因数与因式

2023 年 4 月 20 日

目录

1 最大公因子

为了描述，我们需要引入一个新的集合，不同于我们已经讲了的整数集和自然数集，还有一个Q =所有有理数（分数）的集合。即所有形如a/b的数。其中a, b是整数且$b \neq 0$，还有R =所有实数的集合，C = 所以复数的集合。

然后我们介绍一下经常用的

长除法 长除法指的是用非0整数a除以整数b得到

$$\frac{b}{a} = q + \frac{r}{a}$$

其中q是整数且$0 \leq r/a < 1$

1.1 除法算式

给定整数a, b且$a \neq 0$，则存在唯一的整数q, r满足

$$b = qa + r,\ 0 \leq r < |a|$$

证明：先证明$a > 0,\ b \leq 0$的情况。

设集合C为所有形如$b - na$的非负整数构成的集合，其中$n \geq 0$，因为由假设可得$b = b - 0a \in C$。由于假设了$b \geq 0$，所以$C \neq \emptyset$，由最小原理可得C有一个最小元。我们设为$r = b - qa(q \geq 0)$，有$r \geq 0$，假设$r \geq a$，那么有

$$b - (q+1)a = b - qa - a = r - a \geq 0$$

那么r在这个时候不是最小整数，矛盾。所以$0 \leq r < a$

现在我们来证明唯一性。我们假设b存在两个不同的分解，有

$$b = qa + r = q'a + r'$$

其中$0 \leq r,,r' < a$那么

$$(q-q')a = r' - r$$

不妨有$r' \geq r$，那么$r' - r \geq 0$有$q - q' \geq 0$ 假设$q \neq q'$，则有$q - q' \leq 1$（因为q, q'为整数），现在因为有$a > 0$，所以

$$(q-q')a \geq a$$

另一方面，我们有$r' < a$，那么

$$r' - r < a - r \leq a$$

得到$(q-q')a \geq a$而$r' - r < a$，那么我们得到了一个矛盾。为此$q = q'$且$r = r'$

1.2 定义：商和余数

设$a, b \in Z$且$a \neq 0$，那么除法算式中的整数q, r分别称为a除b的商和余数。

1.3 推论：素数存在无穷多个

证明：我们只假设素数存在有限多个，我们取$p_1, \cdots, p_k$表示所有的素数，那么定义$M = p_1p_2 \cdots p_k + 1$，那么由因式分解可知，$M$要么是一个素数，要么是一个素数的乘积。但是由假设有M不是素数，且没有任何的素因子p_i，因为任意的$p_i, i = 1, 2, 3, \cdots$都不整除M，得到的余数永远是1，为此由长除法可得，商和余数分别为$p_1 \cdots p_k$和1，而$r = 1 \neq 0$这说明不存在一个素因子p_i为M的因子，矛盾。所以素数存在无限多个。

1.4 整除

设a, b为整数，若存在整数d使得$b = ad$，那么a为b的一个因子（也

称为a整除b，或者说b是a的倍数），记作

$$a|b$$

例如$3|6$，但是$3\not|5$，前者是因为3是6的一个因子，后者不是。

1.5 定义：最大公因子

若整数c满足$c|a, c|b$，则c为整数a, b的公因子，a, b的最大公因子记为$gcd(a, b)$，我们有时候也记为(a, b)。定义为

$$\gcd(a,b) = \begin{cases} 0, & a = 0 = b \\ a, b\text{最大公因子} & \text{其他} \end{cases}$$

1.6 命题：公因子和素数

设p为素数，b为任意整数，那么

$$\gcd(p,b) = \begin{cases} p & p|b \\ 1 & p\not|b \end{cases}$$

显而易见有：当$p|b$的时候，p是b的一个公因子，而且p的因子只有自身和1，所以$(p, b) = p$，当$(p, b) = 1$的时候，p不整除b，则p不是b的因子，最大共因数只有1

1.7 线性组合

定义：整数a, b的一个线性组合指的是形如

$$sa + tb$$

的整数，其中s, t为整数

1.8 定理：a, b如果是整数，那么$\gcd(a, b)$为线性组合

证明：我们假设a, b至少有一个不为0，构造集合

$$I = \{sa + tb : s, t \in Z\}$$

有$a \in I$（取$s = 1, t = 0$即可得到），$b \in I$（$(s = 0, t = 1)$。那么可知所有的正整数构成集合I，且根据最小元素可知，集合I存在一个最小正整数。我们设为d。且我们断言d是a, b的最大公因数。

