第28卷第4期 西昌学院学报·自然科学版 Vol.28,NO.4
2014年12月 Journal of Xichang College·Natural Science Edition Dec.,2014

孪生素数猜想的证明

叶雉鸠
(陕西财经职业技术学院,陕西 咸阳 712000)

【摘 要】采用数学归纳法证明了一类缺项同余式方程组恒无解。若这一类缺项同余式方程组恒无解则孪生素数猜想成立,即自然数域中存在无穷多对孪生素数,孪生素数猜想是成立的。

【关键词】数论;孪生素数猜想;数学归纳法;同余式方程组;正整数解
【中图分类号】O156.1;O156.2 【文献标识码】A 【文章编号】1673-1891(2014)04-0027-04

1 引言及预备命题

孪生素数猜想是数论中的著名未解决问题。这个猜想产生已久,在数学家希尔伯特在1900年国际数学家大会的著名报告中,它位列23个“希尔伯特问题”中的第8个问题,可以被描述为“存在无穷多个素数p,并且对每个p而言,有p+2这个数也是素数”[1]。

2013年5月14日,《自然》杂志报道,数学家张益唐证明存在无穷多个素数对相差都小于7000万[2]。陶哲轩随后开始了一个Polymath计划,由网上志愿者合作降低张益唐论文中的上限。截至2014年4月,即张益唐提交证明之后一年,按Polymath8b计划维基所宣称,上限已降至246[3]。沿着张益唐的证明思路,要做进一步的证明也许会更加困难一些。因此仍然有必要另辟蹊径,探索新的证明途径。

《孙子算经》[4]、《数书九章》[5]和《算术探索》[6]都一致指向了同余理论。在对相邻奇数积的数列进行同余分析时,找到了孪生素数猜想成立的一个充分条件[7]——【命题1】。

定义两个集合:

$$\{奇素数\}=\{3,5,7,11,\cdots\cdots\}=P$$

$$\{不大于\sqrt{2a+1}的奇素数\}=\{3,5,\cdots\ p_b\}=P_b\subseteq P$$

【命题1】对于任意大于10的自然数a($a\geq 11$,$a\in N$),方程组(1-1)恒无正整数解。

$$\begin{cases}(2\times4)^2-1\equiv0(\bmod p_{01})\\(2\times5)^2-1\equiv0(\bmod p_{02})\\(2\times6)^2-1\equiv0(\bmod p_{03})\\\cdots\cdots\cdots\cdots\\{[2(a-1)]}^2-1\equiv0(\bmod p_{0(a-4)})\\(2a)^2-1\equiv0(\bmod p_{0(a-4+1)})\\\max(p_{01},p_{02},p_{03}\cdots p_{0(a-4+1)})=p_b\leq\sqrt{2a+1}\end{cases}\qquad(1\text{-}1)$$

其中:

①(1-1)同余式方程左边处于a位置的因子为不小于4的连续自然数.

② p_b是不大于$\sqrt{2a+1}$的奇素数中最大的一个,b表示不大于$\sqrt{2a+1}$的奇素数的总个数。

③(1-1)等式右端模域中的奇素数p_{01},p_{02},p_{03},……$p_{0(\alpha-4-1)}$可以相同,也可以不尽相同,也可以完全不同;p_{01},p_{02},p_{03},……$p_{0(\alpha-4-1)}$不讲究顺序,即并不意味着$p_{01}\leqslant p_{02}\leqslant\cdots p_{0(\alpha-4-1)}$。

④(1-1)同余式方程右边的模的集合是不大于p_b的所有奇素数p_b的子集(或全集),即可以为p_b的全集,也可以为p_b的子集,可以作模域理解。

若【命题1】成立,则孪生素数猜想成立。若孪生素数猜想成立,则【命题1】不一定成立。本文拟采用数学归纳法证明【命题1】成立。

2 数学归纳法论证

2.1 取初始值验证【命题1】成立

当$a=11$时,

由(1-1)得出(1-2)

$$\begin{cases}(2\times4)^2-1\equiv0(\bmod p_{01})\\(2\times5)^2-1\equiv0(\bmod p_{02})\\(2\times6)^2-1\equiv0(\bmod p_{03})\\(2\times7)^2-1\equiv0(\bmod p_{04})\\(2\times8)^2-1\equiv0(\bmod p_{05})\\(2\times9)^2-1\equiv0(\bmod p_{06})\\(2\times10)^2-1\equiv0(\bmod p_{07})\\(2\times11)^2-1\equiv0(\bmod p_{08})\\\max(p_{01},p_{02},p_{03}\cdots p_{08})=p_1=3\leq\sqrt{2\times11+1}\end{cases}\qquad(1\text{-}2)$$

