

互素理论与 费马方程

Coprime theory and Fermat's equation

王瑞林 著

互素理论与费马方程

王瑞林 著

吉林大学出版社

图书在版编目（CIP）数据

互素理论与费马方程 / 王瑞林著. — 长春 : 吉林大学出版社, 2018.7

ISBN 978-7-5692-2589-1

I. ①互… II. ①王… III. ①费马最后定理—研究
IV. ①O156

中国版本图书馆CIP数据核字(2018)第161932号

书 名: 互素理论与费马方程
HUSU LILUN YU FEIMA FANGCHENG

作 者: 王瑞林 著

策划编辑: 邵宇彤

责任编辑: 邵宇彤

责任校对: 张文涛

装帧设计: 林 雪

出版发行: 吉林大学出版社

社 址: 长春市人民大街4059号

邮政编码: 130021

发行电话: 0431-89580028/29/21

网 址: <http://www.jlup.com.cn>

电子邮箱: jdcbs@jlu.edu.cn

印 刷: 吉广控股有限公司

开 本: 787mm × 1092mm 1/16

印 张: 8

字 数: 224千字

版 次: 2018年7月 第1版

印 次: 2018年7月 第1次

书 号: ISBN 978-7-5692-2589-1

定 价: 32.00元

版权所有 翻印必究

作者简介

王瑞林，男，1944年生，汉族。吉林省通榆县人，中共党员，工程师。1969年毕业于吉林工业大学（现吉林大学）汽车系汽车专业，在吉林省镇赉县参加工作，在县运输公司、县汽车修配厂、县职工学校当过车工、电焊工、汽车修理工，以及大型货车和大型客车驾驶员，还做过车队、公司、厂技术员，广播电视大学专职教师（教授英语和数学分析）。1984年加入公务员序列，先后任职于县总工会、县交通运输局。2004年退休。

符号说明

本书符号说明如下:

$>$ 表示大于.

$<$ 表示小于.

$\geq$ 表示大于等于.

$\leq$ 表示小于等于.

$p|p, c|c, p|c$ 分别表示奇素数对、奇合数对、混合数对, 用于第三篇文章, $|$ 是对称线, 不表示整除.

$c \cup c, c \cap c$ 分别表示有相同因子及有不同因子的奇合数对, 用于第三篇文章.

$N_{p|p}, N_{c|c}, N_{p|c}$ 分别表示奇素数对、奇合数对、混合数对的个数, 用于第三篇文章.

$N_{c \cap c}$ 分别表示有相同因子及有不同因子的奇合数对的个数, 用于第三篇文章.

$\frac{c}{c}, \frac{p}{c}$ 分别表示奇素数对、奇合数对、混合数对, 用于第四篇文章. $-$ 是对称线, 不是分数线.

$N_{\frac{p}{c}}, N_{\frac{c}{c}}, N_{\frac{p}{c}}$ 分别表示奇素数对、奇合数对、混合数对的个数, 用于第四篇文章.

$[]$ 在第三篇文章表示只取其内数字的整数部分, 如 $[4.1]=4$, 在其他篇文章只做一般括号使用.

$\langle \rangle$ 只做一般括号使用.

$\{ \}$ 除集合外, 做一般括号使用.

$(a, b)=k$ 表示 a, b 的最大公约数等于 k , $(a, b)=1$ 表示 a, b 的最大公约数等于 1, 即 a, b 互素.

$\psi(p, x, y)$ 表示以 p, x, y 为自变量的一个特定的三元函数, 具体意义见第一篇和第二篇文章.

C_n^k 表示通常意义下的组合种数, $C_n^k = \frac{n!}{(n-k)!k!}$.

$\binom{n}{k}$ 表示通常意义下的组合种数, $\binom{n}{k} = \frac{n!}{(n-k)!k!}$.

$a \in A$ 表示 a 为集合 A 的元素.

$A = \{a_1, a_2, a_3, \dots, a_n\}$ 表示集合 A 的元素为 $a_1, a_2, a_3, \dots, a_n$.

$A = B \cap C$ 表示集合 A 是集合 B 与集合 C 的交集.

L.C.M. 表示最小公倍数 (Lowest Common Multiple) 用于第五篇文章.

F 表示万有引力 (矢量), 用于序言和第七篇文章.

a 表示加速度 (矢量), 用于第七篇文章.

r^0 表示单位矢量, 用于序言和第七篇文章. r 表示矢量 r 的模, 即 $r = |r|, r^0 = \frac{r}{|r|} = \frac{r}{r}$.

$\sum_{j=1}^n a_j = a_1 + a_2 + a_3 + \dots + a_n$.

$\prod_{a \in A} a = \prod_{j=1}^n a_j = a_1 a_2 a_3 \dots a_n, A = \{a_1, a_2, a_3, \dots, a_n\}$ 表示集合 A 的全体元素连乘.

目 录

符号说明 / (1)

序言 / (1—2)

互素理论与费马方程 (A 篇) / (3—29)

互素理论与费马方程 (B 篇) / (30—52)

对称与偶数表为两素数之和 / (53—71)

对称与孪生素数猜想 / (72—78)

罗素不等式与偶数表为两素数之和 / (79—104)

关于 Collatz 猜想 / (105)

$\xi(M, r) = \ln r^{-GM}$ 是牛顿引力方程之源头 / (106—108)

牛顿水桶实验到底该如何解读? / (109—111)

Einstein 火车用没用光速不变原理? / (112—114)

汽车: 刹车与油门的施力方向应做成直角 / (115)

科学随想录 / (116—117)

跋 / (118)

序 言

对于任何自然数 $n > 2$, 费马方程

$$x^n + y^n = z^n \quad (\text{a})$$

无非零整数解 x, y, z , 即费马最后定理, 简称 FLT. 问题早已归结到只需解决 $n = p > 3$ 为奇素数, x, y, z 为两两互素之正整数之情形. 于是我们讨论方程

$$x^p + y^p = z^p. \quad (\text{b})$$

由(b)的左端想到二项式定理及其变形:

$$(x+y)^p = x^p + C_p^1 x^{p-1} y + C_p^2 x^{p-2} y^2 + \cdots + C_p^{p-2} x^2 y^{p-2} + C_p^{p-1} x y^{p-1} + y^p, \quad (\text{c})$$

$$x^p + y^p = (x+y) \left\{ (x+y)^{p-1} - pxy \left[\frac{x^{p-2} + y^{p-2}}{x+y} + \frac{C_p^2 (x^{p-4} + y^{p-4})}{p(x+y)} xy + \cdots + \frac{C_p^{(p-1)/2}}{p} (xy)^{(p-3)/2} \right] \right\}. \quad (\text{d})$$

