经全国中小学教材审定委员会
2005年初审通过

普通高中课程标准实验教科书

数学

选修 4–6

初等数论初步

人民教育出版社　课程教材研究所
中学数学课程教材研究开发中心　编著

人民教育出版社
A版

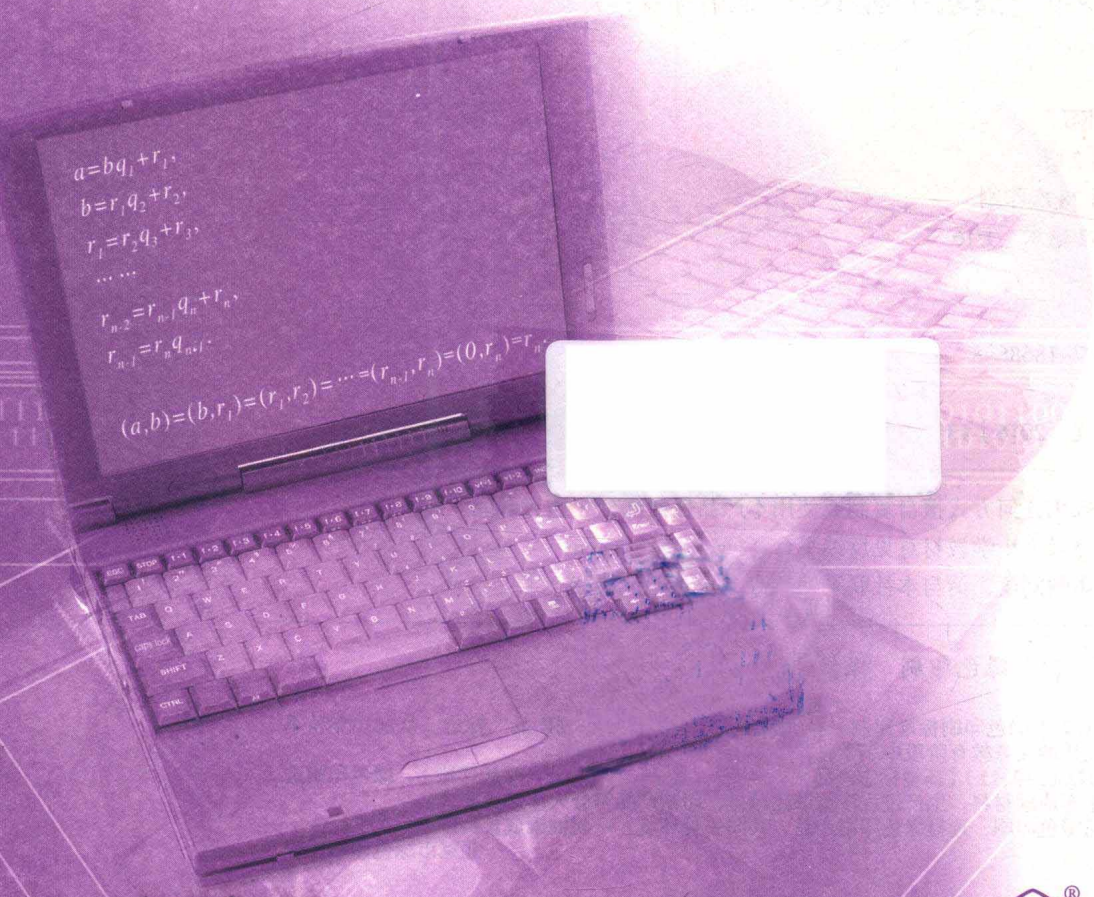
普通高中课程标准实验教科书

数学

选修 4–6

初等数论初步

人民教育出版社　课程教材研究所
中学数学课程教材研究开发中心　编著



人民教育出版社
A版

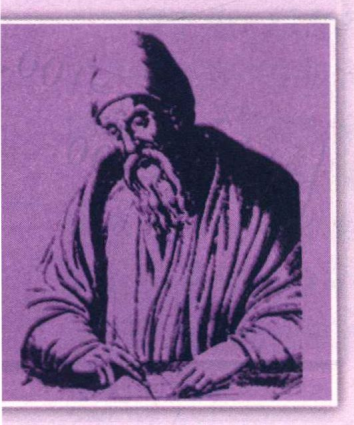
普通高中课程标准实验教科书　数学　选修 4-6　A 版　初等数论初步

人民教育出版社　课程教材研究所
中学数学课程教材研究开发中心　编著

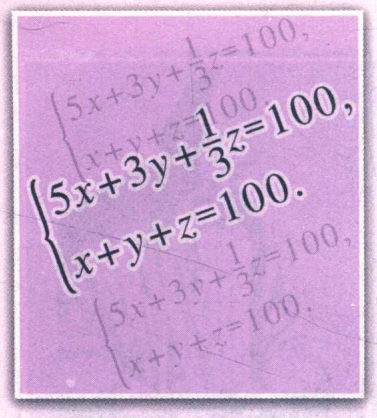
出版发行　人民教育出版社
（北京市海淀区中关村南大街17号院1号楼　邮编：100081）
网　　址　http://www.pep.com.cn
经　　销　全国新华书店
印　　刷　北京天宇星印刷厂
版　　次　2007 年 2 月第 2 版
印　　次　2017 年 7 月第 28 次印刷
开　　本　787 毫米 × 1092 毫米　1/16
印　　张　3.75
字　　数　77 千字
书　　号　ISBN 978-7-107-18686-8
定　　价　4.00 元
价格依据文件号：京发改规［2016］13号

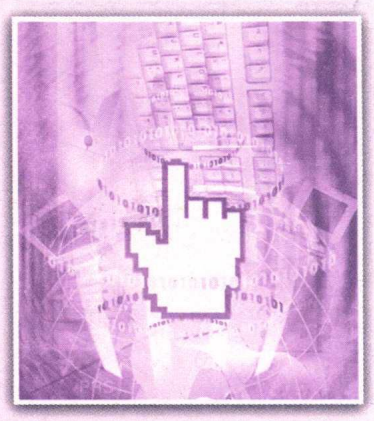
主　　编：刘绍学
副 主 编：钱珮玲　章建跃

主要编者：胡永建
责任编辑：张劲松
美术编辑：王俊宏　王　艾
封面设计：林荣桓　吴　敬



