经典部分)在计算机科学、组合数学、代数编码、密码学、信号的数字处理、数值计算等领域内得到广泛的应用.例如代数编码中设计出的各种纠错码,基本上是以有限域和数论作为理论依据的,而有限域与数论又是紧密相联的.最近,Bremmer和Morton^[3]宣布一些不定方程在编码上得到应用,为此他们给出了椭圆曲线 $y^2 = 4cx^3 + 13$, $c = 1, 3, 9$ 的全部整数解.在数字信号处理中,为了快速计算卷积和离散付里叶变换(DFT),提出了各种变换,例如快速付里叶变换(FFT),快速数论变换(NTT),Wnograd快速变换算法

(WFTA),多项式变换(PT)等,所有这些变换有一个共同的特点,就是以数论作为理论依据.关于数论在以上诸方面的应用,有兴趣的读者可分别参看以下各文献.关于数论在计算机科学中的应用,可参看[4]和[5];在代数编码中的应用,可参看[6]和[7];在组合论中的应用,可参看[8]和[9];在密码学中的应用,可参看[10]和[11];在信号处理中的应用,可参看[12],[13]和[14];在数值计算中的应用可参看[15].

下面二节,我们分别介绍有关孙子定理的一些应用以及数论在公开密钥体制中的应用.其中,也包括我们近期的工作.

二、关于孙子定理的应用

我们知道,数论中的孙子定理有着广泛的应用.例如,利用孙子定理可构造整数的模系数记数法.设 $s > 1$, $m_1, \dots, m_s$ 两两互素, $M = m_1 \dots m_s$, $0 \leq x < M$, 所谓整数 x 的模系数记数法是指 x 对模 $m_1, \dots, m_s$ 的剩余表示 $\{\langle x \rangle_{m_1}, \dots, \langle x \rangle_{m_s}\}$, 其中 $\langle x \rangle_{m_j}$ 表示 x 模 m_j ($j = 1, 2, \dots, s$)的最小非负剩余.这一记数法在计算机上是很有用的^[16], 它虽然没有固定基数制的许多优点,但用它来实现加法和乘法时,由于不用进位,可节省时间.

设 $Z_M = \{0, 1, \dots, M-1\}$ 是一个模 M 的剩余类环, $Z_M^* = Z_{m_1} \times Z_{m_2} \times \dots \times Z_{m_s}$, 等式右端表示环 $Z_{m_1}, Z_{m_2}, \dots, Z_{m_s}$ 的直积. $x \in Z_M$, 如果知道了 x 对模 $m_1, \dots, m_s$ 的剩余表示, 那

• 1985年4月28日收到.

么, 用孙子定理可得

$$x = \left\langle \sum_{j=1}^s M'_j M_j \langle x \rangle_{m_j} \right\rangle_m, \quad (1)$$

其中 $M = \prod_{j=1}^s m_j M_j$ ($j = 1, \dots, s$),

$$M'_j M_j \equiv 1 \pmod{m_j}, \quad j = 1, \dots, s \quad (2)$$

因为, 由孙子定理可知 Z_M 和 Z_M^* 之间存在一一对应的关系。因此, Z_M 中任意数的剩余表示是唯一的, 反之亦真。 Z_M^* 可看成 Z_M 中所有整数的剩余表示所成的集。我们定义 Z_M^* 中的加法 $\oplus$ 为

$$\begin{aligned} & \{\langle x \rangle_{m_1}, \dots, \langle x \rangle_{m_s}\} \oplus \{\langle y \rangle_{m_1}, \dots, \langle y \rangle_{m_s}\} \\ &= \{\langle \langle x \rangle_{m_1} + \langle y \rangle_{m_1} \rangle_{m_1}, \dots, \langle \langle x \rangle_{m_s} + \langle y \rangle_{m_s} \rangle_{m_s}\} = \{\langle x+y \rangle_{m_1}, \dots, \langle x+y \rangle_{m_s}\}. \end{aligned}$$

Z_M^* 中的乘法可类似的定义。因此, 用模系数记数法, Z_M 中的数对模 M 的运算, 可以通过 Z_M^* 中的元对运算 $\oplus$ 和 $\odot$ 来完成, 也可以分别通过 Z_{m_j} 中的数对模 m_j ($j = 1, \dots, s$) 的运算来完成。

