

DOI:10.11830/ISSN.1000-5013.202103002



# 奇数的拆分循环及应用

吴金钗

(华侨大学 数学科学学院, 福建 泉州 362021)

**摘要:** 因 Mersenne 数( $M_p$ )和 Fermat 数( $F_n$ )都是二进制形式的数,故采用二进制数研究  $M_p, F_n$  的性质,导出奇数的拆分循环概念和相关理论.结果表明:这套理论可用于分析大数的性质及分解,并具有一定的普遍性和通用性.

**关键词:** Mersenne 数; Fermat 数; 奇数和式拆分与差式拆分; 素数的拆分循环

**中图分类号:** O 156.1 **文献标志码:** A **文章编号:** 1000-5013(2021)05-0701-08

## Odd Number Splitting Cycle and Its Application

WU Jincai

(School of Mathematical Sciences, Huaqiao University, Quanzhou 362021, China)

**Abstract:** Because both Mersenne numbers ( $M_p$ ) and Fermat numbers ( $F_n$ ) are numbers in binary form, binary numbers were used to study the properties of  $M_p, F_n$ . The concept of odd number splitting cycles and related theories are derived. The results show that these theories can be used to analyze the properties of large numbers and their decomposition, and possess a certain universality and versatility.

**Keywords:** Mersenne numbers; Fermat numbers; odd number sum splitting and difference splitting; prime number splitting cycle

Mersenne 数  $M_p = 2^p - 1$  是以 2 为底的幂再减 1 的数<sup>[1-4]</sup>, Fermat 数  $F_n = 2^{2^n} + 1$  是以 2 为底的幂再加 1 的数<sup>[4-9]</sup>. 在 Mersenne 数的分解方面, Cambraia<sup>[10]</sup> 给出了方程  $M_m + M_n = 2p^a$  的整数解  $(m, n, a)$ , 其中,  $m, n \geq 2, p$  是一个质数,  $a$  是一个正整数. 目前, 国内外学者对于 Fermat 数分解算法研究的不多, 国外有专门的网站介绍分解 Fermat 数的进展<sup>[10-12]</sup>. Wang<sup>[13]</sup> 提出分解 Fermat 数的新方法, 理论上可分解  $F_n (n > 100\ 001)$  的任何 Fermat 数. 王钰<sup>[14]</sup> 对 Wang<sup>[13]</sup> 的方法进行优化, 运用 Maple 数学软件解析 Fermat 数小因数, 优化后的算法提高了计算效率. 然而, Wang<sup>[13]</sup> 利用 GMP 大数库运算在 32 位系统中只能计算到  $F_{22}$ , 王钰<sup>[14]</sup> 利用 Maple 在 64 位系统中也只能计算到  $F_{29}$ . 因此, 研究更通用、更高效的大数算法是很有必要的. 基于此, 本文提出奇数的拆分循环及其应用.

### 1 奇数的和式拆分循环

#### 1.1 奇数的和式拆分

设  $p = 2a + 1 = 2^n + \delta_{n-1}2^{n-1} + \delta_{n-2}2^{n-2} + \cdots + \delta_12 + 1$ , 其中,  $\delta_i = 1$  或  $0, i = 1, 2, \cdots, n-1$ . 命奇数集  $\{1, 3, 5, \cdots, a^*\}$  为  $A, a^* = \begin{cases} a, & a \text{ 为奇数,} \\ a-1, & a \text{ 为偶数.} \end{cases}$  当  $a$  为奇数时,  $A$  有  $(a+1)/2$  个元素; 当  $a$  为偶数时,  $A$  有

收稿日期: 2021-03-02

通信作者: 吴金钗(1938-), 男, 副教授, 主要从事数论、偏微分方程的研究. E-mail: fruitful@xmu.edu.cn.

$a/2$  个元素. 因此, 对  $\forall \alpha \in A, \exists \beta \in A$  及数  $l(1 \leq l \leq n)$ , 使得  $p = \alpha + 2^l \beta$ , 其中,  $p$  为一个和式拆分,  $\alpha$  为拆分的起点,  $\beta$  为拆分的接点,  $l$  为拆分的指数.

由于  $A$  是有限集合, 所以  $\forall \alpha_0 \in A, \exists \alpha_i \in A$ , 不妨设  $i = 1, 2, \dots, k$  及数  $l_1, l_2, \dots, l_k$ , 使得  $p - \alpha_{i-1} = 2^{l_i} \alpha_i, \alpha_0 = \alpha_k$ , 拆分序列为

$$p - \alpha_0 = 2^{l_1} \alpha_1, \quad p - \alpha_1 = 2^{l_2} \alpha_2, \quad \dots, \quad p - \alpha_{k-1} = 2^{l_k} \alpha_k = 2^{l_k} \alpha_0. \tag{1}$$

式(1)中: 拆分序列是一个起点为  $\alpha_0$  的和式拆分循环;  $\alpha_0, \alpha_1, \dots, \alpha_{k-1}$  为循环的节点,  $m = \sum_{i=1}^k l_i$  为拆分循环的指数和.

如果式(1)中的节点和指数用字母表示, 则节点循环记为  $\dot{\alpha}_0 \alpha_1 \dots \dot{\alpha}_k$ , 指数循环记为  $\dot{l}_1 l_2 \dots \dot{l}_k$ . 如果节点和指数用具体的数表示, 则节点循环记为  $\alpha_0 - \alpha_1 - \dots - \alpha_k$ , 指数循环记为  $l_1 - l_2 - \dots - l_k$ . 称节点个数为奇数的循环为奇循环, 节点个数为偶数的循环为偶循环. 此外, 称起点为 1 的循环为基循环.

如果奇数  $p$  有两个拆分循环, 且两个循环有一个相同的节点, 则这两个循环的节点必完全相同, 即这两个循环实质是同一个拆分循环, 只是它们的起点不同. 如果  $p$  有两个拆分循环 (I), (II), 则仅当拆分循环 (I) 的节点与拆分循环 (II) 的节点全不相同时, 才称拆分循环 (I), 拆分循环 (II) 是  $p$  的两个不同的拆分循环. 当  $p$  为素数时, 则  $p$  与拆分循环的各节点的最大公因数  $(p, \alpha_0, \alpha_1, \dots, \alpha_{k-1}) = 1$ ; 当  $p$  是合数时, 如  $p = p_1 \cdot p_2$  ( $p_1, p_2$  为素数), 则  $p$  与拆分循环的各节点的最大公因数  $(p, \alpha_0, \alpha_1, \dots, \alpha_{k-1}) = 1$  或  $p_1$  或  $p_2$ .

