信息安全数学基础

教师

孙达志 刘健

课程资源

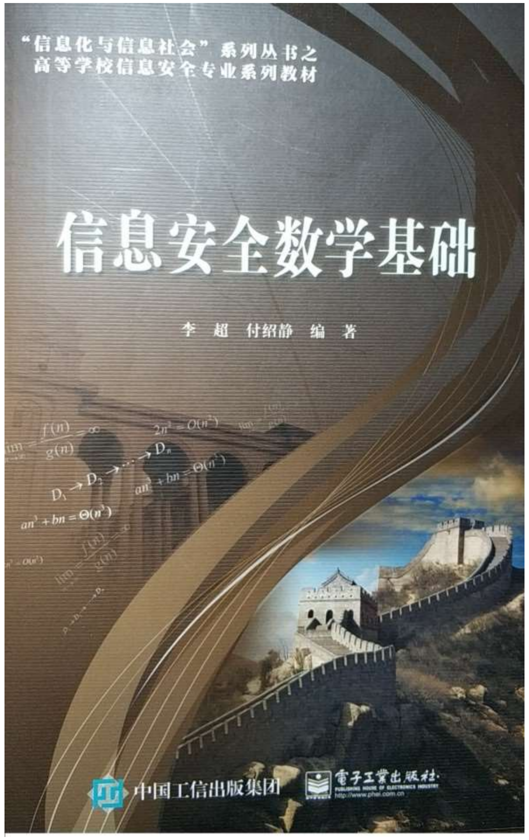
智慧树、　微信群

教师联系方式

孙达志 sundazhi@tju.edu.cn/13652199735(微信)

参考书

李超，付绍静　编著，　信息安全数学基础，电子工业出版社，2015年11月



第一讲 初等数论

1

数论是研究整数的科学，是数学的重要分支。实践表明，数论在信息安全中有很多应用。特别是，在密码学中，大多数公钥密码算法都是以数论为理论基础设计的。数论中又以同余理论在密码学中应用的最为广泛。

本讲提要

- 整数的基本概念

1 整除性

定义1 对于整数$a \neq 0$，b。我们说a整除b，如果存在一个整数k使得$b=ka$，我们把a叫做b的因数，b叫做a的倍数，记为$a|b$。如果这个k不存在，我们说a不整除b，记为$a\nmid b$。

性质1 (1) 对于任意$a \neq 0, a|0$，$a|a$，对于任意$b, 1|b$。

(2) 如果$a|b$，$b|c$，则$a|c$。

(3) 如果$a|b$，$a|c$，则$a|(sb+tc)$，这里s和t是任意整数。

性质1证明. (1) 显而易见。

(2) 由定义存在k和l，满足$b=ka$，$c=lb$，所以有$c=kla$。

(3) 由定义可写出$b=k_1a$，$c=k_2a$，所以$sb+tc=(sk_1+tk_2)a$

即$a|sb+tc$。

1 整除性(续)

定理1 设a，b是两个整数，其中$b>0$，则存在两个唯一的整数q及r，使得

$$a=bq+r，0\le r<b$$

成立。

1 整除性(续)

定理1证明.

做序列：

$\ldots,-3b,-2b,-b,0,b,2b,3b,\ldots$。

a必在序列某两项之间，即存在某个整数q，有

$qb \le a < (q+1)b$。

令$r = a - qb$，除余式成立。

1 整除性(续)

定理1证明.（续）

如果还存在另一对整数$q_1, 0 \le r_1 < b$即有

$q_1 b + r_1 = a = qb + r$。

于是$b(q_1 - q) = r - r_1$，故$b\,|\,q_1 - q\,| = |\,r - r_1\,|$。

而$|\,r - r_1\,| < b$。

$\therefore\ r = r_1, q = q_1$。

2 最大公约数

定义2 设a_1，$a_2,\cdots$，a_n是n个不全为零的整数。若整数d是它们之中每一个的因数，那么d就叫a_1，$a_2,\cdots$，a_n的一个公因数。整数a_1，$a_2,\cdots$，a_n的公因数中最大的一个叫最大公约数，记作$(a_1,a_2,\cdots,a_n)$，若$(a_1,a_2,\cdots,a_n)=1$，就说a_1，$a_2,\cdots$，a_n互素。