把[]里的式子归拢一下, 写成

$$x^p + y^p = (x+y) \left\{ (x+y)^{p-1} - pxy \psi(p, x, y) \right\}, \quad (\text{e})$$

显然有

$$\psi(p, x, y) = \frac{x^{p-2} + y^{p-2}}{x+y} + \frac{C_p^2 (x^{p-4} + y^{p-4}) xy}{p(x+y)} + \cdots + \frac{C_p^{(p-1)/2}}{p} (xy)^{(p-3)/2}. \quad (\text{f})$$

(e)比(d)好, 右端变得简捷. 接着, 我们从(e)右端的三个代数式 $x+y$, pxy , $\psi(p, x, y)$ 之间的关系入手, 寻找划分类型的根据, 而且找到了. 历史上分为两种情况: p 整除 xyz 和 p 不整除 x, y, z . 与历史根本不同, 我们先分为两种情况: $(x+y, p)=1$ 和 $(x+y, p)=p$, 再化成三个模型: $(xy, p)=p$, $(x+y, p)=p$ 和 $(\psi(p, x, y), p)=p$. 历史没谈“根据”, 只是说“不久就可以看到, 把以下两种情况分清才方便.” 因为划分类型用到了 $\psi(p, x, y)$, 所以由(d)到(e)这一步至关重要. 若(d)写不成(e), 就意味着 $\psi(p, x, y)$ 不是整数, 我们的三个模型就不对. 到底由(d)能不能写成(e), 引起美国一所著名大学的一位数学家的关注和怀疑. 我告诉他, p 是奇素数, 就能写成, p 是奇合数, 写不成. 他不再往下看了. 这是 1997 年的事. 谈论奇合数, 还得回到(a). 如果 n 为奇合数, 令 $n = kp$, p 为奇素数, (a)化为 $x^{kp} + y^{kp} = z^{kp}$, 写成 $(x^k)^p + (y^k)^p = (z^k)^p$, 就绕回到(b)了. 是能绕回来, 不过难免让人费思量, 好像有“潜伏者”. 而仔细想来, 也没什么. 麻烦出在 k 上, 降它的地位就是了. 虽然它仍在底数的高位上, 而从全式的总体看, 它毕竟是在底数上. 审稿人也不是想不到这些, 最大的可能, 还是因为领路人没走(c)(d)(e)(f). 数学家是跟着领路人走的, 全世界都一样. 关于 FLT, 作者写了 A 和 B 两篇文章. A 篇的英文稿还在这位美国朋友的手上.

(e)的右端也可以看成是对左端的因式分解. 显然, 我们与法国数学家拉梅(Gabriel Lame)不同, 拉梅把(e)的左端分解成了复数线性因子. 那是 1847 年的事.

去年 4 月互联网上有消息, 说浙江大学教授汪家禾先生 1994 年写过一篇关于 FLT 的文章. 找来一看他的思路, 也以二项式定理为平台, 也用了系统的可除性, 我倍感兴奋. 原来我并不孤独. 汪老很有名气, 是国际刊物《Appl. Math. Mech.》编委, 美国刊物《Math. Rev.》特约评论员.

1997 年还有一件事, 发生在 $\psi(p, x, y)$ 那件事之后, 也应该说及. 另一位美国数学家也看了我关于 FLT 的 A 篇. 与他联系时, 他正在英国威尔士大学讲学. 找到他, 是因为我在国内一个杂志上看到了他发表在“The mathematical Intelligencer (Vol. 19, No. 1, 1997)”上, 批评 Andrew Wiles 的文章

“Modular elliptic curves and Fermat’s Last Theorem(Ann of Math,141,1995)” 的文章的译文. 他的文章提到了哥德尔第二不完全性定理、ZF 系统的协调性、Hilbert 方案等. 他曾在 Wisconsin 大学、Texas 大学、Toronto 大学教书. 他没对 $\psi(p,x,y)$ 提出任何看法. 大约二十几天, 我们共同顺利地走到第一模型的收笔处. 这时他似乎有了看法, 用阿拉伯数字写了一个式子, 后面打了一个问号, 发过来. 我不解其意, 回了一句 “I don’t know What you say.” 从此没有了消息. 多年后回忆此事, 只记得 A 文中没有 “不含定理 9 的另证”, 记不清是否把该文的定理 9 发给了这位美国数学家, 也记不清当时是否已明确地得到定理 9. 岁月如流, 光阴似箭, 往事如烟.

关于 FLT 的 A 篇, 当时共 21 页, 第一位数学家看完了前 4 页, 包括极其重要的 $\psi(p,x,y)$. 第二位数学家看完前 14 页, 第一模型结束, 实际相当于读完全文. 文中三个模型的路线相同, 个别部位不同, 如果从拓扑学的眼光, 有点像同一个图形被扭曲了两次.

对称太神奇, OSRS 中的对称尤其值得关注. 这个无穷序列很像人类历史的长河. “自从盘古开天地, 三皇五帝到如今, …”, 这种对称或许在年份的序数中有反映, 出现某些相似. 那么 ESRS 中的对称有什么意义呢? 至少, 没有 ESRS 中的, 就联想不出 OSRS 中的, 当然, 也许不止.

(1+1)之所以成立, 那是因为 ESRS 中生成了足够多的奇合数对, 计算公式也表明, 奇合数对越多, 奇素数对也越多. 相反相成, 彰显唯物辩证法的光芒. 数论融进系统论, 不是转角度, 而是添维度, 是旧戏开了新生面.

我们一直坚持从特殊到一般的认识论. 可惜的是, 举例子时 E 不能选得太大. 于是 ESRS 中方根素数足迹的对称看得就很不开心. 比如同一行, 对称线右侧是方根素数 3 的足迹, 左侧是方根素数 5,7,11 的足迹, 这样的行下次出现是在此行往下数第 $3 \times 5 \times 7 \times 11$ 行, 即在此行往下数第 1155 行. 一页文稿全划成行, 才 40 行, 30 页才能看到. 想要看清楚 OSRS 中方根素数运动足迹的对称, 更为艰难, “叹人间美中不足今方信, …”

罗素不等式为研究(1+1)带来了 “无穷递降”, 如果认为加两倍平均值不安全, 可以加三倍, 加四倍, 加五倍, … 总能找到一个 n 、一个 q_n , 一个 E 与之对应. 这样的局面, 是未曾想到的.

