初等数论讲义

Lectures on Elementary Number Theory

King　整理

目　　录

第一讲　数论简介与数的进制

教学目标：	了解数论及历史、掌握数的进制
教学重点：	数的进制与不同进制数的转化
教学难点：	不同进制数的转化
教学方法和手段：	讲授
教学时数：	2 课时

➤1.1　数论这门学科最初就是从研究整数开始的, 所以叫做整数论. 后来整数论又进一步拓展, 就叫数论了. 确切地说, 数论就是一门研究整数性质的学科.

一、整数

➤1.2　把 $0,1,2,3,\cdots,n,\cdots$ 叫做自然数, 也叫做非负整数. 所有自然数构成的集合, 叫做**自然数集**, 记作 $\mathbb{N}$.

➤1.3　把 $1,2,3,\cdots,n,\cdots$ 叫做正整数. 所有正整数构成的集合, 叫做**正整数集**, 记作 $\mathbb{N}^*$.

➤1.4　把 $-1,-2,-3,\cdots,-n,\cdots$ 叫做负整数. 所有负整数构成的集合, 叫做**负整数集**, 记作 $\mathbb{Z}^-$.

➤1.5　正整数、零、负整数统称为整数. 所有整数构成的集合, 叫做**整数**集, 记作 $\mathbb{Z}$.

二、数的进制

1.2.1　十进制及其计数法

➤1.6　一个 $n+1$ 位自然数

$$\begin{aligned} m &= \overline{a_n a_{n-1}\cdots a_1 a_0} \\ &= a_n\times 10^n + a_{n-1}\times 10^{n-1} + \cdots + a_1\times 10 + a_0 \\ &= \sum_{i=0}^{n} a_i 10^i (a_i\in\mathbb{N}, 0\leqslant a_i\leqslant 9, a_n\neq 0). \end{aligned}$$

这里的 10 也叫**基**.

➤1.7 定理 1　如果 n 是自然数, 则 n 表示成十进制的形式是唯一的.

➤1.8 例 1　已知:$a_3>a_1, b_3\neq 0$, 且 $\overline{a_3a_2a_1}-\overline{a_1a_2a_2}=\overline{b_3b_2b_1}$, 求证:

$$\overline{b_3b_2b_1}+\overline{b_1b_2b_3}=1089.$$

1.2.2 k 进制数

➤1.9 定义 1 如果 k 是大于或等于 2 的整数, 而任一自然数

$$n = b_n k^n + b_{n-1}k^{n-1} + \cdots + b_1 k + b_0 = \sum_{i=0}^{n} b_i k^i$$

$$(b_n \neq 0, b_i \in \mathbf{N}, 0 \leqslant b_i < k, i = 0, 1, 2, \cdots, n)$$

就称 n 是由 k 的幂的和表示的,n 也可以写成

$$n = (b_n b_{n-1} \cdots b_1 b_0)_k$$

我们称 n 是用 k 进制表示的.

➤1.10 定义 2 k 进制小数

$$\begin{aligned}(0.b_1 b_2 \cdots b_n)_k &= \frac{b_1}{k} + \frac{b_2}{k^2} + \cdots + \frac{b_n}{k^n} \\ &= \sum_{i=1}^{n} \frac{b_i}{k^i} \quad (0 \leqslant b_i < k, b_i \in \mathbb{N})\end{aligned}$$

➤1.11 定理 2 设 $k \geqslant 2$ 且是整数, 则任一自然数 n 仅有一种 k 进制的形式**:**

$$\begin{aligned}n &= b_n k^n + b_{n-1}k^{n-1} + \cdots + b_1 k + b_0 \\ &= \sum_{i=0}^{n} b_i k^i \quad (b_i \in \mathbb{N}, 0 \leqslant b_i < k, b_n \neq 0)\end{aligned}$$

1.2.3 不同进制数的互化

➤1.12 例 2 $2866 = (\quad)_5 = (\quad)_7 = (\quad)_8 = (\quad)_2$

解: 因为

$$\begin{aligned}2866 &= 5 \times 573 + 1 \\ &= 5 \times (5 \times 114 + 3) + 1 \\ &= 114 \times 5^2 + 3 \times 5 + 1 \\ &= (5 \times 22 + 4) \times 5^2 + 3 \times 5 + 1 \\ &= 5^3 \times 22 + 4 \times 5^2 + 3 \times 5 + 1 \\ &= 5^3 \times (5 \times 4 + 2) + 4 \times 5^2 + 3 \times 5 + 1 \\ &= 4 \times 5^4 + 2 \times 5^3 + 4 \times 5^2 + 3 \times 5 + 1\end{aligned}$$

所以 $2866 = (42431)_5$

以后称这种化十进制数为 k 进制数的方法为**除 k 取余法**, 并采用下面的除法算式:

$$
\begin{array}{r|l}
5 & 2866 \\
\hline
5 & 573 \quad \text{余 } 1 \\
\hline
5 & 114 \quad \text{余 } 3 \\
\hline
5 & 22 \quad \text{余 } 4 \\
\hline
5 & 4 \quad \text{余 } 2 \\
\hline
 & 0 \quad \text{余 } 4
\end{array}
$$

所以 $2866 = (42431)_5$.

同理 $2866 = (112331)_7$.

$2866 = (5462)_8$.

$2866 = (101100110010)_2$.

➤1.13 例 3 计算

(1) $(1234)_5 + (2341)_5$;

(2) $(2341)_5 - (1234)_5$;

(3) $(2341)_5 \times (1234)_5$;

(4) $(3023)_5 \div (1234)_5$;

解: 上述四题均可先将五进制数改成十进制后按要求算出结果后, 再将十进制的结果转换成五进制; 但也可以直接计算.

(1)$\because \quad (1234)_5 = 1 \times 5^3 + 2 \times 5^2 + 3 \times 5 + 4 = 194$

$(2341)_5 = 2 \times 5^3 + 3 \times 5^2 + 4 \times 5 + 1 = 346$

$194 + 346 = 540$

$$
\begin{array}{r|l}
5 & 540 \\
\hline
5 & 108 \quad \text{余 } 0 \\
\hline
5 & 21 \quad \text{余 } 3 \\
\hline
5 & 4 \quad \text{余 } 1 \\
\hline
 & 0 \quad \text{余 } 4
\end{array}
$$

$540 = (4130)_5$,

$\therefore (1234)_5 + (2341)_5 = (4130)_5$.

(2)$\because 346 - 194 = 152$,

$\therefore (2341)_5 - (1234)_5 = (1102)_5$

(3)$\because 194 \times 346 = 67124$

$\therefore (2341)_5 \times (1234)_5 = (4121444)_5$.

(4)$\because (3023)_5 = 3 \times 5^3 + 2 \times 5 + 3 = 388$

$388 \div 194 = 2$,

$\therefore (3023)_5 \div (1234)_5 = (2)_5$

练习 1 $(1)56132 = (\quad)_2 = (\quad)_8$

$(2)2000 = (\quad)_3 = (\quad)_7$

$= (\quad)_9 = (\quad)_{12}$

$(3)(12301)_5 = (\quad)_7$

练习 2 计算

(1) $(110)_2 + (1011)_2, (10101)_2 - (111)_2,$
$(10101)_2 \times (101)_2, (1101001)_2 \div (1010)_2,$

(2) $(2517)_8 + (3124)_8, (15721)_8 - (452)_8$
$(301)_8 \times (125)_8, (212)_8 \div (27)_8$

作业：	练习 1、2
教学后记：	

第二讲　数的整除性

教学目标：	掌握数的整除性的概念与性质
教学重点：	数的整除性的概念与性质
教学难点：	整除的性质
教学方法和手段：	讲授
教学时数：	4 课时

一、数的整除性

➤2.1 定义 1　设 a,b 为两个整数, $b\neq 0$. 如果存在整数 c, 使得 $a=bc$, 则称 a **被** b **整除或** b **整除** a, 记作 $b\mid a$, 并称 a 是 b 的**倍数**,b 是 a 的**因数** (或**约数**), 如果不存在整数 c, 使得 $a=bc$ 成立, 则称 a **不被** b **整除**或 b **不整除** a, 记作 $b\nmid a$.

➤2.2　每个非零整数至少有 ± 1 和 $\pm a$ 作为它的因数, 称它们为 a 的**平凡因数**;a 的异于 ± 1 和 $\pm a$ 的因数, 称为 a 的**非平凡因数**, 或 a 的**真因数**.

➤2.3 e.g.$3\mid 8; 5\mid 125; 5\mid (-25); 13\mid 1001; 2018\mid 0; 1\mid a; a\mid a(a\neq 0); 5\nmid 12$.

➤2.4 性质 1 (传递性) 若 $b\mid c$, 且 $c\mid a$, 则 $b\mid a$.

证明: 因为 $b\mid c$, 所以存在整数 q, 满足 $c=bq$. 因为 $c\mid a$, 所以存在整数 p, 满足 $a=cp$. 于是

$$a=cp=(bq)p=(pq)b$$

因为 $p,q\in\mathbb{Z}$, 所以 $pq\in\mathbb{Z}$, 故 $b\mid a$.

➤2.5 例 1　求证:$13\mid \overline{abcabc}(a\neq 0)$.

证明: 因为 $\overline{abcabc}=\overline{abc}\times 1000+\overline{abc}=\overline{abc}\times 1001$, 所以 $1001\mid \overline{abcabc}$. 因为 $13\mid 1001$, 所以 $13\mid \overline{abcabc}$.

➤2.6 性质 2 (可加性) 若 $b\mid a$, 且 $b\mid c$, 则对任意整数 k,l, 有 $b\mid (ka+lc)$;

一般, 若 $b\mid a_i(i=1,2,\cdots,n)$, 则 $b\mid (a_1x_1+a_2x_2+\cdots+a_nx_n)$, 其中 $x_i(i=1,2,\cdots,n)$ 是任意整数.

➤2.7 例 2　求证:$37\mid (333^{777}+777^{333})$.

证明: 因为 $111\mid 333^{777}, 111\mid 777^{333}$, 所以 $111\mid (333^{777}+777^{333})$. 因为 $37\times 3=111$, 所以 $37\mid (333^{777}+777^{333})$.

➤**2.8 性质 3 (可乘性)** 若 $b \mid a.d \mid c$, 则 $bd \mid ac$.

➤**2.9 性质 4** $b \mid a \Leftrightarrow |b| \mid |a|$.(若 $b \mid a, a \neq 0$, 则 $|b| \leqslant |a|$; 若 $b \mid a$, 且 $|a| < |b|$, 则 $a = 0$; 若 $b \mid a$, 且 $a \mid b$,$a > 0, b > 0$, 则 $a = b$.)

➤**2.10** (I) 若 n 是正整数, 则 $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$;

(II) 若 n 是正奇数, 则在上式中以 $(-b)$ 代换 b, 得

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

➤**2.11 例 3** 证明 $\underbrace{10\cdots01}_{50个0}$ 能被 1001 整除.

证明: 由分解公式 (II), 有

$$\begin{aligned}\underbrace{10\cdots01}_{50个0} &= 10^{51} + 1 = \left(10^3\right)^{17} + 1 \\ &= \left(10^3 + 1\right)\left[\left(10^3\right)^{16} - \left(10^3\right)^{15} + \cdots - 10^3 + 1\right]\end{aligned}$$

所以,$10^3 + 1 = 1001$ 整除 $\underbrace{10\cdots01}_{50个0}$.

➤**2.12 例 4** 若 n 是奇数, 证明 $8 \mid (n^2 - 1)$.

证明: 设 $n = 2k + 1 (k \in \mathbf{Z})$, 则 $n^2 - 1 = (2k+1)^2 - 1 = 4k(k+1)$. 由于 k 和 $k+1$ 中必有一个是偶数, 所以 $8 \mid (n^2 - 1)$.

➤**2.13 注** ①任何奇数的平方于 1 的差都能被 8 整数.

②任何整数的平方被 4 除的余数为 0 或 1, 被 3 除的余数为 0 或 1;

③任何整数的立方除 9 的余数为 0,1 或 8 等等.

➤**2.14 例 5** 设 $m > n \geqslant 0$, 证明:$(2^{2^n} + 1) \mid (2^{2^m} - 1)$.

证明: 由于 $m > n \geqslant 0$, 故 $m - n - 1 \geqslant 0$. 在分解公式 (I) 中, 令 $a = 2^{2^{n+1}}, b = 1$, 则

$$\begin{aligned}2^{2^m} - 1 &= \left(2^{2^{n+1}}\right)^{2^{m-n-1}} - 1 \\ &= \left(2^{2^{n+1}} - 1\right)\left[\left(2^{2^{n+1}}\right)^{2^{m-n-1}-1} + \cdots + 2^{2^{n+1}} + 1\right]\end{aligned}$$

所以 $\left(2^{2^{n+1}} - 1\right) \mid \left(2^{2^m} - 1\right)$. 又 $2^{2^{n+1}} - 1 = \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right)$, 因此 $\left(2^{2^n} + 1\right) \mid \left(2^{2^{n+1}} - 1\right)$.

由性质 1 知 $\left(2^{2^n} + 1\right) \mid \left(2^{2^m} - 1\right)$.

➤**2.15 注** $F_n \mid (F_m - 2)$, 即存在整数 t, 使得 $F_m - 2 = t \cdot F_n$.

➤**2.16 注** 在例 5 中, 直接证明 $\left(2^{2^n}+1\right) \mid \left(2^{2^m}-1\right)$ 不易入手, 因此尝试选择适当的中间量 $\left(2^{2^{n+1}}-1\right)$, 使之满足定理 1.1.1 之 (I) 的条件, 再利用整除的传递性导出所证结论.

➤**2.17 例 6** 设正数 n 的十进制表示为 $n = a_k \cdots a_1 a_0 (0 \leqslant a_i \leqslant 9, 0 \leqslant i \leqslant k, a_k \neq 0)$, 且

$$S(n) = a_k + a_{k-1} + \cdots + a_1 + a_0$$

证明:$9 \mid n$ 的充分必要条件是 $9 \mid S(n)$.

证明: 由于

$$n = a_k \times 10^k + \cdots + a_1 \times 10 + a_0, \quad S(n) = a_k + a_{k-1} + \cdots + a_1 + a_0$$

所以 $n - S(n) = a_k\left(10^k - 1\right) + \cdots + a_1(10-1)$

对于所有的 $0 \leqslant i \leqslant k$, 有 $9 \mid (10^i - 1)$, 故上式右端 k 个加项中的每一项都是 9 的倍数, 由定理 1.1 .1 之 (I) 知, 它们的和也被 9 整除, 即 $9 \mid [n - S(n)]$, 从而 $9|n \Leftrightarrow 9|S(n)$.

➤**2.18 注** 一个十进制整数被另一个正整数整除的条件 (如例 4 及习题 1.1 的第 2 题), 称为**整除的数字特征**. 例 4 得出十进制正整数 n 被 9 整除的数字特征是:9 整除 n 的各位数字之和.

二、整数的奇偶性

➤**2.19 定义 2** 能被 2 整除的整数叫做偶数; 不能被 2 整除的整数叫做奇数.

➤**2.20 性质 5** 偶数 $\pm$ 偶数 $=$ 偶数; 偶数 $\pm$ 奇数 $=$ 奇数; 奇数 $\pm$ 奇数 $=$ 偶数.

只证明: 一个偶数与一个奇数之和为奇数.

证明: 设任一偶数 $a = 2n(n \in \mathbb{Z})$; 任一奇数 $b = 2m+1(m \in \mathbb{Z})$, 则

$$a + b = 2n + (2m+1) = 2(n+m) + 1$$

可见,$a+b$ 是奇数.

➤**2.21 推论 1** 若干个偶数之和为偶数; 正偶数个奇数之和为偶数; 正奇数个奇数之和为奇数.

➤**2.22 例 7** 有 7 个茶杯, 杯口全朝上, 每次同时翻转 4 个称为一次远动, 可否经若干次远动使杯口全朝下?

解: 一个茶杯由口朝上翻转为口朝下, 须经奇数次翻转.

设经 k 次运动可使杯口全朝下, 此时每个茶杯翻转的次数分别记作

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7$$

因为杯口全朝下, 所以 $a_1, a_2, a_3, a_4, a_5, a_6, a_7$ 均为奇数.

故 7 个茶杯翻转的总次数 $a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = s$ 必是奇数.

另一方面, 每次同时翻转 4 个为一次远动, 若经 k 次运动使 7 个茶杯的杯口全朝下, 此时翻转的总次数为 $4k$, 这是一个偶数. 这与 s 为奇数矛盾. 故不可能经过若干次运动使杯口全朝下.

➤**2.23 性质 6** 奇数 × 奇数 = 奇数; 偶数 × 整数 = 偶数.

➤**2.24 推论 2** 若干个奇数之积为奇数.

➤**2.25 例 8** 设 $a_1, a_2, \cdots, a_n$ 是 $1, 2, \cdots, n$ 的任一新排列,n 为奇数, 求证:$(a_1 - 1)(a_2 - 2)\cdots(a_n - n)$ 为偶数.

