第十届全国教育图书展优秀畅销图书
国家集训队教练执笔联合编写
在香港出版繁体字版和网络版
版版畅销，网络销量居榜首

畅销15年
超1200万册

总主编　单　墫　熊　斌

奥数教程
学习手册

·配《奥数教程》第六版·

教辅资料站

电子教辅　试卷练习
知识总结　备课资源

扫码关注获取更多学习资料

高三年级

余红兵　编著

华东师范大学出版社
全国百佳图书出版单位

总主编　单　墫　熊　斌

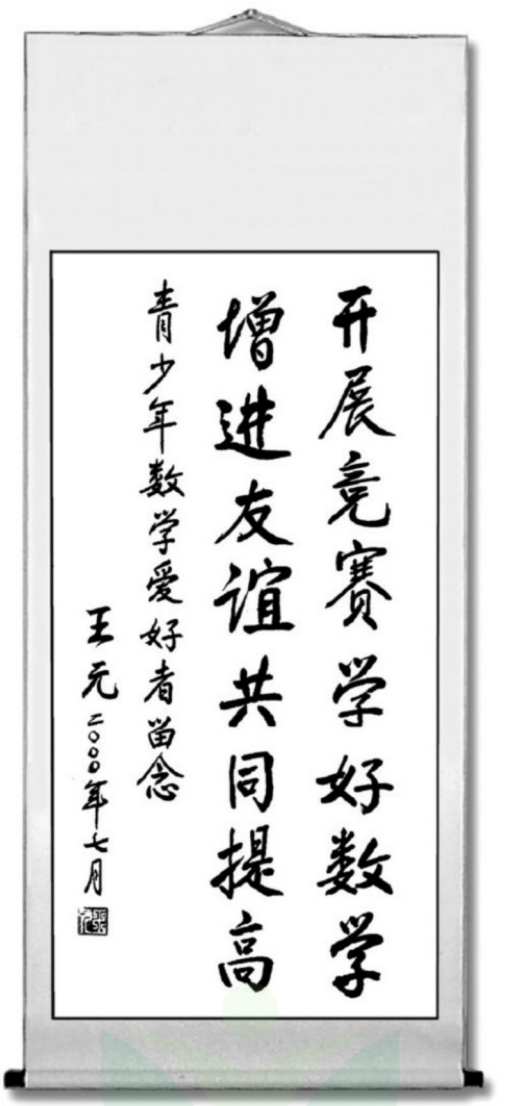
奥数教程
学习手册

·配《奥数教程》第六版·

华东师范大学出版社

高三年级

余红兵　编著



著名数学家、中国科学院院士、原中国数学奥林匹克委员会主席王元先生致青少年数学爱好者

前　言

据说在很多国家，特别是美国，孩子们害怕数学，把数学作为“不受欢迎的学科”. 但在中国，情况很不相同，很多少年儿童喜爱数学，数学成绩也都很好. 的确，数学是中国人擅长的学科，如果在美国的中小学，你见到几个中国学生，那么全班数学的前几名就非他们莫属.

在数(shǔ)数(shù)阶段，中国儿童就显出优势.

中国人能用一只手表示 1～10，而很多国家非用两只手不可.

中国人早就有位数的概念，而且采用最方便的十进制(不少国家至今还有 12 进制，60 进制的残余).

中国文字都是单音节，易于背诵，例如乘法表，学生很快就能掌握，再“傻”的人也都知道“不管三七二十一”. 但外国人，一学乘法，头就大了. 不信，请你用英语背一下乘法表，真是佶屈聱牙，难以成诵.

圆周率 $\pi=3.141\,59\cdots$. 背到小数后五位，中国人花一两分钟就够了. 可是俄国人为了背这几个数字，专门写了一首诗，第一句三个单词，第二句一个……要背 π 先背诗，这在我们看来简直是自找麻烦，可他们还作为记忆的妙法.

四则运算应用题及其算术解法，也是中国数学的一大特色. 从很古的时候开始，中国人就编了很多应用题，或联系实际，或饶有兴趣，解法简洁优雅，机敏而又多种多样，有助于提高学生的学习兴趣，启迪学生智慧. 例如：

“一百个和尚一百个馒头，大和尚一个人吃三个，小和尚三个人吃一个，问有几个大和尚，几个小和尚?”

外国人多半只会列方程解. 中国却有多种算术解法，如将每个大和尚“变”成 9 个小和尚，100 个馒头表明小和尚是 300 个，多出 200 个和尚，是由于每个大和尚变小和尚，多变出 8 个，从而 $200\div8=25$ 即是大和尚人数. 小和尚自然是 75 人，或将一个大和尚与 3 个小和尚编成一组，平均每人吃一个馒头. 恰好与总体的平均数相等. 所以大和尚与小和尚这样编组后不多不少，即大和尚是 $100\div(3+1)=25$ 人.

中国人善于计算，尤其善于心算. 古代还有人会用手指计算(所谓“掐指一算”). 同时，中国很早就有计算的器械，如算筹、算盘. 后者可以说是计算机的雏形.

在数学的入门阶段——算术的学习中，我国的优势显然，所以数学往往是我国聪明的孩子喜爱的学科.

几何推理，在我国古代并不发达(但关于几何图形的计算，我国有不少论著)，比希腊人稍逊一筹. 但是，中国人善于向别人学习. 目前我国中学生的几何水平，在世界上遥遥领先. 曾有一个外国教育代表团来到我国一个初中班，他们认为所教的几何内容太深，学生不可能接受，但听课之后，不得不承认这些内容中国的学生不但能够理解，而且掌握得很好.

我国数学教育成绩显著. 在国际数学竞赛中，我国选手获得众多奖牌，就是最有力的证明. 从1986年我国正式派队参加国际数学奥林匹克以来，中国队已经获得了14次团体冠军，可谓是成绩骄人. 当代著名数学家陈省身先生曾对此特别赞赏. 他说：“今年一件值得庆祝的事，是中国在国际数学竞赛中获得第一……去年也是第一名.”(陈省身1990年10月在台湾成功大学的讲演“怎样把中国建为数学大国”)

陈省身先生还预言：“中国将在21世纪成为数学大国.”

成为数学大国，当然不是一件容易的事，不可能一蹴而就，它需要坚持不懈的努力. 我们编写这套丛书，目的就是：(1)进一步普及数学知识，使数学为更多的青少年喜爱，帮助他们取得好的成绩；(2)使喜爱数学的同学得到更好的发展，通过这套丛书，学到更多的知识和方法.

“天下大事，必作于细.”我们希望，而且相信，这套丛书的出版，在使我国成为数学大国的努力中，能起到一点作用. 本丛书初版于2000年，现根据课程改革的要求对各册再作不同程度的修订.

著名数学家、中国科学院院士、原中国数学奥林匹克委员会主席王元先生担任本丛书顾问，并为青少年数学爱好者题词，我们表示衷心的感谢. 还要感谢华东师大出版社及倪明、孔令志先生，没有他们，这套丛书不会是现在这个样子.

单 墫 熊 斌

2014年5月

目　录

习题详细解答

第 1 讲　排列与组合 …… 1
第 2 讲　二项式系数 …… 4
第 3 讲　计数:对应与递推 …… 9
第 4 讲　计数:容斥原理 …… 14
第 5 讲　组合问题 …… 17
第 6 讲　数的整除 …… 21
第 7 讲　素数 …… 26
第 8 讲　同余(一) …… 30
第 9 讲　不定方程(一) …… 33
第 10 讲　数论问题 …… 37
第 11 讲　多项式的运算与整除 …… 40
第 12 讲　多项式的零点 …… 42
第 13 讲　整系数多项式 …… 45
第 14 讲　多项式的插值与差分 …… 47
第 15 讲　单位根及其应用 …… 49
第 16 讲　生成函数方法 …… 51
第 17 讲　集合与子集族 …… 53
第 18 讲　图论问题 …… 56
第 19 讲　同余(二) …… 59

第 20 讲　不定方程(二) …… 62

综合练习 …… 65

专题选讲

专题 1　组合问题 …… 81
专题 2　数论问题 …… 109

第 1 讲

排列与组合

1 (i) P_6^3; (ii) 6^3.

2 所求的数目等于 1, 2, …, 9 的 7-排列数减去 8, 9 相邻的排列数. 这是 $P_9^7 - 2! \times 6 \times P_7^5 = 151\,200$. (8, 9 相邻的 7- 排列数可这样确定:第一步,取 1,2, …, 7 的一个 5- 排列,有 P_7^5 种方法;第二步,将 8, 9 看作一个整体插在 5- 排列的首、尾或任两个数字之间,有 6 种方法;最后,将 8, 9 作全排列有 2!种方法,由乘法原理知这样的排列数是 $2! \times 6 \times P_7^5$.)

3 6 个歌唱节目有 6! 种排法,每一种排法产生 7 个"空档",将 4 个舞蹈节目插入这 7 个"空档",共有 P_7^4 种方法. 因此节目单有 6! P_7^4 种排法.

4 由有重复元素的全排列公式知,共有 $\frac{9!}{2!\ 3!\ 4!}$ 种方案.

5 易知,所说的"单词"可分为三类:2 个 a, 3 个 c; 2 个 a, 1 个 b, 2 个 c; 1 个 a, 1 个 b, 3 个 c. 于是由加法原理及有重复元素的全排列公式知,所求数目为 $\frac{5!}{2!0!3!} + \frac{5!}{2!1!2!} + \frac{5!}{1!1!3!} = 60$.

6 先让男生围成一圈,由圆周排列公式知共有 $(n-1)!$ 种方法. 每两个男生之间都有一个空位,共有 n 个. 现在让 n 个女生在这 n 个空位上排列,有 $n!$ 种方法. 所以共有 $(n-1)!n!$ 种排法. (应当注意,当男生排好之后,女生的排法便是(直线)排列,而不能再看作圆周排列.)

7 显然,有两个球放入一盒,而其余球各放入一盒. 第一

步，在 $n+1$ 个球中取两个，有 $\binom{n+1}{2}$ 种方法；第二步，将这两个球视为一体，与其余 $n-1$ 个球放入 n 个（不同的）盒子中，有 $n!$ 种方法. 故共有 $\binom{n+1}{2}n! = \frac{n}{2}(n+1)!$ 种放法.

8 掷出的结果是 1，2，…，6 的一个 k 可重组合. 故所求的数目等于 $\binom{k+6-1}{k} = \binom{k+5}{k}$.

9 将所说的整数被 3 除得的余数分为三类：$A = \{3, 6, \cdots, 300\}$，$B = \{2, 5, \cdots, 299\}$，$C = \{1, 4, \cdots, 298\}$. 所取的三个数之和被 3 整除有四种情况：三数同属 A、B、C 之一或三数分别取自 A、B、C. 由加法原理，取法共有 $3\binom{100}{3} + 100^3$ 种.

10 设五个点为 A_1、A_2、A_3、A_4、A_5. 两两连成的直线有 $\binom{5}{2} = 10$ 条. 每三点构成一个三角形，共有 $\binom{5}{3} = 10$ 个三角形. 由其中任四点可连 $\binom{4}{2} = 6$ 条直线，自另一点可作这 6 条直线的垂线，故总共可作 $5\times 6 = 30$ 条垂线. 这些垂线至多有 $\binom{30}{2} = 435$ 个交点. 但在上述 10 条连线的每一条上有三条垂线互相平行（没有交点），因而应减去 30 个交点；此外，10 个三角形中每三条高交于一点，因而又要减去 20 个交点；而每个点 A_i 都是 6 条垂线的交点，所以还要减去 $5\binom{6}{2} = 75$ 个交点. 最后得交点至多为 310 个.

11 设 $|A| = k$，则由条件(1)可知 $|B| = 12-k$. 由于 A、B 非空，故 $k \neq 0$，12. 由条件(3)可知 $k \in A$，$12-k \notin B$. 故由(1)可知 $k \in B$，$12-k \in A$.

显然 $k \neq 6$，否则 $6 \in B$，且 $6 = 12-6 \in A$，与条件(2)不符合.

对每个 k ($1\leqslant k\leqslant 11$, $k\neq 6$),已确定了 $12-k\in A$,及 $k\in B$,故 A 的其余 $k-1$ 个元素,在 $A\cup B$ 集合中除去 k 及 $12-k$ 剩下的 10 个元素中选取,共有 $\binom{10}{k-1}$ 种取法;再由条件(1)可唯一地确定了 B.

故 $N=\sum\limits_{k=1}^{11}\binom{10}{k-1}-\binom{10}{6-1}=2^{10}-\binom{10}{5}=772$. (其中等式 $\sum\limits_{k=1}^{11}\binom{10}{k-1}=\sum\limits_{k=0}^{10}\binom{10}{k}=2^{10}$,可以直接计算,也可参考第 2 讲中的(8).)

12 由于 A, B, $\overline{A\cup B}$ 两两的交集是空集,而它们的并集为集合 S(这里 $\overline{A\cup B}$ 为 $A\cup B$ 关于 S 的补集). 因此 S 的任何一个元素或在 A 中,或在 B 中,或在 $\overline{A\cup B}$ 中,共三种情形,则 S 中满足 $A\cap B=\varnothing$ 的有序子集对(A, B) 的个数为 3^{10}(参见本讲例 4).

上面求得的个数中包含了 A, B 为空集的情形,应当排除:若 $A=\varnothing$,则 S 的每个元素或在 B 中,或在 $\overline{B}$ 中,故此时集合 B 有 2^{10} 个. 同样,当 $B=\varnothing$ 时,集合 A 有 2^{10} 个. 又因为 A, B 均为空集的集合对只有一个. 因此 A, B 中至少有一个为空集的对数有 $2^{10}+2^{10}-1=2^{11}-1$ 个. 故满足 $A\cap B=\varnothing$ 的非空的有序子集对(A, B) 共有 $3^{10}-(2^{11}-1)$ 个,则无序的个数应该是 $\frac{1}{2}(3^{10}+1)-2^{10}=28\,501$ 个.

第2讲

二项式系数

1 对 k 进行归纳. 当 $k=1$ 时结论显然成立. 设当 $k-1$ 时等式成立($k\geqslant 2$),则由归纳假设及(5)可知

$$\begin{aligned}\sum_{i=0}^{k}(-1)^i\binom{n}{i}&=(-1)^{k-1}\binom{n-1}{k-1}+(-1)^k\binom{n}{k}\\&=(-1)^{k-1}\left(\binom{n-1}{k-1}-\binom{n}{k}\right)\\&=(-1)^{k-1}\left(-\binom{n-1}{k}\right)\\&=(-1)^k\binom{n-1}{k}.\end{aligned}$$

2 设 $a_n=\sum_{k=0}^{n}\binom{n+k}{k}\frac{1}{2^k}(n\geqslant 1)$,则 $a_1=2$,由(5)可得

$$\begin{aligned}a_{n+1}&=\sum_{k=0}^{n+1}\binom{n+1+k}{k}\frac{1}{2^k}=\sum_{k=0}^{n+1}\binom{n+k}{k}\frac{1}{2^k}+\sum_{k=0}^{n+1}\binom{n+k}{k-1}\frac{1}{2^k}\\&=a_n+\binom{2n+1}{n+1}\frac{1}{2^{n+1}}+\frac{1}{2}\sum_{k=1}^{n+2}\binom{n+1+k-1}{k-1}\frac{1}{2^{k-1}}-\binom{2n+2}{n+1}\frac{1}{2^{n+2}}\\&=a_n+\frac{1}{2}a_{n+1}.\end{aligned}$$

故 $a_{n+1}=2a_n$ 对所有 $n\geqslant 1$ 都成立,由此及 $a_1=2$ 可得 $a_n=2^n$.

3 记所说的和为 a_n,则 $a_0=a_1=1$. 对 $n\geqslant 2$,我们有(利用(5)式)

$$a_n=\sum_{k=0}^{\left[\frac{n}{2}\right]}\frac{(-1)^k}{4^k}\binom{n-k-1}{k}+\sum_{k=1}^{\left[\frac{n}{2}\right]}\frac{(-1)^k}{4^k}\binom{n-k-1}{k}.$$

在第一项中，如 n 是奇数，则 $\left[\frac{n}{2}\right]=\left[\frac{n-1}{2}\right]$；如 n 是偶数，则当 $k=\frac{n}{2}$ 时 $\binom{n-k-1}{k}=0$，而 $\left[\frac{n}{2}\right]-1=\left[\frac{n-1}{2}\right]$. 故上面第一项是 $\sum_{k=0}^{\left[\frac{n-1}{2}\right]}\frac{(-1)^k}{4^k}\binom{n-1-k}{k}=a_{n-1}$. 类似地，第二项是

$$\sum_{k=1}^{\left[\frac{n}{2}\right]}\frac{(-1)^k}{4^k}\binom{n-1-k}{k}=-\frac{1}{4}\sum_{k=0}^{\left[\frac{n-2}{2}\right]}\frac{(-1)^k}{4^k}\binom{n-2-k}{k}.$$

因此我们导出 $a_n=a_{n-1}-\frac{1}{4}a_{n-2}(n\geqslant 2)$. 此即

$$a_n-\frac{1}{2}a_{n-1}=\frac{1}{2}\left(a_{n-1}-\frac{1}{2}a_{n-2}\right).$$

易知 $a_n-\frac{1}{2}a_{n-1}=\frac{1}{2^n}$. 故对 $n\geqslant 1$ 有

$$a_n=\frac{1}{2^n}+\frac{1}{2}a_{n-1}=\frac{1}{2^n}+\frac{1}{2}\left(\frac{1}{2^{n-1}}+\frac{1}{2}a_{n-2}\right)$$

$$=\cdots=\frac{n}{2^n}+\frac{a_0}{2^n}=\frac{n+1}{2^n}.$$

4 利用 $\frac{1}{k+1}\binom{n}{k}=\frac{1}{n+1}\binom{n+1}{k+1}$ 及二项式定理易得结果. 参考例 1 中(i)的变形方法.

5 记所说的和为 a_n. 利用

$$\frac{1}{k}\binom{n}{k}=\frac{1}{k}\left(\binom{n-1}{k-1}+\binom{n-1}{k}\right)=\frac{1}{k}\binom{n-1}{k}+\frac{1}{n}\binom{n}{k}$$

及二项式定理，可得

$$a_n=\sum_{k=1}^{n-1}(-1)^{k+1}\frac{1}{k}\binom{n}{k}+(-1)^{n+1}\frac{1}{n}$$
$$=\sum_{k=1}^{n-1}(-1)^{k+1}\frac{1}{k}\binom{n-1}{k}+\frac{1}{n}\sum_{k=1}^{n-1}(-1)^{k+1}\binom{n}{k}+(-1)^{n+1}\frac{1}{n}$$
$$=a_{n-1}+\frac{1}{n}\sum_{k=1}^{n}(-1)^{k+1}\binom{n}{k}=a_{n-1}+\frac{1}{n}.$$

因为 $a_1=1$，由上式及归纳法即得结果.

6 当 $n<m$ 和 $n=m$ 时易知结论成立. 当 $n>m$ 时，用(12)及(9)，我们得出

$$\sum_{k=m}^{n}(-1)^{k+m}\binom{n}{k}\binom{k}{m}=\sum_{k=m}^{n}(-1)^{k+m}\binom{n}{m}\binom{n-m}{k-m}\ (\text{记 } i=k-m)$$
$$=\binom{n}{m}\sum_{i=0}^{n-m}(-1)^{i}\binom{n-m}{i}=0.$$

7 记所说的和为 a_n，并记 $b_n=\sum_{k=n+1}^{2n}\binom{2n}{k}$，这是与 a_n“互补”的数列，则 $a_n+b_n=2^{2n}$，又由(4)可得

$$b_n=\sum_{k=n+1}^{2n}\binom{2n}{2n-k}=\sum_{k=0}^{n-1}\binom{2n}{k}=a_n-\binom{2n}{n}.$$

由此易得结果.

8 记 $a_n=\sum_{k=0}^{\left[\frac{n}{2}\right]}\left\{\binom{n}{k}^2+\binom{n}{k-1}^2\right\}$，$b_n=2\sum_{k=0}^{\left[\frac{n}{2}\right]}\binom{n}{k}\binom{n}{k-1}$.

我们证明 $a_n-b_n=\frac{1}{n+1}\binom{2n}{n}$.

当 n 为偶数时，由(4)及范德蒙恒等式易知(参考注 4).

$$a_n=\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n},$$

$$b_n=\sum_{k=0}^{n}\binom{n}{n-k}\binom{n}{k-1}=\binom{2n}{n-1}=\binom{2n}{n+1}.$$

故 $a_n-b_n=\binom{2n}{n}\left(1-\frac{n}{n+1}\right)=\frac{1}{n+1}\binom{2n}{n}$. 如果 n 是奇数，则

$$a_n=\binom{2n}{n}-\left(\frac{n}{\frac{n+1}{2}}\right)^2,\ b_n=\binom{2n}{n-1}-\left(\frac{n}{\frac{n-1}{2}}\right)^2.$$

由此即得 $a_n-b_n=\binom{2n}{n}-\binom{2n}{n-1}=\frac{1}{n+1}\binom{2n}{n}$.

9 假设有 n、k 使所说的四个数成等差数列，则从 $2\binom{n}{k+1}=\binom{n}{k}+\binom{n}{k+2}$ 得出

$$\frac{k+1}{n-k}+\frac{n-k-1}{k+2}=2. \qquad ①$$

再由 $2\binom{n}{k+2}=\binom{n}{k+1}+\binom{n}{k+3}$ 可推出，将 k 换为 $k+1$ 时①也成立. 此外，用 $n-k-2$ 代换 k，①的左边不变. 因①去分母后是关于 k 的二次方程，上面的讨论表明，该二次方程有四个根：k、$k+1$、$n-k-2$、$n-(k+1)-2$. 因此必须有 $k=n-k-3$，$k+1=n-k-2$. 由此得 $n=2k+3$，故 n 是奇数，而 $k=\frac{n-3}{2}$，所以问题中说的四个数是 n 阶二项式系数中的中间四项，由二项式系数的单峰性，即知它们不能成等差数列.

10 从 $2n$ 个不同元素中取 2 个元素，有 $\binom{2n}{2}$ 种取法. 另一方面，这也可按下面的方式计数：将 $2n$ 个元素（任意）分为两个 n 元集合，可在同一个集中取 2 个元素，或各在一个集合中取 1 个元

素. 前者有 $2\binom{n}{2}$ 种取法，后者(由乘法原理)有 n^2 种取法. 这两类取法显然没有重复，故共有 $2\binom{n}{2}+n^2$ 种取法，由此得到结果.

11 由(11)、(4)及范德蒙恒等式，我们有

$$\sum_{k=1}^{n}k\binom{n}{k}^2=\sum_{k=1}^{n}n\binom{n-1}{k-1}\binom{n}{k}=n\sum_{k=1}^{n}\binom{n-1}{n-k}\binom{n}{k}$$
$$=n\binom{2n-1}{n}=n\binom{2n-1}{n-1}.$$

考虑下面的计数问题，可导出等式的一个组合证明：从 n 个男士、n 个女士中选取 n 人组成委员会，并规定委员会的主席必须为女士.

首先，从 n 个女士中选一人作为主席的方式共 n 种；选定主席后，再从剩下的 $2n-1$ 个人中选取 $n-1$ 人(作为委员会的成员)，共有 $\binom{2n-1}{n-1}$ 种选法. 由乘法原理，所说的 n 人委员会的选取方式共有 $n\binom{2n-1}{n-1}$ 种.

另一方面，对任意 k $(1\leqslant k\leqslant n)$，先从 n 个女士中选取 k 个人作为委员会成员的方式有 $\binom{n}{k}$ 种，而其中一人任主席的方式有 k 种选法；再于 n 位男士中选取 $n-k$ 人作为委员的方式有 $\binom{n}{n-k}$ 种，因此，有 k 位女士(其中一人为主席)的 n 人委员会有 $k\binom{n}{k}\binom{n}{n-k}=k\binom{n}{k}^2$ 种选法. 由加法原理，对 $k=1,\cdots,n$ 求和，则所说的选法共有 $\sum_{k=1}^{n}k\binom{n}{k}^2$ 种. 综合这两种计数结果，即得求证的等式.

第3讲

计数:对应与递推

1 设 f 是满足要求的任一映射,并设 $f(1)$, $f(2)$, …, $f(n)$(从左往右)依次有 x_1 个 1, x_2 个 2, …, x_n 个 n,则 $(x_1, \cdots, x_n)$ 是方程 $x_1+\cdots+x_n=n$ 的一组有序非负整数解. 反过来,由方程的任一组非负整数解 $(x_1, \cdots, x_n)$ 可作出一个符合要求的映射 f(取 $f(1)=\cdots=f(x_1)=1$, $f(x_1+1)=\cdots=f(x_1+x_2)=2$, …, $f(x_1+\cdots+x_{n-1}+1)=\cdots=f(x_1+\cdots+x_n)=n$). 从而由例 1 知所求的个数是 $\binom{2n-1}{n}$.

2 第 i 种明信片的寄法等于 $x_1+\cdots+x_n=a_i$ 的(有序)非负整数解的个数,即为 $\binom{a_i+n-1}{n-1}$. 故所求的方法数是

$$\binom{a_1+n-1}{n-1}\cdots\binom{a_k+n-1}{n-1}.$$

3 用例 1 的解法:将 n 个相同的球排成一行,每两个球之间有一个空隙,共有 $n-1$ 个空隙,每个空隙均有"插"与"不插"隔板两种选择. 而一种插隔板的方式对应了 n 的一个有序分拆,且一个有序分拆也对应了一种插隔板的方式. 因此所求的分拆数是 2^{n-1}.

4 圆周上每四个点构成一个凸四边形,其对角线(是所考虑的两条弦)交于一点. 因此每四点的集合对应于一个交点. 由于无三弦交于一点,所以不同的四点集对应于不同的交点. 反过来,

对任一交点，易知有一个四点集合（如上所说的）与之对应. 所以，交点的个数就是 n 个点的四元子集的个数 $\binom{n}{4}$.

5 设 n 条直线将平面分成了 a_n 个部分，则易知 $a_1=2$，$a_{n+1}=a_n+n+1$. 由此知 $a_n=\dfrac{n(n+1)}{2}+1$.

6 记所求的个数为 a_n. 则 $a_1=2$，$a_2=3$. 将符合要求的子集分为两类：第一类不含 n，这样的子集共 a_{n-1} 个；第二类含有 n，因而不能包含 $n-1$，这样的子集有 a_{n-2} 个. 故 $a_n=a_{n-1}+a_{n-2}$. 这与斐波那契数列 f_n 的递推公式相同. 考虑到 a_n 的初值，我们得出 $a_n=f_{n+2}$，其中 f_n 的定义为 $f_1=f_2=1$，$f_n=f_{n-1}+f_{n-2}(n\geqslant 3)$，其通项公式极易求出.

请注意，若将符合要求的子集按 0 元集，1 元集，…，n 元集分类，并应用例 8 的结果，我们得出 $a_n=\sum\limits_{k=0}^{n}\binom{n-k+1}{k}$，结合上面的结果，则产生一个有趣的恒等式

$$\sum_{k=0}^{n}\binom{n-k+1}{k}=f_{n+2}.$$

7 记 b_n 是所求的个数. 则 $b_1=2$，$b_2=3$，$b_3=5$. 当 n 为奇数时，将所说的序列分为两类：若 $a_n=1$，则 $a_{n-1}=1$，故符合要求的序列为 b_{n-2} 个；若 $a_n=0$，当 $a_{n-1}=1$ 时，序列的个数是 b_{n-2}，当 $a_{n-1}=0$ 时，必须 $a_{n-2}=0$，这样的序列有 b_{n-3} 个，因此

$$b_n=2b_{n-2}+b_{n-3}(n\geqslant 4). \qquad ①$$

这一递推公式在 n 为偶数时仍成立. 最后，不难由①及归纳法证明 $b_n=b_{n-1}+b_{n-2}$. 从而 $b_n=f_{n+2}$，这里 f_n 是斐波那契数列.

8 设取出的 k 个数为 $a_1<a_2<\cdots<a_k$，证明这一组数与 $a_1<a_2-1<a_3-2<\cdots<a_k-(k-1)$ 一一对应，后者是 $n-(k-1)$ 个元素 1，2，…，$n-(k-1)$ 的一个 k-组合. 从而所求的个数是

$\binom{n-k+1}{k}$.

9 令 $b_i=a_i-i+1$ $(i=1,\cdots,n)$，则 $1\leqslant b_1\leqslant b_2\leqslant\cdots\leqslant b_k\leqslant n-k+1$，且每个 b_i 是奇数. 反过来，每一个这样的序列 b_i 均决定一个符合要求的序列 a_i. 因此，所求的个数等于 1，2，…，$n-k+1$ 中全体奇数的 k 可重组合的个数，即为 $\binom{m+k-1}{k}$，这里 $m=\left[\frac{n-k+2}{2}\right]$.

10 设 0 出现偶数次的序列有 x_n 个，出现奇数次的有 y_n 个. 则 $x_n+y_n=k^n$.

在 a_1，a_2，…，a_{n-1} 中含偶数个 0 时，取 $a_n\neq 0$；否则，取 $a_n=0$，这就产生 n 项且含偶数个 0 的序列. 易见，每个 n 项且含偶数个 0 的序列均可这样产生. 所以 $x_n=(k-1)x_{n-1}+y_{n-1}$，结合 $x_{n-1}+y_{n-1}=k^{n-1}$（见前面的结果），得出

$$x_n=(k-2)x_{n-1}+k^{n-1}. \qquad ②$$

为了求解②，我们先利用②导出

$$\begin{aligned}x_n-kx_{n-1}&=(k-2)x_{n-1}+k^{n-1}-k(k-2)x_{n-2}-k^{n-1}\\&=(k-2)x_{n-1}-k(k-2)x_{n-2},\end{aligned}$$

即 $x_n-(2k-2)x_{n-1}+k(k-2)x_{n-2}=0$. 由此易解得 $x_n=\frac{1}{2}[k^n+(k-2)^n]$. 这也可以由②反复递推得出来.

11 采用与例 2 相同的数表，显然，$S_1\subseteq S_2\subseteq\cdots\subseteq S_k$ 等价于数表中任一列中的数（从上到下）为一个由 0，1 构成的单调不减的数列.（用递推）易知这样的数列恰有 $k+1$ 个，由此得出数表共有 $(k+1)^n$ 个，此即所求的子集组的个数.

此外，也不难导出问题的递推公式. 设 $f(n,k)$ 为所求的个数. 对 $0\leqslant i\leqslant n$ 及固定的 i 元子集 S_k，相应的子集组 $(S_1,\cdots,$

S_{k-1}）的个数显然是 $f(i, k-1)$，又因为这种 S_k 有 $\binom{n}{i}$ 个，故

$$f(n, k)=\sum_{i=0}^{n}\binom{n}{i}f(i, k-1), \qquad ③$$

而 $f(0, k)=1$. 由这递推关系不易直接解出 $f(n, k)$；但若猜出了问题的答案，用③及归纳法便极易证明.

12 由 n 个 1，n 个 0 组成的序列有 $\binom{2n}{n}$ 个. 下面计算其中不满足条件(2) 的序列的个数. 将这样的数列称为坏序列. 在一个坏序列 S 中，必有一个时刻(从左向右计数时)，首次出现 0 的个数超过 1 的个数，此时 0 的个数比 1 的个数多 1. 若交换此刻及之前的 0 与 1(将 0 换为 1，同时将 1 换为 0)，则得到的新序列 T 中有 $n+1$ 个 1，$n-1$ 个 0.

不难证明，上述交换 0，1 的法则，给出了从所有坏序列到由 $n+1$ 个 1，$n-1$ 个 0 组成的序列的一个一一对应.

事实上，这个对应是一个单射. 因为对于另一个坏序列 S'，或者 S' 中第一次出现 0 的个数多于 1 的个数的时刻不同于 S 的时刻，或者在相同的时刻 0 的个数多于 1 的个数，由于 $S\neq S'$，则 S 与 S' 在此刻以后的项不全相同. 无论哪一种情况，对应的 T 与 T' 不相同.

这个对应是一个满射：对于任一个由 $n+1$ 个 1 及 $n-1$ 个 0 组成的序列 T，由于其中 1 的个数多于 0 的个数，故将 T 从左向右计数时，必有一个时刻，首次出现 1 的个数多于 0 的个数，将此刻及之前的 0 与 1 交换，则产生了一个坏序列 S，显然，此 S 按所说的交换 0，1 的法则后，恰好就对应 T. 因此这个对应法则是满射.

由于所说的对应是一一对应，故坏序列的个数即是由 $n+1$ 个 1 及 $n-1$ 个 0 组成的序列的个数，这是 $\binom{2n}{n+1}$ 个. 故问题中所求

的序列的个数为$\binom{2n}{n}-\binom{2n}{n+1}=\frac{1}{n+1}\binom{2n}{n}$.

注 数$C_n=\frac{1}{n+1}\binom{2n}{n}$称为第$n$个Catalan数，许多计数问题均与此有关.

第 4 讲

计数:容斥原理

1 记 S_k 是不超过 1000 且被 k 整除的正整数的集合,用定理 2 求 $|S_2 \cup S_3 \cup S_5|$. 答:734.

2 记 S_1 是出现 abc 的全排列,S_2 是出现 ef 的全排列. 则所求的个数是 $|\overline{S}_1 \cap \overline{S}_2| = 6! - 5! - 4! + 3! = 582$.

3 从 X 到 Y 的映射共有 m^n 个(因 X 中任一元的像可为 Y 中的任一个元素). 设 $Y = \{y_1, \cdots, y_m\}$,并设 S_i 是不以 y_i 为像的映射的集合 $(i = 1, \cdots, m)$,则易知 $|S_{i_1} \cap \cdots \cap S_{i_k}| = (m-k)^n$ (这里 $1 \leqslant i_1 < \cdots < i_k \leqslant n$,而 $1 \leqslant k \leqslant m-1$). 由容斥原理(定理 1)可求出满射的个数为

$$|\overline{S}_1 \cap \cdots \cap \overline{S}_m| = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n.$$

4 设 S_k 是 k 与 $k+n$ 相邻的排列的个数 $(k = 1, 2, \cdots, n)$. 对任意 r $(1 \leqslant r \leqslant n)$ 及 $1 \leqslant i_1 < \cdots < i_r \leqslant n$,易知 $|S_{i_1} \cap \cdots \cap S_{i_r}| = 2^r (2n-r)!$. 故由容斥原理(定理 2)知

$$|S_1 \cup \cdots \cup S_n| = \sum_{r=0}^{n} (-2)^r \binom{n}{r} (2n-r)!.$$

5 用注 3 中的记号及上面的结果知 $\sigma_r = 2^r \binom{n}{r} (2n-r)!$ $(r = 1, 2, \cdots, n)$. 由定理 4 得出

$$|S_1 \cup \cdots \cup S_n| < \sigma_1 - \sigma_2 + \sigma_3 = \frac{2}{3} \cdot (2n)!;$$

以及 $|S_1 \cup \cdots \cup S_n| > \sigma_1 - \sigma_2 + \sigma_3 - \sigma_4 > \frac{5}{8} \cdot (2n)!$.

6 作替换 $y_1 = x_1 - 1$，$y_2 = x_2$，$y_3 = x_3 - 4$，$y_4 = x_4 - 2$，则问题化为求

$$y_1 + y_2 + y_3 + y_4 = 13 \qquad ①$$

满足 $0 \leqslant y_1 \leqslant 5$，$0 \leqslant y_2 \leqslant 7$，$0 \leqslant y_3 \leqslant 4$，$0 \leqslant y_4 \leqslant 4$ 的整数解的个数.

记 S 为方程①的非负整数解的集合；S_1、S_2、S_3、S_4 分别是 S 的满足 $y_1 > 5$，$y_2 > 7$，$y_3 > 4$，$y_4 > 4$ 的子集，则所求的解的个数为 $|\overline{S}_1 \cap \overline{S}_2 \cap \overline{S}_3 \cap \overline{S}_4|$.

由第 3 讲例 1 知 $|S| = \binom{16}{3} = 560$. 为求出 $|S_1|$，再令 $y_1' = y_1 - 6$，则 $|S_1|$ 等于 $y_1' + y_2 + y_3 + y_4 = 7$ 的非负整数解的个数 $\binom{4+7-1}{4} = 120$. 同样可算出

$$|S_2| = \binom{4+5-1}{4} = 56,\ |S_3| = |S_4| = \binom{4+8-1}{4} = 165,$$

以及 $|S_1 \cap S_3| = |S_1 \cap S_4| = \binom{4+2-1}{4} = 5$，

$$|S_2 \cap S_3| = |S_2 \cap S_4| = 1,$$

$$|S_3 \cap S_4| = \binom{4+3-1}{4} = 15,\ |S_1 \cap S_2| = 0;$$

而 $|S_i \cap S_j \cap S_k|$ 和 $|S_1 \cap S_2 \cap S_3 \cap S_4|$ 都是 0. 最后由容斥原理求得问题中的解的个数是 81.

