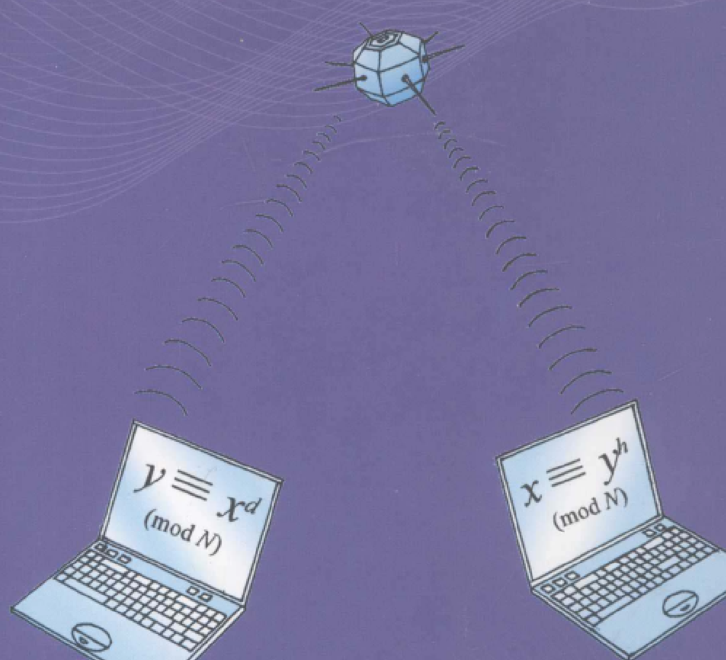
经全国中小学教材审定委员会2005年初审通过

普通高中课程标准

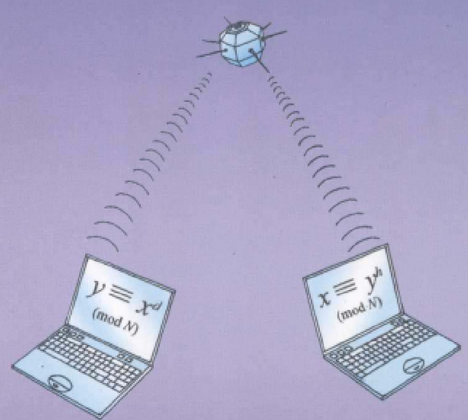
实验教科书

选修系列4－6

初等数论初步



湖南教育出版社



ISBN 7-5355-4608-0

9 787535 546081 >

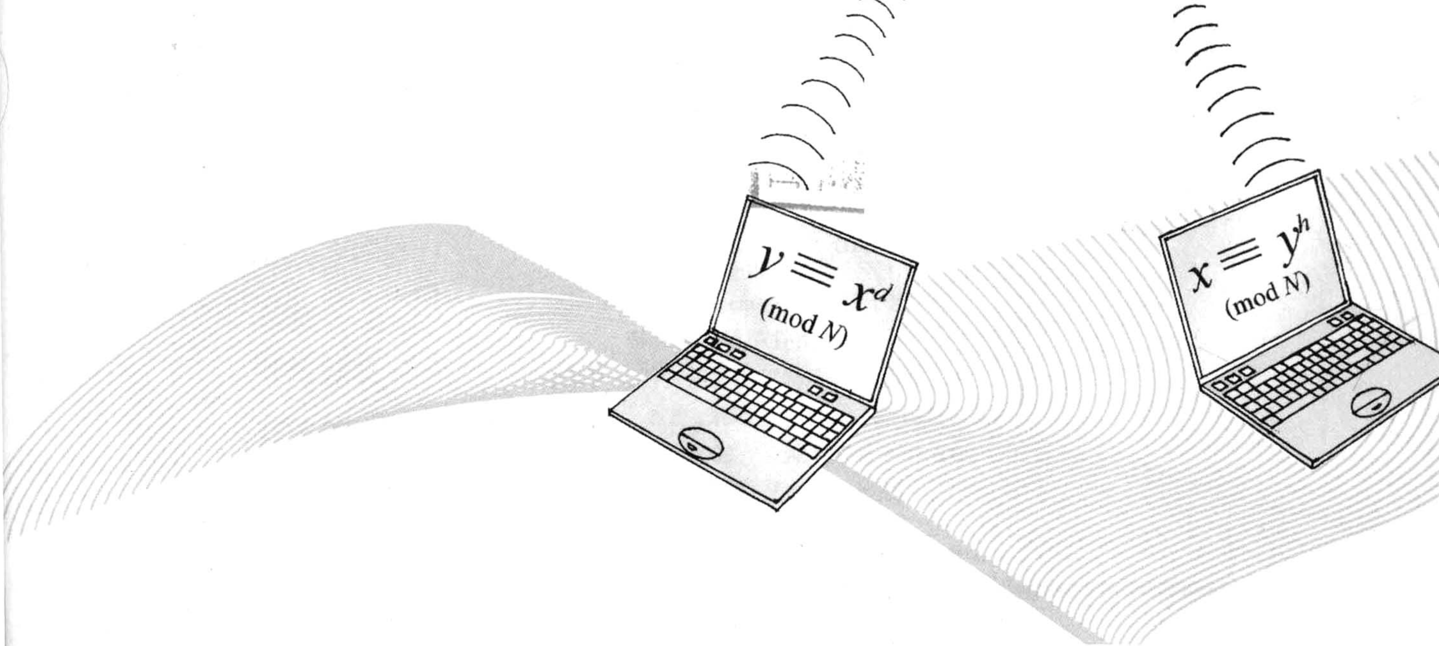
G · 4603 定价:7.05 元

普通高中课程标准

实验教科书

选修系列 4–6

初等数论初步



主　　编　张景中　陈民众
执行主编　李尚志
本册主编　王树禾
编　　委　郑志明　查建国
　　　　　蒋星耀　孟实华

普通高中课程标准实验教科书
选修 4—7
优选法与试验设计初步
责任编辑：孟实华　邹伟华
　　　　　甘　哲　蒋　芳
美术编辑：肖　毅
技术插图：徐　航
湖南教育出版社出版发行（长沙市韶山北路 443 号）
网　　址：http://www.hneph.com
电子邮箱：postmaster@hneph.com
湖南省新华书店经销
湖南新华印刷集团有限责任公司(邵阳)印刷
890×1240　16 开　印张：4.5　字数：110000
