信息安全中的数学基础

张宗洋
zongyangzhang@buaa.edu.cn
电子信息工程学院

本课件基于西安电子科技大学许春香教授课件制作

教材:

《信息安全数学基础》，许春香等编著，清华大学出版社，2015年

主要参考书：

（1)信息安全数学基础（第二版），陈恭亮编著，清华大学出版社，2014年

（2）初等数论，潘承洞,潘承彪著，北京大学出版社,2003年

（3）近世代数（第二版），韩士安，林磊著，科学出版社，2009年

《信息安全数学基础》课程介绍

课程内容：数论，近世代数，有限域

课程目的：培养抽象思维能力和严格的逻辑推理能力，为学习专业基础课及专业课打好基础

重要性：该课程是信息安全专业的重要核心基础课程

- 信息安全所关注的包括：信息的机密性、真实性、完整性和不可抵赖性。
- 机密性：保证信息不能被未被授权者阅读
- 真实性：保证收到的信息确实是由发送者发送的
- 完整性：保证信息在传递过程中没有被篡改
- 不可抵赖性：保证发送者不能否认其发送过消息；接收者不能否认接收到消息。

通过密码技术（基于数学理论的变换）实现以上目标。

- 密码技术是保证信息安全的核心技术
- 数学理论与方法是实现密码算法的基础

掌握必备的数学知识才能学好信息安全！！！

学习方法：课堂认真听讲（成熟、会学习的表现）

课后认真、反复复习，深刻领会相关知识。

课程性质决定需要这样的学习方法。

上课时间：星期二下午5-8节

总成绩构成：平时表现（到课，听课）：20%

作业：10%

期末考试：70%

课程内容：

第一章　整除与同余

第二章　群

第三章　循环群、群的结构

第四章　环

第五章　多项式环与有限域（*）

第六章　同余式

第七章　平方剩余

第八章　原根与离散对数

第一章 整除与同余

第一章 整除与同余

主要内容

- 整除的基本概念（掌握）
- 素数（掌握）
- 同余的概念（掌握）

1.1 整除

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$a = qb$，则我们称b整除a，或a被b整除，记为$b \mid a$，此时称b是a的因子，a是b的倍数.

例1：

$a=10, b=2$则有$2 \mid 10$；若$a=100, b=10$有$10 \mid 100$

例2：

设a是整数，$a \neq 0$, 则$a \mid 0$.

即0是任意整数的倍数

整除的基本性质(定理1-1, pp.1)：

1. 如果$b \mid a$且$a \mid b$，则$b = a$或$b = -a$.
2. 如果$a \mid b$且$b \mid c$，则$a \mid c$.
3. 如果$c \mid a$且$c \mid b$，则$c \mid ua+vb$，其中u，v是整数.

整除的基本性质（证明）：

性质1：如果$b|a$且$a|b$，则$b=a$或$b=-a$.

证明：

（1）由$b|a$，根据整除定义我们可以得出：存在整数q_1使

$$a=q_1b\ ,$$

同理；由$a|b$，则存在整数q_2使

$$b=q_2a.$$

于是$a=q_1b=q_2q_1a$. 所以

$$q_2q_1=1,$$

由于q_1，q_2是整数，则

$$q_2=q_1=1，或q_2=q_1=-1.$$

$$故b=a或b=-a.$$

命题得证。

整除的基本性质（证明）：

性质2：如果a|b且b|c，则a|c

证明：

（2）因为$a \mid b$，则存在整数q_1，使

$$b = q_1 a \quad ①$$

又因为$b \mid c$，则存在整数q_2，使

$$c = q_2 b \quad ②$$

于是将①式带入②式有：

$$c = q_2 b = q_1 q_2 a = qa,$$

其中$q = q_1 q_2$.

故$a \mid c$.

