21世纪高等院校计算机教材系列

计算机安全学

李 辉 编著

购书可获得增值回报
提供教学用电子教

机械工业出版社
CHINA MACHINE PRESS

21世纪高等院校计算机教材系列

计算机安全学

李 辉 编著

机械工业出版社

本书对计算机安全学的理论和应用进行了系统的阐述。

本书共分5章。第1章介绍了必备数学知识；第2章系统讲解了密码学理论，包括加密解密系统、数字签名、数字摘要以及密钥分发和管理等原理；第3～5章分别讨论了安全学理论在计算机网络、操作系统、数据库系统方面的典型应用，对相关应用领域的重要协议进行了分析。本书各章配有习题，供读者练习。

本书可作为高等院校计算机及相关专业的教材，亦可作为计算机从业人员的参考书或广大电脑爱好者的自学读物。

图书在版编目（CIP）数据

计算机安全学/李辉编著 .—北京：机械工业出版社，2005.2
（21世纪高等院校计算机教材系列）
ISBN 7-111-16003-7

Ⅰ.计… Ⅱ.李… Ⅲ.电子计算机－安全技术－高等学校－教材
Ⅳ.TP309

中国版本图书馆CIP数据核字（2005）第002467号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
责任编辑：戴 琳 版式设计：霍永明 责任校对：樊钟英
封面设计：雷明顿 责任印制：杨 曦
北京机工印刷厂印刷·新华书店北京发行所发行
2005年3月第1版·第1次印刷
787mm×1092mm $^{1}/_{16}$ · 17.75印张 · 435千字
0 001—5 000册
定价：25.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、88379646
68326294、68320718
封面无防伪标均为盗版

出 版 说 明

计算机技术是一门迅速发展的现代科学技术，它在经济建设与社会发展中，发挥着非常重要的作用。近年来，我国高等院校十分注重人才的培养，大力提倡素质教育、优化知识结构，提倡大学生必须掌握计算机应用技术。为了满足教育的需求，机械工业出版社组织了这套“21世纪高等院校计算机教材系列”。

在本套系列教材的组织编写过程中，我社聘请了各高等院校相关课程的主讲老师进行了充分的调研和细致的研讨，并针对非计算机专业的课程特点，根据自身的教学经验，总结出知识点、重点和难点，一并纳入到教材中。

本套系列教材定位准确，注重理论教学和实践教学相结合，逻辑性强，层次分明，叙述准确而精炼，图文并茂，习题丰富，非常适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班和自学用书。

参加编写本系列教材的院校包括：清华大学、西安交通大学、北方交通大学、北京邮电大学、北京化工大学、北京科技大学、山东大学、首都经贸大学等。

机械工业出版社

前　言

自从1995年1月中国电信首次向社会公众提供互联网接入以来，互联网在我国已稳健地发展了近10年。今天，互联网已渗透到我们的工作、学习和生活之中，为我们带来了极大的方便。然而，就在人们逐渐离不开互联网和计算机的时候，安全问题也日渐突出。

实际上，安全学理论在第一台计算机诞生之前就已倍受学者关注，并取得一定成果。只是由于今天计算机运算速度更快，计算机及网络应用更丰富、更广泛，计算机安全学才在理论和应用方面开始面临新的挑战。

本书首先对安全学理论进行了详细的介绍，继而将安全学理论运用到计算机网络、操作系统和数据库系统中，从理论与实践相结合的指导思想出发，分析了相关领域的安全问题及相应的解决方案。

全书共分两大部分，第1～2章是第一部分，第3～5章是第二部分。第一部分以密码学理论为核心，讲述计算机安全学的基础理论，包括对称密钥算法、公钥算法、数字签名、数字摘要和密钥分发等内容；第二部分以网络安全为重点，介绍计算机安全学在互联网中的应用，包括虚拟专用网技术、防火墙技术、网络入侵检测技术、操作系统安全和数据库系统安全等内容。为了照顾到不同层次和不同水平的读者，本书在内容安排上由浅入深，循序渐进，各章的习题和思考题的难度也兼顾不同的需求。

本书的特点是：理论与实践相结合、经典与前沿相结合。理论方面，着重强调基本概念、重要定理的阐述和推导，每个定理和算法都举例说明；应用方面，在不失系统性的前提下，着重讨论网络安全、系统安全中的重点问题及主流的解决方案，对应用广泛、成熟的协议进行分析，而非面面俱到。