7 由第 3 讲例 1 可知，方程

$$x_1 + \cdots + x_n = n \qquad ①$$

的非负整数解 $(x_1, \cdots, x_n)$ 的个数为 $\binom{2n-1}{n}$. 若方程 ① 中有一个 $x_i \geqslant 3$，共有 $\binom{n}{1}$ 种选择. 此时以 $x_i - 3$ 换 x_i，则方程的解数与

$$x_1 + \cdots + x_n = n + 3$$

的非负整数解的个数相同，为 $\binom{2n+2}{n+3}$（由第 3 讲，例 1）.

对于 $1 \leqslant k \leqslant n$，若方程 ① 中有 k 个 $x_i \geqslant 3$，这共有 $\binom{n}{k}$ 种选择；将这些 x_i 换为 $x_i - 3$，则此时①的解的个数等于方程

$$x_1 + \cdots + x_n = n + 3k$$

的非负整数的解的个数，这是 $\binom{2n+3k-1}{n+3k} = \binom{2n+3k-1}{n-1}$.

故由容斥原理知，所求的解数是 $\sum_{k=0}^{n} (-1)^k \binom{n}{k} \binom{2n+3k-1}{n-1}$.

第 5 讲

组 合 问 题

1 设黑板上写的数是 a_1，…，a_n，由于 $(1+a)(1+b)=1+(a+b+ab)$，故由操作的规则易知，乘积

$$(1+a_1)(1+a_2)\cdots(1+a_n)$$

在操作下保持不变，在本题的情形下，设最后剩下的数为 x，则

$$1+x=(1+1)\left(1+\frac{1}{2}\right)\cdots\left(1+\frac{1}{100}\right)$$

$$=2\cdot\frac{3}{2}\cdot\frac{4}{3}\cdot\cdots\cdot\frac{100}{99}\cdot\frac{101}{100}=101,$$

故 $x=100$.

2 设 $f(x)=ax^2+bx+c$，则

$$x^2 f\left(\frac{1}{x}+1\right)=a(x+1)^2+bx(x+1)+cx^2$$

$$=(a+b+c)x^2+(2a+b)x+a,$$

其判别式为 $(2a+b)^2-4a(a+b+c)=b^2-4ac$. 同样可验算得知 $(x-1)^2 f\left(\frac{1}{x-1}\right)$ 的判别式也是 b^2-4ac. 故在所说的操作下，$f(x)$ 的判别式保持不变. 因此不能通过操作由 x^2+4x+3 得到 $x^2+10x+9$（因两者的判别式不相等）.

3 (i)能. 不难具体指出变形的方法. (ii)不能. 设表中第一行（从左至右）的三个数是 a_1、a_2、a_3，第二行是 a_4、a_5、a_6，第三行

是 a_7，a_8，a_9，则

$$S=(a_1+a_3+a_5+a_7+a_9)-(a_2+a_4+a_6+a_8)$$

在变形下不变.

4 考虑给定点中距离最大的两个点 A、B，则其余的点都在以 AB 为直径的圆周上，由此易推出 $n\leqslant 4$.

5 易知若 $A=\varnothing$，则 $B=\varnothing$，故此时有 $|A|=|B|$. 若 $A\neq\varnothing$，设 $(a,b)\in A$，令 $f((a,b))=(a+b,a)$. 由于 $a+b\in S$，$(a+b)-a\in S$，故 $(a+b,a)\in B$. 即 f 是 A 到 B 的一个映射.

我们证明这是一个单射，因为若 A 中有两个元素 $(a,b)\neq(a',b')$，但 $f((a,b))=f((a',b'))$，则有 $(a+b,a)=(a'+b',a')$，从而可知 $a=a'$，$b=b'$，矛盾. 因此 f 是 A 到 B 的一个单射，故 $|A|\leqslant|B|$.

同样，对 $(a,b)\in B$，令 $g((a,b))=(b,a-b)$，则易知 g 是 B 到 A 的一个映射，且是单射，从而 $|B|\leqslant|A|$. 综合起来即知 $|A|=|B|$.

6 注意，仅由 1、2 构成的 n 位数共有 2^n 个. 我们对 n 归纳来证明结论. $n=2$ 时易知结论成立，设 $n\geqslant 2$，且结论在 n 时已成立，设 C_1，C_2，…，C_{2^n} 是从某点起始(按逆时针)排列的数，则(按逆时针排列的)2^{n+1} 个数 $\overline{1C_1}$，$\overline{1C_2}$，…，$\overline{1C_{2^n}}$，$\overline{2C_{2^n}}$，…，$\overline{2C_2}$，$\overline{2C_1}$ 符合要求.

7 将 6 道题记为 1，2，…，6. 显然无人做出 6 道题，若有人做出 5 道题，设他未做出的是题 6，则他与任一个学生都未做出的题只能是题 6，从而题 6 无人做出，与条件矛盾. 因此每个人至多做出 4 道题.

(i) 设有人做对 4 道题，设为题 1、2、3、4，则易知没有人同时答对题 5，6. 因答对题 5，6 的人各有 100 人，故全部人数 $\geqslant 200+1=201$.

(ii) 若每位学生至多答对 3 道题，由于全部学生答对的题数

之和=600，故人数$\geqslant\frac{600}{3}=200$.

下面的例子表明，可以恰有200人，设答对题(1，2，3)，(1，5，6)，(2，4，5)，(3，4，6)的各有50人，则学生为200人，且每题恰有100人答对.

因此至少有200个学生.

8 将数表中位于第i行与第j列交叉格子中的数记为$a_{ij}(1\leqslant i,j\leqslant n)$，并将第$i$行中的数之和记为$s_i$，由于只有$n$个列，且每一列中数的对换方式仅有有限种，故能够产生的新数表仅有有限个，故必有一个数表，使相应的$|s_1|+|s_2|+\cdots+|s_n|$取得最小值，我们下面证明，此时必有$|s_k|\leqslant 2\ (k=1,2,\cdots,n)$.

反证法：假设有一个k使$|s_k|>2$，不妨设$s_k>2$. 因数表中的数之和为0，故$s_1+\cdots+s_n=0$，故存在一个i，使$s_i<0$. 此外，显然有一个j使$a_{kj}>a_{ij}$(否则$s_i>s_k$). 将第j列中的a_{kj}与a_{ij}交换，我们证明，交换后得到的数表中相应的$|s_1'|+\cdots+|s_n'|$将严格减少(其中s_m'是新数表中第m行的数之和)，这就产生了矛盾(因我们已选择$|s_1|+\cdots+|s_n|$为最小)，故所有的$|s_k|\leqslant 2$.

为了证明刚才说的断言，我们注意，对$m\neq i,k$，显然有$s_m'=s_m$，而

$$s_k'=s_k-a_{kj}+a_{ij},\ s_i'=s_i+a_{kj}-a_{ij}.$$

由于$|a_{kj}|\leqslant 1$，$|a_{ij}|\leqslant 1$，故$s_k>2\geqslant a_{kj}-a_{ij}$，即$s_k'>0$；又由于$s_i<0$，$a_{kj}-a_{ij}>0$，故有严格的不等式

$$|s_i'|=|s_i+a_{kj}-a_{ij}|<|s_i|+(a_{kj}-a_{ij}).$$

于是

$$\begin{aligned}|s_k'|+|s_i'|&<(s_k-a_{kj}+a_{ij})+(|s_i|+a_{kj}-a_{ij})\\&=|s_k|+|s_i|.\end{aligned}$$

所以$|s_1'|+\cdots+|s_n'|<|s_1|+\cdots+|s_n|$，即上述的结论得证.

9 对n进行归纳. 当$n=1$，2时易知结论成立. 设$n\geqslant 3$，并

设结论当为n时已成立. 现考虑$2(n+1)$个数对(a_i, b_i). 由对称性可设$a_1 \geqslant a_2 \geqslant \cdots \geqslant a_{2n+2}$. 由归纳假设,可将$2n$对$(a_3, b_3)$,$(a_4, b_4)$,…,$(a_{2n+2}, b_{2n+2})$分成两组符合要求. 设$A_1$、$A_2$分别表示第一组与第二组中的$a_i$之和,$B_1$、$B_2$分别表示第一组与第二组中的$b_i$之和,则$|A_1 - A_2| \leqslant a_2$(因为$a_3, \cdots, a_{2n+2} \leqslant a_2$,故$\max\limits_{3\leqslant i\leqslant 2n+2} a_i \leqslant a_2$),及$|B_1 - B_2| \leqslant \max\limits_{3\leqslant i\leqslant 2n+2} b_i$.

无妨设$B_1 \leqslant B_2$. 若$b_1 \leqslant b_2$,则将(a_2, b_2)放入第一组,(a_1, b_1)放入第二组. 此时第一组与第二组的a_i之和分别为$A_1 + a_2$及$A_2 + a_1$,且有

$$\begin{aligned}|(A_1 + a_2) - (A_2 + a_1)| &\leqslant |A_1 - A_2| + |a_1 - a_2| \leqslant a_2 + (a_1 - a_2)\\ &= a_1 = \max_{1\leqslant i\leqslant 2n+2} a_i.\end{aligned}$$

两组中b_i之和分别为$B_1 + b_2$及$B_2 + b_1$,由于$B_1 - B_2 \leqslant 0$,及$b_2 - b_1 \geqslant 0$,故

$$\begin{aligned}|(B_1 + b_2) - (B_2 + b_1)| &= |(B_1 - B_2) + (b_2 - b_1)|\\ &\leqslant \max\{B_2 - B_1, b_2 - b_1\}\\ &\leqslant \max_{1\leqslant i\leqslant 2n+2} b_i.\end{aligned}$$

(利用结论,若x、y异号,则$|x + y| \leqslant \max(|x|, |y|)$.)因此上述的分组方式符合要求.

若$b_1 > b_2$,则将(a_1, b_1)放入第一组,(a_2, b_2)放入第二组,则与上面相同的证明可知,这种分组方式也符合要求(细节这里略去).

第 6 讲

数 的 整 除

1 因 k 的倍数具有形式 kx，x 为一个整数. 因此 1，2，…，n 中被 k 整除的个数，即是满足 $kx \leqslant n$ 的最大整数 x，这由定义可知是 $\left[\frac{n}{k}\right]$.

2 因为 $(ad+bc)-(ab+cd)=(a-c)d-(a-c)b$，能被 $a-c$ 整除，故由条件 $a-c \mid ab+cd$，推出 $a-c \mid ad+bc$.

3 利用 $b(a^2+ab+1)-a(b^2+ab+1)=b-a$（参考注 3 中的(ii)）.

4 记 $(a, b)=d$，则 $a=a_1 d$，$b=b_1 d$，其中 a_1，b_1 是互素整数(性质(11)). 由已知条件可推出 $d \mid a_1+b_1$，故 $d \leqslant a_1+b_1$（性质(3)），从而 $d^2 \leqslant a+b$，即 $d \leqslant \sqrt{a+b}$.

5 设 $d=(2^m-1, 2^n+1)$，则 $2^m-1=du$，$2^n+1=dv$，u，v 为整数. 由 $(du+1)^n=(dv-1)^m$，并将两边展开(注意 m 是奇数)，得出 $dA+1=dB-1$（A、B 为整数），由此易知 $d=1$.

另一种解法：由于 m 是奇数，用公式⑥得出 $(2^n+1) \mid (2^{mn}+1)$. 此外，$2^{mn}-1$ 是 2^m-1 的倍数，设 $2^{mn}-1=(2^m-1)q$，则 2^n+1 整除 $(2^m-1)q+2$. 由此易得出结果(参考注 10).

6 由带余除法，$n=mq+r$，$0 \leqslant r<m$，而 $q \geqslant 0$. 若 q 是偶数，由 $a^n+1=(a^{mq}-1)a^r+(a^r+1)$ 易见，必有 $a^m+1 \mid a^r+1$，但 $0<a^r+1<a^m+1$，这不可能成立. 因此 q 是奇数，由 $a^n+1=(a^{mq}+1)a^r-(a^r-1)$，并注意 $a^m+1 \mid a^{mq}+1$，我们推出 $a^m+1 \mid a^r-1$，但 $0 \leqslant r<m$，故必须 $a^r-1=0$，即 $r=0$，所以

$n=mq$.

7 易知条件是充分必要的. 又易验证 $x=x_0+\frac{b}{(a,b)}t$, $y=y_0-\frac{a}{(a,b)}t$ 是所说方程的解. 我们只要证明方程的任一解 (x',y') 均是这一形式. 将 $ax_0+by_0=c$ 与 $ax'+by'=c$ 相减,得出 $a(x_0-x')+b(y_0-y')=0$. 由此 $a\mid b(y_0-y')$, 故 $\frac{a}{(a,b)}\Big|\frac{b}{(a,b)}(y_0-y')$. 但是 $\frac{a}{(a,b)}$ 与 $\frac{b}{(a,b)}$ 互素(性质(11)),所以 $\frac{a}{(a,b)}\Big|(y_0-y')$. 于是 $y_0-y'=\frac{a}{(a,b)}t$, t 为某个整数,进而 $x'=x_0+\frac{b}{(a,b)}t$.

请注意,为了求出方程①的一组整数解,可以先求方程 $ax+by=(a,b)$ 的一组解,这可以用欧氏算法来求,但当 $|a|$、$|b|$ 不太大时,也可用尝试法求得.

8 由于 $(a,b)=1$, 故有整数 x、y 使 $ax+by=1$. 由带余除法, $x=bq+r$, $0\leqslant r<b$. 令 $aq+y=-s$, 则得出 $ar-bs=1$. 因 $b\neq 1$, 故 $r\neq 0$, 即 $0<r<b$. 由此即知 $0<s<a$. 唯一性的证明可参考(4)的论证.

9 由于 $(a,b)=1$, 故 $ax+by=n$ 必有一组整数解. 由上一题中的做法,我们不妨设 $0\leqslant x<b$. 这样,当 $n>ab-a-b$ 时,我们有

$$by=n-ax>ab-a-b-ax\geqslant ab-a-b-a(b-1)=-b,$$

故 $y>-1$ 也是非负整数.

当 $n=ab-a-b$ 时,如果方程有非负整数解 (x,y),则 $ab=(x+1)a+(y+1)b$, 故 $a\mid(y+1)b$. 因 $(a,b)=1$, 所以 $a\mid y+1$. 因 $y+1>0$, 故 $y+1\geqslant a$. 同理 $x+1\geqslant b$. (参考注 3.)于是 $ab=(x+1)a+(y+1)b\geqslant ab+ab=2ab$. 矛盾.

10 (i) 由 $(a,b)=1$ 及性质(12),推出 $(a^2,b)=1,\cdots,(a^m,b)=1$,进而有 $(a^m,b^2)=1,\cdots,(a^m,b^n)=1$.

(ii) 设 $d=(a,b)$，若 $d=1$，则用(i)可知 $(a^n,b^n)=1$. 因此，我们有

$$d^n=d^n\left(\left(\frac{a}{d}\right)^n,\left(\frac{b}{d}\right)^n\right)=\left(\left(\frac{a}{d}\right)^n\cdot d^n,\left(\frac{b}{d}\right)^n\cdot d^n\right)=(a^n,b^n).$$

(用性质(10)和(11).)

11 设 $ab=x^k$，$x>0$. 由于 $(a,b)=1$，故 $(a^{k-1},b)=1$. 我们设 $(a,x)=d$，则由上一题推出

$$d^k=(a^k,x^k)=(a^k,ab)=a(a^{k-1},b)=a,$$

即 a 是整数的 k 次幂. 同理 $b=(b,x)^k$，b 也是整数的 k 次幂.

12 设有理数 $x=\frac{p}{q}$，(p、q 是互素整数)，由 x^k 是整数，推出 $q^k\mid p^k$. 但 $(p,q)=1$，故 $(p^k,q^k)=1$，所以必须 $q^k=\pm1$，即 $q=\pm1$，从而 $x=\pm p$ 为整数.

13 唯一性是显然的：设 $d\mid mn$，$d\geqslant1$，若 $d=m_1n_1=m_2n_2$，这里 m_1，m_2 为 m 的正约数，n_1，n_2 为 n 的正约数，则 $m_2\mid m_1n_1$，但 $(m,n)=1$，故 $(m_2,n_1)=1$，从而推出 $m_2\mid m_1$. 同样 $m_1\mid m_2$，故 $m_1=m_2$，进而 $n_1=n_2$.

为了证明有所说的表示，设 $d\mid mn$，$d\geqslant1$，则

$$mn=dx，\text{对某个正整数 } x. \qquad ①$$

设 $(d,m)=r$，则 $d=d'r$，$m=m'r$，其中 $(m',d')=1$. 代入①式得 $m'n=d'x$. 故 $d'\mid m'n$，但 $(d',m')=1$，因此 $d'\mid n$. 又 r 显然是 m 的正约数，故 $d=d'r$ 是 m 的一个正约数与 n 的一个正约数的积.

14 (i) 反复用 q 作带余除法，可将 n 表示为所说的形式：

$$n=n_1q+a_0,\ 0\leqslant a_0\leqslant q-1,$$
$$n_1=n_2q+a_1,\ 0\leqslant a_1\leqslant q-1,$$
$$\cdots$$

如此得到的商 n_i 严格递降，最终必然得出 0. 设 k 是使 $a_k \neq 0$ 的最大下标，则 $n = a_0 + n_1 q$，$n_1 = a_1 + n_2 q$，…，$n_{k-1} = a_{k-1} + n_k q$，$n_k = a_k$，于是 $n = a_0 + a_1 q + \cdots + a_k q^k$，其中 $0 \leqslant a_i \leqslant q-1$ $(i = 0, 1, \cdots, k)$，且 $a_k \neq 0$.

假设 n 还有一种符合要求的表示

$$n = a'_0 + a'_1 q + \cdots + a'_l q^l,\ 0 \leqslant a'_i \leqslant q-1\ (i = 0, 1, \cdots, l),$$

则 $q \mid (a_0 - a'_0)$，但 $0 \leqslant |a_0 - a'_0| \leqslant \max(a_0, a'_0) < q$，故必须 $a_0 = a'_0$. 于是我们得到

$$a_1 + a_2 q + \cdots + a_k q^{k-1} = a'_1 + a'_2 q + \cdots + a'_l q^{l-1}.$$

同样得到 $a_1 = a'_1$. 如此进行，可知必须 $k = l$，且 $a_i = a'_i$ $(i = 0, 1, \cdots, k)$.

(ii) 易知 $n_{i+1} = \left[\dfrac{n_i}{q}\right]$（参考注 5），由此不难归纳地推出 $n_i = \left[\dfrac{n}{q^i}\right]$（利用：对正整数 m 有 $\left[\dfrac{[x]}{m}\right] = \left[\dfrac{x}{m}\right]$），于是(ii)显而易见.

15 当 $1 \leqslant k \leqslant 2^n - 1$ 时，由正整数二进制表示的唯一性（见上一题）推知，2^n 个数 $a_0 + a_1 \cdot 2 + \cdots + a_{n-1} \cdot 2^{n-1}$ ($a_i = 0$ 或 1)，恰给出了 $0, 1, \cdots, 2^n - 1$，故 k 是 2^{n-1} 的不同约数之和，从而是 m 的不同约数之和.

当 $2^n - 1 < k \leqslant m$ 时，由带余除法，$k = (2^n - 1)t + r$，$0 \leqslant r < 2^n - 1$. 显然 $t \leqslant 2^{n-1}$，故由上面的结论知，r 与 t 都是 2^{n-1} 的不同约数之和，于是 $(2^n - 1)t$ 可表示为 $m = 2^{n-1}(2^n - 1)$ 的不同约数之和（这些约数与表示 r 的约数显然不会有相同者）.

16 记符合要求的数的集合为 S. 首先证明，若 $m \in S$，则 m 与 a 互素. 事实上，对任意 $n \geqslant 1$，有

$$(a, A_n) = \left(a, 1 + a\sum_{k=0}^{n-1} a^k\right) = (a, 1) = 1.$$

因此，若 $m \in S$，则存在 $n \geqslant 1$，使得 $m \mid A_n$，故 $(m, a) \leqslant (A_n, a) =$

1，从而 m 与 a 互素.

显然 $m=1\in S$. 下面证明，若 $m>1$，$(m,\ a)=1$，则必有 $m\in S$.

考虑 $m+1$ 个数 A_1，A_2，…，A_{m+1}，因整数被 m 除得的余数有 m 种可能的值，故这 $m+1$ 个数中有两个被 m 除得相同的余数，从而这两数之差是 m 的倍数，设为 A_i 与 A_j $(1\leqslant i<j\leqslant m+1)$，因为

$$A_j-a_i=a^{i+1}\sum_{k=0}^{j-i-1}a^k,$$

被 m 整除，但 $(a,\ m)=1$，故 $(a^{i+1},\ m)=1$. 因此由上式推知 $A_{j-i-1}=\sum\limits_{k=0}^{j-i-1}a^k$ 被 m 整除（注意 $m>1$，故 $j-i-1$ 必须为正整数）. 因此 $m\in S$.

综上可知，所求的数是所有与 a 互素的正整数.

第 7 讲

素　　数

1 当 $n=1$ 时结论显然成立. 设 $n>1$, $n=p_1^{\alpha_1}\cdot\cdots\cdot p_k^{\alpha_k}$ 是 n 的标准分解,不妨设 α_1, …, α_l 为偶数,α_{l+1}, …, α_k 为奇数,则

$$\alpha_i=2a_i(i=1,\cdots,l),\ \alpha_j=2b_j+1\ (j=l+1,\cdots,k),$$

由此 n 可表示为

$$n=(p_1^{a_1}\cdot\cdots\cdot p_l^{a_l}p_{l+1}^{b_{l+1}}\cdot\cdots\cdot p_k^{b_k})^2 p_{l+1}\cdot\cdots\cdot p_k,$$

具有形式 q^2r,其中 r 无平方因子.

为了证明唯一性,设 $n=q^2r=q_1^2r_1$,这里 r、r_1 都是无平方因子的整数. 我们证明必有 $r=r_1$,从而 $q=q_1$.

为了证明 $r=r_1$,我们证明 r 与 r_1 的素因子完全相同. 假设这断言不对,不妨设有素数 p 整除 r,但不整除 r_1. 设 p 在 q 与 q_1 中出现的幂次分别为 a 及 a_1. 由于 r 无平方因子,故 p 在 r 中仅出现一次. 因此 p 在 q^2r 及 $q_1^2r_1$ 中出现的幂次分别为 $2a+1$ 及 $2a_1$,这两个幂次一奇一偶,显然不相等,但这不可能. 这就证明了上述的断言.

2 (i) 这可由(8)的第二种证明导出来. 若$\sqrt{n}$不是整数,则 n 的小于$\sqrt{n}$的正约数的个数$\leqslant[\sqrt{n}]$,从而大于$\sqrt{n}$的约数也 $\leqslant[\sqrt{n}]$ 个,故 $\tau(n)\leqslant 2[\sqrt{n}]<2\sqrt{n}$.

若$\sqrt{n}$是整数,则小于$\sqrt{n}$的正约数的个数 $\leqslant\sqrt{n}-1$,从而 $\tau(n)\leqslant 2(\sqrt{n}-1)+1=2\sqrt{n}-1<2\sqrt{n}$.

(ii) 注意,若 d 是 n 的一个正约数,则 $\frac{n}{d}$ 也是 n 的一个正约

数. 因此，若设 $1=d_1<\cdots<d_k=n$ 是 n 的全体正约数，这里 $k=\tau(n)$，则 $\frac{n}{d_k}<\cdots<\frac{n}{d_1}$ 也是 n 的全体正约数. 故

$$d_1\cdot\cdots\cdot d_k=\frac{n}{d_k}\cdot\cdots\cdot\frac{n}{d_1},$$

由此即得结果.

3 由第 6 讲中例 5 可知，$(M_p, M_q)=2^{(p,q)}-1=2-1=1$（对任意素数 $p\neq q$）.

4 对 $n\geqslant 2$，$2^{2^n}+2^{2^{n-1}}+1=(2^{2^{n-1}}+1)^2-(2^{2^{n-2}})^2=(2^{2^{n-1}}-2^{2^{n-2}}+1)(2^{2^{n-1}}+2^{2^{n-2}}+1)$. 因此，若记 $a_n=2^{2^n}+2^{2^{n-1}}+1$，则对 $n\geqslant 2$，有

$$a_n=(2^{2^{n-1}}-2^{2^{n-2}}+1)a_{n-1}. \qquad ①$$

易证 a_{n-1} 与 $2^{2^{n-1}}-2^{2^{n-2}}+1$ 互素. 显然 $a_1>1$ 有（至少一个）素因子. 归纳假设可得 a_{n-1} 至少有 $n-1$ 个不同的素因子（$n\geqslant 2$），由于 $2^{2^{n-1}}-2^{2^{n-2}}+1>1$ 有素因子 p，且 p 不整除 a_{n-1}（因为 $(a_{n-1}, 2^{2^{n-1}}-2^{2^{n-2}}+1)=1$），故由 ① 知 a_n 至少有 n 个不同的素因子.

5 设形如 $4k-1$ 的素数只有有限多个，设为 p_1，…，p_n. 考虑奇数 $N=4p_1\cdots p_n-1$. 易知 $N>1$，故 N 有素因子. 若所有这些素因子都是 $4k+1$ 形式，则它们的积也是这种形式. 但 N 是 $4k-1$ 形式，从而 N 必有一个素因子 p 形如 $4k-1$，又显然 p 不同于 p_1，…，p_n. 矛盾.

同样想法可证明 $6k-1$ 形式的素数有无穷多个（参考（4）的证明）.

6 可取这 n 个数为 $(n+1)!+2$，$(n+1)!+3$，…，$(n+1)!+(n+1)$. 对 $2\leqslant k\leqslant n+1$，因 $(n+1)!+k$ 有真约数 k，故它不是素数.

7 可以区分 n 是 $3k$，$3k+1$ 或 $3k+2$ 三种情况来证明.（或许是）更本质的解法是用第 6 讲练习题中的第 9 题. 由这易知，若

正整数a，b互素，则当$n>ab+a+b$时，n可表示为$ax+by$形式，其中$x\geqslant 2$，$y\geqslant 2$. 在本题中我们取$a=2$，$b=3$.

8 设$n=2^{k-1}m$，其中$k\geqslant 2$，$2\nmid m$. 由第7讲中公式⑤得出$2^km=2n=\sigma(n)=\dfrac{2^k-1}{2-1}\cdot\sigma(m)$，故$\sigma(m)=m+\dfrac{m}{2^k-1}$. 但$m$及$\dfrac{m}{2^k-1}$都是$m$的约数，而$\sigma(m)$为$m$的所有正约数之和，故$m$只有这两个约数，即$m$为素数，且$\dfrac{m}{2^k-1}=1$.

9 设$2^k\leqslant n<2^{k+1}$，则$k\geqslant 1$，我们证明2^k在1，2，…，n(的标准分解)中恰好出现一次. 因若有$m\leqslant n$，$m\neq 2^k$，使$2^k\mid m$，则$n\geqslant m=2^k\cdot l\geqslant 2^k\cdot 2>n$，矛盾！记$M$是不超过$n$的所有奇数之积，则易知

$$\begin{aligned}&M\cdot 2^{k-1}\left(1+\frac{1}{2}+\cdots+\frac{1}{n}\right)\\&=M\cdot 2^{k-1}+\frac{M\cdot 2^{k-1}}{2}+\cdots+\frac{M\cdot 2^{k-1}}{n}\end{aligned}$$

中，除去$\dfrac{M\cdot 2^{k-1}}{2^k}$外，其余项均是整数，因此$M\cdot 2^{k-1}\left(1+\dfrac{1}{2}+\cdots+\dfrac{1}{n}\right)$不是整数，故$1+\dfrac{1}{2}+\cdots+\dfrac{1}{n}(n>1)$不是整数.

10 与上题类似地证明. 设$3^k\leqslant 2n-1<3^{k+1}$，则$k\geqslant 1$. 证明$3^k$在$1$，$3$，…，$2n-1$中恰好出现一次.

11 因为2^k+1是大于1的奇数，故它有奇素数因子p. 从而$2\mid p^k+1$. 这表明，2^k+1的任一个素因子p，及$q=2$符合要求.

12 对任意一个素数p，设$p^{\alpha_i}\mid a_i$，$i=1$，…，n. 则由本讲中的(9)可知，只需证明

$$\max\{\alpha_1,\cdots,\alpha_n\}\geqslant\sum_{i=1}^{n}\alpha_i-\sum_{1\leqslant i<j\leqslant n}\min\{\alpha_i,\alpha_j\}.$$

这个不等式极易验证(不妨设 $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_n$,分别看上述不等式的左、右两边).

13 由于 $(m, n)[m, n] = mn$(见第 6 讲中(16)),故由韦达定理知,数对(m, n) 与数对$((m, n), [m, n])$ 均是二次方程 $x^2 - (m+n)x + mn = 0$ 的两个根. 因此这两组数对完全相同,若 $m = (m, n)$,则 $m \mid n$;若 $n = (m, n)$,则 $n \mid m$.

14 由于 $(ax+by)(ay+bx) = ab(x^2+y^2) + xy(a^2+b^2)$,故由条件知$(a^2+b^2) \mid ab(x^2+y^2)$. 若 a^2+b^2 与 x^2+y^2 互素,则 $(a^2+b^2) \mid ab$. 但是 $a^2+b^2 > ab > 0$,这是不可能的,从而产生矛盾. 因此 a^2+b^2 与 x^2+y^2 不互素.

第 8 讲

同　余　(一)

1 整数模 3 可表示为 $3k$、$3k+1$、$3k+2$ 三种形式之一. 因此其平方模 3 是 0 或 1. 类似地可证明另一个结论.

2 不必将整数模 8 分类,模 2 分类就够了(注意相邻整数之积是偶数).

3 将整数模 3 分类就够了.

4 将整数模 2 分类.

5 对 n 归纳. 当 $n=1$ 时易证. 假设当 $n-1$ 时结论成立,即 $a^{2^{n-1}}=1+2^{n+1}x$ (x 是一个整数),两边平方,即知 $a^{2^n}=1+2^{n+2}x'$ (x' 是一个整数).

另一种证法:利用恒等式(见第 6 讲例 1 的证明)

$$a^{2^n}-1=(a-1)(a+1)(a^2+1)(a^{2^2}+1)\cdots(a^{2^{n-1}}+1).$$

因上式右边是 $n+1$ 个项的积,每一项都是偶数(因 a 为奇数);而 $a-1$ 与 $a+1$ 中必有一个被 4 整除,因此 $2^{2^n}-1$ 能被 2^{n+2} 整除.

6 注意 $k\equiv-(p-k)\pmod p$,故由威尔逊定理得

$$\begin{aligned}&1^2\cdot3^2\cdot\cdots\cdot(p-2)^2\\&\equiv1\cdot(p-1)\cdot3\cdot(p-3)\cdot\cdots\cdot(p-2)\cdot2\cdot(-1)^{\frac{p-1}{2}}\\&=(-1)^{\frac{p-1}{2}}\cdot(p-1)!\equiv(-1)^{\frac{p+1}{2}}\pmod p.\end{aligned}$$

同样证明另一个同余式.

7 我们有 $2^{pq-1}-1=\left(2^{(p-1)q}-1\right)2^{q-1}+2^{q-1}-1$,交换 p、q

得另一个等式，可见问题中的两方面都成立(用费马小定理).

8 设 $n=a_k\times10^k+\cdots+a_1\times10+a_0(0\leqslant a_i\leqslant9,\ i=0,1,\cdots,k,\ a_k\neq0)$，则由 $10^i\equiv1(\mathrm{mod}\ 9)$(对所有 $i\geqslant0$)可知 $S(n)\equiv n(\mathrm{mod}\ 9)$. 由 $10^i\equiv-1(\mathrm{mod}\ 11)$(对奇数 $i\geqslant1$)，可知 $T(n)\equiv n(\mathrm{mod}\ 11)$.

9 设 $1=a_1<\cdots<a_k=m-1$ 是不超过 m，且与 m 互素的全部正整数，这里 $k=\varphi(m)$，$m\geqslant2$. 由于 $(m-a_i,\ m)=(a_i,\ m)=1$，故集合$\{a_1,\cdots,a_k\}$与$\{m-a_k,\cdots,m-a_1\}$相同. 因此 $a_1+\cdots+a_k=(m-a_k)+\cdots+(m-a_1)$，由这即得出结果.

10 在第 4 讲的等式⑥中取 $n=m=p-1$.

11 由于 $(a,\ 10)=1$，我们有 $a^{\varphi(25)}\equiv1(\mathrm{mod}\ 25)$，即 $a^{20}\equiv1(\mathrm{mod}\ 25)$. 又有 $a^2\equiv1(\mathrm{mod}\ 4)$，故 $a^{20}\equiv1(\mathrm{mod}\ 4)$. 因此 $a^{20}\equiv1\ (\mathrm{mod}\ 100)$，即 a^{20} 的末两位是 01(参考(6) 和(10)).

12 如果有一组 $a_i(1\leqslant i\leqslant n)$ 及 $b_i(1\leqslant i\leqslant n)$，使得 $a_1+b_1,\cdots,a_n+b_n$ 是模 n 的完系，则

$$\begin{aligned}1+2+\cdots+n&\equiv(a_1+b_1)+\cdots+(a_n+b_n)\\&\equiv(a_1+\cdots+a_n)+(b_1+\cdots+b_n)\\&\equiv2(1+2+\cdots+n)(\mathrm{mod}\ n),\end{aligned}$$

即 $n\left|\dfrac{n(n+1)}{2}\right.$. 因 n 为偶数，这不能成立.

13 由威尔逊定理，模 p 的任一缩系中数的乘积 $\equiv(p-1)\cdots2\cdot1=(p-1)!\equiv-1(\mathrm{mod}\ p)$.

14 设 $m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 m 的标准分解. 我们只需证明，对任意与 m 互素的 a，有 $a^{\varphi(m)}\equiv1(\mathrm{mod}\ p_i^{\alpha_i})$ $(i=1,\cdots,k)$(参考(10) 及第 7 讲中注 5).

由 $\varphi(m)$ 的计算公式及(6)易知，我们只需证明，对素数 p 及整数 $\alpha\geqslant1$，有 $a^{p^{\alpha-1}(p-1)}\equiv1(\mathrm{mod}\ p^\alpha)$. 这不难对 α 归纳来论证，$\alpha=1$ 的情形就是费马小定理(参考第 5 题的证明).

15 我们证明，对任意整数 a，有 $a^p \equiv a(\bmod p)$（参见注 3）. 由于当 $a \equiv b(\bmod p)$ 时，有 $a^p \equiv b^p(\bmod p)$. 因此只需对 $a = 0, 1, \cdots, p-1$ 来证明结论即可.

对任意整数 i，由二项式定理及例 4，有

$$(i+1)^p - i^p = \sum_{k=0}^{p-1} \binom{p}{k} i^k \equiv \binom{p}{0} = 1(\bmod p),$$

对 $i = 0, 1, \cdots, a-1$ 求和即得结果.

16 若 $p = 2$，则正偶数 n 均符合要求. 若 $p > 2$，取 $n = (p-1)^{2k}$，k 为任意正整数，则由费马小定理得

$$\begin{aligned} 2^n - n = 2^{(p-1)^{2k}} - (p-1)^{2k} &\equiv (2^{p-1})^{(p-1)^{2k-1}} - 1 \\ &\equiv 1 - 1 = 0(\bmod p). \end{aligned}$$

17 对任意给定的正整数 m，取足够大的 n_0，使得 $2^{n_0} + 3^{n_0} - m > 1$，故 $2^{n_0} + 3^{n_0} - 1, 2^{n_0} + 3^{n_0} - 2, \cdots, 2^{n_0} + 3^{n_0} - m$ 均大于 1，从而它们分别有素因子 $p_1, p_2, \cdots, p_m$. 取

$$n_k = n_0 + k(p_1 - 1)(p_2 - 1)\cdots(p_m - 1),$$

其中 k 是任意正整数.

若 $p_i \neq 2$，则由费马小定理知 $2^{p_i-1} \equiv 1(\bmod p_i)$，故

$$2^{n_k} = 2^{n_0} \cdot 2^{k(p_1-1)(p_2-1)\cdots(p_m-1)} \equiv 2^{n_0} \cdot 1 \equiv 2^{n_0}(\bmod p_i);$$

若 $p_i = 2$，上式显然也成立.

