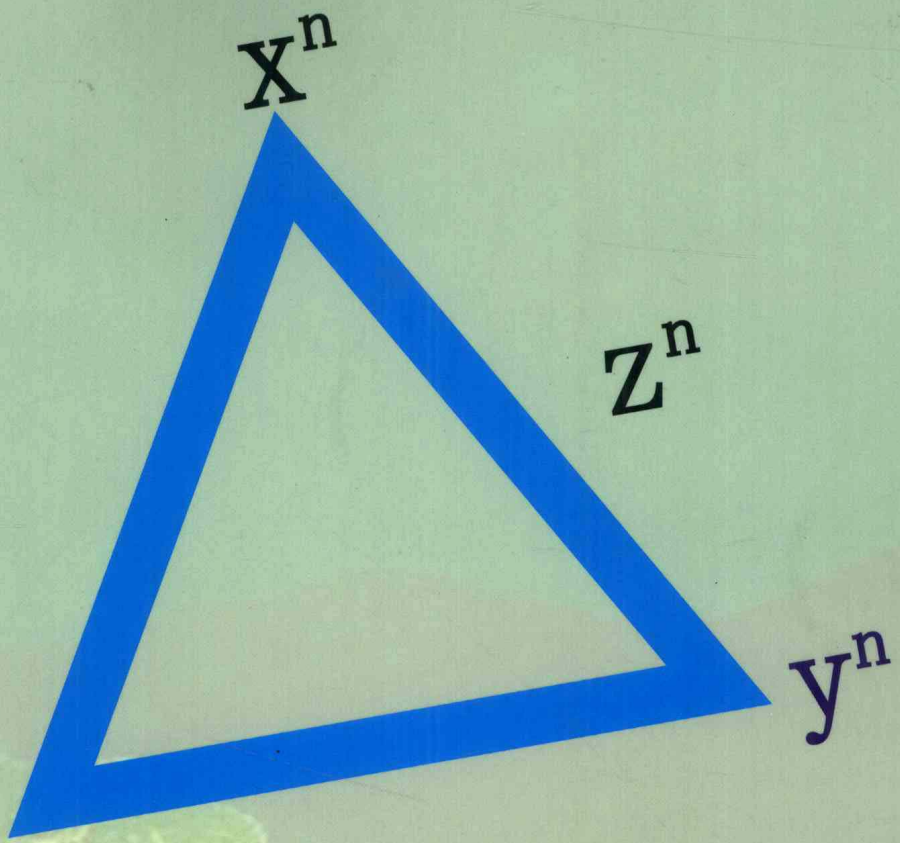
中图分类O156



费马大定理证明之研究

STUDY OF PROOF OF FERMAT'S LAST THEOREM

胡振武◉著

只需证明**两个**指数

只需证明**两种**情形

费马大定理证明之研究

STUDY OF PROOF OF FERMAT'S LAST THEOREM

胡振武◉著

二00七年九月

目录

1. 费马大定理 ……1
1.1 费马其人 ……1
1.2 费马大定理 ……2
2. 前人的成果 ……4
2.1 理论和方法 ……4
2.1.1 整数的整除性 ……4
2.1.2 多项式恒等定理 ……6
2.1.3 排列、组合、二项式定理 ……8
2.1.4 素数和算术基本定理 ……10
2.1.5 同余和同余式 ……11
2.1.6 平凡解和原始解 ……12
2.1.7 只需证两个指数 ……13
2.1.8 只需证两种情形 ……13
2.1.9 费马小定理 ……13
2.1.10 无穷递降法 ……13
2.1.11 巴罗和阿贝尔的关系式 ……14
2.1.12 热尔曼的理论和勒让德 ……15
2.1.13 溫特的定理 ……17
2.1.14 马斯寿太斯和波美的证明 ……18
2.1.15 依恩柯利的证明 ……18
2.1.16 斯维斯塔克的证明 ……18
2.1.17 哥德兹海的证明 ……19
2.1.18 劳的证明 ……19
2.1.19 培利兹—卡绍的证明 ……19
2.1.20 惠维兹的证明 ……19
2.1.21 初等估计 ……20
2.1.22 数集、数环和数域 ……26
2.1.23 分圆域和理想数 ……28
2.1.24 代数数论 ……33
2.1.25 费马曲线 ……33