因此, 数论变换 (即 Z_M 上的 DFT) 和公开钥密码的 RCA 体制 (下一节将作介绍), 都可以通过一个“剩余计算机”来实现。

在应用孙子定理进行计算, 当 m_j ($j = 1, \dots, s$) 和 s 增大时, 求出 (2) 式中的 M'_j 将变得困难。最近, 我们^[17]证明了下面的定理。

定理 1 如果 $(m_1, \dots, m_s)$ 是不定方程

$$\frac{1}{x_1} + \dots + \frac{1}{x_s} - \frac{1}{x_1 \dots x_s} = 1, \quad 1 < x_1 < \dots < x_s, \quad s \geq 2 \quad (3)$$

的一组解, 则对模 $m_1, \dots, m_s$, (2) 式中 M'_j 可取 $M'_j = 1$ ($j = 1, \dots, s$)。我们还指出, 可通过不定方程

$$\frac{1}{x_1} + \dots + \frac{1}{x_s} - \frac{1}{x_1 \dots x_s} = 1, \quad 1 < x_1 < \dots < x_s \quad (4)$$

的解来构造 (3) 式的解, 并给出解的个数的一个下界。

定理 2 设 $m_1^{(j)}, \dots, m_{t-1}^{(j)}$ ($t \geq 3$) 是方程 (3) 在 $s = t-1$ 时的解, $k_j = (m_1^{(j)} \dots m_{t-1}^{(j)})^2 - 1$ ($j = 1, \dots, \Omega(t-1)$), $A(s)$ 和 $\Omega(s)$ 分别表示方程 (3) 和 (4) 解的个数, 则

$$A(t+1) \geq \Omega(t) + \sum_{j=1}^{\Omega(t-1)} \left(\frac{d(k_j)}{2} - 1 \right) \quad (5)$$

其中 $d(k_j)$ 表示 k_j 的正因子的个数 ($j = 1, \dots, \Omega(t-1)$)。对于 $\Omega(s)$, 作者^[18]曾证明 $s \geq 4$ 时 $\Omega(s+1) > \Omega(s) > 0$ 。由此及 (5) 式可得下面的推论。

推论 1 设 $t \geq 3$, 则有 $A(t+1) \geq \Omega(t) + \Omega(t-1)$ 。

推论 2 设 $t \geq 9$, 则有 $A(t+1) \geq \Omega(t) + \Omega(t-1) + 6$ 。

推论 3 设 $t \geq 9$, $t \equiv 1 \pmod{2}$, 则有 $A(t+1) \geq \Omega(t) + \Omega(t-1) + 10$ 。

1964 年, 柯召和作者^[19]给出了方程 (4) 在 $2 \leq s \leq 6$ 的全部解。用类似的方法, 作者和曹珍富给出了 (3) 在 $3 \leq s \leq 6$ 时的全部解。 $s = 6$ 时, 共有 17 组解, 它们是:

(2, 3, 7, 43, 1807, 3263441), (2, 3, 7, 43, 1811, 654133), (2, 3, 7, 43, 1819, 252701), (2, 3, 7, 43, 1825, 173471), (2, 3, 7, 43, 1945, 25271), (2, 3, 7, 43, 1871, 51985), (2, 3, 7, 43, 1901, 36139), (2, 3, 7, 43, 2053, 15011), (2, 3, 7, 43, 2167, 10841), (2, 3, 7, 43, 2501, 6499), (2, 3, 7, 43,

3041, 4447), (2, 3, 7, 43, 3611, 3613), (2, 3, 7, 47, 395, 779729), (2, 3, 7, 47, 481, 2203), (2, 3, 7, 53, 271, 799), (2, 3, 7, 71, 103, 61429), (2, 3, 11, 23, 31, 47057).

最后, 我们指出, 计算 (1) 时, 需要求模 M 的最小非负剩余, 因此, 这不能在只能实行 m_i 的运算而不能实行模 M 的运算的计算机上实现. 那么, 是否存在不用 (1) 式的由 $\{\langle x \rangle_{m_1}, \dots, \langle x \rangle_{m_s}\}$ 到 x 的转换方法? 这样的方法是存在的, 它就是只需要作 m_j 运算的混合基数制记数法.

设 $M = m_1 \cdots m_s$, $x \in \mathbb{Z}_M$, x 是混合基数制记数法表示为

$$x = a_s \prod_{i=1}^{s-1} m_i + \cdots + a_3 m_1 m_2 + a_2 m_1 + a_1, \quad 0 \leq a_i < m_i, \quad i = 1, \dots, s \quad (6)$$

(如果 $m_i = 10$, $i = 1, 2, \dots, s$, 即为通常的十进制).

