信息安全数学基础

中山大学　数据科学与计算机学院
网络空间安全研究所/系

初等数论
第一章 整数的可除性

中山大学 数据科学与计算机学院

网络空间安全研究所/系

辗转相除法的重要性质.

回顾辗转相除法的过程:

$$a = bq_1 + r_2 \Longrightarrow r_2 = a - bq_1$$
$$b = r_2 q_2 + r_3 \Longrightarrow r_3 = b - r_2 q_2$$
$$r_2 = r_3 q_3 + r_4 \Longrightarrow r_4 = r_2 - r_3 q_3$$
$$r_3 = r_4 q_4 + r_5 \Longrightarrow r_5 = r_3 - r_4 q_4$$
$$\cdots\cdots$$
$$r_{n-4} = r_{n-3} q_{n-3} + r_{n-2} \Longrightarrow r_{n-2} = r_{n-4} - r_{n-3} q_{n-3}$$
$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1} \Longrightarrow r_{n-1} = r_{n-3} - r_{n-2} q_{n-2}$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \Longrightarrow r_n = r_{n-2} - r_{n-1} q_{n-1}$$
$$r_{n-1} = r_n q_n$$

所以

$$
\begin{aligned}
r_n &= r_{n-2} - r_{n-1}q_{n-1} \\
&= r_{n-2} - [r_{n-3} - r_{n-2}q_{n-2}]q_{n-1} \\
&= [r_{n-4} - r_{n-3}q_{n-3}] - [r_{n-3} - (r_{n-4} - r_{n-3}q_{n-3})q_{n-2}]q_{n-1} \\
&\cdots\cdots
\end{aligned}
$$

一直这样替换下去, 可以得到下面的形式:

$$r_n = s \cdot a + t \cdot b \quad (s, t \in \mathbb{Z})$$

即有结论:

$$\exists s, t \in \mathbb{Z}, s.t., (a, b) = s \cdot a + t \cdot b$$

定理

设a, b是任意两个正整数，则存在整数s, t使得

$$s \cdot a + t \cdot b = (a, b).$$

这一等式也叫做Bézout等式, 尽管我们似乎很少用这个名字来表示这一定理.

(1) 根据这个定理, 我们有: 如果a与b互素的话, $\exists s,t\in\mathbb{Z}, s.t., s\cdot a+t\cdot b=1$
这里反过来说也对: 如果$\exists s,t\in\mathbb{Z}, s.t., s\cdot a+t\cdot b=1$, 那么$a$与$b$互素.
这是因为: 设$(a,b)=d$, 则有$d|(sa+tb)$, 从而$d|1$, 从而$d=1$.
这样我们得到一个a与b互素的充要条件:

$$(a,b)=1 \iff \exists s,t\in\mathbb{Z}, s.t., s\cdot a+t\cdot b=1$$

(2) 根据这个定理, 我们还可以得到最大公因数的一个等价定义:

$$d=(a,b) \iff (d\,|\,a, d\,|\,b)\wedge(\text{如果}e\,|\,a, e\,|\,b, \text{那么}e\,|\,d)$$

"$\Longleftarrow$": 是显然的: 这表明d是公因数中最大的那个;
在证明"$\Longrightarrow$":

$$\because d=(a,b), \therefore \exists s,t, \text{使得}, d=sa+tb$$

$$\because e|a, e|b, \therefore e|(sa+tb), \therefore e|d$$

(3) 根据这个定理, 我们还可以得到:

$$\forall m \in \mathbb{Z}^+, (am, bm) = (a,b)m$$

事实上, 设$d=(a,b)$, $d'=(am,bm)$, 只需要说明$d'|(dm)$, $(dm)|d'$ 即可,

$$d=(a,b) \Longrightarrow \exists s,t, s.t., sa+tb=d \Longrightarrow s(am)+t(bm)=dm$$

$$\because d'|(am), d'|(bm), \therefore d'|(s(am)+t(bm)), \therefore d'|(dm)$$

另一方面, dm是am与bm的公因数, 而d'是am与bm的最大公因子, 所以有$(dm)|d'$ $\diamond$

将这个结论换个写法:

$$\frac{(am,bm)}{m}=(a,b), m\in\mathbb{Z}^+$$

换个记号:

$$\frac{(x,y)}{z}=(\frac{x}{z},\frac{y}{z}), z\in\mathbb{Z}^+$$

或者:

$$\frac{(x,y)}{|z|}=(\frac{x}{z},\frac{y}{z}), z\in\mathbb{Z}$$

取$z=(x,y)$, 我们就得到

$$(\frac{x}{(x,y)},\frac{y}{(x,y)})=1 \qquad \diamond$$

(4) 根据这个定理, 我们还可以得到:

$$(a,c)=1 \Longrightarrow (ab,c)=(b,c)$$

事实上, 设$d=(ab,c)$, $d'=(b,c)$, 只需要说明$d|d'$, $d'|d$

$$\left.\begin{array}{c} d'|b \Longrightarrow d'|ab \\ d'|c \end{array}\right\} \Longrightarrow d'|d$$

$$\left.\begin{array}{c} (a,c)=1 \Longrightarrow \exists s,t, s.t., sa+tc=1 \Longrightarrow sab+tcb=b \Longrightarrow s(ab)+tb\cdot c=b \\ d|(ab), d|c \end{array}\right\} \Longrightarrow d|b$$

