

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

国信办(国务院信息化工作办公室)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

《信息安全数学基础》与《现代密码学》

- 《信息安全数学基础》可以分为“初等数论”和“抽象代数”两个部分，是《现代密码学》的最重要的先修课程，应按照教学要求理解之掌握之，否则难以开展《现代密码学》的学习。
- “初等数论”部分包括整除、同余、同余方程、原根与指标和素性检验等，是理解和实现各种密码算法的基础，要求熟练掌握相关计算问题的求解方法，理解相关数学概念、定理及其证明过程。
- “抽象代数”部分包括群、环和域的基本概念和一些最基本的性质，是深入理解和研究密码学原理的必备知识，要求了解以“群环域”为核心的抽象代数的基本知识体系，理解其中一些重要的数学概念、定理及其证明过程，熟悉群同态的基本概念，以及循环群和有限域的基本性质。

- 教材:

- 陈恭亮: 《信息安全数学基础》(第二版), 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), 高等教育出版社, 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

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:

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

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:

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

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:

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

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 :

$$c|b, b|a \implies c|a$$

使用整除的定义, 可以看出这个结论是显然的:

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

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



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:

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

使用整除的定义, 可以看出这个结论是显然的:

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

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

◇

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):

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

使用整除的定义, 可以看出这个结论是显然的:

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

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

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

◇

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:

$$c|a_1, c|a_2, \dots, c|a_n \implies c|(s_1a_1 \pm s_2a_2 \pm \dots \pm s_na_n).$$

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 $c = \pm 1$:

$$c|a, c|b, xa + yb = 1 \implies c = \pm 1$$

使用整除的定义, 可以看出这个结论是显然的:

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

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

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

$$\therefore c|1$$

$$\therefore c = \pm 1$$



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) $a|b, b|a \implies a = \pm b$

用整除的定义，可以看出这个结论是显然的：

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

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

$$\therefore pq = 1$$

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

$$\therefore a = \pm b$$

◇

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 $-1, -3, -5, -7$

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 $-1, -3, -5, -7$

0是不是素数？为什么？

定理

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, \dots, 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, \dots, p_n 中的一个, 比如说: $p = p_j$
这样:

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

所以应该有:

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

即: $p \mid 1$. 矛盾. \diamond

类似地, 还可以证明形如 $4k + 3$ 或 $6k + 5$ 的素数有无穷多个, 这里 k 为非负整数.

定理

如果 $p > 1$ 是合数 n 的所有正因子中最小的那一个，那么 p 一定是素数，并且 $p \leq \sqrt{n}$.

证明： 如果 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 ，且 $q < p$. 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.

进一步，还可以将 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：

$$p \leq n_1$$

这样就有：

$$n = p \cdot n_1 \geq p \cdot p = p^2.$$

这个结论给出了最小素因子的一个上界，即 $p \leq \sqrt{n}$. \diamond

推论

对于小于等于 \sqrt{n} 的任意素数 p ，如果 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 来说, 满足 $2 \leq m \leq n$, 所有小于等于 $\sqrt{m}(\leq \sqrt{n})$ 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	

注意，这里漏删了一个3的倍数！

再删去5的倍数:

				7	
11	13			17	19
	23				29
31				37	
41	43			47	49
	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			
		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: $\ln(100) = 4.60517019$, $\frac{100}{\ln(100)} = 21.7147$

进一步还可以证明,

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1.$$

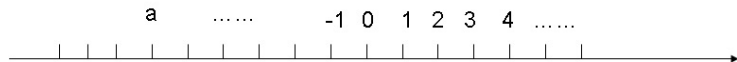
该等式被称为素数定理.

3. 欧几里德除法

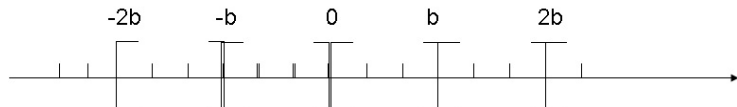
定理

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

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：

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

令 $r = a - bq$ ，则有：

$$a = bq + r, \quad 0 \leq r < b$$

◇

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

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

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 $|b(q - q_1)| \geq b$
但是

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

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**.

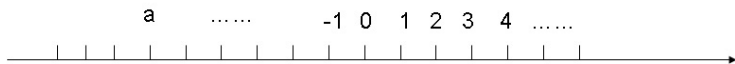
这里的 q 叫做(a 被 b 除所得的)**不完全商**, r 叫做(a 被 b 除所得的)**余数**

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 $r = 0$.