(1-2)还可以进一步明确为(1-3)

$$\begin{cases}(2\times4)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(1)\\(2\times5)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(2)\\(2\times6)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(3)\\(2\times7)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(4)\\(2\times8)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(5)\\(2\times9)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(6)\\(2\times10)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(7)\\(2\times11)^2-1\equiv0(\bmod 3)\cdots\cdots\cdots\cdots\cdots(8)\\\max(p_{01},p_{02},p_{03}\cdots p_{08})=p_1=3\end{cases}\qquad(1\text{-}3)$$

收稿日期:2014-07-20
作者简介:叶雉鸠(1965-),男,陕西乾县人,空军工程大学工程硕士,副教授,主要从事数学和经济学研究。

验算得(1–3)中(3)、(6)无正整数解，所以(1–3)无正整数解，即【命题1】成立。

当a=12时，

由(1–1)得出(1–4)

$$\begin{cases} (2\times4)^2-1\equiv 0(\bmod\ p_{01}) \\ (2\times5)^2-1\equiv 0(\bmod\ p_{02}) \\ (2\times6)^2-1\equiv 0(\bmod\ p_{03}) \\ \cdots\cdots\cdots\cdots \\ (2\times12)^2-1\equiv 0(\bmod\ p_{09}) \\ \max(p_{01},p_{02},p_{03}\cdots p_{09})=p_2=5\le\sqrt{2\times12+1} \end{cases} \qquad (1–4)$$

(1–4)还可以进一步明确为(1–5)

$$\begin{cases} (2\times4)^2-1\equiv 0(\bmod\ 3\vee 5)\cdots\cdots\cdots\cdots(1) \\ (2\times5)^2-1\equiv 0(\bmod\ 3\vee 5)\cdots\cdots\cdots\cdots(2) \\ (2\times6)^2-1\equiv 0(\bmod\ 3\vee 5)\cdots\cdots\cdots\cdots(3) \\ \cdots\cdots\cdots\cdots \\ (2\times12)^2-1\equiv 0(\bmod\ 3\vee 5)\cdots\cdots\cdots\cdots(9) \\ \max(p_{01},p_{02},p_{03}\cdots p_{09})=p_2=5 \end{cases} \qquad (1–5)$$

(1–5)中“∨”表示“或者”，读作“析取”。(1–5)实际上是一组同余式方程组，由于各个方程式的模均存在2种可能，所以9个方程式的组合就构成2^9=512个同余式方程组。(1–5)中模域扩大了1个。验算得(1–5)中(3)、(6)无正整数解，所以(1–5)无正整数解，即【命题1】成立。

当a=13,14,15⋯23时，由(1–1)所给出的同余式方程组模域没有扩大，而方程式的个数逐渐增加。在无解的方程组中再增加新的方程式，则增加方程式之后的方程组更加无解。即此时，【命题1】亦成立。

2.2 假设当$a=n(n\ge11,n\in N)$时【命题1】成立

假设：当$a=n(n\ge11,n\in N)$时，下列方程组(1–6)无正整数解。

$$\begin{cases} (2\times4)^2-1\equiv 0(\bmod\ p_{01}) \\ (2\times5)^2-1\equiv 0(\bmod\ p_{02}) \\ (2\times6)^2-1\equiv 0(\bmod\ p_{03}) \\ \cdots\cdots\cdots\cdots \\ [2(n-1)]^2-1\equiv 0(\bmod\ p_{0(n-4)}) \\ (2n)^2-1\equiv 0(\bmod\ p_{0(n-4+1)}) \\ \max(p_{01},p_{02},p_{03}\cdots p_{0(n-4+1)})=p_b\le\sqrt{2n+1} \end{cases} \qquad (1–6)$$

