CyanMath: 创美营讲义（数学）

LeyuDame

2024 年 12 月 2 日

目录

第一章　因式分解技巧

什么是因式分解

在小学里, 我们学过整数的因数分解. 由乘法, 得

$$3 \times 4 = 12$$

反过来, 12 可以分解: $12 = 3 \times 4$.

当然, 4 还可以继续分解为 2×2 . 于是得

$$12 = 3 \times 2 \times 2$$

这时 12 已经分解成质因数的乘积了.

同样地, 由整式乘法, 得

$$(1+2x)\left(1-x^2\right) = 1+2x-x^2-2x^3$$

反过来, $1+2x-x^2-2x^3$ 可以分解为两个因式 $1+2x$ 与 $1-x^2$ 的乘积, 即

$$1+2x-x^2-2x^3 = (1+2x)\left(1-x^2\right)$$

$1-x^2$ 还可以继续分解为 $(1+x)(1-x)$. 于是

$$1+2x-x^2-2x^3 = (1+2x)(1+x)(1-x)$$

这里 x 的一次多项式 $1+2x, 1+x, 1-x$ 都不能继续分解, 它们是不可约多项式, 也就是既约多项式. 所以, $1+2x-x^2-2x^3$ 已经分解成质因式的乘积了.

把一个整式写成几个整式的乘积, 称为因式分解, 每一个乘式称为积的因式.

在因式分解中, 通常要求各个乘式 (因式) 都是既约多项式, 这样的因式称为质因式.

因式分解的方法, 我们将逐一介绍.

1.1　提公因式

学过因式分解的人爱说: "一提、二代、三分组."

"提" 是指 "提取公因式". 在因式分解时, 首先应当想到的是有没有公因式可提.

几个整式都含有的因式称为它们的公因式.

例如 $ma, mb, -mc$ 都含有因式 m, m 就是它们的公因式.

由乘法分配律, 我们知道

$$m(a+b-c)=ma+mb-mc,$$

因此

$$ma+mb-mc=m(a+b-c).$$

这表明上式左边三项的公因式 m 可以提取出来, 作为整式 $ma+mb-mc$ 的因式. $ma+mb-mc$ 的另一个因式 $a+b-c$ 仍由三项组成, 每一项等于 $ma+mb-mc$ 中对应的项除以公因式 m :

$$a=ma\div m, b=mb\div m, c=mc\div m$$

例 1.1.1 (一次提净)**.** 分解因式: $12a^2x^3+6abx^2y-15acx^2$

解. $12a^2x^3+6abx^2y-15acx^2$ 由

$$12a^2x^3, 6abx^2y, -15acx^2$$

这三项组成, 它们的数系数 $12, 6, -15$ 的最大公约数是 3 , 各项都含有因式 a 和 x^2, 所以 $3ax^2$ 是上述三项的公因式, 可以提取出来作为 $12a^2x^3+6abx^2y-15acx^2$ 的因式, 即有

$$\begin{aligned}&12a^2x^3+6abx^2y-15acx^2\\=&3ax^2(4ax+2by-5c).\end{aligned}$$

注记. *在例 1.1.1中, 如果只将因式 $3a$ 或 $3ax$ 提出, 那么留下的式子仍有公因式可以提取, 这增添了麻烦, 不如一次提净为好. 因此, 应当先检查数系数, 然后再一个个字母逐一检查, 将各项的公因式提出来, 使留下的式子没有公因式可以直接提取.*

还需注意原式如果由三项组成, 那么提取公因式后留下的式子仍由三项组成. 在例 1 中, 这三项分别为 $12a^2x^3, 6abx^2y, -15acx^2$ 除以公因式 $3ax^2$ 所得的商. 初学的同学为了防止产生错误, 可以采取两点措施:

1. *在提公因式前, 先将原式的三项都写成公因式 $3ax^2$ 与另一个式子的积, 然后再提取公因式, 即*

$$\begin{aligned}&12a^2x^3+6abx^2y-15acx^2\\=&3ax^2\cdot 4ax+3ax^2\cdot 2by+3ax^2\cdot(-5c)\\=&3ax^2\cdot(4ax+2by-5c).\end{aligned}$$

   在熟练之后应当省去中间过程, 直接写出结果.

2. *用乘法分配律进行验算. 由乘法得出*

$$\begin{aligned}&3ax^2(4ax+2by-5c)\\=&12a^2x^3+6abx^2y-15acx^2.\end{aligned}$$

例 1.1.2 (视“多”为一). 分解因式: $2a^2b(x+y)^2(b+c)-6a^3b^3(x+y)(b+c)^2$

解. 原式由

$$2a^2b(x+y)^2(b+c),-6a^3b^3(x+y)(b+c)^2$$

这两项组成. 它们的数系数的最大公约数是 2 , 两项都含有因式 a^2 和 b, 而且都含有因式 $x+y$ 与 $b+c$, 因此 $2a^2b(x+y)(b+c)$ 是它们的公因式. 于是有

$$\begin{aligned}&2a^2b(x+y)^2(b+c)-6a^3b^3(x+y)(b+c)^2\\=&2a^2b(x+y)(b+c)\cdot(x+y)-2a^2b(x+y)(b+c)\cdot 3ab^2(b+c)\\=&2a^2b(x+y)(b+c)\left[(x+y)-3ab^2(b+c)\right]\\=&2a^2b(x+y)(b+c)\left(x+y-3ab^3-3ab^2c\right).\end{aligned}$$

在本例中, 我们把多项式 $x+y,b+c$ 分别整个看成是一个字母, 这种观点在因式分解时是很有用的.

例 1.1.3 (切勿漏 1). 分解因式: $(2x+y)^3-(2x+y)^2+(2x+y)$.

解. 我们把多项式 $2x+y$ 看成是一个字母, 因此原式由

$$(2x+y)^3,-(2x+y)^2,2x+y$$

这三项组成, $2x+y$ 是这三项的公因式, 于是

$$\begin{aligned}&(2x+y)^3-(2x+y)^2+(2x+y)\\=&(2x+y)\cdot(2x+y)^2-(2x+y)\cdot(2x+y)+(2x+y)\cdot 1\\=&(2x+y)\left[(2x+y)^2-(2x+y)+1\right].\end{aligned}$$

请注意, 中括号内的式子仍由三项组成, 千万不要忽略最后一项 1. 在省去中间过程时, 尤需加倍留心.

例 1.1.4 (注意符号). 分解因式: $-3ab(2x+3y)^4+ac(2x+3y)^3-a(2x+3y)$.

解. $-3ab(2x+3y)^4+ac(2x+3y)^3-a(2x+3y)$
$=a(2x+3y)\cdot(-3b)\cdot(2x+3y)^3+a(2x+3y)\cdot c(2x+3y)^2+a(2x+3y)\cdot(-1)$

$$=a(2x+3y)\left[-3b(2x+3y)^3+c(2x+3y)^2-1\right].$$

注记. 注意中括号内的最后一项是 *-1* , 千万别漏掉. 本例中, 原式的第一项有个因数 *-1* , 它也可以作为因数提取出来, 即

$$\begin{aligned}&-3ab(2x+3y)^4+ac(2x+3y)^3-a(2x+3y)\\=&-a(2x+3y)\cdot 3b(2x+3y)^3-a(2x+3y)\cdot(-c)(2x+3y)^2-\\&a(2x+3y)\cdot 1\\=&-a(2x+3y)\left[3b(2x+3y)^3-c(2x+3y)^2+1\right].\end{aligned}$$

这样做也是正确的. 但必须注意各项的符号, 提出因数 *-1* 后各项都应改变符号, 所以上式的中括号内三项的符号恰与原式中相应的三项相反.

例 1.1.5 (仔细观察)**.** 分解因式：$(2x-3y)(3x-2y)+(2y-3x)(2x+3y)$.

解. 初看起来, 原式所含的第一项 $(2x-3y)(3x-2y)$ 与第二项 $(2y-3x)(2x+3y)$ 没有公因式, 但进一步观察便会发现

$$2y-3x=-(3x-2y),$$

因此 $3x-2y$ 是两项的公因式. 于是有

$$\begin{aligned}&(2x-3y)(3x-2y)+(2y-3x)(2x+3y)\\=&(3x-2y)[(2x-3y)-(2x+3y)]\\=&-6y(3x-2y).\end{aligned}$$

提出公因式后, 留下的式子如果可以化简, 就应当化简.

例 1.1.6 (化“分”为整)**.** 分解因式: $3a^3b^2-6a^2b^3+\frac{27}{4}ab$.

解. 这里的第三项 $\frac{27}{4}ab$ 的系数是分数, 为了避免分数运算, 我们把 $\frac{1}{4}$ 先提取出来, 这时每项都除以 $\frac{1}{4}$ (也就是乘以 4), 即

$$\begin{aligned}&3a^3b^2-6a^2b^3+\frac{27}{4}ab\\=&\frac{1}{4}\left(12a^3b^2-24a^2b^3+27ab\right)\\=&\frac{3}{4}ab\left(4a^2b-8ab^2+9\right).\end{aligned}$$

熟练以后可以将以上两步并作一步, “一次提净”.

在提出一个分数因数 (它的分母是各项系数的公分母) 后, 我们总可以使各项系数都化为整数 (这个过程实质上就是通分). 并且, 还可以假定第一项系数是正整数, 否则可用前面说过的方法, 把 -1 作为公因数提出, 使第一项系数成为正整数.

注记. *提公因式是因式分解的基本方法之一. 在因式分解时, 首先应该想到是否有公因式可提. 在与其他方法配合时, 即使开始已经提出公因式, 但是经过分组或应用公式后还有可能再出现公因式. 凡有公因式应立即提净. 提公因式时, 应注意各项的符号, 千万不要漏掉一项.*

习题 1

将以下各式分解因式:

1. $5x^2y-10xyz+5xy$.
2. $2a(x-a)+b(a-x)-(x-a)$.
3. $3-2x(x+1)+a(x+1)+(x+1)$.
4. $\frac{3}{2}b^{3n-1}+\frac{1}{6}b^{2n-1}$ (n 是正整数).
5. $2(p-1)^2-4q(p-1)$.

6. $mn\left(m^2+n^2\right)-n^2\left(m^2+n^2\right)$.

7. $(5a-2b)(2m+3p)-(2a-7b)(2m+3p)$.

8. $2(x+y)+6(x+y)^2-4(x+y)^3$.

9. $(x+y)^2(b+c)-(x+y)(b+c)^2$.

10. $6p(x-1)^3-8p^2(x-1)^2-2p(1-x)^2$.

1.2　应用公式

将乘法公式反过来写就得到因式分解中所用的公式, 常见的有七个公式：

1. $a^2-b^2=(a+b)(a-b)$.
2. $a^3+b^3=(a+b)\left(a^2-ab+b^2\right)$.
3. $a^3-b^3=(a-b)\left(a^2+ab+b^2\right)$.
4. $a^2+2ab+b^2=(a+b)^2$.
5. $a^2-2ab+b^2=(a-b)^2$.
6. $a^3+3a^2b+3ab^2+b^3=(a+b)^3$.
7. $a^3-3a^2b+3ab^2-b^3=(a-b)^3$.

以上公式必须熟记, 牢牢掌握各自的特点.

1.2.1　平方差

七个公式中, 平方差公式应用得最多.

例 1.2.1. 分解因式: $9(m-n)^2-4(m+n)^2$.

解. 原式由两项组成, 这两项符号相反, 并且

$$\begin{aligned}9(m-n)^2&=[3(m-n)]^2,\\4(m+n)^2&=[2(m+n)]^2,\end{aligned}$$

因此可以应用平方差公式, 得

$$\begin{aligned}&9(m-n)^2-4(m+n)^2\\=&[3(m-n)]^2-[2(m+n)]^2\\=&[3(m-n)+2(m+n)][3(m-n)-2(m+n)]\\=&(5m-n)(m-5n).\end{aligned}$$

例 1.2.2. 分解因式: $75x^6y-12x^2y^5$.

解.

$$
\begin{aligned}
75x^6y-12x^2y^5 =&3x^2y\left(25x^4-4y^4\right)\\
=&3x^2y\left[\left(5x^2\right)^2-\left(2y^2\right)^2\right]\\
=&3x^2y\left(5x^2+2y^2\right)\left(5x^2-2y^2\right)
\end{aligned}
$$

例 1.2.3. 分解因式: $-\left(3a^2-5b^2\right)^2+\left(5a^2-3b^2\right)^2$.

解.

$$
\begin{aligned}
&-\left(3a^2-5b^2\right)^2+\left(5a^2-3b^2\right)^2\\
=&\left(5a^2-3b^2\right)^2-\left(3a^2-5b^2\right)^2\\
=&\left[\left(5a^2-3b^2\right)+\left(3a^2-5b^2\right)\right]\left[\left(5a^2-3b^2\right)-\left(3a^2-5b^2\right)\right]\\
=&\left(8a^2-8b^2\right)\left(2a^2+2b^2\right)\\
=&16\left(a^2-b^2\right)\left(a^2+b^2\right)\\
=&16(a+b)(a-b)\left(a^2+b^2\right)
\end{aligned}
$$

注记. 例 *1.2.3*表明在因式公解中可能需要多次应用公式或提公因式, 直到不能继续分解为止.

1.2.2　立方和与立方差

例 1.2.4. 分解因式：$9x^5-72x^2y^3$.

解.

$$
\begin{aligned}
9x^5-72x^2y^3 &= 9x^2\left(x^3-8y^3\right)\\
&= 9x^2\left[x^3-(2y)^3\right]\\
&= 9x^2(x-2y)\left(x^2+2xy+4y^2\right)
\end{aligned}
$$

例 1.2.5. 分解因式：a^6+b^6 .

解.

$$
\begin{aligned}
a^6+b^6 &= \left(a^2\right)^3+\left(b^2\right)^3\\
&= \left(a^2+b^2\right)\left[\left(a^2\right)^2-a^2b^2+\left(b^2\right)^2\right]\\
&= \left(a^2+b^2\right)\left(a^4-a^2b^2+b^4\right)
\end{aligned}
$$

1.2.3　完全平方

例 1.2.6. 分解因式：$9x^2-24xy+16y^2$.

解. 原式由三项组成, 第一项 $9x^2=(3x)^2$, 第三项 $16y^2=(4y)^2$, 而

$$2\cdot 3x\cdot 4y=24xy$$

与中间一项只差一个符号, 因此可以利用 (完全) 平方式, 得

$$\begin{aligned}&9x^2-24xy+16y^2\\=&(3x-4y)^2.\end{aligned}$$

不是平方式的二次三项式, 通常用十字相乘法分解 (后面会讲).

例 1.2.7. 分解因式：$8a-4a^2-4$.

解. 首先把原式“理顺”, 也就是将它的各项按字母 a 降幂 (或升幂) 排列, 从而有

$$\begin{aligned}&8a-4a^2-4\\=&-4a^2+8a-4\\=&-4\left(a^2-2a+1\right)\\=&-4(a-1)^2.\end{aligned}$$

注记. *按某个字母降幂排列是一个简单而有用的措施 (简单的往往是有用的), 值得注意.*

例 1.2.8. 分解因式：$4a^2+9b^2+9c^2-18bc-12ca+12ab$.

解. 我们需要引入一个公式. 由乘法可得

$$(a+b+c)^2=a^2+b^2+c^2+2ab+2bc+2ca,$$

即若干项的和的平方等于各项的平方与每两项乘积的 2 倍的和. 上面的式子可写成

$$\begin{aligned}&a^2+b^2+c^2+2ab+2bc+2ca\\=&(a+b+c)^2.\end{aligned}$$

这也是一个因式分解的公式.

联系到例 1.2.8就有

$$\begin{aligned}&4a^2+9b^2+9c^2-18bc-12ca+12ab\\=&(2a)^2+(3b)^2+(-3c)^2+2(3b)(-3c)+2(2a)(-3c)+2(2a)(3b)\\=&(2a+3b-3c)^2.\end{aligned}$$

1.2.4　完全立方

例 1.2.9. 分解因式：$8x^3+27y^3+36x^2y+54xy^2$.

解.

$$\begin{aligned}&8x^3+27y^3+36x^2y+54xy^2\\=&8x^3+36x^2y+54xy^2+27y^3\\=&(2x)^3+3(2x)^2(3y)+3(2x)(3y)^2+(3y)^3x\\=&(2x+3y)^3.\end{aligned}$$

例 1.2.10. 分解因式: $729a^6-243a^4+27a^2-1$.

解.

$$\begin{aligned}&729a^6-243a^4+27a^2-1\\=&\left(9a^2\right)^3-3\cdot\left(9a^2\right)^2\cdot 1+3\cdot\left(9a^2\right)\cdot 1^2-1^3\\=&\left(9a^2-1\right)^3\\=&(3a+1)^3(3a-1)^3\end{aligned}$$

例 1.2.11. 分解因式：a^6-b^6 .

解. a^6 可以看成平方：

$$a^6=\left(a^3\right)^2,$$

也可以看成立方：

$$a^6=\left(a^2\right)^3,$$

于是 a^6-b^6 的分解就有两条路可走.
第一条路是先应用平方差公式：

$$\begin{aligned}a^6-b^6&=\left(a^3\right)^2-\left(b^3\right)^2\\&=\left(a^3+b^3\right)\left(a^3-b^3\right)\\&=(a+b)\left(a^2-ab+b^2\right)(a-b)\left(a^2+ab+b^2\right)\end{aligned}$$

第二条路是从立方差公式入手:

$$\begin{aligned}a^6-b^6&=\left(a^2\right)^3-\left(b^2\right)^3\\&=\left(a^2-b^2\right)\left(a^4+a^2b^2+b^4\right)\\&=(a+b)(a-b)\left(a^4+a^2b^2+b^4\right)\end{aligned}$$

注记. 采用两种方法分解, 获得的结果应当相同. 因此比较

$$(a+b)\left(a^2-ab+b^2\right)(a-b)\left(a^2+ab+b^2\right)$$

与

$$(a+b)(a-b)\left(a^4+a^2b^2+b^4\right),$$

我们知道 $a^4+a^2b^2+b^4$ 不是既约多项式, 并且有

$$a^4+a^2b^2+b^4=\left(a^2+ab+b^2\right)\left(a^2-ab+b^2\right) \tag{1.1}$$

及

$$a^6-b^6=(a+b)(a-b)\left(a^2+ab+b^2\right)\left(a^2-ab+b^2\right). \tag{1.2}$$

于是, 从 a^6-b^6 的分解出发, 不但得到*1.2*式, 而且知道 $a^4+a^2b^2+b^4$ 不是既约多项式, 导出了*1.1*式, 可谓问一知三.

后面我们还要介绍导出*1.1*式的另一种方法.

1.2.5　$2^{1984}+1$ 不是质数

例 1.2.12. 求证 $2^{1984}+1$ 不是质数.

解. 为了将 $2^{1984}+1$ 分解因数, 我们需要知道一个新的公式, 即在 n 为正奇数时

$$a^n+b^n=(a+b)\left(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots-ab^{n-2}+b^{n-1}\right).$$

上式不难用乘法验证, 将右边的两个因式相乘便得到 a^n+b^n . 现在我们有

$$\begin{aligned}2^{1984}+1&=\left(2^{64}\right)^{31}+1^{31}\\&=\left(2^{64}+1\right)\left(2^{64\times30}-2^{64\times29}+\cdots-2^{64}+1\right).\end{aligned}$$

$2^{64}+1$ 是 $2^{1984}+1$ 的真因数, 它大于 1 , 小于 $2^{1984}+1$, 所以 $2^{1984}+1$ 不是质数. 用这个方法可以证明：当 n 有大于 1 的奇数因数时, 2^n+1 不是质数.

注记. 类似地, 由乘法可以得到在 n 为正整数时

$$a^n-b^n=(a-b)\left(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+ab^{n-2}+b^{n-1}\right). \tag{12}$$

这也是一个有用的公式.

例 1.2.13. 分解因式: x^5-1.

解.

$$x^5-1=(x-1)\left(x^4+x^3+x^2+x+1\right)$$

习题 2

将以下各式分解因式：

1. $16-(3a+2b)^2$.
2. $4y^2-(2z-x)^2$.
3. a^4-b^4.
4. $-81a^4b^4+16c^4$.
5. $20a^3x^3-45axy^2$.
6. $\left(3a^2-b^2\right)^2-\left(a^2-3b^2\right)^2$.
7. x^8-y^8.
8. $16x^5-x$.
9. $\left(5x^2+2x-3\right)^2-\left(x^2-2x-3\right)^2$.
10. $32a^3b^3-4b^9$.

11. $8a^3b^3c^3 - 1$.

12. $64x^6y^3 + y^{15}$.

13. $x^2(a+b)^2 - 2xy\left(a^2 - b^2\right) + y^2(a-b)^2$.

14. $a^{n+2} + 8a^n + 16a^{n-2}$.

15. $9a^2 + x^{2n} + 6a + 2x^n + 6ax^n + 1$.

16. $a^2 + b^2 + c^2 + 2ab - 2ac - 2bc$.

17. $x^2 + 9y^2 + 4z^2 - 6xy + 4xz - 12yz$.

18. $(p+q)^3 - 3(p+q)^2(p-q) + 3(p+q)(p-q)^2 - (p-q)^3$.

19. $4a^2b^2 - \left(a^2 + b^2\right)^2$.

20. $(a+x)^4 - (a-x)^4$.