现在, 我们只需要从 x 的模系数表示法 $\{\langle x \rangle_{m_1}, \dots, \langle x \rangle_{m_s}\}$ 来求出 $a_1, \dots, a_s$, 那么由 (6) 也就给出 x . 下面给出的方法求 $a_1, \dots, a_s$ 只需作模 m_i ($i = 1, \dots, s$) 运算.

设 $x_i = \langle x \rangle_{m_i}$, $i = 1, \dots, s$, 由 (6) 得 $a_1 \equiv x_1 \pmod{m_1}$, 故 $x_1 = a_1$, 由 (6) 给出

$$\frac{x - x_1}{m_1} = a_s \prod_{i=2}^{s-1} m_i + \cdots + a_3 m_2 + a_2 \quad (7)$$

设 $m_1 c_{1,2} \equiv 1 \pmod{m_2}$, $0 < c_{1,2} < m_2$, (7) 给出 $a_2 \equiv (x_2 - x_1) c_{1,2} \pmod{m_2}$, 即可得

$a_2 = \langle (x_2 - x_1) c_{1,2} \rangle_{m_2}$. 现由 (7) 得

$$\frac{\frac{x - x_1}{m_1} - a_2}{m_2} = a_s \prod_{i=3}^{s-1} m_i + \cdots + a_3, \quad \text{故}$$

$$\langle (x_3 - x_1) c_{1,3} - a_2 \rangle_{m_3} \equiv a_3 \pmod{m_3},$$

即可求出 a_3 , 依此类推, 如果已求出了 $a_1, a_2, \dots, a_{i-1}$, 那么 a_i 可如下求出

$$a_i = \langle \cdots \langle (x_i - a_1) c_{1,i} - a_2 \rangle_{m_2} - \cdots - a_{i-1} \rangle_{m_i},$$

其中

$$c_{i,j} = \langle m_i^{q(m_j)-1} \rangle_{m_j}, \quad 1 \leq i < j \leq s.$$

例 设 $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $M = 30$, 求 $\{1, 1, 4\}$ 所表示的十进制数.

$$c_{1,2} = \langle 2^{q(3)-1} \rangle_3 = 2, \quad c_{1,3} = \langle 2^{q(5)-1} \rangle_5 = 3, \quad c_{2,3} = \langle 3^{q(5)-1} \rangle_5 = 2,$$

故 $a_1 = 1$, $a_2 = \langle (1 - 1)2 \rangle_3 = 0$, $a_3 = \langle (3 \cdot 3 - 0)2 \rangle_5 = 3$, 由 (6) 得 $x = 3 \cdot 6 + 1 = 19$.

三、数论与公开密钥体制

传统的保密系统, 收发双方有相同的加密密钥和解密密钥, 而加密密钥和解密密钥也是相同的, 或者极易相互推出, 因此我们把它们看成一个密钥, 这需要严格保密不能丢失的. 这样, 整个系统的密钥数量往往很大, 难以分配和管理. 另一方面, 收方可以修改内容, 发方也可以否认所发的内容. 公开密钥码最重要之处有两点, 一是将加密密钥和解密密钥分开, 加密密钥可以公开, 而解密密钥则是严格保密的; 二是, 这一体制可以发送签了名的消息. 因此, 公开密钥体制的提出, 解除了上述传统的保密系统所产生的困难, 这是密码学中的重大突破.

公开密钥码体制是基于1976年Diffie和Hellman [20] 提出的险门单向函数 (trap-

door one-way function), 所谓陷门单向函数是指满足以下三条件的函数 (一般可设为某一区间上的数论函数) $f(n)$:

- ① 对 $f(n)$ 的定义域中的每一个 n , 均存在函数 $f^{-1}(l)$, 使 $f^{-1}(f(n)) = f(f^{-1}(n)) = n$.
- ② $f(n)$ 与 $f^{-1}(l)$ 都容易计算.
- ③ 仅根据已知的计算 $f(n)$ 的算法, 去找出计算 $f^{-1}(l)$ 的容易算法是非常困难的.

第一个找出陷门单向函数的是 Rivest, Shamir 和 Adleman^[21], 即著名的 RSA 公开密钥体制.