整除的基本性质（证明）：

性质3：如果$c|a$且$c|b$，则$c|ua+vb$，其中u，v是整数

证明：

（3）因为$c|a$，则存在整数q_1，使

$$a = q_1 c \quad ①$$

两边同乘以整数u，有

$$ua=p_1 c \text{ (其中} p_1=uq_1\text{)} \quad ②$$

同理$c|b$，有

$$vb=p_2 c \text{ (其中} p_2=vq_2\text{)} \quad ③$$

②+③ 得出：

$$pc=ua+vb$$

其中$p=p_1+p_2=uq_1+vq_2$，

故$c|ua+vb$.

整除的基本性质（补充）：

(1) $a \mid b \Leftrightarrow -a \mid b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid -b \Leftrightarrow |a| \mid |b|$

$b \neq 0$且$a \mid b \Rightarrow |a| \leq |b|$

带余除法：

当两个整数不能整除时，我们有带余除法：

对于a，b两个整数，其中$b\neq 0$，则存在唯一q，r使得：

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

r称为a被b除得到的余数．q称为不完全商.

显然当$r = 0$时，$b \mid a$.

带余除法: 对于a，b两个整数，不失一般性,设$b>0$，则存在唯一q，r使得：

$$a = bq+r,\quad 0 \le r < b.$$

证明 存在性

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

$$qb \le a < (q+1)b$$

令$r= a - qb$，则 $a = qb + r$，$0 \le r < b$

唯一性 如果 $a = qb + r$，$0 \le r < b$

$$a = q_1 b + r_1,\quad 0 \le r_1 < b,\quad q \ne q_1,\ r \ne r_1$$

$$b \le |(q-q_1)\,b| = |-(r-r_1)| < b$$

矛盾！故$q=q_1$，$r=r_1$。

带余除法：

例3　1）$a = -37$，　$b = 5$，则

$$-37 = (-8)\times 5+3，\quad q=-8,\ r = 3.$$

2）$a = 67$，　$b = 7$，则

$$67 = (9)\times(7)+4，\quad q=9,\ r = 4.$$

最大公因子（定义）

定义1-4：

1）设a，b是两个整数，如果整数$c \mid a$且$c \mid b$，则c称为a，b的公因子.

2）设$c>0$是两个不全为零的整数a，b的公因子，如果a，b的任何公因子都整除c，则c称为a，b的最大公因子，记为$c=(a，b)$.

最大公因子（性质）

简单性质：

1. $(a,b)=(-a,b)=(a,-b)=(-a,-b)=(|a|, |b|)$
2. $(0,a)=|a|$

最大公因子（求解）

方法1：因子分解

例4：a=60=2×2 ×3 ×5 ，b=36=2 ×2 ×3×3

观察得：c=（a，b）= 2×2 ×3=12

方法2（一般方法）： **欧几里德除法**也称为**辗转相除法**。

最大公因子（求解）

欧几里德除法（辗转相除法）：

已知正整数a，b，记$r_0=a$，$r_1=b$，

$r_0=q_1r_1+r_2$，$0\le r_2<r_1=b$;

$r_1=q_2r_2+r_3$，$0\le r_3<r_2$;

…

$r_{n-2}=q_{n-1}r_{n-1}+r_n$，$0\le r_n<r_{n-1}$;

$r_{n-1}=q_nr_n$

$r_n=(a，b)$

此方法扩展可用于求元素的逆元

欧几里德算法原理

（1）r_n可以整除r_{n-1}, r_{n-2}，…..,r_2,r_1,r_0, 所以r_n是a,b的公因子。

（2） 若d整除r_0, r_1,则d整除 r_2， r_3，…..,r_{n-2},r_{n-1},r_n。

故，r_n是（a,b）的最大公因子。

最大公因子（求解）

例5：(–3824，1837)=?

(–3824，1837)= (3824，1837).

$$3824 = 2\times 1837+150$$

$$1837 = 12\times 150+37$$

$$150 = 4\times 37+2$$

$$37 = 18\times 2+1$$

$$2 = 2\times 1$$

得(3824，1837) = 1，

故(–3824，1837) = 1.

