关于分布素数公式的研究

吴新生

（中国电子科技集团公司 第十六研究所，合肥 230061）

摘 要：Mersenne，Fermat和Euler都提出了分布素数公式，希望发现一个公式能产生出无限多个连续分布的素数。它也叫作“猎逐素数”公式，即$P=2n\pm\alpha$。本文用随机抽样法证明：$P=2n\pm\alpha$中连续分布的素数只有有限个。因此，$P=2n\pm\alpha$型“猎逐素数”无限多个的公式不存在。

关键词：连续素数；连续分布素数；“猎逐素数”公式；素数的分布公式；自熔黑洞；随机事件。

中图分类号：O212.2，O156.4　　**文献标识码：**A　　**文章编号：**1008-6021（2017）02-0120-05

一、引言

法国数学家Fermat（1601—1665）提出四个不同的公式[1]，用来研究素数分布的问题，即公式（1）至公式（4）。

类型一：$P=kn+l\ (k>0,\ l>0)$

公式（1）$P=4n+1$型素数　（1）

公式（2）$P=6n+1$型素数　（2）

公式（3）$P=8n+1$型素数　（3）

公式（4）$P=8n+3$型素数　（4）

问：公式（1），公式（2），公式（3），公式（4）是否包含无限多个素数？

关于分布素数公式，最早由法国数学家Mersenne（1588-1648）提出，也称Mersenne素数[2]。若输入连续的素数，则公式M_p的结果将是许多连续分布的素数。见下式：

类型二：$P=2n\pm\alpha$（$n>0$，α为一奇数）

$$M_p=2^p-1,\ p=2,3,5,\cdots \tag{5}$$

$M_2=2^2-1=4-1=3$

$M_3=2^3-1=8-1=7$

$M_5=2^5-1=32-1=31$

$M_7=2^7-1=128-1=127$

…

$M_{11}=2^{11}-1=2048-1=2047=89\times23$ 这是一个合数。

法国数学家Fermat发表了自己的连续分布素数公式。他公开宣称自己的公式F_n给出的全部都是素数——连续分布的素数。

$$F_n=(2)^{2^n}+1,\ n=0,1,2,\cdots \tag{6}$$

$F_0=(2)^{2^0}+1=2^1+1=2+1=3$

$F_1=(2)^{2^1}+1=2^2+1=4+1=5$

$F_2=(2)^{2^2}+1=2^4+1=16+1=17$

$F_3=(2)^{2^3}+1=2^8+1=256+1=257$

$F_4=(2)^{2^4}+1=2^{16}+1=65536+1=65537$

Euler研究Fermat公式后，指出

$F_5=(2)^{2^5}+1=2^{32}+1=4294967296+1=4294967297$

$=641\times6700417$（合数）

在Fermat的许多研究成果中，这是唯一让人遗憾的一次。

瑞士数学家Euler（1707—1778）在研究前人分布素数公式的基础上，他提出了自己的分布素数公式。见下式：

$$P=n^2-n+41 \tag{7}$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	…	35	36	37	38	39	40
Pn	41	43	47	53	61	71	83	97	113	131	151	173	197	223	…	1231	1301	1373	1447	1523	1601

当$n=41$时，$P_{41}=1681=41\times41$（合数）

$$P=n^2+n+41 \tag{8}$$

当$n=0、1、\cdots，39$时，公式4给出的都是素数。当$n=40$时，

收稿日期：2016-10-31

作者简介：吴新生（1948-），男，江苏宿迁人，高级工程师。研究方向：数论。

P_{40}=1681=41×41(合数)

$P=n^2-79n+1601$ (9)

N	0	1	2	3	4	5	6	7	8	…	37	38	39
P_u	1601	1523	1447	1373	1301	1231	1163	1097	1033	…	47	43	41
n	40	41	42	43	44	45	46	47	48	…	77	78	79
P_u	41	43	47	53	61	71	83	97	113	…	1447	1523	1601

公式7一共连续得出80个素数。前40个素数和后40个素数,它们的数值相同,次序相反。

当n等于80时。$P_{80}=80^2-79\times80+1601=1681$

$=41\times41$(合数)