2.3 证明当$a=n+1$时【命题1】成立

当$a=n+1(n\ge11$，且$n\in N)$时，“方程组(1–1)无正整数解”的判断是否仍然成立呢？这一步的证明要分两种情况。

①第一种情况——a从n到$n+1$没有引起p_b的变化。

如果a从n到$n+1$没有引起p_b的变化，即就是a从n到$n+1$没有引起同余式方程组模域的变化。模域没有发生变化，方程组中的方程式却增加了一个。在无解的方程组中再增加一个新的方程式，则增加方程式之后的方程组更加无解。即此时，【命题1】成立。

②第二种情况——a从n到$n+1$引起了p_b的变化。

如果a从n到$n+1$引起了p_b的变化，即就是a从n到$n+1$引起了同余式方程组模域的变化。模量添加了一个p_{b+1}，同时方程式还增加了一个。这时的方程组如(1–7)所示。

$$\begin{cases} (2\times4)^2-1\equiv 0(\bmod\ p_{01}) \\ (2\times5)^2-1\equiv 0(\bmod\ p_{02}) \\ (2\times6)^2-1\equiv 0(\bmod\ p_{03}) \\ \cdots\cdots\cdots\cdots \\ (2n)^2-1\equiv 0(\bmod\ p_{0(n-4+1)}) \\ [2(n+1)]^2-1\equiv 0(\bmod\ p_{0[(n+1)-4+1]}) \\ \max(p_{01},p_{02},p_{03}\cdots p_{0[(n+1)-4+1]})=p_{b+1}\le\sqrt{2(n+1)+1} \end{cases} \qquad (1–7)$$

此时，$p_{b+1}=\sqrt{2(n+1)+1}$，即$n=\dfrac{p_{b+1}^2-3}{2}$。

要证明(1–7)在$a=n+1=\dfrac{p_{b+1}^2-1}{2}$时无解，需要采用反证法。

在采用反证法之前，首先要做一项工作，就是把(1–7)与(1–6)中的方程式的个数调整一下，使得(1–7)与(1–6)中的方程式的个数相等。

因为(1–7)中刚刚增加的方程式$[2(n+1)]^2-1\equiv 0(\bmod\ p_{0[(n+1)-4+1]})$必有解，所以可以删去。这样，(1–7)与(1–6)中的方程式的个数就相等了，都等于$n-4+1$。

$[2(n+1)]^2-1\equiv 0(\bmod\ p_{0[(n+1)-4+1]})$必有解的证明步骤如下：

$\because [2(n+1)]^2-1=p_{b+1}^2[2(n+1)-1]$

$\therefore [2(n+1)]^2-1\equiv 0(\bmod\ p_{b+1})$

又$\because \max(p_{01},p_{02},p_{03}\cdots p_{0[(n+1)-4+1]})=p_{b+1}$

$\therefore [2(n+1)]^2-1\equiv 0(\bmod\ p_{0[(n+1)-4+1]})$在(1–7)中必有解。

下面，采用反证法证明(1–7)无解。

【反证法的假设】假设同余式方程组(1–6)无解，而同余式方程组(1–7)有解。

【反证法的递推】当$a=n+1=\dfrac{p_{b+1}^2-1}{2}$时

把(1–7)左边$\{(2n)^2-1|n\ge11\}$中不能被p_b中的元素同余同模表示，只能被p_{b+1}同余同模表示的数表示为$\{(2n_{遗漏})^2-1\}$。并将$\{(2n_{遗漏})^2-1\}$中“所涉及的那些自然数”定义为$n_{遗漏}$，则由(1–7)可以得出(1–8)

$(2n_{遗漏})^2-1\equiv 0 \bmod p_{b+1}$ （1–8）

其中:这里(1–8)中的$n_{遗漏}$也可以理解为——在(1–6)中无解,而在(1–7)中有解的那些方程式中"所涉及的$\{(2n_{遗漏})^2-1\}$中的那些自然数"。

