信息安全数学基础

（内部教材）

院系：计算机科学与技术学院

教师：韩 琦

版本：2023秋_v_20230910

目　录

第一部分

初等数论

导 读

本书所说的数论，严格来说是指初等数论，数论家族还有解析数论、代数数论和几何数论等分支，可以简单的理解为他们的研究对象是一样的，但是研究方法不同。初等数论不借助于其他数学学科，只依靠初等的方法来研究整数性质，是一门十分重要的数学基础课，不仅是数学专业的一门必修课程，也是计算机科学中许多专业方向所需的数学基础。

从数学的角度，本部分首先从整数除法的角度展开讨论，因为在整数集合中，除法并不是“封闭”的，于是有了带余除法的表达方式(事实上，带余除法不仅仅是一种表达方式，更是一个定理，指明了这种表达形式的存在性和唯一性。这是一个非常典型的数学思维，在计算机专业和数学专业学生的眼中，可能有不同的理解，但是个人认为，计算机专业的学生应该试着多从数学的角度去理解，体会数学逻辑体系之严密，培养自己严谨细致的思维习惯。)。基于带余除法，可以证明辗转相除法最终一定能够得到一个整除（不带余数）的表达式，于是发展出一系列基于辗转相除法的计算方法：求最大公因数、解不定方程、解同余方程等等。有了这些工具之后，开始从素数的角度重新认识整数，于是有了整数唯一分解定理，指出了素数作为整数的基本“成分”的事实；进而从同余的角度，重新认识整数集合的“结构”，我们发现一个模数可以把整个整数集合依同余关系划分成若干个集合，每个集合在对该模数的余数方面具有相同性质，再结合互素的概念，有了剩余类、剩余系、非负最小剩余系、即约剩余系等概念。于是我们可以讨论欧拉函数和欧拉定理了，费马小定理是欧拉定理的直接推导，RSA算法的正确性也靠欧拉定理得以证明。最后，围绕素数展开了讨论，即便都是素数，也有一些具有特别的特征，比如孪生素数、梅森素数等，他们的存在性及寻找都是有趣的话题，人们也逐渐认识到素性判断是个很大的难题，素性判断中，原根是个重要的概念。

从信息安全的角度，当有了同余的概念之后，就可以更加严谨的理解和描述古典密码中的代换密码了，把表、移位、仿射变化都归结为一种模运算。基于不定方程，可以去描述背包问题，但是要基于背包问题构建安全的公开密钥算法，则需要理解同余方程，并基于同余方程建立普通背包和超递增背包的关系，把难题留给攻击者，把可行的解背包计算留给合法接收者。当前使用最广泛的RSA公开密钥算法是基于欧拉定理构造的，其加解密过程在形式

上非常简单，就是一个指数运算和一个模运算，但是实际计算中，数值都非常大，这又引出了一个在计算机中如何实现的问题，解决的办法就是模重复平方计算法，几乎一样的方法在程序员圈子里有个更流行的说法，叫快速幂算法。模重复平方计算法关注的是模运算$a^n(\mod m)$中a^n的简化问题，其实在中国剩余定理的加持下，还可以对模数m进行分解和简化。

尽管有一些比穷举稍微简单一点的方法，但从计算机的角度看，在计算速度上并没有质的飞跃，而也正是这一点，迄今为止仍然保护着互联网上很多通信和交易行为的安全。

第 1 章　整数的可除性与辗转相除法

1.1 引言

1.2 整除的概念与性质

整数的和、差、积是整数，但整数的商不一定是整数。初等数论研究的是整数的性质，为此引入整除的概念。

定义 1.1 设a, b是任意两个整数，其中$b \neq 0$，如果存在一个整数q使得等式

$$a = bq \tag{1-1}$$

成立，则称b**整除** a，记作$b|a$。此时b称作a的**因数**，a 称作b 的**倍数**。如果满足等式的整数q不存在，则称b 不能整除a或者a 不被b 整除，记作$b \nmid a$。

整除这个概念虽然简单，但却是初等数论中的基本概念。由整除的定义和乘法的运算性质，容易得到整除的性质。

定理 1.1 设a, b, c是整数，则

(1) 如果$b|a, c|b$，则$c|a$;

(2) 如果$c|a, c|b$，则$c|(a \pm b)$;

(3) 如果$b|a, a|b$，则$a = \pm b$;

(4) 设$m \neq 0$，$b|a$，则$bm|am$。

证明：(1)因为$b|a, c|b$，则a, b可表示为

$$a = bm, b = cn, \text{其中} m, n \text{是整数}$$

因此，$a = c(mn)$，即$c|a$。

(2)因为$c|a, c|b$，则a, b可表示为

$$a = cm, b = cn, \text{其中} m, n \text{是整数}$$

因此，有$a \pm b = c(m \pm n)$，即$c|(a \pm b)$。

(3)因为$b|a, a|b$，所以

$$a = bm, b = an, \text{其中} m, n \text{是整数}$$

因此，$a = a(mn), mn = 1$，所以$n = \pm 1, m = \pm 1$，即$a = \pm b$。

(4)因为$b|a$，所以

$$a = bq, \text{其中} q \text{是整数}$$

因此，$am = (bm)q$，即$bm|am$。 □

定理 1.2 设a, b是两个整数，其中$b > 0$，则存在两个唯一的整数q, r，使得

$$a = bq + r,\ 0 \leq r < b \tag{1-2}$$

成立。

证明：首先证明存在性。考虑整数序列

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

则a必在上述序列的某两项之间，即存在一个整数q使得

$$qb \leq a < (q+1)b \tag{1-3}$$

成立。令$a - qb = r$，则$a = bq + r$，而$0 \leq r < b$。

其次证明唯一性。设q', r'是满足条件的另外整数对，即

$$a = bq' + r', 0 \leq r < b \tag{1-4}$$

所以

$$bq' + r' = bq + r \tag{1-5}$$

于是

$$b(q' - q) = r - r' \tag{1-6}$$

则有

$$b|q'-q| = |r-r'| \tag{1-7}$$

又由于$0 \leq r < b, 0 \leq r' < b$，所以$|r-r'| < b$。如果$q \neq q'$，则式1-7 不能成立。因此$q = q', r = r'$。 □

定义 1.2 称式1-2中的q为a被b除得出的**不完全商**，r为a 被b 除得出的**余数**，也称为**非负最小余数**。

例 1.1 2021除以某自然数，商为50，求除数和余数。

解：设除数为x，余数为y，由题意有

$$2021 = 50x + y, 0 \leq y < x \tag{1-8}$$

故

$$\begin{cases} 50x \leq 2021 \\ 50x + x > 2021 \end{cases} \tag{1-9}$$

解得

$$\begin{cases} x \leq 40\frac{21}{50} \\ x > 39\frac{32}{51} \end{cases} \tag{1-10}$$

而x是整数，故取$x = 40$，从而$y = 21$。因此，所求除数为40，余数为21.

例 1.2 已知$N = 2^{2021} - 2^{2019} + 2^{2017} - 2^{2015} + 2^{2013} - 2^{2011}$，求证：$9|N$。

证明：

$$\begin{aligned} N &= 2^{2011} \times (2^{10} - 2^8 + 2^6 - 2^4 + 2^2 - 1) \\ &= 2^{2011} \times 819 \\ &= 9 \times 91 \times 2^{2011} \end{aligned} \tag{1-11}$$

所以，$9|N$。 □

习题：

1. 若$a_1, a_2, \cdots, a_n$都是m的倍数，$q_1, q_2, \cdots, q_n$ 是任意n 个整数，证明：$q_1a_1 + q_2a_2 + \cdots + q_na_n$是$m$的倍数。

解：因为$a_1, a_2, \cdots, a_n$都是m的倍数，所以有

$$a_1 = s_1m, a_2 = s_2m, \cdots, a_n = s_nm\text{其中}s_1, s_2, \cdots, s_n\text{是整数}$$

因此

$$q_1a_1 + q_2a_2 + \cdots + q_na_n = m(q_1s_1 + q_2s_2 + \cdots + q_ns_n)$$

所以，$q_1a_1 + q_2a_2 + \cdots + q_na_n$是$m$的倍数。

2. 证明：$3|n(n+1)(2n+1)$，其中n是任意整数。**证明：**

$$\begin{aligned} n(n+1)(2n+1) &= n(n+1)(n+2+n-1) \\ &= n(n+1)(n+2) + (n-1)n(n+1) \end{aligned}$$

因为$n(n+1)(n+2)$和$(n-1)n(n+1)$是三个连续的整数，所以

$$3|n(n+1)(n+2), 3|(n-1)n(n+1)$$

因此$3|n(n+1)(n+2) + (n-1)n(n+1)$，从而$3|n(n+1)(2n+1)$。

附注：归纳法证明$3|n(n+1)(n+2)$

证明：

- 当$n = 1$时，$n(n+1)(n+2) = 1\dot{2}\dot{3}$，则$3|n(n+1)(n+2)$;
- 设$n = k$时，满足$3|k(k+1)(k+2)$;
- 当$n = k+1$时，

$$\begin{aligned} n(n+1)(n+2) &= (k+1)(k+2)(k+3) \\ &= k(k+1)(k+2) + 3(k+1)(k+2) \end{aligned}$$

因为

$$3|k(k+1)(k+2), 3|3(k+1)(k+2)$$

所以

$$3|k(k+1)(k+2) + 3(k+1)(k+2)$$

从而$3|n(n+1)(n+2)$。

由此可知，$3|n(n+1)(n+2)$，其中n为任意整数。 □

3. 若$ax_0 + by_0$是形如$ax + by$的数中的最小正数(x, y是任意整数，a, b 是两个不全为零的整数)，证明：$(ax_0 + by_0)|(ax + by)$。

证明：因为a, b不全为零，所以在整数集合$S = \{ax + by|x, y是整数\}$ 中存在正整数，因而有形如$ax + by$的最小正数$ax_0 + by_0$。

由带余除法可知，存在唯一的q, r满足

$$ax + by = (ax_0 + by_0)q + r, 0 \leq r < ax_0 + by_0$$

则

$$r = (ax + by) - (ax_0 + by_0)q = (x - x_0q)a + (y - y_0q)b$$

由上式可知r是集合S中的元素。但$ax_0 + by_0$是S中最小的正数，所以$r = 0$，则有

$$ax + by = (ax_0 + by_0)q$$

即$(ax_0 + by_0)|(ax + by)$。

1.3 辗转相除法与最大公因数

定义 1.3 设$a_1, a_2, \cdots, a_n$是n个不全为零的整数。如果整数d是它们之中每一个的因数，那么d就称为$a_1, a_2, \cdots, a_n$的一个**公因数**。整数$a_1, a_2, \cdots, a_n$的公因数中最大的一个称为**最大公因数**，记作$(a_1, a_2, \cdots, a_n)$。如果$(a_1, a_2, \cdots, a_n) = 1$，就称$a_1, a_2, \cdots, a_n$**互素**或**互质**。

例如设$a = 12, b = 16$，它们的公因子有$\pm1, \pm2, \pm4$，$(12, 16) = 4$。如果整数$a_1, a_2, \cdots, a_n$两两互素，则$(a_1, a_2, \cdots, a_n) = 1$，反之不然。

例如设$a = 12, b = 16, c = 15$，有$(12, 16, 15) = 1$，但12和15并不互素。

为了免去讨论正负数的麻烦，先证明以下定理。

定理 1.3 若$a_1, a_2, \cdots, a_n$是任意n个不全为零的整数，则

(1)$a_1, a_2, \cdots, a_n$与$|a_1|, |a_2|, \cdots, |a_n|$的公因数相同；

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

证明： 设d是$a_1, a_2, \cdots, a_n$的任一公因数。由定义可知$d|a_i, i = 1, 2, \cdots, n$，因而$d||a_i|, i = 1, 2, \cdots, n$，故$d$是$|a_1|, |a_2|, \cdots, |a_n|$的一个公因数。同理可证，$|a_1|, |a_2|, \cdots, |a_n|$的任一公因数都是$a_1, a_2, \cdots, a_n$的一个公因数。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，$(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$。 □

定理1.3告诉我们要讨论最大公因数，不妨仅就非负整数去讨论。

定理 1.4 若b是任一正整数，则

(1)0与b的公因数就是b的因数，反之，b的因数也就是0与b 的公因数；

(2)$(0,b)=b$。

证明：显然，0与b的公因数是b的因数。由于任何非零整数都是0的因数，故b 的因数也就是0 和b 的公因数。其次，b 的最大因数是b，而0和b的最大公因数是b的最大因数，故$(0,b)=b$。 □

推论 1.4 $(0,b)=|b|$。

定理 1.5 设a,b,c是任意三个不全为零的整数，且$a=bq+c$，其中q是整数，则$(a,b)=(b,c)$。

证明：因为$(a,b)|a,(a,b)|b$，所以由$a=bq+c$，有$(a,b)|c$，因而$(a,b)\leq(b,c)$。同理可证$(b,c)\leq(a,b)$，于是$(a,b)=(b,c)$。 □

现在我们可以介绍**辗转相除法**(也称作**欧几里得算法**)，这个辗转相除法不仅可以给出求出两个整数的最大公因数，并且可以推出最大公因数的性质。

设整数$a,b(\neq 0)$，由带余除法，有下列等式

$$\begin{aligned}
&a=bq_1+r_1, && 0<r_1<b\\
&b=r_1q_2+r_2, && 0<r_2<r_1\\
&\ldots, && \ldots\\
&r_{n-2}=r_{n-1}q_n+r_n, && 0<r_n<r_{n-1}\\
&r_{n-1}=r_nq_{n+1}+r_{n+1}, && r_{n+1}=0
\end{aligned} \tag{1-12}$$

因为$|b|>r_1>r_2>\ldots$，故经过有限次带余数除法后，总可以得到一个余数是零，即式1-16中$r_{n+1}=0$。这个过程称为**辗转相除法**。这种方法是我国古代数学家所创造的，这是古代算学书中的求一术，但在外文书籍中，常把它叫做欧几里得算法。

注：根据定理1.5，对任意整数$a>0,b>0$，作辗转相除法，则最后一个非零余数r_n 就是(a,b)。

例 1.3 令$a=456, b=123$，求(a,b)。

解：

$$\begin{aligned}
456 &= 123\times 3+87\\
123 &= 87\times 1+36\\
87 &= 36\times 2+15\\
36 &= 15\times 2+6\\
15 &= 6\times 2+3\\
6 &= 3\times 2
\end{aligned}$$

所以，$(a,b)=3$。

例 1.4 令$a=-1234, b=567$，求(a,b)。

解：因为

$$\begin{aligned}
1234 &= 567\times 2+100\\
567 &= 100\times 5+67\\
100 &= 67\times 1+33\\
67 &= 33\times 2+1\\
33 &= 1\times 33
\end{aligned}$$

