信息安全数学基础

教材：谢敏编著《信息安全数学基础》

西安电子科技大学出版社

内容

- 数论基础
  - 数的整除性质
  - 同余理论
  - 二次剩余
  - 原根与指数
- 代数学基础
  - 群
  - 环
  - 域
  - 有限域

第一章 整 除

初等数论的研究对象主要是整数集合z和正整数集合N^+。

整除理论和同余理论是初等数论的两大支柱，其中整除理论是初等数论的基础，是对涉及除法运算的整数的算术内容作抽象的、系统的总结，它的主要结果是唯一分解定理（也称算术基本定理）和最大公约数理论；同余理论是初等数论的堂奥，它包含了初等数论所特有的思想和手法。

1.1 整数的除法

我们知道在整数集Z中可以进行加法“$+$”和乘法“$\cdot$”运算，这两种运算具备下述特性：

加法“$+$”满足

(1) 交换律：对任意$a,b\in Z$，有$a+b=b+a$；

(2) 结合律：对任意$a,b,c\in Z$，有$(a+b)+c=a+(b+c)$；

(3) 存在零元“0”，对任意$a\in Z$，有$a+0=a$（或$0+a=a$）；

(4) 对任意$a\in Z$，存在负元“$-a$”，使得$a+(-a)=0$（或$(-a)+a=0$）；

依据(1)~(4)，借助并非十分简单的推理，我们还可以知道，

(5) 零元是唯一的；

(6) 负元是唯一的；

(7) 加法满足消去律：若$a,b,c\in Z$且$a+b=a+c$，则$b=c$。

乘法“$\cdot$”满足

(i) 交换律：对任意$a,b\in Z$，有$a\cdot b=b\cdot a$；

(ii) 结合律：对任意$a,b,c\in Z$，有$(a\cdot b)\cdot c=a\cdot(b\cdot c)$；

(iii) 存在单位元“1”，对任意$a\in Z$，有$a\cdot 1=a$（或$1\cdot a=a$）；

(iv) 非零元可消去：若$a,b,c\in Z$，$a\neq 0$，$a\cdot b=a\cdot c$，则$b=c$；

依据(i)~(iii)我们知道乘法还满足

(v) 单位元 1 唯一。

乘法“$\cdot$”对于加法“$+$”还满足分配律

左分配律：对任意$a,b,c\in Z$，有$a\cdot(b+c)=(a\cdot b)+(a\cdot c)$；

或右分配律：对任意$a,b,c\in Z$，有$(b+c)\cdot a=(b\cdot a)+(c\cdot a)$。

为了方便，我们常将乘法$a\cdot b$简记为ab。

注意到整数集对于除法运算是不封闭的，即设$a,b\in Z$，$b\neq 0$，则$\frac{a}{b}$不一定是整数，也就是说不一定存在整数c，使得$a=bc$。由此就产生出初等数论中第一个基本概念：整除。

定义 1.1.1(整除) 设$a,b\in Z$，$b\neq 0$，如果存在整数c使得$a=bc$，则称b整除a（或称a能被b整除），记为$b\mid a$。这时称b是a的一个因数（也称约数、因子），而a为b的倍数。

如果不存在整数c使得$a=bc$，则称b不整除a，记为$b\nmid a$。

例 1 $2\mid 8,\ -3\mid 9,\ 6\nmid 8$。

易见：(1) 对每一整数n，都有$\pm 1\mid n$；

(2) 对于每一非零整数n，都有$n\mid 0,\ \pm n\mid \pm n$。

由整除的定义及乘法“·”的性质，我们可以推出整除有如下性质：

定理 1.1.1 (1) $a\mid b\Leftrightarrow -a\mid b\Leftrightarrow a\mid -b\Leftrightarrow -a\mid -b\Leftrightarrow \mid a\mid\mid b\mid$；

