信息安全数学基础

卢 伟
Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院
网络空间安全研究所/系

信息安全专业要求

国信办和网信办规定核心课程：

- 信息安全数学基础 — 不仅仅是密码学的数学基础，核心课程包括：
  - 数论、组合数学、近世代数
  - 概率论、数学变换
  - 计算复杂度理论
  - 信息论、编码理论
- 信息安全体系结构
- 密码学–算法与协议
- 网络安全概论
- 信息系统安全概论
- 信息安全测评与风险评估

教材和参考资料

- 教材：
  - 陈恭亮：《信息安全数学基础》，清华大学出版社
- 参考书：
  - 覃中平，张焕国：《信息安全数学基础》，清华大学出版社
  - 柯召，孙琦：《数论讲义》(上册)，等教育出版社，2001
  - 潘承洞，潘承彪：《初等数论》(第2版)，北京大学出版社

初等数论
第一章 整数的可除性

卢 伟
Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院
网络空间安全研究所/系

1. 整除

- 整除：
  设a,b是任意两个整数，若存在一个$q \in \mathbb{Z}$使得：$a = bq$成立，
  则称b整除a，或者说a被b整除，记作：$b|a$

1. 整除

- 整除：
  设a, b是任意两个整数，若存在一个$q \in \mathbb{Z}$使得：$a = bq$成立，
  则称b整除a，或者说a被b整除，记作：$b|a$
- 这样b就叫做a的因子(因数)，a叫做b的倍数
- 对应的，q也是a的因子，当我们讨论的对象主要是a, b时，我们可以将q写成$\frac{a}{b}$(在讨论整除的性质时，我们一般都默认因子b不为0，因此我们一般不会显式写出$q \neq 0$)

1. 整除

- 整除：
  设a,b是任意两个整数，若存在一个$q\in\mathbb{Z}$使得：$a=bq$成立，
  则称b整除a，或者说a被b整除，记作：$b|a$
- 这样b就叫做a的因子(因数)，a叫做b的倍数
- 对应的，q也是a的因子，当我们讨论的对象主要是a,b时，我们可以将q写成$\frac{a}{b}$(在讨论整除的性质时，我们一般都默认因子b不为0，因此我们一般不会显式写出$q\neq 0$)
- 另外，0是任意非0整数b的倍数($0=b\cdot 0$，即取$q=0$)
- 1是任意整数的因数($a=1\cdot a$，即取$q=a$)

1. 整除

- 整除：
  设a, b是任意两个整数，若存在一个$q \in \mathbb{Z}$使得：$a = bq$成立，
  则称b整除a，或者说a被b整除，记作：$b|a$
- 这样b就叫做a的因子(因数)，a叫做b的倍数
- 对应的，q也是a的因子，当我们讨论的对象主要是a, b时，我们可以将q写成$\frac{a}{b}$(在讨论整除的性质时，我们一般都默认因子b不为0，因此我们一般不会显式写出$q \neq 0$)
- 另外，0是任意非0整数b的倍数($0 = b \cdot 0$，即取$q = 0$)
- 1是任意整数的因数($a = 1 \cdot a$，即取$q = a$)
- 任意非0整数a是他自身的因数($a = a \cdot 1$，即取$q = 1$)，这也就意味着a是他自身的因数

1. 整除

- 整除：
  设a,b是任意两个整数，若存在一个$q\in\mathbb{Z}$使得：$a=bq$成立，
  则称b整除a，或者说a被b整除，记作：$b|a$
- 这样b就叫做a的因子(因数)，a叫做b的倍数
- 对应的，q也是a的因子，当我们讨论的对象主要是a,b时，我们可以将q写成$\frac{a}{b}$(在讨论整除的性质时，我们一般都默认因子b不为0，因此我们一般不会显式写出$q\neq 0$)
- 另外，0是任意非0整数b的倍数($0=b\cdot 0$，即取$q=0$)
- 1是任意整数的因数($a=1\cdot a$，即取$q=a$)
- 任意非0整数a是他自身的因数($a=a\cdot 1$，即取$q=1$)，这也就意味着a是他自身的因数
- 如果不存在整数q使得$a=bq$成立，则称b不能整除a，a不能被b整除，记作$b\nmid a$