2.2 指数n各次数的证明 ……33
2.2.1 指数n=2 勾股定理(毕达哥拉斯定理) ……33
2.2.2 指数n=3 ……36
2.2.2.1 初等证明 ……37
2.2.2.2 欧拉的证明 ……40
2.2.2.3 高斯的证明 ……42
2.2.3 指数n=4 ……45
2.2.3.1 费马的证明 ……45
2.2.3.2 贝西、莱布尼茨、欧拉的证明 ……47
2.2.4 指数n=5 ……47
2.2.5 指数n=7 ……48
2.2.6 指数n=P ……49
2.2.7 指数P<41000000 ……49
2.3 其它的成果 ……50
2.3.1 莫利斯玛等 ……50
2.3.2 依恩柯利和卡绍 ……50
2.3.3 依恩柯利和海罗 ……50
2.3.4 特亚尼安 ……50
2.3.5 罗特凯也维奇 ……50
2.3.6 爱斯勒 ……51
2.3.7 波鲁克内 ……51
2.3.8 曼福 ……51
2.3.9 欧拉数 ……51
2.3.10 莫德尔猜想和伐尔廷斯 ……52
2.3.11 爱德列曼和海斯一布朗 ……54
2.3.12 数理逻辑方法 ……54
2.4 拓展的成果 ……55
2.4.1 费马的成果 ……55
2.4.1.1 素数形式 ……55
2.4.1.2 4n+1和4n+3 ……55
2.4.1.3 直角三角形斜边 ……55
2.4.1.4 直角三角形面积 ……55

2.4.1.5 平方数之和 ……55
2.4.1.6 $A=a^2-K$ ……56
2.4.1.7 $x^2+2=y^3$ ……56
2.4.1.8 费马数 F_n ……56
2.4.2 $x^3+y^3+z^3=w^3$ ……56
2.4.3 $x^3+y^3+z^3=n$ ……58
2.4.4 $x^3+y^3=kz^3$ ……60
2.4.5 $\Sigma x_i^4=y^4$ ……62
2.4.6 $x^4+y^4=z^4+t^4$ ……63
2.4.7 $\Sigma x_i^4=\Sigma y_i^4$ ……63
2.4.8 $\Sigma x_i^4=ky^2$ ……63
2.4.9 $x^4+ky^4=z^2$ ……64
2.4.10 $\Sigma x_i^j=y^j$ ……66
2.4.11 $ax^m+by^n=cz^p$ ……66
2.4.12 $x^2\pm y^2=z^n$ ……67
2.5 蒋春暄的证明 ……69
2.5-1 用P阶复双曲函数 ……69
2.5.2 用4n阶复双曲函数 ……71
2.6 怀尔斯的证明 ……74
2.6.1 模形式 ……74
2.6.2 谷山一志村猜想 ……74
2.6.3 弗赖方程 ……75
2.6.4 怀尔斯证明谷山一志村猜想 ……75
2.6.5 不是费马设想的证明 ……77
3. 本人的证明 ……78
3.1 证明方法 ……78
3.1.1 带余数除法定理 ……78
3.1.2 多项式恒等定理 ……78
3.1.3 同余理论 ……79
3.1.4 费马小定理 ……79
3.1.5 无穷递降法 ……80

3.1.6 只需证明两个指数 ……80
3.1.7 只需证明两种情形 ……81
3.2 指数 $n=p$ ……81
3.3 指数 n ……98
3.4 费马方程的几何意义 ……109
参考文献 ……110
论文 ……111
p次费马方程证明 ……111
The Proof of the Fermat's equation of Degree p (英文)
……116
后记 ……122

