第二章 同余
2015 年03月31 日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

访问主页
标题页
目录页
第 1 页 共 27 页
返回
全屏显示
关闭
退出

- 什么是欧拉函数?
- 如何计算欧拉函数?
- 什么是简化剩余? 为什么说是从乘法角度来看待它?
- 简化剩余系在什么变换下仍未简化剩余系?
- 如何构造更大模的简化剩余?

2.3 简化剩余系与欧拉函数

2.3.1 欧拉函数

在讨论中, 常常假定两个整数 a, m 互素的条件, 即 $(a, m) = 1$.
现在我们讨论剩余与 m 互素的剩余类的性质.

定义2.3.1 设 m 是一个正整数. 则 m 个整数 $0,\ 1,\ \ldots,\ m-1$ 中与 m 互素的整数的个数, 记作 $\varphi(m)$, 通常叫做**欧拉** (Euler) **函数**.

例2.3.1 设 $m = 10$. 则 10 个整数 $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9$ 中与 10 互素的整数为 $1,\ 3,\ 7,\ 9$, 所以 $\varphi(10) = 4$.

例2.3.2 设$m = p$ 为素数. 则p 个整数$1,\ 2,\ \ldots,\ p-1,\ p$ 中与p 互素的整数为$1,\ 2,\ \ldots,\ p-1$, 所以$\varphi(p) = p-1$.

定理2.3.1 对于素数幂$m = p^\alpha$, 有

$$\varphi(m) = p^\alpha - p^{\alpha-1} = m\prod_{p|m}(1-\frac{1}{p}). \quad (1)$$

证 对于素数幂$m = p^\alpha$, 从1 到m 的m 个整数的形式为

$$\begin{array}{rlrr} 1, & \ldots, & p-1, & 1\cdot p \\ p+1, & \ldots, & p+p-1, & 2\cdot p \\ 2\cdot p+1, & \ldots, & 2\cdot p+p-1, & 3\cdot p \\ & \cdots\cdots & & \\ (p^{\alpha-1}-1)\cdot p+1, & \ldots, & (p^{\alpha-1}-1)\cdot p+p-1, & p^{\alpha-1}\cdot p \end{array} \quad (2)$$

其中与m 不互素的整数为

$$1\cdot p,\ \ 2\cdot p,\ \ \ldots,\ \ (p^{\alpha-1}-1)\cdot p,\ \ p^{\alpha-1}\cdot p, \quad (3)$$

共有$p^{\alpha-1}$ 个整数. 故m 个整数中与m 互素的整数个数为$p^\alpha - p^{\alpha-1}$. 即有(1)

证毕

例2.3.1 设$m = 7^2$. 则$\varphi(7^2) = 7^2(1-\frac{1}{7}) = 42.$

2.3.2 简化剩余类与简化剩余系

前面我们讨论了模同余, 以及模m 剩余类和完全剩余系. 在讨论中, 常常假定两个整数a, m 互素的条件, 即$(a,m)=1$.

现在我们讨论剩余与m 互素的剩余类的性质.

定义2.3.2 一个模m 的剩余类叫做**简化剩余类**, 如果该类中存在一个与m 互素的剩余. 这时, 简化剩余类中的剩余叫做**简化剩余**.

注:

1) 简化剩余类的这个定义与剩余的选取无关.

2) 两个简化剩余的乘积仍是简化剩余.

定理2.3.2 设r_1, r_2 是同一模m 剩余类的两个剩余, 则r_1 与m 互素的充分必要条件是r_2 与m 互素.

证 依题设, 存在整数q, 使得

$$r_1 = r_2 + q \cdot m.$$

所以, $(r_1, m) = (r_2, m)$. 故$(r_1, m) = 1$ 的充要条件是$(r_2, m) = 1$. 证毕

简化剩余系

模m 的简化剩余类的全体所组成的集合通常写成

$$(\mathbf{Z}/m\mathbf{Z})^* = \{C_a \mid 0 \le a \le m-1,\ (a, m) = 1\}. \tag{4}$$

特别地, 当$m = p$ 为素数时, 我们也写成

$$\mathbf{F}_p^* = (\mathbf{Z}/p\mathbf{Z})^* = \{C_1,\ \ldots,\ C_{p-1}\} = \mathbf{F}_p \setminus \{C_0\}. \tag{5}$$

定义2.3.3 设m 是一个正整数. 在模m 的所有不同简化剩余类中, 从每个类任取一个数组成的整数的集合, 叫做模m 的一个**简化剩余系**.

