素数与合数

素数Prime Number 和 合数Composite Number 是初等数论中非常重要的两个概念，也是非零自然数（正整数）的一种分类。

正整数按照因数个数分类为：

$$\{非零自然数或正整数\} = \{1\} \cup \{素数\} \cup \{合数\}$$

本篇还包括了**因数factor（约数）、倍数multiple、分解素因数prime factorization、素因数树枝分解法Factor Tree以及素数的特点。**

因数

因数就是和一个数相乘，可以得到另一个数的数。英文描述如下：
"**Factors**" are the numbers you multiply together to get another number

举例：$\because 1 \times 6 = 2 \times 3 = 6,\ \therefore 6的因数有1, 2, 3, 6$

素数和合数的定义

最复杂的宇宙空间离不开最简单的自然数表达，最简单的自然数又被最难以理解的素数控制着。高斯说：数学是科学的女皇，数论是女皇头上的皇冠。哥德巴赫猜想就是皇冠上的宝石。

两种定义 Definition 如下：
(1) 只能被 **1和自身** 整除的非零自然数，称为素数，也叫质数，否则就是合数。或
(2) 只有 **1和自身** 这两个不同正因数的自然数称为素数；比 1 大且不是素数的自然数（或正整数）就是合数。

特别注意：
（1）0和1 既不是素数也不是合数；
（2）素数只有 2 个不同的正因数；
（3）合数有 2 个以上的正因数。

英文定义描述如下

A **Prime Number** is:

a whole number greater than 1 that can not be made by multiplying other whole numbers

If we can make it by multiplying other whole numbers it is a **Composite Number**, such as $4 = 2 \times 2$.

分解素因数 Prime Factorization（也叫分解质因数）

素因数(prime factor)：如果一个素数是某个数的因数，那么就说这个素数是这个数的素因数

素因数分解的英文描述：
"**Prime Factorization**" is finding which prime numbers multiply together to make the original number.

分解素因数：一个合数用几个素数相乘的形式表示出来，叫做分解素因数，其中每个素数都是这个合数的素因数。

分解素因数的常用方法有：（1）短除法；（2）树枝分解法；（3）口算法等

（1）短除法求所有素因数

$$
\begin{array}{r|l}
\text{最小素因数} p_1 & \underline{\text{待分解的整数}} \\
\text{素因数} p_2 & \underline{\text{商}} \\
\text{素因数} p_3 & \underline{\text{商}} \\
\text{素因数} p_4 & \underline{\text{商}} \\
\text{素因数} p_5 & \underline{\text{商}} \\
\cdots\cdots & \underline{\text{商}} \\
\text{素因数} & \underline{1}
\end{array}
$$

举例

$$
\begin{array}{r|l}
2 & \underline{210} \\
3 & \underline{105} \\
5 & \underline{35} \\
7 & \underline{7} \\
 & \underline{1}
\end{array}
$$

（2）树枝分解法

从最小的素数开始试除，能够除尽的，将商再同样试除素数，直到都是素数为止。

素因数树枝分解法的英文描述如下：
A "**Factor Tree**" can help: find any factors of the number, then the factors of those numbers, etc, until we can't factor any more.

举例 30

$$
\begin{array}{ccc}
 & 30 & \\
\swarrow & & \searrow \\
2 & & 15 \\
 & \swarrow \quad \searrow & \\
 & 3 \quad 5 &
\end{array}
$$

所以 $30 = 2 \times 3 \times 5$，这就是合数的素因数树枝分解法得到的结果。

算术基本定理或唯一分解定理

因为每个大于1的自然数都可以分解为素因数的乘积，所以貌似素数是所有自然数的基石。这个观点对于大数据工作非常有用，譬如在密码学Cryptography中的应用。

因为任意合数都可以分解为素数的乘积（素因数分解），如果将素因数按照从小到大的顺序排列（或者说 不计因数的次序），则这种**素因数分解的形式是唯一的，`There is only one (unique!) set of prime factors for any whole number`**，这就是**唯一分解定理。**

用数学式子描述如下：
$n = \prod_{i=1}^{n} p_i^{ai},\ k \geq 1,\ p_1 < p_2 < \cdots < p_k$是互不相同的素数，$a_1, a_2, \cdots, a_k \in \mathrm{N}^+$

密码学正是利用了大数的素因数分解比较难以实现这个特点来设计密码的。

如果将两个大素数相乘，则得到一个巨大的非素数，只有两个（大）素因子，如 $N = p * q$，其中p，q是两个大素数，N 可以用作公钥，而素因数 p、q 可以用作私钥。 对数据进行的任何操作只能通过了解这两个素因数中的一个来撤消，这对于未加密是非常重要的，如果不知道私钥，想要分解并找到这两个大的素数，是需要花费巨大时间。对于黑客来说，如果任何算法需要花费大量时间来破解代码，这对他们而言是毫无用处的。如RSA加密算法就取决于这一事实。