同样可知 $3^{n_k} \equiv 3^{n_0}(\bmod p_i)$，故有

$$2^{n_k} + 3^{n_k} - i \equiv 2^{n_0} + 3^{n_0} - i \equiv 0(\bmod p_i). \ (i = 1, 2, \cdots, m.)$$

由于 $2^{n_k} + 3^{n_k} - i > 2^{n_0} + 3^{n_0} - i \geqslant p_i$，故由上式可知，$2^{n_k} + 3^{n_k} - i$ 对 $i = 1, 2, \cdots, m$ 均是合数. 由于 k 是任意正整数，故 n_k 有无穷多个.

第9讲

不定方程(一)

1 显然 x 是奇数. 若 y 是奇数,方程分解为

$$(x+1)(x^{y-1}-x^{y-2}+\cdots-x+1)=2^z.$$

上式左端第二个因式是奇数个奇数之和,它只能是1(因右边是2的幂),这导出 $x+1=2^z$,即 $y=1$,矛盾. 当 y 为偶数时,x^y 为奇数平方. 将方程模4知必须 $z=1$,这又导出 $x=1$,矛盾. 因此方程无解.

2 x 是奇数. 若 y 是奇数则方程无解(用第1题的做法);若 y 是偶数,参考正文中方程⑨的解法,得出所有解是 $x=3$, $y=2$, $z=3$.

3 设 $(x-1)x(x+1)=y^k$, x、y 为正整数且 $x\geqslant 2$. 将方程变形为 $(x^2-1)x=y^k$,由于 $(x, x^2-1)=1$,故 x 和 x^2-1 都是正整数的 k 次幂,即 $x^2=(u^2)^k$, $x^2-1=v^k$, u、v 为正整数,易证这不可能(参考例1).

4 设 $n=x^2-y^2$,即 $n=(x-y)(x+y)$. 由于 $x-y$ 与 $x+y$ 同奇偶性,故 n 是奇数或 $4\mid n$(这也可由原方程模4导出来).

反过来,若 n 是奇数,可取 $x-y=1$, $x+y=n$;若 $4\mid n$,可取 $x-y=2$, $x+y=\dfrac{n}{2}$.

5 模9(参考第8讲练习题中的第3题).

6 模16(参考第8讲练习题中的第4题).

7 方程可变形为 $(2x+1)^2=4(y^4+y^3+y^2+y)+1$. 由于

$$4(y^4+y^3+y^2+y)+1=(2y^2+y+1)^2-y^2+2y$$

$$=(2y^2+y)^2+3y^2+4y+1,$$

故当 $y>2$ 或 $y<-1$ 时，有 $(2y^2+y)<(2x+1)^2<(2y^2+y+1)^2$. 从而 $y>2$ 或 $y<-1$ 时方程无解(参考例 4(ii)). 当 $-1\leqslant y\leqslant 2$ 时，易检验方程共有 6 组整数解.

8 可设 $a>b>c>0$. 若 $a+b=2^u$，$b+c=2^v$，$c+a=2^w$，则 $u>w>v$，从而 $u\geqslant w+1$，$u>v+1$，所以 $(c+a)+(b+c)<2^{u-1}+2^{u-1}=2^u=a+b$，矛盾.

9 设三角形边长为整数 a、b、c，由海伦公式易知，问题等价于求方程

$$4(a+b+c)=(a+b-c)(a+c-b)(b+c-a)$$

的所有正整数解. 上式右边三个因数的奇偶性相同，左边被 2 整除，所以右边的因数都是偶数. 令：

$$x=\frac{1}{2}(b+c-a),\ y=\frac{1}{2}(a+c-b),\ z=\frac{1}{2}(a+b-c).$$

不妨设 $a\leqslant b\leqslant c$，则 $x\geqslant y\geqslant z$，且 $x+y+z=xyz$. 由此得 $yz\leqslant 3$，这样可求出 $x=3$，$y=2$，$z=1$，即 $a=3$，$b=4$，$c=5$.

10 将方程模 3 及模 4 知，x、z 都是偶数，设 $x=2m$，$z=2n$，则 $(3^m,\ 2^y,\ 5^n)$ 是一组本原勾股数. 因此有正整数 a、b，且 $(a,\ b)=1$，a、b 一奇一偶，使得

$$2^y=2ab,\ 3^m=a^2-b^2.$$

由 $(a,\ b)=1$ 及 $a>b$，可知 $a=2^{y-1}$，$b=1$. 于是

$$3^m+1=2^{2y-2}.$$

如 $y\geqslant 3$，则上式右边 $\equiv 0(\mathrm{mod}\,8)$，但左边 $\equiv 2,\ 4(\mathrm{mod}\,8)$. 故必须 $y=2$，进而易知 $x=z=2$.

11 设 $(x,\ y,\ z)$ 是方程

$$x^2+y^2=z^2 \qquad ①$$

的一组本原解. 因为 x、z 为奇数，所以 $\frac{z-x}{2}$、$\frac{z+x}{2}$ 都是整数，并且 $\left(\frac{z-x}{2},\ \frac{z+x}{2}\right)=\left(\frac{z-x}{2}+\frac{z+x}{2},\ 2\cdot\frac{z+x}{2}\right)=(z,\ z+x)=(z,\ x)=1$.

又由 ① 得

$$\frac{z-x}{2}\cdot\frac{z+x}{2}=\left(\frac{y}{2}\right)^2.$$

所以 $\frac{z-x}{2}$、$\frac{z+x}{2}$ 都是完全平方数，即有整数 $a>b>0$，$(a,\ b)=1$，使得 $\frac{z+x}{2}=a^2$，$\frac{z-x}{2}=b^2$，$y=2ab$，即

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2. \qquad ②$$

因 x 是奇数，故 a、b 一奇一偶.

反过来，当 a、b 满足上述条件时，我们证明 ② 给出的 $(x,\ y,\ z)$ 是 ① 的本原解，且 $2\mid y$.

首先，易验证 ② 给出的 $(x,\ y,\ z)$ 满足 ①，又显然有 $2\mid y$. 我们只需证明 $(x,\ y)=1$. 设 $(x,\ y)=d$，则 $d\mid x$，$d\mid z$，即 $d\mid(a^2-b^2)$，$d\mid(a^2+b^2)$，故 $d\mid 2a^2$，$d\mid 2b^2$，推出 $d\mid(2a^2,\ 2b^2)$，即 $d\mid 2(a^2,\ b^2)$. 因 $(a,\ b)=1$，故 $(a^2,\ b^2)=1$. 所以 $d\mid 2$. 但 a，b 一奇一偶，这意味着 x 是奇数，从而 $d=1$.

12 当 $m\leqslant 4$ 时，解为 $(m,\ n)=(1,\ 1)$，$(3,\ 3)$；当 $m\geqslant 5$ 时，模 5：$1!+2!+3!+4!\equiv 3\pmod 5$，而当 $k\geqslant 5$ 时，$k!\equiv 0\pmod 5$. 于是 $m\geqslant 5$ 时，有 $1!+2!+\cdots+m!\equiv 3\pmod 5$，但 $n^2\equiv 0,\ \pm 1\pmod 5$. 故当 $m\geqslant 5$ 时方程无解.

13 设 $1\leqslant x_1<\cdots<x_n$ 满足 $x_1\cdots x_n=x_1+\cdots+x_n$. 我们有

$$x_n\cdot(n-1)!\leqslant x_1\cdots x_n=x_1+\cdots+x_n<nx_n,$$

即$(n-1)!<n$，故$n=2$或3. 由此易知解只有$x_1=1$，$x_2=2$，$x_3=3$.

14 易知x、y、z中至少有一个偶数. 再模4，推出x、y、z都是偶数，设$x=2x_1$，$y=2y_1$，$z=2z_1$，代入原方程，重复上述论证，可知x_1、y_1、z_1都是偶数. 如此进行，推出x、y、z均被2的任意正整数次幂整除，只有$x=y=z=0$.

15 设$m=2^kr$，r为奇数，则同余方程有解$x=\dfrac{r+1}{2}$，$y=\dfrac{2^{2k+1}+1}{3}$.

16 设$2^p-1=q^s$，则由第1题的结论知，必须$s=1$.

第10讲

数论问题

1 论证的关键是建立下面的递推关系：

$$a_n = a_{n-1}a_{n-2}\cdots a_1 + k. \quad (n \geqslant 2) \qquad ①$$

这不难用归纳法证明 $n = 2$ 时易知结论成立，设这在 n 时已成立，则由已知的递推公式，得

$$a_{n+1} = a_n(a_n - k) + k = a_n a_{n-1}\cdots a_1 + k,$$

即所说的结果在 $n+1$ 时也成立.

对任意 m、$n(1 \leqslant m < n)$，由①可见，$a_m \mid a_n - k$. 又由归纳法易知 a_m 与 k 互素，故 a_m 和 $(a_n - k) + k = a_n$ 也互素.

2 注意，若 $d \mid n$，则 $\dfrac{n}{d} \Big| n$，因此我们有

$$\begin{aligned} S &= \sum_{i=1}^{k-1} d_i d_{i+1} = n^2 \sum_{i=1}^{k-1} \frac{1}{d_i d_{i+1}} \\ &\leqslant n^2 \sum_{i=1}^{k-1} \left(\frac{1}{d_i} - \frac{1}{d_{i+1}}\right) < \frac{n^2}{d_1} = n^2. \end{aligned}$$

3 设所说等差数列的公差为 d，则这个数列为：a_1，$a_1 + d$，…，$a_1 + (p-1)d$. 因为 $(p, d) = 1$，故这 p 个数构成模 p 的一个完系，故恰有一个 a_i 被 p 整除，而其余 $p-1$ 项在模 p 的意义下是 1，2，…，$p-1$ 的一个排列，故由威尔逊定理（见第 8 讲中(15)）得

$$\frac{a_1 a_2 \cdots a_p}{a_i} \equiv (p-1)! \equiv -1 \pmod{p}.$$

由上式及 $p|a_i$ 即知 $a_1a_2\cdots a_p+a_i\equiv 0\pmod{p^2}$.

4 已知的等式可变形为

$$(a-b)(c-b)=b^2. \qquad ②$$

若有素数 p，使得 $p\mid(a-b,\ c-b)$，则由上式知 $p|b^2$，故 $p|b$，再由 $p\mid c-b$ 推出 $p|c$；由 $p\mid a-b$ 知 $p|a$，从而 $p|(a,\ b,\ c)$，这与已知条件相违. 故 $(a-b,\ c-b)=1$，于是由②即知 $a-b,\ c-b$ 都是完全平方数(注意，由已知的等式及 a、b、c 为正数可推知 $a-b>0$，再由②知 $c-b>0$).

5 不存在所说的两个 2 的方幂. 假设相反，设 $m,\ n$ 是两个符合问题中要求的 2 的方幂，不妨设 $m>n$，则显然 $m<10n$，由于 $m,\ n$ 都是 2 的幂，故 $m=2n$ 或 $4n$，或 $8n$.

记 $S(k)$为 k 的(十进制表示下的)数码之和，则由第 8 讲练习题中第 8 题知，$S(m)\equiv m\pmod 9$，$S(n)\equiv n\pmod 9$. 又 $S(m)=S(n)$，故 $m\equiv n\pmod 9$，即 n，或 $3n$，或 $7n$ 被 9 整除，这不可能(因 n 是 2 的幂).

6 将方程模 4，因为右边$\equiv$2(mod 4)，故 $x=1$；否则左边被 4 整除，产生矛盾.

若 $y>1$，则方程左边$\equiv$0(mod 9)，而 5^z 模 9 周期地为 5，7，8，4，2，1，故 $z=6k+3$. 因此 5^3+1 整除 $5^z+1=(5^3)^{2k+1}+1$，从而 5^3+1 整除 $2\cdot 3^y$，特别地，$7|2\cdot 3^y$，这不可能，故 $y=1$，所以 $z=1$. 因此所求的解为 $x=y=z=1$.

7 可设 $a\geqslant 0$，若 $b=0$，则易知 $a=0$. 以下设 $b\neq 0$，因 $2^{2k}a+b$ 对 $k\geqslant 1$ 均为平方数，故 $4(2^{2k-2}a+b)=2^{2k}a+4b$ 为平方数，设

$$2^{2k}a+b=x_k^2,\ 2^{2k}a+4b=y_k^2,\ (x_k,\ y_k \text{ 为正整数})$$

由此(消去 2^{2k})得到

$$x_k+y_k\leqslant(x_k+y_k)\mid x_k-y_k\mid=\mid x_k^2-y_k^2\mid=\mid 3b\mid.$$

故 $2^{2k}a+b=x_k^2\leqslant(x_k+y_k)^2\leqslant 9b^2$ 对任意 k 成立，从而必须 $a=0$.（因这个不等式的右端为一个有界量，而若 $a>0$，则左端随 k 可任意大.）

8 由归纳法易知 $a_n\equiv 2(\mathrm{mod}\ 3)(n=1,2,\cdots)$，因此 $a_r\cdot a_s\equiv 2\cdot 2\equiv 1(\mathrm{mod}\ 3)$，从而 $a_r\cdot a_s$ 不是数列$\{a_n\}(n\geqslant 1)$中的项.

9 每个 a_i 至少有两个素因子 p_i 及 q_i（p_i 与 q_i 可能相同），可将 a_i 表示为 $a_i=p_iq_ib_i$.

由于对 $i\neq j$，有 $(a_i,a_j)=1$，故 p_i，q_i 与 p_j，q_j 无相同者，设 N 是所有 p_i 及 q_i 中的最大的数，则我们有

$$\sum_{i=1}^{n}\frac{1}{a_i}\leqslant\sum_{i=1}^{n}\frac{1}{p_iq_i}\leqslant\sum_{i=1}^{n}\frac{1}{\min(p_i,q_i)^2}\leqslant\sum_{i=1}^{n}\frac{1}{k^2}<1.$$

第11讲

多项式的运算与整除

1 商式是 x^4-x^2-x+1，余式是 $2x^2-2$.

2 参考例 1.

$$x^4+x^3+x^2+x+1=\left(x^2+\frac{1}{2}x+1\right)^2-\left(\frac{1}{2}\sqrt{5}\right)^2,$$

是唯一的解.

3 反复用性质(20)即得结果.

4 注意 S 中多项式的常数项均是偶数. 如果 S 中存在所说的 $d(x)$，则 $d(x)\mid x$ 且 $d(x)\mid 2$，易知这不能成立.

5 (i) 如果结论不对，可设 $f(x)$、$g(x)$模 p 的次数分别为 n、m，则 $f(x)g(x)$ 中 x^{n+m} 的系数不被 p 整除，从而 $f(x)g(x)\not\equiv 0(\mathrm{mod}\ p)$.

(ii) 设 $m=ab$，a、b 均是大于 1 的整数，则 $f(x)=ax$ 与 $g(x)=bx$ 均$\not\equiv 0(\mathrm{mod}\ m)$. 但显然 $f(x)g(x)=abx^2=mx^2\equiv 0(\mathrm{mod}\ m)$.

6 设 $f(x)=(1+x^2-x^3)^{100}$，$g(x)=(1-x^2+x^3)^{100}$. 由于 $(-x)^{20}=x^{20}$，故 $f(x)$与 $g(x)$中 x^{20} 的系数，分别与 $f(-x)$及 $g(-x)$中 x^{20} 的系数相同. 因为 $f(-x)=(1+x^2+x^3)^{100}$ 是非负系数的多项式，其展开式中诸 x^{20} 的系数均为 1，设共有 n 个 x^{20} 项，则 $f(-x)$ 中 x^{20} 的系数为 n；而在 $g(-x)=(1-x^2-x^3)^{100}$ 的展开式中，x^{20} 项的个数也为 n，每个 x^{20} 的系数为 ± 1，又易知其中必有 -1，因此 $g(-x)$中 x^{20} 的系数小于 n. 从而在 $f(x)$中 x^{20} 的系数

大于 $g(x)$ 中 x^{20} 的系数.

7 由问题中的条件可知，多项式 $x^{2k+1}+x+1-(x^k+x+1)=x^k(x^{k+1}-1)$ 被 x^k+x+1 整除，注意，

当 k 为奇数时，有

$$x^k=(x^k+1)-1=(x+1)(x^{k-1}-x^{k-2}+\cdots-x+1)-1;$$

当 k 为偶数时，有

$$\begin{aligned}x^k&=(x^k-1)+1=((x^2)^{\frac{k}{2}}-1)+1\\&=(x+1)(x-1)(x^{2k-2}+\cdots+x^2+1)+1.\end{aligned}$$

因此有

$$(x^k,\ x^k+x+1)=(x^k,\ x+1)=((-1)^k,\ x+1)=1,$$

结合上面的 $(x^k+x+1)\mid x^k(x^{k+1}-1)$，可知 $x^{k+1}-1$ 被 x^k+x+1 整除，又因为

$$x^{k+1}-1=x(x^k+x+1)-(x^2+x+1).$$

故 x^2+x+1 也被 x^k+x+1 整除. 因此 $k=1$ 或 2. 但 $k=1$ 显然不符合要求，故 $k=2$.

第12讲

多项式的零点

1 用例1的方法. 答：x^3-1.

2 用例7的方法. 答：$n=6k\pm1$ (k 为正整数).

3 条件意味着 $f(x)=(x-a)(x-b)(x-c)-1$. 若有整数 d 使得 $f(d)=0$,则$(d-a)(d-b)(d-c)=1$. 易知这是不可能.

4 设 $f(x)$有整数根 a,则 $f(x)=(x-a)g(x)$,这里 $g(x)$ 是整系数多项式. 由于 $f(k)$、$f(l)$ 均是奇数，我们得出$(k-a)g(k)$、$(l-a)g(l)$ 都是奇数,但k与l的奇偶性不同,故$k-a$和$l-a$中必有一个是偶数. 矛盾!

5 因为多项式 $f(x)$的系数都是非负的,故其根都不是正数. 我们设 $f(x)=(x+\alpha_1)\cdots(x+\alpha_n)$, $\alpha_i\geqslant0$. 因为 $2+\alpha_i=1+1+\alpha_i\geqslant3\sqrt[3]{\alpha_i}$, $(i=1,\cdots,n)$. 由韦达定理,$\alpha_1\cdots\alpha_n=1$. 于是 $f(2)=(2+\alpha_1)\cdots(2+\alpha_n)\geqslant3^n\sqrt[3]{\alpha_1\cdots\alpha_n}=3^n$(算术—几何平均不等式).

6 取 $x_0=0$, $x_{n+1}=x_n^2+1$,则用归纳法易证 $f(x_n)=x_n(n=0,1,\cdots)$. 但 x_n 是严格递增的,从而互不相同,所以方程 $f(x)=x$ 有无穷多个不同的根,故由(5) 知 $f(x)$ 等于 x.

7 将 α 代入方程,并取共轭即知 $f(\bar{\alpha})=0$.

8 $f(x)$的首项系数必须是正数,其标准分解中相同的一次因式必须出现偶数次. 又由于 $f(x)$的二次因式均为 $(x-b)^2+c^2$ 形式,这是两个实多项式的平方和. 最后,恒等式

$$(x_1^2+x_2^2)(y_1^2+y_2^2)=(x_1y_1+x_2y_2)^2+(x_1y_2-x_2y_1)^2$$

表明,上述两个因式的积仍是两个实多项式的平方和(参考注7).

9 设 $k=(p-1)q+r$，由于 $(p-1)\nmid k$，故 $0<r<p-1$. 因 $a^k-1\equiv a^r-1(\mathrm{mod}\ p)$，故我们可设 $0<k<p-1$ 来证明. 由于同余方程 $x^k\equiv 1(\mathrm{mod}\ p)$ 至多有 k 个不同的解(见(6))，而模 p 的缩同余类有 $p-1$ 个，因此存在问题中说的 a.

10 若 $|\alpha|<1$，则无需证明. 设 $|\alpha|>1$，记 $M=\max\limits_{0\leqslant k\leqslant n-1}\left|\dfrac{a_k}{a_n}\right|$. 由 $a_0+\cdots+a_{n-1}\alpha^{n-1}=-a_n\alpha^n$ 得出

$$\begin{aligned}|\alpha|^n&=\left|\frac{a_0}{a_n}+\cdots+\frac{a_{n-1}}{a_n}\alpha^{n-1}\right|\\&\leqslant M(1+|\alpha|+\cdots+|\alpha|^{n-1})\\&<M\frac{|\alpha|^n}{|\alpha|-1}.\end{aligned}$$

故 $|\alpha|<M+1$.

11 若 $\mathrm{Re}(\alpha)\leqslant 0$ 或 $|\alpha|\leqslant 1$，则已无需证明. 对于 $\mathrm{Re}(\alpha)>0$ 且 $|\alpha|>1$，我们有 $\mathrm{Re}\left(\dfrac{1}{\alpha}\right)>0$，故从

$$\begin{aligned}0=\left|\frac{f(\alpha)}{\alpha^n}\right|&\geqslant\left|a_0+\frac{a_1}{\alpha}\right|-\frac{a_2}{|\alpha|^2}-\cdots-\frac{a_n}{|\alpha|^n}\\&\geqslant\mathrm{Re}\left(a_0+\frac{a_1}{\alpha}\right)-\frac{9}{|\alpha|^2}-\cdots-\frac{9}{|\alpha|^n}\\&>1-\frac{9}{|\alpha|^2-|\alpha|},\end{aligned}$$

可导出结论.

12 对任意 $|x|\leqslant 1$，$x\neq 1$，我们有

$$\begin{aligned}&|(1-x)(a_0+a_1x+\cdots+a_nx^n)|\\&=|a_0-(a_0-a_1)x-(a_1-a_2)x^2-\cdots-(a_{n-1}-a_n)x^n-a_nx^{n+1}|\\&\geqslant a_0-|(a_0-a_1)x+(a_1-a_2)x^2+\cdots+a_nx^{n+1}|\\&>a_0-(a_0-a_1)-(a_1-a_2)-\cdots-(a_{n-1}-a_n)-a_n=0,\end{aligned}$$

这是因为$(a_0-a_1)x$，$(a_1-a_2)x^2$，…，a_nx^{n+1}的辐角不能都相等(除非$x\geqslant 0$，但此情形下，结论显然成立). 因此$f(x)$的根的模都大于1.

13 由于所有$c_i>0$，故对$x\geqslant 0$，有$f(x)>0$，故$f(x)$没有非负实根. 若对某个k有$b_k\leqslant 0$，则$x^2+a_kx+b_k$有非负根，从而$f(x)$也如此，此为不可能，因此对任意k，均有$b_k>0$.

另一方面，由多项式的乘法可知$c_1=a_1+\cdots+a_n$. 由于$c_1>0$，故必有某个k，使$a_k>0$. 这表明存在一个符合要求的二次多项式$x^2+a_kx+b_k$.

14 不存在满足条件的集合S.

假设有这样的一个集合$S=\{a_1,\cdots,a_k\}$，设

$$m=\min\{|a_1|,\cdots,|a_k|\},\ M=\max\{|a_1|,\cdots,|a_k|\}.$$

由于S中不含数0，故$M\geqslant m>0$.

设对任意正整数n，有一个次数$N\geqslant n$的多项式$f(x)=b_Nx^N+b_{N-1}x^{N-1}+\cdots+b_1x+b_0$，其系数$b_0$，…，$b_N$及$N$个根$x_1$，…，$x_N$均属于集合$S$. 由韦达定理得

$$x_1+\cdots+x_N=-\frac{b_{N-1}}{b_N},$$

$$x_1x_2+x_1x_3+\cdots+x_1x_N+\cdots+x_{N-1}x_N=\frac{b_{N-2}}{b_N},$$

故得

$$x_1^2+\cdots+x_N^2=\left(-\frac{b_{N-1}}{b_N}\right)^2-2\frac{b_{N-2}}{b_N}.$$

因此

$$Nm^2\leqslant x_1^2+\cdots+x_N^2=\frac{b_{N-1}^2}{b_N^2}-2\frac{b_{N-2}}{b_N}\leqslant\frac{M^2}{m^2}+2\frac{M}{m},$$

故$N\leqslant\frac{M^2}{m^4}+2\frac{M}{m^3}$，即$N$有界. 这与$N\geqslant n$，以及$n$可以任意大矛盾.

第13讲

整系数多项式

1 直接用艾森斯坦判别法.

2 记 $f(x)=x^7+7x+1$，则 $g(x)=f(x-1)$ 可应用艾森斯坦判别法(参考(5)).

3 首先，所说的多项式没有一次因式(只需检查 $x=\pm 1$，± 5 是否为根，参考第12讲，(8)). 因此，如果该多项式在 $\mathbf{Q}$ 上可约(从而也在 $\mathbf{Z}$ 上可约)，必定是二次因式与三次因式的积. 用待定系数法，可导出矛盾.

4 若 n 不是素数，设 $n=ab$ $(a,b>1)$，则所说的多项式可表示为 $\dfrac{x^{ab}-1}{x-1}=\dfrac{(x^a)^b-1}{x-1}$，这易于分解为两个(非常数)整系数多项式的积. 注意，(5)表明本题结论的逆命题正确.

5 记所说的多项式为 $f(x)$，则 $f(-x)=\Phi_p(x)$(参考(5)).

6 记所说的多项式为 $f(x)$. 首先，$f(x)$ 没有一次因式. 因为若 $f(x)$ 有整数根 a，则由 $a^5-a\equiv 0(\mathrm{mod}\,5)$ 知 $5\mid k$. 假设 $f(x)$ 有二次因式 x^2-ax-b，易求出 $f(x)$ 被 x^2-ax-b 除得的余式是 $(a^4+3a^2b+b^2-1)x+(a^3b+2ab^2+k)$；这必须是零多项式，故 $a^4+3a^2b+b^2-1=0$ 及 $a^3b+2ab^2+k=0$. 从而 $a(a^4+3a^2b+b^2-1)-3(a^3b+2ab^2+k)=0$，即 $a^5-a-5ab^2=3k$. 因左边是5的倍数，故 $5\mid k$，矛盾!

7 首先证明，$f(x)$ 的复根的模均大于1. 事实上，设 x_0 是 $f(x)$ 的一个根，若 $|x_0|\leqslant 1$，则

$$\begin{aligned} p &= |\, a_n x_0^n + \cdots + a_0 x \,| \\ &\leqslant |\, a_n \,| \cdot |\, x_0 \,|^n + \cdots + |\, a_1 \,| \cdot |\, x_0 \,| \\ &\leqslant |\, a_n \,| + \cdots + |\, a_1 \,|, \end{aligned}$$

与已知条件矛盾(这里无需 p 是素数). 现在设 $f(x) = g(x)h(x)$, 其中 $g(x)$, $h(x)$均是非常数的整系数多项式,则

$$p = |\, f(0) \,| = |\, g(0) \,| \cdot |\, h(0) \,|. \qquad ①$$

设 b 是 $g(x)$的首项系数,则由韦达定理知,$\dfrac{g(0)}{b}$等于 $g(x)$的所有根的积. 但 $g(x)$的根都是 $f(x)$的根,从而它们的模都大于 1. 因此 $\left|\dfrac{g(0)}{b}\right| > 1$,更有 $|\, g(0) \,| > 1$. 同理 $|\, h(0) \,| > 1$. 但 p 是素数,而 $|g(0)|$, $|h(0)|$都是大于 1 的整数,故①不能成立.

8 设 $f(x)$可分解为两个正次数(整系数)多项式 $g(x)$与 $h(x)$的积. 则由 $|f(m)|$为素数,可知 $|g(m)|$与 $|h(m)|$中有一个为 1,设 $|\, g(m) \,| = 1$.

另一方面,由第 12 讲练习题中第 10 题可知,$f(x)$的根的模均小于 $M+1$. 故若

$$g(x) = a(x-\alpha_1)\cdots(x-\alpha_r)$$

(a 为 $g(x)$的首项系数),则有

$$\begin{aligned} |\, g(m) \,| &\geqslant (m - |\, \alpha_1 \,|)\cdots(m - |\, \alpha_r \,|) \\ &> |\, m - (M+1) \,|^r \geqslant 1, \end{aligned}$$

产生矛盾.

第14讲

多项式的插值与差分

1 $ix^2-(1+i)x+1$.

2 将多项式表示为(参考(8))

$$a\binom{x}{4}+b\binom{x}{3}+c\binom{x}{2}+d\binom{x}{1}+e.$$

用代值法(依次取 $x=0,1,2,3,4$),可求出待定的系数 $a=b=1,c=-1,d=0,e=1$,因此所说的多项式是整值多项式.

3 所求的和是 $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{n-k}k^n$,由欧拉恒等式(见(4))即知这是 $n!$.

4 参考公式⑤的证明.

5 对任意整数 a,$f(x)$ 是整值多项式,等价于 $g(x)=f(x+a)$ 是整值多项式.因此可设连续 $n+1$ 个整数是 $0,1,\cdots,n$.先将 $f(x)$ 表示为⑧的形式,再由 $f(k)$ $(k=0,1,\cdots,n)$ 是整数,可推出诸系数都是整数.

本题的价值主要是在理论上的,它用多项式的(有限个连续整数处的)值,给出了整值多项式的刻画.对于具体的多项式,为判断其是否为整值多项式,我们宁愿用第2题中的待定系数法,将它表示为⑧的形式.

6 答:$n=2$.用例1的两种方法都可以求解.

7 用例2的方法.考虑 $g(x)=(x+1)f(x)-x$,它在 $x=0,1,\cdots,n$ 处的值是0,又因为 $g(-1)=1$.故 $g(x)=\dfrac{(-1)^{n+1}}{(n+1)!}x(x-$

$1)\cdots(x-n)$. 可求出 $f(n+1)=\begin{cases}1, & n\text{ 为奇数};\\ \dfrac{n}{n+2}, & n\text{ 为偶数}.\end{cases}$

8 由拉格朗日插值公式及 $2n+1$ 个值 $f(k)$ $(-n\leqslant k\leqslant n)$，可唯一地确定 $f(x)$：

$$f(x)=\sum_{k=-n}^{n}f(k)\prod_{\substack{i\neq k\\ -n\leqslant i\leqslant n}}\frac{x-i}{k-i}.$$

由条件得出

$$|f(x)|\leqslant\sum_{k=-n}^{n}\prod_{i\neq k}\left|\frac{x-i}{k-i}\right|.$$

对于任意实数 x，$-n\leqslant x\leqslant n$，我们有 $\prod\limits_{\substack{i\neq k\\ -n\leqslant i\leqslant n}}|x-i|\leqslant(2n)!$. 实际上，当 $x\geqslant k$ 时，

$$\begin{aligned}&\prod_{i\neq k}|x-i|\\ &=(|x-(k+1)|\cdots|x-n|)(|x-(k-1)|\cdots|x+n|)\\ &\leqslant(n-k)!\cdot(n-k+1)\cdots(2n)=(2n)!.\end{aligned}$$

同理可证 $x<k$ 的情形. 于是

$$\prod_{i\neq k}\left|\frac{x-i}{k-i}\right|\leqslant(2n)!\prod_{i\neq k}\frac{1}{|k-i|}\leqslant(2n)!\frac{1}{(n+k)!(n-k)!}.$$

由此易得 $|f(x)|\leqslant\sum\limits_{k=0}^{2n}\binom{2n}{k}=2^{2n}$.

第15讲

单位根及其应用

1 用5次单位根.

2 设 $f(x^5)=f(x)q(x)+r(x)$，这里 $r(x)=0$ 或 $\deg r\leqslant 3$. 设 $\zeta\neq 1$ 是一个5次单位根，则 $r(\zeta)=r(\zeta^2)=r(\zeta^3)=r(\zeta^4)=5$，而 $\deg r\leqslant 3$，故必须 $r(x)=5$，即余式是常数5.

3 我们有 $f(x^n)=(x-1)g(x)$. 取 $\zeta=\mathrm{e}^{\frac{2\pi\mathrm{i}}{n}}$ 是一个 n 次单位根，由 $f(1)=0$ 知，$f(\zeta^{kn})=0$ $(k=1,\cdots,n)$. 故 $f(x^n)$ 被 $(x-\zeta)(x-\zeta^2)\cdots(x-\zeta^n)=x^n-1$ 整除.

4 参考例2的解法. 在 $(x+1)^n$ 的二项式展开中，依次用 $x=1,-1,i,-i$（四次单位根）代入即得结果.

5 在(4)中取 $x=1$ 即得(i). (ii)可参考例4的证法.

6 (i)在 $(1+x+x^2)^n$ 的展开式中以 $x=1,-1$（二次单位根）代入即得结果. (ii)的解法与例2类似.

7 记 $\zeta=\mathrm{e}^{\frac{2\pi\mathrm{i}}{m+1}}$ 是一个 $m+1$ 次单位根，则 $1+x+\cdots+x^m$ 的所有根是 ζ^k $(k=1,2,\cdots,m)$（参考(4)）. 因此，$f(x)=1+x^n+\cdots+x^{mn}$ 被 $1+x+\cdots+x^m$ 整除的充分必要条件是 $f(\zeta^k)=0$ $(1\leqslant k\leqslant m)$. 因为

$$f(x)=\frac{x^{n(m+1)}-1}{x^n-1}.$$

所以上述条件等价于 ζ^k 是 $x^{n(m+1)}-1$ 的零点，但不是 x^n-1 的零点（注意，这两个多项式均没有重根）. 前者显然成立，而后者即是

$$\cos\frac{2kn\pi}{m+1}+\mathrm{i}\sin\frac{2kn\pi}{m+1}\neq 1,\ k=1,2,\cdots,m.$$

易知必须(也只需)$m+1$ 与 n 互素.

8 用第 14 讲中例 1 的解法二知

$$\sum_{k=0}^{3n+1}(-1)^k\binom{3n+1}{k}P(3n+1-k)=0,$$

此即

$$729+2\sum_{j=0}^{n}(-1)^{3j+1}\binom{3n+1}{3j+1}+\sum_{j=0}^{n}(-1)^{3j}\binom{3n+1}{3j}=0.$$

用例 2 的方法可求得

$$\sum_{j=0}^{n}(-1)^j\binom{3n+1}{3j+1}=2(\sqrt{3})^{3n-1}\cos\frac{3n-1}{6}\pi,$$

$$\sum_{j=0}^{n}(-1)^j\binom{3n+1}{3j}=2(\sqrt{3})^{3n-1}\cos\frac{3n+1}{6}\pi.$$

故 $729-4(\sqrt{3})^{3n-1}\cos\frac{3n-1}{6}\pi+2(\sqrt{3})^{3n-1}\cos\frac{3n+1}{6}\pi=0.$

区分 n 的奇偶性易得只有 $n=4$.

第16讲

生成函数方法

1 比较 $(1+x)^n=(1+x)(1+x)^{n-1}$ 两边的系数.

2 与例 3 的方法相同. 求证等式的左边是

$$\sum_{k=0}^{n}\binom{n}{k}2^{n-k}(1-x)(x^{-1}+x)^k$$

的常数项.

3 第一个问题用例 5 的方法(参考注 1). 对第二个问题,所求的取法是

$$(x+x^2+x^3)(1+x+x^2+x^3)(x^2+x^3+x^4+x^5+x^6)$$

中 x^8 的系数.

4 参考本讲注 4.

5 本题应将(1)中的原则反过来用. x^k 的系数是方程

$$k=a_1+a_2 \qquad ①$$

的解的个数,这里,$0\leqslant a_1,\ a_2\leqslant n-1$. 对于 $0\leqslant k\leqslant n-1$,则 ① 恰有 $k+1$ 个解.

$$0+k,\ 1+(k-1),\ \cdots,\ (k-1)+1,\ k+0.$$

然而,如果 $n\leqslant k\leqslant 2n-2$,上述解中的 $0+k$, $1+(k-1)$, …, $(k-n)+n$ 及 $k+0$, $(k-1)+1$, …, $n+(k-n)$ 不满足 $a_1,\ a_2\leqslant n-1$. 故此时方程 ① 共有 $k+1-2(k-n+1)=2n-k-1$ 个符合要求的解. 在这两种情况下,x^k 的系数可统一地写作

$$n-|\,n-k-1\,|.$$

6 问题等价于找正整数 $a_1,\cdots,a_6$ 及 $b_1,\cdots,b_6$，满足

$$(x^{a_1}+\cdots+x^{a_6})(x^{b_1}+\cdots+x^{b_6})=(x+\cdots+x^6)(x+\cdots+x^6),$$

而集合$\{a_1,\cdots,a_6\}$ 与$\{b_1,\cdots,b_6\}$ 均不同于$\{1,2,3,4,5,6\}$.

