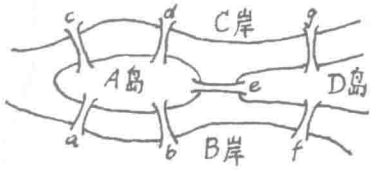
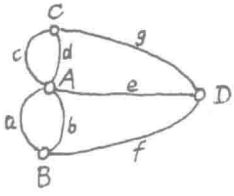
哥德巴赫猜想证明之拓展研究

1 哥德巴赫猜想

1.1 哥德巴赫其人

克里斯蒂安·哥德巴赫(Christian·Goldbach 1690—1764)德国数学家。出生于德国普鲁士王国东普鲁士省的首府哥尼斯堡(Koenigsberg)。此地在1945年德国第二次世界大战战败后，划归苏联的俄罗斯；1946年更名为加里宁格勒(Калининград)，1990年苏联解体，现属俄罗斯的加里宁格勒州。此地历史文化底蕴深厚，名人辈出，是大哲学家康德(Immanuel Kant 1724—1804)、大数学家希尔伯特(David Hilbert 1862—1943)的故乡。此地又是著名的七桥问题所在地，哥尼斯堡有七座桥，连接帕瑞格尔河的两岸和两个岛(如图)。问：一位散步者能否一次走遍这七座桥，且每座桥只经过一次，最后回到出发点？欧拉(Leonhard Euler 1707—1783)在1736年证明了要无重复地一次走遍这七座桥是不可能的。欧拉把四片陆地抽象成四个点，七座桥抽象成连结这四个点的七条线，从而把七桥问题归结为这样的七条线的图形能否一笔画成(如图)。假设图上的一些线相交于若干个点，除了起始点和终点，对于其余点来说，如有从某一点连到该点的一条线，必有该点通向另一点的又一条线，因此汇集在这些点上的线都应有偶数条，此类点叫偶点，奇数条线汇集的点叫奇点。欧拉指出：一个图能一笔画成并且返回起始点的充分且必要条件是这图上的点全是偶点，而奇点个数为0，七桥问题中抽象出来的图，由于四个点都是奇点，所以该图不能一笔画成，也即不能无重复地一次走遍这七座桥。





哥德巴赫曾在英国牛津大学学习，原学法学。曾担任中学教师。又曾是普鲁士派往俄国的公使。1725年，被选为彼得堡科学院院士，1725—1742年兼任科学院会议秘书。1742年移居莫斯科，并在俄国外交部任职。他和数学家欧拉、贝努利(Johann Beernoulli 1667—1748)有密切交往。

1.2 哥德巴赫猜想

1742年6月7日，哥德巴赫写信给大数学家欧拉，提出猜想：是否任何不比6小的偶数均可表示为两个奇素数之和？是否任何不比9小的奇数均可表示成三个奇素数之和？同年6月30日，欧拉回信说：任何大于6的偶数都是两个奇素数之和，虽然我还不能证明它，但我确信无疑地认为这是完全正确的定理。但上述信件直到1843年

才公开出版。哥德巴赫猜想的广泛传播，得益于英国数学家华林（E.Waring 1734－1798）在1770年的著述中对猜想的重新表述。现在，哥德巴赫猜想一般表述为：

(1) 偶数猜想：任何一个不小于6的偶数都可以表示为两个奇素数之和。

(2) 奇数猜想：任何一个不小于9的奇数都可以表示为3个奇素数之和。

用数学语言表示，即为：

(1) $x=p'+p''$，式中 $x\geq 6$，$2|x$，p'，p'' 为奇素数。

(2) $x=p_1+p_2+p_3$，式中 $x\geq 9$，$2\nmid x$，p_1，p_2，p_3 为奇素数。

容易证明，(2)奇数猜想是(1)偶数猜想的推论。因为(1)成立，(2)便随之成立。由 $x_{奇}=(x_{奇}-3)+3$，其中 $x_{奇}\geq 9$，$(x_{奇}-3)$ 是偶数（≥ 6），若(1)成立，就有 $(x_{奇}-3)=p_1+p_2$，把3称为 p_3，即有 $x_{奇}=p_1+p_2+p_3$，但是(2)成立，却反推不出(1)成立。所以最重要的是(1)，这是两个素数，故称之为1+1。

这就是哥德巴赫猜想。

1900年，在法国巴黎召开的第2届国际数学大会上，德国数学家希尔伯特在他著名的演说中，为20世纪数学家指出尚待解决的23个难题，哥德巴赫猜想、黎曼猜想、孪生素数猜想都是第8个难题素数分布问题的组成部分。

1912年，在英国剑桥召开的第5届国际数学大会上，德国数学家朗道（Edmunel Landau 1877－1938）将哥德巴赫猜想列为数论中按当时数学水平不能解决的4个问题之一。

1921年，在德国哥德哈根数学会上，数论泰斗、英国数学家哈代（Godfrey Harod Hardy 1877－1947）演讲宣称，哥德巴赫偶数猜想的困难程度“是可以与数学中任何未解决的问题相比拟的。

1742年起，许多人做了具体的验证，有限个数是可以验证的。到20世纪60年代，有人验证了大于4而不超过330,000,000的偶数，都符合猜想。但验证不是证明。数学要求一般性证明。

希尔伯特说：“数学需要问题，问题的解决锻炼研究者的力量，通过解决问题，他发现新方法及新观点，并扩大他的眼界。”他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的而使我们白费气力。