ESRS 往下伸展, 总长度变为 Q 集全体元素之积, 是将其一般化、抽象化, 是打开全局. 规律在全局中才能看清楚. “第三原则” 是个约定.

R. P. Feynman 在讲到 Newton 引力定律时说: “而真的就是这样一条简单的定律吗? 它的机制 (machinery) 是什么? 我们做过的一切, 只是描写了地球怎样绕太阳转, 可是没有说过其缘由何在 (but we have not said what makes it go), Newton 对此无假设, 他只是满足于找出引力都干了些什么, 而未能深入下去.” 本书找到了牛顿引力方程之源头, 它可写成四种形式:

$$\xi(M,r)=\ln r^{-GM}, \xi(M,r)=-GM \ln r, e^{\xi(M,r)}=r^{-GM}, \xi(M,r)=\ln \frac{1}{r^{GM}},$$

每种形式视角不同. 从源头写起, 方程可写为 $F=-\frac{\partial^2}{\partial} \ln r^{-GM} r^0 m$, 可作为对 R. P. Feynman 的回答.

本书作者

二〇一八年五月于吉林镇赉

互素理论与费马方程(A篇)

摘要: 本文以互素理论为工具, 以二项式定理为平台, 证明了: $p > 3$ 为奇素数, 费马方程 $x^p + y^p = z^p$ 无两两互素的正整数解 x, y, z , 亦即使用在有理整数系统内操作的方法, 证明了费马最后定理成立.

关键词: 互素理论, 费马方程, 费马最后定理

0 引言

对于任何自然数 $n > 2$, 费马方程 $x^n + y^n = z^n$ 无非零整数解 x, y, z 称为费马最后定理, 简称 FLT. 问题早已归结到只需解决 $n = p > 3$ 为奇素数, x, y, z 为两两互素之正整数之情形. Andrew Wiles 未能终结该定理之研究, 他的方法是间接的. 关于他的那篇文章^[5], 我同意 Daniel J. Velleman 的评论^[4].

迄今, 世界上许多数学家, 仍在为找到一个可以被不同学派接受的, 不涉嫌数学基础之争论之方法, 给这个著名定理以真正意义上的证明, 而努力工作. 无疑, 最好是能找到一个直接的方法.

本文的方法: n 为奇素数时, 将二项式定理变形为 $x^n + y^n = (x + y) \left((x + y)^{n-1} - nxy\psi(n, x, y) \right)$. 式中 $\psi(n, x, y)$ 是一个代数式, 因 n 而异 (n 为奇合数时写不成). 之后, 证出 $x + y, xy, \psi(p, x, y)$ 三者两两互素, 将命题先分为两种情况: $(x + y, p) = 1$ 和 $(x + y, p) = p$; 再化成为三个模型: $(xy, p) = p$, $(x + y, p) = p$ 和 $(\psi(p, x, y), p) = p$ 分别讨论.

费马方程外形优雅, 无整数解, 其内必有相悖之处, 破解它应依据对立统一规律 (Law of unity of opposites), 即依据变量之间的互素 (Coprime) 关系和系统的可除性 (Divisibility of System).

本文的每一步都是在求索有关等式成立之必要条件, 最后因发现某个等式的必要条件之间存在矛盾而结束. 论述中暗用了两个可以免证的定理, 即“若干个整数与一个分数之和一定不为整数.”以及“两个或多个分数之和有可能为整数.”本文“整数”只指有理整数, “分数”只指不能化成整数之分数, 未加说明的字母表示整数. 文中所谈“因子”, 一般不涉及 1 和 -1. 为简捷, 用 $a \in M$ 表示 a 是 M 之因子, a, M 为代数式. 此外, 再没使用集合论之任何理论和符号.

本文独立成文, 与任何他人文章无关, 特别是与“同余”“某种形式素数的存在性”“无穷递降法”“分圆域”“椭圆曲线”等无关.

本文之所有公式均以最基本、最直观之形式写出.

作者关于 FLT 写了两篇文章, 本文是第一篇, 自始至终着眼于“系统的可除性”, 另一篇用到了“系统中的变量在数值上的比例关系”.

1 互素理论

定理 1 至定理 5 为加法定理, 定理 6 为乘法定理, 定理 7 为二元 p 次型.

定理 1 若 u, v 为整数, $(u, v) = 1$, 则有 $(u + v, uv) = 1$.

证 我们考虑等式 $u + v = w$. 因 $(u, v) = 1$, 若 $(w, u) = t \neq 1$, 除以 t , 左第二项化为分数; 如果 $(w, v) = t \neq 1$, 除以 t , 左第一项化为分数. 显然, 只有 $(w, uv) = 1$, 该式才有可能成立.

本定理证毕.

定理 2 若 u, k, v 为整数, $(u, v)=1$, 则有 $(u + kv, v)=1$.

证 1. 若 $(u, k)=1$, 由 $(u, v)=1$ 有 $(u, kv)=1$, 由定理 1 有 $(u + kv, ukv)=1$. 2. 若 $(u, k)=t \neq 1$, 令 $u = at, k = bt, (a, b)=1$, 于是 $(u + kv, v)=1$ 化为 $(t(a + bv), v)=1$. 再由 $(u, v)=1, u = at$ 有 $(t, v)=1$, 证出 $(a + bv, v)=1$ 成立即可. 由 $(u, v)=1, u = at, (a, b)=1$ 有 $(a, bv)=1$, 由定理 1 有 $(a + bv, abv)=1$. 本定理证毕.

定理 3 u, v, k_i 为整数, $(u, v)=1, k_0 = |k_n| = 1$, 有 $\left(\sum_{j=0}^n k_j u^{n-j} v^j, uv \right) = 1$.