Contents

1. The Fermat's Last Theorem ……1
1.1 The Fermat its person ……1
1.2 The Fermat's Last Theorem ……2
2. Predecessor's Results ……4
2.1 Theory and Method ……4
2.1.1 Integer divisibility ……4
2.1.2 Multinomial identically equal theorem ……6
2.1.3 Arrangement, Combination, Binomial theorem ……8
2.1.4 Prime number and Arithmetical fundamental theorem ……10
2.1.5 Congruence and Congruent equality ……11
2.1.6 Ordinary solution and Primitive solution ……12
2.1.7 Only must prove two exponent ……13
2.1.8 Only must prove two situations ……13
2.1.9 The Fermat's small theorem ……13
2.1.10 The Method of the Infinite Descent ……13
2.1.11 The Relational formula of Barlow and Abel ……14
2.1.12 Germain's theory and Legendre ……15
2.1.13 Wendt's theorem ……17
2.1.14 Massouties and Pomey Proof ……18
2.1.15 Inkeri's Proof ……18
2.1.16 Swistak's Proof ……18
2.1.17 Goldziher's Proof ……19
2.1.18 Rao's Proof ……19
2.1.19 Pérez-Cacho Proof ……19
2.1.20 Hurwitz's Proof ……19
2.1.21 Elementary Estimates ……20
2.1.22 Numbers Assemble, Number Ring, and Number Field ……26
2.1.23 Cyclotomic Field and Ideal ……28
2.1.24 The Algebraic Number Theory ……33
2.1.25 The Fermat's Curve ……33

2.2 Exponent various numbers of Degree Proof ……33
2.2.1 Exponent $n=2$, The Pythagorean Theorem ……33
2.2.2 Exponent $n=3$ (Cubic) ……36
2.2.2.1 Elementary Proof ……37
2.2.2.2 Euler's Proof ……40
2.2.2.3 Gauss's Proof ……42
2.2.3 EXponent $n=4$ (Biquadratic) ……45
2.2.3.1 Fermat's Proof ……45
2.2.3.2 Bessy, Leibniz, Euler Proof ……47
2.2.4 Exponent $n=5$ (Quintic) ……47
2.2.5 Exponent $n=7$ (Degree Seven) ……48
2.2.6 Exponent $n=p$ ……49
2.2.7 Exponent $p<41,000,000$ ……49
2.3 Other Results ……50
2.3.1 Morishima et al ……50
2.3.2 Inkeri and Cacho ……50
2.3.3 Inkeri and Hyyrö ……50
2.3.4 Terjanian ……50
2.3.5 Rotkiewicz ……50
2.3.6 Eichler ……51
2.3.7 Brückner ……51
2.3.8 Mumford ……51
2.3.9 The Euler Numbers ……51
2.3.10 The Mordell's Conjecture and Faltings ……52
2.3.11 Adleman and Health-Brown ……54
2.3.12 The Method of the Mathematical Logicians ……54
2.4 Extensions Results ……55
2.4.1 The Fermat's Results ……55
2.4.1.1 Prime Number Form ……55
2.4.1.2 $4n+1$ and $4n+3$ ……55
2.4.1.3 Right triangle Hypoteneuse ……55
2.4.1.4 Right triangle Area ……55

2.4.1.5 The Sum of the Square Numbers ……55
2.4.1.6 $A=a^2-K$ ……56
2.4.1.7 $x^2+2=y^3$ ……56
2.4.1.8 The Fermat's Numbers Fn ……56
2.4.2 $x^3+y^3+z^3=w^3$ ……56
2.4.3 $x^3+y^3+z^3=n$ ……58
2.4.4 $x^3+y^3=kz^3$ ……60
2.4.5 $\sum x_i^4=y^4$ ……62
2.4.6 $x^4+y^4=z^4+t^4$ ……63
2.4.7 $\sum x_i^4=\sum y_i^4$ ……63
2.4.8 $\sum x_i^4=ky^2$ ……63
2.4.9 $x^4+ky^4=z^2$ ……64
2.4.10 $\sum x_i^j=y^j$ ……66
2.4.11 $ax^m+by^n=cz^p$ ……66
2.4.12 $x^2\pm y^2=z^n$ ……67
2.5 The Jiang Chunxuan's Proof ……69
2.5.1 Used the Order P Complex Hyperbolic Function ……69
2.5.2 Used the Order 4n Complex Hyperbolic Function ……71
2.6 The Wiles's Proof ……74
2.6.1 The Modular Form ……74
2.6.2 The Yutaka Taniyama-Goro Shimura Conjecture ……74
2.6.3 The Frey's Equation ……75
2.6.4 Wiles proves the Y-G Conjecture ……75
2.6.5 His proof which Fermat's Conceives is not same ……77
3. Myself Proof ……78
3.1 Proof Method ……78
3.1.1 The Complement of a number division Theorem ……78
3.1.2 The Multinomial Identically Theorem ……78
3.1.3 The Congruence Theorem ……79
3.1.4 The Fermot's small Theorem ……79