2005 年 8 月第 1 版　2006 年 7 月第 1 次印刷
ISBN 7—5355—4607—2/G·4602
定　价：6.05 元
本书若有印刷、装订错误，可向承印厂调换。

人之初，学整数

道生一二再生三，盘古开天辟万千.

除法奠基撑大厦，点兵创意铸名篇.

皇冠倾倒英雄辈，妙笔开通智慧泉.

莫道书生空议论，能将信息保平安.

初等数论研究的对象是整数.

自从盘古开天地，人类最早认识的数是整数.

自从来到人世间，每个人最先学习的数也是整数.

整数是数学的基础，数学中所有的研究都离不开整数. 整数的研究中提出的问题，促进了数学学科中很多重要分支的产生和发展.

整数是高贵的皇后，她的魅力让古往今来多少一流的数学家如痴如醉，为解决整数的难题呕心沥血，衣带渐宽终不悔，粉身碎骨也心甘.

整数又是谦恭的仆人，寻常百姓的街谈巷议都可以拿几个有关整数的趣味算题来启迪思维，而在现代信息社会中整数更是一马当先，冲锋陷阵，成为保卫信息安全的数学主将之一.

整数是古老的，又是年轻的，长生不老，永葆青春.

不要小看了整数，以为那是幼儿园和小学的算术. 要知道，专门研究整数的数论课程在大学数学中也不是很容易学习的，而在科学研究中它更是一道难关.

本教材当然不能向你全面介绍高深的数论知识. 但希望你能从中感受整数的魅力，了解整数的用途.

希望你喜欢它.

