数 学 年 刊 A 辑
2023, 44(2):211–224
DOI: 10.16205/j.cnki.cama.2023.0015

k-素数和唯一分解*

董平川[1] 董 浙[2] 姜海益[3]

提要 在本文中, 作者揭示了唯一 k-素因数分解的更深层原因. 在第二节中, 首先引入 S_k 中的 k-组合条件和费马定理; 并证明了下面 4 论断是等价的: (1) k-组合条件成立, (2) S_k 中唯一 k-素因数分解成立, (3) S_k 中费马定理成立, (4) $k=1$ 或 2. 为了更好地理解 k-素数, 在第三节中作者考察了一类特殊的 k-素数, 即 3-素数. 众所周知唯一 3-素因数分解一般是不成立的, 那么 S_3 中的哪些正整数具有唯一 3-素因数分解性质呢? 在第三节中, 作者得到一个 S_3 中的整数具有唯一 3-素因数分解的充要条件. 在第三节最后, 作者引入 $\pi_3(x)$, 它表示小于等于 x 的 3-素数个数. 由素数定理, 作者得到 $\pi_3(x)$ 的一个具体公式以及一些近似公式.

关键词 k-素数, 唯一 k-素因数分解, k-组合条件, 费马定理, 素数定理
MR (2000) 主题分类 11N05
中图法分类 O156.1
文献标志码 A
文章编号 1000-8314(2023)02-0211-14

§1 引言和准备知识

下述问题 3 来自文 [1].

问题 3 (1) S_4 中的哪些数是 4-素数? 举例说明唯一 4-素因数分解不成立;

(2) S_3 中的哪些数是 3-素数? 举例说明唯一 3-素因数分解不成立;

(3) 对哪些正整数 k, S_k 中的唯一 k-素因数分解成立?

这里 $S_k=\{tk+1 \mid t\in\mathbb{N}, t\geqslant 1\}$.

虽然从上述的问题 3 我们知道当 $k=3,4$ 时唯一 k-素因数分解不成立, 但是没有看到有相关的论文研究这种现象背后的原因. 我们对关于这种现象的下述问题颇感兴趣:

为什么唯一 k-素因数分解对于 3-素数或者 4-素数不成立而对于 1-素数或者 2-素数是成立的?

在本文中我们发现唯一 k-素因数分解的更深层次原因. 在第二节中, 通过深入研究经典的唯一素因数分解, 我们引入 S_k 中的 k-组合条件和费马定理. 本文的一个主要贡献是我们证明了 k-组合条件成立, S_k 中唯一 k-素因数分解, S_k 中费马定理成立和 $k=1$ 或 2 是等价的.

为了更好地理解 k-素数, 在第三节中我们考虑 k-素数的一种特殊情形, 即 3-素数. 当然我们可以用相似的方法研究其他 k-素数 ($k=4,5,6,\cdots$). 对于 3-素数来说, 我们知道唯

本文 2021 年 6 月 13 日收到, 2022 年 12 月 8 日收到修改稿.
[1]纽约大学数学系, 纽约 10012-1110, 美国. E-mail: pd2170@nyu.edu
[2]通信作者. 浙江大学数学科学学院, 杭州 310058. E-mail: dongzhe@zju.edu.cn
[3]浙江大学数学科学学院, 杭州 310058. E-mail: jianghaiyi@zju.edu.cn
*本文受到国家自然科学基金 (No. 11871423) 的资助.

一 3-素因数分解不成立. 但是我们可以问在 S_3 中哪些整数具有唯一 3-素因数分解? 在第三节中, 我们得到了一个 S_3 中的整数具有唯一 3-素因数分解的充要条件. 在第三节最后, 我们研究了 3-素数的个数, 它可以帮助我们更好地理解经典素数和 3-素数的不同. 对于经典素数, Legendre 和 Gauss 在十八世纪末分别给出了如下猜想 (称为素数定理):

$$\lim_{x\to+\infty}\frac{\pi(x)}{\frac{x}{\ln(x)}}=\lim_{x\to+\infty}\frac{\pi(x)}{li(x)}=1,$$

这里 $li(x)=\int_2^x\frac{\mathrm{d}t}{\ln(t)}$, $\pi(x)=\sum\limits_{\text{素数 }p\leqslant x}1$ 表示小于等于 x 的素数的个数. 这个猜想首先是由 Hadamard 和 Poussin 在 1896 年分别独立证明的. Selberg[2] 和 Erdös[3] 用初等方法在 1949 年分别独立证明了素数定理. 类似地, 我们引入 $\pi_3(x)=\sum\limits_{\substack{3-\text{ 素数 }p\\p\leqslant x}}1$, 它表示小于等于 x 的 3-素数的个数. 通过 3-素数的特征, 我们得到了关于 $\pi_3(x)$ 的一个具体公式, 通过这个公式我们能用素数的个数来计算 3-素数的个数. 作为推论, 我们得到了关于 $\pi_3(x)$ 的一些近似公式. 通过 Python 编程, 我们画出了关于 $\pi_3(x),\pi(x)$ 以及 $\pi_3(x)$ 的近似公式的两副图.

下面是一些基本概念和准备知识, 它们可以在任何一本关于初等数论的书中找到, 例如文 [4–8]. 这篇论文主要关注整数, 特别是正整数.

定义 1.1 如果存在一个整数 k, 使得 $a=kd$, 那么称 d 整除 a, 记作 $d\mid a$.

定义 1.2 若 a,b 为正整数, 整数 d 满足 $d\mid a$ 和 $d\mid b$ 并且如果 $c\mid a$ 和 $c\mid b$, 有 $d\geqslant c$, 那么称 d 为 a 和 b 的最大公因数, 记作 (a,b). 如果 $(a,b)=1$, 则称 a 与 b 互素.

定义 1.3 一个大于 1 的整数除了自身和 1 外没有其它的正因数称为素数. 一个大于 1 的整数如果不是素数就称为合数.

在下面的定理中, 我们列出在本文中经常用到的关于整除的一些性质.