$P=2n^2+29$，$n=0,1,2,\cdots,28$ (10)

公式(10)的结果写成集合形式为

$P=\{29,31,\cdots,1597\}=\{p\mid p=2n^2+29,n=0,1,2,\cdots,28\}$

它一共连续得出29个素数。当n=29时。

$P_{29}=29\times59$(合数)。

数学家们不断地努力,希望能发现一个公式,它能产生出无限多个连续性的分布素数,故称之为“猎逐素数”公式。以上选择的仅是有代表性的几例,但没有一次成功。是没有找到一个美妙的方法呢?还是这种连续分布素数的公式根本不存在呢?

类型一中公式包含某种形式的素数无限多个,可以合数共生。

类型二中公式包含连续分布的素数无限多个,不能产生合数。这是“猎逐素数”公式的最初设想。

二、定义

定义1:设素数$P_1\leq P_2\leq P_3$,则称P_1,P_2,P_3是从小到大的三个连续素数。

定义2:设$f(n_1)=P_1<f(n_2)=P_2<f(n_3)=P_3$,则称$P_1,P_2,P_3$,是三个连续分布的素数。

定义3:设$5\in G_5=\{5,15,25,\cdots,a_n=10n+5,n\in\mathrm{N}\}$,且首位5是集合$G_5$中唯一的素数,则称集合$G_5$是以5结尾且大于5的素数的自熔黑洞。

定义4:设素数$p\in G$,且集合G中还包含素数的平方数,立方数,…,n次方数,即

$m_1=p^2\in G,m_2=p^3\in G\ldots m_{n-1}=p^n\in G,n\in N^+$

则称$m_1,m_2,\cdots m_{n-1}$为集合G的突变形合数。

定义5:设素数$p_n\in G$,集合G中还包含不同的素因数的积,即

$m=p_1^i\cdot p_2^j\ldots p_n^k\in G,i,j,k=0,1,2,\cdots$

则称合数m为集合G的串形合数。

三、引　理

引理1　设集合$G_1=\{1,11,21,\cdots,a_n=10n+1,n\in N\}$

则　集合G_1包含无限多个突变形合数,以及无限多个串形合数。

证明:集合G_1的解析式为$a_n=10n+1,n\in N$

根据Dirichlet定理,集合G_1包含无限多个素数:

$p_1,p_2\ldots\in G_1$

同理　对集合$G_9=\{9,19,29,\cdots,a_n=10n+9,n\in N\}$

有无限多个素数,$t_1,t_2\ldots\in G_9$

(1)由于$p_1,p_2\cdots$的结尾为1,$p_1^2,p_2^3\ldots p_n^{n+1}$的结尾也为1,而有

$M_1=\{m_1\mid m_1=p_i^j\in G_1,\ i=1,2,\cdots,j=2,3,\cdots\}$ (11)

(2)由于$t_1,t_2\cdots$的结尾为9,$t_1^2,t_2^4,\cdots$的结尾为1,而有

$M_2=\{m_2\mid m_2=t_i^{2n}\in G_1,\ i=1,2,\cdots,n=1,2,\cdots\}$ (12)

(3)下面这些素因数的积的结尾为1,而有

$M_3=\{m_3\mid m_3=p_1^i\cdot p_2^j\ldots p_n^k\in G_1,i,j,k,=0,1,\cdots\}$ (13)

(4)由于$t_1,t_2\cdots$中两两之积的结尾为1,而有

$M_4=\{m_4\mid m_4=t_it_j\in G_1,\ i,j=0,1,\cdots,i\neq j\}$ (14)

