模 n 的剩余类加群(Z_n，+)及模 n 剩余类环(Z_n，+，·)的若干性质

杨树生

(河套大学数学与计算机科学系，内蒙古 巴彦淖尔市 015000)

[摘 要] 模 n 剩余类加群是有限循环群的代表，在群论中占有重要地位，本文具体地给出模 n 的剩余类加群的生成元及其个数、子群个数、自同构个数；还给出了模 n 剩余类环的可逆元及其个数、子环个数、零因子个数等问题的解决.

[关键词] 模 n 剩余类环、模 n 剩余类加群、Euler 函数

[中图分类号]0175.7　　[文献标识码]A　　[文章编号]

本文用到的符号及引理

$|a|$表示元素 a 的阶，$|G|$表示群 G 的阶，T(n)表示数 n 的正因数个数，$\Phi(n)$表示小于 n 且与 n 互素的正整数的个数，即 Euler 函数. (m,n)表示 m 与 n 的最大公因数，(Z_n，+)表示模 n 的剩余类加群，(Z_n，+，·)表示模 n 的剩余类环.

引理：循环群的子群是循环群. 引理证明见[2].

一、(Z_n，+)的若干性质

定理 1：(Z_n，+)中元素[m]是(Z_n，+)的生成元的充要条件为(m,n) = 1，且生成元个数为 $\Phi(n)$个

证明：若(m,n) = 1，则存在整数 s，t，使得 ms + nt = 1

于是[1] = [ms + nt] = [m][s] + [n][t] = [m][s] + [0][t] = [m][s] ∈ ([m])

因此(Z_n，+) = ([m])，[m]是(Z_n，+)的生成元.

反过来，若[m]是(Z_n，+)的生成元，则[1] ⊆ ([m])，也就是说，[1] = s[m]，而[n] = [0]所以[1] = [s][m] + [t][n]，从而(m,n) = 1，且(Z_n，+)的生成元的个数为 $\Phi(n)$个.

定理 2：(Z_n，+)有 T(n)个子群.

证明：只须证对 n 的每个正因数 k，(Z_n，+)有且只有一个 k 阶子群.

(Z_n，+)为 n 阶循环群，令 Z_n = ([m])，则$|[m]| = n$，又设 $k|n$ 并令 n = kq，则$|q[m]| = k$，从而(q[m])是(Z_n，+)的一个 k 阶子群，则由引理知 H 是循环群，设 H = (p[m])，则$|p[m]| = k$，但 p[m]的阶为$\frac{n}{(p,n)}$，从而$\frac{n}{(p,n)} = k$，n = k(p,n)，由上及 n = kq 得 q = (p,n)，$q|p$，于是 p[m] ∈ (q[m])，(p[m]) ⊆ (q[m])，但由于(q[m])与(p[m])的阶都为 k，故(q[m]) = (p[m])，即(Z_n，+)的 k 阶子群是唯一的.

由上知：剩余类加群(Z_n，+)的子群个数为 T(n)个.

定理 3：(Z_n，+)的自同构的个数为 $\Phi(n)$个.

证明：设 f 为(Z_n，+) = ([a])的任一自同构，并设 f([a]) = [b] = m[a]，f[s[a]] = [a]

则 f(sm[a]) = m[a]

因为 f 是自同构，所以[a] = s(m[a]) = s[b]

从而([a]) = ([b]) = (f([a]))

[收稿日期]2004 - 01 - 10

[作者简介]杨树生，(1963)，男，内蒙古赤峰人，河套大学数学与计算机科学系副教授。

即在同构映射下生成元的象仍为生成元.

反之,设[a],[b]是$(Z_n, +) = ([a])$的两个生成元,则易知

$g:([a])\to([a])$

$S[a]\to S[b]$

是([a])一个自同构.

因此,([a])的生成元完全决定了([a])的自同构,([a])有多少个生成元,它就有多少个自同构,而由定理1知$(Z_n, +)$有$\Phi(n)$个生成元,从而有$\Phi(n)$个自同构.

二、$(Z_n, +, \cdot)$的若干性质

定理4:$(Z_n, +, \cdot)$中元素[m]是$(Z_n, +, \cdot)$中可逆元的充要条件为$(m,n)=1$,且可逆元个数为$\Phi(n)$个.

证明:设[m]是$(Z_n, +, \cdot)$中的可逆元,则存在$[s]\in(Z_n, +, \cdot)$使$[m][s]=[1]$,即$[ms]=[1]$,$n|ms-1$,于是存在整数k使$ms-1=nk$,从而有$ms-nk=1$,则$(m,n)=1$.

反之,若$(m.n)=1$,则存在整数u,v使$mu+nv=1$,由此可得$[mu+nv]=[1]$,$[m][u]+[n][v]=[1]$,但$[n][v]=[0]$故$[m][u]=[1]$,即[m]是$(Z_n, +, \cdot)$的可逆元.从而$(Z_n, +, \cdot)$可逆元个数为$\Phi(n)$个.

定理5:$(Z_n, +, \cdot)$有T(n)个子环

证明:由模n的剩余类环$(Z_n, +, \cdot)$的子加群都是子环,而剩余类加群有且仅有T(n)个子加群,所以剩余类环$(Z_n, +, \cdot)$有T(n)个子环.

定理6:$(Z_n, +, \cdot)$有$n-T(n)-1$个零因子.

证明:只须证$(Z_n, +, \cdot)$的元[m]不是可逆元就是零因子,

若$[m]\neq[0]$不是可逆元,则由定理5知:$(m,n)=d>1$,令$m=dm_1$,$n=dn_1$,其中$1<n_1<n$,则$[n_1]\neq[0]$且$[m][n_1]=[mn_1]=[dn_1m_1]=[dm_1n_1]=[nm_1]=[n][m_1]=[0][m_1]=[0]$

即[m]是$(Z_n, +, \cdot)$的零因子.从而由定理5知$(Z_n, +, \cdot)$有$n-T(n)-1$个零因子.

[参考文献]

[1]:张禾瑞《近世代数基础》[M],北京,高等教育出版社,1978

[2]:吴品三《近世代数》[M],北京,高等教育出版社1987

[3]:刘绍学《近世代数基础》[M],北京,高等教育出版社2000

[4]:杨子胥《近世代数》[M],北京,高等教育出版社2000

Some Characteristics of Remainder Plus Group(Zn, +) and Remainder Ring(Zn, +,.) of Mould N

Yang Shusheng

(Department of Mathematics and Computer Science, Hetao University, Bayannur City, P. C: 015000)

Abstract: The remainder plus group of Mould N represents the limited circulation group and plays a significant role in the theory of groups. This article points out specifically the number of resultant elements, sub – groups and self – identical structure of the remainder plus group of Mould N. It also puts forward the number of the reversible elements, sub – rings and zero factors as well as solutions to these problems.

Key words: Remainder ring of Mould N, remainder plus group of Mould N, Euler function