第二章　数论基础（一）

CONTENTS

目录

第 1 节

整除

2.1.1 整除与带余除法

定义2.1.1 设$a,b\in\mathbf{Z}$, $b\neq 0$. 如果存在$q\in\mathbf{Z}$使得$a=qb$, 那么就称a可被b整除或者b整除a, 记为$b|a$, 且称a是b的**倍数**, b是a的**因子**(也可称为**约数**或**除数**). 若a不能被b整除, 则记为$b\nmid a$.

定义2.1.2 若b为a的因子, 且$b\neq\pm 1, b\neq\pm a$, 则称b为a的**真因子**.

定理2.1.1 设$a,b\in\mathbf{Z}$, 则有

(1)$b|a \Leftrightarrow -b|a \Leftrightarrow b|-a \Leftrightarrow |b|\,\big|\,|a|$;

(2)设$a\neq 0$, 如果$b|a$, 那么$|b|\leq|a|$.

定理2.1.2 设$a,b,c\in\mathbf{Z}$,

(1)若$b|a$且$c|b$, 则$c|a$;

(2)若$b|a$, 则$b|ac$;

(3)设$c \neq 0$, 则$b|a\ bc|ac$;

(4)$b|a$且$b|c\Leftrightarrow$对任意的$m,n\in\mathbf{Z}$有$b|am+cn$.

良序原理 每一个由非负整数组成的非空集合**S**必定含有一个最小元素, 也就是说, **S**中存在一个元素a, 对任意$b\in$**S**, 都有$a<b$成立.

定理2.1.3 设a和b为任意整数, $b>0$, 则存在唯一的一对整数q和r, 使

$$a = qb + r, \qquad 0 \leq r \leq b.$$

其中a称为**被除数**, q称为**商**, r称为**余数**(或**非负最小剩余**).

定义2.1.3 设$a, q, r \in \mathbf{Z}$, 满足$a = 2q + r$, $0 \leq r < 2$. 若$r = 0$, 称a为**偶数**；若$r=1$, 称a为**奇数**.

定义2.1.4 一个大于1的整数p, 若仅以1和自身p为其正因子, 则称p为**素数**(或**质数**). 除1以外非素的正整数则称为**合数**(或**复合数**).

定理2.1.4 素数有无穷多个.

定理2.1.5 对任意正整数n, 存在素数p满足$n<p\leq n!+1$.

定理2.1.6 如果整数$n\geq 2$, 那么在$n!+2$与$n!+n$之间必没有素数.

定理2.1.7 若n为合数, 则n必有素因子p满足$p\leq\sqrt{n}$.

2.1.2 最大公因子与辗转相除法

定义2.1.5 设$a_1,a_2,\ldots,a_n$是n个不全为零的整数. 若整数d是它们之中每一个数的因子, 那么d就称为$a_1,a_2,\ldots,a_n$的一个**公因子**. 在整数$a_1,a_2,\ldots,a_n$的所有公因子中最大的一个称为**最大公因子**, 记作$(a_1,a_2,\ldots,a_n)$或者$\gcd(a_1,a_2,\ldots,a_n)$. 特别地, 若$(a_1,a_2,\ldots,a_n)=1$, 我们称$a_1,a_2,\ldots,a_n$**互素**(或**互质**).

定理2.1.8 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$(a,b)=(b,c)$.

定理2.1.9 若任给两个正整数a和b, 则(a,b)就是下式中最后一个不等于零的余数, 即(a,b) $= r_n$.

$$a = bq_1 + r_1, 0 < r_1 < b,$$

$$b = r_1 q_2 + r_2, 0 < r_2 < r_1,$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_n q_{n+1} + r_{n+1}, \qquad r_{n+1} = 0$$

定理2.1.10 若任给两个正整数a和b, 则存在两个整数m,n, 使得

$$(a,b) = ma + nb.$$

即(a,b)是a和b的线性组合.

定理2.1.11 设整数a,b,c满足$c|a$且$c|b$, 则$c|(a,b)$.

定理2.1.12 设有整数a,b,c, 其中$c>0$, 则$(ac,bc)=(a,b)c$.

定理2.1.13 整数a,b互素的充分必要条件是存在整数x,y, 使得

$$xa+yb=1.$$

定理2.1.14 设有整数a,b,c, 若$a|bc$且$(a,b)=1$, 则$a|c$.

