单 增 主编

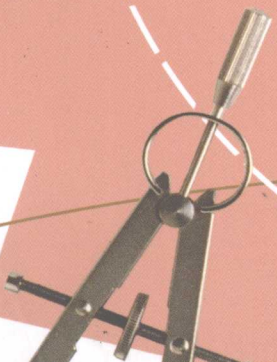
数学奥林匹克

命题人讲座

初等数论

冯志刚 著

上海科技教育出版社



单 墫 主编

数学奥林匹克命题人讲座

初等数论

冯志刚 著

上海科技教育出版社

责任编辑：卢　源　李　凌
封面设计：童郁喜

＊数学奥林匹克命题人讲座＊
初等数论
单　壿　主编
冯志刚　著
上海世纪出版股份有限公司
上海科技教育出版社　出版发行
（上海市冠生园路 393 号　邮政编码 200235）
www.ewen.cc　www.sste.com
全国新华书店经销　上海市印刷七厂有限公司印刷
开本 890×1240　1/32　印张 9.375　字数 243 000
2009 年 1 月第 1 版　2009 年 1 月第 1 次印刷
ISBN 978-7-5428-4767-6/O・596
定价：21.00 元

丛书序

读书，是天下第一件好事。

书，是老师。他循循善诱，传授许多新鲜知识，使你的眼界与思路大开。

书，是朋友。他与你切磋琢磨，研讨问题，交流心得，使你的见识与能力大增。

书的作用太大了！

这里举一个例子：常庚哲先生的《抽屉原则及其他》（上海教育出版社，1980年）问世后，很快地，连小学生都知道了什么是抽屉原则。而在此以前，几乎无人知道这一名词。

读书，当然要读好书。

常常有人问我：哪些奥数书好？希望我能推荐几本。

我看过的书不多。最熟悉的是上海的出版社出过的几十本小册子。可惜现在已经成为珍本，很难见到。幸而上海科技教育出版社即将推出一套“数学奥林匹克命题人讲座”丛书，帮我回答了这个问题。

这套丛书的书名与作者初定如下：

陆洪文	《解析几何》
施咸亮	《代数函数与多项式》
熊　斌	《函数迭代与函数方程》
陈　计　季潮丞	《代数不等式》
曹　纲　叶中豪	《重心坐标与平面几何》
冯志刚	《初等数论》
单　墫	《集合与对应》《数列与数学归纳法》
刘培杰	《组合问题》
任　韩　田廷彦	《图论·组合几何》

唐立华　　《向量与立体几何》

邵嘉林　　《复数·三角函数》

显然，作者队伍非常之强。老辈如陆洪文先生、施咸亮先生都是博士生导师。他们不仅在代数数论、函数逼近等领域的研究上取得了卓越的成绩，而且十分关心数学竞赛。中年如陈计先生于不等式，叶中豪先生于平面几何，都是国内公认的首屈一指的专家。其他各位也都是当下国内数学奥林匹克的领军人物。如熊斌、冯志刚是 2008 年 IMO 中国国家队的正副领队、中国数学奥林匹克委员会委员。他们为我国数学奥林匹克做出了重大的贡献，培养了很多的人才。2008 年 9 月 14 日，“国际数学奥林匹克研究中心”在华东师范大学挂牌成立，担任这个研究中心主任的正是多届 IMO 中国国家队领队、华东师范大学数学系副教授熊斌。又如邵嘉林先生，他指导过的张成同学获得了第 49 届 IMO 的金牌。

这些作者有一个共同的特点：他们都为数学竞赛命过题。

如：

设数 a 具有以下性质：对于任意四个实数 x_1, x_2, x_3, x_4，总可以取整数 k_1, k_2, k_3, k_4，使得

$$\sum_{1\leqslant i<j\leqslant 4}((x_i-k_i)-(x_j-k_j))^2\leqslant a,$$

求这样的 a 的最小值。

这是施咸亮先生供给我国国家集训队选拔的试题。

又如：

设 $S=\{1,2,\cdots,2005\}$。若 S 中任意 n 个两两互素的数组成的集合中都至少有一个素数，试求 n 的最小值。

这是唐立华先生供给西部数学奥林匹克的试题。

叶、熊、冯等几位先生供给竞赛的题举不胜举，这里就不罗列了。

命题人讲座，是田廷彦先生的创意。

命题人写书，富于原创性。有许多新的构想、新的问题、新的解法、新的探讨。新，是这套丛书的一大亮点。读者一定会从这套丛书中学到很多新的知识，产生很多新的想法。

新，会不会造成深、难呢？

这套书当然会有一定的深度，一定的难度。但作者是命题人，充分了解问题的背景（如刘培杰先生就曾专门研究过一些问题的背景），写来能够深入浅出，“百炼钢化为绕指柔”。另一方面，倘若一本书十分浮浅，一点难度没有，那也就失去了阅读的价值。