$r_0=a, r_1=b$

$$r_0 = r_1 q_1 + r_2, \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3, \qquad 0 \le r_3 < r_2$$

$$r_2 = r_3 q_3 + r_4, \qquad 0 \le r_4 < r_3$$

……

$$r_{n-2} = r_{n-1} q_{n-1} + r_n, \qquad 0 \le r_n < r_{n-1}$$

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

有s, t满足

$$s\,a + t\,b = (a, b) = r_n$$

最大公因子定理

定理1-4 设a，b是两个不全为零的整数，则存在两个整数u，v，使

$$(a，b)= ua+vb.$$

最大公因子定理

例6：将$a = 888$，$b = 312$的最大公因子表示为$(a, b) = ua+vb$

解　利用欧几里得除法求最大公因子的过程可以解出.

$$888 = 2\times312+264$$

$$312 = 1\times264+48$$

$$264 = 5\times48+24$$

$$48=2\times24$$

我们有：

$264 = 888-2\times312=a-2b$

$48 = 312-264 = b-(a-2b) = -a+3b$

$24 = 264-5\times48 = (a-2b)-5\times(-a+3b) =6a-17b$

故$(888, 312) = 24 = 6\times888+(-17)\times312$.

互素

定义1-7：设a，b是两个不全为0的整数，如果$(a, b) = 1$，则称a，b互素.

推论1-1：a，b互素的充分必要条件是：

存在u，v，使$ua+vb = 1$.

证明　必要条件是定理1的特例，只需证充分条件.

如果存在u，v，使

$$ua+vb = 1.$$

则由$(a, b) \mid (ua+vb)$，得$(a, b) \mid 1$，

所以$(a, b) = 1$.

互素（性质）

定理1-10，互素有如下性质：

1）如果$c \mid ab$且$(c, a) = 1$，则$c \mid b$.

2）如果$a \mid c$，$b \mid c$，且$(a, b) = 1$，则$ab \mid c$.

3）如果$(a, c) = 1$，$(b, c) = 1$，则$(ab, c) = 1$.

互素性质证明

性质1：如果$c \mid ab$且$(c, a) = 1$，则$c \mid b$.

证明

1）因为$(c, a) = 1$，存在u，v，使

$$ua+vc = 1,$$

两端乘b得

$$uab+vcb = b.$$

由于$c \mid uab+vcb$，故$c \mid b$.

互素性质证明

性质2： 如果$a|c$，$b|c$，且$(a，b)=1$，则$ab|c$.

证明：

2）因为$(a，b)=1$，存在u，v，使

$$ua+vb=1，$$

两端乘c得

$$uac+vbc=c.$$

由 $b|c$，$a|c$，得$ab|uac$，$ab|vbc$，

故$ab|c$.

互素性质证明

性质3： 如果$(a，c)=1$，$(b，c)=1$，则$(ab，c)=1$

证明

3）因为$(a，c)=1$，存在$u，v$，使

$$ua+vc=1，$$

因为$(b，c)=1$，存在$r，s$，使

$$rb+sc=1，$$

于是

$$(ua+vc)(rb+sc)=(ur)ab+(usa+vrb+vsc)c=1.$$

故$(ab，c)=1$.

公倍数，最小公倍数

定义1-5　设a，b是两个不等于零的整数．如果$a \mid d$，$b \mid d$，则称d是a和b的公倍数．a和b的正公倍数中最小的称为a和b的最小公倍数，记为$[a, b]$.

显然，

$[a, b] = [-a, b] = [a, -b] = [-a, -b]$

$=[|a|, |b|]$.

公倍数，最小公倍数

例8 $a = 2$，$b = 3$．它们的公倍数集合为

{0，±6，±12，±18，…}.

而[2，3] = 6.

