

单位群阶为 $2pqr$ 的模 n 剩余类环

张影, 曹炜*

(宁波大学 理学院, 浙江 宁波 315211)

摘要: 应用中国剩余定理与模 n 剩余类环 $\mathbb{Z}_n$ 及其单位群 $U(\mathbb{Z}_n)$ 的分解定理, 讨论并确定了当群 $U(\mathbb{Z}_n)$ 的阶为 $2pqr$ 的部分情形时, $U(\mathbb{Z}_n)$ 的群结构与 n 的取值, 其中 p, q, r 为素数(不必完全不同).

关键词: 剩余类环; 单位群; 中国剩余定理; 欧拉函数

中图分类号: O156.1

文献标志码: A

文章编号: 1001-5132 (2014) 03-0059-04

一些特殊环的单位群历来是代数及数论的重要研究对象, 特别是各类矩阵环、群环、模 n 剩余类环 $\mathbb{Z}_n$ 及高斯整数环等, 文献中有大量关于它们单位群的研究结论^[1]. 设整数 $n = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$, 其中 $q_i (1 \leq i \leq s)$ 为奇素数, 熟知剩余类环 $\mathbb{Z}_n$ 的单位群 $U(\mathbb{Z}_n)$ 有如下的值和分解:

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{2^\alpha}) \oplus U(\mathbb{Z}_{q_1^{\alpha_1}}) \oplus \cdots \oplus U(\mathbb{Z}_{q_s^{\alpha_s}}),$$

其中:

$$U(\mathbb{Z}_{2^\alpha}) \cong \mathbb{Z}_{2^{\alpha-1}},$$

$$\alpha = 1, 2, U(\mathbb{Z}_{2^\alpha}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{\alpha-2}},$$

$$\alpha \geq 3, U(\mathbb{Z}_{q_i^{\alpha_i}}) \cong \mathbb{Z}_{q_i^{\alpha_i-1}(q_i-1)} (1 \leq i \leq s).$$

一个自然的反问题是: 若已知 $U(\mathbb{Z}_n)$ 的结构, 如何确定 $\mathbb{Z}_n$ 和 n 的取值? 文献[2-3]证明了单位群 $U(\mathbb{Z}_n)$ 的非单位元的阶均为 2, 当且仅当 $n=3, 4, 6, 8, 12, 24$, 及非单位元的阶均为奇素数的单位群不存在. 屈寅春等^[4]研究了当模 n 剩余类环 $\mathbb{Z}_n$ 的单位群 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q$ 时, 其中 p, q 为素数, 且 $q > p \geq 3$, 则有:

(1) 若 $2pq+1$ 是素数, 则

$$n = 2pq + 1, 4pq + 2.$$

(2) 若 $2p+1=q$, 则

$$n = (2p+1)^2, 2(2p+1)^2.$$

(3) 若 $2pq+1$ 不是素数, 且 $2p+1 \neq q$, 则满足条件的 n 不存在.

笔者将进一步研究当模 n 剩余类环的单位群阶为 $2pqr$ (其中 p, q, r 为不必完全不同的素数)时, n 的取值和 $U(\mathbb{Z}_n)$ 的结构.

1 预备知识

本文主要结论的证明将用到以下的定义和引理^[5-8].

定义 1 设 $\mathbb{Z}_n$ 是模 n 剩余类环, $[a] \in \mathbb{Z}_n$, 若存在 $[b] \in \mathbb{Z}_n$ 满足 $[a][b] = [1]$, 其中 $[1]$ 为 $\mathbb{Z}_n$ 的单位元, 则称 $[a]$ 为 $\mathbb{Z}_n$ 的一个单位, $\mathbb{Z}_n$ 中全体单位构成的群称为单位群, 记作 $U(\mathbb{Z}_n)$.

定义 2 欧拉函数 $\varphi(n)$ 是一个定义在正整数集上的函数, $\varphi(n)$ 的值等于序列 $1, 2, \dots, n-1$ 中与 n 互素的数的个数. 记

$$A_n = \{[a] | 1 \leq a \leq n-1, (a, n) = 1\},$$

$\varphi(n)$ 为 n 的欧拉函数, 则 $\mathbb{Z}_n$ 的单位群 $U(\mathbb{Z}_n) = \{[a] | a \in A_n\}$, 且有 $|U(\mathbb{Z}_n)| = |A_n| = \varphi(n)$ 成立.

