第3章 密码学数学基础

在现代密码体制中，构建、分析和攻击这些密码体制都需要用到数学理论，包括数论、有限域、群论等，其中数论是应用最广泛的数学理论。

3.1 素数

3.1.1 整除

定义 3-1 设有整数 a 和 b，且 $b\neq 0$。如果存在整数 m，使 $a=mb$，那么就说，a 能被 b 整除，记为 $b|a$，称 b 为 a 的除数。

如 $3|15$；$-15|60$，具有以下性质：

(1) 如果 $a|1$，则 $a=\pm 1$；

(2) 如果 $a|b$ 且 $b|a$，则 $a=\pm b$；

(3) 对任一非 0 整数 b，$b|0$，$b|b$，$1b$ 均成立；

(4) 如果 $a|b$ 且 $b|c$，则 $a|c$ 成立；

证明：设 $b=k_1\times a \quad c=k_2\times b$，则 $c=k_1\times k_2\times a$。

(5) 如果 $b|g$ 且 $b|h$，则对任意整数 m,n 有 $b|(mg+nh)$。

证明：设 $g=b\times g_1 \quad h=b\times h_1$

则 $mg+nh=mg_1b+nh_1b=(mg_1+nh_1)b$

即 $b|(mg+nh)$

3.1.2 素数

定义 3-2 如果正整数 $P>1$ 只能被 1 和它本身整除，则该数为素数(也叫质数)。

100 以内的素数有 25 个，分别是 2、3、5、7、11、13、17、19、23、29、31、37、41、43、47、53、59、61、67、71、73、79、83、89 和 97。

1000 以内的素数如表 3-1 所示。

表 3-1 1000 以内的素数

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	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		

定理 3-1 任何大于 1 的整数 a 都可以分解成素数幂之积，且唯一。

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots\cdots \times p_t^{a_t} \tag{3-1}$$

其中，$p_1 < p_2 < \cdots\cdots < p_t$ 为素数，a_i 为正整数。

例如：$77 = 7^1 \times 11^1$，$504 = 2^3 \times 3^2 \times 7$。

式(3-1)也可以表示为

$$a = \prod_p p^{a_p} (a_p \geqslant 0)。$$

即数 a 是所有素数的乘积。当然，大多的 a_p 都为 0。这样表述的优点在于，两个数的乘法等于对应素数指数的加法。

例如：$6 = 2 \times 3$，$18 = 2 \times 3^2$，则 $6 \times 18 = 2^2 \times 3^3$。

对于 $a|b$，它们的素数因子关系为

$$a|b \rightarrow a_p < b_p (\text{对每一项的素数都如此})$$

素数在密码学中具有重要的作用，尤其是在非对称密码体制中，经常用到很大的素数。

2008 年 9 月，德国人发现的素数为 1300 万位的整数，用 5 号铅字将其印刷，它的长度将达到 30 英里。

3.1.3 最大公约数

定义 3-3 a 和 b 的最大公约数是能够同时整除 a 和 b 的最大正整数，记为

$$\gcd(a,b)。$$

例如：$\gcd(6,4) = 2$；$\gcd(3,7) = 1$。

如果 $\gcd(a,b) = 1$，那么就说 a 和 b 是互素的。

下面分析如何求解两个数的最大公约数。

(1) 对于不是很大的数，利用素数来求解。

例如：$1728=2^6\times3^3$　　$135=3^3\times5$，则 $\gcd(1728,135)=3^3=27$。

(2) 对于很大的数，将其分解为素数乘积的形式比较困难，可以用欧几里得算法求解。

$$\gcd(a,b)=\gcd(b,a \bmod b) \tag{3-2}$$

例如：$\gcd(12\,345,1111)=\gcd(1111,124)=\gcd(124,5)=\gcd(5,4)=\gcd(4,1)=\gcd(1,0)$

到最后的 $a \bmod b=0$ 为止，则最后的 b 为所求，所以 12 345 与 1111 的最大公约数为 1，即它们是互素的。

3.2 模运算

定义 3-4　设整数 a、b 及 $n\neq0$，若 $a-b=kn$（k 为任一整数），则称 a 在 mod n 下与 b 同余，记为 $a\equiv b \bmod n$。