证明: 因为

$$\begin{aligned}&(a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n)\\ =&(a_1 + a_2 + \cdots + a_n) - (1 + 2 + \cdots + n)\\ =&0\end{aligned}$$

这说明奇数个整数 $(a_1 - 1), (a_2 - 2), \cdots, (a_n - n)$ 之和为偶数.

所以 $(a_1 - 1), (a_2 - 2), \cdots, (a_n - n)$ 至少有一个为偶数.

故 $(a_1 - 1)(a_2 - 2)\cdots(a_n - n)$ 为偶数.

➤**2.26 性质 7** 设 a 为整数,n 为正整数, 则 a^n 与 a 奇偶性相同.

➤**2.27 例 9** 对正整数 a, 若存在正整数 b, 使得 $b^2 = a$ 成立, 则称 a 为完全平方数. 类似地可定义完全立方数等.

求证: 任意两个奇数的平方和不是完全平方数.

证明: 设两个奇数分别为 $a = 2n + 1(n \in \mathbb{Z}), b = 2m + 1(m \in \mathbb{Z}), k = a^2 + b^2$, 则 a^2, b^2 均为奇数, 故 $k = a^2 + b^2$ 为偶数.

若 k 为完全平方数, 则只能是一个正偶数的平方 (否则 k 不是偶数).

设 $k = (2q)^2(q$ 为正整数), 则 $k = 4q^2$, 故 $4 \mid k$.

另一方面,$k = a^2 + b^2 = 4(n^2 + m^2 + n + m) + 2$, 可见 $4 \nmid k$, 自相矛盾.

故任意两个奇数的平方和不是完全平方数.

作业:	P3 习题 1.1、1;2;3;4
教学后记:	

第三讲　带余数除法

教学目标：	理解带余数除法
教学重点：	带余数除法
教学难点：	带余数除法的证明
教学方法和手段：	讲授
教学时数：	4 课时

➤3.1 定理 1 (带余数除法) 设 a 与 b 是两个整数,$b \neq 0$, 则存在唯一的一对整数 q 和 r, 使得

$$a = bq + r(0 \leqslant r < |b|) \tag{3.1}$$

此外,$b \mid a$ 的充分必要条件是 $r = 0$.

➤3.2 定理 2 (Peano 公理) 设 $\mathbb{N}$ 是一个非空集合, 满足以下条件:

(i) 对每一个元素 $n \in \mathbb{N}$, 一定有唯一的一个 $\mathbb{N}$ 中的元素与之对应, 这个元素记做 n^+, 称为 n 的后继元素 (或后继);

(ii) 有元素 $e \in \mathbb{N}$, 它不是 $\mathbb{N}$ 中任一元素的后继;

(iii) $\mathbb{N}$ 中的任意一个元素至少是一个元素的后继, 即从 $a^+ = b^+$, 一定可推出 $a = b$;

(iv) (归纳公理) 设 S 是 $\mathbb{N}$ 的一个子集合,$e \in S$, 如果 $n \in S$, 必有 $n^+ \in S$, 那么 $S = \mathbb{N}$.

这样的集合 $\mathbb{N}$ 称为自然数集合, 它的元素称为自然数.

➤3.3 定理 3 (最小自然数原理) 设 T 是 $\mathbb{N}$ 的一个非空子集, 那么, 必有 $t_0 \in T$, 使对任意的 $t \in T$ 有 $t_0 \leqslant t$, 即 t_0 是 T 中的最小自然数.

➤3.4 定理 4 (最大自然数原理) 设 M 是 $\mathbb{N}$ 的一个非空子集, 若 M 有上界, 即存在 $a \in \mathbb{N}$, 使对任意的 $m \in M$ 有 $m \leqslant a$, 那么, 必有 $m_0 \in M$, 使对任意的 $m \in M$ 有 $m \leqslant m_0$, 即 m_0 是 M 中的最大自然数.

证明: *(定理 1 的证明)* **存在性**　若 $b \mid a$, 则存在 $q \in \mathbb{Z}$, 使得 $a = bq$, 此时取 $r = 0$, 即式(3.1)成立.

若 $b \mid a$, 考虑集合 $A = \{a + kb \mid k \in \mathbb{Z}\}$. 在集合 A 中有无限多个正整数, 由自然数的最小数原理知,A 中必有最小的正整数. 设这个最小的正整数为 $r = a + k_0 b$, 则必有结论:

$$0 < r < |b| \tag{3.2}$$

事实上, 若不然, 就有 $r \geqslant |b|$. 因为 $b \mid a$, 所以 $r \neq |b|$, 从而 $r > |b|$, 故

$$r_1 = r - |b| = a + k_0 b - |b| > 0$$

这样就有 $r_1 \in A$ 且 $0 < r_1 < r$, 这与 r 的最小性矛盾. 所以, 式(3.2)成立. 取 $q = -k_0$, 知式(3.1)成立. 存在性得证.

唯一性 假设存在两对整数 q', r' 与 q'', r'' 都使得式(3.1)成立, 即

$$a = q''b + r'' = q'b + r' \quad (0 \leqslant r', r'' < |b|)$$

于是

$$(q'' - q')\, b = r' - r'' \tag{3.3}$$

由此推出 $b \mid (r' - r'')$. 但 $0 \leqslant |r' - r''| < |b|$, 故必须使 $r' - r'' = 0$, 即 $r' = r''$, 代入式(3.3)得 $q' = q''$. 唯一性得证.

当 $a = bq + r$ 时,$b|a \Leftrightarrow b|r$; 而当 $0 \leqslant r < |b|$ 时,$b \mid r \Leftrightarrow r = 0$. 故 $b \mid a \Leftrightarrow r = 0$. 证毕.

证法二:(1) 当 $b > 0$ 时, 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

若 a 与序列中某一项相等, 则 $a = bq$, 即 $a = bq + r, r = 0$.

若 a 与序列序列中任一项不相等, 则必在此序列的某相邻两项之间, 即有确定的整数 q, 使得 $bq < a < b(q + 1) = bq + b$, 所以

$$0 < a - bq < b = |b|.$$

令 $a - bq = r$, 则有

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

(2) 当 $b < 0$ 时, 作整数序列

$$\cdots, 3b, 2b, b, 0, -b, -2b, -3b, \cdots$$

若 a 与序列中某一项相等, 则 $a = bq$, 即 $a = bq + r, r = 0$.

若 a 与序列序列中任一项不相等, 则必在此序列的某相邻两项之间, 即有确定的整数 q, 使得 $bq < a < b(q - 1) = bq - b$, 所以

$$0 < a - bq < -b = |b|.$$

令 $a - bq = r$, 则有

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

综上所述, 对给定的整数 $a, b(b \neq 0)$, 有确定的一对整数 q 和 r, 满足

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

对于给定的整数 $a, b(b \neq 0)$, 如果有两对整数 q_1, r_1, q_2, r_2 满足

$$a = bq_1 + r_1, 0 \leqslant r_1 < |b| \quad ①$$
$$a = bq_2 + r_2, 0 \leqslant r_2 < |b| \quad ②$$

②-①得

$$r_1 - r_2 = (q_2 - q_1)b, 0 \leqslant |r_1 - r_2| < |b|$$

即 $b \mid (r_1 - r_2)$, 且 $|r_1 - r_2| < |b|$,
于是 $r_1 - r_2 = 0$, 则 $r_1 = r_2$, 从而 $q_1 = q_2$.

➤3.5 定义 1 式(3.1)中的 q 称为 a 被 b 除的**不完全商**,r 称为 a 被 b 除的**余数**, 也称为**最小非负剩余**.

➤3.6 注 对于给定的正整数 b, 可以按照被 b 除的余数将整数集分成 b 类, 使得在同一类中的整数被 b 除的余数 r 相同. 这就使得关于全体整数的问题可以化归为对有限个整数类的研究. 此时,r 共有 b 种可能的取值, 即 $0, 1, \cdots, b-1$. 当 $r = 0$ 时, 即为“a 被 b 整除”的情形. 由此, 整除问题往往可以化归为带余数除法问题来解决.

➤3.7 推论 1 设 a, b, d 是给定的整数,$b \neq 0$, 则存在唯一的一对整数 q 和 r, 满足 $a = bq + r(d \leqslant r < |b| + d)$.

证明: 考虑整数 $(a - d)$ 及 b, 由带余数除法知, 存在唯一的整数对 q 和 r_0, 使得 $a - d = bq + r_0$ $(0 \leqslant r_0 < |b|)$, 所以 $a = bq + r$, 其中 $r = r_0 + d(d \leqslant r < |b| + d)$. 由 q 和 r_0 的唯一性得知 q 和 r 唯一存在. 证毕.

➤3.8 e.g. 当 $2 \mid b$ 时, 取 $d = -\dfrac{|b|}{2}$; 当 $2 \nmid b$ 时, 取 $d = -\dfrac{|b|-1}{2}$, 则

$$a = bq + r, \quad \text{其中} \begin{cases} -\dfrac{|b|}{2} \leqslant r < \dfrac{|b|}{2}, & 2 \mid b \\ -\dfrac{|b|-1}{2} \leqslant r < \dfrac{|b|+1}{2}, & 2 \nmid b \end{cases}$$

这种带余数除法中的余数 r 叫做**绝对最小余数**.

➤3.9 例 1 若 $N = 2^{2000} - 2^{1998} + 2^{1996} - 2^{1994} + 2^{1992} - 2^{1990}$, 则 $9 \mid N$.

➤3.10 例 2 当 $n \in \mathbb{N}_+$ 时, 求证:$23 \mid (5^{2n+1} + 2^{n+4} + 2^{n+1})$.

➤3.11 例 3 设 $a_1, a_2, \cdots, a_n$ 为不全为零的整数, 以 y_0 表示集合

$$A = \{y \mid y = a_1x_1 + \cdots + a_nx_n, x_i \in \mathbb{Z}, 1 \leqslant i \leqslant n\}$$

中的最小正数, 则对于任何 $y \in A$, 有 $y_0 \mid y$; 特别地, 有 $y_0 \mid a_i(1 \leqslant i \leqslant n)$.

证明: 设 $y_0 = a_1x_1' + \cdots + a_nx_n' \in A$, 对任意的 $y = a_1x_1 + \cdots + a_nx_n \in A$, 由定理 1 知, 存在 $q, r \in \mathbb{Z}$, 使得 $y = qy_0 + r\,(0 \leqslant r < y_0)$. 因此

$$r = y - qy_0 = a_1\,(x_1 - qx_1') + \cdots + a_n\,(x_n - qx_n') \in A$$

如果 $r \neq 0$, 那么, 因为 $0 < r < y_0$, 所以 r 是 A 中比 y_0 还小的正整数, 这与 y_0 的定义矛盾所以 $r = 0$, 即 $y_0 \mid y$.

显然 $a_i \in A(1 \leqslant i \leqslant n)$, 所以由上述结论得 $y_0 \mid a_i(1 \leqslant i \leqslant n)$. 证毕.

➤3.12 例 4 证明: 任意给出的五个整数中, 必有三个数之和能被 3 整除.

证明: 设这五个整数是 a_i, 令 $a_i = 3q_i + r_i\,(0 \leqslant r_i < 3, i = 1, 2, 3, 4, 5)$. 分别考虑以下两种情形:

(i) 若在 $r_1, r_2, \cdots, r_5$ 中数 $0, 1, 2$ 都出现, 不妨设 $r_1 = 0, r_2 = 1, r_3 = 2$, 此时

$$a_1 + a_2 + a_3 = 3\,(q_1 + q_2 + q_3) + 3$$

能被 3 整除;

(ii) 若在 $r_1, r_2, \cdots, r_5$ 中数 $0, 1, 2$ 至少有一个不出现, 则根据抽民原理至少有三个 r_i 要取相同的值, 不妨设 $r_1 = r_2 = r_3 = r(r$ 是 $0, 1, 2$ 中的某一个), 此时

$$a_1 + a_2 + a_3 = 3\,(q_1 + q_2 + q_3) + 3r$$

能被 3 整除. 综合情形 (i) 和 (ii) 可知, 所证结论成立. 证毕.

➤3.13 注 例 2 涉及的抽屉原理也称为 P.G. Dirichlet 原理, 即把 $n+1$ 个元素或者更多的元素放入 n 个抽屉中, 则在其中一个抽屉里至少要放入 2 个元素. 一般, 将 m 个元素放人 $n(m > n)$ 个抽屉中, 则在其中一个抽屉里至少含有 $\left[\dfrac{m-1}{n}\right] + 1$(中括号表示不超过 $\dfrac{(m-1)}{n}$ 的最大整数) 个元素. 值得注意的是, 利用带余数除法得到的余数进行分类来构造抽屉是数论解 (证) 题中常用的方法.

➤3.14 例 5 设 r 是正奇数, 证明: 对任意的正整数 n, 有 $(n+2) \nmid (1^r + 2^r + \cdots + n^r)$.

证明: 当 $n = 1$ 时, 结论显然成立. 现设 $n \geqslant 2$, 令 $S = 1^r + 2^r + \cdots + n^r$, 则

$$2S = 2 + (2^r + n^r) + [3^r + (n-1)^r] + \cdots + (n^r + 2^r)$$

因为 r 为奇数, 由 1.1 节的分解公式 (II) 可得上式右边中除第一项外, 每一加项 $i^r + (n+2-i)^r$ 都能被 $i + (n+2-i) = n+2(2 \leqslant i \leqslant n)$ 整除, 因此 $2S = 2 + (n+2)Q_1$, 其中 Q_1 是整数. 显然,$2S$ 被 $n+2$ 除得的余数是 2, 由于 $n+2 > 2$, 所以 $(n+2) \mid 2S$, 故 $(n+2) \mid S$. 证毕.

➤**3.15 例 6** 对 m 和 n 为正整数,$m>2$, 证明:$(2^m-1)\nmid(2^n+1)$.

证明: 对正整数 m 和 n 分以下三种情形讨论:

(i) 当 $n=m$ 时,$2^n+1=(2^n-1)+2$, 由于 $n=m, m>2$, 所以 $2^n-1>2$, 因而

$$(2^n-1)\nmid(2^n+1)$$

(ii) 当 $n<m$ 时, 有 $n\leqslant m-1$, 注意到 $m>2$, 有 $2^n+1\leqslant 2^{m-1}+1<2^m-1$, 由定理 1.1.1 之 (IV) 知 $(2^m-1)\,X\,(2^n+1)$.

(iii) 当 $n>m$ 时, 设 $n=mq+r(0\leqslant r<m, q\in\mathbf{N})$, 由于

$$2^n+1=(2^{mq}-1)\cdot 2^r+(2^r+1)$$

由 1.1 节的分解公式 (I) 得 $(2^m-1)\mid(2^{mq}-1)$.

当 $r=0$ 时,

$$2^n+1=(2^{mq}-1)+2=(2^m-1)\cdot M+2\quad(M\in\mathbf{Z})$$

由于 $m>2$, 故 $2^m-1>2$, 因此 $(2^m-1)\nmid 2$, 从而 $(2^m-1)\nmid(2^n+1)$.

当 $0<r<m$ 时, 由 (i) 知 $(2^m-1)\nmid(2^r+1)$.

综上可知, 对一切正整数 m 和 $n(m>2)$, 有 $(2^m-1)\}\,(2^n+1)$. 证毕.

➤**3.16 例 7** 证明: 若 a 被 9 除的余数是 3,4,5 或 6, 则方程 $x^3+y^3=a$ 没有整数解.

证明: 对任意整数 x, y, 记 $x=3q_1+r_1, y=3q_2+r_2$, 其中 $0\leqslant r_1, r_2<3, q_1, q_2\in\mathbf{Z}$. 于是有 $x^3=9Q_1+r_1^3, y^3=9Q_2+r_2^3$, 其中 $Q_1, Q_2\in\mathbf{Z}$. 所以 $x^3+y^3=9\,(Q_1+Q_2)+r_1^3+r_2^3$.

显然,x^3+y^3 被 9 除的余数与 $r_1^3+r_2^3$ 被 9 除的余数相同. 由于 r_1^3, r_2^3 被 9 除的余数为 0,1 或 8, 因此,$r_1^3+r_2^3$ 被 9 除的余数只可能是 $0,1,2,7$ 或 8; 而已知 a 被 9 除的余数是 $3,4,5$ 或 6, 所以,x^3+y^3 不可能等于 a, 即方程 $x^3+y^3=a$ 没有整数解. 证毕.

➤**3.17 注** 若一个整系数方程有整数解, 则用任何非零数同时除此方程两边所得的最小非负余数都相同. 基于这个性质可知, 若一个方程两边用同一个非零整数去除所得的余数不相同, 则此方程必无整数解. 例 5 正是运用了此种基本思想.