引理 1 设 n 的标准分解为 $n = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, 则 $\varphi(n) = (q_1^{\alpha_1-1}) \cdots (q_s^{\alpha_s-1})(q_1-1) \cdots (q_s-1)$.

为分析讨论方便, 将 $\varphi(n)$ 公式作一推广:

$$\varphi(n) = (q_1^{\alpha_1-1})^{\beta_1} \cdots (q_s^{\alpha_s-1})^{\beta_s} (q_1-1)^{\beta_1} \cdots (q_s-1)^{\beta_s},$$

其中: $\beta_i = 0$, 若 $\alpha_i = 0$; $\beta_i = 1$, 若 $\alpha_i \geq 1$.

引理 2(中国剩余定理) 设 $n = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, 其中 $q_i (1 \leq i \leq s)$ 为不同的素数, 则

$$\mathbb{Z}_n \cong \mathbb{Z}_{q_1^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{q_s^{\alpha_s}}.$$

引理 3 设 $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$, 其中 $q_i (1 \leq i \leq s)$ 为不同的素数, 则

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{q_1^{\alpha_1}}) \oplus \cdots \oplus U(\mathbb{Z}_{q_s^{\alpha_s}}).$$

注 引理 2 中的同构是环同构, 而引理 3 中的同构是(乘法)群同构.

2 主要结论及其证明

定理 1 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_p$, 其中 p 为素数, 则有:

- (1) $p=2$ 时, 满足条件的 n 不存在.
- (2) $p=3$ 时, 当且仅当 $n=56, 72, 84$.
- (3) $p \geq 5$, 且 $2p+1$ 为素数时, 当且仅当 $n=16p+8, 24p+12$.

证明 设 $n = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, 其中 $q_i (1 \leq i \leq s)$ 为不同的素数.

若 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_p$, 则 $\varphi(n) = 8p$, 即

$$|U(\mathbb{Z}_n)| = \varphi(n) = q_1^{\alpha_1-1} \cdots q_s^{\alpha_s-1} (q_1-1) \cdots (q_s-1) = 8p. \quad (1)$$

下面讨论 n 的素因子. 设 q_i 是 n 的素因子, 由 (1) 式可知 q_i-1 必能整除 $8p$, 因为 p 是素数, 所以 q_i-1 只可能是 $1, 2, 4, 8, p, 2p, 4p, 8p$. 因而 q_i 有可能为 $2, 3, 5, 2p+1, 4p+1, 8p+1$.

情形 1 当 $p=2$ 时, $\varphi(n)=16$. 此时 $2p+1=5, 4p+1=9$ 不是素数, $8p+1=17$. n 的素因子 q 只能取 $2, 3, 5, 17$. 我们断言 3 和 17 不可能同时是 n 的素因子, 否则 $32 | \varphi(n)$. 同理, 5 和 17 不可能同时是 n 的素因子. 因此 n 的素因子分解式只可能是 $n = 2^{\alpha_1} 17^{\alpha_2}$ 或 $n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3}$, 其中 $\alpha_i \in N$ (N 为非负整数集, 下同).

(1) 当 $n = 2^{\alpha_1} 17^{\alpha_2}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} (17^{\alpha_2-1})^{\beta_2} (2-1)^{\beta_1} (17-1)^{\beta_2} = 16,$$

所以 α_2 只能取 1 . 对 α_i 讨论可得, $\varphi(n)=16$, 当且仅当 $(\alpha_1, \alpha_2) = (0, 1), (1, 1)$, 即 $n=17, 34$.