证 $|k_n|=1$ 时, 为便于表述, 将 k_n 写成 $(-1)^c, c$ 为正整数. 于是当 $k_0 = |k_n| = 1$ 时有

$$\sum_{j=0}^n k_j u^{n-j} v^j = u^n + k_1 u^{n-1} v + k_2 u^{n-2} v^2 + k_3 u^{n-3} v^3 + \cdots + k_{n-3} u^3 v^{n-3} + k_{n-2} u^2 v^{n-2} + k_{n-1} u v^{n-1} + (-1)^c v^n. \quad (1)$$

为便于推理, 逐一分离变量, 将(1)化为

$$\sum_{j=0}^n k_j u^{n-j} v^j = u \left\{ u \left(u \cdots u \left[u(u + k_1 v) + k_2 v^2 \right] + k_3 v^3 + \cdots + k_{n-2} v^{n-2} \right) + k_{n-1} v^{n-1} \right\} + (-1)^c v^n. \quad (2)$$

注意观察(2), 令 $\Omega_1 = u + k_1 v$, 有 $\Omega_2 = u \Omega_1 + k_2 v^2, \Omega_3 = u \Omega_2 + k_3 v^3, \cdots, \Omega_{n-1} = u \Omega_{n-2} + k_{n-1} v^{n-1}, \Omega_n = u \Omega_{n-1} + (-1)^c v^n$, 即 $\sum_{j=0}^n k_j u^{n-j} v^j = \Omega_n$. 于是证出 $(\Omega_n, uv)=1$ 成立即可. 由 $(u, v)=1$ 以及定理 2 有

$(u + k_1 v, v)=1$, 此亦即 $(\Omega_1, v)=1$; 且继而, 再由 $(u, v)=1$ 有 $(u \Omega_1, v)=1, (u \Omega_1, v^2)=1$, 再由定理 2 有 $(u \Omega_1 + k_2 v^2, v^2)=1$, 亦即 $(\Omega_2, v^2)=1$; 之后, 不难看出, 再由 $(u, v)=1$ 有 $(u \Omega_2, v^2)=1, (u \Omega_2, v^3)=1, (u \Omega_2 + k_3 v^3, v^3)=1, (\Omega_3, v^3)=1; \cdots (\Omega_{n-1}, v^{n-1})=1, (u \Omega_{n-1}, v^n)=1, (u \Omega_{n-1}, (-1)^c v^n)=1$. 至此, 由定理 1 有 $(u \Omega_{n-1} + (-1)^c v^n, u \Omega_{n-1} (-1)^c v^n)=1$, 即 $(\Omega_n, u \Omega_{n-1} (-1)^c v^n)=1, (\Omega_n, uv)=1$. 本定理证毕.

定理 4 命题 1: 若 a, b, v 为整数, $(a, v)=|v|, (b, v)=1$, 有 $(a + b, v)=1$; 命题 2: 若 a, b, v 为整数, $(a, v)=|v|, (b, v)=1$, 有 $(a + (a + b), v)=1$.

证 令 k, u 为整数, $a = kv, (k, v)=1, b = u$, 命题 1 化为: u, k, v 为整数, $(u, v)=1$, 有 $(u + kv, v)=1$. 显然此乃定理 2 之命题, 已证. 令 $c = a + b$, 命题 2 化为: a, c, v 为整数, $(a, v)=|v|, (c, v)=1$, 有 $(a + c, v)=1$. 与命题 1 相同. 本定理证毕.

定理 5 a, b 为正整数, $ab \neq 1, (a, b)=1$, 有 $a - b \neq 0$. (证略)

定理 6 1. a, b, c, d 为正整数, $(a, b)=(a, c)=(b, d)=1$, 则只有当 $a = d, b = c$ 时, $ab = cd$ 才有可能成立; 2. a, b, c, d 为正整数, $abcd \neq 0, (a, c)=1$, 只有当 $d = Ua, b = Uc, U \neq 0$ 为整数时 $\frac{a}{c} = \frac{d}{b}$ 才有可能成立. (证略)

我们将 d, b 向 Ua, Uc 的转化叫作 U 变换.

定理 7 u, v 为整数, $uv \neq 0, (u, v)=1, p > 3$ 为奇素数, 且令

$$\psi(p, u, v) = \frac{(u+v)^p - (u^p + v^p)}{(u+v)puv}, \quad (3)$$

则有 $u + v, uv, \psi(p, u, v)$ 三者两两互素, 即

$$(u+v, uv) = (u+v, \psi(p, u, v)) = (uv, \psi(p, u, v)) = 1; \quad (4)$$

且 $(u+v, p)=1$ 时, 有

$$((u+v)^{p-1} - puv\psi(p, u, v), p) = 1, \quad (5)$$

$$(u+v, (u+v)^{p-1} - puv\psi(p, u, v)) = 1; \quad (6)$$

$(u+v, p)=p$ 时, 有

$$\left(\frac{(u+v)^{p-1}}{p} - uv\psi(p, u, v), p \right) = 1, \quad (7)$$

$$\left(p(u+v), \frac{(u+v)^{p-1}}{p} - uv\psi(p, u, v) \right) = 1. \quad (8)$$

证 (3) 可化为

$$u^p + v^p = (u+v) \left\langle (u+v)^{p-1} - puv\psi(p, u, v) \right\rangle. \quad (9)$$

由二项式定理有

$$(u+v)^p = u^p + C_p^1 u^{p-1} v + C_p^2 u^{p-2} v^2 + \cdots + C_p^{p-2} u^2 v^{p-2} + C_p^{p-1} u v^{p-1} + v^p, \quad (10)$$

且可化为

$$u^p + v^p = (u+v) \left\langle (u+v)^{p-1} - puv \left\langle \frac{u^{p-2} + v^{p-2}}{u+v} + \frac{C_p^2 (u^{p-4} + v^{p-4})}{p(u+v)} uv + \cdots + \frac{C_p^{p-2}}{p} (uv)^{(p-3)/2} \right\rangle \right\rangle. \quad (11)$$

比较(9)和(11), 有

$$\psi(p, u, v) = \frac{u^{p-2} + v^{p-2}}{u+v} + \frac{C_p^2 (u^{p-4} + v^{p-4}) uv}{p(u+v)} + \cdots + \frac{C_p^{(p-1)/2}}{p} (uv)^{(p-3)/2}. \quad (12)$$

因 p 为奇素数, 所以 $p-2, p-4, p-6, \cdots$ 皆为奇数, 于是 $u^{p-2} + v^{p-2}, u^{p-4} + v^{p-4}, u^{p-6} + v^{p-6}, \cdots$ 一定能被 $u+v$ 整除, 且亦因 p 为奇素数, $\frac{C_p^k}{p}$ 一定为整数 (因为 $C_p^k = \frac{p!}{(p-k)!k!}$, 其中 p 为素数, 且 $k < p$, 分母诸因子均小于 p , 所以分子中的 p 一定不会与分母之任何素因子相约; 若 p 为奇合数, 则不然), 所以(12)之各项皆为整数.