所以，$(a,b)=(-1234,567)=(|-1234|,|567|)=(1234,567)=1$。

由辗转相除法，还得到一些关于最大公因数的基本性质。

定理 1.6 a,b,c均为整数，其中$c>0$，则有$(a,b)c=(ac,bc)$。

证明：当a,b有一个为零，定理显然成立。令a,b均不为零，由定理1.3 可知

$$(am,bm)=(|a|m,|b|m),(a,b)m=(|a|,|b|)m$$

因此不妨假定a,b都是正数。在式1-16里，把各式两边同乘以c，即得

$$\begin{aligned}
&ac=(bc)q_1+r_1c, && 0<r_1c<bc\\
&bc=(r_1c)q_2+r_2c, && 0<r_2c<r_1c\\
&\ldots, && \ldots\\
&r_{n-2}c=(r_{n-1}c)q_n+r_nc, && 0<r_nc<r_{n-1}c\\
&r_{n-1}c=(r_nc)q_{n+1}+r_{n+1}c, && r_{n+1}c=0
\end{aligned} \tag{1-13}$$

由辗转相除法可得$(ac,bc)=r_nc=(a,b)c$。 □

定理 1.7 a,b,c均为整数，若$(a,b)=1$，则有$(ac,b)=(c,b)$。

证明：因为

$$(ac,b)|ac,(ac,b)|bc$$

所以

$$(ac,b)|(ac,bc)=(a,b)c=c$$

再因为

$$(ac,b)|b$$

所以

$$(ac,b)|(c,b)$$

又

$$(c,b)|ac,(c,b)|b$$

所以

$$(c,b)|(ac,b)$$

于是

$$(ac,b)=(c,b)$$

□

例 1.5 $(1936,16)=(11^2\times 12,16)=(12,16)=4$。

由上面几个定理，容易得到几个常用的结果：a,b,c是三个整数，

- 当$b|ac$时，若$(a,b)=1$，则有$b|c$;
- 当$a|c,b|c$时，若$(a,b)=1$，则有$ab|c$;
- 当$(a,c)=1,(b,c)=1$时，则有$(ab,c)=1$;
- 若$(a,b)=1$，则$(ab,a+b)=1$。

定理 1.8 设正整数c是整数a,b的公因子，则

$$(\frac{a}{c},\frac{b}{c})=\frac{(a,b)}{c} \tag{1-14}$$

证明：$(\frac{a}{c},\frac{b}{c})c=(\frac{a}{c}\cdot c,\frac{b}{c})\cdot c=(a,b)$。
因此，$(\frac{a}{c},\frac{b}{c})=\frac{(a,b)}{c}$。 □

推论 1.5 设$c>0$，那么$(\frac{a}{c},\frac{b}{c})=1$的充分必要条件是$c=(a,b)$。

定理 1.9 假定$a_1,a_2,\cdots,a_n$是任意n个整数，令

$$(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{n-1},a_n)=d_n \tag{1-15}$$

则$(a_1,a_2,\cdots,a_n)=d_n$。

证明： 由$(d_{n-1},a_n)=d_n$可得$d_n|a_n,d_n|d_{n-1}$，同理$d_{n-1}|a_{n-1},d_{n-1}|d_{n-2}$，故$d_n|a_{n-1},d_n|d_{n-2}$。由此类推，最后得到$d_n|a_n,d_n|a_{n-1},\cdots,d_n|a_1$，即$d_n$是$a_1,a_2,\cdots,a_n$的一个公因数。
又设d是$a_1,a_2,\cdots,a_n$的任一公因数，则$d|a_1,d|a_2$，则$d|d_2$，同理有$d|d_3$。由此类推，最后得$d|d_n$。因而$d\le|d|\le d_n$。故d_n是$a_1,a_2,\cdots,a_n$的最大公因数。 □

例 1.6 求$(123,456,789)$。
解：

$$(123,456,789)=(123,(456,789))=(123,3)=3$$

习题

1. 求解$(9876,54321)$。
解：

$$\begin{aligned}54321&=9876\times5+4941\\9876&=4941\times1+4935\\4941&=4935\times1+6\\4935&=6\times822+3\\6&=3\times2\end{aligned}$$

因此，$(9876,54321)=3$。

2. 求解$(98765,-43210)$。
解：

$$\begin{aligned}98765&=43210\times2+12345\\43210&=12345\times3+6175\\12345&=6175\times1+6170\\6175&=6170\times1+5\\6170&=5\times1234\end{aligned}$$

因此，$(98765, -43210) = (98765, 43210) = 5$。

3. 求解$(-987, 654, -321)$。

解：

$$\begin{aligned} 654 &= 321 \times 2 + 12 \\ 321 &= 12 \times 3 + 9 \\ 12 &= 9 \times 1 + 3 \\ 9 &= 3 \times 3 \end{aligned}$$

因此$(654, -321) = (654, 321) = 3$。所以

$$(-987, 654, -321) = (-987, (654, -321)) = (-987, 3) = 3$$

1.4 扩展的欧几里得算法与最小公倍数

由上节的辗转相除法，设a, b是任意两个正整数，则可以得到下列等式：

$$\begin{array}{ll} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1 q_2 + r_2, & 0 < r_2 < r_1 \\ \cdots, & \cdots \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n q_{n+1} + r_{n+1}, & r_{n+1} = 0 \end{array} \tag{1-16}$$

于是有

定理 1.10 假定a, b是任意两个正整数，则

$$Q_k a - P_k b = (-1)^{k-1} r_k, \qquad k = 1, \cdots, n \tag{1-17}$$

其中

$$\begin{array}{llll} P_0 = 1, & P_1 = q_1, & P_k = q_k P_{k-1} + P_{k-2} & \\ Q_0 = 0, & Q_1 = 1, & Q_k = q_k Q_{k-1} + Q_{k-2} & k = 2, \cdots, n \end{array} \tag{1-18}$$

证明： 当$k=1$时，式1-17显然成立。当$k=2$时，

$$\begin{aligned} r_2 &= b - r_1 q_2 \\ &= b - (a - bq_1)q_1 \\ &= -[aq_2 - b(1 + q_1 q_2)] \end{aligned}$$

但

$$1 + q_1 q_2 = P_0 + q_2 P_1, \quad q_2 = q_2 \cdot 1 + 0 = q_2 Q_1 + Q_0$$

故

$$Q_2 a - P_2 b = (-1)^{2-1} r_2, \quad P_2 = q_2 P_1 + P_0, \quad Q_2 = q_2 Q_1 + Q_0$$

假定式1-17和式1-18对于不超过k的正整数都成立，则

$$\begin{aligned} (-1)^k r_{k+1} &= (-1)^k (r_{k-1} - q_{k+1} r_k) \\ &= (Q_{k-1} a - P_{k-1} b) + q_{k+1}(Q_k - P_k b) \\ &= (q_{k+1} Q_k + Q_{k-1}) a - (q_{k+1} P_k + P_{k-1}) b \end{aligned}$$

故$Q_{k+1} a - P_{k+1} b = (-1)^k r_{k+1}$，其中

$$P_{k+1} = q_{k+1} P_k + P_{k-1}, \quad Q_{k+1} = q_{k+1} Q_k + Q_{k-1}$$

由数学归纳法可知定理成立。 □

推论 1.6 对任意不全为零的整数a, b，存在整数u, v，使得$au + bv = (a, b)$。

注： 求解u, v的回代过程被称之为**扩展的欧几里得算法**，是后续章节求解二元一次不定方程的重要步骤。

例 1.7 求解$(1920, 2021)$，并求解满足$1920x + 2021y = (1920, 2021)$的$x, y$。

解：

$$\begin{aligned} 2021 &= 1920 \times 1 + 101 \\ 1920 &= 101 \times 19 + 1 \\ 101 &= 1 \times 101 \end{aligned}$$

所以，$(1920, 2021) = 1$，又

$$\begin{aligned} 1 &= 1920 - 101 \times 19 \\ &= 1920 - (2021 - 1920) \times 19 \\ &= 1920 \times 20 + 2021 \times (-19) \end{aligned}$$

因此，$x = 20, y = -19$。

定义 1.7 设$a_1, a_2, \ldots, a_n$是n个整数$(n \geq 2)$。若整数m是这n个数中每一个数的倍数，则m 就称为这n个数的**公倍数**。在$a_1, a_2, \ldots, a_n$ 的一切公倍数中最小的正数称为**最小公倍数**，记作$[a_1, a_2, \ldots, a_n]$。

定理 1.11 如果$ab > 0$，那么$[a, b](a, b) = ab$。

证 明： 设$[a, b] = m, (a, b) = d$。因为$a|m, b|m$，所以$ab|ma, ab|mb$，因此$ab|(ma, mb)$，即$ab|md$。
又因为$a|\frac{ab}{d}, a|\frac{ab}{d}$，即$\frac{ab}{d}$是$a, b$的公倍数，所以$m|\frac{ab}{d}$，于是$md|ab$。
因此，$ab = md$，定理得证。 □

注： 利用作辗转相除法，可先求出最大公因数，再由$[a, b] = \frac{|ab|}{(a,b)}$ 计算最小公倍数。

例 1.8 求$[231, 7653]$。
解：

$$\begin{aligned} 7653 &= 231 \times 33 + 30 \\ 231 &= 30 \times 8 - 9 \\ 30 &= 9 \times 3 + 3 \\ 9 &= 3 \times 3 \end{aligned}$$

所以，$(7653, 231) = 3$，从而$[231, 7653] = \frac{7653 \times 231}{3} = 589281$。

现在讨论两个以上整数的最小公倍数，设$a_1, a_2, \cdots, a_n$是n个正整数，若

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \cdots, [m_{n-1}, a_n] = m_n \tag{1-19}$$

定理 1.12 若$a_1, a_2, \cdots, a_n$是$n(\geq 2)$个正整数，则$[a_1, a_2, \cdots, a_n] = m_n$。

证 明： 由式1-19可知，$m_i|m_{i+1}, i = 2,3,\cdots,n-1$，且$a_1|m_2, a_i|m_i, i = 2,3,\cdots,n$，故$m_n$是$a_1,a_2,\cdots,a_n$的一个公倍数。
又设m是$a_1,a_2,\cdots,a_n$的任一公倍数，则$a_1|m, a_2|m$，故$m_2|m$。又$a_3|m$，同理有$m_3|m$。以此类推，最后得$m_n|m$。因此$m_n \leq |m|$。
故$m_n = [a_1,a_2,\cdots,a_n]$。 □

例 1.9 求解$[12,34,56]$。
解：

$$\begin{aligned}[12,34,56] &= [12,[34,56]] \\ &= [12,\tfrac{34\times56}{(34,56)}] \\ &= [12,\tfrac{1904}{2}] = [12,952] \\ &= \tfrac{12\times952}{(12,952)} = 2856\end{aligned}$$

习题

1. 求解满足$123x + 456y = (123,456)$的u,v。
解： 首先利用辗转相除法求得$(123,456)$

$$\begin{aligned}456 &= 123\times3+87\\123 &= 87\times1+36\\87 &= 36\times2+15\\36 &= 15\times2+6\\15 &= 6\times2+3\\6 &= 3\times2\end{aligned}$$

因此，$(123, 456) = 3$。再利用扩展的欧几里得算法回代

$$\begin{aligned}
3 &= 15 - 6 \times 2 \\
&= 15 - (36 - 15 \times 2) \times 2 \\
&= 15 \times 5 + 36 \times (-2) \\
&= (87 - 36 \times 2) \times 5 + 36 \times (-2) \\
&= 87 \times 5 + 36 \times (-12) \\
&= 87 \times 5 + (123 - 87) \times (-12) \\
&= 87 \times 17 + 123 \times (-12) \\
&= (456 - 123 \times 3) \times 17 + 123 \times (-12) \\
&= 456 \times 17 + 123 \times (-63)
\end{aligned}$$

因此，$x = -63, y = 17$。

2. 求解$[520, 1314]$。

解：先用辗转相除法求解$(520, 1314)$

$$\begin{aligned}
1314 &= 520 \times 2 + 274 \\
520 &= 274 \times 1 + 246 \\
274 &= 246 \times 1 + 28 \\
246 &= 28 \times 8 + 22 \\
28 &= 22 \times 1 + 6 \\
22 &= 6 \times 3 + 4 \\
6 &= 4 \times 1 + 2 \\
4 &= 2 \times 2
\end{aligned}$$

因此$(520, 1314) = 2$，所以$[520, 1314] = \frac{520 \times 1314}{(520, 1314)} = 341640$。

3. 求解$[200, 360, 510]$。

解：

$$\begin{aligned}
[200, 360, 510] &= [[200, 360], 510] \\
&= [\tfrac{200 \times 360}{(200, 360)}, 510] \\
&= [\tfrac{72000}{40}, 510] = [1800, 510] \\
&= \tfrac{1800 \times 510}{(1800, 510)} = \tfrac{918000}{30} = 30600
\end{aligned}$$

1.5 素数与算术基本定理

定义 1.8 一个大于1的整数，如果它的正因数只有1及它本身，就叫作**素数(或质数)**；否则就叫作**合数**。

1既不是素数，也不是合数，它在正整数中的地位非常特殊。

素数在研究整数的过程中具有重要地位，本节的主要目的就是要证明任何一个大于1 的整数，如果不论次序，能唯一地表示成素数的乘积。

定理 1.13 若a是任一大于1的整数，则a的除1外最小正因数q是一素数，并且当a 是合数时，$q \leq \sqrt{a}$。

证明：假定q不是素数，由定义，q除1及本身外还有一个正因数q_1，因而$1 < q_1 < q$。但$q|a$，所以$q_1|a$，这与q是a的除1外的最小正因数矛盾，故q是素数。

当a是合数时，则$a = a_1 q$，且$a_1 > 1$，否则a是素数。由于q是a的除1 外的最小正因数，所以$q \leq a_1, q^2 \leq q a_1 = a$，故$q \leq \sqrt{a}$。 □

定理 1.14 若p是一素数，a是任一整数，则$p|a$或$(p, a) = 1$。

证明：因为$(p, a)|p, (p, a) > 0$，由素数的定义，$(p, a) = 1$或$(p, a) = p$。即$(p, a) = 1$ 或$p|a$。 □

推论 1.9 设$a_1, a_2, \cdots, a_n$是$n(n \geq 2)$个整数，p是素数。若$p|a_1 a_2 \cdots a_n$，则$p|a_1, p|a_2, \cdots, p|a_n$中总有一个成立。