定理2.1.15 设$a_1,a_2,\dots,a_n$是n个整数, 其中$a_1\neq 0$. 令

$$(a_1,a_2)=d_2,(d_2a_3)=d_3,\dots,(d_{n-1},a_n)=d_n,$$

则

$$(a_1,a_2,\dots,a_n)=d_n.$$

定义2.1.6 设$a_1,a_2,\dots,a_n$是n个整数，若m是这n个数中每一个数的倍数，则m就称为这n个数的一个**公倍数**. 在$a_1,a_2,\dots,a_n$的所有公倍数中最小的正整数称为**最小公倍数**，记作$[a_1,a_2,\dots,a_n]$.

定理2.1.16 设a和b为任意两个互素正整数，则其乘积即为最小公倍数.

定理2.1.17 设a和b为任意正整数，则

(1) 若m是a,b的任一公倍数，则$[a,b]|m$;

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

定理2.1.18 设$a_1,a_2,\ldots,a_n$是n个整数, 令

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

则

$$[a_1,a_2,\ldots,a_n]=m_n.$$

定理2.1.19 设$a_1,a_2,\ldots,a_n$是n个正整数, 如果$a_1|m$, $a_2|m$,…, $a_n|m$, 则

$$[a_1,a_2,\ldots,a_n]|m.$$

2.1.3 连分数

定义2.1.7 设$a_0,a_1,a_2,\ldots,a_n$是一个实数列, 除a_0以外都大于0. 对于整数$n\geq 0$, 我们将分数

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots+\cfrac{1}{a_n}}}} \qquad (2.1.4)$$

叫作n阶有限连分数. 当a_0是整数, $a_1,a_2,\ldots,a_n$都是正整数时, 该分数叫作n阶有限简单连分数. 为书写方便，将上式简记为$[a_0,a_1,\ldots,a_n]$.

我们将有限连分数

$$[a_0,a_1,\ldots,a_k], 0\leq k\leq n$$

叫作有限连分数(2.1.4)式的第k个渐进分数.

当(2.1.4)式中的$n\to\infty$时，则分数

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots}}} \qquad (2.1.7)$$

叫作无限连分数，可简记为

$$[a_0,a_1,a_2,\ldots].$$

当a_0是整数，$a_1,\ldots,a_n$都是正整数时，分数(2.1.7)叫作无限简单连分数. 我们将有限连分数

$$[a_0,a_1,\ldots,a_k],\ k\geq 0$$

叫作无限连分数(2.1.7)的第k个渐进分数.

定理2.1.20 若使连分数$[a_0,a_1,\ldots,a_n]$的渐进分数分别为

$$[a_0,a_1,\ldots,a_i]=\frac{p_i}{q_i},\quad 0\le i\le n,$$

则这些渐进分数间有关系

$$\begin{aligned} p_0 &= a_0, & p_1 &= a_1a_0+1, & \ldots, && p_k &= a_kp_{k-1}+p_{k-2}, \\ q_0 &= 1, & q_1 &= a_1, & \ldots, && q_k &= a_kq_{k-1}+q_{k-2}, \end{aligned}$$

其中$2\le k\le n$.

定理2.1.21 若连分数$[a_0,a_1,\ldots,a_n]$的渐进分数分别为

$$[a_0,a_1,\ldots,a_k]=\frac{p_k}{q_k},\ 0\le k\le n,$$

则p_k和q_k满足

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1},\qquad 1\le k\le n,$$

$$p_kq_{k-2}-p_{k-2}q_k=(-1)^k a_k,\qquad 2\le k\le n.$$

定理2.1.22 对于简单连分数, 我们有

(1) 当k≥2时, $q_k \geq q_{k-1}+1$, 因而对任何k来说, $q_k \geq k$;

(2) $\frac{p_{2k+1}}{q_{2k+1}} < \frac{p_{2k-1}}{q_{2k-1}}, \frac{p_{2k}}{q_{2k}} < \frac{p_{2k-2}}{q_{2k-2}}, \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+1}}{q_{2k+1}}$;

(3) $\frac{p_k}{q_k}$为既约分数, 即p_k与q_k互素.

定理2.1.23 每一个简单连分数表示一个实数.

定理2.1.24 任一无理数可表示成无限简单连分数.

定理2.1.25 任一无理数只可表示成唯一的无限简单连分数.