(2) $b\neq 0$且$a\mid b\Rightarrow \mid a\mid\leq\mid b\mid$；

(3) $a\mid b$且$b\mid c\Rightarrow a\mid c$；

(4) $a\mid b$且$b\mid a\Rightarrow b=\pm a$；

(5) $a\mid b$且$a\mid c\Leftrightarrow$对任意$t,s\in Z$有$a\mid tb+sc$；

(6) 设$m\neq 0$，$a\mid b\Leftrightarrow ma\mid mb$。

定理 1.1.1 (1) $a|b \Leftrightarrow -a|b \Leftrightarrow a|-b \Leftrightarrow -a|-b \Leftrightarrow |a||b|$；

(2) $b \neq 0$ 且 $a|b \Rightarrow |a| \leq |b|$；每一位非零整数的因子只有有限多个

整除具有传递性 (3) $a|b$ 且 $b|c \Rightarrow a|c$；

(4) $a|b$ 且 $b|a \Rightarrow b = \pm a$；

(5) $a|b$ 且 $a|c \Leftrightarrow$ 对任意 $t,s \in Z$ 有 $a|tb+sc$；将整除和线性组合联系起来

(6) 设 $m \neq 0$，$a|b \Leftrightarrow ma|mb$。

例 2 设 n 为整数，求证：若 $3|n$ 且 $4|n$，则 $12|n$。

例 3 设 m 为奇数，$n \in Z$，求证：若 $m|2n$，则 $m|n$。

定义 1.1.2 设 $x \in R$，我们以$[x]$表示不超过 x 的最大整数，称作实数 x 的整数部分；而 $x-[x]$称作实数 x 的小数部分，记为$\{x\}$。

由定义 1.1.2 易知 $x=[x]+\{x\}$，$0 \le \{x\} < 1$。

容易证明：(1) $x \in Z \Leftrightarrow x=[x] \Leftrightarrow \{x\}=0$；

(2) 若 $n \in Z$，则 $\forall x \in R$ 有 $\left[x+n\right]=\left[x\right]+n$。

例 4 $[3.14]=?$，$\{3.14\}=?$；$[-0.6]=?$，$\{-0.6\}=?$。

解： $[3.14]=3$，$\{3.14\}=0.14$；$[-0.6]=-1$，$\{-0.6\}=0.4$。

下面给出整数的一个基本性质------初等数论证明中最重要、最基本、最直接的工具！

定理 1.1.2（带余除法）设a,b是两个给定的整数，$b>0$，则存在唯一决定的一对整数q和r，使得

$$a=qb+r，\ 0\le r<b。$$

注意定理 1.1.2 中要求除数$b>0$，但是很容易推广为$b\neq 0$，因为当除数$b<0$时，我们总可以将之化为除数大于零的情况，事实上此时$\frac{a}{b}=\frac{-a}{-b}$，而$-b>0$。

定理 1.1.2 设 a,b 是两个给定的整数，$b>0$，则存在唯一决定的一对整数 q 和 r，使得 $a=qb+r$，$0\le r<b$。

证明：（存在性）先证满足条件的 q 和 r 是存在的。

（唯一性）再证 q 和 r 是唯一决定的。

最大公约数和最小公倍数

定义 1.1.3 设 a,b 是两个不全为零的整数， a 和 b 的最大公约数是指满足下述条件的整数 d ：

(1) d 为 a 和 b 的公约数，即 $d \mid a$ 且 $d \mid b$；

(2) d 为 a 和 b 的所有公约数中最大的，即对整数 c ，如果 $c \mid a$ 且 $c \mid b$ ，则 $c \le d$ 。

记为 (a,b) ，有时也记为 $\gcd(a,b)$ (gcd 即 the greatest common divisor)。

由定义知 $(a,b)=\max\{d : d \mid a \text{ 且 } d \mid b\}$。

将最大公约数的定义推广，我们可用 $(a_1,a_2,\cdots,a_n)$ 表示不全为零的有限个整数 $a_1,a_2,\cdots,a_n$ 的最大公约数 ：

$$(a_1,\cdots,a_n)=\max\left\{d : \forall 1 \le i \le n, i \in N, d \mid a_i\right\}。$$