整除的性质

易见以下整除的性质：

(1) 如果$a=bq$, 则有$a=(-b)(-q)$成立, 也就是说, 如果b是a的因子, 则$-b$也是a的因子：

$$b|a \Longrightarrow (-b)|a;$$

例如：3是12的因子，那么-3也是12的因子。

(2) 如果$a=bq$，则有$(-a)=b(-q)$成立，也就是说，如果b是a的因子，则b也是$-a$的因子：

$$b|a \Longrightarrow b|(-a);$$

例如：3是12的因子，那么3也是-12的因子。

(3) 如果$a=bq$，则有$(-a)=(-b)q$成立，也就是说，如果b是a的因子，则$-b$也是$-a$的因子：

$$b|a \Longrightarrow (-b)|(-a);$$

例如：3是12的因子，那么-3也是-12的因子。

整除的性质

(4) 整除的传递性：
如果c整除b，b整除a，那么c也能够整除a：

$$c|b, b|a \Longrightarrow c|a$$

使用整除的定义，可以看出这个结论是显然的：

$$\because b = cp, a = bq$$

$$\therefore a = (cp)q = c(pq)$$

$$\diamond$$

例如：3整除6，6整除12，那么3也能够整除12

整除的性质

(5) 如果c整除a，c整除b，那么c也能够整除$a \pm b$，即：

$$c|a, c|b \Longrightarrow c|(a \pm b)$$

使用整除的定义，可以看出这个结论是显然的：

$$\because a = cp, b = cq$$

$$\therefore a \pm b = cp \pm cq = c(p \pm q)$$

$$\diamond$$

例如：3整除9，3整除6，那么3也能够整除$(9+6)$，3也能够整除$(9-6)$

整除的性质

更进一步，如果c整除a，c整除b，那么c也能够整除$sa \pm tb$(s,t为任意整数)：

$$c|a, c|b \Longrightarrow c|(sa \pm tb)$$

使用整除的定义，可以看出这个结论是显然的：

$$\because a = cp, b = cq$$

$$\therefore sa = scp, tb = tcq$$

$$\therefore sa \pm tb = scp \pm tcq = c(sp \pm tq)$$

$$\diamond$$

例如：3整除9，3整除6，那么3也能够整除$(4 \cdot 9 + 2 \cdot 6)$，3也能够整除$(4 \cdot 9 - 2 \cdot 6)$
类似可证：

$$c|a_1, c|a_2, \cdots, c|a_n \Longrightarrow c|(s_1a_1 \pm s_2a_2 \pm \cdots \pm s_na_n).$$

整除的性质

再进一步，已知c整除a，c整除b，而且存在整数x,y，使得$xa+yb=1$，那么$c=\pm1$：

$$c|a, c|b, xa+yb=1 \Longrightarrow c=\pm1$$

使用整除的定义，可以看出这个结论是显然的：

$$\because c|a, c|b$$

$$\therefore c|(sa+tb)(\forall s,t\in\mathbb{Z})$$

$$\therefore c|(xa+yb)(\because x,y\in\mathbb{Z})$$

$$\therefore c|1$$

$$\therefore c=\pm1$$

$$\diamond$$

事实上，我们也知道条件：

$$\exists x,y\in\mathbb{Z}, s.t.(such\ that): xa+yb=1$$

也就是说a与b互素(互素的概念下面就会学到)
所以，a与b的公因子也就是±1了。

整除的性质

(6) $a|b, b|a \Longrightarrow a = \pm b$
用整除的定义，可以看出这个结论是显然的：

$$\because a = bp, b = aq$$

$$\therefore a = (aq)p = a(pq)$$

$$\therefore pq = 1$$

$$\therefore p = \pm 1, q = \pm 1$$

$$\therefore a = \pm b$$

$$\diamond$$

2. 素数

给定非零整数p，如果p除了平凡因子(即$\pm 1, \pm p$)外，没有其他因子，那么这种整数称为素数(也叫质数，或不可约数)

比如11，其因子只有$\pm 1, \pm 11$，所以11是素数.
11是素数，-11也是素数了。

一般的，p是素数，那么$-p$也是素数.
p不是素数，那么$-p$也不是素数，不是素数的数称为合数.
比如12和-12

由于这种对称性，我们一般考虑的素数是非负整数.
比如考虑$1, 3, 5, 7$，而不考虑$-1, -3, -5, -7$

事实上，任何合数n都有素因子，设$1 < p$是所有n的正因子中最小的那一个，那么p一定是素数.

因为p不是素数的话，那么p就是合数，根据合数的定义，那么p一定会有一个非平凡的正因子q(当然有$q < p$).

根据整除的传递性，q也是n的因子，这与p是n的最小正因子矛盾，从而p一定是素数.

命题

素数一定有无穷多个.

证明： 因为如果有有限多个的话，比如为：$p_1, p_2, \cdots, p_n$
令

$$N = p_1 p_2 \cdots p_n + 1$$

则N一定是个合数(因为素数只有n个)，从而它的大于1的最小正因子p是个素数，所以p是$p_1, p_2, \cdots, p_n$中的一个，比如说：$p = p_j$
这样：

$$p|N, p|(p_1 p_2 \cdots p_n)$$

所以应该有：

$$p|(N - p_1 p_2 \cdots p_n)$$

即：$p|1$
不可能!! $\diamond$

如前所述，任意合数n都有素数因子，设$1 < p$是所有n的正因子中最小的那一个，那么p一定是素数.
我们可以将p与n的关系写成：

$$n = p \cdot n_1$$

这样p与n_1都是n的非平凡因子，而p是最小的那个非平凡因子，所以有：

$$p \le n_1$$

这样就有：

$$n = p \cdot n_1 \ge p \cdot p = p^2$$

$\diamond$

这个结论一方面说明任意合数必有素数因子，另一方面也给出了最小素因子的大概界限($p \le \sqrt{n}$).
综合在一起就是：p是正合数n的大于1的最小正因子，那么p必定是素数，并且$p \le \sqrt{n}$.
由此我们知道：如果对所有小于等于$\sqrt{n}$的素数p来说，p都不能整除n，那么n必定是素数.