这表明d是b和c的公因数，但是d'是b和c的最大公因数，所以有$d\,|\,d'$. $\diamond$

一般地, 如果$(a_1,c)=(a_2,c)=\ldots=(a_n,c)=1$, 则有$(a_1a_2\ldots a_n,c)=1$

事实上

$$\left.\begin{array}{c} (a_1,c)=1 \Longrightarrow (a_1a_2,c)=(a_2,c) \\ (a_2,c)=1 \end{array}\right\} \Longrightarrow (a_1a_2,c)=1 \Longrightarrow (a_1a_2a_3,c)=(a_3,c)$$

而$(a_3,c)=1$, 从而$(a_1a_2a_3,c)=1$, 从而$(a_1a_2a_3a_4,c)=(a_4,c)$, 以此类推, 得到

$$(a_1a_2\ldots a_n,c)=1.$$

例: 设n是合数, p是n的素因子, $\binom{n}{p} = \frac{n(n-1)(n-2)\dots(n-p+1)}{p!}$, 且$p^\alpha \| n$ (即$p^\alpha | n, p^{\alpha+1} \nmid n$), 则$p^\alpha \nmid \binom{n}{p}$

证明: 因为p是素数，所以

$$p^\alpha | n \Longrightarrow n = m \cdot p^\alpha$$

$$p^{\alpha+1} \nmid n \Longrightarrow p \nmid m \Longrightarrow (m, p) = 1.$$

另外, $p \nmid (n-1)$, 否则, 如果$p|n-1$, 则$p|n-(n-1)$, 则$p|1$, 矛盾. 所以$(p, n-1) = 1$; 类似地,

$$(p, n-2) = 1, (p, n-3) = 1, \dots, (p, n-(p-1)) = 1.$$

从而,

$$(p, (n-1)(n-2)(n-3)\dots(n-(p-1))) = 1.$$

从而

$$(p, m(n-1)(n-2)(n-3)\dots(n-(p-1))) = 1.$$

因为p与$m(n-1)(n-2)(n-3)\ldots(n-(p-1))$的最大公因数是1, 所以$p$与其的一个因子

$$\frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}$$

的最大公因数也是1, 即

$$(p, \frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}) = 1$$

如果$p^{\alpha} | \binom{n}{p}$, 则

$$p^{\alpha}\text{整除}p^{\alpha-1}\cdot\frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}$$

即

$$p\text{整除}\frac{m(n-1)(n-2)(n-3)\ldots(n-(p-1))}{(p-1)!}$$

矛盾. $\diamond$

$$(a,c)=1 \Longrightarrow (ab,c)=(b,c)$$

在这里，除了条件a与c互素外，如果更进一步，假设$c|ab$，则有:

$$\left.\begin{array}{c}(a,c)=1 \Longrightarrow (ab,c)=(b,c)\\ c|(ab) \Longrightarrow (ab,c)=c\end{array}\right\} \Longrightarrow c=(b,c) \Longrightarrow c|b$$

这里如果取c为素数p，即$p|(ab)$，则$(p,a)=1$，则有$p|b$;
注意到a与b的对称地位，如果$p|(ab)$，且$(p,b)=1$，则有$p|a$;
所以，如果$p|(ab)$，则要么$p|a$，要么$p|b$.

更一般的，如果$p|(a_1a_2\ldots a_n)$，则要么$p|a_1$，要么$p|a_2$，要么$p|a_3$，...,要么$p|a_n$.
这是因为，如果所有的a_i都不能被素数p整除的话，则有$(a_1,p)=1$，$(a_2,p)=1$，$(a_3,p)=1$，...，$(a_n,p)=1$，这样就有$(a_1a_2a_3\ldots a_n,p)=1$. 这与已知条件矛盾.
使用这个结论，我们可以证明著名的算术基本定理.

另外，对于任意的整数x，有

$$(a, b) = (a, ax + b) = (a + bx, b).$$

$$(a_1, a_2, \ldots, a_i, \ldots, a_k) = (a_1, a_2, \ldots, a_i + a_j x, \ldots, a_k),$$

其中$1 \le i \ne j \le k$. 使用这个结论，我们可以快速解决许多有关最大公因数的问题.