定义 1.1.4 当 $(a,b)=1$ 时，我们称 a 和 b 互素（既约），即 a 和 b 只有公约数 ± 1。

定义 1.1.5 设a,b是两个均不为零的整数，a和b的最小公倍数是指满足下述条件的整数m：

(1) m为正整数，且m为a和b的公倍数，即$m>0$，且$a\mid m$，$b\mid m$;

(2) m为a和b的所有正公倍数中最小者，即对整数c，如果$c>0$，且$a\mid c, b\mid c$，则$m\le c$。

记为$[a,b]$，有时也记为$\mathrm{lcm}(a,b)$(lcm 即 the least common multiple)。

由定义知$[a,b]=\min\{m: a\mid m \text{且} b\mid m, m>0\}$。

将最小公倍数的定义推广，我们可用$[a_1,a_2,\cdots,a_n]$表示均不为零的有限个整数$a_1,a_2,\cdots,a_n$的最小公倍数：

$$[a_1,\cdots,a_n]=\min\{m:\forall 1\le i\le n, i\in N, a_i\mid m, m>0\}。$$

下面给出关于最大公约数、最小公倍数的一些有用的性质。

定理 1.1.3 (1) $(a,b)=(b,a)=(-a,b)=(a,-b)=(-a,-b)$，

$[a,b]=[b,a]=[-a,b]=[a,-b]=[-a,-b]$；

(2) 若$a\mid b$，则$(a,b)=\mid a\mid$，$[a,b]=\mid b\mid$；

(3) 对任意整数x，有$(a,b)=(a,b+ax)$；

(4) 对任意整数$d\mid a$，有$[a,b]=[a,b,d]$。

证明：利用最大公约数、最小公倍数的定义和整除的性质（定理 1.1.1（5））。

定理 1.1.4 (1) $a\mid c, b\mid c \Leftrightarrow [a,b]\mid c$；　（公倍数一定是最小公倍数的倍数）

(2) $d\mid a, d\mid b \Leftrightarrow d\mid (a,b)$。　（公约数一定是最大公约数的约数）

证明：(1) ($\Leftarrow$)显然。

($\Rightarrow$)利用带余除法（定理 1.1.2）和最小公倍数的定义。

(2) ($\Leftarrow$)显然。

($\Rightarrow$)设 $d_1, d_2, \cdots, d_n$ 为 a 和 b 的全体公约数，$L=[d_1, d_2, \cdots, d_n]$。

由最大公约数的定义说明 $L=(a,b)$。

推论 1.1.4 $(a,b,c)=((a,b),c)$，$[a,b,c]=[[a,b],c]$。

定理 1.1.5 (1) 设 m 为正整数，则 $m(a,b)=(ma,mb)$，$m[a,b]=[ma,mb]$；

(2) 若 $(m,a)=1$，则 $(m,ab)=(m,b)$；

(3) 若 $(m,a)=1$，$m\mid ab$，则 $m\mid b$；

(4) 若 $(a,b)=d$，则 $(\frac{a}{d},\frac{b}{d})=1$；

(5) $[a,b]=\frac{|ab|}{(a,b)}$。

设m为正整数，则$m(a,b)=(ma,mb)$，$m[a,b]=[ma,mb]$；

证明：(1) 设$D=(a,b),D'=(ma,mb)$。利用最大公约数的定义证明$D'=mD$

类似可证$m[a,b]=[ma,mb]$。

若$(m,a)=1$，则$(m,ab)=(m,b)$；

(2) 只考虑$mb\neq 0$的情形，此时利用$(m,a)=1$，推论 1.1.4，定理 1.1.3(2)以及定理 1.1.5(1)