如果对所有小于等于$\sqrt{n}$的素数p来说，p都不能整除n，那么n必定是素数.
这个结论给出了查找素数的方法:

- 计算$\sqrt{n}$;
- 小于等于$\sqrt{n}$的素数，比如就是：p_1, p_2, p_3, p_4;
- 在小于等于n的数字中，删去所有p_1的倍数，这样剩下的任意数字都不是p_1的倍数;
- 在小于等于n的数字中，删去所有p_2的倍数，这样剩下的任意数字都不是p_2的倍数;
- 在小于等于n的数字中，删去所有p_3的倍数，这样剩下的任意数字都不是p_3的倍数;
- 在小于等于n的数字中，删去所有p_4的倍数，这样剩下的任意数字都不是p_4的倍数;
- 对剩下的任意数字m:$2 \le m \le n$来说，所有小于等于$\sqrt{m}(\le \sqrt{n})$的素数都不能整除m，所以m一定是素数.

示例：找出所有不超过$n = 100$的素数

$\sqrt{n} = 10$；

不超过10的素数是2,3,5,7

	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

在不超过100的数字中删去2的倍数：

		3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	
41		43		45		47		49	
51		53		55		57		59	
61		63		65		67		69	
71		73		75		77		79	
81		83		85		87		89	
91		93		95		97		99	

再删去3的倍数：

				5		7			
11		13				17		19	
		23		25				29	
31				35		37			
41		43				47		49	
51		53		55				59	
61				65		67			
71		73				77		79	
		83		85				89	
91				95		97			

再删去5的倍数：

						7			
11		13				17		19	
		23						29	
31						37			
41		43				47		49	
51		53						59	
61						67			
71		73				77		79	
		83						89	
91						97			

再删去7的倍数：

						7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
51		53						59	
61						67			
71		73						79	
		83						89	
						97			

现在所剩的数就是小于100的素数了.这个找素数的方法叫做Eratosthenes(爱拉托色尼)筛法

我们得到小于100的素数个数为26个.

一般情形：不超过x的素数个数记为$\pi(x)$,这个数字与$\frac{x}{\ln x}$差不多大，即有契比雪夫不等式(chebyshev inequality):

$$\frac{\ln 2}{3}\frac{x}{\ln x} < \pi(x) < 6\ln 2\frac{x}{\ln x}$$

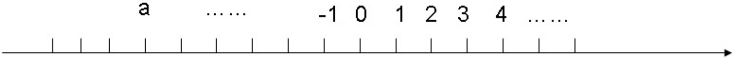
(证明略...)

比如：$\ln(100) = 4.60517019$，$\frac{100}{\ln(100)} = 21.7147$

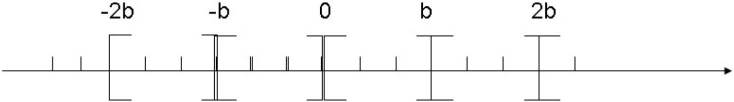
定理

$a \in \mathbb{Z}, b \in \mathbb{Z}^{+}, \exists(q,r), s.t.\ a = bq + r, \quad 0 \le r < b$

这是很显然的：
对于整数a



常数为b的区间将所有整数分成一段一段：



这样a必定落在一个区间内，比如：

$$qb \le a < (q+1)b$$

令$r = a - bq$，则有：

$$a = bq + r, \quad 0 \le r < b \qquad \diamond$$

进一步我们可以说明上述的使得$a = bq + r (0 \le r < b)$成立的(q, r)是唯一的:
事实上, 如果有(q, r)和(q_1, r_1)使得:

$$a = bq + r \qquad a = bq_1 + r_1$$

两者相减, 有

$$0 = b(q - q_1) + (r - r_1)$$

此时, q必定等于q_1, 因为, 如果不等的话, 则必定$|b(q - q_1)| \ge b$
但是

$$0 \le r, r_1 < b$$

所以

$$|r - r_1| < b$$

两个绝对值不相等的数加在一起不可能得到0, 所以$q = q_1$,从而$r = r_1$. $\diamond$

对于$a \in \mathbb{Z}, b \in \mathbb{Z}^+$，存在唯一的$(q, r)$使得$a = bq + r, 0 \leq r < b$成立，我们将这种关系称为欧几里德除法，也叫带余除法.

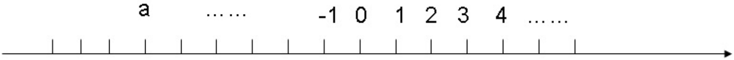
这里的q叫做(a被b除所得的)不完全商，r叫做(a被b除所得的)余数

可以看到，如果这里$r = 0$的话，那么a就被b整除；反之，如果a被b整除的话，那么$r = 0$.

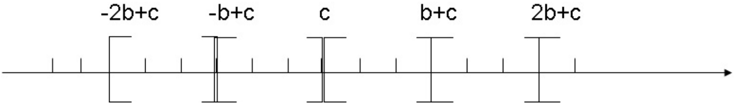
欧几里德除法的变形:

$a \in \mathbb{Z}, b \in \mathbb{Z}^+$，对任意的整数$c$，存在唯一的$(q, r)$使得$a = bq + r, c \leq r < b + c$成立.