作 者

2004 年 12 月

目录

第1章 同余 1

1.1 带余除法 2

习题 1 4

1.2 整除 4

习题 2 5

1.3 奇数与偶数 6

习题 3 7

1.4 同余式 7

习题 4 11

1.5 余数的判别 11

习题 5 13

1.6 同余类算术 14

习题 6 17

数学实验 0—1序列密码 19

第2章 辗转相除法 22

2.1 最大公约数 23

习题 7 26

2.2 二元一次不定方程 26

习题 8 34

2.3 互素的整数 34

习题 9 36

2.4 最小公倍数 37

习题 10 39

第3章 中国剩余定理 40

3.1 《孙子算经》和韩信点兵 41

习题 11 42

3.2　中国剩余定理　42

习题　12　46

第4章　质因数分解　47

4.1　素数　48

习题　13　50

数学文化　哥德巴赫猜想与费马素数　51

4.2　质因数分解　53

习题　14　55

阅读与思考　多项式的带余除法　56

4.3　质因数分解应用举例　59

习题　15　60

阅读与思考　勾股数与费马大定理　62

第5章　幂的余数　65

5.1　公钥密码　66

数学实验　RSA 方案　70

5.2　费马小定理与欧拉定理　72

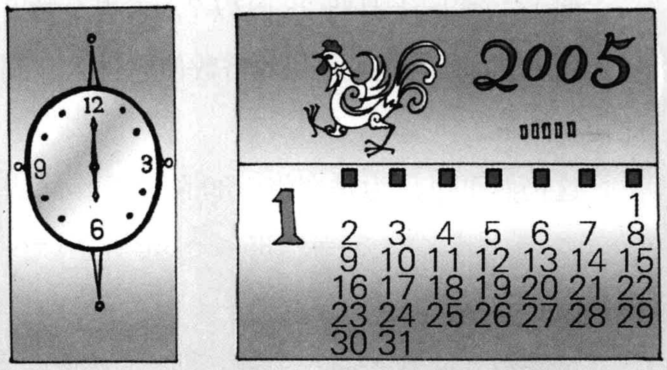
习题　16　78

课程总结报告参考题　79

附录　数学词汇中英文对照表　81

第1章

同　余



在整数研究中，带余除法发挥着最关键的作用，整数的一系列重要性质都由它而来.

今天星期四，2 天之后呢？由 $4+2=6$ 知道是星期六. 34 天之后，$4+34=38$，但不能星期 38，应当将它减去 7 的整倍数，使剩下的余数在 0 到 6 之间.

1.1 带余除法

例 1 假如今天是星期四.

(1) 34 天之后是星期几？

(2) 34 天之前是星期几？

解 (1) $4+34=38$. $38-7\times5=3$. 因此，34 天之后是星期三.

(2) $4-34=-30$. $-30+7\times5=5$. 因此，34 天之前是星期五.

例 1(1)实际上是将 38 除以 7，求得余数 3，因此是星期三.

例 1(2)将 -30 加上 7 的倍数使它进入 0 到 7 的范围，得到 5，因此是星期五.

这仍然可以认为是在将 -30 除以 7 作除法求余数. 由于

$$7\times(-5)=-35<-30<7\times(-4)=-28,$$

因此商 -5. 由

被除数－除数×商＝余数，即 $(-30)-7\times(-5)=5$,

求得余数 5. 因此是星期五.

小学算术只讲了非负整数除以正整数. 这里将它推广到了被除数是负整数的情况.

一般地，设 a 是任意整数，b 是正整数，则可找到最大的整数 q 使 $bq\leqslant a$，也就是

$$bq\leqslant a<b(q+1),$$

将整数 q 称为 a 除以 b 的商(quotient)，而将 $r=a-bp$ 称为 a 除以 b 的余数(remainder).

例 2 求 $2^{22\,222}+1$ 除以 $2^{11\,111}+1$ 的余数.

解 $2^{22\,222}+1=2^{22\,222}-1+2=(2^{11\,111}+1)(2^{11\,111}-1)+2$，因此余数为 2.

例 2 中，在将被除数 a 除以除数 b 时，没有按照

$$bq\leqslant a<b(q+1)$$

的要求去求出商 q，只是将被除数写成了

$$被除数=除数\times(整数\ q)+(整数\ r)$$

的形式，使

$$0\leqslant r<除数,$$

就可以断定 r 是余数，q 是商.