1.3　分组分解

例 1.3.1 (分组分解三部曲)**.** 分解因式：$ax-by-bx+ay$.

解.

$$\begin{aligned}&ax-by-bx+ay\\=&(ax-bx)+(ay-by)\\=&x(a-b)+y(a-b)\\=&(x+y)(a-b).\end{aligned}$$

分组的方法并不是唯一的, 对于上面的整式 $ax-by-bx+ay$, 也可以采用下面的做法：

$$\begin{aligned}&ax-by-bx+ay\\=&(ax+ay)-(bx+by)\\=&a(x+y)-b(x+y)\\=&(x+y)(a-b)\end{aligned}$$

两种做法的效果是一样的, 殊途同归！可以说, 一种是按照 x 与 y 来分组 (含 x 的项在一组, 含 y 的项在另一组)；另一种是按 a 与 b 来分组.

一般地, 分组分解大致分为三步：

1. 将原式的项适当分组；
2. 对每一组进行处理 (“提”或“代”)；
3. 将经过处理后的每一组当作一项, 再采用“提”或“代”进行分解.

一位高明的棋手, 在下棋时, 决不会只看一步. 同样, 在进行分组时, 不仅要看到第二步, 而且要看到第三步.

一个整式的项有许多种分组的方法, 初学者往往需要经过尝试才能找到适当的分组方法, 但是只要努力实践, 多加练习, 就会成为有经验的“行家”.

例 1.3.2 (殊途同归)**.** 分解因式：$x^2+ax^2+x+ax-1-a$.

解. 解法一： 按字母 x 的幂来分组.

$$\begin{aligned}&x^2+ax^2+x+ax-1-a\\=&\left(x^2+ax^2\right)+(x+ax)-(1+a)\\=&x^2(1+a)+x(1+a)-(1+a)\\=&(1+a)\left(x^2+x-1\right).\end{aligned}$$

解法二： 按字母 a 的幂来分组.

$$\begin{aligned}&x^2+ax^2+x+ax-1-a\\=&\left(ax^2+ax-a\right)+\left(x^2+x-1\right)\\=&a\left(x^2+x-1\right)+\left(x^2+x-1\right)\\=&(a+1)\left(x^2+x-1\right).\end{aligned}$$

例 1.3.3 (瞄准公式). 分解因式: $-1-2x-x^2+y^2$.

解.

$$\begin{aligned}&-1-2x-x^2+y^2\\=&y^2-\left(x^2+2x+1\right)\\=&y^2-(x+1)^2\\=&(y+x+1)(y-x-1)\end{aligned}$$

例 1.3.4 (瞄准公式). 分解因式：$ax^3+x+a+1$.

解.

$$\begin{aligned}&ax^3+x+a+1\\=&\left(ax^3+a\right)+(x+1)\\=&a(x+1)\left(x^2-x+1\right)+(x+1)\\=&(x+1)\left(ax^2-ax+a+1\right)\end{aligned}$$

例 1.3.5 (从零开始). 分解因式：$ab\left(c^2-d^2\right)-\left(a^2-b^2\right)cd$.

解. 此式无法直接进行分解, 必须先用乘法分配律将原式变为四项, 再进行分组.

$$\begin{aligned}&ab\left(c^2-d^2\right)-\left(a^2-b^2\right)cd\\=&abc^2-abd^2-a^2cd+b^2cd\\=&\left(abc^2-a^2cd\right)+\left(b^2cd-abd^2\right)\\=&ac(bc-ad)+bd(bc-ad)\\=&(ac+bd)(bc-ad).\end{aligned}$$

从这个例子可以看出, 错误的分组还不如不分组. 聪明的人并不是不犯错误的人, 而是善于改正错误的人.

如果“一提、二代”都不能奏效, 就应当采用分组分解. 分组分解应依照前面所说的三步进行. 这三步是密切联系的, 不仅要看到第二步, 而且要看到第三步. 在第二步与第三步都是提取公因式时, 各组的项数相等 (平均分配). 否则, 应当瞄准公式来进行分组. 应当注意, 分组需要尝试, 失败了, 从零开始. 只要反复实践, 就能掌握分组的技巧, 运用自如.

习题 3

将以下各式分解因式 (对应书本第 14~24 题)：

1. $x^3+bx^2+ax+ab$.
2. $acx^3+bcx^2+adx+bd$.
3. $a^4+a^3b-ab^3-b^4$.

4. $a^4-a^3b-ab^3+b^4$.
5. $a^2b^2-a^2-b^2+1$.
6. $x^2y^2-x^2z^2-y^2z^2+z^4$.
7. $x^2y^2z^2-x^2z-y^2z+1$.
8. $x^4+x^3y+xz^3+yz^3$.
9. $(a+b)^2+(a+c)^2-(c+d)^2-(b+d)^2$.
10. $ax\left(y^3+b^3\right)+by\left(bx^2+a^2y\right)$.
11. $(a+b)^3+(b+c)^3+(c+a)^3+a^3+b^3+c^3$.

1.4　十字相乘

1.4.1　二次三项式

例 1.4.1. 分解因式：x^2-7x+6.

解.

$$x^2-7x+6=(x-1)(x-6).$$

例 1.4.2. 分解因式: x^2+7x-8.

解.

$$x^2+7x-8=(x+8)(x-1).$$

例 1.4.3. 分解因式：$x+12-x^2$.

解.

$$x+12-x^2=-x^2+x+12=-\left(x^2-x-12\right)=-(x+3)(x-4).$$

例 1.4.4 (二次项系数不为 1)**.** 分解因式: $6x^2-7x+2$.

解.

$$6x^2-7x+2=(2x-1)(3x-2).$$

1.4.2　二次齐次式

形如 $ax^2+bxy+cy^2$ 的多项式, 每一项都是 x 与 y 的二次式 (xy 中 x 与 y 的次数都是 1 , 所以 xy 的次数是 $1+1=2$), 称为 x 与 y 的二次齐次式. 它的分解与 x 的二次三项式一样, 采用十字相乘.

例 1.4.5. 分解因式：$6x^2-7xy+2y^2$.

解.

$$6x^2-7xy+2y^2=(2x-y)(3x-2y).$$

1.4.3 系数和为零

如果二次三项式 ax^2+bx+c 的系数和

$$a+b+c=0,$$

那么

$$ax^2+bx+c=(x-1)(ax-c).$$

事实上, 因为

$$b=-(a+c),$$

这时

$$\begin{aligned}&(x-1)(ax-c)\\=&ax^2-(a+c)x+c\\=&ax^2+bx+c.\end{aligned}$$

记住这个结论, 下面的例题就能迎刃而解了.

例 1.4.6. 分解因式: $3x^2+5x-8$.

解.

$$3x^2+5x-8=(x-1)(3x+8)$$

例 1.4.7. 分解因式: $12x^2-19xy+7y^2$.

解.

$$12x^2-19xy+7y^2=(x-y)(12x-7y).$$

注记. x 的二次三项式 *(*或 x 与 y 的二次齐次式*)* 应该用十字相乘来分解因式. 方法是把 x^2 的系数分解为两个因数的积, 把常数项 *(*或 y^2 的系数*)* 也分解为两个因数的积, 再把这些因数交叉相乘, 如果所得乘积的和等于 x 的一次项的系数, 那么就产生出多项式的两个一次因式. 在系数和为零时, 必有一个因式是 $x-1$ *(*或 $x-y$ *)*, 这样, 分解的结果可以直接写出来.

1.4.4 综合运用

例 1.4.8 (换元)**.** 分解因式：x^6-28x^3+27.

解. 设 $x^3=u$, 则原式变为 $u^2-28u+27$, 这是一个二次三项式, 可以分解为 $(u-1)(u-27)$, 所以

$$x^6-28x^3+27=(x^3-1)(x^3-27)=(x-1)(x^2+x+1)(x-3)(x^2+3x+9).$$

例 1.4.9. 分解因式：$\left(x^2+4x+8\right)^2+3x\left(x^2+4x+8\right)+2x^2$.

解. 把 x^2+4x+8 看成一个字母, 得

$$\begin{aligned}&\left(x^2+4x+8\right)^2+3x\left(x^2+4x+8\right)+2x^2\\=&\left(x^2+4x+8+x\right)\left(x^2+4x+8+2x\right)\\=&\left(x^2+5x+8\right)\left(x^2+6x+8\right)\\=&(x+2)(x+4)\left(x^2+5x+8\right).\end{aligned}$$

这里对 x^2+6x+8 再次用十字相乘分解因式, 而 x^2+5x+8 在有理数集内不能分解.

例 1.4.10. 证明：四个连续整数的乘积加 1 是整数的平方.

证明. 设这四个连续整数为

$$x+1,x+2,x+3,x+4,$$

则

$$\begin{aligned}&(x+1)(x+2)(x+3)(x+4)+1\\=&[(x+1)(x+4)][(x+2)(x+3)]+1\\=&\left(x^2+5x+4\right)\left(x^2+5x+6\right)+1.\end{aligned}$$

我们把 $x+1$ 与 $x+4$ 相乘, $x+2$ 与 $x+3$ 相乘, 好处是两个乘积不但二次项相同, 而且一次项也是相同的.

把 x^2+5x+5 看成 u , 这时

$$u=x^2+5x+\frac{4+6}{2}$$

得

$$\begin{aligned}&(x+1)(x+2)(x+3)(x+4)+1\\=&\left[\left(x^2+5x+5\right)-1\right]\left[\left(x^2+5x+5\right)+1\right]+1\\=&\left(x^2+5x+5\right)^2-1+1\\=&\left(x^2+5x+5\right)^2,\end{aligned}$$

这是一个平方数. □

注记. 在本题中把 x^2+5x 或 x^2+5x+4 看成一个字母也是可以的, 但切勿把 $(x+1)(x+2)(x+3)(x+4)$ 全部乘出来写成 x 的四次式, 那样做的结果是破坏了规律性, 难以下手.

例 1.4.11. 分解因式：$4(x+5)(x+6)(x+10)(x+12)-3x^2$.

解. 第一项的四个因式以将 $x+5$ 与 $x+12$ 相乘、$x+6$ 与 $x+10$ 相乘为好, 这时不仅二次项相同, 而且常数项也相同, 于是

$$\begin{aligned}
&4(x+5)(x+6)(x+10)(x+12)-3x^2\\
=&4\left(x^2+17x+60\right)\left(x^2+16x+60\right)-3x^2\\
=&4\left[\left(x^2+16x+60\right)+x\right]\left(x^2+16x+60\right)-3x^2\\
=&4\left(x^2+16x+60\right)^2+4x\left(x^2+16x+60\right)-3x^2\\
=&\left[2\left(x^2+16x+60\right)-x\right]\left[2\left(x^2+16x+60\right)+3x\right]\\
=&\left(2x^2+31x+120\right)\left(2x^2+35x+120\right)
\end{aligned}$$

习题 5

将以下各式分解因式:

1. $x^2+12x+20$.
2. $x^2-12x+20$.
3. x^2-4x-5.
4. $x^2-9x-22$.
5. $12x^2-11xy-15y^2$.
6. $6x^2-13x+6$.
7. $2x^2+7x+3$.
8. $2x^2-5x+3$.
9. $-20xy+64y^2+x^2$.
10. $-x^2+x+56$.

1.5　多项式的因式分解

设 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 为 x 的 n 次多项式, 本节介绍求它的一次因式的方法.

1.5.1　余数定理

我们用 $f(x)$ 表示多项式 $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$, 用 $f(a)$ 表示这个多项式在 $x=a$ 时的值. 例如, 在 $f(x)=x^3+6x^2+11x+6$ 时, 可得

$$f(1)=1+6+11+6=24$$

$$f(-1)=-1+6-11+6=0$$

$$f(+2)=8+24+22+6=60$$

如果我们用一次多项式 $x-c$ 作除式去除多项式 $f(x)$，那么余式是一个数. 设这时商式为多项式 $g(x)$，余式 (余数) 为 r，则

$$f(x)=(x-c)Q(x)+r, \tag{1.3}$$

即被除式等于除式乘以商式再加余式.

在1.3式中令 $x=c$，便得到

$$f(c)=0+r=r,$$

因此, 我们有

$$x-c \text{ 除 } f(x) \text{ 时, 所得的余数为 } f(c)\ .$$

这个结论称为**余数定理**.

如果余数为 0，那么 $f(x)$ 被 $x-c$ 整除, 也就是 $x-c$ 是 $f(x)$ 的因式. 反过来, 如果 $x-c$ 是 $f(x)$ 的因式, 那么 $f(x)$ 被 $x-c$ 整除, 余数为 0 . 因此, 我们有

如果 $f(c)=0$, 那么 $x-c$ 是 $f(x)$ 的因式. 反过来, 如果 $x-c$ 是 $f(x)$ 的因式, 那么 $f(c)=0$.

例 1.5.1. 分解因式: $f(x)=x^3+6x^2+11x+6$.

解. 因为 $f(-1)=0$，根据上面的结论 $x-(-1)=x+1$ 是它的一次因式. 知道这个因式后, 施行除法就可以把商式求出来. 不过, 我们也可以不用除法, 直接去分组分解. 这里分组是“有的放矢”的, 每一组都有一个因式 $x+1$，即

$$\begin{aligned}
&x^3+6x^2+11x+6\\
=&\left(x^3+x^2\right)+\left(5x^2+5x\right)+(6x+6)\\
=&x^2(x+1)+5x(x+1)+6(x+1)\\
=&(x+1)\left(x^2+5x+6\right)\\
=&(x+1)(x+2)(x+3).
\end{aligned}$$

例 1.5.2. 设 $f(x)=2x^3-5x^2+5x-3$, 计算 $f(1), f(-1), f\left(\frac{3}{2}\right)$, 并把 $f(x)$ 分解.

解.

$$\begin{aligned}
&f(1)=2-5+5-3=-1\\
&f(-1)=-2-5-5-3=-15\\
&f\left(\frac{3}{2}\right)=2\cdot\left(\frac{3}{2}\right)^3-5\cdot\left(\frac{3}{2}\right)^2+5\cdot\left(\frac{3}{2}\right)-3\\
&\quad=\frac{27}{4}-\frac{45}{4}+\frac{15}{2}-3=0
\end{aligned}$$

可知 $x-\frac{3}{2}$ 是 $f(x)$ 的一次因式. 为了避免分数运算, 我们把 $x-\frac{3}{2}$ 乘以 2 得 $2x-3, 2x-3$ 仍然是 $f(x)$ 的一次因式.

现在把 $f(x)$ 分组分解, 注意使每组都有因式 $2x-3$ (也就是同一组中两项的系数比为 $2:(-3)$) :

$$\begin{aligned}&2x^3-5x^2+5x-3\\=&\left(2x^3-3x^2\right)-\left(2x^2-3x\right)+(2x-3)\\=&x^2(2x-3)-x(2x-3)+(2x-3)\\=&(2x-3)\left(x^2-x+1\right).\end{aligned}$$

1.5.2　有理根的求法

如果 $f(c)=0$, 那么就说 c 是多项式 $f(x)$ 的根. 因此, 在 c 是 $f(x)$ 的根时, $x-c$ 是 $f(x)$ 的因式. 问题是怎样求出 $f(x)$ 的根?

我们假定 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整系数多项式, 也就是说 $a_n,a_{n-1},\cdots,a_1,a_0$ 都是整数. 又设有理数 $c=\frac{p}{q}$ 是 $f(x)$ 的根, 这里 p, q 是两个互质的整数.

由于 $f(c)=0$, 即

$$a_n\left(\frac{p}{q}\right)^n+a_{n-1}\left(\frac{p}{q}\right)^{n-1}+\cdots+a_1\left(\frac{p}{q}\right)+a_0=0$$

两边同乘 q^n 得

$$a_np^n+a_{n-1}p^{n-1}q+\cdots+a_1pq^{n-1}+a_0q^n=0 \tag{1.4}$$

1.4式右边被 p 整除 (0 被任何一个不等于 0 的数整除), 所以它的左边也被 p 整除. 显然, 左边的前 n 项都被 p 整除, 所以最后一项 a_0q^n 也被 p 整除, 但 p 与 q 互质, 所以 p 整除 a_0 , 即 p 是 a_0 的因数 (约数). 同样地, q 应当整除 a_np^n , 从而 q 是 a_n 的因数 (约数). 于是, 可得

有理根 $c=\frac{p}{q}$ 的分子 p 是常数项 a_0 的因数, 分母 q 是首项系数 a_n 的因数.

例 1.5.3. 分解因式: $f(x)=2x^3-x^2-5x-2$.

解. $a_0=-2$ 的因数是 $\pm1,\pm2,a_n=2$ 的因数是 $\pm1,\pm2$. 因此, $f(x)$ 的有理根只可能是 $\pm1,\pm2$ (分母为 1),$\pm\frac{1}{2}$. 因为

$$\begin{aligned}f(1)&=2-1-5-2=-6\\f(-1)&=-2-1+5-2=0\end{aligned}$$

于是 -1 是 $f(x)$ 的一个根, 从而 $x+1$ 是 $f(x)$ 的因式, 可得

$$\begin{aligned}&2x^3-x^2-5x-2\\=&\left(2x^3+2x^2\right)-\left(3x^2+3x\right)-(2x+2)\\=&2x^2(x+1)-3x(x+1)-2(x+1)\\=&\left(2x^2-3x-2\right)(x+1)\\=&(x-2)(2x+1)(x+1).\end{aligned}$$

例 1.5.4. 分解因式: $f(x)=3x^3+x^2+x-2$.

解. $a_0=-2$ 的因数为 $\pm1,\pm2, a_n=3$ 的正因数为 $+1,+3$ (我们可以认为 $\frac{p}{q}$ 的分母 q 是正的, 因此 a_0 的因数有正有负, a_n 的因数可只取正的). 所以, $f(x)$ 的有理根只可能是 $\pm1,\pm2,\pm\frac{1}{3},\pm\frac{2}{3}$.

由于

$$
\begin{aligned}
f\left(\frac{2}{3}\right) &= 3\cdot\left(\frac{2}{3}\right)^3+\left(\frac{2}{3}\right)^2+\left(\frac{2}{3}\right)-2\\
&=\frac{8}{9}+\frac{4}{9}+\frac{2}{3}-2=0
\end{aligned}
$$

所以 $x-\frac{2}{3}$ 是 $f(x)$ 的因式, 从而 $3x-2$ 是 $f(x)$ 的因式, 可得

$$
\begin{aligned}
&f(x)=3x^3+x^2+x-2\\
=&\left(3x^3-2x^2\right)+\left(3x^2-2x\right)+(3x-2)\\
=&x^2(3x-2)+x(3x-2)+(3x-2)\\
=&(3x-2)\left(x^2+x+1\right).
\end{aligned}
$$

例 1.5.5. 分解因式: $f(x)=6x^4+5x^3+3x^2-3x-2$.

解. $a_0=-2$ 的因数为 $\pm1,\pm2, a_n=6$ 的正因数为 $1,2,3,6$. 所以, $f(x)$ 的有理根只可能为

$$
\pm1,\pm2,\pm\frac{1}{2},\pm\frac{1}{3},\pm\frac{2}{3},\pm\frac{1}{6}
$$

经检验 $c=-\frac{1}{2}$ 是一个根, 所以 $2x+1$ 是 $f(x)$ 的因式, 可得

$$
\begin{aligned}
&6x^4+5x^3+3x^2-3x-2\\
=&\left(6x^4+3x^3\right)+\left(2x^3+x^2\right)+\left(2x^2+x\right)-(4x+2)\\
=&(2x+1)\left(3x^3+x^2+x-2\right)\\
=&(2x+1)(3x-2)\left(x^2+x+1\right).
\end{aligned}
$$

1.5.3　首 1 多项式

对于首项系数为 1 的整系数多项式 $f(x)$, 问题更加简单. 这时 $q=1$, 有理根都是整数根.

例 1.5.6. 分解因式：$x^6+2x^5+3x^4+4x^3+3x^2+2x+1$.

解. 本题有理根只可能为 $\pm1. +1$ 当然不可能为根 (因为多项式的系数全是正的), 经检验 -1 是根, 所以原式有因式 $x+1$, 并且

$$
\begin{aligned}
&x^6+2x^5+3x^4+4x^3+3x^2+2x+1\\
=&\left(x^6+x^5\right)+\left(x^5+x^4\right)+\left(2x^4+2x^3\right)+\left(2x^3+2x^2\right)+\left(x^2+x\right)+(x+1)\\
=&(x+1)\left(x^5+x^4+2x^3+2x^2+x+1\right).
\end{aligned}
$$

容易验证 -1 也是 $x^5+x^4+2x^3+2x^2+x+1$ 的根, 并且

$$\begin{aligned}
& x^5+x^4+2x^3+2x^2+x+1 \\
=& \left(x^5+x^4\right)+\left(2x^3+2x^2\right)+(x+1) \\
=&(x+1)\left(x^4+2x^2+1\right) \\
=&(x+1)\left(x^2+1\right)^2,
\end{aligned}$$

所以

$$\begin{aligned}
& x^6+2x^5+3x^4+4x^3+3x^2+2x+1 \\
=&(x+1)^2\left(x^2+1\right)^2.
\end{aligned}$$

例 1.5.7. 分解因式: $x^3-9x^2+26x-24$.

