1. “物不知其数”

我国有一部古数学书叫孙子算经；它成书于公元三世纪到五世纪之间，但书的作者名字已经失传了．孙子算经和我国许多古数学书一样是按问题编排的，它里面有一个问题叫“物不知其数”，写道：

“今有物不知其数，三三数之剩二，五五数之剩三，
七七数之剩二，问物几何？”

这个问题是说：有一个正整数，用3去除它余数是2，用5去除它余数是3，用7去除它余数是2，问这个正整数等于几？

孙子算经里给出了解这个问题的算法：

“术曰：三三数之剩二，置一百四十；五五数之剩三，置六十三；七七数之剩二，置三十；并之得二百三十三；以二百一十减之即得．凡三三数之剩一，则置七十；五五数之剩一，则置二十一；七七数之剩一，则置十五；一百六以上，以一百五减之即得．”

可以用下面的算式表示这个算法中的第一句话：

$$140+63+30=233,$$
$$233-210=23.$$

23就是“物不知其数”这个问题的解．算法中的第二句话指出70，21和15这三个数是解这个问题的关键数．我们注意到：

$$140=2\cdot 70,\quad 63=3\cdot 21,$$
$$30=2\cdot 15,\quad 210=2\cdot 105.$$

问题是70，21，15这三个数有什么意义呢？还有，105是怎么来的呢？

仔细分析一下就会发现：70是5和7的公倍数，用3去

除它余数是1;21是3和7的公倍数,用5去除它余数是1;15是3和5的公倍数，用7去除它余数是1. 因此，2·70是5和7的公倍数,用3去除它余数是2;3·21是3和7的公倍数,用5去除它余数是3;2·15是3和5的公倍数,用7去除它余数是2. 那么2·70+3·21+2·15=140+63+30=233就是这样一个数:用3去除它余数是2,用5去除它余数是3,用7去除它余数是2. 又105=3·5·7，而233>105,那么从233减去两个105，就得到“物不知其数”这个问题的最小正整数解23.

至于70,21和15这三个关键数是怎样求出来的呢?先看70,即怎样去求5和7的一个倍数，用3去除它余数是1?先看5和7的最小公倍数35是否用3去除它余数是1?不是. 那么再看2·35是否用3去除它余数是1?是. 这样就得到2·35=70. (如果2·35被3去除的余数仍不等于1，就再看3·35,等等.) 至于21和15,用这个办法就更容易求出来了.

公元十六世纪，程大位曾将“物不知其数”这个问题的“术曰”(即算法)编成了一个歌诀:

“三人同行七十稀,
五树梅花廿一枝,
七子团圆整半月,
除百零五便得知.”

(见程大位，算法统宗 (1593).)有了前面对“术曰”的解释，这个歌诀的意思是不难明了的.

为了熟悉“物不知其数”这个问题的算法，再看一个例题.

例题1 有一个正整数，用7去除它余数是1,用9去除它余数是4,用5去除它余数是3. 问这个正整数等于几?

先求关键数. 求一个正整数，它是9和5的倍数，用7去除它余数是1. 先看9和5的最小公倍数45,用7去除它是

否余数是 1？不是，再看 $2\cdot45$ 是否用 7 除余 1？不是．再看 $3\cdot45$, $4\cdot45$, $5\cdot45$, 最后发现 $5\cdot45=225$ 用 7 除余数是 1. 因此 225 是一个关键数.

再求一个正整数，它是 7 和 5 的倍数，用 9 去除它余数是 1. 逐一检查 35, $2\cdot35$, $3\cdot35$, … , 最后发现 $8\cdot35=280$ 用 9 除余数是 1.

再求一个正整数，它是 7 和 9 的倍数，用 5 去除它余数是 1. 逐一检查 63, $2\cdot63$, …, 发现 $2\cdot63=126$ 用 5 除余数是 1.

因此 225, 280, 126 这三个数是关键数．那么

$$1\cdot225+4\cdot280+3\cdot126=1723$$

就是这样一个数，用 7 除余数是 1，用 9 除余数是 4，用 5 除余数是 3．又 $7\cdot9\cdot5=315$, 而 $1723>315$, 因此从 1723 减去 5 个 315, 就得到

$$1723-5\cdot315=148.$$

148 就是这个例题的最小正整数解.

习题 1. 今有物不知其数，七七数之剩一，八八数之剩二，九九数之剩三，问物几何？

习题 2. 有一个正整数，用 3 去除它余数是 1，用 5 去除它余数是 2，用 7 去除它余数是 3，用 8 去除它余数是 4，问这个正整数等于几？

最后我们再看一个例题.

例题 2 求一个正整数，用 6 去除它余数是 5，用 8 去除它余数是 2.

仿照上面的作法，先找关键数．求一个正整数，它是 8 的倍数，而用 6 去除它余数是 1，逐一检查 8, $2\cdot8$, $3\cdot8$, … , 发现它们用 6 去除都不可能余 1. 同样，也找不到 6 的倍数，

用 8 去除它余数是 1. 因此关键数不存在，用原来的解“物不知其数”这个问题的算法不能解这个例题.

我们还可以从另外的途径来分析这个例题. 用 6 去除余数是 5 的正整数必具形状 $6k+5$，这里 k 是正整数. $6k+5$ 是奇数，用偶数 8 去除它，余数一定也是奇数，因此余数不可能是 2，所以这个例题无解.

但是如果我们把这个例题修改一下，求一个正整数，用 6 去除它余数是 5，用 8 去除它余数是 7. 这样就有解了，逐一检查 $6\cdot1+5$，$6\cdot2+5$，$6\cdot3+5$，…，就会发现 $6\cdot3+5=23$ 用 8 除余数是 7. 因此 23 就是这个新问题的解.

因此“物不知其数”这类问题有时有解，有时无解. 以后我们要讨论有解的充分必要条件. 现在我们注意，在“物不知其数”原题里，3，5，7 中任意两个数的最大公约数都是 1，这时可以用求关键数的办法来求解.

习题 3. 证明找不到一个正整数，用 2 去除它余数是 1，用 3 去除它余数是 2，用 8 去除它余数是 4.

