文章编号：2096-1618(2020)02-0244-04

多个正整数的最大公因数与最小公倍数的几个计算关系

肖 瑞，杨 昊，周云秀，廖群英
(四川师范大学数学科学学院，四川 成都 610066)

摘要：熟知对任意正整数 a,b,c，有 $[a,b]=\frac{ab}{(a,b)}$，$[(a,c),(b,c)]=([a,b],c)$，其中 $[\ ],(\ )$ 分别表示最小公倍数和最大公因数. 在RSA公钥算法中涉及两个正整数的最小公倍数和最大公因数的相关计算. 为了给传统的RSA算法提供可能的优化方案，利用初等的方法与技巧，对任意多个正整数的最大公因数和最小公倍数的计算关系做了相关探究，推广了上述结果，给出了任意多个正整数的最大公因数和最小公倍数之间的3种计算关系.

关 键 词：最大公因数；最小公倍数；基础数学；编码密码学理论
中图分类号：O156.1 **文献标志码**：A
doi：10.16836/j.cnki.jcuit.2020.02.017

0 引言

为方便，对任意正整数 $n\geq 2,a_1,\cdots,a_n\in \mathbf{Z}^*$，记 $(a_1,a_2,\cdots,a_n)$ 为 $a_1,a_2,\cdots,a_n$ 的最大公因数，$[a_1,a_2,\cdots,a_n]$ 为 $a_1,a_2,\cdots,a_n$ 的最小公倍数.

熟知，最大公因数和最小公倍数是初等数论中两个非常重要的概念，两个概念之间是对偶关系[1]. 其在信息安全的多方保密计算问题中有重要作用，且在保护隐私的数据挖掘中也有广泛的应用[2]. 在RSA公钥系统中，安全依赖于因数分解的困难性，加密过程中以及概率性素数产生方法的判定中涉及两个正整数的最大公因数的相关计算[3].

另一方面，对 $\forall a,b\in \mathbf{N}^*$，有 $[a,b]=\frac{ab}{(a,b)}$[4]. 这个等式揭示了两个正整数的最大公因数和最小公倍数之间的一种特殊关系.

引理[4] (i) $\forall a,b\in \mathbf{N}^*$，有 $[a,b]=\frac{ab}{(a,b)}$. 特别地，若 $(a,b)=1$，则 $[a,b]=ab$.

(ii) 对 $\forall a_1,a_2,a_3\in \mathbf{N}^*$，有 $[(a_1,a_3),(a_2,a_3)]=([a_1,a_2],a_3)$.

(iii) 设 $\lambda\in \mathbf{Z}^*,a_1,a_2,\cdots,a_n\in \mathbf{Z}^*$，则 $\lambda(a_1,a_2,\cdots,a_n)=(\lambda a_1,\lambda a_2,\cdots,\lambda a_n)$.

引理的(ii)给出了3个正整数的最大公因数和最小公倍数的计算关系，那么 $n(n\geq 3)$ 个正整数时，二者存在什么样的关系呢？利用初等的方法和技巧，本文解决了此问题，并证明了如下主要结果.

定理1 设 $m,n\in \mathbf{Z}^*,a_1,a_2,\cdots,a_m,b_1,b_2,\cdots,b_n\in \mathbf{Z}^*$，则

$$(a_1,\cdots,a_m)(b_1,\cdots,b_n)=(a_1b_1,\cdots,a_1b_n,a_2b_1,\cdots,a_2b_n,\cdots,a_mb_1,\cdots,a_mb_n).$$

定理2 设 $n\in \mathbf{Z}^*$ 且 $n\geq 2,a_1,a_2,\cdots,a_n\in \mathbf{Z}^*$，则

(i) $\prod_{i=1}^{n}a_i=(a_1,a_2,\cdots,a_n)\left[\frac{\prod_{i=1}^{n}a_i}{a_1},\frac{\prod_{i=1}^{n}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{n}a_i}{a_n}\right]$；

(ii) $\prod_{i=1}^{n}a_i=[a_1,a_2,\cdots,a_n]\left(\frac{\prod_{i=1}^{n}a_i}{a_1},\frac{\prod_{i=1}^{n}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{n}a_i}{a_n}\right)$；

(iii) $[(a_1,a_n),(a_2,a_n),\cdots,(a_{n-1},a_n)]=([a_1,\cdots,a_{n-1}],a_n)$.