解. 有理根只可能为

$$\pm1,\pm2,\pm3,\pm4,\pm6,\pm8,\pm12,\pm24$$

经检验, 2 是根, 所以原式有因式 $x-2$, 并且

$$\begin{aligned}
& x^3-9x^2+26x-24 \\
=& \left(x^3-2x^2\right)-\left(7x^2-14x\right)+(12x-24) \\
=&(x-2)\left(x^2-7x+12\right) \\
=&(x-2)(x-3)(x-4).
\end{aligned}$$

例 1.5.8. 分解因式：$x^3-9x^2y+26xy^2-24y^3$.

解.

$$\begin{aligned}
& x^3-9x^2y+26xy^2-24y^3 \\
=&(x-2y)(x-3y)(x-4y).
\end{aligned}$$

这只不过是在上题的解答上添上几个 y 而已.

例 1.5.9. 分解因式：$-24y^3+26y^2-9y+1$.

解. $a_n=-24$, 但 $a_0=1$. 为了避免分数计算的麻烦, 我们把原式改为升幂排列

$$1-9y+26y^2-24y^3$$

如果与上例比较一下, 就会发现两者实质上是相同的, 即在上例中令 $x=1$, 便得到

$$\begin{aligned}
& 1-9y+26y^2-24y^3 \\
=&(1-2y)(1-3y)(1-4y).
\end{aligned}$$

例 1.5.10. 分解因式: $x^3-\frac{5}{3}x^2-\frac{11}{3}x-1$.

解. 原式不是整系数多项式, 但可以先提取 $\frac{1}{3}$, 然后再按上面的办法分解, 得

$$\begin{aligned}
& x^3-\frac{5}{3}x^2-\frac{11}{3}x-1 \\
=&\frac{1}{3}\left(3x^3-5x^2-11x-3\right) \\
=&\frac{1}{3}(x+1)(x-3)(3x+1)
\end{aligned}$$

习题 8

将以下各式分解因式：

1. x^3+4x^2-5.
2. $2x^5+7x^4+12x^3+14x^2+10x+3$.
3. $(x-2y)x^3-(y-2x)y^3$.
4. $x^4+2x^3-3x^2-4x+4$.
5. $2x^4+x^3+7x^2+4x-4$.
6. $3x^3-5x^2y+xy^2+y^3$.
7. $6x^3-5x^2y-3xy^2+2y^3$.
8. $3x^3+6x^2+4x+8$.
9. $8x^3+4(a+b+c)x^2+2(ab+bc+ca)x+abc$.
10. $(a-1)x^3-ax^2-(a-3)x+(a-2)$.
11. $5x^4+12x^3+17x^2+9x-7$.
12. $x^3+px^2+px+p-1$.

1.6　既约多项式

这一单元介绍在有理数集内如何判定一个多项式是否既约.

1.6.1　艾氏判别法

下面我们着重讨论一元的情形.

在复数集内, 只有一次多项式是既约多项式. 在实数集内, 既约多项式是一次或二次多项式. 与这形成鲜明的对比的是, 在有理数集内有任意次的既约多项式. 为了证明这一点, 先介绍一下重要的艾森斯坦 (Eisenstein, 1823∼ 1852) 判别法：

定理 1.6.1 (艾森斯坦判别法)**.** 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整系数多项式.

如果存在一个质数 p 满足以下条件:

1. p 不整除 a_n;
2. p 整除其余的系数 $(a_0,a_1,\cdots,a_{n-1})$;
3. p^2 不整除 a_0 .

那么, $f(x)$ 在有理数集内不可约.

这个定理的证明在高等代数的教材里可以找到, 有兴趣的读者可自行查阅.

例 1.6.1. 证明：对于任意的自然数 n, x^n-2 在有理数集内不可约.

证明. 取 $p=2$, 则 p 整除 $a_0=-2, p^2$ 不整除 a_0, p 整除 $a_1=a_2=\cdots=a_{n-1}=0$ (0 是任何一个非零整数的倍数), p 不整除 $a_n=1$. 根据艾氏判别法, x^n-2 是有理数集内的既约多项式. □

注记. 这表明在有理数集内存在着任意次的既约多项式.

例 1.6.2. 证明：$x^4+x^3+x^2+x+1$ 在有理数集内不可约.

证明. 艾氏判别法不能直接应用. 但令

$$x=y+1,$$

则

$$\begin{aligned}
& x^4+x^3+x^2+x+1 \\
= & \frac{x^5-1}{x-1} \\
= & \frac{(y+1)^5-1}{y} \\
= & y^4+5y^3+10y^2+10y+5
\end{aligned}$$

$y^4+5y^3+10y^2+10y+5$ 中除首项系数 1 以外, 其他系数都被 $p=5$ 整除, 常数项 5 不能被 p^2 整除. 因此, $y^4+5y^3+10y^2+10y+5$ 在有理数集内不能分解. 从而 $x^4+x^3+x^2+x+1$ 也是有理数集内的既约多项式. □

注记. 用这个方法可以证明, 在 p 为质数时, 多项式 $x^{p-1}+x^{p-2}+\cdots+x+1$ 是有理数集内的既约多项式.

例 1.6.3. x^6+x^3+1 在有理数集内不可约.

证明. 令 $x=y+1$, 则

$$\begin{aligned}
& x^6+x^3+1 \\
= & (y+1)^6+(y+1)^3+1 \\
= & y^6+6y^5+15y^4+21y^3+18y^2+9y+3.
\end{aligned}$$

由艾氏判别法 (取 $p=3$) 可知这个多项式是既约多项式. □

1.6.2 奇与偶

如果把所有的奇数用 1 表示, 偶数用 0 表示, 那么就得到一种奇怪的算术：

$$0+0=0, 0+1=1+0=1, 1+1=0$$

它们表示两个偶数的和是偶数；一个偶数与一个奇数的和是奇数；两个奇数的和是偶数. (在数论中, 这是以 2 为模的算术)

采用这种算术, 可以使问题大为简化, 不但整数只有两个 (0 与 1), 而且多项式的个数也大大减少. 一次多项式只有两个, 即

$$x, x+1$$

实际上, 如 $3x+4$ 可以归为第一种, $3x+5$ 可以归为第 2 种, 而 $2x+4=0$ 不是一次多项式. 二次多项式只有 4 个, 即

$$x^2, x^2+x, x^2+1, x^2+x+1,$$

其中, $x^2=x \cdot x, x^2+x=x(x+1), x^2+1=(x+1)^2$, 都不是既约多项式, 只有 x^2+x+1 是既约多项式.

例 1.6.4. 证明：当 $(b+c)d$ 为奇数时, 整系数的三次多项式 x^3+bx^2+cx+d 在有理数集内不可约.

证明. 由于 $(b+c)d$ 是奇数, 所以 $b+c$ 与 d 都是奇数. 如果 x^3+bx^2+cx+d 在有理数集内可以分解, 那么它一定有一次因式, 也就是有有理根, 这根是整数而且是 d 的约数, 因而也是奇数. 采用上面的算术, 就有

$$b+c=1, d=1$$

并且 1 是 x^3+bx^2+cx+d 的根. 但是

$$\begin{aligned}
& 1^3+b \cdot 1^2+c \cdot 1+d \\
= & 1+(b+c)+d \\
= & 1+1+1 \\
= & 1 \neq 0,
\end{aligned}$$

所以, 1 不是 x^3+bx^2+cx+d 的根, 矛盾! 这说明当 $(b+c)d$ 为奇数时, x^3+bx^2+cx+d 在有理数集内不可约. □

例 1.6.5. 证明 x^5+x^2-1 在有理数集内不可约.

证明. 如果 x^5+x^2-1 可以分解, 那么它一定有一个一次因式或一个二次既约因式.

采用上面的算术, 便得到 x^5+x^2-1 应当被 $x, x+1$ 或 x^2+x+1 中某一个整除. 但

$$\begin{aligned}
& x^5+x^2-1 \\
= & x^2\left(x^3-1\right)+1 \\
= & x^2(x+1)\left(x^2+x+1\right)+1 \\
= & x^2\left(x^3-1\right)+1
\end{aligned}$$

可见, x^5+x^2-1 不被 $x, x+1, x^2+x+1$ 中任一个整除. 这就说明 x^5+x^2-1 在有理数集内不可约. □

例 1.6.6. 证明 x^6+x^3-1 在有理数集内不可约.

证明. 采用上面的算术, 得

$$\begin{aligned}
&x^6+x^3-1\\
=&\left(x^6-1\right)+\left(x^3-1\right)+1\\
=&\left(x^3+2\right)\left(x^3-1\right)+1\\
=&\left(x^3+2\right)(x-1)\left(x^2+x+1\right)+1\\
=&x^3(x+1)\left(x^2+x+1\right)+1
\end{aligned}$$

可见, x^6+x^3-1 不被 $x, x+1, x^2+x+1$ 中任一个整除, 故 x^6+x^3-1 没有一次、二次的因式. □

例 1.6.7. 证明 $x^4+3x^3+3x^2-5$ 在有理数集内不可约.

证明. 采用上面的算术, 得

$$\begin{aligned}
&x^4+3x^3+3x^2-5\\
=&x^4+x^3+x^2+1\\
=&x^3(x+1)+\left(x^2+x\right)+(x+1)\\
=&(x+1)\left(x^3+x+1\right),
\end{aligned}$$

因此, 如果 $x^4+3x^3+3x^2-5$ 可以分解, 它一定分解为一个一次因式与一个三次因式的积.

容易验证, $x^4+3x^3+3x^2-5$ 没有有理根, 自然它就没有一次因式, 从而它在有理数集内不可约. □

注记. *在有理数集内, 存在着任意次的既约多项式. 可以利用艾森斯坦判别法、奇偶性 (以 2 为模的算术) 及待定系数法等来证明多项式是既约多项式.*

习题 12

证明以下各式在有理数集内不可约:

1. x^4+x+1.
2. x^4+x^3+1.
3. x^6-x^3-1.
4. $x^4+5x+21$.
5. $x^4+x^3+12x^2+14x+1$.

第二章　整除, 同余和不定方程

符号说明

符号	说明
$a \mid b$	a 整除 b
$a \nmid b$	a 不整除 b
(a,b)	a 与 b 的最大公因数
$[a,b]$	a 与 b 的最小公倍数
$p^{\alpha} \Vert a$	$p^{\alpha} \mid a$ 但 $p^{\alpha+1} \nmid a$
$a \equiv b (\mathrm{mod} m)$	a 与 b 对模 m 同余
$a \not\equiv b (\mathrm{mod} m)$	a 与 b 对模 m 不同余
$a^{-1} (\mathrm{mod} m)$	a 对模 m 的数论倒数
$[x]$	不超过 x 的最大整数
$\max\{a,b\}$	实数 a b 中较大的数
$\min\{a,b\}$	实数 a b 中较小的数

表 2.1: 符号说明

2.1　整除

任意两个整数的和, 差或积都是整数, 但是两个整数做除法时所得的结果不一定是整数, 因此, 数论中的许多问题都是在研究整数之间的除法.

2.1.1　整除的概念与基本性质

定义 2.1.1. 对任给的两个整数 $a, b (a \neq 0)$, 如果存在整数 q, 使得 $b = aq$, 那么称 b 能被 a 整除 (或称 a 能整除 b), 记作 $a \mid b$. 否则, 称 b 不能被 a 整除, 记作 $a \nmid b$.

如果 $a \mid b$, 那么称 a 为 b 的因数, b 为 a 的倍数.

利用整除的定义, 可以非常容易地推导出下面一些经常被用到的性质.

性质 2.1.1. 如果 $a \mid b$, 那么 $a \mid (-b)$, 反过来也成立; 进一步, 如果 $a \mid b$, 那么 $(-a) \mid b$, 反过来也成立. 因此, 我们经常只讨论正整数之间的整除关系.

性质 2.1.2. 如果 $a|b, b|c$, 那么 $a \mid c$. 这表明整除具有传递性.

性质 2.1.3. 若 $a|b, a|c$, 则对任意整数 x, y, 都有 $a \mid bx+cy$. (即 a 能整除 b, c 的任意一个“线性组合”)

例 2.1.1. 若 $a|n, b|n$, 且存在整数 x, y, 使得 $ax+by=1$, 证明: $ab \mid n$.

证明. 由条件, 可设 $n=au, n=bv, u, v$ 为整数. 于是

$$\begin{aligned} n &= n(ax+by) \\ &= nax+nby \\ &= abvx+abuy \\ &= ab(vx+uy). \end{aligned}$$

因此

$$ab \mid n.$$

□

注记. *一般地, 由 $a|n, b|n$, 并不能推出 $ab \mid n$, 例如 $2|6, 6|6$, 但 $12 \nmid 6$. 题中给出的条件实质上表明 a, b 的最大公因数 (见 1.3 节) 为 1 , 即 a 与 b 互素, 在此条件下可推出 $ab \mid n$.*

例 2.1.2. 证明: 无论在数 12008 的两个 0 之间添加多少个 3 , 所得的数都是 19 的倍数.

证明. 记 $a_0=12008, a_n=120\underbrace{3\cdots 3}_{n个3}08, n=1,2,\cdots$.

首先, 因为

$$a_0=19\times 632,$$

故

$$19 \mid a_0.$$

其次, 设 $19 \mid a_n$, 则由

$$a_{n+1}-10a_n=228=19\times 12,$$

可知

$$19 \mid a_{n+1}.$$

所以, 对一切整数 n , 数 a_n 都是 19 的倍数. □

注记. *此题的处理过程中运用了递推的思想, 其基本思路是将 a_{n+1} 表示为 a_n 与 19 的一个线性组合.*

例 2.1.3. 已知一个 1000 位正整数的任意连续 10 个数码形成的 10 位数是 2^{10} 的倍数. 证明: 该正整数为 2^{1000} 的倍数.

证明. 设该正整数 $x=\overline{a_1a_2\cdots a_{1000}}$, 其中 a_i 是十进位数码. 由条件, 可知

$$2^{10}\ |\overline{a_{991}\cdots a_{1000}}, 2^{10}\mid\overline{a_{990}\cdots a_{999}}, \tag{2.1}$$

因此

$$2^{10}\mid\overline{a_{990}\cdots a_{999}}\times 10. \tag{2.2}$$

记 $y=\overline{a_{991}\cdots a_{999}}$, 则式 2.2又可写作

$$2^{10}\mid a_{990}\times 10^{10}+10y,$$

故

$$2^{10}\mid 10y.$$

结合 $2^{10}\mid\overline{a_{991}\cdots a_{1000}}$, 可知

$$2^{10}\mid 10y+a_{1000},$$

于是

$$2^{10}\mid a_{1000},$$

这要求

$$a_{1000}=0.$$

类似地, 朝前倒推, 可得

$$a_{11}=\cdots=a_{1000}=0,$$

即

$$x=\overline{a_1\cdots a_{10}}\times 10^{990}.$$

再结合条件 $2^{10}\mid\overline{a_1\cdots a_{10}}$, 即可得

$$2^{1000}\mid x.$$

□

注记. 这里先证明 $a_{11}=\cdots=a_{1000}=0$ 是非常关键的, 在证明中利用 $\overline{a_{991}\cdots a_{999}}$ 来过渡也是比较巧妙的.

例 2.1.4. 设 m 是一个大于 2 的正整数, 证明: 对任意正整数 n , 都有 $2^m-1\nmid 2^n+1$.

证明. 如果存在正整数 n, 使得 $2^m-1 \mid 2^n+1$, 那么取其中最小的那个 n .

由于 $m>2$, 知 $n>1$, 进一步, 应有 $2^n+1 \geqslant 2^m-1$, 知 $n \geqslant m$, 而 $n=m$ 时, 将导致 $2^m-1 \mid 2$, 矛盾, 故 $n>m$.

现在, 设 $2^n+1=(2^m-1)\,q$, 这里 q 为正整数, 则

$$2^n+2^m=(2^n+1)+(2^m-1)=(2^m-1)\,(q+1).$$

即

$$2^m\left(2^{n-m}+1\right)=(2^m-1)\,(q+1)$$

于是,

$$\left(2^{n-m}+1\right)+(2^m-1)\left(2^{n-m}+1\right)=(2^m-1)\,(q+1),$$

得 $2^{n-m}+1=(2^m-1)\left(q-2^{n-m}\right)$, 因此, $2^m-1 \mid 2^{n-m}+1$, 与 n 的最小性矛盾.

所以, 命题成立. □

注记. 这里用到了两个结论: 一个是“若 $a \mid b, b \neq 0$, 则 $|a| \leqslant |b|$”, 它由整除的定义可直接证出. 另一个是“任意多个正整数中必有最小元”, 这是著名的“最小数原理”.

2.1.2 素数与合数

对任意正整数 $n>1$, 如果除 1 与 n 以外, n 没有其他的因数, 那么称 n 为素数. 否则称 n 为合数. 这样, 我们将正整数分为了三类: 1 , 素数, 合数.

素数从小到大依次为 $2,3,5,7,11,\cdots$. 我们可以非常轻松地写出 100 以内的所有素数, 共 25 个. 但是并不是对每个素数 p , 都能轻易地指出 p 后面的一个素数是多少. 事实上, 当 p 比较大时, 求出它后面的那个素数是十分困难的. 正是素数的这种无规律性, 初等数论才显得魅力无穷, 具有很强的挑战性和极大的吸引力. 素数与合数具有如下的一些性质.

性质 2.1.4. 设 n 为大于 1 的正整数, p 是 n 的大于 1 的因数中最小的正整数, 则 p 为素数.

性质 2.1.5. 如果对任意 1 到 $\sqrt{n}$ 之间的素数 p, 都有 $p \nmid n$, 那么 n 为素数. 这里 $n(>1)$ 为正整数.

证明. 事实上, 若 n 为合数, 则可写 $n=pq, 2 \leqslant p \leqslant q$. 因此 $p^2 \leqslant n$, 即 $p \leqslant \sqrt{n}$.

这表明 p 的素因子 $\leqslant \sqrt{n}$, 且它是 n 的因数, 与条件矛盾. 因此 n 为素数. □

注记. 这里素因子是指正整数的因数中为素数的那些数, 此性质是我们检验一个数是否为素数的最常用的方法.

性质 2.1.6. 素数有无穷多个.

证明. 若只有有限个素数, 设它们是 $p_1 < p_2 < \cdots < p_n$. 考虑数

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

其最小的大于 1 的因数 p, 它是一个素数, 因此, p 应为 $p_1, p_2, \cdots, p_n$ 中的某个数. 设 $p = p_i, 1 \leqslant i \leqslant n$, 并且 $x = p_i y$, 则 $p_1 p_2 \cdots p_n + 1 = p_i y$, 即

$$p_i(y - p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n) = 1.$$

这导致 $p_i \mid 1$. 矛盾.

所以, 素数有无穷多个. □

注记. 如果将所有的素数从小到大依次写出为 $2 = p_1 < p_2 < \cdots$, 并写 $q_n = p_1 p_2 \cdots p_n + 1$, 那么

$$q_1 = 3, q_2 = 7, q_3 = 31, q_4 = 211, q_5 = 2311$$

它们都是素数. 是否每一个 n 都有 q_n 为素数呢? 我们不能被表面现象所迷惑, 再朝下算, 可知 $q_6 = 59 \times 509$ 就是一个合数. 事实上, 后面的 q_7, q_8, q_9, q_{10} 都是合数. 到目前为止, 人们还不知道数列 $q_1, q_2, \cdots$ 中是否有无穷多个素数, 也不知道其中是否有无穷多个合数.

性质 2.1.7. 素数中只有一个数是偶数, 它是 2.

例 2.1.5. 设 n 为大于 1 的正整数. 证明: 数 $n^5 + n^4 + 1$ 不是素数.

证明. 注意到

$$\begin{aligned} & n^5 + n^4 + 1 && (2.3)\\ =& n^5 + n^4 + n^3 - \left(n^3 - 1\right) && (2.4)\\ =& n^3\left(n^2 + n + 1\right) - (n-1)\left(n^2 + n + 1\right) && (2.5)\\ =& \left(n^3 - n + 1\right)\left(n^2 + n + 1\right) && (2.6) \end{aligned}$$

因此, 若 $n^5 + n^4 + 1$ 为素数, 则 $n^3 - n + 1 = 1$, 这要求 $n = 0$ 或 ± 1 .
故当 $n > 1$ 时, $n^5 + n^4 + 1$ 不是素数. □

注记. 利用因式分解来判断一个数是否为素数是数论中的常见方法, 后面也将不断用到.

例 2.1.6. 考察下面的数列:

$$101, 10101, 1010101, \cdots$$

问: 该数列中有多少个素数?

解. 易知 101 是素数. 下证这是该数列中仅有的一个素数.

记 $a_n=1\underbrace{0101\cdots01}_{n\text{ 个}01}$, 则当 $n\geqslant 2$ 时, 有

$$\begin{aligned}a_n&=10^{2n}+10^{2(n-1)}+\cdots+1\\&=\frac{10^{2(n+1)}-1}{10^2-1}\\&=\frac{\left(10^{n+1}-1\right)\left(10^{n+1}+1\right)}{99}.\end{aligned}$$

注意到, $99<10^{n+1}-1, 99<10^{n+1}+1$, 而 a_n 为正整数, 故 a_n 是一个合数 (因为分子中的项 $10^{n+1}-1$ 与 $10^{n+1}+1$ 都不能被 99 约为 1).