定理 1.1 (1) (带余除法) 如果 a 和 b 是两个正整数, 那么一定存在两个唯一的整数 q 和 r, 使得 $a=bq+r$, $0\leqslant r<b$;

(2) 如果 $(a,b)=d$, 那么存在整数 x 和 y, 使得 $ax+by=d$;

(3) 如果 p 是一个素数且 $p\mid ab$, 则 $p\mid a$ 或 $p\mid b$;

(4) 如果 p 是一个素数且 $p\mid a_1a_2\cdots a_s$, 则存在某个 i $(1\leqslant i\leqslant s)$ 有 $p\mid a_i$;

(5) (唯一素因数分解) 每一个大于 1 的正整数 n 可以被写成一些素数的乘积, 并且在不考虑素因数的顺序的情况下这种分解是唯一的, 即有

$$n=q_1q_2\cdots q_s,$$

其中 $q_i(1\leqslant i\leqslant s)$ 都是素数, 这种分解被称作标准素因数分解;

(6) (素数幂分解) 在不考虑顺序的情况下, 每一个大于 1 的正整数 n 可以被唯一地写成如下形式:

$$n=p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t},$$

其中 $p_1, p_2, \cdots, p_t$ 为两两不同的素数.

著名的同余记号 $\equiv$ 是由 Gauss 引入的.

定义 1.4　如果 $m \mid (a-b)$, 则称 $a \equiv b(\bmod m)$ (a 与 b 模 m 同余).

关于同余有如下性质.

命题 1.1　设 a, b, c, d 为整数, 模为 m,
(1) 如果 $a \equiv b(\bmod m)$ 且 $c \equiv d(\bmod m)$, 则 $a+c \equiv b+d(\bmod m)$;
(2) 如果 $a \equiv b(\bmod m)$ 且 $c \equiv d(\bmod m)$, 则 $ac \equiv bd(\bmod m)$;
(3) 如果 $ac \equiv bc(\bmod m)$ 且 $(c, m) = d$, 则 $a \equiv b(\bmod \frac{m}{d})$.

§2　k-素数

设 k 是一个正整数, 令

$$S_k = \{n \in \mathbb{N} \mid n > 1,\ n \equiv 1(\bmod k)\}.$$

由命题 1.1 可得, S_k 关于乘法运算封闭, 即: 如果 $a, b \in S_k$, 则 $ab \in S_k$. 由 S_k 的定义, 我们有

$$S_1 = \{2, 3, 4, 5, \cdots\};$$
$$S_2 = \{3, 5, 7, 9, \cdots\};$$
$$S_3 = \{4, 7, 10, 13, \cdots\};$$
$$S_4 = \{5, 9, 13, 17, \cdots\};$$
$$S_k = \{tk+1 \mid t \in \mathbb{N}, t \geqslant 1\}.$$

引理 2.1　假设 a, b 是正整数且 $a \in S_k$, $b > 1$, 则 $ab \in S_k$ 当且仅当 $b \in S_k$.

证　我们仅需证明必要性. $k = 1$ 时显然. 下面我们不妨设 $k \geqslant 2$. 令 $b \equiv t(\bmod k)$ $(0 \leqslant t < k)$. 既然 $a \in S_k$, $a \equiv 1(\bmod k)$, 因此

$$ab \equiv t(\bmod k).$$

由 $ab \in S_k$ 可得

$$t \equiv 1(\bmod k).$$

此即 $k \mid t-1$. 由于 $-1 \leqslant t-1 < k-1$, 因此 $t-1 = 0 \times k = 0$. 于是 $t = 1$, 从而可得 $b \in S_k$.

定义 2.1　假设 $n \in S_k$, 如果 n 能被表示成 $n = ab$, 其中 $a, b \in S_k$, 则 n 被称作一个 k-合数, 否则称 n 是一个 k-素数.

由定义 2.1, 1- 素数就是经典的素数; 2- 素数就是经典的奇素数. 因为

$$S_3 = \{4, 7, 10, 13, 16, 19, 22, \cdots\},$$

我们知道某些经典的合数 (例如 $4, 10, 22, \cdots$) 都是 3- 素数. 这种现象隐含着 $k(\geqslant 3)$-素数可能具有和经典的 1-素数和 2-素数完全不同的性质. 在这一节中我们主要考虑 S_k 中的唯一 k-素因数分解和费马小定理.

我们首先回忆一下在 1837 年由 Dirichlet 用 L 函数理论证明的著名的 Dirichlet 定理. Selberg[9] 在 1949 年给出了 Dirichlet 定理的一个初等证明. 小于等于 x 的经典素数的个数记作 $\pi(x)$, 设 $\phi(x)$ 为欧拉函数.

定理 2.1 (Dirichlet 定理) 假设 k, r 是满足 $(k, r) = 1$ 的正整数, 则在算术数列 $mk + r (m \in \mathbb{N})$ 中存在无穷多个素数 p, 即存在无穷多个素数 $p \equiv r (\bmod k)$. 更进一步有, 对于 $\pi_{k,r}(x) = \sum\limits_{\substack{p \text{ 素数}, p \leqslant x \\ p \equiv r (\bmod k)}} 1$,

$$\pi_{k,r}(x) \sim \frac{\pi(x)}{\phi(k)}.$$

引理 2.2 S_k 中存在无穷多个 k-素数.

证 在上述 Dirichlet 定理 2.1 中令 $r = 1$, 则由 Dirichlet 定理 2.1 可推得存在无穷多个素数 $p \equiv 1 (\bmod k)$, 于是存在无穷多个素数 $p \in S_k$. 由定义 2.1 可得, S_k 中的每一个经典素数都是 k-素数. 因此 S_k 中存在无穷多个 k-素数.

引理 2.3 每一个 $n \in S_k$ 能被某个 k-素数整除.

证 如果 $n \in S_k$ 不是一个 k-素数, 那么 n 就是一个满足 $n = n_1 m_1$ 的 k-合数, 其中 $n_1, m_1 \in S_k$ 且 $k < n_1 < n$. 如果 n_1 不是一个 k-素数, 那么 $n_1 = n_2 m_2$, 其中 $n_2, m_2 \in S_k$ 且 $k < n_2 < n_1$. 如此做下去, 我们得到一列严格单调减少的 S_k 中的正整数数列 $n > n_1 > n_2 > \cdots > k$. 既然 S_k 中的正整数数列不可能永远严格单调递减下去, 因此我们最终能找到一个 k-素数整除 n.

命题 2.1 每一个 $n \in S_k$ 要么是一个 k-素数要么是一些 k-素数的乘积.