证明：假定$a_1, a_2, \cdots, a_n$都不能被p整除，则

$$(p, a_i) = 1, \qquad i = 1, 2, \cdots, n$$

因此，

$$(p, a_1 a_2 \cdots a_n) = 1$$

这与$p|a_1, p|a_2, \cdots, p|a_n$矛盾，故推论得证。 □

定理 1.15 (算术基本定理)任一大于1的整数a能写成素数的乘积，即

$$a = p_1 p_2 \cdots p_n, \qquad p_1 \leq p_2 \leq \cdots \leq p_n \tag{1-20}$$

其中，$p_i(1 \le i \le n)$是素数。并且若

$$a = q_1 q_2 \cdots q_m, \qquad q_1 \le q_2 \le \cdots \le q_m$$

其中，$q_i(1 \le i \le m)$是素数，则$m = n, q_i = p_i, i = 1, 2, \cdots, n$。

证明： 首先，证明分解式的存在性。当$a = 2$时，分解式显然成立。假定对一切小于a 的正整数，分解式都成立，此时若a是素数，则分解式对a成立；若a 是合数，则有两正整数b, c 满足条件

$$a = bc, \qquad 1 < b < a, 1 < c < a$$

由假定

$$b = p_1' p_2' \cdots p_l', \quad c = p_{l+1}' p_{l+2}' \cdots p_n'$$

于是

$$a = p_1' p_2' \cdots p_l' p_{l+1}' p_{l+2}' \cdots p_n'$$

将p_i'的次序适当调整后即得分解式，故分解式对a成立。
其次，证明素因子分解式的唯一性。若对于a有另外一个分解式

$$a = q_1 q_2 \cdots q_m, \qquad q_1 \le q_2 \le \cdots \le q_m$$

其中，$q_i(1 \le i \le m)$是素数。则

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

因此，$p_1 | q_1 q_2 \cdots q_m, q_1 | p_1 p_2 \cdots p_n$。由推论1.9，有$q_i, p_j$使得$p_1 | q_i, q_1 | p_j$。但$p_1, q_i, q_1, p_j$ 都是素数，因此，$p_1 = q_i, q_1 = p_j$。又$p_j \ge p_1, q_j \ge q_1$，所以$q_j = p_1 \le p_j = q_1$，即$p_1 = q_i = q_1$。同理可得$p_2 = q_2$。以此类推，最后即得$n = m$。 □

如果将算术基本定理中的相同素数因子进行合并，则得到下面的推论。

推论 1.10 设a是大于1的整数，则$a = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}, k_i > 0, i = 1, 2, \cdots, n$，其中$p_i(1 \le i \le n)$是素数，而且$p_i < p_j (i < j)$。

注：我们把推论1.10中a的分解式称为**标准分解式**。

推论 1.11 设a,b是两个整数，且$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_k}, b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_n^{\beta_k}$，其中$\alpha_i \geq 0, \beta_i \geq 0), i=1,2,\cdots,k$，则

$$(a,b)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k} \tag{1-21}$$

$$[a,b]=p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k} \tag{1-22}$$

其中$\delta_i=min(\alpha_i,\beta_i), \delta_i=max(\alpha_i,\beta_i), i=1,2,\cdots,k$。

定理 1.16 素数的个数是无穷的。

证明： 用反证法来证明。假定正整数中只有有限个素数。设为$p_1,p_2,\cdots,p_k$。令$p_1p_2\cdots p_k+1=N$，则$N>1$。由定理1.13，N有一个素因数p。这里$p\neq p_i, i=1,2,\cdots,k$，否则$p|p_1p_2\cdots p_k$，又$p|N$，因此$p|1$，矛盾。故，$p$ 是k 个素数以外的素数，因此定理得证。 □

习题

1. 求50!的标准素因子分解表达式。

解： $50!=2^{47}\times 3^{22}\times 5^{12}\times 7^8\times 11^4\times 13^3\times 17^2\times 19^2\times 23^2$
$\times 29\times 31\times 37\times 41\times 43\times 47$

2. 证明：如果$(a,b)=1$，则$(a+b,a-b)=1$或2。

证明： 设$(a+b,a-b)=k$，则有$a+b=km, a-b=kn$，其中m,n是正数，可得

$$a=\frac{m+n}{2}k$$
$$b=\frac{m-n}{2}k$$

若$2\nmid k$，则由上述等式可知k是a,b的公因子。又因为$(a,b)=1$，因此$k|1$，所以$k=1$。
若$2|k$，则由上述等式可知$\frac{k}{2}$是a,b的公因子。又因为$(a,b)=1$，因此$\frac{k}{2}|1$，所以$k=2$。 □

3. 设a,b是正数，且a^2+b^2是3的倍数，证明a,b均是3的倍数。

证明： 用反证法。假设a与b不都是3的倍数，分情况讨论。
若a与b其中一个是3的倍数，而另一个不是，不妨设a是3的倍数。由$b^2=3-a^2$

知b^2 是3 的倍数，知b也是3的倍数，矛盾，故该情况不成立。
若a与b都不是3的倍数，即a和b除以3余1或2，首先研究形如3k+1和3k+2(k是整数)的数。$(3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k)+1$，$(3k+2)^2 = 9k^2+12k+4 = 3(3k^2+4k+1)+1$。故无论哪种情况，$a^2+b^2$除以3余2，不能被3整除，与题设矛盾。
综上所述，a和b都是3的倍数。 □

4. 若$2^n+1(n>1)$是素数，则n是2的方幂。
证明：用反证法证明。设$n = 2^k l$(l为奇数)，则

$$2^n+1 = 2^{2^k l}+1 = (2^{2^k})^l+1 = (2^{2^k}+1)[2^{2^k(l-1)} - 2^{2^k(l-2)} + \cdots + 1]$$

因为$1 < 2^{2^k}+1 < (2^{2^k})^l+1 = 2^n+1$，所以$2^{2^k}+1$是$2^n+1$ 的因数。这与2^n+1是素数矛盾，所以n一定是2的方幂。 □

1.6 扩展知识:《几何原本》和《九章算术》

思路：

1. 辗转相除法出处：

《九章算术》：关于辗转相除法, 搜了一下, 在我国古代的《九章算术》中就有记载，现摘录如下: 约分术曰：可半者半之，不可半者，副置分母、子之数，以少减多，更相减损，求其等也。以等数约之。其中所说的“等数”，就是最大公约数。求“等数”的办法是“更相减损”法，实际上就是辗转相除法。

《几何原本》英文版第VII卷命题i和ii：$http://aleph0.clarku.edu/\ djoyce/java/elements/bookVII/propVII1.html$

2. 介绍两本中西方的教材概况，介绍作者概况，主要讲欧几里得

3. 从两本教材引申中西方数学思想：中国注重实用，寓理于算；西方注重逻辑演绎。可参考该篇文章：几何原本VS九章算术，中西数学的差别在哪里？

第 2 章　不定方程

所谓不定方程，是指未知数的个数多于方程的个数，并且方程的解受到某种限制(如整数或正整数等)的方程或方程组。古希腊人丢番图于公元3世纪初在他著作《算术》中就研究过这样的方程，所以不定方程又称为丢番图方程。实际上，根据史书记载，我国数学家对不定方程的研究要比丢番图早许多年。公元1世纪的《九章算术》第八章方程第十三题的“五家共井”的问题就是一个不定方程组问题，公元5世纪的《张丘建算经》的百鸡问题标志着中国对不定方程理论有了系统研究。

2.1 二元一次不定方程

二元一次不定方程是指

$$ax + by = c \tag{2-1}$$

其中，a, b, c是给定的整数，$ab \neq 0$。

定理 2.1 二元一次不定方程$ax + by = c$(a, b, c是整数)有整数解的充分必要条件是$d|c$，这里$d = (a, b)$。如果设$x = x_0, y = y_0$是方程的一个解，那么它的任意解可以表示成

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t \tag{2-2}$$

其中t是任意整数。

证明： 首先证明定理的前一个论断。既然x_0, y_0是方程的解，当然满足$ax_0 + by_0 = c$。因此

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = c + (a \cdot \frac{b}{d} - b \cdot \frac{a}{d})t = c$$

这说明式2-2是方程的解。定理的必要条件得证。

下面证明充分性。设x', y'是方程的任一解，则$ax' + by' = c$，与$ax_0 + by_0 = c$相减，即得

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

由$(a,b)=d$，可设$a=a_1d, b=b_1d$代入上式，两边消掉d得到

$$b_1(y'-y_0)=-a_1(x'-x_0)$$

又$d=(a,b)$，所以$(a_1,b_1)=1$。又$b_1|-a_1(x'-x_0)$，所以$b_1|(x'-x_0)$，故设$x'-x_0=b_1t$，其中t为整数，即$x'=x_0+b_1t=x_0+\frac{b}{d}t$。将$x'$代入上式

$$b_1(y'-y_0)=-a_1(x_0+b_1t-x_0)$$

整理可得$y'=y_0-a_1t=y_0-\frac{a}{d}t$。定理得证。 □

由定理2.1可知，解二元一次不定方程的步骤可分为三步：

(1) 求解$d=(a,b)$，判断d是否满足$d|c$，确定方程是否有解；

(2) 若方程有解，求解方程的一组解x_0,y_0;

(3) 写出方程所有的解$x=x_0+\frac{b}{d}t, y=y_0-\frac{a}{d}t$。

步骤(1)可利用第一章介绍的辗转相除法来求解d，从而判断方程是否有解。繁琐的是步骤(2)，同样可利用第一章所学习过的知识。由推论1.6可知存在u,v 满足

$$d=(a,b)=au+bv$$

上式左右两侧同乘$\frac{c}{d}$，可得

$$d\cdot\frac{c}{d}=au\cdot\frac{c}{d}+bv\cdot\frac{c}{d}$$

整理可得

$$c=a\cdot u\frac{c}{d}+b\cdot v\frac{c}{d}$$

对比不定方程的形式可得到方程的一组解，$x_0=u\frac{c}{d}, y_0=v\frac{c}{d}$，其中$u,v$ 可利用扩展的欧几里得算法可求解u,v。最后，代入步骤(3)的公式可得方程全部解。

例 2.1 解二元一次不定方程$312x+753y=345$。

解：按照定理2.1，首先求出$(312,753)$，判断是否能够整除345。先作辗转相除

法

$$\begin{aligned}
753 &= 312 \times 2 + 129 \\
312 &= 129 \times 2 + 54 \\
129 &= 54 \times 2 + 21 \\
54 &= 21 \times 2 + 12 \\
21 &= 12 \times 1 + 9 \\
12 &= 9 \times 1 + 3 \\
9 &= 3 \times 3
\end{aligned}$$

所以，$d = (753, 312) = 3$，而由3|345知方程有解。第二步求解方程的一组解，利用扩展的欧几里得算法，回代：

$$\begin{aligned}
3 &= 12 \times 2 - 21 = (54 - 21 \times 2) \times 2 - 21 = 54 \times 2 - 21 \times 5 \\
&= 54 \times 2 - (129 - 54 \times 2) \times 5 = 54 \times 12 - 129 \times 15 \\
&= (312 - 129 \times 2) \times 12 - 129 \times 5 = 312 \times 12 - 129 \times 29 \\
&= 312 \times 12 - (753 - 312 \times 2) \times 29 = 312 \times 70 + 753 \times (-29)
\end{aligned}$$

由于$345 \div 3 = 115$，所以

$$x_0 = 70 \times 115 = 8050, y_0 = -29 \times 115 = -3335$$

因此，二元一次不定方程的全部解为

$$\begin{aligned}
x &= x_0 + \tfrac{b}{d}t = 8050 + \tfrac{753}{3}t = 8050 + 251t, \\
y &= y_0 - \tfrac{a}{d}t = -3335 - \tfrac{312}{3}t = 3335 - 104t
\end{aligned}$$

其中t 为任意整数。

例 2.2 求解$-15x + 25y = -100$

解：首先求解$(-15, 25) = (15, 25)$，

$$\begin{aligned}
25 &= 15 \times 1 + 10 \\
15 &= 10 \times 1 + 5 \\
10 &= 5 \times 2
\end{aligned}$$

因此，$(-15,25)=5$，且$5|-100$，则方程有解。利用扩展的欧几里得算法，有

$$5=15-10=15-(25-15)=15\times 2-25\times 1=(-15)\times(-2)+25\times(-1)$$

因此，$x_0=(-2)\times\frac{-100}{5}=40$，$y_0=(-1)\times\frac{-100}{5}=20$。所以方程全部解为$x=40+5t,y=20+3t$，其中$t$为任意整数。

习题

1. 求解$22x+30y=14$。

解：

$$\begin{aligned}30&=22\times 1+8\\22&=8\times 2+6\\8&=6\times 1+2\\6&=2\times 3\end{aligned}$$

因此，$(22,30)=2$，又$2|14$，所以方程有解。

$$2=8-6=8-(22-8\times 2)=8\times 3-22=(30-22)\times 3-22=30\times 3+22\times(-4)$$

因此，$x_0=(-4)\times 7=-28$，$y_0=3\times 7=21$。所以$x=-28+15t,y=21-11t$，其中t为任意整数。

2. 求解$306x-360y=630$。

解：

$$\begin{aligned}360&=306\times 1+54\\306&=54\times 5+36\\54&=36\times 1+18\\36&=18\times 2\end{aligned}$$

因此，$(306,-360)=(306,360)=18$，又$18|630$，所以方程有解。

$$\begin{aligned}18&=54-36=54-(306-54\times 5)=54\times 6-306=(360-306)\times 6-306\\&=306\times(-7)+360\times 6=306\times(-7)-360\times(-6)\end{aligned}$$

因此，$x_0=(-7)\times 35=-245$，$y_0=(-6)\times 35=-210$。所以$x=-245-20t,y=-210-17t$，其中t为任意整数。

2.2 多元一次不定方程

多元一次不定方程就是可以下列形式的方程：

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N \tag{2-3}$$

其中，$a_1, a_2, \cdots, a_n, N$都是整数，$n \geq 2$，并且不失一般性，可以假定$a_1, a_2, \cdots, a_n$都不等于零。

定理 2.2 不定方程$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$有整数解的充分必要条件是$(a_1, a_2, \cdots, a_n)|N$。

证明： 设$(a_1, a_2, \cdots, a_n) = d$。首先证明定理的必要性。如果方程有解，则存在整数组$(s_1, s_2, \cdots, s_n)$满足

$$a_1s_1 + a_2s_2 + \cdots + a_ns_n = N$$

所以，$d|a_1s_1 + a_2s_2 + \cdots + a_ns_n$，即有$d|N$，必要条件得证。

其次，证明定理的充分性。因为$(a_1, a_2, \cdots, a_n) = d$，而且很容易将推论1.6推广到有限个整数的情况，所以，存在整数组$b_1, b_2, \cdots, b_n$ 满足

$$a_1b_1 + a_2b_2 + \cdots + a_nb_n = d$$

由于$(a_1, a_2, \cdots, a_n)|N$，可以设$N = dc$，于是

$$a_1b_1c + a_2b_2c + \cdots + a_nb_nc = dc = N$$

即整数组$(b_1c, b_2c, \cdots, b_nc)$是方程的解。 □

定理2.2提供了一个求解$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$的方法，即先顺次求出$(a_1, a_2) = d_2, (d_2, a_3) = d_3, \cdots, (d_{n-1}, a_n) = d_n$，若$d_n|c$，则$n$元一次不定方程