这也是显然的:



长度为b的区间将所有整数分成一段一段:



这样a必定落在其中一个区间内，比如

$$qb + c \leq a < (q + 1)b + c$$

令$r = a - bq$，则有

$$a = bq + r, \quad (c \leq r < b + c).$$

符号: $[x]$

给定实数x, 符号$[x]$表示小于等于x的最大整数,

比如$[3.14] = 3, [-3.14] = -4$

这样, $a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists (q, r), s.t., a = bq + r, 0 \leq r < b$ 中的不完全商q和余数r可以写成:

$$q = [\frac{a}{b}] \qquad r = a - b[\frac{a}{b}]$$

欧几里德除法的应用：正整数的b进制表示

对$1 < b \in \mathbb{Z}^+$，任意正整数n可以表示成

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

的形式，这里$0 \leq a_i < b (i = 1, 2, \ldots, k)$.
事实上,使用欧几里德除法可以很容易得到验证.
首先，用b去除$n \implies n = bq_0 + a_0, (0 \leq a_0 < b)$,
再用b去除$q_0 \implies q_0 = bq_1 + a_1, (0 \leq a_1 < b)$,
再用b去除$q_1 \implies q_1 = bq_2 + a_2, (0 \leq a_2 < b)$,
一直下去,......
因为不完全商q_i越来越小，一定会达到一种情况，那就是$0 \leq q_{k-1} < b$，这时:

$$q_{k-2} = bq_{k-1} + a_{k-1}, (0 \leq a_{k-1} < b)$$

$$q_{k-1} = b \cdot 0 + a_k, (i.e., 0 \leq q_{k-1} = a_k < b)$$

将这些式子一次次代换就会得到:

$$\begin{aligned}
n &= bq_0 + a_0 \\
&= b(bq_1 + a_1) + a_0 \\
&= b^2 q_1 + ba_1 + a_0 \\
&= b^2(bq_2 + a_2) + ba_1 + a_0 \\
&= b^3 q_2 + b^2 a_2 + ba_1 + a_0 \\
&= \ldots\ldots \\
&= b^k q_{k-1} + b^{k-1} a_{k-1} + b^{k-2} a_{k-2} + \ldots + ba_1 + a_0 \\
&= b^k a_k + b^{k-1} a_{k-1} + b^{k-2} a_{k-2} + \ldots + ba_1 + a_0
\end{aligned}$$

$$(0 \le a_k, a_{k-1}, a_{k-2}, \ldots, a_2, a_1, a_0 < b)$$

对$1 < b \in \mathbb{Z}^+$, 任意正整数n可以表示成

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

的形式, 这里$0 \leq a_i < b (i = 1, \ldots, k)$. 这种表示形式是唯一的:
如果有两组系数$\{a_i\}, \{c_i\}$(如果两组个数不等长的话, 短的那组补0使得一样长)使得

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 \quad (0 \leq a_i < b (i = 0, 1, 2, \ldots, k))$$

$$n = c_k b^k + c_{k-1} b^{k-1} + \ldots + c_1 b + c_0 \quad (0 \leq c_i < b (i = 0, 1, 2, \ldots, k))$$

从而

$$0 = (a_k - c_k) b^k + (a_{k-1} - c_{k-1}) b^{k-1} + \ldots + (a_1 - c_1) b + (a_0 - c_0)$$

这时(如果$a_0 = c_0$的话考虑$a_1 - c_1$, 依次类推)

$$a_0 - c_0 = -[(a_k - c_k) b^k + (a_{k-1} - c_{k-1}) b^{k-1} + \ldots + (a_1 - c_1) b]$$

从而

$$b | a_0 - c_0 \quad \therefore |a_0 - c_0| \geq b$$

而

$$0 \leq a_0 < b, 0 \leq c_0 < b \Longrightarrow |a_0 - c_0| < b$$

矛盾!

对$1 < b \in \mathbb{Z}^+$, 任意正整数n可以表示成

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

的形式, 这里$0 \leq a_i < b (i = 1, \ldots, k)$. 这种表示形式是唯一的, 可以将$n$写成

$$n = (a_k a_{k-1} a_{k-2} \ldots a_1 a_0)_b$$

的形式$(0 \leq a_0 < b(i = 1, 2, \ldots, k))$, 称为$n$的$b$进制表示.
比如二进制$(n = 642)$:

$$\begin{aligned}
642 &= 2 \cdot 321 + 0 \quad (i.e., a_0 = 0)\\
321 &= 2 \cdot 160 + 1 \quad (i.e., a_1 = 1)\\
160 &= 2 \cdot 80 + 0 \quad (i.e., a_2 = 0)\\
80 &= 2 \cdot 40 + 0 \quad (i.e., a_3 = 0)\\
40 &= 2 \cdot 20 + 0 \quad (i.e., a_4 = 0)\\
20 &= 2 \cdot 10 + 0 \quad (i.e., a_5 = 0)\\
10 &= 2 \cdot 5 + 0 \quad (i.e., a_6 = 0)\\
5 &= 2 \cdot 2 + 1 \quad (i.e., a_7 = 1)\\
2 &= 2 \cdot 1 + 0 \quad (i.e., a_8 = 0)\\
1 &= 2 \cdot 0 + 1 \quad (i.e., a_9 = 1)
\end{aligned}$$

所以642的二进制表示就是$(1010000010)_2$
类似可以求出642的8进制, 16进制表示.