注记. *这里需要将因式分解式 $x^n-1=(x-1)\left(x^{n-1}+x^{n-2}+\cdots+1\right)$ 反用, 高中阶段它被作为等比数列求和的公式.*

例 2.1.7. 求所有的正整数 n, 使得 $\frac{n(n+1)}{2}-1$ 是一个素数.

解. 记 $a_n=\frac{n(n+1)}{2}-1$, 则 $a_1=0$ 不是素数, 因此只需讨论 $n>1$ 的情形. 我们利用 n 只能是形如 $4k,4k+1,4k+2,4k+3$ 的数分别讨论.

当 n 是形如 $4k+2$ 或 $4k+1$ 的数时, a_n 都是偶数, 要 a_n 为素数, 只能是

$$\frac{n(n+1)}{2}-1=2$$
$$n=2$$

解得

当 $n=4k$ 时, 可得

$$\begin{aligned}a_n&=2k(4k+1)-1 &(2.7)\\&=8k^2+2k-1 &(2.8)\\&=(4k-1)(2k+1), &(2.9)\end{aligned}$$

这是一个合数.

当 $n=4k+3$ 时, 可得

$$\begin{aligned}a_n&=2(k+1)(4k+3)-1 &(2.10)\\&=8k^2+14k+5 &(2.11)\\&=(4k+5)(2k+1), &(2.12)\end{aligned}$$

仅当 $k=0$, 即 $n=3$ 时, a_n 为素数.

所以, 满足条件的 $n=2$ 或 3.

注记. *对 n 分类处理一方面是去分母的需要, 另一方面是为进行因式分解做准备.*

例 2.1.8. 对任意正整数 n , 证明: 存在连续 n 个正整数, 它们都是合数.

证明. 设 n 为正整数, 则

$$(n+1)!+2,(n+1)!+3,\cdots,(n+1)!+(n+1)$$

是 n 个连续正整数, 并且第 k 个数是 $k+1$ 的倍数 (且大于 $k+1$), 故它们是连续的 n 个合数. □

注记. 这个结论表明: 对任意正整数 n , 都存在两个素数, 它们之间至少有 n 个数, 且这些数都是合数. 但是, 让我们来看一些素数对 $(3,5),(5,7),(11,13),(17,19),\cdots,(1997,1999)$, 它们他们所含的两个素数都只相差 2(这是两个奇素数的最小差距), 这样的素数对称为孪生素数. 是否存在无穷多对素数, 它们是孪生素数? 这是数论中一个未解决的著名问题.

例 2.1.9. 设 n 为大于 2 的正整数. 证明: 存在一个素数 p , 满足 $n<p<n!$.

证明. 设 $p_1<p_2<\cdots<p_k$, 且 $p_1,p_2,\cdots,p_k$ 是所有不超过 n 的素数, 考虑数

$$q=p_1p_2\cdots p_k-1$$

在 $n>2$ 时, 2,3 都在 $p_1,\cdots,p_k$ 中出现, 故 $5\leqslant q\leqslant n!-1<n!$, 利用性质 2.1.6证明中的方法, 可知 q 的素因子 p 不等于 $p_1,p_2,\cdots,p_k$ 中的任何一个. 而 $p_1,p_2,\cdots,p_k$ 是所有不超过 n 的素数, 因此 $p>n$, 所以 $n<p\leqslant q<n!$.

从而, 命题成立. □

注记. 利用本题的结论亦可证出: 素数有无穷多个. 贝特朗曾猜测在 $m>1$ 时, 正整数 m 与 $2m$ 之间 (不包括 m 与 $2m$) 有一个素数. 如果将素数从小到大排列为 $p_1<p_2<\cdots$, 该猜测亦即 $p_{n+1}<2p_n$. 这个猜测被契比雪夫证明了. 因此它被称为贝特朗猜想或契比雪夫定理.

例 2.1.10. 设 a,b,c,d,e,f 都是正整数, $S=a+b+c+d+e+f$ 是 $abc+def$ 和 $ab+bc+ca-de-ef-ed$ 的因数. 证明: S 为合数.

证明. 考虑多项式

$$f(x)=(x+a)(x+b)(x+c)-(x-d)(x-e)(x-f)$$

展开后, 可知

$$f(x)=Sx^2+(ab+bc+ca-de-ef-fd)x+(abc+def)$$

由条件可知, 对任意 $x\in\mathbb{Z}$, 都有 $S\mid f(x)$. 特别地, 取 $x=d$, 就有 $S\mid f(d)$, 即 $S\mid(d+a)(d+b)(d+c)$. 由于 a,b,c,d,e,f 都为正整数, 故 $d+a,d+b$, $d+c$ 都小于 S, 所以, S 为合数. □

注记. 对比例 2.1.6, 两个例子中分别用到下面的结论: 若 x,y,z 为正整数, 且 $\frac{xy}{z}$ 亦为整数, 则如果 $x,y>z$, 那么 $\frac{xy}{z}$ 为合数; 如果 $x,y<z$, 那么 z 为合数.

2.1.3 最大公因数与最小公倍数

设 a,b 是不全为零的两个整数, d 是一个非零整数, 如果 $d\mid a$ 且 $d\mid b$, 那么称 d 为 a,b 的公因数.

注意到, 当 $d\mid a$ 且 $d\mid b$ 时, 则 $d\leqslant|a|$ 或 $d\leqslant|b|$ 中必有一个成立 (对 a,b 中不为零的数成立). 因此, a,b 的公因数中有一个最大的, 这个数称为 a,b 的最大公因数, 记为 (a,b) . 如果 $(a,b)=1$, 那么我们称 a,b 互素.

在讨论最大公因数的性质之前, 我们不加证明地引入一个在小学就接触到的、数论中最基本、最常用的结论.

定理 2.1.1 (带余数除法)**.** 设 a, b 是两个整数, $a \neq 0$, 则存在唯一的一对整数 q 和 r, 满足

$$b = aq + r, 0 \leqslant r < |b|$$

其中 q 称为 b 除以 a 所得的商, r 称为 b 除以 a 所得的余数.

性质 2.1.8 (贝祖 (Bezout) 定理)**.** 设 $d = (a, b)$, 则存在整数 x, y , 使得

$$ax + by = d$$

证明. 我们利用带余除法来处理, 此结论的证明过程又是求 a, b 的最大公因数的过程, 它被称为"辗转相除".

不妨设 a, b 都不为零 (当 a, b 中有一个为零时, 结论是显然的), 且 $|a| \leqslant |b|$.

设 $b = aq_1 + r_1$, 其中 $0 \leqslant r_1 < |a|, q_1, r_1$ 为整数. 若 $r_1 = 0$, 则辗转相

除到此为止; 否则用 a 去除以 r_1, 得等式 $a = r_1q_2 + r_2, 0 \leqslant r_2 < r_1$; 依此讨论, 由于 $r_1 > r_2 > r_3 > \cdots$, 因此辗转相除到某一步后, 所得的 $r_{k+1} = 0$, 于是, 我们得到了如下的一系列式子:

$$\begin{aligned}
b &= aq_1 + r_1, 0 < r_1 < |a| \\
a &= r_1q_2 + r_2, 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2 \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
r_{k-2} &= r_{k-1}q_k + r_k, 0 < r_k < r_{k-1} \\
r_{k-1} &= r_kq_{k+1}
\end{aligned}$$

注意到, 从第一个式子到第 k 个式子, 我们依次有

$$d\,|r_1, d|\,r_2, \cdots, d \mid r_k,$$

而从第 $k+1$ 个式子倒推, 又依次有

$$r_k\,|r_{k-1}, r_k|\,r_{k-2}, \cdots, r_k\,|r_1, r_k|\,a, r_k \mid b,$$

所以, r_k 又是 a, b 的公因数, 结合 d 为 a, b 的最大公因数知 $r_k \leqslant d$, 又 $d \mid r_k$, 故 $d \leqslant r_k$, 因此, $d = r_k$. 也就是说, 我们求出了 a, b 的最大公因数.

现在, 利用 $d = r_k$ 及第 k 个式子, 可知

$$d = r_{k-2} - r_{k-1}q_k$$

再由

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}(\text{ 第}k-1\text{ 个式子变形得}),$$

代入上式, 可知 d 可以表示为 r_{k-2} 与 r_{k-3} 的"线性组合"(见性质 2.1.3), 依此倒推, 可知 d 可以表示为 a, b 的"线性组合", 即存在整数 x, y 使得

$$d = ax + by.$$

□

注记. 反过来, 设 x, y 为整数, $d' = ax + by$, 并不能推出 d' 为 a, b 的最大公因数. 事实上, 可以证明: a, b 的最大公因数是形如 $ax + by$ (x, y 为任意整数) 的正整数中最小的那个.

性质 2.1.9. 设 d 为 a, b 的公因数, 则 $d \mid (a, b)$.

这个性质可由前面的贝祖定理证出. 事实上, 贝祖定理也是初等数论中的一个基本定理, 应用非常广泛, 下面的性质是它的一个直接推论.

性质 2.1.10. 设 a, b 是不全为零的整数, 则 a 与 b 互素的充要条件是存在整数 x, y 满足

$$ax + by = 1$$

性质 2.1.11. 设 $a|c, b|c$, 且 $(a, b) = 1$, 则 $ab \mid c$.

这个性质的证明见例 2.1.1.

性质 2.1.12. 设 $a \mid bc$, 且 $(a, b) = 1$, 则 $a \mid c$.

证明. 由性质 2.1.10, 知存在整数 x, y 使得

$$ax + by = 1$$

故 $acx + bcy = c$, 由 $a \mid bc$ 及 $a \mid acx$, 可知 $a \mid c$. □

性质 2.1.13. 设 p 为素数, $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$.

证明. 由于 p 只有两个正约数, 故 $(p, a) = 1$ 或者 $(p, a) = p$. 若 $(p, a) = 1$, 则由性质 5 知 $p \mid b$; 若 $(p, a) = p$, 则 $p \mid a$. □

下面引入公倍数的一些概念和性质.

设 a, b 都是不等于零的整数, 如果整数 c 满足 $a \mid c$ 且 $b \mid c$, 那么称 c 为 a, b 的公倍数. 在 a, b 的所有正的公倍数中, 最小的那个称为 a, b 的最小公倍数, 记作 $[a, b]$.

性质 2.1.14. 设 a, b 为非零整数, d, c 分别是 a, b 的一个公因数与公倍数, 则 $d|(a, b), [a, b]|c$.

证明. 这个性质在本质上反映了最大公因数与最小公倍数的属性. 前者是性质 2.1.9的结论, 这里再次列出是为了对比.

对于后者, 采用反证法予以证明.

若 $[a, b] \nmid c$, 设 $c = [a, b] \cdot q + r, 0 < r < [a, b]$, 则由 $a \mid c$ 及 $a \mid [a, b]$, 可知 $a \mid r$, 同理 $b \mid r$, 即 r 为 a, b 的公倍数, 但 $r < [a, b]$, 这与 $[a, b]$ 是 a, b 的最小公倍数矛盾. 所以 $[a, b] \mid c$. □

性质 2.1.15. 设 a, b 都是正整数, 则 $[a, b] = \frac{ab}{(a,b)}$.

证明. 记 $c=\frac{ab}{(a,b)}$, 则由 $(a,b)\mid a$ 及 $(a,b)\mid b$ 知 $b|c, a|c$. 即 c 为 a,b 的公倍数, 故 $[a,b]\mid c$.

反过来, 由贝祖定理, 知存在整数 x,y , 使得

$$ax+by=(a,b),$$

即

$$\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=1,$$

于是

$$\frac{a[a,b]}{(a,b)}x+\frac{b[a,b]}{(a,b)}y=[a,b],$$

由 $b\mid[a,b]$ 及 $a\mid[a,b]$, 可知

$$c\left|\frac{a[a,b]}{(a,b)}, c\right|\frac{b[a,b]}{(a,b)},$$

所以

$$c\mid[a,b],$$

综上, 可知

$$[a,b]=\frac{ab}{(a,b)}.$$

□

一般地, 对 n 个整数 (非零) $a_1,a_2,\cdots,a_n$, 可以类似地引入最大公因数与最小公倍数的概念, 分别记为 $(a_1,a_2,\cdots,a_n)$ 和 $[a_1,a_2,\cdots,a_n]$. 容易得到下面的一些结论:

性质 2.1.16. $(a_1,a_2,a_3,\cdots,a_n)=\big((a_1,a_2),a_3,\cdots,a_n\big)$;
而 $[a_1,a_2,\ a_3,\cdots,a_n]=\big[[a_1,a_2],a_3,\cdots,a_n\big]$.

性质 2.1.17. 存在整数 $x_1,x_2,\cdots,x_n$, 使得

$$a_1x_1+a_2x_2+\cdots+a_nx_n=(a_1,a_2,\cdots,a_n)$$

特别地, $(a_1,a_2,\cdots,a_n)=1$, 即 $a_1,a_2,\cdots,a_n$ 互素的充要条件是: 存在整数 $x_1,x_2,\cdots,x_n$, 使得

$$a_1x_1+a_2x_2+\cdots+a_nx_n=1$$

注意, n 个数互素, 并不能保证它们两两互素, 例如 ($2\times3,2\times5,3\times\ 5)=1$, 但 6, 10, 15 两两不互素. 反过来, 若 n 个数中有两个数互素, 则这 n 个数互素. 因此, 在 n 个数中, ” 两两互素” 的条件比” 它们互素” 的条件要强得多.

性质 2.1.18. 设 m 为正整数，则

$$(ma_1, ma_2, \cdots, ma_n) = m(a_1, a_2, \cdots, a_n), \tag{2.13}$$

$$[ma_1, ma_2, \cdots, ma_n] = m[a_1, a_2, \cdots, a_n]. \tag{2.14}$$

例 2.1.11. 设 a, b 为正整数，且 $\frac{ab}{a+b}$ 也是正整数. 证明：$(a, b) > 1$.

证明. 若 $(a, b) = 1$ ，则 $(a, a+b) = 1$ (这由性质 2.1.13可推得)，从而，由 $a+b \mid ab$ 及 $(a, a+b) = 1$ ，得 $a+b \mid b$ ，但是 $a+b > b$ ，故 $a+b \mid b$ 不可能成立. 所以，$(a, b) > 1$. □

注记. 在辗转相除求 a, b 的公因数的讨论中，可知对任意整数 x ，都有 $(a, b) = (a, b+ax)$，这一点在利用最大公因数处理数论问题时经常被用到.

例 2.1.12. 设正整数 a, b, c 满足 $b^2 = ac$. 证明：$(a, b)^2 = a(a, c)$.

证明. 如果我们能够证明：$(a, b)^2 = \left(a^2, b^2\right)$ ，那么结合性质 2.1.18，可知

$$(a, b)^2 = \left(a^2, b^2\right) = \left(a^2, ac\right) = a(a, c),$$

命题获证.

为此，记 $d = (a, b)$ ，设 $a = du, b = dv$ ，则由性质 2.1.18可知 u, v 是两个互素的正整数，为证 $\left(a^2, b^2\right) = d^2$ ，只需证明：$\left(u^2, v^2\right) = 1$.

利用贝祖定理，知存在整数 x, y ，使得 $ux + vy = 1$ ，故 $u^2x^2 = (1 - vy)^2 = 1 + v\left(vy^2 - 2y\right)$ ，结合性质 3 可知 $\left(u^2, v\right) = 1$ ，交换 u^2 与 v 的位置，同上再做一次，即有 $\left(v^2, u^2\right) = 1$.

所以，命题成立. □

注记. 利用下一节的算术基本定理可以非常方便地证出：$\left(a^2, b^2\right) = (a, b)^2$ ，但遗憾的是我们还没给出该定理的证明，通常都是先建立最大公因数理论再去证算术基本定理，这里不用该定理是不希望掉入”循环论证”的旋涡，读者在学习中应认真掌握其中的逻辑结构.

例 2.1.13. 求所有的正整数 $a, b(a \leqslant b)$ ，使得

$$ab = 300 + 7[a, b] + 5(a, b). \tag{2.15}$$

解. 设 $[a, b] = x, (a, b) = y$ ，由性质 2.1.15可知 $ab = xy$ ，于是，式 2.15变为

$$xy = 300 + 7x + 5y,$$

即 $(x-5)(y-7) = 5 \times 67$.

由于 $[a, b] \geqslant (a, b)$，故 $x \geqslant y$，进而 $x - 5 > y - 7$，只有如下的两种情形.

情形一 $x - 5 = 67$ 且 $y - 7 = 5$ ；此时，$x = 72, y = 12$ ，于是，可设 $a = 12n, b = 12m, (m, n) = 1$ ，并有 $(12n)(12m) = ab = xy = 12 \times 72$ ，结合 $a \leqslant b$ ，只能是 $(m, n) = (1, 6)$ 或 $(2, 3)$ ，对应的 $(a, b) = (12, 72)$ 或 $(24\ ,\ 36)$.

情形二 $x - 5 = 335$ 且 $y - 7 = 1$ ；对应地，$x = 340, y = 8$ ，但 $y = (a,\ b)$ 是 $x = [a, b]$ 的因数，而 $8 \nmid 340$ ，所以，此时无解.

综上，符合条件的 $(a, b) = (12, 72)$ 或 $(24, 36)$.

例 2.1.14. 求所有的正整数 a,b, 使得

$$(a,b)+9[a,b]+9(a+b)=7ab. \tag{2.16}$$

解. 记 $(a,b)=d$, 设 $a=dx, b=dy$, 则 $(x,y)=1$ (由性质 2.1.18知), $[a,b]=dxy$ (由性质 2.1.15知), 于是代入式 2.16可得

$$1+9xy+9(x+y)=7dxy, \tag{2.17}$$

$$7d=9+9\left(\frac{1}{x}+\frac{1}{y}\right)+\frac{1}{xy},$$

所以

$$9<7d\leqslant 9+9\left(\frac{1}{1}+\frac{1}{1}\right)+\frac{1}{1\times 1}=28,$$

故

$$2\leqslant d\leqslant 4,$$

当 $d=2$ 时, 由式 2.17得

$$5xy-9(x+y)=1,$$

两边乘以 5 , 并将左边因式分解, 得

$$(5x-9)(5y-9)=86=2\times 43,$$

故 $(5x-9,5y-9)=(1,86),(86,1),(2,43),(43,2)$. 分别求解可知只能是 $(x,y)=(2,19),(19,2)$, 对应的 $(a,b)=(4,38),(38,4)$.

分别就 $d=3,4$ 同上讨论, 得 $(a,b)=(4,4)$.

所以, 满足条件的 $(a,b)=(4,38),(38,4),(4,4)$.

例 2.1.15. Fibonacci 数列定义如下: $F_1=F_2=1, F_{n+2}=F_{n+1}+F_n, n=1$, $2,\cdots$. 证明: 对任意正整数 m,n , 都有 $(F_m,F_n)=F_{(m,n)}$.

证明. 当 $m=n$ 时, 命题显然成立. 现在不妨设 $m<n$, 注意到

$$\begin{aligned}
F_n&=F_2F_{n-1}+F_1F_{n-2}\\
&=F_2\left(F_{n-2}+F_{n-3}\right)+F_1F_{n-2}\\
&=\left(F_2+F_1\right)F_{n-2}+F_2F_{n-3}\\
&=F_3F_{n-2}+F_2F_{n-3}\\
&=F_3\left(F_{n-3}+F_{n-4}\right)+F_2F_{n-3}\\
&=F_4F_{n-3}+F_3F_{n-4}\\
&=\cdots\\
&=F_mF_{n-m+1}+F_{m-1}F_{n-m},
\end{aligned}$$

因此, 设 $d \mid F_m$ 且 $d \mid F_n$, 则由上式可知 $d \mid F_{m-1}F_{n\to m}$. 又对任意正整数 m, 有 $(F_m, F_{m-1}) = (F_{m-1}+F_{m-2}, F_{m-1}) = (F_{m-1}, F_{m-2}) = \cdots = (F_2, F_1) = 1$, 所以, $(d, F_{m-1}) = 1$, 故 $d \mid F_{n-m}$; 反过来, 若 $d' \mid F_{n-m}$ 且 $d' \mid F_m$, 则由上式又可知 $d' \mid F_n$. 依此可知 $(F_n, F_m) = (F_{n-m}, F_m)$.

利用上述结论, 对下标进行辗转相除, 就可证得 $(F_n, F_m) = F_{(m,n)}$.

说明由本题的结论还可以推出一个有趣的性质: 若 F_n 为素数, 则 $n=4$ 或者 n 为素数.

事实上, 设 F_n 为素数, 而 n 为合数, 可设 $n = p\cdot q, 2 \leqslant p \leqslant q, p, q$ 为正整数, 则由前面的结论, 可知 $\left(F_n, F_p\right) = F_{(n,p)} = F_p, \left(F_n, F_q\right) = F_{(n,q)} = F_q$. 结合 Fibonacci 数列的定义, 可知 $F_n > F_p, F_n > F_q$, 而 F_n 为素数, 故 $\left(F_n, F_p\right) = \left(F_n, F_q\right) = 1$, 所以, $F_p = F_q = 1$, 再由 $2 \leqslant p \leqslant q$, 可知只能是 $p = q = 2$, 即 $n = 4$. 所以, 性质成立. □

例 2.1.16. 设 n 为大于 1 的正整数. 证明: 存在从小到大排列后成等差数列 (即从第二项起, 每一项与它前面那项的差为常数的数列) 的 n 个正整数, 它们中任意两项互素.