读书，难免遇到困难。遇到困难，不能放弃。要顶得住，坚持下去，锲而不舍。这样，你不但读懂了一本好书，而且也学会了读书，享受到读书的乐趣。

书的作者，当然要努力将书写好。但任何事情都难以做到完美无缺。经典著作尚且偶有疏漏，富于原创的书更难免有考虑不足的地方。从某种意义上说，这种不足毋宁说是一种优点：它给读者留下了思考、想象、驰骋的空间。

如果你在阅读中，能够想到一些新的问题或新的解法，能够发现书中的不足或改进书中的结果，那就是古人所说的“读书得间”，值得祝贺！

我们欢迎各位读者对这套丛书提出建议与批评。

感谢上海科技教育出版社，特别是编辑卢源先生，策划组织编写了这套书。卢编辑认真把关，使书中的错误减至最少，又在书中设置了一些栏目，使这套书增色很多。

单　壿

2008 年 10 月

符号说明

$\mathbf{N}$ 自然数 0,1,2,…组成的集合

$\mathbf{N}^*$ 正整数集

$\mathbf{Z}$ 整数集

$\mathbf{Q}$ 有理数集

$\mathbf{R}$ 实数集

(a,b) 整数 a,b 的最大公因数

$[a,b]$ 整数 a,b 的最小公倍数

$a\mid b$ 整数 a 能整除 b

$a\nmid b$ 整数 a 不能整除 b

$p^\alpha \parallel n$ 表示 $p^\alpha \mid n$ 但 $p^{\alpha+1}\nmid n$,这里 p 为素数,$\alpha\in\mathbf{N}$

$v_p(n)$ 表示上面的 α,其含义是 n 的素因数分解式中素数 p 的幂次

$a^{-1}(\mathrm{mod}\ m)$ 整数 a 关于模 m 的数论倒数

$\delta_m(a)$ 整数 a 对模 m 的指数

$\varphi(m)$ $1,2,\cdots,m$ 中与 m 互素的数的个数

$d(n)$ 正整数 n 的正因数的个数

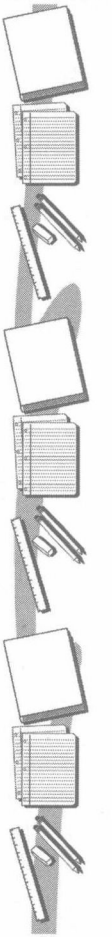
$\sigma(n)$ 正整数 n 的所有正因数之和

$[x]$ 不超过实数 x 的最大整数,即 x 的整数部分

$\{x\}$ 实数 x 的小数部分,即 $\{x\}=x-[x]$

C_n^m 从 n 件物品中取出 m 件物品的方法数

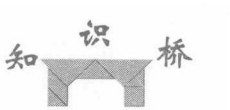
目录



第一讲 整除理论

人类对数的认识源于实践经验，数的发展经历了从自然数到整数、到有理数、到实数、到复数等的过程. 数论是讨论整数及其性质的理论，它是数学的一个重要分支，是数学中的一门基础性学科.

1.1 整　　数



用 $\mathbf{N}^*$ 表示所有正整数 $1,2,3,\cdots$ 组成的集合，其最本质的属性可用数学语言描述如下：

归纳公理　设 $S\subseteq\mathbf{N}^*$，若 S 满足下述条件：

(1) $1\in S$；

(2) 如果 $n\in S$，那么 $n+1\in S$，则 $S=\mathbf{N}^*$.

这条公理是数论的基础与出发点，由它出发可以依次推出下面的一些著名定理.

数学归纳法　设 $P(n)$ 是关于正整数 n 的一个命题，如果

(1) 当 $n=1$ 时，$P(1)$ 成立；

(2) 由命题 $P(n)$ 成立，可以推出 $P(n+1)$ 成立，则对任意 $n\in\mathbf{N}^*$，命题 $P(n)$ 都成立.

第二数学归纳法　设 $P(n)$ 是关于正整数 n 的一个命题，如果

(1) 当 $n=1$ 时，$P(1)$ 成立；

(2) 由命题 $P(1),P(2),\cdots,P(n)$ 都成立，可以推出 $P(n+1)$ 成立，那么，对任意 $n\in\mathbf{N}^*$，命题 $P(n)$ 都成立.