3.1.5 The Method of the Infinite Descent ……80
3.1.6 Only must prove two exponent ……80
3.1.7 Only must prove two situations ……81
3.2 Exponent $n=p$ ……81
3.3 Exponent n ……98
3.4 The Fermat's Equation Geometry Meanings ……109

Bibliography ……110

Paper ……111
p 次费马方程证明 (Chinese) ……111
The Proof of the Fermat's Equation of Degree p ……116

Postscript ……122

1.费马大定理

1.1 费马其人

皮埃尔·德·费马(Pierre de Fermat)是十七世纪最卓越的数学家之一。1601年8月17日出生于法国南部图卢兹附近的博蒙—德洛马涅。他的父亲多米尼克·费马是当地的大皮革商,拥有相当丰厚的产业,由于富有和经营有道,颇受人们尊敬,并因此获得了地方事务顾问的头衔。他从小生活在富裕舒适的环境中。他的母亲克拉莱·德·罗格,出身穿袍贵族。父亲的大富与母亲的大贵构成了他极富贵的身价。他受到叔叔良好的启蒙教育,培养了他广泛的兴趣和爱好,影响了他的性格。他14岁时进入博蒙—德洛马涅公学,毕业后先后在奥尔良大学和图卢兹大学学习法律。十七世纪的法国,男子最讲究的职业是当律师,因此,男子学习法律成为时髦,使人敬羡。当时的法国为那些有产的而缺少资历的"准律师"尽快成为律师创造了很好的条件。他尚未大学毕业,便在博蒙—德洛马涅买好了"律师"和"参议员"的职位。等到1631年,他毕业返回家乡后,便很容易地当上了图卢兹法院的律师和图卢兹议会的议员。他从步入社会直到去世都没有失去官职,而且逐年得到提升。在任了七年地方议会议员后,升任了调查参议员,这个官职有权对行政当局进行调查和质询。1642年,当时最高法院顾问勃里斯亚斯推荐他进入最高刑事法庭和法国大理院主要法庭,使他有了以后更好的升迁机会。1646年他升任议会首席发言人。以后还当过天主教联盟主席等职。他的官场生活没有什么突出政绩值得称道,但他从不利用职权向人们勒索,从不受贿,为人敦厚,公正廉明,而且法律知识渊博,赢得了人们的信任和称赞。他的婚姻使他跻身于穿袍贵族的行列,他娶了他的舅表妹露伊丝·德·罗格,原本就为母亲的贵族血统而感到骄傲的他,如今干脆在自己的姓名上加上贵族姓氏的标志"德"。

费马生有三女二男,大女儿出嫁,其他两个女儿都当上了牧师,次子当上了菲玛雷斯的副主教。长子萨穆尔,不仅继承了他的公职,在1665年当上了律师,而且还整理了他的数学论著。如果不是其长子积极出版他的数学论著,很难说他能对数学产生如此重大的影响,因为大部分论文都是在他死后,由其长子负责发表的。萨摩尔称得上是费马事业的继承人。

费马真正的事业是学术,尤其是数学。他通晓法语、意大利语、西班牙语、拉丁语、希腊语,而且还颇有研究。语言方面的博学给他的数学研究提供了语言工具和便利,使他有能力学习和了解阿拉伯和意大利的代数以及古希腊的数学,为他的数学造诣奠定了良好基础。在数学上不仅可以在数学王国里自由驰骋,而且还可以站在数学天地之外鸟瞰数学,这与他的数学天赋和博学多才有关。他博览群书,见多识广,业余时间喜欢恬静生活,全部精力花费在钻研数学和物理问题上,有时用希腊文、拉丁文、西班牙文写诗作词,自我朗诵消遣。他生性内向,谦抑好静,鄙薄名利,不善推销自己,不善展示自己,因此,他生前极少发表自己的论著,连一部完整的著作也没有出版。他发表的一些文章,也总是隐姓埋名。他的远见卓识见之于他与同时代学者

