信息安全数学基础

密码学基础和数论基础

作者： 熊睿 & Stander-by

组织： HUST-CSE-2004

时间： Mar 7, 2022

版本： 1.0

学习新思想，争做新青年。

特别声明

该笔记是于 2022 年 3 月 7 日开始，针对华中科技大学网络空间安全学院 2020 级信息安全数学基础课程编制的笔记，该课程使用的是 HUST-CSE 汤学明老师所著的《信息安全数学基础》，还有中国科学院大学的陈恭亮老师所编著的《信息安全数学基础》，陈恭亮老师也是汤老师在 WHU 读研的导师。学有余力时，还应去翻阅华罗庚的著作《数论引导》。

该课程所运用的主要编程环境是开源的 SageMath，同时根据需要可以使用 python 和 mathematical 等。

SageMath-GitHub 网址：https://github.com/sagemath/

该课程前有《离散数学》打基础，后为《密码学原理》铺路，是理论实践之间的桥梁，理解抽象知识，提高解决实际数学、密码学问题的能力。

同时使用优美的 LaTeX 来书写，也少不了 WHU 好友的鼎力推荐 (Thanks)，也希望能通过这次机会，去熟悉 LaTeX 的语法，特别是数学公式的编写，和作图能力。

另外，“多分享，多奉献”，之后我会将文档同步于我的 Github 账号，由于编者的水平有限，会存在一些难免的疏漏和问题，请大家批评指正！

我的 GitHub 网址：https://github.com/Stander-by/

我的邮件：`xiongruistanderby@gmail.com`

NodeBB 校内网: http://10.12.162.1:5881/

NodeBB 校外网: http://124.71.166.97:5881/

Stander-by

Mar 7, 2022

目录

第 1 章 整除

第一章讲述整数整除中带余除法、因子、最大公因数、最小公倍数和算术基本定理等基本概念，希望通过从带余除法到最终的算术基本定理的推导过程，掌握整数研究的一般方法，在第三章多项式的唯一因式分解定理的推到过程中，用到这种系统化的方法。

1.1 整除性

定理 1.1 (带余除法)

任意给定整数 a 和整数 b>0，存在唯一的一对整数 q，$0 \leq r < b$，使得：$a = qb + r$。

推论 1.1

任意给定整数 a 和整数 b<0，存在唯一的一对整数 q，$0 \leq r < |b|$，使得：$a = qb + r$。

推论 1.2

任意给定整数 a，c 和整数 b≠0，存在唯一的一对整数 q，$c \leq r < |b| + c$，使得 $a = qb + r$。

定理 1.2 (整除性质)

设 a，b，c 为整数

(1) 若 $a \mid b$，$b \mid a$，则 $a = \pm b$;

(2) 设整数 $k \neq 0$，若 $a \mid b$，则 $\pm ka \mid \pm kb$，反之亦然；

(3) 对任意整数 k，若 $a \mid b$，则 $a \mid kb$;

(4) 若 $a \mid b$，$b \neq 0$，则 $\frac{b}{a} \mid b$;

(5) 若 $a \mid b$，$b \mid c$，则 $a \mid c$;

(6) 若 $a \mid b$，$a \mid c$，则对任意整数 s 和 t，$a \mid sb + tc$;

例题 1.1 若 a 是整数，证明 $a^3 - a$ 是 6 的倍数。

证明

$a^3 - a = (a-1)a(a+1)$

由定理 1.2之 (3) 有，$3 \mid (a-1)a(a+1)$，可设 $(a-1)a(a+1) = 3q$。

同理，因为两个连续的整数中一定有一个是 2 的倍数，所以 $2 \mid (a-1)a(a+1)$，不妨设 $q = 2t$，于是 $(a-1)a(a+1) = 6t$，根据整除的定义，$6 \mid (a-1)a(a+1)$。

例题 1.2 若 x，y 为整数，证明：$10 \mid 2x + 5y \Leftrightarrow 10 \mid 4x + 5y$。

证明

由定理 1.2之 (4) 有

$4x + 5y = 10(x + 2y) - 3(2x + 5y)$

$2x + 5y = 3(4x + 5y) - 10(x + y)$

练习 1.1

1) 是否存在 n，使得 $n + 1 \mid n!$?