当然，这里有个问题：是否存在两组不同的商和余数 (q, r)，(q_1, r_1) 同时满足条件

$$\begin{cases}a=bq+r,\\0\leqslant r<b\end{cases}\quad 和 \quad\begin{cases}a=bq_1+r_1,\\0\leqslant r_1<b.\end{cases}$$

定理　（带余除法）设 a，b 为整数且 $b>0$，则存在唯一的一对整数 q，r 满足以下两个条件：

（1）$a=bq+r$；

（2）$0\leqslant r<b$.

q 称为 a 除以 b 的商，r 称为余数.

证明　q，r 的存在性：只要取 q 为满足条件 $bq\leqslant a$ 的最大整数，并设 $r=a-bq$，则 q，r 满足条件.

只需再证明 q，r 的唯一性.

假定对同样的被除数 a 和除数 b，同时有两对整数 q，r 和 q_1，r_1 满足定理所说的条件．即

（1）$a=bq+r$ 且 $a=bq_1+r_1$；

（2）$0\leqslant r<b$ 且 $0\leqslant r_1<b$.

将等式 $a=bq+r$ 与 $a=bq_1+r_1$ 两边相减得

$$b(q-q_1)+(r-r_1)=0.$$

从而

$$b|q-q_1|=|r_1-r|. \qquad ①$$

如果 $q\neq q_1$，则

$$|q-q_1|\geqslant 1\Rightarrow b|q-q_1|\geqslant b.$$

但另一方面，

$$\begin{cases}0\leqslant r<b\\0\leqslant r_1<b\end{cases}\Rightarrow\ 0\leqslant|r_1-r|<b.$$

这导致

带余除法也可以进一步推广到除数为负整数的情况：

设 a，b 为整数且 $b\neq0$，则存在唯一的商 q 和余数 r 满足以下两个条件：

(1) $a=bq+r$；

(2) $0\leqslant r<|b|$.

比如 $(-26)\div(-7)$，商为 4，余数 $r=(-26)-(-7)\times4=2$.

$$b|q-q_1|>|r_1-r|,$$

与等式①矛盾.

这就证明了只能 $q=q_1$. 代入等式①，得 $0=|r_1-r|$，$r=r_1$.

习题 1

1. (1) 假如现在是早晨 6 点. 32 个小时之后是几点钟？32 个小时之前呢？

   (2) 假如现在是 6 月份. 32 个月之后是几月份？32 个月之前呢？

2. (1) i 是虚数单位（满足条件 $i^2=-1$），$w=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$. 求 $w^{2005}=$？

   (2) 角 $\alpha=-1000^\circ$ 的始边为 x 轴的非负半轴 Ox. 终边在第几象限？

3. 求 $2^{2^{10}}+1$ 除以 $2^{2^9}+1$ 的余数.

1.2 整 除

我们知道，一般地，对任意整数 a，$b(b\neq0)$ 不能保证存在整数 q 使 $a=bq$.

如果对整数 a，$b(b\neq0)$ 恰好存在整数 q 使 $a=bq$，就称 a 被 b 整除(divide exactly)，也称 b 整除 a，记作 $b|a$. 此时还称 a 是 b 的倍数(multiple)，b 是 a 的约数，也称 b 是 a 的因数(divisor)，

显然，±1 是所有的整数的约数，0 是所有的非零整数的倍数.

如果 b 不整除 a，则记 $b\nmid a$.

根据带余除法的定义，显然有：

a 除以 b 的余数为 $0\Leftrightarrow a=bq\Leftrightarrow b|a$.

也就是说，整除是余数为 0 的情形.

由整除的定义可以立即导出整除的如下简单而有用的性质.

定理 1 设 a，b，c，x，y 是整数.

(1) 如果 $c\neq0$，则 $b|c\Leftrightarrow ab|ac$. 特别地，$b|c\Leftrightarrow(\pm b)|(\pm c)$；

(2) 如果 $b|c$ 且 $c|a$，则 $b|a$；

(3) 如果 $b|c$ 且 $b|a$，则 $b|(c\pm a)$，更一般地，$b|(cx+ay)$.