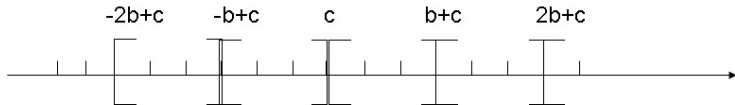
欧几里德除法的变形:

$a \in \mathbb{Z}, b \in \mathbb{Z}^+$, 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

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

绝对值最小余数

$a \in \mathbb{Z}, b \in \mathbb{Z}^+$, 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.

在欧几里得除法的变形形式中, c 取特定的值, 就得到特定的“余数类型”.

例如, 当 $c = 0$, 就是我们最常用的**最小非负余数**.

又例如,

- ① 当 b 为偶数时, 令 $c = -\frac{b}{2}$, 得到 $b + c = \frac{b}{2}$ 以及 $-\frac{b}{2} \leq r \leq \frac{b-2}{2} < \frac{b}{2}$;
- ② 当 b 为偶数时, 令 $c = -\frac{b-2}{2}$, 得到 $b + c = \frac{b+2}{2}$ 以及 $-\frac{b}{2} < -\frac{b-2}{2} \leq r \leq \frac{b}{2}$;
- ③ 当 b 为偶数时, 令 $c = -\frac{b-1}{2}$, 得到 $b + c = \frac{b+1}{2}$ 以及 $-\frac{b}{2} < -\frac{b-1}{2} \leq r \leq \frac{b-1}{2} < \frac{b}{2}$.

总之有,

$$-\frac{b}{2} \leq r < \frac{b}{2} \quad \text{或} \quad -\frac{b}{2} < r \leq \frac{b}{2}.$$

这时的余数 r 叫做**绝对值最小余数**.

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:

$$q = \left[\frac{a}{b} \right] \quad r = a - b \left[\frac{a}{b} \right]$$

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

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

的形式, 这里 $0 \leq a_i < b (i = 1, 2, \dots, k)$.

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:

$$\begin{aligned}n &= bq_0 + a_0 \\&= b(bq_1 + a_1) + a_0 \\&= b^2q_1 + ba_1 + a_0 \\&= b^2(bq_2 + a_2) + ba_1 + a_0 \\&= b^3q_2 + b^2a_2 + ba_1 + a_0 \\&= \dots\dots\dots \\&= b^kq_{k-1} + b^{k-1}a_{k-1} + b^{k-2}a_{k-2} + \dots + ba_1 + a_0 \\&= b^ka_k + b^{k-1}a_{k-1} + b^{k-2}a_{k-2} + \dots + ba_1 + a_0 \\&\quad (0 \leq a_k, a_{k-1}, a_{k-2}, \dots, a_2, a_1, a_0 < b)\end{aligned}$$

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

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

的形式, 这里 $0 \leq a_i < b (i = 1, \dots, k)$. 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

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

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

从而

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

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

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

从而

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

而

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

矛盾!

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

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

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

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

的形式 ($0 \leq a_i < b (i = 1, 2, \dots, k)$), 称为 n 的 b 进制表示.

比如二进制 ($n = 642$):

$$642 = 2 \cdot 321 + 0 \quad (i.e., a_0 = 0)$$

$$321 = 2 \cdot 160 + 1 \quad (i.e., a_1 = 1)$$

$$160 = 2 \cdot 80 + 0 \quad (i.e., a_2 = 0)$$

$$80 = 2 \cdot 40 + 0 \quad (i.e., a_3 = 0)$$

$$40 = 2 \cdot 20 + 0 \quad (i.e., a_4 = 0)$$

$$20 = 2 \cdot 10 + 0 \quad (i.e., a_5 = 0)$$

$$10 = 2 \cdot 5 + 0 \quad (i.e., a_6 = 0)$$

$$5 = 2 \cdot 2 + 1 \quad (i.e., a_7 = 1)$$

$$2 = 2 \cdot 1 + 0 \quad (i.e., a_8 = 0)$$

$$1 = 2 \cdot 0 + 1 \quad (i.e., a_9 = 1)$$

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($= A \cdot 16^6 + B \cdot 16^2 + C \cdot 16^1 + 8 \cdot 16^0$)

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

16进制与2进制相互之间可以比较容易的转换:

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, \dots, a_n , 如果:

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

则称 d 为 a_1, a_2, \dots, a_n 的公因数.

如果 a_1, a_2, \dots, 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, \dots, a_n 的**最大公因数(greatest common divisor, gcd)**, 记做 (a_1, a_2, \dots, a_n) .