证 假设 $n \in S_k$ 是一个 k-合数, 由引理 2.3 可知 n 有一个 k-素因数 p_1. 于是 $n = p_1 n_1$ 且 $n > n_1$. 既然 n 是一个 k-合数, 则 $n_1 > 1$. 由引理 2.1 可得 $n_1 \in S_k$. 如果 n_1 还是一个 k-合数, 那么它会有一个 k-素因数 p_2 且 $n_1 = p_2 n_2$, 其中 $n_1 > n_2 > 1, n_2 \in S_k$. 故 $n = p_1 p_2 n_2$. 如果 n_2 仍然是一个 k-合数, 继续这个过程, 可生成 S_k 中的一个严格单调递减的数列 $n > n_1 > n_2 > \cdots > k$. 因为 S_k 中的正整数数列不可能无限地严格单调递减下去, 所以最终会得到 $n_s = p_{s+1}$ 是一个 k-素数. 从而有

$$n = p_1 n_1 = p_1 p_2 n_2 = \cdots = p_1 p_2 \cdots p_s n_s = p_1 p_2 \cdots p_s p_{s+1}.$$

定义 2.2 整数 $a, b \in S_k$ 的最大公共 k-因数记作 $(a, b)_k$, 它是整数 $d \in S_k$ 且满足 $d \mid a$, $d \mid b$ 以及如果 $c \mid a$, $c \mid b$ 且 $c \in S_k$, 则 $d \geqslant c$. 如果 $a, b (\in S_k)$ 在 S_k 中没有公共的 k-因数, 则我们称 a 和 b 在 S_k 中互素, 记作 $(a, b)_k = 1$.

例如当 $k=3$ 时, 若 $a=2\cdot 7^2\cdot 5^3\cdot 13\in S_3$ 和 $b=2\cdot 7\cdot 5^2\cdot 11\in S_3$, 则由定义可知 $(a,b)_3=7\cdot 5^2$ 以及 $(a,b)=2\cdot 7\cdot 5^2$.

由文 [1] 的问题 3(参见第一节), 我们知道关于 3-素数或 4-素数的唯一因数分解不成立. 事实上我们能够证明当正整数 $k\neq 1,2$ 时, S_k 关于 k-素数的唯一因数分解都不成立. 但是为什么关于 k-素数的唯一因数分解只对 $k=1,2$ 成立呢? 为了理解这种现象背后的原因, 我们追溯到因数分解证明的源头, 发现了产生这种现象的本质原因.

定义 2.3　(k-组合条件) 对于任意 $a,b\in S_k$, 存在整数 x 和 y, 使得 $(a,b)_k=ax+by$.

对于 $k=1$ 或者 2, k-组合条件是成立的, 这是经典的欧几里得算法 (又称辗转相除法) 的重要推论.

引理 2.4　假设 k-组合条件成立, 如果 $p\in S_k$ 是一个 k-素数, $a,b\in S_k$ 且 $p\mid ab$, 则 $p\mid a$ 或者 $p\mid b$.

证　既然 p 是一个 k-素数, 那么有 $(p,a)_k=p$ 或者 $(p,a)_k=1$. 第一种情形下有 $p\mid a$. 第二种情况下, 从 k-组合条件可知, 存在整数 x 和 y, 使得 $px+ay=1$, 于是有 $p(bx)+(ab)y=b$, 从而有 $p\mid b$.

推论 2.1　假设 k-组合条件成立, 如果 $p\in S_k$ 是一个 k-素数且 $p\mid a_1a_2\cdots a_s$, 其中 $a_j\in S_k$ $(1\leqslant j\leqslant s)$, 则存在某个 i $(1\leqslant i\leqslant s)$, 使得 $p\mid a_i$.

证　我们用数学归纳法证之. 当 $k=2$ 时, 由引理 2.4 知结论成立. 假设当 $s=t$ 时结论成立, 我们将证明当 $s=t+1$ 时结论成立. 假设 $p\mid a_1a_2\cdots a_ta_{t+1}$, 即 $p\mid (a_1a_2\cdots a_t)a_{t+1}$. 于是由引理 2.4, 可得

$$p\mid a_1a_2\cdots a_t \quad \text{或者} \quad p\mid a_{t+1}.$$

第一种情形下, 有 $p\mid a_1a_2\cdots a_t$, 从而由归纳假设可得存在某个 i $(1\leqslant i\leqslant t)$, 使得 $p\mid a_i$; 第二种情形下, 有 $p\mid a_i$, 其中 $i=t+1$. 因此, 无论是哪种情形, 都存在 i $(1\leqslant i\leqslant t+1)$, 使得 $p\mid a_i$.

引理 2.5　如果 $k\geqslant 3$ 且有两个素数 p_i $(i=1,2)$ 满足 $p_i\equiv k-1(\mathrm{mod}\ k)$, 则 $n=p_1p_2$ 是 S_k 中的一个 k-素数.

证　既然 $n=p_1p_2\equiv (k-1)^2(\mathrm{mod}\ k)\equiv 1(\mathrm{mod}\ k)$, 那么 $n=p_1p_2\in S_k$. 假设 $n=p_1p_2$ 不是一个 k-素数, 则存在 $a,b\in S_k$, 使得 $n=ab$. 于是 $p_1\mid ab$. 由定理 1.1 得 $p_1\mid a$ 或者 $p_1\mid b$. 不失一般性, 我们不妨设 $p_1\mid a$, 于是 $a=p_1q$. 如果 $q>1$, 我们有

$$n=p_1p_2=ab=p_1qb.$$

从而有 $p_2=qb$, 这与 p_2 是一个素数矛盾. 如果 $q=1$, 则 $p_1=a\equiv 1(\mathrm{mod}\ k)$. 由于 $k-1\geqslant 2$, 那么与 $p_1\equiv k-1(\mathrm{mod}\ k)$ 矛盾. 因此 $n=p_1p_2$ 是一个 k-素数.

定理 2.2　下述论断是等价的:

(1) k-组合条件成立;

(2) S_k 中唯一 k-素因数分解成立;

(3) $k=1$ 或者 2.