1.2 拆分循环结果

因为  $p - \alpha_0 = 2^{l_1} \alpha_1 = 2^{l_1} (p - 2^{l_2} \alpha_2) = 2^{l_1} p - 2^{l_1+l_2} \alpha_2 = 2^{l_1} p - 2^{l_1+l_2} (p - 2^{l_3} \alpha_3) = (2^{l_1} - 2^{l_1+l_2}) p + 2^{l_1+l_2+l_3} \alpha_3$ , 所以当  $2j < k$  时, 有

$$p \cdot (2^{l_1+l_2+\dots+l_{2j-1}} - 2^{l_1+l_2+\dots+l_{2j-2}} + \dots + 2^{l_1} - 1) = 2^{l_1+l_2+\dots+l_{2j}} \alpha_{2j} - \alpha_0; \tag{2}$$

当  $2j - 1 < k$  时, 有

$$p \cdot (2^{l_1+l_2+\dots+l_{2j-2}} - 2^{l_1+l_2+\dots+l_{2j-3}} + \dots - 2^{l_1} + 1) = 2^{l_1+l_2+\dots+l_{2j-1}} \alpha_{2j-1} + \alpha_0. \tag{3}$$

当  $k = 2s$  时,  $\alpha_{2s} = \alpha_0$ , 由拆分序列(1), 有

$$p \cdot (2^{l_1+l_2+\dots+l_{2s-1}} - 2^{l_1+l_2+\dots+l_{2s-2}} + \dots + 2^{l_1} - 1) = \alpha_0 (2^{l_1+l_2+\dots+l_{2s}} - 1) = \alpha_0 (2^m - 1). \tag{4}$$

式(4)中:  $m = \sum_{i=1}^{2s} l_i$ .

当  $k = 2s - 1$  时,  $\alpha_{2s-1} = \alpha_0$ , 由拆分序列(1), 有

$$p \cdot (2^{l_1+l_2+\dots+l_{2s-2}} - 2^{l_1+l_2+\dots+l_{2s-3}} + \dots - 2^{l_1} + 1) = \alpha_0 (2^{l_1+l_2+\dots+l_{2s-1}} + 1) = \alpha_0 (2^m + 1), \tag{5}$$

式(5)中:  $m = \sum_{i=1}^{2s-1} l_i$ .

综上所述, 当  $p$  的拆分循环为偶循环时,  $p | 2^m - 1$ ; 当  $p$  的拆分循环为奇循环时,  $p | 2^m + 1$ .

1.3 拆分指数和

因为  $p$  的拆分个数与奇数集  $A$  的个数  $|A|$  相同, 所以  $p$  的拆分个数为  $|A| = \begin{cases} (a+1)/2, a \text{ 为奇数}, \\ a/2, a \text{ 为偶数}. \end{cases}$  设  $p$  的和式拆分指数和为  $L$ ,  $p$  的和式拆分的指数为  $l$  的个数为  $N_l (l = 1, 2, \dots, n)$ , 则

$$L = nN_n + (n-1)N_{n-1} + \dots + 2N_2 + 1 \cdot N_1.$$

**定理 1** 设  $p = 2a + 1 = 2^n + \delta_{n-1} 2^{n-1} + \delta_{n-2} 2^{n-2} + \dots + \delta_n 2^2 + \delta_1 2 + 1, \delta_i$  取 1 或 0,  $i = 1, 2, \dots, n-1$ , 则  $p$  的全体和式拆分的指数和为  $a$ , 即  $L = nN_n + (n-1)N_{n-1} + \dots + 2N_2 + N_1 = a$ . 因此,  $p$  是素数或合数,  $a$  是奇数或偶数, 此结论均成立.

证明: 将  $p$  改写为

$$p = 2a + 1 = 2^l (2^{n-l} + \delta_{n-1} 2^{n-1-l} + \dots + \delta_{l+1} 2 + \delta_l 2 - 1) + [(1 - \delta_l) 2^l + \delta_{l-1} 2^{l-1} + \dots + \delta_1 2 + 1],$$

则右端第一项圆括号中的数和第二项的数都是奇数, 所以和式拆分指数  $\geq l$  的拆分节点为奇数, 即 1, 3,

$$5, \cdots, 2^{n-l} + \delta_{n-1} 2^{n-1-l} + \cdots + \delta_{l+1} 2 + \delta_l 2 - 1.$$

和式拆分指数 $\geq 1$ 的拆分个数为

$$N_n + N_{n-1} + \cdots + N_l = [(2^{n-l} + \delta_{n-1} 2^{n-1-l} + \cdots + \delta_{l+1} 2 - \delta_l 2 - 1) + 1] \div 2 = 2^{n-1-l} + \delta_{n-1} 2^{n-2-l} + \cdots + \delta_{l+2} 2 + \delta_{l+1} + \delta_l,$$

因此，

$$\begin{aligned} N_n + N_{n-1} + \cdots + N_1 &= 2^{n-2} + \delta_{n-1} 2^{n-3} + \cdots + \delta_3 2 + \delta_2 + \delta_1, \\ N_n + N_{n-1} + \cdots + N_2 &= 2^{n-3} + \delta_{n-1} 2^{n-4} + \cdots + \delta_4 2 + \delta_3 + \delta_2, \\ &\vdots \\ N_n + N_{n-1} + N_{n-2} &= 2 + \delta_{n-1} + \delta_{n-2}, \\ N_n + N_{n-1} &= 1 + \delta_{n-1}, \\ N_n &= 1, \\ L = nN_n + (n-1)N_{n-1} + \cdots + 2N_2 + 1N &= 2^{n-1} + \delta_{n-1} 2^{n-2} + \cdots + \delta_1 2 + 1 = a. \end{aligned}$$

1.4 超半和式拆分及所有超半拆分的指数和

设  $p = 2a + 1, \forall$  奇数  $\alpha, a < \alpha < p, \exists$  奇数  $\beta < a$  及数  $l \geq 1$ , 使得  $p = \alpha + 2^l \beta$ , 由于  $\alpha > \frac{p}{2}$ , 所以称这种拆分为超半和式拆分.  $\alpha$  为拆分的起点,  $\beta$  为接点,  $l$  为拆分的指数. 因为  $1, 3, 5, \cdots, p-2$  的奇数有  $a$  个, 和式拆分有  $|A|$  个, 所以超半拆分有  $a - |A| = \begin{cases} (a-1)/2, a \text{ 为奇数}, \\ a/2, a \text{ 为偶数}. \end{cases}$

设  $p = \alpha + 2^l \beta$  是一个和式拆分, 则  $\alpha, \beta \leq a$ , 且  $2^l \beta > a$ . 若  $1 < l \leq n$ , 则  $p = (\alpha + 2^{l-1} \beta) + 2^{l-1} \beta, p = (\alpha + 2^{l-1} \beta + 2^{l-2} \beta) + 2^{l-2} \beta, \cdots, p = (\alpha + 2^{l-1} \beta + 2^{l-2} \beta + \cdots + 2\beta) + 2\beta$ , 这是  $l-1$  个超半拆分, 其指数和为  $l(l-1)/2$ . 设全体超半拆分指数和为  $L_1$ , 则

$$L_1 = \frac{n \cdot (n-1)}{2} N_n + \frac{(n-1) \cdot (n-2)}{2} N_{n-1} + \cdots + \frac{3 \cdot 2}{2} N_3 + \frac{2 \cdot 1}{2} N_2.$$