我们都知道, 16进制用$0-9, A(10), B(11), C(12), D(13), E(14), F(15)$表示.
比如$(ABC9)_{16}$即为10进制的$43796 (= A \cdot 16^6 + B \cdot 16^2 + C \cdot 16^1 + 8 \cdot 16^0)$

16进制与2进制相互之间可以比较容易的转换:

0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

比如$(ABC8)_{16} = (1010\ 1011\ 1100\ 1000)_2$
$(101\ 1101\ 1111\ 1110\ 1001)_2 = (5DFE9)_{16}$

4. 最大公因数与互素

给定整数$a_1, a_2, \ldots, a_n$，如果:

$$d|a_1, d|a_2, \ldots, d|a_n$$

则称d为$a_1, a_2, \ldots, a_n$的公因数.
如果$a_1, a_2, \ldots, a_n$不全为0，那么它们的公因数中存在最大的一个，这个公因数称为$a_1, a_2, \ldots, a_n$的最大公因数(greatest common divisor, gcd)，记做$(a_1, a_2, \ldots, a_n)$.

按照这个定义，可以看到，$(a_1, a_2, \ldots, a_n) = (a_{i_1}, a_{i_2}, \ldots, a_{i_n})(i_1, i_2, \ldots, i_n$从$1-n$取值各不相同).
如果$a_1, a_2, \ldots, a_n$的最大公因数为1的话，称$a_1, a_2, \ldots, a_n$互素，互质.

比如，14的因数为$\pm1, \pm3, \pm7, \pm14$,21的因数为$\pm1, \pm3, \pm7, \pm21$,
它们的公因数为$\pm1, \pm7$，最大公因数为7
-15和21的公因数为$\pm1, \pm3$，最大公因数为3.
$14, -15, 21$的最大公因数为1，即$14, -15, 21$互素.
7和14的最大公因数就是7本身.

一般地，如果$a, b \in \mathbb{Z}^+, b|a$，那么$(a, b) = b$.

小结论

(1) 给定一个整数a和一个素数p, 如果a不是p的倍数的话, 它一定和p互素.
事实上, 假设$(a, p) = d$, 则有$d|p$.
所以$d = 1$或p.
如果$d = p$的话, 就会有$p|a$, 这与条件矛盾. $\diamond$

使用公因数和最大公因数的定义马上就可得到下面几个显然的结论:
(2) $a_1, a_2, \ldots, a_n$的公因数与$|a_1|, |a_2|, \ldots, |a_n|$的公因数相同
(3) $(a_1, a_2, \ldots, a_n) = (|a_1|, |a_2|, \ldots, |a_n|)$
(4) $(a, b) = (a, -b) = (-a, b) = (-a, -b)$
(5) $(0, b) = |b|$
(6) $a = bq + c \Longrightarrow (a, b) = (b, c)$
证明: 设$d = (a, b), d' = (b, c)$
要说明$d = d'$, 只需要说明$d \leq d'$, $d' \leq d$即可:
事实上,

$$d|a, d|b \Longrightarrow d|(a - bq) \Longrightarrow d|c \Longrightarrow d \leq d'$$

$$d'|b, d'|c \Longrightarrow d'|(bq + c) \Longrightarrow d'|a \Longrightarrow d' \leq d$$

(当然这里也有$a = bq + c \Longrightarrow (a, q) = (q, c)$成立.)
利用这个结论可以很方便的帮助我们求任意两个整数的最大公因数.

辗转相除法

比如给定任意两个正整数a, b, 使用欧几里德除法存在如下式子成立:

$$a = bq_1 + r_2 \quad (0 \leq r_2 < b)$$

这时我们知道$(a, b) = (b, r_2)$
所以要求(a, b), 只需要求(b, r_2).
而要求(b, r_2), 可以类似求(a, b)的做法:

$$b = r_2 q_2 + r_3 \quad (0 \leq r_3 < r_2)$$

这时我们知道$(a, b) = (b, r_2) = (r_2, r_3)$
所以要求(a, b), 只需要求(r_2, r_3).
而要求(r_2, r_3), 可以类似求(b, r_2)的做法:

$$r_2 = r_3 q_3 + r_4 \quad (0 \leq r_4 < r_3)$$

这时我们知道$(a, b) = (b, r_2) = (r_2, r_3) = (r_3, r_4)$
所以要求(a, b), 只需要求(r_3, r_4).

可以看到余数越来越小，所以继续这个过程一定会有下面的情况出现:

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad (0 \le r_n < r_{n-1})$$

$$r_{n-1} = r_n q_n \quad (i.e., r_{n+1} = 0)$$

这时我们知道

$$(a,b) = (b,r_2) = (r_2,r_3) = (r_3,r_4) = \ldots = (r_{n-2},r_{n-1}) = (r_{n-1},r_n) = r_n$$

可见，使用这种方法，无论给定多么大的整数a和b，都可以经过有限步求出他们的最大公因数，而按照最大公因数的定义求任意两个数的最大公因数的话，必须将给定的数进行分解，但对大数进行分解是件困难的事.
上面这种求最大公因数的方法叫做辗转相除法，也叫广义欧几里德除法.