(3) 还可化为

$$\begin{aligned} \psi(p, u, v) = & \frac{1}{puv} \left\{ (u+v)^{p-1} - \langle (u^{p-1} + v^{p-1}) - (u^{p-3} + v^{p-3}) uv + (u^{p-5} + v^{p-5}) (uv)^2 - \right. \\ & \left. \cdots + (-1)^{(p-3)/2} (u^2 + v^2) (uv)^{(p-3)/2} + (-1)^{(p-1)/2} (uv)^{(p-1)/2} \right\} \end{aligned} \quad (13)$$

注意到, 当 j 为偶数时, 有

$$\begin{aligned} u^j + v^j = & (u+v)^j + L_1 (u+v)^{j-2} uv + L_2 (u+v)^{j-4} (uv)^2 + L_3 (u+v)^{j-6} (uv)^3 + \cdots \\ & + L_{(j-4)/2} (u+v)^4 (uv)^{(j-4)/2} + L_{(j-2)/2} (u+v)^2 (uv)^{(j-2)/2} + L_{j/2} (uv)^{j/2}. \end{aligned} \quad (14)$$

至此, 易见(12)和(13)最终皆可转化为

$$\begin{aligned} \psi(p, u, v) = & k_0 (u+v)^{p-3} + k_1 (u+v)^{p-5} uv + k_2 (u+v)^{p-7} (uv)^2 + \cdots \\ & + k_{(p-5)/2} (u+v)^2 (uv)^{(p-5)/2} + k_{(p-3)/2} (uv)^{(p-3)/2}. \end{aligned} \quad (15)$$

因 $p-2$ 为奇数, 由 $a^p + b^p = (a+b)(a^{p-1} - a^{p-2}b + \cdots - ab^{p-2} + b^{p-1})$ 易得

$$u^{p-2} + v^{p-2} = (u+v) \left\langle (u^{p-3} + v^{p-3}) - (u^{p-5} + v^{p-5}) uv + (u^{p-7} + v^{p-7}) (uv)^2 - \cdots + (-1)^{(p-3)/2} (uv)^{(p-3)/2} \right\rangle,$$

显见(12)右第一项可化为

$$(u^{p-3} + v^{p-3}) - (u^{p-5} + v^{p-5})uv + (u^{p-7} + v^{p-7})(uv)^2 - \cdots + (-1)^{(p-3)/2} (uv)^{(p-3)/2}.$$

而(15)右第一项正是由此式第一项 $(u^{p-3} + v^{p-3})$ 转化而来, 于是显见有 $k_0=1$. 事实上, 只要注意到 $(u+v)^{p-3}$ 是由 $(u^{p-3} + v^{p-3})$ 转化而来的, 观察(13)向(15)之转化, 显然有

$$k_0 = \frac{1}{p} (C_{p-1}^1 + 1) = 1. \quad (16)$$

现在来证明 $|k_{(p-3)/2}|=1$. 首先易见 $k_{(p-3)/2}$ 是当 $j=2, 4, 6, \dots, p-1$ 时, (13)中的 $u^j + v^j$ 向(15)中的 $(u+v)^j$ 转化时生成的以 uv 为因子, 不以 $u+v$ 为因子的项 (简称 uv 项) 的系数的代数和. 我们用 σ_j 表示 uv 项的系数, 显见 σ_j 亦即(14)中的 $L_{j/2}$. 例如

$$\begin{aligned} u^2 + v^2 &= (u+v)^2 - 2uv, \quad \sigma_2 = -2; \\ u^4 + v^4 &= (u+v)^4 - 4(u+v)^2 uv + 2(uv)^2, \quad \sigma_4 = 2. \end{aligned}$$

我们先根据(14)挑出(13)中的 uv 项, 即

$$\begin{aligned} \psi(p, u, v) \text{ 中的 } uv \text{ 项} &= \frac{1}{puv} \{0 - \langle \sigma_{p-1} (uv)^{(p-1)/2} - \sigma_{p-3} (uv)^{(p-3)/2} uv + \sigma_{p-5} (uv)^{(p-5)/2} (uv)^2 - \cdots \\ &\quad + (-1)^{(p-3)/2} \sigma_2 uv (uv)^{(p-3)/2} + (-1)^{(p-1)/2} (uv)^{(p-1)/2} \rangle\} \\ &= \frac{1}{p} \{0 - \langle \sigma_{p-1} - \sigma_{p-3} + \sigma_{p-5} - \sigma_{p-7} + \cdots + (-1)^{(p-3)/2} \sigma_2 + (-1)^{(p-1)/2} \rangle\} (uv)^{(p-3)/2}. \end{aligned} \quad (17)$$

再由(17)得到

$$k_{(p-3)/2} = \frac{1}{p} \{0 - \langle \sigma_{p-1} - \sigma_{p-3} + \sigma_{p-5} - \sigma_{p-7} + \cdots + (-1)^{(p-3)/2} \sigma_2 + (-1)^{(p-1)/2} \rangle\} \quad (18)$$

现在来考察 σ_j 的变化规律. 首先注意到 $j \geq 4$ 时, 有

$$u^j + v^j = (u^2 + v^2)(u^{j-2} + v^{j-2}) - (u^{j-4} + v^{j-4})(uv)^2. \quad (19)$$

注意到 j 为偶数, 我们先写出(19)的 uv 项, 即

$$\sigma_j (uv)^{j/2} = \sigma_2 uv \sigma_{j-2} (uv)^{(j-2)/2} - \sigma_{j-4} (uv)^{(j-4)/2} (uv)^2 = (\sigma_2 \sigma_{j-2} - \sigma_{j-4}) (uv)^{j/2}. \quad (20)$$

由(20)易见有

$$\sigma_j = \sigma_2 \sigma_{j-2} - \sigma_{j-4},$$

再由 $\sigma_2 = -2$, 有

$$\sigma_j = -2 \sigma_{j-2} - \sigma_{j-4}. \quad (21)$$

由(21)显然有

$$\begin{aligned} \sigma_6 &= -2 \sigma_4 - \sigma_2 = -2(2) - (-2) = -2, \\ \sigma_8 &= -2 \sigma_6 - \sigma_4 = -2(-2) - 2 = 2, \\ \sigma_{10} &= -2 \sigma_8 - \sigma_6 = -2(2) - (-2) = -2, \\ \sigma_{12} &= -2 \sigma_{10} - \sigma_8 = -2(-2) - 2 = 2, \\ &\dots \end{aligned}$$