$\because\ (2n_{遗漏})^2-1=(2n_{遗漏}-1)(2n_{遗漏}+1)$

$\therefore$由(1–8)可以得出(1–9)或者(1–10)

$2n_{遗漏}-1\equiv 0 \bmod p_{b+1}$ （1–9）

$2n_{遗漏}+1\equiv 0 \bmod p_{b+1}$ （1–10）

于是,$2n_{遗漏}$可以表示为$2n_{遗漏}=(2r+1)p_{b+1}\pm 1$,此处$r$为某些使得$2n_{遗漏}$为不大于$p_{b+1}^2-3$的自然数的那些自然数($2\times 4\le 2n_{遗漏}\le p_{b+1}^2-3$)。

把$2n_{遗漏}=(2r+1)p_{b+1}\pm 1$代入(1–8),有下式(1–11)存在

$(2n_{遗漏})^2-1=(2r+1)p_{b+1}[(2r+1)p_{b+1}\pm 2]$ （1–11）

如果把$2n_{遗漏}=(2r+1)p_{b+1}\pm 1$回代到(1–9)或者(1–10)时,则会得到

$(2r+1)p_{b+1}\equiv 0 \bmod p_{b+1}$ （1–12）

(1–11)和(1–12)中均有$2r+1$,所以针对$2r+1$来展开讨论。

首先,确定$2r+1$的数域范围

$\because\ 4\le n_{遗漏}\le n=\dfrac{p_{b+1}^2-3}{2}$

$\therefore\ 8\le 2n_{遗漏}\le p_{b+1}^2-3$ （1–13）

又$\because\ 2n_{遗漏}=(2r+1)p_{b+1}\pm 1$

$\therefore\ 8\le (2r+1)p_{b+1}\pm 1\le p_{b+1}^2-3$ （1–14）

展开(1–14),可得(1–15)

$8\le(2r+1)p_{b+1}+1\le p_{b+1}^2-3$或者$8\le(2r+1)p_{b+1}-1\le p_{b+1}^2-3$ （1–15）

即$7/p_{b+1}\le 2r+1\le p_{b+1}-4/p_{b+1}$或者$9/p_{b+1}\le 2r+1\le p_{b+1}-2/p_{b+1}$ （1–16）

从而由(1–16)得出(1–17)

$1\le 2r+1\le p_{b+1}-1$ （1–17）

即$2r+1\in\{1,3,5,7,9,\cdots,p_{b+1}-2\}$ （1–18）

接下来,对$2r+1$进行分类讨论。分$2r+1=1$和$2r+1\ne 1$两种情形。

当$2r+1=1$时,由(1–11)得出(1–19)

$(2n_{遗漏})^2-1=p_{b+1}(p_{b+1}\pm 2)$ （1–19）

如果(1–19)中$p_{b+1}\pm 2$是合数,则必有(1–20)成立

$(2n_{遗漏})^2-1\equiv 0 \bmod p_{某b}$,$p_{某b}\in P_{\mathrm{b}}$ （1–20）

即(1–6)有正整数解。这与假设相矛盾,故【命题1】成立 （1–21）

如果(1–19)中$p_{b+1}\pm 2$是素数,则等于在此范围内找到了一对孪生素数,即孪生素数猜想成立(1–22)

当$2r+1\ne 1$时,$2r+1\in\{3,5,7,9,\cdots,p_{b+1}-2\}$

此时,$2r+1\equiv 0 \bmod p_{某b}$,$p_{某b}\in P_{\mathrm{b}}$ （1–23）

由(1–23)可以得出(1–24)

即$(2r+1)p_{b+1}[(2r+1)p_{b+1}\pm 2]\equiv 0 \bmod p_{某b}$,$p_{某b}\in P_{\mathrm{b}}$ （1–24）

由(1–24)和(1–11)得出(1–25)