定理

设a,b是任意两个正整数，则存在整数s,t使得$s\cdot a+t\cdot b=(a,b)$.

下面来考虑计算定理中s和t的方法, 即广义欧几里得除法.
例如计算$s,t\in\mathbb{Z}, s.t., (169,121)=s\cdot 169+t\cdot 121$, 其具体求解过程是:

$$\begin{aligned}169&=1\cdot 121+48\\121&=2\cdot 48+25\\48&=1\cdot 25+23\\25&=1\cdot 23+2\\23&=11\cdot 2+1\\2&=2\cdot 1\end{aligned}$$

这样我们知道:

$$\begin{aligned}1&=23-11\cdot 2\\&=23-11\cdot(25-1\cdot 23)=12\cdot 23-11\cdot 25\\&=12\cdot(48-1\cdot 25)-11\cdot 25=12\cdot 48-23\cdot 25\\&=12\cdot 48-23\cdot(121-2\cdot 48)=-23\cdot 121+58\cdot 48\\&=-23\cdot 121+58\cdot(169-1\cdot 121)=58\cdot 169-81\cdot 121\end{aligned}$$

回顾辗转相除法的过程:

$$a = bq_1 + r_2, \quad b = r_2 q_2 + r_3$$

$$r_2 = r_3 q_3 + r_4$$

$$r_3 = r_4 q_4 + r_5$$

$$\cdots\cdots$$

$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

$$r_{n-1} = r_n q_n$$

将a和b换个记号, 分别写成r_0和r_1:

$$r_0 = r_1 q_1 + r_2, \quad r_1 = r_2 q_2 + r_3$$

$$r_2 = r_3 q_3 + r_4$$

$$r_3 = r_4 q_4 + r_5$$

$$\cdots\cdots$$

$$r_{n-3} = r_{n-2} q_{n-2} + r_{n-1}$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

$$r_{n-1} = r_n q_n$$

采用不完全商和余数的记号, 这里的q_i就是$q_i = [\frac{r_{i-1}}{r_i}]$

这里的r_{i+1}就是$r_{i+1} = r_{i-1} - r_i[\frac{r_{i-1}}{r_i}]$

并且, 如果$r_{n+1} = 0$, 那么r_n就是(a, b), 这个可以看作n的终止的判别准则.

j	辗转相除	q_{j+1}	r_{j+2}	s_j	t_j	$r_j = s_j a + t_j b$ $(= s_j r_0 + t_j r_1)$
0	$r_0 = r_1[\frac{r_0}{r_1}] + r_2$	$[\frac{r_0}{r_1}]$	$r_0 - r_1[\frac{r_0}{r_1}]$	1	0	$a(= r_0)$
1	$r_1 = r_2[\frac{r_1}{r_2}] + r_3$	$[\frac{r_1}{r_2}]$	$r_1 - r_2[\frac{r_1}{r_2}]$	0	1	$b(= r_1)$
2	$r_2 = r_3[\frac{r_2}{r_3}] + r_4$	$[\frac{r_2}{r_3}]$	$r_2 - r_3[\frac{r_2}{r_3}]$	1 $(= s_0 - q_1 s_1)$	$-q_1$ $(= t_0 - q_1 t_1)$	$a - bq_1(= r_2)$
3	$r_3 = r_4[\frac{r_3}{r_4}] + r_5$	$[\frac{r_3}{r_4}]$	$r_3 - r_4[\frac{r_3}{r_4}]$	$s_3 = ?$	$t_3 = ?$	$s_3 a + t_3 b(= r_3)$

事实上, 我们有:

$$r_3 = r_1 - q_2 r_2 = (s_1 a + t_1 b) - (s_2 a + t_2 b) q_2 = (s_1 - q_2 s_2) a + (t_1 - q_2 t_2) b = s_3 a + t_3 b.$$

所以, 我们有:

j	辗转相除	q_{j+1}	r_{j+2}	s_j	t_j	$r_i=s_ja+t_jb$ $=(s_jr_0+t_jr_1)$
0	$r_0=r_1[\frac{r_0}{r_1}]+r_2$	$[\frac{r_0}{r_1}]$	$r_0-r_1[\frac{r_0}{r_1}]$	1	0	$a(=r_0)$
1	$r_1=r_2[\frac{r_1}{r_2}]+r_3$	$[\frac{r_1}{r_2}]$	$r_1-r_2[\frac{r_1}{r_2}]$	0	1	$b(=r_1)$
2	$r_2=r_3[\frac{r_2}{r_3}]+r_4$	$[\frac{r_2}{r_3}]$	$r_2-r_3[\frac{r_2}{r_3}]$	1 $(=s_0-q_1s_1)$	$-q_1$ $(=t_0-q_1t_1)$	$a-bq_1(=r_2)$
3	$r_3=r_4[\frac{r_3}{r_4}]+r_5$	$[\frac{r_3}{r_4}]$	$r_3-r_4[\frac{r_3}{r_4}]$	$s_1-q_2s_2$	$t_1-q_2t_2$	$s_3a+t_3b(=r_3)$
4	$r_4=r_5[\frac{r_4}{r_5}]+r_6$	$[\frac{r_4}{r_5}]$	$r_4-r_5[\frac{r_4}{r_5}]$	$s_4=?$	$t_4=?$	$s_4a+t_4b(=r_4)$