目录





引言

九　月						
日	一	二	三	四	五	六
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

数论是研究整数的性质和方程的整数解的一门学科. 它起源于古代的东方，距今大约有 3000 年的历史.

我国古代数学家在数论方面取得了一些重要成就. 《周髀算经》记载有西周人商高提出的“勾广三，股修四，径隅五”的论断，它实际上给出了方程 $x^2+y^2=z^2$ 有一组正整数解 (3，4，5). 《九章算术》记载有另外的四组正整数解：(5，12，13)，(8，15，17)，(7，24，25)，(20，21，29). 我国另一部重要数学著作《孙子算经》中记载有“物不知数”问题：“今有物不知其数，三三数之余二，五五数之余三，七七数之余二，问物几何?”答曰：“二十三.”这一问题和它的解法一起被后人称为孙子定理（国外文献称之为中国剩余定理).

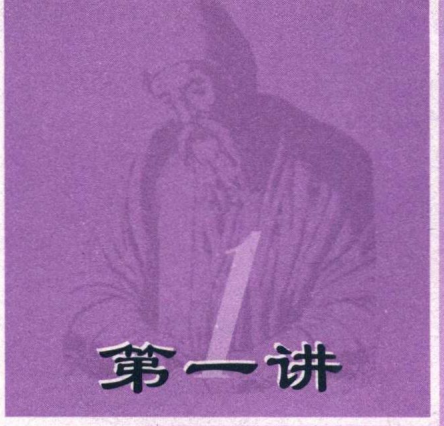
我国古代的数论研究具有鲜明的直观、实用和算法特性. 古希腊的数论研究则具有理性的特点，其成就集中反映在两部数学著作中，一部是欧几里得的《几何原本》，它给出了算术基本定理、素数有无限多个、辗转相除法等初等数论的重要结果；另一部是丢番图的《算术》，这是历史上第一部脱离几何，完全讲述数论的著作，书中讨论了 300 多个数论问题，列举了一些一次方程和二次方程的整数解的解法.

数论是一门古老而又基础的数学分支，至今仍有许多没有解决的问题. 这些数论问题对人类智慧产生极大的挑战，人们为解决这些数论问题所作的贡献，对数论乃至整个数学的发展起了重要的推动作用. 一个典型的例子就是费马猜想的解决.