有解。做方程组

$$\begin{cases} a_1x_1 + a_2x_2 = d_2t_2 \\ d_2t_2 + a_3x_3 = d_3t_3 \\ \cdots \\ d_{n-2}t_{n-2} + a_{n-1}x_{n-1} = d_{n-1}t_{n-1} \\ d_{n-1}t_{n-1} + a_nx_n = c \end{cases}$$

首先求出最后一个方程的一切解，然后把t_{n-1}的每一个值带入倒数第二个方程，求出他的一切解，这样做下去即可得出n元一次不定方程的一切解。

在实际解n元一次不定方程时，常把t_i看成常数，求出上面方程组第$i-1$个方程的整数解的一般形式，再从结果中消去$t_2, t_3, \cdots, t_{n-1}$，即可得$n$元一次不定方程的解。

例 2.3 求解不定方程$50x + 45y + 36z = 10$。

解： 因为$(50, 45) = 5, (5, 36) = 1$，又$1|10$，所以此方程有解，原方程可以化为

$$\begin{cases} 50x + 45y = 5t \\ 5t + 36z = 10 \end{cases} \text{即} \begin{cases} 10x + 9y = t \\ 5t + 36z = 10 \end{cases}$$

这里t是参数，在第一个方程中，把t看作常量，在第二个方程中，又把t看作变量，分别解之，得

$$\begin{cases} x = t + 9k_1 \\ y = -t - 10k_1 \end{cases} \text{和} \begin{cases} t = -70 + 36k_2 \\ z = 10 - 5k_2 \end{cases}$$

这里k_1, k_2是任意整数，消去t得到原方程的通解。

$$\begin{cases} x = -70 + 9k_1 + 36k_2 \\ y = 70 - 10k_1 - 36k_2 \\ z = 10 - 5k_2 \end{cases}$$

例 2.4 解不定方程$6x + 15y + 21z + 9w = 30$

解： 原不定方程可以化为

$$2x + 5y + 7z + 3w = 10$$

因为$(2,5)=1,(1,7)=1,(1,3)=1$，又$1|10$，所以原不定方程有解，可以转化为

$$\begin{cases} 2x+5y=t_1 \\ t_1+7z=t_2 \\ t_2+3w=10 \end{cases}$$

这里t_1,t_2是参数，在方程的左边把它们看作变量，在方程的右边把他们看作是常量，分别解之，得

$$\begin{cases} x=3t_1+5k_1 \\ y=-t_1-2k_1 \end{cases} \quad \begin{cases} t_1=-6t_2+7k_2 \\ z=t_2-k_2 \end{cases} \quad \begin{cases} t_2=1+3k_3 \\ w=3-k_3 \end{cases}$$

这里k_1,k_2,k_3是任意整数，消去t_1,t_2得原不定方程的解

$$\begin{cases} x=-18+5k_1+21k_2-54k_3 \\ y=6-2k_1-7k_2+18k_3 \\ z=1-k_2+3k_3 \\ w=3-k_3 \end{cases}$$

考虑由m个n元一次不定方程组成的方程组，其中$m<n$，可以消去$m-1$个未知数，从而也就消去了$m-1$个不定方程式，将方程转化为一个$n-m+1$元的一次不定方程。因此，在掌握了一次不定方程有关解法的基础上，可以研究一次不定方程组的解法。

例 2.5 解不定方程组

$$\begin{cases} 2x-y-2z+4w=10 \\ 4x+y-4z-2w=-14 \\ 3x+4y-z+w=12 \end{cases}$$

解：先通过方程组前两式消去w，可得

$$10x+y-10z=-18$$

再利用方程组后两式消去w，可得

$$10x + 9y - 6z = 10$$

上述两式再消去x，化简可得

$$2y + z = 7$$

解之得

$$\begin{cases} y = t_1 \\ z = 7 - 2t_1 \end{cases}$$

其中t_1是整数，进一步可得

$$10x + 21t_1 = 52$$

解之得

$$\begin{cases} x = 1 + 21t_2 \\ t_1 = 2 - 10t_2 \end{cases}$$

其中，t_2是整数。将t_1代入y, z，可得

$$\begin{cases} y = 2 - 10t_2 \\ z = 3 + 20t_2 \end{cases}$$

将x, y, z代入原不定方程组，可得$w = 4 - 3t_2$。所以，原不定方程组的解为

$$\begin{cases} x = 1 + 21t_2 \\ y = 2 - 10t_2 \\ z = 3 + 20t_2 \\ w = 4 - 3t_2 \end{cases}$$

例 2.6 (百鸡问题)鸡翁一，值钱五，鸡母一，值钱三，鸡雏三，值钱一。百钱买百鸡，问鸡翁、母、雏各几何？
(译文：每只大公鸡售价为五个钱，每只母鸡售价三个钱，每三只小鸡售价一个钱。现有100 个钱，问公鸡、母鸡和小鸡各应买几只？)

解：设公鸡、母鸡和小鸡的只数分别为x, y, z，故得

$$\begin{cases} 15x + 9y + z = 300 \\ x + y + z = 100 \end{cases}$$

消去z得

$$7x + 4y = 100$$

因为$x_0 = -100, y_0 = 200$是$7x + 4y = 100$的一组解，故

$$\begin{cases} x = -100 - 4t \\ y = 200 + 7t \end{cases}$$

其中，t为任意的整数。代入$x + y + z = 100$，得$z = -3t$。所以元不定方程组的全部解为

$$\begin{cases} x = -100 - 4t \\ y = 200 + 7t \\ z = -3t \end{cases}$$

根据题意，x, y, z均为非负整数。因此，

$$x = -100 - 4t \geq 0, y = 200 + 7t \geq 0, z = -3t \geq 0$$

得$-28 \leq t \leq -25$。因此，得4组解如下：

t	x	y	z
-28	12	4	84
-27	8	11	81
-26	4	18	78
-25	0	25	75

例 2.7 背包公钥密码

背包问题：有物品若干及背包一个，由于背包太小，不能将所有物品放入，问如何选择部分物品放入，能使背包的容积得到最充分的利用。

将背包问题稍加演变，给定n个正整数$a_1, a_2, \cdots, a_n$及一个正整数s，已知s是某一些a_i之和，确定这些a_i，这就是密码学的背包问题。从$a_1, a_2, \cdots, a_n$中

选出一个子集，很容易算出这个子集之和。但反过来，给定一个自己的个数之和，要确定这个子集，一般来说就很困难了。

利用背包问题可以得到背包公钥密码：将$a_1, a_2, \cdots, a_n$作为公开密钥，设$(m_1, m_2, \cdots, m_n)$为明文，$m_i = 0$或1，令$s = \sum_{i=1}^{n} m_i a_i$，将$s$作为密文，它是$a_1, a_2, \cdots, a_n$的一个部分和。从$s$求解明文$(m_1, m_2, \cdots, m_n)$就相当于解背包问题。不过对于一般的$a_1, a_2, \cdots, a_n$，即使合法的接收方也同样难于解密，所以不能用一半的$a_1, a_2, \cdots, a_n$设计密码。在下面一个特殊情况，背包问题将变得很容易解。设

$$a_1 < a_2, a_1 + a_2 < a_3, \cdots, a_1 + a_2 + \cdots + a_{n-1} < a_n$$

即前面一段数之和小于紧跟其后的一个数，这时称$a_1, a_2, \cdots, a_n$为超递增序列。设$a_1, a_2, \cdots, a_n$为超递增的，如以它为公开钥，以$s = \sum_{i=1}^{n} m_i a_i$作为明文$(m_1, m_2, \cdots, m_n)$的密文，则由于$a_1, a_2, \cdots, a_n$为公开钥，利用一次不定方程，任何人都会从$s$解出$(m_1, m_2, \cdots, m_n)$。所以这样做是不行的，必须设法将$a_1, a_2, \cdots, a_n$隐藏起来。

2.3 扩展知识:《算术》与丢番图

来源：豆丁丢番图和不定方程

习题

1. 求解$9x + 24y - 5z = 1000$。

解：因为$(9, 24) = 3, (3, -5) = 1$，故方程有解。原方程可以化为

$$\begin{cases} 9x + 24y = 3t \\ 3t - 5z = 1000 \end{cases} \text{即} \begin{cases} 3x + 8y = t \\ 3 - 5z = 1000 \end{cases}$$

分别求解可得

$$\begin{cases} x = 3t - 8k_1 \\ y = -t + 3k_1 \end{cases} \quad \begin{cases} t = 2000 + 5k_2 \\ z = 1000 + 3k_2 \end{cases}$$

其中，k_1, k_2是整数。消去t可得

$$\begin{cases} x = 6000 - 8k_1 + 15k_2 \\ y = -2000 + 3k_1 - 5k_2 \\ z = 1000 + 3k_2 \end{cases}$$

2. 解多元一次不定方程$12x + 6y - 5z = 13$。

解：由于$(12, 6) = 6, (6, -5) = 1, 1|13$，所以方程有解。原方程转化为

$$\begin{cases} 12x + 6y = 6w \\ 6w - 5z = 13 \end{cases} \text{即} \begin{cases} 2x + y = w \\ 6w - 5z = 13 \end{cases}$$

分别解之得

$$\begin{cases} x = w + t \\ y = -w - 2t \end{cases} \quad \begin{cases} w = 3 - 5s \\ z = 1 - 6s \end{cases}$$

原不定方程的解为

$$\begin{cases} x = 3 - 5s + t \\ y = -3 + 5s - 2t \\ z = 1 - 6s \end{cases}$$

其中s, t都是整数。

3. 21世纪有这样的年份，这个年份减去1等于它各个数字和的404倍，求这个年份。

解：设该年份的十位数为x，个位数为y，根据题意可得

$$2000 + 10x + y - 1 = 404(2 + x + y)$$

整理得

$$394x + 403y = 1191$$

因为$(394, 403) = 1$，所以方程有解。解得

$$\begin{cases} x = 179 \times 1191 - 403t \\ y = -175 \times 1191 + 394t \end{cases}$$

其中t为整数。又$0 \leq x \leq 9, 0 \leq y \leq 9$，所以

$$\begin{cases} 0 \leq 179 \times 1191 - 403t \leq 9 \\ 0 \leq -175 \times 1191 + 394t \leq 9 \end{cases}$$

又因为t为整数，解得$t = 529$。所以$x = 2, y = 1$。因此该年份为2021。

4. 取1分、2分、5分的硬币共10枚，需付1角8分钱，问有几种不同取法。

解：设1分、2分、5分的硬币分别为x枚、y枚、z枚，依题意得方程组

$$\begin{cases} x + y + z = 10 \\ x + 2y + 5z = 18 \end{cases}$$

消去z，整理可得$4x + 3y = 32$，解得

$$\begin{cases} x = 32 - 3t \\ y = -32 + 4t \end{cases}$$

其中t为整数。将x, y代入不定方程组，可得$z = 10 - t$。又$x \geq 0, y \geq 0, z \geq 0$，因此$8 \leq t \leq 10$。所有$t$分别取$8, 9, 10$对应三种取法

$$\begin{cases} x = 8 \\ y = 0 \\ z = 2 \end{cases} \quad \begin{cases} x = 5 \\ y = 4 \\ z = 1 \end{cases} \quad \begin{cases} x = 2 \\ y = 8 \\ z = 0 \end{cases}$$

第 3 章　同余

日常生活中有很多周期性事物，如每天24小时一循环，每周7天一循环，我国的生肖每12年一循环，古代的干支纪年每60年一循环。假设这个月1号是周一，当需要明确30号是周几的时候，实际上我们关注的是30除以7之后得到的余数。这样，就产生了同余的概念。本章首先介绍同余的概念和性质，进而介绍剩余类和欧拉函数，然后建立两个著名的定理。

3.1 同余的概念和性质

定义 3.1 给定一个正整数m，如果用m去除两个整数a,b所得的余数相同，则称a,b对模数m**同余**，并称$a \equiv b(mod\ m)$为**同余式**。如果用m去除两个整数a,b所得的余数不同，则称a,b对模数m不同余，记作$a \not\equiv b(mod\ m)$。

定理 3.1 整数a和b模m同余的充要条件是$m|a-b$。

证明：首先证明必要性。设$a = mq_1 + r_1, b = mq_2 + r_2, 0 \le r_1 \le m, 0 \le r_2 \le m$。

若$a \equiv b(mod\ m)$，则$r_1 = r_2$。所以$a - b = m(q_1 - q_2)$，因此$m|a-b$。

接着证明充分性。由上述假设可得$a-b = m(q_1-q_2)+(r_1-r_2)$，若$m|a-b$，则$m|r_1 - r_2$。

又因为$0 \le |r_1 - r_2| < m$，所以$r_1 - r_2 = 0$，即$r_1 = r_2$。故$a \equiv b(mod\ m)$。

例 3.1 每一个整数a恰与$0, 1, 2, \cdots, m-1$中的某一个数对于模m同余。

证明：对于a和m有且只有两个整数q和r，使

$$a = mq + r, 0 \le r < m$$

即$a - r = mq$，所以$m|a-r$，即$a \equiv r(mod\ m)0 \le r < m$。

由于q和r是唯一确定的，因此结论成立。 □

由第一章知道，若$m|a-b \Leftrightarrow$存在整数t，使$a - b = mt$，即$a = mt + b$。因此，

$$a \equiv b(mod\ m) \Leftrightarrow m|a-b \Leftrightarrow a = b + mt, t\text{为整数}$$

上述等价关系是整数的同一性质的不同表述形式而已，因而在以后的应用中三者可以不加区别的交换使用。但是，同余式在讨论整数整除问题比整除符号及带余除式方便有效。

定理 3.2 同余是整数间的一种等价关系，即有

(1)自反性：$a \equiv a(mod\ m)$;

(2)对称性：若$a \equiv b(mod\ m)$，则$b \equiv a(mod\ m)$；

(3)传递性：若$a \equiv b(mod\ m), b \equiv c(mod\ m)$，则$a \equiv c(mod\ m)$。

证明：

(1)因为$a - a = 0, m|0$，所以$m|a - a$，即$a \equiv a(mod\ m)$。

(2)因为$m|a - b$，所以$m|b - a$，即$b \equiv a(mod\ m)$。

(3)由$m|a-b, m|b-c$，得$m|(a-b)+(b-c)$，即$m|a-c$，所以$a \equiv c(mod\ m)$。

□

定理 3.3 设$a \equiv b(mod\ m), c \equiv d(mod\ m)$，则

$$a \pm c \equiv b \pm d(mod\ m), \quad ac \equiv bd(mod\ m), \quad at \equiv bt(mod\ m)$$