定理2 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$(a,b)=(b,c)$。

2 最大公约数(续)

定理2证明.

$$\left.\begin{aligned} (a,b) &\mid a \\ (a,b) &\mid b \\ c = a &- bq \end{aligned}\right\} \Rightarrow (a,b) \mid c \Rightarrow (a,b) \le (b,c)$$

同理$(b,c) \le (a,b)$，于是$(a,b) = (b,c)$。

2 最大公约数(续)

Euclidean算法的表述

不失一般性假定任意 $a>0$，$b>0$有

$$a=bq_1+r_1, 0<r_1<b$$
$$b=r_1q_2+r_2, 0<r_2<r_1$$
$$r_1=r_2q_3+r_3, 0<r_3<r_2$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}, 0<r_{n-1}<r_{n-2}$$
$$r_{n-2}=r_{n-1}q_n+r_n, 0<r_n<r_{n-1}$$
$$r_{n-1}=r_nq_{n+1}+r_{n+1}，\quad r_{n+1}=0。$$

定理3 任意$a>0$，$b>0$，则(a,b)就是上述过程中最后一个不等于零的余数， 即$(a,b)=r_n$。

2 最大公约数(续)

定理3证明.

根据定理2, $(r_n, r_{n+1}) = (r_n, 0) = r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (b, r_1) = (a, b)$。

2 最大公约数(续)

定理4 若任给整数$a>0$，$b>0$，则存在两个整数m，n使得

$$(a,b)=ma+nb。$$

定理4证明.

$r_n=r_{n-2}-r_{n-1}q_n$，$r_{n-1}=r_{n-3}-r_{n-2}q_{n-1}$

$\Rightarrow r_n=r_{n-2}(1+q_nq_{n-1})-r_{n-3}q_n,\ldots$，$r_n=ma+nb=(a,b)$。

推论1 a和b的公因子是(a,b)的因数。

2 最大公约数(续)

例子1 计算$(1180, 482)$。

$$1180 = 2 \cdot 482 + 216$$

$$482 = 2 \cdot 216 + 50$$

$$216 = 4 \cdot 50 + 16$$

$$50 = 3 \cdot 16 + 2$$

$$16 = 2 \cdot 8 + 0$$。

因此,$(1180, 482) = 2$。

可以看到余数都经历了：余数 $\to$ 除数 $\to$ 被除数 $\to$ 忽略的过程。

2 最大公约数(续)

根据定理3,我们还可以得到递推公 式:

$x_1 = 1$, $x_2 = -q_2$, $x_j = -q_j x_{j-1} + x_{j-2}$,

$y_1 = -q_1$, $y_2 = 1 + q_1 q_2$, $y_j = -q_j y_{j-1} + y_{j-2}$,

其中$2 < j \le n$。

则$ax_n + by_n = (a,b)$。

因此, $x_1 = 1$, $x_2 = -2$, $x_3 = -4x_2 + x_1 = 9$,

$x_4 = -3x_3 + x_2 = -29$。

同样有$y_4 = 71$, 所以$1180 \cdot (-29) + 482 \cdot 71$

$= 2 = (1180, 482)$。

这一过程被称为扩展 Euclidean 算法。

2 最大公约数(续)

递推公式推导.

$a = bq_1 + r_1 \Rightarrow r_1 = a - bq_1 \Rightarrow x_1 = 1$，$y_1 = -q_1$

$b = r_1 q_2 + r_2 \Rightarrow r_2 = b - r_1 q_2 = b - (a - bq_1)q_2 = -q_2 a + b(q_1 q_2 + 1)$

$\Rightarrow x_2 = -q_2$，$y_2 = 1 + q_1 q_2$。

考虑

$$\left.\begin{aligned} r_{j-2} &= ax_{j-2} + by_{j-2} \\ r_{j-1} &= ax_{j-1} + by_{j-1} \\ r_{j-2} = r_{j-1}q_j + r_j &\Rightarrow r_j = r_{j-2} - r_{j-1}q_j \end{aligned}\right\} \Rightarrow$$

$r_j = a(-q_j x_{j-1} + x_{j-2}) + b(-q_j y_{j-1} + y_{j-2})$。

2 最大公约数(续)

定理5 若$a\mid bc,(a,b)=1$，则$a\mid c$。

定理5证明.