本书是编者根据多年来在国内外计算机安全领域的设计和工程经验，以及近几年在高等院校计算机安全学课程上的一线教学成果，参阅了大量国外科技文献后编写而成。编写过程中，广泛征求了业内专家、高年级本科生、研究生的意见和建议，力求把本书写成一本既反映学科前沿，又具有较高的理论水平和实用价值的教科书。

本书适用于高等院校计算机及相关专业的本科或研究生教学，亦可作为计算机工作者的参考资料或电脑爱好者的自学读物。

由于编写时间仓促，书中缺点和不当之处在所难免，欢迎广大教师、同行专家以及各位读者批评指正。

本书提供教学用电子教案，读者可到机械工业出版社网站 www.cmpbook.com 免费下载。

作　者

目　录

第 1 章　安全学基础

1.1　数论基础

数论知识是现代密码学的基础，如：Elgamal 算法、椭圆曲线算法用到有限域及循环群的概念和性质；RSA 算法基于欧拉定理；Rabin 算法用到中国剩余定理和扩展欧几里德算法等等。

本节将系统地介绍数论中的一些基本概念和定理。为强调实用性，与计算机安全学关系不大的概念和定理在此没有一一介绍。

有数学专业基础的读者可跳过此节。

1.1.1　循环群

定义 1-1　（等价关系）设 ~ 是集合 G 上的一个二元关系，若满足以下条件：

1）自反性：对任何 $a\in G$，有 $a\sim a$

2）对称性：对任何 a，$b\in G$，有 $a\sim b\Rightarrow b\sim a$

3）传递性：对任何 a，b，$c\in G$，有 $a\sim b$ 且 $b\sim c\Rightarrow a\sim c$

则称 ~ 为 G 中的一个等价关系（Equivalence Relation）。

定义 1-2　（等价类）子集 $\bar{a}=\{x\mid x\in G,\ x\sim a\}$ 称为 a 所在的等价类（Equivalence Class）。

换句话说，等价类就是与 a 等价的元素的集合。

【例 1-1】（同余关系）设 m 为非零整数，a、b 为整数，如果 $m\mid a-b$，称 a 与 b 对模 m 是同余关系（Congruence）。

不难验证，同余关系是一种等价关系，它满足等价关系的自反性、对称性和传递性。

1）自反性：对于任何整数 a，a 与 a 对模 m 同余。

2）对称性：对于任何整数 a、b，如果 a 与 b 对模 m 同余，那么显然有 b 与 a 对模 m 同余。

3）传递性：对于任何整数 a、b、c，如果 a 与 b 对模 m 同余，b 与 c 对模 m 同余，那么 a 与 c 对模 m 同余。

定义在整数集 Z 上的同余关系，可以将整数集 Z 划分为“同余类”。

【例 1-2】（同余类）称集合 $\{b:\ b\equiv a\ (\mathrm{mod}\,m)\}$ 为模 m 的同余类，又称同余子集，记为 $[a]_m$，如果 $a_0\in[a]_m$，且 $0\leqslant a_0<m$，则称 a_0 为 $[a]_m$ 的主余数，记为 $<a>_m$。

定义 1-3　（商集）针对某个等价关系 ~，集合 G 的所有等价类构成的集合，称为集合 G 关于 ~ 的商集，记作 $A/\sim$，即 $A/\sim=\{\bar{a}\mid a\in A\}$。

【例 1-3】Z 对模 m 的同余关系的商集记为 Z_m，显然，商集 Z_m：$Z/\equiv\ (\mathrm{mod}\,m)$ 由同余子集 $[0]_m$，$[1]_m$，…，$[m-1]_m$ 构成。

定义 1-4　（群、半群、含么半群、交换群）G 为非空集合，如果在 G 上定义的二元

运算“$*$”满足：

1）（封闭性）对于任意 a，b，$c\in G$，$a*b\in G$，

2）（结合律）对于任意 a，b，$c\in G$，有 $(a*b)*c=a*(b*c)$

3）（么元）存在么元 e 使得对于任意 $a\in G$，$e*a=a*e=a$

4）（逆元）对于任意 $a\in G$ 存在逆元 a^{-1}，使得 $a^{-1}*a=a*a^{-1}=e$

则称（G，$*$）是群（Group），有时简称 G 是群。如果仅满足 1）和 2）则称 G 是一个半群（Semigroup）。如果仅满足 1）、2）和 3）则称 G 是一个含么半群（Monoid）。