作业:	P6 习题 1.2、1;3
教学后记:	

第四讲　最大公因数

教学目标：	掌握最大公因数的概念、性质及其求法
教学重点：	最大公因数的性质及其求法
教学难点：	最大公因数的性质
教学方法和手段：	讲授
教学时数：	10 课时

一、最大公因数的概念

➤**4.1 定义 1**　若 $b \mid a_1, b \mid a_2, \cdots, b \mid a_n$, 则 b 叫作 $a_1, a_2, \cdots, a_n$ 的公因数.

➤**4.2 e.g.**$-3, 6$ 都是 12 与 18 的公因数, 其中 6 是 12 与 18 的所有公因数中最大的一个, 叫作 12 与 18 的最大公因数, 记作 $(12, 18) = 6$.

➤**4.3 定义 2**　整数 $a_1, a_2, \cdots, a_n$ 共有的因数中最大的一个叫作 $a_1, a_2, \cdots, a_n$ 的最大公因数, 记作 $(a_1, a_2, \cdots, a_n)$, 读作 $a_1, a_2, \cdots, a_n$ 的最大公因数.

显然 $(a_1, a_2, \cdots, a_n)$ 是正整数.

➤**4.4 定理 1**　整数 $a_1, a_2, \cdots, a_n$ 的最大公因数唯一存在.

➤**4.5 定义 3**　若 $(a_1, a_2, \cdots, a_n) = 1$, 则称 $a_1, a_2, \cdots, a_n$ 互质; 若 $a_1, a_2, \cdots, a_n$ 中任意两个互质, 则称 $a_1, a_2, \cdots, a_n$ 两两互质 $((a_i, a_j) = 1 (1 \leqslant i, j \leqslant n, i \neq j))$.

若几个数两两互质, 则这几个数一定互质. 反之未必成立.

➤**4.6 e.g.**$2, 3, 5$ 两两互质, 它们也互质;$3, 4, 6$ 互质但不两两互质.

➤**4.7 定理 2**　若 $a_1, a_2, \cdots, a_n$ 是不全为零的整数, 则

$$a_1, a_2, \cdots, a_n 与 |a_1|, |a_2|, \cdots, |a_n|$$

有相同的公因数, 且

$$(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$$

证明: 设 $p \mid a_k (k = 1, 2, 3, \cdots, n)$, 则存在 n 个整数 q_k, 使得 $a_k = pq_k$. 所以 $a_k| = |pq_k| = p(\pm |q_k|)$, 所以

$$p||a_k \mid (k = 1, 2, 3, \cdots, n)$$

即 $a_1, a_2, \cdots, a_n$ 的任意公因数是 $|a_1|, |a_2|, \cdots, |a_n|$ 的公因数.

反之, 同理可证 $|a_1|, |a_2|, \cdots, |a_n|$ 的任意公因数也是 $a_1, a_2, \cdots, a_n$ 的公因数.

故 $a_1, a_2, \cdots, a_n$ 与 $|a_1|, |a_2|, \cdots, |a_n|$ 有相同的公因数. 当然, 其中最大者也相同, 即

$$(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$$

➤**4.8 注** 该定理告诉我们, 讨论任意几个不全为零的整数的最大公因数问题, 可以转化为讨论几个非负整数的最大公因数问题, 因此本节下面的讨论将在非负整数范围内进行.

➤**4.9 定理 3** (i)$(a, b) = (b, a)$

(ii) 若 $a \neq 0$, 则 $(a, 0) = |a|, (a, a) = |a|$.

二、最大公因数的性质

➤**4.10 定理 4** 若 $a = bq + r(0 \leqslant r < b)$, 则 $(a, b) = (b, r)$.[定理 1.3.1(ii)]

证明: 设 $(a, b) = d, (b, r) = e$, 则 $d|a, d|b$, 故 $d \mid (a - bq) = r, d$ 是 b, r 的一个公因数, 而 $(b, r) = e$, 故 $d \leqslant e$. 同理可得 $e \leqslant d$. 故 $d = e$, 即 $(a, b) = (b, r)$.

➤**4.11 e.g.** 由 $377 = 319 \times 1 + 58$, 可得 $(319, 377) = (319, 58)$.

➤**4.12 注** 定理的证法也是证明两个最大公因数相等的常用方法, 同时, 还是展转相除法求最大公因数的理论基础.

➤**4.13 定理 5** 设 $a_1, a_2, \cdots, a_n \in \mathbf{Z}$, 记 $A = \left\{ y \mid y = \sum_{i=1}^{n} a_i x_i, x_i \in \mathbf{Z}, 1 \leqslant i \leqslant n \right\}$. 如果 y_0 是集合 A 中最小的正数, 则 $y_0 = (a_1, a_2, \cdots, a_n)$.[定理 1.3.2]

证明: 由于 y_0 是集合 A 中最小的正数, 故 $y_0 = \sum_{i=1}^{n} a_i x_i^0 \left(x_i^0 \in \mathbf{Z}, 1 \leqslant i \leqslant n\right)$. 设 d 是 $a_1, a_2, \cdots, a_n$ 的任意一个公因数, 则 $d \mid y_0 = \sum_{i=1}^{n} a_i x_i^0$, 所以 $d \leqslant y_0$.

又由 1.2 节例 1 的结论知 $y_0 \mid a_i (1 \leqslant i \leqslant n)$, 故 y_0 也是 $a_1, a_2, \cdots, a_n$ 的公因数. 因此,y_0 是 $a_1, a_2, \cdots, a_n$ 所有公因数中的最大正数, 由此即得 $y_0 = (a_1, a_2, \cdots, a_n)$. 证毕.

➤**4.14 注** 由于 $(a_1, a_2, \cdots, a_n)$ 是集合 $A = \left\{ y \mid y = \sum_{i=1}^{n} a_i x_i, x_i \in \mathbf{Z}, \right.$

$1 \leqslant i \leqslant n\}$ 的最小正数, 由定理 1.3.2 的证明过程直接得到如下推论.

➤**4.15 推论 1** 设不全为零整数 $a_1, a_2, \cdots, a_n$ 的最大公因数是 $(a_1, a_2, \cdots, a_n)$, 则存在整数 $x_1', x_2', \cdots, x_n'$, 使得 $a_1x_1' + a_2x_2' + \cdots + a_nx_n' = (a_1, a_2, \cdots, a_n)$.[推论 1.3.1]

➤**4.16 定理 6** 若 $d > 0, d \mid a, d \mid b$, 则 $(a, b) = d \Leftrightarrow$ 存在整数 s, t, 使得 $d = as + bt$.(贝祖 (Bézout) 等式).

➤**4.17 推论 1** 设 d 是 $a_1, a_2, \cdots, a_n$ 的任意一个公因数, 则 $d \mid (a_1, a_2, \cdots, a_n)$. [设 q 是 a, b 的任意一个公因数,d 是 a, b 的一个公因数, 则 $d = (a, b) \Leftrightarrow q \mid d$][推论 1.3.2]

证明: 由推论 1.3.1 知, 存在整数 $x_1', \cdots, x_n'$ 使得

$$a_1x_1' + \cdots + a_nx_n' = (a_1, \cdots, a_n)$$

所以由 $d \mid a_i (1 \leqslant i \leqslant n)$, 有 $d \mid (a_1x_1' + \cdots + a_nx_n')$, 即 $d \mid (a_1, a_2, \cdots, a_n)$. 证毕.

➤**4.18 注** 推论 1.3.2 对最大公因数的本质属性做了非常深刻的刻画: 最大公因数不但是公因数中最大的, 而且是 $a_1, a_2, \cdots, a_n$ 所有公因数的倍数.

➤**4.19 定理 7** [定理 1.3.3]$(a_1, a_2, \cdots, a_n) = 1$ 的充分必要条件是存在整数 $x_1, x_2, \cdots, x_n$, 使得

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1 \tag{4.1}$$

证明: 必要性由推论 1.3.1 即可得到式(4.1).

充分性若式(4.1)成立, 令 $(a_1, a_2, \cdots, a_n) = d$, 由 $d \mid a_i (1 \leqslant i \leqslant n)$ 推出:

$$d \mid (a_1x_1 + a_2x_2 + \cdots + a_nx_n) = 1$$

故 $d = 1$, 即 $(a_1, a_2, \cdots, a_n) = 1$. 证毕.

➤**4.20 定理 8** 设 $d|a, d|b$, 则 $d = (a, b) \Leftrightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

证明: 必要性.

设 $\left(\frac{a}{d}, \frac{b}{d}\right) = p > 1$, 则 $p \left|\frac{a}{d}, p\right| \frac{b}{d}, \therefore dp|a, dp|b$, 这说明 dp 是 a 与 b 的一个公因数, 而 $dp > d$, 这与 $d = (a, b)$ 矛盾, 故 $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

充分性.

若 $(a, b) = q > d$, 则因为 $d|a, d|b$, 由推论 2 可知 $d \mid q$.

设 $q = dp (p > 1)$, 因为 $(a, b) = q$, 所以 $q|a, q|b$

因为 $dp|a, dp|b$, 所以 $p \left|\frac{a}{d}, p\right| \frac{b}{d}$

即 p 是 $\frac{a}{d}, \frac{b}{d}$ 的一个大于 1 的公因数, 这与 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$ 矛盾.

故 $(a, b)=d$.

➤**4.21 推论 1** 设 $d \mid a_k(k=1,2, \cdots, n)$, 则

$$(a_1, a_2, \cdots, a_n)=d \Leftrightarrow \left(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_n}{d}\right)=1$$

➤**4.22 定理 9** $(ac, bc)=c(a, b)$

证明: 设 $(a, b)=d$, 则 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$

因为 $\left(\frac{ac}{dc}, \frac{bc}{dc}\right)=1$, 所以 $(ac, bc)=dc=c(a, b)$.

➤**4.23 推论 1** $(ma_1, ma_2, \cdots, ma_n)=|m|(a_1, a_2, \cdots, a_n)$, 其中 $m \neq 0$.

例如,$(12, 28, 64)=4(3, 7, 16)=4 \times 1=4$.

➤**4.24 例 1** 若 $(a, b)=1$, 求 $(a-b, a+b)$.

解: 设 $(a-b, a+b)=d$, 则 $d|a-b, d|a+b$, 所以 $d|2a, d|2b, d \mid (2a, 2b)=2(a, b)=2$

于是 $d=1$ 或 $d=2$.

➤**4.25 注** 定理 8 给出了一个证明数论问题的常用方法: 由两个不全为零且不互素的整数, 可自然地产生一对互素的整数. 利用这一结论, 数论中不全为零且不互素的整数可以化归为互素的整数, 从而达到简化问题证明过程的目的.

➤**4.26 定理 10** 由 $b \mid ac$ 及 $(a, b)=1$ 可以推出 $b \mid c$.[定理 1.3.5(i)]

证明: 证法一: 若 $(a, b)=1$, 由定理 1.3.3 知, 存在整数 x 与 y, 使得 $ax+by=1$. 因此,

$$acx+bcy=c \tag{4.2}$$

由式(4.2)及 $b \mid ac$ 得到 $b \mid c$. 结论得证.

证法二: 因为 $(a, b)=1$, 所以 $c=c(a, b)=(ac, bc)$,

因为 $b \mid bc, b \mid ac$, 于是 $b \mid (ac, bc)=c$.

➤**4.27 推论 1** 设 p 为质数, 若 $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$.

➤**4.28 定理 11** 由 $b|c, a|c$ 及 $(a, b)=1$ 可以推出 $ab \mid c$.[定理 1.3.5(ii)]

证明: 证法一: 因为 $(a, b)=1$, 由定理 1.3.3 知, 存在整数 x, y 使得式(4.2)成立. 又由 $b \mid c$ 与 $a \mid c$, 得 $ab|ac, ab|bc$, 再由式(4.2)得 $ab \mid c$. 故结论得证. 证毕.

证法二:

e.g. 因为 $2 \mid 12, 3 \mid 12, (2, 3)=1$, 所以 $2 \times 3=12$.

➤**4.29 推论 1** 若 $(a,b)=1$, 则 $(a,bc)=(a,c)$.[推论 1.3.3]

证明: 证法一: 由于 $(a,b)=1$, 由定理 1.3.3 知, 存在整数 x,y 使得式(4.2)成立.

设 $d=(a,bc), d'=(a,c)$, 则 $d|a, d|bc$, 由式(4.2)得 $d \mid c$, 即 d 是 a 与 c 的公因数, 故 $d \leqslant d'$; 又 d' 是 a 与 c 的公因数, 则它也是 a 与 bc 的公因数. 因此 $d' \leqslant d$, 故 $(a,bc)=(a,c)$. 证毕.

证法二: 设 $(a,bc)=d, (a,c)=h$, 则 $d|a, d|bc$.

因为 $(a,b)=1, d|a, (d,b)=1$, 所以 $d|c, d \mid h$.

反之, 同理可得 $h \mid d$, 所以 $d=h$, 即 $(a,bc)=(a,c)$.

例如,$(9,1350)=(9,135)=(9,27)=9$.

➤**4.30 推论 2** 若 $(a_i,b_j)=1(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m)$, 则 $(a_1a_2\cdots a_n, b_1b_2\cdots b_m)=1$.[推论 1.3.4]

特别地, 若 $(a,b)=1$, 则对任意正整数 m 和 n 有 $(a^n,b^m)=1$.

证明: 由于 $(a_i,b_j)=1(1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m)$, 由推论 1.3.1 得

$$(a_i, b_1b_2\cdots b_m)=(a_i, b_2\cdots b_m)=\cdots=(a_i,b_m)=1 \quad (1 \leqslant i \leqslant n)$$

故 $(a_1a_2\cdots a_n, b_1b_2\cdots b_m)=(a_2\cdots a_n, b_1b_2\cdots b_m)=\cdots=(a_n, b_1b_2\cdots b_m)=1$. 证毕.

➤**4.31 推论 3** 设 a,b 是不全为零的整数,n 为正整数, 则 $(a^n,b^n)=(a,b)^n$.

提示:$(a,b)=d(d \geqslant 1) \Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right)=1 \Rightarrow \left(\frac{a^n}{d^n}, \frac{b^n}{d^n}\right)=1$.

➤**4.32 定理 12** 对于任意 n 个不全为零的整数 $a_1, a_2, \cdots, a_n$, 记

$$(a_1,a_2)=d_2, (d_2,a_3)=d_3, \cdots, (d_{n-2},a_{n-1})=d_{n-1}, (d_{n-1},a_n)=d_n$$

则 $d_n=(a_1,a_2,\cdots,a_n)$[定理 1.3.6]

证明: 由已知条件及整除的传递性, 有

$$d_n=(d_{n-1},a_n) \Rightarrow d_n \,|a_n, d_n|\, d_{n-1}$$
$$d_{n-1}=(d_{n-2},a_{n-1}) \Rightarrow d_{n-1} \,|a_{n-1}, d_{n-1}|\, d_{n-2}, \text{故} d_n \,|a_n, d_n|\, a_{n-1}, d_n \mid d_{n-2}$$
$$d_{n-2}=(d_{n-3},a_{n-2}) \Rightarrow d_{n-2} \,|a_{n-2}, d_{n-2}|\, d_{n-3}, \text{故} d_n \,|a_n, d_n|\, a_{n-1}, d_n \,|a_{n-2}, d_n|\, d_{n-3}$$
$$\cdots$$
$$d_2=(a_1,a_2) \Rightarrow d_n \,|a_n, d_n|\, a_{n-1}, \cdots, d_n \,|a_2, d_n|\, a_1$$

即 d_n 是 $a_1, a_2, \cdots, a_n$ 的一个公因数.

又对于 $a_1, a_2, \cdots, a_n$ 的任何公因数 d, 由推论 1.3.2 及 $d_2, \cdots, d_n$ 的定义, 依次得出

$$d \mid a_1, d \mid a_2 \Rightarrow d \mid d_2$$
$$d \mid d_2, d \mid a_3 \Rightarrow d \mid d_3$$
$$\cdots$$
$$d \mid d_{n-1}, d \mid a_n \Rightarrow d \mid d_n$$

故 d_n 是 $a_1, a_2, \cdots, a_n$ 公因数中的最大者. 因此,$d_n = (a_1, a_2, \cdots, a_n)$. 证毕.

➤**4.33 注** 定理 1.3.6 指出了求 $n(n > 2)$ 个不全为零整数最大公因数的方法, 其实质是先化归为 $n-1$ 个整数的最大公因数问题, 最终化归为两个整数的最大公因数问题来解决.

➤**4.34 定理 13** [定理 1.3.7]设 a, b, c, n 是正整数,$ab = c^n, (a, b) = 1$, 则存在正整数 u, v, 使得

$$a = u^n, \quad b = v^n, \quad c = uv, \quad (u, v) = 1$$

证明: 因为 $(a, b) = 1$, 所以 $(b, a^{n-1}) = 1$, 故 $a = a(b, a^{n-1}) = (ab, a^n) = (c^n, a^n) = (c, a)^n$;

同理得 $b = (c, b)^n$. 令 $u = (a, c), v = (b, c)$, 则 $a = u^n, b = v^n, c = uv$, 且

$$(u, v) = ((a, c), (b, c)) = (a, b, c) = ((a, b), c) = (1, c) = 1$$

故定理结论成立. 证毕.