根据定理4，有$ma+nb=1$。$\therefore\ mac+nbc=c$。

设$n>2$，$a_1>0$，$a_2>0,\cdots$，$a_n>0,(a_1,a_2)=d_2$，
$(d_2,a_3)=d_3,\cdots,(d_{n-2},a_{n-1})=d_{n-1},(d_{n-1},a_n)=d_n$，
那么有下面的定理。

定理6 若a_1，$a_2,\cdots$，$a_n(n>2)$是n个正整数，则

$$(a_1,a_2,\cdots,a_n)=d_n。$$

2 最大公约数(续)

定理6证明.

$d_n \mid d_{n-1}$，$d_n \mid a_n$，而$d_{n-1} \mid d_{n-2}$，$d_{n-1} \mid a_{n-1}$，

$\therefore\ d_n \mid d_{n-2}$，$d_n \mid a_{n-1}$。

依次类推得$d_n \mid a_n$，$d_n \mid a_{n-1}$,...，$d_n \mid a_2$，$d_n \mid a_1$。

令$(a_1, a_2, \cdots, a_n) = d$。

$\therefore\ d_n \le d$。

$d \mid d_2$，$d \mid d_3$,$\cdots$，$d \mid d_n$，

$\therefore\ d \le d_n$。

$\therefore\ d_n = (a_1, a_2, \cdots, a_n)$。

2 最大公约数(续)

定理7 若a_1，$a_2,\cdots$，$a_n(n>2)$是n个正整数，则存在整数x_1，$x_2,\cdots$，x_n使得

$$a_1x_1+a_2x_2\cdots+a_nx_n=(a_1,a_2,\cdots,a_n)。$$

定理7证明.

根据定理4结合定理6，有

$$\begin{aligned}
d_n &= z_n d_{n-1} + y_n a_n,\\
d_{n-1} &= z_{n-1} d_{n-2} + y_{n-1} a_{n-1},\\
&\vdots\\
d_3 &= z_3 d_2 + y_3 a_3,\\
d_2 &= z_2 a_1 + y_2 a_2,
\end{aligned}$$

依次代换d_{n-1},...，d_3，d_2可得结论。

3 最小公倍数

定义3 设a_1，$a_2,\cdots$，a_n是$n(\geq 2)$个不为0的整数。若m是这n个数中每一个的倍数，那么m就叫这n个数的一个公倍数。在a_1，$a_2,\cdots$，a_n的一切公倍数中最小的正整数叫做最小公倍数，记作$[a_1,a_2,\cdots,a_n]$。

定理8 设a，b是任意的两个正整数，则

(1) a，b的所有公倍数就是$[a,b]$的所有倍数。

(2) $[a,b]=\dfrac{ab}{(a,b)}$。

3 最小公倍数(续)

定理8证明.

令m为a,b的任意公倍数，则 $m = ak = bk'$，令$a = a_1(a,b)$，$b = b_1(a,b)$。代入$ak = bk'$，得$a_1 k = b_1 k'$，

$\because (a_1, b_1) = 1, \therefore b_1 \mid k \Rightarrow k = b_1 t$。

$\therefore m = ak = ab_1 t = a\dfrac{b}{(a,b)}t$，这里 t满足$k = b_1 t$。

反之，观察上式 t为任意整数时，$\dfrac{ab}{(a,b)}t$都为a,b的一个公倍数。

$\therefore$ 上式可表示 a,b的一切公倍数。

显然，$t = 1$为最小，即$[a,b] = \dfrac{ab}{(a,b)}$。因此，定理中 (1),(2) 同时得证。

3 最小公倍数(续)

设$n>2$，$a_1>0$，$a_2>0,\cdots$，$a_n>0,[a_1,a_2]=m_2$,
$[m_2,a_3]=m_3,\cdots,[m_{n-2},a_{n-1}]=m_{n-1},[m_{n-1},a_n]=m_n$,
那么有下面的定理。

定理9 若$a_1,a_2,\cdots,a_n$是$n(n>2)$个正整数，则

$$[a_1,a_2,\cdots,a_n]=m_n。$$

3 最小公倍数(续)

定理9证明.