(4) 如果 $b|a$ 且 $a\neq 0$，则 $|b|\leqslant|a|$；

定理 2 设 a，b，c 是整数，且 $b\neq 0$.

$a-c$ 被 b 整除$\Leftrightarrow a$ 与 c 除以 b 的余数相等.

证明 设 a 除以 b 的商为 q_1，余数为 r_1；c 除以 b 的商为 q_2，余数为 r_2. 则

$$a=bq_1+r_1, \quad c=bq_2+r_2.$$

如果 $a-c$ 被 b 整除，则 $a-c=bk$，k 是某个整数. 于是

$$a=bk+c=bk+bq_2+r_2=b(k+q_2)+r_2,$$

其中 $k+q_2$ 是整数，$0\leqslant r_2<|b|$. 这说明 a 除以 b 的商为 $k+q_2$，余数为 r_2，与 c 除以 b 的余数相同.

反之，设 a，c 除以 b 的余数 r_1 与 r_2 相等. 则

$$a-c=(bq_1+r_1)-(bq_2+r_2)=b(q_1-q_2)+(r_1-r_2)=b(q_1-q_2),$$

其中 q_1-q_2 是整数，因而 $a-c$ 被 b 整除.

例 求 123 456 789 除以 5 的余数.

解 123 456 789－9＝123 456 780，由于 $5|10|123\ 456\ 780$，因此 123 456 789 与 9 除以 5 的余数相同，余数等于 4.

习题 2

1. 设 n 是整数，求证：$6|(n^3-n)$.
2. 一个六位数，它的前三位数码与后三位数码相同，求证：7，11，13 是它的约数.
3. a，b 为整数，$a\neq b$，n 为正整数，求证：$(a-b)|(a^n-b^n)$.
4. (1) 求一个三位数，它能被它的三位数字之和整除，且所得的商最大；

   (2) 求一个三位数，它的三个数字都不为 0，它能被它的三位数字之和整除，且所得的商最大.
5. 试给出定理 1 的证明.

1.3 奇数与偶数

中国民间口头流传很多数学问题. 其中一个问题是这样的：

“三十六口缸，九只船来装，装单不装双.”

用数学语言翻译出来，就是：

有 36 口缸，用 9 只船来装. 要求每只船所装缸的数目都是奇数. 每只船各装多少口缸？

题目中所说的“装单不装双”，“单”是指单数，就是奇数. “双”是指双数，就是偶数.

每个整数 n 除以 2 的余数有两个值：$r=0$ 或 1.

如果 $2\mid n$，即 $r=0$，就称 n 为**偶数**(even number). 每个偶数 n 可以写成 $n=2q$ 的形式，其中 q 是整数.

如果 $2\nmid n$，即 $r=1$，就称 n 为**奇数**(odd number). 每个奇数 n 可以写成 $n=2q+1$ 的形式，其中 q 是整数.

9 个奇数之和能够等于 36 吗？

不必知道奇数和偶数的具体值，我们也知道：

$$\text{偶数}+\text{偶数}=\text{偶数},$$
$$\text{偶数}+\text{奇数}=\text{奇数},$$
$$\text{奇数}+\text{奇数}=\text{偶数}.$$

利用这些公式，可以证明此题没有解.

例 求证：不存在 9 个奇数，它们的和为 36.

证明

$$\begin{aligned}&\text{奇数}+\text{奇数}+\text{奇数}+\text{奇数}+\text{奇数}+\text{奇数}+\text{奇数}+\text{奇数}+\text{奇数}\\=&(\text{奇数}+\text{奇数})+(\text{奇数}+\text{奇数})+(\text{奇数}+\text{奇数})+\\&(\text{奇数}+\text{奇数})+\text{奇数}\\=&\text{偶数}+\text{偶数}+\text{偶数}+\text{偶数}+\text{奇数}\\=&\text{偶数}+\text{奇数}=\text{奇数}\neq 36.\end{aligned}$$

可见，不论是哪 9 个奇数，它们的和一定是奇数. 而 36 是偶数，

因此，9 个奇数之和一定不能等于 36. 原题没有解，你也不必白费工夫再去苦苦搜寻了.