(2) 当 $n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} (3^{\alpha_2-1})^{\beta_2} (5^{\alpha_3-1})^{\beta_3}.$$

$$(2-1)^{\beta_1} (3-1)^{\beta_2} (5-1)^{\beta_3} = 16,$$

所以 α_2 和 α_3 只能取 0 或 1 . 对 α_i 分类讨论可得, $\varphi(n)=16$, 当且仅当

$$(\alpha_1, \alpha_2, \alpha_3) = (5, 0, 0), (3, 0, 1), (4, 1, 0), (2, 1, 1),$$

即

$$n = 32, 40, 48, 60.$$

由单位群的分解定理(引理 3)得:

$$U(\mathbb{Z}_{17}) \cong U(\mathbb{Z}_{34}) \cong \mathbb{Z}_{16}, \quad U(\mathbb{Z}_{32}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_8,$$

$$U(\mathbb{Z}_{40}) \cong U(\mathbb{Z}_{48}) \cong U(\mathbb{Z}_{60}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4,$$

即

不存在自然数 n 满足:

$$U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2.$$

情形 2 当 $p=3$ 时, $\varphi(n)=8p=24$. 此时 $2p+1=7, 4p+1=13, 8p+1=25$ 不是素数, 所以 n 的素因子 q_i 只能取 $2, 3, 5, 7, 13$. 我们断言 5 和 13 不可能同时是 n 的素因子. 否则 $48 | \varphi(n)$. 同理可知 7 和 13 不可能同时是 n 的素因子. n 的素因子分解式只可能是 $n = 2^{\alpha_1} 3^{\alpha_2} 13^{\alpha_3}$ 或 $n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} 7^{\alpha_4}$, 其中 $\alpha_i \in N$.

(1) 当 $n = 2^{\alpha_1} 3^{\alpha_2} 13^{\alpha_3}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} (3^{\alpha_2-1})^{\beta_2} (13^{\alpha_3-1})^{\beta_3}.$$

$$(2-1)^{\beta_1} (3-1)^{\beta_2} (13-1)^{\beta_3} = 24,$$

所以 α_3 只能取 0 或 1 . 对 α_i 讨论可得, $\varphi(n)=24$, 当且仅当

$$(\alpha_1, \alpha_2, \alpha_3) = (0, 1, 1), (1, 1, 1), (2, 0, 1), (3, 2, 0),$$

即

$$n = 39, 52, 72, 78.$$

(2) 当 $n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} 7^{\alpha_4}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} (3^{\alpha_2-1})^{\beta_2} (5^{\alpha_3-1})^{\beta_3} (7^{\alpha_4-1})^{\beta_4}.$$

$$(2-1)^{\beta_1} (3-1)^{\beta_2} (13-1)^{\beta_3} (7-1)^{\beta_4} = 24.$$

所以 α_3 和 α_4 只能取 0 或 1 . 对 α_i 分类讨论可得, $\varphi(n)=24$, 当且仅当

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (0, 0, 1, 1), (1, 0, 1, 1), (2, 1, 0, 1),$$

$$(3, 0, 0, 1), (1, 2, 1, 0), (0, 2, 1, 0), (3, 2, 0, 0),$$

即

$$n = 35, 45, 56, 70, 72, 84, 90.$$

由单位群的分解定理(引理 3)可得:

$$U(\mathbb{Z}_{35}) \cong U(\mathbb{Z}_{39}) \cong U(\mathbb{Z}_{45}) \cong U(\mathbb{Z}_{52}) \cong U(\mathbb{Z}_{70}) \cong$$

$$U(\mathbb{Z}_{78}) \cong U(\mathbb{Z}_{90}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4,$$

和

$$U(\mathbb{Z}_{56}) \cong U(\mathbb{Z}_{72}) \cong U(\mathbb{Z}_{84}) \cong$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3,$$

所以 $p=3$ 时 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$, 当且仅当 $n=56, 72, 84$.

情形 3 当 $p \geq 5$ 时, $\varphi(n)=8p$. q_i-1 可能是

$1, 2, 4, 8, p, 2p, 4p, 8p$. n 的素因子 q_i 有可能为 $2, 3, 5, 2p+1, 4p+1, 8p+1$. 我们断言 $2p+1$ 和 $8p+1$ 不可能同时是 n 的素因子. 否则, $16p^2 \mid \varphi(n)$. 同理, $4p+1$ 和 $8p+1$, 3 和 $8p+1$, 5 和 $8p+1$, $2p+1$ 和 $4p+1$, 5 和 $4p+1$ 不可能同时是 n 的素因子, 所以 n 的素因子分解式只可能是 $n = 2^{\alpha_1} (8p+1)^{\alpha_2}$, 或 $n = 2^{\alpha_1} 3^{\alpha_2} (4p+1)^{\alpha_3}$, 或 $n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} (2p+1)^{\alpha_4}$, 其中 $\alpha_i \in \mathbb{N}$.