证明. 考虑下面的 n 个数:

$$n!+1, 2\times(n!)+1, \cdots, n\times(n!)+1$$

这 n 个正整数组成一个公差为 $n!$ 的等差数列.

我们证明其中任意两项是互素的.

事实上, 若存在 $1 \leqslant i < j \leqslant n$, 使得数 $i\times(n!)+1$ 与数 $j\times(n!)+1$ 不互素, 设 $d = (i\times(n!)+1, j\times(n!)+1) > 1$. 考虑 d 的素因子 p, 可知

$$p \mid (j\times(n!)+1) - (i\times(n!)+1)$$

即 $p \mid (j-i)\times n!$. 由性质 6 知 $p \mid j-i$ 或 $p \mid n!$, 结合 $1 \leqslant j-i < n$, 可知 $(j-i) \mid n!$, 所以, 总有 $p \mid n!$. 但是, $p|d, d|i\times(n!)+1$, 故 $p \mid i\times(n!)+1$, 结合 $p \mid n!$, 导致 $p \mid 1$, 矛盾.

所以, 命题成立. □

注记. *此题为导出与反设矛盾的结论, 采用了素因子分析的方法. 该方法在数论中有广泛的应用.*

2.1.4 算术基本定理

在前面我们引入了素数与合数的概念, 对每个大于 1 的正整数 n, 如果 n 为合数, 那么可写 $n = n_1 n_2$, 其中 $2 \leqslant n_1 \leqslant n_2$. 再分别对 n_1, n_2 重复这样的讨论, 即可将 n 表示为一些素数的乘积. 对这个过程认真思考, 就能得到下面的重要定理, 在解数论的问题时经常会直接或间接地用到它.

定理 2.1.2 (算术基本定理). 设 n 是大于 1 的正整数, 则 n 可以分解成若干个素数的乘积的形式, 并且在不考虑这些素数相乘时的前后次序时, 这种分解是唯一的. 即对任意大于 1 的正整数 n, 都存在唯一的一种素因数分解形式:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

这里 $p_1 < p_2 < \cdots < p_k$ 为素数, $\alpha_1, \alpha_2, \cdots, \alpha_k$ 为正整数.

证明. 利用前面的分析, 可证得存在性, 下面证明唯一性.

若 n 有两种素因数分解形式:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_2}$$

其中 $p_1 < p_2 < \cdots < p_k, q_1 < q_2 < \cdots < q_l$, 且都是素数, α_i, β_j 都为正整数, $1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l$.

我们证明 $k = l$ 且 $p_i = q_i, \alpha_i = \beta_i$.

事实上, 由 (1) 知 $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$, 利用性质 2.1.13可知, 存在某个 j 使 $p_i \mid q_j^{\beta_j}$, 再用一次性质 2.1.13, 知 $p_i \mid q_j$, 这要求 $p_i = q_j$. 即对 $1 \leqslant i \leqslant k$ 及每个 p_i , 在 $q_1, q_2, \cdots, q_l$ 中总有一个 q_j , 使得 $p_i = q_j$. 反过来对 q_j 分析, 又有对 $1 \leqslant j \leqslant l$ 及每个 q_j , 在 $p_1, p_2, \cdots, p_k$ 中总有一个 p_i , 使得 $q_j = p_i$. 这表明 $k = l$, 且 $q_1, q_2, \cdots, q_l$ 是 $p_1, p_2, \cdots, p_k$ 的一个排列, 结合 $p_1 < p_2 < \cdots < p_k$ 及 $q_1 < q_2 < \cdots < q_l$, 知 $p_i = q_i, 1 \leqslant i \leqslant k$. 进一步证明 $\alpha_i = \beta_i$ 是容易的. □

利用正整数 n 的素因数分解式, 我们可以简单地得到下面的一些结论.

推论 2.1.1. 设 n 的所有正因数 (包括 1 和 n) 的个数为 $d(n)$, 那么

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

由此公式易知: n 是一个完全平方数的充要条件是 $d(n)$ 为奇数.

推论 2.1.2. 设 n 的所有正因数之和为 $\sigma(n)$, 那么

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k})$$

由此可知: $\sigma(n)$ 为奇数的充要条件是 n 为完全平方数或者某个完全平方数的两倍.

推论 2.1.3. 设 n, m 的素因数分解分别为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

这里 $p_1 < p_2 < \cdots < p_k$, 都为素数, α_i, β_i 都是非负整数, 并且对每个 $1 \leqslant i \leqslant k, \alpha_i$ 与 β_i 不全为零, 那么, 我们有 $(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$; $[m, n] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$, 其中 $\gamma_i = \min\{\alpha_i, \beta_i\}, \delta_i = \max\{\alpha_i, \beta_i\}, 1 \leqslant i \leqslant k$.

例 2.1.17. 在一个走廊上依次排列着编号为 $1, 2, \cdots, 2012$ 的灯共 2012 盏, 最初每盏灯的状态都是开着的. 一个好动的学生做了下面的 2012 次操作: 对 $1 \leqslant k \leqslant 2012$, 该学生第 k 次操作时, 将所有编号是 k 的倍数的灯的开关都拉了一下. 问: 最后还有多少盏灯是开着的?(提示: $44^2 = 1936, 45^2 = 2025$)

解. 设 $1 \leqslant n \leqslant 2012$, 我们来考察第 n 盏灯的状态, 依题意, 该盏灯的开关被拉了 $d(n)$ 次. 而偶数次拉动开关不改变灯的初始状态, 奇数次拉动开关, 灯的状态与初始状态不同.

利用 $d(n)$ 的性质及前面的讨论, 因为 $1, 2, \cdots, 2012$ 中恰有 44 个数为完全平方数, 可知最后还有 $2012 - 44 = 1968$ 盛灯是开着的.

例 2.1.18. 求所有的正整数 n, 使得 $n=d(n)^2$.

解. 当 $n=1$ 时, 符合条件, 下面考虑 $n>1$ 的情形.

由条件知 n 为完全平方数, 因此 $d(n)$ 为奇数, 设 $d(n)=2k+1$. 鉴于对任意正整数 d, 当 $d\mid n$ 时, 有 $\frac{n}{d}\Big| n$, 因此, 我们将 d 与 $\frac{n}{d}$ 配对后, 可知 $d(n)$ 等于数 $1,2,\cdots,2k-1$ 中为 n 的因数的个数的两倍加上 1 . 又 $1,2,\cdots,2k-1$ 中的偶数都不是 $n\left(=(2k+1)^2\right)$ 的因数, 因此结合 $d(n)=2k+1$, 可知 1 , $2,\cdots,2k-1$ 中的每一个奇数都是 n 的因数.

注意到, 当 $k>1$ 时, $(2k-1,2k+1)=(2k-1,2)=1$, 故 $2k-1\nmid(2k+1)^2$. 所以 $k>1$ 时, $n=(2k+1)^2$ 不符合要求, 故 $k=1,n$ 只能等于 9 .

直接验证, 可知 1 和 9 满足条件, 所以 $n=1$ 或 9.

注记. 此题考虑了 n 的因数关于 $\sqrt{n}$ 的对称性, 分析出一个非常强的条件, 从而解决了问题.

它还有一个一般性的处理方法, 需要用到如下的估计: 设 p 为不小于 5 的素数, 则 $p^\alpha>(\alpha+1)^2$. 而 $\alpha\geqslant 2$ 时, $3^\alpha\geqslant(\alpha+1)^2$. 这两个不等式都可以用数学归纳法予以证明 (对 α 归纳).

现在设 $n(>1)$ 是一个满足条件的正整数, 则 n 为一个奇数的平方, 于是, 可设 $n=3^\alpha\cdot p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$, 其中 $3<p_1<p_2<\cdots<p_k$, 并且 $\alpha,\beta_1,\beta_2,\cdots,\beta_k$ 都是偶数. 如果 $k>0$, 那么由前面的分析, 知 $n>(\alpha+1)^2\left(\beta_1+1\right)^2\cdot\left(\beta_2+1\right)^2\cdots\left(\beta_k+1\right)^2=d(n)^2$, 矛盾, 故 $n=3^\alpha$. 进一步分析, 可知 $\alpha>2$ 时, 有 $3^\alpha>(\alpha+1)^2$, 故 $\alpha=2$, 即 $n=9$.

例 2.1.19. 设 n 为正整数. 证明: 数 $2^{2^n}+2^{2^{n-1}}+1$ 至少有 n 个不同的素因子.

证明. 我们作如下的分解:

$$
\begin{aligned}
&2^{2^n}+2^{2^{n-1}}+1\\
=&\left(2^{2^{n-1}}+1\right)^2-2^{2^{n-1}}\\
=&\left(2^{2^{n-1}}+2^{2^{n-2}}+1\right)\left(2^{2^{n-1}}-2^{2^{n-2}}+1\right)\\
=&\left(2^{2^{n-2}}+2^{2^{n-3}}+1\right)\left(2^{2^{n-2}}-2^{2^{n-3}}+1\right)\left(2^{2^{n-1}}-2^{2^{n-2}}+1\right)\\
=&\cdots\\
=&\left(2^{2^1}+2^{2^0}+1\right)\left(2^{2^1}-2^{2^0}+1\right)\left(2^{2^2}-2^{2^1}+1\right)\cdots\left(2^{2^{n-1}}-2^{2^{n-2}}+1\right)
\end{aligned}
$$

这样, 我们将 $2^{2^n}+2^{2^{n-1}}+1$ 表示为 n 个大于 1 的正整数之积, 为证明它有 n 个不同的素因子, 只需证明这 n 个大于 1 的正整数两两互素.

注意到, 当 $m>l$ 时, $2^{2^l}+2^{2^{L-1}}+1$ 与 $2^{2^l}-2^{2^{L-1}}+1$ 都是 $2^{2^m}+2^{2^{m-1}}+1$ 的因数, 因此

$$
\begin{aligned}
&\left(2^{2^m}-2^{2^{m-1}}+1,2^{2^l}\pm 2^{2^{L-1}}+1\right) &(2.18)\\
\leqslant&\left(2^{2^m}-2^{2^{m-1}}+1,2^{2^m}+2^{2^{m-1}}+1\right) &(2.19)\\
=&\left(2^{2^m}-2^{2^{m-1}}+1,2\times 2^{2m-1}\right) &(2.20)
\end{aligned}
$$

由于, $2\times 2^{2m-1}$ 中只有一个素因子 2 , 而 $2^{2^m}-2^{2^{m-1}}+1$ 为奇数, 故

$$\left(2^{2^m}-2^{2^{m-1}}+1, 2\times 2^{2^{m-1}}\right)=1,$$

因此

$$\left(2^{2^m}-2^{2m-1}+1, 2^{2^l}\pm 2^{2^{2-1}}+1\right)=1.$$

所以, $2^{2^1}+2^{2^0}+1, 2^{2^1}-2^{2^0}+1, 2^{2^2}-2^{2^1}+1, \cdots, 2^{2^{n-1}}-2^{2^{n-2}}+1$ 两两互素, 进而 $2^{2^n}+2^{2^{n-1}}+1$ 至少有 n 个不同的素因子. □

例 2.1.20. 设 m,n 是正整数, 且 m 的所有正因数之积等于 n 的所有正因数之积. 问: m 与 n 是否必须相等?

解. m 与 n 必须相等.

事实上, 将 m 的正因数 d 与 $\frac{m}{d}$ 配对, 可知 m 的所有正因数之积为 $m^{\frac{d(m)}{2}}$, 因此, 条件等价于

$$m^{d(n)}=n^{d(n)}, \tag{2.21}$$

此式表明 m,n 有相同的素因子, 可设

$$m=p_1^{a_1}p_2^{a_2}\cdots p_k^{\alpha_k}, n=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k},$$

其中 $p_1<p_2<\cdots<p_k$ 为素数 α_i 与 β_i 都是正整数, $1\leqslant i\leqslant k$.

代入2.21式, 利用算术基本定理, 可知

$$\alpha_i d(m)=\beta_i d(n), 1\leqslant i\leqslant k, \tag{2.22}$$

若 $d(m)>d(n)$, 则对 $1\leqslant i\leqslant k$, 都有 $\alpha_i<\beta_i$, 于是, $\alpha_i+1<\beta_i+1$, 故 $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)<(\beta_1+1)(\beta_2+1)\cdots(\beta_k+1)$, 这导致 $d(m)<d(n)$, 矛盾. 同样, 由 $d(m)<d(n)$, 利用2.22式也可导出矛盾. 所以 $d(m)=d(n)$, 进而由2.21式得 $m=n$.

注记. *一般地, 由 $\sigma(m)=\sigma(n)$ (即考虑 m,n 所有正因数之和) 并不能导出 $m=n$ (例如 $\sigma(6)=\sigma(11)=12$), 此题是对两个正整数的所有正因数作乘积方面的思考得出的结论.*

例 2.1.21. 求所有的正整数 x,y, 使得

$$y^x=x^{50}$$

解. 设 x,y 为满足条件的正整数, 并且 $x=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 为 x 的素因数分解式, 则

由 y 为正整数, 知对 $1\leqslant i\leqslant k$, 都有 $x\mid 50\alpha_i$. 现在先讨论 x 的素因子.

如果 x 有一个不同于 2 和 5 的素因子 p , 并设 $p^\alpha\|x$, 那么由前面的结果知 $x\mid 50\alpha$, 当然有 $p^\alpha\mid 50\alpha$, 又 $p\neq 2,5$, 故 $p^\alpha\mid\alpha$. 但是, 对任意素数 p 及正整数 α , 有 $p^\alpha>\alpha$, 所以, $p^\alpha\mid\alpha$ 不能成立, 这表明 x 的素因子只能为 2 或 5 .

于是, 我们可设 $x=2^\alpha\cdot 5^\beta$ (其中 α,β 为非负整数), 这时 $x|50\alpha, x|50\beta$, 故 $2^\alpha\left|50\alpha, 5^\beta\right|50\beta$, 前者要求 $2^{\alpha-1}\mid\alpha$, 后者要求 $5^{\beta-2}\mid\beta$. 注意到, 当 $\alpha\geqslant 3$ 时, $2^{\alpha-1}>\alpha$, 而 $\beta\geqslant 3$ 时, $5^{\beta-2}>\beta$, 所以, $0\leqslant\alpha\leqslant 2, 0\leqslant\beta\leqslant 2$. 这表明 x 只能取 $1,2,2^2,5,5^2,2\times 5,2^2\times 5,2\times 5^2,2^2\times 5^2$.

将 x 的上述取值逐个代入 (1) 式, 可得到全部解为 $(x,y)=(1,1)$, $\left(2,2^{25}\right)$, $\left(2^2,2^{25}\right)$, $\left(5,5^{10}\right)$, $\left(5^2,5\right.$
共 8 组解.

注记. 上面两例直接用到算术基本定理, 所涉及的变量数看似增加或会变难, 但这时不等式估计的手段可介入, 问题求解反而有了着力点.

例 2.1.22. 给定正整数 $n>1$, 设 $d_1,d_2,\cdots,d_n$ 都是正整数, 满足: $(d_1,d_2,\cdots\ ,d_n)=1$, 且对 $j=1,2,\cdots,n$ 都有 $d_j\mid\sum_{i=1}^n d_i$ (这里 $\sum_{i=1}^n d_i=d_1+d_2+\cdots+\ d_n$).

(1) 证明: $d_1d_2\cdots d_n\mid\left(\sum_{i=1}^n d_i\right)^{n-2}$;

(2) 举例说明: $n>2$ 时, 上式右边的幂次不能减小.

证明. (1) 设 p 为 $d_1d_2\cdots d_n$ 的素因数, 且 k 为各 d_i 的素因数分解式中 p 的幂次的最大值, 则由 $d_j\mid\sum_{i=1}^n d_i$ 可知, $p^k\mid\sum_{i=1}^n d_i$, 故 $p^{k(n-2)}\mid\left(\sum_{i=1}^n d_i\right)^{n-2}$.

而 $(d_1,d_2,\cdots,d_n)=1$, 故存在 d_i , 使得 $p\nmid d_i$, 结合 $p\mid\sum_{i=1}^n d_i$, 可知 d_1 , $d_2,\cdots,d_n$ 中至少有两个数不是 p 的倍数. 所以, p 在 $d_1d_2\cdots d_n$ 中的幂次不超过 $k(n-2)$, 依此可知结论成立.

(2) 设 $d_1=1,d_2=n-1,d_i=n,3\leqslant i\leqslant n$, 则 $\sum_{i=1}^n d_i=n(n-1)$ 是每个 d_i 的倍数, 且 $(d_i,d_2,\cdots,d_n)=1$.

此时, $d_1d_2\cdots d_n=n^{n-2}(n-1)$, 结合 $(n,n-1)=1$, 可知满足 $n^{n-2}(n-\ 1)\mid(n(n-1))^m$ 的最小正整数 $m=n-2$. □

习题 1

1. 设 n 为大于 1 的正整数. 证明: n^4+4^n 是一个合数.

2. 求使得 $\left|4x^2-12x-27\right|$ 为素数的所有整数 x .

3. 设 m 为大于 1 的正整数, 且 $m \mid (m-1)!+1$. 证明: m 是一个素数.

4. 是否存在 3 个不同的素数 p,q,r , 使得下面的整除关系都成立?

$$qr\left|p^2+d,rp\right|q^2+d,pq \mid r^2+d$$

   其中 (1) $d=10;(2)d=11$.

5. 设 p 为正整数, 且 2^p-1 是素数. 求证: p 为素数.

6. 设 n 为正整数, 且 2^n+1 是素数. 证明: 存在非负整数 k , 使得 $n=2^k$.

7. 求所有形如 n^n+1 且不超过 10^{19} 的素数, 这里 n 为正整数.

8. 设 a,b,c,d 都是整数, 且 $a\neq c, a-c \mid ab+cd$. 证明: $a-c \mid ad+bc$.

9. 设 a,b,c,d 为整数, 且 $ac, bc+ad, bd$ 都是某个整数 u 的倍数. 证明: 数 bc 和 ad 也是 u 的倍数.

10. 设 a,b,n 为给定的正整数, 且对任意正整数 $k(\neq b)$, 都有 $b-k \mid a-k^n$. 证明: $a=b^n$.

11. 已知正整数 n 的正因数中, 末尾数字为 $0,1,2,\cdots,9$ 的正整数都至少有一个. 求满足条件的最小的 n .

12. 求一个 9 位数 M , 使得 M 的数码两两不同且都不为零, 并对 $m=2,3,\cdots,9$, 数 M 的左边 m 位数都是 m 的倍数.

13. 对于一个正整数 n , 若存在正整数 a,b , 使得 $n=ab+a+b$, 则称 n 是一个" 好数", 例如 $3=1\times1+1+1$, 故 3 为一个" 好数". 问: 在 $1,2,\cdots,100$ 中, 有多少个" 好数"?

14. 设素数从小到大依次为 $p_1,p_2,p_3,\cdots$. 证明: 当 $n\geqslant 2$ 时, 数 p_n+p_{n+1} 可以表示为 3 个大于 1 的正整数 (可以相同) 的乘积的形式.

15. 设 n 为大于 1 的正整数. 证明: n 为合数的充要条件是存在正整数 a,b , x,y , 使得 $n=a+b,\frac{x}{a}+\frac{y}{b}=1$.

16. 证明: 数列 $10001,100010001,1000100010001,\cdots$ 中, 每一个数都是合数.

17. 设 a,b,c,d 都是素数, 且 $a>3b>6c>12d, a^2-b^2+c^2-d^2=1749$. 求 $a^2+b^2+c^2+d^2$ 的所有可能值.

18. 数列 $\{a_n\}$ 的每一项都是正整数, $a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots$, 且对任意正整数 k , 该数列中恰有 k 项等于 k . 求所有的正整数 n , 使得 $a_1+a_2+\cdots+a_n$ 是素数.

19. 由正整数组成的数列 $\{a_n\}$ 满足: 对任意正整数 m , n , 若 $m \mid n, m<n$, 则 $a_m \mid a_n$, 且 $a_m<a_n$. 求 a_{2000} 的最小可能值.

20. 设 p 为奇素数, 正整数 m, n 满足 $\frac{m}{n}=1+\frac{1}{2}+\cdots+\frac{1}{p-1}$. 证明: $p \mid m$.

21. 设 a, m, n 为正整数, $a>1$, 且 $a^m+1 \mid a^n+1$. 证明: $m \mid n$.

22. 证明: 对任意正整数 n 及正奇数 m , 都有 $(2^m-1, 2^n+1)=1$.

23. 费马数 F_n 定义为 $F_n=2^{2^n}+1$. 证明: 对任意两个不同的正整数 m, n , 都有 $(F_n, F_m)=1$

24. 已知正整数 a, b, c, d 的最小公倍数为 $a+b+c+d$. 证明: $abcd$ 是 3 或 5 的倍数.

25. 记 M_n 为正整数 $1,2, \cdots, n$ 的最小公倍数. 求所有的正整数 $n(>1)$, 使得 $M_n=M_{n-1}$.

26. 设 a, m, n 为正整数, $a>1$. 证明: $(a^m-1, a^n-1)=a^{(m, n)}-1$.

27. 设 a, n 为正整数, $a>1$, 且 a^n+1 是素数. 证明: $d\left(a^n-1\right) \geqslant n$.