示例:
求$(-1859, 1573)$

$$(-1859, 1573) = (1859, 1573)$$

$$1859 = 1 \cdot 1573 + 286 \Longrightarrow (1859, 1573) = (1573, 286)$$

$$1573 = 5 \cdot 286 + 143 \Longrightarrow (1573, 286) = (286, 143)$$

$$286 = 2 \cdot 143 \Longrightarrow (286, 143) = 143$$

$$\therefore (-1859, 1573) = 143$$

示例：求$(46480, 39423)$

$$
\begin{aligned}
46480 &= 1 \cdot 39423 + 7057 \\
39423 &= 5 \cdot 7057 + 4138 \\
7057 &= 1 \cdot 4138 + 2919 \\
4138 &= 1 \cdot 2919 + 1219 \\
2919 &= 2 \cdot 1219 + 481 \\
1219 &= 2 \cdot 481 + 257 \\
481 &= 1 \cdot 257 + 224 \\
257 &= 1 \cdot 224 + 33 \\
224 &= 6 \cdot 33 + 26 \\
33 &= 1 \cdot 26 + 7 \\
26 &= 3 \cdot 7 + 5 \\
7 &= 1 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}
$$

$$\therefore (46480,39423) = 1$$

注：求$a_1, a_2, \ldots, a_n$的最大公因数

$$(a_1, a_2, \ldots, a_n)$$

可以先求出

$$d_2 = (a_1, a_2)$$

再求出

$$d_3 = (d_2, a_3)$$

再求出

$$d_4 = (d_3, a_4)$$

再求出

$$d_5 = (d_4, a_5)$$

$$\cdots\cdots$$

最后求出

$$d_n = (d_{n-1}, a_n)$$

则有

$$d_n = (a_1, a_2, \ldots, a_n)$$

注: 给定两个正整数a,b, 利用欧几里德除法我们知道:

$$\exists q\in\mathbb{Z}, r(0\le r<b), s.t., a=bq+r \Longrightarrow 2^a=2^r\cdot 2^{bq}$$
$$\Longrightarrow 2^a-1=2^r(2^{bq}-1)+(2^r-1)$$
$$\Longrightarrow 2^a-1=2^r(2^b-1)(q_1)+(2^r-1)$$
$$\Longrightarrow 2^a-1=(2^b-1)(2^r\cdot q_1)+(2^r-1)$$
$$\Longrightarrow 2^a-1=(2^b-1)q'+(2^r-1)\quad (q'\in\mathbb{Z}, 0\le 2^r-1<2^b-1)$$

即

$$a=bq+r_2(0\le r_2<b)\Longrightarrow 2^a-1=(2^b-1)q'+(2^{r_2}-1)(q'\in\mathbb{Z},0\le 2^{r_2}-1<2^b-1)$$

类似地, 我们有:

$$b=r_2q_2+r_3(0\le r_3<r_2)\Longrightarrow 2^b-1=(2^{r_2}-1)q_2'+(2^{r_3}-1)(q_2'\in\mathbb{Z},0\le 2^{r_3}-1<2^{r_2}-1)$$

$$r_2=r_3q_3+r_4(0\le r_4<r_3)\Longrightarrow 2^{r_2}-1=(2^{r_3}-1)q_3'+(2^{r_4}-1)(q_3'\in\mathbb{Z},0\le 2^{r_4}-1<2^{r_3}-1$$
$$r_3=r_4q_4+r_5(0\le r_5<r_4)\Longrightarrow 2^{r_3}-1=(2^{r_4}-1)q_4'+(2^{r_5}-1)(q_4'\in\mathbb{Z},0\le 2^{r_5}-1<2^{r_4}-1$$

这个过程一直持续下去, 如果左边的余数$r_i\neq 0$的话, 右边的余数$2^{r_i}-1\neq 0$; 如果左边的余数$r_i=0$的话, 右边的余数$2^{r_i}-1=0$.
这样最终在我们到达a与b的最大公因数$r_n=(a,b)$的时候, 我们也就得到了2^a-1与2^b-1的最大公因数, 也就是$2^{r_n}-1$, 即$2^{(a,b)}-1$

由前, 我们有:

$$(2^a-1,2^b-1)=2^{(a,b)}-1$$

因此, 如果a与b互素的话, 有

$$(a,b)=1 \Longrightarrow 2^{(a,b)}-1=1 \Longrightarrow (2^a-1,2^b-1)=1$$

反之, 如果2^a-1与2^b-1互素的话, 有

$$(2^a-1,2^b-1)=1 \Longrightarrow 2^{(a,b)}-1=1 \Longrightarrow (a,b)=1$$

即

$$(a,b)=1 \iff (2^a-1,2^b-1)=1$$

辗转相除法的重要性质.