令$[a_1,a_2,\cdots,a_n]=m$。由于$[m_{n-1},a_n]=m_n$,知$m_{n-1}\mid m_n$，$a_n\mid m_n$;

由于$[m_{n-2},a_{n-1}]=m_{n-1}$，知$m_{n-2}\mid m_{n-1}$，$a_{n-1}\mid m_{n-1}$。

$\therefore$ $a_{n-1}\mid m_n$，$m_{n-2}\mid m_n$。

依次类推可以得到 $a_1\mid m_n$,...，$a_{n-2}\mid m_n$，$a_{n-1}\mid m_n$。

$\therefore$ 知$m_n\geq m$。

又由$[a_1,a_2]=m_2$，$a_1\mid m$，$a_2\mid m$，由定理 8可知$m_2\mid m$。结合

$[m_2,a_3]=m_3$，$a_3\mid m$，可知$m_3\mid m$。

依次类推可以得到 $m_n\mid m$，即$m\geq m_n$。

$\therefore$ $m=m_n$。

4 素数

定义 4 一个大于1的正整数，如果它的正 因数只有1和它本身，就叫做素数，否则就叫 做合数。

性质2 设a是任一大于1的整数，则a的除1以外的最小正因数q是素数，并且当a是合数时，

$$q \le \sqrt{a}。$$

性质2证明.

（反证法）q不是素数，则其还有因 子$1 < q_1 < q$，由于$q_1 \mid q$，$q|a, \therefore q_1 \mid a$，这与$q$是最小因子矛盾。故$q$是素数。

a是合数，则$a = a_1 q$，且$q \le a_1$，故$a \ge q^2 \Rightarrow q \le \sqrt{a}$。

4 素数(续)

定理10 素数的个数是无穷的。

定理10证明.

如果素数的个数是有限的，可令$p_1=2$，$p_2=3,\cdots$，p_k是全体素数。再令$p=p_1p_2\cdots p_k+1$，知其必为合数，而p不可为p_1，$p_2,\cdots$，p_k之中任意一个整除，必然存在其它素数，因此，与素数的个数是有限的假设矛盾。

定理11 存在无穷多个形如$4n-1$的素数。

定理11证明.

（反证法）假定p是最大$4n-1$型素数，令

$N=2^2\cdot3\cdot5\cdot7\cdots p-1$，其中$3\cdot5\cdot7\cdots p$表示所有$\le p$的奇素数之积。

$\because N$为$4n-1$型，$\therefore N$为合数。$\because N$的素因数大于p，而两个$4n+1$型之积还是$4n+1$型，$\therefore$必有一个大于p的$4n-1$型素因子因数。

4 素数(续)

定理12 对于任意给定整数 x_0，不存在整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0(a_n\neq 0,n>0)$，使得$x$取所有 $\geq x_0$的整数时，$f(x)$都表示素数。

定理12证明.

设$f(x_0)=p$为一素数，对正整数 y，有

$f(x_0+py)-f(x_0)=pM \Rightarrow f(x_0+py)=p(M+1)$。

而至多只有n个y使得

$f(x_0+py)=p$。

$\therefore$当y充分大时，$f(x_0+py)$不总是一个素数。

4 素数(续)

200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

定理13 (素数数量定理) 如果$\pi(x)$表示小于x的所有素数，则有

$\pi(x) \approx \dfrac{x}{\ln x}$，也就是说当$x \to \infty$时，比率$\pi(x)/(x/\ln x) \to 1$。

在各种密码应用中经常要求使用300位左右的十进制素数,

通过定理13我们可以估计

$$\pi(10^{300}) - \pi(10^{299}) \approx \frac{10^{300}}{\ln 10^{300}} - \frac{10^{299}}{\ln 10^{299}} \approx 1.3 \times 10^{297},$$

因此，足够使用。

谢谢！