因为$d \in I$，为此d是一个线性组合（关于a, b的）那么存在整数s, t使得

$$d = sa + tb$$

为了得到线性组合，我们利用长除法，那么$a = qd + r$其中$0 \leq r < d$，若$r > 0$有

$$r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b \in P$$

我们得到一个矛盾，最小元不是d是r。为此$r = 0$且$d|a, d|b$ 若c是a, b的一个公因子，那么$a = ca'$, $b = cb'$则$d = sa + tb = c(sa' + tb')$，所以$c|d$。因为$c|d$那么$|c| \leq d$，所以$d$才是$a, b$的最大公因子。，这是一个求公因数很好的方法，因为整数a, b的最大公因数d可被写为线性组合$d = sa + tb$。

1.9 推论：I,Z

设I是Z的一个子集，满足

1. $0 \in I$
2. 若$a, b \in I$则$a - b \in I$
3. 若$a \in I, q \in Z$有$qa \in I$

1.10 欧几里得引理

若p是素数且$p|ab$，那么$p|b$或者$p|a$，更一般的，若p整除$a_1a_2\cdots a_n$，则p至少整除其中一个因子。反之，若整数$m \geq 2$满足：当$m|ab$时总有$m|a$或者$m|b$，那么m是一个素数。

证明：假设$p \nmid a$，那么我们要证明的是$p|b$。我们已经有$\gcd(a,p)=1$，那么由定理1.8就有

$$1 = sp + ta,\ s,t \in Z$$

和

$$b = spb + tab$$

因为$p|ab$，那么存在c使得分解$ab = pc$成立，因此

$$b = spb + tpc = p(sb + tc)$$

为此，$p|b$成立。

另一方面，我们设m是合数，且$m = ab$其中$a < m, b < m$，有$m|ab$，那么由题可知$m|a$或者$m|b$。但因为$a < m$和$b < m$，则$m \nmid a, b$。矛盾。

欧几里得在一般情况下不成立，如果p不是素数，那么举反例有$6|12$但$6 \nmid 4$和$6 \nmid 3$

1.11 命题：若p是素数，则$p|\binom{p}{j}$

若p是素数，则$p|\binom{p}{j},\ 0 < j < p$

在上一章有另一个习题，但和命题是反过来的，即证明$\binom{n}{j}|n$。但现在先让我们看看

$$\left(\begin{array}{c} n \\ j \end{array} \right) = \frac{n!}{(n-j)!\cdot j!} = \frac{p(p-1)\cdots(p-j+1)}{j!}$$

有

$$j! \left(\begin{array}{c} n \\ j \end{array} \right) = p(p-1)\cdots(p-j+1)$$

那么$p|j!\binom{p}{j}$，如果$p|j!$那么由欧几里得引理可知p肯定整除其中的某个因子。但题目已经有$0 < j < p$，为此每个j都严格小于p，所以p不整除任意一个$j!$中的元素。但$p \nmid j!$，又因为$p|j!\binom{p}{j}$，所以p一定整除$\binom{n}{j}$

命题的一些其他情况呢？考虑$p=4, j=2$的情况，有$\binom{4}{2}=6$但是$4 \nmid 6$，所以p是素数是必要的。

1.12 定义：互素的公因子为± 1

推论： 设a, b, c为整数，若c, a互素且$c|ab$，那么$c|b$

1.13 引理：每个非零有理数r都有既约表达式

既约表达式 若a, b互素，那么有理数a/b的表达式是既约的

因为r为有理数，那么存在整数$a.b$使得$r = a/b$，若$d = (a, b)$，那么有$a = a'd,\ b = b'd$。则$a/b = a'd/b'd = a'/b'$，其中$(a', b') = 1$ 而当$d' > 1$的时候存在d'为a', b'的一个因子使得$d'd > d$为a, b的一个更大的公因子，这与我们的题设矛盾。