因为  $N_n + N_{n-1} + \cdots + N_k = 2^{n-k-1} + \delta_{n-1} 2^{n-k-2} + \cdots + \delta_{k+2} 2 + \delta_{k+1} + \delta_k, N_n + N_{n-1} + \cdots + N_{k+1} = 2^{n-k-2} + \delta_{n-1} 2^{n-k-3} + \cdots + \delta_{k+3} 2 + \delta_{k+2} + \delta_{k+1}$ , 所以  $N_k = 2^{n-k-2} + \delta_{n-1} 2^{n-k-3} + \cdots + \delta_{k+3} 2 + \delta_{k+2} + \delta_k (k = 1, 2, \cdots, n-2)$ , 而  $N_n = 1, N_{n-1} = \delta_{n-1}, N_{n-2} = 1 + \delta_{n-2}$ , 有

$$\begin{aligned} L_1 &= \frac{n \cdot (n-1)}{2} + \frac{(n-1) \cdot (n-2)}{2} \delta_{n-1} + \frac{(n-2) \cdot (n-3)}{2} (1 + \delta_{n-2}) + \cdots + \\ &\quad \frac{k \cdot (k-1)}{2} (2^{n-k-2} + \delta_{n-1} 2^{n-k-3} + \cdots + \delta_{k+3} 2 + \delta_{k+2} + \delta_k) + \cdots + \\ &\quad \frac{2 \cdot 1}{2} \cdot (2^{n-4} + \delta_{n-1} 2^{n-5} + \cdots + \delta_5 2 + \delta_4 + \delta_2) = \\ &\quad \left[ \frac{n \cdot (n-1)}{2} + \frac{(n-2) \cdot (n-1)}{2} \cdot 1 + \frac{(n-3) \cdot (n-4)}{2} \cdot 2 + \right. \\ &\quad \left. \frac{(n-4) \cdot (n-5)}{2} \cdot 2^2 + \cdots + \frac{2 \cdot 1}{2} \cdot 2^{n-4} \right] + \\ &\quad \delta_{n-1} \left[ \frac{(n-1) \cdot (n-2)}{2} + \frac{(n-3) \cdot (n-4)}{2} \cdot 1 + \frac{(n-4) \cdot (n-5)}{2} \cdot 2 + \cdots + \right. \\ &\quad \left. \frac{2 \cdot 1}{2} \cdot 2^{n-5} \right] + \cdots + \delta_4 \left( \frac{4 \cdot 3}{2} + \frac{2 \cdot 1}{2} \right) + \delta_3 \cdot \frac{3 \cdot 2}{2} + \delta_2 \cdot \frac{2 \cdot 1}{2}. \end{aligned} \tag{6}$$

引理 1 对任意的  $n \geq 1$ , 有

$$\begin{aligned} &\frac{n \cdot (n-1)}{2} + \frac{(n-2) \cdot (n-3)}{2} \cdot 1 + \frac{(n-3) \cdot (n-4)}{2} \cdot 2 + \frac{(n-4) \cdot (n-5)}{2} 2^2 + \cdots + \\ &\quad \frac{k \cdot (k-1)}{2} 2^{n-2-k} + \cdots + \frac{3 \cdot 2}{2} \cdot 2^{n-5} + \frac{2 \cdot 1}{2} 2^{n-4} = 2^{n-1} - 1. \end{aligned} \tag{7}$$

将式(7)代入式(6), 全体超半拆分的指数和为

$$\begin{aligned} L_1 &= 2^{n-1} - 1 + (2^{n-2} + 1) \delta_{n-1} + (2^{n-3} - 1) \delta_{n-2} + \cdots + (2^2 - 1) \delta_3 + (2 - 1) \delta_2 = \\ &\quad 2^{n-1} + \delta_{n-1} 2^{n-2} + \delta_{n-2} 2^{n-3} + \cdots + \delta_3 2^2 + \delta_2 2 + \delta_1 - (1 + \delta_{n-1} + \delta_{n-2} + \cdots + \delta_2 + \delta_1) = \end{aligned}$$

$$a-(1+\delta_{n-1}+\delta_{n-2}+\cdots+\delta_1).$$

证明:对任意自然数  $n$ ,有恒等式

$$\frac{n \cdot (n-1)}{2} + \frac{(n-2) \cdot (n-3)}{2} \cdot 1 + \frac{(n-3) \cdot (n-4)}{2} \cdot 2 + \frac{(n-4)(n-5)}{2} \cdot 2^2 + \cdots + \frac{k \cdot (k-1)}{2} 2^{n-2-k} + \cdots + \frac{3 \cdot 2}{2} \cdot 2^{n-5} + \frac{2 \cdot 1}{2} \cdot 2^{n-4} = 2^{n-1} - 1$$

成立.

设  $a_n = \frac{n \cdot (n-1)}{2} + \frac{(n-2) \cdot (n-3)}{2} \cdot 1 + \frac{(n-3) \cdot (n-4)}{2} \cdot 2 + \frac{(n-4) \cdot (n-5)}{2} \cdot 2^2 + \cdots + \frac{k \cdot (k-1)}{2} \cdot 2^{n-2-k} + \cdots + \frac{3 \cdot 2}{2} \cdot 2^{n-5} + \frac{2 \cdot 1}{2} \cdot 2^{n-4}$ , 那么,  $a_{n-1} = \frac{(n-1) \cdot (n-2)}{2} + \frac{(n-3) \cdot (n-4)}{2} \cdot 1 + \frac{(n-4) \cdot (n-5)}{2} \cdot 2 + \frac{(n-5) \cdot (n-6)}{2} \cdot 2^2 + \cdots + \frac{(k-1) \cdot (k-2)}{2} \cdot 2^{n-3-k} + \cdots + \frac{3 \cdot 2}{2} \cdot 2^{n-6} + \frac{2 \cdot 1}{2} \cdot 2^{n-5}$ .