的信件和一批以手稿形式传播的论文。他的崇拜者常常催促他发表著述，但都遭到拒绝。他的很多论述，特别在数论方面的论述，从来没有正式发表过。他死后，很多论述遗留在故纸堆里，或阅读过的书的页边空白处，书写的年月无从查考；还有的保留在他给朋友们的书信中。他的长子萨摩尔·费马将遗稿进行整理，将其笔记、批注及书信整理成书，汇编成册；《数学论集》共分两卷，分别于1670年和1679年在图卢兹出版；第一卷有丢番图的《算术》，带有校订和注解；第二卷包括抛物形求面积法、极大极小及重心的论述，各类问题的解答，这些内容后来成为微积分的一部分；还有球切面、曲线求长等；另有他和数学家、物理学家笛卡儿、帕斯卡、惠更斯等的通讯函件。费马大定理即以这种方式公布于世。时间性对于科学非常重要，在十七世纪这个问题也相当突出，费马的数学研究成果不及时发表，得不到传播和发展，并不完全是个人的名誉损失，而是影响了那个时代数学前进的步伐。

费马一生身体健康，只是在1652年的瘟疫中险些丧命。1665年元旦刚过，他开始感到身体有变，因此于1月10日停职，第三天即去世，被安葬在卡斯特雷斯公墓，后来改葬在图卢兹的家族墓地中。

费马从未受过专门的数学教育，数学研究不过是业余爱好，研究的方式也颇不正规，但成果非凡，被人们誉为“业余数学大师”、“业余数学家之王”。他和笛卡儿(Descartes 1596—1650)分享创立解析几何的荣誉；他和牛顿(Newton 1642—1727)、莱布尼茨(Leibniz 1646—1716)一样对微积分的诞生作出重要贡献；他发展了组合论原理，和帕斯卡(Pascal 1623—1662)、惠更斯(Huygens 1629—1695)同是概率论的开拓者；他是公认的数学分析的先驱之一；他独撑十七世纪数论天地，他的名字几乎是数论的同义语，他给出素数的近代定义，提出一些重要命题；“费马大定理”、“费马小定理”、“费马数”、“费马螺线”、“费马最小光程原理”等都和费马的名字紧紧相连；费马对约方问题也相当重视，对约方数学结构有兴趣，把构成约方的思想扩充到空间，即组成具有与约方类似性质的立方体，约方理论对解方程组有用。

1.2 费马大定理

古希腊数学家丢番图(Diophantus 246—330)著《算术》一书。1621年，数学家巴切(Bachet de Meziriac 1581—1638)将该书从希腊文译成拉丁文在法国出版。费马买到该译本，对其中的数论问题极感兴趣，公余时间对一些问题进行研究和推广。当读到第二卷第八命题“将一个平方数分为两个平方数”时，他想到了更一般的问题，在页边空白处用拉丁文写了一段话：“将一个立方数分为两个立方数，一个四次幂分为两个四次幂，或者一般地将一个高于二次的幂分为两个同次的幂，这是不可能的。关于此，我确信已发现一种奇妙的证法，可惜这里的空白太小，写不下。”

这段叙述用现代数学语言来说，就是：方程

$x^n + y^n = z^n$ 当整数指数 $n>2$ 时，没有正整数解。

这就是费马大定理，更多地叫做费马最后定理（Fermat's Last Theorem），简记为FLT。名字的来源很大可能是费马提出很多数论命题，到1840年左右，只剩下FLT没有被人证明，因此称为最后定理。中国较普遍叫做费马大定理，是为了区别费马小定理。

数学家希尔伯特（Hilbert 1862－1943）认为，鉴别好的数学问题的一般准则有两条，首先是问题应具有"清晰性和易懂性，因为清楚的、易于理解的问题吸引着人们的兴趣，而复杂的问题使人望而生畏"；"其次，为着具有吸引力，应该是困难的，但却不应是完全不可解决而使我们白费气力"。

FLT就是这样一个好的数学命题，它形式简单，内容易懂，连中学生都可以理解；实践证明它又是十分困难的问题。1900年在巴黎召开的国际数学家代表大会上，希尔伯特做了一次震动数学界的讲演，他站在数学发展的前沿，高瞻远瞩地提出尚待解决的二十三个问题。这些问题的解决大都是相当困难的。他没有把FLT列入二十三个问题中，但把它作为一个典型例子，说明这样一个非常特殊、似乎不十分重要的问题会对科学产生怎样令人鼓舞的影响。