2) 如果 $n \mid x^2 - y^2$，那么 $n \mid x + y$ 或者 $n \mid x - y$ 是否成立？

笔记

1.2 欧几里得辗转相除法

定义 1.1

(a, b) $gcd(a, b)$ 表示为 a 和 b 的最大公因数。♣

定理 1.3

设 a，b 是两个不全为 0 的整数，且 $a = qb + r$，r 为整数，则 $(a, b) = (b, r)$。♡

证明

设 $d = (a, b)$ $d' = (b, r)$

由定理 1.2 (6) 得，$d \mid (a - qb)$ 即 $d \mid r$

且 $d \leq d'$，所以 $d = d'$。

推论 1.3

设 a，b 是两个不全为 0 的整数，q 为整数，则 $(a, b) = (a \pm bq, b) = (a, b \pm aq)$。♡

例题 1.3 证明：若 n 为整数，则 $(21n + 4, 14n + 3) = 1$，$(n^3 + 2n, n^4 + 3n^2 + 1) = 1$。

定理 1.4 (辗转相除法)

设 a，b 是两个正整数，下式为起欧几里得辗转相除算式

令 $r_0 = a \quad r_1 = b$，反复运用带余除法算式：

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_1 + r_3 & 0 \leq r_3 < r_2 \\
&\vdots & \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_n + r_{n+1} & r_{n+1} = 0
\end{aligned}
$$

由于 $r_{n+1} < r_n < r_{n-1} < \dot{<} r_2 < r_1 = b$，且 b 为有限正整数，所以经过有限的正整数，所以经过有限的步骤，必然存在 n，使得 $r_{n+1} = 0$。

(1) $(a, b) = r_n$

(2) 存在整数 s，t，使得 $r_n = sa + tb$

(3) 任意整数 c，若满足 $c \mid a$ 且 $c \mid b$，则 $c \mid r_n$ ♡

定理 1.5

设 a，b 是两个正整数，q_i 为其欧几里得辗转相除算式的部分商，则由

$$
\begin{aligned}
S_0 &= 0 \\
S_1 &= 1 \\
S_{i+1} &= S_{i-1} - q_{n-i} S_i \quad i \geq 1
\end{aligned}
$$

所得的 S_{n-1} 和 S_n 满足 $S_{n-1}a+S_nb=r_n$。

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\begin{pmatrix} r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$$

$$\cdots\cdots$$

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}$$

例题 1.4 试求 s，t，使得 $30111s+4520t=(30111,4520)$。

解

i	0	1	2	3	4	5	6	7	8	9	10	11
q_{12-i}			2	1	1	4	1	21	1	1	1	6
S_i	0	1	-2	3	-5	23	-28	611	-639	1250	-1889	12584

笔记 $S_{i+1}=S_{i-1}-q_{n-i}S_i$

练习 1.2

1) 如果 $(a,b)=d$，那么 $\{sa+tb \mid s,t\in Z\}$ 是什么？
2) 试求出一对整数 s 和 t 满足 $s*12345-t*345=(12345,345)$。

1.3 一次不定方程

定理 1.6

设 a，b 是两个不全为 0 的整数，则

(1) 对于任何正整数 k，$(ka,kb)=k(a,b)$

(2) $(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$

证明 (2) 由 (1)，$(a,b)(\frac{a}{(a,b)},\frac{b}{(a,b)})=((a,b)\frac{a}{(a,b)},(a,b)\frac{b}{(a,b)})=(a,b)$

因为 $(a,b)\neq 0$，所以 $(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$。

定理 1.7

设 a，b，c 为整数，$a\neq 0,c\neq 0$，若 $(a,b)=1$，则 $(a,bc)=(a,c)$。

注 $d=(a,bc),d'=(a,c)\quad proof d \mid d' \; and \; d' \mid d$。

推论 1.4

设 a，b，c 为整数，$a\neq 0$，若 $(a,b)=1$，$a\mid bc$，则 $a\mid c$。

例题 1.5 证明：若 $a_1b_1-a_2b_2=1$，则 $(a_1+a_2,b_1+b_2)=1$。

证明 $a_1b_1-a_2b_2=1\Rightarrow(b_1,b_2)=1,(a_1,a_2)=1$ comes from 1.2(6)