1 主要结果的证明

1.1 定理1的证明

设 $m,n\in \mathbf{Z}^*,a_1,a_2,\cdots,a_m,b_1,b_2,\cdots,b_n\in \mathbf{Z}^*$，令 $(b_1,\cdots,b_n)=B$，则由引理的(iii)得

$$(a_1,\cdots,a_m)(b_1,\cdots,b_n)=(a_1,\cdots,a_m)B=(a_1B,\cdots,a_mB).$$

又对任意 $i=1,\cdots,m$，有 $a_iB=a_i(b_1,\cdots,b_n)$. 故由引理的(iii)可得

$$a_iB=a_i(b_1,\cdots,b_n)=(a_ib_1,\cdots,a_ib_n),$$

故 $(a_1,\cdots,a_m)(b_1,\cdots,b_n)=(a_1b_1,\cdots,a_1b_n,a_2b_1,\cdots,a_2b_n,\cdots,a_mb_1,\cdots,a_mb_n)$.

这就完成了定理1的证明.

1.2 定理2的证明

1.2.1 定理2(i)的证明

设 $n\in \mathbf{Z}^*,a_1,a_2,\cdots,a_n\in \mathbf{Z}^*$，对 n 作归纳证明. 当

收稿日期：2019-11-03
基金项目：四川省科技厅科研重点资助项目(2016JY0134)

$n=2$ 时,即为引理的(i). 现设 $n=k(k\geq 2)$ 时结论成立,即

$$\prod_{i=1}^{k}a_i=(a_1,a_2,\cdots,a_k)\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right] \tag{1}$$

则 $n=k+1$ 时,令 $(a_1,a_2,\cdots,a_k)=C(C\in\mathbf{Z}^*)$,由引理的(i)得

$$[C,a_{k+1}]=\frac{a_{k+1}C}{(C,a_{k+1})}=\frac{(a_1,a_2,\cdots,a_k)a_{k+1}}{((a_1,a_2,\cdots,a_k),a_{k+1})} \tag{2}$$

由式(1)得

$$[C,a_{k+1}]=\left[\frac{\prod_{i=1}^{k}a_i}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right]},a_{k+1}\right] \tag{3}$$

又由 $\dfrac{\prod_{i=1}^{k}a_i}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right]}=C$ 可知 $\left[\dfrac{\prod_{i=1}^{k}a_i}{a_1},\cdots,\dfrac{\prod_{i=1}^{k}a_i}{a_k}\right]$ 为 $\prod_{i=1}^{k}a_i$ 的因子,且 $\left[\dfrac{\prod_{i=1}^{k}a_i}{a_1},\cdots,\dfrac{\prod_{i=1}^{k}a_i}{a_k}\right]$ 也为 $\left[\dfrac{\prod_{i=1}^{k}a_i}{a_1},\dfrac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\dfrac{\prod_{i=1}^{k}a_i}{a_k}\right]a_{k+1}$ 的因子,故式(3)等价于

$$\frac{\left[\prod_{i=1}^{k}a_i,\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right]a_{k+1}\right]}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right]}=\frac{\left[\frac{\prod_{i=1}^{k+1}a_i}{a_1},\frac{\prod_{i=1}^{k+1}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k+1}a_i}{a_k},\frac{\prod_{i=1}^{k+1}a_i}{a_{k+1}}\right]}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right]}.$$

由式(1)得

$$\frac{(a_1,\cdots,a_k)a_{k+1}}{((a_1,\cdots,a_k),a_{k+1})}=\frac{\prod_{i=1}^{k+1}a_i}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right](a_1,\cdots,a_k,a_{k+1})}.$$

则式(2)等价于 $\dfrac{\left[\frac{\prod_{i=1}^{k+1}a_i}{a_1},\frac{\prod_{i=1}^{k+1}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k+1}a_i}{a_k},\frac{\prod_{i=1}^{k+1}a_i}{a_{k+1}}\right]}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right]}=\dfrac{\prod_{i=1}^{k+1}a_i}{\left[\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right](a_1,a_2,\cdots,a_k,a_{k+1})}$. 整理得

$$\prod_{i=1}^{k+1}a_i=(a_1,a_2,\cdots,a_{k+1})\left[\frac{\prod_{i=1}^{k+1}a_i}{a_1},\frac{\prod_{i=1}^{k+1}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k+1}a_i}{a_k}\right].$$

这就完成了定理 2 的(i)的证明.