若$(m,a)=1$，$m\mid ab$，则$m\mid b$；

(3) 利用定理 1.1.3 和(2)。

若$(a,b)=d$，则$(\frac{a}{d},\frac{b}{d})=1$；

(4) 考虑$(a,b)=(d\cdot\frac{a}{d},d\cdot\frac{b}{d})$

$[a,b]=\frac{|ab|}{(a,b)}$。

(5) 先考虑$(a,b)=1$的情形，再利用（1）证明$(a,b)\neq 1$的情形。

以上结论均从定义出发来证明，这种方法、技巧在整除理论中十分基础、重要。

下面我们从线性组合的角度来考查最大公约数。

定理 1.1.6 设a,b为不全为零的整数，则

$$(a,b)=\min\{s:s=ax+by,x,y\in Z,s>0\}。$$

证明： 令$S=\{s:s=ax+by,x,y\in Z\}$。考虑S中最小的正整数s_0，证明$s_0=(a,b)$。

推论 1.1.6 设$a,b\in Z$且不全为 0，$S=\{s:s=ax+by,x,y\in Z\}$，则S由a,b最大公约数的所有倍数构成。

定理 1.1.6 给出了最大公约数的一个明确表达式，使得我们在证明它们的性质时有了另外一种推导方法。定理 1.1.5 由定义出发给出的证明可以利用该表达式重新给出更为简明的证明。

例 5 求证：$m(a,b)=(ma,mb)$。

借助上述的结论我们还可以探讨二元一次不定方程$ax+by=c(a,b,c\in Z)$的整数解并获得下述定理。

1.2 算术基本定理 （唯一分解定理）

定义 1.2.1 设 p 为大于 1 的正整数，如果 p 除 1 和它自身外没有其它正因子，则称 p 为素数（或质数，不可约数）；否则称为合数。

定理 1.2.1 设 p 是素数，$a_1, a_2, \cdots, a_n$ 为整数，其中 $n \geq 2, n \in Z$，如果 $p \mid \prod_{k=1}^{n} a_k$，则必

$$\exists i, 1 \leq i \leq n，使得 \ p \mid a_i。$$

证明：利用数学归纳法来证明。

定理 1.2.2（算术基本定理） 设整数$n>1$，那么必有$n=\prod_{i=1}^{m} p_i$，其中$p_i(1\le i\le m)$为素数；若不计素因子的次序，这个分解式是唯一的。

证明：先证明分解式的存在性。利用数学归纳法。

再证分解式的唯一性。

将分解式 $n = p_1 p_2 \cdots p_m$ 中相同的素数进行合并，即得

$$n = \prod_{i=1}^{s} p_i^{e_i},$$

其中 $e_i (1 \le i \le s)$ 均为正整数， $p_1, \cdots, p_s$ 为两两不同的素数。

上式称为 n 的标准算术分解式。

例 1 $32 = 2 \times 2 \times 2 \times 2 \times 2$

$180 = 2 \times 2 \times 3 \times 3 \times 5$

定理 1.2.3 设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$，其中 $p_1, \cdots, p_s$ 是不同的素数，α_i, β_i 是非负整数，则

(1) $ab = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}$，其中 $\gamma_i = \alpha_i + \beta_i, (1 \le i \le s)$；

(2) $a \mid b \Leftrightarrow \alpha_i \le \beta_i \quad (1 \le i \le s)$；

(3) $(a,b) = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$，其中 $\forall 1 \le i \le s, e_i = \min\{\alpha_i, \beta_i\}$；

(4) $[a,b] = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$，其中 $\forall 1 \le i \le s, d_i = \max\{\alpha_i, \beta_i\}$；

(5) $(a,b)[a,b] = ab$。

例 2 求解$(45,100)$和$[45,100]$

1.3 素数

由上节内容可以看到，素数的研究也是一个重要课题。关于素数的问题有很多，例如素数的多少，素数的分布及素性判断等，这些问题的研究对于密码学的发展也起到了重要作用。在这里我们仅介绍一些重要结论，更多内容请查阅相关文献。

关于“素数是否有无穷多个”这个问题，早在公元前3世纪，Euclid就给出了肯定的回答：

定理 1.3.1 素数有无穷多个。

证明：利用反证法。考虑 

令$\pi(x)$表示不超过x的素数的个数（其中x为任意正实数）。下面两个定理给出了素数分布的一些性质，说明素数在正整数中的分布是稀疏的。

定理 1.3.2 $\lim\limits_{x\to+\infty}\dfrac{\pi(x)}{x}=0$。

定理 1.3.3（素数定理） $\lim\limits_{x\to+\infty}\dfrac{\pi(x)}{\dfrac{x}{\ln x}}=1$。

密码学中经常要用到一些大素数，这就涉及到素性判断的问题，或者寻找素数的问题，这里我们介绍一种较为古老的寻找素数的方法——Eratosthenes 筛法。在以后的章节中，我们将会陆续介绍几种利用数论知识而设计的素性检验方法。