定理2.1.26 (1) 若有理分数$\alpha = [a_0, a_1, \dots, a_n] = [b_0, b_1, \dots, b_m]$, 且$a_n > 1, b_m > 1$, 则有

$$m = n, a_i = b_i (i = 0,1, \dots, n).$$

(2) 任一有理分数α有且仅有两种有限简单连分数表示式, 即

$$\alpha = [a_0, a_1, \dots, a_n] = [a_0, a_1, \dots, a_n - 1,1],$$

其中a_n＞1.

定义2.1.8 对于无限简单连分数$[a_0, a_1, a_2, \dots]$, 如果存在整数m≥0, 且对于m存在正整数k使得对于所有n≥m, 有

$$a_{n+k} = a_k \text{ ,}$$

那么, 我们把这个无限简单连分数叫作**循环简单连分数**, 简称**循环连分数**, 记为

$$[a_0, a_1, \dots, a_{m-1}, \overline{a_m, \dots, a_{m+k-1}}].$$

显然, $\sqrt{3} = [1, \overline{1,2}]$是循环连分数.

2.1.4 算术基本定理

定理2.1.27 设p为素数且$p|ab$, 则$p|a$或$p|b$.

推论 设p为素数, 若$p|a_1a_2...a_n$, 其中$a_1,a_2,...,a_n$是n个整数, 则$p|a_1,p|a_2,...,p|a_n$至少有一个成立.

定理2.1.28 设$a_1,a_2,...,a_n$,c是整数, 如果$(a_i,c) = 1$, $1 \leq i \leq n$, 则 $(a_1a_2...a_n,c) = 1$.

定理2.1.29 任一大于1的整数都可以表示成素数的乘积, 且在不考虑乘积顺序的情况下, 该表达式是唯一的. 即

$$n = p_1 p_2 \ldots p_s, p_1 \le p_2 \le \cdots \le p_s,$$

其中$p_1, p_2, \ldots, p_s$是素数, 并且若

$$n = p_1 p_2 \ldots p_t, p_1 \le p_2 \le \cdots \le p_t,$$

其中$q_1, q_2, \ldots, q_t$是素数, 则$s = t, p_i = q_i (i = 1,2, \ldots, s)$.

以上定理被称为**算术基本定理**, 也叫作整数的**唯一分解定理**.

推论 任一大于1的整数都能够唯一地表示成

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}, \alpha_i > 0, i = 1,2, \ldots, s$$

其中$p_i < p_j$ $(i < j)$是素数. 上式称为n的**标准分解式**.

定理2.1.30 设n是大于1的任一整数，其标准分解式由$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_s}^{\alpha_s}, \alpha_i > 0, i = 1,2,\ldots,s$式给出，那么$d$是$n$的正因子的充要条件是

$$d = {p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_s}^{\beta_s}, \alpha_i \geq \beta_i \geq 0, i = 1,2,\ldots,s.$$

定理2.1.31 设正整数n的标准分解式为

$$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_s}^{\alpha_s}, \alpha_i > 0, i = 1,2,\ldots,s.$$

$\tau(n)$表示n的所有正因子的个数，则

$$\tau(n) = \tau({p_1}^{\alpha_1})\tau({p_2}^{\alpha_2})\ldots\tau({p_s}^{\alpha_s}) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_s + 1).$$

定理2.1.32 设a,b为两个正整数，其素因子分解式分别为

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},\ \alpha_i \geq 0,\ i = 1,2,\dots,s,$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s},\ \beta_i \geq 0,\ i = 1,2,\dots,s,$$

那么

$$(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s},\ \gamma_i = \min(\alpha_i,\beta_i),\ i = 1,2,\dots,s,$$

$$[a,b] = p_1^{\delta_1} p_2^{\delta_2} \dots p_s^{\delta_s},\ \delta_i = \min(\alpha_i,\beta_i),\ i = 1,2,\dots,s.$$

对于任意的整数α,β，显然有

$$\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta,$$

由此可得

$$(a,b)[a,b] = ab.$$

2.1.5 梅森素数和费马素数

定义2.1.9 若正整数n的所有正因子之和等于$2n$, 则n称为**完全数**.