例如：$11 \bmod 7=4$；$4 \bmod 7=4$；则 $11\equiv4 \bmod 7$。

模运算有以下性质：

(1) $a\equiv a \bmod n$。

(2) 若 $a\equiv b \bmod n$，则 $b\equiv a \bmod n$。

(3) 若 $a\equiv b \bmod n$ 且 $b\equiv c \bmod n$，则 $a\equiv c \bmod n$。

(4) 若 $a\equiv b \bmod n$ 且 $c\equiv d \bmod n$，则 $a+c\equiv(b+d) \bmod n$，$a-c\equiv(b-d) \bmod n$，$ac\equiv(bd) \bmod n$。

(5) $(a+b) \bmod n=((a \bmod n)+(b \bmod n)) \bmod n$，

$(a-b) \bmod n=((a \bmod n)-(b \bmod n)) \bmod n$，

$(a\times b) \bmod n=((a \bmod n)\times(b \bmod n)) \bmod n$。

(6) 若 $ac\equiv(bd) \bmod n$，$c\equiv d \bmod n$ 且 $\gcd(c,n)=1$，则 $a\equiv b \bmod n$。

(7) 若 $\gcd(a,n)=1$，则存在唯一整数 b，$0<b<n$ 且 $\gcd(b,n)=1$，使得 $ab\equiv1 \bmod n$。此时 a 称为 b 在 mod n 下的反元素；b 称为 a 在 mod n 下的反元素。

(8) 若 $ax\equiv1 \bmod n$ 有解，则 $\gcd(a,n)=1$。

例 3-1　计算 $11^7 \bmod 13$。

解：利用 $(a\times b) \bmod n=((a \bmod n)\times(b \bmod n)) \bmod n$，得

$$\begin{aligned}11^7 \bmod 13&=(11\times11^2\times11^4) \bmod 13\\&=(11\times4\times3) \bmod 13\\&=132 \bmod 13\\&=2\end{aligned}$$

例 3-2　证明 $5^{60}-1$ 是 56 的倍数。

该问题等价于 $5^{60} \bmod 56=1$。

证明：$5^3 \bmod 56=13$

$5^6 \bmod 56=13^2 \bmod 56=1$

$5^{60} \bmod 56=1^{10} \bmod 56=1$

即 $5^{60}-1$ 是 56 的倍数。

3.3 模逆元

在密码学中，经常用到模逆元。

定义 3-5 模逆元是指寻找一个最小正整数 x，使 $ax\equiv 1 \bmod n$，这里 a 和 n 皆为正整数，且 a 与 n 互素，x 称为 a 的模 n 逆元，记为 $x=a^{-1} \bmod n$。