$(b_1,b_1+b_2)=(b_1,b_2)=1$

$(b_1+b_2,b_1(a_1+a_2))=(b_1+b_2,a_1+a_2)$

$(b_1+b_2,b_1(a_1+a_2))=(b_1+b_2,b_1(a_1+a_2)-a_2(b_1+b_2))=(b_1+b_2,1)=1$。

定理 1.8

设 a，b 是两个完全不为 0 的整数，整系数不定方程 $ax+by=c$ 有解的充分条件是 $(a,b)=c$。此时，若 $x=x_0,y=y_0$ 是方程的一个特解，那么方程的所有整数解可以表示为:

$$\begin{cases} x=x_0-\dfrac{b}{(a,b)}t \\ y=y_0+\dfrac{a}{(a,b)}t \\ t\in Z \end{cases}$$

例题 1.6 求不定方程 $18x+7y=44$ 的所有整数解

解 根据辗转相除法可得

$18*2+7*(-5)=1$ 特解为:

$$\begin{cases} x=2 \\ y=-5 \end{cases}$$

不定方程 $18x+7y=44$ 的特解为:

$$\begin{cases} x_0=2\times 44=88 \\ y_0=(-5)\times 44=-220 \end{cases}$$

原不定方程的特解为:

$$\begin{cases} x=88-7t \\ y=-220+18t \\ t\in Z \end{cases}$$

例题 1.7

1. 求不定方程 $a_1x_1+a_2x_2+\dot{+}a_{n-1}x_{n-1}+x_n=N$ 的所有整数解。
2. 求不定方程 $18x+7y+6z=44$ 的所有整数解。
3. 求不定方程 $6x+10y+15z=44$ 的所有整数解。

解

2.$(18,7)=1\Rightarrow 18x+7y$ 可以表示任何整数，z 可以任取。

转化为 $18x+7y=44-6z$ 来求得二元不定方程的解。

3.$(6,10)=2\Rightarrow 6x+10y=2t$

原方程转化为 $2t+15z=44$

其解为:

$$\begin{cases} t=-308-15t_1 \\ z=44+2t_1 \\ t_1\in Z \end{cases}$$

$3x+5y=t$ 的所有整数解可以表示为;

$$\begin{cases} x=2t-5t_2 \\ y=-t+3t_2 \\ t_2\in Z \end{cases}$$

练习 1.3 求解不定方程 $x^2+y^2=z^2$

1.4 最小公倍数

定义 1.2

设 a，b 是两个不全为 0 的整数，整数满足 $a \mid c, b \mid c$，则称 c 为 a 和 b 的公倍数，在 a 和 b 的所有公倍数中，一定有一个正的最小公倍数，称为 a 和 b 的最小公倍数，记作 $[a,b]$，或者 $lcm(a,b)$。♣

定理 1.9

设 a，b 是两个正整数，且 $(a,b)=1$，

(1) 若 $a \mid c, b \mid c$，则 $ab \mid c$

(2) $[a,b]=ab$ ♡

定理 1.10

设 a，b 是两个正整数，

(1) 对于任何正整数 k，$[ka,kb]=k[a,b]$

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

(3) 若 $a \mid c, b \mid c$，则 $[a,b] \mid c$ ♡

例题 1.8 若 $x,y,\sqrt{x}+\sqrt{y}$ 均为整数，试证明 $\sqrt{x},\sqrt{y}$ 均为整数。

证明 若 $\sqrt{x}+\sqrt{y}=0$，则 $x=y=0$，结论成立

$\sqrt{x}=\frac{1}{2}((\sqrt{x}+\sqrt{y})+(\sqrt{x}-\sqrt{y}))$ 所有 $\sqrt{x},\sqrt{y}$ 都是有理数

不妨设 $\sqrt{x}=\frac{b}{a}$，a，b 为正整数，且 $(a,b)=1$

$x=\frac{b^2}{a^2}$ 为整数，$(a^2,b^2)=a^2 \Rightarrow (a,b)=(a,b^2)=(a^2,b^2)$

所以 $a=1$，$\sqrt{x}$ 为整数。

定理 1.11

$a_1,a_2,\ldots,a_n$ 不全为 0 的整数，不妨设 $a_1 \neq 0$，定义 $d_1=(a_1,a_2), d_2=(d_1,a_3),\ldots,d_{n-1}=(d_{n-2},a_n)$，则 $(a_1,a_2,\ldots,a_n)=d_{n-1}$。♡