最小数原理　正整数集的任意一个非空子集都有一个最小元.

需要指出的是：由数学归纳法证出的结论是对任意有限数 n，命题

$P(n)$成立，并不意味着 $P(+\infty)$也成立. 对这一点的理解会随着数学知识的增多和能力的增强而逐渐加深，它从一个侧面反映了“有限”与“无限”的本质区别.

1.2 整除的概念与基本性质

由于整数集对加法、减法和乘法运算都是封闭的，但对除法运算不封闭，因而初等数论将更多地关注除法运算.

定义 设 $a,b\in\mathbf{Z},a\neq0$，若存在 $q\in\mathbf{Z}$，使得 $b=aq$，则称 b 能被 a 整除(或称 a 能整除 b)，记作 $a|b$. 否则，称 b 不能被 a 整除，记作 $a\nmid b$.

如果 $a|b$，那么我们称 a 为 b 的因数，b 为 a 的倍数. 关于数的整除，有下面的一些基本性质.

定理 1 (1) 下面的等价关系成立：

$$a|b\Leftrightarrow(-a)|b\Leftrightarrow a|(-b).$$

因此，整除理论总是讨论正整数之间的整除关系.

(2) 若 $a|b,b|c$，则 $a|c$.

(3) 若 $a|b,a|c$，则对任意 $x,y\in\mathbf{Z}$，都有 $a|(bx+cy)$，即 a 整除 b，c 的任意一个整系数线性组合.

(4) 若 $a|b,b\neq0$，则 $|a|\leqslant|b|$. 依此可知，若 a,b 都是正整数，$a|b$ 且 $b|a$，则 $a=b$，这给出了证明两个正整数相等的常用方法.

这些基本性质都可由整除的定义非常容易地推导出来，它们看上去是如此的平凡，但都是非常有用的.

定理 2(带余除法) 设 $a,b\in\mathbf{Z},a\neq0$，则存在唯一的一对整数 q 和 r，满足：

$$b=aq+r, \tag{1}$$

这里 $0\leqslant r<|a|$.

证明 先证存在性.

如果 $a|b$，那么 $r=0$，$q=\dfrac{b}{a}$ 符合(1)式.

如果 $a\nmid b$，考察集合

$$T=\{b-aq\mid q\in\mathbf{Z}\}.$$

由于 T 中有正整数，设 T 的所有正整数组成的集合为 T^*，则由最小数原理知 T^* 中有最小元 r，并设 $b-aq=r$，则 $r<|a|$（否则设 $r\geqslant|a|$，若 $r=|a|$，导出 $a|b$，矛盾，故 $r>|a|$，这时 $b-aq-|a|=r-|a|$ 是小于 r 的正整数，与 r 为 T^* 中最小的正整数矛盾），所以，存在符合要求的整数对 (q,r).

再证唯一性.

若存在两个整数对 (q_1,r_1) 和 (q_2,r_2) 符合(1)式，则有

$$aq_1+r_1=aq_2+r_2,$$

即 $a(q_1-q_2)=r_2-r_1$，故 $a|(r_2-r_1)$. 由 $0\leqslant r_1,r_2<|a|$，知

$$0\leqslant|r_2-r_1|<|a|,$$

这样，由定理 1 中的(4)可知，必有 $|r_2-r_1|=0$，从而 $r_2=r_1$，进而 $aq_1=aq_2$，导出 $q_1=q_2$. 矛盾. 唯一性获证.

带余除法定理可以说是初等数论中最重要、最基本、最直接的一个工具，它的一个重要应用是下面的辗转相除法（即通常所说的欧几里得(Euclid)算法）.

定理 3（欧几里得算法） 设 u_0,u_1 是两个给定的整数，$u_1\neq0$，且 $u_1\nmid u_0$，则由定理 2，可经有限步运算（辗转相除）得到下面的等式：

$$u_0=u_1q_0+u_2,\ 0<u_2<|u_1|,$$

$$u_1=u_2q_1+u_3,\ 0<u_3<u_2,$$

$$\cdots$$

$$u_{k-1}=u_kq_{k-1}+u_{k+1},\ 0<u_{k+1}<u_k,$$

$$u_k=u_{k+1}q_k.$$

这个相对较繁的算法在理论和应用方面都有很重要的价值.

训练营

例 1 设 a,b,n 为给定的正整数，已知对任意 $k\in\mathbf{N}^*$ $(k\neq b)$，都有

$(b-k)\mid(a-k^n)$. 证明：$a=b^n$.