➤**4.35 注** 定理 1.3.7 说明, 如果互素的两个正整数之积是一个整数的 n 次幂, 则这两个正整数都是整数的 n 次幂. 此结论还可推广为: 如果正整数 $a, b, \cdots, c$ 之积是一个整数的 n 次幂, 若 $a, b, \cdots, c$ 两两互素, 则 $a, b, \cdots, c$ 都是整数的 n 次幂. 这个性质表现了整数互素的重要性, 其应用较广泛.

➤**4.36 例 2** 设 n 是正整数, 证明:$(n! + 1, (n + 1)! + 1) = 1$.

证明: 设 $d = (n!+1, (n+1)!+1)$, 由于 $(n!+1)(n+1)-[(n+1)!+1] = n$, 于是有 $d \mid n$. 进一步有 $d \mid n!$, 结合 $d \mid (n! + 1)$ 可知 $d \mid 1$, 故 $d = 1$. 证毕.

➤**4.37 例 3** 证明: 任意两个费马数 $(F_m, F_n) = 1 (m \neq n)$.

证明: 不妨设 $m > n$. 由 1.1 节例 3 知, 当 $m > n \geqslant 0$ 时, 费马数满足 $F_n \mid (F_m - 2)$, 即存在整数 t, 使得 $F_m = 2 + tF_n$. 设 $d = (F_m, F_n)$, 则 $d = (2 + tF_n, F_n) = (2, F_n) = 2$, 故 $d = 1$ 或 $d = 2$. 但 F_n 显然是奇数, 故必有 $d = 1$, 即费马数是两两互素的. 证毕.

➤**4.38 例 4** 设 $m,n>0,mn\mid(m^2+n^2)$, 证明:$m=n$.

证明: 设 $(m,n)=d$, 则 $m=m_1d,n=n_1d$, 其中 $(m_1,n_1)=1$. 于是, 已知条件化为 $m_1n_1\mid(m_1^2+n_1^2)$, 由此得 $m_1\mid(m_1^2+n_1^2)$, 故 $m_1\mid n_1^2$. 但是 $(m_1,n_1)=1$, 结合 $m_1\mid n_1^2$, 可知必须 $m_1=1$. 同理 $n_1=1$. 因此 $m=n$. 证毕.

➤**4.39 注** 由例 4 知, 对于给定的两个不全为零的整数, 常借助于它们的最大公因数来产生两个互素的整数, 以便能利用互素的性质作进一步讨论, 这实质上是将原问题化归为互素的特殊情形.

➤**4.40 例 5** 设 k 为正奇数, 证明:$1+2+\cdots+n$ 整除 $1^k+2^k+\cdots+n^k$.

证明: 因为 $1+2+\cdots+n=\dfrac{n(n+1)}{2}$, 且 $(n,n+1)=1$, 所以结论等价于证明

$$n\left|2\left(1^k+2^k+\cdots+n^k\right),\quad (n+1)\right|2\left(1^k+2^k+\cdots+n^k\right)$$

事实上, 由于 k 是奇数, 利用配对法可得

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

上式的每个加项显然都是 n 的倍数, 故其和也是 n 的倍数. 同理得

$$2\left(1^k+2^k+\cdots+n^k\right)=\left(1^k+n^k\right)+\left[2^k+(n-1)^k\right]+\cdots+\left(n^k+1^k\right)$$

上式是 $n+1$ 的倍数, 故 $n(n+1)\mid 2\left(1^k+2^k+\cdots+n^k\right)$. 证毕.

三、最大公因数的求法

根据最大公因数的定义和性质, 我们可以得到多种求最大公因数的方法, 在此只介绍常用的、重要的基本方法.

4.3.1 分解质因数法

根据推论 1.3.2 可知, 几个数的公因数是这几个数最大公因数的因数, 由此和最大公因数的定义, 我们可以得到求最大公因数的分解质因数法, 其过程如下:

(1) 写出各数的标准分解式;

(2) 写出各分解式共同的质因数及其最小次方数, 并把如此得到的幂写成连乘的形式.

➤**4.41 例 6** 求 $(60,108,24)$.

解: 因为 $60=2^2\times3\times5,108=2^2\times3^3,24=2^3\times3$,

所以 $(60,108,24)=2^2\times3=12$

4.3.2 提取公因数法 (短除法)

根据定理 1.3.4, 可用逐步提取公因数的方法求几个数的最大公因数.

➤**4.42 例 7** 求 $(162, 216, 378, 108)$.

解:

$$\begin{aligned}(162, 216, 378, 108) &= 2 \times (81, 108, 189, 54) = 2 \times 9 \times (9, 12, 21, 6) \\ &= 18 \times 3 \times (3, 4, 7, 2) = 54 \times 1 = 54\end{aligned}$$

这一过程通常写成下面的短除形式:

2	162	216	378	108
9	81	108	189	54
3	9	12	21	6
	3	4	7	2

因为 $(3, 4, 7, 2) = 1$, 所以 $(162, 216, 378, 108) = 2 \times 9 \times 3 = 54$.

4.3.3 辗转相除法

➤**4.43 定义 4** 下面的一组带余数除法, 称为辗转相除法.

设 a 和 b 是整数.$b \neq 0$, 依次作带余数除法**:**

$$\left.\begin{array}{ll} a = bq_1 + r_1, & 0 < r_1 < |b| \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1 \\ \cdots & \\ r_{k-1} = r_kq_{k+1} + r_{k+1}, & 0 < r_{k+1} < r_k \\ \cdots & \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1} & r_{n+1} = 0 \end{array}\right\} \tag{4.3}$$

由于 b 是固定的, 且 $|b| > r_1 > r_2 > \cdots$, 所以式(4.3)中仅包含有限个等式.

➤**4.44 定理 14** 使用式(4.3)中的记号, 记

$$\begin{aligned} &P_0 = 1, \quad P_1 = q_1, \quad P_k = q_kP_{k-1} + P_{k-2} \quad (k \geqslant 2) \\ &Q_0 = 0, \quad Q_1 = 1, \quad Q_k = q_kQ_{k-1} + Q_{k-2} \quad (k \geqslant 2) \end{aligned}$$

则

$$aQ_k - bP_k = (-1)^{k-1}r_k \quad (k = 1, 2, \cdots, n) \tag{4.4}$$

证明: 当 $k=1$ 时, 式(4.4)成立. 当 $k=2$ 时, 有

$$Q_2 = q_2Q_1 + Q_0 = q_2, \quad P_2 = q_2P_1 + P_0 = q_2q_1 + 1$$

此时由式(4.3)得

$$aQ_2 - bP_2 = aq_2 - b\left(q_2q_1+1\right) = \left(a - bq_1\right)q_2 - b = r_1q_2 - b = -r_2$$

即式(4.4)成立.

假设对于 $k < m(1 \leqslant m \leqslant n)$ 式(4.4)成立, 由此假设及式(4.3)得到

$$\begin{aligned} aQ_m - bP_m =& a\left(q_mQ_{m-1} + Q_{m-2}\right) - b\left(q_mP_{m-1} + P_{m-2}\right) \\ =& \left(aQ_{m-1} - bP_{m-1}\right)q_m + \left(aQ_{m-2} - bP_{m-2}\right) \\ =& (-1)^{m-2}r_{m-1}q_m + (-1)^{m-3}r_{m-2} \\ =& (-1)^{m-1}\left(r_{m-2} - r_{m-1}q_m\right) = (-1)^{m-1}r_m \end{aligned}$$

即当 $k=m$ 时式(4.4)也成立.

由归纳原理, 式(4.4)对一切正整数 k 都成立.

➤**4.45** 定理14的结论可利用表 1.1 来记忆与实现: 按箭头所指方向, 依照斜线相乘、横线相加的原则, 可依次求出 P_k 和 $Q_k(k \geqslant 2)$.

k	0	1	2	3	$\cdots$	k	$\cdots$	n
q_k		q_1	q_2	q_3	$\cdots$	q_k	$\cdots$	q_n
P_k	P_0	P_1	P_2	P_3	$\cdots$	$P_k = q_kP_{k-1} + P_{k-2}$	$\cdots$	P_n
Q_k	Q_0	Q_1	Q_2	Q_3	$\cdots$	$Q_k = q_kQ_{k-1} + Q_{k-2}$	$\cdots$	Q_n

➤**4.46 定理 15** 使用式(4.3)中的记号, 有 $r_n = (a,b)$.

证明: 由(4.3)式得

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \cdots = (r_1, r_2) = (b, r_1) = (a,b)$$

➤**4.47** 由此知, 利用辗转相除法可以求出不全为零的整数 x, y, 使得

$$ax + by = (a,b) \tag{4.5}$$

成立.

事实上, 在式(4.4)中, 令 $k=n$, 则 $aQ_n - bP_n = (-1)^{n-1}r_n$, 于是有

$$(-1)^{n-1}Q_na + (-1)^nP_nb = r_n = (a,b) \tag{4.6}$$

比较式(4.5)和式(4.6)得

$$x = (-1)^{n-1}Q_n, \quad y = (-1)^nP_n$$

➤**4.48 注** 若 $x = x_0, y = y_0$ 是适合式(4.5)的一对整数, 则等式 $a(x_0 + bs) + b(y_0 - as) = (a, b)$(其中 s 为任意整数) 说明, 满足此式的 x, y 有无穷多组, 并且在 $ab > 0$ 时, 可人为地选择 x 为正 (负) 数,y 相应地为负 (正) 数. 此结论常用于证明最大公因数相关问题.

➤**4.49 例 8** 求 $(5767, 4453)$.

解: $\because 5767 = 4453 \times 1 + 1314, \therefore (5767, 4453) = (4453, 1314)$;

$\because 4453 = 1314 \times 3 + 511, \therefore (4453, 1314) = (1314, 511)$;

$\because 1314 = 511 \times 2 + 292, \therefore (1314, 511) = (511, 292)$;

$\because 511 = 292 \times 1 + 219, \therefore (511, 292) = (292, 219)$

$\because 292 = 219 \times 1 + 73, \therefore (292, 219) = (219, 73)$

$\because 219 = 73 \times 3 + 0, \therefore (219, 73) = 73$

$\therefore (5767, 4453) = 73$

上述过程数据、符号书写重复太多, 可以简化为下面的竖式:

1	4453	5767		q_1	b	a	
	3942	4453			r_1q_2	bq_1	
2	511	1314	3	q_3	r_2	r_1	q_2
	292	1022			r_3q_4	r_2q_3	
1	219	292	1	q_5	r_4	r_3	q_4
	219	219			r_5q_6	r_4q_5	
	0	73	3		r_6	r_5	q_6

所以 $(5767, 4453) = 73; (a, b) = (b, r_1) = (r_1, r_2) = \cdots$

➤**4.50 例 9** 求 $(1008, 1260, 882, 1134)$.

分析: 可改求 $(((1008, 1260), 882), 1134)$ 或 $((1008, 1260), (882, 1134))$.

解: 由辗转相除法可得

$$(1008, 1260) = 252, (882, 1134) = 126$$

而 $(252, 126) = 126$, 故 $(1008, 1260, 882, 1134) = 126$.

➤**4.51 例 10** 用辗转相除法求 $(125, 17)$, 并求整数 x, y, 使得 $125x + 17y = (125, 17)$.

证明: 作辗转相除法, 有

$$\begin{aligned} 125 &= 7 \times 17 + 6, \quad q_1 = 7, \quad r_1 = 6 \\ 17 &= 2 \times 6 + 5, \quad q_2 = 2, \quad r_2 = 5 \\ 6 &= 1 \times 5 + 1, \quad q_3 = 1, \quad r_3 = 1 \\ 5 &= 5 \times 1, \quad q_4 = 5 \end{aligned}$$

由定理15得 $(125, 17) = r_3 = 1$.

下面利用定理15的结论来计算满足条件的整数 x 和 y. 根据上面的计算及定理14, 有

$$P_0=1,\quad P_1=7,\quad P_2=2\times7+1=15,\quad P_3=1\times15+7=22$$
$$Q_0=0,\quad Q_1=1,\quad Q_2=2\times1+0=2,\quad Q_3=1\times2+1=3$$

上述计算过程如表 1.2 所列, 依照斜线相乘、横线相加原则，依次求出 P_k 和 $Q_k(2\leqslant k\leqslant3)$.

k	0	1	2	3
q_k		7	2	1
P_k	1	7	$P_2=2\times7+1=15$	$P_3=1\times15+7=22$
Q_k	0	1	$Q_2=2\times1+0=2$	$Q_3=1\times2+1=3$

取 $x=(-1)^{3-1}Q_3=3, y=(-1)^3P_3=-22$, 则 $125\times3+17\times(-22)=(125,17)=1$.

➤**4.52 例 11** 设 m,n 是正整数, 证明:$(2^m-1,2^n-1)=2^{(m,n)}-1$.

证明: 不妨设 $m\geqslant n$. 由带余数除法得 $m=q_1n+r_1, 0\leqslant r_1<n$. 于是有

$$2^m-1=2^{nq_1+r_1}-2^{r_1}+2^{r_1}-1=2^{r_1}\left(2^{nq_1}-1\right)+2^{r_1}-1$$

由上式及 $(2^n-1)\mid(2^{nq_1}-1)$ 得

$$(2^m-1,2^n-1)=(2^n-1,2^{r_1}-1)$$

注意到 $(m,n)=(n,r_1)$, 若 $r_1=0$, 则 $(m,n)=n$, 结论成立. 若 $r_1>0$, 则继续对 $(2^n-1,2^{r_1}-1)$ 进行类似讨论. 利用辗转相除法得

$$\begin{aligned}
n&=q_2r_1+r_2\,(0<r_2<r_1)\\
&\vdots\\
r_{k-2}&=q_kr_{k-1}+r_k\,(0<r_k<r_{k-1})\\
r_{k-1}&=q_{k+1}r_k\,(r_{k+1}=0)
\end{aligned}$$

则 $(2^n-1,2^{r_1}-1)=(2^{r_1}-1,2^{r_2}-1)=\cdots=(2^{r_k}-1,2^{r_{k+1}}-1)=(2^{r_k}-1,0)=2^{r_k}-1=2^{(m,n)}-1$. 证毕.

➤**4.53 例 12** 设 $a>1,m,n>0$, 证明:$(a^m-1,a^n-1)=a^{(m,n)}-1$.

证明: 令 $d=(a^m-1,a^n-1)$, 考虑证明 $\left(a^{(m,n)}-1\right)\mid d$ 且 $d\mid\left(a^{(m,n)}-1\right)$ 来导出所证结论.

事实上, 因为

$$\left(a^{(m,n)}-1\right)\Big|\left(a^m-1\right),\quad\left(a^{(m,n)}-1\right)\Big|\left(a^n-1\right)$$

由推论 1.3.2 知

$$\left(a^{(m,n)}-1\right) \mid \left(\left(a^{m}-1\right),\left(a^{n}-1\right)\right)$$

即

$$\left(a^{(m,n)}-1\right) \mid d \tag{4.7}$$

又设 $d_1=(m,n)$, 因为 $m,n>0$, 故可选择正整数 x,y 使得

$$mx-ny=d_1 \tag{4.8}$$

由 $d \mid (a^m-1)$ 得 $d \mid (a^{mx}-1)$; 同理, 由 $d \mid (a^n-1)$, 得 $d \mid (a^{ny}-1)$. 故 $d \mid (a^{mx}-a^{ny})$.

由式(4.7)得

$$a^{mx}-a^{ny}=a^{ny+d_1}-a^{ny}=a^{ny}\left(a^{d_1}-1\right)$$

即

$$d \mid a^{ny}\left(a^{d_1}-1\right) \tag{4.9}$$

又因为 $a>1$ 及 $d \mid (a^m-1)$, 故 $(d,a)=1$, 进而

$$(d,a^{ny})=1$$

由上式及式(4.9)得 $d \mid \left(a^{d_1}-1\right)$, 即

$$d \mid \left(a^{(m,n)}-1\right) \tag{4.10}$$

结合式(4.7)和式(4.10)知 $(a^m-1,a^n-1)=a^{(m,n)}-1$. 证毕.

作业：	P11 习题 1.3、2;3;4　P17 习题 1.5、1;2
教学后记：	

第五讲　最小公倍数

教学目标：	掌握最小公倍数的概念、性质及其求法
教学重点：	最小公倍数的性质及其求法
教学难点：	最小公倍数的性质
教学方法和手段：	讲授
教学时数：	4 课时

一、最小公倍数的概念

$3 \mid 48, 6 \mid 48$, 可见,48 是 $3, 6$ 公有的倍数, 我们称之为 $3, 6$ 的一个公倍数.