事实上, 我们有:

$$r_4=r_2-q_3r_3=(s_2a+t_2b)-(s_3a+t_3b)q_3=(s_2-q_3s_3)a+(t_2-q_3t_3)b=s_4a+t_4b.$$

所以，我们有:

j	辗转相除	q_{j+1}	r_{j+2}	s_j	t_j	$r_i=s_ja+t_jb$ $=(s_jr_0+t_jr_1)$
0	$r_0=r_1[\frac{r_0}{r_1}]+r_2$	$[\frac{r_0}{r_1}]$	$r_0-r_1[\frac{r_0}{r_1}]$	1	0	$a(=r_0)$
1	$r_1=r_2[\frac{r_1}{r_2}]+r_3$	$[\frac{r_1}{r_2}]$	$r_1-r_2[\frac{r_1}{r_2}]$	0	1	$b(=r_1)$
2	$r_2=r_3[\frac{r_2}{r_3}]+r_4$	$[\frac{r_2}{r_3}]$	$r_2-r_3[\frac{r_2}{r_3}]$	1 $(=s_0-q_1s_1)$	$-q_1$ $(=t_0-q_1t_1)$	$a-bq_1(=r_2)$
3	$r_3=r_4[\frac{r_3}{r_4}]+r_5$	$[\frac{r_3}{r_4}]$	$r_3-r_4[\frac{r_3}{r_4}]$	$s_1-q_2s_2$	$t_1-q_2t_2$	$s_3a+t_3b(=r_3)$
4	$r_4=r_5[\frac{r_4}{r_5}]+r_6$	$[\frac{r_4}{r_5}]$	$r_4-r_5[\frac{r_4}{r_5}]$	$s_2-q_3s_3$	$t_2-q_3t_3$	$s_4a+t_4b(=r_4)$

类似的, 我们有:

j	q_{j+1}	s_j	t_j	$r_j = s_j a + t_j b$ $(= s_j r_0 + t_j r_1)$
0	$[\frac{r_0}{r_1}]$	1	0	$a (= r_0)$
1	$[\frac{r_1}{r_2}]$	0	1	$b (= r_1)$
2	$[\frac{r_2}{r_3}]$	1 $(= s_0 - q_1 s_1)$	$-q_1$ $(= t_0 - q_1 t_1)$	$a - bq_1 (= r_2)$
3	$[\frac{r_3}{r_4}]$	$s_1 - q_2 s_2$	$t_1 - q_2 t_2$	r_3
4	$[\frac{r_4}{r_5}]$	$s_2 - q_3 s_3$	$t_2 - q_3 t_3$	r_4
...				
j	$[\frac{r_j}{r_{j+1}}]$	$s_{j-2} - q_{j-1} s_{j-1}$	$t_{j-2} - q_{j-1} t_{j-1}$	r_j
...				
$n-1$	$[\frac{r_{n-1}}{r_n}]$	$s_{n-3} - q_{n-2} s_{n-2}$	$t_{n-3} - q_{n-2} t_{n-2}$	r_{n-1}
n		$s_{n-2} - q_{n-1} s_{n-1}$	$t_{n-2} - q_{n-1} t_{n-1}$	r_n

至此, 已得到最大公因数r_n, 计算可以结束, s, t也已经得到.

上述求最大公因数和s,t的过程可以总结为:

1. 初始化r_0, r_1分别为a, b, 初始化$s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$;
2. 计算$r_0 = q_1 r_1 + r_2$(从而得到q_1, r_2);
3. 对$j = 2, 3, 4, \ldots$
   1. 计算$r_{j-1} = q_j r_j + r_{j_1}$(从而得到$q_j, r_{j+1}$);
   2. 计算$s_j = s_{j-2} - q_{j-1} s_{j-1}$, $t_j = t_{j-2} - q_{j-1} t_{j-1}$;
   3. 如果$r_{j+1} = 0$, 则停止计算, 输出$s = s_j, t = t_j, (a, b) = r_j$.

