Goldbach' Conjecture (6): The Chinese Remainder Theorem And Goldbach' Primes

Tong Xin Ping

Abstract: By the Chinese Remainder Theorem, we can obtain Goldbach' PrimeS

“1+1”浅见之六：哥德巴赫素数的计算方法

童 信 平

1 名词、术语、符号。

N——偶数中的复合数。N＝4，6，8，10，.....。

p_i、p_r、p_{r+1}——素数，$2\leqslant p_i\leqslant p_r<\sqrt{N}<p_{r+1}<N$ 。i =1, 2, …, r 。r=π($\sqrt{N}$)。

p——闭区间[p_r+1, N− p_r−1]内的素数。必有(N−p)＞p_r。p 的数量是 π (N)$_r$= π (N−p_r−1)−r。

N(p_i)－－用 p_i 去除 N 所得到的余数。0≤N(p_i)≤(p_i−1)。

当 i=1 ~ r 时，N(p_i)= N(p_1)，N(p_2)，…，N(p_i)，…，N(p_r)。

p(p_i)－－用 p_i 去除某一个 p 所得到的余数。1≤p(p_i)≤(p_i−1)。

当 i=1 ~ r 时，p(p_i)= p(p_1)，p(p_2)，…，p(p_i)，…，p(p_r)。

p_N(p_i)－－在 p(p_i)= p(p_1)，p(p_2)，…，p(p_i)，…，p(p_r)中，去除 p(p_i)= N(p_i)后的数列。

p——闭区间[p_r+1, N− p_r−1]内的全体素数 p。

p(p_i)－－用 p_i 去除全体 **p** 所得到的余数。**p**(p_i)= 1，2，…，(p_i−1)。即 **p**(2)= 1；**p**(3)= 1，2；**p**(5)= 1，2，3，4；**p**(7)= 1，2，3，4，5，6；…；。**p**(p_r)= 1，2，…，(p_r−1)。（见引理 3。）

$\mathbf{p}_N$(p_i)－－在 **p**(2)= 1；**p**(3)= 1，2；**p**(5)= 1，2，3，4；**p**(7)= 1，2，3，4，5，6；…；。**p**(p_r)= 1，2，…，(p_r−1)中，除去 **p**(3)=N(3)，**p**(5)=N(5)，**p**(7)=N(7)，…，**p**(p_r)=N(p_r)等元素后的数列。

哥德巴赫素数——满足哥德巴赫猜想的素数。即“1+1”的答案(解)。

根据以上规定，我们有 N= p_i +(N− p_i)= p +(N− p)。

有许多 N 的(N−p_i)都是合数。我们讨论(N−p)中的哥德巴赫素数。

2 p_r～N 之间的素数的计算。

引理 1　如果a是一个大于 1 的正整数，而所有≤$\sqrt{a}$ 的素数都除不尽a，则a是素数。

引理 2（中国剩余定理即孙子定理）　若m_1，m_2，…，m_r是两两互素的正整数，则下列同余式组(1)中有小于M=$m_1m_2\cdots m_r$的唯一的解。

(1)　$x\equiv a_1 \pmod{m_1}$，$x\equiv a_2 \pmod{m_2}$，$x\equiv a_3 \pmod{m_3}$，…，$x\equiv a_r \pmod{m_r}$。

引理 3　如果**p**(p_i)是用p_i去除全体**p**所得到的余数。则**p**(p_i)= 1，2，…，(p_i−1)。

证明　不大于 N 的正整数可以用 0+ p_i n、1+ p_i n、2+ p_i n、3+ p_i n、…、(p_i −1)+ p_i n 表示。除 0+ p_i n 中只有一个素数 p_i 外，其余素数(包括 **p**)都存在于 1+ p_i n ~ (p_i −1)+ p_i n 之中，所以，**p**(p_i)= 1，2，…，(p_i−1)是充分的条件。

根据等差数列中的素数定理，N→∞时，上述 1+ p_i n ~ (p_i −1)+ p_i n 的每一个等差数列中的素数数量大约是 $\frac{\pi(N)}{p_i-1}$。换句话说，**p**(p_i)中如果少了一个元素，就会失去 $\frac{\pi(N)}{p_i-1}$ 个素数，所以，**p**(p_i)= 1，2，…，(p_i−1)也是必要条件。证毕。

