算数基本定理

2023 年 4 月 24 日

目录

1 算数基本定理

1.1 算数基本定理

每个整数$a \geq 2$或是素数，或是素数的积，而且，若a有分解式

$$a = p_1 \cdots p_m \text{和 } a = q_1 \cdots q_n$$

其中$p_i, q_j, i = 1, 2, 3, \cdots, m,\ \ j = 1, 2, \cdots, n$都是素数，那么$n = m$，且对下标$i, j$重新编排则可以使所有$i$有$q_i = p_i$

定理是说：每个分解是唯一的，如果不唯一，则只是每个素数所在的位置对应的素数不一样。重新排列就是一样的式子了

证明：我们假设$m \geq n$，对m应用归纳法当$m = 1$的时候$a = p_1 = q_1$成立。而由等式可知，$p_m | q_1 \cdots q_n$，那么由欧几里得引理可知，p_m整除某项q_i，由于q_i是素数。那么$p_m = q_i$，为此我们整理，不妨假设$q_n = p_m$，消去后剩下

$$p_1 \cdots p_{m-1} = q_1 \cdots q_{n-1}$$

现在再由归纳假设有$n - 1 = m - 1$，那么只需要对式子重新排列就使得对所有i有$q_i = p_i$

1.2 推论：整数分解定理

若$a \geq 2$是整数，则存在唯一的相异素数p_i和唯一的整数$\epsilon_i > 0$使得

$$a = p_1^{\epsilon_1} \cdots p_n^{\epsilon_n}$$

证明：我们只需要把分解中相同的素数合在一起即可。

1.3 推论：上述式子的有理数分解是唯一的

每个正有理数$r \neq 1$有唯一分解式子

$$r = p_1^{g_1} \cdots p_n^{g_n}$$

证明：我们设$r = a/b$，$a, b \in Z$，若存在$a = p_1^{l_1} \cdots p_n^{l_n}$,$b = p^{f_1} \cdots p_n^{f_n}$，那么$r = p_1^{g_1} \cdots p_n^{g_n}$，其中$g_i = e_i - f_i$。在等式中，我们是允许指数为0的情况出现的。那么由于指数为0，就可以假设等式存在相等的素数，例如$168 = 2^3 3^1 7^1 = 2^3 3^1 5^0 7^1$，$60 = 2^2 3^1 5^1 = 2^2 3^1 5^1 7^0$，这样子就能把元素一一对应。若$g_i = 0$，则我们消掉$p^{g_i}$得要证的分解式子。

另一个方面，我们假设

$$r = p_1^{k_1} \cdots p^{k_n}$$

跟上面一样，我们允许指数为0的情况，那么可以把素数一一对应起来。如果有必要，我们可以重排下标，我们假设对某个j有$g_j \neq h_j$，不妨假设$j = 1, g_1 > h_1$那么

$$p_1^{g_1 - h_1} p_2^{g_2} \cdots p_n^{g_n} = p_2^{h_2} \cdots p_{h_n}^{n}$$

现在，因为某些指数可能是负数，所以是一个有理数等式，现在只需要交叉相乘就能得到整数的形式。但左边含有p_1右边不含，这与算数基本定理矛盾。所以表示是唯一的。

若r的分解式中所有指数为整数，那么r就是一些整数的乘积，所以r是正数，反之，由于r是整数，那么素数分解的指数都是正数。

1.4 引理

设正整数a, b的素数分解式子为

$$a = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},\ \ b = p_1^{f_1} \cdots p_n^{f_n}$$

其中，$p_1, \cdots, p_n$是互异的素数。对所有$i, e_i, f_i \geq 0$，$a|b$当且仅当对所有i，$e_i \leq f_i$

对于所有的$i, e_i \leq f_i$，那么$b = ac$设c的分解式子为$c = p_1^{f_1 - e_1} \cdots p_n^{f_n - e_n}$，而$f_i - e_i \geq 0, i = 1, 2, \cdots, n$，由推论1.3可知$c$是整数,那么$a|b$ 反之，对

于$b=ac$，我们设一个c的素分解为$c=p_1^{g_1}\cdots p_n^{g_n}$,而$g_i\geq 0,\ i=1,2,\cdots,n$,，那么由算数基本定理可知$e_i+g_i=f_i$，那么对所有$i$都有$f_i-e_i=g_i\geq 0\Rightarrow f_i\geq e_i$证毕。

1.5 定义 公倍数

设a,b是整数，若整数m满足$a|m$和$b|m$，则说m是a,b的一个公倍数，若$a\neq 0,b\neq 0$，那么a,b的最小公倍数就是指最小的正公倍数，如果a,b有一个是0，那么最小公倍数是0，而a,b的最小公倍数记作$lcm(a,b)$或者记为$[a,b]$