1637 年，法国数学家费马提出猜想：方程 $x^n+y^n=z^n$ 没有正整数解，其中 n 为大于 2 的整数. 300 多年来，许多专业数学家和业余数学爱好者为解决此猜想作了不懈的努力，最终于 1994 年被英国数学家威尔斯（Wiles）解决. 在费马猜想的研究过程中，人们创造了研究数论的许多新方法，建立了数论的一些新分支，发现了它与数学其他领域的奇妙而深刻的联系.

当今的数论已经发展成为一门艰深的学问. 而且，随着计算机技术和数字通信技术的飞速发展，数论已经成为计算机科学和通信工程的重要数学工具之一.

本专题中，同学们将通过具体的问题，学习有关整数和整除的知识，探索用辗转相除法求解一次同余方程、一次同余方程组、简单的一次不定方程等，从中体会数论的基本思想方法，同时了解我国古代数学的一些重要成就.



$$a=bq_1+r_1,$$
$$b=r_1q_2+r_2,$$
$$r_1=r_2q_3+r_3,$$
$$\cdots\cdots$$
$$r_{n-2}=r_{n-1}q_n+r_n,$$
$$r_{n-1}=r_nq_{n+1}.$$

第一讲 整数的整除

我们知道，两个整数进行加法、减法、乘法运算，结果仍为整数. 但是，两个整数相除，不一定能除尽，也就是说，所得结果不一定为整数.

给定非零整数 n，如何找出所有除尽 n 的整数和被 n 除尽的整数；给定两个非零整数 a 和 b，如何找出所有同时除尽 a，b 的整数和同时被 a，b 除尽的整数. 如果给定的是多个非零整数，又该如何？

这些问题不仅有理论意义，而且还是后面解同余方程和不定方程的基础. 要完整地回答这些问题，我们需要学习整数的一些基本知识.

一 整除

1. 整除的概念和性质

思考

如何从乘法角度判断一个整数能除尽另一个整数？

我们知道，乘法与除法是互逆的两种运算. 要判断一个整数能否除尽另一个整数，只需考察被除数能否写成除数和某个整数的乘积. 只有当被除数可以表示为除数和某个整数的乘积时，除数恰好能除尽被除数. 此时，我们就说除数整除被除数，或者说被除数能被除数整除.

一般地，设 a，b 为整数，且 $b\neq 0$. 如果存在整数 q，使得 $a=bq$，那么称 b 整除 a，或者 a 能被 b 整除，记作 $b\mid a$. 并且称 b 是 a 的因数，a 是 b 的倍数. 如果这样的整数 q 不存在，就称 b 不整除 a，记作 $b\nmid a$.

例如，$6\mid -24$，$-4\mid 56$，$-4\nmid 14$，$8\mid 0$.

由此可知，能被非零整数 n 整除的整数是 n 的倍数，其一般形式为 nq，这里 q 为任意整数. 能除尽 n 的整数是 n 的因数，例如，能除尽 6 的整数为 1，-1，2，-2，3，-3，6，-6.

探究

由整除的概念，你能否推出下列整除的基本性质？

(1) 若 $a \mid b$，$b \mid a$，则 $a=b$，或 $a=-b$.

(2) 若 $a \mid b$，$b \mid c$，则 $a \mid c$.

(3) 若 $a \mid b$，$a \mid c$，则对任意整数 x，y，恒有 $a \mid bx+cy$.

如何判断一个非零整数整除给定的正整数？对某些特殊的非零整数，我们可以通过观察发现一些简单的判别方法.

观察

给定两组正整数：

第一组　6，　18，　21，　54，　81，　96，　108，　243

第二组　5，　17，　43，　80，　85，　98，　121，　212

第一组数有什么规律？它们能被什么整数整除？第二组数呢？计算每组数的各位数字之和，你能发现什么特征？

观察发现，第一组数能被 3 整除，并且其中每一个数的各位数字之和都能被 3 整除；第二组数不能被 3 整除，并且其中每一个数的各位数字之和也不能被 3 整除.

由此，我们猜想：

(1) **一个正整数的各位数字之和能被 3 整除，那么这个正整数能被 3 整除.**

这个命题是否正确？我们证明一下.

下面仅对 4 位正整数情形给出证明，同学们可以类比证明一般的情形.

证明：设 N 为 4 位正整数，且它的个、十、百和千位数字依次为 a，b，c，d，则

$$\begin{aligned} N &= d\times 10^3+c\times 10^2+b\times 10+a \\ &= d\times(999+1)+c\times(99+1)+b\times(9+1)+a \\ &= 999d+99c+9b+d+c+b+a. \end{aligned}$$

因为 $3 \mid 999d+99c+9b$，所以，当 $3 \mid d+c+b+a$ 时，$3 \mid N$.