哥德巴赫猜想与费马大定理相仿，就是这样的好的数学问题，它形式简单，内容易懂，连中学生都可以理解，而实践又证明它是十分困难的问题。

从1742年哥德巴赫猜想提出，已经过了二百多年，许多杰出的数学家为破解猜想

作出巨大的努力，艰难的攀登。我国数学家陈景润在1966－1973年证得(1+2)，被国际数学界称之为"陈氏定理"。至今还是在哥德巴赫猜想证明上的最好成绩，没有人超过他。

破解哥德巴赫猜想这个世界难题，将会给数论乃至数学带来新的变化，将会给人类思维智慧带来新的成果，将会给人类文化发展带来新的推动，将会给人类社会带来无可估量的新的价值。

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, …, n, …, 叫做正整数, 又叫自然数。其中1, 3, 5, 7, 9, …, 叫做奇数。2, 4, 6, 8, 10, …, 叫做偶数。-1, -2, -3, …, -n, …, 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: $[\alpha]\leq\alpha<[\alpha]+1$. (1)

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

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

$$a=qb+r,\ 0\leq r<b,\text{并且}q\text{及}r\text{是唯一的。} \tag{3}$$

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

$$a=q_1b+r_1,\ 0\leq r<b. \tag{4}$$

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$|r-r_1|\geq b$, 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$b\pm c=(q_1\pm q_2)a$. 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是两个整数，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 约公元前330—前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$bs+a_1a_2\cdots a_n\top=1$.

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 最大整数和零头

记号$[y]$表示取不超过y的最大整数；$\{y\}$表示取y的零头部分；$\{y\}=y-[y]$，则有：

(1) $y=[y]+\{y\}$.

(2) $[y]\leqslant y<[y]+1$，$y-1<[y]\leqslant y$，$0\leqslant\{y\}<1$.

(3) $[n+y]=n+[y]$，其中n为整数。

(4) $[x]+[y]\leqslant[x+y]$，$\{x\}+\{y\}\geqslant\{x+y\}$.

(5) $[-y]=\begin{cases}-[y]-1, & \text{其中 } y \text{ 不是整数;}\\ -[y], & \text{其中 } y \text{ 是整数。}\end{cases}$

(6) 若a,b是两个整数，$b>0$，则$a=b\left[\frac{a}{b}\right]+b\left\{\frac{a}{b}\right\}$，$0\leqslant b\left\{\frac{a}{b}\right\}\leqslant b-1$.

(7) 若a,b是任意两个正整数，则不大于a而为b的倍数的正整数的个数是$\left[\frac{a}{b}\right]$.

2.1.3 排列 组合 二项式定理

1)加法原理：做一件事，完成它可以有n类方法，在第一类办法中有m_1种不同的方法，在第二类办法中有m_2种不同的方法，……，在第n类办法中有m_n种不同的方法，那么完成这件事共有$N=m_1+m_2+\cdots+m_n$种不同的方法。

2)乘法原理：做一件事，完成它需要分成n个步骤，做第一步有m_1种不同的方法，

做第二步有m_2种不同的方法，……，做第n步有m_n种不同的方法，那么完成这件事共有$N=m_1\times m_2\times\cdots\times m_n$种不同的方法。

3）排列：从n个不同元素中，任取$m(m\leqslant n)$个不同的元素，按照一定的顺序排成一列，叫做从n个不同的元素中取出m个元素的一个排列。

4）n的阶乘：自然数从1到n的连乘积，叫做n的阶乘，用$n!$表示，即$n!=1\times2\times3\times\cdots\times n$，规定$0!=1$.

5）排列数：从n个不同的元素中取出$m(m\leqslant n)$个元素的所有排列的个数，叫做从n个不同元素中取出m个元素的排列数，用符号P_n^m表示.

6）排列数公式：$P_n^m=n(n-1)(n-2)\cdots(n-m+1)$或$P_n^m=\frac{n!}{(n-m)!}$.

7）全排列：n个不同元素全部取出的一个排列，叫做n个不同元素的一个全排列。

8）全排列数公式：$P_n^m=n!$.

9）组合：从n个不同元素中，任取$m(m\leqslant n)$个元素并成一组，叫做从n个不同元素中取出m个元素的一个组合。

10）组合数：从n个不同元素中取出$m(m\leqslant n)$个元素的所有组合的个数，叫做从n个不同元素中取出m个元素的组合数，用符号C_n^m表示。

11）组合数公式：$C_n^m=\frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}$或$C_n^m=\frac{n!}{m!(n-m)!}$.

12）组合数的性质：

(1) $C_n^m=C_n^{n-m}$；

(2) $C_{n+1}^m=C_n^m+C_n^{m-1}$；

(3) $kC_n^k=nC_{n-1}^{k-1}$.

13）二项展开式：$(a+b)^n=a^n+C_n^1a^{n-1}b+C_n^2a^{n-2}b^2+\cdots+C_n^{n-1}ab^{n-1}+C_n^nb^n$.

14）二项式系数：二项展开式中的系数$C_n^r(r=0,1,2,\cdots,n)$.