$(2n_{遗漏})^2-1\equiv 0 \bmod p_{某b}$,$p_{某b}\in P_{\mathrm{b}}$ （1–25）

即(1–6)有解——这是与假设相矛盾的。故这种情形下【命题1】成立。

【结论】根据数学归纳法得出,对一切自然数n($n\ge 11$,且$n\in N$),【命题1】恒成立。

由于【命题1】成立,随着的$a\to+\infty$不断递增,孪生素数前赴后继,逐渐显现,所以孪生素数猜想成立。

3 缺项单无解定理的提出及论证

3.1 缺项单无解定理的提出

虽然(1–22)的判断本身是正确的,但是就整个证明而言(1–22)是一个逻辑漏洞。因为反证法的证明思路是一直向上的无解递推,而(1–22)则显示为有解。这导致一直向上的无解递推中断,即不能朝着无穷大的自然数向上持续递推。

如何来弥补这个漏洞?

有一个思路——那就是从数学归纳法证明一开始,就舍去具备(1–19)特性的那两个方程式。提前舍去了具备(1–19)特性的两个方程式,该漏洞就不存在了。这需要在【命题1】的基础上提出一个更强的在(1–1)中舍去两个"具备(1–19)特性"的方程式的【命题2】。

【命题2】对于任意大于10的自然数a($a\ge 11$,且$a\in N$),方程组(1–1)中舍去2个"具备(1–19)特性"的方程式之后的同余式方程组无正整数解。

【命题2】存在一个更强的命题【命题3】

【命题3】对于任意大于10的自然数a($a\ge 11$,且$a\in N$),方程组(1–1)中舍去任意2个相邻方程式之后的同余式方程组无正整数解。

【命题2】和【命题1】中方程式个数的关系是局部与整体的关系,局部无解则整体无解,整体无解则局部不一定无解。即若【命题2】无解则【命题1】无解;若【命题1】无解则【命题2】不一定无解——此所谓【命题2】比【命题1】更强。

【命题3】和【命题2】中所舍去方程式的区别是任意与特定的关系,任意无解则特定无解,特定无解则任意不一定无解。即若【命题3】无解则【命题2】无解;若【命题2】无解则【命题3】不一定无解——此所谓【命题3】比【命题2】更强。

不妨把【命题3】称之为"缺项单无解定理"。值

得说明的是,如果本文直接证明“缺项单无解定理”可能会使人们不容易理解,所以本文先给出前面(1–2)到(1–25)的证明。在大家都熟悉了证明的框架思路之后,再给出“缺项单无解定理”的证明就容易理解一些。下面采用数学归纳法证明【命题3】。

3.2 取初始值验证【命题3】成立

如前所验,当a=11时,由(1–1)得出(1–2),(1–2)还可以进一步明确为(1–3)。前面已经验算得出在(1–3)中(3)、(6)无正整数解。由于(1–3)中的(3)、(6)并不相邻,所以在(1–3)中舍去任意2个相邻方程式之后的同余式方程组仍然无正整数解,即【命题3】成立。

当a=12时,由(1–1)得出(1–4),(1–4)还可以进一步明确为(1–5)。(1–5)中模域扩大了1个。前面已经验算得处在(1–5)中(3)、(6)无正整数解。由于(1–5)中的(3)、(6)并不相邻,所以在(1–5)中舍去任意2个相邻方程式之后的同余式方程组依然无正整数解,即【命题3】成立。

3.3 证明当 时【命题3】成立

假设:当$a=n$($n\geq 11, n\in N$)时,方程组(1–6)中舍去任意2个相邻方程式之后的同余式方程组无正整数解。

当a=n+1($n\geq 11$,且$n\in N$)时,“方程组(1–6)中舍去任意2个相邻方程式之后的同余式方程组无正整数解”的判断是否仍然成立呢?这一步的证明要分两种情况。

①第一种情况——a从n到$n+1$没有引起p_b的变化。

如果a从n到$n+1$没有引起p_b的变化,即就是a从n到$n+1$没有引起同余式方程组模域的变化。模域没有发生变化,方程组中的方程式却增加了一个。在无解的方程组中再增加一个新的方程式,则增加方程式之后的方程组更加无解。即此时,【命题3】成立。