更一般的，我们设$a_1,\cdots,a_n$是整数，$n\geq 2$，若整数m满足对所有i有$a_i|m$，那么m是$a_1,\cdots,a_n$的一个公倍数。若$a_i\neq 0$，那么最小的公倍数指的是最小的正公倍数。否则，最小公倍数就是0，而最小公倍数记为

$$[a_1,\cdots,a_n]$$

1.6 命题

设$a=p_1^{e_1}\cdots p_n^{e_n}$，$b=p_1^{f_1}\cdots p_n^{f_n}$其中$p$为互异的素数。设$e_i,f_i\geq 0,i=1,2,3,\cdots,n$，定义

$$m_i=\min\{e_i,f_i\},\ \ M_i=\max\{e_i,f_i\}$$

则

$$gcd(a,b)=p_1^{m_1}\cdots p_n^{m_n},\ \ lcm(a,b)=p_1^{M_1}\cdots p_n^{M_n}$$

证明：设$d=p_1^{m_1}\cdots p_n^{m_n}$，那么是可以被整除的由于$d$取的是指数最小的素数，我们假设这个数是$e_i$，那么$f_i-e_i\geq 0$是一个整数，且$e^i$为指数的素数可以被自己整除，由引理1.4可知$d$是$a,b$的公因子（正的）。而且，若$c$是一个$a,b$任一公因子，设$c=p_1^{g_1}\cdots p_n^{g_n}$有$0\leq g_i\leq \min\{e_i,f_i\}=m_i,i=1,2,3,\cdots,n$那么$c|d$

对于另一个方面。我们有

$D = p_1^{M_1} \cdots p_n^{M_n}$为$a, b$的公倍数。由于我们取的是最大的，有定义1.5可知$D$是$a, b$的公倍数，因为$M_i$是最大的对于每个$e_i, f_i$都有$M_i - e_1 \geq 0$和$M_i - f_i \geq 0$是整数。且对于其他的公倍数$C$，设$C = p_1^{G_1} \cdots p_n^{G_n}$，由于$0 \geq G_i \geq M_i$，那么$C|D$成立。为此可以整除$a, b$的其他任意公倍数。

1.7 命题

若a, b是正整数，则

$$lcm(a, b)gcd(a, b) = ab$$

证明：对于m_i和M_i有

$$m_i + M_i = e_i + f_i$$

其中$m_i = \min\{e_i, f_i\}$而$M_i = \max\{e_i, f_i\}$ 运用命题1.6有

$$\begin{aligned} lcm(a, b)gcd(a, b) =& p_1^{m_1} \cdots p_n^{m_n} p_1^{M_1} \cdots p_n^{M_n} \\ =& ab \end{aligned}$$

为此，其中的差别只是些许符号的不同，而每个元素取自a或者b。只需要重新排列就可以得到$lcm(a, b)gcd(a, b) = ab$

2 习题

2.1 1

判断对错

1. $|2^{19} - 3^{12}| < \frac{1}{2}$ 错
2. 若$r = p_1^{e_1} \cdots p_n^{e_n}$，其中$p_i$是互异的素数，且$e_i$是整数，则$r$是一个整数当且仅当每个$g_i$都是非负的。 对
3. 若a, b互素，则$(a^2, b^2) = 1$ 对

1 我们不妨把式子更改为

$$|19\ln(2) - 12\ln(3)| < \ln(1) - \ln(2)$$

$\ln(2) \approx 0.69$，而$\ln(3) \approx 1.09$ 那么粗略计算题目就是在求

$$|13.17 - 13.18| < \ln(1) - \ln(2)$$

那么还原回去就是$1/e^{0.01} < 1/2$矛盾，因为等式左边是0.99

2 由推论1.3可知对于$e_i > 0$的成立，其中考虑$g_i = 0$的情况，这个时候$r = 1$是整数，所以综上所述命题成立。

3 由$(a,b) = 1$就有$(a^2,b) = 1$否则存在一个素数$p|a, p|b$矛盾，那么进一步的有$(a^2,b^2) = 1$，否则存在其的一个公因子的一个素因子整除a, b矛盾。

4

1. 证明整数$m \geq 2$是一个完全平方数当且仅当它的每个素因子出现偶数次
2. 若m是一个正整数且$\sqrt{m}$是有理数，那么m是一个完全平方数，由此知若m不是完全平方数，则$\sqrt{m}$是无理数。

1 我们假设$m = p_1^{e_1} \cdots p_n^{e_n}$是一个素分解，且$p_i, i = 1,2,3,\cdots,n$是互异的素数且$e_i$是整数，若$m$不是一个完全平方数，则存在某个$\frac{1}{2}e_i$不是整数，为此对于某个奇数$e_i$都不是一个完全平方数。而对于每个$e_i = 2k$有$1/2e_i = k$，$k$是整数有$m$是一个开方后为完全平方数的整数。证毕