最小公倍数与最大公因子关系

定理1-8 1）设d是a，b的任意公倍数，则

$$[a，b] \mid d.$$

2）$[a，b]=\dfrac{|ab|}{(a，b)}$，特别地，如果$(a，b)=1$，$[a，b]=|ab|$.

定理2证明

证明

1）做带余除法： $d = q[a, b] + r$，$0 \le r < [a, b]$，

由于$a \mid d$，$b \mid d$，那么

$$a \mid [a, b]，b \mid [a, b]，$$

则$a \mid r$，$b \mid r$，r也是a，b的公倍数，

所以 $r = 0$，故$[a, b] \mid d$.

定理2证明

2）不失一般性，假设a，b均是正整数．我们现在证明 $\frac{ab}{(a,b)}$ 是a，b的公倍数而且对于a，b的任意公倍数d都有

$$\frac{ab}{(a,b)} \mid d$$

设$a = k_a(a,b)$，$b = k_b(a,b)$，其中$(k_a, k_b) = 1$．则

$$\frac{ab}{(a,b)} = k_a b = k_b a,$$

所以 $\frac{ab}{(a,b)}$ 是a，b的公倍数．

设a，b的任意公倍数$d = q_a a = q_b b$，于是

$$d = q_a k_a(a，\ b) = q_b k_b(a，\ b)，$$

$$q_a k_a = q_b k_b.$$

因为$(k_a，\ k_b) = 1$，则

$$k_a \mid q_b，$$

$$k_a b \mid q_b b = d，$$

$$\frac{ab}{(a，\ b)} \mid d$$

这表明 $\frac{ab}{(a，\ b)}$ 是公倍数中最小的，定理得证.

最小公倍数与最大公因子的关系

例1-10 $a = 888$，$b = 312$，求$[a, b]$.

解 $(888, 312) = 24$，则$[888, 312] = =11544$.

1.2 素数

定义1-8　如果一个大于1的整数p除±1和$\pm p$外无其他因子，则p称为一个素数，否则称为合数.

定理1-11　设p是一个素数，则
1）对任意整数a，如果p不整除a，则$(p, a) = 1$.
2）如果$p \mid ab$，则$p \mid a$，或$p \mid b$.

算术基本定理

定理1-12 （算术基本定理）每个大于1的整数a都可以分解为有限个素数的乘积：

$$a = p_1 p_2 \cdots p_r .$$

该分解除素数因子的排列外是唯一的.

标准因子分解式

由于p_1，p_2，…，p_r中可能存在重复，所以a的分解式可表示为有限个素数的幂的乘积：

$$a = p_1^{k1} p_2^{k2} \cdots p_m^{km}.$$

这称为a的标准因子分解式.

例**1.2.2**　2100的标准因子分解式：

$$2100 = 2\times2\times3\times 5\times 5\times7 = 2^2\times3^1\times5^2\times7^1.$$

Eratosthenes筛法

定理1.2.3 设a是任意大于1的整数，则a的除1外最小正因子q是一素数，并且当a是一合数时，

$$q \le \sqrt{a}$$

证明 由算术基本定理，该定理的前一点是显然的.

当a是一合数时，可设

$$a = a_1 q，\text{其中} a_1 \ge q，$$

$$\text{则} a = a_1 q \ge q^2，$$

$$\sqrt{a} \ge q$$

定理证毕.

Eratosthenes筛法

对于一般N，Eratosthenes筛法可表述如下：

第1步　找出的$\leq \sqrt{N}$全部素数：p_1，p_2，…，p_m.

第2步　在1~N中分别划去p_1，p_2，…，p_m全部倍数.

第2步完成后剩下的数除1外就是不超过N的全部素数.

筛法原理如下：对于一个数$a \leq N$，如果p_1，p_2，…，p_m都不整除a，则a是素数．这是因为如果a是合数，则由定理3，它必有一素因子在p_1，p_2，…，p_m中.

Eratosthenes筛法

求不超过100的全部素数.

第1步　找出 $\leq \sqrt{100} = 10$ 的全部素数：2，3，5，7.