上式即是

$$\begin{aligned}&(x^{a_1}+\cdots+x^{a_6})(x^{b_1}+\cdots+x^{b_6})\\&=x\frac{x^6-1}{x-1}=x\cdot\frac{x^3-1}{x-1}(x^3+1)\\&=x^2(x^2+x+1)^2(x+1)^2(x^2-x+1)^2.\end{aligned}$$

因为 a_i 是正整数，故 $x^{a_1}+\cdots+x^{a_6}$ 必含因式 x；又必须含有因式 $x+1$ 与 x^2+x+1(因 $x^{a_1}+\cdots+x^{a_6}$ 在 $x=1$ 的值为 6). 同样的结论对$x^{b_1}+\cdots+x^{b_6}$ 也成立. 于是只有因式$(x^2-x+1)^2$ 可供选择. 注意x^2-x+1 在整数集上不可约，故只有取

$$x^{a_1}+\cdots+x^{a_6}=x(x+1)(x^2+x+1)=x+2x^2+2x^3+x^4,$$

$$\begin{aligned}x^{b_1}+\cdots+x^{b_6}&=x(x+1)(x^2+x+1)(x^2-x+1)^2\\&=x+x^3+x^4+x^5+x^6+x^8,\end{aligned}$$

即$\{a_1,\cdots,a_6\}=\{1,2,2,3,3,4\}$，$\{b_1,\cdots,b_6\}=\{1,3,4,5,6,8\}$ 是唯一的一组解.

第17讲

集合与子集族

1 设有 m 个政党. 以 X 记所有诺言的集合，A_i 记第 i 个政党的诺言的集合 $(i=1, \cdots, m)$，则 $|X|=n$，$A_i \cap A_j \neq \varnothing$，且 $A_i \neq A_j (1 \leqslant i, j \leqslant m, i \neq j)$. 由例 1 的证法知 $m \leqslant 2^{n-1}$. 不难构造例子表明等号可以取得.

2 考虑任一个小于 n 的元素 a，如果 a 在不含 n 的子集 A 中，则它也在含 n 的子集 $A \cup \{n\}$ 中，反之亦然. 因此，如 a 在 A 的交错和的贡献为 $+a$（或 $-a$），则它在 $A \cup \{n\}$ 的交错和的贡献为 $-a$（或 $+a$），反之亦然. 于是 a 在交错和的总和中贡献是 0.

又元素 n 在每个含 n 的子集的交错和中贡献都是 n，故易知 n 对总和的贡献是 $n \cdot 2^{n-1}$. 综上所述，$S=n \cdot 2^{n-1}$.（参考例 2 的解法一.）

3 $B_1, \cdots, B_k$ 中任意一个元素个数大于 3 的子集，均产生 A 的一个三元子集族，由条件知，这些族中不会有共同的三元子集，因此，为使 k 最大，必须每个 B_i 满足 $|B_i| \leqslant 3 (i=1, \cdots, k)$. 又易知，所有的一元、二元、三元子集的族满足问题中的要求，故 k 的最大值是 $\binom{10}{1}+\binom{10}{2}+\binom{10}{3}=175$.

4 用例 4 中的方法得（参见②与③）

$$\frac{1}{10}\left(\sum_{i=1}^{k}|A_i|\right)^2 \leqslant \sum_{i=1}^{k}|A_i|+2\sum_{1\leqslant i<j\leqslant k}|A_i \cap A_j|.$$

故有 $\frac{1}{10}(5k)^2 \leqslant 5k+2\binom{k}{2}\times 2$，解得 $k \leqslant 6$. 请读者构造实例以表

明最大的 k 为 6.

5 设 n 是符合要求的最少的锁的个数. 设 A_i 是第 i 个委员可以打开的锁的集合 $(i=1, \cdots, 11)$, A 是所有锁的集合. 条件意味着, $A_1, \cdots, A_{11}$ 中任意5个的并不等于 A, 而任意6个的并等于 S, 故由例3第一段的论证(注意, 这里并不需要 $|A_1|=|A_2|=\cdots$), 得出

$$n=|A| \geqslant \binom{11}{5}.$$

下面指出, 如果加 $\binom{11}{5}$ 把锁, 则可以按问题中的要求向委员们分配钥匙:

我们将这 $\binom{11}{5}$ 把锁与集合 $\{1, 2, \cdots, 11\}$ 的5元子集之间建立一一对应. 如果某把锁对应于子集 $\{i_1, \cdots, i_5\}$, 那么就将它的钥匙交给所有标号不是 $i_1, \cdots, i_5$ 的委员掌管. 极易验证, 这种分配符合要求.

6 设元素 a_j 属于 m_j 个 $A_i(1 \leqslant i \leqslant n)$, 则用集合与元素的从属关系表, 易知 $m_1+\cdots+m_n=2n$.

另一方面, 如果有某个 $m_j>2$, 则至少有三个子集含有 a_j, 其中有两个为 A_s、A_t (s、t 均不等于 j), 但由已知条件, 因为 $A_s \cap A_t$ 非空(因为均含 a_j), 故其中必有一个为 $\{a_s, a_t\}$, 但这不含 a_j, 矛盾! 因而所有 $m_j \leqslant 2$, 故必须所有的 $m_j=2$.

7 如果十元子集 S' 具有性质: 对任何 $k \in S'$, 均有 $f(S' \backslash \{k\}) \neq k$, 则称 S' 是“好集”, 否则称为“坏集”.

如果 S' 为坏集, 则存在 $k_0 \in S'$, 使得

$$f(S' \backslash \{k_0\})=k_0.$$

令 $T=S' \backslash \{k_0\}$, 则 $|T|=9$, $f(T)=k_0$, 所以 $S'=T \cup \{f(T)\}$. 这说明每一个坏集都是由一个九元集(及 f) 产生的. 并且, 任一个九元集按上式至多产生一个坏集. 所以坏集的个数不超过 S 的九

元子集的个数$\binom{20}{9}$.但十元子集的个数为$\binom{20}{10}$,因$\binom{20}{10}>\binom{20}{9}$,故好集必然存在.(论证的要点是,指出坏集到九元子集的一个单值对应.)

第18讲

图论问题

1 不能. 参考例 1.

2 用点代表人，如两人是朋友，则在相应的点之间连一条边，得一个图 G. 要证明 G 中至少有两个顶点的次数相同. 因次数非负且 $\leqslant n-1$，故次数只能是 $0, 1, 2, \cdots, n-1$ 之一. 但显然 0 和 $n-1$ 不能同时出现，所以次数只能为 $0, 1, 2, \cdots, n-2$ 或 $1, 2, \cdots, n-1$. 因此，在 n 个点中至少有两点的次数相同.

3 像上一题那样作图 G，则问题化为证明：G 有 $2n$ 个点，每个顶点的次数 $\geqslant n$，则 G 中有一个四边形.

若 $G=K_{2n}$ 则结论显然成立. 若 $G\neq K_{2n}$，则存在点 v_1、v_2 不相连，由于 $d(v_1)+d(v_2)\geqslant 2n$，故 G 的其余点中必有两个点与 v_1、v_2 都相连，设为 v_3 和 v_4，则 v_1、v_2、v_3、v_4 就构成了四边形.

4 将每个三角形的最长边都涂上红色(如果是等腰三角形或正三角形，则可能有两条或三条最长边)，然后将剩下的边涂上蓝色. 由例 5，一定有同色三角形存在. 在这个三角形中必有一条最长边，它是红色的，因此，这个三角形的三边都是红色的. 又它的最小边是红色的，因而是一个三角形的最大边.

请注意，这里的三角形有双重含义，一方面是图论意义下的三角形，另一方面是通常几何中的三角形(可论及其边的长短等).

5 (i) 未必. 可如下构造一个例子：取 5 个完全图 K_{100}，用每个顶点代表一个人，若两个人不认识，则在相应点之间连一条边(注意，这种定义与前面的不同). 由于每个 K_{100} 的顶点与这个图中其他顶点相连，而不与其他 4 个完全图的顶点相连，故每个人认识

400 人. 又任取 6 个顶点中，必有两个顶点在同一个完全图中，而这两点代表的人不认识.

(ii) 可由例 6 推出来(取 $r=6$)：仍然用点代表人，如果两人认识则在相应的两点之间连一边. 这里的作图法与(i)中正好相反，但这仅是为了叙述的便利，并非是实质的差异.

6 将一个五边形的边涂红色，并将顶点连成的五角星的边涂成蓝色.

7 本题等价于证明 $R(3,3,3)\leqslant 17$(参考注 4). 将 K_{17} 的边涂(红、蓝、白)三种颜色. 任取一顶点 v，它连出的 16 条边中必有 6 条边同色，无妨设 v 和 $v_1, v_2, \cdots, v_6$ 连了红边. 以 $v_1, \cdots, v_6$ 为顶点的完全子图 K_6 中，如果含有红边 $v_iv_j(1\leqslant i\neq j\leqslant 6)$，则 K_{17} 中有红色三角形 vv_iv_j. 如 K_6 中不含红边，则它的边仅涂有两种颜色，由例 5，其中必含有同色三角形，从而 K_{17} 中也含有同色三角形.

请注意，能够将 K_{16} 的边涂三种颜色，使其中不含同色三角形(读者可以试试)，从而 $R(3,3,3)\geqslant 17$. 综合起来即知 $R(3,3,3)=17$.

8 设 G 的顶点为 $x_1, \cdots, x_n$，记 $d(x_i)=d_i(i=1,\cdots,n)$. 设 x_i 和 x_j 相连，A 是除 x_j 外与 x_i 相连的顶点集合，B 是除 x_i 外与 x_j 相连的顶点集合，则图中以 x_ix_j 为边的三角形的个数是

$$|A\cap B|=|A|+|B|-|A\cup B|\geqslant d_i+d_j-n$$

(因为 $|A|=d_i-1$，$|B|=d_j-1$，$|A\cup B|\leqslant n-2$). 因为每个三角形有 3 条边，故 G 中三角形的个数至少是

$$k=\frac{1}{3}\sum_{x_i\text{与}x_j\text{相连}}(d_i+d_j-n).$$

由于每个 d_i 在上面和中出现 d_i 次，而 G 有 m 条边，故

$$k=\frac{1}{3}\Big(\sum_{i=1}^{n}d_i^2-mn\Big).$$

因为 $\sum_{i=1}^{n} d_i = 2m$，故由柯西不等式得出

$$k \geqslant \frac{1}{3}\left(\frac{1}{n}\left(\sum_{i=1}^{n} d_i\right)^2 - mn\right) = \frac{1}{3}\left(\frac{4m^2}{n} - mn\right) = \frac{4m}{3n}\left(m - \frac{n^2}{4}\right).$$

由本题结果当然推出了例 7(参考例 7 的证法二).

第19讲

同　余　（二）

1 设 q 是 2^x+1 的任一个素因子. 考虑 2 模 q 的阶 k，由 $2^p\equiv -1(\mathrm{mod}\ q)$，得 $2^{2p}\equiv 1(\mathrm{mod}\ q)$，故 $k\mid 2p$. 因为 p 是素数，故 $k=1,2,p$ 或 $2p$. 由此结合 $2^p\equiv -1(\mathrm{mod}\ q)$ 易知 $k=2$ 或 $2p$. 与例 2 相同地可推出 $q=3$ 或 $q=2px+1$，x 为正整数.

2 设 q 是 a^p-1 的任一素因子，则易证 a 模 q 的阶 k 为 1 或 p. 由此与例 2 相同地可知 $q\mid a-1$ 或 $q=2px+1$（x 为正整数）.

注意 $\dfrac{a^p-1}{a-1}$ 的素因子 q 当然是 a^p-1 的素因子. 因此由上面结果知 $a\equiv 1(\mathrm{mod}\ q)$，或 $q=2px+1$. 若是前一情形，则由

$$\frac{a^p-1}{a-1}=a^{p-1}+\cdots+a+1$$

可见，一方面，$a^{p-1}+\cdots+a+1\equiv 0(\mathrm{mod}\ q)$；

另一方面，由 $a\equiv 1(\mathrm{mod}\ q)$ 得

$$a^{p-1}+\cdots+a+1\equiv \underbrace{1+\cdots+1}_{p\text{个}}=p(\mathrm{mod}\ q).$$

故素数 p 与 q 必须相等.

3 设 d_1 是 $d_1\equiv 1(\mathrm{mod}\,4)$，$d_1\equiv 0(\mathrm{mod}\,5)$，$d_1\equiv 0(\mathrm{mod}\,7)$ 的一个解，即 d_1 满足 $d_1\equiv 1(\mathrm{mod}\ 4)$ 及 $35\mid d_1$，因而可取 $d_1=-35$. 同样，可取 $d_2=56$ 满足 $d_2\equiv 1(\mathrm{mod}\,5)$ 及 $28\mid d_2$；可取 $d_2=-20$ 满足 $d_2\equiv 1(\mathrm{mod}\,7)$ 和 $20\mid d_3$. 于是同余方程组的解是 $x\equiv -35\times 1+56\times 2-20\times 4\equiv -3(\mathrm{mod}\,140)$.

4 因素数有无穷多个，故可取 $2n$ 个互不相同的素数 p_1，…，p_n 及 q_1，…，q_n. 因为 $p_iq_i(1\leqslant i\leqslant n)$ 两两互素，故由中国剩余定理知，同余方程组

$$x\equiv -1(\mathrm{mod}\ p_1q_1),\ \cdots,\ x\equiv -n(\mathrm{mod}\ p_nq_n)$$

有正整数解 x. 易知 $x+1$，…，$x+n$ 符合要求.

5 先用归纳法证明 $2^{\varphi(5^n)}-1$ 被 5^n 整除，但不被 5^{n+1} 整除，由此便易于证明结论. 实际上，设 2 模 5^n 的阶是 k，则 $k\mid\varphi(5^n)$. 又 2 模 5 的阶是 4，故由 $2^k\equiv 1(\mathrm{mod}\ 5)$ 知 $4\mid k$，从而 $k=4\times 5^{l-1}=\varphi(5^l)$. 如果 $l<n$，则由 $2^{\varphi(5^l)}\equiv 1(\mathrm{mod}\ 5^n)$ 得 $2^{\varphi(5^l)}\equiv 1(\mathrm{mod}\ 5^{l+1})$，与上面的结论相违.

6 如果不超过 k 的全体素数都是 m 的因子，则模 m 的任一缩系都满足要求.

考虑相反的情形，取 N 是不超过 k 且和 m 互素的全部素数之积，则 $N>1$. 设 r 满足 $(r,\ m)=1$. 因为 $(m,\ N)=1$，故同余方程组

$$x\equiv r(\mathrm{mod}\ m),\ x\equiv 1(\mathrm{mod}\ N)$$

有解，且任一解的素因子都大于 k（因与 N 互素也和 m 互素）. 当 r 取模 m 的任一缩系中 $\varphi(m)$ 个数时，相应得出的解 x_r 就构成符合要求的缩系.

7 因素数有无穷多个，故可取 $(2n+1)^2$ 个互不相同的素数 $p_{i,\ j}$，$-n\leqslant i,\ j\leqslant n$，则同余方程组

$$x\equiv i(\mathrm{mod}\ p_{i,\ j}),\ -n\leqslant i,\ j\leqslant n,$$

及

$$y\equiv j(\mathrm{mod}\ p_{i,\ j}),\ -n\leqslant i,\ j\leqslant n$$

有解 $x=a$，$y=b$. 若有一个既约整点 $(x',\ y')$ 与 $(a,\ b)$ 之间的距离 $\leqslant n$，则可设 $a-x'=i$，$b-y'=j$，其中 $-n\leqslant i,\ j\leqslant n$. 即 $x'=a-i$，$y'=b-j$. 但 $p_{i,\ j}\mid a-i$，$p_{i,\ j}\mid b-j$，从而 $(x',\ y')$ 不是既约整点.

8 设 p 是 m 的任一个素因子，并设 $p^{\alpha} \parallel m$，$\alpha \geqslant 1$. 由问题中的条件知，A 中有一个无穷子集 A_1，其中的元素均不被 p 整除，因而 A_1 中有无穷多个元素，它们被 mn 除得相同的余数. 设这些数构成的集合记为 A_2，并设其中的数均满足 $\equiv a(\bmod mn)$，这里 $p \nmid a$.

因为 $(m, n)=1$，故 $\left(p^{\alpha}, \dfrac{mn}{p^{\alpha}}\right)=1$. 由中国剩余定理知同余方程组

$$\begin{cases} x \equiv a^{-1}(\bmod p^{\alpha}) \\ x \equiv 0\left(\bmod \dfrac{mn}{p^{\alpha}}\right) \end{cases}, \qquad ①$$

有无穷多个正整数解（其中 a^{-1} 是 a 模 p^{α} 的逆）. 任取一个正整数解 x，并记 B_p 是 A_2 中任意 x 个不同元素的集合，则在 B_p 中的元素之和 $S_p \equiv ax(\bmod mn)$，结合①可知：

$$S_p \equiv ax \equiv 1(\bmod p^{\alpha}),\ S_p \equiv 0\left(\bmod \frac{mn}{p^{\alpha}}\right).$$

现在设 $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$，由上述的论证可知，对每个 $p_i (1 \leqslant i \leqslant k)$，可选出 A 的有限子集 B_{p_i}，其中 $B_{p_i} \subset A \backslash B_{p_1} \cup \cdots \cup B_{p_{i-1}} (2 \leqslant i \leqslant k)$，使得 B_{p_i} 中的元素之和 S_{p_i} 满足：

$$S_{p_i} \equiv 1(\bmod p_i^{\alpha_i}),\ S_{p_i} \equiv 0\left(\bmod \frac{mn}{p_i^{\alpha_i}}\right). \qquad ②$$

考虑集合 $B = \bigcup_{i=1}^{k} B_{p_i}$，则 B 的元素之和 $S = \sum_{i=1}^{k} S_{p_i}$（因为 B_{p_i} 两两不交）. 由②可知，对 $i = 1, 2, \cdots, k$，有

$$S \equiv 1(\bmod m)，且\ S \equiv 0(\bmod n).$$

所以集合 B 满足要求.（请参考本讲(5)给出的中国剩余定理的证明.）

第20讲

不定方程(二)

1 设整数 $c>b>a$ 是直角三角形三边长，若 $\frac{1}{2}ab=2u^2$ 是平方数的二倍，即 $ab=(2u)^2$. 设 $(a,b)=d$，$a=a_1d$，$b=b_1d$，则 $(a_1,b_1)=1$. 从而 a_1b_1 是平方数，故 $a_1=r^2$，$b_1=s^2$ (r，s 是整数). 又由于 $d|c$，设 $c=dc_1$，则由 $a^2+b^2=c^2$ 导出 $r^4+s^4=c_1^2$，与例 2 相违.

若边长是整数 a、a、b 的等腰三角形面积是平方数 u^2，则由海伦公式得出 $b^4+(2u)^4=(4ab)^2$，与例 2 相违.

2 第一个结论不必用例 4，若 $4k+3=x^2+y^2$，模 4 即得矛盾.

为证第二个结论，取 p、q 都是模 4 余 3 的素数，且 $p\neq q$. 由第 7 讲练习题中第 5 题知，我们有无穷多个数 p、q. 显然 $pq\equiv 1(\mathrm{mod}\,4)$；又由例 4 知，$pq$ 不能写成两个整数的平方和.

3 注意 $\binom{x}{2k}a^{2k-2}=\frac{x(x-1)}{2}\binom{x-2}{2k-2}\frac{2a^{2k-2}}{2k(2k-1)}$. 设 $\frac{x(x-1)}{2}$ 中含 2 的最高次幂为 2^r，则易知等式左边被 2^{r+1} 整除，矛盾.

4 x 必是奇数. 而方程可化为 $y^2+1=(x+2)((x-1)^2+3)$，由引理易得矛盾. 参考例 5.

5 与例 5 相同地可知 $x\equiv 1(\mathrm{mod}\,4)$. 而方程可化为 $y^2+4^2=x^3+3^3=(x+3)(x^2-3x+3^2)$.

6 设 $\dfrac{a^2+b^2}{ab+1}=q$（q 是正整数），则

$$a^2+b^2=q(ab+1). \qquad ①$$

将①看作 a，b 的二元方程，显然 $a=b$ 将推出 $q=1$. 我们设 $a>b$，并且在这些解中，取 a 达到最小的一组解 (a_0, b_0). 考虑 x 的一元二次方程

$$x^2-qb_0x+b_0^2-q=0. \qquad ②$$

它已有解 $x=a_0$，另一解是 $a_1=qb_0-a_0$，这是整数，若 q 不是平方数，则 $a_0a_1=b_0^2-q\neq 0$，故 $a_1\neq 0$，若 a_1 是负数，则

$$a_1^2-qb_0a_1+b_0^2-q>-qb_0a_1-q\geqslant q-q=0,$$

与 $x=a_1$ 是②的根矛盾. 于是，若 q 不是平方数，则 a_1 是正整数，即 (b_0, a_1) 是①的正整数解，且

$$a_1=\frac{b_0^2-q}{a_0}<\frac{b_0^2-1}{b_0}<b_0,$$

又 $b_0<a_0$，故 (b_0, a_1) 是①的“更小”的解，矛盾. 从而 q 必是平方数.

7 用反证法. 假设结论不对，我们在所有面积为平方数的勾股三角形中选取一个面积最小的，设其边长为 $x<y<z$，且 $\dfrac{1}{2}xy$ 是平方数. 与例 2 类似，现在必有 $(x, y)=1$. 因为 $x^2+y^2=z^2$，故存在整数 $a>b>0$，a，b 一奇一偶，$(a, b)=1$，使得（不妨设 y 为偶数）

$$x=a^2-b^2,\ y=2ab,\ z=a^2+b^2.$$

由于 $\dfrac{1}{2}xy=(a-b)(a+b)ab$ 是平方数，而易知 $a-b$、$a+b$、a、b 两两互素，故它们都是平方数，即

$$a=p^2,\ b=q^2,\ a+b=u^2,\ a-b=v^2. \qquad ③$$

所以 $u^2-v^2=2q^2$，即 $(u-v)(u+v)=2q^2$. 因为 u、v 都是奇数，易知 $(u-v,\ u+v)=2$. 于是 $u-v$ 和 $u+v$ 中有一个是 $2r^2$，另一个是 $(2s)^2$，而 $q^2=4r^2s^2$. 另一方面，由③得

$$p^2=a=\frac{1}{2}(u^2+v^2)=\frac{1}{4}[(u+v)^2+(u-v)^2]$$

$$=\frac{1}{4}[(2r^2)^2+(2s)^4]=r^4+4s^4.$$

所以，以 r^2、$2s^2$、p 为边的三角形是直角三角形，其面积等于 $\frac{1}{2}r^2\cdot 2s^2=(rs)^2$ 是平方数，但

$$(rs)^2=\frac{q^2}{4}=\frac{b}{4}<(a^2-b^2)ab=\frac{1}{2}xy,$$

于是我们造出了一个面积更小的勾股三角形，矛盾！

综 合 练 习

1 先选 1 名女生有$\binom{5}{1}$种方法. 另两人都为女生共有$\frac{\binom{5}{1}\binom{4}{2}}{3}=10$种选法;另两人一男一女共有$\frac{\binom{5}{1}\binom{8}{1}\binom{4}{1}}{2}=80$种选法;另两人都是男生有$\binom{5}{1}\binom{8}{2}=140$种选法. 因此所求的选法是$10+80+140=230$种.

2 用容斥原理可知排法有$P_6^6-2P_5^5+P_4^4=504$种.

3 考虑由 1、2 组成的 n 位数之集 M. 对 $a\in M$,用 $M(a)$表示 M 中数 b 之集,其中 b 与 a 至多有一位数码不同. 显然 $M(a)$中恰有 n 个与 a 不同的数,$a\in M(a)$,故 $|M(a)|=n+1$.

设 $a_1,\cdots,a_k\in M$ 满足,对 $i\neq j$,a_i 和 a_j 至少有三位数码不同,则$M(a_i)\cap M(a_j)=\varnothing(i\neq j)$. 故 $M(a_1)\cup\cdots\cup M(a_k)$中恰有 $k(n+1)$ 个数,而 $|M|=2^n$,于是 $k(n+1)\leqslant 2^n$.

4 用 $b_1\geqslant\cdots\geqslant b_{17}$,$g_1\geqslant\cdots\geqslant g_{17}$ 分别表示男、女由高到低排列后的高度. 如果有一个 i,使 $|b_i-g_i|>10$,不妨设 $b_i-g_i>10$,则当 $j\geqslant i$ 时,$b_i-g_j>10$;而当 $k\leqslant i$ 时,更有 $b_k-g_j>10$. 又原先 $b_1,\cdots,b_i$ 需配 i 个人,但现在至多有 $i-1$ 个人 $g_1,\cdots,g_{i-1}$. 矛盾!

5 设有 n 位棋手比赛,考虑比赛次数最少的人,设他共赛了 m 局. 现在用两种方法估计(比赛中)分数的总和 S. 一方面,$S\leqslant kn$;另一方面,每赛一局,总分增加 1 分,而一局由两人比赛,故比赛的局数至少是$\frac{mn}{2}$(这里用到 m 的最小性),于是 $S\geqslant\frac{mn}{2}$. 综合起来得 $m\leqslant 2k$.

6 考虑取胜最多的选手 A. 由已知，必有 C 胜了 A，又败给 A 的人中必有胜 C 的选手（否则 C 比 A 胜的次数多），设此人为 B，则 A，B，C 符合要求.

7 $\sum\limits_{i=1}^{n} a_i^3 - \sum\limits_{i=1}^{n} a_i = \sum\limits_{i=1}^{n} (a_i^3 - a_i)$. （参考第 6 讲注 2.）

8 记所说的数列为 $\{a_n\}(n \geqslant 1)$，则易知 a_1、a_2、a_3 模 3 分别同余于 1、2、1，用 $S(n)$ 表示 n 的数码之和，则由 $a_1 \equiv a_3 \pmod 3$，得 $S(a_1) \equiv S(a_3) \pmod 3$，故 $a_2 = a_1 + S(a_1) \equiv a_3 + S(a_3) = a_4 \pmod 3$. 由此可知 $\{a_n\}(n \geqslant 1)$ 模 3 是周期的，因为 $123456 \equiv 0 \pmod 3$，故它不在数列中.

9 本题解法甚多. 例如，由 $\binom{2n+1}{n+1} = \frac{2n+1}{n+1}\binom{2n}{n}$，得 $(n+1)\binom{2n+1}{n+1} = (2n+1)\binom{2n}{n}$，而 $(n+1, 2n+1) = 1$，故 $n+1 \mid \binom{2n}{n}$.

也可以由上面的结果更直接地导出：$\frac{2n+1}{n+1}\binom{2n}{n} = \binom{2n+1}{n+1} = \binom{2n}{n+1} + \binom{2n}{n}$. 因此 $\frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$ 是两个整数之差，故是一个整数.

10 本题的困难在于要看出这实际上是一个代数问题：由二项式定理易知

$$(x+y)^n + (x-y)^n = 2\sum_{0 \leqslant i \leqslant \frac{n}{2}} \binom{n}{2i} y^{2i} x^{n-2i}.$$

由此可知，所说的和即为

$$\frac{1}{2}((1+\sqrt{3})^{2n} + (1-\sqrt{3})^{2n} = \frac{1}{2}((4+2\sqrt{3})^n + (4-2\sqrt{3})^n)$$

$$= 2^{n-1}((2+\sqrt{3})^n + (2-\sqrt{3})^n)$$

$$= 2^n \sum_{0 \leqslant i \leqslant \frac{n}{2}} \binom{n}{2i} 3^i \cdot 2^{n-2i},$$

这显然是 2^n 的倍数.

11 $m\binom{m+n}{m} = (m+n)\binom{m+n-1}{m-1}$，又 $(m, m+n) = 1$，故 $m \mid \binom{m+n-1}{m-1}$.

12 由带余除法，$xm = \left[\frac{xm}{n}\right]n + r_x$（参考第 6 讲注 5）. 对 $1 \leqslant x, y \leqslant n-1$，$x \neq y$，由 $(m, n) = 1$，易知余数 $r_x \neq r_y$，故 $r_1, \cdots, r_{n-1}$ 是 $1, 2, \cdots, n-1$ 的一个排列. 由此易得求证的结果.

13 设 $f(x) = x^5 + x^4 + 1$，ω 是三次单位根，$\omega \neq 1$. 易知 $f(\omega) = f(\omega^2) = 0$，故 $x^2 + x + 1 \mid f(x)$. 特别地，$n^2 + n + 1 \mid f(n)$. 又由于 $f(n) > n^2 + n + 1$（对 $n > 1$），故当 $n > 1$ 时，$f(n)$不是素数.

14 可以证明（更强的结论）：$a_n \not\equiv 0 \pmod 4$（参见第 9 讲注 2）. 实际上，用归纳法易于得知$\{a_n\}$模 4 是循环的，并且可确定其循环节. 模 3 也能解决本题.

15 对 $h \in H$，令 $x = (1-h)^{-1}$，则 $h = \frac{x-1}{x}$. 而 $h^n = -1$ 等价于 $(x-1)^n + x^n = 0$，即 $2x^n + \sum_{k=1}^{n} (-1)^k \binom{n}{k} x^{n-k} = 0$.

记 $S = \{x = (1-h)^{-1} \mid h \in H\}$，则 S 与 H 一一对应，故所求的和等于 $\sum_{x \in S} x^2 = \left(\frac{n}{2}\right)^2 - 2(-1)^2 \frac{\binom{n}{2}}{2} = \frac{n(2-n)}{4}$（用韦达定理）.

16 对任意 k，$4 = k^2 - (k+1)^2 - (k+2)^2 + (k+3)^2$. 因此，若 n 有问题中所说的表示，则

$$n + 4 = \varepsilon_1 1^2 + \varepsilon_2 2^2 + \cdots + \varepsilon_m m^2 + (m+1)^2$$

$$-(m+2)^2-(m+3)^2+(m+4)^2,$$

即 $n+4$ 也有所说的表示. 由于 1，2，3，4 均可表示为所说的形式，故所有 n 均如此.

17 设 $a_1<\cdots<a_n$ 已确定，我们证明，可求得 a_{n+1}，使 $A_{n+1}=a_1^2+\cdots+a_n^2+a_{n+1}^2$ 被 $B_{n+1}=a_1+\cdots+a_n+a_{n+1}$ 整除(且 $a_{n+1}>a_n$). 由 $A_{n+1}=A_n+(a_{n+1}-B_n)(a_{n+1}+B_n)+B_n^2$ 可见，如果 $A_n+B_n^2$ 被 B_{n+1} 整除，则 A_{n+1} 被 B_{n+1} 整除. 因此只要取 $a_{n+1}=A_n+B_n^2-B_n$ (这时 $A_n+B_n^2=B_{n+1}$，且显然 $a_{n+1}>a_n$).

18 设 p_1，…，p_n 是互不相同的 $4k+3$ 型的素数(这有无穷多个，见第 7 讲练习题中的第 5 题). 由中国剩余定理，同余式组

$$x\equiv p_i-i(\mathrm{mod}\ p_i^2)\ (i=1,2,\cdots,n)$$

有解. 取一个正解 x，则 p_i 在 $x+i$ 中恰出现一次，于是 $x+i$ 不能表示为两个整数的平方和($1\leqslant i\leqslant n$)(参考第 19 讲注 8，第 20 讲例 4).

19 设 M 中 1 的个数 大于 $\frac{1}{2}(4n-3)^2$. 如果 M 中不含元素都是 1 的 $2\times n$ 子数表，我们用两种方法计算 M 中元素都是 1 的 2×1 子数表 T 的个数.

按行算，由于 M 中无全 1 的 $2\times n$ 子表格，故任两行构成的 $2\times(4n-3)$ 数表中所含 T 的个数 小于等于 $n-1$. 因此 M 中含 T 的个数小于等于 $(n-1)\binom{4n-3}{2}$.

按列算，设 M 中第 j 列中有 d_j 个 1($1\leqslant j\leqslant4n-3$)，则 M 中 T 的个数是

$$\sum_{j=1}^{4n-3}\binom{d_j}{2}=\frac{1}{2}\sum_{j=1}^{4n-3}d_j^2-\frac{1}{2}\sum_{j=1}^{4n-3}d_j.$$

我们已假设 $\sum\limits_{j=1}^{4n-3}d_j>\frac{1}{2}(4n-3)^2$，故可设

$$\sum_{j=1}^{4n-3} d_j = \frac{1}{2}(4n-3)^2 + \frac{1}{2}.$$

易知，当诸 d_j 相差最小时，$\sum_{j=1}^{4n-3} d_j^2$ 达到最小，而

$$\frac{1}{2}(4n-3)^2 + \frac{1}{2} = 8n^2 - 12n + 5 = (2n-2)(4n-3) + 2n - 1,$$

因此，当 d_j 中有 $2n-2$ 个取 $2n-2$，$2n-1$ 个取 $2n-1$ 时，$\sum d_j^2$ 最小，即

$$T \text{ 的个数} \geqslant \binom{2n-2}{2}(2n-2) + \binom{2n-1}{2}(2n-1).$$

于是，$(n-1)\binom{4n-3}{2} \geqslant (2n-2)\binom{2n-2}{2} + (2n-1)\binom{2n-1}{2}$，易知这不可能.

20 (i) $B(2n+1) = B(2n)$，及(ii) $B(2n) = B(2n-1) + B(n)$.

(i)是显然的，因 $2n+1 = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_r} + 1$ ($i_1 \geqslant i_2 \geqslant \cdots \geqslant i_r \geqslant 0$) 唯一地对应 $2n$ 的一个分拆：$2n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_r}$.

为证明(ii)，将 $2n$ 写成 2 的方幂和的分拆集合写成 $A_n \cup B_n$，其中 A_n 中的元素是如下的分拆

$$2n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_r} + 1,\ i_1 \geqslant i_2 \geqslant \cdots \geqslant i_r \geqslant 0,$$

而 B_n 中的元素是如下的分拆

$$2n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_r},\ i_1 \geqslant i_2 \geqslant \cdots \geqslant i_r \geqslant 1.$$

于是 $A_n \cap B_n = \varnothing$. 又 A_n 中的元素唯一地对应了 $2n-1$ 的一个分拆，而 B_n 中的元素唯一地对应了 n 的一个分拆. 因此(ii)成立. 由(i)、(ii)易用归纳法证明 $B(n)$为偶数.

21 由 $r^{m-1} + \cdots + r + 1 = 0$，得出

$$\begin{aligned} -1 &= r(1 + r + \cdots + r^{2^k-1}) = r(1+r)(1+r^2)\cdots(1+r^{2^{k-1}}) \\ &= (r + r^2)(1+r^2)\cdots(1+r^{2^{k-1}}). \end{aligned} \quad ①$$

(见第 11 讲中例 4.)注意到 $r+r^2=r^2+r^{m+1}=r^2+r^{2(2^{k-1}+1)}$. 故①式右边每一项都是(系数为整数的)平方和,它们的乘积也如此. 这就产生了整系数多项式 $f(x)$ 与 $g(x)$,使得 $f^2(r)+g^2(r)=-1$(参考第 12 讲练习题中的第 8 题).

22 对任意 $m>1$, $x_m\equiv 1=x_1(\mathrm{mod}\,x_m-1)$. 而对任意整数 u、v,有 $(u-v)\mid p(u)-p(v)$. 故 $p(x_m)-p(x_1)\equiv 0(\mathrm{mod}\,x_m-1)$,即 $x_{m+1}\equiv x_2(\mathrm{mod}\,x_m-1)$. 依此类推,可知数列 $\{x_n\}$ 模 x_m-1 是周期的,为 x_1, x_2, …, x_{m-1}.

由已知条件,对 $N=x_m-1$,存在 x_k 使 $x_m-1\mid x_k$. 结合前面结果,可设 $1\leqslant k\leqslant m-1$. 而 $\{x_n\}$ 严格递增,且 $x_m-1\geqslant x_{m-1}$,故必须 $k=m-1$,即 $x_m-1\mid x_{m-1}$,于是 $x_{m-1}\geqslant x_m-1$. 因此 $x_m-1=x_{m-1}$,即 $p(x_{m-1})-1=x_{m-1}$. 所以 $p(x)=x+1$ 有无穷多个不同的根,故 $p(x)=x+1$.

23 当 m 为奇数时, $a^m-1=(a-1)(a^{m-1}+\cdots+a+1)$,后一因式是奇数,故 $2^m\mid a^m-1$ 意味着 $2^m\mid a-1$,这样的 m 只有有限多个. 当 m 为偶数时,我们(以 $2m$ 代换 m)证明至多有有限个 m,使 $2^m\mid (a^2)^m-1$ 就够了. 这相当于在原问题中以 a^2 代换 a,因此可设给定的 a 满足 $a\equiv 1(\mathrm{mod}\,8)$.

设 $a-1=2^l a_1$, $2\nmid a_1$,而 $l\geqslant 3$. 关键是证明,当 $m\geqslant l$ 时, a 模 2^m 的阶是 2^{m-l}. 为此,可先用归纳法证明:当 $m\geqslant l$ 时, $a^{2^{m-l}}-1$ 被 2^m 整除,但不被 2^{m+1} 整除(细节留给读者).

我们设 r 是 a 模 2^m 的阶($m\geqslant l$),则 $r\mid 2^{m-l}$,于是 $r=2^t$. 若 $t<m-l$,则由 $a^{2^t}\equiv 1(\mathrm{mod}\,2^m)$ 推出 $a^{2^t}-1$ 被 2^{t+l+1} 整除,与前面的结论相违,故 $t=m-l$,即 $r=2^{m-l}$.