(5)设$m_2\in M_2$,$m_3\in M_3$,$m_4\in M_4$,且m_2,m_3,m_4为集合M_2,M_3,M_4中任一元素的代表而有

$M_{51}=\{m_{51}\mid m_{51}=m_2\cdot m_3\in G_1\}$,

$M_{52}=\{m_{52}\mid m_{52}=m_3\cdot m_4\in G_1\}$。

(1),(2),(3),(4),(5)中,突变形合数有无限多个,串形合数有无限多个。　证毕

引理2　设集合$G_3=\{3,13,23,\cdots,a_n=10n+3,n\in N\}$

则集合G_3包含无限多个串形合数。

证明集合G_3的解析式为$a_n=10_n+3$,$n\in N$。

根据Dirichlet定理,集合G_3包含无限多个素数:

$q_1,q_2\ldots\in G_3$。

设素数$p_1,p_2\ldots\in G_1$,

素数$s_1,s_2\ldots\in G_7$,

素数$t_1,t_2\ldots\in G_9$。

(1)由于p_1和q_1的结尾分别为1和3,积的结尾为3,以此类推,而有

$M_1=\{m_1\mid m_1=p_jq_i\in G_3,\ j,i=1,2,\cdots\}$ (15)

(2)由于s_1,t_1的结尾分别为7和9,积的结尾为3,以此类推,而有

$M_2=\{m_2\mid m_2=s_it_j\in G_3,\ i,j=1,2,\cdots\}$ (16)

(3)由于q_1,q_2的结尾为3,s_1结尾为7,三者的积的结尾为3,以此类推,而有

$M_3=\{m_3\mid m_3=q_i\cdot q_j\cdot s_k\in G_3,i,j,k=1,2,\cdots\}$ (17)

(4)由于$m=p_1^i\cdot p_2^j\ldots p_n^k$的结尾为1,而有

$M_{41}=\{m_{41}|m_{41}=p_1^i\cdot p_2^j\ldots p_n^k q_t\in G_3,\ i,j,k=1,2,\cdots,t=1,2,\cdots\}$

$M_{42}=\{m_{42}|m_{42}=p_1^i\cdot p_2^j\ldots p_n^k s_e\cdot t_f\in G_3,i,j,k=1,2,\cdots,e,f=1,2\cdots\}$

$M_{43}=\{m_{43}|m_{43}=p_1^i\cdot p_2^j\ldots p_n^k\cdot q_e\cdot q_f\in G_3,i,j,k=1,2,\cdots,e,f=1,2\cdots\}$。

(1),(2),(3),(4)中有无限多个串形合数。证毕

引理3　设集合 $G_7=\{7,17,27,\cdots,a_n=10+7,n\in N\}$

则集合 G_7 包含无限多个串形合数。

证明　集合 G_7 的解析式为 $a_n=10n+7,n\in N$

根据Dirichlet定理,集合 G_7 包含无限多个素数:

$S_1,S_2\ldots\in G_7$

由引理1知,素数 $p_1,p_2\ldots\in G_1$

(1)由于 p_1 和 s_1 的结尾分别是1和7,积的结尾为7,依次类推,而有

$$M_1=\{m_1|m_1=p_i\cdot s_j\in G_7,\quad i,j=1,2,\cdots\} \tag{18}$$

(2)由于 $p_1^2,p_1^3\ldots p_1^n$ 的结尾为1,它们与 s_1 的积的结尾为7,依此类推,而有

$$M_2=\{m_2|m_2=p_i^j\cdot s_i\in G_7,\quad i=1,2,\cdots,j=2,3,\cdots\} \tag{19}$$

(3)下面这些素因数的积的结尾为7,而有

$$M_3=\{m_3|m_3=p_1^i\cdot p_2^j\ldots p_n^k\cdot s_r\in G_7,\ i,j,k=0,1,\cdots,r=1,2,\cdots\} \tag{20}$$