证明 注意到，对任意 $k\in\mathbf{N}^*$ $(k\neq b)$，有

$$b^n-k^n=(b-k)(b^{n-1}+b^{n-2}k+\cdots+k^{n-1}),$$

故$(b-k)\mid(b^n-k^n)$，结合$(b-k)\mid(a-k^n)$，可知

$$(b-k)\mid((a-k^n)-(b^n-k^n)),$$

即$(b-k)\mid(a-b^n)$.

取 $k=b+1+|a-b^n|$，可知

$$-(1+|a-b^n|)\mid(a-b^n),$$

这样，由定理 1 的(4)可知 $a-b^n=0$，命题获证.

点评 此题处理中蕴含了一个思想：在处理整除性问题时，应尽量让被除数简单化、常数化.

例 2 设 $k\in\mathbf{N}^*$，$k\geqslant 2$，而 n 是一个不小于 $2k$ 的正整数.

(1) 证明：存在整数 $i\in\{0,1,2,\cdots,k-1\}$，使得$(n-i)\nmid C_n^k$；

(2) 证明：对每个 $k\geqslant 2$，存在正整数 $n_k\geqslant 2k$，使得恰有一个 $i\in\{0,1,2,\cdots,k-1\}$，满足$(n_k-i)\nmid C_{n_k}^k$.

证明 (1) 用反证法证明，若否，设存在 $k\geqslant 2$ 及 $n\geqslant 2k$，使得 $n,n-1,\cdots,n-(k-1)$都是组合数 C_n^k 的因数.

由 $n(n-1)\cdot\cdots\cdot(n-(k-1))=k!C_n^k$，我们有

$$\begin{cases}(n-1)(n-2)\cdot\cdots\cdot(n-k+1)\in(k!)\mathbf{N}^*,\\ n(n-2)\cdot\cdots\cdot(n-k+1)\in(k!)\mathbf{N}^*,\\ \cdots\\ n(n-1)\cdot\cdots\cdot(n-k+2)\in(k!)\mathbf{N}^*,\end{cases}$$

这里$(k!)\mathbf{N}^*=\{x\mid x=(k!)y,\ y\in\mathbf{N}^*\}$.

将上面的式子从第二个起，每一个减去前面一个式子，可得

$$\begin{cases}(n-2)(n-3)\cdot\cdots\cdot(n-k+1)\in(k!)\mathbf{N}^*,\\ n(n-3)\cdot\cdots\cdot(n-k+1)\in(k!)\mathbf{N}^*,\\ \cdots\\ n(n-1)(n-2)\cdot\cdots\cdot(n-k+3)\in(k!)\mathbf{N}^*.\end{cases}$$

经过这样的处理后，我们由 k 个式子变为了 $k-1$ 个式子. 依此操作 $k-1$ 次后，得

$$2\cdot 3\cdot\cdots\cdot(k-1)\in(k!)\mathbf{N}^*,$$

这要求 $k!\mid(k-1)!$，即 $\frac{1}{k}\in\mathbf{N}^*$，与 $k\geqslant 2$ 矛盾.

所以，至少有一个 $i\in\{0,1,2,\cdots,k-1\}$，使得 $(n-i)\nmid C_n^k$.

(2) 对 $k=2$，取 $n_2=4$ 即可；而当 $k\geqslant 3$ 时，取 $n_k=k!$，可知

$$C_{n_k}^k=(n_k-1)\cdot\cdots\cdot(n_k-(k-1))$$

满足条件.

点评 这个问题的解决尽管只用到了整除的一些基本性质，但它无疑是一个难题. 被除数之间的相互联系需要有敏锐的观察力才能发现. 数学中往往最简单的都是本质的和困难的.

1.3 最大公因数与最小公倍数

如果 m 是 a 的因数，也是 b 的因数，那么称 m 为 a 和 b 的公因数. 由整除性质知，当 $a\neq 0$ 时，有 $m\leqslant|a|$，依此可得，若 a,b 不全为零，则 a 和 b 的公因数中有一个最大的数(这可由最小数原理导出)，记这个最大的公因数为 (a,b). 进一步，类似地，我们可以定义 n 个整数 a_1，$a_2,\cdots,a_n$ 的最大公因数，记作 $(a_1,a_2,\cdots,a_n)$.