2. 辗转相除法

在上节我们见到，解“物不知其数”这个问题的关键是求出关键数 70，21 和 15．70 是这样一个正整数，它是 35＝5·7 的倍数，而用 3 去除它余数是 1．注意 35 和 3 的最大公约数等于 1．我们可以一般地提出下面的问题．

问题一．设 M 和 m 是两个正整数，它们的最大公约数是 1．要求一个正整数，它是 M 的倍数，而用 m 去除它余数是 1．

这个问题实际上是要求一个正整数 k 使得 $kM=qm+1$，这里 q 是用 m 去除 kM 所得的商．这时有 $kM+(-q)m=1$．反过来，如果我们能够找到两个整数 r 和 s 使 $rM+sm=1$，那么问题一也就迎刃而解了．实际上，如果 $r>0$，那么就一定有 $s<0$，于是令 $k=r$，$q=-s$ 就行了．如果 $r<0$，设 t 是一个正整数使 $r+tm>0$，那么就有 $(r+tm)M+(s-tM)m=1$，于是令 $k=r+tm$，$q=tM-s$ 就行了．因此问题一就化成了下面的问题二．

问题二．设 M 和 m 是两个正整数，它们的最大公约数是 1．要求两个整数 r 和 s 使 $rM+sm=1$．

还可以更一般地提出下面的问题三．

问题三．设 a 和 b 是两个正整数．求它们的最大公约数 d，并且求两个整数 r 和 s 使 $ra+sb=d$．这时我们说 d 表成了 a 和 b 的整系数（r 和 s 的）线性组合．

通常我们把 a 和 b 的最大公约数记作 (a,b)，而当 $(a,b)=1$ 时，我们就说 a 和 b 互素（或互质）．例如，$(6,8)=2$，$(27,15)=3$，$(81,64)=1$．

我们知道，可以用著名的辗转相除法来求两个正整数的最大公约数．我们先来介绍带余除法算式．

设 m 是一个正整数，而 a 是另一个整数．设用 m 去除 a 得到的商是 q，而余数是 r，(我们要求 r 不能是负数)，写成式子

$$a=qm+r,\quad 0\leqslant r<m. \tag{1}$$

这个式子就叫带余除法算式，它非常基本，一定要熟记．例如，用 15 去除 37，商是 2，余数是 7，于是就写

$$37=2\cdot 15+7,\quad 0<7<15.$$

又如，用 15 去除 -37，商是 -3，余数是 8 (注意，我们要求余数一定不能是负数!)，于是就写

$$-37=(-3)15+8,\quad 0<8<15.$$

习题 1．用 31 去除 117，并写成带余除法算式．再将 14 去除 -31 的结果写成带余除法算式．

如果在(1)式中 $r=0$，我们就说 m 除尽 a，并记作 $m|a$．这时我们也说 a 是 m 的倍数，m 是 a 的约数．如果在(1)式中 $r\neq 0$，我们就说，m 除不尽 a，记作 $m\nmid a$．例如 $3\mid 12$，$21\mid -63$，$3\nmid 8$ 等等．

我们先举一个例子，看怎样用辗转相除法来求两个正整数的最大公约数．

例题 1．计算 (6188, 4709)．

先用 4709 去除 6188，商是 1，余数是 1479，写成带余除法算式

$$6188=1\cdot 4709+1479, \tag{2}$$

再用刚才得到的余数 1479 去除刚才除法中的除数 4709，商是 3，余数是 272，写成

$$4709=3\cdot 1479+272. \tag{3}$$

再用余数 272 去除上面除法中的除数 1479, 商是 5，余数是 119, 写成

$$1479 = 5 \cdot 272 + 119, \tag{4}$$

再用 119 去除 272, 商是 2, 余数是 34, 写成

$$272 = 2 \cdot 119 + 34. \tag{5}$$

再用 34 去除 119, 商是 3, 余数是 17, 写成

$$119 = 3 \cdot 34 + 17. \tag{6}$$

再用 17 去除 34, 正好除尽，商是 2, 余数是 0, 写成

$$34 = 2 \cdot 17.$$

因此

$$(6188, 4709) = 17.$$

习题 2. 计算 (187, 221).

习题 3. 计算 (628, 318).

下面我们来介绍辗转相除法的严格叙述，请读者耐心地把它读完.

设 a 和 b 是两个正整数. 记 $r_{-1} = a, r_0 = b$. 先用 r_0 去除 r_{-1}, 设所得的商是 q_1，余数是 r_1, 写成带余除法算式

$$r_{-1} = q_1 r_0 + r_1, \qquad 0 \leqslant r_1 < r_0. \tag{7}$$

如果 $r_1 = 0$, 那么 $r_0 = b$ 除尽 $r_{-1} = a$，因此 a 和 b 的最大公约数就是 b.

如果 $r_1 \neq 0$，再用 r_1 去除 r_0, 设商是 q_2, 余数是 r_2，即

$$r_0 = q_2 r_1 + r_2, \qquad 0 \leqslant r_2 < r_1. \tag{8}$$

如果 $r_2 = 0$, 那么 $r_1 \mid r_0$, 再由 (7) 式知 $r_1 \mid r_{-1}$，所以 r_1 是 $r_{-1} = a$ 和 $r_0 = b$ 的一个公约数. 反之，由 (7) 式，$r_{-1} = a$ 和 $r_0 = b$ 的任何一个公约数一定除尽 r_1，因此 r_1 是 a 和 b 的最大公约数.

如果 $r_2 \neq 0$, 再用 r_2 去除 r_1, 设商是 q_3，余数是 r_3, 即

$$r_1 = q_3 r_2 + r_3, \qquad 0 \leqslant r_3 < r_2. \tag{9}$$

如果 $r_3=0$，那么 $r_2 \mid r_1$，再由(8)式知 $r_2 \mid r_0$，再由(7)式知 $r_2 \mid r_{-1}$，所以 r_2 是 $r_{-1}=a$ 和 $r_0=b$ 的一个公约数. 反之，$r_{-1}=a$ 和 $r_0=b$ 的任何一个公约数，由(7)式，一定除尽 r_1，再由(8)式一定也除尽 r_2，所以 r_2 是 a 和 b 的最大公约数.

如果 $r_3 \neq 0$，再用 r_3 去除 r_2，等等. 由于 $r_0>r_1>r_2>\cdots$ 逐步小下来，而又都是正整数，因此经过有限步骤后一定达到一个 $r_n>0$，而 $r_{n+1}=0$. 这时 $(a, b)=r_n$，下面我们要证明这一点.

辗转相除法在国外叫做欧几里得算法，见于欧几里得的几何原本 (公元前 300 年左右). 这个算法不但给出了求最大公约数的算法，而且还可以利用其计算过程找到整数 r 和 s 使 $ra+sb=(a, b)$. 我们再用前面的例题 1 来说明.

例题 1 (续) 已知 $(6188, 4709)=17$. 求两个整数 r 和 s 使 $r \cdot 6188+s \cdot 4709=17$.

由(6)式，

$$17=1 \cdot 119+(-3) \cdot 34.$$

从(5)式解出 34，代入上式，得

$$\begin{aligned} 17 &= 1 \cdot 119+(-3)[272+(-2)119] \\ &= (-3) \cdot 272+7 \cdot 119. \end{aligned}$$

从(4)式解出 119，代入上式，得

$$\begin{aligned} 17 &= (-3) \cdot 272+7[1479+(-5) \cdot 272] \\ &= 7 \cdot 1479+(-38) \cdot 272 \end{aligned}$$

从(3)式解出 272，代入上式，得

$$\begin{aligned} 17 &= 7 \cdot 1479+(-38)[4709+(-3) \cdot 1479] \\ &= (-38) \cdot 4709+121 \cdot 1479 \end{aligned}$$

最后从(2)式解出 1479，代入上式，得

$$17=(-38)\cdot 4709+121[6188+(-1)\cdot 4709]$$
$$=121\cdot 6188+(-159)\cdot 4709.$$

因此所求的 $r=121, s=-159$.