②第二种情况——a从n到$n+1$引起了p_b的变化。

如果a从n到$n+1$引起了p_b的变化,即就是a从n到$n+1$引起了同余式方程组模域的变化。模量添加了一个p_{b+1},同时方程式还增加了一个。这时的完整方程组如(1–7)所示,所不同的是【命题3】需要面对的是“方程组(1–7)中舍去任意2个相邻方程式之后的同余式方程组”。

此时,$p_{b+1}=\sqrt{2(n+1)+1}$,即$n=\dfrac{p_{b+1}^2-3}{2}$。

要证明“(1–7)舍去任意2个相邻方程式之后的同余式方程组”在$a=n+1=\dfrac{p_{b+1}^2-1}{2}$时无解,需要采用反证法。

在采用反证法之前,照样要做一项工作,就是把(1–7)与(1–6)中的方程式的个数调整一下,使得(1–7)与(1–6)中的方程式的个数相等。

因为(1–7)中刚刚增加的方程式$[2(n+1)]^2-1\equiv 0(\bmod\ p_{0[(n+1)-4+1]})$必有解,所以可以删去。这样,(1–7)与(1–6)中的方程式的个数就相等了,都等于$n-4+1$。

下面,采用反证法证明“(1–7)舍去任意2个相邻方程式之后的同余式方程组”无解。

【反证法的假设】假设“(1–6)舍去任意2个相邻方程式之后的同余式方程组”无解,而“(1–7)舍去任意2个相邻方程式之后的同余式方程组”有解。

【反证法的递推】当$a=n+1=\dfrac{p_{b+1}^2-1}{2}$时,仍然有(1–8)到(1–25)的递推,所不同的是(1–22)的内容发生了变化。如果(1–19)中$p_{b+1}\pm 2$是素数,则(1–19)作为相邻的可以舍去的方程式。即便同时有解,考虑到$2r+1\neq 1$的情况,也不会影响“(1–7)舍去任意2个相邻方程式之后的同余式方程组”的无解性。

【结论】根据数学归纳法得出,对一切自然数n($n\geq 11$,且$n\in N$),【命题3】恒成立。

【命题3】成立⇒【命题2】成立⇒【命题1】成立。

由于【命题1】成立,随着的$a\to+\infty$不断递增,孪生素数前赴后继,逐渐显现,所以孪生素数猜想成立。

注释及参考文献:

[1]孪生素数猜想.百度百科[EB/OL].http://baike.baidu.com/view/272607. 2013–06–05.
[2]数学家张益唐破译“孪生素数猜想”.新华网[EB/OL].http://news.xinhuanet.com/edu. 2013–05–18.
[3]孪生素数.维基百科[EB/OL].http://zh.wikipedia.org/wiki. 2014–06–16.
[4](唐)李淳风等.孙子算经.汉典古籍[EB/OL]. http://gj.zdic.net/archive.php?aid=15923.
[5](南宋)秦九韶.数书九章[M].上海:商务印书馆,1936.
[6]高斯.算术探索[M].潘承彪,张明尧,译.2012–7–1.
[7]叶雉鸠.孪生素数猜想成立的一个充分条件[J].高师理科学刊,2014(6):

(下转第33页)

The Simulation of Virtual Laboratory Based on MATLAB

ZHANG Jing-jing

(School of Physics and Electrics, Hubei University of Arts and Science, Xiangyang, Hubei 441053)

Abstract: MATLAB is simplicity of programming, high efficiency of calculation, powerful function of drawing. The introduction of MATLAB simulation in "electrician basis" course teaching can make up the deficiency of traditional teaching. This paper studies the MATLAB function programming and virtual experiment two kinds of simulation methods, and discusses the application of MATLAB simulation and virtual experiment of two kinds of simulation methods through the example of sinusoidal steady state circuit.

Key words: MATLAB; simulation; virtual experiment

(上接第30页)

Proving the Twin Prime Conjecture

YE Zhi-jiu

(Shannxi Vocational College of Finance and Economics, Xianyang, Shannxi 712000)

Abstract: No solution of a class of lack of congruence equations with constant is proved by mathematical induction, which twin prime conjecture is established. The infinitely many prime twins exist in natural number field. The twin prime conjecture is correct.

Key words: number theory; the twin prime conjecture; mathematical induction; congruence equation; positive integer solution