(1),(2),(3)中有无限多个串形合数。证毕

引理4　设集合 $G_9=\{9,19,29,\cdots,a_n=10n+9,n\in N\}$

则集合 G_9 包含无限多个突变形合数以及无限多个串形合数。

证明　集合 G_9 的解析式为 $a_n=10n+9,n\in N$

根据Dirichlet定理,集合 G_9 包含无限多个素数:

$$t_1,t_2\ldots\in G_9$$

由引理2知素数 $p_1,p_2\ldots\in G_1$,

素数 $q_1,q_2\ldots\in G_3$。

(1)由于 q_1 的结尾为3,$q_1^2,q_1^6\cdots$ 的结尾为9,而有

$$M_1=\{m_1|m_1=q_i^{2n}\in G_9,\quad i=1,2,\cdots,n=1,3\cdots\} \tag{21}$$

(2)在 $q_1,q_2\cdots$ 中,其两两之积的结尾为9,而有

$$M_2=\{m_2|m_2=q_i\cdot q_j\in G_9,i=1,2,\cdots,j=1,2,\cdots,i\neq j\} \tag{22}$$

(3) p_1 与 t_1 的积的结尾为9,依此类推

而有 $M_3=\{m_3|m_3=p_i\cdot t_j\in G_9,\quad i,j,=1,2,\cdots\}$　(23)

(4)下面这些素因数的积的结尾为9,而有

$M_{41}=\{m_{41}|m_{41}=p_1^i\cdot p_2^j\ldots p_n^k\cdot t_e\in G_9,i,j,k=0,1,\cdots,e=1,2,\cdots\}$,

$M_{42}=\{m_{42}|m_{42}=p_1^i\cdot p_2^j\ldots p_n^k\cdot q_s^{2t}\in G_9,i,j,k=0,1,\cdots,s=1,2,\cdots,t=1,3\cdots\}$,

$M_{43}=\{m_{43}|m_{43}=p_1^i\cdot p_2^j\ldots p_n^k\cdot q_s\cdot q_t\in G_9,i,j,k=0,1,\cdots,s,t=1,2,\cdots\}$。

(1),(2),(3),(4)中有无限多个突变形合数,有无限多个串形合数。证毕

四、定理

类型一:$P=kn+l\ (k>0,\ l>0)$

定理1(Dirichlet)[3],若 $K>0,\ l>0,(k,l)=1$,

则形如 $kn+l$ 之素数个数无穷。

1834年,德国数学家Dirichlet证明了定理1。这是关于等差级数中分布素数的一个著名而且重要的定理。其叙述如下:

任何一个算数级数,只要其首项与公差是互素的,就必定包含无限多个素数。

这个定理解决了Fermat所提出的4个公式中的问题,给出了一个肯定的结果;这个定理还对类型一中的许多公式,都是广泛的判断标准。

关于Fermat所提(1)式,即

$P=4n+1$ 型素数

2006年,作者对这个问题,已有定量的结果[4]:

定理2 设 $\pi(x;4,1)$ 表示不超过 x,且形如 $4n+1$ 形素数的个数,则

$$\pi(x;4,1)=\frac{x}{2\ln x}+\frac{x}{2\ln^2 x}+\frac{x}{\ln^3 x}+\cdots+O\left(\frac{x}{\ln^{m+1}x}\right) \tag{24}$$

关于 $P=4n+3$ 型素数个数的结果与此类似。

类型二:$P=2n\pm\alpha$($n>0$,α 为一奇数)

$n^2\pm n=n(n\pm1)$ 是两个连续整数之积,它为偶数,α 为奇数。$n^2\pm n\pm\alpha$ 的结果为一奇数,满足它是素数的必要条件。

定理3 若素数 $P=n^2\pm n\pm\alpha,n>0,\alpha=1,11,17,\cdots$ (25)

则它包含连续分布素数的个数只有有限个。

证明一　使用构造法[5]

设 $m\in N^+,f(n_1)=p_1\leq f(n_2)=p_2$ 则

$$p_2-p_1>m \tag{26}$$

可以构造 m 个连续合数:

$(m+1)!+2,(m+1)!+3,\cdots,(m+1)!+(m+1)$

其中第 j 个数为

$(m+1)!+(j+1)$

由于 $1\leq j\leq n$,$(m+1)!$ 以 $(j+1)$ 为因子,因此

$(m+1)!+(j+1)$

一定能被($j+1$)整除。

这里($j+1$)可以从2开始一直取到($m+1$)。所以这m个整数都是连续的合数。

令 $p_1 \leq (m+1)!+2$，

$(m+1)!+(m+1) \leq p_2$。

由于$(m+1)!+2$是偶数，$(m+1)!+1$是奇数(奇素数或奇合数)。

有 $p_1 \leq (m+1)!+1$，

故 $p_2-p_1 > m$

M个连续合数中，有奇合数，偶合数(>2)，这些突变形合数或串形合数不是奇素数，故连续分布的素数中断。 证毕

先论证$p=n^2 \pm n+\alpha$

证明二，用随机抽样法[6]