1.14 命题：$\sqrt{2}$是无理数

设$\sqrt{2}$是有理数，那么$\sqrt{2} = \frac{a}{b}$其中$(a, b) = 1$。两边平方有$2 = a^2/b^2 \Rightarrow 2b^2 = a^2$，那么$a^2$是一个偶数，有$(2m)^2 = a^2 = 2b^2$得到$2m^2 = b^2$这说明$b^2$是可以被2整除的，但与$(a, b) = 1$是个矛盾，所以$\sqrt{2}$不可能是一个有理数

1.15 欧几里得算法

设a, b是正整数，则存在求最大公因子$d = (a, b)$的一种算法，且存在整数s, t使得$d = sa + tb$的算法

关于命题的下半段我们已经证明了存在性。现在我们先来看看怎么描

述定理我们令$b = r_0,$, $a = r_1$，那么对每个整数q_i和r_i和方程有

$$\begin{aligned} b =& q_1 a + r_2, & r_2 < a \\ a = r_1 =& q_2 r_2 + r_3, & r_3 < r_2 \\ \cdots & & \\ r_{n-3} =& q_{n-2} r_{n-2} + r_{n-1}, & r_{n-1} < r_{n-2} \\ r_{n-2} =& q_{n-1} r_{n-1} + r_n, & r_n < r_{n-1} \\ r_{n-1} =& q_n r_n & \end{aligned}$$

由推论1.8可知最大公因式是最后的余数。为了方便，重写等式的记号。最前的两个等式为

$$\begin{aligned} b =& qa + r \\ a =& q' r + s \end{aligned}$$

若c为a, b的公因子，那么由等式有$c|r$和$c|s$（因为 $c|a, c|r$，所以$c|s$），因此一值看到最后c都整除每个余数。特别的$c|d$。

然后我们重写后面的几个等式

$$\begin{aligned} f =& ug + h \\ g =& u' h + k \\ h =& u'' k + d \\ k =& vd \end{aligned}$$

由最后的等式可知$d|k$，所以$d|h$，因为$d|k, d|h$那么$d|g$以此类推得到$d|a, d|b$。所以d是一个公因子。若c是任意一个公因子，那么$c|d$，所以$d = (a, b)$

为了将d表示成线性组合，我们重写等式有

$$\begin{aligned} d =& h - u'' k \\ =& h - u''(g - u' h) \\ =& (1 + u'' u') h - u'' g \end{aligned}$$

然后只需要不断的重复这个式子直到用d写成了a, b表示的线性组合即可。

1.16 拉梅定理

设$b \geq a$为正整数，$d(a)$是a的十进制表示中数字的个数。若n是用欧几里得算法计算最大公因子(a,b)的步数，则

$$n \leq 5d(a)$$

证明：我们在欧几里得算法的证明中用r_0表示b，用r_1表示a，就使得有一个通项公式表达等式，即

$$r_j = r_{j+1}q_{j+1} + r_{j+2}$$

（除了最后一个等式），即

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

注意的是$q_n \geq 2$，若$q_n \leq 1$，那么就存在$r_{n-1} \leq r_n$，这说明了一种情况，没有除干净。与$r_n < r_{n-1}$矛盾。类似的，任意的$q_i, i = 1,2,3,\cdots,n-1 \geq 1$，由于每个$q_i, r_i$都是整数，那么当$q < 1$的时候存在$q_j = 0$使得$r_{j+1} = r_{j-1}$这与我们的严格不等式$r_n < r_{n-1} < \cdots < r_1 = b$矛盾。

现在我们需要利用一些斐波那契数列，回忆一下，斐波那契数列是指

$$F_0 = 0.F_1 = 1, F_n = F_{n-1} + F_{n-2}, \quad n \geq 2$$

现在有

$$r_n \geq 1 = F_2$$

由于$q_n \geq 2$

$$r_{n-1} = r_n q_n \geq 2r_n \geq 2F_2 \geq 2 = F_3$$

然后我们要对$j \geq 0$应用归纳法证明

$$r_{n-j} \geq F_{j+2}$$

由归纳假设有

$$\begin{aligned} r_{n-j-1} =& r_{n-j}q_{n-j} + r_{n-j+1} \\ \geq& r_{n-j} + r_{n-j+1} \qquad \text{因为} q_{n-j} \geq 1 \\ \geq& F_{j+2} + F_{j+1} = F_{j+3} \end{aligned}$$