定理 1　如果 i=1～r，公式 (2) 有解，当 $x<N$ 时，x 是素数。

(2)　$x \equiv \mathbf{p}(p_i) \pmod{p_i}$

证明　根据引理 3，i=1～r 时，公式 (2) 可以写成下面更详细的同余式组：

$$x \equiv 1 \pmod 2$$

$$x \equiv 1 \pmod 3,\quad x \equiv 2 \pmod 3$$

$$x \equiv 1 \pmod 5,\quad x \equiv 2 \pmod 5,\quad x \equiv 3 \pmod 5,\quad x \equiv 4 \pmod 5$$

$$x \equiv 1 \pmod 7,\quad x \equiv 2 \pmod 7,\quad x \equiv 3 \pmod 7,\quad x \equiv 4 \pmod 7,\quad x \equiv 5 \pmod 7,\quad x \equiv 6 \pmod 7$$

$$\vdots$$

$$x \equiv 1 \pmod{p_i},\quad x \equiv 2 \pmod{p_i},\quad x \equiv 3 \pmod{p_i},\quad \ldots,\quad x \equiv (p_i-1) \pmod{p_i}$$

$$\vdots$$

$$x \equiv 1 \pmod{p_r},\quad x \equiv 2 \pmod{p_r},\quad x \equiv 3 \pmod{p_r},\quad \ldots,\quad x \equiv (p_r-1) \pmod{p_r}$$

根据 $\mathbf{p}(p_i)$的变化，式(2)的每一行中有(p_i-1)个同余式，即：第一行中有(p_1-1)个同余式；第二行中有 (p_2-1) 个同余式；…；第 i 行中有(p_i-1)个同余式；…；最后一行有(p_r-1)个同余式。

i=1～r 时，依次在公式 (2) 的每一行中取一个同余式，组成彼此之间至少有一个同余式不相同的同余式组时，这些同余式组的数量将是(p_1-1)、(p_2-1)、…、(p_r-1)的乘积。根据引理 2，这里的每一个同余式组都有小于 $w_r=p_1 p_2 \cdots p_r$ 的唯一的解，故解的数量也是$(p_1-1)(p_2-1)\cdots(p_r-1)$。

因为答案 x 皆不能依次被 p_1、p_2、…、p_r 整除。根据引理 1，$x<N$ 时。x 是素数。证毕。

公式(2)的解的数量是 $u=(p_1-1)(p_2-1)\cdots(p_r-1)$，而小于 N 的素数数量是 $\pi(N)$，所以，出现 $x>N$ 的机会是很多的。换句话说，用这种方法得到素数的效率是很低的。

3　(p_r+1)～$(N-p_r-1)$之间的哥德巴赫素数的计算。

定理 2　如果 i=1～r，公式 (3) 有解，当 $p_r+1<x<N-p_r-1$ 时，x 是哥德巴赫素数。

(3)　$x \equiv \mathbf{p}_N(p_i) \pmod{p_i}$

证明　根据定理 1，如果 i=1～r，$x \equiv \mathbf{p}(p_i) \pmod{p_i}$，且 $p_r+1<x<N-p_r-1$。则 x 是素数。

$\mathbf{p}_N(p_i)$去除的是 $p(p_i)=p(p_1)$，$p(p_2)$，…，$p(p_i)$，…，$p(p_r)$中的 $p(p_i)=N(p_i)$，也就是去除了(N-p)=合数时的 p，留下的就是哥德巴赫素数。证毕。

在 $p(p_i)=p(p_1)$，$p(p_2)$，…，$p(p_i)$，…，$p(p_r)$中去除 $p(p_i)=N(p_i)$时，如果 $N(p_i)\neq 0$，$p(p_i)$的元素个数量还有(p_i-2)；如果 $N(p_i)=0$，$p(p_i)$的元素个数还是$(p_i-1)=(p_i-2)\dfrac{p_i-1}{p_i-2}$；i=1～r 时，依次在公式(3)的每一行中取一个同余式，组成彼此之间至少有一个同余式不相同的同余式组时，这些同余式组的数量(也是解的数量)v 如公式 (4) 所示。

(4)　$v=\prod_{3\leqslant p\leqslant\sqrt{N}}^{(p,N)=1}(p-2)\prod_{2\leqslant p\leqslant\sqrt{N}}^{(p,N)=p}(p-1)=\prod_{3\leqslant p\leqslant\sqrt{N}}(p-2)\prod_{3\leqslant p\leqslant\sqrt{N}}^{p\mid N}\frac{p-1}{p-2}$　（已省略 $p_1-1=1$。）