15）杨辉三角：$(a+b)^n$，当$n=0,1,2,3,\cdots,n$时，其系数构成一个三角形

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

……

1 C_n^1 C_n^2 …… C_n^{n-2} C_n^{n-1} 1

这个三角形在我国宋朝数学家杨辉1261年所著的《详解九章算法》一书中就已出现，我们称它为杨辉三角，在国外也叫帕斯卡三角（Blaise Pascal 1623—1662 法国数学家）。

16)二项展开式的通项公式：展开式的第r+1项为$T_{r+1}=C_n^r a^{n-r}b^r$.

17)二项展开式的中间项：n为奇数时，中间项为$T_{\frac{n+1}{2}}$和$T_{\frac{n+1}{2}+1}$，n为偶数时，中间项为$T_{\frac{n}{2}+1}$.

18)二项式系数和：

$C_n^0+C_n^1+C_n^2+\cdots+C_n^n=2^n$，

$C_n^0+C_n^2+C_n^4+\cdots=2^{n-1}$，

$C_n^1+C_n^3+C_n^5+\cdots=2^{n-1}$.

19)二项式系数的主要性质：

(1)在二项展开式中，与首末两端"等距离"的两项的二项式系数相等。

(2)如果二项式的幂指数是偶数，中间一项的二项式系数最大；如果二项式的幂指数是奇数，中间两项的二项式系数相等并且最大。

2.1.4 皮亚诺算术公理

1889年，皮亚诺(G. Peano 1858—1932)对算术作了公理化处理，把算术建立在五条算术公理的基础上。

(1) 0是一个自然数，是自然数的一个空集合。

(2) 每个自然数n，都有不同于n的后继n'(n'表示n的后继运算，n'=n+1)。

(3) 不存在自然数n的后继n'为0.

(4) 对于任意自然数m和n，如果m'=n'，那么，m=n.

(5) 对于任何含有0的自然数集A，如果对任意的$n\in A$，都有$n'\in A$，那么，A含有所有自然数($n\in A$表示n属于A)。

2.1.5 集合

2.1.5.1 集合

集合是把那些确定的能够区分的对象汇集一起的一个整体，简称集。

组成一个集合的各个对象，叫做这一集合的元素。

如果a是集合A的元素，则称a属于集合A，记成$a\in A$；如果a不是集合A的元素，则称a不属于集合A，记成$a\notin A$(或$a\overline{\in}A$)。

如果两个集合有相同元素，即，对于任一元素x，若$x\in S_1$，则有$x\in S_2$；反之若$x\in S_2$，则有$x\in S_1$，此时就说这两个集合相等，记成$S_1=S_2$.

表示一个集合的常用方法有：

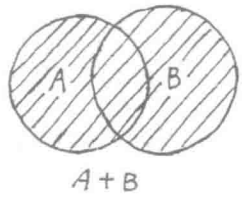
(1)外延法：适用于有限集，尤其是元素较少的有限集，即是把所有元素写在花

括号里，例如，$A=\{a_1,a_2,\cdots,a_n\}$.

(2) 概括法：适用于元素很多甚至无穷多的集合，即是把满足条件 $P(x)$ 的一切元素写在花括号里，例如，$A=\{x|P(x)\}$ 或 $A=\{x:P(x)\}$.

2.1.5.2 运算

(1) 并运算：由或属于 A 或属于 B 的所有元素所组成的集合，叫做 A 和 B 的并集合，简称 A 和 B 的并(或并集)，记成 $A\cup B$ 或 $A\vee B$ 或 $A+B$. $\cup$、$\vee$、$+$ 是集合的运算符号，相当于算术的加法，其运算称并运算，两个集合的并也叫两个集合的和(如图)。



$A+B$

如果 Φ 是空集合，A，B，C 是任意集合，则有：

$A\vee\Phi=A$

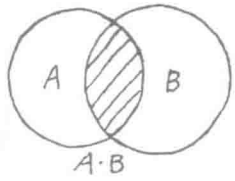
$A\vee A=A$ (幂等律)

$A\vee B=B\vee A$ (交换律)

$A\vee(B\vee C)=(A\vee B)\vee C$ (结合律)

如果 $B\subseteq A$，则 $A\vee B=A$

(2) 交运算：由既属于 A 又属于 B 的所有元素所组成的集合，叫做 A 和 B 的交集合，简称 A 和 B 的交(或交集)，记成 $A\cap B$ 或 $A\wedge B$，或 $A\cdot B$，$\cap$，$\wedge$、$\cdot$ 是集合的运算符号，相当于算术的乘法，其运算称交运算，两个集合的交也叫两个集合的积(如图)。



$A\cdot B$

如果 Φ 是空集合，A，B，C 是任意集合，则有：

$A\wedge\Phi=\Phi$

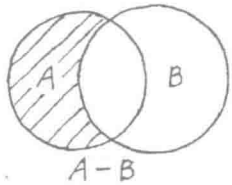
$A\wedge A=A$ (合等律)

$A\wedge B=B\wedge A$ (交换律)

$A\wedge(B\wedge C)=(A\wedge B)\wedge C$ (结合律)

如果 $B\subseteq A$，则 $A\wedge B=B$

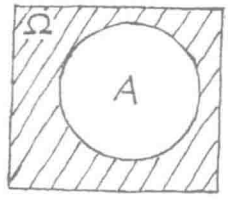
(3) 补运算：由属于 A 但不属于 B 的所有元素所组成的集合，叫做 B 相对于 A 的补集合，记作 $A\setminus B$ 或 $A-B$，$\setminus$、$-$ 是集合的运算符号，其运算称相对补运算，也叫差运算。特别地，当 $B\subseteq A$ 时，$A\setminus B$ 还叫做 B 相对于 A 的余集合(如图)。