定理2.1.33 若正整数n的标准分解式为

$$\mathrm{n} = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \ldots {p_s}^{\alpha_s},$$

则

$$\sigma(n) = \frac{{p_1}^{\alpha_1+1}-1}{p_1-1} \ldots \frac{{p_s}^{\alpha_s+1}-1}{p_s-1}.$$

定理2.1.34 若$2^n - 1$为素数, 则$2^{n-1}(2^n - 1)$为偶完全数, 且无其他偶完全数存在.

定理2.1.35 若2^n-1为素数，则n必为素数.

定义2.1.10 设p是一个素数，形如2^p-1的数叫作**梅森数**，记为$M_p=2^p-1$. 当M_p为素数时，则称其为**梅森素数**.

定理2.1.36 若2^m+1为素数，则$m=2^n$.

定义2.1.11 若n为非负整数，则称$F_n=2^{2^n}+1$为**费马数**. 当F_n为素数时，则称其为**费马素数**.

定理2.1.37 任给两个费马数F_a, F_b, $a\neq b$，则F_a, F_b互素.

课后习题----解答题

- 1. 求如下整数对的最大公因子：
  （1）$(55, 85)$；（2）$(202, 282)$；（3） $(666, 1414)$；
  （4）$(20785, 44350)$.

- 2. 求如下整数对的最小公倍数：
  （1）$(231, 732)$；（2） $(-871, 728)$.

- 3. 求以下整数的标准分解式：
  （1）36；（2）69；（3）200；（4）289.

- 4. 设 a 为正整数，问$a^4 - 3a^2 + 9$是素数还是合数？

课后习题---证明题

- 1. 证明若 2|n， 5|n， 7|n， 那么 70|n .
- 2. 证明任意三个连续的正整数的乘积都被6整除.
- 3. 证明每个奇数的平方都具有 8k+1 的形式.
- 4. 证明若 m-p|mn+pq， 则 m-p|mq+np .
- 5. 证明若 a 是整数， 则$a^3 - a$能被3整除.
- 6. 证明对于任意给定的正整数 k， 必有 k 个连续的正整数都是合数.
- 7. 证明若整数 a,b 满足 (a,b)=1， 那么 (a+b,a-b)=1 或2.
- 8. 证明若整数 a,b 满足 (a,b)=1， 那么 $(a+b, a^2+b^2) = 1$或2.
- *9. 证明若 m,n,a 为正整数且 a>1， 则有$(a^m-1, a^n-1) = a^{(m,n)} - 1$.

课后习题---证明题

- 10. 证明$12|n^4+2n^3+11n^2+10n$.
- 11. 设$3|a^2+b^2$，证明$3|a$且$3|b$.
- 12. 设 n,k 是正整数，证明n^k与n^{k+4}的个位数字相同.
- 13. 证明对于任何整数 n,m，等式$n^2+(n+1)^2=m^2+2$不可能成立.
- *14. 证明对于任意给定的 n 个整数，必可以从中找出若干个数作和，使得这个和能被 n 整除.
- 15. 证明在$1,2\cdots,2n$中任取 n+1 个数，其中至少有一个能被另一个整除.
- *16. 证明$1+\frac{1}{2}+\cdots+\frac{1}{n}(n\geq 2)$不是整数.
- 17. 证明 n 的标准分解式中次数都是偶数当且仅当 n 是完全平方数.
- 18. 证明$\sqrt[3]{5}$为无理数.

课后习题---练习题

- 1. 利用Eratosthenes筛法求出500内的全部素数.
- 2. 编写程序求1000000内的所有素数.
- 3. 编写程序计算整数 a,b 的最大公因子.
- 4. 编写程序求正整数 n 的素因子分解.

第 2 节

同余

定义2.2.1 给定一个正整数m, 如果用m去除两个整数a和b所得的余数相同, 则称a和b模m**同余**, 记作

$$a \equiv b(mod\ m);$$

否则, 称a和b模m**不同余**, 记作

$$a \not\equiv b(mod\ m).$$

关系式$a \equiv b(mod\ m)$称为模m的同余式, 或简称**同余式**.

定理2.2.1 整数a和b模m同余的充要条件是$m|a-b$.

定理2.2.2 整数a和b模m同余的充要条件是存在一个整数k使得

$$a = b + km.$$

定理2.2.3 同余具有等价关系, 即

(1) 自反性：$a \equiv a(mod\ m)$；

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

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

定理2.2.4 设a_1, a_2, b_1, b_2为四个整数, 如果

$$a_1 \equiv b_1(mod\ m), \qquad a_2 \equiv b_2(mod\ m)$$

则有

(1) $a_1x + a_2y \equiv b_1x + b_2y(mod\ m)$, 其中$x, y$为任意整数；

(2) $a_1a_2 \equiv b_1b_2(mod\ m)$；

(3) $a_1^n \equiv b_1^n(mod\ m)$, 其中$n$>0.