1.2.2　定理 2(ii)的证明

设 $n\in\mathbf{Z}^*,a_1,a_2,\cdots,a_n\in\mathbf{Z}^*$. $n=2$ 时,即为引理的(i). 假设当 $n=k,(k\geq 2)$ 时结论成立,即

$$\prod_{i=1}^{k}a_i=[a_1,a_2,\cdots,a_k]\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right) \tag{4}$$

则当 $n=k+1$ 时,若令 $[a_1,a_2,\cdots,a_k]=C'(C'\in\mathbf{Z}^*)$,由引理的(i)得

$$(C',a_{k+1})=\frac{a_{k+1}C'}{[C',a_{k+1}]}=\frac{[a_1,a_2,\cdots,a_k]a_{k+1}}{[[a_1,a_2,\cdots,a_k],a_{k+1}]} \tag{5}$$

由式(4)得

$$(C',a_{k+1})=\left(\frac{\prod_{i=1}^{k}a_i}{\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)},a_{k+1}\right) \tag{6}$$

由 $\dfrac{\prod_{i=1}^{k}a_i}{\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)}=C'$ 知 $\left(\dfrac{\prod_{i=1}^{k}a_i}{a_1},\cdots,\dfrac{\prod_{i=1}^{k}a_i}{a_k}\right)$ 为 $\prod_{i=1}^{k}a_i$ 的因子,且 $\left(\dfrac{\prod_{i=1}^{k}a_i}{a_1},\cdots,\dfrac{\prod_{i=1}^{k}a_i}{a_k}\right)$ 也为 $\left(\dfrac{\prod_{i=1}^{k}a_i}{a_1},\dfrac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\dfrac{\prod_{i=1}^{k}a_i}{a_k}\right)a_{k+1}$ 的因子,故式(6)等价于

$$\frac{\left(\prod_{i=1}^{k}a_i,\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)a_{k+1}\right)}{\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)}=\frac{\left(\prod_{i=1}^{k}a_i,\frac{\prod_{i=1}^{k+1}a_i}{a_1},\frac{\prod_{i=1}^{k+1}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k+1}a_i}{a_k}\right)}{\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)}.$$

由式(4)得 $\dfrac{[a_1,a_2,\cdots,a_k]a_{k+1}}{[[a_1,a_2,\cdots,a_k],a_{k+1}]}=\dfrac{\prod_{i=1}^{k+1}a_i}{[a_1,\cdots,a_k,a_{k+1}]\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)}$. 则式(5)等价于

$$\frac{\left(\frac{\prod_{i=1}^{k+1}a_i}{a_k},\left(\frac{\prod_{i=1}^{k+1}a_i}{a_1},\frac{\prod_{i=1}^{k+1}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k+1}a_i}{a_k}\right)\right)}{\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_{k-1}}\right)}=\frac{\prod_{i=1}^{k+1}a_i}{[a_1,\cdots,a_{k+1}]\left(\frac{\prod_{i=1}^{k}a_i}{a_1},\frac{\prod_{i=1}^{k}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}\right)}.$$

整理得

$$\prod_{i=1}^{k+1}a_i=[a_1,a_2,\cdots,a_k,a_{k+1}]\left(\frac{\prod_{i=1}^{k+1}a_i}{a_1},\frac{\prod_{i=1}^{k+1}a_i}{a_2},\cdots,\frac{\prod_{i=1}^{k+1}a_i}{a_{k+1}}\right).$$

这就完成了定理 2(ii)的证明.

1.2.3　定理 2(iii)的证明

设 $n\in\mathbf{Z}^*,a_1,a_2,\cdots,a_n\in\mathbf{Z}^*$. 当 $n=3$ 时,即为引理的(ii). 假设 $n=k,(k\geq 3)$ 时结论成立,即

$$[(a_1,a_k),(a_2,a_k),\cdots,(a_{k-1},a_k)]=([a_1,\cdots,a_{k-2},a_{k-1}],a_k) \tag{7}$$

当 $n=k+1$ 时,由式(7)得

$$[(a_1,a_{k+1}),(a_2,a_{k+1}),\cdots,(a_k,a_{k+1})]=[([a_1,a_2,\cdots,a_{k-1}],a_{k+1}),(a_k,a_{k+1})] \tag{8}$$

再由定理 2 的(ii)得

$$[([a_1,\cdots,a_{k-1}],a_{k+1}),(a_k,a_{k+1})]=\left[\left(\frac{\prod_{i=1}^{k-1}a_i}{\left(\prod_{i=1}^{k-1}a_i/a_1,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)},a_{k+1}\right),(a_k,a_{k+1})\right]$$

$$=\left[\left(\frac{\left(\prod_{i=1}^{k-1}a_i,\left(\prod_{i=1}^{k-1}a_i/a_1,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)a_{k+1}\right)}{\left(\prod_{i=1}^{k-1}a_i/a_1,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)},(a_k,a_{k+1})\right)\right] \tag{9}$$