那么$a = r_1 = r_{n-(n-1)} \geq F_{n-1+2} = F_{n+1}$，由推论：斐波那契不等式[1]可知$F_{n+1} > \gamma^{n-1}$其中$\gamma = \frac{1}{2}(1+\sqrt{5})$。那么$a > \gamma^{n-1}$，然后

$$\log_{10}\gamma > \log_{10}(1.6) > \frac{1}{5}$$

那么

$$\log_{10}(a) > (n-1)\log_{10}\gamma > (n-1)/5$$

因此

$$n - 1 < 5\log_{10} a < 5d(a)$$

其中$d(a) = \lfloor \log_{10} a \rfloor + 1$，因为$d(a)$是整数，所以$5d(a)$也是整数。有$n \geq 5d(a)$

例如：为了计算$d(78)$，$d(78) = 2$(因为$\log_{10}(78) = 1.8\cdots$)，所以计算该最大公因式至少要10步。但实际上只需要5步

1.17 命题：每个正整数都可以表示成一个多项式

若$b \geq 2$，则每个正整数m都有以b为底数的表达式，即存在整数$d_i, 0 \leq d_i < b$，使得

$$m = d_k b^k + d_{k-1} b^{k-1} + \cdots + d_0$$

并且，$d_k \neq 0$，则表达式是唯一的。数$d_k, d_{k-1}, \cdots, d_0$称为$m$的b-进位数。

例如：整数5754可以表达为

$$5 \times 10^3 + 7 \times 10^2 + 5 \times 10 + 4$$

每个关于10的幂次都带有一个常数，这个常数我们叫10−进位数。因为每个幂次都是代表了个十百千的位数。这个数是10，所以叫10−进位数。

[1]对于整数$n \geq 3$有$F_n > \gamma^{n-2}, \gamma = \frac{1}{2}(1+\sqrt{5})$

证明：对于每个a_i和d，我们利用长除法就有

$$\begin{aligned} m =& a_0 b + d_0 \quad 0 \leq d_0 < b \\ a_0 =& a_1 b + d_1 \quad 0 \leq d_1 < b \\ a_1 =& a_2 b + d_2 \quad 0 \leq d_2 < b \\ \cdots \end{aligned}$$

现在我们把每个元素给替换回去归纳有

$$\begin{aligned} m =&(a_1 b + d_1)b + d_0 && = a_1 b^2 + b d_1 + d_0 \\ m =&((a_2 b + d_2)b + d_1)b + d_0 && = a_2 b^3 + d_2 b^2 + d_1 b + d_0 \\ \cdots \\ m =& b^{i+1} a_i + b^i d_i + b^{i-1} d_{i-1} + \cdots + b d_1 + d_0 \end{aligned}$$

那么就存在一个整数k满足$b^k \leq m < b^{k+1}$，对于这个大于m的b^{k+1}，它的系数$a_k = 0$，否则若$a \neq 0$则有$a_k \geq 1$且$m \geq b^{k+1} a_k \geq b^{k+1}$表示$b^{k+1}$是小于$m$的，矛盾。所以

$$m = b^k d_k + b^{k-1} d_{k-1} + \cdots + b d_1 + d_0$$

在证明唯一性之前，我们有对所有的i存在$0 \leq d_i < b$，则

$$\sum_{i=0}^{k} d_i b^i \leq \sum_{i=0}^{k} (b-1) b^i = \sum_{i=0}^{k} b^{i+1} - \sum_{i=0}^{k} b^i = b^{k+1} - 1 < b^{k+1}$$