探究

请用类似的方法证明能被 9，11，7 整除的正整数的下列特征：

(2) 一个正整数的各位数字之和能被 9 整除，那么这个正整数能被 9 整除；

(3) 一个正整数的奇数位数字之和与偶数位数字之和的差能被 11 整除，那么这个正整数能被 11 整除；

(4) 一个正整数的末三位数字组成的数与末三位数字之前的数字组成的数之差能被 7（或 11）整除，那么这个正整数能被 7（或 11）整除.

例 1 判断 710316 能否被 9，11 整除.

解：因为 7+1+0+3+1+6=18 能被 9 整除，所以 710316 能被 9 整除.

又因为 710316 的奇数位数字之和为 6+3+1=10，偶数位数字之和为 1+0+7=8，而 10−8=2 不能被 11 整除，所以 710316 不能被 11 整除.

2. 带余除法

我们知道，14÷3 的商为 4，余数为 2，即 14=3×4+2，这种表示法在整数集中仍然成立，我们把它叫做带余除法（或欧氏除法算式）.

一般地，设 a，b 为整数，且 $b\neq 0$，则存在惟一的一对整数 q 和 r，使得

$$a=bq+r,\ 0\leqslant r<|b|.$$

事实上，对任意整数 a 和非零整数 b，如果 a 是 b 的倍数，那么存在整数 q，使得 $a=bq$，此时 $r=0$. 如果 a 不是 b 的倍数，如图 1-1 所示（$b>0$ 的情形），由于 b 的倍数在数轴上是等距分布的，而且相邻两个倍数之间的距离为 $|b|$，而 a 是数轴上的一点，那么它一定落在 b 的两个相邻倍数之间. 此时，将紧邻 a 的左侧 b 的倍数记作 bq，选取 r 为 a 与 bq 的距离，此时 $a=bq+r$（从数轴上可以直观地看出）. 这就说明了满足上述等式的整数 q 和 r 是存在的.

图 1-1

下面说明 q 和 r 是惟一的，如果整数对 q' 和 r' 也满足

$$a=bq'+r',\ 0\leqslant r'<|b|,$$

那么 $a=bq+r=bq'+r'$，即 $r-r'=b(q'-q)$，

于是 $b\mid(r-r')$，而 $-|b|<r-r'<|b|$，

因此，$r-r'=0$，即 $r=r'$，从而 $q=q'$.

所以，q 和 r 是惟一的.

我们把带余除法中惟一的 q 和 r 分别叫做 a 除以 b 的商和余数. 显然，a 能被 b 整除当且仅当余数 $r=0$.

例 2 2004 除以某个整数，其商为 74，求除数和余数.

解：设除数为 b，余数为 r，则

$$2004=74b+r,\ 0\leqslant r<b.$$

欧几里得（Euclid，生卒年不详，约活动于公元前 300 年前后），古希腊数学家.

古希腊的数论成就集中反映在欧几里得的几何《原本》一书中，全书共 13 卷，其中 5 卷讲数论，主要包括欧氏除法算式、算术基本定理、素数有无限多个等.

由此可得

$$74b\leqslant 2004<74b+b=75b,$$

从而有

$$74\leqslant\frac{2004}{b}<75,$$

所以

$$\frac{2004}{75}<b\leqslant\frac{2004}{74},$$

即

$$26\frac{18}{25}<b\leqslant 27\frac{3}{37}.$$

因此，$b=27$，$r=2004-27\times 74=6$.

探究

我们用符号$[x]$❶表示不超过实数x的最大整数，试用a，b表示a除以正整数b的商q和余数r.

3. 素数及其判别法

考察正整数的正因数，我们发现，有的正整数仅有一个正因数（如1），有的正整数仅有两个正因数（如3，13，31），而有的正整数至少有三个正因数（如12，14，81）.

我们把仅有两个正因数的正整数叫做**素数**，不是素数又不是1的正整数叫做**合数**.

由定义知，3，13，31是素数，12，14，81是合数，1既不是素数，也不是合数.

显然，2是惟一的偶素数，也是最小的素数. 每个合数总可以表示成两个大于1的正整数的乘积，而素数则不能.

观察

找出下列每个正整数的正因数：

6，7，9，21，65，77，121.