如果群（G，$*$）还满足交换律：

5）对于任意，a，$b\in G$，有：$a*b=b*a$

则称 G 为交换群或阿贝尔群（Abel Group）。

【例 1-4】Z 是整数集合，$+$ 和 $*$ 分别是整数的加法和乘法运算，（Z，$+$）是群。但是，（Z，$*$）不是群，这是因为除 1 和 -1 外的其他元素都没有逆元。

【例 1-5】设 $G=\{1,-1\}$，$*$ 是数的乘法，则（G，$*$）是群。

【例 1-6】（Klein 四元群）设集合 $K=\{e,a,b,c\}$，K 中的二元运算“$*$”由表 1-1 中的 Klein 乘法表给出：

表 1-1　Klein 乘法表

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

则（K，$*$）是群。

首先，不难验证（K，$*$）满足结合律，么元是 e，每个元素的逆元是它本身，所以（K，$*$）是群，而且还是交换群。

【例 1-7】（么群）（$\{0\}$，$+$）是群。由于只包含么元，所以该群又称么群。

除了（$\{0\}$，$+$）是么群外，（$\{1\}$，$*$）也是么群。

关于群的么元和逆元有以下结论：

1）么元是惟一的：设 G 有两个么元分别为 e_1 和 e_2，则：

$$e_1=e_1*e_2=e_2$$

2）逆元是惟一的：设 G 中元素 a 有两个逆元，分别为 a_1^{-1} 和 a_2^{-1}，则：

$$a_1^{-1}=a_1^{-1}*e=a_1^{-1}*(a*a_2^{-1})=(a_1^{-1}*a)*a_2^{-1}=e*a_2^{-1}=a_2^{-1}$$

3）a_1*a_2 的逆元是 $a_2^{-1}*a_1^{-1}$；

4）$a_1*a_2*\cdots*a_n$ 的逆元是 $a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$。

【例 1-8】* 由定义在有限域上的椭圆曲线的整数坐标点和无穷远点构成的集合是群，该群的么元为无穷远点。

有关椭圆曲线的定义和群的证明见第 2 章。

定义 1-5　（无限群、有限群、群的阶）设（G，$*$）是群，G 的元素个数是无限时，G 称为无限群；G 的元素个数是有限时，G 称为有限群；G 的元素个数称为群 G 的阶。

定义 1-6 （元素的阶）满足 $a^n = e$ 的最小正整数 n，称为元素 a 的阶，记作 $o(a)$。如果 $a^n = e$ 永不成立，则称 a 的阶为无穷大。

定理 1-1 设 G 是群，$a \in G$，则 $a^m = 1 \Leftrightarrow o(a) \mid m$.

证明：如果 $a^m = 1$，设 $o(a) = n \leqslant m$，$m = kn + r$，$0 \leqslant r < n$，于是

$$a^m = a^{kn+r} = a^{kn}a^r = a^r = 1$$

但是 a 的阶是 n 而不是 r，所以 $r = 0$，$m = kn$，因此 $o(a) \mid m$；

反之，如果 $o(a) \mid m$，则 $m = kn$，于是：

$$a^m = a^{kn} = (a^n)^k = 1^k = 1$$

命题得证。

定义 1-7 （子群）设 S 是群 G 的一个非空子集，如果 S 对 G 的运算也构成群，则称 S 是 G 的子群（Subgroup），记作：$S \leqslant G$。

【例 1-9】（循环子群、生成元）设 G 是群，$a \in G$，令 $H = \{a^k \mid k \in Z\}$，H 对于二元运算同时满足：

1）封闭性：对于任意的 a^{k_1}，$a^{k_2} \in G$，$a^{k_1} * a^{k_2} = a^{k_1+k_2} \in G$

2）结合律：对于任意的 a^{k_1}，a^{k_2}，$a^{k_3} \in G$，$(a^{k_1} * a^{k_2}) * a^{k_3} = a^{k_1} * (a^{k_2} * a^{k_3})$

3）么元：么元是 G 的么元 e

4）逆元：对于任意的 $a^k \in G$，逆元为 $a^{-k} \in G$，$a^k * a^{-k} = a^{-k} * a^k = e$

因此 H 是 G 的子群，称为循环子群（Cyclic Subgroup），记作 $< a >$，a 是该子群的生成元。

特别地，当 $G = < a >$ 时，称 G 是循环群，下面给出循环群的完整定义。

定义 1-8 （循环群）一个群（G，$*$）称为循环群，如果存在一个元素 $a \in G$，使得：

$$G = \{a^n \mid n \in Z\}$$

【例 1-10】（Z，+）是由 1 生成的循环群。因为任何整数都可以写成若干个 1 相加的形式。

实际上，循环群（Z，+）的生成元只能是 1 和 -1，因为：设生成元为 a，由于 $1 \in Z$，必存在 k 使得 $ka = 1$，于是 $a = \pm 1$。