证 (1)⇒(2) 对于 $n\in S_k$, 由命题 2.1 可得 n 能被写成 k-素数的乘积. 假设 n 能用两种不同的方式写成 k-素数的乘积如下:

$$n=p_1p_2\cdots p_t=q_1q_2\cdots q_s.$$

因为 $p_1\mid q_1q_2\cdots q_s$, 由推论 2.1 可得存在某个 i $(1\leqslant i\leqslant s)$, 使得 $p_1\mid q_i$. 令 $q_i=n_1p_1$. 如果 $n_1>1$, 由引理 2.1 可得 $n_1\in S_k$. 于是 q_i 是一个 k-合数. 这个矛盾推出 $n_1=1$ 以及存在某个 i $(1\leqslant i\leqslant s)$, 使得 $p_1=q_i$. 因此这些因数可以被删除, 于是得到

$$p_2\cdots p_t=q_1\cdots q_{i-1}q_{i+1}\cdots q_s.$$

类似地我们可以得到 p_2 等于剩下的 q 中的一个, 从而也可以被删除. 如此继续下去, 我们得到 p 中的每一个正好是 q 中的一个. 当我们删除完这些 p 后, 就没有 q 剩下来了. 于是乘积中具有相同的因数, 可能顺序会有所不同. 因此此时 S_k 关于 k-素数具有唯一因数分解.

(2)⇒(3) 假设 S_k 关于具有唯一 k-素因数分解, 又设 $k\geqslant 3$, 于是 $(k,k-1)=1$. 由 Dirichlet 定理 2.1 可得存在无穷多个素数 p, 使得 $p\equiv k-1(\bmod k)$. 选取两个素数 p_i $(i=1,2)$ 满足 $p_i\equiv k-1(\bmod k)$ 且 $p_1\neq p_2$, 由引理 2.5 可得, 对于 $n=p_1^2p_2^2\in S_k$, 存在两个不同的 k-素因数分解如下:

$$n=(p_1p_1)\cdot(p_2p_2)=(p_1p_2)\cdot(p_1p_2).$$

由此可得 $k=1$ 或者 2.

(3)⇒(1) 我们知道 1-素数就是经典的素数以及 2-素数就是经典的奇素数. 因此对于 $k=1$ 或者 2, k-组合条件成立是众所周知的 (参见定理 1.1).

在第二节的剩下部分, 我们将引入 S_k 中的费马定理, 并在 S_k 中研究唯一 k-素因数分解和费马定理之间的关系. 经典的费马定理有时被叫做费马小定理, 以示与费马大定理 (以 x,y,z 为未知数的代数方程 $x^n+y^n=z^n(n>2,n\in\mathbb{N})$ 没有正整数解) 有所区别. 首先我们回顾一下经典的费马定理.

定理 2.3 (费马定理) 如果 p 是一个素数且 a 是一个满足 $(a,p)=1$ 的正整数, 那么 $a^{p-1}\equiv 1(\bmod p)$.

那么 S_k 中的费马定理会是什么呢?

S_k 中的费马定理 如果 p 是 S_k 中的一个 k-素数且 $a\in S_k$ 是一个满足 $(a,p)_k=1$ 的正整数, 那么 $a^{p-1}\equiv 1(\bmod p)$.

定理 2.4 如果 k 是一个正整数, 那么 S_k 中的费马定理成立当且仅当 $k=1$ 或者 2.

证 我们仅需证明必要性. 假设 $k\geqslant 3$, 于是 $(k,\,k-1)=1$. 由 Dirichlet 定理 2.1 可得, 存在无穷多个 q, 使得 $q\equiv k-1(\bmod k)$. 选取两个素数 p_i $(i=1,2)$ 满足 $p_i\equiv k-1(\bmod k)$ 且 $p_1\neq p_2$. 令 $p=p_1^2$ 以及 $a=p_1p_2$. 由引理 2.5 可知 $a,p\in S_k$ 且都是 k-素数. 又

$(a,p)_k=1$ 以及 $(a,p)=p_1$. 由于我们假设 S_k 中的费马定理成立, 那么

$$a^{p-1}\equiv 1(\operatorname{mod} p),$$

即有

$$\text{存在某个整数 } m, \text{ 使得} a^{p-1}=1+mp.$$

因此 $p_1 \mid a^{p-1}-mp=1$. 这个矛盾可推得 $k=1$ 或者 2.

结合定理 2.2 和定理 2.4 我们可直接得到本文的一个主要结果.

推论 2.2　假设 k 是一个正整数, 则下述论断是等价的:

(1) k-组合条件成立;

(2) S_k 中唯一 k-素因数分解成立;

(3) S_k 中的费马定理成立;

(4) $k=1$ 或者 2.

§3　3- 素数

为了更好地理解 k-素数, 本节我们将专门讨论一类特殊的 k-素数, 即 3-素数.

定理 3.1　假设 $n\in S_3$ 以及 $n=p_1p_2\cdots p_s$ 是标准的素因数分解, 则 n 是一个 3-素数当且仅当

(1) $s=1$ 且 $p_1\equiv 1(\operatorname{mod} 3)$;

(2) $s=2$ 且 $p_i\equiv 2(\operatorname{mod} 3)$ $(i=1,2)$.

证　当 $s=1$ 时充分性是显然的. 现在考虑 $s=2$, 设 $n=p_1p_2$ 且满足 $p_i\equiv 2(\operatorname{mod} 3)$, 则由引理 2.5 可直接得到 n 是一个 3-素数.

下面我们来证明必要性. 假设 $n=p_1p_2\cdots p_s\in S_3$ 是一个 3-素数. 下面我们分情况讨论:

(1) $s=1$. 既然 $n=p_1\in S_3$, 则我们有 $p_1\equiv 1(\operatorname{mod} 3)$;

(2) $s=2$. 这时, $n=p_1p_2\in S_3$ 是一个 3-素数. 由于 $n\in S_3$, 则每一个 $p_i\not\equiv 0(\operatorname{mod} 3)$, 此时有如下两种情况:

(a) 如果对于 $i=1,2$, 其中有一个 $p_i\equiv 1(\operatorname{mod} 3)$ (不妨设 $p_1\equiv 1(\operatorname{mod} 3)$), 那么由引理 2.1 可得 $p_2\equiv 1(\operatorname{mod} 3)$. 于是 $n=p_1p_2$ 是一个 3-合数, 这是一个矛盾.

(b) 如果每一个 $p_i\equiv 2(\operatorname{mod} 3)$, 那么 $p_i\notin S_3$ 且 $n=p_1p_2\equiv 4(\operatorname{mod} 3)\equiv 1(\operatorname{mod} 3)$.