2 由题有：若$\sqrt{m}$是有理数，且m是整数，那么$\sqrt{m} = \frac{p}{q}$，其中p, q是整数且$\sqrt{m}$是既约真分数，有$m = \frac{p^2}{q^2}$为整数，由习题1的第三个小题可知$(p^2, q^2) = 1$得到$q^2 = 1$。所以$\sqrt{m}$是一个整数。再由第一问的结论有当m是完全平方数的时候是次数都是偶次可知，若m是一个整数且它的完全平方数是有理数，那么$\sqrt{m}$一定是整数。就有$\sqrt{m}$如果不是一个完全平方数，那么$\sqrt{m}$是无理数。

2.2 5

设$n=p^r m$，其中p是素数但不能整除$m\geq 1$，证明$p\nmid\binom{n}{p^r}$

$$\binom{n}{p^r}=\binom{p^r m}{p^r}=\frac{(p^r m)!}{p^r!(p^r m-p^r)!}$$

为此，我们的关注点主要是n中含有多少个p相关的因子。设p整除$p|\binom{n}{p^r}$那么p至少整除其中一个因子。

考虑一个简单例子：10!中有多少个2的因子，3呢？当我们利用取整符号，即$\lfloor 10/2\rfloor=5$，这说明存在5个可以被2整除的数，更一般的，$10/2^2=2$存在2个可以被整除的数字。但最多到3，也就是$10/2^3=1$。那么2在10!中的因子一共有5+2+1 $=8$个，以此类推，3在10中的因子个数有$\sum_{i=1}^{2}10/3=4$存在4个，那么得到一个新的定理——阶乘分解

$n!$中含有素因子p的个数为

$$\sum_{t>0}\left\lfloor\frac{n}{p^t}\right\rfloor$$

我们要证明的就是，看是分子的素因子个数多还是分母的多，如果是分母的多或者是存在一样的个数，那么就没办法整除。即证

$$\sum_{t>0}\left\lfloor\frac{p^r m}{p^t}\right\rfloor-\sum_{t>0}\left\lfloor\frac{p^r}{p^t}\right\rfloor-\sum_{t>0}\left\lfloor\frac{p^r(m-1)}{p^t}\right\rfloor>0$$
$$\text{或者}\sum_{t>0}\left\lfloor\frac{p^r m}{p^t}\right\rfloor-\sum_{t>0}\left\lfloor\frac{p^r}{p^t}\right\rfloor-\sum_{t>0}\left\lfloor\frac{p^r(m-1)}{p^t}\right\rfloor\leq 0$$

那么有

$$\begin{aligned}&\sum_{t>0}\left\lfloor\frac{p^r m}{p^t}\right\rfloor-\sum_{t>0}\left\lfloor\frac{p^r}{p^t}\right\rfloor-\sum_{t>0}\left\lfloor\frac{p^r(m-1)}{p^t}\right\rfloor\\&=\sum_{t>0}\left\lfloor mp^{r-t}\right\rfloor-\sum_{t>0}\left\lfloor p^{r-t}\right\rfloor-\sum_{t>0}\left\lfloor(m-1)p^{r-t}\right\rfloor\\&=\sum_{t>0}\left\lfloor mp^{r-t}\right\rfloor-\left(\sum_{t>0}\left\lfloor p^{r-t}+(m-1)p^{r-t}\right\rfloor\right)\\&=\sum_{t>0}\left\lfloor mp^{r-t}\right\rfloor-\sum_{t>0}\left\lfloor mp^{r-t}\right\rfloor=0\end{aligned}$$

其中包括当$t>r$的情况，对于$t>r$有$\lfloor m/p^{t-r}\rfloor=\lfloor(m-1)/p^{t-r}\rfloor$，因为$p\nmid m$取整后得到相等。而分母的因子$p^r/p^t$因为是一个小数直接取0即可

（$t > r$）。综上所述分子分母包含素因子个数是一样的，消去之后剩下的项不能整除p，所以$p \nmid \binom{n}{p^r}$

2.3 命题

给定整数$m \geq 0$

1. 若$a_i \equiv a' \pmod m, i = 1, 2, 3, \cdots, n$，则

$$a_1 + \cdots + a_n \equiv a_1' + \cdots + a_n' \pmod m$$

   特别的，若$a \equiv a' \pmod m$，$b \equiv b' \pmod m$，则

$$a + b \equiv a' + b' \pmod m$$

2. 若$a_i \equiv a_i' \pmod m$