根据这一基本定理，可以得到一个推论：**正约数的个数定理**, 参见我的另外一篇文章 约数与倍数

GeoGebra中作程序实现

- 添加乘号文本：text1=\times
- 添加滑动条：n=slider(2,10000,1)
- 添加输入合数框(InputBox),关联滑动条n
- 对合数框进行因数分解：M_1 = Factors(n)
- 利用内置的函数power，创建列表：
  L_1=Zip(power(Element(p, 1), Element(p, 2)), p, M_1)
- 创建显示内容列表：
  L_2=Append(L_1(1), Sequence(text1 + (L_1(i)), i, 2, Length(L_1)))

GGB分解素因数

Python和GeoGebra中实现素因数分解

Python中用sympy库中的函数 `factorint(n)` 可以得到素因数及其个数。

```
>>> import sympy
>>> sympy.factorint(357)
{3: 1, 7: 1, 17: 1}
>>>
```

除此之外，sympy库中还有 `prime(nth)`返回第n个素数； `primerange(a, b)`返回区间(a,b)之间的所有素数； `isprime(n)`判断n是否为素数；`randprime(a, b)`随机返回一个在区间(a,b)的素数；`prevprime(n, ith=1)`返回一个小于n的第i个素数；`nextprime(n)`返回大于n的素数。

GeoGebra中利用函数 `Factors(n)` 也可以得到素因数及其个数列表。

将合数分解为多个素因数的乘积或者素数之和

1. 合数可以分解为素因数的乘积
2. 大于2的偶数可以分解为两个素数的和
3. 大于7的奇数可以分解为三个素数之和

哥德巴赫猜想 Goldbach Conjecture

公元1742年,德国数学家Christian Goldbach(1690-1764)与大数学家Leonhard Euler（1707-1783）的几次通信中提到关于正整数和素数之间关系的两个推测。

1. 偶数的猜想：任何一个不小于6（或大于4）的**偶数**都是两个奇素数之和；这是欧拉的表述，被人称为"**关于偶数的哥德巴赫猜想**"或"**强哥德巴赫猜想**"。
2. 奇数的猜想:任何一个不小于9（或大于7）的**奇数**都是三个奇素数之和。这被称为"**关于奇数的哥德巴赫猜想**"或"**弱哥德巴赫猜想**"。

实际上，第二个问题可以理解为 $2n+1=2(n-1)+3$，显然可以由第一个问题推得。

有关哥德巴赫猜想的证明，目前最好的结论是我国数学家陈景润于1966年的证明，简称 **"1+2"陈氏证明**：每一个充分大的偶数都可以表示为（1）**两个素数的和**，或是（2）**一个素数和一个半素数的和**。基本证明了哥德巴赫猜想的正确性。

数学中，两个素数的乘积所得的自然数我们称之为**半素数**（也叫双素数，二次殆素数）。 半素数表参见本章末尾说明——**Python代码得到开始62个半素数表**

举例

- 分解素因数：$147=3\times49=3\times7\times7=3\times7^2$
- 素数之和：$147=139+3+5=137+3+7=131+5+11=\cdots$
- 分解素因数：$90=9\times10=3^2\times2\times5=2\times3^2\times5$
- 素数之和：$90=7+83=11+79=17+73=19+71=23+67=29+61=31+59=37+53=43+47$

素数的特性

1. 素数 p 的约数只有两个：1 和 p；
2. 大于2的素数只能是奇数；
3. 0和1既不是素数也不是合数；
4. 2是唯一的偶素数, 大于2的素数一定是奇数；
5. 如果两个素数的和或差是奇数，则其中必有一个素数是2；如果两个素数的积是偶数，则其中必有一个是2；
6. 初等数学基本定理：任何大于1的自然数，要么本身是素数，要么可以分解为几个素数之积，且这种分解是唯一的；
7. 素数的个数是无限的；
8. 素数的个数公式 π(n) 是不减函数；
9. 若 n 为正整数，在 n^2 到 $(n+1)^2$ 之间至少有一个素数；
10. 若素数 p 为不超过 $n(n\geq4)$ 的最大素数，则 $p>\frac{n}{2}$；
11. 所有大于 10 的素数中，个位数只能是 $1,3,7,9$。
12. 如果 p 是素数，且 $p\mid bc$, 则必有 $p\mid b$ 或 $p\mid c$

证明：素数的个数是无穷的

欧几里得的《几何原本》中的证明使用了反证法。
具体证明如下：假设素数只有有限的 n 个，从小到大依次排列为 p_1，p_2，$\cdots$，p_n，设 $N=p_1\times p_2\times\cdots\times p_n$，那么，$N+1$ 是素数或者不是素数。