习题 4. 将(187, 221)表成 187 和 221 的整系数线性组合.

习题 5. 将(628, 318)表成 628 和 318 的整系数线性组合.

现在我们把前面介绍的关于 $r_{-1}=a$ 和 $r_0=b$ 的辗转相除法诸算式写在一起:

$$r_{-1}=q_1r_0+r_1, \qquad 0<r_1<r_0 \tag{10.1}$$
$$r_0=q_2r_1+r_2, \qquad 0<r_2<r_1 \tag{10.2}$$
$$\cdots \quad \cdots \quad \cdots \qquad \cdots \cdots \cdots$$
$$r_{k-2}=q_kr_{k-1}+r_k, \qquad 0<r_k<r_{k-1} \tag{10.k}$$
$$\cdots \quad \cdots \quad \cdots \qquad \cdots \cdots \cdots$$
$$r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}, \qquad 0<r_{n-1}<r_{n-2} \tag{10.n-1}$$
$$r_{n-2}=q_nr_{n-1}+r_n, \qquad 0<r_n<r_{n-1} \tag{10.n}$$
$$r_{n-1}=q_{n+1}r_n \tag{10.n+1}$$

我们先证明 $r_n=(a, b)$. 首先, 由(10.n+1)知 $r_n \mid r_{n-1}$. 再由(10.n)和 $r_n \mid r_{n-1}$, 知 $r_n \mid r_{n-2}$. 再由(10.n−1)和 $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$, 知 $r_n \mid r_{n-3}$. 如此继续下去, 最后可知 $r_n \mid r_0$, $r_n \mid r_{-1}$. $r_0=b$, $r_{-1}=a$, 因此 r_n 是 a 和 b 的一个公约数. 再设 $d=(a, b)$. 那么 $d \mid r_{-1}$, $d \mid r_0$. 由(10.1)推出 $d \mid r_1$, 再由(10.2)推出 $d \mid r_2$. 如此继续下去, 最后推出 $d \mid r_n$. 因为 d 是最大公约数, 因此 $r_n=d=(a, b)$.

其次我们指出利用(10)式可以将 r_n 表成 a 和 b 的整系数线性组合. 利用(10.n)式, 可将 r_n 表成 r_{n-2} 和 r_{n-1} 的整系数线性组合

$$r_n=r_{n-2}+(-q_n)r_{n-1}.$$

再由(10. $n-1$)式，得

$$r_{n-1}=r_{n-3}+(-q_{n-1})r_{n-2},$$

将它代入 r_n 的上述表达式，就将 r_n 表成 r_{n-3} 和 r_{n-2} 的整系数线性组合

$$r_n=(-q_n)r_{n-3}+(1+q_nq_{n-1})r_{n-2}.$$

如此继续下去，最后就将 r_n 表成 $r_{-1}=a$ 和 $r_0=b$ 的整系数线性组合.

因此辗转相除法给出了解问题三的一个切实可行的算法，特别也给出了解问题二和问题一的 切实可行的算法.

我们再回到"物不知其数"中求关键数这个问题去.

例题 2. 求 35 的一个倍数，用 3 去除它余数是 1.

用辗转相除法求(35, 3).

$$35=11\cdot 3+2,$$
$$3=1\cdot 2+1.$$

于是(35, 3)=1. 然后将 1 表成 35 和 3 的整系数线性组合

$$\begin{aligned}1&=3+(-1)\cdot 2\\&=3+(-1)[35+(-11)\cdot 3]\\&=(-1)\cdot 35+12\cdot 3.\end{aligned}$$

还要将 35 前面的系数变成正数. 用 3 去除 -1, 得

$$-1=-1\cdot 3+2,$$

代入上式，得

$$\begin{aligned}1&=(-1\cdot 3+2)\cdot 35+12\cdot 3\\&=2\cdot 35+(-23)\cdot 3.\end{aligned}$$

于是 $2\cdot 35=70$ 就是 35 的一个倍数，用 3 除它余数是 1.

应该指出，当数字大时，用辗转相除法去求关键数远比第一节所介绍的逐一检查法要好得多.

习题 6. 求 202 的一个倍数，用 97 去除它余数是 1.

习题 7. 今有一正整数，用 5 去除它余 3，用 43 去除它余 26，用 716 去除它余 199. 问这个正整数等于几?

3. 同 余 式

用近代数学的语言来说，“物不知其数”这个问题就是要求一个正整数 n，它适合下面三个同余式

$$n\equiv 2 \pmod 3$$
$$n\equiv 3 \pmod 5$$
$$n\equiv 2 \pmod 7.$$

因此我们就来介绍一下同余和同余式的概念.

设 m 是一个正整数，而 a 和 b 是两个整数. 设用 m 去除 a 得的商是 q，余数是 r，即

$$a=qm+r, \quad 0\leqslant r<m.$$

再设用 m 去除 b 得的商是 q'，余数是 r'，即

$$b=q'm+r', \quad 0\leqslant r'<m.$$

如果 $r=r'$，即用 m 去除 a 和 b 得的余数相同，我们就说 a 和 b 同余 mod m. 显然 $r=r'$，当且仅当 $m\mid a-b$. 因此当 $m\mid a-b$ 时，a 和 b 同余 mod m. 用符号

$$a\equiv b \pmod m$$

来表示 a 和 b 同余mod m，读作 a 同余 b 模 m. 如果 a 和 b 不同余 mod m，就记作

$$a\not\equiv b \pmod m,$$

读作 a 不同余 b 模 m.

例 1. $8\equiv 5 \pmod 3$，$-10\equiv 2 \pmod 3$，$7\not\equiv 5 \pmod 3$.

例 2. 当 $m=1$ 时，任何两个整数都是同余的.

定理 1 同余有以下这些性质：

1) $a\equiv a \pmod m$. (反身性)

2) 如果 $a\equiv b \pmod m$，那么 $b\equiv a \pmod m$. (对称性)

3）如果 $a\equiv b \pmod m$，$b\equiv c \pmod m$，那么 $a\equiv c \pmod m$.（传递性）

并且还有

4）如果 $a\equiv b \pmod m$，$c\equiv d \pmod m$，那么 $a+c\equiv b+d \pmod m$，$a-c\equiv b-d \pmod m$.

5）如果 $a\equiv b \pmod m$，$c\equiv d \pmod m$，那么 $ac\equiv bd \pmod m$.

这几个性质都是不难证明的，留作习题，请读者一定要自己证一下．但是要注意，同余式两边不能同除一个数，例如 $6\equiv 9 \pmod 3$，但是 $2\not\equiv 3 \pmod 3$.

习题 1. 证明定理 1.

习题 2. 证明 0，1，2，…，7 这八个数两两不同余 mod 8，而任何一个整数都和它们之中的一个同余 mod 8.

习题 3. 证明 0，1，2，…，$m-1$ 这 m 个数两两不同余 mod m，而任何一个整数都和它们之中的一个同余 mod m.