对于s_i和t_j，有以下等式：

$$s_j = \begin{cases} 1 & j = 0 \\ 0 & j = 1 \\ s_{j-2} - q_{j-1} s_{j-1} & j \geq 2 \end{cases}, t_j = \begin{cases} 0 & j = 0 \\ 1 & j = 1 \\ t_{j-2} - q_{j-1} t_{j-1} & j \geq 2 \end{cases}.$$

示例:

$a = 1859, b = 1573,$

1. $r_0 = 1859, r_1 = 1573, s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1;$
2. $q_1 = 1, r_2 = 286;$
3. $j = 2$:
    1. $q_2 = 5, r_3 = 143$
    2. $s_2 = 1, t_2 = -1$
    3. $r_3 \neq 0$

   $j = 3$:
    1. $q_3 = 2, r_4 = 0$
    2. $s_3 = -5, t_3 = 6$
    3. $r_4 = 0$, stop and output: $s = -5, t = 6, (a, b) = 143(-5 \cdot 1859 + 6 \cdot 1573)$

示例: $a = 75, b = 28$

j	r_j	q_j	s_j	t_j
0	75		1	0
1	28	2	0	1
2	19	1	1	-2
3	9	2	-1	3
4	1	9	3	-8

考虑广义欧几里得除法的计算复杂性

令$a = r_0$，$b = r_1$以及$(a,b) = r_n$，其中$a > b$，且r_n是广义欧几里得除法中最后一个非零余数，即一次广义欧几里得除法需要使用n次欧几里得除法.

对于自然数n，引入斐波那契(Fibonacci)数列:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

对于$n \geq 1$，可以证明斐波那契数列满足$F_{n+1} = F_n + F_{n-1}$，并且

$$\log(3/2)\cdot n \leq \log F_n \leq \log 2 \cdot n.$$

用数学归纳法可以证明，对于$1 \leq j \leq n+1$，有不等式$r_{n-j+1} \geq F_j$成立.
特别地，取$j = n$，我们有$b = r_1 \geq F_n$，进而得到

$$\log b \geq \log F_{n-1} \geq \log(3/2)\cdot n.$$

最后，$n \leq 5\log b$，即使用欧几里得除法的次数不超过$5\log b$.

算术基本定理

任意正整数$n > 1$, 都可以表示成素数的乘积:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s \quad (p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_s)$$

比如$45 = 3 \cdot 3 \cdot 5$, $100 = 2 \cdot 2 \cdot 5 \cdot 5$

证明: 对n使用数学归纳法: 当$n = 2$时, $2 = 2$.
假设对小于n的正整数, 这个结论都成立, 下面考虑n自身:

- 如果n自身是素数: $n = n$;
- 如果n是合数, 我们知道它有非平凡因子, 比如

$$n = bc \quad 1 < b < n, 1 < c < n$$

b和c都小于n, 可以使用归纳假设, 即b和c都有素数的分解:

$$b = p_1' p_2' \ldots p_u', \qquad c = p_{u+1}' p_{u+2}' \ldots p_s'$$

这样就有

$$n = p_1' p_2' \ldots p_u' \cdot p_{u+1}' p_{u+2}' \ldots p_s'$$

对右边的素数调整下顺序, 使得满足从小到大的顺序即可得到结论. ◇

如果不考虑素数的先后顺序的话，上面n的素数分解式是唯一的：如果

$$n = p_1 p_2 \dots p_s \quad (p_1 \le p_2 \le \dots \le p_s)$$

$$n = q_1 q_2 \dots q_t \quad (q_1 \le q_2 \le \dots \le q_t)$$

这里p_i, q_j都是素数，则有

$$s = t, p_1 = q_1, p_2 = q_2, \dots, p_s = q_s$$

证明：事实上，

$$p_1 p_2 \dots p_s = q_1 q_2 \dots q_t \Longrightarrow p_1 | (q_1 q_2 \dots q_t)$$

$$\Longrightarrow \exists j, s.t., p_1 | q_j \Longrightarrow p_1 = q_j$$

同样的

$$\exists k, s.t., q_1 | p_k \Longrightarrow q_1 = p_k$$

$$\therefore p_1 \le p_k = q_1 \le q_j = p_1$$

$$\therefore p_1 = q_1$$

类似的可以证明$p_2 = q_2, p_3 = q_3, \dots$，而它们同为$n$的因数分解，自然也就有$s = t$.

将n的素数分解中相同的素数合并成幂的写法就有:
任意正整数$n > 1$可以唯一的表示成

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \quad \alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{Z}^+$$

这里$p_1, p_2, \ldots, p_t$是互不相同的素数.
这被称为n的标准分解式.