其中t为任意整数。

证明：因为$m|(a-b), m|(c-d)$，所以$m|(a-b) \pm (c-d)$，即$m|(a \pm c) - (b \pm d)$，因此$a \pm c \equiv b \pm d(mod\ m)$。

再因为$m|(a-b)$，所以$m|(a-b)t = (at - bt)$，因此$at \equiv bt(mod\ m)$。

又$a \equiv b(mod\ m)$，所以$ac \equiv bc(mod\ m)$。由$c \equiv d(mod\ m)$，由$bc \equiv bd(mod\ m)$，所以$ac \equiv bd(mod\ m)$。 □

特别地，如果$a \equiv b(mod\ m)$，则对于任意整数n，有

$$a^n \equiv b^n(mod\ m)$$

定理 3.4 设$ca \equiv cb(mod\ m)$，并且$(c, m) = 1$，则$a \equiv b(mod\ m)$。

证明：因为$m|c(a-b)$，而$(c, m) = 1$，因此$m|(a-b)$，即$a \equiv b(mod\ m)$ □

定理 3.5 设$ca \equiv cb(mod\ m)$，并且$(c,m)=d$，则$a \equiv b(mod\ \frac{m}{d})$。

证明： 因为$m|c(a-b)$，有$\frac{m}{d}|\frac{c}{d}(a-b)$。但是$(\frac{c}{d},\frac{m}{d})=1$，所以$\frac{m}{d}|(a-b)$，即定理结论成立。 □

定理 3.6 设$a \equiv b(mod\ m)$，k为正整数，则$ka \equiv kb(mod\ km)$。

证明： 由$a \equiv b(mod\ m)$，知$m|a-b$，从而$km|k(a-b)$，即$km|ka-kb$。所以，$ka \equiv kb(mod\ km)$，故结论成立。 □

定理 3.7 设$a \equiv b(mod\ m), a \equiv b(mod\ n)$。若$k=[m,n]$,则$a \equiv b(mod\ k)$。

证明： 因为$m|(a-b), n|(a-b)$，所以$a-b$是m,n的公倍数，于是$k|(a-b)$，即有$a \equiv b(mod\ k)$。 □

例 3.2 试证明一个整数能被3整除的充分必要条件是它的10进位数码的和能被3 整除。

证明： 设a是一正整数，并将a写成10进位数的形式

$$a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_0, \quad 0 \le a_i < 10$$

因为$10 \equiv 1(mod\ 3)$，所以

$$a \equiv a_n + a_{n-1} + \cdots + a_0 (mod\ 3)$$

因此，$3|a$当且仅当$3|a_n + a_{n-1} + \cdots + a_0$。 □

同样也可以证明：一个整数能被9整除的充分必要条件是它的10进位数码的和能被9 整除。

例 3.3 由于整数123456789的各位数码的和为$1+2+\cdots+9=45$，它能被3和9整除，所以123456789能被3和9整除。

例 3.4 求3^{123}写成十进制数时的个位数。

解： 按题意应确定a，使$3^{123} \equiv a(mod\ 10)$，其中$0 \le a \le 9$。可先确定$n$，使$3^n \equiv 1(mod\ 10)$。

因为$3^2 \equiv 9 \equiv -1(mod\ 10)$，两边同时进行平方运算可得$3^4 \equiv 1(mod\ 10)$。又$(3^4)^{30} \equiv 1^{120}(mod\ 10)$，即$3^{120} \equiv 1(mod\ 10)$，所以$3^{123} \equiv 3^{120} \cdot 3^3 \equiv 3^3 \equiv 7(mod\ 10)$。即所求的个位数是7。

例 3.5 求所有能使$2^n - 1$被7整除的正整数n

解：本题实际上求满足$2^n \equiv 1(mod\ 7)$的所有正整数n。

因为$2^3 \equiv 1(mod\ 7)$，所以$2^{3k} \equiv 1(mod\ 7)$，其中k为正整数。

又当$n = 3k + 1$和$n = 3k + 2$时，有

$$2^{3k+1} \equiv 2^{3k} \cdot 2 \equiv 1 \cdot 2 \equiv 2(mod\ 7)$$
$$2^{3k+2} \equiv 2^{3k} \cdot 2^2 \equiv 1 \cdot 2^2 \equiv 4(mod\ 7)$$

故只有当$n = 3k$时，$2^n \equiv 1(mod\ 7)$，即$7|2^n - 1$。

例 3.6 求4除$1^3 + 2^3 + \cdots + 99^3 + 100^3$所得的余数。

解：在100项和数中，底数是偶数的各项幂，对模4都与零同余，因而求和数对模4的余数，只需考虑奇数为底的幂，共50项，即

$$1^3 + 3^3 + \cdots + 99^3$$

这50项的底对模4，仅与$+1$和-1同余，幂指数3是奇数，所以它们是依次$+1, -1$排列，恰好各占半数，它们的和也是零。因此

$$\begin{aligned} & 1^3 + 2^3 + \cdots + 99^3 + 100^3 \\ \equiv\ & (1^3 + 3^3 + \cdots + 99^3) + (2^3 + 4^3 + \cdots + 100^3) \\ \equiv\ & (1^3 + 3^3 + \cdots + 99^3)(mod\ 4) \\ \equiv\ & 1 - 1 + 1 - \cdots - 1(mod\ 4) \\ \equiv\ & 0(mod\ 4) \end{aligned}$$

习题：

1. 举例说明

(1)由$a^2 \equiv b^2(mod\ m)$，不能推出$a \equiv b(mod\ m)$；

(2)由$a \equiv b(mod\ m)$，不能推出$a^2 \equiv b^2(mod\ m^2)$；

解：只给出一例

(1)$1^2 \equiv 2^2(mod\ 3)$，但$1 \not\equiv 2(mod\ 3)$；

(2)$1 \equiv 6(mod\ 5)$，但$1^2 \not\equiv 6^2(mod\ 5^2)$.

2. 求2^{100}的十进制数表示中的个位数。

解：因为$2^4 \equiv 6(mod\ 10)$，所以$(2^4)^{25} \equiv 6^{25}(mod\ 10)$。又因为6的任何幂次模10都是得6，因此$2^{100}$的十进制数的个位数是6。

3. 已知2021年元旦是周五，问这一天以后的第2^{2021}天是周几？

解：因为$2^3 \equiv 1(mod\ 7)$，所以$(2^3)^{673} \equiv 1(mod\ 7)$。又$2^{2021} \equiv (2^3)^{673} \cdot 2^2 \equiv 4(mod\ 7)$，所以第$2^{2021}$天是周二。

4. 若$69, 90$和125关于某数d同余，证明：对于d，81和4同余。

证明：因为$69, 90$和125关于某数d同余，所以$d|(90-69), d|(125-90)$，又$81-4 = 77 = 2(90-69)+(125-90)$，因此$d|(81-4)$，从而81和4对模$d$同余。

3.2 剩余类与欧拉函数

上节介绍了同余的概念，就可以把余数相同的数放在一起，这样就产生了剩余类的概念。本节的目的就是讨论剩余类以及与剩余类有关的性质。

定义 3.2 对于模m，与已知整数a同余的所有整数构成的集合，称为模m的**剩余类**(也称同余类)，记作$[a]_m$，也就是说

$$[a]_m = \{x | x \equiv a(mod\ m), x \in \mathbb{Z}\}$$

因此，模m的m个剩余类可表示为：$[0]_m, [1]_m, [2]_m, \cdots, [m-1]_m$。

例如，$m = 3$，有下面3个剩余类：

$$[0]_3 = \{\cdots, -6, -3, 0, 3, 6, \cdots\};$$
$$[1]_3 = \{\cdots, -5, -2, 1, 4, 7, \cdots\};$$
$$[2]_3 = \{\cdots, -4, -1, 2, 5, 8, \cdots\}。$$

定义 3.3 从模m的每一个剩余类中各取一个数所得到的的m个数，称为模m的**完全剩余系**。

显然，模m有无数个完全剩余系。特别地，把$0, 1, 2, \cdots, m-1$称为模m的最小非负完全剩余系，因为它们分别是模m的m个剩余类

$$[0]_m, [1]_m, [2]_m, \cdots, [m-1]_m$$

中的最小非负数(称为模m的最小非负剩余)。

定理 3.8 整数$a_1, a_2, \cdots, a_k$是模m的完全剩余系的充分必要条件是

(1) $k = m$;

(2) $a_i \not\equiv a_j (mod\ m)(i \neq j)$。

证明：首先证明充分性。因整数$a_1, a_2, \cdots, a_k$这k个数对于模m两两不同余，所以它们应分别属于m个不同的剩余类。又$k = m$，因此它们是模m的一个完全剩余系。

其次证明必要性。如果整数$a_1, a_2, \cdots, a_k$是模m的完全剩余系，那么它们应取自m个不同的剩余类，因此$k = m$，其$a_i \not\equiv a_j (mod\ m)(i \neq j)$。 □

例 3.7 试证：$-11, -4, 18, 20, 32$是模5的一个完全剩余系。

解：根据定理3.8只需判定这五个数两两不同余，为此应利用同余将这些数转化为模5的最小非负剩余。如果所得的最小非负剩余互不相同，那么可以判定所给五个数两两不同余。

$$-11 \equiv 4(mod\ 5), -4 \equiv 1(mod\ 5), 18 \equiv 3(mod\ 5)$$

$$20 \equiv 0(mod\ 5), 32 \equiv 2(mod\ 5)$$

可知$-11, -4, 18, 20, 32$这五个数对于模5两两不同余。因此，它们是模5的一个完全剩余系。

定理 3.9 若$a_1, a_2, \cdots, a_m$是模m的完全剩余系，且$(a, m) = 1$，b为任意整数，则$aa_1 + b, aa_2 + b, \cdots, aa_m + b$也是模$m$的完全剩余系。

证明：由定理3.8，只要证明$aa_i + b \not\equiv aa_j + b(mod\ m), i \neq j$即可。下面利用反证法证明，假如$aa_i + b = aa_j + b(mod\ m), i \neq j$。那么$aa_i \equiv aa_j (mod\ m), a_i \equiv a_j (mod\ m)$，这与$a_1, a_2, \cdots, a_m$是模$m$的完全剩余系矛盾。因此，定理得证。

例 3.8 试证：$3, 8, 13, 18$是模4的一个完全剩余系。

解：本题利用定理3.9证明。因为$0, 1, 2, 3$是模4的一个完全剩余系，而$3 = 5 \times 0 + 3, 8 = 5 \times 1 + 3, 13 = 5 \times 2 + 3, 18 = 5 \times 3 + 3$，且$(5, 4) = 1$。所以，3.9是模4的一个完全剩余系。 □

定义 3.4 在模m的一个完全剩余系中，与m互质的数的全体称为模m的一个**既约剩余系**，也称**既约剩余系**。

例如，模8的完全剩余系为{0,1,2,3,4,5,6,7}，而模8的既约剩余系为{1,3,5,7}。

为了讨论模m的既约剩余系，引进一个重要的函数－－－－Euler函数。

定义 3.5 设m是一个正整数，Euler函数$\varphi(m)$表示所有不大于m且与m互素的正整数的个数。

定理 3.10 k个整数$x_1, x_2, \cdots, x_k$是模m的既约剩余系的充分必要条件是

(1) $k = \varphi(m)$;

(2) $x_i \not\equiv x_j (mod\ m), i \neq j$;

(3) $(x_i, m) = 1, i = 1, 2, \cdots, k$。

例 3.9 验证$3, 9, 21, 27, 33, 39, 51, 57$是模20的一个既约剩余系。

证明： 模20的最小既约剩余系：$1, 3, 7, 9, 11, 13, 17, 19$。而

$$3 \equiv 3(mod\ 20), 9 \equiv 9(mod\ 20), 21 \equiv 1(mod\ 20), 27 \equiv 7(mod\ 20)$$

$$33 \equiv 13(mod\ 20), 39 \equiv 19(mod\ 20), 51 \equiv 11(mod\ 20), 57 \equiv 17(mod\ 20)$$

可见，$3, 9, 21, 27, 33, 39, 51, 57$这8个数与模20的最小既约剩余系分别同余，所以它们也是模20的一个既约剩余系。 □

定理 3.11 若$x_1, x_2, \cdots, x_{\varphi(m)}$是模$m$的一个既约剩余系，且$(a, m) = 1$，则$ax_1, ax_2, \cdots, ax_{\varphi(m)}$也是模$m$的既约剩余系。

证明： 因为

$$x_i \not\equiv x_j (mod\ m), (a, m) = 1$$

所以

$$ax_i \not\equiv ax_j (mod\ m), i \neq j, i, j = 1, 2, \cdots, \varphi(m)$$

又因$(x_i, m) = 1, (a, m) = 1$,所以$(ax_i, m) = 1, i = 1, 2, \cdots, \varphi(m)$。由定理3.10可知，$ax_1, ax_2, \cdots, ax_{\varphi(m)}$也是模$m$的一个既约剩余系。 □

下面给出计算Euler函数$\varphi(m)$的一般公式。

引理 3.6 若p是素数，k是自然数，则

$$\varphi(p^k) = p^k(1 - \frac{1}{p})$$

证明：在p^k的完全剩余系中与p^k 不互素的数只有p的倍数

$$p, 2p, \cdots, p^{k-1}p$$

共有p^{k-1}个，其余$p^k - p^{k-1} = p^k(1-\frac{1}{p})$个数与$p^k$互素，因此$p^k$的既约剩余系含有$p^k(1-\frac{1}{p})$个数，即$\varphi(p^k) = p^k(1-\frac{1}{p})$。 □

根据引理3.6,有$\varphi(3) = 2, \varphi(3^2) = 3^2 \times (1-\frac{1}{3}) = 6, \varphi(3^3) = 3^3 \times (1-\frac{1}{3}) = 18$。

引理 3.7 设$(a,b) = 1$，则$\varphi(ab) = \varphi(a)\varphi(b)$。

证明：既然欧拉函数来源于既约剩余系，可以考虑转化为既约剩余系的问题来解决。于是，该引理的意思就是：若a,b互质，则模ab的既约剩余系中数的个数等于模a和模b的既约剩余系中数的个数之积。因此，证明的关键是确定模ab的一个既约剩余系，因此从模a,b的既约剩余系出发。

假设$x_1, \cdots, x_{\varphi(a)}, y_1, \cdots, y_{\varphi(b)}$分别是$a,b$的既约剩余系，构造数组

$$bx_i + ay_j, i = 1, \cdots, \varphi(a), j = 1, \cdots, \varphi(b) \tag{3-1}$$

显然，含有$\varphi(a)\varphi(b)$个数。下面用反证法来证明数组3-1是模ab的既约剩余系即可。

设

$$bx_i + ay_j \equiv bx_k + ay_s (mod\ ab)$$

其中i与k,j与s至少有一对互异。于是存在整数t_1和t_2，使得：

$$\begin{aligned} bx_i + ay_j &= abt_1 + r \\ bx_k + ay_s &= abt_2 + r \end{aligned}$$