如果 a 与 n 不互素，那么不存在 x，使 $ax\equiv 1 \bmod n$。

模逆元的计算可以通过扩展欧几里得算法实现。

扩展欧几里得算法可以描述为

(1) $(X_1,X_2,X_3)\leftarrow(1,0,n)$；$(Y_1,Y_2,Y_3)\leftarrow(0,1,a)$。

(2) 如果 $Y_3=0$，返回 $X_3=\gcd(a,n)$；无逆元。

(3) 如果 $Y_3=1$，返回 $Y_3=\gcd(a,n)$；$Y_2=a^{-1} \bmod n$。

(4) $Q=\lfloor X_3/Y_3 \rfloor$(即除数，并往下取整)。

(5) $(T_1,T_2,T_3)\leftarrow(X_1-QY_1,X_2-QY_2,X_3-QY_3)$。

(6) $(X_1,X_2,X_3)\leftarrow(Y_1,Y_2,Y_3)$。

(7) $(Y_1,Y_2,Y_3)\leftarrow(T_1,T_2,T_3)$。

(8) 返回第(2)步。

如果有逆元，Y_2 为逆元，$Y_3=\gcd(a,n)$ 是 a 和 n 的最大公约数。

例 3-3 用扩展欧几里得算法求 $\gcd(7,26)$ 和 $7^{-1} \bmod 26$。

解：

Q	X_1	X_2	X_3	Y_1	Y_2	Y_3
	1	0	26	0	1	7
3	0	1	7	1	−3	5
1	1	−3	5	−1	4	2
2	−1	4	2	3	−11	1

所以 $\gcd(7,26)=1$，$7^{-1} \bmod 26=-11 \bmod 26=15$。

3.4 费马欧拉定理

3.4.1 费马定理

定理 3-2(费马定理 1) 如果 p 是素数，且 p 不能被 a 整除，那么 $a^{p-1}\equiv 1 \bmod p$。例如：$a=5$，$p=11$

$$a^{p-1} \bmod p = 5^{10} \bmod 11 = (5^3\times 5^3\times 5^3\times 5) \bmod 11$$
$$= (64\times 5)\bmod 11 = 45 \bmod 11 = 1$$

定理 3-3(费马定理 2)　如果 p 是素数，a 是正整数，且 $\gcd(a,p)=1$，那么 $a^p \equiv a \bmod p$。例如：$a=2, p=5$

$$a^p \bmod p = 2^5 \bmod 5 = 32 \bmod 5 = 2$$

3.4.2　欧拉定理

定义 3-6　当 $m>1$ 时，欧拉函数 $\varphi(m)$ 表示比 m 小，且与 m 互素的正整数的个数。

例如：$m=12$，比 12 小且与 12 互素的正整数为 1、5、7、11，所以

$$\varphi(12) = 4$$

欧拉函数具有以下性质：

(1) 当 m 是素数时，$\varphi(m)=m-1$，即比 m 小的所有正整数，如 $\varphi(11)=10$。

(2) 当 $m=pq$，且 p、q($p\neq q$)均为素数时，$\varphi(m)=\varphi(p)\varphi(q)=(p-1)(q-1)$。

证明：$m=pq$，比 m 小的正整数的集合 $Z=\{1、2、\cdots\cdots、pq-1\}$。

在集合 Z 中，与 m 不互素的数为 p 的倍数和 q 的倍数。

p 的倍数的集合为$\{p、2p、\cdots\cdots、(q-1)p\}$，共$(q-1)$个数。

q 的倍数的集合为$\{q、2q、\cdots\cdots、(p-1)q\}$，共$(p-1)$个数。

所以，$\varphi(m)=(pq-1)-(q-1)-(p-1)=(p-1)\times(q-1)=\varphi(p)\varphi(q)$。

例如：$m=15=3\times5$，$\varphi(m)=2\times4=8$

比 15 小且与 15 互素的正整数为 1、2、4、7、8、11、13、14，所以 $\varphi(15)=8$。

(3) 当 $m=p^2$，且 p 为素数时，$\varphi(m)=p(p-1)$。

证明：$m=p^2$，比 m 小的正整数的集合 $Z=\{1、2、\cdots\cdots、p^2-1\}$。

在集合 Z 中，与 m 不互素的数为 p 的倍数。

p 的倍数的集合为$\{p、2p、\cdots\cdots、(p-1)p\}$，共$(p-1)$个数，

所以，$\varphi(m)=(p^2-1)-(p-1)=p(p-1)$。

例如：$m=9=3^2$，$\varphi(m)=3\times2=6$

比 9 小且与 9 互素的正整数为 1、2、4、5、7、8，所以 $\varphi(9)=6$。

当计算一个数的欧拉函数 $\varphi(m)$时，可以采用以下两个公式进行计算。

(1) 若一个数 m 可以写成 $m=p_1^{e_1}\times p_2^{e_2}\times\cdots\cdots\times p_t^{e_t}$($p_i$ 为素数)，则

$$\varphi(m) = \prod_{i=1}^{t} p_i^{e_i-1}(p_i-1) \tag{3-3}$$

例如：$m=120=2^3\times3\times5$

$\varphi(m)=2^2\times(2-1)\times(3-1)\times(5-1)=32$

(2) 对任一正整数 m，若其可写成 $p_1^{e_1}\times p_2^{e_2}\times\cdots\cdots\times p_t^{e_t}$，则