若令 $\left(\frac{\left(\prod_{i=1}^{k-1}a_i,\left(\prod_{i=1}^{k-1}a_i/a_1,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)a_{k+1}\right)}{\left(\prod_{i=1}^{k-1}a_i/a_1,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)}\right)=D$, 则由引理的(i)得

$$[D,(a_k,a_{k+1})]=\frac{D(a_k,a_{k+1})}{(D,(a_k,a_{k+1}))}=\frac{D(a_k,a_{k+1})}{(D,a_k,a_{k+1})}$$

$$=\frac{\left(\prod_{i=1}^{k-1}a_i,\frac{\prod_{i=1}^{k-1}a_ia_{k+1}}{a_1},\cdots,\frac{\prod_{i=1}^{k-1}a_ia_{k+1}}{a_{k-1}}\right)(a_k,a_{k+1})}{\left(\prod_{i=1}^{k-1}a_i,\left(\prod_{i=1}^{k-1}a_i/a_1,\prod_{i=1}^{k-1}a_i/a_2,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)(a_{k+1},a_k)\right)} \tag{10}$$

令 $\left(\prod_{i=1}^{k-1}a_i/a_1,\prod_{i=1}^{k-1}a_i/a_2,\cdots,\prod_{i=1}^{k-1}a_i/a_{k-1}\right)=A,\prod_{i=1}^{k-1}a_i=X$, 则

$$\frac{\left(\prod_{i=1}^{k-1}a_i,\frac{\prod_{i=1}^{k-1}a_ia_{k+1}}{a_1},\cdots,\frac{\prod_{i=1}^{k-1}a_ia_{k+1}}{a_{k-1}}\right)(a_k,a_{k+1})}{\left(\prod_{i=1}^{k-1}a_i,\left(\frac{\prod_{i=1}^{k-1}a_i}{a_1}a_{k+1},\cdots,\frac{\prod_{i=1}^{k-1}a_i}{a_{k-1}}\right)(a_{k+1},a_k)\right)}=\frac{(X,Aa_{k+1})(a_k,a_{k+1})}{(X,A(a_{k+1},a_k))}=\frac{(Xa_k,Xa_{k+1},Aa_ka_{k+1},Aa_{k+1}^2)}{(X,Aa_k,Aa_{k+1})} \tag{11}$$

再考虑式(7)的右边,当 $n=k+1$ 时,由定理 2 的(ii)得

$$([a_1,\cdots,a_{k-1},a_k],a_{k+1})=\left(\frac{\prod_{i=1}^{k}a_i}{\left(\prod_{i=1}^{k}a_i/a_1,\prod_{i=1}^{k}a_i/a_2,\cdots,\prod_{i=1}^{k}a_i/a_k\right)},a_{k+1}\right)=$$

$$\frac{\left(\prod_{i=1}^{k}a_i,\frac{\prod_{i=1}^{k}a_i}{a_1}a_{k+1},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}a_{k+1}\right)}{\left(\prod_{i=1}^{k}a_i/a_1,\prod_{i=1}^{k}a_i/a_2,\cdots,\prod_{i=1}^{k}a_i/a_k\right)},$$

即

$$\frac{\left(\prod_{i=1}^{k}a_i,\frac{\prod_{i=1}^{k}a_i}{a_1}a_{k+1},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_{k-1}}a_{k+1},\frac{\prod_{i=1}^{k}a_i}{a_k}a_{k+1}\right)}{\left(\prod_{i=1}^{k}a_i/a_1,\prod_{i=1}^{k}a_i/a_2,\cdots,\prod_{i=1}^{k}a_i/a_{k-1},\prod_{i=1}^{k}a_i/a_k\right)}=\frac{(Xa_k,Aa_ka_{k+1},Xa_{k+1})}{(X,Aa_k)} \tag{12}$$

要证明式(11)与式(12)相等,则将分子与分母交叉乘积,即

$$(Xa_k,Xa_{k+1},Aa_ka_{k+1},Aa_{k+1}^2)(X,Aa_k)=(X^2a_k,X^2a_{k+1},AXa_ka_{k+1},AXa_{k+1}^2,XAa_k^2,XAa_ka_{k+1},A^2a_k^2a_{k+1},A^2a_{k+1}^2a_k),$$