回顾辗转相除法的过程:

$$a = bq_1 + r_2 \Longrightarrow r_2 = a - bq_1$$

$$b = r_2q_2 + r_3 \Longrightarrow r_3 = b - r_2q_2$$

$$r_2 = r_3q_3 + r_4 \Longrightarrow r_4 = r_2 - r_3q_3$$

$$r_3 = r_4q_4 + r_5 \Longrightarrow r_5 = r_3 - r_4q_4$$

$$\cdots\cdots$$

$$r_{n-4} = r_{n-3}q_{n-3} + r_{n-2} \Longrightarrow r_{n-2} = r_{n-4} - r_{n-3}q_{n-3}$$

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

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

$$r_{n-1} = r_nq_n$$

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:

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

(1) 根据这个结论, 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) 根据这个结论, 我们还可以得到最大公因数的一个等价定义:

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

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

$$\because d=(a,b), \therefore \exists s,t, s.t., d=sa+tb$$

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

(3) 根据这个结论，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) 根据这个结论, 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$d|d'$, $d'|d$

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

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

$\diamond$

由此, 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

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

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

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

证明: 事实上,

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

$$p^{\alpha+1} \nmid n \Longrightarrow p \nmid m \Longrightarrow (m,p) = 1(\because p \text{ is prime})$$

另外, 如果$p|n-1$, 则$p|n-(n-1)$, 则$p|1$, 不可能, 所以, $p \nmid (n-1)$, 又因为p是素数, 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

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

从而

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

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

从而

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

(这是因为p与$m(n-1)(n-2)(n-3)\dots(n-(p-1))$的最大公因数是1, 所以与$m(n-1)(n-2)(n-3)\dots(n-(p-1))$的因子

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

的最大公因数肯定也是1.)

如果$p^\alpha | \binom{n}{p}$, 则

$$p^\alpha | [p^{\alpha-1} \cdot \frac{m(n-1)(n-2)(n-3)\dots(n-(p-1))}{(p-1)!}]$$

即

$$p | [\frac{m(n-1)(n-2)(n-3)\dots(n-(p-1))}{(p-1)!}]$$

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$p|(a_1a_2\dots a_n)$, 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$(a_1a_2a_3\dots a_n,p)=1$. 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.

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

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

Proof: 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

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

则

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

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

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

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:

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

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

展开来写就是

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

这样就有

$$q|(p_1\ldots p_1)_{\alpha_1}\cdot(p_2\ldots p_2)_{\alpha_2}\cdot\ldots\cdot(p_t\ldots p_t)_{\alpha_t}$$

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

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

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

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

两边同时约去$p_1^{\alpha_1}$

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

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

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

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

下面我们看看s和t的求法:

比如求$s,t\in\mathbb{Z}, s.t., (169,121)=s\cdot 169+t\cdot 121$, 其具体求解过程是:

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

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:

$$a = bq_1 + r_2, \quad b = r_2q_2 + r_3$$
$$r_2 = r_3q_3 + r_4$$
$$r_3 = r_4q_4 + r_5$$
$$\cdots\cdots$$
$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$
$$r_{n-1} = r_nq_n$$

将a和b换个记号，分别写成r_0和r_1:

$$r_0 = r_1q_1 + r_2, \quad r_1 = r_2q_2 + r_3$$
$$r_2 = r_3q_3 + r_4$$
$$r_3 = r_4q_4 + r_5$$
$$\cdots\cdots$$
$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1}$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$
$$r_{n-1} = r_nq_n$$

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	$s_j a + t_j b (s_j r_0 + t_j r_1$
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	$r_3 = r_4[\frac{r_3}{r_4}] + r_5$	$[\frac{r_3}{r_4}]$	$r_3 - r_4[\frac{r_3}{r_4}]$	$s_1 - q_2 s_2$	$t_1 - q_2 t_2$	?

事实上，我们有:

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

所以，我们有：

j	辗转相除	q_{j+1}	r_{j+2}	s_j	t_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	$r_3 = r_4[\frac{r_3}{r_4}] + r_5$	$[\frac{r_3}{r_4}]$	$r_3 - r_4[\frac{r_3}{r_4}]$	$s_1 - q_2 s_2$	$t_1 - q_2 t_2$	r_3
4	$r_4 = r_5[\frac{r_4}{r_5}] + r_6$	$[\frac{r_4}{r_5}]$	$r_4 - r_5[\frac{r_4}{r_5}]$	$s_2 - q_3 s_3$	$t_2 - q_3 t_3$	?