从 $j=2$ 起, σ_j 按照 $-2, 2, -2, 2, \dots$ 的规律排列, $j/2$ 为奇, $\sigma_j = -2$, $j/2$ 为偶, $\sigma_j = 2$. 显见, $(p-1)/2$ 为奇数时(18)化为

$$k_{(p-3)/2} = \frac{1}{p} \{0 - \langle (-2) - 2 + (-2) - 2 + \cdots + (-2) - 1 \rangle\}, \quad (22)$$

即

$$k_{(p-3)/2} = \frac{1}{p} \left\{ 0 - \left\langle (-2) \frac{p-1}{2} - 1 \right\rangle \right\} = 1; \quad (23)$$

$(p-1)/2$ 为偶数时(18)化为

$$k_{(p-3)/2} = \frac{1}{p} \{ 0 - \langle 2 - (-2) + 2 - (-2) + \cdots + 2 + 1 \rangle \}, \quad (24)$$

$$k_{(p-3)/2} = \frac{1}{p} \left\{ 0 - \left\langle 2 \cdot \frac{p-1}{2} + 1 \right\rangle \right\} = -1. \quad (25)$$

至此, 我们已经得到 $k_0 = |k_{(p-3)/2}| = 1$. 由 $(u, v) = 1$ 有 $(u+v, uv) = 1$, $((u+v)^2, uv) = 1$, 再由定理 3 有

$$\left(\sum_{j=0}^{(p-3)/2} k_j \langle (u+v)^2 \rangle^{\frac{p-3}{2}-j} (uv)^j, (u+v)^2 uv \right) = 1. \text{ 因(15)即 } \psi(p, u, v) = \sum_{j=0}^{(p-3)/2} k_j \langle (u+v)^2 \rangle^{\frac{p-3}{2}-j} (uv)^j, \text{ 于是, 显然有}$$

$$(\psi(p, u, v), (u+v)^2 uv) = 1, \text{ 再注意到 } (u+v, uv) = 1, \text{ 易见(4)成立.}$$

如果 $(u+v, p) = 1$, 由(4)容易看出有 $((u+v)^{p-1}, puv\psi(p, u, v)) = 1$, 之后, 再由定理 1 不难看出有 $((u+v)^{p-1} - puv\psi(p, u, v), (u+v)^{p-1} puv\psi(p, u, v)) = 1$. 由此知(5)(6)成立.

如果 $(u+v, p) = p$, 由(4)容易看出有 $\left(\frac{(u+v)^{p-1}}{p}, uv\psi(p, u, v) \right) = 1$, 之后, 再由定理 1 不难看出有

$$\left(\frac{(u+v)^{p-1}}{p} - uv\psi(p, u, v), \frac{(u+v)^{p-1}}{p} uv\psi(p, u, v) \right) = 1, \text{ 注意到此时 } \left(\frac{(u+v)^{p-1}}{p}, p \right) = p, \text{ 于是易见(7)(8)成立.}$$

本定理证毕.

将 v 换成 $-v$, 本定理仍成立, 其形式称为减法形式, 写为:

$$\psi(p, u, -v) = \frac{(u-v)^p - (u^p - v^p)}{-(u-v)puv},$$

$$u^p - v^p = (u-v) \langle (u-v)^{p-1} + puv\psi(p, u, -v) \rangle.$$

定理 8 a, b 为正整数, $p > 3$ 为奇素数, 令 $\psi(p, a, b) = \frac{(a+b)^p - (a^p + b^p)}{(a+b)pab}$, 有

$$\psi(p, a, b) - \frac{(a+b)^{p-1} - (a^{p-1} + b^{p-1})}{2ab} < 0.$$

证 被证式亦即

$$\frac{(a+b)^p - (a^p + b^p)}{(a+b)pab} - \frac{(a+b)^{p-1} - (a^{p-1} + b^{p-1})}{2ab} < 0,$$

$$\frac{(a+b)^p - (a^p + b^p)}{(a+b)pab} - \frac{(a+b)^p - (a+b)(a^{p-1} + b^{p-1})}{(a+b)2ab} < 0,$$

$$2 \langle (a+b)^p - (a^p + b^p) \rangle - p \langle (a+b)^p - (a+b)(a^{p-1} + b^{p-1}) \rangle < 0,$$

$$(p-2) \langle (a+b)^p - (a^p + b^p) \rangle - pab(a^{p-2} + b^{p-2}) > 0,$$

展开 $(a+b)^p$, 显见成立. 本定理证毕.

定理 9 a, b 为正整数, $a - 2b > 0$, $0 < \varepsilon < 1$, 有 $1 < \frac{a-b\varepsilon}{a-b} < 2$.

证 由题设条件, 且每一步都时刻注意题设条件, 有

$$0 < 2b < a,$$

$$\begin{aligned}
0 &< 2b - b\varepsilon < a, \\
0 &< b - b\varepsilon < a - b, \\
0 + (a - b) &< b - b\varepsilon + (a - b) < a - b + (a - b), \\
a - b &< a - b\varepsilon < 2(a - b), \\
1 &< \frac{a - b\varepsilon}{a - b} < 2.
\end{aligned}$$

本定理证毕.

2 费马最后定理之证明

定理 10 $p > 3$ 为奇素数, 费马方程

$$x^p + y^p = z^p \quad (26)$$

无两两互素的正整数解 x, y, z .

证 将(26)看成一个等式, 考虑两两互素的正整数 x, y, z 具有怎样的结构及这些结构之间具有怎样的关系时, 它才有可能成立. 我们先寻找这些结构及关系, 然后指出其中的矛盾. 显然, 不妨只考虑 $x < y$ 的情形.

2.1 两种情况

结论 1 若 $x=1$, 则(26)不能成立.

证 令 $x=1, z=(y+1)+t, t \geq 0$ 为整数, 于是, (26)化为 $1+y^p = \langle (y+1)+t \rangle^p$. 显然, 这是一个一定不能成立的式子. 本结论证毕.

令

$$\psi(p, x, y) = \frac{(x+y)^p - (x^p + y^p)}{(x+y)pxy}, \quad (27)$$

则由定理 7 有: $x+y, xy, \psi(p, x, y)$ 三者两两互素, 即

$$(x+y, xy) = (x+y, \psi(p, x, y)) = (xy, \psi(p, x, y)) = 1; \quad (28)$$

$(x+y, p)=1$ 时, (26)可化为

$$(x+y) \left\langle (x+y)^{p-1} - pxy\psi(p, x, y) \right\rangle = z^p, \quad (29)$$

有

$$(x+y, (x+y)^{p-1} - pxy\psi(p, x, y)) = 1; \quad (30)$$

$(x+y, p)=p$ 时, (26)可化为

$$p(x+y) \left\langle \frac{(x+y)^{p-1}}{p} - xy\psi(p, x, y) \right\rangle = z^p, \quad (31)$$

有

$$\left(p(x+y), \frac{(x+y)^{p-1}}{p} - xy\psi(p, x, y) \right) = 1. \quad (32)$$

由(29)(30)(31)(32)显见, 应分为以下两种情况进行讨论:

情况 I: $(x+y, p)=1$;

情况 II: $(x+y, p)=p$.