定理2.2.5 设$f(t)=a_nt^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$与$g(t)=b_nt^n+b_{n-1}t^{n-1}+\cdots+b_1+b_0$是两个整系数多项式, 满足

$$a_i\equiv b_i(mod\ m),\qquad 0\le i\le n,$$

那么, 若$x\equiv y(mod\ m)$, 则

$$f(x)\equiv g(x)(mod\ m).$$

定理2.2.6 若$ac \equiv bc(mod\ m)$, 且$(c,m) = d$, 则$a \equiv b(mod\ \frac{m}{d})$.

定理2.2.7 若$a \equiv b(mod\ m)$, 则有$ak \equiv bk(mod\ mk)$, 其中k为正整数.

定理2.2.8 若$a \equiv b(mod\ m)$, 且有正整数d满足$d|m$, 则$a \equiv b(mod\ d)$.

定理2.2.9 若$a \equiv b(mod\ m_i)$, $i = 1,2,\ldots,n$, 则

$$a \equiv b(mod\ [m_1, m_2, \ldots, m_n]).$$

定理2.2.10 若$a \equiv b(mod\ m)$, 则$(a,m) = (b,m)$.

2.2.2 剩余类和欧拉定理

定义2.2.2 设m是一给定正整数，令C_r表示所有与整数r模m同余的整数所组成的集合，则任意一个这样的C_r叫作模m的一个**剩余类**。一个剩余类中的任一数叫作该类的**代表元**。

定理2.2.11 设m为一正整数，$C_0,C_1,\ldots,C_{m-1}$是模m的剩余类，则

(1) 任一整数恰包含在一个C_r中，这里$0\leq r\leq m-1$；

(2) $C_a = C_b$的充要条件是$a \equiv b(mod\ m)$；

(3) C_a与C_b的交集为空集的充要条件是a和b模m不同余.

定义2.2.3 在模m的剩余类$C_0,C_1,\ldots,C_{m-1}$中各取一代表元$a_i\in C_i$, $i=0,1,\ldots,m-1$, 则此m个数$a_0,a_1,\ldots,a_{m-1}$称为模m的一个完全剩余系.

定理2.2.12 m个整数$a_0,a_1,\ldots,a_{m-1}$为模m的一个完全剩余系的充要条件是它们两两模m不同余.

定义2.2.4 对于正整数m,

(1) $0,1,\ldots,m-1$为模m的一个完全剩余系, 叫作模m的最小非负完全剩余系;

(2) $1,2,\ldots,m-1,m$为模m的一个完全剩余系, 叫作模m的最小正完全剩余系;

(3) $-(m-1),\ldots,-1,0$为模m的一个完全剩余系, 叫作模m的最大非正完全剩余系;

(4) $-m,-(m-1),\ldots,-1$为模m的一个完全剩余系, 叫作模m的最大负完全剩余系.

定理2.2.13 设k是满足$(k,m)=1$的整数，b是任意整数，若$a_0,a_1,\ldots,a_{m-1}$是模m的一个完全剩余系，则$ka_0+b,\ ka_1+b,\ldots,\ ka_{m-1}+b$也是模$m$的一个完全剩余系. 即若$x$遍历模$m$的一个完全剩余系，则$kx+b$也遍历模$m$的一个完全剩余系.

定理2.2.14 若x_i $(i=0,1,\ldots,m_1-1)$是模m_1的完全剩余系，y_j $(j=0,1,\ldots,m_2-1)$是模m_2的完全剩余系，其中$(m_1,m_2)=1$，则$m_2x_i+m_1y_j$ $(i=0,1,\ldots,m_1-1,\ j=0,1,\ldots,m_2-1)$是模$m_1m_2$的完全剩余系.

定义2.2.5 与模m互素的剩余类的个数记为$\varphi(m)$，$\varphi(m)$称为**欧拉函数**.

定义2.2.6 在与模m互素的 个剩余类中, 各取一个代表元

$$a_1, a_2, \dots, a_{\varphi(m)},$$

它们所组成的集合叫作模m的一个缩剩余系, 简称为缩系.