再设  $b_k = a_k - a_{k-1}$ , 则  $b_n = a_n - a_{n-1} = (n-1) + (n-3) + (n-4) \cdot 2 + (n-5) \cdot 2^2 + \cdots + (k-1) 2^{n-2-k} + \cdots + 3 \cdot 2^{n-6} + 2 \cdot 2^{n-5} + 1 \cdot 2^{n-4}$ ,  $b_{n-1} = a_{n-1} - a_{n-2} = (n-2) + (n-4) + (n-5) \cdot 2 + (n-6) \cdot 2^2 + \cdots + (k-1) 2^{n-3-k} + \cdots + 3 \cdot 2^{n-7} + 2 \cdot 2^{n-6} + 2^{n-5}$ . 所以有

$$b_n - b_{n-1} = 1 + 1 + 2 + 2^2 + \cdots + 2^{n-6} + 2^{n-5} + 2^{n-4} = 2^{n-3}.$$

由数列  $b_n = b_{n-1} - b_{n-2} = 2^{n-4}, \cdots, b_3 - b_2 = 1, b_2 - b_1 = 1$ , 有  $b_3 = 2, b_2 = 1, b_1 = 0$ , 所以有  $b_n = 2^{n-2}$ .

$$\sum_{i=2}^n b_i = \sum_{i=1}^{n-1} (a_{i+1} - a_i) = a_n - a_1 = 2^{n-2} + 2^{n-3} + \cdots + 2 + 1 + 0 = 2^{n-1} - 1.$$

由数列  $a_n = 2^{n-1} - 1$ , 得  $a_1 = 0$ .

1.5 范例

例 1 求下列各数的所有和式拆分循环:a) 素数  $p=23$ ;b) 素数  $p=43$ ;c) 合数  $p=35$ .

a)  $p=2a+1=2 \cdot 11+1=23, a=11, \frac{a+1}{2}=6$ , 因此, 23 有 6 个和式拆分,  $23-1=2 \cdot 11, 23-11=2^2 \cdot 3, 23-3=2^2 \cdot 5, 23-5=2 \cdot 9, 23-9=2 \cdot 7, 23-7=2^4 \cdot 1$ , 其节点循环为 1-11-3-5-9-7, 由此偶循环导出  $23 \cdot (2^7-2^6+2^5-2^3+2^1-1)=2^{11}-1$ .

b)  $p=2a+1=2 \cdot 21+1=43, a=21, \frac{a+1}{2}=11$ , 因此, 43 有 11 个和式拆分.

$43-1=2 \cdot 21, 43-21=2 \cdot 11, 43-11=2^5 \cdot 1$ , 由此奇循环导出  $43 \cdot (2^2-2+1)=2^7+1$ ;  
 $43-\underline{3}=2^3 \cdot 5, 43-5=2 \cdot 19, 43-19=2^3 \cdot \underline{3}$ , 由此奇循环导出  $43 \cdot (2^4-2^3+1)=3 \cdot (2^7+1)$ ;  
 $43-\underline{7}=2^2 \cdot 9, 43-9=2 \cdot 17, 43-17=2 \cdot 13, 43-13=2 \cdot 15, 43-15=2^2 \cdot \underline{7}$ , 由此奇循环导出了  $43 \cdot (2^5-2^4+2^3-2^2+1)=7 \cdot (2^7+1)$ .

c)  $p=2a+1=2 \cdot 17+1=35, a=17, \frac{a+1}{2}=9$ , 因此, 35 有 9 个和式拆分.

其基循环为  $35-\underline{1}=2 \cdot 17, 35-17=2 \cdot 9, 35-9=2 \cdot 13, 35-13=2 \cdot 11, 35-11=2^3 \cdot 3$ , 其偶循环为  $35-3=2^5 \cdot \underline{1}$ , 由此循环导出  $35 \cdot (2^7-2^4+2^3-2^2+2-1)=2^{12}-1$ ;  $35-\underline{5}=2 \cdot 15, 35-15=2^2 \cdot \underline{5}$ , 由此循环导出  $35 \cdot (2-1)=5 \cdot (2^3-1)$ ;  $35-\underline{7}=2^2 \cdot \underline{7}, 35=7 \cdot (2^2+1)$ .

因此, 素数 43 有 3 个奇循环, 且各循环的指数和都是 7; 而合数 35 有偶循环, 也有奇循环, 各循环的指数和也不一样.

例 2 用 a)  $p=23$ ; b)  $p=35$  的超半拆分, 验证超半拆分指数和定理.

a)  $p=2a+1=2 \cdot 11+1=23=2^4+2^2+2+1$ , 故  $a=11, \delta_1=1, \delta_2=1, \delta_3=0, a-(\delta_3+\delta_2+\delta_1+1)=8$ . 23 的超半拆分为  $23-13=2 \cdot 5, 23-15=2^3, 23-17=2 \cdot 3, 23-19=2^2, 23-21=2$ , 这些超半拆分指数和是 8.

b)  $p=2a+1=2 \cdot 17+1=35=2^5+2+1$ , 所以  $a=17, \delta_4=0, \delta_3=0, \delta_2=0, \delta_1=1, a-(\delta_4+\delta_3+\delta_2+$

$\delta_1+1)=17-2=15$ . 35 的超半拆分为  $35-19=2^4, 35-21=2\cdot 7, 35-23=2^2\cdot 3, 35-25=2\cdot 5, 35-27=2^3, 35-29=2\cdot 3, 35-31=2^2, 35-33=2^1$ , 超半拆分的指数和是 15.

## 2 奇数的差式拆分循环

### 2.1 奇数的差式拆分

设  $p=2a+1=2^n+\delta_{n-1}2^{n-1}+\delta_{n-1}2^{n-2}+\cdots+\delta_12+1$ , 令奇数集  $\{1, 3, 5, \cdots, p-2\}$  为  $B, |B|=a$ , 则  $\forall \alpha\in B, \exists \beta\in B$  及数  $l(1\leq l\leq n+1)$ , 使得  $p=2^l\beta-\alpha$ , 其中,  $p$  为一个差式拆分,  $\alpha$  为拆分的起点,  $\beta$  为拆分的接点,  $l$  为拆分的指数.

由于  $B$  是有限集, 所以  $\forall \alpha_0\in B, \exists \alpha_i\in B$  及数  $l_i, 1\leq l_i\leq 2n(i=1, 2, \cdots, k), \alpha_k=\alpha_0$ , 使得

$$p+\alpha_0=2^{l_1}\alpha_1, \quad p+\alpha_1=2^{l_2}\alpha_2, \quad \cdots, \quad p+\alpha_{k-1}=2^{l_k}\alpha_k=2^{l_k}\alpha_0. \tag{8}$$

式(8)中: 拆分序列是一个以  $\alpha_0$  为起点的差式拆分循环.