设 集合$G=\{1,3,5,7,9,\cdots\}$，对集合G

有如下分类：

$G_1=\{1,11,21,\cdots, a_n=10n+1, n \in N\}$，

$G_3=\{3,13,23,\cdots, a_n=10n+3, n \in N\}$，

$G_5=\{5,15,25,\cdots, a_n=10n+5, n \in N\}$，

$G_7=\{7,17,27,\cdots, a_n=10n+7, n \in N\}$，

$G_9=\{9,19,29,\cdots, a_n=10n+9, n \in N\}$，

$G=G_1 \cup G_3 \cup G_5 \cup G_7 \cup G_9$

其中子集G_5是以5结尾的素数的自熔黑洞。

令 $\Omega=\{p \mid p=n^2 \pm n+\alpha, n>0\}$

设 $\alpha=11,17,41$， $n=0,1,2$,时

(25)式分别有：

$\{11,11,13$或$11,11,17\}$， (27)

$\{17,17,19$或$17,17,23\}$， (28)

$\{41,41,43$或$41,41,47\}$。 (29)

(27),(28),(29)三个括号中确实有连续分布的素数，但个数有限。

对于$\Omega=\{p \mid p=n^2 \pm n+\alpha, n>0\}$

当给定n一个具体数值时，由(25)式得到的是：一个偶数加上一个奇数，它可能是一个奇素数，也可能是一个奇合数，这实在是一个随机事件。

由于奇素数$p \in G$，且在集合G中的分布是随机分布的。而集合Ω中每一个奇数p_i($i=1,2,\cdots$)，可能是一个奇素数，也可能是一个奇合数，也是随机变化的。而有

$$\Omega \subseteq G$$

因此，可以把集合Ω中奇数$p=n^2 \pm n+\alpha$看作是从集合G中随机抽取的样本，对“猎逐素数”公式起作用的是从子集G_1,G_3,G_7,G_9中抽取的奇素数。

在条件组S下令n大量连续取值，集合Ω中奇数$p=n^2 \pm n+\alpha$也大量增多，那么这些奇数相当于从集合G中随机抽取大量的样本。由于素数分布的独立性，因此，集合中的奇数：

$\Omega=\{p \mid p=n^2 \pm n+\alpha, n>0\}$

都是独立同分布的随机变量列。当样本充分多时，抽取集合G中每一个奇数都具有相同的可能性。

一种情况是：大量的随机样本都是奇素数，即

$P_{11}=10^i m+10^j n+\ldots+10k+1$，$m,n,k=0,1,2,\cdots 9$；$i,j=0,1,\cdots,i=j+1$

$P_{33}=10^i m+10^j n+\ldots+10k+3$，$m,n,k=0,1,2,\cdots 9$；$i,j=0,1,\cdots,i=j+1$

$P_{77}=10^i m+10^j n+\ldots+10k+7$，$m,n,k=0,1,2,\cdots 9$；$i,j=0,1,\cdots,i=j+1$

$P_{99}=10^i m+10^j n+\ldots+10k+9$，$m,n,k=0,1,2,\cdots 9$；$i,j=0,1,\cdots,i=j+1$

当样本数量充分多时，一定会出现一个以1或3或7或9结尾的随机样本p_m为合数，不论它是一个突变形合数或一个串形合数，连续分布的素数中断。

另一种情况是：当大量的随机抽样中出现以1或3或7或9结尾的样本时(这些样本可能是奇素数也可能是奇合数)。设上述样本皆为奇素数，那么只要样本数量充分多，同时一定会出现以5结尾的随机变量 $p_n=10^i m+10^j n+\ldots+10k+5$，$m,n,k=0,1,2,\cdots 9$；$i,j=0,1,\cdots, i=j+1$.但是