其中r是两个带余除法相同的余数，进而：

$$\begin{aligned} bx_i &= abt_1 - ay_j + r \\ bx_k &= abt_2 - ay_s + r \end{aligned}$$

可见，bx_i和bx_k关于a是同余的，即：

$$bx_i \equiv bx_k (mod\ a)$$

因为$(a,b)=1$，所以$x_i \equiv x_k(mod\ a)$。但x_i, x_k是模a的既约剩余系中的数，所以$x_i = x_k$，因此$i=k$。同理可证$j=s$，因此，$bx_i + ay_j = bx_k + ax_s$。这与上述假设矛盾。这就是说，数组3-1中的任意两数对模ab都不同余。
又因为$(x_i,a)=1,(b,a)=1$，所以

$$(bx_i,a)=1, i=1,2,\cdots,\varphi(a)$$

因此，

$$(bx_i+ay_j,a)=1, j=1,2,\cdots,\varphi(b)$$

同理可得$(bx_i+ay_j,b)=1$，于是$(bx_i+ay_j,ab)=1$。这也就是说，数组3-1中任一数都与ab互质。至此，已经证明了数组3-1满足定理3.10中的条件(2)和(3)，余下还需证明数组3-1的个数就是$\varphi(ab)$。

由上述证明可知，数组3-1是模ab的某一个既约剩余系的子集。如果该既约剩余系中还有某数不在数组3-1中，那么该数与ab互质，且与数组3-1中任何数不同余。于是，如果能够证明任意与ab互质的数z必与数组3-1中某个bx_i+ay_j关于模ab同余，那么也就证明了3-1就是模ab的一个既约剩余系。
现设$(z,ab)=1$，因为$(a,b)=1$，所以

$$bx_0+ay_0=1$$

于是，存在整数x,y使得

$$z=bx+ay$$

但$(z,a)=1$，即$(bx+ay,a)=1$，所以$(bx,a)=1$，因此$(x,a)=1$。
于是，存在某一个x_i，使得

$$x \equiv x_i(mod\ a)$$

这是因为$x_1,x_2,\cdots,x_{\varphi(a)}$是模$a$ 的既约剩余系，所以与a 互质的数必与某一个x_i关于模a同余。
同理，存在某一个y_j，使得

$$y \equiv y_j(mod\ b)$$

从而

$$bx \equiv bx_i(mod\ ab), ay \equiv ay_j(mod\ ab)$$

所以

$$bx + ay \equiv bx_i + ay_j (mod\ ab)$$

即$z \equiv bx_i + ay_j (mod\ ab)$。这就证明了与$ab$互质的数必与数组3-1中的某一个数同余，因此3-1是模ab的既约剩余系。 □

由引理3.7的证明，可以得到下面结论：

若$x_1, x_2, \cdots, x_{\varphi(a)}$和$y_1, y_2, \cdots, y_{\varphi(b)}$分别是$a$和$b$ 的既约剩余系，且$(a,b) = 1$，则$bx_i + ay_j, i = 1,2,\cdots,\varphi(a); j = 1,2,\cdots,\varphi(b)$是模$ab$的既约剩余系。

有了引理3.6和引理3.7，可以很容易得到$\varphi(m)$的计算公式。

定理 3.12 若m的标准分解式是$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$，则

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

证明：根据引理3.6和引理3.7，

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) \\ &= \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k}) \\ &= p_1^{a_1}(1 - \tfrac{1}{p_1}) p_2^{a_2}(1 - \tfrac{1}{p_2}) \cdots p_k^{a_k}(1 - \tfrac{1}{p_k}) \\ &= m(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_k}) \end{aligned}$$

定理得证。 □

例 3.10 求$\varphi(75600)$。

解：因为$75600 = 2^4 \times 3^3 \times 5^2 \times 7$，所以

$$\begin{aligned} \varphi(75600) &= 75600 \times (1 - \tfrac{1}{2}) \times (1 - \tfrac{1}{3}) \times (1 - \tfrac{1}{5}) \times (1 - \tfrac{1}{7}) \\ &= 75600 \times \tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{4}{5} \times \tfrac{6}{7} \\ &= 17280 \end{aligned}$$

习题：

1. (1)写出模9的一个完全剩余系，且每个数都是奇数；
(2) 写出模9的一个完全剩余系，且每个数都是偶数；
(3) 对于模10的完全剩余系能实现(1)、(2)的要求吗？

解：(1) $\{1,3,5,7,9,11,13,15,17\}$

(2) $\{2,4,6,8,10,12,14,16,18\}$

(3) 不能实现

2. 下列各组数是否是模8的完全剩余系

(1) $2,4,6,8,17,21,23$；

(2) $-7,-12,-17,-22,-27,-32,-37,-42$。

解：(1) 该集合个数为7，不是模8的完全剩余系；

(2) $-7\equiv 1(mod\ 8), -12\equiv 4(mod\ 8), -17\equiv 7(mod\ 8)$

$-22\equiv 2(mod\ 8), -27\equiv 5(mod\ 8), -32\equiv 0(mod\ 8)$

$-37\equiv 3(mod\ 8), -42\equiv 6(mod\ 8)$

因此，该集合是模8的一个完全剩余系。

3. 验证$8,16,24,32,40,48$是模7的既约剩余系。

解：模7的最小既约剩余系为$1,2,3,4,5,6$，又

$8\equiv 1(mod\ 7), 16\equiv 2(mod\ 7)$

$24\equiv 3(mod\ 7), 32\equiv 4(mod\ 7)$

$40\equiv 5(mod\ 7), 48\equiv 6(mod\ 7)$

这6个数与模7的最小既约剩余系分别同余，所以它们也是模7的一个既约剩余系。

4. 当$m>2$时，证明$\varphi(m)$是偶数。

证明：写出m的标准分解式

$$m=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$$

因为$m>2$，所以m一定含有一个奇素因子，不妨设为p_i，则$\varphi(m)$含有因子$\varphi(p_i^{a_k})=p_i^{a_k-1}(p_i-1)$为偶数，因此$\varphi(m)$是偶数。

5. 求$\varphi(3823963)$.

解：因为$3823963=11^3\times 13^2\times 17$，所以$\varphi(3823963)=3823963(1-\frac{1}{11})(1-\frac{1}{13})(1-\frac{1}{17})=3020160$。

6. 证明$\varphi(1)+\varphi(p)+\cdots+\varphi(p^\alpha)=p^\alpha$，$p$是素数。

解：

$$\begin{aligned} & \varphi(1)+\varphi(p)+\cdots+\varphi(p^{\alpha}) \\ = \ & 1+p(1-\tfrac{1}{p})+p^2(1-\tfrac{1}{p})+\cdots+p^{\alpha}(1-\tfrac{1}{p}) \\ = \ & 1+(1-\tfrac{1}{p})(p+p^2+\cdots+p^k) \\ = \ & 1+p^{\alpha}-1=p^{\alpha} \end{aligned}$$

3.3 欧拉定理与费马小定理

定理 3.13 (欧拉定理) 设m是大于1的整数，$(a,m)=1$，则$a^{\varphi(m)} \equiv 1(mod\ m)$。

证明：注意到结论中有欧拉函数$\varphi(m)$，拟从模m的既约剩余系出发进行论证。

假设$x_1,x_2,\cdots,x_{\varphi(m)}$是模$m$的既约剩余系，因为$(a,m)=1$，所以，由定理3.10可知，$ax_1,ax_2,\cdots,ax_{\varphi(m)}$也是模$m$的既约剩余系，于是$ax_1,ax_2,\cdots,ax_{\varphi(m)}$必与$x_1,x_2,\cdots,x_{\varphi(m)}$中的某数关于模$m$同余，即

$$ax_1 \equiv x_{i_1}, ax_2 \equiv x_{i_2},\cdots,ax_{\varphi(m)} \equiv x_{i_{\varphi(m)}}(mod\ m)$$

其中，$x_{i_1},x_{i_2},\cdots,x_{i_{\varphi(m)}}$的一个排列。所以

$$ax_1 \cdot ax_2 \cdot \cdots \cdot ax_{\varphi(m)} \equiv x_1 \cdot x_2 \cdot \cdots \cdot x_{\varphi(m)}(mod\ m)$$

即

$$a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)} \equiv x_1x_2\cdots x_{\varphi(m)}(mod\ m)$$

又因为$(x_i,m)=1,i=1,2,\cdots,\varphi(m)$，所以$(x_1x_2\cdots x_{\varphi(m)},m)=1$。由同余式性质，两边约去$x_1x_2\cdots x_{\varphi(m)}$得到$a^{\varphi(m)} \equiv 1(mod\ m)$。定理得证。 □

特别地，当m是素数时，可得到费马小定理。

定理 3.14 (费马小定理)设p是素数，且a是与p互质的整数，则$a^{p-1} \equiv 1(mod\ p)$。

证明：根据欧拉定理有$a^{\varphi(p)} \equiv 1(mod\ p)$。因为$p$是素数，所以$\varphi(p)=p-1$。因此，$a^{p-1} \equiv 1(mod\ p)$。 □

特别地，将费马小定理同余式两侧同乘以a，费马小定理可变形为：

$$a^p \equiv a(mod\ p)$$

费马小定理是相对于费马大定理而言的，它是费马与1640年提出的，但未加证明。1736年才由欧拉证明了这个定理，进一步给出了更一般的欧拉定理。

例 3.11 证明：$1979^{2022} \equiv 1(mod\ 43)$。

证明： 因为43是素数，由费马小定理有$1979^{42} \equiv 1(mod\ 43)$。又$2022 = 42 \times 48 + 6$，所以

$$\begin{aligned} 1979^{2022} &= 1979^{42\times 48} \times 1979^6 \\ &= (1979^{42})^{48} \times 1979^6 \\ &\equiv 1979^6 (mod\ 43) \\ &\equiv 1^6 \equiv 1(mod\ 43) \end{aligned}$$

例 3.12 求6^{2022}除以10的非负最小余数。

解： 因为$(6, 10) = 5 \neq 1$，所以不能直接用欧拉定理求解。注意到

$$6^{2022} = 2 \times 3 \times 6^{2021}, 14 = 2 \times 5, 5\text{为质数}$$

可以先确定$6^{2021} \equiv x(mod\ 5)$中的$x$。

易知$6^2 \equiv 1(mod\ 5)$，而$2021 = 2 \times 1010 + 1$，所以

$$6^{2021} = (6^2)^{1010} \times 6 \equiv 6 \equiv 1(mod\ 5)$$

两边同乘3，可得$3 \times 6^{2021} \equiv 3(mod\ 5)$，进而由定理3.6可得

$$2 \times 3 \times 6^{2021} \equiv 2 \times 3(mod\ 10)$$

即$6^{2022} \equiv 6(mod\ 10)$，因此$6^{2022}$除以10的非负最小余数是6。

例 3.13 设p是不等于3和7的奇素数，证明$p^6 \equiv 1(mod 168)$。

证明： 注意到$168 = 8 \times 7 \times 3$，其中$8, 7, 3$两两互素，根据定理3.6，可以把问题转化为证明$p^6 \equiv 1(mod\ 8), p^6 \equiv 1(mod\ 7), p^6 \equiv 1(mod\ 3)$成立。

设$p = 2m + 1$，其中m是正整数，则

$$p^2 = 4m(m + 1) + 1$$

因为$m(m + 1)$一定是偶数，所以$8|4m(m + 1)$，所以$p^2 \equiv 1(mod\ 8)$，从而$p^6 \equiv 1(mod\ 8)$。

由题意知$(p,3)=1,(p,7)=1$，由费马小定理有

$$p^2\equiv 1(mod\ 3),p^6\equiv 1(mod\ 7)$$

于是，$p^6\equiv 1(mod\ 3)$。由定理3.7，可得$p^6\equiv 1(mod\ 8\times 7\times 3)$，即$p^6\equiv 1(mod\ 168)$。

习题：

1. 求下列各题的非负最小余数

(1) 8^{1234}除以13；

(2) 54^{1234}除以17。

解：(1)因为$(8,13)=1$，由欧拉定理可得$8^{12}\equiv 1(mod\ 13)$。又$1234=12\times 102+10$，所以$8^{1234}=(8^{12})^{102}\times 8^{10}\equiv 8^{10}\equiv(13\times 4+12)^5\equiv 12^5\equiv 12(mod\ 13)$。

(2) 因为$(54,17)=1$，由欧拉定理可得$54^{16}\equiv 1(mod\ 17)$。又$1234=16\times 77+2$，所以$(54^{16})^{77}\times 54^2\equiv 54^2\equiv 9(mod\ 17)$。

2. 设p,q是两个大于3的素数，求证$p^2\equiv q^2(mod\ 24)$。

证明：由题意可设$p=2m+1$，而$8|4m(m+1)$，可得$p^2\equiv 1(mod\ 8)$，同理可得$q^2\equiv 1(mod\ 8)$，进而$p^2-q^2\equiv 0(mod\ 8)$。

由题意知$(p,3)=1$，由欧拉定理可得$p^2\equiv 1(mod\ 2)$。同理可得$p^2\equiv 1(mod\ 2)$，进而$p^2-q^2\equiv 0(mod\ 3)$。又$[3,8]=24$，由定理3.7可得，$p^2-q^2\equiv 0(mod\ 24)$，即$p^2\equiv q^2(mod\ 24)$。

3. 已知p是素数，$(a,p)=1$，求证：

(1) 当a是奇数时，$a^{p-1}+(p-1)^a\equiv 0(mod\ p)$；

(2) 当a是偶数时，$a^{p-1}-(p-1)^a\equiv 0(mod\ p)$。

证明：

因为$(a,p)=1$，由欧拉定理可得$a^{p-1}\equiv 1(mod\ p)$。又

$$(p-1)^a=C_a^0p^0(-1)^a+C_a^1p^1(-1)^{a-1}+\cdots+C_a^ap^a(-1)^0$$

所以$(p-1)^a\equiv(-1)^a(mod\ p)$。

(1) 当a是奇数时，$(-1)^a=-1$，即$(p-1)^a\equiv -1(mod\ p)$。又$a^{p-1}\equiv 1(mod\ p)$，所以$a^{p-1}+(p-1)^a\equiv 0(mod\ p)$；

(1) 当a是偶数时，$(-1)^a=1$，即$(p-1)^a\equiv 1(mod\ p)$。又$a^{p-1}\equiv 1(mod\ p)$，所以$a^{p-1}-(p-1)^a\equiv 0(mod\ p)$；