为揭示 z 与 $x+y$ 之间的关系, 令

$$z = (x + y) - h, \quad (33)$$

显然 h 为正整数, 于是(26)可化为

$$x^p + y^p = \langle (x + y) - h \rangle^p. \quad (34)$$

展开(34), 且注意到由(27)有 $(x + y)^p - (x^p + y^p) = (x + y)pxy\psi(p, x, y)$, 易见有

$$\begin{aligned} & h^p - C_p^{p-1}(x + y)h^{p-1} + C_p^{p-2}(x + y)^2h^{p-2} - C_p^{p-3}(x + y)^3h^{p-3} + \cdots \\ & + C_p^3(x + y)^{p-3}h^3 - C_p^2(x + y)^{p-2}h^2 + C_p^1(x + y)^{p-1}h - (x + y)pxy\psi(p, x, y) = 0. \end{aligned} \quad (35)$$

结论 2 1. 只有 $(h, p) = p$ 且 $((x + y)xy\psi(p, x, y), p) = p$ 时, (35)才可能成立; 2. $(x + y, p) = p$, $(xy, p) = p$, $(\psi(p, x, y), p) = p$, 不能同时有其二, 或同时有其三.

证 除左第一项外, (35)各项明显含有因子 p , 如果 $(h, p) = 1$, 除以 p , 左第一项化为分数, (35)一定不能成立; 而 $(h, p) = p$ 时, 若 $((x + y)xy\psi(p, x, y), p) = 1$, 除以 p^2 , 左最后一项化为分数, (35)亦一定不能成立, 显见第一命题为真. 再由(28)知第二命题为真. 本结论证毕.

结论 3 只有当 h 只在 $(x + y)pxy\psi(p, x, y)$ 内选择因子时, (35)才有可能成立.

证 除左最后一项之外, (35)各项明显含有因子 h , 于是易见, 只有最后一项亦以 h 为因子, 亦即 $\frac{(x + y)pxy\psi(p, x, y)}{h}$ 为整数, (35)才有可能成立. 而 $\frac{(x + y)pxy\psi(p, x, y)}{h}$ 为整数, 只有当 h 只在 $(x + y)pxy\psi(p, x, y)$ 内选择因子时才有可能. 本结论证毕.

结论 4 对于情况 I, 1. 只有当

$$(h, x + y) = (x + y)^{1/p} \quad (36)$$

时, (35)才有可能成立; 2. 令 k, m 为正整数且分别表示 $xy\psi(p, x, y)$ 和 h 所含因子 p 的最高指数, 亦即 $p^k \in xy\psi(p, x, y)$ 且 $\left(\frac{xy\psi(p, x, y)}{p^k}, p\right) = 1$, $p^m \in h$ 且 $\left(\frac{h}{p^m}, p\right) = 1$, 则只当 $k = m$ 时, (35)才有可能成立.

证 除以 $(x + y)$, (35)化为

$$\begin{aligned} & \frac{h^p}{x + y} - C_p^{p-1}h^{p-1} + C_p^{p-2}(x + y)h^{p-2} - C_p^{p-3}(x + y)^2h^{p-3} + \cdots \\ & + C_p^3(x + y)^{p-4}h^3 - C_p^2(x + y)^{p-3}h^2 + C_p^1(x + y)^{p-2}h - pxy\psi(p, x, y) = 0. \end{aligned} \quad (37)$$

不难看出, 只有左第一项亦为整数, (37)才有可能成立, 而显然只有 $(h, x + y) \neq 1$, 左第一项才有可能为整数. 本情况有 $(x + y, pxy\psi(p, x, y)) = 1$, 所以(37)左最后一项不再含有 $(x + y)$ 的任何素因子, 而由 $(h, x + y) \neq 1$ 知(37)左第二项必含 $(x + y)$ 的某些素因子且左第三项至倒数第二项明显含 $(x + y)$ 之全部因子, 于是若 $\left(\frac{h^p}{x + y}, x + y\right) = t \neq 1$, 除以 t 的一个素因子 t_1 , 左最后一项化为分数,

(37)一定不能成立. 无疑只有 $\left(\frac{h^p}{x + y}, x + y\right) = 1$, (37)才有可能成立. 由(30)知本情况 $x + y$ 为一个 p

次幂是(29)成立的必要条件, 所以 $\left(\frac{h^p}{x + y}, x + y\right) = 1$ 可化以为 $\left\langle \frac{h}{(x + y)^{1/p}}, \langle (x + y)^{1/p} \rangle^p \right\rangle = 1$, 且易

见由此有 $\left(\frac{h}{(x + y)^{1/p}}, (x + y)^{1/p}\right) = 1$, $(h, (x + y)^{2/p}) = (x + y)^{1/p}$, 显见第一命题为真; 若 $k > m$, 除以 p^{m+2} , 左倒数第二项化为分数, (37)一定不能成立; 若 $k < m$, 除以 p^{m+1} , 左最后一项化为分数,

(37)亦一定不能成立. 我们注意到当 $k=m$ 时, 除以 $p^{m+\zeta}$, ζ 为正整数, 当 $\zeta=1$ 时, (37)无分数项, 当 $\zeta \geq 2$ 时, 左最后两项同时化为分数, (37)有可能成立. 由此显见第二命题为真. 本结论证毕.

结论 5 对于情况 II, 只有当

$$(h, p(x+y)) = \langle p(x+y) \rangle^{1/p} \quad (38)$$

时, (35)才有可能成立.