利用陷门单向函数, 就可以构成如下的体制. 有一个部门, 下设 A, B, C, ... 若干机构, 各机构均有自己的陷门单向函数, 分别设为 $f_A(n)$, $f_B(n)$, $f_C(n)$, ..., 即分别为它们各自编码方法而予公开, 而各译码方法, 即诸 $f_A^{-1}(l)$, $f_B^{-1}(l)$, $f_C^{-1}(l)$, ... 则是保密的. 这样, 部门中的任一个机构 (包括部门外的机构), 都可给其中某一个机构, 例如 A 发保密信. 设 B 向 A 发保密信, 方法是, B 向 A 发的明文为 n , 代入 A 公开的陷门单向函数得 $f_A(n) = m$, m 即为密文, 由于只有 A 知道 $f_A^{-1}(m)$ 的算法, 因此, A 可由 $f_A^{-1}(m) = f_A^{-1}(f_A(n)) = n$ 脱密.

另外, 部门内的各成员可以彼此发签名信. 例如, B 给 A 发签名信, 设明文为 n , 先用 $f_B^{-1}(l)$ 对 n 加密得 $f_B^{-1}(n) = m$, 再用 $f_A(n)$ 对 m 加密得 $f_A(m) = l$. A 收到 l 后, 由 $f_A^{-1}(l) = m$ 得 $f_B(m) = f_B(f_B^{-1}(n)) = n$. 因为只有 B 才能发这样的双重加密信, 所以 B 的签名无法伪造.

RSA 体制的陷门单向函数定义为

$$f(n) = \langle n^s \rangle_m = l, \quad f^{-1}(l) = \langle l^t \rangle_m.$$

其中 n 为 $[1, m-1]$ 中任一整数, $m = pq$, p, q 是两个不同的大素数, $s > 0$, $(s, (p-1)(q-1)) = 1$, $0 < t < (p-1)(q-1)$ 满足 $st \equiv 1 \pmod{(p-1)(q-1)}$. 由于 m 大时, 分解 m 十分困难, 所以只知道 s 和 m , 难以求出 t (或 p, q). 因此, $f(n) = \langle n^s \rangle_m$ 是一个陷门单向函数. 由此构造的公开钥密码是很难破的.

用有限域 F_p 上多项式的性质, 我们 [22] 给出一类新的陷门单向函数.

定理 设 $n > 0$ 是一个整数, p 是一个素数, $n = a_h p^h + \dots + a_0$, 整数 a_j 满足 $0 \leq a_j < p$, $j = 0, 1, \dots, h-1$, $1 \leq a_h < p$ (简记为 $n = [a_h, a_{h-1}, \dots, a_0]_p$), 任给区间 $[1, M]$, 选取有限域 F_p 上的一个 m 次多项式 $g(x) = g'_1(x) \dots g'_k(x)$ 使得对任一 $n \in [1, M]$, $n = [a_h, \dots, a_0]_p$ 均有 $(g(x), a_h x^h + \dots + a_0) = 1$ 和 $m > h$. 这里 $l_j \geq 1$, $g_j(x)$ 是 F_p 上的 m_j 次不可约多项式, $j = 1, \dots, k$. 再设 $s > 0$, $(s, p^m \prod_{i=1}^k (1 - \frac{1}{p^{m_i}})) = 1$, 定义函数

$$f(n) = [b_t, b_{t-1}, \dots, b_0]_p, \quad n \in [1, M],$$

$n = [a_h, \dots, a_0]_p$, 这里 $b_t, \dots, b_0$ 是 F_p 上多项式 $(a_h x^h + \dots + a_0)^s$ 模 $g(x)$ 的余式 $b_t x^t + \dots + b_0$ 的系数, 记为

$$\langle (a_h x^h + \dots + a_0)^s \rangle_{g(x)} = b_t x^t + \dots + b_0,$$

则 $f(n)$ 是一个陷门单向函数.

设 $\varphi(p, g(x)) = p^m \prod_{i=1}^k (1 - \frac{1}{p^{m_i}})$, 由于 $(s, \varphi(p, g(x))) = 1$, 存在整数 l 满足

$$sl \equiv 1 \pmod{\varphi(p, g(x))}, \quad 0 < l < \varphi(p, g(x)),$$

设 $m' = [c_q, \dots, c_0]_p$, $m' = f(n)$, 定义

$$F(m') = [d_e, \dots, d_0]_p,$$

这里 $d_e, \dots, d_0$ 为 F_p 上多项式 $\langle (c_q x^q + \dots + c_0) \rangle_{g(x)} = d_e x^e + \dots + d_0$ 的系数. 易证 $F(m') = f^{-1}(m')$.