定理2.2.15 若$a_1, a_2, \dots, a_{\varphi(m)}$是$\varphi(m)$个与$m$互素的整数, 则$a_1,a_2,\dots, a_{\varphi(m)}$是模$m$的一个缩系的充要条件是它们两两模$m$不同余.

定理2.2.16 若a是满足$(a,m) = 1$的整数$a_1, a_2, \dots, a_{\varphi(m)}$是模$m$的一个缩系, 则$aa_1, aa_2, \dots, aa_{\varphi(m)}$ 也是模m的一个缩系. 即若x遍历模m的一个缩系, 则ax也遍历模m的一个缩系.

定理2.2.17 若a是满足$(a,m)=1$的整数, 则存在整数c, $1\leq c< m$且$(c,m)=1$, 使得

$$ac \equiv 1 (mod\ m).$$

定理2.2.18 设m是大于1的整数, 若a是满足$(a,m)=1$的整数, 则

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

定理2.2.18又称作**欧拉定理**, 通过这个定理可推出著名的**费马小定理**, 即定理2.2.19.

定理2.2.19 若p是素数, 则对任意整数a, 有

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

定理2.2.20 设m_1,m_2为互素的两个正整数, 若x_1,x_2分别遍历模m_1和模m_2的缩系, 则$m_2x_1 + m_1x_2$遍历模m_1m_2的缩系.

定理2.2.21 设m_1,m_2为互素的两个正整数, 则

$$\varphi(m_1 m_2)=\varphi(m_1)\varphi(m_2).$$

定理2.2.22 设m有标准分解式

$$m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s},\alpha_i>0,\mathrm{i}=1,2,\ldots,s,$$

则

$$\varphi(m)=m\prod_{i=1}^{s}(1-\frac{1}{p_i}).$$

2.2.3 线性同余方程

定义2.2.6 设多项式

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0,$$

其中$n>0$, $a_i\,(i=0,1,\ldots,n)$是整数, 又设$m>0$, 则同余式

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

称为模m的同余方程. 若a_n不能被m整除, 则n称为$f(x)$的次数, 记为$degf(x)$.

定理2.2.23 设$(a,m)=1$, 则同余方程

$$ax \equiv b(mod\ m)$$

有且仅有一个解$x \equiv ba^{\varphi(m)-1}(mod\ m)$.

定理2.2.24 设$(a,m)=d$, 则同余方程$ax \equiv b(mod\ m)$有解的充要条件是$d|b$. 并且在$ax \equiv b(mod\ m)$有解时, 它的解数为d, 以及若$x \equiv x_0(mod\ m)$是$ax \equiv b(mod\ m)$ 的特解, 则它的d个解为

$$x \equiv x_0 + \frac{m}{d}t(mod\ m),$$

其中$t=0,\ldots,d-1$.

定义2.2.8 对于正整数m和整数a, 满足$(a,m)=1$, 则存在唯一一个剩余类, 从中任意选择的元素整数，都会使

$$aa' \equiv 1(mod\ m)$$

成立, 此时称a'为a的模m逆元, 记作$a^{-1}(mod\ m)$.

推论 满足定理2.2.24条件的一次同余方程

$$ax \equiv b(mod\ m)$$

的全部解为

$$x \equiv \frac{b}{d}\left(\left(\frac{a}{d}\right)^{-1}\left(mod\ \frac{m}{d}\right)\right)+\frac{m}{d}t(mod\ m),$$

其中$t=0,1,\dots,d-1$.

2.2.4 孙子定理与同余方程组

定理2.2.25(孙子定理/中国剩余定理) 设$m_1, m_2, \dots, m_k$是k个两两互素的正整数, 若令

$$m = m_1 m_2 \dots m_k, m = m_i M_i, i = 1,2, \dots, k,$$

则对任意的整数$b_1, \dots, b_k$, 同余方程组

$$\begin{cases} x \equiv b_1 (mod\ m_1) \\ x \equiv b_2 (mod\ m_2) \\ \quad\quad \vdots \\ x \equiv b_k (mod\ m_k) \end{cases}$$

有唯一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k (mod\ m),$$

其中

$$M_i' M_i \equiv 1 (mod\ m_i), i = 1,2, \dots, k.$$

定理2.2.26 设$m_1, m_2, \ldots, m_k$是k个两两互素的正整数，令

$$m = m_1 m_2 \ldots m_k,$$

$$m = m_i M_i,$$

$$M_i' M_i \equiv 1 (mod\ m_i), i = 1,2, \ldots, k,$$

若$b_1, b_2, \ldots, b_k$分别遍历模$m_1, m_2, \ldots, m_k$的完全剩余系，则

$$M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k$$

遍历模m的完全剩余系.