1. 如果 $N+1$ 为素数，则 $N+1$ 要大于 p_1，p_2，$\cdots$，p_n，所以它不在那些假设的素数集合中。
2. 如果 $N+1$ 为合数，因为任何一个合数都可以分解为几个素数的积；而 N 和 $N+1$ 的最大公约数是1，所以 $N+1$ 不可能被 p_1，p_2，$\cdots$，p_n 整除，所以该合数分解得到的素因数肯定不在假设的素数集合中。

矛盾，故素数有无限个。

例题

例题1 特别关注偶素数2的巧用

（1）两个素数的和是39，这两个素数的差是多少?
（2）三个互不相同的素数相加，和为40，这三个素数分别是多少?

解析：通常情况下，素数都是奇数（除了2以外），所以除2以外的两个素数的和为偶数。

（1）两个素数的和39是奇数，说明必有一个素数为偶数，而偶素数只有一个2，故另一个素数只能是39-2=37，故它们的差为37-2=35

（2）三个不同的素数之和为偶数，则必有一个偶素数2，故另外两个奇素数之和为38，拆分成两个素数为7, 31 (19+19相同，不合题意，舍去)。从而这三个素数分别是2，7，31。

例题2 分解素因数

$(1)\ 360;\qquad (2)\ 539;\qquad (3)\ 1001;\qquad (4)12660$
解：可以用短除法从2，3，5，7，11，... 一个一个试一下。
$(1)\ 360=2^3\times 3^2\times 5;\qquad (2)\ 539=7^2\times 11;\qquad (3)\ 1001=7\times 11\times 13;\qquad (4)12660=2^2\times 3\times 5\times 211$

例题3 连续自然数问题

三个连续自然数的乘积等于39270，那么这三个连续自然数的和等于多少?

解：先对39270进行素因数分解，得到 $2\times 3\times 5\times 7\times 11\times 17$

可以适当组合，得到三个连续自然数为 $3\times 11=33,\ 2\times 17=34,\ 5\times 7=35$

从而得到这三个自然数的和为 $33+34+35=102$
答：这三个自然数的和为102。

例题4 求乘积末尾有多少个连续的0

$975\times 935\times 972\times \square$, 要使这个连乘积的最后4个数字都是0，方框内最小应填什么数?

解析：末尾每个0，代表乘以10，而 $10=2\times 5$, 所以需要 $10^4=2^4\times 5^4$, 才能满足题目要求。

对已知的三个数进行素因数分解，得到：
$975\times 935\times 972=2^2\times 3^6\times 5^3\times 11\times 13\times 17$, 故需要补充2个2和1个5，方框内最小应填 $2^2\times 5=20$

答：方框内最小应填 20

例题5 末尾多少个连续的0

（1）算式 $1\times 2\times 3\times 4\times\cdots\times 29\times 30$ 的计算结果的末尾有多少个连续的0?
（2）算式 $31\times 32\times 33\times 34\times\cdots\times 149\times 150$ 的计算结果的末尾有多少个连续的0?

解析：
（1）显然 连乘的结果中，素因数 2 的个数比 5 多，所以，我们只要弄清楚连乘结果分解素因数中 5 的个数。因为数字较小，最大只有30，故可以枚举出来：含有5的数有5, 10, 15, 20, 25,30, 共有 7 个素因数5，故末尾有7个连续0。
（2）用阶乘符号表示 $n!=1\times 2\times 3\times\cdots\times n$, 则原式= $\dfrac{150!}{30!}$。
150！含有多少个素因数5呢？有 $[\dfrac{150}{5}]+[\dfrac{150}{5^2}]+[\dfrac{150}{5^3}]=30+6+1=37$ 个素因数；
由第（1）问，知道 30！含有7个素因数。
故原式有37-7=30个素因数5，即末尾有30个连续的0.

练习题

1. 如果三个互不相同的素数相加，和为52，这三个素数可能是多少?

2. 分解素因数 (1) 2635; (2) 22425

3. 三个自然数的乘积为84，其中两个数的和正好等于另一个数，求这三个数。

4. 算式 $924 \times 175 \times 140 \times 95$ 的计算结果的末尾有多少个连续的0?

5. 算式 $2 \times 4 \times 6 \times 8 \cdots \times 98 \times 100$ 的计算结果的末尾有多少个连续的0?

6. 正整数N满足：$\frac{N}{2}$ 是一个整数的平方，$\frac{N}{5}$ 是一个整数的五次方，符合要求的N最小是多少?