证 除以 $p(x+y)$, (35)化为

$$\begin{aligned} & \frac{h^p}{p(x+y)} - \frac{C_p^{p-1}}{p} h^{p-1} + \frac{C_p^{p-2}}{p} (x+y) h^{p-2} - \frac{C_p^{p-3}}{p} (x+y)^2 h^{p-3} + \cdots \\ & + \frac{C_p^3}{p} (x+y)^{p-4} h^3 - \frac{C_p^2}{p} (x+y)^{p-3} h^2 + \frac{C_p^1}{p} (x+y)^{p-2} h - xy\psi(p, x, y) = 0. \end{aligned} \quad (39)$$

p 为奇素数, C_p^k/p 一定为整数, 易见除了左第一项外, (39)各项皆为整数. 无疑, 只有左第一项亦为整数, (39)才有可能成立. 而显见, 只有 $(h, p(x+y)) \neq 1$, 左第一项才有可能为整数. 注意到本情况 $(p(x+y), xy\psi(p, x, y)) = 1$, 所以(39)左最后一项不再含 $p(x+y)$ 之任何素因子, 且显见由 $(h, p(x+y)) \neq 1$ 知左第二项必含 $p(x+y)$ 之某些素因子, 且左第三项至倒数第二项均含 $p(x+y)$ 之全部因子, 于是若 $\left(\frac{h^p}{p(x+y)}, p(x+y)\right) = t \neq 1$, 除以 t 的一个素因子 t_1 , 左最后一项化为分数, (39)一定不能成立. 只有 $\left(\frac{h^p}{p(x+y)}, p(x+y)\right) = 1$, (39)才可能成立. 由(32)知本情况 $p(x+y)$ 为一个 p 次

幂是(31)成立的必要条件, 于是 $\left(\frac{h^p}{p(x+y)}, p(x+y)\right) = 1$ 可化为 $\left[\left\langle \frac{h}{\langle p(x+y) \rangle^{1/p}} \right\rangle^p, \langle \langle p(x+y) \rangle^{1/p} \rangle^p\right] = 1$,

由此有 $\left(\frac{h}{\langle p(x+y) \rangle^{1/p}}, \langle p(x+y) \rangle^{1/p}\right) = 1$, $(h, \langle p(x+y) \rangle^{2/p}) = \langle p(x+y) \rangle^{1/p}$, 易见本结论成立. 本结论证毕.

为揭示 x, y, z, h 之间的关系, 令

$$x = z - r, \quad (40)$$

$$y = z - s, \quad (41)$$

显然 r, s 为正整数. 于是(26)(34)分别化为

$$(z-r)^p + (z-s)^p = z^p, \quad (42)$$

$$(z-r)^p + (z-s)^p = \left\{ \langle (z-r) + (z-s) \rangle - h \right\}^p. \quad (43)$$

注意到 $z = \langle (z-r) + (z-s) \rangle - \langle z - (r+s) \rangle$, 于是(42)可写为

$$(z-r)^p + (z-s)^p = \left\{ \langle (z-r) + (z-s) \rangle - \langle z - (r+s) \rangle \right\}^p. \quad (44)$$

由(43)(44)有

$$h = z - (r+s), \quad (45)$$

且由此有

$$z - r = s + h, \quad (46)$$

$$z-s=r+h, \quad (47)$$

$$z=r+s+h. \quad (48)$$

于是(42)又可写为

$$(s+h)^p+(r+h)^p=(r+s+h)^p. \quad (49)$$

$$(s+h)^p+(r+h)^p=z^p. \quad (49-1)$$

展开(42)有

$$\begin{aligned} & z^p - C_p^1(r+s)z^{p-1} + C_p^2(r^2+s^2)z^{p-2} - C_p^3(r^3+s^3)z^{p-3} + \cdots \\ & + C_p^{p-3}(r^{p-3}+s^{p-3})z^3 - C_p^{p-2}(r^{p-2}+s^{p-2})z^2 + C_p^{p-1}(r^{p-1}+s^{p-1})z - (r^p+s^p) = 0. \end{aligned} \quad (50)$$

结论 6 对(42)的讨论, 只考虑 z, r, s 三者两两互素之情形即可.

证 由本定理的题设 x, y, z 两两互素以及(40)(41)有 $(z-r, z-s) = (z-r, z) = (z-s, z) = 1$. 注意到只有当 $(z, r) = 1$ 时, $(z-r, z) = 1$ 才有可能成立, 如若 $(z, r) = t \neq 1$, 则一定有 $(z-r, z) = t \neq 1$, 与 $(z-r, z) = 1$ 相悖. 同理, 只有当 $(z, s) = 1$ 时, $(z-s, z) = 1$ 才有可能成立. 且易见当 $(z, rs) = 1$ 时, 只有 $(r, s) = 1$, (50)才有可能成立, 因如果 $(r, s) = t \neq 1$, 除了左第一项外, (50)各项均含因子 t , 除以 t , 左第一项将化为分数. 本结论证毕.

由定理 7, 且注意到 $(z-r) + (z-s) = z + \langle z - (r+s) \rangle$, 易见(42)亦可写为

$$\langle (z-r) + (z-s) \rangle \left\{ \langle (z-r) + (z-s) \rangle^{p-1} - p(z-r)(z-s)\mu(p, z-r, z-s) \right\} = z^p, \quad (51)$$

$$\left\{ z + \langle z - (r+s) \rangle \right\} \left\{ \left\{ z + \langle z - (r+s) \rangle \right\}^{p-1} - p(z-r)(z-s)\mu(p, z-r, z-s) \right\} = z^p, \quad (52)$$

$((z-r) + (z-s), p) = p$ 时, 还可写为

$$p \left\{ z + \langle z - (r+s) \rangle \right\} \left\{ \frac{\left\{ z + \langle z - (r+s) \rangle \right\}^{p-1}}{p} - (z-r)(z-s)\mu(p, z-r, z-s) \right\} = z^p; \quad (53)$$

且 $((z-r) + (z-s), p) = 1$ 时有

$$\left(z + \langle z - (r+s) \rangle, \left\{ z + \langle z + (r+s) \rangle \right\}^{p-1} - p(z-r)(z-s)\mu(p, z-r, z-s) \right) = 1, \quad (54)$$

$((z-r) + (z-s), p) = p$ 时有

$$\left(p \left\{ z + \langle z - (r+s) \rangle \right\}, \frac{\left\{ z + \langle z - (r+s) \rangle \right\}^{p-1}}{p} - (z-r)(z-s)\mu(p, z-r, z-s) \right) = 1. \quad (55)$$

结论 7 对于情况 I, 即 $((z-r) + (z-s), p) = 1$ 时, 只有令

$$z = qA, \quad (56)$$

$$r+s = qB, \quad (57)$$

$$(A, B) = 1, \quad (58)$$

$$h = q(A-B), \quad (59)$$

$$(q, A(A-B)) = 1, \quad (60)$$

$$(z-r) + (z-s) = q^p, \quad (61)$$

$$(h, (z-r) + (z-s)) = q, \quad (62)$$