$A-B$

2.1.5.3 全集和子集

相对于集合 A，在全集 Ω 中所有不属于 A 的元素所组成的集合，叫做 A 的补集合，记作 $\overline{A}$ 或 $-A$ (如图)。



$\overline{A}$

如果集合 A 的每一个元素也都是集合 B 的一个元素，则 A 是 B 的一个子集合，简称 B 的子集，记作 $A\subseteq B$ 或 $B\supseteq A$，叫做 A 包含在 B 中，或 B 包含 A (如图)。

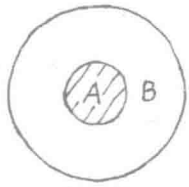
对任意集合A,B,C,有性质:

(1) $A\subseteq A$ (自反性)

(2) 若 $A\subseteq B$ 且 $B\subseteq A$,则 $A=B$ (反对称性)

(3) 若 $A\subseteq B$ 且 $B\subseteq C$,则 $A\subseteq C$ (传递性)

整数集记作Z,有理数集记作Q,实数集记作R,复数集记作C.



$A\subseteq B$

2.1.6 素数和算术基本定理

定义:一个大于1的整数,如果它的正因数只有1及它本身,就叫做素数(或质数);否则叫做合数。

以后用 p,或 $p_1,p_2,\cdots$,表示素数。

由定义,可以把自然数分为三类:1、素数、合数。

定理1 设 p 为素数,a 是任一整数,则或 $(p,a)=1$,或 $p\mid a$.

证明 因为 $(p,a)\mid p$,由素数定义,或 $(p,a)=1$,或 $(p,a)=p$,即 $p\mid a$. □

定理2 设 $a_1,a_2,\cdots,a_n$ 是 n 个整数,p 是素数。若 $p\mid a_1a_2\cdots a_n$,则 p 至少整除 $a_1,a_2,\cdots,a_n$ 中的一个。

证明 若 $p\nmid a_i$, $i=1,2,\cdots,n$. 由定理1知 $(p,a_i)=1$,再由互素性质2)得 $(p,a_1a_2\cdots a_n)=1$,与题设矛盾。□

定理3(算术基本定理) 任一大于1的整数 n,只有一种方法分解成素因数的乘积。

证明 要证 $n>1$ 必能分解成下面的形式

$$n=p_1p_2\cdots p_s\ ,\ p_1\le p_2\le\cdots\le p_s \tag{1}$$

其中 $p_1,p_2,\cdots,p_s$ 为素数,称为素因数,并且这种表示式是唯一的。

首先证明 n 一定能分解成(1)的形式。若 n 为素数,则(1)式显然成立;若 n 为非素数,则必有

$$n=p_1n_1\ ,\ 1<p_1<n_1$$

这里素数 p_1 为 n 的最小正因数。若 n_1 为素数,则(1)已证;若 n_1 为非素数,则有

$$n=p_1p_2n_2\ ,\ 1<n_2<n_1<n$$

这里素数 p_2 为 n_1 的最小正因数。继续下去,可以得到 $n>n_1>n_2>\cdots>1$. 这种过程最多不能超过 $\frac{n}{2}$ 次,实际不超过 $\log_p n$ 次,p 为最小正因数,故最后得

$$n=p_1p_2\cdots p_s\ ,\ p_1<p_2<\cdots<p_s\ ,\text{其中 } p_1,p_2,\cdots,p_s \text{为素数。}$$

其次证明(1)的表示法是唯一的。若 n 还可以分解成

$$n=q_1q_2\cdots q_t\ ,\ q_1<q_2<\cdots<q_t \tag{2}$$

其中 $q_1,q_2,\cdots,q_t$ 为素数,由(1)和(2)得到

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t \tag{3}$$

由定理2，存在 p_k（$1 \leq k \leq s$）及 q_l（$1 \leq l \leq t$）使

$$q_1 | p_k \ , \quad p_1 | q_l$$

但 p_k，q_l 为素数，所以 $p_k = q_l$，$q_l = p_1$．又 $p_1 \leq p_k$，$q_1 \leq q_l$，故 $q_l = p_1 \leq p_k = q_1$，即 $p_1 = q_1$．因此，从(3)得 $p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t$

同样可得 $p_2 = q_2$．依此类推，最后得到 $s = t$，且 $p_i = q_i$（$1 \leq i \leq s$）．唯一性得证。 □

推论 任一整数 n（$n > 1$）能够唯一地分解成

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \tag{4}$$

其中 $p_1, p_2, \cdots, p_s$ 是素数，$r_1, r_2, \cdots, r_s$ 是正整数。(4)叫做 n 的标准分解式。

定理（欧几里得） 素数无穷多。

证明 用反证法。若素数只有有限个，设为 $p_1, p_2, \cdots, p_n$，令

$$N = p_1 p_2 \cdots p_n + 1$$

则 $N > 1$，并且 $p_1, p_2, \cdots, p_n$ 都不能整除 N，故 N 再无其它新素因数是不可能的。 □

2.1.7 指数和对数

2.1.7.1 指数

n 个相同因子的乘积，叫做 n 次幂，例如

$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{个}}$ ．其中，a 为非零实数，叫做幂的底数，n 叫做幂的指数，a^n 叫做 a 的 n 次幂，也叫 a 的 n 次乘方。由于 n 是整数，所以叫正整数指数幂。