定理2.2.27 同余方程组

$$\begin{cases} x \equiv b_1\ (mod\ m_1) \\ x \equiv b_2\ (mod\ m_2) \end{cases}$$

有解的充要条件是$(m_1, m_2) | b_1 - b_2$. 如果上述条件成立，则同余方程组模(m_1, m_2)有唯一解.

定理2.2.28 设$m_{1,}m_2,\ldots,m_k$是k个两两互素的正整数, 令$\mathrm{m}=m_1m_2\ldots m_k$, 则同余方程

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

与同余方程组

$$\begin{cases} x\equiv b_1(mod\ m_1) \\ x\equiv b_2(mod\ m_2) \\ \quad\vdots \\ x\equiv b_k(mod\ m_k) \end{cases}$$

等价. 若用T_i表示同余方程

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

的解数（即解的个数）, $i=1,2,\ldots,k$, 用T表示同余方程$f(x)\equiv 0(mod\ m)$的解数, 则

$$T=T_1T_2\ldots T_k.$$

定理2.2.29 矩阵K在模26运算下存在可逆矩阵的充分必要条件是(det K,26)=1（det K表示矩阵K的行列式的值）.

定理2.2.30 如果二阶矩阵

$$K=\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

可逆, 则其逆矩阵为

$$K^{-1}=(\det K)^{-1}\begin{pmatrix} k_{11} & -k_{12} \\ -k_{21} & k_{22} \end{pmatrix}(mod\ 26).$$

2.2.5 高次同余方程

定理2.2.31 设$x \equiv x_1 (mod\ p)$是同余方程

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

的一个解, 且满足$(f'(x_1), p)$=1, 则同余方程$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$有解

$$x \equiv x_\alpha (mod\ p^\alpha).$$

其中x_α由以下关系式递归得到：

$$\begin{cases} x_i \equiv x_{i-1} + p^{i-1} t_{i-1} & (mod\ p) \\ t_{i-1} \equiv -\dfrac{f(x_{i-1})}{p^{i-1}} \left((f'(x_1))^{-1} (mod\ p) \right) & (mod\ p) \end{cases}$$

i = 2,3,…,α . 这里, $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$表示$f(x)$的导函数.

定理2.2.32 设

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

为n次整系数多项式,

$$g(x) = x^m + b_{m-1} x^{n-1} + \cdots + b_1 x + b_0$$

为m次首一（最高项系数为1）整系数多项式, 其中m≥1, 则存在整系数多项式$q(x)$和r(x)使得

$$f(x) = g(x)q(x) + r(x),$$

其中deg r(x) ＜deg $g(x)$.

定理2.2.33 同余方程$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (mod\ p)$与一个次数小于$p$ 的模p 的同余方程等价.

定理2.2.34(拉格朗日(Lagrange)定理) 同余方程$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (mod\ p)$最多有$n$个解.

定理2.2.35 如果同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 (mod\ p)$$

的解的个数大于n, 则$p | a_i, i = 0,1, \ldots, n$.

定理2.2.36 如果同余方程$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0(mod\ p)$

有k个不同的解

$$x \equiv x_i(mod\ p), i = 1,2, \ldots, k, 1 \le k \le n,$$

则对任意整数x，均有

$$f(x) \equiv (x - x_1)(x - x_2) \ldots .(x - x_n) f_k(x)(mod\ p),$$

其中$f_k(x)$是首项系数为a_n的$n - k$次多项式.

定理2.2.37 对于素数p与正整数$n, n \le p$, 同余方程

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0(mod\ p)$$

有n个解的充要条件是$x^p - x$被$f(x)$除所得余式的所有系数均能被p整除.