因为模m 的最小正完全剩余系$\{1,\ 2,\ \ldots,\ m-1,\ m\}$ 中, 与m 互素的整数全体构成模m 的简化剩余系, 所以模m 的简化剩余系的元素个数为$\varphi(m)$.

因此, $|(\mathbf{Z}/m\mathbf{Z})^*| = \varphi(m)$.

性质2.3.1 设$m > 1$ 是整数, $a,\ b$ 是模m 的两个简化剩余. 则它们的乘积也是简化剩余. **证** 直接由定理**??** 得到. 证毕

例2.3.4 设m 是一个正整数. 则

i) m 个整数$0,\ 1,\ \dots,\ m-1$ 中与m 互素的整数全体组成模m 的一个简化剩余系, 叫做模m的**最小非负简化剩余系**;

ii) m 个整数$1,\ \dots,\ m-1,\ m$ 中与m 互素的整数全体组成模m 的一个简化剩余系, 叫做模m的**最小正简化剩余系**;

iii) m 个整数$-(m-1),\ \dots,\ -1,\ 0$ 中与m 互素的整数全体组成模m 的一个简化剩余系, 叫做模m的**最大非正简化剩余系**;

iv) m 个整数$-m,\ -(m-1),\ \dots,\ -1$ 中与m 互素的整数全体组成模m 的一个简化剩余系, 叫做模m的**最大负简化剩余系**;

v) m 个整数$1,\ \dots,\ m-1,\ m$ 中与m 互素的整数全体组成模m 的一个简化剩余系, 叫做模m的**最小正简化剩余系**;

例2.3.4(续) 设m 是一个正整数. 则

vi) 当m 分别为偶数时, m 个整数

$$-\frac{m}{2},\ -\frac{m-2}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-2}{2},$$

或m 个整数

$$-\frac{m-2}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-2}{2},\ \frac{m}{2},$$

中与m 互素的整数全体组成模m 的一个简化剩余系,

当m 分别为奇数时,m 个整数

$$-\frac{m-1}{2},\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ \frac{m-1}{2}$$

中与m 互素的整数全体组成模m 的一个简化剩余系, 上述两个简化剩余系统称为模m 的一个**绝对值最小简化剩余系**.

例2.3.5 $1,\ 3,\ 7,\ 9$ 是模 10 的简化剩余系, $\varphi(10)=4$.

例2.3.6 $1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$ 是模 30 的简化剩余系, $\varphi(30)=8$.

例2.3.7 $1,\ 2,\ 3,\ 4,\ 5,\ 6$ 是模 7 的简化剩余系, $\varphi(7)=6$.

例2.3.8 当 $m=p$ 为素数时, $1,\ 2,\ \ldots,\ p-1$ 是模 p 的简化剩余系, 所以 $\varphi(p)=p-1$.

定理2.3.3 若 $r_1,\ \ldots,\ r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数, 并且两两模 m 不同余, 则 $r_1,\ \ldots,\ r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

证 依定理假设, 知 $\varphi(m)$ 个整数 $r_1,\ \ldots,\ r_{\varphi(m)}$ 是模 m 的所有不同简化剩余类的剩余. 故 $r_1,\ \ldots,\ r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

定理2.3.4 设 $(a,m)=1$. 如果 x 遍历模 m 的一个简化剩余系, 则 ax 也遍历模 m 的一个简化剩余系.

证 因为 $(a,m)=1$, $(x,m)=1$, 所以 $(ax,m)=1$. 这说明 ax 是简化剩余类的剩余. 又 $ax_1 \equiv ax_2 \pmod m$ 时, 有 $x_1 \equiv x_2 \pmod m$. 因此, x 遍历模 m 的一个简化剩余系时, ax 遍历 $\varphi(m)$ 个数, 且它们两两模 m 不同余. 根据定理 2, ax 遍历模 m 的一个简化剩余系.

例2.3.9 已知 1, 7, 11, 13, 17, 19, 23, 29 是模 30 的简化剩余系, $(7,30)=1$. 所以

$$\begin{array}{lll} 7\cdot 1 \equiv 7, & 7\cdot 7 = 49 \equiv 19, & 7\cdot 11 = 77 \equiv 17, \\ 7\cdot 13 = 91 \equiv 1, & 7\cdot 17 = 119 \equiv 29, & 7\cdot 19 = 133 \equiv 13, \\ 7\cdot 23 = 161 \equiv 11, & 7\cdot 29 = 203 \equiv 23 & \pmod{30}. \end{array}$$

因此, $7\cdot 1$, $7\cdot 7$, $7\cdot 11$, $7\cdot 13$, $7\cdot 17$, $7\cdot 19$, $7\cdot 23$, $7\cdot 29$ 是模 30 的简化剩余系.