现在不难证明本题的结论,若 m 满足 $2^m\mid a^m-1$,当 $m\geqslant l$ 时,将有 $2^{m-l}\mid m$. 于是或者 $m<l$,或者 $2^{m-l}\leqslant m$,这样的 m 显然只有有限多个.

24 由第 14 讲公式⑥可见

$$\sum_{\varepsilon_j=0,1}(-1)^{\varepsilon_1+\cdots+\varepsilon_n}(\varepsilon_1x_1+\cdots+\varepsilon_nx_n)^i=\begin{cases}0, & \text{如 } i<n;\\ (-1)^n n!x_1\cdots x_n, & \text{如 } i=n.\end{cases}$$

取 $x_1=1$，$x_2=2$，…，$x_n=2^{n-1}$，则当 $\varepsilon_j=0$，1 时，$\varepsilon_1+2\varepsilon_2+\cdots+2^{n-1}\varepsilon_n$ 恰给出 0，1，2，…，2^n-1. 因此，当 $i<n$ 时，所求的和是 0；而当 $i=n$ 时，所求和是 $(-1)^n n!2^{\frac{n(n-1)}{2}}$（当 $i<n$ 时的结果也不难通过对 i 归纳来证明）.

25 记 $f(k)=(k+a_1)\cdots(k+a_n)$，这看作 k 的多项式是 n 次的（且首项系数是 1），因此

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}f(k)=n!$$

（见第 14 讲公式⑤）. 因为 $f(0)$ 整除 $f(k)$（$k=0,1,\cdots,n$），故 $f(0)\mid n!$，从而 $f(0)\leqslant n!$（注意 $f(0)$ 为正数）. 但 $f(0)$ 是 n 个不同正整数的积，故 a_1，…，a_n 必是 1，2，…，n 的一个排列.

26 答案为 $n=2^k$，其中 k 为非负整数.

首先，若 n 有大于 1 的奇约数 r，则由 2^r-1 整除 2^n-1 知，2^r-1 整除 m^2+9. 因为 $3\nmid 2^r-1$，并且 $2^r-1\equiv-1\pmod 4$，故 2^r-1 必有一个 $\equiv-1\pmod 4$ 的素约数 $p>3$，从而 $m^2+3^2\equiv 0\pmod p$，进而 p 整除 m 与 3，故 $p=3$，矛盾（参看第 20 讲，注 8）. 因此 n 必须是 2 的幂.

现在证明 $n=2^k$ 符合要求. 记 $F_i=2^{2^i}+1$（$i\geqslant 0$），则有（见第 6 讲中例 1 的解法）

$$2^{2^k}-1=F_{k-1}F_{k-2}\cdots F_1F_0.$$

又同余方程

$$x^2\equiv-1\pmod{F_i}$$

有解 $x\equiv 2^{2^{i-1}}\pmod{F_i}$，其中 $i\geqslant 1$. 而对 $i\neq j$，有 $(F_i,F_j)=1$（第 6 讲例 4），故由中国剩余定理知，同余方程组

$$x\equiv 2^{2^{i-1}}\pmod{F_i},\ i=1,2,\cdots,k-1$$

有解 x_0. 显然,数 x_0 满足 $x_0^2 \equiv -1 (\mathrm{mod}\, F_i)$ $(i = 1, \cdots, k-1)$,故 $x_0^2 + 1$ 被 $F_{k-1}F_{k-2}\cdots F_1$ 整除(再一次用到了 F_i 两两互素).

我们取 $m = 3x_0$,则 $m^2 + 9 = 9(x_0^2 + 1)$ 被 $F_{k-1}\cdots F_1 F_0 = 2^{2^k} - 1$ 整除.

27 对任意整数 $x > 1$,我们用 p_x 表示 x 的最小素因子. 证明需下面的引理:

引理 若 p 是素数,使得 $p \mid 2^x + 1$,且 $p < p_x$,则 $p = 3$.

证明 显然 p 是奇素数,设 2 模 p 的阶为 d,则由 $2^{p-1} \equiv 1 (\mathrm{mod}\, p)$ 知,$d \mid p-1$. 又 $p \mid 2^x + 1$,故 $2^{2x} \equiv 1 (\mathrm{mod}\, p)$,从而 $d \mid 2x$. 于是 $d \mid (2x, p-1)$. 但 $p < p_x$,故 $p-1$ 不能有整除 x 的素约数,从而 $(2x, p-1) = 2$,即 $d \mid 2$,由此知 $d = 2$,故 $p = 3$.

现在我们解答本题. 设有符合问题中要求的整数 a、b、c,则 a、b、c 都是奇数,且 p_a、p_b、p_c 两两不同,不妨设 p_a 是三者中最小的,因为 $a \mid 2^b + 1$,故 $p_a \mid 2^b + 1$,但 $p_a < p_b$,故由引理推知 $p_a = 3$. 我们记 $a = 3a'$.

设 a'、b、c 的最小素因子为 p,我们来证明,必有 $p \mid b$. 假设 p 整除 a',则由 $(a, c) = 1$ 及 $p \leqslant p_c$ 可知,必须有 $p < p_c$. 但是 $a \mid 2^c + 1$,故 $p \mid 2^c + 1$,于是由上述引理知 $p = 3$,故 $9 \mid a$. 因此 $9 \mid 2^c + 1$,进而 $9 \mid 2^{2c} - 1$. 但易验证 2 模 9 的阶为 6,故 $6 \mid 2c$,即 $3 \mid c$,这与 a、c 互素矛盾. 因此 $p \nmid a'$. 类似地可证明 $p \nmid c$. 因此只能 $p \mid b$.

设 2 模 p 的阶为 d,则与上述引理相同地可证明 $d \mid (2a, p-1)$,即 $d \mid (6a', p-1)$. (利用 $p \mid b$ 及 $b \mid 2^a + 1$.)由 p 的选取可知,$p-1$ 与 a' 互素,于是 $(6a', p-1)$ 整除 6,即 $d \mid 6$. 因此 $p \mid 2^6 - 1$,故 $p = 7$. 但是

$$2^a + 1 = (2^3)^{a'} + 1 \equiv 2 (\mathrm{mod}\, 7),$$

因此 p 不整除 $2^a + 1$,矛盾.

28 不妨设 $a_1, \cdots, a_{k+1}$ 模 $n + k$ 互不同余. 我们考虑下面三组数(其中 $S = a_1 + \cdots + a_{k+1}$):

(i) a_1，a_2，…，a_{k+1}；

(ii) $S-a_1$，$S-a_2$，…，$S-a_{k+1}$；

(iii) S，$S+a_{k+2}$，$S+a_{k+2}+a_{k+3}$，…，$S+a_{k+2}+\cdots+a_n$.

这共有 $(k+1)+(k+1)+n-(k+2)+2=n+k+2$ 个数，故其中必有两个数模 $n+k$ 同余. 显然，(i)中的数互不同余；(ii)中的数也如此. 注意，我们可假设(iii)中无两数同余，(i)与(iii)中的数没有两个同余，(ii)与(iii)中的数也没有两个同余，否则易知结论成立. 因此(i)与(ii)中必有两个数模 $n+k$ 同余. 若有 $i\neq j$，使 a_i 与 $S-a_j$ 模 $n+k$ 同余，则结论显然成立. 故必有 i 使 a_i 与 $S-a_i$ 模 $n+k$ 同余 $(1\leqslant i\leqslant k+1)$.

若满足 $a_i\equiv S-a_i(\bmod n+k)$ 的 a_i 至多有两个，则从(i)中将这样的 a_i 删去. 这时，前面考虑的数至少剩下 $n+k$ 个. 因现在(i)与(ii)中已无两数模 $n+k$ 同余，故剩下的数中无两数模 $n+k$ 同余，从而它们恰有 $n+k$ 个，特别，其中有一个模 $n+k$ 同余于 0，由此知结论成立.

若至少有三个 a_i 满足上述同余式，不妨设为 a_1、a_2、a_3. 则 $2a_1\equiv 2a_2\equiv 2a_3(\bmod n+k)$. 如 $n+k$ 为奇数，这给出 $a_1\equiv a_2\equiv a_3(\bmod n+k)$，与前面关于 a_1，…，a_{k+1} 的假设相违；如 $n+k$ 为偶数，则 $a_1\equiv a_2\equiv a_3\left(\bmod \dfrac{n+k}{2}\right)$，即 $a_1=a_2+\dfrac{n+k}{2}M_1$，$a_1=a_3+\dfrac{n+k}{2}M_2$，这里 M_1、M_2 都是奇数(否则 $a_1\equiv a_2$，或 $a_1\equiv a_3(\bmod n+k)$). 于是

$$a_2=a_3+\frac{n+k}{2}(M_2-M_1)\equiv a_3(\bmod n+k),$$

产生矛盾.

29 记 $t=\dfrac{r^2+s^2+k}{rs}$. 由问题中的递推关系得(对 $n\geqslant 2$)

$$a_{n+2}a_n=a_{n+1}^2+k,\ a_{n+1}a_{n-1}=a_n^2+k.$$

两式相减，产生

$$\frac{a_{n+2}+a_n}{a_{n+1}}=\frac{a_{n+1}+a_{n-1}}{a_n}.$$

由此递推地得出（对 $n\geqslant 1$）

$$\frac{a_{n+2}+a_n}{a_{n+1}}=\cdots=\frac{a_3+a_1}{a_2}=\frac{r^2+s^2+k}{rs}=t.$$

故 $a_{n+2}=ta_{n+1}-a_n$. 因此，若 t 为整数，则由归纳法即知所有 a_n 都是整数.

反过来，若所有 a_n 都是整数，则 t 是有理数，设 $t=\frac{u}{v}$，这里 $(u, v)=1$ 且 $v>0$. 由 $a_3=\frac{u}{v}a_2-a_1$，并注意 a_1、a_2、a_3 都是整数，可知 $v|a_2$. 类似地，$v|a_i$（对 $i=2, 3, \cdots$）. 再由 $a_4=\frac{u}{v}a_3-a_2$，及 v 整除 a_2、a_3、a_4 知，$v^2|a_3$. 类似地，对 $i=3, 4, \cdots$，有 $v^2|a_i$. 如此进行，易于证明，对正整数 n，有 $v^n \mid a_{n+i}(i=1, 2, \cdots)$.

现在，若 $v\neq 1$，则可取自然数 N 足够大，使 $v^N>|k|$. 在等式 $k=a_{N+1}a_{N+3}-a_{N+2}^2$ 中，右边被 v^N 整除，但左边显然不被 v^N 整除，矛盾. 故 $v=1$，即 t 是整数.

30 我们首先证明，当 $m=5^n$ 时，存在一个 n 位数是 5^n 的倍数，且它的各位数码都是奇数.

用归纳法，$n=1$ 时，一位数 5 符合要求. 假设当 $n=k$ 时，数 $\overline{a_ka_{k-1}\cdots a_1}$ 是满足要求的 k 位数. 我们要证明，存在一个 $a_{k+1}\in\{1, 3, 5, 7, 9\}$，使得 $k+1$ 位数

$$\overline{a_{k+1}a_k\cdots a_1}=a_{k+1}\times 10^k+\overline{a_k\cdots a_1}$$

是 5^{k+1} 的倍数. 由于 $\overline{a_k\cdots a_1}$ 是 5^k 的倍数，故上式右端为 $5^k(a_{k+1}\times 2^k+l)$，其中 l 为一个奇数. 易知，当 $k=1, 2, \cdots$ 时，2^k 模 5 周期地为 2、4、3、1. 由此易验证，对任何奇数 l 及正整数 k，均有所需的 a_{k+1}，使得 $a_{k+1}\times 2^k+l$ 被 5 整除，从而 $\overline{a_{k+1}a_k\cdots a_1}$ 被 5^{k+1} 整除.

现在设 m 是任一个奇数. 将 m 分解为 $5^k \cdot m_1$，其中 $k \geqslant 0$，m_1 是与 10 互素的正整数. 由上面的结论，我们可先作出 5^k 的一个倍数 $\overline{a_k a_{k-1} \cdots a_1}$，它的各位数码都是奇数. (在 $k = 0$ 时，将这个数取为 1.)考虑数列 $\{A_n\}$ $(n \geqslant 1)$，其中 A_n 是将数 $\overline{a_k \cdots a_1}$(从左至右)重复写 n 次产生的(nk 位)数，即 A_n 具有形式

$$\overline{a_k \cdots a_1 a_k \cdots a_1 \cdots a_k \cdots a_1}.$$

$\{A_n\}$中必有两个的差被 m_1 整除；这个差可表示为形式 $A_i \times 10^j$ $(i \geqslant 1,\ j \geqslant 1)$. 因 m_1 与 10 互素，故 m_1 整除 A_i. 又 A_i 是 5^k 的倍数，故 A_i 为 $5^k \times m_1$ 的倍数(又一次用到 m_1 和 5 互素)，而 A_i 的数码当然都是奇数.

31 记 $\sum S(a^*)$ 表示 $n!$ 个排列 a^* 所对应的 $S(a^*)$之和. 假定结论不对，我们通过计算 $\sum S(a^*)$ 来产生矛盾.

一方面，因为对 $a^* \neq b^*$，$n!$ 不整除 $S(a^*) - S(b^*)$，而共有 $n!$ 种不同的排列，故诸 $S(a^*)$模 $n!$ 的余数恰是 0，1，…，$n! - 1$. 因此

$$\sum S(a^*) \equiv \frac{(n! - 1)n!}{2} (\mathrm{mod}\, n!). \qquad ①$$

另一方面，在 $n!$ 种排列 $a^* = (a_1, \cdots, a_n)$ 中，$a_1 = k$ 的排列共有 $(n-1)!$ 种，这里 $k = 1, 2, \cdots, n$. 因此在 $\sum S(a^*)$ 中，c_1 的系数为

$$(n-1)!(1 + 2 + \cdots + n) = \frac{(n+1)!}{2}.$$

同样的结论对其余 c_i 也成立. 因此

$$\sum S(a^*) = \frac{(n+1)!}{2} \sum_{i=1}^{n} c_i. \qquad ②$$

综合①、②得出

$$\frac{(n+1)!}{2}\sum_{i=1}^{n}c_i\equiv\frac{(n!-1)n!}{2}(\mathrm{mod}\,n!).$$

因 n 为奇数，故上式左边被 $n!$ 整除；而对 $n>1$，右边不是 $n!$ 的倍数，矛盾.

32 我们只要模 2 考虑问题. 任一个三元整数组(A, B, C)在模 2 意义下共有八种可能(A_j, B_j, C_j)，这里 A_j、B_j、C_j 是 0 或 1 $(j=0, 1, \cdots, 7)$，并且 $A_0=B_0=C_0=0$. 易于验证，对任一个三元数组(a_i, b_i, c_i)(其中 a_i，b_i，c_i 中至少有一个是奇数)，八个数

$$a_iA_j+b_iB_j+c_iC_j(j=0, 1, \cdots, 7)$$

中恰有四个偶数、四个奇数. 因此，七个数

$$a_iA_j+b_iB_j+c_iC_j(j=1, \cdots, 7)$$

中恰有三个偶数及四个奇数. 由此可知下面的数

$$a_iA_j+b_iB_j+c_iC_j(j=1, \cdots, 7, i=1, \cdots, n)$$

中恰有 $4n$ 个奇数. 但上面的数可分成七个组，其中第 j 个组中的数为 $a_iA_j+b_iB_j+c_iC_j(i=1, \cdots, n)$，而 $1\leqslant j\leqslant 7$. 因此必有一个组中，奇数的个数 $\geqslant\frac{4}{7}n$.

33 记 $S=\{a_1, a_2, \cdots, a_{2000}\}$. 我们只要证明 S 有两个非空子集 C 和 D 满足条件(i)、(ii)、(iii)就够了. 因若有了这样的 C、D，取 $A=C\backslash D$ 及 $B=D\backslash C$，则 A，B 便符合问题中的要求.

为了证明，我们将 S 的每个非空子集 E 对应一个(有序)三元数组：

$$E\longrightarrow(f_0(E), f_1(E), f_2(E)),$$

这里 $f_i(E)$表示 E 中元素的 i 次幂之和 $(i=0, 1, 2)$. 我们证明，这一映射不是单射，从而有子集 C 和 D，使 C、D 的像相同，即 $f_i(C)=f_i(D)$ $(i=0, 1, 2)$，于是 C、D 符合上面说的要求(参

考第 3 讲中注 5).

因为 $|S|=2000$ 以及 S 中最大数小于 10^{100}，故对任意 E，我们有

$$f_0(E)\leqslant 2000,\ f_1(E)\leqslant 2000\times 10^{100},\ f_2(E)\leqslant 2000\times 10^{200}.$$

因此，像元素的个数不超过

$$(2000)^3\times 10^{300}<(2^{11})^3\times(2^{10})^{100}=2^{1033}.$$

若上述的映射为单射，则 S 的非空子集的个数，应不超过像元素的个数，即有 $2^{2000}-1<2^{1033}$，矛盾.

34 设 $S_{n-1}=\{a_1,a_2,\cdots,a_k\}$，这里 $a_1<a_2<\cdots<a_k$. 显然 S_n 中最小数为 a_1，最大数为 a_k+1. 我们注意，对 $i\geqslant 2$，$a_i\notin S_n$ 当且仅当 $a_i-1\in S_{n-1}$，即 $a_{i-1}=a_i-1$. 因此，我们有

$$\sum_{a\in S_n}x^a\equiv(1+x)\sum_{a\in S_{n-1}}x^a(\mathrm{mod}\ 2).$$

由归纳立知，对 $n\geqslant 1$，有

$$\sum_{a\in S_n}x^a\equiv(1+x)^n\sum_{a\in S_0}x^a(\mathrm{mod}\ 2).$$

另一方面，由同余式 $(1+x)^2\equiv 1+x^2(\mathrm{mod}\ 2)$，并对 n 归纳，易于得出 $(1+x)^{2^n}\equiv x^{2^n}+1(\mathrm{mod}\ 2)$. 因此，若 N 是 2 的幂，我们有

$$\sum_{a\in S_N}x^a\equiv(1+x^N)\sum_{a\in S_0}x^a(\mathrm{mod}\ 2).$$

最后，进一步取 N 大于 S_0 中最大的数，则由上式得出

$$S_N=S_0\cup\{N+a:a\in S_0\}.$$

35 将给定的整数作为一个图的顶点，若两个整数互素，则将这两个数相应的点之间连一条边. 我们的结论是：若图的边数大于 94，则图中必有一个长度为 4 的循环子图，即有顶点 a、b、c、d，使得 a 与 b 相连，b 与 c 相连，c 与 d 相连，而 d 与 a 相连.

我们证明下面更一般的图论结果：

若图 G 有 n 个顶点，不包含长度为 4 的循环子图，则 G 的边数 m 满足

$$m \leqslant \frac{n}{4}(1+\sqrt{4n-3}).$$

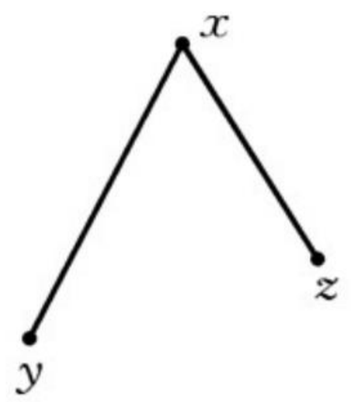
为了证明，记 G 的顶点集为 V，对任意 $u \in V$，用 $d(u)$ 表示 u 的次数（即从 u 引出的边数）. 证明的要点是计数 G 中如图所示的图形的个数（其中 x 与 y 及 z 相连，$y \neq z$，但不考虑 y 和 z 是否相连）.

因为对每个 $u \in V$，恰有 $\binom{d(u)}{2}$ 个上述图形，故这种图形的个数是 $\sum\limits_{u\in V}\binom{d(u)}{2}$. 另一方面，每一对顶点 $\{y, z\}$ 至多有一个 x 与 y、z 都相连（否则 G 中就有一个长度为 4 的循环子图）. 因此我们有（参考第 3 讲中注 4）

$$\sum_{u\in V}\binom{d(u)}{2} \leqslant \binom{n}{2},$$

此即

$$\sum_{u\in V} d^2(u) \leqslant n(n-1)+\sum_{u\in V} d(u).$$



（第 35 题）

由柯西不等式，得出

$$\Big(\sum_{u\in V} d(u)\Big)^2 \leqslant n\sum_{u\in V} d^2(u).$$

而熟知 $\sum\limits_{u\in V} d(u) = 2m$. 因此我们有

$$4m^2 \leqslant n^2(n-1)+2nm,$$

解得 $m \leqslant \frac{n}{4}(1+\sqrt{4n-3})$.

36 我们证明，有一个正整数序列 $\{a_n\}$，使得 $a_1^2+\cdots+a_n^2$ 都是奇数的平方. 取 $a_1 = 1$，若 a_1，…，a_n 已取定，并设 $a_1^2+\cdots+$

$a_n^2=(2k+1)^2$，取 $a_{n+1}=2k^2+2k$，则由 $(2k+1)^2+(2k^2+2k)^2=(2k^2+2k+1)^2$，即知 $a_1^2+\cdots+a_n^2+a_{n+1}^2$ 也是奇数的平方.

37 对 $i=1,\cdots,k-1$，连续 k 个整数之积 $(i+1)\cdot\cdots\cdot(i+k)$ 被 $k!$ 整除，故 $i^k\equiv b_1 i^{k-1}+\cdots+b_k(\mathrm{mod}\,k!)$，这里 $b_1,\cdots,b_k$ 都是整数. 故由条件知

$$\sum_{i=1}^{n}a_i i^k\equiv\sum_{i=1}^{n}(b_1a_i i^{k-1}+\cdots+b_k a_i)$$

$$=b_1\Big(\sum_{i=1}^{n}a_i i^{k-1}\Big)+\cdots+b_k\Big(\sum_{i=1}^{n}a_i\Big)\equiv 0(\mathrm{mod}\,k!).$$

38 设非常数的整系数多项式 $f(x)=a_n x^n+\cdots+a_1x+a_0$ 对 $x=0,1,\cdots$，仅有有限个不同的素因子 $p_1,\cdots,p_k$，则 $a_0\neq 0$. 取 $x=p_1\cdot\cdots\cdot p_k a_0 t$，并设整数 t 充分大，则 $f(x)$可表示为如下形式：

$$f(x)=a_0(p_1\cdot\cdots\cdot p_k A_t+1),$$

这里 A_t 是一个依赖于 t 的整数，在 t 充分大时，$|A_t|>1$. 故 $p_1\cdot\cdots\cdot p_kA_t+1$ 有素因子 p，显然 p 不同于 $p_1,\cdots,p_k$，与前面的假设矛盾.

39 可取 $f(x)=x^n+210(x^{n-1}+\cdots+x^2)+105x+12$.

由 Eisenstein 判别法(取 $p=3$)可知，$f(x)$不能分解为两个非常数的整系数多项式之积. ($210=2\times3\times5\times7$，$105=3\times5\times7$，$12=2^2\times3$，故 3 整除 $x,\cdots,x^{n-1}$的系数，3^2 不整除常数项，而 3 不整除首项系数 1.)

对任意整数 x，因 $f(x)=x(x^{n-1}+105)+210(x^{n-1}+\cdots+x)+12$，故 $f(x)$的值总是偶数. 因此$|f(x)|$不可能取奇素数值.

若 $f(x)=2$ 有整数解 x，则

$$f_1(x)=x^n+210(x^{n-1}+\cdots+x^2)+105x+10$$

有整数根. 但由 Eisenstein 判别法(取 $p=5$) 可知，$f_1(x)$不能分

解为两个非常数的整系数多项式的积，故更不能有一次整系数因式，与 $f_1(x)=0$ 有整数根矛盾.

若 $f(x)=-2$ 有整数解 x，则

$$f_2(x)=x^n+210(x^{n-1}+\cdots+x^2)+105x+14$$

有整数根. 但由 Eisenstein 判别法(取 $p=7$) 可知，$f_2(x)$不能分解为两个非常数的整系数多项式的积，矛盾. 因此，$|f(x)|$也不可能取偶素数 2.

40 由于素数有无穷多个，故可(归纳地)选取一个无穷的素数列$\{p_n\}(n=0,1,\cdots)$，使得 $p_n>p_1+\cdots+p_{n-1}$ 对所有 $n\geqslant 1$ 成立. 由第 13 讲练习题中第 7 题可知，多项式

$$f_n(x)=p_0x^n+\cdots+p_{n-1}x+p_n\quad(\text{对所有 } n\geqslant 1)$$

不能分解为两个非常数的整系数多项式之积，从而 $x^nf_n\left(\frac{1}{x}\right)$ 也如此，即 $p_nx^n+p_{n-1}x^{n-1}+\cdots+p_1x+p_0$ 对所有 $n\geqslant 1$，不能分解为两个非常数的整系数多项式之积.

本题也可用第 13 讲中的例 6 来构造符合要求的数列. 我们取$\{p_n\}$是一个无穷的素数列，满足 $p_0<p_1<\cdots<p_n<\cdots$，则由第 13 讲中例 6 可知，多项式

$$f_n(x)=p_0x^n+p_1x^{n-1}+\cdots+p_n(n\geqslant 1)$$

不能分解为两个非常数的整系数多项式之积，从而 $x^nf_n\left(\frac{1}{x}\right)$也如此，即 $p_nx^n+\cdots+p_1x+p_0$ 对所有 $n\geqslant 1$，不能分解为两个非常数的整系数多项式之积(参考第 13 讲中注 4).

专题1

组 合 问 题

本节介绍一些组合问题，其中有一些较为困难，解决它们需要灵活地应用有关的知识和方法，这正是组合问题最为显著的特点.

例1 设 S 是正整数集合 $\mathbf{N}^*$ 的一个真子集，对任意 x，$y\in S$（允许 $x=y$），有 $x+y\in S$. 设 $a_1<a_2<\cdots$ 是不属于 S 的所有正整数. 证明：$a_1+\cdots+a_n\leqslant n^2$（对 $n\geqslant 1$）.

证明 显然 $1\notin S$（否则由条件推出 $2=1+1\in S$，$3=1+2\in S$，…，进而所有正整数在 S 中，与 S 为 $\mathbf{N}^*$ 的真子集相违），即 $a_1=1$. 我们现在证明

$$a_k\leqslant 2k-1,\text{对所有 } k\geqslant 1 \text{ 成立.} \qquad ①$$

（参见下面的注 2.）显然可设 $k\geqslant 2$. 由于 $a_k\notin S$，故对 $m=1$，2，…，$\left[\frac{a_k}{2}\right]$，正整数 m 与 a_k-m 中必有一个不在 S 中（否则，由条件推出它们的和 a_k 在 S 中，与所设矛盾），我们任取其中的一个记为 $f(m)$，即 $f(m)$ 为 m 或 a_k-m. 注意 $0<f(m)<a_k$，而 $f(m)\notin S$，故由定义知 $f(m)$ 为 a_1，…，a_{k-1} 之一.

进一步，由于 $m\leqslant\left[\frac{a_k}{2}\right]$，故 $m\leqslant a_k-m$. 由此易知，对 $1\leqslant m_1$，$m_2\leqslant\left[\frac{a_k}{2}\right]$，$m_1\neq m_2$，总有 $f(m_1)\neq f(m_2)$. 因此，f 是集合 $A=\left\{1,2,\cdots,\left[\frac{a_k}{2}\right]\right\}$ 到集合 $B=\{a_1,\cdots,a_{k-1}\}$ 的一个单射，故 $|A|\leqslant|B|$，即 $\left[\frac{a_k}{2}\right]\leqslant k-1$，由此即知 $a_k\leqslant 2k-1$，从而①得证.

将①对 $k=1,2,\cdots,n$ 求和，即得 $a_1+\cdots+a_n\leqslant n^2$.

注1 取 S 为大于 m 的所有正整数之集(这里 m 为一个大于1的整数)，则 S 符合问题中的要求，此时，不在 S 中的正整数的集合 $\overline{S}$ 是一个有限集 $\{1,2,\cdots,m\}$.

取 S 为全体正偶数之集，则 $\overline{S}$ 为全体正奇数的集合，这是一个无限集. 在这一情形下，问题中的不等式化为了等式.

注2 若注意到 $1+3+\cdots+(2n-1)=n^2$，则求证的不等式即为

$$\sum_{k=1}^{n}a_k\leqslant\sum_{k=1}^{n}(2k-1).$$

因此，从代数角度看，我们应期望有“单项”的不等式：$a_k\leqslant 2k-1$，$k=1,\cdots,n$. 注1中举的例子，则是这一期望结果的正确性的一个支持.

此外，若试图用归纳法解决本题，也能诱导证明不等式①：我们希望由归纳假设 $a_1+\cdots+a_{k-1}\leqslant(k-1)^2$，产生

$$a_1+\cdots+a_{k-1}+a_k\leqslant(k-1)^2+a_k\leqslant k^2,$$

当然应当期望有 $a_k\leqslant 2k-1\ (k\geqslant 1)$.

注3 证明①的方法值得一提，我们并非是只着眼于“单项” a_k，而是用两种不同的角度考虑一个与 a_k 有关的“整体”的量：小于 a_k 且不在 S 中的全部正整数. 综合这两个方面，产生所需的结果.

在许多问题中，单个的量并无适用的性质，而某种整体的量，则有相当好的性态. 从整体看问题，是数学中，特别是组合数学中一种非常基本的想法，本书中已有不少这样的例子，下面几个例子也是这样做的(请参考第17讲的注3及相关的例子).

例2 12个球队比赛，每两队主客场各赛一次，胜者得3分，平者各得1分，负者得0分. 比赛结束后，问第一名至第十二名各队积分表上，相邻名次的积分相差的最大值是多少?

解 设第一名至第十二名的积分依次为 a_1，a_2，…，a_{12}，则

$$a_1 \geqslant a_2 \geqslant \cdots \geqslant a_{12}. \qquad ②$$

对于 $1 \leqslant n \leqslant 11$，直接估计“整体”$a_n - a_{n+1}$ 并不易入手，我们将分别作出“单项”a_n 及 a_{n+1} 的上、下界.

由②可知

$$a_n \leqslant \frac{1}{n}(a_1 + \cdots + a_n), \qquad ③$$

而整体的量 $a_1 + \cdots + a_n$ 有适用的上界信息：因为任两队比赛一场的得分之和不超过 3 分，而前 n 名之间共进行了 $2\binom{n}{2}$ 场比赛；前 n 名与后 $12-n$ 名各个队共进行了 $2n(12-n)$ 场比赛. 因此前 n 名的得分总和 $a_1 + \cdots + a_n \leqslant 3 \cdot 2\binom{n}{2} + 3 \times 2n(12-n) = (69-3n)n$.

故由 ③ 知 $a_n \leqslant 69 - 3n$.

同样，由于任两队比赛一场的得分之和不少于 2 分，而后 $12-n$ 名各队彼此比赛了 $2\binom{12-n}{2}$ 场，因此后 $12-n$ 名各队的得分之和 $a_{n+1} + \cdots + a_{12} \geqslant 2 \cdot 2\binom{12-n}{2} = 2(12-n)(11-n)$. 故由②知

$$a_{n+1} \geqslant \frac{1}{12-n}(a_{n+1} + \cdots + a_{12}) \geqslant 2(11-n).$$

从而 $a_n - a_{n+1} \leqslant (69-3n) - (22-2n) = 47 - n \leqslant 46$.

又易见，若第一名全胜，其余队之间皆平时，第一、二名的积分之差取得 46 分，因此所求的最大值为 46.

例 3 对正实数 x，记 $S(x) = \{[kx] \mid k = 1, 2, \cdots\}$. 设 a、b、c 是三个大于 1 的实数，满足 $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$，则三个集合 $S(a)$、

$S(b)$、$S(c)$中，必有两个的交集是无限集(即有无穷多个元素).

证明　我们不直接考虑无限集合 $S(a)$、$S(b)$和 $S(c)$，而是引入一个参量 n(n 为正整数)，考虑有限集合

$$S_n(a) = S(a) \bigcap \{1, 2, \cdots, n\}.$$

$S_n(b)$及 $S_n(c)$类似地定义.

由容斥原理，注意到 $| S_n(a) \bigcap S_n(b) \bigcap S_n(c) | \geqslant 0$，我们得

$$\begin{aligned} n &\geqslant | S_n(a) \bigcup S_n(b) \bigcup S_n(c) | \\ &\geqslant | S_n(a) | + | S_n(b) | + | S_n(c) | - | S_n(a) \bigcap S_n(b) | \\ &\quad - | S_n(b) \bigcap S_n(c) | - | S_n(c) \bigcap S_n(a) |. \end{aligned}$$

此外，易知 $| S_n(a) | \geqslant \left[\frac{n}{a}\right]$，$| S_n(b) | \geqslant \left[\frac{n}{b}\right]$及 $| S_n(c) | \geqslant \left[\frac{n}{c}\right]$，故我们有

$$\begin{aligned} &| S_n(a) \bigcap S_n(b) | + | S_n(b) \bigcap S_n(c) | + | S_n(c) \bigcap S_n(a) | \\ \geqslant &\left[\frac{n}{a}\right] + \left[\frac{n}{b}\right] + \left[\frac{n}{c}\right] - n > \left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1\right) n - 3. \end{aligned}$$

由于 $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} - 1$ 是正的常数，故上式右边随 n 可任意地大；从而$S(a)$、$S(b)$、$S(c)$中必有两个的交集是无限集(否则上式左边对任何 n 均保持有界).

例 4　将若干个球分为 n 堆，然后合并起来，重新分成 $n+k$ 堆. 证明：至少有 $k+1$ 个球第二次是分在比第一次小的堆中.

证明　如果一个球第一次所在的堆中有 a 个球，第二次所在的堆中有 b 个球，我们就将这个球与有序数对$\left(\frac{1}{a}, \frac{1}{b}\right)$对应.

考虑纵坐标与横坐标的差$\frac{1}{b} - \frac{1}{a}$.

我们希望至少有 $k+1$ 个这样的差是正数(差为正等价于 $b < a$，即

这个球第二次是在比第一次小的堆中).

由于问题没有判别每个单项差是否为正的信息,我们因此考虑它们的总和 S.

为了计算 S,可以分别算出横、纵坐标之和. 由于同一堆中 b 个球的纵坐标之和是 $b\times\frac{1}{b}=1$. $\left(\text{这就是为什么用}\frac{1}{b}\text{作为坐标.}\right)$ 故第二次 $n+k$ 堆中的所有球的纵坐标之和是 $(n+k)\times 1=n+k$. 同理 n 堆中所有球的横坐标之和是 n. 因此

$$S=(n+k)-n=k. \tag{4}$$

由于每个差 $\frac{1}{b}-\frac{1}{a}<1$,故由④推出,$S$ 中至少有 $k+1$ 个差是正的,这就证明了结论.

例 5 设 k 个整数

$$1\leqslant a_1<a_2<\cdots<a_k\leqslant n$$

中,任意两个数 a_i、a_j 的最小公倍数 $[a_i,\ a_j]>n$,则

$$\sum_{i=1}^{k}\frac{1}{a_i}<\frac{3}{2}.$$

证明 考虑下面的数:

$$\left.\begin{array}{l} a_1,\ 2a_1,\ \cdots,\ \left[\dfrac{n}{a_1}\right]a_1,\\ a_2,\ 2a_2,\ \cdots,\ \left[\dfrac{n}{a_2}\right]a_2,\\ \cdots\\ a_k,\ 2a_k,\ \cdots,\ \left[\dfrac{n}{a_k}\right]a_k. \end{array}\right\} \tag{5}$$

这些数均不超过 n,且无一个数是 1(因 $a_1\neq 1$,否则 $[a_1,\ a_2]=[1,\ a_2]=a_2\leqslant n$,与题设不合). 此外,⑤中的数没有两个相等. 因为同一行中的数显然互不相等;若有 $i\neq j$ 及整数 r、$s\left(1\leqslant r\leqslant\right.$

$\left[\frac{n}{a_i}\right]$，$1 \leqslant s \leqslant \left[\frac{n}{a_j}\right]$），使得

$$ra_i = sa_j,$$

则 $[a_i, a_j] \leqslant [ra_i, a_j] = [sa_j, a_j] = sa_j \leqslant n$，与题设相违.