$$a^{-n} = \frac{1}{a^n} \quad (a \neq 0)$$

$$a^0 = 1$$

$$a^{\frac{m}{n}} = \sqrt[n]{a^m} \quad (a \geq 0) \quad \text{式中，} m, n \text{均为正整数。}$$

$$a^{-\frac{m}{n}} = \frac{1}{\sqrt[n]{a^m}} \quad (a > 0)$$

指数律：

(1) $a^{x_1} \cdot a^{x_2} = a^{x_1 + x_2}$

(2) $\frac{a^{x_1}}{a^{x_2}} = a^{x_1 - x_2}$

(3) $(a^{x_1})^{x_2} = a^{x_1 x_2}$

(4) $(ab)^x = a^x \cdot b^x$

(5) $\left(\frac{a}{b}\right)^x = \frac{a^x}{b^x}$ 式中，$a > 0$，$b > 0$，x_1, x_2, x 为任意实数。

2.1.7.2 对数

若 $a^x=b$ （$a>0$，$a\neq 1$），则 x 叫做 b 的以 a 为底的对数，记作 $x=\log_a b$，a 叫做对数的底数，b 叫做对数的真数。

当 $a=10$ 时，$\log_{10} b$ 记作 $\lg b$，叫常用对数，用来简化数值计算。

当 $a=e$ 时，$\log_e b$ 记作 $\ln b$（数论中常记作 $\log b$），叫自然对数，用来刻划变化规律。$e=\lim\limits_{n\to\infty}(1+\frac{1}{n})^n\approx 2.71828\cdots$，$e$ 是数列 $\{(1+\frac{1}{n})^n\}$ 当 n 趋于无穷大即 $n\to\infty$ 时的最终有限极限值。$\lim\limits_{n\to\infty}$ 或 $\lim\limits_{x\to 0}$ 表示极限。

性质有：

(1) $a^{\log_a b}=b$

(2) $\log_a a^x=x$

(3) $\log_a 1=0$

(4) $\log_a a=1$

运算法则有：

(1) $\log_a(b_1b_2\cdots b_n)=\log_a b_1+\log_a b_2+\cdots+\log_a b_n$

(2) $\log_a(\frac{b_1}{b_2})=\log_a b_1-\log_a b_2$

(3) $\log_a b^x=x\log_a b$ （x 为任意实数）

换底公式：$\log_a b=\frac{\log_c b}{\log_c a}$；$\ln b=\frac{\lg b}{\lg e}$。

常用对数求法：

设正数 $b=10^n\cdot N$（n 为整数，$1\leq N<10$），则

$\log b=n+\lg N$ 式中 n 叫做首数，$\lg N$ 叫做尾数，可通过查常用对数表求得。

2.1.8 素数的最大方次数

设 h 为 $n!$ 中含指定素数 p 的最大方次数，有

$$h=[\frac{n}{p}]+[\frac{n}{p^2}]+[\frac{n}{p^3}]+\cdots=\sum_{r=1}^{\infty}[\frac{n}{p^r}]$$

记号 Σ 表示连加，例如：$\sum\limits_{n=1}^{m}f(n)=f(1)+f(2)+\cdots+f(m)$。

若 $p^s>n$，则 $[\frac{n}{p^s}]=0$，故上式只有有限项不为零。

把 $2,\cdots,n$ 都分解成标准分解式，则由算术基本定理可知，h 就是这 $(n-1)$ 个分解式中 p 的指数之和。设其中 p 的指数是 r 的有 n_r 个（$1\leq r$），则

$$\begin{aligned}h&=n_1+2n_2+3n_3+\cdots\\&=n_1+n_2+n_3+\cdots\\&\quad+n_2+n_3+\cdots\\&\quad+n_3+\cdots\\&\quad+\cdots\end{aligned}$$

$$= N_1 + N_2 + N_3 + \cdots$$

其中 $N_r = n_r + n_{r+1} + \cdots$

恰好是 $2, \cdots, n$ 这 $(n-1)$ 个数中能被 p^r 除尽的个数 $N_r = \left[\frac{n}{p^r}\right]$，因此有写法：

$$n! = \prod_{p \le n} p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$$

式中 $\prod_{p \le n}$ 表示在不超过 n 的一切素数上的乘积式子。

记号 $\prod$ 表示连乘，例如，$\prod_{n=1}^{m} f(n) = f(1) \cdot f(2) \cdots f(m)$.

由 $n = (n-k) + k$，有 $\left[\frac{n}{p^r}\right] \ge \left[\frac{n-k}{p^r}\right] + \left[\frac{k}{p^r}\right]$

$$\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right] \ge \sum_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right] + \sum_{r=1}^{\infty}\left[\frac{k}{p^r}\right]$$

故 $\prod_{p \le n} p^{\sum_{r=1}^{\infty}\left[\frac{n-k}{p^r}\right] + \sum_{r=1}^{\infty}\left[\frac{k}{p^r}\right]} \Big| \prod_{p \le n} p^{\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$

也即有 $k!(n-k)! \mid n!$，整除性证得。

2.1.9 同余和同余式

2.1.9.1 同余和同余式

定义 给定一个正整数 m，把它叫做模。如果用 m 去除任意两个整数 a 与 b 所得的余数相同，则说 a, b 对模 m 的同余，记作 $a \equiv b \pmod m$. 否则，说 a, b 对 m 不同余，记作 $a \not\equiv b \pmod m$.