这个问题是口头叙述而不是文字叙述的. 原题其实是"三石六口缸"，3 块石头，6 口缸，总共 9 个东西，每只船装 1 个（都是奇数），9 只船正好装完. 它故意让你听了之后理解为"三十六口缸"，误入歧途，找不到解. 因此，这个题考的其实不是数学，而是"脑筋急转弯".

习题 3

1. 求证：如果 a，b，c 都是奇数，则方程 $ax^2+bx+c=0$ 无整数解.
2. 是否存在 4 个整数，它们的和等于 9，立方和等于 100？
3. 设 n 是整数，求证：$2|n(n+1)$.
4. 奇数的平方除以 4 的余数是多少？除以 8 的余数是多少？

1.4 同余式

在 1.3 中，我们用到了关于奇偶数加法的三条性质：

偶数＋偶数＝偶数，

偶数＋奇数＝奇数，

奇数＋奇数＝偶数.

这些公式为什么是正确的？比如，要证明第三条性质，只要将任意两个奇数写成 $2k+1$，$2m+1$ 的形式，其中 k，$m\in\mathbf{Z}$，就得到

$$(2k+1)+(2m+1)=2(k+m+1).$$

可见它们的和是偶数.

不难发现，不必用 $2k+1$，$2m+1$ 代表两个奇数，可以将 $2k$，$2m$ 都扔掉，直接用两个 1 代表两个奇数，这样，在求和的时候只是扔掉了 2 的倍数 $2k+2m$，并不影响所得的和的奇偶性. 由于

$$1+1=2$$

是偶数，就可断言任何两个奇数相加都是偶数.

我们用符号

$$a\equiv 1 \pmod 2$$

来表示整数 a 与 1 除以 2 的余数相同，同为奇数．这样，前面第三条性质的证明就可以改为：

$$奇数+奇数\equiv 1+1=2\equiv 偶数 \pmod 2.$$

一般地，如果两个整数 a，b 除以同一个除数 n 的余数相等，就称 a，b 模 n 同余．记为

$$a\equiv b \pmod n.$$

这样表示两个整数同余的式子称为同余式.

如果两个整数 a，b 除以 n 的余数不相等，就说它们模 n 不同余，记 $a\not\equiv b \pmod n$.

根据同余的定义，立即看出：

$$\begin{cases} a\equiv b \pmod n \\ b\equiv c \pmod n \end{cases} \Rightarrow \quad a\equiv c \pmod n.$$

注意

$$a\equiv 0 \pmod n \quad \Leftrightarrow \quad n\mid a.$$

在 1.2 定理 2 中我们还知道

$$a\equiv b \pmod n \quad \Leftrightarrow \quad n\mid (a-b) \quad \Leftrightarrow \quad a-b\equiv 0 \pmod n.$$

同余式的这条性质与等式很类似.

因此，“模 n 同余”的定义通常叙述为：

如果两个整数 a，b 的差被 n 整除，就称它们模 n 同余.

例 1　求 $a=25\ 000\ 000$ 除以 11 的余数.

分析　$a=25\ 000\ 000=2\times 10^7+5\times 10^6$.

我们有 $10\equiv -1 \pmod{11}$，假如能够将 a 的表达式中的 10 用 -1 替换：

$$\begin{array}{c} a=2\times 10^7 \quad + \quad 5\times 10^6 \\ \quad\quad \downarrow \quad\quad\quad\quad \downarrow \\ a_1=2\times(-1)^7+5\times(-1)^6=3 \end{array}$$

而能够保持除以 11 的余数不变，就可知道 a 除以 11 的余数为 3.

例 1 提出的问题是：假如 $a\equiv a_1 \pmod n$ 且 $b\equiv b_1 \pmod n$，$y=f(a,b)$是由 a，b 经过加、减、乘运算得出的整数，要求 y 除以 n 的余数，如果先将 a，b 分别替换成与之同余的 a_1，b_1，用 $y_1=f(a_1, b_1)$代替 y，能否保证所求的余数不变?