例2.3.10 设 $m = 7$. 设 a 表示第一列数, 为与 m 互素的给定数. 设 x 表示第一行数, 遍历模 m 的简化剩余系. 设 a 所在行与 x 所在列的交叉位置表示 ax 模 m 最小非负剩余. 则我们得到如下的列表,

$a \setminus x$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

其中 a 所在行的数表示 ax 随 x 遍历模 m 的简化剩余系.

例2.3.11 设$m = 15$. 设a 表示第一列数, 为与m互素的给定数. 设k 表示第一行数, 遍历模m 的简化剩余系. 设a 所在行与k 所在列的交叉位置表示$a \cdot k$ 模m 最小非负剩余. 则我们得到如下的列表,

$a \setminus k$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

其中a 所在行的数表示$a \cdot k$ 随k 遍历模m 的简化剩余系.

$a \backslash k$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

$a \backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	0	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

定理2.3.5 设 $(a,m)=1$. 则存在整数 a', $1\le a'<m$ 使得

$$aa'\equiv 1 \pmod m.$$

证一 (存在性证明). 因为 $(a,m)=1$, 根据定理 3, x 遍历模 m 的一个最小简化剩余系时, ax 也遍历模 m 的一个简化剩余系. 因此, 存在整数 $x=a'$, $1\le a'<m$ 使得 aa' 属于 1 的剩余类, 即 $aa'\equiv 1 \pmod m$. 证毕.

因为在实际运用中, 我们常常需要具体地求出整数, 所以我们运用广义欧几里得除法给出定理2.3.5 的构造性证明.

证二 (构造性证明). 因为 $(a,m)=1$, 根据定理1.3.7, 运用广义欧几里得除法, 可找到整数 s, t 使得

$$sa+tm=(a,m)=1.$$

因此, 整数 $a'=s \pmod m$ 满足 $aa'\equiv 1 \pmod m$.

例2.3.12 设 $m = 7, a$ 表示与 m 互素的整数. 根据定理2.3.5, 我们得到相应的同余式:

$$1 \cdot 1 \equiv 1,\ \ 2 \cdot 4 \equiv 1,\ \ 3 \cdot 5 \equiv 1, \qquad (\bmod\ 7)$$
$$4 \cdot 2 \equiv 1,\ \ 5 \cdot 3 \equiv 1,\ \ 6 \cdot 6 \equiv 1, \qquad (\bmod\ 7).$$

例2.3.13 设 $m = 737,\ a = 635$. 根据例1.3.19, 由广义欧几里得除法, 可找到整数 $s = -224,\ t = 193$ 使得

$$(-224) \cdot 635 + 193 \cdot 737 = 1.$$

因此, $a' = -224 \equiv 513 \pmod{737}$ 使得

$$635 \cdot 513 \equiv 1 \pmod{737}.$$

2.3.3 两个模的简化剩余系

定理2.3.6 设m_1, m_2 是互素的两个正整数. 如果k_1, k_2 分别遍历模m_1 和模m_2的简化剩余系, 则

$$m_2 \cdot k_1 + m_1 \cdot k_2 \tag{6}$$

遍历模$m_1 \cdot m_2$的简化剩余系.

证 首先证明: $(k_1, m_1) = 1$, $(k_2, m_2) = 1$时,

$$(m_2 \cdot k_1 + m_1 \cdot k_2, m_1 \cdot m_2) = 1.$$

事实上, 因为$(m_1, m_2) = 1$, 根据定理1.3.3 和定理1.3.11, 我们有

$$(m_2 \cdot k_1 + m_1 \cdot k_2, m_1) = (m_2 \cdot k_1, m_1) = (k_1, m_1) = 1,$$

$$(m_2 \cdot k_1 + m_1 \cdot k_2, m_2) = (m_1 \cdot k_2, m_2) = (k_2, m_2) = 1,$$