观察每个正整数除1外的最小的一个正因数，从中你能发现什么规律？

我们发现，每个正整数n除1外的最小正因数p是一个素数. 事实上，假设p不是素数，因为$p>1$，所以p为合数，那么p必然有1，p以外的正因数q，使得$q\mid p$. 因为

❶ $[x]$通常叫做取整函数（或高斯函数），它是数论中一个常见的函数，具有许多有趣的性质.

$p \mid n$，所以 $q \mid n$，于是 q 是 n 的除 1，p 以外且小于 p 的正因数，这与已知矛盾，故最小正因数 p 是一个素数. 一般地，任何大于 1 的整数，总存在一个素数因数. 通常，把一个正整数的素数因数叫做它的素因数.

思考

是否总可将任何大于 1 的整数 n 分解为一些素数的乘积?

对大于 1 的整数 n，如果 n 不是素数，我们可以将 n 分解为一个素数和某个大于 1 的整数 a 的乘积，如果 a 是一个素数，则过程停止. 否则，又可将 a 分解为一个素数和某个大于 1 的整数 b 的乘积. 对 b 又分两种情形：若 b 为素数，则过程停止；若 b 不是素数，则将 b 继续分解为一个素数和某个大于 1 的整数 c 的乘积. 如此进行下去，直到过程停止，最后总可将 n 分解为一些素数的乘积. 例如，$12=2\times2\times3$，$78=2\times3\times13$.

既然任何大于 1 的整数 n 总可分解为一些素数的乘积，那么素数有多少个? 有限还是无限? 为什么?

我们不妨假设素数有有限个，即 m_1，m_2，m_3，…，m_k，记这 k 个素数的乘积为 N，即

$$N=m_1m_2m_3\cdots m_k.$$

由此可知，任意一个素数 $m_i(i=1, 2, \cdots k)$ 都整除 N，但不能整除 $N+1$. 又由于 $N+1$ 为大于 1 的正整数，所以它一定能被某个素数整除，这就产生了矛盾. 因此，假设素数有有限个是错误的，**素数有无穷多个**.

欧几里得证明素数有无穷多个这个命题时使用了反证法，这是数学上第一批使用反证法的命题.

思考

对给定的大于 1 的正整数，如何判断它是不是素数呢? 例如，要判断 61 是不是素数，是否需要用 2～60 之间的数一一试除 61 呢?

没有必要. 因为 2 不是 61 的因数，那么 2 的倍数也不是 61 的因数. 同样地，若 3 不是 61 的因数，那么 3 的倍数也不是 61 的因数. 这就是说只需用 2～60 之间的素数试除 61 即可.

另一方面，如果 61 是合数，那么它一定可以表示成两个大于 1 的正因数的乘积，其中较小的一个正因数一定不超过$\sqrt{61}$，并且它的素因数也是 61 的素因数. 这就是说，如果 61 是合数，那么它一定存在不超过$\sqrt{61}$的素因数.

因此只需用 2～60 之间不超过$\sqrt{61}$的素数试除 61 即可.

不超过$\sqrt{61}$的素数为 2，3，5，7，由于它们都不整除 61，所以 61 是素数.

一般地，我们有下面的判别法：

> **如果大于 1 的整数 a 不能被所有不超过$\sqrt{a}$的素数整除，那么 a 一定是素数.**

这个判别法实际上给出了一种寻找素数的有效方法.

例 3　找出 1～100 中的全部素数.

解：只需把 1 与 1～100 之间的合数去掉即可. 而对于 1～100 之间的每个合数 a，它一定能被某个不超过$\sqrt{a}$的素数整除，从而能被不超过 $\sqrt{100}=10$ 的素数整除. 我们知道，不超过 10 的素数为 2，3，5，7. 在 1～100 中首先去掉 1，然后分别去掉 2，3，5，7 除自身以外的倍数，最后剩下的数就是不超过 100 的全部素数. 具体做法如下表：

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

因此不超过 100 的素数为 2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97，共 25 个. 这种寻找素数的方法叫做**埃拉托斯特尼（Eratosthenes）筛法.**

1. 判断下列整数中哪些能分别被 3，7，9，11 整除：
   45，98，120，189，1001，1331，56382.
2. 探究并证明能被 11 整除的 5 位正整数的特征.
3. 已知 1626 除以某个整数，其商为 81，求除数与余数.
4. 判断 343，2027 是素数还是合数.