如果有 m 个整数两两不同余 mod m，而任何一个整数都和它们之中的一个同余 mod m，我们就说这 m 个整数是 mod m 的一组完全剩余系．例如，根据习题 3，0，1，2，…，$m-1$ 这 m 个数就是 mod m 的一组完全剩余系，同样，1，2，…，m 这 m 个整数也是 mod m 的一组完全剩余系.

习题 4. 证明{4，9，10，−1}和{0，1，2，−1}都是 mod 4 的完全剩余系.

设 $f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$，其中 $n>0$，$a_i(i=0,1,2,\cdots,n)$ 都是整数，又设 $m>0$，则

$$f(x)\equiv 0 \pmod m \tag{1}$$

叫做模 m 的同余式．如果 $a_0\not\equiv 0$，n 叫做同余式(1)的次数．如果有整数 x_0 满足 $f(x_0)\equiv 0 \pmod m$，则 x_0 就叫做同余式(1)

的解. 不同的解是指互不同余 mod m 的解.

要求同余式(1)的解, 只要逐个把 0, 1, 2,…, $m-1$ 代入(1)进行验算就可以了. 但当 m 或 n 大时, 计算量往往太大.

例题 1. 求同余式

$$x^5+2x^3+2\equiv 0 \pmod 5$$

的解.

用验算的方法知只有 1, 2 是解.

例题 2. 求同余式

$$x^2+1\equiv 0 \pmod 7$$

的解 .

用验算的方法知这个同余式无解.

我们不准备讨论一般同余式有解的条件, 解的个数以及怎样求解这些问题, 这会远离本书的主题. 我们只局限于讨论一次同余式有解的条件, 解的个数以及怎样求解的问题.

定理 2 设 m 是正整数, a 和 b 是整数. 再设 $(a, m)=d$. 那么同余式

$$ax\equiv b \pmod m \tag{2}$$

有解的充分必要条件是 $d\mid b$. 更进一步, 如果(2)有解, 那么(2)有 d 个解; 设 t 是(2)的一个解, 那么

$$t,\ t+\frac{m}{d},\ t+2\frac{m}{d},\ \cdots,\ t+(d-1)\frac{m}{d} \tag{3}$$

就是(2)的全部两两不同余的解.

证明 先证明第一个断言. 设(2)有解, 而 t 是(2)的一个解, 那么 $at\equiv b \pmod m$. 于是 $m\mid at-b$, 即有整数 k 使 $at-b=km$, 那么 $b=at-km$, 因此 $d\mid b$. 反之, 设 $d\mid b$. 因 $(a, m)=d$, 由第二节问题三, 有整数 r 和 s 使

$$ra+sm=d. \tag{4}$$

由 $d\mid b$, 可设有整数 l 使 $b=ld$, 将(4)式双方乘以 l, 得

$$lra+lsm=ld=b,$$

于是

$$a(lr)\equiv b \pmod{m},$$

这就是说 lr 是(2)的一个解.

再证明第二个断言. 设(2)有解而 t 是(2)的一个解, 即 $at\equiv b \pmod{m}$. 再设 t' 是(2)的任一解, 即 $at'\equiv b \pmod{m}$. 那么 $a(t'-t)\equiv 0 \pmod{m}$, 于是有整数 k 使 $a(t'-t)=km$, 写 $a=a_1d$, $m=m_1d$, 那么 $a_1(t'-t)=km_1$. 因 $(a_1, m_1)=1$, 所以 $m_1 | t'-t$, 即有整数 l 使 $t'-t=lm_1$, 那么 $t'=t+lm_1=t+l\frac{m}{d}$. 再证 $t+i\frac{m}{d}$, $i=0, 1, 2, \cdots$, 都是(2)的解:

$$a\left(t+i\frac{m}{d}\right)=at+i\frac{a}{d}m\equiv b \pmod{m}.$$

不难证明(2)的任一解 $t'=t+l\frac{m}{d}$ 一定和(3)中的一个数同余mod m, 而(3)中的 d 个数两两不同余mod m, 这样就完成了第二个断言的证明.

例题 3. 求同余式 $6x\equiv 3 \pmod{15}$ 的解.

$(6, 15)=3$. 用辗转相除法求得 $3=15+(-2)6$. 于是 -2 就是一个解. 根据定理 2, $6x\equiv 3 \pmod{15}$ 一共有 3 个解, 它们是 -2, $-2+\frac{15}{3}=3$, $-2+2\cdot\frac{15}{3}=8$.

习题 5 求下列同余式的解:

1) $101x\equiv 74 \pmod{221}$,

2) $135x\equiv 100 \pmod{160}$.

定理 2 有下面这个特例.

定理 3 设 m 是正整数, a 是整数, $(m, a)=1$ 那么对于任意整数 b, 同余式

$$ax \equiv b \pmod{m}$$

总有解，而且解唯一（即任意两个解都同余 mod m）.

最后，我们利用同余式来回答第一节末尾提出的问题.

定理 4 设m_1和m_2是两个正整数，$(m_1, m_2) = d$. 再设a_1和a_2是整数. 那么同余式

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2} \end{aligned} \tag{5}$$

有公共解的充分必要条件是$d \mid a_1 - a_2$.

证明 设x_0是(5)的一个公共解，那么$x_0 = a_1 + q_1 m_1 = a_2 + q_2 m_2$，于是$a_1 - a_2 = q_2 m_2 - q_1 m_1$. 设$m_1 = m_1' d$，$m_2 = m_2' d$，那么$a_1 - a_2 = (q_2 m_2' - q_1 m_1')d$，因此$d \mid a_1 - a_2$.

反之，假定$d \mid a_1 - a_2$. 设$a_1 - a_2 = qd$. 由于第二节问题三有解，有整数r和s使$d = rm_1 + sm_2$. 那么$a_1 - a_2 = q(rm_1 + sm_2)$. 于是$a_1 - qrm_1 = a_2 + qsm_2$就是(5)的公共解.

利用定理 4 也不难看出第一节例题 2 无解.

4. 孙子定理

上一节里，我们把“物不知其数”这个问题表达成求同余式组

$$n\equiv 2 \pmod 3$$
$$n\equiv 3 \pmod 5$$
$$n\equiv 2 \pmod 7$$

的公共解的问题，这里3, 5, 7是三个两两互素的整数. 这个问题自然可以推广成下面的问题四.

问题四. 给了r个正整数$m_1, m_2, \cdots, m_r$，它们两两互素；又给了r个整数$a_1, a_2, \cdots, a_r$. 求一个正整数x适合以下同余式组

$$x\equiv a_1 \pmod{m_1},$$
$$x\equiv a_2 \pmod{m_2},$$
$$\cdots\cdots \quad \cdots \quad \cdots$$
$$x\equiv a_r \pmod{m_r}.$$

我们要问：问题四的解是否存在？如果存在，那么解是否在某种意义下唯一？下面的定理回答了这两个问题.