【例 1-11】如果 p 是素数，那么（Z_p，+）是循环群（Z_p 的定义见例 1-3）。

令 $p = 6$，$Z_6 = \{[0]_6, [1]_6, \cdots, [5]_6\}$，循环群 Z_6 的么元是 $[0]_m$，元素 $[1]_m$ 是生成元，元素 $[1]_m$ 的阶是 6，元素 $[2]_m$ 的阶是 3，元素 $[3]_m$ 的阶是 2。

【例 1-12】如果 p 是素数，那么（Z_p^*，$*$）是循环群，其中 $Z_m^* = Z_m \setminus [0]_m$。

该命题是定理 1-4 的一个特例，因此可参考定理 1-4 的证明。

表 1-2 给出了当生成元为 2，$p = 11$ 时 $2^b \bmod 11$ 的计算结果。可以看到 $2^{b+10} \bmod 11$ 与 $2^b \bmod 11$ 的值相同，出现循环。

表 1-2 生成元为 2，$p = 11$ 时的循环群

b	1	2	3	4	5	6	7	8	9	10	11
$2^b \bmod 11$	2	4	8	5	10	9	7	3	6	1	2

关于循环群（Z_p，+）的生成元还有以下性质：

定理 1-2 （Z_p，+）的生成元只能是 $[a]_p$，其中 $\gcd(a, n) = 1$。

证明：设 $[a]_p$ 是生成元，因为 $[a]_p$ 必有逆，即

$$k[a]_p = 1$$

则存在 t 使得

$$k[a]_p + tn = 1$$

说明 gcd（a，n）=1，证毕。

定义 1-9 （环、交换环、零环）集合 G 以及定义在 G 上的封闭运算“+”和“*”，如果满足以下条件：

1）（G，+）是交换群。

2）（G，*）满足结合律：$a*(b*c)=(a*b)*c$（对于任意的 a，b，$c\in G$）。

3）（G，+，*）满足分配律：$a*(b+c)=a*b+a*c$（对于任意的 a，b，$c\in G$）。

则称（G，+，*）是环，简称 G 是环。如果（G，*）满足交换律，则 G 是交换环。

环的定义中并没有要求（G，*）存在乘法么元，所以最小的环可以只包含加法的么元，此时把 G 称为零环。

事实上，条件 2）等同于（G，*）是半群。

【例 1-13】（整数环）整数集 Z 对整数加法是交换群，对整数乘法是半群，并且对整数加法和乘法适用分配律，所以（Z，+，*）是环，同时 Z 对整数乘法还满足交换律，所以也是交换环。

【例 1-14】（同余类环）同余商集 Z_m 对模 m 的加法是交换群，对模 m 的乘法是半群，并且也满足分配律，所以 Z_m 也是环，称为同余类环。

【例 1-15】（多项式环）$R(x)=\{a_0+a_1x+\cdots+a_nx^n \mid a_i\in R,\ n\in Z,\ n\geqslant 0\}$是全体多项式集合，$R(x)$ 对多项式加法构成群，对多项式乘法构成半群，因此是环，称为多项式环。

定义 1-10 （子环、扩环）设（F，+，*）是环，S 是 F 的非空子集，称 S 为 F 的子环，称 R 是 S 的扩环，如果对于任意的 a，$b\in S$，有：