结论 若正整数 $d=(a_1,a_2,\ldots,a_n)$，则存在整数 $s_1,s_2,\ldots,s_n$，使得 $d=s_1a_1+s_2a_2+\cdots+s_na_n$

定理 1.12

正整数 c 是 $a_1,a_2,\ldots,a_n$ 的最大公因数，当且仅当：

(1) $c \mid a_1, c \mid a_2, \ldots, c \mid a_n$。

(2) 任何整数 c' 若满足 $c' \mid a_1, c' \mid a_2, \ldots, c' \mid a_n$，则 $c' \mid c$。♡

定理 1.13

设 $a_1,a_2,\ldots,a_n$ 是 n 个不为 0 的整数，定义 $m_1=[a_1,a_2], m2=[m_1,a_3],\ldots,m_{n-1}=[m_{n-2},a_n]$，则 $[a_1,a_2,\ldots,a_n]=m_{n-1}$。♡

定理 1.14

正整数 m 是 $a_1,a_2,\ldots,a_n$ 的最大公因数，当且仅当：

(1) $a_1 \mid m, a_2 \mid m, \ldots, a_n \mid m$。

(2) 任何整数 m' 若满足 $a_1 \mid m', a_2 \mid m', \ldots, a_n \mid m'$，则 $m \mid m'$。♡

1.5 素数与算术基本定理

定义 1.3

设 p 是一个整数，$p \neq 0, \pm 1$，如果除了 $\pm 1, \pm p$ 外，p 没有其他因数，则称 p 为素数 (或者质数，不可约数)，否则为合数 (可约数)，最小的素数为 2。

定理 1.15

合数 m 的最小不等于 1 的正因子 p 一定是素数，且 $p \leq \sqrt{m}$。

证明 反证法证明 p 一定是素数。
由 1.2 (4) $\Rightarrow \frac{m}{p} \mid m$，又 $1 < \frac{m}{p} < m$，$p \leq \frac{m}{p} \Rightarrow p \leq \sqrt{m}$。
结论 设整数 $m > 1$, 如果所有不大于 $\sqrt{m}$ 的素数都不是 m 的因子，那么 m 是素数。
整数 $m > 1$ 是合数的充要条件是存在不大于 $\sqrt{m}$ 的素因子。

定理 1.16

素数有无穷多个。

证明 反证法证明，有有限个素数 $p_1, p_2, \ldots, p_n$
考虑整数 $A = p_1 p_2 \ldots p_n + 1$
不妨设 $p_i \mid A \Rightarrow p_i \mid A - p_1 p_2 \ldots p_n$，即 $p_i \mid 1$，矛盾。

定理 1.17 (素数定理)

$\pi(x)$ 表示不超过 x 的素数个数。

$$\lim_{x \to \infty} \pi(x) \frac{ln(x)}{x} = 1$$

定理 1.18 (伯特兰-切比雪夫定理)

设整数 $n > 3$, 至少存在一个素数 p 满足 $n < p < 2n - 2$。

定理 1.19 (算术基本定理)

设 n 是一个大于 1 的正整数，那么 n 一定可以分解成一些素数的乘积。若规定 n 的所有素因子按照从小到大的顺序排列，那么 n 的分解方式是唯一的。

定义 1.4

设 n 是大于 1 的正整数，$n = \prod_{i=1}^{s} p_i^{\alpha_i} (\alpha_i > 0, p_i < p_j (i < j))$ 称为 n 的标准分解式。

例题 1.9 设 $m = \prod_{i=1}^{s} p_i^{\alpha_i}$，$n = \prod_{i=1}^{s} p_i^{\beta_i}, \alpha_i \geq 0, \beta_i \geq 0$，$p_i \neq p_j (i \neq j)$ proof:

(1) $m \mid n \Leftrightarrow 1 \leq i \leq s, \alpha_i \leq \beta_i$

(2) $(m, n) = \prod_{i=1}^{s} p_i^{\min \alpha_i, \beta_i}$

(3) $[m, n] = \prod_{i=1}^{s} p_i^{\max \alpha_i, \beta_i}$

练习 1.4 证明形如 $4k + 3$ 的素数有无穷多个。
证明 反证法证明，假设形如 $4k+3$ 素数仅有有限个，其全部为 $p_1, p_2, \ldots, p_n$，均为大于 1 的正整数，考虑整奇