因此, 再根据定理1.3.12, 我们得到

$$(m_2 \cdot k_1 + m_1 \cdot k_2, m_1 \cdot m_2) = 1.$$

其次, 证明模$m_1 \cdot m_2$的任一简化剩余可表示为(6), 其中$(k_1, m_1) = 1$, $(k_2, m_2) = 1$. 事实上, 根据定理2.2.4, 模$m_1 \cdot m_2$的任一剩余可以表示为:

$$m_2 \cdot k_1 + m_1 \cdot k_2.$$

因此, 当$(m_2 \cdot k_1 + m_1 \cdot k_2, m_1 \cdot m_2) = 1$时, 根据定理1.3.11 和定理1.3.3, 我们有

$$(k_1, m_1) = (m_2 \cdot k_1, m_1) = (m_2 \cdot k_1 + m_1 \cdot k_2, m_1) = 1.$$

同理, $(k_2, m_2) = 1$. 结论成立. 证毕

例2.3.14 设$m_1 = 14$, $m_2 = 15$. 则当k_1, k_2 分别遍历模m_1, m_2 的简化剩余系, $k_3 = m_2 \cdot k_1 + m_1 \cdot k_2$ 遍历模$m_1 \cdot m_2 = 210$ 的简化剩余系.

$k_1 \setminus k_3 \diagdown k_2$	1	2	4	7	8	11	13	14
1	29	43	71	113	127	169	197	1
3	59	73	101	143	157	199	17	31
5	89	103	131	173	187	19	47	61
9	149	163	191	23	37	79	107	121
11	179	193	11	53	67	109	137	151
13	209	13	41	83	97	139	167	181

2.3.4 欧拉函数的性质

从定理2.3.6 可推出欧拉函数 φ 的性质 (即 φ 是所谓的乘性函数).

定理2.3.7 设 m, n 是互素的两个正整数. 则

$$\varphi(mn) = \varphi(m)\varphi(n).$$

证 考虑形为

$$ym + xn$$

的整数. 根据定理2.3.6, 当 x 遍历模 m 的简化剩余系, 共 $\varphi(m)$ 个整数以及 y 遍历模 n 的简化剩余系, 共 $\varphi(m)$ 个整数时, $ym + xn$ 遍历模 mn 的简化剩余系, 其整数个数为 $\varphi(m)\varphi(n)$. 但模 mn 的简化剩余系的元素个数又为 $\varphi(mn)$. 因此, 所以 $\varphi(mn) = \varphi(m)\varphi(n)$.

例2.3.15 $\varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60.$

例2.3.16 $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = 1 \cdot 2 \cdot 4 = 8.$

定理2.3.8 设 n 有标准因数分解式为

$$n=\prod_{p|n}p^{\alpha}=p_1^{\alpha_1}\cdots p_k^{\alpha_s}.$$

则 $\varphi(n)=n\prod_{p|n}(1-\frac{1}{p})=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$

证 当 $n=p^{\alpha}$ 为素数幂时, 模 n 的完全剩余系为

$$0,\ 1,\ \ldots,\ p-1,\ldots\qquad p(p^{\alpha-1}-1),\ p(p^{\alpha-1}-1)+1,\ \ldots,\ p^{\alpha}-1,$$

共有 $n=p^{\alpha}$ 个整数, 其中与 n 不互素的整数为

$$p\cdot 0,\ \ p\cdot 1,\ \ \ldots,\ \ p(p^{\alpha-1}-1),$$

共有 $p^{\alpha-1}$ 个整数. 因此, 模 $n=p^{\alpha}$ 的简化剩余系元素个数为 $p^{\alpha}-p^{\alpha-1}$. 即 $\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$. 根据定理2.3.7, 有

$$\varphi(n)=\prod_{p|n}\varphi(p^{\alpha})=\prod_{p|n}(p^{\alpha}-p^{\alpha-1})=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k}).$$

推论 设 p, q 是不同的素数. 则 $\varphi(pq) = pq - p - q + 1$.

证明 由定理2.3.8, 有 $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = pq - p - q + 1$.

注 当 n 为合数, 且不知道 n 的因数分解式时, 通常很难求出 n 的欧拉函数值 $\varphi(n)$.

例2.3.17 设正整数 n 是两个不同素数的乘积. 如果知道 n 和欧拉函数值 $\varphi(n)$, 则可求出 n 的因数分解式.

证 考虑未知数 p, q 的方程组:

$$\begin{cases} p+q &= n+1-\varphi(n) \\ p\cdot q &= n. \end{cases}$$

根据多项式的根与系数之间的关系, 我们可以从二次方程

$$z^2 - (n+1-\varphi(n))z + n = 0$$

求出 n 的因数 p, q.