1）加法封闭：$a+b\in S$

2）存在加法逆：$-a\in S$

3）乘法封闭：$a*b\in S$

其中，条件 1）可以由 $a-b\in S$ 替代。

显然，{0}和 F 都是 F 的子环。

定义 1-11 （域）集合 G 以及定义在 G 上的封闭运算“+”和“*”，如果满足以下条件：

1）（G，+）是交换群。

2）（$G*$，*）是交换群。

3）（G，+，*）满足分配律：$a*(b+c)=a*b+a*c$（对于任意的 a，b，$c\in G$）。

则称（G，+，*）是域，简称 G 是域。

定义 1-12 （子域、扩域）设 S 是域 F 的子环，并且 S 是域，则称 S 是 F 的子域，F 是 S 的扩域。

定义 1-13 （有限域）如果域 K 的基数是有限数，则称 K 为有限域。

下面的定理将给出（Z_m，+，*）是有限域的充要条件。

定理 1-3 当且仅当 m 是素数时，$(Z_m, +, *)$ 是有限域。

证明：对于加法而言，$[0]_m$ 是么元，于是 $Z_m^* = Z_m \setminus [0]_m$。

令 $m = ab$，其中 $0 < a < m$，$0 < b < m$，则有

$$[a]_m, [b]_m \in Z_m^*$$

但是

$$[a]_m * [b]_m = [ab]_m = [n]_m = [0]_m \notin Z_m^*$$

因此 Z_m^* 不可能对乘法成为群，于是 Z_m 也不可能成为域。

如果 m 为素数，取 Z_m^* 的任意元素 $[p]_m$，则 m，p 的最大公因数必为 1。

存在整数 k_1 和 k_2 使得：

$$k_1 m + k_2 p = 1$$

两边取同余式可得：

$$[k_1]_m * [p]_m = [1]_m$$

$[1]_m$ 是 Z_m^* 的乘法么元，所以 $[k_1]_m$ 是 $[p]_m$ 的逆元。

有么元，有逆元，也满足交换律，于是 $(Z_m^*, *)$ 是交换群，$(Z_m, +, *)$ 是有限域。证毕。

定义 1-14 （特征）设 $(F, +, *)$ 是域，若么元在群 $(F, +)$ 中的阶为素数 p，则称 p 为域 F 的特征，记为 $\mathrm{ch}F$；若么元在 $(F, +)$ 中的阶为无穷大，则称 F 的特征为 0。

显然，若 $\mathrm{ch}F = 0$，则 F 为无限域；若 $\mathrm{ch}F$ 为某个素数，则 F 为有限域。

定理 1-4 域 F 的任何有限子乘群都是循环群。

证明：设 G 是域 F 的有限子乘群，令 m 是使 G 中任何元素 a 都满足 $a^m = 1$ 的最小正整数。又设 $c \in G$ 且 $o(c) = m$，显然 $m \leqslant |G|$。

同时，G 中的元素均满足 $x^m - 1 = 0$，而多项式 $f(x) = x^m - 1$ 在 F 上最多有 m 个不同的根，故 $|G| \leqslant m$，因此 $|G| = m$，命题得证。

在由域 F 的任何有限子乘群构成的循环群中，相应的生成元又叫本原元。例如：例 1-12 中，2 是 Z_{11} 的本原元。

1.1.2 欧几里德算法

定理 1-5 （欧几里德算法）两个正整数 $r_0 > r_1$，欧几里德算法包括下列分式组：

$$\begin{aligned}
&r_0 = q_1 r_1 + r_2 && 0 < r_2 < r_1\\
&r_1 = q_2 r_2 + r_3 && 0 < r_3 < r_2\\
&\cdots\cdots\\
&r_{m-2} = q_{m-1} r_{m-1} + r_m && 0 < r_m < r_{m-1}\\
&r_{m-1} = q_m r_m
\end{aligned} \tag{1-1}$$

通过欧几里德算法可以得出 r_0 和 r_1 的最大公约数 r_m：

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{m-1}, r_m) = r_m$$

【例 1-16】求解 $\gcd(2001, 99)$。

$$2001 = 20 \times 99 + 21$$
$$99 = 4 \times 21 + 15$$
$$21 = 1 \times 15 + 6$$
$$15 = 2 \times 6 + 3$$
$$6 = 2 \times 3$$
$$r_m = 3$$

因此 gcd（2001，99）= gcd（99，21）= … = gcd（6，3）= 3。

定理 1-6 （欧几里德扩展算法）根据欧几里德算法的参数 q_1，q_2，…，q_m，构造序列 t_0，t_1，…，t_m：

$$t_0 = 0$$
$$t_1 = 1$$
……
$$t_j = t_{j-2} - q_{j-1} t_{j-1} \bmod r_0$$

对于 $0 \leqslant j < m$，$r_j \equiv t_j r_1 \bmod r_0$ 恒成立。

证明：容易验证当 $j = 0$ 和 $j = 1$，等式 $r_j \equiv t_j r_1 \bmod r_0$ 成立。

假设当 $j = i - 2$ 和 $j = i - 1$ 时等式成立，即：

$$r_{i-2} \equiv t_{i-2} r_1 \bmod r_0$$
$$r_{i-1} \equiv t_{i-1} r_1 \bmod r_0$$

那么

$$\begin{aligned} r_i &= r_{i-2} - q_{i-1} r_{i-1} \\ &= t_{i-2} r_1 - q_{i-1} t_{i-1} r_1 \\ &= (t_{i-2} - q_{i-1} t_{i-1}) r_1 \\ &\equiv t_i r_1 (\bmod r_0) \end{aligned}$$