28. 对怎样的正整数 $n(>2)$, 存在 n 个连续正整数, 使得其中最大的数是其余 $n-1$ 个数的最小公倍数的因数?

29. 设正整数 a, b, m, n 满足: $(a, b)=1, a>1$, 且 $a^m+b^m \mid a^n+b^n$. 证明: $m \mid n$

30. 证明: 存在 2012 个不同的正整数, 使得其中任意两个不同的数 a, b 都满足 $(a-b)^2 \mid ab$.

31. 设 a, b 为正整数, 且 $(a, b)=1$. 证明: 对任意正整数 m , 数列

$$a, a+b, a+2b, \cdots, a+nb, \cdots$$

中, 有无穷多个数与 m 互素.

32. 已知正整数数对 (a, b) 满足: 数 $a^a \cdot b^b$ 在十进制表示下, 末尾恰有 98 个零. 求 ab 的最小值.

33. 求所有的正整数 m, 使得 $m=d(m)^4$.

34. 证明: 每一个正整数都可以表示为两个正整数之差, 且这两个正整数的素因子个数相同.

35. 求所有的正整数 a, b, c, 使得 a^2+1 和 b^2+1 都是素数, 且满足

$$\left(a^2+1\right)\left(b^2+1\right)=c^2+1$$

36. 用 $p(k)$ 表示正整数 k 的最大奇因数. 证明: 对任意正整数 n , 都有 $\frac{2}{3}n < \sum_{k=1}^{n} \frac{p(k)}{k} < \frac{2}{3}(n+1)$

37. 设 a,b,c 都是大于 1 的正整数. 求代数式 $\frac{a+b+c}{2} - \frac{[a,b]+[b,c]+[c,a]}{a+b+c}$ 的最小可能值.

38. 对任意给定的素数 p , 有多少个整数组 (a,b,c) , 使得 (1) $1 \leqslant a,b,c \leqslant 2p^2$; (2) $\frac{[a,c]+[b,c]}{a+b} = \frac{p^2+1}{p^2+2} \cdot c$.

39. 黑板上写着数 $1,2,\cdots,33$. 每次允许进行下面的操作: 从黑板上任取两个满足 $x \mid y$ 的数 x,y , 将它们从黑板上去掉, 写上数 $\frac{y}{x}$. 直至黑板上不存在这样的两个数. 问: 黑板上至少剩下多少个数?

40. 设 n 是一个正整数. 证明: 数 $1+5^n+5^{2n}+5^{3n}+5^{4n}$ 是一个合数.

2.2　同余

同余是由大数学家高斯引入的一个概念. 我们可以将它理解为" 余同", 即余数相同. 正如奇数与偶数是依能否被 2 整除而得到的关于整数的分类一样, 考虑除以 $m(\geqslant 2)$ 所得余数的不同, 可以将整数分为 m 类. 两个属于同一类中的数相对于" 参照物" m 而言, 具有" 余数相同" 这个性质. 这种为对比两个整数的性质, 引入一个参照物的思想是同余理论的一个基本出发点.

同余是初等数论中的一门语言, 是一件艺术品. 它为许多数论问题的表述赋予了统一的, 方便的和本质的形式.

2.2.1　同余的概念与基本性质

定义 2.2.1. 如果 a, b 除以 $m(\geqslant 1)$ 所得的余数相同, 那么称 a, b 对模 m 同余, 记作 $a \equiv b(\bmod m)$. 否则, 称 a, b 对模 m 不同余, 记作 $a \neq b(\bmod m)$.

性质 2.2.1. $a \equiv b(\bmod m)$ 的充要条件是 $m \mid a-b$.

性质 2.2.2. 若 $a \equiv b(\bmod m), c \equiv d(\bmod m)$, 则 $a+c \equiv b+d(\bmod m)$, $a-c \equiv b-d(\bmod m), ac \equiv bd(\bmod m)$.

证明. 这些结论与等式的一些相关结论极其相似, 它们都容易证明. 我们只给出第 3 个式子的证明.

只需证明: $m \mid ac-bd$.

因为

$$
\begin{aligned}
ac-bd &= ac-bc+bc-bd && (2.23)\\
&= (a-b)c+b(c-d) && (2.24)
\end{aligned}
$$

由条件 $m|a-b, m|c-d$, 知 $m \mid ac-bd$. □

注记. *与同余有关的许多结论都要用到性质 1, 事实上, 很多数论教材中利用性质 1 来引入同余的定义.*

性质 2.2.3. 若 $a \equiv b(\bmod m), n$ 为正整数, 则 $a^n \equiv b^n(\bmod m)$.

性质 2.2.4. 若 $a \equiv b\left(\bmod m_1\right), a \equiv b\left(\bmod m_2\right)$, 则 $a \equiv b\left(\bmod \left[m_1, m_2\right]\right)$.

性质 2.2.5. 若 $ab \equiv ac(\bmod m)$, 则 $b \equiv c\left(\bmod \frac{m}{(a, m)}\right)$.

在同余式两边约去一个数时, 应将该数与 m 的最大公因数在" 参照物" 中同时约去.

性质 2.2.6. 如果 $(a, m)=1$, 那么存在整数 b , 使得 $ab \equiv 1(\bmod m)$. 这个 b 称 a 对模 m 的数论倒数, 记为 $a^{-1}(\bmod m)$, 在不会引起误解时常常简记为 a^{-1} .

证明. 利用贝祖定理, 可知存在整数 x, y 使得

$$ax+my=1$$

于是, $m \mid ax-1$, 即 $ax \equiv 1(\bmod m)$, 故存在符合条件的 b . □

注记. 由数论倒数的定义, 易知当 $(a,m)=1$ 时, $\left(a^{-1}\right)^{-1} \equiv a(\bmod m)$.

例 2.2.1. 求所有的素数 $p,q,r(p \leqslant q \leqslant r)$, 使得

$$pq+r, pq+r^2, qr+p, qr+p^2, rp+q, rp+q^2$$

都是素数.

解. 若 $p>2$, 则 p,q,r 都是奇数, 此时 $pq+r$ 是一个大于 2 的偶数, 矛盾, 故 $p=2$. 现在, 数

$$2q+r, 2q+r^2, qr+2, qr+4, 2r+q, 2r+q^2$$

都是素数.

若 q,r 中有偶数, 则 $qr+2$ 为一个大于 2 的偶数, 矛盾, 故 q,r 都是奇素数. 若 $q>3$, 则 $3 \nmid qr$. 此时, 若 $qr \equiv 1(\bmod 3)$, 则 $qr+2 \equiv 0(\bmod 3)$, 与 $qr+2$ 为素数矛盾; 若 $qr \equiv 2(\bmod 3)$, 则 $qr+4 \equiv 0(\bmod 3)$, 与 $qr+4$ 为素数矛盾, 故 $q=3$. 这样, 数

$$6+r, 6+r^2, 3r+2, 3r+4, 2r+3, 2r+9$$

都是素数.

若 $r \neq 5$, 则 $r \neq 0(\bmod 5)$, 但分别当 $r \equiv 1,2,3,4(\bmod 5)$ 时, 对应地, 数 $3r+2, 3r+4, 2r+9, 6+r$ 为 5 的倍数, 矛盾, 故 $r=5$.

直接验证, 可知它们满足条件, 所求的素数为

$$p=2, q=3, r=5$$

例 2.2.2. 设 n 为大于 1 的正整数, 且 $1!, 2!, \cdots, n$! 中任意两个数除以 n 所得的余数不同. 证明: n 是一个素数.

证明. 注意到, $n! \equiv 0(\bmod n)$, 而 $n=4$ 时, 有 $2! \equiv 3!(\bmod 4)$. 因此,

如果能够证明: 当 n 为大于 4 的合数, 都有 $(n-1)! \equiv 0(\bmod n)$, 就能依题中的条件导出矛盾. 从而证出 n 为素数.

事实上, 若 n 为大于 4 的合数, 则可对 n 作分解, 变为下述两种情形.

情形一: 可写 $n=pq, 2 \leqslant p<q, p, q$ 为正整数, 这时 $1<p<q<n-1$, 从而 $pq \mid (n-1)!$, 即 $(n-1)! \equiv 0(\bmod n)$.

情形二: 当 $n=p^2, p$ 为素数时, 由 $n>4$, 知 $p \geqslant 3$, 故 $1<p<2p<(n-1)$, 从而 $p \cdot (2p) \mid (n-1)!$, 于是, $(n-1)! \equiv 0(\bmod n)$.

综上可知, n 只能是素数. □

注记. 反过来, 当 n 为素数时, 并不能保证 $1!, 2!, \cdots, n$! 中任意两个数对模 n 不同余. 例如 $p=5$ 时, $3! \equiv 1!(\bmod 5)$.

例 2.2.3. 设整数 x,y,z 满足

$$(x-y)(y-z)(z-x)=x+y+z. \tag{2.25}$$

证明: $x+y+z$ 是 27 的倍数.

证明. 考虑 x, y, z 除以 3 所得的余数, 如果 x, y, z 中任意两个对模 3 不同余, 那么

$$x + y + z \equiv 0 + 1 + 2 \equiv 0(\bmod 3)$$

但是 $3 \nmid (x-y)(y-z)(z-x)$, 这与式 2.25矛盾.

现在 x, y, z 中必有两个对模 3 同余, 由对称性, 不妨设 $x \equiv y(\bmod 3)$, 这时由式 2.25知

$$3 \mid x + y + z,$$

于是

$$z \equiv -(x+y) \equiv -2x \equiv x(\bmod 3)$$

这表明

$$x \equiv y \equiv z(\bmod 3)$$

从而由式 2.25知

$$27 \mid x + y + z.$$

□

例 2.2.4. 是否存在 19 个不同的正整数, 使得在十进制表示下, 它们的数码和相同, 并且这 19 个数之和为 1999 ?

解. 此题需要用到一个熟知的结论: 在十进制表示下, 每个正整数与它的数码和对模 9 同余. (这个结论只需利用 $10^k \equiv 1(\bmod 9)$ 即可得证)

若存在 19 个满足条件的不同正整数, 则由它们的数码和相同 (设这个相同的数码和为 k) , 可知 $1999 \equiv 19k(\bmod 9)$, 故 $k \equiv 1(\bmod 9)$. 又这 19 个数之和为 1999 , 故其中必有一个数不大于 $\frac{1999}{19}$, 即有一个数 $\leqslant 105$, 所以 $k \leqslant 18$. 结合 $k \equiv 1(\bmod 9)$, 知 $k = 1$ 或 10 .

若 $k = 1$, 则这 19 个数为 $1, 10, 100, \cdots$, 和不可能为 1999 , 所以, $k = 10$. 而当 $k = 10$ 时, 最小的数码和为 10 的 20 个正整数是

$$19, 28, 37, \cdots, 91, 109, 118, 127, \cdots, 190, 208$$

前面 19 个数之和为 1990 , 故符合要求的 19 个正整数中必有一个 $\geqslant 208$, 此时

$$\text{这19 个数之和 } \geqslant 208 + (19 + 28 + \cdots + 91) + \tag{2.26}$$
$$(109 + 118 + 127 + \cdots + 181) \tag{2.27}$$
$$= 2198 > 1999 \tag{2.28}$$

矛盾.

所以不存在 19 个不同的整数满足条件.

例 2.2.5. 设 m, n, k 为正整数, $n \geqslant m + 2, k$ 为大于 1 的奇数, 并且 $p = k \times 2^n + 1$ 为素数, $p \mid 2^{2^m} + 1$. 证明: $k^{2^{n-1}} \equiv 1(\bmod p)$.

证明. 由条件知 $2^{2^m} \equiv -1(\bmod p)$, 而 $n \geqslant m+2$, 故 2^{m+1} 是 $n \cdot 2^{n-1}$ 的因数, 所以, $2^{n \cdot 2^{n-1}} \equiv (-1)^{2t} = 1(\bmod p)$ (这里 $t = n \cdot 2^{n-m-2}$) .

现在, 由 $k \cdot 2^n \equiv -1(\bmod p)$, 知 $k^{2^{n-1}} \cdot 2^{n \cdot 2^{n-1}} \equiv (-1)^{2^{n-1}} = 1(\bmod p)$, 结合上面的结论, 即可得 $k^{2^{n-1}} \equiv 1(\bmod p)$. □

注记. 本题的背景是讨论费马数 *(形如 $F_m = 2^{2^m} + 1$ 的数为费马数)* 的素因数的性质.

2.2.2　剩余系及其应用

对任意正整数 m 而言, 一个整数除以 m 所得的余数只能是 $0, 1, 2, \cdots, m-1$ 中的某一个, 依此可将整数分为 m 个类 (例如 $m = 2$ 时, 就是奇数或偶数), 从每一类中各取一个数所组成的集合就称为模 m 的一个完全剩余系, 简称为模 m 的完系. 依此定义, 可以容易地得到下面的两个性质.

性质 2.2.7. 若整数 $a_1, a_2, \cdots, a_m$ 对模 m 两两不同余, 则 $a_1, a_2, \cdots, a_n$ 构成模 m 的一个完系.

性质 2 任意连续 m 个整数构成模 m 的一个完系, 其中必有一个数为 m 的倍数.

引入完系的概念, 蕴含了" 整体处理" 的思想, 在用同余方法处理数论问题时, 我们常常需要选择不同的完系来达到目的, 做出恰当地分析.

例 1 证明: 在十进制表示下, 任意 39 个连续正整数中, 必有一个数的数码和是 11 的倍数.

证明由于连续 10 个正整数中必有一个为 10 的倍数, 故连续 39 个正整数中必有 3 个数为 10 的倍数, 这 3 个数中必有一个数的十位数字不大于 8 , 且该数后有至少 19 个数在所取的 39 个连续的正整数中. 设这个数为 a, 并设它的数码和为 $S(a)$, 现在考虑数

$$a, a+1, \cdots, a+9, a+19$$

这 11 个数都是所取的 39 个数中的数, 并由 a 的选择知, 它们的数码和分别为 $S(a), S(a)+1, \cdots, S(a)+10$, 构成 11 个连续的正整数, 其中必有一个数为 11 的倍数. 命题获证.

说明是否命题对连续 38 个连续正整数也对呢？答案是否定的, 原因是可能找不到由数码和构成的模 11 的完系. 一个反例是: 999981, 999982, , 1000018 , 这 38 个数中没有一个数的数码和是 11 的倍数.

例 2 设 n 为正奇数. 证明: 数

$$2-1, 2^2-1, \cdots, 2^{n-1}-1$$

中必有一个数是 n 的倍数.

证明当 $n = 1$ 时, 命题显然成立.

考虑 $n > 1$ 的情形, 此时, 在数

$$1, 2, \cdots, 2^{n-1}$$

中没有一个数为 n 的倍数, 故它们除以 n 所得的余数只能是 $1,2,\cdots,n-1$. 所以, 这 n 个数中必有两个数对模 n 同余, 即存在 $0\leqslant i<j\leqslant n-1$, 使得 $2^i\equiv 2^j(\bmod n)$. 又 n 为奇数, 故 $\left(2^i,n\right)=1$, 所以, $2^{j-i}\equiv 1(\bmod n)$, 即 $n\mid 2^{2^{-i}}-1$. 命题获证.

说明在处理数论中的一些存在性问题时, 经常需要将同余方法与抽屉原则相结合.

例 3 设 m,n 为正整数, m 为奇数, 且 $(m,2^n-1)=1$. 证明: 数 $1^n+2^n+\cdots+m^n$ 是 m 的倍数.

证明由于 m 为奇数, 而 $1,2,\cdots,m$ 是模 m 的一个完系, 故 $2\times 1,2\times 2,\cdots,2\times m$ 也是模 m 的一个完系, 所以,

$$1^n+2^n+\cdots+m^n\equiv(2\times 1)^n+(2\times 2)^n+\cdots+(2\times m)^n(\bmod m).$$

即 $m\mid\left(2^n-1\right)\left(1^n+2^n+\cdots+m^n\right)$, 结合 $(m,2^n-1)=1$ 可知命题成立.

说明这里凸现了" 整体处理" 的妙处. 一个有趣的技巧是: 当 n 为奇数时, 利用因式分解可知对 $1\leqslant k\leqslant m-1$, 有 $k^n+(m-k)^n$ 是 m 的倍数, 因此, 可对和数 $1^n+\cdots+m^n$ 进行配对处理后证出结论. 但这个方法对 n 是偶数的情形就失效了.

例 4 (1) 证明: 存在无穷多组整数 (x,a,b,c) , 使得

$$x^2+a^2=(x+1)^2+b^2=(x+2)^2+c^2$$

(2) 问: 是否存在整数组 (x,a,b,c,d) , 使得

$$x^2+a^2=(x+1)^2+b^2=(x+2)^2+c^2=(x+3)^2+d^2?$$

解 (1) 对大于 1 的正整数 k , 令 $x=4k^3-1,a=2k^2+2k,b=2k^2+1,c=2k^2-2k$, 可知整数组 (x,a,b,c) 符合要求.

这里 (x,a,b,c) 的构造思路如下:

由题目的要求, 知 $a^2-b^2=2x+1,b^2-c^2=2x+3$, 于是, 设 $b=c+n,a=b+m=c+n+m$, 应有

$$\begin{cases}2cn+n^2=2x+3\\ 2cm+2mn+m^2=2x+1\end{cases}$$

这要求 m,n 都为奇数, 两式相减后, 得 $c=\frac{1+mm}{n-m}-\frac{n+m}{2}$, 为使其为整数,

取 $n=m+2$, 得 $c=\frac{1+m(m+2)}{2}-\frac{2m+2}{2}=\frac{m^2-1}{2}$, 令 $m=2k+1$, 就得到了我们的构造.

(2) 不存在这样的整数组.

事实上, 对任意整数 y , 我们有

$$y^2\equiv\begin{cases}0(\bmod 8),\ 若 y\equiv 0(\bmod 4);\\ 1(\bmod 8),\ 若 y\equiv 1\text{ 或}3(\bmod 4);\\ 4(\bmod 8),\ 若 y\equiv 2(\bmod 4).\end{cases}$$

所以, 对整数 y,z 有

$$y^2+z^2\equiv\begin{cases}0,1\text{ 或}4(\bmod 8),\ 若 y\equiv 0(\bmod 4);\\ 1,2\text{ 或}5(\bmod 8),\ 若 y\equiv 1\text{ 或}3(\bmod 4);\\ 0,4\text{ 或}5(\bmod 8),\ 若 y\equiv 2(\bmod 4).\end{cases}$$

如果存在符合要求的整数组 (x,a,b,c,d) , 记 $T=x^2+a^2$, 由于 x , $x+1,x+2,x+3$ 构成模 4 的一个完系, 不妨设 $x\equiv 0(\bmod 4)$, 那么 $x+1\equiv 1(\bmod 4), x+2\equiv 2(\bmod 4)$, 所以, 应有

$$T(\bmod 8)\in\{0,1,4\}\cap\{1,2,5\}\cap\{0,4,5\}=\varnothing$$

这是一个矛盾.

例 5 设 n 为正整数. 证明: 存在一个各数码都是奇数的正整数, 它是 5^n 的倍数.

证明我们利用递推方法构造符合条件的 n 位正整数.

当 $n=1$ 时, 取 $a_1=5$, 即可.

设 $n=m$ 时, 存在一个各数码都是奇数的 m 位正整数 a_m , 使得 $5^m\mid a_m$.

设 $a_m=5^m\times q$, 其中 $q\equiv r(\bmod 5), r=0,1,2,3$ 或 4 . 现在考虑数

$$10^m, 3\times 10^m, 5\times 10^m, 7\times 10^m, 9\times 10^m$$

它们除以 5^m 后, 所得的商数分别为

$$2^m, 3\times 2^m, 5\times 2^m, 7\times 2^m, 9\times 2^m$$

其中任意两个数之差不是 5 的倍数, 它们构成模 5 的一个完系. 故其中必有一个数 $\equiv 5-r(\bmod 5)$, 设 $a\times 2^m\equiv 5-r(\bmod 5)$, 这里 a 是 $1,3,5,7,9$ 中的某个数. 令 $a_{m+1}=a\times 10^m+a_m$, 则

$$5^m\mid a_{m+1}$$

且

$$\frac{a_{m+1}}{5^m}\equiv a\times 2^m+r\equiv 5-r+r\equiv 0(\bmod 5)$$

故

$$5^{m+1}\mid a_{m+1}$$

因此, 存在一个 $m+1$ 位正整数 a_{m+1}, 其各数码都是奇数, 且 $5^{m+1}\mid a_{m+1}$. 命题获证.

说明这里我们采用了加强命题的方式, 证明了不仅存在满足条件的数, 并且该数还是一个 n 位数. 在递推构造中, 这个加强带来了很大的方便.

例 6 一次圆桌会议共有 2012 个人参加, 中场休息后, 他们依不同的次序重新围着圆桌坐下. 证明: 至少有两个人, 他们之间的人数在休息前与休息后是相等的.

证明记 $n=1006$, 我们对每个座位标号, 将座位的号码依顺时针方向依次记为

$$1,2,3,\cdots,2n$$

因而, 每一个人可对应一个数对 (i,j), 其中 i,j 分别为他在休息前后的座位号. 显然, 所有的" 横坐标" i 与" 纵坐标" j 都取遍 (1), 亦即恰好构成模 $2n$ 的完全剩余系.