对于RSA体制, 由于 $(s, (p-1)(q-1)) = 1$, 设 s 模 $(p-1)(q-1)$ 的次数为 h , 则由 $n^s \equiv l \pmod{m}$ 可得 $n \equiv n^{s^h} \equiv l^{s^{h-1}} \pmod{m}$,

因此, 只要对 l 连续施行 $h-1$ 次 s 方幂 $\pmod{m}$, 就可还原出 n , 这就使得RSA体制的保密性受到一定的限制.

最近, 作者^[23]给出代数整数环上一类单向陷门函数, 适当选择代数数域, 特别是选择复数域 $Q(i)$, 用某些给定的主理想为模, 可以建立公开密钥体制, 这样就把RCA体制推广到代数数域中去了. 和RCA体制相比较, 新的体制有如下特点:

①对理想数的分解, 其困难性不低于对整数 m 的分解. 一般来说, 还要困难一些.

②虽然在加密(或解密)时, 代数整数的幂模理想的运算比整数的幂模 m 的运算要复杂一些, 但对加密后的数 l 连续施行 s 方幂来还原明文 n 时, 就比RSA困难, 这也就增加了新体制的保密性.

我们证明了下面两个主要的定理.

设 $K = Q(\theta)$ 是一个 n 次代数数域, D 是 K 的代数整数环, 若 A 是 D 中的非零理想数, D/A 为其商环, 称为模 A 的剩余类环, 它的乘群记为 $R(A)$. 设 $N(A) = |D/A|$, $\varphi(A) = |R(A)|$, 熟知

$$\varphi(A) = N(A) \prod_{p|A} \left(1 - \frac{1}{N(p)}\right),$$

这里 P 过 A 的所有不同的素理想数因子.

如果对于 D 中两个代数整数 a, β , 有 $A | a - \beta$, 则记 $a \equiv \beta \pmod{A}$.

定理 1 设 $K = Q(i)$ 是复数域, D 是高斯整环, $m = q_1^{m_1} \cdots q_k^{m_k}$, $q_j \equiv 3 \pmod{4}$ ($j = 1, \dots, k$) 是 k 个不同的素数, $s > 0$, $(s, m^2 \prod_{j=1}^k (1 - \frac{1}{q_j^2})) = 1$, 则对任一 $a \in T = \{a + bi, 0 \leq a, b < m, a, b$ 中至少有一个与 $q_1 \cdots q_k$ 互素}, 定义

$$f(a) = a' + b'i = \beta,$$

其中 $0 \leq a', b' < m$, $\beta \equiv a^s \pmod{[m]}$, 则 $f(a)$ 是高斯整数环上的一类陷门单向函数.

可类似的给出高斯整数环上任意给定的理想为模以及某些二次代数整数环(如爱森斯坦环)的陷门单向函数, 这里不再赘述.

在一般代数数域 $K = Q(\theta)$ 上, 我们有下面的定理.

定理 2 设 $K = Q(\theta)$ 是一个 n 次代数数域, $\omega_1, \dots, \omega_n$ 是 D 的一组整底, Δ 为 K 的基数, $m = p_1 \cdots p_k$, $p_1, \dots, p_k$ 为不同的素数, 且 $p_j \nmid \Delta$, $j = 1, \dots, k$. 又设 $s > 0$, $(s, \varphi([m])) = 1$, $\varphi([m]) = m^n \prod_{j=1}^k (1 - \frac{1}{N(p_j)})$, 其中 $p_1, \dots, p_k$ 过 $[m]$ 的不同的素理想数因子, 则对任一 $a \in T_1 = \{a_1 \omega_1 + \dots + a_n \omega_n, 0 \leq a_j < m, j = 1, \dots, n\}$, 定义 $f(a) = \beta = b_1 \omega_1 + \dots + b_n \omega_n$, 其中 $0 \leq b_j < m, j = 1, \dots, n$, $\beta \equiv a^s \pmod{[m]}$, 则 $f(a)$ 是 D 上的一类陷门单向函数.