公式(3)的解的数量是 v，而小于 N 的哥德巴赫素数数量根据经验是很少的，所以，出现 $x>N$ 的机会是很多的。换句话说，用这种方法得到哥德巴赫素数的效率是很低的。

4　举例。

例 1：计算 134 的哥德巴赫素数。($p_i=2$，3，5，7，11。$134(p_i)=0$，2，4，1，2。p=13～113。)

根据前面所述，N=134 时，公式(3)可以写成更详细的同余式组如下：

$$x \equiv 1 \pmod 2$$

$$x \equiv 1 \pmod 3$$

$$x \equiv 1 \pmod 5,\quad x \equiv 2 \pmod 5,\quad x \equiv 3 \pmod 5$$

$x \equiv 2 (\mathrm{mod}\ 7)$，$x \equiv 3 (\mathrm{mod}\ 7)$，$x \equiv 4 (\mathrm{mod}\ 7)$，$x \equiv 5 (\mathrm{mod}\ 7)$，$x \equiv 6 (\mathrm{mod}\ 7)$

$x \equiv 1 (\mathrm{mod}\ 11)$，$x \equiv 3 (\mathrm{mod}\ 11)$，$x \equiv 4 (\mathrm{mod}\ 11)$，$x \equiv 5 (\mathrm{mod}\ 11)$，…，$x \equiv 10 (\mathrm{mod}\ 11)$

依次在上式的每一行中取一个同余式，组成彼此之间至少有一个同余式不相同的同余式组时，可得到(1，1，1，2，1) ~ (1，1，3，6，10)共 v=(3−2)(5−2)(7−2)(11−2)=135 个同余式组，每一组同余式组的解如下：{31}——哥德巴赫素数。[331]——素数。961——合数