数：$A = 4p_1p_2 \dots p_n - 1$

A 是一个形如 $4k+3$ 的合数

所以 A 的素因子全部都是形如 $4k+1$ 的素数，但形如 $4k+1$ 的整数相乘仍然是形如 $4k+1$ 的整数，矛盾。

练习 1.5

1. 试证明：$\max\{a,b,c\} = a+b+c+\min\{a,b,c\} - \min\{a,b\} - \min\{b,c\} - \min\{a,c\}$
2. 试证明：$gcd(a, lcm(b,c)) = lcm(gcd(a,b), gcd(a,c))$
3. 试用算术基本定理证明：

$$\prod_p \frac{p}{p-1} = \sum_{i=1}^{+\infty} \frac{1}{i}$$

1.6 高斯函数

定义 1.5

实数 x 的高斯函数 $[x]$ 是指不超过 x 的最大的整数，$[x]$ 也称为 x 的整数部分，x 的小数部分 x 是指 $x-[x]$。

定理 1.20

对于 $[x]$，以下结论正确：

1. 若 $x \le y \Rightarrow [x] \le [y]$
2. 整数 a 满足 $x-1 < a \le a+1 \Leftrightarrow a = [x]$
3. 整数 a 满足 $a \le x < a+1 \Leftrightarrow a = [x]$
4. 对于任意整数 n，$[n+x] = n + [x]$

证明 (4)

$n+x-1 < [n+x] \le n+x$

$x-1 < [n+x] - n \le x$

$[n+x] - n = [x]$

例题 1.10 对于任意实数 x，y，试证明 $[x+y] \ge [x] + [y]$

证明

$[x+y] = [[x]+[y]+\{x\}+\{y\}]$

$[x+y] = [x]+[y]+[\{x\}+\{y\}]$

$[\{x\}+\{y\}] \ge 0$

$[x+y] \ge [x]+[y]$

定理 1.21

对于整数 a，b，且 $b>0$，带余除法算式为 $a = qb+r, 0 \le r < b$，则 $q = [\frac{a}{b}]$。

证明

$q = \frac{a}{b} - \frac{r}{b}$，$\quad 0 \le \frac{r}{b} < 1$

$\frac{a}{b} - 1 \le q = \frac{a}{b} - \frac{r}{b} < \frac{a}{b}$

定理 1.22

设 p 是一个素数，则 $n!$ 中包含 p 的幂次为 $\sum_{i>1}[\frac{n}{p^i}]$。

for example:

$$30! = 1 \times 2 \times \cdots \times 30 = p_1^{e_1} p_2^{e_2} \cdots = 2^{e_1} 3^{e_2} \cdots$$
$$[\frac{30}{2}] + [\frac{30}{2^2}] + [\frac{30}{2^3}] + [\frac{30}{2^4}] + [\frac{30}{2^5}] \cdots$$
$$= 15 + 7 + 3 + 1 + 0 + \cdots$$

所以 $e1 = 15 + 7 + 3 + 1$

证明 定理 1.22

p^i 的倍数共有 $[\frac{n}{p^i}]$

当 $(p,k) = 1$ 时，整数 $p^i k$ 为 $n!$ 提供的 p 的幂次为 i

由于 $p^i k$ 同时是 $p, p^2, \ldots, p^i$ 的倍数，所以恰好共计数了 i 次

因此 $n!$ 中包含 p 的幂次为 $\sum_{i>1}[\frac{n}{p^i}]$

例题 1.11 试证明 $\binom{100}{50}$, 的十进制末位数不为 0.

证明

$\binom{100}{50} = \frac{100!}{50!50!}$

$100! = 2^{e_1} 3^{e_2} 5^{e_3} \cdots$

$50! = 2^{b_1} 3^{b_2} 5^{b_3} \cdots$

$b_3 = [\frac{50}{5}] + [\frac{50}{25}] + [\frac{50}{125}]$

$e_3 = [\frac{100}{5}] + [\frac{100}{25}] + [\frac{100}{125}]$

所以 $\binom{100}{50}$ 没有素因数 5，所以末位不为 0.