因此，⑤中数的个数不超过 $n-1$，即

$$\sum_{i=1}^{k} \left[\frac{n}{a_i}\right] \leqslant n-1 \qquad ⑥$$

(参考第 8 讲(18)的证明). 于是

$$\sum_{i=1}^{k} \frac{n}{a_i} - k < n-1,$$

即

$$\sum_{i=1}^{k} \frac{n}{a_i} < n-1+k. \qquad ⑦$$

另一方面，不难证明

$$k \leqslant \left[\frac{n+1}{2}\right]. \qquad ⑧$$

事实上，如果⑧不成立，则在 $n = 2m$ 时，有 $k > m$. 将每个 a_i 写成 $2^{\lambda_i} b_i$ 的形式，这里 $\lambda_i \geqslant 0$，b_i 是奇数，且 $b_i < n = 2m$. 因为 1，2，…，$2m$ 中只有 m 个不同的奇数，故 $k(>m)$ 个奇数 b_1，…，b_k 中至少有两个相同，设 $b_i = b_j (1 < i < j \leqslant k)$，则在 $a_i = 2^{\lambda_i} b_i$ 和 $a_j = 2^{\lambda_j} b_j$ 中，由 $a_i < a_j$ 知 $\lambda_i < \lambda_j$，故 $a_i \mid a_j$，从而 $[a_i, a_j] = a_j \leqslant n$，与题设不合.

如果 $n = 2m+1$，则 $k > m+1$. 因在 1，2，…，$n = 2m+1$ 中只有 $m+1$ 个奇数，因而仍有两个 a_i 和 a_j，使 $a_i \mid a_j$，同样产生矛盾. 因此⑧得证.

最后，由⑦和⑧得出

$$\sum_{i=1}^{k} \frac{n}{a_i} < n-1+\left[\frac{n+1}{2}\right] \leqslant n-1+\frac{n+1}{2} < \frac{3n}{2},$$

故 $\sum_{i=1}^{k}\frac{1}{a_i}<\frac{3}{2}$.

例 5 的关键，是(利用已知条件)制造及计数数集⑤，进而(由考虑整体)产生不等式⑥.

不等式⑧的论证，事实上证明了下面(稍强)的结果：

在不超过 n 的任意 $\left[\frac{n+1}{2}\right]+1$ 个正整数中，必有一个被另一个整除.(请注意，若将 $\left[\frac{n+1}{2}\right]+1$ 换为 $\left[\frac{n+1}{2}\right]$，则结论不一定成立.)

本题出自当代著名数学家厄尔迪希(Erdös)之手，极具巧思，值得仔细玩味.

下面的例 6 也与厄尔迪希有关. 其中问题(ii)的证明是厄尔迪希作出的，而(iii)则是他曾经提过的一个问题.

例 6 设 $\{a_1, \cdots, a_n\}$ 是 n 个(不同)正整数的集合，其不同的子集具有不等的元素之和. 证明：

(i) $a_1+\cdots+a_n\geqslant 2^n-1$；

(ii) $a_1^2+\cdots+a_n^2\geqslant\frac{1}{3}(4^n-1)$；

(iii) $\frac{1}{a_1}+\cdots+\frac{1}{a_n}\leqslant 2-\frac{1}{2^{n-1}}$.

证明 由正整数的二进制表示的唯一性可知，数 $a_i=2^{i-1}$ $(i=1, \cdots, n)$ 满足问题中的要求；并且对这样的 a_i，所说的三个不等式均取得等号.

因此，若设 $a_1<\cdots<a_n$，我们可期望证明单项的不等式 $a_i\geqslant 2^{i-1}(i=1, \cdots, n)$. 然而，当 $n\geqslant 4$ 时，这一不等式并不一定成立.(请参看下面的例 7.)

(i) 论证的想法是考虑整体：集合 $\{a_1, \cdots, a_n\}$ 共有 2^n-1 个不同的(非空)子集，(由假设)这些子集中数的和是互不相同的正整数，而 $a_1+\cdots+a_n$ 是其中最大的，故

$$a_1+\cdots+a_n\geqslant 2^n-1.$$

(ii) 这一问题较为困难，其论证需要一个相当别致的技巧：2^n 个数

$$\pm a_1\pm a_2\pm\cdots\pm a_n \tag{9}$$

的平方之和中，乘积项显然两两抵消，故

$$\sum(\pm a_1\pm a_2\pm\cdots\pm a_n)^2=2^n\sum_{i=1}^{n}a_i^2.$$

另一方面，⑨中的数互不相同、均不为 0（这里用到了问题中的假设），并且具有相同的奇偶性，于是

$$\begin{aligned}&\sum(\pm a_1\pm a_2\pm\cdots\pm a_n)^2\\ \geqslant\ &1^2+(-1)^2+3^2+(-3)^2+\cdots+(2^n-1)^2+(1-2^n)^2\\ =\ &\frac{1}{3}(4^n-1)\cdot 2^n.\end{aligned}$$

因此，我们得出

$$\sum_{i=1}^{n}a_i^2\geqslant\frac{1}{3}(4^n-1).$$

(iii) 我们证明

$$\frac{1}{a_1}+\cdots+\frac{1}{a_n}\leqslant 1+\frac{1}{2}+\cdots+\frac{1}{2^{n-1}}.$$

这等价于证明

$$\begin{aligned}&\frac{1}{a_1}+\cdots+\frac{1}{a_n}-\left(1+\frac{1}{2}+\cdots+\frac{1}{2^{n-1}}\right)\\ =\ &\frac{1-a_1}{a_1}+\frac{2-a_2}{2a_2}+\cdots+\frac{2^{n-1}-a_n}{2^{n-1}a_n}\leqslant 0.\end{aligned}$$

不妨设 $a_1<a_2<\cdots<a_n$，并记 $b_i=\dfrac{1}{2^{i-1}a_i}$，$c_i=2^{i-1}-a_i$，$i=1,\cdots,n$. 则

$$b_1 > b_2 > \cdots > b_n. \tag{10}$$

另一方面，对任意 $k(1 \leqslant k \leqslant n)$，集合 $\{a_1, \cdots, a_k\}$ 显然仍具有问题中所说的性质，因此由(i)的结果推出，$a_1 + \cdots + a_k \geqslant 2^k - 1$，即

$$S_k = c_1 + \cdots + c_k \leqslant 0,\ k = 1, 2, \cdots, n. \tag{11}$$

因此，由 Abel 求和，并利用⑩及⑪，得出

$$\begin{aligned}
&\frac{1}{a_1} + \cdots + \frac{1}{a_n} - \left(1 + \frac{1}{2} + \cdots + \frac{1}{2^{n-1}}\right) \\
&= \sum_{i=1}^{n} b_i c_i = b_1 S_1 + b_2 (S_2 - S_1) + \cdots + b_n (S_n - S_{n-1}) \\
&= (b_1 - b_2) S_1 + (b_2 - b_3) S_2 + \cdots + (b_{n-1} - b_n) S_{n-1} + b_n S_n \leqslant 0. \qquad ⑫
\end{aligned}$$

注 4 解答中说的 Abel 求和，实际上是一个恒等式，这是处理和式的一个有用的工具. 我们顺便对此作一简单评述.

设 $\{b_k\}$、$\{c_k\}$ $(1 \leqslant k \leqslant n)$ 是两个数列，若前者相邻项的差以及后者的部分和 $S_k = c_1 + \cdots + c_k (1 \leqslant k \leqslant n)$ 均有适用的信息，则利用恒等式(参见⑫中所示的变形)

$$\begin{aligned}
&b_1 c_1 + \cdots + b_n c_n \\
&= (b_1 - b_2) S_1 + (b_2 - b_3) S_2 + \cdots + (b_{n-1} - b_n) S_{n-1} + b_n S_n,
\end{aligned}$$

可给出和 $\sum_{i=1}^{n} b_i c_i$ 的某种信息.

(iii)的上述证明的入手点是，已知条件蕴含着部分和的信息⑪，因此可期望利用 Abel 求和解决问题.

注 5 例 6 的(iii)可以作极大的推广，限于本书的目的，我们对此不作讨论.

例 7 证明：对 $n \geqslant 4$，存在正整数 $1 \leqslant a_1 < \cdots < a_n < 2^{n-1}$，使得集合 $\{a_1, \cdots, a_n\}$ 的任意两个不同的子集具有不等的元素和.

证明　采用归纳法. $n=4$ 时,集合 $\{3,5,6,7\}$ 符合要求. 设 $n\geqslant 4$ 时已有 n 个正整数 $a_1<a_2<\cdots<a_n<2^{n-1}$ 符合要求,我们将构造 $n+1$ 个正整数 $b_1<b_2<\cdots<b_{n+1}<2^n$ 满足要求.

我们首先可尝试在 $S_n=\{a_1,\cdots,a_n\}$ 中添加适当的正整数 $x<2^n$,使得 $n+1$ 元集合 $S_{n+1}=S_n\cup\{x\}$ 符合要求. 显然,对于 S_{n+1} 的任两个子集,若它们均不含 x,或均含 x,则由归纳假设知,这两个子集的元素之和不相等. 若这两个子集中恰有一个含 x,则 x 必须不是 S_n 中两个子集(包括空集)的元素和之差. 但限制 $x<2^n$,这样的 x 未必存在. 事实上,当 $n=4$ 时便没有这样的解.

(我们顺便提出,若不限制 n 个数中的最大数小于 2^{n-1},则问题极易由归纳法解决:取 a_1 为任一个正整数. 归纳假设 n 个正整数 $a_1<\cdots<a_n$ 已符合要求,我们取 a_{n+1} 为大于 $a_1+\cdots+a_n$ 的任一整数,例如,取 $a_{n+1}=a_1+\cdots+a_n+1$,则前面的讨论表明,$n+1$ 元集合 $\{a_1,\cdots,a_n,a_{n+1}\}$ 符合要求. 特别地,若取 $a_1=1$,则这一构造产生的数为 $1,2,2^2,\cdots,2^{n-1},\cdots$.)

回到原问题,我们首先基于 S_n 作一个与 S_n 具有同样性质的 n 元集合 S_n'(参见本书第 10 讲注 6). 这可以尝试 S_n 的平移或倍乘. 易于看到,前一手续对现在的问题并不适宜(参见前面的讨论);而对所有整数 $t\geqslant 2$,S_n 的倍乘集合 $tS_n=\{ta_1,\cdots,ta_n\}$ 均满足要求. 但为了保证其中的最大数 $ta_n<2^n$,我们取 $t=2$. 现在,我们希望在 n 元集合

$$S_n'=\{2a_1,\cdots,2a_n\}$$

中添加一个正整数 $x<2^n$,使得 $S_n'\cup\{x\}$ 满足要求. 由前面的讨论可知,这要求 x 不能是 S_n' 中两个子集(包括空集)的元素和之差. 但 S_n' 的任一子集的元素和显然都是偶数!(空集的元素和为零.)因此取 x 为小于 2^n 的任一个正奇数均满足要求. 为简单起见,我们总取 $x=1$,由此对 $n=4,5,\cdots$,可递推地给出符合要求的 n 元集合:$\{3,5,6,7\}$,$\{1,2\times 3,2\times 5,2\times 6,2\times 7\}$,$\{1,2\times 1,2^2\times 3,2^2\times 5,2^2\times 6,2^2\times 7\}$,$\cdots$. 证毕.

下面的例 8 也与“子集和”有关.

例 8 证明：对任意不同的 m 个正整数 $a_1, \cdots, a_m$，存在不同的 n 个正整数 $b_1, \cdots, b_n$，其中 $n \leqslant m$，使得

(1) $\{b_1, \cdots, b_n\}$ 的任意两个不同子集的元素之和不相同；

(2) $a_1, \cdots, a_m$ 中每一个数，都是 $\{b_1, \cdots, b_n\}$ 的某个子集的元素之和.

证明 我们注意，若不限制 $n \leqslant m$，则问题甚为容易：将每个 a_i 均写成二进制，并将所有这些表示中出现的(不同的)2 的方幂作为 $b_1, \cdots, b_n$，则由正整数的二进制表示的唯一性，可见 $\{b_1, \cdots, b_n\}$ 的任意两个不同子集的元素之和不相等；而 b_i 的选取则自动保证了(2) 成立，但这样选择的数的个数 n 可能大于 m.

为了解决原问题，我们采用归纳法. 注意到例 7 解答中用到的事实，我们这里对 $N=a_1+\cdots+a_m$ 归纳(而不是对 m 归纳).

当 $N=1$ 时，有 $m=a_1=1$，故 $n=1$，可取 $b_1=1$. 假设结论对所有满足总和小于 N 的不同正整数已成立. 现在考虑(互不相同的)正整数 $a_1, \cdots, a_m$ 满足 $a_1+\cdots+a_m=N$ 的情形.

若 $a_1, \cdots, a_m$ 都是偶数，设 $a_i'=\dfrac{a_i}{2}$ $(1 \leqslant i \leqslant m)$，则 $a_1'+\cdots+a_m'<N$，故由归纳假设知，对 $a_1', \cdots, a_m'$，有 n 个互不相同的正整数 $b_1', \cdots, b_n'$，$n \leqslant m$，满足(1)和(2)，从而 $2b_1', \cdots, 2b_n'$ 是对应于 $a_1, \cdots, a_m$ 的满足(1)和(2)的解.

若 a_i 不全是偶数，不妨设 a_m 是其中最小的奇数，令

$$a_i'=\begin{cases}\dfrac{a_i}{2}, & \text{若 } a_i \text{ 为偶数；}\\ \dfrac{a_i-a_m}{2}, & \text{若 } a_i \text{ 是奇数，且 } i \neq m.\end{cases}$$

则易知 $a_1'+\cdots+a_{m-1}'<N$(这里，若 $a_1', \cdots, a_{m-1}'$ 中有相同的数，则彼此相同的只取其中一个)，由归纳假设，对于 $a_1', \cdots, a_{m-1}'$，存在互不相同的正整数 $b_1', \cdots, b_k'$ $(k \leqslant m-1)$ 满足(1)与(2). 因 a_m

为奇数，故 $a_m \neq 2b_i'$ $(1 \leqslant i \leqslant k)$. 现在不难验证，$k+1$ 个互不相等的正整数 $2b_1'$，…，$2b_k'$，a_m 是对应于 a_1，…，a_m 的满足(1)与(2)的解(注意 $k+1 \leqslant m$)，从而完成了归纳构造.(事实上，由归纳假设易知这 $k+1$ 个数满足(2)；而由集合 $\{b_1', \cdots, b_k'\}$ 满足(1)以及 a_m 为奇数，可知 $\{2b_1', \cdots, 2b_k', a_m\}$ 也满足(1). 请参考例 7 的证明.)

例 9 设 $n \geqslant 1$，S 是一个 n 元集合，$0 \leqslant N \leqslant 2^n$. 证明：可以将 S 的全部子集染黑、白两色之一，使得任意两个白色集的并集仍是白色的，任意两个黑色集的并集仍是黑色的，且黑色子集的个数恰为 N.

证法一 对 n 作归纳法. 当 $n=1$ 时易知结论成立. 假设结论对 n 元集合及 $0 \leqslant N \leqslant 2^n$ 均有符合要求的染色法，现考虑 $n+1$ 元集合 S' 及 $0 \leqslant N' \leqslant 2^{n+1}$ 的情形. 不妨设 $S' = \{1, 2, \cdots, n+1\}$. 我们区分两种情况：

(i) 设 $0 \leqslant N' \leqslant 2^n$，由归纳假设，集合 $S = \{1, 2, \cdots, n\}$ 的全部子集有符合要求的染色法，其中黑色子集的个数为 N'. 显然 S' 的其余未染色的子集都包含 $n+1$，我们将它们都染白色，则 S' 的全部子集都染了黑、白两色之一，且易于验证，这种染法符合问题中的要求(黑色子集为 N' 个).

(ii) 设 $2^n+1 \leqslant N' \leqslant 2^{n+1}$. 记 $N = 2^{n+1} - N'$，则 $0 \leqslant N \leqslant 2^n$. 由归纳假设，集合 $S = \{1, 2, \cdots, n\}$ 的全部子集有符合要求的染色法，其中黑色子集的个数为 N. 我们将 S' 的含 $n+1$ 的所有子集均染白色. 则易见，这样的染色法保证了 S' 的两个黑色子集之并为黑色，两个白色子集之并为白色，但黑色子集的个数为 N，不等于 N'.

现在，我们改换上述的染色：将已染为白色的换成黑色，已染成黑色的换为白色. 不难看到，这样的染色满足问题中的要求(黑色子集的个数为 $2^{n+1} - N = N'$).

这就完成了归纳证明.

证法二 设 $S=\{x_0, x_1, \cdots, x_{n-1}\}$. 对每个 $k(1\leqslant k\leqslant 2^n-1)$ 的(唯一的) 二进制表示

$$k=\varepsilon_0+2\varepsilon_1+\cdots+2^{n-1}\varepsilon_{n-1},\ \varepsilon_i=0,1\ (1\leqslant i\leqslant n-1),$$

令

$$A_k=\{x_i\mid \varepsilon_i=1,\ 1\leqslant i\leqslant n-1\}.$$

则易知这建立了不超过 2^n-1 的正整数与 S 的全部非空子集的一个一一对应.

当 $N=0$ 或 2^n 时易知结论成立. 当 $1\leqslant N\leqslant 2^n-1$ 时,设 N 的二进制表示为

$$N=2^{a_1}+\cdots+2^{a_m},$$

则 $0\leqslant a_i\leqslant n-1$, a_i 互不相同.

我们按下列规则将 S 的全体子集染色:将空集染上白色. 对 $1\leqslant k\leqslant 2^n-1$, 若 k 的二进制表示中 2 的最高次幂为某个 $2^{a_i}(1\leqslant i\leqslant m)$,则将 k 对应的子集 A_k 染上黑色,否则将 A_k 染上白色. 则这一染色法符合问题的要求.

事实上,设 A_k 与 A_l 是两个黑色子集,且 k 与 l 的二进制表示中 2 的最高次幂分别为 2^{a_i} 及 2^{a_j},设 $A_k\cup A_l$ 所对应的整数为 t,则 t 的二进制展开中 2 的最高次幂为 $\max(2^{a_i}, 2^{a_j})$,从而是 2^{a_i} 或 2^{a_j},故 A_t 染黑色,即 $A_k\cup A_l$ 为黑色. 同样可知,两个白色子集的并仍是白色子集.

另一方面,给定 $0\leqslant a_i\leqslant n-1$, 则二进制表示中最高次幂恰为 2^{a_i} 的 k $(1\leqslant k\leqslant 2^n-1)$,显然共有 2^{a_i} 个($j>a_i$ 时,$\varepsilon_j=0$; $\varepsilon_{a_i}=1$;而对 $0\leqslant j\leqslant a_i-1$, ε_j 可任意取 0 或 1,共 2^{a_i} 个取法). 因此黑色子集的个数恰为 $2^{a_1}+2^{a_2}+\cdots+2^{a_m}$, 即 N 个. 证毕.

本题的两种解法,表现了(与正整数 n 有关的)存在性命题 $P(n)$的两种精神的构造:归纳(递推)构造及通式构造. (这有些类

似于数列的两种基本表示:递推公式及通项公式.)证法一从 $n=1$ 时的染色法,递推地作出了每个 n 元集合的染色法;而证法二则给出了适用所有 n 元集合的一种染色法.(请注意,符合要求的染色法一般并不唯一,这不难从证法一看出来.)

例 7 与例 8 均采用了归纳构造(有兴趣的读者可试试是否能作出通式的构造). 下面例 10 的两种解法,采用的均是通式构造.

例 10 证明:存在常数 $c>0$,使得对所有 $n\geqslant 4$,集合 $S=\{1,\cdots,n\}$ 有一个子集 A_n,满足 $|A_n|\leqslant c\sqrt{n}$,而 S 中每个不小于 2 的数均可表示为 A_n 中两个(可以相同的)数之和.

证明 设 T_0 是不超过 n,其二进制表示中只含 2 的偶次幂的正整数之集,T_1 是不超过 n,其二进制表示中只含 2 的奇次幂的正整数之集. 令 $A_n=T_0\cup T_1$. 由于每个正整数可表示为 2 的幂的和,因此 S 中不是 2 的幂的正整数可表示为 $T_0\cup T_1$ 中两个数之和. 而对于 $2^k\in S\ (k\geqslant 1)$,由 $2^{k-1}\in T_0\cup T_1$,以及 $2^k=2^{k-1}+2^{k-1}$,可知 2^k 可表示为 $T_0\cup T_1$ 中两个数之和. 因此 S 中每个不小于 2 的数可表示为 A_n 中两个数的和.

现在估计 A_n 中元素的个数.

由定义,T_0 中的数具有形式 $2^{2\alpha_1}+\cdots+2^{2\alpha_k}$,其中 $0\leqslant\alpha_1<\cdots<\alpha_k$,$k\geqslant 1$. 由正整数的二进制表示的唯一性可知,$T_0$ 与 $2^{\alpha_1}+\cdots+2^{\alpha_k}$ 组成的数集 T_0' 一一对应,故 $|T_0|=|T_0'|$.

另一方面,显然 $2^{2\alpha_k}\leqslant n$,故 $2^{\alpha_k}\leqslant\sqrt{n}$. 因此

$$2^{\alpha_1}+\cdots+2^{\alpha_k}\leqslant 2^{\alpha_k+1}-1<2^{\alpha_k+1}\leqslant 2\sqrt{n},$$

即 T_0' 中的数均不超过 $2\sqrt{n}$,从而 $|T_0'|\leqslant 2\sqrt{n}$,故 $|T_0|\leqslant 2\sqrt{n}$.

同样,T_1 中的数具有形式 $2^{2\beta_1+1}+\cdots+2^{2\beta_l+1}$,$0\leqslant\beta_1<\cdots<\beta_l$,$l\geqslant 1$. 由 $2^{2\beta_l+1}\leqslant n$,得 $2^{\beta_l}\leqslant\sqrt{\frac{n}{2}}$. 从而

$$2^{\beta_1}+\cdots+2^{\beta_l}<2^{\beta_l+1}\leqslant\sqrt{2n}.$$

因此 $|T_1|\leqslant\sqrt{2n}$. 故 $|A_n|=|T_0|+|T_1|\leqslant(2+\sqrt{2})\sqrt{n}$.

本题也可采用下面的构造(与上述的完全不同):

设 t 是一个(待定)整数, $2\leqslant t<n$. 设

$$T_0=\{1,2,\cdots,t-1\},\ T_1=\left\{t,2t,\cdots,\left[\frac{n}{t}\right]t\right\},$$

并设 $A_n=T_0\cup T_1$,我们首先证明,S 中的不小于 2 的数均可表示为 A_n 中的两个数之和.

事实上,设 $x\in S$, $x>t$,且 x 不被 t 整除. 则由带余除法,x 可表示为 $x=kt+r$,这里 $1\leqslant r\leqslant t-1$, $1\leqslant k\leqslant\left[\frac{x}{t}\right]$,即 $r\in T_0$, $kt\in T_1$,故 x 是 A_n 中两个数之和. 若 $2\leqslant x\leqslant t$,则 x 是 T_0 中两个数的和. 若 $x>t$ 且被 t 整除,则易知 x 是 T_1 中两个数的和. 故上述断言得证.

现在我们取参数 $t=[\sqrt{n}]+1$,以使 $|A_n|$ 尽可能小,得到

$$\begin{aligned}|A_n|&=|T_0|+|T_1|=t-1+\left[\frac{n}{t}\right]\\&\leqslant\frac{n}{t}+t-1\leqslant\frac{n}{\sqrt{n}}+(\sqrt{n}+1)-1=2\sqrt{n}.\end{aligned}$$

注 6 例 10 的要点在于 $|A_n|$ 的上界 $c\sqrt{n}$(若只要求 A_n 满足所说的第二个要求,则问题很平凡,取 $A_n=S$ 即可). 我们注意,这一上界从(关于 n 的)量级而言,已是最佳的结果. 因为不难证明,若 A_n 是 S 的一个子集,使得 S 中任意不小于 2 的数可表示为 A_n 中两个数之和,则必有 $|A_n|\geqslant\sqrt{2(n-1)}$.

事实上,一方面,每个 $k(2\leqslant k\leqslant n)$ 可表示为 $k=a+a'$, a, $a'\in S$,这样的 k 共有 $n-1$ 个;另一方面,数对 (a,a'),其中 $a\leqslant a'$,共有 $\binom{|A_n|}{2}+|A_n|$ 个. 因此

$$\binom{|A_n|}{2}+|A_n|\geqslant n-1,$$

即$|A_n|(|A_n|+1)\geqslant 2(n-1)$，由此易得$|A_n|\geqslant\sqrt{2(n-1)}$.

例 11 设A是n^2元集合($n\geqslant 2$). F是A的一个子集族，每个子集有n个元，F中任意两个集合至多有一个公共元. 证明：$|F|\leqslant n^2+n$.

证法一 对$x\in A$，设$\mathrm{d}(x)$是F中含x的集合B的个数. 则有(参见第17讲例4中的④)

$$\sum_{x\in A}\mathrm{d}(x)=\sum_{B\in F}|B|=n|F|. \tag{13}$$

我们将给出每个单项$\mathrm{d}(x)$的上界，进而产生上式左边和的上界，由此即得$|F|$的上界.

设F中含x的集合为$B_1,\cdots,B_{\mathrm{d}(x)}$，则$B_1\backslash\{x\},\cdots,B_{\mathrm{d}(x)}\backslash\{x\}$是$A\backslash\{x\}$的互不相交的子集(因任意两个不同的$B_i$、$B_j$只有一个公共元$x$). 故

$$\sum_{i=1}^{\mathrm{d}(x)}|B_i\backslash x|\leqslant|A\backslash\{x\}|=n^2-1. \tag{14}$$

但每个B_i均是n元集，故上式左端和中的每个单项都等于$n-1$. 由此得$(n-1)\mathrm{d}(x)\leqslant n^2-1$，即$\mathrm{d}(x)\leqslant n+1$，故⑬的左边的和$\leqslant n^2(n+1)$，从而$|F|\leqslant n^2+n$. 证毕.

等式⑬及不等式⑭，均是考虑某种整体的产物. 由⑬与⑭，结合相关的单项的信息，产生所需的结果. “整体”与“单项”在上述证明中相辅相成，这也正是组合数学中的基本的手法.

证法二 设$F=\{B_1,\cdots,B_m\}$. 我们用两种方式计数有序对$(B_i,\{x,y\})$的个数，其中$\{x,y\}\subseteq B_i$，$1\leqslant i\leqslant m$.

一方面，对固定的B_i，由于$|B_i|=n$，故$\{x,y\}\subseteq B_i$有$\binom{n}{2}$种

选取方式，而 B_i 有 m 种取法，故所说的有序对有 $m\binom{n}{2}$ 个.

另一方面，二元集 $\{x, y\}$ 共有 $\binom{|A|}{2}=\binom{n^2}{2}$ 种取法，而每一个这样的二元集至多在一个 B_i 中（由于任两个不同的 B_i，B_j 至多有一个公共元），因此所说的有序对 $\leqslant\binom{n^2}{2}$.

综合两个方面，得出 $m\binom{n}{2}\leqslant\binom{n^2}{2}$，即 $|F|=m\leqslant n^2+n$. 证毕.

证法二的方法，以两种方式计数一个适当的（分量间有某种关联的）有序组，进而产生所需的结果. 下面的例 12，看起来较为复杂，但用这种方法处理，并不很困难.

例 12 一所大学有 n 个学生（n 为大于 1 的奇数），一些学生一起成立了若干个俱乐部（同一个学生可以属于不同的俱乐部），一些俱乐部一起成立了若干个社团（一个俱乐部可以属于不同的社团）. 假设下面的条件满足：

（1）每一对学生都恰属于一个俱乐部；

（2）对于每个学生及每个社团，这位学生恰属于这个社团里的一个俱乐部；

（3）每个俱乐部中的学生数均为（大于 1 的）奇数，且具有 $2m+1$（$m>0$）个学生的俱乐部恰属于 m 个社团.

试求社团的个数 k 的所有可能的值.

解 用 a、C、S 分别表示一个学生，一个俱乐部，及一个社团. 我们用两种方式计数有序三元组 (a, C, S) 的个数，其中 $a\in C$，$C\in S$.

一方面，固定一个学生 a 及一个社团 S，由条件（2），有唯一的 C，使 $a\in C$，且 $C\in S$. 又因为有序二元组 (a, S) 有 nk 种取法，故所说的三元组共有 nk 个.

另一方面，固定一个俱乐部 C，其中的学生数目记作 $|C|$，则由

条件(3)可知，C 恰属于 $\frac{|C|-1}{2}$ 个社团. 因此，包含俱乐部 C 的符合要求的三元组共有 $\frac{|C|(|C|-1)}{2}=\binom{|C|}{2}$ 个. 设 M 为所有俱乐部的集合，我们求得，所说的三元组共有 $\sum_{C\in M}\binom{|C|}{2}$ 个.

我们注意，$\binom{|C|}{2}$ 恰是俱乐部 C 中产生的(无序)学生对的个数，故由条件(1)推知

$$\sum_{C\in M}\binom{|C|}{2}=\binom{n}{2}.$$

综合上述两个方面，得出 $nk=\binom{n}{2}$，故 $k=\frac{n-1}{2}$. 又当所有学生同属一个俱乐部，而这俱乐部属于 $\frac{n-1}{2}$ 个社团时，问题中的条件均能满足. 因此 $k=\frac{n-1}{2}$ 是唯一的可能的解.

例 13 设 a、b、m、n 都是自然数. 若 $m\times n$ 的(大)矩形可划分为若干个 $a\times b$ 的矩形的并(小矩形的边与大矩形的边平行)，则 m、n 中必有一个为 a 的倍数，也必有一个为 b 的倍数.

证明 因 $a\times b$ 的矩形可划分为 $a\times 1$ 的矩形之并，因此，我们只要证明，若 $m\times n$ 的矩形可划分为 $a\times 1$ 的矩形之并，则 m、n 中必有一个为 a 的倍数(对称地，可证明关于 b 的结论).

将大矩形放置于水平位置，并将它划分为 mn 个 1×1 的单位正方形. 解答的基本精神是，在每个单位正方形中赋予适当的数值，以两种方式计算这 mn 个数的和，比较这两种结果，导出求证的结论.

由于 $m\times n$ 矩形可划分为若干个 $a\times 1$ 小矩形的并，故这 mn 个数的总和 S 自然地分为了相应的“单项”之和，这里的一个“单项”是一个 $a\times 1$ 小矩形中 a 个数的和. 我们首先希望各个“单项”

的值均相同，由此 S 即有一个简明的结果.

由于没有 $a\times 1$ 小矩形的位置信息，因此，为了上述目的，我们希望每一行(或列)中，一个 $a\times 1$ 小矩形中的数之和具有平移不变性，即在任一行(列)中以周期 a 循环地放置 n(或 m)个数. 此外，为了使 $a\times 1$ 小矩形中的数易于求和，我们可尝试使任一行(列)中的数成等比数列.

对 $1\leqslant k\leqslant m$，设第 k 行中的数(从左至右)为 c_kz，c_kz^2，…，c_kz^a，c_kz^{a+1}，….由这一数列周期为 a，我们特别地有 $c_kz=c_kz^{a+1}$，即 $z^a=1$，故 z 为一个 a 次单位根.

现在对 $1\leqslant l\leqslant n$，第 l 列中的 m 个数(由上至下)为 c_1z^l，c_2z^l，…，c_az^l，$c_{a+1}z^l$，….由它们成周期为 a 的等比数列，可推知 $c_j=z_1^j$，$j=1,2,\cdots,m$，这里 z_1 也是一个 a 次单位根.

由于对任一个 a 次单位根 $S\neq 1$，有 $1+S+\cdots+S^{a-1}=0$，故若取 z，z_1 均不等于 1，则由上述讨论知，任一个 $a\times 1$ 小矩形中 a 个数的和均为零，从而大矩形中的 mn 个数之和 $S=0$，这一结果与 a、m、n 均无关(请注意，若取 $z=z_1=1$，则易于导出 $\dfrac{mn}{a}$ 为整数，不能解决问题).

现在，我们以另一种方式计算所放置的数的总和 S. 因为第 k 行与第 l 列交叉的 1×1 正方形放置的数为 $z^kz_1^l$($1\leqslant k\leqslant m$，$1\leqslant l\leqslant n$)，故所有这些数的和

$$S=\sum_{k=1}^{m}\sum_{l=1}^{n}z^kz_1^l=\Big(\sum_{k=1}^{m}z^k\Big)\Big(\sum_{l=1}^{n}z_1^l\Big)$$

$$=\frac{z(z^m-1)}{z-1}\cdot\frac{z_1(z_1^n-1)}{z_1-1}\text{(这与 } a\text{、}m\text{、}n\text{ 均有关).}$$

比较前面的结果，我们得出 $(z^m-1)(z_1^n-1)=0$，故

$$z^m-1=0,\text{或 } z_1^n-1=0.$$

最后，我们取 $z=z_1=\mathrm{e}^{\frac{2\pi i}{a}}$，则由上式便导出 $a\mid m$ 或 $a\mid n$.(实

际上，将 z 与 z_1 取为任一个本原的 a 次单位根，均能产生所需的结果.）

例 14 给定四个全等的直角三角形. 可对它们作如下的操作：从直角顶点向斜边作垂线，将这个三角形分成两个直角三角形. 对产生的新的直角三角形可反复进行这种操作. 证明：无论怎样进行操作，在所得的三角形中必有两个全等.

证明 我们可设开始给定的直角三角形的斜边长为 1，并记两直角边为 a、b. 显然可假定 $a \neq b$（否则结论平凡地成立）.

易于得知，经过若干次操作得出的直角三角形，与原先给定的三角形相似，且相似比为 $a^m b^n$，这里 m、n 为某两个非负整数，我们将这一个三角形对应于有序数对 (m, n).

将对应于 (m, n) 的三角形操作一次，则得出的两个三角形对应的数对为 $(m+1, n)$ 及 $(m, n+1)$. 由于

$$\frac{1}{2^{m+n}} = \frac{1}{2^{(m+1)+n}} + \frac{1}{2^{m+(n+1)}},$$

故若将对应于 (m, n) 的三角形对应于权 $\frac{1}{2^{m+n}}$，则所有三角形的权的总和在操作下不变！

开始时，三角形的权之和为 4. 若在操作的某个阶段没有两个三角形全等，则所有三角形对应的数对 (m, n) 彼此互不相等. 设其中 $m+n$ 的最大值为 N. 注意，对非负整数 l，方程 $m+n=l$ 的有序非负整数解 (m, n) 的个数为 $l+1$. 故此阶段所有三角形的权之和至多为

$$\begin{aligned}\sum_{l=0}^{N} \frac{l+1}{2^{l+1}} &= \frac{1}{2} + \sum_{l=0}^{N} \frac{l}{2^{l+1}} + \sum_{l=1}^{N} \frac{1}{2^{l+1}} \\ &< 1 + 2 \times 1 + 2 \times \frac{1}{2} = 4,\end{aligned}$$

这与前面所说的权之和是不变量 4 矛盾. 因此操作的任何阶段总有两个三角形对应的数对相同，从而这两个三角形全等. 证毕.

这一解答的要点是考虑某个与问题有关的量，一方面，它是操作下的不变量；另一方面，若求证的结论不成立，则这个量将发生改变，产生矛盾.

例 15 数列

$$1，0，1，0，1，0，3，\cdots$$

中，(从第七项起)每一项等于它前面六项之和的末位数字. 证明：数列中没有连续的六项构成

(i) 1，7，0，0，7，1；(ii) 0，1，0，1，0，1.

证明 考虑数列$\{a_n\}(n\geqslant 1)$，其中前六项依次为 1，0，1，0，1，0，而对 $n\geqslant 1$，

$$a_{n+6}=a_{n+5}+\cdots+a_{n+1}+a_n. \tag{15}$$

显然，问题中的数列即是将$\{a_n\}$中各项模 10 产生的数列.

(i)甚为容易. 因 2 是 10 的约数，在模 10 的基础上进一步模 2，(用归纳法)易知，数列$\{a_n\}$成为周期数列 1，0，1，0，1，0，1，0，…. 由此可见，(i)中的数不能成为数列中的连续六项.

容易看到，上面的方法对(ii)中的数不能奏效. 事实上，这一问题困难得多.

论证的想法是构造一个不变量：将数列$\{a_n\}(n\geqslant 1)$中连续六项 a_n，a_{n+1}，…，a_{n+5}，对应一个数 $f(a_n，a_{n+1}，\cdots，a_{n+5})$，使得它模 10 保持不变(对所有的 $n\geqslant 1$)，但

$$f(1，0，1，0，1，0)\not\equiv f(0，1，0，1，0，1)(\mathrm{mod}\ 10), \tag{16}$$

由此就证明了问题中的结论.

因为$\{a_n\}$满足线性递推关系⑮，我们可以期望有一个线性函数的不变量，即尝试着取

$$f(a_n，a_{n+1}，\cdots，a_{n+5})=x_1a_n+x_2a_{n+1}+\cdots+x_6a_{n+5}, \tag{17}$$

其中 x_1，…，x_6 是待定的整数，模 10 不全为零.