➤**5.1 定义 1**　设 $a_k(k = 1, 2, \cdots, n)$,m 都是整数, 若 $a_k \mid m$, 则 m 叫作 $a_1, a_2, \cdots, a_n$ 的公倍数.

e.g.$\pm 6, \pm 12, \pm 24, \pm 48, \cdots$ 都是 $2, 3, 6$ 三个数的公倍数, 其中,6 是这些公倍数中最小的正整数, 叫作 $2, 3, 6$ 的最小公倍数, 记作 $[2, 3, 6] = 6$.

可见, 几个数的公倍数有无穷多个, 几个数的最小公倍数有且只有一个.

➤**5.2 定义 2**　几个非零整数 $a_1, a_2, \cdots, a_n$ 公有的倍数中最小的正整数, 叫作 $a_1, a_2, \cdots, a_n$ 的最小公倍数, 记作 $[a_1, a_2, \cdots, a_n]$.

➤**5.3 定理 1**　几个非零整数 $a_1, a_2, \cdots, a_n$ 的最小公倍数唯一存在.

证明: 存在性

显然,$a_1 a_2 \cdots a_n$ 是 $a_1, a_2, \cdots, a_n$ 的一个公倍数, 这说明 $a_1, a_2, \cdots, a_n$ 的公倍数存在. 根据最小数原理, 其正的公倍数中必存在最小正整数, 即存在最小公倍数.

唯一性

设 $[a_1, a_2, \cdots, a_n] = m, [a_1, a_2, \cdots, a_n] = q$.

若 $m < q$, 则与 $[a_1, a_2, \cdots, a_n] = q$ 矛盾;

若 $q > m$, 则与 $[a_1, a_2, \cdots, a_n] = m$ 矛盾.

故 $m = q$. 即 $a_1, a_2, \cdots, a_n$ 的最小公倍数唯一.

➤**5.4 定理 2**　若 $a_1, a_2, \cdots, a_n$ 均为非零整数, 则

$$[a_1, a_2, \cdots, a_n] = [|a_1|, |a_2|, \cdots, |a_n|].$$

该定理说明, 求几个非零整数的最小公倍数可化为求几个正整数的最小公倍数.

➤**5.5 定理 3** (i)$[a,1]=|a|,[a,a]=|a|$, 其中 $a\neq 0$;

(ii)$[a,b]=[b,a]$;

(iii) 若 $a\mid b$, 则 $[a,b]=|b|$.

二、最小公倍数的性质

➤**5.6 定理 4** [推论 1.4.3] 设 m 是 $a_1,a_2,\cdots,a_n$ 的一个公倍数,q 是 $a_1,a_2,\cdots,a_n$ 的任意一个公倍数, 则 $m=[a_1,a_2,\cdots,a_n]\Leftrightarrow m\mid q$.

证明: 必要性. 若 $m\nmid q$, 因为 $m=[a_1,a_2,\cdots,a_n]$, 所以 $m<q$. 设 $q=mx+r(\leqslant r<m)$. 因为 $a_k\mid m,a_k\mid q$, 所以 $a_k\mid(q-mx)=r(k=1,2,\cdots,n)$. 于是 r 也是 $a_1,a_2,\cdots,a_n$ 的一公倍数, 而 $r<m$, 这与 $m=[a_1,a_2,\cdots,a_n]$ 矛盾. 故 $m\mid q$

充分性. 设 $[a_1,a_2,\cdots,a_n]=p\neq m$. 因为 $m\mid q$,p 是 $a_1,a_2,\cdots,a_n$ 的公倍数, 所以 $m\mid p,m<p$, 这与 $[a_1,a_2,\cdots,a_n]=p$ 矛盾. 故 $p=m$.

➤**5.7 定理 5** 设 $a_p\mid m(p=1,2,\cdots,n)$, 则

$$m=[a_1,a_2,\cdots,a_n]\Leftrightarrow\left(\frac{m}{a_1},\frac{m}{a_2},\cdots,\frac{m}{a_2}\right)=1$$

证明: 必要性. 设 $\left(\frac{m}{a_1},\frac{m}{a_2},\cdots,\frac{m}{a_2}\right)=q>1$, 则 $q\mid\frac{m}{a_k}$. 所以 $qa_k\mid m$. 于是 $a_k\mid\frac{m}{q}$, 这说明 $\frac{m}{q}$ 是 a_k 的公倍数 $(p=1,2,\cdots,n)$. 而 $\frac{m}{q}<m$, 与 $m=[a_1,a_2,\cdots,a_n]$ 矛盾, 故

$$\left(\frac{m}{a_1},\frac{m}{a_2},\cdots,\frac{m}{a_2}\right)=1$$

充分性. 设 $[a_1,a_2,\cdots,a_n]=k<m$, 则由定理4可知,$k\mid m$. 设 $m=kq(q>1)$, 则由 $a_p\mid k(p=1,2,\cdots,n)$, 得 $a_p\mid\frac{m}{q}$, 于是 $q\mid\frac{m}{a_p}$, 则 q 是 $\frac{m}{a_k}(p=1,2,\cdots,n)$ 的大于 1 的公因数, 这与 $\left(\frac{m}{a_1},\frac{m}{a_2},\cdots,\frac{m}{a_2}\right)=1$ 矛盾. 故 $m=[a_1,a_2,\cdots,a_n]$.

➤**5.8 定理 6** [推论 1.4.2]$[ka_1,ka_2,\cdots,ka_n]=k[a_1,a_2,\cdots,a_n]$

➤**5.9 定理 7** [定理 1.4.2] 对任意正整数 a,b, 有 $[a,b]=\frac{ab}{(a,b)}$.

证明: 设 $[a,b]=m$, 由定理5得 $\left(\frac{m}{a},\frac{m}{b}\right)=1$, 故

$$\left(\frac{mb}{ab},\frac{ma}{ab}\right)=1,\left(\frac{b}{\frac{ab}{m}},\frac{a}{\frac{ab}{m}}\right)=1$$

由定理 1.3.4 得 $(a,b)=\dfrac{ab}{m}$, 从而 $m=\dfrac{ab}{(a,b)}$, 即

$$[a,b]=\frac{ab}{(a,b)}.$$

➤**5.10 注:** 两个非零整数的最小公倍数的问题实质上可化归为它们的最大公因数问题.

➤**5.11 推论 1** [推论 1.4.1] 若 $a\mid m, b\mid m$, 则 $[a,b]\mid m$.

➤**5.12** 推论1刻画了最小公倍数的一个重要属性: 两个非零整数的最小公倍数不但是最小的公倍数, 而且是这两个整数的任意公倍数的因数.

➤**5.13 推论 2** [推论 1.4.2] 设 m,a,b 是正整数, 则 $[ma.mb]=m[a,b]$.

证明: 由定理 1.4.2 及定理 1.3.4 得到

$$[ma,mb]=\frac{m^2ab}{(ma,mb)}=\frac{m^2ab}{m(a,b)}=\frac{mab}{(a,b)}=m[a,b].$$

➤**5.14 推论 3** 若 $(a,b)=1$, 则 $[a,b]=(a,b)$.

➤**5.15 推论 4** $[a^n,b^n]=[a,b]^n$.

证明: $[a^n,b^n]=\dfrac{a^nb^n}{(a^n,b^n)}=\dfrac{a^nb^n}{(a,b)^n}=\left(\dfrac{ab}{(a,b)}\right)^n=[a,b]^n$.

➤**5.16 推论 5** 若 $(a,b)=1$, 则 $[a,bc]=b[a,c]$.

➤**5.17 定理 8** [定理 1.4.3] 对于任意 n 个非负整数 $a_1,a_2,\cdots,a_n$, 记

$$[a_1,a_2]=m_2,[m_2,a_3]=m_3,\cdots,[m_{n-2},a_{n-1}]=m_{n-1},[m_{n-1},a_n]=m_n$$

则 $[a_1,a_2,\cdots,a_n]=m_n$.

证明: 由于

$$m_n=[m_{n-1},a_n]\Rightarrow m_{n-1}\,|m_n,a_n|\,m_n$$

$$m_{n-1}=[m_{n-2},a_{n-1}]\Rightarrow m_{n-2}\,|m_{n-1}|\,m_n,a_n\,|m_n,a_{n-1}|\,m_{n-1}\mid m_n$$

$$m_{n-2}=[m_{n-3},a_{n-2}]\Rightarrow m_{n-3}\,|m_{n-2}|\,m_n,a_n\,|m_n,a_{n-1}|\,m_n,a_{n-2}\mid m_n$$

$$\cdots$$

$$m_2=[a_1,a_2]\Rightarrow a_n\,|m_n,\cdots,a_2|\,m_n,a_1\mid m_n$$

因此,m_n 是 $a_1,a_2,\cdots,a_n$ 的一个公倍数.

又对于 $a_1,a_2,\cdots,a_n$ 的任何公倍数 m, 反复利用推论 1.4 .1 及 $m_2,\cdots,m_n$ 的定义, 得

$$m_2\,|m,m_3|\,m,\cdots,m_n\mid m$$

所以 $m_n \leqslant m$, 即 m_n 是 $a_1, a_2, \cdots, a_n$ 最小的正的公倍数.

➤5.18 定理 9 [定理 1.4.4] 对于任意非零整数 $a_1, a_2, \cdots, a_n$ 及整数 $k(1 \leqslant k \leqslant n)$. 证明:

$$[a_1, a_2, \cdots, a_n] = [[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]].$$

证明: 因为 $[a_1, a_2, \cdots, a_n]$ 是 $a_1, \cdots, a_k$ 和 $a_{k+1}, \cdots, a_n$ 的公倍数, 所以

$$[a_1, \cdots, a_k] \mid [a_1, a_2, \cdots, a_n]$$

且 $[a_{k+1}, \cdots, a_n] \mid [a_1, a_2, \cdots, a_n]$ 因此, 由推论 1. 4.3 得

$$[[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]] \mid [a_1, a_2, \cdots, a_n] \tag{5.1}$$

又对于任意的 $a_i(1 \leqslant i \leqslant n)$, 显然

$$a_i \mid [[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]]$$

所以, 由推论 1.4 .3 可知

$$[a_1, a_2, \cdots, a_n] \mid [[a_1, \cdots, a_k], [a_{k+1}, \cdots, a_n]]$$

综合上式及式(5.1), 定理得证.

e.g. $[4, 8, 12] = [[4, 8], 12] = [8, 12] = 24.$

$[2, 4, 9, 8, 27] = [[2, 4, 8], [9, 27]] = [8, 27] = 216.$

➤5.19 定理 10 若 $(h, a_m = 1)(m = k+1, k+2, \cdots, n)$, 则

$$[ha_1, ha_2, \cdots, ha_k, a_{k+1}, \cdots, a_n] = h[a_1, a_2, \cdots, a_k, a_{k+1}, \cdots, a_n]$$

证明: 因为 $(h, a_m = 1)(m = k+1, k+2, \cdots, n)$, 所以 $(h, a_{k+1} \cdots a_n) = 1$. 于是 $a_{k+1} \cdots a_n$ 是 $a_{k+1}, \cdots, a_n$ 的公倍数, 所以 $[a_{k+1}, \cdots, a_n] \mid a_{k+1} \cdots a_n$, 故 $(h, [a_{k+1}, \cdots, a_n]) = 1$. 又由 5.8 定理和 5.18 定理可知,

$$\begin{aligned}
&[ha_1, ha_2, \cdots, ha_k, a_{k+1}, \cdots, a_n] \\
=&[[ha_1, ha_2, \cdots, ha_k], [a_{k+1}, \cdots, a_n]] \\
=&[h[a_1, a_2, \cdots, a_k], [a_{k+1}, \cdots, a_n]] \\
=&h[[a_1, a_2, \cdots, a_k], [a_{k+1}, \cdots, a_n]] \\
=&h[a_1, a_2, \cdots, a_k, a_{k+1}, \cdots, a_n].
\end{aligned}$$

e.g. $[2, 4, 12, 9, 17, 18]$

$$\begin{aligned}
&=2 \times [1, 2, 6, 9, 17, 9] \\
&=2 \times 2 \times [1, 1, 3, 9, 17, 9] \\
&=4 \times 3 \times [1, 1, 1, 3, 17, 3] \\
&=12 \times 3 \times [1, 1, 1, 1, 17, 1] \\
&=36 \times 17 = 612.
\end{aligned}$$

➤**5.20 例 1** 设 a,b,c 是正整数, 证明 : $[a,b,c](ab,bc,ca)=abc$.

证明: 由定理 1.4 .3 和定理 1.4 .2, 有

$$[a,b,c]=[[a,b],c]=\frac{[a,b]c}{([a,b],c)} \tag{5.2}$$

由推论 1.4.2 及定理 1.3. 4, 有

$$\begin{aligned}(ab,bc,ca)=&(ab,(bc,ca))=(ab,c(a,b))=\\&\left(ab,\frac{abc}{[a,b]}\right)=\frac{(ab[a,b],abc)}{[a,b]}=\frac{ab([a,b],c)}{[a,b]}\end{aligned} \tag{5.3}$$

综合式(5.2)与式(5.3)得到所证结论.

➤**5.21 例 2** 设 a,b,c 是正整数, 证明:$[a,b,c][ab,bc,ca]=[a,b][b,c][c,a]$.

证明: 由推论 1.4.2, 有

$$\begin{aligned}[a,b,c][ab,bc,ca]=&[[a,b,c]ab,[a,b,c]bc,[a,b,c]ca]=\\&\left[\left[a^2b,ab^2,abc\right],\left[abc,b^2c,bc^2\right],\left[a^2c,abc,ac^2\right]\right]=\\&\left[a^2b,ab^2,abc,abc,b^2c,bc^2,a^2c,abc,ac^2\right]=\\&\left[abc,a^2b,a^2c,b^2c,b^2a,c^2a,c^2b\right]\end{aligned}$$

以及

$$\begin{aligned}[a,b][b,c][c,a]=&[[a,b]b,[a,b]c][c,a]=\left[ab,b^2,ac,bc\right][c,a]=\\&\left[ab[c,a],b^2[c,a],ac[c,a],bc[c,a]\right]=\\&\left[abc,a^2b,b^2c,b^2a,ac^2,a^2c,bc^2,bca\right]=\\&\left[abc,a^2b,a^2c,b^2c,b^2a,c^2a,c^2b\right]\end{aligned}$$

综上即得结论.

三、最小公倍数的求法

根据最小公倍数的定义和性质, 对照最大公因数的求法, 可以得到几个求最小公倍数的方法.

(1) 分解质因数法.

根据定义和定理 3 可知, 几个数的最小公倍数首先是这几个数的一个公倍数, 其次, 它又是这几个数的任意公倍数的因数. 由此可以得到求几个数最小公倍数的分解质因数法, 其步骤如下:

1. 写出各数的标准分解式;
2. 写出各分解式中所有的质因数及其最高次数, 并把得到的幂连乘起来.

➤**5.22 例 3** 求 $[735, 108, 24]$.

解: 因为 $735 = 3 \times 5 \times 7^2, 108 = 2^2 \times 3^3, 24 = 2^3 \times 3$, 所以

$$[735, 108, 24] = 2^3 \times 3^3 \times 5 \times 7^2 = 52920$$

(2) 提取公因数法.

根据定理 5、定理 6 推论和定理 8, 求几个数的最小公倍数可以用提取公因数法, 其步骤如下:

1. 先提取这几个数的最大公因数 (各商数互质但不一定两两互质) ;
2. 在不互质的商数中提取公因数, 其他商数照写下来, 直到各商数两两互质为止;
3. 把提取的各数及各商数连乘起来.

➤**5.23 例 4** 求 $[62, 48, 378]$.

解:

$$\begin{aligned}[62, 48, 378] &= 2 \times [31, 24, 189] = 2 \times 3 \times [31, 8, 63] \\ &= 6 \times 31 \times 8 \times 63 = 93744\end{aligned}$$

这一过程通常简写成下面的形式, 叫作短除式:

2	62	48	378
3	31	24	189
	31	8	63

因为 $31, 8, 63$ 两两互质, 所以 $[62, 48, 378] = 2 \times 3 \times 31 \times 8 \times 63 = 93744$.

(3) 先求最大公因数法.

根据定理 6 , 通过 $[a, b](a, b) = ab$, 先求 (a, b).

此法一般用于求公因数不明显的几个数的最小公倍数.

➤**5.24 例 5** 求 $[24871, 3468]$.

解: 由辗转相除法求得 $(24871, 3468) = 17$, 从而

$$[24871, 3468] = 24871 \times 3468 \div 17 = 5073684.$$

作业:	P11 习题 1.3、2;3;4　P17 习题 1.5、1;2
教学后记:	

第六讲　素数与合数

教学目标：	掌握素数与合数的概念及素数的判定
教学重点：	素数与合数的概念
教学难点：	素数的判定质
教学方法和手段：	讲授
教学时数：	2 课时

一、素数与合数的概念

➤**6.1 定义 1**　若 a 为大于 1 的整数, 如果 a 的正因数只有 1 和 a 自身, 则称 a 为素数 (或质数). 若 a 有正的真因数, 则称 a 为合数.