第2步　在1～100中分别划去第1步找出的每个素数的全部倍数：分别划去2的全部倍数、3的全部倍数、5的全部倍数和7的全部倍数.

（1）划去2的全部倍数：

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Eratosthenes筛法

得到剩下的数：

1	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99

Eratosthenes筛法

（2）划去3的全部倍数：

1	2	3	5	7	~~9~~
11		13	~~15~~	17	19
~~21~~		23	25	~~27~~	29
31		~~33~~	35	37	~~39~~
41		43	~~45~~	47	49
~~51~~		53	55	~~57~~	59
61		~~63~~	65	67	~~69~~
71		73	~~75~~	77	79
~~81~~		83	85	~~87~~	89
91		~~93~~	95	97	~~99~~

Eratosthenes筛法

得到剩下的数：

1	2	3	5	7	
11		13		17	19
		23	25		29
31			35	37	
41		43		47	49
		53	55		59
61			65	67	
71		73		77	79
		83	85		89
91			95	97	

Eratosthenes筛法

同理可以将因子5，7的倍数划去：

（3）划去5的全部倍数：

（4）划去7的全部倍数：

最终经过上述步骤后剩下的数除1外就是不超过100的全部素数：（25个）

2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97

Eratosthenes筛法

对于一般N，Eratosthenes筛法可表述如下：

第1步　找出不大于$\sqrt{N}$ 全部素数：p_1，p_2，…，p_m.

第2步　在1~N中分别划去p_1，p_2，…，p_m全部倍数.

第2步完成后剩下的数除1外就是不超过N的全部素数.

筛法原理如下：对于一个数$a \le N$，如果p_1，p_2，…，p_m都不整除a，则a是素数．这是因为如果a是合数，则由定理3，它必有一素因子在p_1，p_2，…，p_m中.

素数无穷个

定理1-13 素数有无穷多个.

证明 用反证法. 假设素数是有限个，设它们为：

p_1，p_2，…，p_k. 令$M = p_1p_2\cdots p_k + 1$.

设p是M的一个素因子，则

$$p \mid M,$$

而p在p_1，p_2，…，p_k中，则

$$p \mid p_1p_2\cdots p_k,$$

于是

$$p \mid (M - p_1p_2\cdots p_k)，\text{而}(M - p_1p_2\cdots p_k) = 1,$$

因为$p>1$，这显然是不可能的. 定理得证.

1.3 同余

定义1-9　给定一个称为模的正整数m．如果m除整数a，b得相同的余数，即

$$a = q_1 m + r，\quad b = q_2 m + r，\quad 0 \le r < m，$$

则称a和b关于模m同余，记为

$$a \equiv b \pmod{m}.$$

例1-15　$25 \equiv 1 \pmod 8$，$16 \equiv -5 \pmod 7$.

1.3 同余

定理1-15 整数a，b对模m同余的充分必要条件是：$m \mid (a-b)$，即$a = b+mt$，t是整数.

注释：整数a，b对模m同余

$\Longleftrightarrow$ 存在整数q_1，q_2，使得$a= q_1m+r$，$b = q_2m+r$，$0 \le r < m$

$\Longleftrightarrow$ $m \mid (a-b)$

$\Longleftrightarrow$ 存在整数t，使得$a = b+mt$

1.3 同余

证明 设 $a = q_1m+r_1$，$0 \le r_1 < m$，$b = q_2m+r_2$，$0 \le r_2 < m$.

（必要性）如果 $a \equiv b \pmod m$，则 $r_1 = r_2$

因此　　$a-b = m(q_1-q_2)$，$m \mid (a-b)$.

（充分性）如果 $m \mid (a-b)$，

则　　$m \mid m(q_1-q_2)+(r_1-r_2)$，

于是 $m \mid (r_1-r_2)$. 由于 $|r_1-r_2| < m$，

故　　$(r_1-r_2) = 0$，$r_1 = r_2$.