例题 1.12 设 n，m 为正整数，$n > m$，试证明：$\binom{n}{m} = \frac{n(n-1)\ldots(n-m+1)}{m!}$ 是整数。

证明

$\binom{n}{m} = \frac{n!}{m!(n-m)!}$

只需证明 $\sum_{i\geq 1}[\frac{n}{p_i}] \geq \sum_{i\geq 1}[\frac{m}{p_i}] + \sum_{i\geq 1}[\frac{n-m}{p_i}]$

由例题 1.10 可知 $[\frac{n}{p_i}] \geq [\frac{m}{p_i}] + [\frac{n-m}{p_i}]$

第 1 章 练习

1. 设 a，m，n 均为正整数，试着证明 $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$

   证明 $Might\ as\ well, m \geq n, m = nq + r, 0 \leq r < n$

   $a^m - 1 = a^{nq+r} - a^r + a^r - 1 = a^r(a^{nq} - 1) + a^r - 1$

   $= a^r(a^n - 1)(1 + a^n + a^{2n} + \cdots + a^{(q-1)n}) + a^r - 1$

so $(a^m - 1) mod (a^n - 1) = a^r - 1$

$using\ division\ algorithm,\ the\ answer\ is\ a^{(m,n)} - 1.$

2. $The\ Fermat\ number\ is\ F_n = 2^{2^n} + 1, if\ F_n\ is\ prime\ number\ , try\ to\ proof:$
$if\ 2^m + 1\ is\ prime\ number\ then\ m\ just\ like\ 2^n \in Z.$

证明

第 2 章 同余

2.1 同余的基本性质

定义 2.1

设 m 是正数，a，b 为两个整数，如果 a-b 是 m 的倍数，那么称 a 和 b 关于 m 同余，记作 $a \equiv b(mod\,m)$，否则称 a 和 b 关于 m 不同余，记作 $a \not\equiv b(mod\,m)$。

定理 2.1

同余式等价关系

1. 自反性
2. 对称性
3. 传递性

定义 2.2

设 m 是正整数，全体整数按照模 m 同余可以划分成 m 个不同的等价类，称为模 m 剩余类，整数 a 所在的剩余类记为 $\bar{a}$，整数 x 属于剩余类 $\bar{a}$ 当且仅当 $x \equiv a(mod\,m)$。从每个剩余类中取出一个整数形成的 m 元素称为模 m 完全剩余系。

例如，若 m=6，则模 6 剩余类共有 6 个可以表示为 $\bar{0}, \bar{1}, \bar{2}, \cdots, \bar{5}$ 而 $0, 1, 2, 3, 4, 5, -6, 7, 2, 3, 4, 5$ 都是模 6 完全剩余系。

定义 2.3

设 m 是正整数，如果整数 a 与 m 互素，那么 a 所在的剩余类 $\bar{a}$ 称为模 m 简化剩余类，从每个简化剩余类中取出一个整数形成的集合称为模 m 的简化剩余系。在整数 1，2，$\cdots$，m 中所有与 m 互素的整数的个数称为 m 的欧拉函数，记作 $\varphi(m)$，简化剩余系共有 $\varphi(m)$ 个整数。

例题 2.1 设 m，n 为正整数，试将模 m 的剩余类 $\bar{a}$ 拆分成模 mn 的剩余类的和。

解

- 模 m 剩余类 $a(mod\,m)$ 可以表示为 $\{a + mk | k \in Z\}$，而全体整数按照模 n 又可以分成 n 个剩余类，即 $\bar{0}, \bar{1}, \cdots, \overline{n-1}$。
- $\{a + mk|k \in Z\} = \{a + m(tn)|t \in Z\} \cup \{a + m(tn + 1)|t \in Z\} \cup \cdots \cup \{a + m(tn + n - 1)|t \in Z\}$。
- $= \{a + mnk|t \in Z\} \cup \{a + m + mnt|t \in Z\} \cup \cdots \cup \{a + m(n - 1) + mnt|t \in Z\}$
- 也就是，模 m 的剩余类 $\bar{a}$ 可以拆分成 n 个模 mn 的剩余类，$\bar{a}, \overline{a + m}, \cdots, \overline{a + m(n - 1)}$。

定理 2.2 (同余的性质)