按照这个定义, 可以看到, $(a_1, a_2, \dots, a_n) = (a_{i_1}, a_{i_2}, \dots, a_{i_n})(i_1, i_2, \dots, i_n \text{ 从 } 1 - n \text{ 取值各不相同})$.

如果 a_1, a_2, \dots, a_n 的最大公因数为1的话, 称 a_1, a_2, \dots, a_n 互素, 互质.

比如, 14的因数为 $\pm 1, \pm 2, \pm 7, \pm 14$, 21的因数为 $\pm 1, \pm 3, \pm 7, \pm 21$,

它们的公因数为 $\pm 1, \pm 7$, 最大公因数为7

-15和21的公因数为 $\pm 1, \pm 3$, 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, \dots, a_n 的公因数与 $|a_1|, |a_2|, \dots, |a_n|$ 的公因数相同

(3) $(a_1, a_2, \dots, a_n) = (|a_1|, |a_2|, \dots, |a_n|)$

(4) $(a, b) = (a, -b) = (-a, b) = (-a, -b)$

(5) $(0, b) = |b|$

(6) $a = bq + c \implies (a, b) = (b, c)$

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,

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

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

(当然这里也有 $a = bq + c \implies (a, q) = (q, c)$ 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) , 只要求 (b, r_2) .

而要求 (b, r_2) , 可以类似求 (a, b) 的做法:

$$b = r_2q_2 + r_3 \quad (0 \leq r_3 < r_2)$$

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:

$$r_2 = r_3q_3 + r_4 \quad (0 \leq r_4 < r_3)$$

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:

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

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

这时我们知道

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

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 $(-1859, 1573)$

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

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

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

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

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

示例: 求(46480, 39423)

$$46480 = 1 \cdot 39423 + 7057$$

$$39423 = 5 \cdot 7057 + 4138$$

$$7057 = 1 \cdot 4138 + 2919$$

$$4138 = 1 \cdot 2919 + 1219$$

$$2919 = 2 \cdot 1219 + 481$$

$$1219 = 2 \cdot 481 + 257$$

$$481 = 1 \cdot 257 + 224$$

$$257 = 1 \cdot 224 + 33$$

$$224 = 6 \cdot 33 + 26$$

$$33 = 1 \cdot 26 + 7$$

$$26 = 3 \cdot 7 + 5$$

$$7 = 1 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

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

注: 求 a_1, a_2, \dots, a_n 的最大公因数

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

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

$$d_5 = (d_4, a_5)$$

.....

最后求出

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

则有

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

注: 给定两个正整数 a, b , 利用欧几里德除法我们知道:

$$\begin{aligned}\exists q \in \mathbb{Z}, r(0 \leq r < b), s.t., a = bq + r &\implies 2^a = 2^r \cdot 2^{bq} \\ &\implies 2^a - 1 = 2^r(2^{bq} - 1) + (2^r - 1) \\ &\implies 2^a - 1 = 2^r(2^b - 1)(q_1) + (2^r - 1) \\ &\implies 2^a - 1 = (2^b - 1)(2^r \cdot q_1) + (2^r - 1) \\ &\implies 2^a - 1 = (2^b - 1)q' + (2^r - 1) \quad (q' \in \mathbb{Z}, 0 \leq 2^r - 1 < 2^b - 1)\end{aligned}$$

令 $a = r_0$, $b = r_1$, 下面反复利用这个事实, 我们有

$$a = bq + r_2(0 \leq r_2 < b) \implies 2^a - 1 = (2^b - 1)q'_1 + (2^{r_2} - 1)(0 \leq 2^{r_2} - 1 < 2^b - 1)$$

类似地, 我们得到:

$$b = r_2q_2 + r_3(0 \leq r_3 < r_2) \implies 2^b - 1 = (2^{r_2} - 1)q'_2 + (2^{r_3} - 1)(0 \leq 2^{r_3} - 1 < 2^{r_2} - 1)$$

$$r_2 = r_3q_3 + r_4(0 \leq r_4 < r_3) \implies 2^{r_2} - 1 = (2^{r_3} - 1)q'_3 + (2^{r_4} - 1)(0 \leq 2^{r_4} - 1 < 2^{r_3} - 1)$$

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 $2^{r_i} - 1 \neq 0$.

最终在我们到达 a 与 b 的最大公因数 $r_n = (a, b)$ 的时候, 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

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

反之, 如果 $2^a - 1$ 与 $2^b - 1$ 互素的话, 有

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

即

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