利用⑮，我们有

$$f(a_{n+1}, a_{n+2}, \cdots, a_{n+6}) - f(a_n, a_{n+1}, \cdots, a_{n+5})$$

$$= (x_6 - x_1)a_n + (x_6 + x_1 - x_2)a_{n+1} + (x_6 + x_2 - x_3)a_{n+2}$$

$$+ (x_6 + x_3 - x_4)a_{n+3} + (x_6 + x_4 - x_5)a_{n+4} + x_5 a_{n+5}.$$

显然,如上选取的 f 模 10 不变,当且仅当 $x_1, \cdots, x_6$ 满足

$$x_6 \equiv x_1,\ x_6 + x_i - x_{i+1} \equiv 0\ (1 \leqslant i \leqslant 4),\ x_5 \equiv 0\ (\mathrm{mod}\ 10). \tag{18}$$

易于得知,⑱有一组解(模 10 不全为零):

$$x_1 = 2,\ x_2 = 4,\ x_3 = 6,\ x_4 = 8,\ x_5 = 10,\ x_6 = 12;$$

并且易验证,相应于⑰确定的 f 满足⑯. 这就完成了证明.

注 7 因为 $10 = 2 \times 5$,故模 10 不变,等价于模 2 和模 5 都不变. 然而,读者可验证,数列 $\{a_n\}$ 模 2 没有非平凡的、形如⑯那样的不变量(即这种不变量中,诸系数 x_i 模 2 都是零). 因此,就本题而言,形如⑯的模 5 的不变量,与模 10 的不变量的实质相同.

注 8 数列 $\{a_n\}$ 模 2 后成为周期数列,这一点并非偶然. 实际上,给定 $m > 1$,若 $\{x_n\}(n \geqslant 1)$ 是由递推公式

$$x_{n+k} = f(x_{n+k-1}, \cdots, x_{n+1}, x_n)$$

决定的整数数列,其中 f 是 k 元整系数多项式,初值 $x_1, \cdots, x_k$ 为给定的整数. 则 $\{x_n\}$ 模 m 后终将成为周期数列.

为了证明,我们用 $\overline{x}_i$ 表示 x_i 被 m 除得的余数 $(0 \leqslant \overline{x}_i < m)$. 考虑有序的 k 元数组

$$A_n = \langle \overline{x}_n, \overline{x}_{n+1}, \cdots, \overline{x}_{n+k-1} \rangle\ (n = 1, 2, \cdots).$$

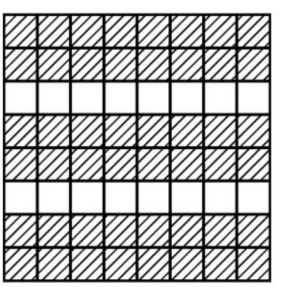
由于每个 $\overline{x}_i$ 至多有 m 个值,故互不相同的数组 A_n 至多有 m^k 个. 因此,在 $m^k + 1$ 个 k 元数组 $A_1, A_2, \cdots, A_{m^k+1}$ 中,必有两个完全相同. 设 $A_i = A_j (i < j)$,即

$$\overline{x}_{i+t} = \overline{x}_{j+t} (t = 0, 1, \cdots, k-1).$$

再由$\{x_n\}$的递推公式及同余式的基本性质易推出，当$t=k$时，亦有$\overline{x}_{i+k}=\overline{x}_{j+k}$. 于是用归纳法即可证明，对任意$t\geqslant 0$，都有$\overline{x}_{i+t}=\overline{x}_{j+t}$. 这意味着，数列$\{\overline{x}_n\}$从第$i$项开始，每$j-i$个一组，将循环出现(但请注意，$\{\overline{x}_n\}$未必是纯周期的数列).

我们顺便提一下，就本题而言，因$\{a_n\}$模10是周期数列，若能确定模10后数列的最小周期(及其中所有项)，则易于判别给定的数能否作为其连续的项. 但实际上，本题中数列的最小周期相当地大，因而这一方法并非是实效的方法.

例16 有一张8×8的方格表，表中填上64个非负整数(每格一数). 所谓一次操作是指：从表中任取一个3×3或4×4的子方格表(所取的各行、各列必须是相连的)，并将其中的9个或16个数都加1. 证明：存在一张非负整数的方格表，使得无论怎样操作都不能将表中的64个数全变为10的倍数.



例16

证明 考虑图中带阴影线的48个方格. 容易验证，无论取哪个3×3或4×4子方格表，其中总含有偶数个带阴影线的小方格. 因此，再进行一次操作，总使带阴影方格中的48个数之和增加一个偶数. 这样，如果开始在表中填数时，使这48个数之和为奇数，则无论怎样操作，这48个数之和永远是奇数. 而如果方格表中的数都是10的倍数时，这48个数之和应为偶数. 因此上面作出的数表符合问题的要求.

这一解法，构造与不变量相辅相成，值得仔细玩味.

本题也可采用下面的方法：由于一个数为10的倍数即是其末位数为0，因此问题等价于：在填上64个一位数(0，1，…，9)的8×8方格表中，一定有一个，使得无论对它怎样操作，都不能将表中数都变成“0”(凡一个数变成二位数后，就将它改成末位数，换句话说，我们按模10考虑问题). 或者反过来看：从一张全0数表(即64个数都是0)出发，不可能得到上述的所有方格表.

事实上，由于每个方格可填 10 个数之一，故 8×8 的数表共有 10^{64} 种.

另一方面，8×8 的表格中共有 $6\times6=36$ 个 3×3 子方格表，以及 $5\times5=25$ 个 4×4 子方格表，即总共有 61 个子方格表. 又在模 10 的意义下，每张子方格表只能进行 10 次操作. 所以，从全 0 表出发，最多只能得到 10^{61} 种不同的(一位数)数表.

因 $10^{61}<10^{64}$，故必有某个 8×8 方格表不能从全 0 表得到. 证毕.

上面的方法，称为计数论证. 一方面计数事物的总数，另一方面，估计不符合某种要求的事物的个数. 如果后者小于前者，那么就必然存在符合某种要求的事物(参考第 1 讲注 7).

例 17 证明：可以将整数 1，2，…，1986 涂上两种颜色(即分为两类)，使得同一种颜色的数不能组成一个有 18 项的等差数列.

证明 我们首先估计从 1，2，…，1986 中选出 18 个数组成等差数列的种数.

设等差数列的首项为 a，公差为 d，则 $a+17d\leqslant1986$，因此 $d\leqslant\left[\dfrac{1986-a}{17}\right]$.

于是，对每个固定的 a，有 $\left[\dfrac{1986-a}{17}\right]$ 个以 a 为首项的、18 项的等差数列. 又由于 $a\leqslant1986-17=1969$，故所求的种数是

$$S=\sum_{a=1}^{1969}\left[\frac{1986-a}{17}\right].$$

由此易知

$$S\leqslant\frac{1}{17}\sum_{a=1}^{1969}(1986-a)=\frac{1}{17}\times1969\times1001<\frac{2^{11}\times2^{10}}{2^4}=2^{17}.$$

现在将 1，2，…，1986 涂两种颜色，由于每个数都有两种不同的涂法，故总的涂色方式为 2^{1986}.

另一方面，含有同色的、18 项的等差数列的涂法不超过 $2\times$

$S\times 2^{1986-18}=S\cdot 2^{1969}$ 种. 这是因为，选出 18 项成等差数列的方法数为 S；这 18 个数同色，有两种涂法；其余的 $1986-18$ 个数有 $2^{1986-18}$ 种涂色法，由乘法原理，得出所说的上界（涂法重复的计算在内）.

由于 $S<2^{17}$，因此 $S\times 2^{1969}<2^{1986}$，这表明，并非所有的涂法中都包含 18 项同色的等差数列. 证毕.

本题与组合数论中著名的**范德瓦尔登(Van der Waerden)定理**有点关联. 这一定理断言，对任意给定的整数 $l\geqslant 3$，存在正整数 n_0（与 l 有关），使得当 $n\geqslant n_0$ 时，将 $1, 2, \cdots, n$ 任意涂两种颜色，都一定有一个项数为 l 的同色等差数列.

如果记 W_l 为具有上述性质的最小整数 n_0，则易知 $W_3=9$. 本题表明 $W_{18}>1986$，实际上，更深入的方法能将这一下界作极大的改进，但目前尚不能求出 W_{18}，更不用说一般的 W_l 了（请读者千万不要轻易地碰这个艰难的问题）.

范德瓦尔登定理可看作是一个拉姆塞型结果（参考第 18 讲注 4），其大意是说，当某一个系统的元素足够多时，就具有指定的性质或规律. 数学竞赛中有不少这样的问题，我们再举一个例子.

例 18 在一个由 $mn+1$ 个互不相同的实数组成的数列 $a_1, a_2, \cdots, a_{mn+1}$ 中，或者存在一个项数大于 m 的递增子数列，或者存在一个项数大于 n 的递减子数列.（所谓子数列，是指取自原数列里的一些项，并且按原数列中同样的顺序写成的一个数列.）

证明 我们用 l_i^+ 表示从 a_i 开始的最长的递增子数列的项数，l_i^- 表示从 a_i 开始的最长的递减子数列的项数 $(i=1, 2, \cdots, mn+1)$. 如果结论不对，则对所有的 i $(1\leqslant i\leqslant mn+1)$ 有 $l_i^+\leqslant m$，且 $l_i^-\leqslant n$，下面来导出矛盾.

我们将集合 $A=\{a_1, \cdots, a_{mn+1}\}$ 中每个元素 a_i 与一个有序数对相对应：$f(a_i)=(l_i^+, l_i^-)$. 由于 $l_i^+\leqslant m$ 及 $l_i^-\leqslant n$，故 f 是 A 到 $B=\{(k, l)\mid 1\leqslant k\leqslant m, 1\leqslant l\leqslant n\}$ 的一个映射，我们证明这

是一个单射，即对于 $a_i \neq a_j$，有 $f(a_i) \neq f(a_j)$.

不妨设 $i<j$. 当 $a_i<a_j$ 时，易知 $l_i^+ > l_j^+$，因为至少可以加一个项(即 a_i)到从 a_j 开始的长度最大的递增子数列的左边，从而得到一个从 a_i 开始的长度大于 l_j^+ 的递增子数列；同样，当 $a_i > a_j$ 时，有 $l_i^- > l_j^-$. 因此，$a_i \neq a_j$ 就意味着 $(l_i^+, l_i^-) \neq (l_j^+, l_j^-)$，因为这两个有序数对中至少有一个坐标是不同的，从而 $f(a_i) \neq f(a_j)$. 这就证明了 f 是单射，从而 $|A| \leqslant |B|$，即 $mn+1 \leqslant mn$，这当然是不可能的. 证毕.

我们提一下，例 18 中的 m 与 n 显然是对称的；而若将数 $mn+1$ 换为 mn，则结论便不一定成立.

上述解法的要点，是数列中的每一项都对应一个有序数对，并且这一对应是一个单射(因此，若结论不对，则由原像集合的元素个数不超过像集的元素个数，产生矛盾. 参见第 3 讲中注 4).

根据问题的特点，产生一个映射，这是组合数学中的非常基本的方法，下面的例子也是这样做的.

例 19 设 A、B 是由正整数构成的有限集合，$|A|=m$，$|B|=n$，且 A 满足下面的条件：

若 $x+y=u+v$ $(x, y, u, v \in A)$，则 $x=u$，$y=v$，或 $x=v$，$y=u$. 证明：$|A+B| \geqslant \dfrac{m^2 n}{m+n-1}$，这里 $A+B=\{a+b \mid a \in A, b \in B\}$.

证明 记 $t=|A+B|$，并记所有的和 $a+b$ $(a \in A, b \in B)$ 中，互不相同的值为 $x_1, \cdots, x_t$. 对 $1 \leqslant k \leqslant t$，令

$$A_k = \{a \mid a \in A, \text{使得 } a+b=x_k, \text{对某个 } b \in B\}$$

(注意 $A_k \neq \varnothing$). 由于所有的和 $a+b(a \in A, b \in B)$ 共 $|A| \cdot |B|$ 个，由 A_k 的定义知其中等于 x_k 的和恰为 $|A_k|$ 个 $(k=1, 2, \cdots, t)$. 因此

$$\sum_{k=1}^{t} |A_k| = |A| \cdot |B| = mn.$$

当 $|A_k| > 1$ 时，A_k 中的数共产生 $\binom{|A_k|}{2}$ 个有序数对 (a, a')，其中 $a, a' \in A_k$，$a > a'$. 每一个这样的数对，由 A_k 的定义，都唯一对应一个有序数对 (b, b')，其中 $b, b' \in B$，$b < b'$，满足

$$a + b = a' + b' = x_k.$$

我们现在证明，如上所说的对应是一个单射！

显然，若 (a, a') 与 (a_1, a_1') 均由 A_k 产生，则它们如上对应的 (b, b') 与 (b_1, b_1') 不同.

进一步我们证明，若 (a, a') 与 (a_1, a_1') 分别由 A_k 及 A_i 产生，则它们对应的 (b, b') 与 (b_1, b_1') 也不同.

事实上，当 $(a, a') = (a_1, a_1')$ 时，所说的断言显然成立（因 $x_i \neq x_k$）. 当 $(a, a') \neq (a_1, a_1')$ 时，若 $(b, b') = (b_1, b_1')$，则由

$$\begin{cases} a + b = a' + b', \\ a_1 + b_1 = a_1' + b_1', \end{cases}$$

得出 $a - a_1 = a' - a_1'$，即 $a + a_1' = a_1 + a'$，故由集合 A 的性质推出 $a = a_1$，$a' = a_1'$（注意 $a > a'$，$a_1 > a_1'$），与假设相违，故此时所说的断言也成立.

由上述结果，并注意有序数对 $(b, b')(b < b')$ 共有 $\binom{|B|}{2} = \binom{n}{2}$ 个，我们得出

$$\sum_{k=1}^{t} \binom{|A_k|}{2} \leqslant \binom{n}{2}.$$

由此，利用柯西不等式，易得

$$\binom{n}{2} \geqslant \sum_{k=1}^{t} \frac{|A_k|^2}{2} - \frac{1}{2}\sum_{k=1}^{t} |A_k|$$

$$\geqslant \frac{1}{2t}\Big(\sum_{k=1}^{t} |A_k|\Big)^2 - \frac{1}{2}\sum_{k=1}^{t} |A_k| = \frac{(mn)^2}{2t} - \frac{mn}{2},$$

解得 $t \geqslant \dfrac{m^2 n}{m+n-1}$，这就证明了结论.

专题2

数 论 问 题

本讲再介绍数论中的一些问题.

数论问题,尤其是较困难的数论问题,解决它们不仅需要技巧,更重要的是需要好的想法,以及对问题涉及的概念与背景的把握和理解.

例1 设 a、b 是互素的正整数,证明:数列 $\{bx+a\}$ $(x=0,1,\cdots)$ 中有一个无穷子列,其中的项两两互素.(关于子列的定义,请见前一讲例 18.)

证明 我们证明更强的结论:所说的数列中有一个无穷子列,其中的项两两互素,且均和 a 互素.下面归纳地定义一个这样的数列.

取 $u_1=a+b$,由于 $(a,b)=1$,故 $(u_1,a)=1$.若 $u_1<\cdots<u_n$ 已确定,使得它们两两互素且与 a 互素,则取

$$u_{n+1}=b(u_1\cdots u_n)+a,$$

显然 u_{n+1} 是数列 $\{a+bx\}$ $(x\geqslant 0)$ 中的一项且 $u_{n+1}>u_n$.又现在有

$$\begin{aligned}(u_{n+1},u_i)&=(bu_1\cdots u_n+a,u_i)\\&=(a,u_i)=1\quad(i=1,\cdots,n),\end{aligned}$$

以及

$$(u_{n+1},a)=(bu_1\cdots u_n,a)=1.$$

故 u_{n+1} 与 a 互素且 $u_1,\cdots,u_n,u_{n+1}$ 两两互素.按归纳法,我们得出了一个符合要求的无穷子列.

注1 一般性的、更强的命题可能更容易解决.因为问题的

(恰当的)一般性提法可能更容易揭示其内在规律,而特殊的问题中,这些本质的属性常常被特殊性掩盖.“将问题一般化”的例子,数学中俯拾皆是,我们不多讨论.

例 1 的上述方法,用归纳法递推地构造一个子列,要点是将结论加强.归纳论证中,由于命题加强后,归纳假设也加强了,使我们具有更多的条件完成归纳证明,这从例 1 的解法中可看得很清楚.这种“加强归纳假设”的手法,用处极多.

注 2 何时以及怎样加强命题,当然得针对具体问题而定,这往往需要对问题作反复的探索、尝试才能实现.事实上,提出并解决一个恰当的“加强命题”可能远非易事.

首先,“更强的命题”不一定是正确的.其次,即使命题是正确的,也可能极难证明,甚至是目前人们尚不能解决的难题.下面是一个容易说明的例子:

证明:数列 $\{2^n-1\}$ $(n=1,2,\cdots)$ 中有一个无穷子列,其中的数两两互素.

这一问题并不困难(参见第 7 讲练习题中第 3 题).然而,如果试图证明(更强的命题)“$\{2^n-1\}$ $(n=1,2,\cdots)$ 中有无穷多个素数”,则需要一种非凡的勇气:将一个经典难题当练习做(参考第 7 讲例 1 及注 4).

注 3 回到例 1,我们提一下,下面更强的命题是正确的:

首项与公差互素的(正整数的)无穷等差数列中,一定包含无穷多个素数.

这一重要结果的证明极为困难(本书中不作讨论).因此,用这样一个大定理解例 1 那样的小问题,并不合适.

注 4 例 1 也可采用不同的(归纳)构造法,这基于下面的引理.

引理 设 a、b 是互素的正整数,m 是任意给定的正整数,则数列 $\{bx+a\}$ $(x=0,1,\cdots)$ 中必有一项(从而有无穷多项)与 m 互素.

引理的来源从下面的证明中一目了然(而由例 1 的结论可见它必定是正确的).

引理的证明:设 m' 是 m 的与 b 互素的最大约数. 若 $m'=1$,则 m 的素因子都是 b 的素因子,但是 $(a, b)=1$,故 $(a, m)=1$,结论显然成立.

若 $m'>1$,由中国剩余定理,同余式组

$$x \equiv a(\mathrm{mod}\, b),\ x \equiv 1(\mathrm{mod}\, m')$$

有正整数解 x,则 x 即是所求的一个项. 因为对 m 的任意素因子 p,若 $p \mid m'$,则由上面第二个同余式知 $p \nmid x$;若 $p \nmid m$,则由 m' 的定义知 $p \mid b$,但 $(a, b)=1$,所以 $p \nmid a$,从而由 $x \equiv a(\mathrm{mod}\, b)$ 知 $p \nmid x$,因此 $(x, m)=1$.

现在通过引理证明例 1:

在数列中任取一项作为 u_1,如果 $u_1<\cdots<u_n$ 已取定,且它们两两互素. 由引理,数列中必有一项 u_{n+1} 与 $m=u_1, \cdots, u_n$ 互素,且 $u_{n+1}>u_n$. 于是,$u_1, \cdots, u_n, u_{n+1}$ 两两互素,由此作出了符合要求的子列.

例 2 设 a、b 是整数且 $b \neq 0$. 证明:数列 $\{bx+a\}$ $(x=0, 1, \cdots)$ 中,有无穷多项具有相同的素因子.

证明 显然,我们可设 $b>0$,进而可设 $a>0$(因为若 $a \leqslant 0$,取正整数 n 使得 $a'=nb+a>0$,则由 $bx+a=b(x-n)+a'$ 知,只需考虑 $x=n, n+1, \cdots$ 时数列的项).

如果 $a=1$,则结论是显然的,因为当 $x=\dfrac{(b+1)^k-1}{b}$ 时,数列中相应的项为等比数列 $(b+1)^k$ $(k=1, 2, \cdots)$.

一般情形下,由

$$bx+a=a\left(1+\frac{b}{a}x\right),$$

取 $x=ay$,便将问题化为上述特殊情形.

于是，取 $x=\frac{a}{b}((b+1)^k-1)$，数列中相应的项 $a(b+1)^k$ $(k=1,2,\cdots)$ 组成等比数列，它们当然具有相同的素因子.

注5 将一般性的问题化归为(某个)特殊情形解决，这与注1中的手法“相反相成”，也是数学中极其基本的想法(本书前面已出现过这样的例子，参考第6讲(16)，第14讲中的(1)及注1).

例3 证明：有无穷多个正整数 n，使得 $[\sqrt{2}n]$ 为完全平方数.

证明 显然，$[\sqrt{2}n]=q^2$(q 为一个正整数)，等价于

$$q^4<2n^2<q^4+2q^2+1.$$

我们因此期望有无穷多个正整数 n，q，满足

$$2n^2=q^4+a\ (a\text{ 是某个固定的正整数}).$$

然而，这一方程不易处理；事实上，它至多有有限组正整数解(见后面的注7).

现在，我们转而考虑方程

$$2n^2=q^4+q^2.$$

这本质上是一个二次方程：两边同除以 q^2，得 $2\left(\frac{n}{q}\right)^2=q^2+1$. 因右边是整数，故左边也是整数，即 q 整除 n. 于是我们产生了沛尔方程

$$x^2-2y^2=-1.$$

易知这有无穷多组正整数解(参见第9讲中第二节). 对任一组解 (x,y)，取 $n=xy$，$q=x$，就得出了所求的(无穷组)解.(若考虑方程 $2n^2=q^4+2q^2$，则产生沛尔方程 $x^2-2y^2=1$，同样可以解决问题.)

例4 证明：存在无穷多个边长为互素整数的三角形，其面积为完全平方数.

证明 如果不限制边长互素，则问题极为容易(找出一个面积为平方数的整边三角形，将其“扩大”任意正整数 d 倍，即得无穷多个这样的三角形). 现在的问题要困难得多.

首先注意，(边长为整数的)直角三角形、等腰三角形这些“较简单”的三角形均不符合问题的要求(即它们的面积决不会是一个完全平方数). 这些事实的证明并不平凡，参考第 20 讲练习题中的第 1 题和第 7 题.

我们因此考虑一般的(边长为整数的)三角形. 设三角形三边长为 x、y、z(暂不顾及它们是否互素). 记 $p=\frac{1}{2}(x+y+z)$，则面积为

$$\Delta=\sqrt{p(p-x)(p-y)(p-z)}. \tag{①}$$

为了减少变元，我们(尝试着)取 $p-z=1$(参考下面的注 6)，即

$$z=x+y-2. \tag{②}$$

于是①化简为

$$\Delta=\sqrt{(x-1)(y-1)(x+y-1)}. \tag{③}$$

上式右边出现 x 与 y 的和，不利于选择 x、y，使 Δ 为完全平方数. 我们希望将它变形为两个一元整式的积. 为此，设

$$y-1=(a-1)x, \tag{④}$$

这里 a 是(待定的)整数参量. 于是③可化为

$$\Delta=x\sqrt{a(a-1)(x-1)}. \tag{⑤}$$

由⑤我们可以(试)取 $x-1=a(a-1)$，但这时 $\Delta=a(a-1)\cdot[a(a-1)+1]$，为两个连续整数之积，不能是完全平方数.

现在我们转而取

$$x-1=4a(a-1). \tag{⑥}$$

则

$$\Delta = a(2a-2)(2a-1)^2.$$

于是，我们的任务就化为：找无穷多个正整数 a，使 a 及 $2a-2$ 都是完全平方数. 这一点用沛尔方程的知识极易证明(参考第 9 讲第二节). 也可采用下面的(归纳)构造法：取 $a_1 = 3^2$，则 $2a_1 - 2 = 4^2$. 若 a_n 与 $2a_n - 2$ 都是平方数，令 $a_{n+1} = (2a_n - 1)^2$，则 a_{n+1} 当然是平方数，而

$$2a_{n+1} - 2 = 4a_n(2a_n - 2)$$

也是平方数.

现在，由②、④、⑥可知，取

$$x = (2a_n - 1)^2,\ y = (a_n - 1)(2a_n - 1)^2 + 1,$$

$$z = a_n(2a_n - 1)^2 - 1,$$

其中 $a_1 = 9$，$a_{n+1} = (2a_n - 1)^2$，则以 x、y、z 为边长的三角形符合要求.(三角形的面积是平方数，而 x、y、z 显然互素. 实际上，x、y、z 是两两互素的.)

注 6 没有参量便无从选择，但如果参(变)量太多也往往难以处理.

①中有三个变量，首先可尝试取定两边长，只保留一个变量，但这时整数边长三角形只有有限多个，不能解决问题.

若取定一边长，而保留两个变量，虽然有无穷多个(整数边长的)三角形，但能够证明，其中至多有有限多个面积平方数的三角形(见注 7).

让 x、y、z 满足②，即增加一个线性约束条件，目的还是为了消去一个变元(见③). 这样做的另一个好处是，由②，只要 x、y、z 中有一个是奇数，则它们就互素.

注 7 设 $z = \alpha$ 是固定的正整数. 又可设 $y \geqslant x$，则 $y = x + r$ $(r = 0, 1, \cdots, \alpha - 1)$. 易知①可化为 α 个形如

$$ax^2+bx+c=16t^4 \tag{7}$$

的方程，其中 $t^2=\Delta$，a、b、c 是常数（只依赖于 α），且 $a\neq 0$. 能够证明（但本书不作讨论），方程⑦至多只有有限多个整数解 (x, t). 即使不了解这一结果，面临⑦这样棘手的四次方程，我们应当改弦更张（参考注 2）. 顺便提一下，较深入的方法能够证明：若 n，d 是固定的整数，而 $n\geqslant 3$，则将⑦的右边换为 dt^n 的方程，也至多有有限组整数解.

例 4 也可采用下面的解法：将①变形为

$$\Delta=\frac{1}{4}\sqrt{((x+y)^2-z^2)(z^2-(x-y)^2)}. \tag{8}$$

设

$$x-y=1 \tag{9}$$

（这相当于②）. 我们希望选择 $x+y$（用 z 表示），使 $(x+y)^2-z^2$ 可分解出因式 z^2-1. 较自然的取法是 $x+y=z^2$，得出 $\Delta=\frac{1}{4}z(z^2-1)$，易知这不能是平方数（除非 $z=1$）. 现在取

$$x+y=z(2z^2-1), \tag{10}$$

则 $\Delta=\frac{z^2-1}{2}\cdot z^2$. 由沛尔方程的知识可知，有无穷多个（奇整数）$z$，使 $\frac{z^2-1}{2}$ 是完全平方数（且不难写出 z 的表达式）. 对这样的 z，由⑨、⑩知，以 $x=z^3-\frac{z-1}{2}$、$y=z^3-\frac{z+1}{2}$、z 为边长的三角形符合问题中的要求.

例 5 证明：有无穷多对奇素数 p、q，满足 $pq\mid 2^{pq-1}-1$.

证明 首先，我们将问题分解. 由第 8 讲练习题中第 7 题知，若 p，q 是不同的奇素数，则 $pq\mid 2^{pq-1}-1$ 等价于

$$p\mid 2^{q-1}-1 \quad 及\ q\mid 2^{p-1}-1. \tag{11}$$

证明有无穷对素数 p、q 满足⑪颇不容易. 下面的论证基于梅森数(第 7 讲注 4):设 r 是一个奇素数,设 p 是 2^r-1 的一个素因子,则 $p-1=2rx$,这里 x 是一个整数(见第 19 讲例 2).

进一步,若 2^r+1 是 3 的幂,易知必须 $r=3$. 因此只要 $r>3$,则 2^r+1 就有一个素因子 $q\neq 3$,从而 $q-1=2ry$,其中 y 是一个整数(见第 19 讲练习题中第 1 题).

上面作出的 p、q 显然不同. 由于 $2^r-1\mid 2^{2ry}-1$,故 $p\mid 2^{q-1}-1$. 同样,由 $2^r+1\mid 2^{2rx}-1$ 知 $q\mid 2^{p-1}-1$,即 p,q 满足⑪. 此外,由于素数有无穷多个,故素数 r 可任意地大,而上述作出的 p,q 显然都 $\geqslant 2r+1$,故符合要求的 p,q 有无穷多对.

注 8 上面的论证中,更自然的或许是将 q 取为 2^r-1 的不同于 p 的素因子,若能做到这一点,证明将更为直接. 但是,目前我们尚不知道是否有无穷多个素数 r,使 2^r-1 至少有两个不同的素因子(参考本讲注 2,第 7 讲注 4,以及第 9 讲练习题中第 16 题).

注 9 若期望取问题中的 $p=q$,则由

$$2^{p^2-1}-1=(2^{p^2-p}-1)2^{p-1}+2^{p-1}-1,$$

及 $p^2\mid 2^{p^2-p}-1$(欧拉定理)可知,$p^2\mid 2^{p^2-1}-1$ 等价于

$$2^{p-1}\equiv 1(\bmod p^2). \tag{⑫}$$

然而,是否有无穷多个素数 p 使⑫成立,则是一个极其困难的未解决问题.(参考注 2.)

注 10 由费马小定理可知,若 n 是素数,则

$$2^n\equiv 2(\bmod n). \tag{⑬}$$

但也有合数 n 使⑬成立,这样的数称为伪素数.

易于验证,最小的伪素数是 $341=11\times 31$. 例 5 表明,有无穷多个伪素数恰有两个素因子.

证明有无穷多个伪素数当然不必用例 5. 我们证明,若 n 是一

个伪素数，则 $m=2^n-1$ 也是伪素数. 事实上，因 n 是合数，故 $m=2^n-1$ 也是合数. 由 $n\mid 2^n-2$，可设 $m-1=kn$（k 为正整数），于是 $2^{m-1}-1=2^{kn}-1$ 被 2^n-1 整除，故 $m\mid 2^m-2$.

因 341 是伪素数，于是我们递推地得出了无穷多个伪素数.

例 6 设 n 是奇数，$n>1$，k 是正整数，且对 n 的任一素因子 p，有 $(p-1)\nmid k$. 记

$$S_k(n)=\sum_{\substack{i=1\\(i,\ n)=1}}^{n} i^k.$$

证明：$n\mid S_k(n)$.

证明 论证的出发点是第 8 讲注 1 中说的原则（参考第 8 讲例 5 的解法二）. 由于对任意与 n 互素的整数 a，$\varphi(n)$ 个数 ai（$1\leqslant i\leqslant n$ 且 i 与 n 互素）是模 n 的一个缩系（第 8 讲的(11)），因此

$$\sum_{\substack{i=1\\(i,\ n)=1}}^{n} i^k\equiv\sum_{\substack{i=1\\(i,\ n)=1}}^{n}(ai)^k\pmod n,$$

即

$$(a^k-1)S_k(n)\equiv 0\pmod n. \tag{14}$$

我们希望能选择参量 a，使得 $(a,\ n)=(a^k-1,\ n)=1$，由此及⑭便证明了结论.

由第 12 讲练习题中的第 9 题知，对任意素数 p，若 $p-1\nmid k$，则存在整数 a，使 $p\nmid a$ 且 $p\nmid a^k-1$. 现在设 n 的不同素因子为 $p_1,\ \cdots,p_l$. 由于 $p_i-1\nmid k$，故对每个 p_i，存在 a_i 使

$$(a_i,\ p_i)=(a_i^k-1,\ p_i)=1\ (i=1,\ \cdots,\ l).$$

由中国剩余定理，同余式组

$$a\equiv a_i\pmod{p_i}\ (i=1,\ \cdots,\ l)$$

有解. 这样的 a 显然满足 $p_i\nmid a$（$1\leqslant i\leqslant l$），从而 $(a,\ n)=1$；又 $a^k-1\equiv a_i^k-1\pmod{p_i}$，故 $p_i\nmid a^k-1$（$1\leqslant i\leqslant l$），即 a 满足 $(a^k-1,\ n)=1$. 这就完成了证明.

注 11　当 k 为奇数时(此时,$(p-1)\nmid k$ 自动成立),例 6 可以更初等和直接地解决. 参考第 6 讲例 6,及第 8 讲中(16)的证法二.

注 12　当 n 为奇素数 p 时,由例 6 及费马小定理推出

$$S_k=1^k+2^k+\cdots+(p-1)^k\equiv\begin{cases}0, & (\mathrm{mod}\ p),\text{若 } p-1\nmid k;\\ -1, & (\mathrm{mod}\ p),\text{若 } p-1\mid k.\end{cases}$$

这一结论相当基本,因此我们再给出其一种初等的证明:

由带余除法,$k=(p-1)q+r$,其中 $0\leqslant r<p-1$;而由费马小定理易知,$S_k\equiv S_r(\mathrm{mod}\ p)$. 因此,我们可假设 $0\leqslant k<p-1$ 来论证.

当 $k=0$ 时结论显然成立. 为解决 $k>0$ 的情形,我们用归纳法. 当 $k=1$ 时易知结论成立;设 $1<k<p-1$,若所说的结论对 $<k$ 的正整数已成立,下面我们来证明 $S_k\equiv 0(\mathrm{mod}\ p)$.

论证基于 S_1,…,S_k 的一个递推关系:由二项式定理,

$$(m+1)^{k+1}=m^{k+1}+\binom{k+1}{1}m^k+\cdots+\binom{k+1}{k}m+1.$$

对 $m=1$,…,$p-1$ 求和,我们有

$$\binom{k+1}{1}S_k+\binom{k+1}{2}S_{k-1}+\cdots+\binom{k+1}{k}S_1=p^{k+1}-p.$$

由上式及归纳假设易知 $p\Big|\binom{k+1}{1}S_k$. 但 $1<k+1\leqslant p-1$,故 $p\nmid\binom{k+1}{1}$,从而素数 $p|S_k$,这就完成了证明.

注 13　对任意正整数 n,记 $S_i(n)=1^i+2^i+\cdots+n^i$,则与上面相同地可证明:对正整数 k 有

$$\sum_{i=0}^{k}\binom{k+1}{i}S_i(n)=(n+1)^{k+1}-1.$$

这给出了前 n 个正整数的方幂和与二项式系数的(递推)关系,也是一个基本的恒等式.

下面的例 7 是关于二项式系数算术性质的一个基本结果.

例 7 设 n 是正整数,p 是素数,

$$n=(k_m\cdots k_1k_0)_p=k_0+k_1p+\cdots+k_mp^m$$

是 n 的 p 进制表示,这里 k_i 是满足 $0\leqslant k_i<p$ $(i=0,1,\cdots,m)$ 且 $k_m\neq 0$ 的整数.

证明:二项式系数 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中恰有

$$N=(k_0+1)(k_1+1)\cdots(k_m+1) \tag{15}$$

个数不被 p 整除,并确定对怎样的 n 有 $N=n+1$.

证明 为了证明,将多项式 $(x+1)^n$ 模 p 运算(参考第 11 讲的第四节,以及第 11 讲练习题中的第 3 题),我们有

$$(x+1)^n=\prod_{i=0}^{m}(x+1)^{k_ip^i}\equiv\prod_{i=0}^{m}(x^{p^i}+1)^{k_i}\pmod p.$$

因 $0\leqslant k_i<p$,故 $(x^{p^i}+1)^{k_i}$ 展开后共有 k_i+1 个非零项,所以上式右端乘开后共有 $\prod\limits_{i=0}^{m}(k_i+1)$ 个非零项(即系数不被 p 整除的项),结合 $(x+1)^n$ 的展开式,即知 $\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中共有 N 个不被 p 整除.

下面我们证明,$N=n+1$(即 n 阶二项式系数均不被 p 整除)的充分必要条件是 $k_i=p-1$ $(i=0,1,\cdots,m-1)$,而 $k_m\neq 0$.

事实上,由⑮我们有

$$N=k_m\prod_{i<m}(k_i+1)+k_{m-1}\prod_{i<m-1}(k_i+1)+\cdots+(k_0+1). \tag{16}$$

此外,因为 $k_i\leqslant p-1$ $(i=1,\cdots,m)$,故

$$\prod_{i<r}(k_i+1)=(k_0+1)\cdots(k_{r-1}+1)\leqslant p^r(r\geqslant 1). \qquad ⑰$$

由⑯、⑰得出，

$$\sum_{i=0}^{m}k_ip^i+1=n+1=N\leqslant\sum_{i=0}^{m}k_ip^i+1.$$

从而⑰必须对所有 r 取等号，即 $k_i=p-1$ $(i=0,1,\cdots,m-1)$.

由本题特别地推出，$\binom{n}{0},\binom{n}{1},\cdots,\binom{n}{n}$ 中恰有 2^s 个奇数，其中 s 是 n 的二进制表示中数码 1 的个数；从而 n 阶二项式系数均为奇数的充分必要条件是，n 具有形式 2^k-1（k 为正整数）.

例 8 设 x、y 是复数 $(x\neq y)$，若 $a_n=\dfrac{x^n-y^n}{x-y}$ 对某四个连续正整数 n 为整数. 证明：对所有 $n\geqslant 0$，a_n 都是整数.