➤**6.2 e.g.** $2,3,5,7,11,\cdots$ 都是质数;$4,6,8,9,10,\cdots$ 都是合数.

➤**6.3 注**　全体正整数被分成三类: 数 1(单独作一类)、素数和合数.

➤**6.4 定理 1** a 是合数的充要条件是 $a=bc$, 其中 $b,c\in\mathbb{N}_+, 1<b<a, 1<c<a$.

证明: (充分性证明) 因为 $a=bc, b,c\in\mathbb{N}_+, 1<b<a, 1<c<a$

所以 $a>1$, 则 a 的合数.

(必要性证明) 因为 a 是合数, 所以一定有一个 $b\in\mathbb{N}_+$ 且 $1<b<a$, 使 $b\mid a$, 即 $a=bc$. 又由于 $a,b\in\mathbb{N}_+$, 故 $c\in\mathbb{N}_+$. 因为 $a>b$, 所以 $bc>b$, 又因为 $b>1$, 所以 $c>1$.

由于 $c\mid a, c, a\in\mathbb{N}_+$, 故 $c<a$, 则 $1<c<a$.

结论成立.

➤**6.5 例 1**　求证:$173^{12}+4$ 是合数.

证明: 只要找到一个不是 1 也不是它本身的正因数即可, 可考虑试用配方法把它分解因式.

$$\begin{aligned}\because 173^{12}+4&=\left(173^6\right)^2+2^2\\&=\left(173^6+2\right)^2-4\times173^6\\&=\left(173^6+2\right)^2-\left(2\times173^3\right)^2\\&=\left(173^6+2\times173^3+2\right)\left(173^6-2\times173^3+2\right),\end{aligned}$$

$\therefore 173^{12}+4$ 是合数.

➤**6.6 定理 2**　如果素数 p 是整数 a 的因数, 则称 p 是 a 的素因数.

素数在正整数中特别重要, 一般常用字母 p 表示素数.

二、素数的判定

➤6.7 定理 3 任何大于 1 的正整数必有一个素因数.

证明: 设 a 是大于 1 的正整数, 由于 a 就是自身的因数, 所以 a 必有大于 1 的因数. 若 a 是素数, 则定理 1.6.1 成立是显然的. 若 a 不是素数, 则它有正的真因数, 设它们是 $d_1, d_2, \cdots, d_k\,(d_i > 1; i = 1, 2, \cdots, k)$, 令 d 是其中最小的, 若 d 不是素数, 则存在 $1 < e_1, e_2 < d$ 使得 $d = e_1 \cdot e_2$, 因此 e_1 和 e_2 也是 a 的正的真因数, 这与 d 的最小性矛盾. 所以 d 是素数, 因而 a 必有一个素因数. 证毕.

➤6.8 推论 1 [推论 1.6.1]如果 a 是大于 1 的整数, 则 a 的大于 1 的最小因数必为素数.

➤6.9 推论 2 [推论 1.6.2]合数 a 的最小素因数 p 满足 $p \leqslant \sqrt{a}$.

证明: 由于 a 是合数, 于是有 $a = p \cdot q$, 其中 p 是 a 的最小素因数,$q \in \mathbb{N}$, 由于 $1 < p \leqslant q < a$, 从而 $p^2 \leqslant a$, 即 $p \leqslant \sqrt{a}$. 证毕.

➤6.10 推论 3 [推论 1.6.3]若大于 1 的整数 a 不能被任何适合 $p \leqslant \sqrt{a}$ 的素数 p 整除, 则 a 必为素数.

证明: 反证法. 若不然, 由于 $a > 1$, 则 a 必为合数, 由推论 1.6.2 知,a 的最小素因数 p 满足 $p \leqslant \sqrt{a}$, 这与 a 不能被任何适合 $p \leqslant \sqrt{a}$ 的素数 p 整除矛盾, 故 a 必为素数. 证毕.

➤6.11 注 根据推论 1.6.3 可得出求“不超过某个正整数 a 的所有素数”的方法

➤6.12 定理 4 [定理 1.6.2]设 p 为素数,a 是任意一个整数, 则或者 p 整除 a, 或者 p 与 a 互素.

证明: 事实上,p 与 a 的最大公约数 (p, a) 必整除 p. 由于 p 为素数, 故 $(p, a) = 1$ 或者 $(p, a) = p$, 即 p 与 a 互素或者 p 整除 a. 证毕.

➤6.13 定理 5 [定理 1.6.3]设 p 为素数,a, b 为整数, 若 $p \mid ab$, 则 a, b 中至少有一个数被 p 整除.

证明: 反证法. 若 a, b 均不能被 p 整除, 则由定理 1.6.2 知,p 与 a, b 都互素, 从而 p 与 ab 互素. 这与 $p \mid ab$ 矛盾. 故 a, b 中至少有一个数被 p 整除. 证毕.

特别地, 若 p 为素数, 且 $p \mid a^n (n \geqslant 1)$, 则 $p \mid a$.

➤6.14 例 2 求出不超过 30 的所有素数.

解: 先将不超过 30 的正整数排列如下:

~~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~~

再按以下步骤进行:

① 删去 1, 剩下的后面的第一个数是 2,2 是素数;

② 删去 2 后面的被 2 整除的数, 剩下的 2 后面的第一个数是 3,3 是素数;

③ 再删去 3 后面的被 3 整除的数, 剩下的 3 后面的第一个数是 5,5 是素数;

④ 再删去 5 后面的被 5 整除的数, 剩下的 5 后面的第一个数是 7,7 是素数;

按照以上步骤依次得到不超过 30 的素数:$2,3,5,7,11,13,17,19,23,29$.

➤6.15 注 上述方法的理论依据是: 由推论 1.6.3 可知, 不超过 30 的合数必有一个不超过 $\sqrt{30}\leqslant 6$ 的素因数, 而不超过 6 的素数只有 $2,3,5$, 因此在删除了所有能被 $2,3,5$ 整除的数之后剩下的数必为素数, 这样就得到了不超过 30 的全部素数.

此种寻找素数的方法称为 **Eratosthenes 筛法**.

➤6.16 例 3 判定 173 和 1957 是质数还是合数.

解: (1) 因为 $13<\sqrt{173}<14$, 所以用不超过 13 的质数 $2,3,5,7,11,13$ 依次去除 173, 发现都不能整除, 所以 173 是质数.

(2) 因为 $44<\sqrt{1957}<45$, 所以用不超过 13 的质数从小到大依次去除 1957, 发现都不能整除, 所以 1957 是质数.

➤6.17 例 4 判定 359 是质数还是合数.

解: 因为 $18<\sqrt{359}<19$, 所以用不超过 $\sqrt{359}$ 的质数 $2,3,5,7,11,13,17$ 依次去除 359, 发现都不能整除, 所以 359 是质数.

➤6.18 例 5 证明: 素数有无穷多个.

证明: 证法一反证法. 假设素数只有有限多个, 设这有限个素数为 $p_1,p_2,\cdots,p_k$. 考虑数 $a=p_1p_2\cdots p_k+1$, 显然 $a>1$, 故 a 有素因数 p. 因为 $p_1,p_2,\cdots,p_k$ 包含了全部的素数, 故 p 必等于某个 $p_i(1\leqslant i\leqslant k)$, 从而 $p\mid p_1p_2\cdots p_k$, 于是由 $p\mid a$ 推得 $p\mid 1$, 从而 $p=1$ 或 $p=-1$, 这与 p 是素数矛盾. 因此, 素数有无穷多个.

证法二由于每个费马数 $F_n=2^{2^n}+1(n=0,1,2,\cdots)$ 都大于 1, 故它至少有一个素因数. 由 1.3 节例 2 知, 任意两个费马数 $(F_m,F_n)=1(m\neq n)$, 因此, 这些素因数必定是互不相同的. 由于两两互素的费马数有无限多个, 故素数有无穷多个. 证毕.

➤6.19 例 6 证明: 存在无穷多个正整数 a, 使得 $n^4+a(n=1,2,3,\cdots)$ 都是合数.

证明: 令 $a=4k^4(k=2,3,\cdots)$, 则对任意的 $n\in\mathbb{N}$, 有

$$n^4+4k^4=\left(n^2+2k^2\right)^2-4n^2k^2=\left(n^2+2k^2+2nk\right)\cdot\left(n^2+2k^2-2nk\right)$$

因为 $n^2+2k^2-2nk=(n-k)^2+k^2\geqslant k^2>1$

所以, 对于任意的 $k=2,3,\cdots$ 以及任意的 $n\in\mathbf{N}, n^4+a$ 都是合数.

➤6.20 例 7 若 $a>1, a^n-1$ 是素数, 证明:$a=2$, 并且 n 是素数.

证明: 若 $a>2$, 则由

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

可知 a^n-1 是合数. 所以 $a=2$.

若 n 是合数, 则 $n=xy(x>1,y>1)$, 于是由

$$2^{xy}-1=(2^x-1)\left(2^{x(y-1)}+2^{x(y-2)}+\cdots+1\right)$$

以及 $2^x-1>1$ 可知 2^n-1 是合数. 所以当 2^n-1 是素数时,n 必是素数.

作业:	P20 习题 1.6、1;2
教学后记:	

第七讲　算术基本定理

教学目标：	了解算术基本定理
教学重点：	算术基本定理
教学难点：	算术基本定理
教学方法和手段：	讲授
教学时数：	2 课时

➤7.1 引理 1　任何大于 1 的正整数 n 都可表示成素数之积, 即

$$n = p_1 p_2 \cdots p_m \tag{7.1}$$

其中 $p_i (1 \leqslant i \leqslant m)$ 是素数.

证明: 对正整数 n 进行归纳. 当 $n = 2$ 时, 式(7.1)显然成立.

假设式(7.1)对任意小于 n 的正整数都成立, 现在考虑 n, 如果 n 是素数, 则式(7.1)显然成立.

如果 n 是合数, 则 n 有正的真因数 a, b 使得 $n = a \cdot b (1 < a, b < n)$, 根据归纳假设知,$a, b$ 均可以分解为有限个素数之积, 从而 n 也可以分解为有限个素数之积.

由归纳法原理, 对一切大于 1 的正整数 n 都能分解成式(7.1)的形式. 证毕.

➤7.2 定理 1 (算术基本定理) 任何大于 1 的正整数 n 都可唯一表示成

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{7.2}$$

其中,$p_1, p_2, \cdots, p_k$ 是素数,$p_1 < p_2 < \cdots < p_k$, 且 $\alpha_1, \alpha_2, \cdots, \alpha_k$ 是正整数.

证明: 存在性　由上述引理可知, 任何大于 1 的正整数 n 都可分解成式(7.1)的形式, 即

$$n = p_1 p_2 \cdots p_m$$

其中 $p_i (1 \leqslant i \leqslant m)$ 是素数. 适当调整分解式(7.1)中素数的顺序, 并将式(7.1)中相同素因数的乘积写成该素数的方幂的乘积, 则 n 可表示成

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{\alpha_k}$$

其中 $p_1 < p_2 < \cdots < p_k$, 且 $\alpha_1, \alpha_2, \cdots, \alpha_k$ 是正整数.

唯一性　假设 $p_i (1 \leqslant i \leqslant k)$ 与 $q_j (1 \leqslant j \leqslant l)$ 都是素数, 且

$$p_1 \leqslant p_2 \leqslant \cdots \leqslant p_k, \quad q_1 \leqslant q_2 \leqslant \cdots \leqslant q_l \tag{7.3}$$

并且

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l \tag{7.4}$$

则由定理 1.6.3 知, 必有某个 $q_j (1 \leqslant j \leqslant l)$, 使得 $p_1 \mid q_j$, 由于 p_1 和 q_j 都是素数, 所以 $p_1 = q_j$; 同理, 必有某个 $p_i (1 \leqslant i \leqslant k)$, 使得 $q_1 \mid p_i$, 所以 $q_1 = p_i$. 于是, 结合式 (7.3)可知

$$q_j = p_1 \leqslant p_i = q_1 \leqslant q_j = p_1$$

故 $p_1 = q_1$, 从而由式(7.4)得到

$$p_2 \cdots p_k = q_2 \cdots q_l$$

反复进行上述操作, 最后必有 $k = l, p_i = q_i (1 \leqslant i \leqslant k)$, 即唯一性得证.

证毕.

➤7.3 定义 1 正整数 n 的分解式 $n = p_1^{a_1} p_2^{a_2} \cdots p_{k^k}^{a_k}$ 称为 n 的标准分解式, 其中 $p_1, p_2, \cdots, p_k$ 是素数,$p_1 < p_2 < \cdots < p_k$, 且 $\alpha_1, \alpha_2, \cdots, \alpha_k$ 是正整数.

➤7.4 注 算术基本定理又称为**唯一分解定理**.

➤7.5 推论 1 [推论 1.7.1]设 n 的标准分解式为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{a_k}$, 则:

(i) n 的任一正约数 d 具有形式 $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ $(\gamma_i \in \mathbf{Z}, 0 \leqslant \gamma_i \leqslant \alpha_i, 1 \leqslant i \leqslant k)$;

(ii) n 的正倍数 m 具有形式 $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} M$ $(M \in \mathbf{N}, \beta_i \in \mathbf{N}, \beta_i \geqslant \alpha_i, 1 \leqslant i \leqslant k)$.

➤7.6 推论 2 [推论 1.7.2]若正整数 a 与 b 的分解式分别为 $a = p_1^{a_1} p_2^{\alpha_2} \cdots p_k^{a_k}, b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, 其中 $p_1, p_2, \cdots, p_k$ 是互不相同的素数,$\alpha_i, \beta_i (1 \leqslant i \leqslant k)$ 是非负整数, 则

$$(a, b) = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_k^{\lambda_k}, \quad \lambda_i = \min\{\alpha_i, \beta_i\} (1 \leqslant i \leqslant k)$$
$$[a, b] = p_1^{\mu_1} p_2^{\mu_2} \cdots p_k^{\mu_k}, \quad \mu_i = \max\{\alpha_i, \beta_i\} (1 \leqslant i \leqslant k)$$

➤7.7 例 1 若 n 的标准分解式为 $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, 设 $d(n)$ 为 n 的正因数的个数,$\sigma(n)$ 为 n 的所有正因数之和, 则有

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) \tag{7.5}$$

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \cdots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1} \tag{7.6}$$

若 $(a, b) = 1$, 则有

$$d(ab) = d(a) d(b) \tag{7.7}$$

$$\sigma(ab) = \sigma(a)\sigma(b) \tag{7.8}$$

证明: 当 $n > 1$ 时, 利用推论 1.7.1 容易推出式(7.5)成立. 当 $n = 1$ 时, 由于 $d(1) = 1$, 则式(7.5)也成立, 此即为 $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$ 的情形. 为了证明式(7.6), 仍然利用推论 1.7.1, 有

$$\alpha(n) = \sum_{\substack{0\leqslant\beta_i\leqslant a_i \\ 1\leqslant i\leqslant k}} p_1^{\beta_1}\cdots p_{k^k}^{\beta_k} = \sum_{\beta_1=0}^{a_1} p_1^{\beta_1}\cdot\left(\sum_{0\leqslant\beta_i\leqslant a_i} p_2^{\beta_2}\cdots p_k^{\beta_k}\right) = \cdots =$$

$$\left(\sum_{\beta_1=0}^{a_1} p_1^{\beta_1}\right)\cdots\left(\sum_{\beta_k=0}^{a_k} p_k^{\beta_k}\right) = \frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdot\cdots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

由于两整数互素, 这就意味着它们的标准分解式中没有相同的素因子; 反之亦然. 因此, 当 $(a, b) = 1$ 时, 式(7.7)和式(7.8)分别是式(7.5)和式(7.6)的直接推论. 证毕.

作业：	
教学后记：	

第八讲　函数 $[x]$ 与 $\{x\}$ 及 $n!$ 的标准分解式

教学目标：	了解算术基本定理
教学重点：	算术基本定理
教学难点：	算术基本定理
教学方法和手段：	讲授
教学时数：	2 课时

➤**8.1 定义 1**　设 x 是实数, 以 $[x]$ 表示不超过 x 的最大整数, 称 $[x]$ 为 x 的**整数部分**, 称 $\{x\}=x-[x]$ 为 x 的**小数部分**.

➤**8.2**　如 : $[\pi]=3,[-\pi]=-4,\left[\dfrac{1}{3}\right]=0,\left\{-\dfrac{1}{5}\right\}=\dfrac{4}{5}$.

➤**8.3 定理 1**　设 x 与 y 是实数, 则:

(i) $0\leqslant\{x\}<1, x-1<[x]\leqslant x<[x]+1$

(ii) $x\leqslant y\Rightarrow[x]\leqslant[y]$;

(iii) 若 m 是整数, 则 $[m+x]=m+[x],\{m+x\}=\{x\}$;

(iv) $[x+y]=\begin{cases}[x]+[y], & 若\{x\}+\{y\}<1\\ [x]+[y]+1, & 若\{x\}+\{y\}\geqslant 1\end{cases}$, 即 $[x]+[y]\leqslant[x+y]\leqslant[x]+[y]+1$, 其中等号不能同时成立.