孙子定理 设$m_1, m_2, \cdots, m_r$是r个两两互素的正整数. 任给r个整数$a_1, a_2, \cdots, a_r$，那么总存在一个整数x使得

$$x\equiv a_i \pmod{m_i}, \quad i=1,2,\cdots,r. \tag{1}$$

更进一步，如果令$m=m_1m_2\cdots m_r$，那么同余式组(1)的解$x \bmod m$是唯一的，即如果x和y是(1)的两个解，那么$x\equiv y \pmod m$.

孙子定理中解的唯一性部分是不难证明的. 设x和y是同余式组(1)的两个解，那么$x\equiv a_i \pmod{m_i}$, $y\equiv a_i \pmod{m_i}$, $i=1, 2, \cdots, r$. 于是$x\equiv y \pmod{m_i}$, $i=1, 2, \cdots, r$, 即

$m_i \mid x-y$，$i=1, 2, \cdots, r$．因为 $m_1, m_2, \cdots, m_r$ 两两互素，所以 $m_1 m_2 \cdots m_r \mid x-y$，即 $m \mid x-y$，也即 $x \equiv y \pmod{m}$．

要证明孙子定理中解的存在性部分，只要写出同余式组(1)的一个解就可以了．关键仍是先求出关键数．作乘积 $M_i = m_1 \cdots \hat{m}_i \cdots m_r$，即 M_i 是 $m_1, m_2, \cdots, m_r$ 这个 r 数中除去 m_i 之后剩下的 $r-1$ 个数的乘积．逐一检查 $M_i, 2M_i, 3M_i, \cdots$，看那一个先 $\equiv 1 \pmod{m_i}$．设 $k_i M_i \equiv 1 \pmod{m_i}$，那么

$$x = a_1 k_1 M_1 + a_2 k_2 M_2 + \cdots + a_r k_r M_r$$

就是同余式组(1)的一个解．再从 x 减去 $m = m_1 m_2 \cdots m_r$ 的一个适当倍数，就可以得到同余式组(1)的一个最小正整数解．

上面的证明还需要补证一定存在一个正整数 k_i 使 $k_i M_i \equiv 1 \pmod{m_i}$．因为 $(M_i, m_i) = 1$，根据第二节问题二，总存在整数 r_i 和 s_i 使 $s_i M_i + r_i m_i = 1$．那么 $s_i M_i \equiv 1 \pmod{m_i}$．如果 $s_i > 0$，令 $k_i = s_i$ 即可．如果 $s_i < 0$，根据带余除法算式有 $s_i = q_i m_i + t_i$，$0 < t_i < m_i$，令 $k_i = t_i$ 即可．

孙子定理的解的存在性证明实际上还给出了一个求解的算法．但在求关键数时，需要一个一个地检查 $M_i, 2M_i, \cdots$，看那一个先 $\equiv 1 \pmod{m_i}$，从而得到 $k_i > 0$ 使 $k_i M_i \equiv 1 \pmod{m_i}$．这样做是很麻烦的．因此有必要寻找求 k_i 的简便方法．在第二节中我们介绍过利用辗转相除法，即用欧几里得算法来求，但是欧几里得算法传入我国很晚．公元十三世世，南宋的数学家秦九韶（公元1202—1261年）在研究一次同余式组的解的时候，独立地提出了欧几里得算法，并增补了一个更易于求 k_i 的算法，它还可用来解决第二节问题三．这个算法叫做“大衍求一术”，记录在他的名著《数书九章》(1274年)之中．“大衍求一术”神奇而巧妙，其思想对后来的数学都有影响.我们将在下一节里介绍它．

5. “大衍求一术”

“大衍求一术” 设a和b是两个正整数. 令$r_{-1}=a$, $r_0=b$. 对r_{-1}和r_0进行辗转相除, 各次除法的商依序记作q_1, q_2, …, 而余数依序记作r_1, r_2, …. 我们有

$$r_{k-2}=q_k r_{k-1}+r_k, \quad 0<r_k<r_{k-1}, \quad k=1, 2, 3, \cdots \tag{1}$$

令$c_{-1}=1$, $c_0=0$, $d_{-1}=0$, $d_0=1$. 再按以下公式归纳地定义c_k, d_k, $k=1, 2, 3, \cdots$:

$$c_k=q_k c_{k-1}+c_{k-2}, \tag{2}$$

$$d_k=q_k d_{k-1}+d_{k-2}. \tag{3}$$

设n是最小足码使$r_n \mid r_{n-1}$, 即$r_{n+1}=0$, 那么$r_n=(a, b)$, 而

$$r_n=(-1)^{n-1} c_n a+(-1)^n d_n b. \tag{4}$$

特别, 当$(a, b)=1$时, $(-1)^{n-1} c_n a \equiv 1 \pmod{b}$. 因此, 如果要求最小正整数$k$, 使$k \cdot a \equiv 1 \pmod{b}$, 那么当$(-1)^{n-1} c_n>0$时, 有$k=(-1)^{n-1} c_n$; 而当$(-1)^{n-1} c_n<0$时, 用$b$去除$(-1)^{n-1} c_n$, 设余数是$r$, 即$(-1)^{n-1} c_n=qb+r$, $0<r<b$, 就有$k=r$.

例题 1 用“大衍求一术”计算$(6188, 4709)$, 并求两个整数r和s使$r \cdot 6188+s \cdot 4709=(6188, 4709)$.

列计算格式如下:

k	q_k	r_k	c_k	d_k
−1		6188	1	0
0		4709	0	1
1	1	1479	1	1
2	3	272	3	4
3	5	119	16	21
4	2	34	35	46
5	3	17	121	159
6	2	0		

因此 $r_5=17=(6188, 4709)$，而

$$17=121\cdot 6188+(-159)\cdot 4709.$$

例题 2. 求最小正整数 k, 使 $k\cdot 35\equiv 1 \pmod 3$

先用大衍求一术求 $(35, 3)$，并把它表成 35 和 3 的整系数线性组合．列计算格式如下：

k	q_k	r_k	c_k	d_k
−1		35	1	0
0		3	0	1
1	11	2	1	11
2	1	1	1	12
3	2	0		

因此

$$(35,\ 3)=r_2=1=(-1)35+12\cdot 3.$$

那么 $(-1)\cdot 35\equiv 1 \pmod 3$．用 3 去除 −1，列出除法算式

$$-1=(-1)\cdot 3+2,\quad 0<2<3$$

于是 $2\cdot 35\equiv 1 \pmod 3$．因此 $70\equiv 1 \pmod 3$．

现在我们来证明大衍求一术的正确性．$r_n=(a, b)$这一事实是在第二节中已经证明了的，还需要证明(4)式成立．可以一般地先证明

$$r_k=(-1)^{k-1}c_k r_{-1}+(-1)^k d_k r_0,\ k=1,2,\cdots,n \quad (5)$$

然后在(5)式中令 $k=n$ 就得到(4)式.

我们对 k 作归纳来证明(5)式.

当 $k=-1$ 时

$$c_{-1}r_{-1}+(-d_{-1})r_0=1\cdot r_{-1}+0\cdot r_0=r_{-1},$$

当 $k=0$ 时,

$$(-c_0)r_{-1}+d_0 r_0=0\cdot r_{-1}+1\cdot r_0=r_0.$$

因此当 $k=-1$ 和 0 时, (5)式成立.