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院

下面进一步考虑欧拉函数的性质, 该性质将用于原根的构造.

定理2.3.9 设m 是一个正整数. 则

$$\sum_{d\,|\,m} \varphi(d) = m. \tag{7}$$

证 我们对m 个整数集$C = \{1, \dots, m\}$ 按照与m 的最大公因数进行分类.
对于正整数$d \mid m$, 记 $C_d = \{n \mid 1 \le n \le m,\ (n, m) = d\}$.
因为$(n, m) = d$的充要条件是$\left(\frac{n}{d}, \frac{m}{d}\right) = 1$, 所以$C_d$中元素$n$ 的形式为

$$C_d = \{n = k \cdot d \mid\ 1 \le k \le \frac{m}{d}, \quad (k, \frac{m}{d}) = 1\ \}.$$

因此, C_d 中的元素个数$\#(C_d)$ 为$\varphi\left(\frac{m}{d}\right)$. 因为整数$1, \dots, m$中的每个整数属于且仅属于一个类$C_d$, 所以

$$\#(C) = \sum_{d\,|\,m} \#(C_d) \quad \text{或} \quad m = \sum_{d\,|\,m} \varphi\left(\frac{m}{d}\right).$$

又d 遍历整数m 的所有正因数时, $\frac{m}{d}$ 也遍历整数m 的所有正因数. 故

$$m = \sum_{d\,|,m} \varphi\left(\frac{m}{d}\right) = \sum_{d\,|\,m} \varphi(d).$$

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院

例2.3.18 设整数 $n = 50$. 则 n 的正因数为 $d = 1,\ 2,\ 5,\ 10,\ 25,\ 50$. 这时, 定理2.3.9 的分类为:

$$C_1 = \{1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19,\ 21,\ 23,\ 27,\ 29,\ 31,\ 33,\ 37,\ 39,\ 41,\ 43,\ 47,\ 49\};$$

$$C_2 = \{2,\ 4,\ 6,\ 8,\ 12,\ 14,\ 16,\ 18,\ 22,\ 24,\ 26,\ 28,\ 32,\ 34,\ 36,\ 38,\ 42,\ 44,\ 46,\ 48\};$$

$$\begin{array}{ll} C_5 = \{5,\ 15,\ 35,\ 45\}; & c_{10} = \{10,\ 20,\ 30,\ 40\}; \\ C_{25} = \{25,\}; & C_{50} = \{50\}. \end{array}$$

这六类的元素个数分别为:

$$\begin{array}{ll} \#(C_1) = \varphi(50) = 20, & \#(C_2) = \varphi(25) = 20, \\ \#(C_5) = \varphi(10) = 4, & \#(C_{10}) = \varphi(5) = 4, \\ \#(C_{25}) = \varphi(2) = 1, & \#(C_{50}) = \varphi(1) = 1. \end{array}$$

验算, 有

$$50 = \varphi(50) + \varphi(25) + \varphi(10) + \varphi(5) + \varphi(2) + \varphi(1) = \sum_{d|50} \varphi(d).$$

例2.3.19 设整数 $n = 30$. 则 n 的正因数为 $d = 1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 15,\ 30$. 这时, 定理2.3.9 的分类为:

$$
\begin{aligned}
&C_1 = \{1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29\}; && c_2 = \{2,\ 4,\ 8,\ 14,\ 16,\ 22,\ 26,\ 28\};\\
&C_3 = \{3,\ 9,\ 21,\ 27\}; && c_5 = \{5,\ 25\};\\
&C_6 = \{6,\ 12,\ 18,\ 24\}; && c_{10} = \{10,\ 20\};\\
&C_{15} = \{15,\}; && C_{30} = \{30\}.
\end{aligned}
$$

这八类的元素个数分别为:

$$
\begin{aligned}
&\#(C_1) = \varphi(30) = 8, && \#(C_2) = \varphi(15) = 8,\\
&\#(C_3) = \varphi(10) = 4, && \#(C_5) = \varphi(6) = 2,\\
&\#(C_6) = \varphi(5) = 4, && \#(C_{10}) = \varphi(3) = 2.\\
&\#(C_{15}) = \varphi(2) = 1, && \#(C_{30}) = \varphi(1) = 1.
\end{aligned}
$$

验算, 有

$$30 = \varphi(30)+\varphi(15)+\varphi(10)+\varphi(6)+\varphi(5)+\varphi(3)+\varphi(2)+\varphi(1) = \sum_{d|30} \varphi(d).$$