如果每两个人 $(i_1, j_1), (i_2, j_2)$ 在休息前后, 坐在他们之间的人数都不相同, 则应有

$$j_2 - j_1 \neq i_2 - i_1.$$

注意, 上式中当 $j_2 < j_1$ (或 $i_2 < i_1$) 时, j_2 应换成 $2n + j_2$ (或 i_2 应换 $2n+ i_2$). 当然更好的写法是

$$j_2 - j_1 \not\equiv i_2 - i_1 (\bmod 2n)$$

也就是

$$j_2 - i_2 \not\equiv j_1 - i_1 (\bmod 2n)$$

上式的含义是任意两个人的纵横坐标之差都对模 $2n$ 不同余, 从而

$$j_1 - i_1, j_2 - i_2, \cdots, j_{2n} - i_{2n}$$

也是模 $2n$ 的一个完全剩余系.
考虑到模 $2n$ 的每一个完全剩余系的各数之和应与

$$1 + 2 + 3 + \cdots + 2n = \frac{2n(2n+1)}{2} = n(2n+1)$$

对模 $2n$ 同余, 但 $n(2n+1) \not\equiv 0 (\bmod 2n)$, 故 (2) 中各数之和不能被 $2n$ 整除, 从而不能等于 0. 这与

$$\sum_{k=1}^{2n} (j_k - i_k) = \sum_{k=1}^{2n} j_k - \sum_{k=1}^{2n} i_k = \sum_{k=1}^{2n} j - \sum_{k=1}^{2n} i = 0$$

矛盾. 这表明至少有两个人, 他们之间的人数在休息前后是相同的.
说明本质上是因为模 $2n$ 的两个完系对应各数之差不能构成模 $2n$ 的一个完系, 才会有本题的结论.

2.2.3　费马小定理及其应用

费马 (Fermat) 小定理是初等数论中的一个重要定理, 数学竞赛中经常需要用到.

Fermat 小定理设 p 为素数, a 为整数, 则 $a^p \equiv a (\bmod p)$. 特别地, 若 $p \nmid a$, 则 $a^{p-1} \equiv 1 (\bmod p)$.

请注意该定理中 p 为素数这个条件, 下面的证明中这个条件是非常重要的.

证明当 $p \mid a$ 时, 结论显然成立.
当 $p \nmid a$ 时, 设 $x_1, x_2, \cdots, x_{p-1}$ 是 $1, 2, \cdots, p-1$ 的一个排列, 我们先证: $ax_1, ax_2, \cdots, ax_{p-1}$ 中任意两个数对模 p 不同余.

事实上, 若存在 $1 \leqslant i < j \leqslant p-1$, 使得 $ax_i \equiv ax_j (\bmod p)$, 则 $p \mid a\left(x_i - x_j\right)$, 而 $p \nmid a$, 故 $p \mid x_i - x_j$ (注意, 这里用到 p 为素数), 但 x_i 与 x_j 对模 p 不同余, 矛盾.

又 $ax_1, ax_2, \cdots, ax_{p-1}$ 中显然没有一个数为 p 的倍数, 因此, ax_1 , $ax_2, \cdots, ax_{p-1}$ 除以 p 所得的余数是 $1, 2, \cdots, p-1$ 的一个排列, 利用同余的性质, 知

$$\left(ax_1\right)\left(ax_2\right) \cdots \left(ax_{p-1}\right) \equiv x_1 x_2 \cdots x_{p-1} (\bmod p)$$

再由 $x_1x_2\cdots x_{p-1}=(p-1)$, , 它不是 p 的倍数 (注意, 这里再次用到 p 为素数), 所以, $a^{p-1}\equiv 1(\bmod p)$.

说明这个证明体现了整体处理的思想, 它将模 p 的余数全体对等考虑, 分别将模 p 的两个剩余系 (都不包括零) 作乘积后得到一个同余式, 然后证出要证的式子.

例 1 设 n 为正整数. 证明: $7\mid 3^n+n^3$ 的充要条件是 $7\mid 3^nn^3+1$.

证明若

$7\mid 3^n+n^3,$

于是, 由 Fermat 小定理, 知

$$n^6\equiv 1(\bmod 7)$$

从而, 由

$7\mid 3^n+n^3,$

知

$7\mid \left(3^n+n^3\right)n^3,$

故

$$7\mid 3^nn^3+1$$

反过来, 若

则

并且

即

利用 Fermat 小定理知

故

命题获证.

说明涉及指数的同余式经常需要用到 Fermat 小定理, 因为由 Fermat 小定理得出的结论中, 同余式的一边是 1, 这带来很大的方便.

例 2 设 x 为整数, p 是 x^2+1 的奇素因数, 证明: $p\equiv 1(\bmod 4)$.

证明由于 p 为奇素数, 若 $p\neq 1(\bmod 4)$, 则 $p\equiv 3(\bmod 4)$, 可设 $p=4k+3$, 此时, 由 $x^2\equiv -1(\bmod p)$, 得

$$x^{p-1}=x^{4k+2}=\left(x^2\right)^{2k+1}\equiv(-1)^{2k+1}\equiv -1(\bmod p)$$

而由 Fermat 小定理, 应有

$$x^{p-1}\equiv 1(\bmod p)$$

结合上式将导出 $p\mid 2$. 矛盾.

所以, $p\equiv 1(\bmod 4)$.

说明利用此题的结论, 我们可以证明: 存在无穷多个模 4 余 1 的正整数为素数.

事实上, 若只有有限个素数模 4 余 1 , 设它们是 $p_1,p_2,\cdots,p_n$. 考虑数 $(2p_1p_2\cdots p_n)^2+1$ 的素因数即可导出矛盾.

例 3 设 x 为整数, p 是数 $x^6+x^5+\cdots+1$ 的素因数. 证明: $p=7$ 或 $p\equiv 1(\bmod 7)$.

证明当 $x=1$ 时, $p=7$; 当 $x\neq 1$ 时, p 是 $\frac{x^7-1}{x-1}$ 的素因子, 因此, $x^7\equiv 1(\bmod p)$, 这表明 $p\nmid x$, 于是, 由 Fermat 小定理, 可知 $x^{p-1}\equiv 1(\bmod p)$, 进而 $x^{(7,p-1)}\equiv 1(\bmod p)$.

如果 $7\nmid p-1$, 即 $p\neq 1(\bmod 7)$, 那么 $(7,p-1)=1$, 得 $x\equiv 1(\bmod p)$, 于是,

$$0\equiv x^6+x^5+\cdots+1\equiv 1^6+1^5+\cdots+1=7(\bmod p)$$

得 $p=7$.

所以, 命题成立.

说明本题的解答中用到下面的结论: 若 $(a,m)=1$, 且 $a^u\equiv 1(\bmod m)$, $a^v\equiv 1(\bmod m)$, 则 $a^{(u,v)}\equiv 1(\bmod m)$.

它可以由下面的方法来得到.

由贝祖定理, 知存在整数 x,y , 使得 $ux+vy=(u,v)$, 于是,

$$a^{(u,v)}=a^{ux+vy}=(a^u)^x\cdot(a^v)^y\equiv 1^x\cdot 1^y=1(\bmod m)$$

这里在 x,y 为负整数时, 用数论倒数去理解.

另一方面, 本题的结论可推广为: 设 q 为奇素数, x 为整数, 则数 $x^{q-1}+\cdots+1$ 的素因数 p 满足: $p=q$ 或者 $p\equiv 1(\bmod q)$.

例 4 设 p 为素数. 证明: 存在无穷多个正整数 n , 使得 $p\mid 2^n-n$.

证明如果 $p=2$, 那么取 n 为偶数, 就有 $p\mid 2^n-n$, 命题成立.

设 $p>2$, 则由 Fermat 小定理知

$$2^{p-1}\equiv 1(\bmod p)$$

因此, 对任意正整数 k , 都有

$$2^{k(p-1)}\equiv 1(\bmod p)$$

所以, 只需证明存在无穷多个正整数 k , 使得

$$k(p-1)\equiv 1(\bmod p)\big(\text{ 这样, 令}n=k(p-1)\text{, 就有}p\mid 2^n-n\big)\,.$$

而这只需 $k\equiv -1(\bmod p)$, 这样的 k 当然有无穷多个.

所以, 命题成立.

说明用 Fermat 小定理处理数论中的一些存在性问题有时非常方便, 简洁.

例 5 由 Fermat 小定理知, 对任意奇素数 p , 都有 $2^{p-1}\equiv 1(\bmod p)$. 问: 是否存在合数 n , 使得 $2^{n-1}\equiv 1(\bmod n)$ 成立?

解这样的合数 n 存在, 而且有无穷多个. 其中最小的满足条件的合数 $n=341=11\times 31$ (它是从两个不同奇素数作乘积去试算出来的).

事实上, 由于

$$2^{10}-1=1023=341\times 3, \tag{2.29}$$

$$2^{10}\equiv 1(\bmod 341) \tag{2.30}$$

$$2^{340}\equiv 1^{34}\equiv 1(\bmod 341) \tag{2.31}$$

故

所以

故 341 符合要求.

进一步, 设 a 是一个符合要求的奇合数, 则 2^a-1 也是一个奇合数 (这一点利用因式分解可知). 再设 $2^{a-1}-1=a\times q, q$ 为正奇数, 则

$$
\begin{aligned}
2^{2^a-1-1}-1 &= 2^{2\left(2^{a-1}-1\right)}-1 &\quad (2.32)\\
&= 2^{2aq}-1 &\quad (2.33)\\
&= (2^a)^{2q}-1 &\quad (2.34)\\
&\equiv 1^{2q}-1 &\quad (2.35)\\
&\equiv 0\,(\mathrm{mod} 2^a-1) &\quad (2.36)
\end{aligned}
$$

因此 2^a-1 也是一个符合要求的数. 依此递推 (结合 341 符合要求), 可知有无穷多个满足条件的合数.

说明满足题中的合数 n 称为" 伪素数", 如果对任意 $(a,n)=1$ 都有 $a^{n-1}\equiv 1(\mathrm{mod}\ n)$ 成立, 那么合数 n 称为" 绝对伪素数". 请读者寻找" 绝对伪素数".

例 6 求所有的素数 p, 使得 $\frac{2^{p-1}-1}{p}$ 是一个完全平方数.

解设 p 是一个满足条件的素数, 则显然 p 是一个奇素数. 由 Fermat 小定理知

而

$$p \mid 2^{p-1}-1$$

故

$$2^{p-1}-1=\left(2^{\frac{p-1}{2}}-1\right)\left(2^{\frac{p-1}{2}}+1\right),$$
$$p\left|2^{\frac{p-1}{2}}-1\ \text{或} p\right|2^{\frac{p-1}{2}}+1.$$

由于 $\left(2^{\frac{p-1}{2}}-1,2^{\frac{t-1}{2}}+1\right)=\left(2^{\frac{p-1}{2}}-1,2\right)=1$, 所以, $p\left|2^{\frac{p-1}{2}}-1\right.$ 与 $p\left|2^{2^{\frac{p-1}{2}}}+1\right.$ 中恰有一个成立.

若 $p\left|2^{\frac{p-1}{2}}-1\right.$, 则由条件及 $\left(2^{\frac{p-1}{2}}-1,2^{\frac{p-1}{2}}+1\right)=1$ 可知存在正整数 x , 使得

$$2^{\frac{n_1^2}{2}}+1=x^2,$$

此时

$$(x-1)(x+1)=2^{\frac{p-1}{2}},$$

这表明 $x-1$ 与 $x+1$ 都是 2 的幂次, 而 x 为奇数, 故 $x-1$ 与 $x+1$ 是两个相邻的偶数, 所以, 只能是

$$x-1=2, x+1=4$$

故

$$x=3 \quad (2.37)$$

$$p=7 \quad (2.38)$$

此时

若 $p \Big| 2^{\frac{b-1}{2}}+1$, 则同上知存在正整数 x , 使得

$$2^{\frac{p-1}{2}}-1=x^2$$

当 $p>3$ 时, 导致

$$x^2=2^{\frac{p-1}{2}}-1\equiv -1(\mathrm{mod} 4)$$

矛盾, 故 $p=3$.

另一方面, 当 $p=3$ 和 7 时, $\frac{2^{p-1}-1}{p}$ 分别为 1 和 9 , 都是完全平方数.

综上可知 $p=3$ 或 7.

2.2.4　奇数与偶数

奇数与偶数是对整数的最简单的分类, 初等数论经常需要对式子两边进行奇偶性分析, 导出矛盾或得出某个变量的特性, 奇偶分析法是一种重要的解题方法.

性质 1 奇数 $\neq$ 偶数.

这个简单的事实对导出矛盾是十分重要的.

性质 2 奇数的因数都是奇数, 即偶数不能整除奇数.

注意, 反过来, 偶数是有奇因数的.

性质 3 奇数个奇数之和为奇数, 偶数个奇数之和为偶数. 任何整数加上一个偶数, 其奇偶性不变, 加上一个奇数, 其奇偶性改变; 任何整数乘以一个奇数, 其奇偶性不变, 乘以一个偶数都变为偶数.

这一节和下一节都是专题讨论, 一个是重要的方法, 另一个是内容丰富的特殊数. 它们在初中阶段是研究和学习的重点之一.

例 1 已知 p 为素数, 求所有的整数对 (x,y) , 使得 $|x+y|+(x-y)^2=p$.

解注意到, $x+y$ 与 $x-y$ 要么都是奇数, 要么都是偶数, 故 $|x+y|+(x-y)^2$ 为偶数, 从而 $p=2$. 这表明 $|x+y|+(x-y)^2=2$.

由于 $|x+y|$ 与 $(x-y)^2$ 具有相同的奇偶性, 又 $(x-y)^2$ 是一个完全平方数, 故 $\left(|x+y|,(x-y)^2\right)=(2,0),(1,1)$. 分别求解, 可知

$(x,y)=(1,1),(-1,-1),(0,1),(0,-1),(1,0),(-1,0)$.

说明从奇偶性出发, 先确定式子中的素数应具有的一些特性, 然后再处理就容易了.

例 2 将 $1,2,\cdots,49$ 填入一个 7×7 的表格 (每格一个数), 分别计算每行, 每列中的各数之和, 得到 14 个和数. 用 A 表示这 14 个和数中的奇数之和, B 表示这 14 个和数中的偶数之和. 问: 是否存在一种填表方式, 使得 $A=B$?

解若有一种填表方式, 使得 $A=B$, 则

$$A=B=\frac{1}{2}(A+B)=\frac{1}{2}\times 2\times(1+2+\cdots+49)=25\times 49$$

这要求 B 为奇数, 但是 B 是若干个偶数之和, 不可能为奇数, 矛盾.

所以, 不存在使 $A=B$ 成立的填表方式.

说明这里 $A+B$ 是表格中所有行和之和 (它等于表格中所有数之和) 与所有列和之和 (也等于表格中所有数之和) 的和, 因此 (1) 成立. 这里蕴含了整体处理的思想.

例 3 在十进制表示下, 将某个 17 位数加上它的反序数. 证明: 所得的和数中必有一个数码为偶数.

又问: 将 17 改为一般的正整数 n , 命题成立吗? 对怎样的 n 成立?

证明若存在一个 17 位数 $\overline{a_1a_2\cdots a_{17}}$, 使得 $M=\overline{a_1\cdots a_{17}}+\overline{a_{17}a_{16}\cdots a_1}$ 的各数码都是奇数, 则考察个位数, 可知 a_1+a_{17} 为奇数. 现在再考察最前面一位的求和, 若 a_2+a_{16} 产生进位, 则由 a_1+a_{17} 为奇数, 可知 M 中有一位为偶数, 矛盾. 故 a_2+a_{16} 不产生进位. 依此可知 $\overline{a_3a_4\cdots a_{15}}+\overline{a_{15}a_{14}\cdots a_3}$ 的各数码都是奇数. 同样的推导可知 $\overline{a_5\cdots a_{13}}+\overline{a_{13}\cdots a_5}$ 的各数码都是奇数, $\cdots$, 最后 a_9+a_9 为奇数, 这是一个矛盾. 所以, M 中必有一个数码为偶数.

对一般的正整数 n , 同上讨论, 可知 $n\equiv 1(\bmod 4)$ 时, 命题依然成立. 当 n 为偶数时, 设 $n=2m$, 则数 $\underbrace{4\cdots}_{m\uparrow}\underbrace{5\cdots 5}_{m\text{ 个}}$ 与其反序数之和的各数码都是奇数; 当 $n\equiv 3(\bmod 4)$ 时, 设 $n=4k+3$, 则数 $\underbrace{6464\cdots 645}_{k+1\uparrow 64}\underbrace{45\cdots 45}_{k\uparrow 45}$ 与其反序数之和的各数码都是奇数.

所以, 当且仅当 $n\equiv 1(\bmod 4)$ 时, 命题成立.

例 4 (1) 已知存在 n 个整数, 它们的和等于零, 而它们的积等于 n . 证明: $4\mid n$;

(2) 设正整数 n 是 4 的倍数. 证明: 存在 n 个整数, 其和为零, 而积为 n.

解 (1) 设整数 $a_1,a_2,\cdots,a_n$ 满足:

$$\begin{cases} a_1+a_2+\cdots+a_n=0 \\ a_1a_2\cdots a_n=n \end{cases}$$

若 n 为奇数, 则由 (2) 知 $a_1,a_2,\cdots,a_n$ 为奇数, 故 $a_1+a_2+\cdots+a_n$ 是奇数个 (n 个) 奇数之和, 这与 (1) 矛盾. 所以, n 为偶数.

现在若 n 不是 4 的倍数, 则由 (2) 知 $a_1,a_2,\cdots,a_n$ 中恰有一个数为偶数, 此时 $a_1+a_2+\cdots+a_n$ 是一个偶数加上奇数个 ($n-1$ 个) 奇数, 其和为奇数, 同样与 (1) 矛盾. 所以, $4\mid n$.

(2) 只需给出一个例子, 按 $n\equiv 0(\bmod 8)$ 与 $n\equiv 4(\bmod 8)$ 分别处理.

当 $n\equiv 0(\bmod 8)$ 时, 设 $n=8k$, 此时存在 n 个整数

$$4k,2,\underbrace{1,\cdots,1}_{2k-2\uparrow},\underbrace{-1,-1,\cdots,-1}_{6k\uparrow}$$

满足和为零, 积为 n.

当 $n\equiv 4(\bmod 8)$ 时, 设 $n=8k+4$, 则存在 n 个整数

$$4k+2,-2,\underbrace{1,\cdots,1}_{2k+1\uparrow},\underbrace{-1,\cdots,-1}_{6k+1\uparrow}$$

满足和为零, 积为 n.

所以, 命题成立.

例 5 已知 4 枚硬币中可能混有假币, 其中真币每枚重 10 克, 假币每枚重 9 克. 现有一台托盘秤, 它可以称出托盘中物体的总重量. 问: 至少需要称几次, 才能保证可以鉴别出每一枚硬币的真假?

解至少称 3 次可以做到.
事实上, 设 4 枚硬币分别是 a,b,c,d . 分 3 次称出 $a+b+c, a+b+d, a+c+d$ 的重量. 这 3 个重量之和等于 $3a+2(b+c+d)$, 因此, 如果这 3 个重量之和为奇数, 那么 a 为假币, 否则 a 为真币. 当 a 确定后, 解关于 b,c,d 的三元一次方程组可确定 b,c,d 的真假. 所以, 3 次是足够的.

下证: 只称两次不能保证测出每枚硬币的真假.
注意到, 如果有两枚硬币, 例如 a,b, 它们在每次称量中要么同时出现, 要么同时不出现, 那么在 a,b 是一真一假时, 改变 a,b 的真假对称量结果没有影响, 故不能确定 a,b 的真假.

现在如果有一次称量中至多只出现两枚硬币, 例如 a,b, 那么另一次称量中 c,d 只能恰有一个在托盘中出现 (否则对换 c,d 的奇偶性不影响结果), 此

时, 有一枚硬币在两次称量中都不出现, 它的真假改变不影响称量结果, 从而不能断定它的真假. 故每次称量托盘中都至少有 3 枚硬币, 这时必有两枚硬币同时在两次称量中出现, 亦导致矛盾.

综上可知, 至少需要称 3 次.
例 6 一个边长为 3 的正方体被分割为 27 个单位正方体, 将 $1,2,\cdots,27$ 随机地放入单位正方体, 每个单位正方体中一个数. 计算每一行 (横, 竖, 列) 上 3 个数之和, 得到 27 个和数. 问: 这 27 个和数中至多有多少个奇数?

解计算这 27 个和数的和 S , 由于每个数恰在 3 行中出现, 故

$$S=3\times(1+2+\cdots+27)=3\times27\times14$$

即 S 为偶数, 所以, 这 27 个和数中奇数的个数为偶数.
若这 27 个和数中有 26 个奇数, 不妨设那个偶数为图 1 中的第一横行上的 3 个数之和, 即 $a_1+a_2+a_3$ 为偶数, 而图 1 中其余的 5 个行和都是奇数. 这时, 分别按横行和竖行求图 1 中的各数之和, 得

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

图 1

$$(a_1+a_2+a_3)+(a_4+a_5+a_6)+(a_7+a_8+a_9) \tag{2.39}$$
$$=(a_1+a_4+a_7)+(a_2+a_5+a_8)+(a_3+a_6+a_9) \tag{2.40}$$

但此式左边为两奇一偶, 右边为 3 个奇数之和, 导出左边为偶数, 而右边为奇数, 矛盾.