根据数学归纳法，$r_j \equiv t_j r_1 \bmod r_0$ 恒成立，命题得证。

定理 1-7 设 gcd（r_0，r_1）= 1，则 $t_m = r_1^{-1} \bmod r_0$。

证明：根据定理 1-5，可得：

$$r_m = \gcd(r_0, r_1) = 1$$

在定理 1-6 中，令 $j = m$，有：

$$t_m r_1 \equiv r_m \equiv 1 \bmod r_0$$

因此 $t_m = r_1^{-1} \bmod r_0$ 成立。命题得证。

利用定理 1-7 可计算有限域上的元素倒数，算法描述如下：

1）$a = r0$

2）$b = r1$

3）$c = 0$

4）$d = 1$

5）$q = [a/b]$

6）$r = a - q \times b$

7）while $r > 0$ *do*

8） $temp = c - q \times d$

9） if $temp > 0$ then $temp = temp \bmod a$

10） else $temp = n\text{-}temp \bmod a$

11） $c = d$

12） $d = temp$

13） $a = b$

14） $b = r$

15） $q = [a/b]$

16） $r = a - q \times b$

17） if $b \neq 1$ then $r1$ 的模 $r0$ 逆不存在

18） else d 是 $r1$ 的模 $r0$ 逆

【例 1-17】求解 $7^{-1} \bmod 26$。

解：

$$26 = 3 \times 7 + 5, \qquad t_0 = 0$$

$$7 = 1 \times 5 + 2, \qquad t_1 = 1$$

$$5 = 2 \times 2 + 1, \qquad t_2 = t_0 - q_1 t_1 = 0 - 3 \times 1 = 23 \ (\text{mod}26)$$

$$2 = 2 \times 1, \qquad t_3 = t_1 - q_2 t_2 = 1 - 1 \times 23 = 4 \ (\text{mod}26)$$

$$7^{-1} = t_4 = t_2 - q_3 t_3 = 23 - 2 \times 4 = 15 \ (\text{mod}26)$$

容易验证：$7 \times 15 = 105 = 1 \ (\text{mod}26)$。

1.1.3 中国剩余定理

《孙子算经》中曾经提出一个问题：“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?”。

这是一个典型的同余式组求解的问题，描述如下：

$$\begin{aligned} x &= a_1 \bmod m_1 \\ x &= a_2 \bmod m_2 \\ &\cdots\cdots \\ x &= a_n \bmod m_n \end{aligned} \tag{1-2}$$

该问题将在下一章中的 Rabin 公钥算法中遇到。

同余式组问题通常由中国剩余定理求解，中国剩余定理也称孙子定理。

定理 1-8 （中国剩余定理）设 m_1，m_2，…，m_n 是 n（$n \geqslant 2$）个两两互素的大于 1 的整数，令

$$M = m_1 m_2 \cdots m_n = m_1 M_1 = m_2 M_2 = \cdots = m_n M_n$$

则同余方程组（1-2）的解为：

$$x \equiv a_1 b_1 M_1 + a_2 b_2 M_2 + \cdots + a_n b_n M_n (\bmod M) \tag{1-3}$$

其中，b_i（$1 \leqslant i \leqslant n$）是满足同余方程

$$M_i x_i \equiv 1 (\bmod m_i) \tag{1-4}$$

的一个特解。

证明：可以分成两步来证明：1）证明式（1-3）是同余方程组（1-2）的解；2）证明同

余方程组的解均在式（1-2）中。

1）将式（1-3）代入同余方程组（1-2）中，对于任意第 i 个方程，等式左边等于：

$$x \equiv a_1 b_1 M_1 + a_2 b_2 M_2 + \cdots + a_n b_n M_n (\mathrm{mod}\, M)$$

其中，除第 i 项外其余各项都能被 m_i 整除，而第 i 项为 $a_i b_i M_i$，由式（1-4）可得：

$$a_i b_i M_i \equiv a_i (\mathrm{mod}\, m_i)$$

2）设 x'是同余方程组（1-2）中的任意一个解：

$$x' \equiv a_i (\mathrm{mod}\, m_i), i = 1,2,\cdots,n$$

设 x 是由式（1-3）和式（1-4）确定的解，则：

$$x - x' \equiv 0 (\mathrm{mod}\, m_i), i = 1,2,\cdots,n$$

$$m_i \mid (x - x'), i = 1,2,\cdots,n$$

又因为 m_1，m_2，…，m_n 两两互素，所以

$$m_1 m_2 \cdots m_n \mid (x - x')$$

$$x' \equiv x (\mathrm{mod}\, M)$$

也就是说 x'被包含于由式（1-3）和式（1-4）确定的解中。

命题得证。显然，同余方程组（1-2）的最小非负整数解是 x 对模 M 的主余数。

此外，中国剩余定理还有另一种表述："设 m_1，m_2，…，m_n 是 n 个（$n \geqslant 2$）两两互素的大于 1 的整数，令 $M = m_1 m_2 \cdots m_n$，则对于任意的 j（$1 \leqslant j \leqslant n$），以下联立同余式有解：