据说希尔伯特曾宣称他能证明FLT，但他认为，在解决FLT的过程中能给数学发展创造许多新途径，一旦解决了这个难题，这些有益的副产品就得不到了，所以他避而不去解决它。他满怀深情地说："我应更加注意，不要杀掉这只经常为我们生出金蛋的母鸡。"在这里，我以为，对于证明FLT一事，费马不会自我欺骗，希尔伯特可能故弄玄虚。

在解决FLT的过程中，数学家们在享受研究FLT的乐趣的同时，还充分意识到其研究成果的影响不限于解决FLT，势必推动数学许多分支的发展，从而促进科学技术的进步以及整个人类的文明。科学技术生产力和精神力量是无法从经济上计算价值的，故称它们为"无价之宝"。如果哪个国家的数学家能在这个问题上取得重大突破，或者给予最后解决，无疑标志着这个国家至少在这个问题上处于领先地位。希尔伯特说得好："在数学中没有不可知。"

2.前人的成果

2.1 理论和方法

2.1.1 整数的整除性

$1,2,3,\cdots,n,\cdots$，叫做正整数，又叫自然数，其中$1,3,5,7,9,\cdots$，叫做奇数，$2,4,6,8,10,\cdots$，叫做偶数；$-1,-2,-3,\cdots,-n,\cdots$，叫做负整数；正整数、负整数和零统称整数。两个整数的和、差、积仍为整数，但两个整数相除(除数不为零)，所得的商却不一定是整数。因此，许多整数问题都与整数除法有关，研究这些问题，就是整数的整除性。

用$[\alpha]$表示不超过α的最大整数，例如，$[-4.5]=-5$，$[2]=2$，$[\pi]=3$，$[6.4]=6$.

关于$[\alpha]$，显然下面不等式成立：$[\alpha]\leqslant\alpha<[\alpha]+1$ (1)

取α为有理数$\frac{a}{b}$(a,b为整数，$b>0$)，则由(1)可以得 $0\leqslant\frac{a}{b}-[\frac{a}{b}]<1$

或 $0\leqslant a-b[\frac{a}{b}]<b$ 由此可得 $a=[\frac{a}{b}]b+r$，$0\leqslant r<b$ (2)

因此，得到下面的定理.

定理1(带余数除法)任给两个整数a，$b>0$，必存在两个整数q及r，使得

$$a=qb+r,\quad 0\leqslant r<b,$$ 并且q及r是唯一的 (3)

证明 (2)已经指明存在性，只要证明唯一性就够3。若还存在整数q_1及r_1，使得

$$a=q_1b+r_1,\quad 0\leqslant r_1<b \tag{4}$$

则从(3)和(4)可得 $qb+r=q_1b+r_1$，即有 $b|q-q_1|=|r-r_1|$，因为r及r_1为$<b$的正数，所以$|r-r_1|<b$，若$q\neq q_1$，则有$|r-r_1|\geqslant b$，得出矛盾。故有$q=q_1$，从而推出$r=r_1$.

证毕。

(3)中的q叫做不完全商，r叫做余数。当$r=0$时，(3)变成 $a=qb$,(5)这时就说b整除a，或a被b整除，b是a的因数，a是b的倍数。用$b|a$表示b整除a，用$b\nmid a$表示b不整除a.

下面是整除的一些简单性质。

1)若$a|b$，$b|c$，则$a|c$.

证明 因为$a|b$，$b|c$，故有整数q_1，q_2使 $b=q_1a$，$c=q_2b$，因此，$c=q_1q_2a$，由于q_1q_2是整数，所以$a|c$. □(代表证毕)

2)若$a|b$，则$a|bc$，c是任意整数。

证明 因为$a|b$，则有整数q使$b=qa$，因此，$bc=(qc)a$，由于qc是整数，所以$a|bc$. □

3)若$a|b$，$a|c$，则$a|(b\pm c)$.

证明 因为$a|b$，$a|c$，则有整数q_1，q_2使 $b=q_1a$，$c=q_2a$，因此$b\pm c=(q_1+q_2)a$.