作业

1. 把下面的数分解素因数：240，1518，3553

2. 用扑克牌玩24点游戏，每次抽出4张牌，每张牌点数为牌面数字大小（其中 J 为11点，Q 为12点，K 为13点）。有一次抽到的四个数为a、a、b、1，算 24 点时有：$(a \times a - 1) \times b = 24$. 如果知道 a和b 都是素数，求所有符合上述条件的 a和b。（a、b可以相同）

3. 某校师生为贫困地区捐款1995元，这个学校共有35名教师和14个教学班。各班学生人数相同且多于30人不超过45人。如果平均每人捐款的钱数是整数，那么平均每人捐款多少元?

4. 从 20 到 50 之间选出 4 个数相乘，乘积的末尾最多有几个连续的0？请写出一种选法。

5. 算式 $50 \times 53 \times 56 \times \cdots \times 110$ 的结果中，末尾有几个连续的0?

素数表Prime number chart (<100)

100以内的素数表(共25个素数，占比25%)

范围	个位1	个位3	个位7	个位9	素数个数
(1,10)	2	3	5	7	4
(10,20)	11	13	17	19	4
(20,30)		23		29	2
(30,40)	31		37		2
(40,50)	41	43	47		3
(50,60)		53		59	2
(60,70)	61		67		2
(70,80)	71	73		79	3
(80,90)		83		89	2
(90,100)			97		1

注意：除第一行外，其它行都是对应末尾位。

Python代码得到开始62个半素数表

```
>>a=[2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97]
>>b=[a[i]*a[j] for i in range(len(a)) for j in range(i,len(a))]
>>b.sort()
>>b
```

[4, 6, 9, 10, 14, 15, 21, 22, 25, 26, 33, 34, 35, 38, 39, 46, 49, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95, 106, 111, 115, 118, 119, 121, 122, 123, 129, 133, 134, 141, 142, 143, 145, 146, 155, 158, 159, 161, 166, 169, 177, 178, 183, 185, 187, 194, 201, 203, 205, 209, 213, 215, 217, 219, 221, 235, 237, 247, 249, 253, 259, 265, 267, 287, 289, 291, 295, 299, 301, 305, 319, 323, 329,

335, 341, 355, 361, 365, 371, 377, 391, 395, 403, 407, 413, 415, 427, 437, 445, 451, 469, 473, 481, 485, 493, 497, 511, 517, 527, 529, 533, 551, 553, 559, 581, 583, 589, 611, 623, 629, 649, 667, 671, 679, 689, 697, 703, 713, 731, 737, 767, 779, 781, 793, 799, 803, 817, 841, 851, 869, 871, 893, 899, 901, 913, 923, 943, 949, 961, 979, 989, 1003, 1007, 1027, 1037, 1067, 1073, 1079, 1081, 1121, 1139, 1147, 1157, 1159, 1189, 1207, 1219, 1241, 1247, 1261, 1271, 1273, 1333, 1343, 1349, 1357, 1363, 1369, 1387, 1403, 1411, 1457, 1501, 1513, 1517, 1537, 1541, 1577, 1591, 1633, 1643, 1649, 1679, 1681, 1691, 1711, 1739, 1763, 1769, 1817, 1829, 1843, 1849, 1891, 1909, 1927, 1943, 1961, 2021, 2047, 2059, 2077, 2117, 2173, 2183, 2201, 2209, 2231, 2257, 2263, 2279, 2291, 2407, 2419, 2449, 2479, 2491, 2501, 2537, 2573, 2581, 2623, 2627, 2701, 2747, 2759, 2773, 2809, 2813, 2867, 2881, 2911, 2923, 2993, 3007, 3053, 3071, 3127, 3139, 3149, 3233, 3239, 3293, 3337, 3397, 3403, 3431, 3481, 3551, 3569, 3589, 3599, 3649, 3713, 3721, 3763, 3827, 3869, 3901, 3953, 3977, 4087, 4171, 4183, 4187, 4189, 4307, 4331, 4399, 4453, 4489, 4559, 4661, 4717, 4757, 4819, 4891, 4897, 5041, 5063, 5141, 5183, 5251, 5293, 5329, 5429, 5561, 5609, 5723, 5767, 5893, 5917, 5963, 6059, 6241, 6319, 6497, 6499, 6557, 6887, 6889, 7031, 7081, 7387, 7663, 7921, 8051, 8633, 9409]

开始62个半素数为 4, 6, 9, 10, 14, 15, 21, 22, 25, 26, 33, 34, 35, 38, 39, 46, 49, 51, 55, 57, 58, 62, 65, 69, 74, 77, 82, 85, 86, 87, 91, 93, 94, 95, 106, 111, 115, 118, 119, 121, 122, 123, 129, 133, 134, 141, 142, 143, 145, 146, 155, 158, 159, 161, 166, 169, 177, 178, 183, 185, 187, 194

它们包含 1 及自己在内共有 3个 或 4个 因数。