(1) 当 $n = 2^{\alpha_1} (8p+1)^{\alpha_2}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} ((8p+1)^{\alpha_2-1})^{\beta_2}.$$

$$(2-1)^{\beta_1} (8p+1-1)^{\beta_2} = 8p,$$

所以 α_2 只能取 1. 对 α_1 讨论可得, $\varphi(n) = 8p$, 当且仅当 $(\alpha_1, \alpha_2) = (0, 1), (1, 1)$, 即

$$n = 8p+1, 16p+2.$$

(2) 当 $n = 2^{\alpha_1} 3^{\alpha_2} (4p+1)^{\alpha_3}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} (3^{\alpha_2-1})^{\beta_2} ((4p+1)^{\alpha_3-1})^{\beta_3} (2-1)^{\beta_1}.$$

$$(3-1)^{\beta_2} (4p+1-1)^{\beta_3} = 8p,$$

所以 α_2 只能取 1. 对 α_1 讨论可得, $\varphi(n) = 8p$, 当且仅当 $(\alpha_1, \alpha_2, \alpha_3) = (0, 1, 1), (1, 1, 1), (2, 0, 1)$. 即

$$n = 12p+3, 24p+6, 16p+4.$$

(3) 当 $n = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} (2p+1)^{\alpha_4}$ 时,

$$\varphi(n) = (2^{\alpha_1-1})^{\beta_1} (3^{\alpha_2-1})^{\beta_2} (5^{\alpha_3-1})^{\beta_3} ((2p+1)^{\alpha_4-1})^{\beta_4}.$$

$$(2-1)^{\beta_1} (3-1)^{\beta_2} (5-1)^{\beta_3} (2p+1-1)^{\beta_4} = 8p,$$

所以 α_4 只能取 1. 对 α_i 分类讨论可得, $\varphi(n) = 8p$, 当且仅当

$$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) =$$

$$(0, 0, 1, 1), (1, 0, 1, 1), (2, 1, 0, 1), (3, 0, 0, 1),$$

即

$$n = 10p+5, 20p+10, 24p+12, 16p+8.$$

由单位群的分解定理(引理 3)得:

当 $8p+1$ 为素数时, 有:

$$U(\mathbb{Z}_{8p+1}) \cong U(\mathbb{Z}_{16p+2}) \cong \mathbb{Z}_8 \oplus \mathbb{Z}_p [0, 1].$$

当 $4p+1$ 和 $2p+1$ 均为素数时, 有:

$$U(\mathbb{Z}_{10p+5}) \cong U(\mathbb{Z}_{12p+3}) \cong U(\mathbb{Z}_{16p+4}) \cong$$

$$U(\mathbb{Z}_{20p+10}) \cong U(\mathbb{Z}_{24p+6}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_p.$$

当 $2p+1$ 为素数时, 有:

$$U(\mathbb{Z}_{16p+8}) \cong U(\mathbb{Z}_{24p+12}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_p,$$

所以对于 $p \geq 5$, 当 $2p+1$ 为素数时有:

$$U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_p,$$

当且仅当 $n = 16p+8, 24p+12$.

证毕.

应用类似的方法, 可以讨论其余的情形. 我们有以下的结论.

定理 2 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$, 其中 p 为奇素数, 则

(1) $p=3$ 时, 当且仅当 $n=63, 126$.

(2) $p>3$ 时, 满足条件的 n 不存在.

定理 3 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{p^2}$, 其中 p 为奇素数, 则有:

(1) $p=3$ 时, 当且仅当 $n=57, 76, 108, 114$.

(2) $p>3$, 且 $2p^2+1$ 为素数时, 当且仅当 $n=6p^2+3, 12p^2+6, 8p^2+4$.

(3) $p>3$, 且 $2p^2+1$ 不是素数, 则满足条件的 n 不存在.