由拆分序列(8)导出

$$\begin{aligned} p+\alpha_0 &= 2^{l_1}(2^{l_2}\alpha_2-k) = 2^{l_1+l_2}(2^{l_3}\alpha_3-p) - 2^{l_1}p = 2^{l_1+l_2+l_3}(2^{l_4}\alpha_4-p) - 2^{l_1}p - 2^{l_1+l_2}p = \cdots = \\ & 2^{l_1+l_2+\cdots+l_k}\alpha_0 - 2^{l_1}p - 2^{l_1+l_2}p - \cdots - 2^{l_1+l_2+\cdots+l_{k-1}}p, \end{aligned}$$

即  $p\cdot(2^{l_1+l_2+\cdots+l_{k-1}}+2^{l_1+l_2+\cdots+l_{k-2}}+\cdots+2^{l_1+l_2}+2^{l_1}+1)=\alpha_0(2^{l_1+l_2+\cdots+l_k}-1)=\alpha_0(2^m-1)$ , 其中,  $m=\sum_{i=1}^kl_i$ . 当  $p$  是素数时,  $p$  与拆分循环的各节点的最大公因数  $(p\cdot\alpha_0\cdot\alpha_1, \cdots, \alpha_{k-1})=1$ ; 当  $p$  是合数时, 如  $p=p_1\cdot p_2(p_1, p_2$  为素数), 则  $(p, \alpha_0, \alpha_1, \cdots, \alpha_{k-1})=1$  或  $p_1$  或  $p_2$ .

### 2.2 奇数 $p$ 的差式拆分循环与和式拆分循环的关系

设  $p-\alpha_0=2^{l_1}\alpha_1, p-\alpha_1=2^{l_2}\alpha_2, \cdots, p-\alpha_{2s-1}=2^{l_{2s}}\cdot\alpha_0$  是  $p$  的一个和式拆分偶循环,  $p$  的指数和为  $\sum_{i=1}^{2s}l_i=m$ . 当  $l_1=1$  时, 由于  $p-\alpha_0=2\alpha_1, p-\alpha_1=2^{l_2}\alpha_2$ , 所以  $p+\alpha_0=2\alpha_1+2\alpha_0=2(\alpha_1+\alpha_0)=2(\alpha_1+p-2\alpha_1)=2^{1+l_2}\alpha_2=2^{l_1+l_2}\alpha_2$ , 即当  $l_1=1$  时, 由  $p-\alpha_0=2\alpha_1, p-\alpha_1=2^{l_2}\alpha_2$ , 导出  $l_1$  个起点为  $\alpha_0$ , 节点为  $\alpha_2$  的差式拆分, 其指数为  $l_1+l_2$ .

当  $l_1>1$  时, 由于

$$\begin{aligned} p+\alpha_0 &= 2(2^{l_1-1}\alpha_1+\alpha_0), \\ p+(2^{l_1-1}\alpha_1+\alpha_0) &= 2^{l_1-1}\alpha_1+2(2^{l_1-1}\alpha_1+\alpha_0)=2[(2^{l_1-1}+2^{l_1-2})\alpha_1+\alpha_0], \\ p+[(2^{l_1-1}+2^{l_1-2})\alpha_1+\alpha_0] &= 2[(2^{l_1-1}+2^{l_1-2}+2^{l_1-3})\alpha_1+\alpha_0]=\cdots, \\ p+[(2^{l_1-1}+2^{l_1-2}+\cdots+2)\alpha_1+\alpha_0] &= 2[(2^{l_1-1}+2^{l_1-2}+\cdots+2+1)\alpha_1+\alpha_0]= \\ & 2[(2^{l_1}-1)\alpha_1+\alpha_0]=2(p-\alpha_1)=2^{1+l_2}\alpha_2, \end{aligned}$$

由  $p-\alpha_0=2^{l_1}\alpha_1, p-\alpha_1=2^{l_2}\alpha_2$  导出  $l_1$  个差式拆分序列, 这个拆分序列前  $l_1-1$  个的拆分指数为 1, 最后一个拆分的指数为  $l_2+1$ . 所以这个拆分的指数和为  $l_1+l_2$ . 与这  $l_1$  个拆分序列对应的节点序列起点是  $\alpha_0$ , 最后的节点是  $\alpha_2$ .

同理可证, 由  $p-\alpha_2=2^{l_3}\alpha_3, p-\alpha_3=2^{l_4}\alpha_4$ , 可导出  $l_3$  个差式拆分序列, 前  $l_3-1$  个拆分的指数为 1, 最后一个拆分的指数为  $l_4+1$ . 所以这个拆分序列的指数和为  $l_3+l_4$ . 这个拆分序列的起点为  $\alpha_2$ , 最后的节点是  $\alpha_4$ . 最后, 由  $p-\alpha_{2s-2}=2^{l_{2s-1}}\alpha_{2s-1}, p-\alpha_{2s-1}=2^{l_{2s}}\alpha_0$ , 导出  $l_{2s-1}$  个差式拆分, 其前  $l_{2s-1}-1$  个拆分的指数为 1, 最后一个拆分的指数为  $l_{2s}+1$ , 所以这个拆分序列的指数和为  $l_{2s-1}+l_{2s}$ . 这个拆分序列的起点为  $\alpha_{2s-2}$ , 最后的节点是  $\alpha_{2s}=\alpha_0$ . 于是  $l_1+l_3+\cdots+l_{2s-1}$  个差式拆分序列构成一个差式拆分循环, 其指数和  $(l_1+l_2)+(l_3+l_4)+\cdots+(l_{2s-1}+l_{2s})=\sum_{i=1}^{2s}l_i=m$ . 由  $p$  的和式拆分循环, 还可导出一个起点为  $\alpha_1$ , 含有  $l_2+l_4+\cdots+l_{2s}$  个差式拆分, 指数和为  $(l_2+l_3)+(l_4+l_5)+\cdots+(l_{2s}+l_1)=m$  的差式拆分循环.

因此, 如果  $p$  有一个指数和为  $m=\sum_{i=1}^{2s}l_i$  的和式拆分偶循环, 则由该偶循环可导出两个指数和均为  $m$  的差式拆分循环, 其中, 一个循环的节点有  $l_1+l_3+\cdots+l_{2s-1}$  个, 另一循环的节点有  $l_2+l_4+\cdots+l_{2s}$  个, 进而可导出  $p|2^{2m}-1$ .

同理可证,若  $p$  有一个和式拆分奇循环,即

$$p-\alpha_{i-1}=2^{l_i}\alpha_i(i=1,2,\cdots,2s-1),\quad \alpha_{2s-1}=\alpha_0,\quad m=\sum_{i=1}^{2s-1}l_i,$$

则由此可导出一个指数和为  $2m$ ,节点个数也是  $m=\sum_{i=1}^{2s-1}l_i$  的差式拆分循环,进而可导出  $p|2^{2m}-1$ .

2.3 范例

例 3 求  $p=23$  的导出结果.