(3) $s\geqslant 3$. 这时, $n=p_1p_2\cdots p_s\in S_3$ 是一个 3-素数. 既然 $n\in S_3$, 则每一个 $p_i\not\equiv 0(\operatorname{mod} 3)$. 此时有如下两种情况:

(a) 如果对于 $i=1,2,\cdots,s$, 其中有一个 $p_i\equiv 1(\operatorname{mod} 3)$ (不妨设 $p_1\equiv 1(\operatorname{mod} 3)$), 那么由引理 2.1 可得 $p_2\cdots p_s\in S_3$. 于是 $n=p_1\cdot(p_2\cdots p_s)$ 是一个 3-合数, 这是一个矛盾.

(b) 如果每一个 $p_i\equiv 2(\operatorname{mod} 3)$, 那么 $p_1p_2\equiv 1(\operatorname{mod} 3)$ 且 $p_1p_2\in S_3$. 再次由引理 2.1 可得 $p_3\cdots p_s\in S_3$ (由于 $s\geqslant 3$). 于是 $n=(p_1p_2)\cdot(p_3\cdots p_s)$ 是一个 3-合数, 这是一个矛盾.

结合 (1)–(3), 我们得到如果 $n = p_1p_2\cdots p_s \in S_3$ 是一个 3-素数, 那么 $s = 1$ 且 $p_1 \equiv 1(\mathrm{mod}\ 3)$ 或者 $s = 2$ 且 $p_i \equiv 2(\mathrm{mod}\ 3)$ $(i = 1, 2)$.

推论 3.1 假设 $n \in S_3$ 以及 $n = p_1p_2\cdots p_s$ 是标准的素因数分解, 则 n 是一个 3-合数当且仅当 $s = 2$ 且 $p_i \equiv 1(\mathrm{mod}\ 3)$ $(i = 1, 2)$ 或者 $s \geqslant 3$.

例 3.1 由于 $685 = 5 \times 137$ 是标准的素因数分解以及 $5, 137 \equiv 2(\mathrm{mod}\ 3)$, 由定理 3.1 可知 685 是一个 3-素数;

$2275 \in S_3$ 且 $2275 = 5 \times 5 \times 7 \times 13$ 是标准的素因数分解, 由推论 3.1 可知 2275 是一个 3-合数.

由推论 2.2 我们知道关于 3-素数的唯一因数分解一般是不成立的, 但推论 2.2 没有给出一个具体判别 S_3 中的哪些整数具有关于 3-素数的唯一因数分解的方法. 通过分析一些特殊的例子, 我们得到了下述判别定理.

定理 3.2 假设 $n \in S_3$ 和 $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$, 其中 $p_1, p_2, \cdots, p_t$ 为不同的素数 (素数幂分解), 令 $P = \{p_i \mid p_i \equiv 2(\mathrm{mod}\ 3), 1 \leqslant i \leqslant t\}$, 则 n 在不考虑顺序的情况下能唯一地表示成 3-素数的乘积当且仅当 $\mathrm{card}(P) = 0, 1$ 或者 $\mathrm{card}(P) = 2, P = \{p_{i_1}, p_{i_2}\}$ 且 $\{e_{i_1}, e_{i_2}\}$ 中至少有一个是 1.

证 充分性. 如果 $\mathrm{card}(P) = 0$, 那么 $n \in S_3$ 推出每一个 $p_i \equiv 1(\mathrm{mod}\ 3)$ $(1 \leqslant i \leqslant t)$. 于是每一个素数 p_i 都是 3-素数. 从而 n 能写成 3-素数的乘积

$$n = \underbrace{p_1\cdots p_1}_{e_1}\underbrace{p_2\cdots p_2}_{e_2}\cdots\underbrace{p_t\cdots p_t}_{e_t}.$$

类似于下面 $\mathrm{card}(P) = 1$ 的情形, 我们可以证明上述表达式在不考虑顺序的情况下是唯一的.

如果 $\mathrm{card}(P) = 1$, 不失一般性我们假设 $P = \{p_1 \mid p_1 \equiv 2(\mathrm{mod}\ 3)\}$. $n \in S_3$ 可推出 e_1 是偶数. 由定理 3.1 得 $p_1^2 \in S_3$ 是一个 3-素数且每一个素数 p_i $(2 \leqslant i \leqslant t)$ 都是 3-素数. 于是 n 能被写成 3-素数的乘积

$$n = \underbrace{p_1^2\cdots p_1^2}_{\frac{e_1}{2}}\underbrace{p_2\cdots p_2}_{e_2}\cdots\underbrace{p_t\cdots p_t}_{e_t}.$$

接下来我们将证明在不考虑顺序的情况下上述表达式是唯一的. 假设 $n = q_1q_2\cdots q_s$ 是 3-素数的另一种分解表达式. 于是

$$n = \underbrace{p_1^2\cdots p_1^2}_{\frac{e_1}{2}}\underbrace{p_2\cdots p_2}_{e_2}\cdots\underbrace{p_t\cdots p_t}_{e_t} = q_1q_2\cdots q_s. \tag{3.1}$$

既然 $p_2 \mid q_1q_2\cdots q_s$, 则由定理 1.1 可得存在某个 j_0, 使得 $p_2 \mid q_{j_0}$. 假设 $q_{j_0} = p_2q$. 如果 $q > 1$, 那么由引理 2.1 可推得 $q \in S_3$, 从而 q_{j_0} 是一个 3-合数. 这个矛盾推得存在某个 j_0 使得 $p_2 = q_{j_0}$. 于是 p_2 和 q_{j_0} 可在方程 (3.1) 的两边同时消去. 如此继续做下去, 我们可以得到 p_i $(2 \leqslant i \leqslant t)$ 中的每一个都是 q_j $(1 \leqslant j \leqslant s)$ 中的一个. 当我们将 p_i $(2 \leqslant i \leqslant t)$ 中

的元素消除完毕, 我们就可以将方程 (3.1) 变为

$$\underbrace{p_1\cdots p_1}_{e_1}=q_{j_1}\cdots q_{j_k}, \tag{3.2}$$

而 $p_1\mid q_{j_1}\cdots q_{j_k}$ 可推出存在某个 l, $1\leqslant l\leqslant k$, 使得 $p_1\mid q_{j_l}$. 既然 q_{j_l} 是一个 3-素数, 则由定理 3.1 以及 $p_1\equiv 2(\bmod 3)$ 可证得 $q_{j_l}=p_1\cdot p_1'$, 其中 p_1' 是素数且 $p_1'\equiv 2(\bmod 3)$. 于是 $p_1'\mid \underbrace{p_1\cdots p_1}_{e_1}$, 从而 $p_1'=p_1$. 于是有 $q_{j_l}=p_1^2$, 这样我们可以在方程 (3.2) 的两边同时消去 q_{j_l} 和 p_1^2. 如此持续地做下去, 我们可以得到 p_1^2 就是 $q_{j_x}(1\leqslant x\leqslant k)$ 中的一个. 当我们把 p_1^2 ($\underbrace{p_1\cdots p_1}_{e_1}=(p_1^2)^{\frac{e_1}{2}}$) 消除完毕, 则没有 $q_{j_x}(1\leqslant x\leqslant k)$ 可剩下. 因此得到在 $\operatorname{card}(P)=1$ 情形 3-素数的分解是唯一的.