定理 整数 a, b 对模 m 同余的充分与必要条件是 $m \mid a-b$，即 $a = b + mt$，t 是整数。

证明 设 $a = mq_1 + r_1$，$b = mq_2 + r_2$，$0 \le r_1 < m$，$0 \le r_2 < m$. 若 $a \equiv b \pmod m$，则 $r_1 = r_2$，因此 $a - b = m(q_1 - q_2)$. 反之，若 $m \mid a-b$，则 $m \mid [m(q_1 - q_2) + (r_1 - r_2)]$，因此 $m \mid r_1 - r_2$，但 $|r_1 - r_2| < m$，故 $r_1 = r_2$. □

有了同余的概念，就可把余数相同的数放在一起，从而产生了所谓剩余类概念。对模 m，用它去除任何整数所得余数 r，总满足 $0 \le r \le m-1$. 若把余数为 r 的数放在一起、记作 k_r，则可以把全体整数分为 m 个集合：$k_0, k_1, \cdots, k_{m-1}$，称它们为模 m 的剩余类。

剩余类具有下列性质：

1) 每一个整数必包含在而且仅在上述一个集合里。

2) 两个整数同在一个集合里的充分与必要条件是这两个整数对模 m 同余。

定义 若 $a_0, a_1, \cdots, a_{m-1}$ 是 m 个整数，并且其中任何两数都不在同一个剩余类里，则称 $a_0, a_1, \cdots, a_{m-1}$ 为模 m 的一个完全剩余系。

例如，$0, 1, 2, \cdots, m-1$ 便是模 m 的一个完全剩余系。

定义 把完全剩余系中与模m互素的整数全体叫做模m的一个简化剩余系。

例如，$m=10$时，1,3,7,9组成一个简化剩余系。

定义 欧拉(Euler)函数$\varphi(x)$是定义在正整数上的函数，它在正整数a上的值等于序列$0,1,2,\cdots,a-1$中与a互素的数的个数。

例如，$\varphi(10)=4$，$\varphi(5)=4$.

同余式：若$f(x)$表示多项式$a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0$，其中，$a_n$，$a_{n-1}$，$\cdots$，$a_0$是整数，$m$是一个正整数，则

$$f(x)\equiv 0 \pmod m \tag{1}$$

叫做模m的同余式。若$m\nmid a_n$，$f(x)\equiv 0 \pmod m$，则(1)叫做n次同余式。

若a是使$f(a)\equiv 0 \pmod m$成立的一个整数，则$x\equiv a \pmod m$叫做同余式(1)的一个解。

2.1.9.2 费马小定理

定理 对于整数a和素数p，$p\nmid a$，那么a^p-a可以被p整除，即$p\mid a^p-a$，有

$$a^p-a\equiv 0 \pmod p,\quad a^{p-1}-1\equiv 0 \pmod p,\quad a^p\equiv a \pmod p.$$

证明 因为$p\nmid a$，则$a,2a,\cdots,(p-1)a$分别按某个重排顺序模p同余于$1,2,\cdots,(p-1)$. 故有$(p-1)!\,a^{p-1}\equiv(p-1)! \pmod p$. 因为$p$是素数，所以$p\nmid(p-1)!$故得$a^{p-1}\equiv 1 \pmod p$，即得$a^p\equiv a \pmod p$，$a^p-a\equiv 0 \pmod p$，$a^{p-1}-1\equiv 0 \pmod p$. □

例如：$5^3-5\equiv 0 \pmod 3$，$5^{3-1}-1\equiv 0 \pmod 3$，$2^5\equiv 2 \pmod 5$.

2.1.9.3 二次剩余

同余式 $x^2\equiv n \pmod m$ 式中$(n,m)=1$，$n<m$.

如果同余式有解，n即为模m的二次剩余；

如果同余式无解，n即为模m的二次非剩余。

由此，可以将与m互素的且不超过m的正整数分成两类，例如，模7的二次剩余是1,2,4. 二次非剩余是3,5,6. 模13的二次剩余是1,3,4,9,10,12. 二次非剩余是2,5,6,7,8,11.

当$m=2$时，有$1^2\equiv 1 \pmod 2$，每一个奇数都是模2的二次剩余。

定理(拉格朗日 Lagrange) 同余方程$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0\equiv 0 \pmod p$ 式中p为素数，$1\leqslant x\leqslant p$，a_n，a_{n-1}，$\cdots$，a_1，a_0都是正整数且$p\nmid a_n$，方程的解数$\leqslant n$，重解也计算在内。

证明 如果方程无解，则定理已成立。

如果$x=a$是方程的一个解，有 $f(x)=(x-a)f_1(x)+r_1$

以$x=a$代入，得$p\mid r_1$，故 $f(x)\equiv(x-a)f_1(x) \pmod p$

如果 $x=a$ 又是 $f_1(x)\equiv 0 \pmod p$ 的解，此时 a 为 $f(x)\equiv 0 \pmod p$ 的重解，那么同样可得 $f_1(x)\equiv (x-a)f_2(x) \pmod p$

继续上述过程，如果 $f(x)\equiv (x-a)^h g_1(x) \pmod p$，式中 $g_1(a)\not\equiv 0 \pmod p$，则称 a 是 $f(x)\equiv 0 \pmod p$ 的 h 重解。

由上可知，$g_1(x)$ 的次数是 $(n-h)$.