换句话说，能否将同余式 $a\equiv a_1 \pmod{n}$ 且 $b\equiv b_1 \pmod{n}$ 代入 $y=f(a, b)$ 右边，而仍然得到同余式 $y\equiv f(a_1, b_1) \pmod{n}$？

定理 如果 $a\equiv a_1 \pmod{n}$ 且 $b\equiv b_1 \pmod{n}$，则

(1) $a\pm b\equiv a_1\pm b_1 \pmod{n}$；

(2) $ab\equiv a_1b_1 \pmod{n}$；

(3) 对任意正整数 m，$a^m\equiv a_1^m \pmod{n}$.

证明 我们有 $a=a_1+nk$，$b=b_1+nk_1$，其中 k，k_1 是整数.

(1) $a\pm b=(a_1+nk)\pm(b_1+nk_1)=(a_1\pm b_1)+n(k\pm k_1)$

$\equiv a_1\pm b_1 \pmod{n}$；

(2) $ab=(a_1+nk)(b_1+nk_1)=a_1b_1+n(kb_1+k_1a_1+nkk_1)$

$\equiv a_1b_1 \pmod{n}$；

(3) 在

$$ab\equiv a_1b_1 \pmod{n} \quad ①$$

中将 b，b_1 分别用 a，a_1 代入得到

$$a^2\equiv a_1^2 \pmod{n}. \quad ②$$

在①中将 b，b_1 分别用 a^2，a_1^2 代入得到

$$a^3\equiv a_1^3 \pmod{n}. \quad ③$$

照此进行下去，最后可得

$$a^m\equiv a_1^m \pmod{n}.$$

可将这里的证明改为对 m 用数学归纳法来完成.

上面定理的意思是，将两个同余式两边同时相加，或相减，或相乘，得到的同余式仍成立. 将一个同余式两边同时乘方同样的次数，所得的同余式仍成立.

这个性质也与等式类似.

定理 1 还告诉我们，如果整数 $y=f(a_1,a_2,\cdots,a_k)$ 是由若干个整数 a_1，a_2，…，a_k 经过加、减、乘、指数为正整数的乘方计算得到，要计算 y 除以 n 的余数，可以将 a_1，a_2，…，a_k 分别替换成与它们同余的 b_1，b_2，…，b_k 来计算.

例 2 试导出奇偶数的乘法公式.

解 整数×偶数$\equiv r\times 0=0 \pmod{2}\Rightarrow$整数×偶数=偶数.

奇数×奇数$\equiv 1\times 1=1 \pmod{2}\Rightarrow$奇数×奇数=奇数.

例3 已经知道2004年10月1日是星期五. 2008年国际奥林匹克运动会将于8月8日在北京举行开幕式. 这一天是星期几?

解 从2004年10月1日到2008年10月1日,一共经过了4年.

其中前3年(2004年10月1日到2007年10月1日)是平年,每年365天,一共365×3天.

最后1年(2007年10月1日到2008年10月1日)包括了闰年2008年的2月,一共366天.

从2008年10月1日星期二倒着往回计算到同年的8月1日,经过2个月,其中9月份30天,8月份31天,共应减去$(30+31)$天. 再从8月1日到同月8日,加$(8-1)$天.

最后,由

$$a=5+365\times3+366-(30+31)+(8-1)$$

除以7的余数来计算这一天是星期几.

由于$365\equiv1 \pmod 7$,$366\equiv2 \pmod 7$,在计算a除以7的余数的时候,可以将a的表达式中的365换成1,366换成2. 由此得到

$$a\equiv5+1\times3+2-61+7\equiv10-61\equiv-51\equiv-51+7\times8\equiv5 \pmod 7.$$

这一天是星期五.

以上计算星期几的时候用到关于日历的如下知识:

1. 每月多少天?

每年12个月的天数如下:

月份	1	2	3	4	5	6	7	8	9	10	11	12
天数	31	28或29	31	30	31	30	31	31	30	31	30	31

其中2月份的天数比较特殊,平年为28天,闰年为29天.

2. 每年多少天?

平年365天,闰年366天.

设年份数为a.

(1) 如果a不被4整除,是平年;

(2) 如果a被4整除而不能被100整除,是闰年;

(3) 如果a被100整除而不被400整除,是平年;