如果 $\operatorname{card}(P)=2$ 且 $P=\{p_{i_1},p_{i_2}\}$, $\{e_{i_1},e_{i_2}\}$ 中至少有一个是 1, 不失一般性, 我们假设 $P=\{p_1,p_2\}$ 且 $e_1=1$. $n\in S_3$ 可推得 e_2 是奇数. 由定理 3.1 可得 p_1p_2, p_2^2 以及每一个 p_i $(3\leqslant i\leqslant t)$ 都是 3-素数. 类似于 $\operatorname{card}(P)=1$ 的情形, 我们可以证明 n 能唯一地写成 3-素数的乘积, 即有

$$n=(p_1p_2)\cdot\underbrace{p_2^2\cdots p_2^2}_{\frac{e_2-1}{2}}\underbrace{p_3\cdots p_3}_{e_3}\cdots\underbrace{p_t\cdots p_t}_{e_t}.$$

必要性. 假设对于 n 来说 3-素数乘积分解是唯一的.

(1) $\operatorname{card}(P)=r\geqslant 4$. 不失一般性, 我们可以假设

$$P=\{p_1,p_2,p_3,p_4,\cdots,p_r\}.$$

$n\in S_3$ 可推得 $e_1+e_2+\cdots+e_r$ 是偶数. 于是我们有

$$n=p_1p_2p_3p_4n_1.$$

因为 $p_1p_2p_3p_4\equiv 1(\bmod 3)$, 由引理 2.1 可得 $n_1\in S_3$. 由命题 2.1 知, n_1 能被写成 3-素数的乘积

$$n_1=q_1\cdots q_s.$$

于是由定理 3.1 可知 n 能用下述两种不同的方式表示成 3-素数的乘积:

$$n=(p_1p_2)(p_3p_4)q_1\cdots q_s=(p_1p_3)(p_2p_4)q_1\cdots q_s.$$

(2) $\operatorname{card}(P)=3$. 不失一般性, 我们可以假设 $P=\{p_1,p_2,p_3\}$ 且 $e_1+e_2+e_3\geqslant 4$ 与 $e_1\geqslant 2$ 都是偶数. 于是我们有

$$n=p_1^2p_2p_3n_1.$$

接下来的证明和上述 (1) 中的证明完全相同.

(3) $\operatorname{card}(P)=2$. 我们假设 $P=\{p_1,p_2\}$ 且 $e_1\geqslant e_2>1$. $n\in S_3$ 可推出 e_1+e_2 是偶数, 从而 e_1,e_2 有相同的奇偶性. 由定理 3.1 知, p_1p_2, p_1^2 以及 $p_2^2\in S_3$ 都是 3-素数. 我们有下述四种情形:

(a) $e_1=e_2>1$ 为偶数. 由定理 3.1 可得 n 能用下述两种不同的方式表示成 3-素数的乘积:

$$\begin{aligned} n &= \underbrace{(p_1p_2)\cdots(p_1p_2)}_{e_1}\underbrace{p_3\cdots p_3}_{e_3}\cdots\underbrace{p_t\cdots p_t}_{e_t} \\ &= \underbrace{(p_1^2)\cdots(p_1^2)}_{\frac{e_1}{2}}\underbrace{(p_2^2)\cdots(p_2^2)}_{\frac{e_2}{2}}\underbrace{p_3\cdots p_3}_{e_3}\cdots\underbrace{p_t\cdots p_t}_{e_t}. \end{aligned}$$

(b) $e_1=e_2>1$ 为奇数.

(c) $e_1>e_2>1$ 为偶数.

(d) $e_1>e_2>1$ 为奇数.

在上述情形 (b)–(d) 中我们可以类似地证明 n 可以用两种不同的方式表示成 3-素数的乘积.

由 (1), (2) 以及 (3) 可得 $\mathrm{card}(P)=0,1$ 或者 $\mathrm{card}(P)=2, P=\{p_{i_1},p_{i_2}\}$ 且 $\{e_{i_1},e_{i_2}\}$ 中至少有一个是 1.

例 3.2 $2275=5^2\times 7\times 13$ 是 2275 的素数幂分解且 $P=\{5\}$. 由定理 3.2 直接可得 2275 有唯一 3-素因数分解, 即 $2275=7\times 13\times 25$, 这里 $7,13,25$ 都是 S_3 中的 3-素数;

$3850=2\times 5^2\times 7\times 11$ 是 3850 的素数幂分解且 $P=\{2,5,11\}$. 由定理 3.2 可知关于 3-素数的唯一因数分解不成立. 事实上,

$$3850=7\times 22\times 25=7\times 10\times 55,$$

这里 $7,10,22,25,55$ 都是 S_3 中的 3-素数.

在本节的末尾, 我们打算估计一下 3-素数的个数. 下述是小于 1000 的 3-素数表 (通过 Python 编程计算所得):

4, 7, 10, 13, 19, 22, 25, 31, 34, 37, 43, 46, 55, 58, 61, 67, 73, 79, 82, 85, 94, 97, 103, 106, 109, 115, 118, 121, 127, 139, 142, 145, 151, 157, 163, 166, 178, 181, 187, 193, 199, 202, 205, 211, 214, 223, 226, 229, 235, 241, 253, 262, 265, 271, 274, 277, 283, 289, 295, 298, 307, 313, 319, 331, 334, 337, 346, 349, 355, 358, 367, 373, 379, 382, 391, 394, 397, 409, 415, 421, 433, 439, 445, 451, 454, 457, 463, 466, 478, 487, 493, 499, 502, 505, 514, 517, 523, 526, 529, 535, 538, 541, 547, 562, 565, 571, 577, 583, 586, 601, 607, 613, 619, 622, 631, 634, 643, 649, 655, 661, 667, 673, 685, 691, 694, 697, 706, 709, 718, 727, 733, 739, 745, 751, 757, 766, 769, 778, 781, 787, 799, 802, 811, 823, 829, 835, 838, 841, 853, 859, 862, 865, 877, 883, 886, 895, 898, 901, 907, 913, 919, 922, 934, 937, 943, 955, 958, 967, 979, 982, 985, 991, 997.