$p_n \in G_5$且$p_n>5$

集合G_5是以5结尾的素数的自熔黑洞，不论p_n是一个突变形合数或者一个串形合数，连续分布的素数此时中断。

关于$p=n^2 \pm n-\alpha$

一个偶数减去一个奇数，其结果可能是一个奇素数，也可能是一个奇合数。这实在是一个随机事件。

同理，$p=n^2 \pm n-\alpha$有和$p=n^2 \pm n+\alpha$相同的论证结果。证毕

五、结论

古希腊数学家Euclid(公元前325年左右—公元前265年左右)在《几何原本》一书中指出：“素数是无限的”早在远古时代，人们就寻找一般公式$P=f(n)$，$n \in N$。由$f(n)$产生出的素数有无限多个。$f(n)$就是理想中的“猎逐素数”公式。

Euler提出二次三项式的研究是一次巨大的推动。$E_n=n^2-n+41$ ($n \in N$)形素数是其提出的几个公式

之一。Mersenne素数Mp和Fermat素数Fn相继发表，研究活跃。但网上查询发现能分布几个素数的公式很多，但是都没有成功。数学家们对公式进行分类研究。1834年，Dirichlet证明了类型一，$P=kn+l$，即：

$l, l+k, l+2k, \cdots, l+nk$（$l>0, k>0$）且（$l, k$）=1。

此式含有无限多个某种形式的素数，也含有相同形式的合数。（L, k）=1是关键的条件。

已经提出的作为研究对象的“猎逐素数”公式，无论它是如何简洁的解析式或者复杂的解析式，其中一大类都是属于类型二：$P=2n\pm\alpha$。对于代表式$P=n^2\pm n\pm\alpha$，可以做最简单的验证：

令$n=\alpha$，而有

$$P=\alpha^2\pm\alpha\pm\alpha=\alpha(\alpha\pm1\pm1)=\begin{cases}\alpha^2 & \text{合数}\\ \alpha(\alpha+2) & \text{合数}\\ \alpha(\alpha-2), \ \alpha>3 & \text{合数}\end{cases}$$

只有在$\alpha<n$且(n, α)=1的情况下，公式才有可能出现几个连续分布的素数，这个数量是有限的而不是无限的。本文用随机抽样法证明这一点是更加可靠的推理证明。归属于$P=2n\pm\alpha$类型“猎逐素数”公式是不可能产生出无限多个连续性分布素数。因此，$P=2n\pm\alpha$类型“猎逐素数”无限多个的公式不存在。

参考文献：

[1] 华罗庚.堆垒素数论[M].北京：中国科学院，1953.

[2] 堀場芳数.素数的奥秘[M].丁树森，译.北京：科学出版社，2000.

[3] 华罗庚.数论导引[M].北京：科学出版社，1979：258-262.

[4] 吴新生.N^2+1形式素数个数的估计[J].安徽广播电视大学学报，2006：121-125.

[5] 楼世拓.邬冬华，黎曼猜想[M].沈阳：辽宁教育出版社，1987：147-161.

[6] 吴新生.大偶数表为两个素数之和[J].安徽广播电视大学学报，2000(4)：86-88.

The Research on Formula of Distributing Primes

WU Xin-sheng

(The 16th institute, China Electronics Technology Group Corporation, Hefei 230061, China)

Abstract: Mersenne，Fermat and Euler put forward several formulas of distributing primes. They hope to find a formula which can produce out an infinite number of continuous distributing primes. It is also called “hunting primes” formula，that is P=2n±α. The paper uses random sampling method to prove that there are only a finite number of continuous distributing primes in P = 2n ± α. Therefore, infinite formula of “hunting primes for” form of P=2n±α do not exist.

Key words: continuous primes; continuous distributing primes; the formula of “hunting primes”；formula of prime distribution; black cave of oneself melt；random event

［责任编辑　李潜生］