设方程另有一解 $x=b$，那么，

$$0\equiv f(b)\equiv (b-a)^h g_1(b) \pmod p$$

因 $p\nmid (b-a)$，所以必定 $g_1(b)\equiv 0 \pmod p$

如果 $x=b$ 是 $g_1(x)\equiv 0 \pmod p$ 的 k 重解，那么，同样有

$$f(x)\equiv (x-a)^h (x-b)^k g_2(x) \pmod p$$

继续上述过程，可得

$$f(x)\equiv (x-a)^h (x-b)^k \cdots (x-c)^l g(x) \pmod p$$

可知 $g(x)$ 的次数是 $n-h-k-\cdots-l$，且 $g(x)\equiv 0 \pmod p$ 不再有解，所以 $f(x)\equiv 0 \pmod p$ 的解数是 $n-h-k-\cdots-l\leqslant n$. □

定理（威尔逊 Wilson） 如果 p 是素数，那么 $(p-1)!\equiv -1 \pmod p$.

证明 已知 $x^{p-1}-1\equiv 0 \pmod p$，$1\leqslant x\leqslant p$，有 $(p-1)$ 个解，所以

$$x^{p-1}-1\equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p$$

以 $x=0$ 代入，即得 $-1\equiv (-1)^{p-1}(p-1)! \pmod p$

当 $p=2$ 时，定理显然成立。当 $p>2$ 时，$2\mid (p-1)$，所以 $(-1)^{p-1}=1$，即得

$$(p-1)!\equiv -1 \pmod p.$$ □

定理 在 $\leqslant (p-1)$ 的正整数中，共有 $\frac{1}{2}(p-1)$ 个模 p 的二次剩余，$\frac{1}{2}(p-1)$ 个模 p 的二次非剩余，且 $1^2, 2^2, \cdots, (\frac{1}{2}(p-1))^2$ 用 p 除所得的余数，就是模 p 的全体二次剩余。其中 $p>2$，为奇素数。

证明 显然由 $x^2\equiv n \pmod p$，式中 $x=1,2,\cdots,(p-1)$；可知用 p 除各数所得的余数都是模 p 的二次剩余，而且仅是这些。

假定 $1\leqslant n<p$，如果同余式 $x^2\equiv n \pmod p$，$1\leqslant x\leqslant p-1$，有解，那么至多有二个解，由 $(p-x)^2\equiv (-x)^2\equiv x^2\equiv n \pmod p$ 可知，还有一个解 $(p-x)$，如果 $\frac{1}{2}(p-1)<x\leqslant (p-1)$，那么 $1\leqslant p-x\leqslant \frac{1}{2}(p-1)$，因此总有一个解适合于 $1\leqslant x\leqslant \frac{1}{2}(p-1)$.

如果 n 是模 p 的二次剩余，那么 n 必定模 p 同余于 $1^2, 2^2, \cdots, (\frac{1}{2}(p-1))^2$ 中的一个数。而且 n 中是模 p 的二次剩余恰有 $\frac{1}{2}(p-1)$ 个，因为其中任何两个数模 p 都互不同余。用反证法，假定 $a>b$，且 $a^2\equiv b^2 \pmod p$，得 $p\mid (a+b)(a-b)$，有 $p\mid (a+b)$ 或 $p\mid (a-b)$，但 $1\leqslant a+b<p$，$1\leqslant a-b<p$，这是不可能的。因此 n 中任何两数都模 p 互不同余。□

定理(欧拉) 有关系式

$$n^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod p, \text{当 } n \text{ 是模 } p \text{ 的二次剩余。} \\ -1 \pmod p, \text{当 } n \text{ 是模 } p \text{ 的二次非剩余。} \end{cases}$$

证明 假定 n 是模 p 的二次剩余,那么同余式 $x^2 \equiv a \pmod p$ 有解 x,即 $p|(x^2-n)$,由 $x^{p-1}-n^{\frac{p-1}{2}}=\left((x^2)^{\frac{p-1}{2}}-n^{\frac{p-1}{2}}\right)=(x^2-n)\left((x^2)^{\frac{p-1}{2}-1}+(x^2)^{\frac{p-1}{2}-2}n+\cdots+x^2n^{\frac{p-1}{2}-2}+n^{\frac{p-1}{2}-1}\right)$,可知 $p|(x^{p-1}-n^{\frac{p-1}{2}})$,又知 $p|(x^{p-1}-1)$,则有 $p|(x^{p-1}-1-x^{p-1}+n^{\frac{p-1}{2}})$,即 $n^{\frac{p-1}{2}} \equiv 1 \pmod p$.