又$(q_1\pm q_2)$是整数，所以$a|(b\pm c)$ □

4) 若 $a|b_i$，$i=1,2,\cdots,n$，则 $a|(k_1b_1+k_2b_2+\cdots+k_nb_n)$，$k_i$，$i=1,2,\cdots,n$ 是任意整数。由4)可推出

5) 若在一个等式中，除某项外其余各项都是 a 的倍数，则此项也是 a 的倍数。

6) 若 $a|b$，$b|a$，则 $b=\pm a$.

证明 令 a,b 都不为零。因为 $a|b$，$b|a$，则有整数 q_1，q_2 使 $b=aq_1$，$a=bq_2$，因此 $a=aq_1q_2$，约去 a 得 $1=q_1q_2$，整数 q_1，q_2 的积为1，故此两个整数必都为 ±1，因而 $b=\pm a$. □

用 $|a|$ 表示 a 的绝对值，例如，$|5|=|-5|=5$.

现在讨论两个整数的因数与倍数问题。

设 a,b 是两个数，若 d 是 a 的因数，也是 b 的因数，则 d 叫做 a,b 的一个公因数。a,b 所有公因数中最大的一个叫做 a,b 的最大公因数，记作 (a,b)；特别，若 $(a,b)=1$，则称 a,b 互素。a,b 的公因数与 $|a|,|b|$ 的公因数相同，因而有 $(a,b)=(|a|,|b|)$，因此，讨论最大公因数，可以就非负整数去讨论。

辗转相除法，可以用来求两个正整数的最大公因数，而且还可以借此推导出最大公因数的一些重要性质。这个方法是我国古代数学家首先创造的，在古算书里叫求一术，但在国外叫欧几里得(Euclide 约前330—275)除法。

设 a,b 是任意两个正整数，且 $a>b$，由带余数除法，可以得到下列等式：

$$\begin{aligned}
&a=bq_1+r_1,\quad 0<r_1<b\\
&b=r_1q_2+r_2,\quad 0<r_2<r_1\\
&\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n,\quad 0<r_n<r_{n-1}\\
&r_{n-1}=r_nq_{n+1}+r_{n+1},\quad r_{n+1}=0
\end{aligned}\tag{6}$$

因为每进行一次带余数除法，余数至少减1，而 b 是有限的，所以最多进行 b 次带余数除法，可以得到一个余数为零的等式，即 $r_{n+1}=0$ 这就是辗转相除法。

定理2 若 a,b,c 是三个不全为零的整数，且 $a=bq+c$，则 $(a,b)=(b,c)$.

定理3 设 a,b 是任意两个正整数，则 $(a,b)=r_n$.

证明 利用(6)及定理2可以得到 $r_n=(0,r_n)=(r_{n+1},r_n)=(r_n,r_{n-1})=\cdots=(r_1,b)=(a,b)$ □

定理3给出一个求最大公因数的实际方法，当 a,b 中有一个为零时，(a,b) 等于不为零的那个数；当 a,b 都不为零，$(a,b)=r_n$.

推论 若 $(a,b)=d$，则存在两个整数 s,t，使 $as+bt=d$

现在给出最大公因数的两个重要性质：

设 a,b 是两个正整数，则

1) $(am,bm)=(a,b)m$，m 为任意正整数。

2) 若 d 是 a,b 的任一公因数，则 $\left(\frac{a}{d},\frac{b}{d}\right)=\frac{(a,b)}{d}$ 特别有 $\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$

现在给出互素的两个性质：

1) 若 $(a,b)=1$，$a|bc$，则 $a|c$

证明 因为 $(a,b)=1$，由推论可知，存在整数 s,t，使 $as+bt=1$，从而

$$acs+bct=c \tag{7}$$

由题设 $a|bc$，故 a 整除(7)的左端每一项，因此 $a|c$. □

2) 若 b 与 $a_1,a_2,\cdots,a_n$ 都互素，则 b 与 $a_1a_2\cdots a_n$ 互素。

证明 由题设及推论，对于 a_i、b 存在整数 s_i，t_i，使 $bs_i+a_it_i=1$，$i=1,2,\cdots,n$

把所有这 n 个式子乘起来，右边得 1，左边有 2^n 项，其中有一项包含 $a_1a_2\cdots a_n$，而其余各项都包含 b，所以乘起来的式子可写成 $bs+a_1a_2\cdots a_nT=1$

由此可见，b 和 $a_1a_2\cdots a_n$ 任何公因式必整除 1，故两者互素。□

下面研究最小公倍数。

设 a,b,m 是正整数，若 $a|m$，$b|m$，则称 m 是 a,b 的一个公倍数。a,b 所有公倍数中最小的一个叫做 a,b 的最小公倍数，记作 $[a,b]$.