(v) $\begin{cases}-[x], & 若x\in\mathbb{Z}\\ -[x]-1, & 若x\notin\mathbb{Z}\end{cases}$,

证明: (i),(ii),(iii) 可由定义直接推出.

(iv) 由于 $[x+y]=[[x]+\{x\}+[y]+\{y\}]=[x]+[y]+[\{x\}+\{y\}]$, 若 $\{x\}+\{y\}<1$, 则 $[\{x\}+\{y\}]=0$, 故 $[x+y]=[x]+[y]$; 若 $\{x\}+\{y\}\geqslant 1$, 则 $[\{x\}+\{y\}]=1$, 故 $[x+y]=[x]+[y]+1$. 由此 (iv) 成立.

(v) 因为 $[-x]=[-([x]+\{x\})]=-[x]+[-\{x\}]$, 由于 $0\leqslant\{x\}<1$, 因而 $-1<-\{x\}\leqslant 0$. 若 $x\in\mathbb{Z}$, 则 $[-\{x\}]=0$; 若 $x\notin\mathbb{Z}$, 则 $[-\{x\}]=-1$. 证毕.

➤**8.4 定理 2**　设 a 与 b 是正整数, 则在 $1,2,\cdots,a$ 中能被 b 整除的整数有 $\left[\dfrac{a}{b}\right]$ 个.

证明: 能被 b 整除的正整数是 $b,2b,3b,\cdots$, 因此, 若数 $1,2,\cdots,a$ 中能被 b 整除的整数 k 个, 则 $kb\leqslant a<(k+1)b\Rightarrow k\leqslant\frac{a}{b}<k+1\Rightarrow k=\left[\dfrac{a}{b}\right]$. 证毕.

➤**8.5**　由定理 1.8.2 可知, 若 b 是正整数, 那么对于任意整数 a, 有

$$a=b\cdot\left[\frac{a}{b}\right]+b\cdot\left\{\frac{a}{b}\right\}$$

即在带余数除法 $a=bq+r(0\leqslant r<b)$ 中有 $q=\left[\frac{a}{b}\right], r=b\left\{\frac{a}{b}\right\}$.

➤8.6 定理 3 设 n 是正整数,$n!$ 的标准分解式为 $n!=p_1^{\alpha_1}p_1^{a_2}\cdots p_k^{a_k}$, 则素因数 p_i 的指数为

$$\alpha_i=\sum_{r=1}^{\infty}\left[\frac{n}{p_i^r}\right] \tag{8.1}$$

证明: 对于任意固定的素数 p, 以 $p(k)$ 表示在 k 的标准分解式中 p 的指数, 则

$$p(n!)=p(1)+p(2)+\cdots+p(n)$$

以 n_j 表示 $p(1),p(2),\cdots,p(n)$ 中素数 p 的指数等于 j 的数的个数, 则

$$p(n!)=1\cdot n_1+2\cdot n_2+3\cdot n_3+\cdots \tag{8.2}$$

显然,n_3 就是在 $1,2,\cdots,n$ 中满足 $p^j\mid a$ 且 $p^{j+1}\rangle a$ 的整数 a 的个数, 所以, 由定理 1.8 .2 有

$$n_j=\left[\frac{n}{p^j}\right]-\left[\frac{n}{p^{j+1}}\right]$$

将上式代入式(8.2), 得到

$$\begin{aligned}p(n!)&=1\cdot\left(\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]\right)+2\cdot\left(\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]\right)+3\cdot\left(\left[\frac{n}{p^3}\right]-\left[\frac{n}{p^4}\right]\right)+\cdots\\&=\sum_{r=1}^{\infty}\left[\frac{n}{p^r}\right]\end{aligned}$$

证毕.

➤8.7 推论 1 设 n 是正整数, 则 $n!=\prod\limits_{p\leqslant n}p^{\sum\limits_{r=1}^{\infty}\left[\frac{n}{p^r}\right]}$, 其中 $\prod\limits_{p\leqslant n}$ 表示对不超过 n 的所有素数 p 求积.

➤8.8 定理 4 [定理 1.8.4]设 n 是正整数,$1\leqslant k\leqslant n-1$, 则

$$\mathrm{C}_n^k=\frac{n!}{k!(n-k)!}\in\mathbf{N} \tag{8.3}$$

若 n 是素数, 则 $n\mid\mathrm{C}_n^k(1\leqslant k\leqslant n-1)$.

证明: 由定理 1.8.3, 对于任意素数 p, 整数 $n!,k!$ 与 $(n-k)!$ 的标准分解式中所含的素因数 p 的指数分别是

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

利用定理 1.8.1 的性质 (iv) 可知

$$\left[\frac{k+(n-k)}{p^r}\right]=\left[\frac{n}{p^r}\right]\geqslant\left[\frac{k}{p^r}\right]+\left[\frac{n-k}{p^r}\right]$$

故 $\sum\limits_{r=1}^{\infty}\left[\dfrac{n}{p^r}\right]\geqslant\sum\limits_{r=1}^{\infty}\left[\dfrac{k}{p^r}\right]+\sum\limits_{r=1}^{\infty}\left[\dfrac{n-k}{p^r}\right]$

因此,C_n^k 是整数.

若 n 是素数, 则对于 $1\leqslant k\leqslant n-1$, 有 $(n,k!)=1,(n,(n-k)!)=1\Rightarrow(n,k!(n-k)!)=1$, 由此及

$$\mathrm{C}_n^k=\frac{n\cdot(n-1)!}{k!(n-k)!}\in\mathbb{N}$$

推出 $k!(n-k)!\mid(n-1)!$, 从而 $n\mid\mathrm{C}_n^k$. 证毕.

➤8.9 例 1 设 x 与 y 是实数, 证明:

$$[2x]+[2y]\geqslant[x]+[x+y]+[y]\tag{8.4}$$

解: 设 $x=[x]+\alpha(0\leqslant\alpha<1),y=[y]+\beta(0\leqslant\beta<1)$, 则

$$[x]+[x+y]+[y]=2[x]+2[y]+[\alpha+\beta]\tag{8.5}$$

及

$$[2x]+[2y]=2[x]+2[y]+[2\alpha]+[2\beta]\tag{8.6}$$

如果 $[\alpha+\beta]=0$, 那么显然有 $[\alpha+\beta]\leqslant[2\alpha]+[2\beta]$.

如果 $[\alpha+\beta]=1$, 那么 α 与 β 中至少有一个不小于 $\dfrac{1}{2}$, 于是

$$[2\alpha]+[2\beta]\geqslant1=[\alpha+\beta]$$

因此, 无论 $[\alpha+\beta]=0$ 或 1, 都有 $[\alpha+\beta]\leqslant[2\alpha]+[2\beta]$, 由此及式(8.5)和式(8.6)可推出式(8.4).

➤8.10 例 2 设 n 是正整数,x 是任一实数, 证明:

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx]\tag{8.7}$$

解: 设 $x=[x]+\alpha(0\leqslant\alpha<1)$, 则有

$$\begin{aligned}&[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]\\=&[[x]+\alpha]+\left[[x]+\alpha+\frac{1}{n}\right]+\cdots+\left[[x]+\alpha+\frac{n-1}{n}\right]\\=&n[x]+[\alpha]+\left[a+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]\end{aligned}$$

又 $[nx]=[n([x]+\alpha)]=n[x]+[n\alpha]$

故只须证明

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha]\quad(0\leqslant\alpha<1)\tag{8.8}$$

事实上, 若 $0 \leqslant \alpha < \dfrac{1}{n}$, 则 $[\alpha] + \left[\alpha + \dfrac{1}{n}\right] + \cdots + \left[\alpha + \dfrac{n-1}{n}\right] = 0 = [n\alpha]$.

若 $\dfrac{i}{n} \leqslant \alpha < \dfrac{i+1}{n} (1 \leqslant i \leqslant n-1)$, 则

① 当 $1 \leqslant i \leqslant n-i-1$ 时, 恒有 $\left[a + \frac{i}{n}\right] = 0$;

② 当 $n-i \leqslant i \leqslant n-1$ 时, 恒有 $\left[\alpha + \frac{i}{n}\right] = 1$.

故 $[\alpha] + \left[\alpha + \dfrac{1}{n}\right] + \cdots + \left[\alpha + \dfrac{n-1}{n}\right] = i = [n\alpha]$. 因而, 恒有式(8.8)成立.

由式(8.8)可知式(8.7)成立. 证毕.

作业：	
教学后记：	

第九讲　同余的基本性质

教学目标：	掌握同余的概念与基本性质
教学重点：	同余的基本性质
教学难点：	同余的基本性质
教学方法和手段：	讲授
教学时数：	4 课时

一、同余的概念

➤**9.1 e.g.** 今天星期六, 从今天起第 36 天和第 43 天分别是星期几?

36 和 43 除以 7 的余数即可, 余数都是 1, 所以答案都是星期日.

➤**9.2 定义 1** 设 m 是给定的正整数,a, b 是任意整数, 如果整数 $m \mid (a-b)$, 则称 a 与 b 关于模 m 同余, 记为

$$a \equiv b(\mathrm{mod}\ m)$$

如果整数 $m \nmid (a-b)$, 则称 a 与 b 关于模 m 不同余, 记为 $a \not\equiv b(\mathrm{mod}\ m)$.

显然 $a \equiv 0(\mathrm{mod}\ m) \Leftrightarrow m \mid a$.

➤**9.3 定理 1** a 与 b 关于模 m 同余的充分必要条件是,a 和 b 被 m 除后所得的最小非负余数相等, 即若 $a = q_1 m + r_1\,(0 \leqslant r_1 < m), b = q_2 m + r_2\,(0 \leqslant r_2 < m)$, 则 $a \equiv b(\mathrm{mod} m) \Leftrightarrow r_1 = r_2$.

证明: 由题设有 $a - b = (q_1 - q_2)\,m + (r_1 - r_2)$, 因此 $m \mid (a-b)$ 的充分必要条件是 $m \mid (r_1 - r_2)$, 由此及 $0 \leqslant |r_1 - r_2| < m$ 即得 $r_1 = r_2$, 亦即 $a \equiv b(\mathrm{mod} m) \Leftrightarrow r_1 = r_2$.

➤**9.4 推论 1** $a \equiv b(\mathrm{mod}\ m) \Leftrightarrow a = b + mt (t \in \mathbb{Z})$.

e.g.$n = 8t + 7 (t \in \mathbb{Z}) \Leftrightarrow 8 \mid (n-7) \Leftrightarrow n \equiv 7(\mathrm{mod} 8)$.

二、同余的性质

➤**9.5 定理 2** 同余是一种等价关系, 即同余具有下面性质:

(i) 反身性:$a \equiv a(\mathrm{mod}\ m)$;

(ii) 对称性:$a \equiv b(\mathrm{mod}\ m) \Leftrightarrow b \equiv a(\mathrm{mod}\ m)$;

(iii) 传递性:$a \equiv b, b \equiv c(\mathrm{mod}\ m) \Rightarrow a \equiv c(\mathrm{mod}\ m)$.

证明: 由 $m|(a-a) = 0, m|(a-b) \Leftrightarrow m \mid (b-a)$ 以及 $m|(a-b), m|(b-c) \Rightarrow m \mid (a-b) + (b-c) = a - c$, 即可推出上述三条性质.

➤**9.6 定理 3** (可加性) 若 $a \equiv b(\mathrm{mod}\ m), c \equiv d(\mathrm{mod}\ m)$, 则 $a + c \equiv b + d(\mathrm{mod}\ m)$.

证明: 由 $m \mid (a-b)$ 及 $m|(c-d) \Rightarrow m|(a-b)+(c-d)$, 即得 $m \mid (a+c)-(b+d)$; 对于减法同理可证. 故结论成立.

➤**9.7 推论 1** 若 $a + c \equiv b(\mathrm{mod} m), c \in \mathbb{Z}$, 则 $a \equiv b - c(\mathrm{mod}\ m)$.

➤**9.8 定理 4** (可乘性)

(1) 若 $a \equiv b(\mathrm{mod}\ m), c \in \mathbb{Z}$, 则 $ac \equiv bc(\mathrm{mod}\ m)$.

(2) 若 $a \equiv b(\mathrm{mod}\ m), c \equiv d(\mathrm{mod}\ m)$, 则 $ac \equiv bd(\mathrm{mod}\ m)$.

(3) 若 $a \equiv b(\mathrm{mod}\ m), n \in \mathbb{N}^*$, 则 $a^n \equiv b^n(\mathrm{mod}\ m)$.

(4) 若 $a \equiv b\,(\mathrm{mod}\ m_1), a \equiv b\,(\mathrm{mod}\ m_2), (m_1, m_2) = 1$, 则 $a \equiv b\,(\mathrm{mod}\ m_1 m_2)$;

若 $a \equiv b\,(\mathrm{mod}\ m_1), a \equiv b\,(\mathrm{mod}\ m_2)$, 则 $a \equiv b\,(\mathrm{mod}\ [m_1, m_2])$.

证明: (1)$\because a \equiv b(\mathrm{mod}\ m), \therefore m \mid (a-b)$;

$\therefore m \mid (a-b)c = ac - bc$.

$\therefore ac \equiv bc(\mathrm{mod}\ m)$.

(2)$\because a \equiv b(\mathrm{mod}\ m), \therefore ac \equiv bc(\mathrm{mod}\ m)$;

$\because c \equiv d(\mathrm{mod}\ m), \therefore bc \equiv bd(\mathrm{mod}\ m)$.

$\therefore ac \equiv bd(\mathrm{mod}\ m)$.

(3)$\because a \equiv b(\mathrm{mod}\ m), \therefore m \mid (a-b)$

$\therefore m \mid (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) = a^n - b^n$

$\therefore a^n \equiv b^n(\mathrm{mod}\ m)$.

(4)$\because a \equiv b\,(\mathrm{mod}\ m_1), a \equiv b\,(\mathrm{mod}\ m_2)$,

$\therefore m_1 \mid (a-b), m_2 \mid (a-b), \therefore [m_1, m_2] \mid (a-b)$

$\therefore a \equiv b\,(\mathrm{mod}\ [m_1, m_2])$.

➤**9.9 推论 1** (1) 若 $a \equiv b\,(\mathrm{mod}\ m_1), a \equiv b\,(\mathrm{mod}\ m_2), \cdots, a \equiv b\,(\mathrm{mod}\ m_n)$, 且 $m_1, m_2, \cdots, m_n$ 一两互质, 则

$$a \equiv b\,(\mathrm{mod}\ m_1 m_2 \cdots m_n)\,;$$

(2) 若 $a \equiv b\,(\mathrm{mod}\ m_1), a \equiv b\,(\mathrm{mod}\ m_2), \cdots, a \equiv b\,(\mathrm{mod}\ m_n)$, 则

$$a \equiv b\,(\mathrm{mod}\ [m_1, m_2, \cdots, m_n])\,.$$

➤**9.10 推论 2** (1) 若 $a_i \equiv b_i(\mathrm{mod}\ m)(i = 1, \cdots, n)$, 则

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=0}^{n} b_i(\mathrm{mod}\ m); \prod_{i=1}^{n} a_i \equiv \prod_{i=0}^{n} b_i(\mathrm{mod}\ m)$$

(2) 设整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$, 若 $x_1\equiv x_2(\mathrm{mod}\ m)$, 则

$$f(x_1)\equiv f(x_2)(\mathrm{mod}\ m)$$

➤9.11 定理 5 [(可约性)]

(1) $a\equiv b(\mathrm{mod}\ m), d\mid m, d>0\Rightarrow a\equiv b(\mathrm{mod}\ d)$

$a\equiv b(\mathrm{mod}\ m), d\mid (a,b,m), d>0\Rightarrow \dfrac{a}{d}\equiv\dfrac{b}{d}\left(\mathrm{mod}\ \dfrac{m}{d}\right)$;

(2) $a\equiv b(\mathrm{mod}\ m)\Rightarrow (a,m)=(b,m)$;

(3) $a\equiv b(\mathrm{mod}\ m)\Rightarrow ak\equiv bk(\mathrm{mod}\ mk)(k>0,k\in\mathbb{N})$;

(4) $ac\equiv bc(\mathrm{mod}\ m),(c,m)=1\Rightarrow a\equiv b(\mathrm{mod}\ m)$.

证明: (1) 显然成立.

(2) 由于 $m\mid(a-b)$, 存在 $t\in\mathbb{Z}$, 使得 $a=b+mt$, 于是 $(a,m)=(b+mt,m)=(b,m)$.