现在设 $k>0$, 并假定(5)式对 $k-2$, $k-1$ 都成立. 那么由归纳假设及(1), (2), (3)式就有

$$\begin{aligned}r_k&=r_{k-2}-q_k r_{k-1}\\&=(-1)^{k-3}c_{k-2}r_{-1}+(-1)^{k-2}d_{k-2}r_0\\&\quad-q_k[(-1)^{k-2}c_{k-1}r_{-1}+(-1)^{k-1}d_{k-1}r_0]\\&=(-1)^{k-3}(c_{k-2}+q_k c_{k-1})r_{-1}\\&\quad+(-1)^{k-2}(d_{k-2}+q_k d_{k-1})r_0\\&=(-1)^{k-1}c_k r_{-1}+(-1)^k d_k r_0,\end{aligned}$$

因此(5)式对 k 也成立, 这就完成了归纳法证明.

最后我们指出, 如果用辗转相除法去求第二节问题三的解, 特别是把 a 和 b 的最大公约数表成 a 和 b 的整系数线性组合, 需要把辗转相除的每个除法算式都保留下来, 留作最后代入时用. 但用大衍求一术来做, 就不必这样, 因此如果用电子计算机来做, 就节省了存贮量. 当然秦九韶的时代还没有电子计算机. 在今天电子计算机的时代, 我们更可看出大衍求一术的优越性.

习题 1. 用大衍求一术将(187,221)表成 187 和 221 的整系数线性组合.

习题 2. 用大衍求一术将(628, 318)表成 628 和 318 的整系数线性组合.

6. 多项式的情形

前面几节讨论的都是有关整数的问题，对于多项式也有平行的理论.

我们先复习一下多项式的除法. 设有多项式 $f(x)=x^4-4x^2-3x+5$ 和 $g(x)=x^2+x+1$，我们要用 $g(x)$ 去除 $f(x)$，这样 $f(x)$ 称为被除式，$g(x)$ 称为除式. 列除法竖式如下：

$$
\begin{array}{r|l}
x^2+x+1 & x^2-x+4 \\
\hline
x^4+4x^2-3x+5 & \\
x^4+x^3+x^2 & \\
\hline
-x^3+3x^2-3x+5 & \\
-x^3-x^2-x & \\
\hline
4x^2-2x+5 & \\
4x^2+4x+4 & \\
\hline
-6x+1 &
\end{array}
$$

于是得到商 x^2-x+4，余式 $-6x+1$. 我们可以把这个除法写成带余除法算式的形式：

$$x^4+4x^2-3x+5=(x^2-x+4)(x^2+x+1)+(-6x+1)$$

我们注意到余式 $-6x+1$ 的次数 $<$ 除式 x^2+x+1 的次数，因为否则还可以再除下去.

习题 1. 用 $g(x)=x^3-x^2+1$ 去除 $f(x)=x^6+2$，求商和余式，并写出带余除法算式.

一般地，我们有：设 $f(x)$ 和 $g(x)$ 是两个不等于零的多项式. 设用 $g(x)$ 去除 $f(x)$ 得到商 $q(x)$ 和余式 $r(x)$，那么 $r(x)=0$ 或 $\deg r(x)<\deg g(x)$（这里 $\deg r(x)$ 和 $\deg g(x)$ 分别表示 $r(x)$ 和 $g(x)$ 的次数）. 可以将这个除法写成带余除法

算式:

$$f(x)=q(x)g(x)+r(x),$$
$$r(x)=0 \text{ 或 } \deg r(x)<\deg g(x). \tag{1}$$

这个式子是非常基本的.

如果在(1)式中, $r(x)=0$, 我们就说 $g(x)$除尽 $f(x)$, 记作 $g(x)\mid f(x)$; 这时我们也说 $f(x)$是 $g(x)$的倍式, 而 $g(x)$是 $f(x)$的因式. 如果 $r(x)\neq 0$, 我们就说 $g(x)$除不尽 $f(x)$, 记作 $g(x)\nmid f(x)$.

带余除法算式的一个重要推论是:

余式定理 用 $x-a$ 去除多项式 $f(x)$得到的余式是常数 $f(a)$.

证明 写出带余除法算式

$$f(x)=q(x)(x-a)+r(x),$$
$$r(x)=0 \text{ 或 } \deg r(x)<\deg (x-a). \tag{2}$$

由 $\deg r(x)<\deg (x-a)=1$, 推出 $r(x)$是个常数, 记作 r. 将 $x=a$ 代入(2)式就得出 $f(a)=r$.

既然有了带余除法算式, 因此多项式也有辗转相除法. 辗转相除法的算式和整数的情形完全相似.

假定 $a(x)$和 $b(x)$是两个不等于零的多项式. 令 $r_{-1}(x)=a(x)$, $r_0(x)=b(x)$. 用 $r_0(x)$去除 $r_{-1}(x)$, 得到商 $q_1(x)$和余式 $r_1(x)$, 也就是

$$r_{-1}(x)=q_1(x)r_0(x)+r_1(x),$$
$$r_1(x)=0 \text{ 或 } \deg r_1(x)<\deg r_0(x).$$

如果 $r_1(x)=0$, 那么 $a(x)$和 $b(x)$的最高公因式就是 $r_0(x)$, 即 $b(x)$.

如果 $r_1(x)\neq 0$, 就用 $r_1(x)$去除 $r_0(x)$, 得到商 $q_2(x)$和余式 $r_2(x)$, 也就是

$$r_0(x)=q_2(x)r_1(x)+r_2(x),$$
$$r_2(x)=0 \text{ 或 } \deg r_2(x)<\deg r_1(x).$$

如果 $r_2(x)=0$，那么 $r_1(x)$就是 $a(x)$和 $b(x)$的最高公因式.

如果 $r_2(x)\neq 0$，就用 $r_2(x)$去除 $r_1(x)$，得

$$r_1(x)=q_3(x)r_2(x)+r_3(x),$$
$$r_3(x)=0 \text{ 或 } \deg r_3(x)<\deg r_2(x).$$

这样进行下去，得到一系列多项式

$$r_0(x),\ r_1(x),\ r_2(x),\ r_3(x),\ \cdots,$$

它们的次数一个比一个小. 因此不能无限下去，一定到某一步 n 会出现

$$r_{n-2}(x)=q_n(x)r_{n-1}(x)+r_n(x),$$
$$r_n(x)\neq 0 \text{ 且} \deg r_n(x)<\deg r_{n-1}(x),$$

及

$$r_{n-1}(x)=q_{n+1}(x)r_n(x).$$

那么，$r_n(x)$就是 $a(x)$是 $b(x)$的最高公因式.

习题 2. 证明 $r_n(x)$是 $a(x)$和 $b(x)$的最高公因式.

习题 3. 求 $x^5+x^3+2x^2+2$ 和 $x+1$ 的最高公因式.