定理 4 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{p^2}$, 其中 p 为奇素数, 则有:

(1) $p=3$ 时, 当且仅当 $n=37, 74$.

(2) $p>3$, 且 $4p^2+1$ 为素数时, 当且仅当 $n=4p^2+1, 8p^2+2$.

(3) $p>3$, 且 $4p^2+1$ 不是素数, 则满足条件的 n 不存在.

定理 5 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_4 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q$, 其中 p, q 为奇素数且 $q>p \geq 3$, 则有:

(1) 若 $4pq+1$ 为素数, 则

$$n = 4pq+1, 8pq+2.$$

(2) 若 $4p+1=q$, 则

$$n = (4p+1)^2, 2(4p+1)^2.$$

(3) 若 $4pq+1$ 不是素数, 且 $4p+1 \neq q$, 则满足条件的 n 不存在.

定理 6 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q$, 其中 p, q 为奇素数, 且 $q>p \geq 3$, 则有:

(1) 若 $2pq+1$ 为素数, 则

$$n = 6pq+3, 8pq+4, 12pq+6.$$

(2) 若 $2p+1, 2q+1$ 均为素数, 则

$$n = (2p+1)(2q+1), 2(2p+1)(2q+1).$$

(3) 若 $2p+1=q$, 则

$$n = 3(2p+1)^2, 4(2p+1)^2, 6(2p+1)^2.$$

(4) 若 $2pq+1$ 不是素数, 且 $2p+1 \neq q$, 且 $2p+1, 2q+1$ 有 1 个不是素数, 那么满足条件的 n 不存在.

定理 7 设 $U(\mathbb{Z}_n) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \mathbb{Z}_r$, 其中 p, q, r 为奇素数, 且 $r>q>p \geq 3$, 则

- (1) 若 $2pqr+1$ 为素数, 则
 $n = 2pqr+1, 2(2pqr+1)$.
- (2) 若 $2pq+1=r$, 则
 $n = (2pq+1)^2, 2(2pq+1)^2$.
- (3) 若 $2pr+1=q$, 则
 $n = (2pr+1)^2, 2(2pr+1)^2$.
- (4) 若 $2pqr+1$ 不是素数, 且 $2pq+1 \neq r$, $2pr+1 \neq q$, 则满足条件的 n 不存在.
- 参考文献:**
- [1] Ireland K, Rosen M. A classical introduction to modern number theory[M]. New York: Springer-Verlag, 1990: 28-49.
- [2] 梁华. 单位群 $U(\mathbb{Z}_n)$ 里非单位元的阶都是 2 的剩余类环[J]. 喀什师范学院学报, 2009, 30(6):13-14.
- [3] 居腾霞, 王立周. 模 n 的剩余类环的单位群 $U(\mathbb{Z}_n)$ [J]. 南通大学学报: 自然科学版, 2011, 10(4):83-87.
- [4] 屈寅春, 李立斌. 单位群的阶为 $2pq$ 的模 n 的剩余类环[J]. 湖北大学学报: 自然科学版, 2011, 33(1):1-6.
- [5] 张禾瑞. 近世代数基础[M]. 北京: 高等教育出版社, 1978:80-124.
- [6] 柯召, 孙琦. 数论讲义(上)[M]. 北京: 高等教育出版社, 2003:27-60.
- [7] Kenneth H R. 初等数论及其应用[M]. 北京: 机械工业出版社, 2007:174-182.
- [8] Joseph J R. Advanced modern algebra[M]. 北京: 机械工业出版社, 2007:176-189.

Residue Class Ring of Integers Modulo n with Unit Group of Order $2pqr$

ZHANG Ying, CAO Wei*

(Faculty of Science, Ningbo University, Ningbo 315211, China)

Abstract: Using the Chinese remainder theorem and the decomposition theorem for the structures of the residue class ring mod n and its unit group, the precise values of n and the group structures of $U(\mathbb{Z}_n)$ are discussed and determined for some cases in which the order of $U(\mathbb{Z}_n)$ is equal to $2pqr$, where p , q and r are prime numbers (not necessarily distinct).

Key words: residue class ring; unit group; Chinese remainder theorem; Euler's totient function

(责任编辑 史小丽)