事实上，我们有：

$$s_4 a + t_4 b = (s_2 - q_3 s_3)a + (t_2 - q_3 t_3)b = (s_2 a + t_2 b) - (q_3 s_3 a + q_3 t_3 b) = r_2 - q_3 r_3 = r_4$$

所以，我们有：

j	辗转相除	q_{j+1}	r_{j+2}	s_j	t_j	$s_ja+t_jb(s_jr_0+t_jr_1$
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	$r_3=r_4[\frac{r_3}{r_4}]+r_5$	$[\frac{r_3}{r_4}]$	$r_3-r_4[\frac{r_3}{r_4}]$	$s_1-q_2s_2$	$t_1-q_2t_2$	r_3
4	$r_4=r_5[\frac{r_4}{r_5}]+r_6$	$[\frac{r_4}{r_5}]$	$r_4-r_5[\frac{r_4}{r_5}]$	$s_2-q_3s_3$	$t_2-q_3t_3$	r_4

类似的，我们有：

j	辗转相除	q_{j+1}	r_{j+2}	s_j	t_j
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
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
2	$r_2 = r_3[\frac{r_2}{r_3}] + r_4$	$[\frac{r_2}{r_3}]$	$r_2 - r_3[\frac{r_2}{r_3}]$	$1(= s_0 - q_1 s_1)$	$-q_1(= t_0 - q_1$
3	$r_3 = r_4[\frac{r_3}{r_4}] + r_5$	$[\frac{r_3}{r_4}]$	$r_3 - r_4[\frac{r_3}{r_4}]$	$s_1 - q_2 s_2$	$t_1 - q_2 t_2$
4	$r_4 = r_5[\frac{r_4}{r_5}] + r_6$	$[\frac{r_4}{r_5}]$	$r_4 - r_5[\frac{r_4}{r_5}]$	$s_2 - q_3 s_3$	$t_2 - q_3 t_3$
$\cdots$					
j	$r_j = r_{j+1}[\frac{r_j}{r_{j+1}}] + r_{j+2}$	$[\frac{r_j}{r_{j+1}}]$	$r_j - r_{j+1}[\frac{r_j}{r_{j+1}}]$	$s_{j-2} - q_{j-1} s_{j-1}$	$t_{j-2} - q_{j-1} t_j$
$\cdots$					
$n-1$	$r_{n-1} = r_n[\frac{r_{n-1}}{r_n}] + r_{n+1}$	$[\frac{r_{n-1}}{r_n}]$	$r_{n-1} - r_n[\frac{r_{n-1}}{r_n}]$	$s_{n-3} - q_{n-2} s_{n-2}$	$t_{n-3} - q_{n-2} t_r$
n				$s_{n-2} - q_{n-1} s_{n-1}$	$t_{n-2} - q_{n-1} t_r$

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$r_0=q_1r_1+r_2$(从而得到q_1,r_2);
3. 对$j=2,3,4,\ldots$
    1. 计算$r_{j-1}=q_jr_j+r_{j_1}$(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$s=s_j,t=t_j,(a,b)=r_j$.

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: $s = -5, t = 6, (a, b) = 143(-5 \cdot 1859 + 6 \cdot 1573)$

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.

最小公倍数的性质

(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$ab \le [a,b]$，而ab本身又是a与b的公倍数，从而$[a,b] \le ab$，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的倍数，也是b的倍数，即是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$a_1,a_2,a_3,\ldots,a_n$的最小公倍数的话，可以逐次求:

$$[[[[a_1,a_2],a_3],a_4],a_5\ldots,a_n]$$

(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.

6. 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$a_1x+a_2y=n$有整数解 $\iff (a_1,a_2)|n$
且有解时，全部解可以表示为$x=x_0+a_2t, y=y_0-a_1t$，其中x_0,y_0为任意一组解，t为任意整数.

证明: "$\Longrightarrow$:" 显然
"$\Longleftarrow$:" 不失一般性可设$a_1,a_2>0$，则

$$\exists u,v,s.t., a_1u+a_2v=(a_1,a_2)$$

又由$(a_1,a_2)|n$，所以$n=(a_1,a_2)t=a_1ut+a_2vt$
则

$$x=x_0=ut, y=y_0=vt$$

就是该一次不定方程的一组解.

假设, x_1, y_1 是另一组不同的解, 则有:

$$\begin{cases} a_1x_0 + a_2y_0 = n & (1) \\ a_1x_1 + a_2y_1 = n & (2) \end{cases}$$

$(2) - (1)$得:

$$a_1(x_1 - x_0) + a_2(y_1 - y_0) = 0 \Longrightarrow \frac{x_1 - x_0}{a_2} = -\frac{y_1 - y_0}{a_1}$$

令

$$\frac{x_1 - x_0}{a_2} = -\frac{y_1 - y_0}{a_1} = t$$

则有

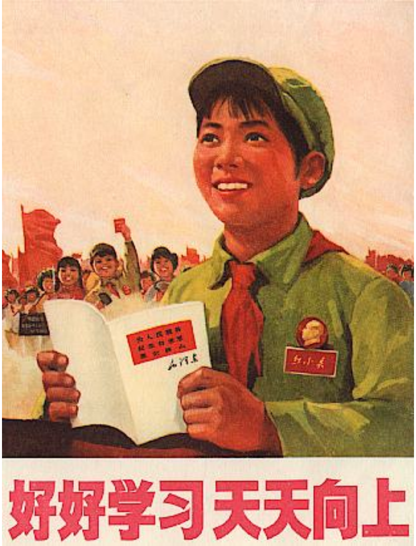
$$x_1 = x_0 + a_2t, y_1 = y_0 - a_1t, t \in \mathbb{Z}$$

由x_1, y_1的任意性知

$$x = x_0 + a_2t, y = y_0 - a_1t, t \in \mathbb{Z}$$

就是该一次不定方程的全部解.

◇


好好学习天天向上