(1,1,1,2,1)→[331]；(1,1,1,2,3)→[751]；(1,1,1,2,4)→961；(1,1,1,2,5)→[1171]；
(1,1,1,2,6)→[1381]；(1,1,1,2,7)→1591；(1,1,1,2,8)→[1801]；(1,1,1,2,9)→[2011]；
(1,1,1,2,10)→[2221]；(1,1,1,3,1)→[661]；(1,1,1,3,3)→1081；(1,1,1,3,4)→[1291]；
(1,1,1,3,5)→1501；(1,1,1,3,6)→1711；(1,1,1,3,7)→1921；(1,1,1,3,8)→2031；
(1,1,1,3,9)→{31}；(1,1,1,3,10)→[241]；(1,1,1,4,1)→[991]；(1,1,1,4,3)→1411；
(1,1,1,4,4)→[1621]；(1,1,1,4,5)→[1831]；(1,1,1,4,6)→2041；(1,1,1,4,7)→[2251]；
(1,1,1,4,8)→[151]；(1,1,1,4,9)→361；(1,1,1,4,10)→[571]；(1,1,1,5,1)→[1321]；
(1,1,1,5,3)→[1741]；(1,1,1,5,4)→[1951]；(1,1,1,5,5)→[2161]；(1,1,1,5,6)→{61}；
(1,1,1,5,7)→[271]；(1,1,1,5,8)→481；(1,1,1,5,9)→[691]；(1,1,1,5,10)→901；
(1,1,1,6,1)→1651；(1,1,1,6,3)→2071；(1,1,1,6,4)→[2281]；(1,1,1,6,5)→781；
(1,1,1,6,6)→391；(1,1,1,6,7)→[601]；(1,1,1,6,8)→[811]；(1,1,1,6,9)→[1021]；
(1,1,1,6,10)→[1231]；(1,1,2,2,1)→1717；(1,1,2,2,3)→[2137]；(1,1,2,2,4)→{37}；
(1,1,2,2,5)→247；(1,1,2,2,6)→[457]；(1,1,2,2,7)→667；(1,1,2,2,8)→[877]；
(1,1,2,2,9)→[1087]；(1,1,2,2,10)→[1297]；(1,1,2,3,1)→2047；(1,1,2,3,3)→[157]；
(1,1,2,3,4)→[367]；(1,1,2,3,5)→[577]；(1,1,2,3,6)→[787]；(1,1,2,3,7)→[997]；
(1,1,2,3,8)→1207；(1,1,2,3,9)→1417；(1,1,2,3,10)→[1627]；(1,1,2,4,1)→{67}；
(1,1,2,4,3)→[487]；(1,1,2,4,4)→697；(1,1,2,4,5)→[907]；(1,1,2,4,6)→[1117]；
(1,1,2,4,7)→[1327]；(1,1,2,4,8)→1537；(1,1,2,4,9)→[1747]；(1,1,2,4,10)→1957；
(1,1,2,5,1)→[397]；(1,1,2,5,3)→817；(1,1,2,5,4)→1027；(1,1,2,5,5)→[1237]；
(1,1,2,5,6)→[1447]；(1,1,2,5,7)→[1657]；(1,1,2,5,8)→[1867]；(1,1,2,5,9)→2077；
(1,1,2,5,10)→[2287]；(1,1,2,6,1)→[727]；(1,1,2,6,3)→1147；(1,1,2,6,4)→1357；
(1,1,2,6,5)→[1567]；(1,1,2,6,6)→[1777]；(1,1,2,6,7)→[1987]；(1,1,2,6,8)→2197；
(1,1,2,6,9)→{97}；(1,1,2,6,10)→[307]；(1,1,3,2,1)→793；(1,1,3,2,3)→[1213]；
(1,1,2,2,4)→[1423]；(1,1,3,2,5)→1633；(1,1,3,2,6)→1843；(1,1,3,2,7)→[2053]；
(1,1,3,2,8)→2263；(1,1,3,2,9)→[163]；(1,1,3,2,10)→[373]；(1,1,3,3,1)→[1123]；
(1,1,3,3,3)→[1543]；(1,1,3,3,4)→[1753]；(1,1,3,3,5)→1963；(1,1,3,3,6)→2173；
(1,1,3,3,7)→{73}；(1,1,3,3,8)→[283]；(1,1,3,3,9)→493；(1,1,3,3,10)→703；
(1,1,3,4,1)→[1453]；(1,1,3,4,3)→[1873]；(1,1,3,4,4)→[2083]；(1,1,3,4,5)→[2293]；
(1,1,3,4,6)→[193]；(1,1,3,4,7)→403；(1,1,3,4,8)→[613]；(1,1,3,4,9)→[823]；
(1,1,3,4,10)→[1033]；(1,1,3,5,1)→1243；(1,1,3,5,3)→[2203]；(1,1,3,5,4)→{103}；
(1,1,3,5,5)→[313]；(1,1,3,5,6)→[523]；(1,1,3,5,7)→[733]；(1,1,3,5,8)→943；
(1,1,3,5,9)→[1153]；(1,1,3,5,10)→1363；(1,1,3,6,1)→[1733]；(1,1,3,6,3)→[223]；
(1,1,3,6,4)→[433]；(1,1,3,6,5)→[643]；(1,1,3,6,6)→[853]；(1,1,3,6,7)→[1063]；
(1,1,3,6,8)→1273；(1,1,3,6,9)→[1483]；(1,1,3,6,10)→[1693]。

整理后，从小到大的排列是：{31}、{37}、{61}、{67}、{73}、{97}、{103}、[151]、[157]、[163]、[193]、[223]、[241]、247、[271]、[283]、[307]、[313]、[331]、361、[367]、[373]、391、[397]、403、[433]、[457]、481、[487]、493、[523]、[571]、[577]、[601]、[613]、[643]、[661]、667、[691]、697、703、[727]、[733]、[751]、781、[787]、793、[811]、817、[823]、[853]、[877]、901、[907]、943、961、[991]、[997]、[1021]、1027、[1033]、[1063]、1081、[1087]、[1117]、[1123]、1147、[1153]、[1171]、1207、[1213]、[1231]、[1237]、1243、1273、[1291]、[1297]、[1321]、[1327]、1357、1363、[1381]、1411、1417、[1423]、

[1447]、[1453]、[1483]、1501、1537、[1543]、[1567]、1591、[1621]、[1627]、1633、1651、[1657]、[1693]、1711、1717、[1733]、[1741]、[1747]、[1753]、[1777]、[1801]、[1831]、1843、[1867]、[1873]、1921、[1951]、1957、1963、[1987]、[2011]、2031、2041、2047、[2053]、2071、2077、[2083]、[2137]、[2161]、2173、2197、[2203]、[2221]、[2251]、2263、[2281]、[2287]、[2293]。

5 讨论。

以上讨论了得到哥德巴赫素数的方法，用这种方法得到哥德巴赫素数的效率是很低的。但是，目前只有这个方法和《“1+1”浅见之三：用 Eratosthenes 筛法得到哥德巴赫素数》的正、反方向的“植(砍)树问题”法。

2010-07-20