3.4 扩展知识：欧拉与费马

第 4 章　同余方程

在代数里面，一个主要的问题就是求解代数方程。本章要讨论的正是与求解代数方程相类似的问题：求解同余式的解。

4.1 一次同余方程

定义 4.1 若$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$是关于$x$的整系数多项式，$m$是大于1的整数，且$a_n\not\equiv 0(mod\ m)$，则

$$f(x)\equiv 0(mod\ m)$$

称作含有未知数x的关于模m的n次同余方程，简称n次**同余方程**。

定义 4.2 若a是使$f(a)\equiv 0(mod\ m)$成立的一个整数，则$x\equiv a(mod\ m)$称作同余方程$f(x)\equiv 0(mod\ m)$的一解或根。两个对模m同余的一切数算作同余方程$f(x)\equiv 0(mod\ m)$的一个解，即

$$x=a+mt,\quad t=0,\pm1,\pm2,\cdots$$

定义 4.3 **一元一次同余方程**是指

$$ax\equiv b(mod\ m) \tag{4-1}$$

其中$a\not\equiv 0(mod\ m),m>1$。

如果$x=x_0$满足式4-1，则$x\equiv x_0(mod\ m)$ 称为**一元一次同余方程的解**。有时也把x_0称为同余方程的解。不同的解是指对模数m 互不同余的解。

逐个将$0,1,\cdots,m-1$代入式4-1进行验算可求出式4-1的解，但当m很大时，计算量很大。下面给出基于不定方程的求解方法。

定理 4.1 设$(a,m)=d$，则式4-1有解的充分必要条件是$d|b$。且式4-1 有解时，恰有d 个解，它们是$x\equiv x_0+\frac{m}{d}t(mod\ m),t=0,1,\cdots,d-1$。其中$x_0$ 是式4-1的任意一个解。

证明：首先证明充分性。当$d|b$时，由$(a,m)=d$，有$au+mv=d$，从而得$au\frac{b}{d}+mv\frac{b}{d}=b$，于是$au\frac{b}{d}\equiv b(mod\ m)$，即$x\equiv u\frac{b}{d}(mod\ m)$是式4-1的解。

其次证明必要性。设$x\equiv x_0(mod\ m)$是式4-1的一个解，则$ax_0\equiv b(mod\ m)$，从而有整数y_0使$ax_0-b=my_0$，根据定理2.1可知$(a,m)=d|b$。

当式4-1有解时，显然$x\equiv x_0+\frac{m}{d}t(mod\ m), t=0,1,\cdots,d-1$是式4-1的$d$个互不同余的解，其中$x_0$是式4-1的一个解。又如果$x_1$是式4-1的任意一个解，则有$ax_1\equiv b(mod\ m)$，又$a(x_0+\frac{m}{d}t)\equiv b(mod\ m)$，于是

$$a(x_1-x_0-\frac{m}{d}t)\equiv 0(mod\ m)$$

根据定理3.5，进而有

$$x_1-x_0-\frac{m}{d}t\equiv 0(mod\ \frac{m}{d})$$

即$x_1\equiv x_0(mod\ \frac{m}{d})$，因此有$t_1$使$x_1=x_0+\frac{m}{d}t_1$，记$t\equiv t_1(mod\ d), 0\le t\le d-1$，则$x_1\equiv x_0+\frac{m}{d}t(mod\ m)$，这说明了式4-1恰有所给的$d$个解。定理得证。 □

注：当$(a,m)=1$时，同余方程$ax\equiv 1(modm)$恰有一个解x_0，有时称这个解x_0为a 模m的**逆**，并记为a^{-1}。

例 4.1 解一次同余方程$14x\equiv 26(mod\ 38)$。

解：作辗转相除法

$$38=14\times 3-4$$
$$14=4\times 3+2$$
$$4=2\times 2$$

所以$(38,14)=2|26$，同余方程有两个解。再回代

$$2=14-4\times 3=14-(14\times 3-38)\times 3=14\times(-8)+38\times 3$$

由$26\div 2=13$，知$x_0\equiv(-8)\times 13\equiv -104\equiv 10(mod\ 38)$ 是同余方程的解。

再由$38\div 2=19$，知其两个解为$x\equiv 10, 10+19\equiv 10, 29(mod\ 38)$。

例 4.2 解一次同余方程$111x\equiv 75(mod\ 321)$。

解：作辗转相除法

$$321 = 111 \times 2 + 99$$
$$111 = 99 \times 1 + 12$$
$$99 = 12 \times 8 + 3$$
$$12 = 3 \times 4$$

所以3|75，同余方程有3个解。再回代

$$\begin{aligned} 3 &= 99 - 12 \times 8 = 99 - (111 - 99) \times 8 = 99 \times 9 + 111 \times (-8) \\ &= (321 - 111 \times 2) \times 9 + 111 \times (-8) \\ &= 321 \times 9 + 111 \times (-26) \end{aligned}$$

由$75 \div 3 = 25$，知$x_0 \equiv (-26) \times 25 \equiv -650 \equiv 313 (mod\ 321)$ 是同余方程的解。再由$321 \div 3 = 107$，知其三个解为

$$x \equiv 313 + 107t (mod\ 321)$$

即$x \equiv 99, 206, 313 (mod\ 321)$。

习题：

1.求解$24x \equiv 42 (mod\ 30)$。

解：

$$\begin{aligned} 30 &= 24 \times 1 + 6 \\ 24 &= 6 \times 4 \end{aligned}$$

因此，$(24, 30) = 6$，又6|42，因此方程有解，且有6个解。又

$$6 = 30 + 24 \times (-1)$$

所以

$$x_0 = (-1) \times \frac{42}{6} = -7 \equiv 23 (mod\ 30)$$

进而

$$x \equiv x_0 + \frac{m}{d}t \equiv 23 + \frac{30}{6}t \equiv 23 + 5t, t = 0, 1, \cdots, 5$$

即$x \equiv 3, 8, 13, 18, 23, 28 (mod\ 30)$。

2. 求解$90x \equiv 21 (mod\ 429)$。

解：

$$\begin{aligned} 429 &= 90 \times 4 + 69 \\ 90 &= 69 \times 1 + 21 \\ 69 &= 21 \times 3 + 6 \\ 21 &= 6 \times 3 + 3 \\ 6 &= 3 \times 2 \end{aligned}$$

因此，$(90, 429) = 3$，又$3|21$，因此方程有解，且有3个解。又

$$\begin{aligned} 3 &= 21 - 6 \times 3 = 21 - (69 - 21 \times 3) \times 3 \\ &= 21 \times 10 + 69 \times (-3) = (90 - 69) \times 10 + 69 \times (-3) \\ &= 90 \times 10 + 69 \times (-13) = 90 \times 10 + (429 - 90 \times 4) \times (-13) \\ &= 90 \times 62 + 429 \times (-13) \end{aligned}$$

所以

$$x_0 = 62 \times \frac{21}{3} = 434 \equiv 5(mod\ 429)$$

进而

$$x \equiv x_0 + \frac{m}{d}t \equiv 5 + \frac{429}{3}t \equiv 5 + 143t, t = 0, 1, 2$$

即$x \equiv 5, 148, 291(mod\ 429)$。

3. 求解$432x \equiv 23(mod\ 179)$。

解：

$$\begin{aligned} 432 &= 179 \times 2 + 74 \\ 179 &= 74 \times 2 + 31 \\ 74 &= 31 \times 3 + 12 \\ 31 &= 12 \times 2 + 7 \\ 12 &= 7 \times 1 + 5 \\ 7 &= 5 \times 1 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 1 \times 2 \end{aligned}$$

因此，$(432, 179) = 1$，又$1|23$，因此方程有解，且有1个解。又

$$\begin{aligned} 1 &= 5 - 2 \times 2 = 5 \times 3 + 7 \times (-2) \\ &= 12 \times 3 + 7 \times (-5) = 12 \times 13 + 31 \times (-5) \\ &= 74 \times 13 + 31 \times (-31) = 74 \times 75 + 179 \times (-31) \\ &= 432 \times 75 + 179 \times (-181) \end{aligned}$$

所以

$$x_0 = 75 \times 23 = 1725 \equiv 114(mod\ 179)$$

方程有一个解，即$x \equiv 114(mod\ 179)$。

4. 设$d = (m_1, m_2)$，证明：同余方程组

$$\begin{cases} x \equiv a_1(mod\ m_1) \\ x \equiv a_2(mod\ m_2) \end{cases}$$

有解的充分必要条件是$d|a_1 - a_2$。

证明：首先证明必要性。设$x \equiv c$是方程组的一个解，即

$$\begin{cases} c \equiv a_1(mod\ m_1) \\ c \equiv a_2(mod\ m_2) \end{cases}$$

则

$$\begin{cases} c \equiv a_1(mod\ (m_1, m_2)) \\ c \equiv a_2(mod\ (m_1, m_2)) \end{cases}$$

于是$a_1 \equiv a_2(mod\ d)$，即$d|a_1 - a_2$。

其次证明充分性。假设$d|a_1 - a_2$，则同余方程

$$m_2 y \equiv a_1 - a_2(mod\ m_1)$$

有解，设为$y \equiv d(mod\ m_1)$，于是有

$$a_2 + m_2 d \equiv a_1(mod\ m_1)$$

另一方面，易见

$$a_2 + m_2 d \equiv a_2 (mod\ m_2)$$

因此，同余方程组有解$x = a_2 + m_2 d$。

4.2 一次同余方程组

在代数方程中，两个不同的一元一次方程是没有公共解的，因而在代数方程中不存在对一元一次方程组的求解问题。但是，对于一元一次同余方程，情况则不同。因为模数不同，所以两个不同的一元一次同余方程可以存在公共解。因此，研究一次同余方程组的解就变成有意义的问题了。

设$f_i(x)(1 \leq i \leq k, k \geq 2)$是整系数多项式，含有未知数$x$的一组同余式

$$\begin{cases} f_1(x) \equiv 0(mod m_1) \\ f_2(x) \equiv 0(mod m_2) \\ \cdots \\ f_k(x) \equiv 0(mod m_k) \end{cases} \tag{4-2}$$

称为同余方程组。

若整数c同时满足$f_i(c) \equiv 0(mod\ m_i)1 \leq i \leq k$，则称$c$是同余方程组4-2的解。这时，若令$m = [m_1, m_2, \cdots, m_k]$，则模$m$的剩余类$[c]_m$中的任一整数也是同余方程组4-2的解。因此，如果$c$是同余方程组4-2的解，那么通常用

$$x \equiv c(mod\ m)$$

表示同余方程组4-2的解。只有当c_1, c_2都是同余方程组4-2的解，且$c_1 \not\equiv c_2(mod\ m)$，才把它们看作不同的解。

把所有对模m两两不同余的同余方程组4-2的解的个数称为同余方程组4-2的解数。因此，同余方程组4-2的解数至多为m。此外，与代数方程组一样，只要同余方程组4-2中有一个同余方程无解，则4-2一定无解。

关于解一次同余方程组的问题，我国古代就有驰名中外的中国剩余定理。在《孙子算经》里已经提出并很好解决了这样的问题，也就是《孙子算经》下卷第26题“物不知数”题：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”“答曰二十三”。所以，此定理也称为孙子定理。

定理 4.2 (孙子定理)设$m_1, m_2, \cdots, m_k$是k个两两互素的整数，则同余方程组

$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \cdots \\ x \equiv a_k (mod\ m_k) \end{cases}$$

对于模$m = m_1 m_2 \cdots m_k$有唯一解

$$x \equiv \frac{m}{m_1} x_1 a_1 + \cdots + \frac{m}{m_k} x_k a_k (mod\ m)$$

其中，$\frac{m}{m_i} x_i \equiv 1 (mod\ m_i)$。

证明： 首先证明存在性。因为$m_1, m_2, \cdots, m_k$两两互素，且$m = m_1 m_2 \cdots m_k$，所以$(\frac{m}{m_i}, m_i) = 1$。根据定理4.1，知同余方程$\frac{m}{m_i} x \equiv 1 (mod\ m_i)$有唯一解$x_i$，即

$$\frac{m}{m_i} x_i \equiv 1 (mod\ m_i)$$

从而

$$\frac{m}{m_i} x_i a_i \equiv a_i (mod\ m_i)$$

又因$m_i | \frac{m}{m_j} (i \neq j)$，所以

$$\frac{m}{m_j} x_j \equiv 0 (mod\ m_i) (i \neq j)$$

于是，若令$\alpha = \frac{m}{m_1} x_1 a_1 + \frac{m}{m_2} x_2 a_2 + \cdots + \frac{m}{m_k} x_k a_k$，则$\alpha \equiv a_i (mod\ m_i)$，因而$x \equiv \alpha (mod\ m)$是同余方程组的解。

其次证明唯一性。设存在另一整数β，满足$\beta \equiv a_i (mod\ m_i), i = 1, 2, \cdots, k$，则$\alpha \equiv \beta (mod\ m_i)$，所以

$$\alpha \equiv \beta (mod\ [m_1, m_2, \cdots, m_i])$$

即$\alpha \equiv \beta (mod\ m)$。这就是说，对于模$m$，同余方程只有一个解。 □

例 4.3 解同余方程组

$$\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$$

解：因3，5，7两两互质，根据孙子定理，先分别解出同余方程

$$35x_1 \equiv 1(mod\ 3), 21x_2 \equiv 1(mod\ 5), 15x_3 \equiv 1(mod\ 7)$$

得

$$x_1 = 2, x_2 = 1, x_3 = 1$$

于是所求的同余方程组的解为

$$x \equiv 35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 \equiv 233 \equiv 23(mod\ 3 \times 5 \times 7)$$

即$x \equiv 23(mod\ 105)$。

例 4.4 (韩信点兵)有兵3万多，若均分成5营，则与1人；均分成6营，则余5人；均分成7营，则余4人；均分成11营，则余10人；均分成13营，则余5人。求兵数。
解：设兵数为x，则$30000 < x < 40000$，故有

$$\begin{cases} x \equiv 1(mod\ 5) \\ x \equiv 5(mod\ 6) \\ x \equiv 4(mod\ 7) \\ x \equiv 10(mod\ 11) \\ x \equiv 5(mod\ 13) \end{cases}$$

因为5,6,7,11,13两两互质，所以可用孙子定理求解。由于所含同余方程较多，可先分别算出$m = 5 \times 6 \times 7 \times 11 \times 13$和

$$\frac{m}{m_1} = \frac{30030}{5} = 6006, \quad \frac{m}{m_2} = \frac{30030}{6} = 5005$$

$$\frac{m}{m_3} = \frac{30030}{7} = 4290, \quad \frac{m}{m_4} = \frac{30030}{11} = 2730, \quad \frac{m}{m_5} = \frac{30030}{13} = 2310$$

再分别解出以下同余方程

$$6006x_1 \equiv 1(mod\ 5) \quad 5005x_2 \equiv 1(mod\ 6)$$

$$4290x_3 \equiv 1(mod\ 7), \quad 2730x_4 \equiv 1(mod\ 11), \quad 2310x_5 \equiv 1(mod\ 13)$$