所以, 这 27 个和数中至多有 24 个数为奇数.
下面的例子 (如图 2 所示) 表明存在一种填数方式, 使得 27 个和数中可以有 24 个为奇数. 图 2 各表中的 0 表示偶数, 1 表示奇数, 从左到右依次为最上层, 中层和最下层的单位正方体.

0	1	0
1	1	1
0	1	0

1	1	1
1	0	0
1	0	0

0	1	1
1	0	0
0	0	1

图 2
所以, 这 27 个和数中最多有 24 个为奇数.

2.2.5　完全平方数

数学竞赛中的许多问题涉及到完全平方数, 需要用到完全平方数的一些特性.

性质 1 完全平方数 $\equiv 0$ 或 $1(\bmod 4)$, 奇数的平方 $\equiv 1(\bmod 8)$.
性质 2 相邻两个完全平方数之间没有一个正整数是完全平方数. (这个性质经常用来证明某一类数不是完全平方数)

性质 3 若两个互素的正整数之积是完全平方数, 则这两个数都是完全平方数.

注意, " 两个完全平方数之积是完全平方数" 这个结论是显然的.
这里的性质 2 与性质 3 对一般的 n 次方数都成立, 而性质 1 只列出了完全平方数模 4 和模 8 的性质, 模其余的数亦有一些相应的性质. 例如: 完全平方数 $\equiv 0$ 或 $1(\bmod 3)$, 完全平方数的末尾数字只能是 $0,1,4,5,6,9$ 等等.

例 1 设素数从小到大依次排列为 $p_1, p_2, \cdots$. 证明: 对任意大于 1 的正整数 n , 数 $p_1p_2\cdots p_n-1$ 和 $p_1p_2\cdots p_n+1$ 都不是完全平方数.

证明注意到, $n\geqslant 2$ 时, $3\mid p_1p_2\cdots p_n$, 故

$$p_1p_2\cdots p_n-1\equiv 2(\bmod 3)$$

所以, $p_1p_2\cdots p_n-1$ 不是完全平方数.
又 $n\geqslant 2$ 时, $p_2\cdots p_n$ 为奇数, 设 $p_2\cdots p_n=2k+1$, 就有

$$p_1p_2\cdots p_n+1=2(2k+1)+1=4k+3\equiv 3(\bmod 4)$$

所以, $p_1p_2\cdots p_n+1$ 也不是完全平方数.
说明在处理与完全平方数有关的问题时, 经常要用到同余的方法, 其中取恰当的" 参照物"(即模哪个数) 是非常关键的.

例 2 已知正整数 a,b 满足关系式

$$2a^2+a=3b^2+b$$

证明: $a-b$ 和 $2a+2b+1$ 都是完全平方数.

证明由条件, 知

$$b^2=2a^2+a-\left(2b^2+b\right)=(a-b)(2a+2b+1)$$

上式左边大于零, 右边中 $2a+2b+1$ 大于零, 故 $a-b$ 大于零.

由 (1) 知, 要证 $a-b$ 与 $2a+2b+1$ 都是完全平方数, 只需证明

$$(a-b,2a+2b+1)=1$$

设 $(a-b,2a+2b+1)=d$, 则由 (1) 知 $d^2\mid b^2$, 故 $d\mid b$. 进而结合 $d\mid a-b$, 知 $d\mid a$, 故 $d\mid 2(a+b)$. 又 $d\mid 2a+2b+1$, 所以, $d\mid 1$, 进而 $d=1$.

命题获证.

说明这里我们并没有求出 (1) 中 a,b 的值 (这是比较困难的), 但是我们对 (1) 作恰当变形, 使一边为完全平方数, 另一边是两个式子之积后, 问题解决起来就容易了.

例 3 设正整数 x,y,z 满足 $(x,y,z)=1$, 并且 $\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$. 证明: $x+y,x-z,y-z$ 都是完全平方数.

证明设 $(x,y)=m$, 并设 $x=mn,y=ml$, 这里 m,l,n 都是正整数, 且 $(l,n)=1$. 从而, 由条件可知

$$(l+n)z=mln$$

利用 $(x,y,z)=1$, 知 $(m,z)=1$, 于是, 由 (1) 知 $z\mid \ln$. 而 $(l,n)=1$, 故 $(l,l+n)=1,(n,l+n)=1$, 因此, 由 (1) 知 $l|z,n|z$, 再由 $(l,n)=1$, 知 $ln\mid z$. 所以, $z=ln$, 进而 $m=l+n$. 这样, 我们有

$$x+y=m(l+n)=(l+n)^2$$
$$x-z=mn-ln=n(m-l)=n^2$$
$$y-z=ml-ln=l(m-n)=l^2$$

命题获证.

说明另一种处理方式基于下面的变形:

$$\begin{aligned}\frac{x+y}{xy}=\frac{1}{z}&\Rightarrow\frac{x+y}{x}=\frac{y}{z} &(2.41)\\ &\Rightarrow\frac{x+y}{x}=\frac{x}{x-z} &(2.42)\\ &\Rightarrow(x+y)(x-z)=x^2 &(2.43)\end{aligned}$$

然后对最后一式利用上例的方法可证 $x+y$ 与 $x-z$ 都是完全平方数, 这种处理或许更能体现问题的本质.

例 4 求所有的素数 p , 使得 p^3-4p+9 是一个完全平方数.

解设 $p^3-4p+9=x^2,x$ 为非负整数, 则 $p\mid x^2-9$, 即 $p\mid(x-3)(x+3)$, 结合 p 为素数, 可设 $x=kp\pm3,k$ 为非负整数. 于是,

$$p^3-4p=x^2-9=k^2p^2\pm6kp$$

得 $p^2-4=k^2p\pm 6k$, 这表明: $p\mid 6k\pm 4$.
当 $p>2$ 时, p 为奇素数, 可知 $p\mid 3k\pm 2$, 故总有 $p\leqslant 3k+2$, 这表明: $\frac{1}{3}\left(p^2-2p-9\right)\leqslant pk-3\leqslant x$.

若 $x\leqslant\frac{p^2}{4}$, 则 $\frac{1}{3}\left(p^2-2p-9\right)\leqslant\frac{p^2}{4}$, 得 $p\leqslant 8+\frac{36}{p}$, 可知 $p\leqslant 11$;
若 $x>\frac{p^2}{4}$, 则 $p^3-4p+9=x^2>\frac{p^4}{16}$, 得 $p<16-\frac{16(4p-9)}{p^3}$, 可知 $p\leqslant 13$.

综上可知, $p\leqslant 13$, 直接枚举, 得 $(p,x)=(2,3),(7,18),(11,36)$. 求得 $p=2,7$ 或 11 .

说明此例所处理的等式两边不是齐次的, 想方设法得到素数 p 的一个范围后去枚举是常用的方法, 这时一些数论知识的运用结合不等式估计往往是有效的.

例 5 已知 n 为正整数, 且 $2n+1$ 与 $3n+1$ 都是完全平方数. 证明: $40\mid n$. 证明设 $2n+1=x^2,3n+1=y^2$, 其中 x,y 都是正整数.
由性质 1, 知 $x^2\equiv 1(\bmod 8)$ (因为 x^2 为奇数, 故 x 为奇数), 从而

$$n\equiv 0(\bmod 4)$$

进而 $3n+1$ 为奇数, 故

即

$$y^2\equiv 1(\bmod 8)$$

$$3n+1\equiv 1(\bmod 8)$$

于是

$$n\equiv 0(\bmod 8)$$

另一方面, 对任意整数 a , 有

$$a\equiv 0,\pm 1,\pm 2(\bmod 5)$$
$$a^2\equiv 0,1\text{ 或}4(\bmod 5).$$

故

由条件知 $x^2+y^2=5n+2\equiv 2(\bmod 5)$,
结合前面推出的结论, 可知

故

从而

$$x^2\equiv y^2\equiv 1(\bmod 5)$$
$$2n+1\equiv 1(\bmod 5)$$
$$n\equiv 0(\bmod 5)$$

利用 $(5,8)=1$, 可知 $40\mid n$.
说明最小的使得 $2n+1$ 与 $3n+1$ 都是完全平方数的正整数 $n=40$, 请读者找到下一个符合要求的正整数 n.

例 6 若 a,b 是使得 $ab+1$ 为完全平方数的正整数, 则记 $a\sim b$. 证明: 若 $a\sim b$, 则存在正整数 c , 使得 $a\sim c,b\sim c$.

证明由 $a\sim b$, 可设 $ab+1=x^2$, 这里 x 为正整数, 下一个与 a,b,x 有关的完全平方数是 $(a+x)^2$ 或 $(b+x)^2$, 于是, 我们取 $c=2x+a+b$, 则

$$\begin{aligned} ac+1&=a(2x+a+b)+1 &(2.44)\\ &=2ax+a^2+ab+1 &(2.45)\\ &=2ax+a^2+x^2=(x+a)^2 &(2.46)\\ bc+1&=(x+b)^2 &(2.47)\end{aligned}$$

命题获证.

说明此题对代数式变形的能力要求较高. 在寻找完全平方数时, 往往需要构造完全平方式, 因为当一个整式中的字母都取整数时, 这个整式的平方显然是完全平方数. 当然, 反过来并不需要这样的条件.

题中的 c 还可以这样来找: 设 $ac+1=y^2$, 则 $a(c-b)=y^2-x^2=(y-x)(y+x)$, 取 $y-x=a$ (此时 $c-b=y+x$) 可符合此式, 依此知应取 $c=b+y+x=2x+a+b$.

例 7 求所有的正整数数对 (a,b), 使得

$$a^3+6ab+1,b^3+6ab+1$$

都是完全立方数.

解不妨设 $a\leqslant b$, 则

$$b^3<b^3+6ab+1\leqslant b^3+6b^2+1<(b+2)^3$$

由 $b^3+6ab+1$ 是一个完全立方数, 可知

$$b^3+6ab+1=(b+1)^3$$

即有

$$6ab=3b^2+3b \tag{2.48}$$

$$b=2a-1 \tag{2.49}$$

从而

$$a^3+6ab+1=a^3+12a^2-6a+1$$

注意到 $(a+1)^3\leqslant a^3+12a^2-6a+1<(a+4)^3$,
因此, 由 a^3+12a^2-6a+1 是完全立方数, 可知只能是

$$a^3+12a^2-6a+1=(a+1)^3,(a+2)^3,(a+3)^3.$$

分别求解, 可得只能是 $a=1$.

所以, 满足条件的数对 $(a,b)=(1,1)$.

说明先确定某个 n 次方数夹在哪两个 n 次方数之间, 然后确定该 n 次方数的取值. 这是用不等式估计处理问题的常见方法.

例 8 求最小的正整数 n, 使得存在整数 $x_1, x_2, \cdots, x_n$, 满足

$$x_1^4 + x_2^4 + \cdots + x_n^4 = 1599$$

解由性质 1, 对任意整数 a, 可知

$$a^2 \equiv 0(\bmod 4) \text{ 或} a^2 \equiv 1(\bmod 8),$$

由此可得

$$a^4 \equiv 0 \text{ 或} 1(\bmod 16).$$

利用这个结论, 可知, 若 $n < 15$, 设

$$x_1^4 + x_2^4 + \cdots + x_n^4 \equiv m(\bmod 16)$$

则

$$m \leqslant n < 15$$

而

$$1599 \equiv 15(\bmod 16)$$

矛盾, 所以

$$n \geqslant 15$$

另外, 当 $n = 15$ 时, 要求

$$x_1^4 \equiv x_2^4 \equiv \cdots \equiv x_n^4 \equiv 1(\bmod 16)$$

即 $x_1, x_2, \cdots, x_n$ 都为奇数, 这为我们找到合适的数指明了方向. 事实上, 在 $x_1, x_2, \cdots, x_{15}$ 中, 1 个数取为 5,12 个取为 3 , 另外两个取为 1 , 就有

$$\begin{aligned} & x_1^4 + x_2^4 + \cdots + x_{15}^4 && (2.50) \\ = & 5^4 + 12 \times 3^4 + 2 && (2.51) \\ = & 625 + 972 + 2 && (2.52) \\ = & 1599. && (2.53) \end{aligned}$$

所以, n 的最小值为 15 .

习题 2

1 设 p, q 都是素数, 且 $7p + q, pq + 11$ 也都为素数, 求 $\left(p^2 + q^p\right)\left(q^2 + p^q\right)$ 的值.

2 设 $p_1 < p_2 < p_3 < p_4 < p_5$ 是 5 个素数, 且 p_1, p_2, p_3, p_4, p_5 成等差数列. 求 p_5 的最小值.

3 对每个正整数 n , 用 $S(n)$ 表示 n 在十进制表示下各数码之和. 证明: 对任意正整数

m , 存在正整数 n , 使得 $S(n)=mS(3n)$.

4 求最大的正整数 k , 使得存在正整数 n , 满足 $2^k \mid 3^n+1$.

5 设 n 为正整数. 证明: 存在十进制表示中只出现数码 0 和 1 的正整数 m , 使得 $n \mid m$.

6 设 n 是一个正奇数. 证明: 存在一个十进制表示中每个数码都是奇数的正整数 m , 使得 $n \mid m$.

7 证明: 对每个正整数 n , 数 $19\times 8^n+17$ 都是合数.

8 Fibonaccia 数列 $\{F_n\}$ 定义如下: $F_1=F_2=1, F_{n+2}=F_{n+1}+F_n, n=1$, $2,\cdots$

(1) 证明: 该数列任意连续 10 项之和是 11 的倍数;

(2) 求最小的正整数 k , 使得该数列中任意连续 k 项之和是 12 的倍数.

9 设整数 a,b 满足: $21 \mid a^2+b^2$. 证明: $441 \mid a^2+b^2$.

10 正整数 a,b,c 满足: $c^2=a^2+b^2+ab$. 证明: c 有一个大于 5 的素因子.

11 将整数 $1,2,\cdots,9$ 填入一个 3×3 的表格, 每格一个数, 使得每行, 每列及每条对角线上各数之和都是 9 的倍数.

(1) 证明: 该表格中正当中那个方格内的数是 3 的倍数;

(2) 给出一个正当中方格内所填数为 6 的满足条件的放置方法.

12 下面的算式给出了一种判别一个数是否为 19 的倍数的方法: 每次去掉该数的最后一位数字, 将其两倍与剩下的数相加, 依此类推, 直到数变为 20 以内的数为止, 若最后一个数为 19 , 则最初的那个数为 19 的倍数, 否则原数不是 19 的倍数.

$$
\begin{array}{cccccc}
 & 6 & 7 & 9 & 4 & \cancel{4} \\
 & & & & 8 & \\
\hline
 & 6 & 8 & 0 & \cancel{2} & \\
 & & & 4 & & \\
\hline
 & 6 & 8 & \cancel{4} & & \\
 & & 8 & & & \\
\hline
 & 7 & \cancel{6} & & & \\
1 & 2 & & & & \\
\hline
1 & 9 & & & &
\end{array}
$$

$$
\begin{array}{cccccc}
 & 4 & 4 & 9 & 7 & \cancel{6} \\
 & & & 1 & 2 & \\
\hline
 & 4 & 5 & 0 & \cancel{9} & \\
 & & 1 & 8 & & \\
\hline
 & 4 & 6 & \cancel{8} & & \\
 & 1 & 6 & & & \\
\hline
 & 6 & \cancel{2} & & & \\
 & 4 & & & & \\
\hline
1 & 0 & & & &
\end{array}
$$

例如上面判定了 67944 为 19 的倍数, 而 44976 不是 19 的倍数.

(1) 试证明: 上面的判别方法是正确的;

(2) 请给出判别一个数是否为 29 的倍数的类似方法.

13 能否将 2010×2010 的方格表的每个方格染成黑色或白色, 使得关于表格的中心对称的方格颜色不同, 且每行, 每列中黑格数与白格数都各占一半?

14 标号为 $1,2,\cdots,100$ 的火柴盒中有一些火柴, 如果每次提问允许问其中任意 15 盒中所有火柴数之和的奇偶性. 那么要确定 1 号盒中火柴数的奇偶性, 至少需要提问几次?

15 求所有的正整数 n , 使得可以在一个 $n \times n$ 的方格表的每个方格内写上 +1 或 -1 , 满足: 每个标号为 +1 的方格的相邻格中恰有一个标号是 -1 , 而每个标号为 -1 的方格的相邻格中恰有一个标号是 +1 .

16 设 $a_1,a_2,\cdots,a_{100}$ 是 $1,2,\cdots,100$ 的一个排列, 令 $b_i = a_1 + a_2 + \cdots + a_i$, $i = 1,2,\cdots,100$, 记 r_i 为 b_i 除以 100 所得的余数. 证明: $r_1,r_2,\cdots,r_{100}$ 中至少有 11 个不同的数.

17 求所有满足下述条件的正整数 a 的个数: 存在非负整数 $x_0,x_1,x_2,\cdots,x_{2001}$, 使得 $a^{x_0} = a^{x_1} + a^{x_2} + \cdots + a^{x_{2001}}$.

18 设 m,n 为正整数, $m>1$. 证明: $m\left(2^m-1\right) \mid n$ 的充要条件是 $\left(2^m-1\right)^2 \mid 2^n-1$.

19 设正整数 a,b 互素, p 为奇素数. 证明: $\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1$ 或 p.

20 求最小的正整数 a , 使得对任意整数 x , 都有 $65 \mid \left(5x^{13}+13x^5+9ax\right)$.

21 是否存在整数 a,b,c , 使得方程

$$ax^2+bx+c=0 \text{ 和} (a+1)x^2+(b+1)x+(c+1)=0$$

都有两个整数根?

22 求所有的正整数组 (x,y,z,w) , 使得 $x!+y!+z!=w!$.

23 求满足下述条件的整数数组 (a,b) 的组数: $0 \leqslant a,b \leqslant 36$, 且 $a^2+b^2=0(\bmod 37)$.

24 设 m,n 为正整数, 且 $mn \mid m^2+n^2+m$. 证明: m 是一个完全平方数.

25 证明: 若正整数 n 可以表示为三个正整数的平方和的形式, 则 n^2 也可以表示为三个正整数的平方和的形式.

26 求所有的正整数 n , 使得 n 的三次方根等于 n 去掉最后三位数字后得到的正整数.

27 证明: 存在无穷多个整数 n , 使得数 $n,n+1,n+2$ 都可以表示为两个整数 (不必不同) 的平方和. 例如: $0=0^2+0^2, 1=0^2+1^2, 2=1^2+1^2$, 故 $n=0$ 即为一个满足条件的整数.

28 求最小的正整数 n , 使得在十进制表示下 n^3 的末三位数字是 888 .

29 设正整数 $n>1$, 证明: 数 2^n-1 既不是完全平方数, 也不是完全立方数.

30 设 a,b,c 为正整数, 且 $\sqrt{a}+\sqrt{b}+\sqrt{c}$ 为整数. 证明: a,b,c 都是完全平方数.

31 已知正整数 c 是一个奇合数. 证明: 存在正整数 a , 使得 $a \leqslant \frac{c}{3}-1$, 且 $(2a-1)^2+8c$ 是一个完全平方数.

32 设整数 a,b 满足: 对任意正整数 n , 数 $2^n \cdot a+b$ 都是完全平方数. 证明: $a=0$.

33 求不能表示为 42 的正倍数与一个合数之和的最大正整数.

34 求一个正整数 n , 使得数 $n,n+1,\cdots,n+20$ 中每个数都与 30030 不互素.

35 是否存在连续 13 个正整数, 其中每个数都是 $2,3,5,7,11$ 中的某个数的倍数? 连续 14 个呢?

36 设 p 为素数, a, n 都是正整数, 且 $2^p+3^p=a^n$. 证明: $n=1$.

37 圆周上排列着 2000 个点, 在某个点上标上数 1 , 按顺时针方向数两个点, 在其上标数 2 , 再数 3 个点标数 3 , 依此继续, 标出数 $1,2,\cdots,2000$. 这样, 有些点上没有标数, 有些点上所标的数不止一个. 问: 被标上 2000 的那个点上所标的数中最小的是多少?

38 圆周上有 800 个点, 依顺时针方向标号为 $1,2,\cdots,800$, 它们将圆周分为 800 个间隙. 现在选定某个点, 将其染上红色, 然后进行下述操作: 如果第 k 号点染成了红色, 那么依顺时针方向转过 k 个间隙, 将所到达的点染成红色. 问: 依此规则, 圆周上最多有多少个点被染成了红色？证明你的结论.

39 设 m 为正整数, 且 $m\equiv 2(\bmod 4)$. 证明: 至多存在一对正整数 (a,b) , 使得 $m=ab$, 且 $0<a-b<\sqrt{5+4\sqrt{4m+1}}$.

40 设 n 是一个大于 10 的正整数, 且 n 的每个数码都为 $1,3,7$ 或 9 . 证明: n 有一个大于 10 的素因子.

41 求所有的素数对 (p,q) , 使得 $pq\mid p^p+q^q+1$.

42 设 $f(n)=1+n+n^2+\cdots+n^{2010}$. 证明: 对任意整数 m , 若 $2\leqslant m\leqslant 2010$, 则不存在正整数 n, 使得 $m\mid f(n)$.

43 是否存在整数 x,y , 使得 $x^{2012}-2010=4y^{2011}+4y^{2010}+2011y$?