定理 1.3.4 设整数$n \geq 2$，若n是合数，则必有素数$p \mid n$，$p \leq \sqrt{n}$。

定理 1.3.4 给出了一个寻找素数的有效方法。

例 1 求出不超过 100 的所有素数。

	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

	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~~

下面我们来介绍密码学中常用的，具有特殊形式的几种素数。

定义 1.3.1 形如$F_n = 2^{2^n} + 1$的整数称为 Fermat 数；形如$F_n = 2^{2^n} + 1$的素数称为 Fermat 素数。

定义 1.3.2 p 为素数，形如 $M_p = 2^p - 1$ 的素数称为 Mersenne 素数。

1644 年，法国数学家 M. Mersenne 研究这类素数，成果较为显著，故而后来人们称这类素数为 Mersenne 素数。

到 2005 年为止，人们共发现了 42 个 Mersenne 素数，它们对应于素数 $p = 2,3,5,7,\cdots,25964951$。其中目前知道的最大 Mersenne 素数 $M_{25964951}$ 是由一名德国数学爱好者发现的，它是一个 7816230 位的数。

定义 1.3.3 除以 4 余 3 的素数称为 Blum 素数，两个 Blum 素数的乘积称为 Blum 整数。

1.4 Euclid算法（辗转相除法）

定理 1.4.1（Euclid 算法） 设$a_0, a_1 \in Z, a_1 > 0$，按下述方式反复作带余除法，有限步后必可除尽，

由定理 1.4.1 叙述中倒数第二式可得 $a_{n-2}=q_{n-2}a_{n-1}+a_n$

$$a_n=(a_0,a_1)=a_{n-2}-q_{n-2}a_{n-1},$$

即a_0,a_1的最大公约数可以表示为a_{n-1}和a_{n-2}的整系数线性组合。

同理，由定理 1.3.1 叙述中倒数第三式可将a_{n-1}表为a_{n-2}和a_{n-3}的整系数线性组合，将之代入

$$a_n=(a_0,a_1)=a_{n-2}-q_{n-2}a_{n-1}=a_{n-2}-q_{n-2}(a_{n-3}-q_{n-3}a_{n-2}),$$