关于两个数的最大公因数与最小公倍数的关系有下面的定理：

定理4 $[a,b]=\frac{ab}{(a,b)}$. 特别地，若 $(a,b)=1$，则 $[a,b]=ab$.

最大公因数及最小公倍数的概念可以推广到多于两个数的情形。

2.1.2 多项式恒等定理

关于 x 的多项式，一般可表示成：

$$a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n$$

的形式，其中 a_0x^n、a_1x^{n-1}、a_2x^{n-2}、…、a_n，叫做多项式的项；字母 x 的指数 n、$n-1$、$n-2$、…，叫做这一项的次数，而常数项 a_n ($a_n\neq0$) 规定次数为零；a_0、a_1、a_2、…、a_n，叫做各项的系数。若 $a_0\neq0$，那么这个多项式的次数是 n，这个多项式就叫做 n 次多项式。a_0 叫做首项系数。

一个不等于零的常数叫做零次多项式，例如，-3，$\frac{1}{2}$，4，a ($a\neq0$) 等都是 x 的零次多项式。

各项系数都是零的多项式，即 $0x^n+0x^{n-1}+0x^{n-2}+\cdots+0$

叫做零多项式。零多项式是没有次数的。零多项式恒等于零，通常用数“0”来表示。

多项式的恒等定理 由零多项式的定义知道，零多项式是恒等于零的；反过来，

如果一个多项式恒等于零，那么，这个多项式的各项系数必全等于零，这也就是说，它是一个零多项式。

定理1 如果$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$是一个恒等式，那么$a_0=0$，$a_1=0$，…，$a_{n-1}=0$，$a_n=0$

现在用数学归纳法对这个定理加以证明。

当$n=1$时，有恒等式$f(x)=a_0x+a_1=0$

任取$x=q$、m（$q\neq m$）分别得

$$qa_0+a_1=0$$

$$ma_0+a_1=0$$

由上两式解得$a_1=0$，$a_0=0$，所以当$n=1$时，论断是正确的。

假设$n=k-1$时，有恒等式$a_0x^{k-1}+a_1x^{k-2}+\cdots+a_{k-2}x+a_{k-1}=0$。那么就有$a_0=0$，$a_1=0$，…，$a_{k-2}=0$，$a_{k-1}=0$。

令$n=k$，就有恒等式$f(x)=a_0x^k+a_1x^{k-1}+\cdots+a_{k-1}x+a_k=0$。 (1)

以$2x$代替(1)中的x，得

$$f(2x)=2^ka_0x^k+2^{k-1}a_1x^{k-1}+\cdots+2a_{k-1}x+a_k=0. \quad (2)$$

再以$2^k\times(1)$得

$$2^kf(x)=2^ka_0x^k+2^ka_1x^{k-1}+\cdots+2^ka_{k-1}x+2^ka_k=0. \quad (3)$$

(3)−(2)得

$$2^{k-1}(2-1)a_1x^{k-1}+2^{k-2}(2^2-1)a_2x^{k-2}+\cdots+2^{k-p}(2^p-1)a_px^{k-p}+\cdots+2(2^{k-1}-1)a_{k-1}x+(2^k-1)a_k=0. \quad (4)$$

(4)是一个$k-1$次多项式，根据假设可知

$$2^{k-1}(2-1)a_1=0;$$

$$2^{k-2}(2^2-1)a_2=0;$$

……

$$2^{k-p}(2^p-1)a_p=0;$$

……

$$2(2^{k-1}-1)a_{k-1}=0;$$

$$(2^k-1)a_k=0,$$

又因$2^{k-p}\neq0$，$2^p-1\neq0$，所以$a_p=0$，即$a_1=a_2=\cdots=a_{k-1}=a_k=0$。

那么恒等式(1)就变成$a_0x^k=0$。

令$x=1$得$a_0=0$。