多项式也有大衍求一术.

大衍求一术 设 $a(x)$和 $b(x)$是两个不等于 0 的多项式. 令 $r_{-1}(x)=a(x)$，$r_0(x)=b(x)$. 对 $r_{-1}(x)$和 $r_0(x)$进行辗转相除，各次除法的商依序记作 $q_1(x)$，$q_2(x)$，…，而余数依序记作 $r_1(x)$，$r_2(x)$，…. 我们有

$$r_{k-2}(x)=q_k(x)r_{k-1}(x)+r_k(x),\ \deg r_k(x)<\deg r_{k-1}(x),$$

$k=1,2,\cdots$. 令 $c_{-1}(x)=1$，$c_0(x)=0$，$d_{-1}(x)=0$，$d_0(x)=1$. 再按以下公式归纳地定义 $c_k(x)$，$d_k(x)$，$k=1,2,3,\cdots$：

$$c_k(x)=q_k(x)c_{k-1}(x)+c_{k-2}(x),$$
$$d_k(x)=q_k(x)d_{k-1}(x)+d_{k-2}(x).$$

设 n 是最小足码使 $r_n(x) \mid r_{n-1}(x)$，即 $r_{n+1}(x)=0$，那么 $r_n(x)=(a(x), b(x))$，而

$$r_n(x)=(-1)^{n-1}c_n(x)a(x)+(-1)^n d_n(x)b(x). \quad (3)$$

习题 4. 证明(3)式成立.

例题 1. 求 x^4+x^3+2x+2 和 x^2+1 的最高公因式，并把它表成 x^4+x^3+2x+2 和 x^2+1 的以多项式为系数的线性组合.

用大衍求一术来做. 列出计算格式如下:

k	$q_k(x)$	$r_k(x)$	$c_k(x)$	$d_k(x)$
-1		x^4+x^3+2x+2	1	0
0		x^2+1	0	1
1	x^2+x-1	$x+3$	1	x^2+x-1
2	$x-3$	10	$x-3$	x^3-2x^2-4x+4
3	$\frac{1}{10}(x+3)$	0		

因此 $(x^4+x^3+2x+2, x^2+1)=1$，而

$$10=(-1)(x-3)\cdot(x^4+x^3+2x+2)+(x^3-2x^2-4x+4)\cdot(x^2+1).$$

于是

$$1=\left(-\frac{1}{10}x+\frac{3}{10}\right)\cdot(x^4+x^3+2x+2)+\left(\frac{1}{10}x^3-\frac{1}{5}x^2-\frac{2}{5}x+\frac{2}{5}\right)\cdot(x^2+1).$$

习题 5. 求 $x^5+x^3+2x^2+1$ 和 x^2+x+1 的最高公因式，并把它表成 $x^5+x^3+2x^2+1$ 和 x^2+x+1 的以多项式为系数的线性组合.

对于多项式也可以引进同余和同余式等概念. 由于和整数情形完全一样, 我们就不重复了. 对于多项式, 孙子定理也成立.

孙子定理 设 $m_1(x)$, $m_2(x)$, $\cdots$, $m_r(x)$是r个两两互素的多项式. 任给r个多项式 $a_1(x)$, $a_2(x)$, $\cdots$, $a_r(x)$, 那么总存在一个多项式$f(x)$使得

$$f(x)\equiv a_i(x)\ (\mathrm{mod}m_i(x)),\ i=1,2,\cdots,r. \qquad (4)$$

更进一步, 如果令 $m(x)=m_1(x)m_2(x)\cdots m_r(x)$, 那么同余式组(4)的解 $f(x)\bmod m(x)$是唯一的.

解的唯一性部分的证明和整数的情形完全一样. 解的存在性部分的证明也一样, 这里是先找关键多项式$A_1(x)$, $A_2(x),\cdots,A_r(x)$, $A_i(x)$是 $M_i(x)=m_1(x)\cdots\hat{m}_i(x)\cdots m_r(x)$的倍式而与$m_i(x)$互素. 这可以用大衍求一术算出. 那么

$$f(x)=a_1(x)A_1(x)+a_2(x)A_2(x)+\cdots+a_r(x)A_r(x)$$

就是同余式组(4)的一个解.

例题 2. 有一个多项式, 用 $x+1$ 去除它余式是 2, 用 x^2+1 去除它余式是 $x+1$, 用 x^2+3 去除它余式是 $2x$. 求出这个多项式.

先求被$(x^2+1)(x^2+3)$除尽, 而用 $x+1$ 去除余式是 1 的多项式. 由余式定理, 用 $x+1$ 去除$(x^2+1)(x^2+3)$, 得余式 8. 因此 $\frac{1}{8}(x^2+1)(x^3+3)$被$(x^2+1)(x^2+3)$除尽, 而用 $x+1$ 除它余式是 1.

再求被$(x+1)(x^2+3)$除尽, 而用 x^2+1 去除余式是 1 的多项式. 用大衍求一术来求$(x+1)(x^2+3)=x^3+x^2+3x+3$和 x^2+1 的最高公因式. 列出计算表格:

k	$q_k(x)$	$r_k(x)$	$c_k(x)$	$d_k(x)$
-1		x^3+x^2+3x+3	1	0
0		x^2+1	0	1
1	$x+1$	$2x+2$	1	$x+1$
2	$\frac{1}{2}x-\frac{1}{2}$	2	$\frac{1}{2}x-\frac{1}{2}$	$\frac{1}{2}x^2+\frac{1}{2}$
3	$x+1$	0		

因此$(x^3+x^2+3x+3, x^2+1)=1$，而

$$2=\frac{1}{2}(-x+1)(x^3+x^2+3x+3)+\frac{1}{2}(x^2+1)(x^2+1),$$

于是

$$1=\frac{1}{4}(-x+1)\cdot(x^3+x^2+3x+3)+\frac{1}{4}(x^2+1)^2.$$

那么 $\frac{1}{4}(-x+1)(x^3+x^2+3x+3)$被$(x+1)(x^2+3)$除尽，而用 x^2+1 去除余式是 1.

再求被$(x+1)(x^2+1)$除尽，而用x^2+3去除余式是 1 的多项式. 用大衍求一术来求做，可得

$$1=\frac{1}{8}(x-1)\cdot(x^3+x^2+x+1)-\frac{1}{8}(x^2-3)\cdot(x^2+3).$$

那么$\frac{1}{8}(x-1)\cdot(x^3+x^2+x+1)$被$(x+1)(x^2+1)$除尽，而用 x^2+3 去除余式是 1.

于是我们求得了三个关键多项式

$$\frac{1}{8}(x^2+1)(x^2+3),\quad \frac{1}{4}(-x+1)(x^3+x^2+3x+3),$$

$$\frac{1}{8}(x-1)(x^3+x^2+x+1).$$

因此

$$2\cdot\frac{1}{8}(x^2+1)(x^2+3)+(x+1)\cdot\frac{1}{4}(-x+1)\cdot$$

$$(x^3+x^2+3x+3)+2x\cdot\frac{1}{8}(x-1)(x^3+x^2+x+1)$$

$$=-\frac{1}{2}x^3+\frac{1}{2}x^2+\frac{1}{2}x+\frac{3}{2},$$

就是要求的多项式.