得$x_1 = 1, x_2 = 1, x_3 = 6, x_4 = 6, x_5 = 3$。于是所求同余方程组的解为

$$\begin{aligned} x &\equiv 6006 \times 1 \times 1 + 5005 \times 1 \times 5 + 4290 \times 6 \times 4 + 2730 \times 6 \times 10 + 2310 \times 3 \times 5 \\ &\equiv 332441 \\ &\equiv 2111(mod\ 30030) \end{aligned}$$

即$x = 2111 + 30030t, t = 0, 1, 2, \cdots$。由题意，有$30000 < 2111 + 30030t < 40000$，解得$t = 1$。因此$x = 2111 + 30030 = 32141$。

例 4.5 解同余方程组

$$\begin{cases} 3x \equiv 2(mod\ 5) \\ 7x \equiv 3(mod\ 8) \\ 4x \equiv 7(mod\ 11) \end{cases}$$

解：模5,8,11两两互素，可用孙子定理求解。但是必须先将各同余方程中x的系数化为1。注意到每个同余方程均有唯一解，所以

$$3x \equiv 2(mod\ 5) \Leftrightarrow 3x \equiv 2 + 10(mod\ 5) \Leftrightarrow x \equiv 4(mod\ 5)$$

$$7x \equiv 3(mod\ 8) \Leftrightarrow -x \equiv 3(mod\ 5) \Leftrightarrow x \equiv -3(mod\ 8) \Leftrightarrow x \equiv 5(mod\ 8)$$

$$4x \equiv 7(mod\ 11) \Leftrightarrow 4x \equiv 7 - 11(mod\ 11) \Leftrightarrow x \equiv -1(mod\ 11) \Leftrightarrow x \equiv 10(mod\ 11)$$

于是得同解的同余方程组

$$\begin{cases} x \equiv 4(mod\ 5) \\ x \equiv 5(mod\ 8) \\ x \equiv 10(mod\ 11) \end{cases}$$

由$m = 5 \times 8 \times 11 = 440$，且

$$\frac{m}{m_1} = \frac{440}{5} = 88, \frac{m}{m_2} = \frac{440}{8} = 55, \frac{m}{m_3} = \frac{440}{11} = 40$$

解同余方程

$$88x_1 \equiv 1(mod\ 5), 55x_2 \equiv 1(mod\ 8), 40x_3 \equiv 1(mod\ 11)$$

得

$$x_1 = 2, x_2 = 7, x_3 = 8$$

因此

$$\begin{aligned} x &\equiv 88 \times 2 \times 4 + 55 \times 7 \times 5 + 40 \times 8 \times 10 \\ &\equiv 5829 \\ &\equiv 109(mod\ 440) \end{aligned}$$

习题：

1. 试解下列各题（续古摘奇算法）：

(1) 十一数余三，七二数余二，十三数余一，问本数；

(2) 二数余一，五数余二，七数余三，九数余四，问本数。

解：(1)由题意可得同余方程组

$$\begin{cases} x \equiv 3(mod\ 11) \\ x \equiv 2(mod\ 72) \\ x \equiv 1(mod\ 13) \end{cases}$$

因为11,72,13两两互质，采用孙子定理求解。有$m = 11 \times 72 \times 13 = 10296$，$\frac{m}{m_1} = \frac{10296}{11} = 936$，$\frac{m}{m_2} = \frac{10296}{72} = 143$，$\frac{m}{m_3} = \frac{10296}{13} = 792$。再分别解出下列同余方程

$$936x_1 \equiv 1(mod\ 11), 143x_2 \equiv 1(mod\ 72), 792x_3 \equiv 1(mod\ 13)$$

得$x_1 = 1, x_2 = 71, x_3 = 12$，所以同余方程组的解为

$$\begin{aligned} x &\equiv 936 \times 1 \times 3 + 143 \times 71 \times 2 + 792 \times 12 \times 1 \\ &\equiv 32618 \\ &\equiv 1730(mod\ 10296) \end{aligned}$$

(2)由题意可得同余方程组

$$\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 2(mod\ 5) \\ x \equiv 3(mod\ 7) \\ x \equiv 4(mod\ 9) \end{cases}$$

因为2,5,7,9两两互质，采用孙子定理求解。有$m = 2 \times 5 \times 7 \times 9 = 630$，$\frac{m}{m_1} = \frac{630}{2} = 315$，$\frac{m}{m_2} = \frac{630}{5} = 126$，$\frac{m}{m_3} = \frac{630}{7} = 90$，$\frac{m}{m_4} = \frac{630}{9} = 70$。再分别解出下列同余方程

$$315x_1 \equiv 1(mod\ 2), 126x_2 \equiv 1(mod\ 5), 90x_3 \equiv 1(mod\ 7), 70x_4 \equiv 1(mod\ 9)$$

得$x_1 = 1, x_2 = 1, x_3 = 6, x_4 = 4$，所以同余方程组的解为

$$\begin{aligned} x &\equiv 315 \times 1 \times 1 + 126 \times 1 \times 2 + 90 \times 6 \times 3 + 70 \times 4 \times 4 \\ &\equiv 3307 \\ &\equiv 157(mod\ 630) \end{aligned}$$

2. 解同余方程组

$$\begin{cases} x \equiv 1(mod\ 7) \\ 3x \equiv 4(mod\ 5) \\ 8x \equiv 4(mod\ 9) \end{cases}$$

解：模5,7,9两两互素，可用孙子定理求解。但是必须先将各同余方程中x的系数化为1。注意到每个同余方程均有唯一解，所以

$$3x \equiv 4(mod\ 5) \Leftrightarrow 3x \equiv 4 + 20(mod\ 5) \Leftrightarrow x \equiv 8(mod\ 5)$$

$$8x \equiv 4(mod\ 9) \Leftrightarrow -x \equiv 4(mod\ 9) \Leftrightarrow x \equiv -4(mod\ 9) \Leftrightarrow x \equiv 5(mod\ 9)$$

于是得同解的同余方程组

$$\begin{cases} x \equiv 1(mod\ 7) \\ x \equiv 8(mod\ 5) \\ x \equiv 5(mod\ 9) \end{cases}$$

由$m = 7 \times 5 \times 9 = 315$，且

$$\frac{m}{m_1} = \frac{315}{7} = 45, \frac{m}{m_2} = \frac{315}{5} = 63, \frac{m}{m_3} = \frac{315}{9} = 35$$

解同余方程

$$45x_1 \equiv 1(mod\ 7), 63x_2 \equiv 1(mod\ 5), 35x_3 \equiv 1(mod\ 9)$$

得

$$x_1 = 5, x_2 = 2, x_3 = 8$$

因此

$$\begin{aligned} x &\equiv 45 \times 5 \times 1 + 63 \times 2 \times 8 + 35 \times 8 \times 5 \\ &\equiv 2633 \\ &\equiv 113(mod\ 315) \end{aligned}$$

4.3 扩展知识：仿射密码算法和RSA公钥密码算法

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。通常情况下，一个完整的密码算法(体制)包含五部分内容：

- 明文空间M：所有可能明文m的集合；
- 密文空间C：所有可能密文c的集合；
- 密钥空间K：所有可能密钥k的集合，其中每一密钥k由加密密钥k_e 和解密密钥k_d组成，即$k = (k_e, k_d)$；
- 加密算法E：一簇由加密密钥控制的从M到C的加密变换；
- 解密算法D：一簇由解密密钥控制的从C到M的解密变换。

根据加密算法与解密算法所使用的密钥是否相同，可以将密码体制分为对称密码体制和非对称密码体制。当加密密钥和解密密钥相同时，该密码体

制被称之为对称密码体制(单钥密码体制、秘密密钥密码体制和常规密码体制)。当加密密钥和解密密钥不相同时，该密码体制被称之为非对称密码体制(双钥密码体制)。由于加密密钥可以公开，该密码体制也常被称之为公钥密码体制。根据本章讲述内容，本节介绍两个相关的密码算法。仿射密码算法归属对称密码体制，RSA公钥密码算法归属于非对称密码体制。

4.3.1 仿射密码

仿射密码的明文空间M和密文空间C均是集合$\mathbb{Z}_{26} = 0, 1, 2, \cdots, 25$，密钥空间为$K = \{(k_1, k_2)|k_1 \in \mathbb{Z} k_2 \in \mathbb{Z}(k_1, 26) = 1\}$。对任意的$m \in M, c \in C, k = (k_1, k_2) \in K$，
加密变换为

$$c \equiv E_k(m) \equiv k_1 m + k_2 (mod\ 26)$$

解密变换为

$$m \equiv D_k(c) \equiv k_1^{-1}(c - k_2)(mod\ 26)$$

其中，$k_1 k_1^{-1} \equiv 1(mod\ 26)$。

注：

- 当$k_1 = 1$时，该密码体制也被称作移位密码；
- 当$k_2 = 0$时，该密码体制也被称作乘法密码。

下面通过一道例题熟悉一下仿射密码的加解密过程。

例 4.6 设明文消息为$china$，密钥$k = (k_1, k_2) = (9, 2)$试用仿射密码进行加密，然后再进行解密。

解：仿射密码的明文空间为$\mathbb{Z}_{26}$，首先按照下表将明文转化为数字。

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

明文字母对应的数字为：$2, 7, 8, 13, 0$，按照仿射密码算法，可知

- 加密变换为：$E_k(m) \equiv k_1 m + k_2 (mod\ 26) \equiv 9m + 2(mod\ 26)$
- 解密变换为：$D_k(c) \equiv k_1^{-1}(c - k_2) \equiv 3(c - 2) \equiv 3c - 6(mod\ 26)$

其中，通过求解$k_1 k_1^{-1} \equiv 1(mod\ 26)$可得$k_1^{-1} = 3$。

将明文对应数字代入上述公式，则

$$E_k(m) = 9 \times \begin{pmatrix} 2 \\ 7 \\ 8 \\ 13 \\ 0 \end{pmatrix} + \begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 13 \\ 22 \\ 15 \\ 2 \end{pmatrix} (mod\ 26) = \begin{pmatrix} u \\ n \\ w \\ p \\ c \end{pmatrix}$$

因此，密文为$unwpc$。而解密过程如下

$$E_k(m) = 3 \times \begin{pmatrix} 20 \\ 13 \\ 22 \\ 15 \\ 2 \end{pmatrix} - \begin{pmatrix} 6 \\ 6 \\ 6 \\ 6 \\ 6 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 7 \\ 8 \\ 13 \\ 0 \end{pmatrix} (mod\ 26) = \begin{pmatrix} c \\ h \\ i \\ n \\ a \end{pmatrix}$$

即恢复的明文消息为$china$。

4.3.2 RSA公钥密码

RSA公钥密码体制是美国麻省理工学院的三位科学家Rivest、Shamir、Adleman于1978年提出，并以三位数学家名字首字母命名的公钥秘密系统。实际上，RSA稍后于背包公钥密码实用系统，但它的影响超过了背包公钥密码体系。它是最广泛接受并实现的通用公钥密码算法。RSA体制的理论基础是数论的欧拉定理，安全性依据是大整数分解的难度。

RSA公钥密码体制的描述如下：

- 选取两个大素数p, q。
- 计算$n = pq, \varphi(n) = (p-1)(q-1)$。
- 随机选取正整数$e, 1 < e < \phi(n)$，满足$(e, \varphi(n)) = 1$。
- 计算d，满足$de \equiv 1(mod\ \varphi(n))$，$p, q, \varphi(n), d$是保密的，称之为私钥，$e$是公开的，称之为公钥。
- 加密变换：对明文$m, 1 < m < n$，加密后的密文为$c = m^e(mod\ n)$。
- 解密变换：对密文$c, 1 < c < n$，解密后的明文为$m = c^d(mod\ n)$。

证明： 因为$de \equiv 1(mod\ \varphi(n))$，则有$de = 1 + t\varphi(n)$，其中$t$为整数。所以

$$c^d \equiv (m^e)^d \equiv m^{de} \equiv m^{1+t\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^t (mod\ n)$$

若$(m, n) = 1$，由欧拉定理可得$m^{\varphi(n)} \equiv 1(mod\ n)$，则

$$(m^{\varphi(n)})^t \equiv 1^t \equiv 1(mod\ n)$$

所以

$$c^d \equiv m \cdot (m^{\varphi(n)})^t \equiv m \cdot 1 \equiv 1(mod\ n)$$

若$(m, n) \neq 1$，且$n = pq$，不妨设$(m, n) = p$，则有$(m, q) = 1$。因为$(m, q) = 1$，由欧拉定理可得

$$m^{\varphi(q)} \equiv 1(mod\ q)$$

即$m^{q-1} \equiv 1(mod\ q)$，则

$$m^{t\varphi(n)} \equiv m^{t(p-1)(q-1)} \equiv (m^{q-1})^{t(p-1)} \equiv 1(mod\ q)$$

可设$m^{t\varphi(n)} = 1 + sq$，s为任意整数。另$(m, n) = p$，则有$m = pb(1 \leq b < q)$，此时

$$m^{t\varphi(n)+1} = m^{t\varphi(n)} \cdot m = (1 + sq) \cdot pb = pb + sbpq = pb + sbn$$

因此，$m^{t\varphi(n)+1} \equiv m(mod\ n)$，即

$$c^d \equiv m^{de} \equiv m^{1+t\varphi(n)} \equiv m(mod\ n)$$

□

例 4.7 设$p = 23, q = 47, e = 3$，明文$m = 320$，建立RSA公钥密码体制加密m并解密。

解： 首先计算

$$n = pq = 23 \times 47 = 1081, \phi(n) = (p - 1)(q - 1) = 22 \times 46 = 1012$$

显然$(e, \varphi(n)) = (3, 1012) = 1$，进而将$e = 3$代入同余方程$ed \equiv 1(mod\ \varphi(n))$，

即

$$3x \equiv 1(mod\ 1012)$$

可求得$d = 675$。于是可建立RSA 公钥密码体制：$p = 23, q = 47, \varphi(n) = 1012, d = 675$是需要保密的；$n = 1081, e = 3$ 是可以公开的。

对于明文$m = 320$，加密得密文

$$c \equiv 320^3 \equiv 728(mod\ 1081)$$

即密文为$c = 728$。解密得明文

$$m \equiv 728^{675}(mod\ 1081)$$

注：显然，RSA公钥密码算法的步骤很简洁，最核心的计算是下面两个步骤：

(1)私钥的求解：同余方程求解给出了私钥d的理论求解方法，具体实现可依据定理1.10 采用迭代法求解；

(2)加解密运算：加密和解密均是整数的模幂运算，当数值较大时，无法直接运算，可采用蒙哥马利快速算法(读者可自行查询具体算法)。