二 最大公因数与最小公倍数

1. 最大公因数

给定两个整数 a，b，必有公共的因数，叫做它们的**公因数**. 当 a，b 不全为零时，在有限个公因数中最大的一个叫做 a，b 的**最大公因数**，记作(a, b).

例如，-8 和 14 的全部公因数为 1，-1，2，-2，最大的公因数为 2，所以

$$(-8, 14)=2.$$

如果 a，b 的最大公因数为 1，那么称 a，b 是**互素**的.

类似地，我们可以定义三个或更多个整数的最大公因数和互素的概念. 将整数 a，b，c 的最大公因数记作(a, b, c)，依此类推.

如何计算一组非零整数的最大公因数呢？我们已经学习过一种算法——短除法.

思考

试用短除法计算下列两组数的最大公因数：

(1) 375，105； (2) 1840，667.

从中你能感受到什么？

我们发现，用短除法求最大公因数有一定的局限性，因为用它每进行一次操作必须事先观察到一个大于 1 的公因数，而这一点有时难以做到. 特别是求两个较大整数的公因数时，这一点显得更为突出.

如何求 (1840，667)？一个自然的考虑是把 1840，667 通过适当的方式都变小，变小后，公因数就容易求出了. 如何变小呢？看下面的问题.

思考

如果 b 除 a 的余数为 r，那么(a, b)是否等于(b, r)？

事实上，若 d 为 a，b 的公因数，即 $d \mid a$，$d \mid b$，则 $d \mid a-bq=r$，从而 d 为 b，r 的公因数. 同理可证，r，b 的公因数也是 a，b 的公因数. 因此，a，b 公因数的集合与 r，b 公因数的集合相同，从而它们的最大公因数相等，即$(a, b)=(b, r)$.

按照这种思路，我们来求$(1840, 667)$.

因为 $1840=667\times 2+506$，所以$(1840, 667)=(667, 506)$；又因为 $667=506\times 1+$

161，所以(667，506)=(506，161)；又因为 506=161×3+23，所以(506，161)=(161，23)，而(161，23)=23. 因此

$$(1840，667)=23.$$

这种求最大公因数的方法，叫做**辗转相除法**❶. 它是一种古老而有效的算法. 下面，我们给出辗转相除法的一般形式.

设 a 和 b 为任意两个整数，且 $b\neq 0$. 应用带余除法，以 b 除 a，得商 q_1 和余数 r_1. 如果 $r_1\neq 0$，那么再以 r_1 除 b，得商 q_2 和余数 r_2. 如果 $r_2\neq 0$，再以 r_2 除 r_1，如此继续下去，$r_i(i=1，2，\cdots)$越来越小，有限次这种除法后，必然得到一个余数 $r_n\neq 0$，它整除前一个余数 r_{n-1}. 于是，我们有：

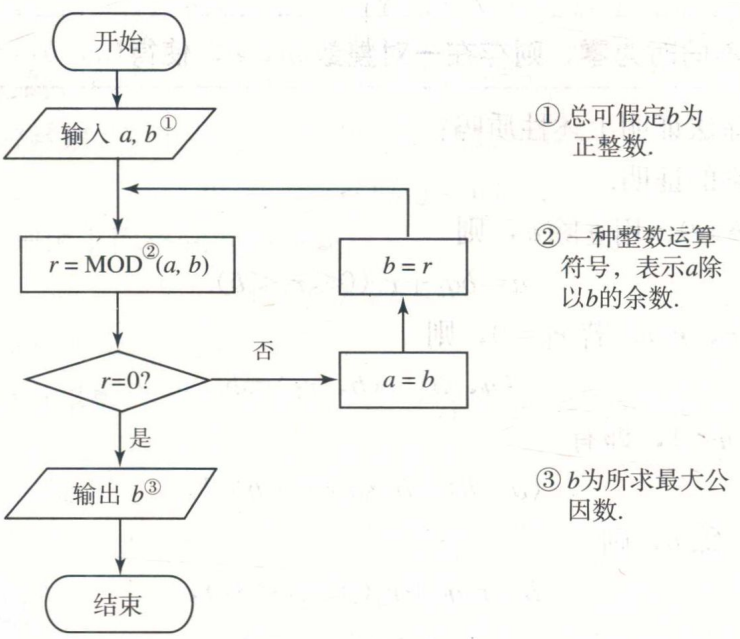
$$\begin{aligned}
&a=bq_1+r_1，\\
&b=r_1q_2+r_2，\\
&r_1=r_2q_3+r_3，\\
&\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n，\\
&r_{n-1}=r_nq_{n+1}.
\end{aligned}$$

即

$$(a，b)=(b，r_1)=(r_1，r_2)=\cdots=(r_{n-1}，r_n)=(0，r_n)=r_n.$$

也就是说，r_n 是 a，b 的最大公因数.