证明 我们首先应当作出 a_n 的递推公式（参考第 3 讲注 9），这件事甚为容易. 由等式

$$x^n-y^n=(x^{n-1}-y^{n-1})(x+y)-xy(x^{n-2}-y^{n-2}),$$

得出

$$a_n=\alpha a_{n-1}-\beta a_{n-2},\ (n\geqslant 2), \qquad ⑱$$

其中 $\alpha=x+y$，$\beta=xy$. 因为 $a_0=0$，$a_1=1$ 都是整数，故只要（并且也必须）证明 α、β 都是整数，则由⑱及归纳法即知结论成立.

设正整数 k 使得 a_k、a_{k+1}、a_{k+2}、a_{k+3} 都是整数，则

$$a_{k+2}=\alpha a_{k+1}-\beta a_k,\ a_{k+3}=\alpha a_{k+2}-\beta a_{k+1}. \qquad ⑲$$

由⑲，α 与 β“显然”都是有理数，但证明它们都是整数，则颇为困难.

眼下能够做的事情似乎只有从⑲中解出 α、β. 不难得出

$$\alpha=\frac{a_{k+2}a_{k+1}-a_{k+3}a_k}{a_{k+1}^2-a_ka_{k+2}},\ \beta=\frac{a_{k+2}^2-a_{k+1}a_{k+3}}{a_{k+1}^2-a_ka_{k+2}}. \qquad ⑳$$

我们应当检查上面“形式”解的分母是否为零（这一非常基本的小

事将是下面论证的入手点),为了做到这一点,当然应回到 a_n 的定义中去,得到

$$a_{n+1}^2 - a_n a_{n+2} = (xy)^n = \beta^n. \tag{21}$$

因此,我们需要区分两种情形:$xy = 0$ 及 $xy \neq 0$.

当 $xy = 0$ 时,不妨设 $x = 0$,则由 y^k、y^{k+1} 为整数知,$y = \dfrac{y^{k+1}}{y^k}$ 是有理数;再结合 y^{k+1} 是整数,推出 y 是整数(参考第 6 讲练习题中第 12 题),从而结论显然成立.

当 $xy \neq 0$ 时,由(21)可见,β^k 与 β^{k+1} 都是非零整数,类似地推出 β 是整数.

为了证明有理数 α 是一个整数,我们回到(18),以考察 a_n 与递推公式的初值及系数的联系:

$$a_2 = \alpha,\ a_3 = \alpha^2 - \beta,\ a_4 = \alpha^3 - 2\alpha\beta,\ a_5 = \alpha^4 - 3\alpha^2\beta + \beta^2,\ \cdots.$$

由此可以猜想,并且用归纳法极易证明,有一个首项系数是 1 的 $n-1$ 次整系数多项式 $f_{n-1}(x)$,使得 $a_n = f_{n-1}(\alpha)$. 特别地,有理数 α 是首项系数为 1 的整系数多项式 $f_{k+1}(x) - a_{k+2}$ 的零点,故 α 是整数(参考第 12 讲的(8)及注 5). 证毕.

注 14 方程组(19)及其解(20),在论证过程中起着很基本的作用,但就本题的解答而言,并不需要它们.

例 9 证明:有无穷多个正整数 n,使得和

$$\left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right]$$

为偶数.

证明 和式中每一项的奇偶性均不易确定,我们因此期望给予这个和的一种不同表达式.

用 $f(n)$ 记所说的和,首先来考虑 $f(n+1) - f(n)$,以期望得出 $f(n)$ 的递推信息(参考第 3 讲注 9).

设 $1 \leqslant k \leqslant n+1$,由带余除法,

$$n+1=qk+r,\ 0\leqslant r\leqslant n.$$

若 $k\nmid n+1$，即 $r\geqslant 1$，则易知 $\left[\frac{n+1}{k}\right]=\left[\frac{n}{k}\right]$；若 $k\mid n+1$，则 $\left[\frac{n+1}{k}\right]=q=\left[\frac{n}{k}\right]+1$. 所以

$$\left[\frac{n+1}{k}\right]=\begin{cases}\left[\frac{n}{k}\right],\text{若 } k\nmid n+1;\\ \left[\frac{n}{k}\right]+1,\text{若 } k\mid n+1.\end{cases}\qquad ㉒$$

由此可得

$$\left[\frac{n+1}{1}\right]+\left[\frac{n+1}{2}\right]+\cdots+\left[\frac{n+1}{n+1}\right]-\left[\frac{n}{1}\right]-\left[\frac{n}{2}\right]-\cdots-\left[\frac{n}{n}\right]$$
$$=n+1\text{ 的正约数的个数}=\tau(n+1),$$

即有递推关系

$$f(n+1)-f(n)=\tau(n+1).\qquad ㉓$$

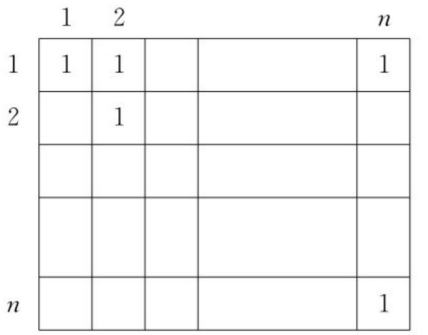
注意 $f(1)=1=\tau(1)$，故由㉓得出

$$f(n)=\tau(1)+\tau(2)+\cdots+\tau(n).\qquad ㉔$$

利用㉔，极易解决问题. 因为 $\tau(k)$ 为奇数的充分必要条件是 k 为完全平方数(第 7 讲中(8)). 因此，在㉔中右边的和为偶数的充分必要条件是，1，2，…，n 中的平方数恰有偶数个，即 $[\sqrt{n}]$ 为偶数. 我们实际上确定了使 $f(n)$ 为偶数的所有 n；取(例如) $n=(2m+1)^2$ $(m=1,2,\cdots)$，则 $f(n)$ 为偶数，这样的 n 当然有无穷多个.

注 15 等式㉔是数论中很基本的一个事实，它也可以用下面较为直观的方式来证明：考虑图中的 $n\times n$ 数表，对 $1\leqslant i,j\leqslant n$，若 $i\mid j$，则在第 i 行与第 j 列交叉的方格中填 1，否则填 0. 于是，

表中第 j 列中数之和，就是 j 的约数的个数 $\tau(j)$. 因此，按列计算表中全部数的和，即是㉔的右端. 另一方面，第 i 行中 1 的个数，就是 $1, 2, \cdots, n$ 中被 i 整除的数的个数，这是 $\left[\frac{n}{i}\right]$，故按行计算表中数的总和，便得出了 $f(n)$. 因此㉔成立.



例 9

例 10 对正整数 n，用 $r(n)$ 表示

$$n \div 1, n \div 2, \cdots, n \div n$$

的余数之和. 证明：有无穷多个 n，使得 $r(n) = r(n-1)$.

证明 首先求出 $r(n)$ 的一个表达式. 用(具有“确切形式”不完全商的)带余除法，这一步并不困难(见第 6 讲注 5).

设 m 是正整数，对 $1 \leqslant k \leqslant m$，我们有

$$m = \left[\frac{m}{k}\right] \cdot k + r,\ 0 \leqslant r < k.$$

将这些等式相加，得出

$$r(m) = m^2 - \sum_{k=1}^{m} k\left[\frac{m}{k}\right].$$

由此我们推出，$r(n) = r(n-1)$ 等价于

$$\sum_{k=1}^{n} k\left[\frac{n}{k}\right] - \sum_{k=1}^{n-1} k\left[\frac{n-1}{k}\right] = 2n-1. \qquad ㉕$$

第二步至关重要：㉕式左边的和有一个简单的算术意义，它等于 $\sigma(n)$(n 的所有正约数之和). 实际上，与证明㉒相同地可导出

$$k\left[\frac{n}{k}\right] = \begin{cases} k\left[\frac{n-1}{k}\right], & \text{若 } k \nmid n; \\ k\left[\frac{n-1}{k}\right] + k, & \text{若 } k \mid n. \end{cases}$$

由此即得出我们宣称的结论.

最后,证明有无穷多个 n 满足

$$\sigma(n)=2n-1.$$

这需要一点机智(用第 7 讲中公式⑤反而容易走入歧途). 由

$$1+2+2^2+\cdots+2^l=2^{l+1}-1=2\times 2^l-1$$

可见, $n=2^l(l=1,2,\cdots)$ 符合要求.

注 16 类似于㉔(及其证明),不难导出

$$\sum_{k=1}^{n}k\left[\frac{n}{k}\right]=\sum_{k=1}^{n}\sigma(k). \tag{26}$$

但本题不需要这个公式.

我们顺便提一下,用注 15 中的方法,也能证明㉖. 这只需将注 15 中表格的填数方式作些修改:若 $i\mid j$,则在第 i 行与第 j 列交叉的方格中填 i,否则填 0. 细节请读者自己完成(参考第 3 讲注 2).

例 11 证明:对任意的 $N\geqslant 1$,存在自然数 $n\geqslant 1$,使得 2^n 的末 N 位数码仅由 1 与 2 构成.

证明 用归纳法. 因为 $2^5=32$, $2^9=512$,故结论对 $N=1$, 2 皆成立.

假设对 $N\geqslant 2$,存在着 n,使得 2^n 的末 N 位数码仅由 1 与 2 构成,我们来证明,必存在 m,使得 2^m 的末 $N+1$ 位数码只含 1 与 2.

论证的策略是,首先作出几个(适当的)2 的幂,使得它们与 2^n 的末 N 位数码相同,再期望证明其中有一个符合我们(上述)的要求.

为了这一目的,我们注意,对任意正整数 r,五个数

$$2^n,\ 2^{n+r},\ 2^{n+2r},\ 2^{n+3r},\ 2^{n+4r} \tag{27}$$

中,任意两个的差均被 2^r-1 及 2^n 整除. 由于显然有 $n\geqslant N+1$,故只要取(参数)r 满足

$$5^N\mid(2^r-1), \tag{28}$$

(这样的 r 一定存在,参见第 19 讲). 则在㉗中任两个数的差被 $2^{N+1}\times 5^N = 2\times 10^N$ 整除. 因此,这五个数的末 N 个数码皆对应相等(从而均只含 1 与 2),并且它们的倒数第 $N+1$ 个数码具有相同的奇偶性.

现在,我们期望可进一步选择 r,使得这五个数的倒数第 $N+1$ 个数码互不相同,从而,按已证明了的事实,它们只能是 1, 3, 5, 7, 9 或 0, 2, 4, 6, 8 的一个排列. 无论哪种情况,在㉗的数中,必有一个数的倒数第 $N+1$ 个数码为 1 或 2,这就指出了符合要求的 2^m.

我们假设在㉗中有两个数的倒数第 $N+1$ 个数码相同,即它们的差被 10^{N+1} 整除,这给出

$$2^{n+sr}(2^{tr}-1)\equiv 0(\mathrm{mod}\ 10^{N+1}),$$

其中 s, t 是满足 $0\leqslant s\leqslant 3$, $1\leqslant t\leqslant 4$ 的整数. 因此,

$$2^{tr}\equiv 1(\mathrm{mod}\ 5^{N+1}). \qquad ㉙$$

由第 19 讲练习题中第 5 题,2 模 5^{N+1} 的阶为 $\varphi(5^{N+1}) = 4\times 5^N$,故由㉙推出 $4\times 5^N \mid tr$ (第 19 讲(1)).

注意 $tr<5r$,故若取 $r=\varphi(5^N)=4\times 5^{N-1}$,则㉘得以满足(欧拉定理);但 $0<tr<4\times 5^N$,这与 $4\times 5^N \mid tr$ 矛盾. 于是我们证明了,取(参数) $r=4\times 5^{N-1}$,则在㉗中任两个数的倒数第 $N+1$ 个数码彼此不同,这完成了归纳证明.

例 12 设 a_1, a_2, …, a_n 为 n 个不同整数. 证明:

$$\prod_{1\leqslant l<k\leqslant n}\frac{a_k-a_l}{k-l}$$

是一个整数.

证明 本题相当困难. 我们将证明下面的命题:

对任意整数 $b>1$, $a_k-a_l(1\leqslant l<k\leqslant n)$ 中被 b 整除的数目,不少于 $k-l$ $(1\leqslant l<k\leqslant n)$ 中被 b 整除的数目.

由这命题,特别地取 $b=p^s$ (p 为任意素数, s 为任意正整数),

即知本题的结论成立.

为了证明上述命题,我们分几步进行.

第一步,给予 $a_k-a_l(1\leqslant l<k\leqslant n)$ 中被 b 整除的数目的一个适当的表达式.这一工作并不困难.设 $a_1,\cdots,a_n$ 中恰有 n_r 个数被 b 除余 r $(r=0,1,\cdots,b-1)$,则

$$n_0+n_1+\cdots+n_{b-1}=n.$$

而 $a_k-a_l(1\leqslant l<k\leqslant n)$ 中被 b 整除的数目为

$$\begin{aligned}N&=\binom{n_0}{2}+\binom{n_1}{2}+\cdots+\binom{n_{b-1}}{2}\\&=\frac{1}{2}\sum_{i=0}^{b-1}n_i^2-\frac{1}{2}\sum_{i=0}^{b-1}n_i\\&=\frac{1}{2}\sum_{i=0}^{b-1}n_i^2-\frac{n}{2}.\end{aligned}$$

另一方面,易知(参见下面的注 17)

$$b\sum_{i=0}^{b-1}n_i^2=\Big(\sum_{i=0}^{b-1}n_i\Big)^2+\sum_{0\leqslant i<j\leqslant b-1}(n_i-n_j)^2. \tag{30}$$

故得出

$$N=\frac{1}{2b}\Big[\sum_{0\leqslant i<j\leqslant b-1}(n_i-n_j)^2\Big]+\frac{n^2}{2b}-\frac{n}{2}. \tag{31}$$

同样,设 $1,2,\cdots,n$ 中恰有 n'_r 个数被 b 除余 r $(r=0,1,\cdots,b-1)$,则 $k-l$ $(1\leqslant l<k\leqslant n)$ 中被 b 整除的数目为

$$N'=\frac{1}{2b}\Big[\sum_{0\leqslant i<j\leqslant b-1}(n'_i-n'_j)^2\Big]+\frac{n^2}{2b}-\frac{n}{2}. \tag{32}$$

第二步,考虑特殊情形:$b\mid n$.设 $n=mb$,则 $n'_0=n'_1=\cdots=n'_{b-1}=m$.由㉛和㉜立知 $N\geqslant N'$,即此时上述命题成立.

第三步,我们将一般情形化归为上述的特殊情形.

设 $n=mb+r$,$0<r<b$.此时 $n'_1,\cdots,n'_r$ 都等于 $m+1$,而 $n'_{r+1},\cdots,n'_{b-1}$ 与 n'_0 都等于 m.此外由于 $n_0,n_1,\cdots,n_{b-1}$ 的和为

$n=mb+r$，故其中必有一项不超过 m，设 $n_t \leqslant m$ $(0 \leqslant t \leqslant b-1)$. 现在于 a_1，…，a_n 中增加一个整数 a_{n+1}，使 $a_{n+1} \equiv t(\mathrm{mod}\ b)$，则 $a_k - a_l$ 形式的数增加 n 个：

$$a_{n+1}-a_1,\ \cdots,\ a_{n+1}-a_n.$$

显然，增加的数中有 n_t 个被 b 整除. 而 $k-l$ 形式的数也增加 n 个：

$$(n+1)-1,\ \cdots,\ (n+1)-n,\text{即为}\ 1,\ 2,\ \cdots,\ n.$$

其中恰有 $m \geqslant n_t$ 个被 b 整除.

因此，若证明了 $a_k-a_l(1 \leqslant l<k \leqslant n+1)$ 中被 b 整除的个数 M 不小于 $k-l$ $(1 \leqslant l<k \leqslant n+1)$ 中被 b 整除的个数 M'，则可推出，$a_k-a_l(1 \leqslant l<k \leqslant n)$ 中被 b 整除的数目，不小于 $k-l$ $(1 \leqslant l<k \leqslant n)$ 中被 b 整除的数目，即 $N \geqslant N'$.

若 $b \mid (n+1)$，则与第二步同样地有 $M \geqslant M'$，从而 $N \geqslant N'$ 得证. 若 $b \nmid (n+1)$，我们在 a_1，…，a_n，a_{n+1} 中再添入一个适当整数，重复 $(b-r$ 次) 上述论证，最终化为第二步那样的特殊情形，进而证得 $N \geqslant N'$. (参考本讲中注 5.)

注 17 恒等式㉚，是下面著名的拉格朗日恒等式的特殊情形：

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2=\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right)-\sum_{1 \leqslant i<j \leqslant n}(a_i b_j-a_j b_i)^2.$$

顺便说一下，若 a_i、$b_i(1 \leqslant i \leqslant n)$ 都是实数，则由这一等式给出了柯西不等式

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leqslant\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right),$$

并且易确定等号成立的条件.

例 13 设 q_0，q_1，…是无穷的整数列，满足

(i) 对任意 $m>n \geqslant 0$，$(m-n) \mid (q_m-q_n)$.

(ii) 存在多项式 $P(x)$，使得 $|q_n|<P(n)$ 对所有 n 成立.

证明:存在多项式 $Q(x)$,使得 $q_n = Q(n)$ 对所有 n 成立.

证明 我们设 $d = \deg P(x)$,用拉格朗日插值公式,由数列 $\{q_n\}$ $(n \geqslant 0)$ 的前 $d+1$ 项可唯一地决定一个次数不超过 d 的多项式,即有多项式 $Q(x)$,满足 $Q(i) = q_i$ $(i = 0, 1, \cdots, d)$,且 $\deg Q(x) \leqslant d$. 实际上,这个多项式可表示为

$$Q(x) = q_0 L_0(x) + q_1 L_1(x) + \cdots + q_d L_d(x),$$

这里 $L_i(x) = \prod\limits_{\substack{0 \leqslant j \leqslant d \\ j \neq i}} \dfrac{x-j}{i-j}$ $(i = 0, 1, \cdots, d)$(参考第 14 讲第一节). 我们将证明,有理系数多项式 $Q(x)$ 符合问题中的要求,为此令 $r_n = k(Q(n) - q_n)$ $(n = 0, 1, \cdots)$,这里 k 是 $Q(x)$ 系数的公分母. 为了证明 $r_n = 0$ $(n = 0, 1, \cdots)$,我们从两个方面进行.

首先,由条件(ii)知,

$$| r_n | \leqslant k(| Q(n) | + | q_n |) < k(| Q(n) | + P(n)),$$

故有一个次数不超过 d 的多项式 $R(x)$,使得

$$| r_n | < R(n), \text{ 对所有 } n \geqslant 0. \tag{33}$$

此外,$kQ(x)$ 是整系数多项式,故对于 $m > n \geqslant 0$,易知 $kQ(m) - kQ(n)$ 被 $m - n$ 整除. 结合条件(i)知

$$(m-n) \mid r_m - r_n, \text{ 对所有 } m > n \geqslant 0. \tag{34}$$

因为对 $i = 0, 1, \cdots, d$,有 $r_i = 0$,于是由(34)推出,对所有的 $n > d$ 有 $(n-i) \mid r_n - r_i = r_n (0 \leqslant i \leqslant d)$,因此 r_n 是 $n, n-1, \cdots, n-d$ 的最小公倍数的倍数(第 6 讲的(14)).

另一方面,我们将证明,存在正整数 N,使得

$$[n, n-1, \cdots, n-d] > R(n), \text{ 对所有 } n \geqslant N. \tag{35}$$

若(35)已证明,则由 $[n, n-1, \cdots, n-d] \mid r_n$ 及(33)推出,对于 $n \geqslant N$ 有 $r_n = 0$(参考第 6 讲的(3));而对 $n < N$,在(34)中取 m 是任意大于 N 的整数,则 $(m-n) \mid r_n$,故必须 $r_n = 0$(对 $n = 0, 1, \cdots, N$).

于是对所有 n 有 $r_n=0$，即 $q_n=Q(n)$.

为了证明㉟，我们应用第 7 讲练习题中第 12 题，得出

$$[n,\ n-1,\ \cdots,\ n-d]\geqslant\frac{n(n-1)\cdots(n-d)}{\prod\limits_{1\leqslant i<j\leqslant d}(n-i,\ n-j)}.$$

因为 $(n-i,\ n-j)=(n-i,\ j-i)\leqslant j-i$，故

$$\prod_{1\leqslant i<j\leqslant d}(n-i,\ n-j)\leqslant\prod_{1\leqslant i<j\leqslant d}(j-i)\text{（这是一个常数）；}$$

注意 $n(n-1)\cdots(n-d)$（作为 n 的多项式）的次数是 $d+1$，而 $R(x)$ 的次数不超过 d. 因此对于充分大的 n，有

$$[n,\ n-1,\ \cdots,\ n-d]\geqslant\frac{n(n-1)\cdots(n-d)}{\prod\limits_{1\leqslant i<j\leqslant d}(j-i)}>R(n),$$

于是存在 N，使㉟成立. 证毕.

例 14 设正整数 m，$n\geqslant 2$，a_1，$\cdots$，a_n 为整数，其中没有一个是 m^{n-1} 的倍数. 证明：存在不全为零的整数 e_1，$\cdots$，e_n，使得 $|e_i|<m\ (1\leqslant i\leqslant n)$，且 $e_1a_1+\cdots+e_na_n$ 是 m^n 的倍数.

证明 设 B 是所有有序 n 元数组 $\vec{b}=(b_1,\ \cdots,\ b_n)$ 构成的集合，其中 b_i 满足 $0\leqslant b_i<m$. 令

$$f(\vec{b})=b_1a_1+\cdots+b_na_n.$$

我们证明，存在不同的 $\vec{b}$，$\vec{b'}\in B$，使得

$$f(\vec{b})\equiv f(\vec{b'})\ (\mathrm{mod}\ m^n).$$

由此易知本题的结论成立. 因为令 $e_i=b_i-b_i'\ (1\leqslant i\leqslant n)$，则 e_i 不全为零，且 $|e_i|<m\ (1\leqslant i\leqslant n)$，以及

$$e_1a_1+\cdots+e_na_n\equiv 0(\mathrm{mod}\ m^n).$$

若任意两个 $f(\vec{b})$ 模 m^n 互不同余，则由于 $|B|=m^n$，而模 m^n

的剩余类也恰为 m^n 个，故当$\vec{b}$取遍 B 中所有元素时，$f(\vec{b})$模 m^n 的余数恰是 $0, 1, \cdots, m^n-1$ 的一个排列，即 $f(\vec{b})(\vec{b}\in B)$是模 m^n 的一个完系.

设 $\zeta=\mathrm{e}^{\frac{2\pi i}{m^n}}$ 是一个 m^n 次单位根，则由上面说的结果可知

$$\sum_{\vec{b}\in B}\zeta^{f(\vec{b})}=1+\zeta+\zeta^2+\cdots+\zeta^{m^n-1}=0.$$

另一方面，

$$\begin{aligned}\sum_{\vec{b}\in B}\zeta^{f(\vec{b})}&=\sum_{\substack{0\leqslant b_i<m\\1\leqslant i\leqslant n}}\zeta^{b_1a_1+\cdots+b_na_n}\\&=\prod_{i=1}^{n}(1+\zeta^{a_i}+\zeta^{2a_i}+\cdots+\zeta^{(m-1)a_i})\\&=\prod_{i=1}^{n}\frac{1-\zeta^{ma_i}}{1-\zeta^{a_i}}\neq 0.\end{aligned}$$

矛盾！（最后一步利用了 ma_i 不是 m^n 的倍数，故 $\zeta^{ma_i}\neq 1$.）

注 18 本题的条件“任一个 a_i 不被 m^{n-1} 整除”是必要的. 因为若取 $a_i=m^{i-1}(i=1,\cdots,n)$，则由

$$e_1a_1+\cdots+e_na_n\equiv 0(\mathrm{mod}\,m^n),\ |e_i|<m,$$

推出 $e_1+me_2+\cdots+m^{n-1}e_n\equiv 0(\mathrm{mod}\,m)$，故 $e_1\equiv 0(\mathrm{mod}\,m)$，从而 $m\mid e_1$. 但 $|e_1|<m$，所以 $e_1=0$. 于是上面的同余式可化为

$$e_2+me_3+\cdots+m^{n-2}e_n\equiv 0(\mathrm{mod}\,m^{n-1}).$$

同上可证 $e_2=0$. 重复进行，我们得出 $e_i=0\ (1\leqslant i\leqslant n)$，故在 $a_i=m^{i-1}\ (1\leqslant i\leqslant n)$ 时，没有符合要求的解.

注 19 设 m 为大于 1 的整数，$a_1,\cdots,a_m$ 是模 m 的一个完系，$\zeta\neq 1$ 是任意一个 m 次单位根，则我们有（见第 15 讲）

$$\zeta^{a_1}+\cdots+\zeta^{a_m}=0.$$

这是某些涉及完系的问题的一个基本入手点. 本题便是这样的一

个例子.

注 20 上述结论的逆命题并不正确(易于举出反例),但在 m 为素数这一重要的特殊情形,逆命题是正确的.换句话说,我们有下面的结果:

设 p 是素数,$\zeta\neq 1$ 是一个 p 次单位根.若整数 $a_1,\cdots,a_p$ 满足

$$\zeta^{a_1}+\cdots+\zeta^{a_p}=0, \tag{36}$$

则 $a_1,\cdots,a_p$ 是模 p 的一个完系.

为了证明,显然可设 $0\leqslant a_i\leqslant p-1$ $(i=1,\cdots,p-1)$.对 $k=0,1,\cdots,p-1$,设在 $a_1,\cdots,a_p$ 中共有 α_k 个为 k,则

$$\alpha_0+\alpha_1+\cdots+\alpha_{p-1}=p, \tag{37}$$

且等式(36)即为

$$\alpha_0+\alpha_1\zeta+\cdots+\alpha_{p-1}\zeta^{p-1}=0.$$

由 $\zeta^{p-1}=-(\zeta^{p-2}+\cdots+\zeta+1)$,上式可化为

$$(\alpha_0-\alpha_{p-1})+(\alpha_1-\alpha_{p-1})\zeta+\cdots+(\alpha_{p-2}-\alpha_{p-1})\zeta^{p-2}=0.$$

设 $f(x)=(\alpha_{p-2}-\alpha_{p-1})x^{p-2}+\cdots+(\alpha_1-\alpha_{p-1})x+(\alpha_0-\alpha_{p-1})$,则由上式可知 $f(\zeta)=0$.这表明,整系数多项式 $f(x)$ 与 $\Phi_p(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 有一个公共根 $x=\zeta$;但 $\Phi_p(x)$ 在 Q 上不可约(见第 13 讲中的(5)),故在 $Q[x]$ 上 $\Phi_p(x)$ 整除 $f(x)$(见第 12 讲中(14)).但 $\Phi_p(x)$ 的次数为 $p-1$,而 $f(x)$ 或为零多项式,或者次数不超过 $p-2$,故 $f(x)$ 必须为零,即 $\alpha_{p-1}=\alpha_{p-2}=\cdots=\alpha_1=\alpha_0$.结合(37),得出 $\alpha_k=1$ $(0\leqslant k\leqslant p-1)$,这就证明了 $a_1,\cdots,a_p$ 是 $0,1,\cdots,p-1$ 的一个排列.

例 15 设 $a_0,a_1,\cdots,a_n,x_0,x_1,\cdots,x_n$ $(n\geqslant 2)$ 均为整数,$r\geqslant 2$ 为整数,满足

$$\sum_{j=0}^{n}a_jx_j^k=0,\ k=1,2,\cdots,r.$$

证明:对任意正整数 m,$r+1\leqslant m\leqslant 2r+1$,均有

$$\sum_{j=0}^{n} a_j x_j^m \equiv 0 (\mathrm{mod}\, m).$$

证明　只要证明，对每个素数幂 $p^\alpha \mid m$，有 $p^\alpha \mid \sum_{j=0}^{n} a_j x_j^m$，为此目的，我们希望证明，对每个 $m(r+1 \leqslant m \leqslant 2r+1)$，有一个 m'，其中 $1 \leqslant m' \leqslant r$，使得

$$\sum_{j=0}^{n} a_j x_j^m \equiv \sum_{j=0}^{n} a_j x_j^{m'} (\mathrm{mod}\, p^\alpha),$$

由此及已知条件即得所需结果.

因为 $m \leqslant 2r+1$，故 $\frac{m}{p} \leqslant \frac{2r+1}{2} < r+1$；注意 $\frac{m}{p}$ 为整数，因此 $\frac{m}{p} \leqslant r$. 于是(注意 $\alpha \geqslant 1$)

$$r \geqslant \frac{m}{p} \geqslant p^{\alpha-1} \geqslant \alpha.$$

此外，因为 $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$，故 $\varphi(p^\alpha) \mid \left(m - \frac{m}{p}\right)$.

对任意 $x_j(0 \leqslant j \leqslant n)$，若 $p \mid x_j$，则由 $m > \frac{m}{p} \geqslant \alpha$ 得到

$$x_j^m \equiv x_j^{\frac{m}{p}} (\mathrm{mod}\, p^\alpha). \qquad ㊳$$

若 $p \nmid x_j$，则由 $\varphi(p^\alpha) \left| \left(m - \frac{m}{p}\right)\right.$ 及欧拉定理，得出 $x_j^{m-\frac{m}{p}} \equiv 1 (\mathrm{mod}\, p^\alpha)$，从而㊳对于 $p \nmid x_j$ 也成立. 因此㊳对于任意 x_j 均成立.

因为 $\frac{m}{p} \leqslant r$，故由㊳及已知条件得出

$$\sum_{j=0}^{n} a_j x_j^m \equiv \sum_{j=0}^{n} a_j x_j^{\frac{m}{p}} = 0 (\mathrm{mod}\, p^\alpha),$$

即 $p^{\alpha} \mid \sum_{j=0}^{n} a_j x_j^m$ 对所有 $p^{\alpha} \mid m$ 成立，从而结论得证.

例 16 设 $p>3$ 是素数，a、b 为正整数. 证明：

$$\binom{pa}{pb} \equiv \binom{a}{b} (\mathrm{mod}\ p^3).$$

证明 可设 $a>b$，否则结论显然成立.

论证的第一步，是将 $\binom{pa}{pb}$ 表示成 $\binom{a}{b}$ 与某个特别形式的数的乘积，设

$$F(x)=(x-1)\cdot\cdots\cdot(x-(p-1)). \tag{39}$$

则易于得到

$$\begin{aligned}\binom{pa}{pb} &= \frac{pa}{pb}\cdot\frac{F(pa)}{F(pb)}\cdot\frac{pa-p}{pb-p}\cdot\frac{F(pa-p)}{F(pb-p)}\cdot\cdots\cdot\\ &\quad \frac{(pa-(b-1)p)}{(pb-(b-1)p)}\cdot\frac{F(pa-(b-1)p)}{F(pb-(b-1)p)}\\ &= \binom{a}{b}\frac{\prod\limits_{t=a-b+1}^{a} F(pt)}{\prod\limits_{t=1}^{b} F(pt)}.\end{aligned} \tag{40}$$

当 $p>3$ 时，对上式右边的每个“单项”$F(pt)$，由 (39) 我们有

$$\begin{aligned}F(pt) &= (pt)^{p-1}-S_1(pt)^{p-2}+\cdots+S_{p-3}(pt)^2-S_{p-2}(pt)+S_{p-1}\\ &\equiv S_{p-3}(pt)^2-S_{p-2}(pt)+S_{p-1}(\mathrm{mod}\ p^3),\end{aligned} \tag{41}$$

这里 $S_{p-1}=(p-1)!$，$S_{p-2}=(p-1)!\left(1+\frac{1}{2}+\cdots+\frac{1}{p-1}\right)$.

在第 12 讲例 9 中，我们已证明了对素数 $p>3$，数 S_1，…，S_{p-3} 都是 p 的倍数，而 S_{p-2} 被 p^2 整除，故由 (41) 知

$$F(pt)\equiv(p-1)!(\mathrm{mod}\ p^3).$$

现在由㊵得到

$$\binom{pa}{pb}\equiv\binom{a}{b}\frac{((p-1)!)^b}{((p-1)!)^b}\equiv\binom{a}{b}(\mathrm{mod}\ p^3).\ \text{证毕.}$$

注 21　对 $a=2$，$b=1$ 这一特殊情形，本题可更直接地证明如下：

由范德蒙恒等式(见第 2 讲注 4)，我们有

$$\binom{2p}{p}=\sum_{k=0}^{p}\binom{p}{k}^2=2+p^2\sum_{k=1}^{p-1}\frac{1}{k^2}\binom{p-1}{k-1}^2,$$

由此结合第 8 讲例 4 及例 5 得出，对 $p\geqslant 5$，

$$\binom{2p}{p}\equiv 2+p^2\sum_{k=1}^{p-1}\frac{1}{k^2}\equiv 2(\mathrm{mod}\ p^3).$$

例 17　证明：不定方程 $x^2-2=7^y$ 仅有一组正整数解 $x=3$，$y=1$.

证明　显然 $x=3$，$y=1$ 是方程的解. 下面证明，方程没有 $y>1$ 的解.

将方程模 8，易知左端 $\equiv -2,-1,2(\mathrm{mod}\ 8)$，右端 $\equiv(-1)^y(\mathrm{mod}\ 8)$，故 y 必是奇数. 设 $y=2k+1$，$k\geqslant 1$.

将方程两边同乘 7^y 并配方，得到

$$(7^{2k+1}+1)^2-7(7^kx)^2=1.$$

因此 $u=7^{2k+1}+1$，$v=7^kx$ 是沛尔方程

$$u^2-7v^2=1 \qquad ㊷$$

的一组解. 易知这一方程的基本解为 $u=8$，$v=3$，故其全部正整数解 (u_n,v_n) 由

$$u_n+v_n\sqrt{7}=(8+3\sqrt{7})^n,\ n=1,2,\cdots \qquad ㊸$$

给出.(参见第 9 讲中第二节的(2)，特别是公式⑭.)因此，有一个 $n\geqslant 1$，使得

$$7^{2k+1}+1=8^n+\binom{n}{2}8^{n-2}\cdot 3^2\cdot 7+\binom{n}{4}8^{n-4}\cdot 3^4\cdot 7^2+\cdots, \tag{44}$$

$$7^k x=\binom{n}{1}8^{n-1}\cdot 3+\binom{n}{3}\cdot 8^{n-3}\cdot 3^3\cdot 7+\binom{n}{5}8^{n-5}\cdot 3^5\cdot 7^2+\cdots. \tag{45}$$

现在我们比较等式㊺两边所含的 7 的幂次. 设 $7^l \parallel n$, 易知, 当 $m\geqslant 1$ 时, $\binom{n}{2m+1}7^m=\frac{n}{2m+1}\binom{n-1}{2m}7^m$ 中所含的 7 的幂次 $>l$, 故右边所含的 7 的幂次为 l, 而左边所含的 7 的幂次至少是 k, 故 $k\geqslant l$, 即 $7^k \mid n$, 从而 $n\geqslant 7^k$. 所以当 $k\geqslant 1$ 时有

$$8^n\geqslant 8^{7^k}>7^{2k+1}+1,$$

故等式㊹的右边大于左边, 矛盾. 这证明了当 $k\geqslant 1$, 即 $y>1$ 时方程无正整数解.

注 22 有几种显然的方式, 可以将本题中的方程化为沛尔型方程. 例如, 设 $y=2k+1$, 则 $u=x$, $v=7^k$ 是方程

$$u^2-7v^2=2, \tag{46}$$

的一组正整数解.

方程㊻有正整数解 $u=3$, $v=1$. 由此可知它有无穷组正整数解 $\begin{cases}u=3u_n+7v_n,\\ v=3v_n+u_n,\end{cases}$

这里 (u_n, v_n) 是方程㊷的解(请见第 9 讲中的(2), 特别是公式⑯). 但这些解是否为㊻的全部正整数解, 需要单独研究. 因此, 将问题化为方程㊻, 将引出一些麻烦, 我们宜改弦更张.

将原方程化为沛尔方程㊷, 或许需要一点机智. 产生㊷的优点在于, 其全部正整数解有一个简明的表达式, 即㊸式.

注 23 上述论证的第二个要点是证明等式㊹及㊺在 $n>1$ 时不能成立.

在初等范围中, 证明两个整数 a、b 不相等的方式主要有两

种. 其一是代数角度的考虑:若 $a>b$(或 $a<b$),自然有 $a\neq b$;其二是算术(同余)角度的考虑:若有一个正整数 m,使 a、b 被 m 除得的余数不同,则必然 $a\neq b$(参见第 9 讲中注 2).

本题中,我们首先通过比较㊺两边(素数)7 的幂,产生 n 满足的必要条件(这本质上是同余角度的考虑,参见第 20 讲中注 2);基于此,再由代数角度的考虑,导出等式㊹不能成立.