我们对$k \geq 0$用归纳假设，若$b^k \leq m < b^{k+1}$,，那么表达式$m = \sum_{i=0}^{k} d_i b^i$中的$b-$进位数由$m$唯一确定，设

$$m = \sum_{i=0}^{k} d_i b^i = \sum_{i=0}^{k} c_i b^i$$

那么对所有的i存在$0 \leq d_i < b$和$0 \leq c_i < b$，有

$$\sum_{i=0}^{k} (d_i - c_i) b^i = 0$$

然后我们还得做一个步骤，由于等式中可能出现$d_j = c_i$，和$d_i < c_j$或者$d_j > c_i$诸如此类可能会产生负项的情况。为此，排除所有的$d_i - c_j = 0$和负选项（颠倒顺序）得到一个等式

$$L = \sum_{i \in I} (d_i - c_i) b^i = \sum_{j \in J} (c_j - d_j) b^j = R$$

其中所有的系数经过调整之后都是正数，且I,J这两个指标集不相交，有$I\cap J=\emptyset$。设I中最大元为p。而q为J中的最大元。由于I,j不相交。我们假设$q<p$，那么L中含有b^p，系数也不为0，则$L\geq b^p$，但根据假设又有$R<b^{q+1}\leq b^p$矛盾。为此$b-$进位数是唯一确定的。

2 习题

2.1 1

不用欧几里得引理而用命题整数的分解来证明根号2是无理数我们引入一个命题：奇数的平方还是奇数。

证明：形如$2k+1,k\in Z$的叫奇数，那么$(2k+1)^2=4k^2+4k+1$前面两个都是偶数，还多了个1项，这表明奇数的平方不被2整除，为此奇数的平方确实是奇数。同样的，偶数的平方也是偶数，$(2k)^2=4k$被2整除。

为此，对于每个有理数都可以表示为a/b的既约真分数。如果$\sqrt{2}$是有理数，不妨假设$\sqrt{2}=a/b$，$a,b\in Z$我们假设b是偶数而a是奇数，那么

$$\begin{aligned}2=&a^2/b^2\\2b^2=&a^2\end{aligned}$$

由命题可知a是奇数，那么a^2也是奇数，我们的证明出现了a^2是偶数的情况，即可被2整除，为此得到一个矛盾。$\sqrt{2}$不可能是有理数。

2.2 2

证明：若d,d'互相整除且是非零整数，那么$d'=\pm d$

解：由题有$d=qd'$和$d'=pd$其中p,q是一个整数。那么$qd'-pd=d-pd=0$当$p=1$或者$d=0$的时候满足条件，但$d',d\neq 0$，所以$p=1$，为此$d'=d$。另一种情况，对于$p=-1$则有$d-(-1)(-d')=d-d=0$成立。所以$d'=\pm d$

2.3 3

证明：每个正整数m都可以表示成2的不同幂的和，且表示法是唯一的。每个$m\geq 1$存在分解

$$m=m_1 2+d_1\quad 0\leq d_0<2$$

其中a_0为奇数，且该分解是唯一的。则继续分解有

$$\begin{aligned} m_1 =& m_2 2 + d_2 \qquad 0 \le d_1 < 2 \\ &\cdots \\ m_n =& m_{n+1} 2 + d_n \quad 0 \le d_n < 2 \end{aligned}$$

那么整合就得到

$$m = 2^{i+1}d_i + 2^i d_i \cdots + bd_1 + d_0$$

那么对于某个$2^{k+1} > m \ge 2^k$有系数$d_k = 0$，那么这说明每个m都可以被表示成

$$m = d_k 2^k + \cdots + d_1 2 + d_0$$

成立。

2.4 4

若F_n表示斐波那契数列的第n项，证明对所有$n \ge 1$，F_{n+1}和F_n互素。

对于斐波那契数列有

$$F_n = F_{n-1} + F_{n-2}$$

给出一个定义来辅助证明：设$a_1, a_2, \cdots, a_n$是整数，若整数c满足对所有i都有$c|a_i$，那么c是$a_1, a_2, \cdots, a_n$的一个公因子，而最大的一个公因子记为$(a_1, a_2, \cdots, a_n)$

设整数$a \ge 1$是一个关于F_{n+1}的公因子，那么$a|F_{n+1} \Rightarrow a|F_n, a|F_{n-1}$，那么一直除就存在

$$\begin{aligned} &a|F_n \Rightarrow a|F_{n-1},\ a|F_{n-2} \\ &a|F_{n-1} \Rightarrow a|F_{n-2}, a|F_{n-3} \\ \cdots& \\ &a|F_2 \Rightarrow a|F_1 = a|1, a|F_0 = a|1 \end{aligned}$$

而$a|F_1 = a|1$，但1不能被任意除了自身之外的数整除，矛盾。

所以$(F_{n+1}, F_n) = 1$