$p=23$  只有一个和式拆分偶循环,指数和为  $m=11$ .  $p=23$  的一个差式拆分循环为  $23+\underline{1}=2^3\cdot 3$ ,  $23+3=2\cdot 13,23+9=2^5\cdot \underline{1}$ ,此循环导出的结果为  $23\cdot (2^6+2^4+2^3+1)=1\cdot (2^{11}-1)$ .  $23$  的另一个差式拆分循环为  $23+\underline{5}=2^2\cdot 7,23+7=2\cdot 15,23+15=2\cdot 19,23+19=2\cdot 21,23+21=2^2\cdot 11,23+11=2\cdot 17,23+17=2^3\cdot \underline{5}$ . 此循环导出的结果为  $23\cdot (2^8+2^7+2^5+2^4+2^3+2^2+1)=5\cdot (2^{11}-1)$ .

例 4 求  $p=43$  的导出结果.

$p=43$  的基循环  $43-1=2\cdot 21,43-21=2\cdot 11,43-11=2^5$  是一个指数和  $m=7$  的奇循环,此循环导出的结果为  $43\cdot (2^2-2+1)=1\cdot (2^7+1)$ .

对应于此奇循环, $43$  有一个差式拆分循环: $43+\underline{1}=2^2\cdot 11,43+11=2\cdot 27,43+27=2\cdot 35,43+35=2\cdot 39,43+39=2\cdot 41,43+41=2^2\cdot 21,43+21=2^6\cdot \underline{1}$ ,此循环导出的结果为

$$43\cdot (2^8+2^6+2^5+2^4+2^3+2^2+1)=2^{2\cdot 7}-1=2^{14}-1.$$

3 素数和式拆分循环

3.1 素数的和式拆分

定理 2 素数  $p$  的任一偶循环的指数和都是奇数.

证明:设素数  $p$  有一偶循环  $p-\alpha_{k-1}=2^{l_k}\alpha_k(k=1,2,\cdots,2s),\alpha_{2s}=\alpha$ ,指数和为  $m=\sum_{i=1}^{2s}l_k$ .

由反证法,设  $m$  为偶数,且  $m=2m_1$ . 因为  $p|2^m-1=(2^{m_1}-1)(2^{m_1}+1)$ ,所以  $2^{m_1}\equiv 1(\bmod p)$  或  $2^{m_1}\equiv -1(\bmod p)$ . 因  $m_1<m$ ,故存在  $k,1\leq k\leq 2s$ ,使得  $l_1+l_2+\cdots+l_{k-1}<m_1\leq l_1+l_2+\cdots+l_k$ . 当  $m_1<l_1+l_2+\cdots+l_k$  时,存在数  $t(0<t<l_k)$ ,使得  $m_1+t=l_1+l_2+\cdots+l_k$ .

当  $k$  为奇数时, $p|2^{l_1+l_2+\cdots+l_k}\alpha_k+\alpha_0$ ,即  $2^{m_1+t}\alpha_k+\alpha_0\equiv 0(\bmod p)$ ,因为  $2^{m_1}\equiv \pm 1(\bmod p),0<t<l_k$ ,从而  $2^{t'}\alpha_k<a,\alpha_0<a$ ,又偶数  $2^{t'}\alpha_k\neq \alpha_0$ ,所以  $2^{m_1+t'}\alpha_k+\alpha_0\equiv \pm 2^{t'}\alpha_k+\alpha_0\equiv 0(\bmod p)$ ,这与  $p$  的偶循环的拆分序列得到的结论矛盾. 当  $k$  为偶数时,由拆分序列得  $2^{l_1+l_2+\cdots+l_k}\alpha_k-\alpha_0\equiv 0(\bmod p)$ ,即  $2^{m_1+t'}\alpha_k-\alpha_0\equiv 0(\bmod p)$ ,则由  $2^{m_1}\equiv \pm 1(\bmod p)$  及  $0<t<l_k$ ,得  $2^{t'}\alpha_k<a,2^{t'}\alpha_k\neq \alpha_0$ ,所以  $2^{m_1+t'}\alpha_k-\alpha_0\equiv \pm 2^{t'}\cdot \alpha_k-\alpha_0\equiv 0(\bmod p)$ ,这与  $p$  的拆分序列导出的结论也相矛盾. 如果  $t=0,m_1=l_1+l_2+\cdots+l_{k-1}$  时,由  $2^{m_1}\equiv 1$  或  $-1(\bmod p)$ ,同样证法得出与拆分序列导出的结论相悖. 因此, $m$  不是偶数,否则,与  $p$  的拆分序列导出结论矛盾, $m$  只能是奇数.

推论 1 设素数  $p$  有一个偶循环,指数和为  $m$ ,则所有满足  $2^r\equiv 1(\bmod p),\min r=m$ .

证明:设  $(m,r)=m_1$ ,若  $m_1=1$ ,则  $m,r$  互素,因此  $\exists P>0,Q>0$ ,使得  $Pm-Qr=1$ ,或  $Pr-Qm=1$ . 因为  $2^{Pm}=2^{Qr+1}$ ,或  $2^{Pr}=2^{Qm+1}$ ,所以  $1\equiv 2^{Pm}\equiv 2^{Qr+1}\equiv 2(\bmod p)$  或  $1\equiv 2^{Pr}\equiv 2^{Qm+1}\equiv 2(\bmod p)$  不成立. 若  $1<m_1<m$ ,用定理 2 的证法,可证  $m_1$  不能小于  $m$ ,所以  $m_1=m,r=dm$ . 即所有满足  $2^r\equiv 1(\bmod p)$  的  $r$ , $\min r=m$ ,且若  $2^r\equiv 1(\bmod p)$ ,则  $r=dm$ .

定理 3 素数  $p$  的基循环若是指数和为  $m$  的偶循环,则  $p$  的任一循环都是指数和为  $m$  的偶循环. 素数  $p$  的基循环若是指数和为  $m$  的奇循环,则  $p$  的任一循环都是指数和为  $m$  的奇循环.

证明:若  $p$  只有一个拆分循环,定理结论自然成立. 设  $p$  有一个异于基循环,指数和为  $m_1$  的循环 (I),若循环 (I)是偶循环,则由定理 2 可断定  $m_1|m$ ,则基循环是偶循环,且  $p|2^{m_1}-1$ . 由定理 2 可断定  $m|m_1$ ,因此, $m_1=m$ .