$$\varphi(m) = m\times\prod_{p_i}\left(1-\frac{1}{p_i}\right) \tag{3-4}$$

例如：$m=120$

$$\varphi(m)=120\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=32$$

定理 3-4(欧拉定理)　对于任何互素的两个整数 a 和 n，有 $a^{\varphi(n)}\equiv1 \bmod n$。

欧拉定理具有以下性质：

(1) 当 n 为素数时，欧拉定理相当于费马定理；

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

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

例如：$a=7, n=10, \varphi(10)=4, 7^4 \bmod 10=1$。

例 3-4 求 7^{803} 的后三位数字。

解：原题等价于 $7^{803} \bmod 1000$。

$1000=2^3\times5^3$，所以 $\varphi(1000)=1000\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=400$

由于 7 与 1000 互素，根据欧拉定理得

$$7^{\varphi(1000)} \bmod 1000 = 1$$

$$7^{400} \bmod 1000 = 1$$

所以 $7^{803} \bmod 1000=(7^3\times7^{400}\times7^{400}) \bmod 1000=343$，即 7^{803} 的后三位数字为 343。

3.4.3 本原元

定义 3-7 对于任何互素的两个整数 a 和 n，在方程 $a^m=1 \bmod n$ 中，至少有一个正整数 m 满足这一方程(因为 $\varphi(n)$ 是其中的一个解)，那么，最小的正整数解 m 为模 n 下 a 的阶。如果 a 的阶 $m=\varphi(n)$，称 a 为 n 的本原元。

例如：$a=7$, $n=10, \varphi(10)=4$

在方程 $7^m=1 \bmod 10$ 中，$7^1=7 \bmod 10, 7^2=9 \bmod 10, 7^3=3 \bmod 10, 7^4=1 \bmod 10$，而 $\varphi(10)=4$，所以 7 为 10 的本原元。

例如：$a=7$, $n=19, \varphi(19)=18$

在方程 $7^m=1 \bmod 19$ 中，$7^1=7 \bmod 19, 7^2=11 \bmod 19, 7^3=1 \bmod 19$，而 $\varphi(19)=18$，所以 7 不是 19 的本原元。

这里需要注意两点：

(1) 一个数的本原元不唯一；

(2) 有些数没有本原元。

例如：$a=2$, $n=19, \varphi(19)=18$

经过计算 2 是 19 的本原元。同理，3、10、13、14、15 都是 19 的本原元。

例如：$a=3, n=8, \varphi(8)=4$

经过计算 3 不是 8 的本原元。同理 5 和 7 也不是 8 的本原元，所以 8 没有本原元。

概括地说，只有 2、4、p^a、$2p^a$ 有本原元，其中 a 为正整数，p 为奇素数。

3.5 中国余数定理

孙子算经：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？

其含义其实是求正整数解 x 满足：

$$\begin{cases} x = 2 \bmod 3 \\ x = 3 \bmod 5 \\ x = 2 \bmod 7 \end{cases}$$

定理 3-5　令 $n_1,n_2,\cdots,n_t$ 为两两互质的正整数，$N=\prod_{i=1}^{t} n_i$，则 $x=a_1 \bmod n_1=a_2 \bmod n_2=\cdots=a_t \bmod n_t$ 在$[0,N-1]$中有唯一解，称为中国余数定理。