设 m，n 是正整数，$a \equiv b(mod\,mn)$，则 $a \equiv b(mod\,m), a \equiv b(mod\,n)$。

笔记 定理 2.2 的逆定理不成立

定理 2.3

设 m，n 是正整数，若 $a \equiv b(mod\,n), a \equiv b(mod\,n)$，则 $a \equiv b(mod[m, n])$。

定理 2.4

关于同余，以下性质成立。

(1) 若 $a \equiv b(mod\ m) \Rightarrow a+c=b+c(mod\ m)$。

(2) 若 $a \equiv b(mod\ m), k \in Z \Rightarrow ak \equiv bk(mod\ m)$。

(3) 若 $ak \equiv bk(mod\ m), k \in Z, (k,m)=1 \Rightarrow a \equiv b(mod\ m)$。

(4) 若 $a \equiv b(mod\ m), k \in Z^+ \Leftrightarrow ak \equiv bk(mod\ mk)$。

(5) 若 $a \equiv b(mod\ m)$，$f(x)$ 为任一整系数多项式，则 $f(a) \equiv f(b)(mod\ m)$。

结论 若 $a_1 \equiv a_2(mod\ m), b_1 \equiv b_2(mod\ m) \Rightarrow a_1+b_1 \equiv a_2+b_2(mod\ m), a_1b_1 \equiv a_2b_2(mod\ m)$。

例题 2.2 试证明正整数 m 能被 3 整除的充要条件是它的十进制表示各数位上数字之和是 3 的倍数。

证明 $m=(a_{n-1}\cdots a_1a_0)_{10}$

$\sum_{i=0}^{n-1} a_i 10^i \equiv \sum_{i=0}^{n-1} a_i 1^i$

$m(mod\ 3)=\sum_{i=0}^{n-1} a_i(mod\ 3)$

笔记 讨论 9,7,11,1001,13

- $\sum_{i=0}^{n-1} a_i 10^i \equiv \sum_{i=0}^{n-1} a_i 1^i = \sum_{i=0}^{n-1} a_i(mod\ 9)$
- $\sum_{i=0}^{n-1} a_i 10^i \equiv \sum_{i=0}^{n-1} a_i(-1)^i(mod\ 11)$
- $12345678 = 12\times(10^3)^2+345\times10^3+678$
  $=12\times(-1)^2+345\times(-1)+678(mod\ 1001)$
- $1001=7\times11\times13$

练习 2.1

1. 若 x，y 为整数，证明 $10|2x+5y \Leftrightarrow 10|4x+5y$。

   解

   $10|2x+5y \Leftrightarrow 2|2x+5y, 5|2x+5y.$

$$\begin{cases} 2x+5y\equiv 0(mod\ 2) \\ 2x+5y\equiv 0(mod\ 5)\end{cases} \Leftrightarrow \begin{cases} y\equiv 0(mod\ 2) \\ 2x\equiv 0(mod\ 5)\end{cases} \quad (2,5)=1 \quad \Leftrightarrow \begin{cases} y\equiv 0(mod\ 2) \\ x\equiv 0(mod\ 5)\end{cases}$$

$$\begin{cases} 4x+5y\equiv 0(mod\ 2) \\ 4x+5y\equiv 0(mod\ 5)\end{cases} \Leftrightarrow \begin{cases} x\equiv 0(mod\ 2) \\ y\equiv 0(mod\ 5)\end{cases}$$

2. 计算 $2^{1024}(mod\ 10240)$

   解

   考虑 $2^{1024}\equiv x(mod\ 10240) \Rightarrow 2^{1013}\equiv y(mod\ 5)$

$$\begin{aligned} 2^{1013} &= 2\times 2^{1012} \\ &= 2(2^2)^{506} \\ &\equiv 2(-1)^{506} \end{aligned}$$

   所以 $2^{1013}\equiv 2(mod\ 5)$

2.2 欧拉函数

2.2.1 剩余系的遍历

定理 2.5

设 m 是正整数，若 $(a,m)=1$，则当 x 遍历模 m 的一个完全剩余系时，对于任意整数 b，$ax+b$ 遍历模 m 的一个完全剩余系；当 x 遍历模 m 的一个简化剩余系，ax 遍历模 m 的一个简化剩余系。

证明 m 的剩余系为 $\{x_1,x_2,\cdots,x_m\}$
不妨设 $1\le i\le j\le m$
$ax_i+b\equiv ax_j+b(mod\, m)\Rightarrow x_i\equiv x_j(mod\, m)$
矛盾
ax_i 与 m 互素，且两两互不同余。