对称地，若 m 既是 a 的倍数，也是 b 的倍数，则称 m 为 a 和 b 的公倍数(这里当然要求 a,b 都不为零). 用 $[a,b]$ 表示 a 和 b 的公倍数中最小的那个正整数，类似地，可定义 n 个非零整数 $a_1,a_2,\cdots,a_n$ 的最小公倍数，记作 $[a_1,a_2,\cdots,a_n]$.

关于最大公因数有如下著名的定理：

贝祖(Bezout)定理 设 a,b 是不全为零的整数，则存在整数 x,y，使得

$$ax+by=(a,b). \tag{1}$$

证明 记 $d=(a,b)$，在上一节定理 3 的欧几里得算法中，取 $u_0=a,u_1=b$(这里不妨设 $b\neq 0$)，则由整除的性质，可知 $d\mid u_2,d\mid u_3,\cdots,d\mid u_{k+1}$. 所以，$d\leqslant u_{k+1}$.

反过来，再由整除的性质，可知 $u_{k+1}\mid u_k,u_{k+1}\mid u_{k-1},\cdots,u_{k+1}\mid u_1,u_{k+1}\mid u_0$，即 u_{k+1} 为 a 与 b 的一个公因数. 因此，$u_{k+1}\leqslant d$.

上述讨论表明：$d=u_{k+1}$. 现在倒过来利用欧几里得算法中的式子，可知

$$u_{k+1}=u_{k-1}-u_kq_{k-1}=u_{k-1}-(u_{k-2}-u_{k-1}q_{k-2})q_{k-1}=\cdots$$

我们依次用 u_{k-1} 与 u_k 的线性组合表示出了 u_{k+1}；用 u_{k-2} 与 u_{k-1} 的线性组合表示出了 u_{k+1}；……；最后用 u_0,u_1 的线性组合表示出了 u_{k+1}. 因此，使得(1)成立的整数 x,y 存在.

类似地，对更多的整数 $a_1,a_2,\cdots,a_k$ 亦有同样的结论.

如果 $(a,b)=1$，那么称 a 与 b 互素，依上述定理结合整除的性质，可知

$(a,b)=1\Leftrightarrow$存在 $x,y\in\mathbf{Z}$，使得 $ax+by=1$.

利用贝祖定理结合整除的性质，我们还可知：(a,b) 是集合 $\{ax+by\mid x,y\in\mathbf{Z}\}$ 中的最小正整数，这体现了“最大”与“最小”的某种统一.

下面我们列出一些与最大公因数和最小公倍数有关的结论.

(1) 若 m 为 a,b 的公因数，则 $m\mid(a,b)$.

(2) 若 $a\mid bc$，且 $(a,b)=1$，则 $a\mid c$.

事实上，由贝祖定理知，存在 $x,y\in\mathbf{Z}$，使得 $ax+by=1$，故

$$acx+bcy=c.$$

结合 $a\mid bc$，即可得 $a\mid c$，所以(2)成立. 类似可证下面的.

(3) 若 $a\mid c,b\mid c$，且 $(a,b)=1$，则 $ab\mid c$.

(4) 设 m 为正整数，则 $(ma,mb)=m(a,b)$，$[ma,mb]=m[a,b]$.

证明 记 $d'=(ma,mb)$，$d=(a,b)$，则 $md\mid ma,md\mid mb$，故 $md\leqslant d'$. 反过来，由贝祖定理知，存在 $x,y\in\mathbf{Z}$，使得 $ax+by=d$，所以，

$$amx+bmy=md,$$

依此可知 $d'\mid md$，故 $d'\leqslant md$. 所以，$md=d'$. 另外，由 $ma\mid m[a,b]$，$mb\mid m[a,b]$，可知 $[ma,mb]\leqslant m[a,b]$，而由 $ma\mid[ma,mb]$ 知 $a\left|\frac{[ma,mb]}{m}\right.$，同理 $b\left|\frac{[ma,mb]}{m}\right.$，故

$$[a,b]\leqslant\frac{[ma,mb]}{m}.$$

(4) 获证.

(5) 设 a,b 都为正整数，则 $(a,b)\cdot[a,b]=ab$.

证明 先证当 $(a,b)=1$ 时，有 $[a,b]=ab$.

事实上，由 $a\mid[a,b]$，$b\mid[a,b]$，以及 $(a,b)=1$，利用(3)就有 $ab\mid[a,b]$，故 $ab\leqslant[a,b]$. 另一方面，ab 显然是 a 与 b 的公倍数，故 $[a,b]\leqslant ab$. 所以，$[a,b]=ab$.

再证 $(a,b)\cdot[a,b]=ab$.