比如$100 = 2^2 \cdot 5^2$

假设$n>1$有标准分解式

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_t^{\alpha_t},\quad \alpha_1,\alpha_2,\ldots,\alpha_t\in\mathbb{Z}^+$$

则

$$d|n(d>0)\iff d=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_t^{\beta_t},\quad \alpha_1\geq\beta_1,\alpha_2\geq\beta_2,\ldots,\alpha_t\geq\beta_t$$

"$\Longleftarrow$" 显然;
"$\Longrightarrow$:" 因为$d|n$, 则d的素数分解式必为形式:

$$d=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_t^{\beta_t},\quad (\beta_i\geq 0)$$

这是因为, 如果d的分解式中含有某个不是n的素因子的素因子, 比如d的分解式为:

$$d=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_t^{\beta_t}\cdot q^{\gamma},\quad (\gamma\geq 1)$$

$$\therefore (p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_t^{\beta_t}\cdot q^{\gamma})|(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_t^{\alpha_t})$$

这样就有

$$q \mid \underbrace{p_1 \cdots p_1}_{\alpha_1} \cdot \underbrace{p_2 \cdots p_2}_{\alpha_2} \cdot \cdots \cdot \underbrace{p_t \cdots p_t}_{\alpha_t}$$

所以就有q整除某个$p_i (i = 1, 2, \ldots, t)$, 矛盾. 所以必有$d$的形式为

$$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_t^{\beta_t}, \quad (\beta_i \geq 0)$$

再说明

$$\beta_1 \leq \alpha_1, \beta_2 \leq \alpha_2, \ldots, \beta_t \leq \alpha_t$$

这是因为, 否则的话, 比如$\beta_1 > \alpha_1$, 则有

$$p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_t^{\beta_t} | p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$$

两边同时约去$p_1^{\alpha_1}$

$$p_1^{\beta_1 - \alpha_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_t^{\beta_t} | p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}$$

从而p_1要整除$p_2, p_3, \ldots, p_t$中的某一个, 不可能. $\diamond$

假设$n>1$有标准分解式

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \quad \alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{Z}^+$$

则我们可以知道n的因数个数为

$$(1+\alpha_1) \cdot (1+\alpha_2) \cdot \ldots \cdot (1+\alpha_t)$$

假设a有分解式

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \quad \alpha_1, \alpha_2, \ldots, \alpha_t \geq 0$$

b有分解式

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_t^{\beta_t}, \quad \beta_1, \beta_2, \ldots, \beta_t \geq 0$$

我们知道它们的因数形式是

$$d_a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_t^{a_t}, \quad \alpha_1 \geq a_1 \geq 0, \alpha_2 \geq a_2 \geq 0, \ldots, \alpha_t \geq a_t \geq 0$$

$$d_b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_t^{b_t}, \quad \beta_1 \geq b_1 \geq 0, \beta_2 \geq b_2 \geq 0, \ldots, \beta_t \geq b_t \geq 0$$

这样,a与b的最大公因数就是

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_t^{\min(\alpha_t,\beta_t)}$$

关于整数分解的一个性质

命题

给定正整数$n>1$，如果存在整数a,b使得

$$n \mid a^2-b^2, \quad n \nmid a-b, \quad n \nmid a+b,$$

则$(n,a-b)$和$(n,a+b)$都是n的真因数。

证明： 若$(n,a-b)$不是真因数，则$(n,a-b)=1$或$(n,a-b)=n$.

- 如果$(n,a-b)=1$，由$n \mid a^2-b^2$推出$n \mid a+b$，矛盾.
- 如果$(n,a-b)=n$，直接退出$n \mid a-b$，矛盾.

所以，$(n,a-b)$必须是n的真因数. 同理可证，$(n,a+b)$必须是n的真因数.

意义：如果能找到满足命题条件的a和b，则可以分解整数n. 在下学前期的《现代密码学》课程中我们将知道，该命题与证明Rabin密码体制的安全性有密切联系。

5. 最小公倍数

如果整数m是整数a_1的倍数，整数m是整数a_2的倍数，整数m是整数a_3的倍数，...，整数m是整数a_n的倍数，这时把整数m称为是$a_1, a_2, a_3, \ldots, a_n$的公倍数.

$a_1, a_2, a_3, \ldots, a_n$的所有公倍数中最小的哪个正整数叫做$a_1, a_2, a_3, \ldots, a_n$的最小公倍数，记作$[a_1, a_2, a_3, \ldots, a_n]$

比如$2, 3$的最小公倍数是6.

(1) 假设m是a与b的公倍数，如果a与b互素的话，则$ab|m$.

证明: 事实上,

$$\left.\begin{array}{r}\left.\begin{array}{r} a|m \Longrightarrow m = ak \\ b|m \end{array}\right\} \Longrightarrow b|(ak) \\ (a,b)=1 \end{array}\right\} \Longrightarrow b|k \Longrightarrow (ab)|(ak) \Longrightarrow (ab)|m$$

(2) 如果a与b互素的话(都是正数)，则$[a,b]=ab$.

这是因为a,b互素，所以$ab|[a,b]$，从而$ab \leq [a,b]$，而ab本身又是a与b的公倍数，从而$[a,b] \leq ab$，所以$ab=[a,b]$

(3) 对两个不同的素数p与q来说，$[p,q]=pq$.