下面来分析如何求中国余数定理的解。

令 $N_i=\dfrac{N}{n_i}$，则 $x=\sum_{i=1}^{t} N_i \times y_i \times a_i \bmod N$，其中

$N_i \times y_i=1(\bmod n_i)$，亦即 $y_i=N_i^{-1} \bmod n_i$。

孙子算经之例子解法如下：

$$N=3\times5\times7=105$$

$$N_1=5\times7=35, N_2=3\times7=21, N_3=3\times5=15$$

$$35\times y_1=1 \bmod 3 \Rightarrow y_1=2$$

$$21\times y_2=1 \bmod 5 \Rightarrow y_2=1$$

$$15\times y_3=1 \bmod 7 \Rightarrow y_3=1$$

所以，$x=35\times2\times2+21\times1\times3+15\times1\times2=23 \bmod 105$。

中国余数定理的计算可以总结为

给定 a_1,a_2,n_1,n_2 且 $n_1<n_2$，$\gcd(n_1,n_2)=1$，求 x，使得 $0\leqslant x<n_1\cdot n_2$ 并满足 $x=a_1 \bmod n_1=a_2 \bmod n_2$。

解法如下：

首先，求出 u 满足 $u\cdot n_2=1 \bmod n_1$。

(1) 若 $a_1\geqslant(a_2 \bmod n_2)$，则

$$x=(((a_1-(a_2 \bmod n_1))\cdot u) \bmod n_1)\cdot n_2+a_2$$

(2) 若 $a_1<(a_2 \bmod n_2)$，则

$$x=(((a_1+n_1-(a_2 \bmod n_1))\cdot u) \bmod n_1)\cdot n_2+a_2$$

在非对称密码算法 RSA 中，利用中国余数定理可以使得解密速度约为原来的四倍。应用中国余数定理可解决安全广播系统、密钥确认、存取控制等问题。

3.6　单向函数与单向暗门函数

一个单向函数 $f:X\to Y$，应满足下列条件：

(1) 对任一 $x\in Y$，可以很容易算出 $y=f(x)$。

(2) 给定任一 $y\in Y$，算出 x 满足 $y=f(x)$在计算上不可行。

一个单向暗门函数 $f:X\to Y$，应满足下列条件：

(1) 对任一 $x\in X$，可以很容易算出 $y=f(x)$。

(2) 给定任一 $y\in Y$，算出 $x=f^{-1}(y)$在计算上不可行；若知道某一个额外的秘密参数(称为暗门)，则可以很容易算出 $x=f^{-1}(y)$。

单向函数的应用如将某一个秘密值转换成一个公开值，而任何人无法从公开值中求得该秘密值。例如，将密钥转换成一个公开值存放于一个公开目录中，握有真正密钥的人可以将其密钥先经过单向函数转换后，再与存放于公开目录的公开值加以比对，而达到验证身分

的目的。

单向暗门函数的应用如将某一个秘密值转换成一个公开值后，借由暗门可以将该公开值反解成原来的秘密值。例如，加解密运算的暗门为密钥。

例如，在多项式中，令 $y=f(x)=(a_0+a_1x+\cdots+a_{n-1}x^{n-1}+x^n) \bmod p$。若给定 a_0，a_1，…，a_n、p 和 x，很容易算出 $y=f(x)$。但若给定 a_0，a_1，…，a_n、p 和 y，欲求出 $f(x)$的根 x，则至少需要 $n^2(\log_2 p)^2$ 个乘法。当 n 与 p 很大时，求出 $f(x)$的根 x 是相当困难的。

再如，在离散对数中，令 p 为质数且 $p-1$ 含有一个大质因子 q。给定一整数 g、$1<g<p-1$ 与 x，计算 $y=g^x \bmod p$ 最多仅需 $\lfloor \log_2 x \rfloor + w(x)-1$ 个乘法，其中 $w(x)$表示二进制表示法 x 内 1 的个数。反之，给定一整数 g 与 y，求出 x 满足 $y=g^x \bmod p$ 需要 $\exp\{(\ln p \ln(\ln p))^{1/2}\}$次运算。

习题

1. 一个数的本原根是什么？
2. 对两个连续的整数 n 和 $n+1$，为什么 $\gcd(n,n+1)=1$？
3. 利用 Fermat 定理计算 $3^{201} \bmod 11$。
4. 找出 25 的所有本原根。
5. 用扩展欧几里得算法求 $\gcd(7,31)$和 $7^{-1} \bmod 31$。
6. 利用中国剩余定理求解下式。

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 5 \\ x \equiv 1 \bmod 7 \end{cases}$$