课后习题---解答题

- 1. 求7^{2046}写成十进制数时的个位数.
- 2. 求2^{1000}的十进制表示中的末尾两位数字.
- 3. 求$1^5+2^5+3^5+\cdots+99^5$被4除的余数.
- 4. 计算555^{555}被7除的余数.
- 5. 写出模9的一个完全剩余系，满足:

  (1)其中的每个数都是奇数;

  (2)其中的每个数都是偶数.
- 6. 求模11的一个完全剩余系$\{r_1,r_2,\cdots r_{11}\}$，使得$r_i\equiv 1(mod\ 3),1\le i\le 11$.
- 7. 计算以下整数的欧拉函数:

  (1) 24；(2) 64；(3) 187；(4) 360.

课后习题---解答题

- 8. 利用费马小定理求解以下题目：
- (1)求数$a(0 \le a < 73)$，使得$a \equiv 9^{794}(mod\ 73)$.
- (2) 解方程$x^{86} \equiv 6(mod\ 29)$.
- (3) 解方程$x^{39} \equiv 3(mod\ 13)$.
- 9. 求$229^{-1}(mod\ 281)$.
- 10. 如果 m>3， 解释$\varphi(m)$为什么总是偶数.
- *11. 列出所有$\varphi(m)$不能被4整除的m.
- 12. 求解下列一次同余方程：
- (1) $27x \equiv 12(mod\ 15)$
- (2) $24x \equiv 6(mod\ 81)$
- (3) $91x \equiv 26(mod\ 169)$
- (4) $71x \equiv 32(mod\ 3441)$

课后习题---解答题

- 13. 如果在一个密码系统中，明文 x 被加密成密文y，使得$y \equiv 7x + 3(mod\ 26)$，那么由密文y 解密得到明文 x 的公式是什么？

- 14. 求解线性同余方程组.

$$(1)\begin{cases} x \equiv 9(mod\ 12) \\ x \equiv 6(mod\ 25) \end{cases}$$

$$(2)\begin{cases} x \equiv 5(mod\ 7) \\ x \equiv 12(mod\ 15) \\ x \equiv 18(mod\ 22) \end{cases}$$

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

- 15. 有总数不满50人的一队士兵. 一至三报数，最后一人报"一"；一至五报数，最后一人报"二"；一至七报数，最后一人也报"二". 这队士兵有多少人?
- 16. 利用转化成联立方程组的方法解$91 \equiv 419(mod\ 440)$.
- 17. 求13的倍数，使得该数被3, 5, 7, 11除所得的余数均为2.
- 18. 求相邻的4个整数，它们依次可被$2^2, 3^2, 5^2, 7^2$整除.
- 19. 已知Hill密码中的明文分组长度是2，密钥**K**是一个2阶可逆方阵. 假设明文3, 14, 2, 19所对应的密文是1, 14, 11, 21，试求密钥**K**.
- 20. 求解同余方程

$$3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0(mod\ 5).$$

课后习题---证明题

- 1. 证明正整数 n （十进制）能被3整除的充要条件是将 n 的各位数字相加所得之和能被3整除.
- 2. 设 f(x) 是整系数多项式，且$f(1), f(2), \cdots, f(m)$都不能被 m 整除，证明 f(x)=0 没有整数解.
- 3. 证明当 m>2 时，$0^2, 1^2, \cdots, (m-1)^2$一定不是模m 的完全剩余系.
- 4. 设有 m 个整数，它们都不属于模 m 的0剩余类，证明其中必有两个数属于同一剩余类.
- 5. 证明$2, 2^2, 2^3, \cdots, 2^{18}$是模27的一个缩系.

课后习题---证明题

- 6. 证明如果 a 是整数，且 $(a,3)=1$，那么$a^7 \equiv a(mod\ 63)$.
- 7. 证明 m>3 时，$\varphi(m)$总是偶数.
- 8. 证明不存在整数 n 满足$\varphi(n)=14$.
- 9. 设 a>2 是奇数，证明

  (1) 一定存在正整数$d \le a-1$，使得$a|2^d-1$;

  (2) 若d_0是满足(1)的最小正整数，那么$a|2^h-1$的充要条件是$d_0|h$.

- 10. 证明同余方程$2x^3-x^2+3x+11 \equiv 0(mod\ 5)$有3个解.

课后习题---练习题

- 1. 编写计算正整数欧拉函数的程序.

- 2. 编程判断两个正整数 m,n 是否互素，如果互素，求出 $m^{-1}(mod\ n)$和$n^{-1}(mod\ m)$.

- 3. 编程判断同余方程$ax \equiv b(mod\ m)$是否有解，如果有解，求出所有的解.

- 4. 编程实现中国剩余定理.