(4) $[a,b]=\dfrac{ab}{(a,b)}$
这是因为, 我们知道
$$(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$$
而两个互素的数的最小公倍数就是它们的乘积, 所以有
$$[\frac{a}{(a,b)},\frac{b}{(a,b)}]=\frac{a}{(a,b)}\cdot\frac{b}{(a,b)}$$
这说明$\dfrac{ab}{d^2}$是$\dfrac{a}{d}$的倍数, 也是$\dfrac{b}{d}$的倍数, 从而, $\dfrac{ab}{d}$是a和b的公倍数.
设z也是a和b的公倍数, 则z必定不小于$\dfrac{ab}{d}$, 否则的话, 即$z<\dfrac{ab}{d}$, 则$\dfrac{z}{d}<\dfrac{ab}{d^2}$,
而且$\dfrac{z}{d}$是$\dfrac{a}{d}$的倍数, 也是$\dfrac{b}{d}$的倍数, 这样$\dfrac{z}{d}$就是比$\dfrac{ab}{d^2}$更小的$\dfrac{a}{d}$, $\dfrac{b}{d}$的公倍数, 不可能!
所以$z\geq\dfrac{ab}{d}$, 即, $\dfrac{ab}{d}$是a和b的最小公倍数, 即$[a,b]=\dfrac{ab}{d}=\dfrac{ab}{(a,b)}$. $\diamond$
这个结论给出了求两个整数最小公倍数的方法(先求最大公因数).
如果要求$a_1,a_2,a_3,\dots,a_n$的最小公倍数的话, 可以逐次求:
$$[[[[a_1,a_2],a_3],a_4],a_5\dots,a_n]$$

(5) m是a和b的公倍数, 则$[a,b]|m$.

这是因为

$$a|m, b|m \Longrightarrow \frac{a}{d}|\frac{m}{d}, \frac{b}{d}|\frac{m}{d}$$

而$\frac{a}{d}$与$\frac{b}{d}$ 互素, 所以$(\frac{a}{d}\cdot\frac{b}{d})|\frac{m}{d}$
从而$\frac{ab}{d}|m$, 即$[a,b]|m$. $\diamond$

更一般的情况也成立, 即

$$a_1|m, a_2|m, \ldots, a_n|m \Longrightarrow [a_1, a_2, \ldots, a_n]|m$$

(6) 假设a有素数分解式

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}, \quad \alpha_1, \alpha_2, \ldots, \alpha_t \geq 0$$

b有素数分解式

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_t^{\beta_t}, \quad \beta_1, \beta_2, \ldots, \beta_t \geq 0$$

我们知道它们的倍数形式是:

$$d_a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_t^{a_t}, \quad a_1 \geq \alpha_1 \geq 0, a_2 \geq \alpha_2 \geq 0, \ldots, a_t \geq \alpha_t \geq 0$$

$$d_b = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_t^{b_t}, \quad b_1 \geq \beta_1 \geq 0, b_2 \geq \beta_2 \geq 0, \ldots, b_t \geq \beta_t \geq 0$$

这样,a与b的最小公倍数就是

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \cdot p_2^{\max(\alpha_2, \beta_2)} \cdot \ldots \cdot p_t^{\max(\alpha_t, \beta_t)}$$

(7) $\forall a,b\in\mathbb{Z}^+,\exists a'|a,b'|b,(a',b')=1,s.t.,a'\cdot b'=[a,b]$

假设a,b有素数分解式

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s},\quad \alpha_1,\alpha_2,\ldots,\alpha_s\geq 0$$

$$b=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_s^{\beta_s},\quad \beta_1,\beta_2,\ldots,\beta_s\geq 0$$

对其中的素数$p_1,p_2,\ldots,p_s$重新排序为$p_{i_1},p_{i_2},\ldots,p_{i_t},p_{i_{t+1}},\ldots,p_{i_s}$，使得:

$$a=\underline{p_{i_1}^{\alpha_{i_1}}\cdot p_{i_2}^{\alpha_{i_2}}\cdot\ldots\cdot p_{i_t}^{\alpha_{i_t}}}\cdot\underbrace{p_{i_{t+1}}^{\alpha_{i_{t+1}}}\cdot p_{i_{t+2}}^{\alpha_{i_{t+2}}}\cdot\ldots\cdot p_{i_s}^{\alpha_{i_s}}},\quad \alpha_1,\alpha_2,\ldots,\alpha_s\geq 0$$

$$b=\underline{p_{i_1}^{\beta_{i_1}}\cdot p_{i_2}^{\beta_{i_2}}\cdot\ldots\cdot p_{i_t}^{\beta_{i_t}}}\cdot\underbrace{p_{i_{t+1}}^{\beta_{i_{t+1}}}\cdot p_{i_{t+2}}^{\beta_{i_{t+2}}}\cdot\ldots\cdot p_{i_s}^{\beta_{i_s}}},\quad \beta_1,\beta_2,\ldots,\beta_s\geq 0$$