对于经典素数的情形, Legendre 和 Gauss 在十八世纪末分别给出了如下猜测:

$$\lim_{x\to+\infty}\frac{\pi(x)}{\frac{x}{\ln(x)}}=\lim_{x\to+\infty}\frac{\pi(x)}{li(x)}=1,$$

这里 $li(x)=\int_2^x\frac{\mathrm{d}t}{\ln(t)}$ 以及 $\pi(x)=\sum\limits_{\text{素数 } p\leqslant x}1$, $\pi(x)$ 表示个数小于等于 x 的素数的个数. 上述断言现在以素数定理扬名世界, 在 1896 年 Hadamard 和 Poussin 分别独立地给出了证

明. Selberg 和 Erdös 在 1949 年分别独立地给出了素数定理的初等证明. 值得一提的是 Selberg 在次年获得了 Fields 奖而 Erdös 也在 35 年后获得了 Wolf 奖.

我们引入 $\pi_3(x) = \sum\limits_{\substack{3-\text{素数 } p\\ p\leqslant x}} 1$, 它表示小于等于 x 的 3-素数的个数. 我们回忆一下在 Dirichlet 定理 2.1 中 $\pi_{3,r}(x) = \sum\limits_{\substack{p\ \text{素数}, p\leqslant x\\ p\equiv r(\mathrm{mod}\ 3)}} 1$. 由定理 3.1, 我们知道 3-素数具有两种不同的型. 因此我们可以得到 $\pi_3(x)$ 的一个公式, 利用它我们可以通过素数的个数来计算 3-素数的个数.

定理 3.3　对于 $x\in S_3$, 我们有关于 $\pi_3(x)$ 的下述公式:

$$\pi_3(x) = \pi_{3,1}(x) + \sum_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}} \Big(\pi_{3,2}\Big(\Big[\frac{x}{p}\Big]\Big) - \pi_{3,2}(p-1)\Big),$$

其中 $[\cdot]$ 表示取整函数.

证　由定理 3.1 可得

$$\pi_3(x) = \pi_{3,1}(x) + \sum_{\substack{p_1p_2\leqslant x, p_1\leqslant p_2\\ \text{素数 } p_i\equiv 2(\mathrm{mod}\ 3)}} 1. \tag{3.3}$$

令

$$\begin{aligned} S &= \{p_1\cdot p_2 \mid p_1\cdot p_2\leqslant x, p_1\leqslant p_2,\ \text{素数 } p_i\equiv 2(\mathrm{mod}\ 3)\}\\ &= \bigcup_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}} \Big\{p\cdot q \mid \text{素数 } q\equiv 2(\mathrm{mod}\ 3) \text{ 且 } p\leqslant q\leqslant \Big[\frac{x}{p}\Big]\Big\}. \end{aligned}$$

因此由 $\pi_{3,2}(x)$ 的定义, 可得

$$\mathrm{card}(S) = \sum_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}} \Big(\pi_{3,2}\Big(\Big[\frac{x}{p}\Big]\Big) - \pi_{3,2}(p-1)\Big).$$

结合方程 (3.3), 我们可以得到如下结果:

$$\pi_3(x) = \pi_{3,1}(x) + \sum_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}} \Big(\pi_{3,2}\Big(\Big[\frac{x}{p}\Big]\Big) - \pi_{3,2}(p-1)\Big).$$

例 3.3　对于 $x = 268\in S_3$, $\pi_{3,1}(268) = 24$. 若素数 p 在区间 $[2, [\sqrt{268}]] = [2, 16]$ 上且满足 $p\equiv 2(\mathrm{mod}\ 3)$, 则 $p = 2, 5, 11$. 于是有

$$\begin{aligned} &\pi_{3,2}\Big(\Big[\frac{268}{2}\Big]\Big) - \pi_{3,2}(2-1) = \pi_{3,2}(134) - 0 = 18,\\ &\pi_{3,2}\Big(\Big[\frac{268}{5}\Big]\Big) - \pi_{3,2}(5-1) = \pi_{3,2}(53) - 1 = 8 \end{aligned}$$

以及

$$\pi_{3,2}\Big(\Big[\frac{268}{11}\Big]\Big) - \pi_{3,2}(11-1) = \pi_{3,2}(24) - 2 = 3.$$

从而由定理 3.3 有 $\pi_3(268)=24+18+8+3=53$. 对照例 3.2 后的 3-素数表进行检验, 发现 $\pi_3(268)=53$ 是正确的.

由 Dirichlet 定理和素数定理, 我们可以得到如下关于 $\pi_3(x)$ 的一些近似公式.

推论 3.2 对于 $x\in S_3$, 我们有下述关于 $\pi_3(x)$ 的近似公式:

(1) $\pi_3(x)\approx\frac{1}{2}\cdot\Big\{\pi(x)+\sum\limits_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}}\Big(\pi\Big(\Big[\frac{x}{p}\Big]\Big)-\pi(p-1)\Big)\Big\}$;

(2) $\pi_3(x)\approx\frac{1}{2}\cdot\Big\{\frac{x}{\ln x}+\sum\limits_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}}\Big(\frac{[\frac{x}{p}]}{\ln[\frac{x}{p}]}-\frac{p-1}{\ln(p-1)}\Big)\Big\}$;

(3) $\pi_3(x)\approx\frac{1}{2}\cdot\Big\{li(x)+\sum\limits_{\substack{2\leqslant p\leqslant[\sqrt{x}]\\ \text{素数 } p\equiv 2(\mathrm{mod}\ 3)}}\Big(li\Big(\Big[\frac{x}{p}\Big]\Big)-li(p-1)\Big)\Big\}$, 这里 $li(x)=\int_2^x\frac{\mathrm{d}t}{\ln(t)}$.

证 (1) 由 Dirichlet 定理 2.1, 我们知道对于任意的正整数 y, 有

$$\pi_{3,1}(y)\sim\frac{\pi(y)}{\phi(3)}=\frac{\pi(y)}{2}\quad 且\quad \pi_{3,2}(y)\sim\frac{\pi(y)}{\phi(3)}=\frac{\pi(y)}{2}.$$

于是近似公式可由定理 3.3 得到.