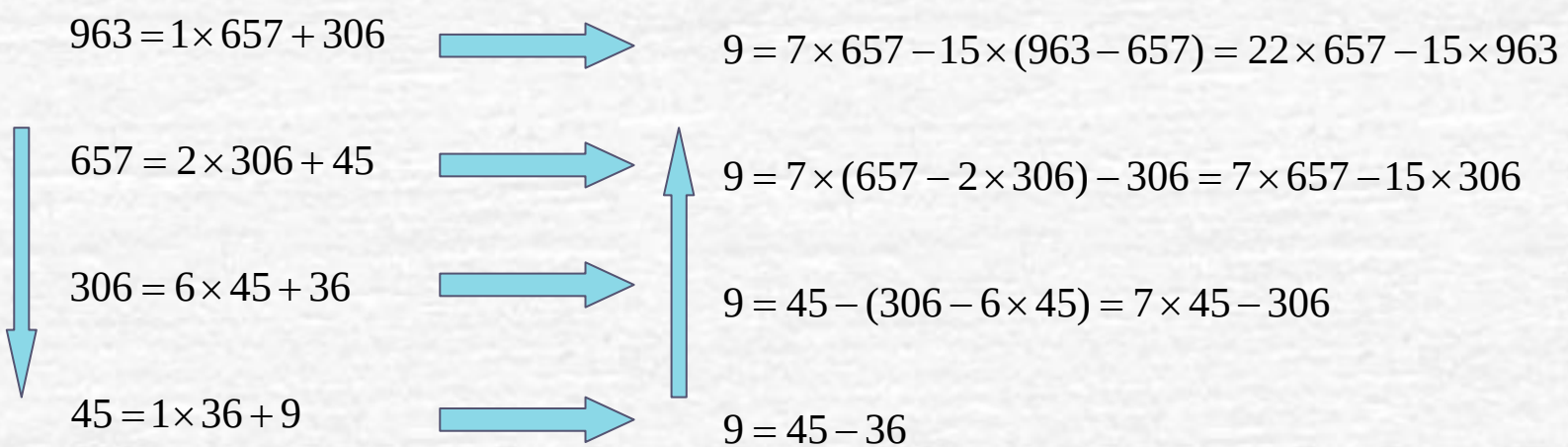
即可得a_n由a_{n-2}和a_{n-3}的线性表出。

利用定理 1.4.1 叙述中倒数第四式，又可得a_n由a_{n-3}和a_{n-4}的线性表出，依次下去，最后就可以得到a_n表为a_0,a_1的整系数线性组合。

辗转相除法不但可以导出“$\exists x_0,y_0\in Z$,使得$(a,b)=ax_0+by_0$”这一重要的结论，而且蕴涵了线性表出系数x_0,y_0的具体求法。

例 1：求 963，657 的最大公约数，并把它表示为 963，657 的整系数线性组合。

解：利用辗转相除法可得：



$36 = 4 \times 9$

即 $(963, 657) = 9 = 22 \times 657 + (-15) \times 963$，换一个角度来看，

$$x = -15, y = 22$$

就是二元一次不定方程 $963x + 657y = 9$ 的一组解。

Euclid 算法的计算机实现可描述如下，

输入：整数 $a > b \geq 0$

输出：a 和 b 的最大公约数(a, b)

1. $X \leftarrow a$;　$Y \leftarrow b$;
2. while($Y \neq 0$) do

   (i) R=X mod Y;
   (ii) X=Y;
   (iii) Y=R;
3. return X=(a, b)。

算法输入要求 $a > b \geq 0$，是出于表达方便的目的，具体实现时，可利用性质 $(a,b) = (|a|,|b|)$ 来具体调整输入。

在本书中称上述的实现为原始的 Euclid 算法

推广的 Euclid 算法的描述如下：

输入：整数 $a > b \geq 0$

输出：a 和 b 的最大公约数(a, b)，及整数 x_0, y_0 使得 $ax_0 + by_0 = (a,b)$

1. $(X_1, X_2, X_3) \leftarrow (1,0,a)$；$(Y_1, Y_2, Y_3) \leftarrow (0,1,b)$；　　(*初始化)

2. while($Y_3 \neq 0$) do

   (i) $Q = \left\lfloor \frac{X_3}{Y_3} \right\rfloor$；

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

   (iii) $(X_1, X_2, X_3) \leftarrow (Y_1, Y_2, Y_3)$；

   (iv) $(Y_1, Y_2, Y_3) \leftarrow (T_1, T_2, T_3)$；

3. return $X_3 = (a, b)$；$X_1 = x_0$；$X_2 = y_0$。

利用数学归纳法可以证明算法中的变量满足以下关系：

$$aT_1 + bT_2 = T_3;\ aX_1 + bX_2 = X_3;\ aY_1 + bY_2 = Y_3。$$

这一关系正是保证算法输出满足条件的关键所在。

例 2 利用推广的 Euclid 算法来求解例 1 中的问题。

解：我们用下表给出推广的 Euclid 算法的一系列结果：

循环次数	Q	X_1	X_2	X_3	Y_1	Y_2	Y_3
初值		1	0	963	0	1	657
1	1	0	1	657	1	−1	306
2	2	1	−1	306	−2	3	45
3	6	−2	3	45	13	−19	36
4	1	13	−19	36	−15	22	9
5	4	−15	22	9	73	−107	0

所以 $(963,657)=9=936\times(-15)+657\times 22$ 。