以上两个定理, 分解 $[m]$ 是困难的, 特别是定理 2 中的 $[m]$, 除了把 m 分解为 $p_1 \cdots p_k$, 还要进一步把 $p_1, \dots, p_k$ 分解为素理想数的乘积.

如何用这两个定理对明文进行加密呢? 设明文为 u , $u = a_h 10^h + \dots + a_1 10 + a_0$, $a_h \neq 0$,

$0 \leq a_j < 10, j = 0, 1, \dots, h$, 即 u 在 10 进制记数法中, 位数为 $h+1$.

①应用定理 1 对明文加密时, 如果 $0 < u < m$, $(u, m) = 1$ 时, 可直接令 $a = u$ 代入 $f(a)$ 加密. 如果 $u > m$ 时, 可将 u 划为二段, 将前半段和后半段, 分别设为 u_1 和 u_2 , 使 $0 < u_1 < m$, $0 < u_2 < m$, 且 u_1 和 u_2 中至少有一个与 m 互素, 则令 $a = u_1 + u_2 i$ 代入 $f(a)$ 加密.

例 $m = q_1 \cdot q_2, g_1 = 2411, g_2 = 4423, m = 10663853, u = 574321089$, 则令 $a = 57432 + 1089i$ 或 $a = 5743 + 21089i$ 等等均可.

②应用定理 2 对明文加密, 如果 $0 < u < m$ 时, 可直接令 $a = u$ 代入 $f(a)$ 加密. 如果 $u > m$ 时, 可将 u 划分为几段, 分别设为 $u_1, \dots, u_n$, 使 $0 < u_j < m, j = 1, \dots, n$, 则令 $a = u_1 \omega_1 + \dots + u_n \omega_n$ 代入 $f(a)$ 加密.

③在前面①、②部分的论述中, 当 $0 < u < m$ 时, 也可分段处理.

公开密钥体制的提出, 是数论在密码学中的重要应用, 同时, 也促进了数论学科本身的发展. 例如, 采用 RCA 体制, 首先需寻找一些大素数, 目前, 关于判定大数是否素数方面, 有许多重要的工作^[24]. 其次, 这方面需要寻找分解整数 m 的有效方法, 目前还没有找到.

参 考 文 献

- [1] Hardy, G. H., 一个数学家的自白, 数学译林, 3(1984).
- [2] Gamow, G., 从一到无穷大, 科学出版社, 1978.
- [3] Bremner, A., Morten, P.; The Integer Points on Three Related Elliptic Curves, 159(1982).
- [4] Knuth, The Art of Computer Programming (II), 1969.
- [5] Szabo, Tanaka, Residue Arithmetic and its Applications to computer technologic, 1967.
- [6] 万哲先, 代数和编码, 科学出版社, 1976.
- [7] 丁石孙, 线性移位寄存器序列, 上海科技出版社, 1980.
- [8] 柯召、魏万迪, 组合论 (上册), 科学出版社, 1980.
- [9] Byser, H. J., Combinatorial Mathematics, 1963.
- [10] Ronheim A., G., Cryptography: A primer, 1981.
- [11] 陶仁骥, 密码学与数学, 自然杂志, 7(1984).
- [12] 柯召、孙琦, 数论在数字信号处理中的应用, 3(1982).
- [13] McClellam, J. H., Rader, C. M., Number Theory in Digital Signal Processing, 1979.
- [14] 孙琦、郑德勋、沈仲琦, 快速数论变换, 科学出版社, 1980.
- [15] 华罗庚、王元, 数论在近似分析中的应用, 科学出版社, 1978.
- [16] 同 [5].
- [17] 孙琦、曹珍富, 关于方程 $\frac{1}{x_1} + \dots + \frac{1}{x_s} - \frac{1}{x_1 \dots x_s} = 1$ 及其应用, 科学通报, 2(1985).
- [18] 孙琦, 关于单位分数表 1 的表法个数, 2—3(1978).
- [19] 柯召、孙琦, 关于单位分数表 1 的问题, 1(1964).
- [20] Diffie, Hellman, New Directions in Cryptograph, IEEE Trans Inform. theory, 22(1976).
- [21] Rivest, R. L., Shamir, L., Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Commun. ACM, 20(1978).
- [22] 孙琦, 一类陷门单向函数 (待发表).
- [23] 孙琦, 代数整数环上的一类陷门单向函数 (待发表).
- [24] Dixon John D., Factorization and primality tests, Amer. Math. Monthly, 6(1984).