若循环 (I)是奇循环,则  $p|2^{m_1}+1$ ,由定理 2 及推论 1 易证, $m_1$  是所有满足  $2^r+1\equiv 0(\bmod p)r$  的最小值. 若  $2^r+1\equiv 0(\bmod p)$ ,则  $m_1|r$ . 如果  $p|2^{m_1}+1$  成立,则因为  $p|2^m-1,p|2^m+1$  不能同时成立,

故  $m_1 \neq m$ . 若  $m < m_1$ , 设  $m_1 = m_2 m + r_1, 0 \leq r_1 < m$ , 则  $-1 \equiv 2^{m_1} \equiv 2^{m_2 m + r_1} \equiv 2^{r_1} \pmod{p}$ , 当  $r = 1$  时, 同余式显然不成立; 当  $r_1 > 0$  时, 则由于  $r_1 < m_1$ , 而所有满足  $2^r + 1 \equiv 0 \pmod{p}$  的最小值是  $m_1$ , 所以有  $2^{r_1} \not\equiv -1 \pmod{p}$ , 即  $m_1$  不能大于  $m$ . 若  $m > m_1$ , 设  $m = m_2 m_1 + r, 0 \leq r < m_1$ , 则  $1 \equiv 2^m \equiv 2^{m_1 m_2 + r} \equiv (-1)^{m_2} \cdot 2^r \pmod{p}$ , 当  $r > 0$  时, 由于  $r < m, r < m_1, 2^r \not\equiv \pm 1 \pmod{p}$ ; 当  $r = 0$  时, 同余式成立的条件是  $m_2$  为偶数, 从而  $m = m_1 \cdot m_2$  是偶数, 但这与定理 2 结论相悖. 综上所述, 若  $p \mid 2^{m_1} + 1$ , 则  $m_1 \neq m, m_1$  不大于  $m, m_1$  也不小于  $m$ , 所以  $p \nmid 2^{m_1} + 1$ , 即假设  $p$  有奇循环是错误的, 循环 (I) 只能是偶循环, 且  $m = m_1$ .

**推论 2** 如果素数  $p = 2a + 1$  有  $b$  个拆分循环, 每个循环的指数和为  $m$ , 那么,  $p$  的和式拆分的指数和  $a = bm$  (定理 1), 即  $p = 2a + 1 = 2bm + 1$ .

3.2 范例

$M_p = 2^p - 1$  形的数为 Mersenne 数, 其中,  $p$  为素数. 当  $p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 807, 1\,279, 2\,203, 2\,281$  时,  $M_p$  为素数<sup>[1]</sup>. 近代大型计算机偶然算出几个大数  $p$  的  $M_p$  是素数.

**例 5** 如果  $p = 4m + 3$  是素数,  $q = 2p + 1$  也是素数, 则  $q \mid 2^p - 1, M_p = 2^p - 1$  是合数.  
证明: 根据定理 3, 素数  $q$  的拆分循环的指数和  $m$  必须整除  $p, p$  为素数, 所以  $q$  的拆分循环指数和为  $p$ , 且  $q$  仅有一个拆分循环, 其节点数为  $\frac{p+1}{2} = \frac{4n+3+1}{2} = 2n+2$  个, 即  $q$  的拆分循环为偶循环,  $q \mid 2^p - 1, M_p$  是合数. 如  $p = 11, q = 2 \cdot p + 1 = 23, 23 \mid 2^{11} - 1; p = 23, q = 47, 47 \mid 2^{23} - 1; \cdots; p = 179, q = 2p + 1 = 359, 359 \mid 2^{179} - 1; p = 191, q = 2p + 1 = 383, 383 \mid 2^{191} - 1$  等.

要证明  $M_{23} = 2^{23} - 1$  有素因数  $p = 2 \cdot 23 + 1 = 47$ , 设  $2^{23} - 1 = (2 \cdot 23 + 1)(2 \cdot 23 \cdot 4b + 1)$ , 则  $2^{22} - 1 = (2^{11} - 1)(2^{11} + 1) = 2 \cdot 23^2 \cdot 4b + 23 \cdot (1 + 4b)$ . 因为  $2^{11} = 2\,048, 2^{11} - 1 = 2\,047 = 23 \cdot 89$ , 所以  $89 \cdot 2\,049 - 1 = 4 \cdot 47b, 22 \cdot 2\,049 + 512 = 47b$ , 令  $b = 2b_1$ , 得  $47b_1 = 11 \cdot 2\,049 + 256 = 22\,795$ , 求得  $b_1 = 485, b = 970, 2 \cdot 23 \cdot 4b + 1 = 8 \cdot 23 \cdot 970 + 1 = 178\,481$ , 即  $2^{23} - 1 = 47 \cdot 178\,481$ .

**例 6** 设素数  $p = 4n + 1, q = 2p + 1$  也是素数, 则  $q \mid 2^p + 1$ .  
证明:  $q$  仅有一个指数和为  $p$  的拆分循环, 其节点个数为  $\frac{p+1}{2} = 2n + 1$  个, 所以  $p$  的拆分循环是奇循环,  $q \mid 2^p + 1$ . 如  $p = 5, q = 2p + 1 = 11, 11 \mid 2^5 + 1; p = 29, q = 59, 59 \mid 2^{29} + 1; \cdots; p = 41, q = 83, 83 \mid 2^{41} + 1; p = 53, q = 107, 107 \mid 2^{53} + 1; p = 89, q = 179, 179 \mid 2^{89} + 1$  等.

**例 7**  $p$  为素数, 且  $q = 4p + 1$  也是素数, 则  $q \mid 2^{2p} + 1$ .  
证明: 设  $q$  的拆分循环指数和为  $m, m \mid 2p$ , 若  $m = p, q$  有两个拆分循环, 两循环的节点个数之和必是偶数, 而  $q$  的节点总个数为奇数  $2p/2 = p$ , 所以  $m \neq p, m = 2p$ . 因为  $q$  只有一个指数和为  $2p$  的奇循环, 所以  $q \mid 2^{2p} + 1$ . 如  $p = 3, q = 4p + 1 = 13, 13 \mid 2^{2p} + 1 = 2^6 + 1; p = 13 \cdot q = 4p + 1 = 53, 53 \mid 2^{26} + 1$ .

例 5 说明  $p = 4m + 3$  是素数,  $q = 2p + 1$  是素数, 则  $M_p$  必为合数. 反之, 若  $p = 4m + 3$  是素数,  $q = 2p + 1$  是合数, 则  $M_p$  必为素数. 如  $p = 31, q = 2p + 1 = 63$  是合数,  $M_{31} = 2^{31} - 1$  是素数;  $p = 61, q = 2p + 1 = 123$  是合数,  $M_{61}$  是素数;  $p = 107, q = 2p + 1 = 215$  是合数,  $M_{107}$  是素数;  $p = 127, q = 2p + 1 = 255$  是合数,  $M_{127}$  是素数;  $p = 807, q = 2p + 1 = 2 \cdot 807 + 1$  是合数,  $M_{807}$  是素数;  $p = 1\,279, q = 2p + 1 = 2 \cdot 1\,279 + 1 = 2\,559$  是合数,  $M_{1\,279}$  是素数;  $p = 2\,203, q = 2p + 1 = 2 \cdot 2\,203 + 1 = 4\,407$  是合数,  $M_{2\,203}$  是素数.