$$x_j \equiv 1 \mathrm{mod}\, m_j$$

$$x_j \equiv 0 \mathrm{mod}\, m_i, i \neq j$$

令 $x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$，则$[x]_m$ 是同余式组（1-2）的解。"

只需证明 $x_i = b_i M_i$ 就可说明两种表述的等价性，感兴趣的读者可将此命题的证明作为习题。

【例 1-18】求解 x，x 满足下列同余式组：

$$\begin{cases} x \equiv 5 (\mathrm{mod}7) \\ x \equiv 3 (\mathrm{mod}11) \\ x \equiv 10 (\mathrm{mod}13) \end{cases}$$

解：

$$a_1 = 5, a_2 = 3, a_3 = 10$$

$$m_1 = 7, m_2 = 11, m_3 = 13$$

$$M = m_1 m_2 m_3 = 1001$$

$$M_1 = m_2 m_3 = 143, M_2 = m_1 m_3 = 91, M_3 = m_1 m_2 = 77$$

可通过定理 1-7 来求解 b_i：

$$b_1 = 143^{-1} = 5 (\mathrm{mod}7)$$

$$b_2 = 91^{-1} = 4 (\mathrm{mod}11)$$

$$b_3 = 77^{-1} = 12 (\mathrm{mod}13)$$

该同余方程组最终的解为：

$$x = 13907 = 894 (\mathrm{mod}1001)$$

中国剩余定理不仅可以用来求解同余方程组，还可以用来求解二次同余方程，其方法就是

将二次同余方程化为同余方程组来求解。

【例 1-19】求解二次同余方程：$x^2+3x+2\equiv 0\ (\mathrm{mod}35)$.

解：可将二次同余方程变为同余方程组：

$$\begin{cases} x^2+3x+2\equiv 0(\mathrm{mod}5) \\ x^2+3x+2\equiv 0(\mathrm{mod}7) \end{cases} \tag{1-5}$$

因为 $x^2+3x+2=(x+1)(x+2)$，所以进一步可将二次同余方程组（1-5）分解为 4 个一阶同余方程组：

$$\begin{cases} x\equiv 3(\mathrm{mod}5) \\ x\equiv 5(\mathrm{mod}7) \end{cases} \quad \begin{cases} x\equiv 3(\mathrm{mod}5) \\ x\equiv 6(\mathrm{mod}7) \end{cases}$$

$$\begin{cases} x\equiv 4(\mathrm{mod}5) \\ x\equiv 5(\mathrm{mod}7) \end{cases} \quad \begin{cases} x\equiv 4(\mathrm{mod}5) \\ x\equiv 6(\mathrm{mod}7) \end{cases}$$

根据定理 1-8 可分别求出 4 个同余方程组的解：

$$x\equiv 33,13,19,34(\mathrm{mod}35)$$

1.1.4 欧拉定理

定义 1-15 （欧拉函数）自变量为正整数 n 的函数 $\varphi(n)$ 称为欧拉函数，$\varphi(n)$ 表示小于 n 且与 n 互素的正整数的个数。

显然，当 n 为素数时，$\varphi(n)=n-1$。

下面的定理有助于求解欧拉函数的值。

定理 1-9 若 $\gcd(a,b)=1$，则 $\varphi(ab)=\varphi(a)\varphi(b)$。

证明：任意 x（$0\leqslant x<ab$）与数对（k_1，k_2）一一对应：

$$\begin{cases} x\equiv k_1(\mathrm{mod}a) \\ x\equiv k_2(\mathrm{mod}b) \end{cases}$$

因为 $<0>_m$，$<1>_m$，…，$<ab-1>_m$ 一共是 ab 个数，（k_1，k_2）也一共有 ab 种组合，且都各不相同。

对于 $0\leqslant x<ab$ 的任意 x，x 与 ab 互素等价于 x 与 a 和 b 都互素，用反证法易证。

而 x 与 a 和 b 都互素又等价于 k_1 与 a 互素且 k_2 与 b 互素。

因此，与 ab 互素的数 x 的个数等于数对$\{(k_1,k_2)\mid \gcd(k_1,a)=1,\gcd(k_2,b)=1\}$的个数，即 $\varphi(ab)=\varphi(a)\varphi(b)$，命题得证。