定理 2.6

设 m，n 为正整数，$(m,n)=1$，则当 x 遍历模 m 的一个完全剩余系，y 遍历模 m 的一个完全剩余系时，$mx+ny$ 遍历模 mn 的一个完全剩余系；当 x 遍历模 m 的一个简化剩余系，y 遍历模 m 的一个简化剩余系时。$mx+ny$ 遍历 mn 的一个简化剩余系。

证明 (x_i,y_j) 一共有 mn 种取法
$i=j$ 取法相同，$i\ne j$ 取法不同
$mx_i+ny_j\equiv mx_{i'}+ny_{j'}(mod\, mn)$
$\Rightarrow y_j\equiv y_{j'}(mod\, m)$
$proof:(x_i,n)=1,(y_j,m)=1\Rightarrow(mx_i+ny_j,mn)=1$
$(mx_i+ny_j,m)=1,(mx_i+ny_j,n)=1$
$\varphi(m)\varphi(n)$ 个元素和 mn 互素
$\varphi(m)\varphi(n)\le\varphi(mn)$
证明 $\varphi(mn)$ 无遗漏
当 x 遍历完全，y 遍历完全，$mx+ny$ 遍历完全
$\forall a\in Z,\exists x_i,y_j\Rightarrow a\equiv a\equiv mx_i+ny_j(mod\, mn)$

$$(a,mn)=1\Rightarrow\begin{cases}(a,m)=1\\(a,n)=1\end{cases}\Rightarrow\begin{cases}(mx_i+ny_j,m)=1\\(mx_i+ny_j,n)=1\end{cases}\Rightarrow\begin{cases}(y_j,m)=1\\(x_i,n)=1\end{cases}$$

2.2.2 欧拉函数

定理 2.7

设 m,n 为正整数，若 $(m,n)=1$，则 $\varphi(mn)=\varphi(m)\varphi(n)$[积性函数]。

证明

由定理 2.6，当 x 遍历模 n 的一个简化剩余系，y 遍历模 m 的一个简化剩余系时，mx+ny 遍历模 mn 的一个简化剩余系，所以模 mn 的一个简化剩余系中的元素个数为 $\varphi(mn)=\varphi(m)\varphi(n)$。

定理 2.8

设 p 为素数，e 为正整数，则 $\varphi(p^e)=p^e-p^{e-1}$。

证明

p 是素数 $\varphi(p)=p-1(1,2,\cdots,p-1)$

$\varphi(p^e)$ 不互素的有 $p,p^2,\cdots,p^{e-1},p^e$

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

定理 2.9

设 m 为正整数，其标准分解式为 $m=\prod_{i=0}^{s}p_i^{\alpha_i}$，则 $\varphi(m)=m\prod_{i=0}^{s}(1-\frac{1}{p_i})$

证明 由定理 2.7 和定理 2.8，

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

例题 2.3 试求 $\varphi(2^3 3^2 7)$

解

$\varphi(2^3 3^2 7)=2^3 3^2 7\times(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{7})=144$

例题 2.4 假设 m 是两个不相等的素数的乘积，如果已知 $\varphi(m)=a$，试求这两个素数。

解

由题意可设 $m=pq$，p，q 为不相等的素数，可得二元二次方程组，

$$\begin{cases} m=pq \\ (p-1)(q-1)=a \end{cases}$$

整理可得 $p+q=m+1-a$，因此 p，q 为以下一元二次方程的两个解

$$x^2-(m+1-a)x+m=0$$

练习 2.2

1. 证明 $m>2,2|\varphi(m)$

   证明

   方法一：

   $\varphi(m)=\prod(p_i^{\alpha_i}-p_i^{\alpha_i-1})$

   分为两种情况考虑：

   1.m 含有至少一个奇数因子

   2.m 就是等于 $2^i,i>1$

   方法二：

   m 为奇数

   $1,2,3,\cdots,\frac{m-1}{2},\frac{m+1}{2},\cdots,m$

   $(i,m)=1\Rightarrow(m-i,m)=1$

2. 证明，当 $m|n$ 时，$\varphi(m)|\varphi(n)$。

   证明

   $\varphi(m)=\prod\varphi(p_i^{\alpha_i})$

   $\varphi(n)=\prod\varphi(p_i^{\beta_i})$

2.3 欧拉定理

2.3.1 欧拉定理和费马定理

定义 2.4 (欧拉定理)

设 m 为正整数，$(a, m) = 1$，那么 $a^{\varphi(m)} \equiv 1(mod\, m)$。♣