**例 8**  $p = 19$  是素数,  $2p + 1 = 39$  是合数, 而  $M_{19} = 2^{19} - 1$  是素数.  
证明: 由反证法, 设  $M_{19}$  是合数, 其素数因素  $p = 2a + 1$  的拆分循环是偶循环, 指数和为 19.  $p$  的节点总数应当为偶数, 当  $a$  为奇数时, 因为  $19 \mid a$  且  $\frac{a+1}{2}$  为偶数,  $a$  必须是形如  $19 \cdot (4a_1 + 1)$  的数; 当  $a$  为偶数时, 因为  $19 \mid a$  且  $\frac{a}{2}$  为偶数,  $a$  必须是形如  $19 \cdot 4a_1$  的数. 因此, 命  $M_{19} = 2^{19} - 1 = [2 \cdot 19(4a + 1) + 1] \cdot [2 \cdot 4 \cdot 19b + 1]$ , 从而有  $\frac{2^{18} - 1}{19} = 2 \cdot 19(4a + 1) \cdot 4b + 4a + 1 + 4b, \frac{2^{18} - 20}{19} = 2 \cdot 19(4a + 1) \cdot 4b + 4a + 4b, \frac{2^{16} - 5}{19} = \frac{(19 \cdot 13 + 9)^2 - 5}{19} = 13^2 \cdot 19 + 2 \cdot 13 \cdot 9 + 4 = 3\,449 = [2 \cdot 19 \cdot (4a + 1) + 1] \cdot b + a$ . 由素数表查得, 当  $a$  分别取 7, 10, 19, 20, 29 时,  $2 \cdot 19 \cdot (4a + 1) + 1$  分别为素数 1 103, 1 559, 2 927, 3 079

及  $4\,447$ , 其中, 前 4 个素数不能整除  $3\,449 - a$ , 而  $4\,447 > 3\,449 - 29$ , 故  $3\,449 - a = [2 \cdot 19(4a + 1) + 1] \cdot b$  无整数解,  $M_{19}$  是素数.

**例 9** 用拆分理论证明  $F_5 = 2^{2^5} + 1 = 2^{32} + 1$  是合数.

证明: 设  $F_5 = 2^{32} + 1 = p \cdot q$ ,  $p = 2a + 1$  为  $F_5$  的素因数,  $p$  的拆分循环为奇循环, 指数和为  $2^5 = 32$ ,  $2^5 \mid a$ ,  $p$  应当是形如  $2 \cdot 2^5 n + 1$  的数. 当  $n$  为奇数时,  $p$  有奇数个拆分奇循环, 其总节点数应当是奇数, 这与  $p = 2 \cdot 2^5 n + 1$  的节点总数  $2^4 n$  个矛盾, 故  $n$  应当是偶数.

设  $p = 2 \cdot 2^5 \cdot 2a + 1 = 2^7 a + 1$ ,  $q = 2^7 b + 1$ , 即  $F_5 = 2^{32} + 1 = (2^7 a + 1)(2^7 b + 1)$ , 则  $2^{25} = 2^7 ab + a + b$ , 令  $a + b = 2^7 c$ , 则  $2^{18} = ab + c = 2^7 ca - a^2 + c$ , 即  $2^{18} + a^2 = (2^7 a + 1)c$ , 将其变形为  $2^{18} a + a^3 = (2^7 a + 1)ca$ ,  $2^{18} a + 2^{11} - 2^{11} + a^3 = (2^7 a + 1)ca$ ,  $-2^{11} + a^3 = (2^7 a + 1)(ca - 2^{11})$ , 再变形为  $2^4 + a^4 = (2^7 a + 1)(ca^2 - 2^{11} a + 2^4)$ .

若  $ca^2 - 2^{11} a + 2^4 = 1$ , 则  $2^4 - 1 + a^4 = 5 \cdot 3 + a^4 = 2^7 a$ . 取  $a = 5$ , 则  $3 + 5^3 = 128 = 2^7$ , 所以  $F_5 = 2^{2^5} + 1$  有一素因数  $p = 2^7 \cdot 5 + 1 = 641$ . 再由  $ca^2 - 2^{11} a + 2^4 = 25c - 2\,048 \cdot 5 + 16 = 1$ , 求得  $c = 409$ ,  $b = 2^7 c - a = 128 \cdot 409 - 5 = 52\,347$ ,  $q = 2^7 b + 1 = 128 \cdot 52\,347 + 1 = 6\,700\,417$ .

参考文献:

[1] 华罗庚. 数论导引[M]. 北京: 科学出版社, 1957.

[2] WIKIPEDIA. Mersenne prime[EB/OL]. (2017-07-21)[2021-02-05]. [http://tcs.nju.edu.cn/wiki/index.php/Mersenne\\_prime](http://tcs.nju.edu.cn/wiki/index.php/Mersenne_prime).

[3] 蔡天新. 完美数与黄金分割比[J]. 数学进展, 2019, 48(4): 127-129. DOI:10.11845/sxjz.2019001e.

[4] 周忠奇, 黄文豪. 梅森数、瓦格斯塔夫数推广及其整数因子研究[J]. 佳木斯大学学报(自然科学版), 2017, 35(6): 1009-1010. DOI:10.3969/j.issn.1008-1402.2017.06.034.

[5] 陈景润. 初等数论 I [M]. 北京: 科学出版社, 1978.

[6] 陈景润. 初等数论 II [M]. 北京: 科学出版社, 1980.

[7] 闵嗣鹤, 严士健. 初等数论[M]. 2 版. 北京: 人民教育出版社, 1982.

[8] BANERJEE S, BATAVIA M, KANE B, *et al.* Fermat's polygonal number theorem for repeated generalized polygonal numbers[J]. Journal of Number Theory, 2020, 220: 163-181. DOI:10.1016/j.jnt.2020.05.024.

[9] BANERJEE S, BATAVIA M, KANE B, *et al.* Expect at most one billionth of a new Fermat Prime! [J]. Mathematical Intelligencer, 2016, 39(1): 1-3. DOI:10.1007/s00283-016-9644-3.

[10] CAMBRAIA A J, KNAPP M P, LEMOS A, *et al.* On prime factors of Mersenne numbers[EB/OL]. (2021-04-29)[2021-05-03]. <https://arxiv.org/pdf/1606.08690.pdf>.

[11] KELLER W. Prime factors  $k \cdot 2n + 1$  of fermat numbers fm and complete factoring status[EB/OL]. (2021-03-03)[2021-05-03]. <http://www.prothsearch.com/fermat.html>.

[12] KELLER W. Distributed search for fermat number divisors[EB/OL]. (2020-10-22)[2021-02-05]. <http://www.fermatsearch.org/>.

[13] WANG Xinbo. Algorithm available for factoring big fermat numbers[J]. Journal of Software, 2020, 15(3): 86-97. DOI:10.17706/jsw.15.3.86-97.

[14] 王钰. 一个费马数分解算法的剖析与优化[J]. 现代计算机, 2020(36): 64-67. DOI:10.3969/j.issn.1007-1423.2020.36.012.

(责任编辑: 陈志贤      英文审校: 黄心中)