定理 1-10 如果 $n=p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}$，其中 p_i 为素数，$0<i\leqslant m$，那么：

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$$

证明：首先证明 $\varphi(p^a)=p^a\left(1-\frac{1}{p}\right)$。

任意 x（$0\leqslant x<n$）要么是 p 的倍数，要么与 p^a 互素。其中：p 的倍数分别是

$$0,p,2p,\cdots,(p^{a-1}-1)p$$

一共有 p^{a-1}个，因此与 p^a 互素的数是$p^a-p^{a-1}=p^a\left(1-\frac{1}{p}\right)$个。

根据定理 1-9 得

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m})\\ &= \varphi(p_1^{a_1})\varphi(p_2^{a_2})\cdots\varphi(p_m^{a_m})\\ &= p_1^{a_1}\left(1-\frac{1}{p_1}\right)\cdot p_2^{a_2}\left(1-\frac{1}{p_2}\right)\cdots\cdots p_m^{a_m}\left(1-\frac{1}{p_m}\right)\\ &= p_1^{a_1}p_2^{a_2}\cdots p_m^{a_m}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)\end{aligned}$$

命题得证。

定理 1-11 （欧拉定理）a、n 为整数，如果 gcd（a，n）$=1$，则有：

$$a^{\varphi(n)} \equiv 1 \bmod n$$

证明：设 $\varphi(n)=k$，假设 r_1，r_2，…，r_k 是与 n 互素的模 n 的同余类的主余数。

由于 gcd（a，n）$=1$，ar_1，ar_2，…，ar_k 也应该是互素的，而且对于模 n 两两不同余，因此：

$$(ar_1)(ar_2)\cdots(ar_k) \equiv a^k r_1 r_2\cdots r_k \equiv r_1 r_2\cdots r_k \pmod n$$

$$(a^k-1)r_1 r_2\cdots r_n \equiv 0 \bmod(n)$$

因为 r_1，r_2，…，r_k 与 n 互素，所以 $a^k \equiv 1 \pmod n$，命题得证。

【例 1-20】设 $n=16$，$a=9$，满足 gcd（a，n）$=1$，与 n 互素的数分别为 1、3、5、7、9、11、13、15，所以 $\varphi(n)=8$，$a^{\varphi(n)}=9^8=43046721=1 \pmod{16}$。

定理 1-12 （费马定理）设 a 为整数，n 是素数，如果 gcd（a，n）$=1$，则有：

$$a^{n-1} \equiv 1 \bmod n$$

证明：因为 n 是素数，所以欧拉函数 $\varphi(n)=n-1$，再根据定理 1-11 即可证明。

【例 1-21】设 $n=7$，$2^6=64=1 \pmod 7$，$3^6=729=1 \pmod 7$，$4^6=4096=1 \pmod 7$，$5^6=15625=1 \pmod 7$，$6^6=46656=1 \pmod 7$。

定理 1-13 （威尔逊定理）p 是素数$\Leftrightarrow$ $(p-1)! \equiv -1 \bmod p$。

证明：已知 $(p-1)! \equiv -1 \bmod p$，若 p 不是素数，不妨设 $p=ab$，$1<a<p$，$1<b<p$，显然：

$$a \mid (p-1)!$$

因为 $(p-1)! \equiv -1 \bmod p$，所以：

$$p \mid (p-1)!+1 \Rightarrow a \mid (p-1)!+1 \Rightarrow a \mid 1$$

产生矛盾，故 p 必为素数。

反过来，如果 p 是素数，当 p 取 2、3 时，容易验证 $(p-1)! \equiv -1 \bmod p$，命题成立；当 $p>3$ 时，考虑集合 $S=\{2, 3, \cdots, p-2\}$ 中的任意元素 a，因为（a，p）$=1$，有整数 k_1 和 k_2 使得：

$$k_1 a + k_2 p = 1$$

$$k_1 a \equiv 1 \pmod p$$

于是，存在 b 是 a 的逆元，$1<b<p-1$，使得 $b \equiv k_1 \pmod p$。

接下来证明 $b \neq a$：

如果 $b=a$，则 $a^2 \equiv 1 \pmod p$，a 要么等于 1，要么等于 $p-1$，都与 $a \in S$ 产生矛盾，