(2) 和 (3) 这两个近似公式可由 (1) 以及素数定理直接得到.

通过 Python 编程, 我们画了图 1– 图 2 帮助我们从直观和视觉方面来了解 3-素数. 图 1 展示了 $\pi(x)$ 与 $\pi_3(x)$ 之间的差异.

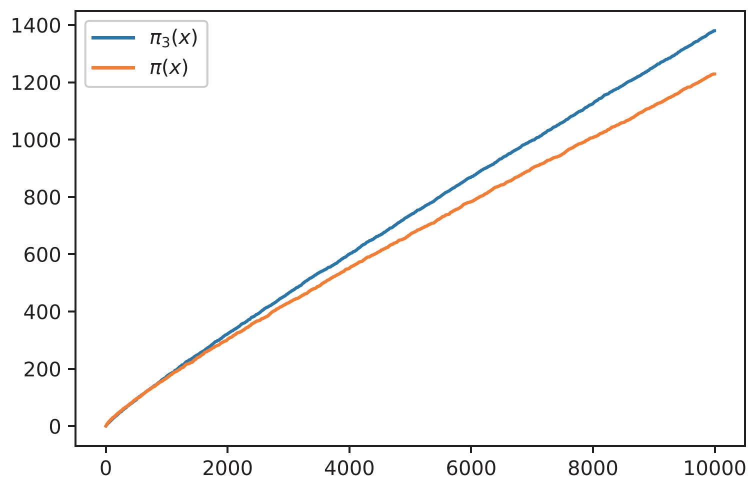

图 1

在图 2 中, 曲线 (1), (2) 以及 (3) 分别对应推论 3.2 中的三个近似公式. 从图 2 我们可以看出推论 3.2 中的第二个近似公式当 $x\leqslant 10000$ 时表现最佳.

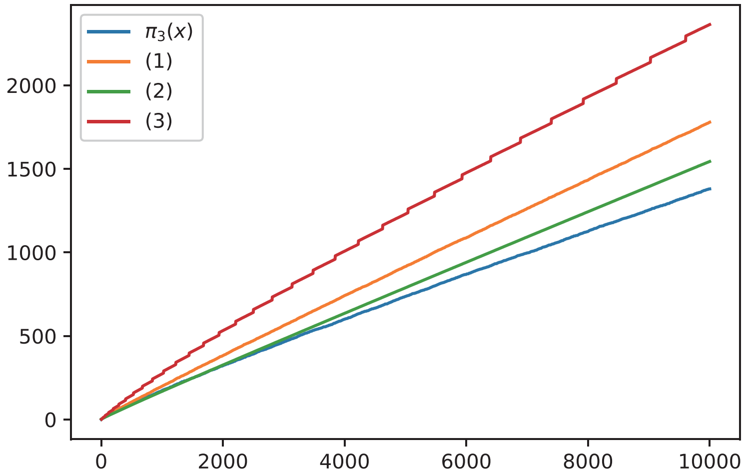

图 2

但是直到现在为止, 在推论 3.2 中我们还不能用符号 $\sim$ 替代符号 $\approx$, 其中符号 $\sim$ 表示当 x 趋向于无穷时两边的比值趋向于 1. 如果这是正确的, 那么推论 3.2 就可以称作 3-素数定理. 这也将成为我们未来更深入研究的主题.

参　考　文　献

[1] Ross program 2019 application problems. http://rossprogram.org/applications/2019/problems.pdf.

[2] Selberg A. An elementary proof of the prime number theorem [J]. *Ann of Math*, 1949, 50:305–313.

[3] Erdös P. On a new method in elementary number theory which leads to an elementary proof of the prime number theorem [J]. *Proc Nat Acad Sci Amer*, 1949, 35:374–384.

[4] Cai T X, The book of numbers [M]. Singapore: World Scientific Publishing Co Pre Ltd, 2017.

[5] Dudley U. A guide to elementary number theory [M]//Dolciani Mathematical Expositions, 41, MAA Guides 5, Washington: The Mathematical Association of America, 2009.

[6] Rosen K H. Elementary number theory and its application. Sixth Edition [M]. Pearson Education Inc, Boston: Addison Wesley Longman, 2011.

[7] Guy R K. Unsolved problems in number theory, Third Version [M]. Beijing: Springer Science, 2007.

[8] Klee V, Wagon S. 平面几何与数论中未解决的新老问题 [M]. 阚家海 (译), 哈尔滨: 哈尔滨工业大学出版社, 2013.

[9] Selberg A. An elementary proof of Dirichlet's theorem about primes in an arithmetic progression [J]. *Ann of Math*, 1949, 50:297–304.

k-Primes and the Unique Factorization

DONG Pingchuan[1] DONG Zhe[2] JIANG Haiyi[3]

[1]Department of Mathematics, New York University, NY 10012-1110, USA. E-mail: pd2170@nyu.edu

[2]Corresponding author. School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China. E-mail: dongzhe@zju.edu.cn

[3]School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China. E-mail: jianghaiyi@zju.edu.cn

Abstract In this paper, the authors try to find out the deeper reasons for the unique factorization into k-primes. In Section 2, the authors introduce the k-combination condition and Fermat's theorem in S_k. One major result of this paper is that the following 4 assertions are equivalent (1) the k-combination condition holds; (2) S_k has the unique factorization into k-primes; (3) Fermat's theorem in S_k is true; (4) $k = 1$ or 2. In order to understand k-primes more precisely, in Section 3 the authors investigate a special case of k-primes, i.e. 3-primes. It is well-known that the unique factorization into 3-primes fails in general. However which integers in S_3 have the unique factorization into 3-primes? In Section 3, the authors obtain a sufficient and necessary condition for which integers in S_3 have the unique factorization into 3-primes. In the end of Section 3, the authors introduce $\pi_3(x)$ which represents the number of 3-primes less than or equal to x. By the prime number theorem, the authors obtain a concrete formula and some approximate formulae for $\pi_3(x)$.

Keywords k-Prime, Unique factorization, k-Combination condition, Fermat's theorem, Prime number theorem

2000 MR Subject Classification 11N05

The English translation of this paper will be published in
Chinese Journal of Contemporary Mathematics, Vol. 44 No. 2, 2023
by ALLERTON PRESS, INC., USA