满足条件:

$$\alpha_{i_1}\geq\beta_{i_1},\alpha_{i_2}\geq\beta_{i_2},\ldots,\alpha_{i_t}\geq\beta_{i_t}$$

$$\alpha_{i_{t+1}}<\beta_{i_{t+1}},\alpha_{i_{t+2}}<\beta_{i_{t+2}},\ldots,\alpha_{i_t}<\beta_{i_t}$$

则

$$[a,b]=\underline{p_{i_1}^{\alpha_{i_1}}\cdot p_{i_2}^{\alpha_{i_2}}\cdot\ldots\cdot p_{i_t}^{\alpha_{i_t}}}\cdot\underbrace{p_{i_{t+1}}^{\beta_{i_{t+1}}}\cdot{}_{i_{t+2}}^{\beta_{i_{t+2}}}\cdot\ldots\cdot p_{i_s}^{\beta_{i_s}}}$$

取

$$a'=p_{i_1}^{\alpha_{i_1}}\cdot p_{i_2}^{\alpha_{i_2}}\cdot\ldots\cdot p_{i_t}^{\alpha_{i_t}},\quad b'=p_{i_{t+1}}^{\beta_{i_{t+1}}}\cdot{}_{i_{t+2}}^{\beta_{i_{t+2}}}\cdot\ldots\cdot p_{i_s}^{\beta_{i_s}}$$

即得结果.

7. 一次不定方程

形如

$$a_1x_1 + a_2x_2 + \ldots + a_mx_m = n$$

其中$a_1, a_2, \ldots, a_m, n \in \mathbb{Z}$的方程称为$m$元一次不定方程.

特殊地, 形如

$$a_1x + a_2y = n$$

其中$a_1, a_2, n \in \mathbb{Z}$的方程称为二元一次不定方程.

定理

二元一次方程$ax+by=c$有整数解当且仅当$(a,b)\mid c$，且有解时，全部解可以表示为$x=x_0+bt, y=y_0-at$，其中x_0, y_0为任意一组解，t为任意整数.

证明: "$\Longrightarrow$:" 如果有整数解, 那么c可以表示为a和b的某一整系数线性组合. 又因为(a,b)整除a和b的任意整系数线性组合, 所以$(a,b)\mid c$.
"$\Longleftarrow$:" 不失一般性可设$a, b>0$, 则

$$\exists\, u, v \in \mathbb{Z}, \text{使得}, ua+vb=(a,b)$$

又因为$(a,b)\mid c$, 所以存在整数q使得$c=(a,b)q=auq+bvq$
则

$$x=x_0=uq, y=y_0=vq$$

就是该一次不定方程的一组(特)解.

假设, x_1, y_1 是另一组不同的解, 则有:

$$\begin{cases} ax_0 + by_0 = c & (1) \\ ax_1 + by_1 = c & (2) \end{cases}$$

$(2)-(1)$得:

$$a(x_1 - x_0) + b(y_1 - y_0) = 0 \Longrightarrow \frac{x_1 - x_0}{b} = -\frac{y_1 - y_0}{a}$$

令

$$\frac{x_1 - x_0}{b} = -\frac{y_1 - y_0}{a} = t$$

则有

$$x_1 = x_0 + bt, \quad y_1 = y_0 - at, t \in \mathbb{Z}$$

由x_1, y_1的任意性知

$$x = x_0 + bt, \quad y = y_0 - at, t \in \mathbb{Z}$$

就是该一次不定方程的全部解.

◇

8. 第一章小结

1. 如果c整除a，c整除b，那么c也能够整除$sa+tb$, 其中s,t为任意整数.
2. 证明素数一定有无穷多个.
3. 合数n的最小正因子p一定是素数，且$p \le \sqrt{n}$.
4. $a = bq + c \Longrightarrow (a,b) = (b,c)$.
5. 使用辗转相除法计算最大公因数.
6. 设a,b是任意两个正整数，则存在整数s,t使得$s\cdot a + t\cdot b = (a,b)$.
7. $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{|d|}$, 其中$d$是$a$和$b$的公因数. 特别地, $(\frac{x}{(x,y)}, \frac{y}{(x,y)}) = 1$.
8. $(a,c) = 1 \Longrightarrow (ab,c) = (b,c)$.
9. 使用广义欧几里得除法计算整数s和t, 使得$s\cdot a + t\cdot b = (a,b)$.
10. 算术基本定理, 整数的标准分解式.
11. $[a,b] = \dfrac{ab}{(a,b)}$
12. 一次不定方程解的存在性及表示，使用广义欧几里得除法求解一次不定方程.