(3)$a\equiv b(\mathrm{mod}\ m)\Rightarrow m|(a-b)\Rightarrow km|(ka-kb)\Rightarrow ka\equiv kb(\mathrm{mod}\ km)$

(4) 因为 $ac\equiv bc(\mathrm{\ mod\ \ }m)\Rightarrow m\mid c(a-b)$, 又 $(c,m)=1$, 故 $m\mid(a-b)$, 即 $a\equiv b(\mathrm{mod}\ m)$.

证毕.

➤9.12 例 1 设整数 a 的十进制表示为 $a=\overline{a_{n-1}a_{n-2}\cdots a_0}\,(0\leqslant a_i\leqslant 9, 0\leqslant i\leqslant n-1, a_{n-1}\neq 0)$, 即 $a=a_{n-1}\times 10^{n-1}+\cdots+a_1\times 10+a_0$, 证明:

(i) $3|a\Leftrightarrow 3|\sum\limits_{i=0}^{n-1}a_i$

(ii) $9|a\Leftrightarrow 9|\sum\limits_{i=0}^{n-1}a_i$;

(iii) $11|a\Leftrightarrow 11|\sum\limits_{i=0}^{n-1}(-1)^ia_i$;

(iv) $13|a\Leftrightarrow 13|\overline{a_2a_1a_0}-\overline{a_5a_4a_3}+\cdots$

证明: 由 $10^\circ\equiv 1,10^1\equiv 1,\cdots,10^i\equiv 1(\mathrm{mod}\ 3)(i\in\mathbb{N})$ 及推论 2.1.1 得

$$a=\sum_{i=0}^{n-1}a_i\times 10^i\equiv\sum_{i=0}^{n-1}a_i(\mathrm{mod}\ 3)$$

由此可得结论 (i). 类似可证结论 (ii)、(iii) 和 (iv). 证毕.

➤9.13 注 一般, 当求十进制数 $a=\overline{a_{n-1}a_{n-2}\cdots a_1a_0}\,(0\leqslant a_i\leqslant 9)$ 被 m 除的数字特征时, 首先求出正整数 k, 使得 $10^k\equiv -1$ 或 $1(\mathrm{mod}\ m)$.

其次, 将 $a=\overline{a_{n-1}a_{n-2}\cdots a_1a_0}$ 写成 $a=\overline{a_{k-1}a_{k-2}\cdots a_1a_0}\times 10^0+\overline{a_{2k-1}a_{2k-2}\cdots a_k}\times 10^k+\cdots$ 的形式, 最后利用推论 2.1.1 可证得结论.

➤**9.14 例 2** 求 $2^{2^5}+1$ 被 641 除的余数.

解: 依次计算同余式 $2^2 \equiv 4, 2^4 \equiv 16, 2^8 \equiv 256, 2^{16} \equiv 154, 2^{32} \equiv -1(\mathrm{mod}\ 641)$. 因此 $2^{2^5}+1 \equiv 0(\mathrm{mod}\ 641)$, 即 $641 \mid \left(2^{2^5}+1\right)$. 这个结论说明费马数 $F_5 = 2^{2^5}+1$ 是合数.

➤**9.15 注** 一个整数模 m 的余数有 m 种可能值, 但对于幂次方整数, 模 m 的余数的个数则可能大大减少, 如, 一个完全平方数模 4 同余于 0 或 1, 模 8 同余于 0,1 和 4, 模 3 同余于 0 或 1, 模 5 同余于 0 或 ± 1, 一个完全立方数模 9 同余于 0 或 ± 1, 一个整数的四次方模 16 同余于 0 或 1. 这些事实构成利用同余知识解 (证) 问题的一个基本点.

➤**9.16 例 3** 求 $n = 7^{7^7}$ 的个位数字.

解: 由于 $7^1 \equiv -3, 7^2 \equiv -1, 7^4 \equiv 1(\mathrm{mod}\ 10)$, 因此, 若 $7^7 \equiv r(\mathrm{mod}\ 4)$, 则

$$n = 7^{7^7} \equiv 7^r(\mathrm{mod}\ 10) \tag{9.1}$$

由于 $7^7 \equiv (-1)^7 \equiv -1 \equiv 3(\mathrm{mod}\ 4)$, 所以, 由式(9.1)得

$$n = 7^{7^7} \equiv 7^3 \equiv (-3)^3 \equiv -7 \equiv 3(\mathrm{mod}\ 10)$$

即 n 的个位数字是 3.

➤**9.17** 一般的, 求 a^{b^c} 关于模 m 的余数, 可按以下步骤进行:

① 求出整数 k, 使得 $a^k \equiv 1(\mathrm{mod}\ m)$;(求 k 的目的是为了简化同余式的计算)

② 求出正整数 $r(r<k)$, 使得 $b^c \equiv r(\mathrm{mod}\ k)$;

③ 再计算 $a^{b^c} \equiv a^r(\mathrm{mod}\ m)$.

作业:	
教学后记:	

第十讲　二元一次不定方程

教学目标：	掌握二元一次不定方程的解法
教学重点：	二元一次不定方程的解法
教学难点：	二元一次不定方程的解法
教学方法和手段：	讲授
教学时数：	4 课时

➤10.1 一只箱子中有若干只蜜蜂和蜘蛛, 它们共有 46 只脚, 问其中蜜蜂和蜘蛛各多少只?

如果设箱子中蜜蜂、蜘蛛数分别为 x, y 只, 则依题意得

$$6x + 8y = 46 \tag{10.1}$$

这一方程有无限多组解, 但是, 符合题意的 x 和 y 只能是取正整数的解.

在介绍一般不定方程的求解之前, 先尝试解决如上给出的蜜蜂和蜘蛛的只数问题.

由式(10.1)可得 $x = \dfrac{23 - 4y}{3}$, 由于 x, y 必须是正整数, 故 y 只能取 $1, 2, 3, 4, 5$(否则, 若 y 大于 5, 则 x 必为负数). 下面通过直接计算得到相应的 x 值为

y	1	2	3	4	5
x	$\dfrac{19}{3}$	5	$\dfrac{11}{3}$	$\dfrac{7}{3}$	1

由此可知, 蜜蜂和咖蛛的只数分别为 $x = 5, y = 2$ 或 $x = 1, y = 5$.

➤10.2 定义 1 设 a, b 是非零整数,c 是整数, 关于未知数 x, y 的方程

$$ax + by = c \tag{10.2}$$

称为二元一次不定方程.

讨论二元一次方程是否有整数解的判别条件.

约定: 将整数 $a_1, \cdots, a_k$ 的最大公因数记作 $\gcd(a_1, \cdots, a_k)$.

➤10.3 定理 1 设 $d = \gcd(a, b)$, 则式(10.2)有整数解的充分必要条件是 $d \mid c$.

证明: 必要性 若式(10.2)有一组整数解, 设为 $x = x_0, y = y_0$, 则 $ax_0 + by_0 = c$. 因 d 整除 a 及 b, 因而也整除 c. 必要性得证.

充分性 若 $d \mid c$, 则存在整数 c_1, 使得 $c = dc_1$. 又由于 $d = \gcd(a, b)$, 由推论 1.3.1 知, 存在整数 s, t 满足

$$as + bt = d$$

于是有

$$a\left(sc_1\right)+b\left(tc_1\right)=dc_1$$

令 $x_0=sc_1, y_0=tc_1$, 即得 $ax_0+by_0=c$, 故式(10.2)有整数解 $(x_0,y_0)=(sc_1,tc_1)$. 充分性得证.

证毕.

下面讨论当式(10.2)有解时, 如何求得其全部整数解.

➤10.4 定理 2 若方程(10.2)有整数解 (x_0,y_0), 则其全部整数解为

$$\begin{cases}x=x_0-b_1t\\ y=y_0+a_1t\end{cases}\qquad(t=0,\pm1,\pm2,\cdots)\tag{10.3}$$

其中,$d=\gcd(a,b), a=a_1d, b=b_1d$.

证明: 首先证明, 式(10.3)给出的任一组整数 (x,y) 都适合式(10.2).

事实上, 由于 $x=x_0,y=y_0$ 是式(10.2)的解, 所以 $ax_0+by_0=c$. 因此, 将式(10.3)代人式(10.2)得

$$\begin{aligned}a\left(x_0-b_1t\right)+b\left(y_0+a_1t\right)&=\left(ax_0+by_0\right)+\left(ba_1-ab_1\right)t\\&=c+\left(db_1a_1-da_1b_1\right)t=c\end{aligned}$$

这就表明对任意整数 t, 式(10.3)给出的任一组整数 (x,y) 是式(10.2)的解.

其次证明, 式(10.2)的任一组解 (x',y') 都具有式(10.3)的形式.

设 (x',y') 是式(10.2)的任一组解, 则 $ax'+by'=c$; 又因为 $ax_0+by_0=c$, 两式相减得

$$a\left(x'-x_0\right)+b\left(y'-y_0\right)=0$$

但 $a=a_1d, b=b_1d$, 于是

$$a_1\left(x'-x_0\right)=-b_1\left(y'-y_0\right)\tag{10.4}$$

由于 $d=\gcd(a,b)$, 故 $\gcd\left(a_1,b_1\right)=1$, 因此, 由式(10.4)知 $a_1\mid(y'-y_0)$. 故存在整数 t, 使得 $y'-y_0=a_1t$, 亦即 $y'=y_0+a_1t$, 代入式 (10.4)得 $x'=x_0-b_1t$, 因此,(x',y') 可以表示成式(10.3)的形式, 故式(10.3)给出了式(10.2)的一切整数解. 证毕.

➤10.5 注 定理 3.1.2 中的式(10.3)也可写成

$$\begin{cases}x=x_0+b_1t\\ y=y_0-a_1t\end{cases}\qquad(t=0,\pm1,\pm2,\cdots)$$

的形式.

➤**10.6** 从定理 3.1.1 的证明过程可以发现, 关键是证明方程

$$ax + by = \gcd(a, b) = d$$

有整数解. 因此, 若要找出一般二元一次不定方程求特解的方法, 应该从此方程人手.

首先, 方程 $ax + by = \gcd(a, b)$ 等价于

$$\frac{a}{\gcd(a, b)}x + \frac{b}{\gcd(a, b)}y = 1$$

而在此方程里, 未知数 x, y 的系数是互素的, 所以, 不失一般性, 只要讨论如何求出形如

$$ax + by = 1, \quad \gcd(a, b) = 1 \tag{10.5}$$

的方程的一个整数解即可.

容易知道, 由式(10.5)的一个特殊解可以得出方程 $|a|x + |b|y = 1$ 的一个特殊解, 反之亦然. 于是, 可以假定 $a > 0, b > 0$. 为了求出满足式(10.5)的 x, y, 运用辗转相除法, 有

$$\begin{aligned}
&a = bq_1 + r_1, && 0 < r_1 < b\\
&b = r_1q_2 + r_2, && 0 < r_2 < r_1\\
&\quad \cdots\\
&r_{n-2} = r_{n-1}q_n + r_n, && 0 < r_n < r_{n-1}\\
&r_{n-1} = r_nq_{n+1}, && r_{n+1} = 0
\end{aligned}$$

因为 $\gcd(a, b) = 1$, 故 $r_n = 1$. 由定理 1.5.1 知, 利用辗转相除及列表方法可计算出

$$Q_na - P_nb = (-1)^{n+1}r_n$$

即 $a\left[(-1)^{n-1}Q_n\right] + b\left[(-1)^nP_n\right] = 1$

因此, 式(10.5)有一组特解

$$x_0 = (-1)^{n-1}Q_n, \quad y_0 = (-1)^nP_n$$

➤**10.7 注** 求解二元一次不定方程步骤:

① 首先利用定理 3.1.1 判断不定方程是否有解;

② 在有解的情况下, 关键在于求出其特解;

③ 当不定方程有解且其系数绝对值不大时, 可用观察法求出其特解; 当方程系数较大时, 可考虑用辗转相除法求特解.

➤**10.8 例 1** 求不定方程 $18x + 24y = 9$ 的整数解.

解: 由于 $\gcd(18, 24) = 6 \nmid 9$, 所以原方程无整数解.

➤10.9 例 2 求 $10x-7y=17$ 的全部整数解.

解: 由于 $\gcd(10,7)=1\mid 17$, 所以原方程有整数解. 由观察可得原方程的一组特解为 $x_0=1,y_0=-1$. 因此, 原方程的全部整数解是

$$x=1-7t,\quad y=-1-10t\quad (t=0,\pm1,\pm2,\cdots)$$

➤10.10 例 3 求方程 $907x_1+731x_2=2107$ 的整数解.

解: 解法一先用展转相除法得

1	731	907	
	704	731	
6	27	176	4
	14	162	
1	13	14	1
	13	13	
	0	1	13

故 $\gcd(907,731)=1$. 再用列表方法计算相应的特解如下表.

n	0	1	2	3	4	5
q_n		1	4	6	1	1
P_n	1	1	5	31	36	67
Q_n	0	1	4	25	29	54

所以 $907\times 54-731\times 67=\gcd(907,731)=1$

因而, 原方程有一组特解

$$x_1'=54\times 2107,\quad x_2'=-67\times 2107$$

故, 原方程组的一切整数解为

$$\begin{cases}x_1=54\times 2107+731t\\ x_2=-67\times 2107-907t\end{cases}\qquad (t=0,\pm1,\cdots)$$

解法二因为 $\gcd(907,731)=1$, 故方程有整数解. 对系数绝对值较小的 x_2 进行如下变形:

$$x_2=\frac{1}{731}(-907x_1+2107)=-x_1+3+\frac{1}{731}(-176x_1-86)\in\mathbb{Z}$$

令 $x_3=\dfrac{1}{731}(-176x_1-86)\in\mathbb{Z}$, 则

$$x_1=-4x_3+\frac{1}{176}(-27x_3-86)$$

令 $x_4=\dfrac{1}{176}\left(-27x_3-86\right)\in\mathbb{Z}$, 则

$$x_3=-7x_4-3+\frac{1}{27}\left(13x_4-5\right)$$

令 $x_5=\dfrac{1}{27}\left(13x_4-5\right)\in\mathbb{Z}$, 则

$$x_4=2x_5+\frac{1}{13}\left(x_5+5\right)$$

令 $x_6=\dfrac{1}{13}\left(x_5+5\right)\in\mathbb{Z}$, 则

$$x_5=13x_6-5$$

此处 x_5 的系数为 1, 辗转相除到此为止, 将 x_6 视为参数, 按上述过程逆向依次代入, 直至得出 x_1,x_2 的表达式为止. 具体操作过程是

$$\begin{aligned}
&x_4=2x_5+x_6=2\left(-5+13x_6\right)+x_6=-10+27x_6\\
&x_3=-7x_4-3+x_5=-7\left(-10+27x_6\right)-3+\left(-5+13x_6\right)=62-176x_6\\
&x_1=-258+731x_6\\
&x_2=323-907x_6
\end{aligned}$$

令 $x_6=t$, 则方程的解为

$$\begin{cases}x_1=-258+731t\\ x_2=323-907t\end{cases}\qquad(t=0,\pm1,\pm2,\cdots)$$

➤10.11 例 4 求不定方程 $117x_1+21x_2=38$ 的整数解.

解: $x_2=\dfrac{1}{21}\left(-117x_1+38\right)=-6x_1+2+\dfrac{1}{21}\left(9x_1-4\right)$

令 $x_3=\dfrac{1}{21}\left(9x_1-4\right)\in\mathbb{Z}$, 则

$$x_1=\frac{1}{9}\left(21x_3+4\right)=2x_3+\frac{1}{9}\left(3x_3+4\right)$$

令 $x_4=\dfrac{1}{9}\left(3x_3+4\right)\in\mathbb{Z}$, 则

$$x_3=3x_4-1-\frac{1}{3}$$

此式表示 x_3,x_4 不可能同时为整数, 所以原不定方程无整数解.

➤10.12 例 5 甲种书每本 5 元, 乙种书每本 3 元, 丙种书 1 元三本, 现用 100 元买这三种书籍共 100 本, 问甲、乙、丙三种书各买多少本?

解: 设甲、乙、丙三种书籍分别买 x, y, z 本, 依题意得方程组

$$\begin{cases} 5x + 3y + \dfrac{1}{3}z = 100 \\ x + y + z = 100 \end{cases}$$

消去 z, 得

$$7x + 4y = 100 \tag{10.6}$$

显然 $x = 0, y = 25$ 是方程(10.6)的特解, 因此, 方程(10.6)的所有整数解是

$$\begin{cases} x = 4t \\ y = 25 - 7t \end{cases} \qquad (t = 0, \pm 1, \pm 2, \cdots)$$

令 $x \geqslant 0, y \geqslant 0$, 所以 $0 \leqslant t \leqslant 3$, 即 t 可以取整数值 $t_1 = 0, t_2 = 1, t_3 = 2, t_4 = 3$. 相应地求得 x, y, z 的值是 $(x, y, z) = (0, 25, 75), (4, 18, 78), (8, 11, 81), (12, 4, 84)$.

作业：	
教学后记：	