证毕。

定理 模m同余是等价关系,即

(1) 对任一整数a, $a \equiv a \pmod{m}$; (自反性)

(2)若$a \equiv b \pmod{m}$,则$b \equiv a \pmod{m}$; (对称性)

(3)若$a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$,

则$a \equiv c \pmod{m}$ (传递性)

证 (1) 因$m \mid a-a=0$,所以$a \equiv a \pmod{m}$.

(2)若$a \equiv b \pmod{m}$,则$m \mid a-b$,有$m \mid b-a$,于是

$$b \equiv a \pmod{m}.$$

(3)若$a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$,则$m \mid a-b$, $m \mid b-c$,

于是$m \mid (a-b)+(b-c)=a-c$,故$a \equiv c \pmod{m}$.

同余性质及推论

同余具有下列性质：

如果$a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$，则

1. $a_1+a_2 \equiv b_1+b_2 \pmod m$
2. $a_1-a_2 \equiv b_1-b_2 \pmod m$
3. $a_1a_2 \equiv b_1b_2 \pmod m$
4. 设$ac \equiv bc \pmod m$，且$(c, m) = 1$，则$a \equiv b \pmod m$
5. 设$a \equiv b \pmod m$，且$d \mid m$，d是正整数，则$a \equiv b \pmod d$
6. 设$a \equiv b \pmod m$，d是正整数，则$ad \equiv bd \pmod{md}$
7. 设$a \equiv b \pmod m$，$d \mid (a,b,m)$，则$a/d \equiv b/d \pmod{m/d}$

同余性质及推论

由$a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$，得$m \mid (a_1 - b_1)$，$m \mid (a_2 - b_2)$，则

1）$m \mid (a_1 - b_1) + (a_2 - b_2) = (a_1 + a_2) - (b_1 + b_2)$，故$a_1 + a_2 \equiv b_1 + b_2 \pmod m$.

2）$m \mid (a_1 - b_1) - (a_2 - b_2) = (a_1 - a_2) - (b_1 - b_2)$，故$a_1 - a_2 \equiv b_1 - b_2 \pmod m$.

3）$m \mid a_2(a_1 - b_1) + b_1(a_2 - b_2) = a_1a_2 - b_1b_2$，故$a_1a_2 \equiv b_1b_2 \pmod m$.

4）由$ac \equiv bc \pmod m$，得$m \mid ac - bc = c(a - b)$，

因为$(c, m) = 1$，则$m \mid (a - b)$，$a \equiv b \pmod m$.

5）由$a \equiv b \pmod m$，得$m \mid (a - b)$，而$d \mid m$，则$d \mid (a - b)$，$a \equiv b \pmod d$.

6）同上，得$md \mid (ad - bd)$，则$ad \equiv bd \pmod{md}$

7）同上，得 $m/d \mid (a/d - b/d)$

定理 设m是一个正整数, $ad \equiv bd \pmod{m}$, 如果$(d,m)=1$, 则

$$a \equiv b \pmod{m}$$

证 若 $ad \equiv bd \pmod{m}$, 则$m \mid ad-bd$,即

$$m \mid d(a-b)$$

因 $(d,m)=1$, 所以$m \mid a-b$,故

$$a \equiv b \pmod{m}$$

上面几个性质,其模m不发生变化,属于基本性质.

以下是模发生变化的几个性质.

定理 设m是正整数, $a \equiv b \pmod{m}, k > 0$, 则

$$ak \equiv bk \pmod{mk}$$

证 由$a \equiv b \pmod{m} \Rightarrow m \mid a-b$

$$\Rightarrow mk \mid (a-b)k = ak - bk$$

$$\Rightarrow ak \equiv bk \pmod{mk}$$

定理 设m是正整数, $a \equiv b \pmod{m}$,如果d是a, b及m的任一公因数,则

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

证 因$a \equiv b \pmod{m}$,所以存在整数k,使得

$$a = b + mk$$

于是 $\frac{a}{d} = \frac{b}{d} + \frac{m}{d}k,$ 因$\frac{a}{d}, \frac{b}{d}, \frac{m}{d}$都是整数,故

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

定理 设m是正整数, $a \equiv b \pmod{m}$, 如果 $d \mid m$, $d>0$, 则

$$a \equiv b \pmod{d}.$$

证　因$a \equiv b \pmod{m}$, 所以$m \mid a-b$.