上述辗转相除法的过程可用下面的程序框图表示：



❶ 这种算法是欧几里得在公元前 300 年左右提出的，因此又叫欧几里得算法.

探究

你能根据上面的程序框图，编写一个计算机程序，求两个整数的最大公因数吗？

下面探讨三个整数的最大公因数的求法.

探究

1. 自己列举几组整数 a，b，c，计算并比较(a, b, c)，$((a, b), c)$，从中你能发现什么规律？

2. 求三个整数的最大公因数与求两个整数的最大公因数之间有什么联系？

我们发现，无论怎样选取 a，b，c，恒有

$$(a, b, c)=((a, b), c).$$

这表明，求三个整数的最大公因数，总可以转化为求两次两个整数的最大公因数.

对于多于三个整数的最大公因数，我们也有类似的结论.

关于最大公因数，有一条重要的性质. 这条性质在求解一次同余方程和不定方程时经常要用到.

设整数 a，b 不同时为零，则存在一对整数 m，n，使得$(a, b)=am+bn$.

你能用辗转相除法证明上述性质吗？

下面我们给出它的证明.

证明：不妨设 $b>0$，用 b 除 a，则

$$a=bq_1+r_1(0\leqslant r_1<b).$$

因为$(a, b)=(b, r_1)$，若 $r_1=0$，则

$$(a, b)=(b, r_1)=b.$$

此时取 $m=0$，$n=1$，即有

$$(a, b)=b=a\times 0+b\times 1.$$

若 $r_1\neq 0$，用 r_1 除 b，则

$$b=r_1q_2+r_2(0\leqslant r_2<r_1),$$

且

$$(b, r_1)=(r_1, r_2).$$

若 $r_2=0$，则

$$(a, b)=(r_1, r_2)=r_1=a-bq_1.$$

此时取 $m=1$，$n=-q_1$，即有

$$(a, b)=r_1=a\times 1+b\times(-q_1).$$

若 $r_2\neq 0$，用 r_2 除 r_1，则

$$r_1=r_2q_3+r_3\ (0\leqslant r_3<r_2),$$

且
$$(r_1,\ r_2)=(r_2,\ r_3).$$

若 $r_3=0$，则

$$(a,\ b)=(r_2,\ r_3)=r_2=b-r_1q_2=b-(a-bq_1)q_2$$
$$=a\times(-q_2)+b\times(1+q_1q_2).$$

此时取 $m=-q_2$，$n=1+q_1q_2$，即有

$$(a,\ b)=a\times(-q_2)+b\times(1+q_1q_2).$$

若 $r_3\neq0$，再用 r_3 除 r_2，依次类推.

由上可知，这样的 m 和 n 是存在的.

这个性质对多于两个整数情形仍然成立，由它还可以推出整除的一条重要性质.

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

下面我们给出它的证明.

证明：因为$(a,\ b)=1$，

所以存在一对整数 m，n，使得 $am+bn=1$.

于是　$(ac)m+(bc)n=c$.

又因为　$a\mid ac$，$a\mid bc$，

所以　$a\mid(ac)m+(bc)n$，即　$a\mid c$.

由整除的上述性质，我们可以得出素数的一条重要性质.

设 p 为素数，若 $p\mid ab$，则 $p\mid a$，或 $p\mid b$.

下面我们给出它的证明.

证明：因为 p 为素数，其正因数只有 1，p，所以

$$(p,\ a)=1，或(p,\ a)=p.$$

若$(p,\ a)=1$，则由上面整除的性质知

$$p\mid b.$$

若$(p,\ a)=p$，则 $p\mid a$.

素数的这条性质可以推广到一般情形：设 p 为素数，若 $p\mid a_1a_2\cdots a_k$，则存在 $a_i(1\leqslant i\leqslant k)$，使得 $p\mid a_i$.

你能给出它的证明吗?

2. 最小公倍数

甲、乙两个齿轮互相啮合，齿数分别为 84，36，在转动过程中同时啮合的两齿到下次再同时啮合，甲、乙两个齿轮分别转过多少圈?