而上式的解数不超过 $\frac{p-1}{2}$ 个,正好有 $\frac{p-1}{2}$ 个解,即模 p 的 $\frac{p-1}{2}$ 个二次剩余,所以若 n 是模 p 的二次非剩余,必然 $p\nmid(n^{\frac{p-1}{2}}-1)$,但已知 $p|(n^{p-1}-1)=(n^{\frac{p-1}{2}}-1)(n^{\frac{p-1}{2}}+1)$,又已知 $p|(n^{\frac{p-1}{2}}+1)$,即 $n^{\frac{p-1}{2}} \equiv -1 \pmod p$. □

勒让德(A.M.Legendre)符号 $\left(\frac{a}{p}\right)$:假定 p 是奇素数,a 是正整数,$(a,p)=1$,规定:$\left(\frac{a}{p}\right)=\begin{cases} +1, \text{当 } a \text{ 是 } p \text{ 的二次剩余(平方剩余)。} \\ -1, \text{当 } a \text{ 是 } p \text{ 的二次非剩余(平方非剩余)。} \end{cases}$ 有 $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

雅可比符号 $\left(\frac{a}{m}\right)$:由于运用勒让德符号计算时,要将 a 分解成标准分解形式,十分麻烦,因此产生雅可比符号,它是勒让德符号的一种推广,首先由普鲁士数学家雅可比(Carl Gustav Jacobi 1804—1851)在1837年引进。设 m 是一个正奇数,其素因数分解式为 $m=\prod_{i=1}^{s} p_i$,并且正整数 a 满足 $(a,m)=1$,那么 $\left(\frac{a}{m}\right)=\prod_{i=1}^{s}\left(\frac{a}{p_i}\right)$.

k 次剩余:假定 $k>2$,$(n,m)=1$,且同余式 $x^k \equiv n \pmod m$ 有解,就叫 n 为模 m 的 k 次剩余;无解,n 就叫模 m 的 k 次非剩余。

用 $n_k(p)$ 表示模 p 的最小正 k 次非剩余,例如 $n_2(7)=3$,$n_2(11)=2$,等等。最有名的问题是估计 $n_2(p)$ 的上界。1957年,布尔吉斯(D.A.Burgess)证明:

定理(布尔吉斯) $n_2(p)=O(p^{\frac{1}{4\sqrt{e}}+\varepsilon})$,其中 ε 是任意给定的正数,而与 O 有关的常数仅依赖于 ε.

类似的还有:

定理 假定 ε 为任意正数,则当 p 充分大时有:

1) $n_k(p) \leqslant p^{\frac{1}{4e^{\frac{k-1}{2}}}+\varepsilon}$ $(k \geqslant 2)$

2) $n_k(p) \leqslant p^{\frac{1}{12}}$ $(n \geqslant 21)$

3) $n_k(p) \leqslant p^{\frac{\ln\ln k+3}{4\ln k}}$ $(k \geqslant e^{33})$

似乎应该还有:

1) $n_2(p)=O((\ln p)^2)$,在广义黎曼猜想真实的假定下,可给予证明。

2) $n_2(p)=O((\ln p)^{1+\varepsilon})$,此处与 O 有关的常数仅依赖于 ε.

3) $n_2(p)=\Omega(\ln p)$,可以证明。

关于 $n_k(p)$ $(k>2)$ 的猜测结果，也是与 $n_2(p)$ 完全一样。

另一个有名的问题是关于模 p 的最小原根。假定 g 是一个自然数，且 $p\nmid g$，那么 $g^{p-1}\equiv 1 \pmod p$。如果当 $1\leqslant l<p-1$ 时都有 $g^l\not\equiv 1 \pmod p$，就称 g 是模 p 的原根，可以证明模 p 的原根是存在的，用 $g(p)$ 表示模 p 的最小正原根，例如，$g(11)=2$，$g(41)=6$，$g(409)=21$，$g(467)=2$，等等。关于原根最著名的问题之一是估计 $g(p)$ 的上界。

定理　$g(p)=O(p^{\frac{1}{4}+\varepsilon})$，其中 ε 为任意正数，而与 O 有关的常数仅与 ε 有关。

但这与关于 $g(p)$ 的猜测结果 $g(p)=O((\ln p)^2)$ 或 $g(p)=O((\ln p)^{1+\varepsilon})$ 相差很远。在广义黎曼猜想真实的假定下，可以证明 $g(p)=O(m^6(\ln p)^2)$，此处 m 表示 $p-1$ 的互异的素因数个数。

关于原根的另一个重要问题是1927年阿丁（E. Artin）提出的猜测：对于任意不等于1，$p-1$ 及完全平方的正整数 a，必定存在无穷多个素数 p，以 a 为原根；特别是存在无穷多个素数 p，以2为原根。1967年霍勒（C. Hooley）在某种黎曼猜测成立的假定下，证明了阿丁猜测，并得到了以 a 为原根的适合于 $p\leqslant x$ 的素数个数的渐近表达式。

2.1.9.4 中国剩余定理（孙子定理）

中国古代名著《孙子算经》下卷有一道名题“物不知其数”：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰：二十三。”

用同余式表示，就是求 x，使

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 2 \pmod 7 \end{cases}$$

孙子解法为：“凡三三数之剩一，则置七十。”现剩二，就给出 $70\times 2=140$；“五五数之剩一，则置二十一。”现剩三，就给出 $21\times 3=63$；“七七数之剩一，则置十五。”现剩二，就给出 $15\times 2=30$；“并之，得二百三十三，一百六以上，以一百五减之，即得。”将这三个数相加，再减去若干个105，直到最小的正整数，即为所求的解，即

$$140+63+30-105-105=23$$

明朝数学家程大位在《算法统宗》（1592年）里把孙子解法编成歌诀：“孙子歌曰：三人同行七十稀，五树梅花廿一枝，七子团圆正半月，除百零五便得知。”

上述孙子算法，在国外称为“中国剩余定理”。其现代的一般表述形式为：

设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，$m=m_1m_2\cdots m_k$，$M_1=\frac{m}{m_1}$，$M_2=\frac{m}{m_2}$，$\cdots$，$M_k=\frac{m}{m_k}$，