以及

$$(Xa_k,Aa_ka_{k+1},Xa_{k+1})(X,Aa_k,Aa_{k+1})=(X^2a_k,XAa_k^2,AXa_ka_{k+1},A^2a_{k+1}^2a_k,AXa_ka_{k+1},A^2a_k^2a_{k+1},X^2a_{k+1},AXa_{k+1}^2).$$

故

$$(Xa_k,Xa_{k+1},Aa_ka_{k+1},Aa_{k+1}^2)(X,Aa_k)=(Xa_k,Aa_ka_{k+1},Xa_{k+1})(X,Aa_k,Aa_{k+1}),$$

等式两边同时除以$(X,Aa_k)(X,Aa_k,Aa_{k+1})$,即得

$$\frac{(Xa_k,Aa_ka_{k+1},Xa_{k+1})}{(X,Aa_k)}=\frac{(Xa_k,Xa_{k+1},Aa_ka_{k+1},Aa_{k+1}^2)}{(X,Aa_k,Aa_{k+1})} \tag{13}$$

于是由式(8)~(13)式可得

$$\frac{\left(\prod_{i=1}^{k}a_i,\frac{\prod_{i=1}^{k}a_i}{a_1}a_{k+1},\cdots,\frac{\prod_{i=1}^{k}a_i}{a_k}a_{k+1}\right)}{\left(\prod_{i=1}^{k}a_i/a_1,\prod_{i=1}^{k}a_i/a_2,\cdots,\prod_{i=1}^{k}a_i/a_{k-1},\prod_{i=1}^{k}a_i/a_k\right)}=$$

$$\frac{\left(\prod_{i=1}^{k-1}a_i,\frac{\prod_{i=1}^{k-1}a_ia_{k+1}}{a_1},\cdots,\frac{\prod_{i=1}^{k-1}a_ia_{k+1}}{a_{k-1}}\right)(a_k,a_{k+1})}{\left(\prod_{i=1}^{k-1}a_i,\left(\frac{\prod_{i=1}^{k-1}a_i}{a_1}a_{k+1},\cdots,\frac{\prod_{i=1}^{k-1}a_i}{a_{k-1}}a_{k+1}\right)(a_{k+1},a_k)\right)},$$

即

$$[(a_1,a_{k+1}),(a_2,a_{k+1}),\cdots,(a_k,a_{k+1})]=([a_1,a_2,\cdots,a_{k-1},a_k],a_{k+1}).$$

这就完成了定理 2(iii)的证明.

2 结束语

利用数学归纳法, 给出任意多个正整数的最大公

因数和最小公倍数之间的 3 种计算关系. 对于多个正整数的最大公因数与最小公倍数的计算,已有相应的程序算法具体算法.

熟知,RSA 公开密钥密码体制是基于两个正整数的运算,其加密算法中涉及到两个正整数的最大公因数. 本文推广得出的关于多个正整数的最大公因数的 3 个结论,是否能运用到加密的过程中,并提高该密码体制的安全性,是之后探讨和研究的一个方向.

参考文献:

[1] 陈全国,刘森. 关于最大公因数和最小公倍数的一点注记[J]. 牡丹江大学学报,2014,23(10):141-142.

[2] 刘娅茹. 安全多方计算中两个基础问题的研究[D]. 西安:西安科技大学,2018.

[3] 朱文余,孙琦. 计算机密码应用基础[M]. 北京:科学出版社,2000.

[4] 闵嗣鹤,严士健. 初等数论[M]. 3 版. 北京:高等教育出版社,2003.

[5] 汤剑红. 求多个数的最大公约数的算法设计[J]. 计算机时代,2012(6):21-22.

Several Calculation Relationships between the Greatest Common Divisor and the Least Common Multiple

XIAO Rui, YANG Hao, ZHOU Yunxiu, LIAO Qunying

(School of Mathematics, Sichuan Normal University, Chengdu 610066, China)

Abstract: It's well-known that for any positive integers a,b,c, $[a,b]=\frac{ab}{(a,b)}$, $[(a,c),(b,c)]=([a,b],c)$, where [ ] and ( ) represent the least common divisor and the greatest multiply, respectively. The RSA algorithm involved the related calculation of the greatest common divisor and the least common multiple. In order to provide a possible optimization scheme for the traditional RSA algorithm, the present paper takes advantage of the elementary methods and skills to explore the calculation relationship between the greatest common divisor and the least common multiple of any positive integers. The result mentioned above is promoted to obtain three calculation relationships between the greatest common divisor and the least common multiple of any positive integers.

Keywords: greatest common divisor; least common multiple; pure mathematics; coding and cryptography theory