又因　$d \mid m$,　于是　$d \mid a-b$.

故　　$a \equiv b \pmod{d}$

例9　因 $190 \equiv 50 \pmod{70}$,

所以 $19 \equiv 5 \pmod{7}$, $190 \equiv 50 \pmod{7}$

同余性质及推论

推论　如果$a_1 \equiv b_1 \pmod m$，$a_2 \equiv b_2 \pmod m$，则

1）$a_1x + a_2y \equiv b_1x + b_2y \pmod m$，其中$x$，$y$是任意整数.

2）$a_1^n = b_1^n \pmod m$，其中n是正整数.

3）$f(a_1) \equiv f(b_1) \pmod m$，其中$f(x)$是任一给定的整系数多项式：　$f(x) = c_0 + c_1x + \ldots + c_kx_k$.

推论的证明留做习题.

同余应用

例1.3.2　求$2^{64} \pmod{641}$

解

$2^8 = 256$，

$2^{16} = 65536 \equiv 154 \pmod{641}$，

$2^{32} \equiv 154^2 = 23716 \equiv 640 \equiv -1 \pmod{641}$.

$2^{64} \equiv (-1)^2 \equiv 1 \pmod{641}$

同余应用

例1.3.3 2004年9月8 日星期三，问2^{2005}天后是星期几？

解：

按照星期定义，问题可以转化为2^{2005}模7余几的问题。

由$2^3 \equiv 1$（mod7）知

$$2^{2005} \equiv 2^{3\times 668+1} \equiv (2^3)^{668} \times 2 \equiv 2 \text{（mod7）}$$

所以2^{2005}天后是星期五。

同余应用

例4　验证28997×39495 = 1145236415是否正确.

如果28997×39495 = 1145236415，则有28997×39495 ≡ 1145236415(mod 9)，即

$(2\times10^4+8\times10^3+9\times10^2+9\times10+7)\times(3\times10^4+9\times10^3+4\times10^2+9\times10+5)$

$\equiv(1\times10^9+1\times10^8+4\times10^7+5\times10^6+2\times10^5+3\times10^4+6\times10^3+4\times10^2+1\times10+5)\pmod 9$,

于是有

$(2+8+9+9+7)\times(3+9+4+9+5)\equiv(1+1+4+5+2+3+6+4+1+5)\pmod 9$,

即 $[(2+7)+8+9+9]\times[3+9+(4+5)+9]$

$\equiv[1+1+(4+5)+2+(3+6)+(4+5)+1]\pmod 9$,

于是有 $8\times3\equiv5\pmod 9$,

显然此式错误，故28997×39495 = 1145236415错误.

第一章 整除与同余

重点:

1. 最大公因数求法: 欧几里得除法
2. 最大公因数定理：扩展欧几里得
3. 最小公倍数的求法
4. Eratosthenes筛法
5. 算术基本定理及标准因子分解式
6. 同余定义及其性质

欧几里得除法:

1. (a, b)
2. [a, b]
3. (a, b)=sa+tb
4. 1=sa+tb, 则a^{-1}=s(modb), b^{-1}=t(moda)
5. $1 = s \cdot \frac{a}{(a,b)} + t \cdot \frac{b}{(a,b)}$, 则 $(\frac{a}{(a,b)})^{-1} \equiv s(\mathrm{mod}\frac{b}{(a,b)})$

作 业 P13

- 1，2，4，5，6，7， 11，12，13，14，15

谢谢！