例题 3. 设(a_1, b_1), (a_2, b_2), …, (a_r, b_r)是平面上的r个点，求一个多项式$f(x)$，有性质$f(a_i)=b_i$, $i=1, 2, \cdots r$.

根据余式定理，这就是说要求一个多项式，用$x-a_i$去除它，余式是b_i, $i=1, 2, \cdots, r$. 因此可以用孙子定理来求解.

先求关键多项式. 即求一多项式，它是$M_i(x)=(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_r)$的倍式，而用$x-a_i$去除它余式是1. 根据余式定理，用$x-a_i$去除$M_i(x)$，余式是$(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_r)$. 因此

$$l_i(x)=\frac{(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_r)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_r)}$$

就是$M_i(x)$的倍式，而用$x-a_i$去除它余式是1. 于是

$$f(x)=b_1\frac{(x-a_2)(x-a_3)\cdots(x-a_r)}{(a_1-a_2)(a_1-a_3)\cdots(a_1-a_r)}$$

$$+b_2\frac{(x-a_1)(x-a_3)\cdots(x-a_r)}{(a_2-a_1)(a_2-a_3)\cdots(a_2-a_r)}$$

$$+\cdots+b_i\frac{(x-a_1)\cdots(x-a_{i-1})(x-a_{i-1})\cdots(x-a_r)}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_r)}$$

$$+\cdots+b_r\frac{(x-a_1)(x-a_2)\cdots(x-a_{r-1})}{(a_r-a_1)(a_r-a_2)\cdots(a_r-a_{r-1})} \tag{5}$$

就是用 $x-a_i$ 去除余式是 b_i $(i=1,2,\cdots r)$ 的多项式. $f(x)$ 通常叫做Lagrange 插值多项式，而关键多项式 $l_i(x)$ 通常叫做基插值多项式.

Lagrange 插值多项式是计算数学中一个十分基本的公式.要验证(5)式满足问题的要求是很容易的，但要独立写出(5)式却颇费思索. 由上面说明却显示它不过是孙子定理的一个简单应用. 读者还可以由孙子定理中的唯一性知道 $f(x)$ 是满足问题要求的最低次多项式.

习题 6. 求一个二次多项式 $f(x)$，它有性质 $f(1)=0$, $f(-1)=-3$, $f(2)=4$.

7. 孙子定理对近代数学的影响

孙子定理是我国古代在数学上的重大贡献. 国外学者称它为“中国剩余定理”. 它对近代数学的发展很有影响, 孕育了近代数学的一些思想. 除了上节提到的 Lagrange 插值多项式外, 我们再举两个例子.

(一) 对近代环论的影响

再回到“物不知其数”这个问题. “术曰”中 70, 21, 15 这三个关键数有以下性质:

$70^2 \equiv 70 \pmod{105}$, $21^2 \equiv 21 \pmod{105}$,

$15^2 \equiv 15 \pmod{105}$, $70 \cdot 21 \equiv 0 \pmod{105}$,

$70 \cdot 15 \equiv 0 \pmod{105}$, $21 \cdot 15 \equiv 0 \pmod{105}$,

$1 \equiv 70 + 21 + 15 \pmod{105}$.

用近代环论的语言来说, 70, 21 和 15 是环 $\mathbf{Z}/105\mathbf{Z}$ 中的三个两两正交的幂等元, 而它们的和是环 $\mathbf{Z}/105\mathbf{Z}$ 的单位元 1. 在近代环论中, 将环的单位元分解成有限个两两正交的幂等元之和是研究环的结构的基本工具.

设 $m_1, m_2, \cdots, m_r$ 是 r 个两两互素的正整数. 令 $m = m_1 m_2 \cdots m_r$. 设 x 是一个整数, 用 $x \bmod m$ 表示 x 所属的 mod m 的同余类, 它是环 $\mathbf{Z}/m\mathbf{Z}$ 的元素, 同样 $x \bmod m_i$ 表示 x 所属的 mod m_i 的同余类, 它是环 $\mathbf{Z}/m_i\mathbf{Z}$ 的元素. 用

$$\mathbf{Z}/m_1\mathbf{Z} \oplus \mathbf{Z}/m_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/m_r\mathbf{Z}$$

表示环 $\mathbf{Z}/m_1\mathbf{Z}$, 环 $\mathbf{Z}/m_2\mathbf{Z}$, $\cdots$, 环 $\mathbf{Z}/m_r\mathbf{Z}$ 的直和. 建立映射

$$\psi: \mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/m_1\mathbf{Z} \oplus \mathbf{Z}/m_2\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/m_r\mathbf{Z}$$
$$x \bmod m \mapsto (x \bmod m_1, x \bmod m_2, \cdots, x \bmod m_r)$$

那么 ψ 是映上的，就相当于对任意 r 个整数 $a_1, a_2, \cdots, a_r$，同余式组

$$x \equiv a_i \pmod{m_i}$$

有解，即孙子定理中解的存在性部分;而 ψ 是单的,就相当于孙子定理中解的唯一性部分.因此孙子定理就等于说环 $\mathbf{Z}/m\mathbf{Z}$ 分成了环 $\mathbf{Z}/m_1\mathbf{Z}$, 环 $\mathbf{Z}/m_2\mathbf{Z}$, $\cdots$,环 $\mathbf{Z}/m_r\mathbf{Z}$ 的直和. 因此也可以说环的直和分解这一概念与孙子定理密切相关. 而孙子定理证明中找 r 个关键数实际上就是找 $\mathbf{Z}/m\mathbf{Z}$ 的 r 个两两正交的幂等元，它们在 ψ 之下分别映到 $\mathbf{Z}/m_1\mathbf{Z}$, $\mathbf{Z}/m_2\mathbf{Z}$, $\cdots$, $\mathbf{Z}/m_r\mathbf{Z}$ 的单位元，而它们的和正好是 $\mathbf{Z}/m\mathbf{Z}$ 的单位元.

孙子定理和近代环论的这些联系是十分有启发的.

(二) 对近代赋值论的影响

设 p 是个素数. 再设 m 是个整数. 如果 $m \neq 0$, $p^n \mid m$, 而 $p^{n+1} \nmid m$, 就规定 $|m|_p = p^{-n}$. 如果 $m=0$, 就规定 $|0|_p = 0$. 这是一种新的"绝对值"，它有着通常绝对值所具有的一些性质:

1) $|m|_p \geqslant 0$; $|m|_p = 0$ 当且仅当 $m=0$.

2) $|m_1 m_2|_p = |m_1|_p \cdot |m_2|_p$.

3) $|m_1 + m_2|_p \leqslant |m_1|_p + |m_2|_p$

它还有比3)更强的性质:

3′) $|m_1 + m_2|_p \leqslant \mathrm{Max}(|m_1|_p, |m_2|_p)$.

这种"绝对值" $|\ \ |_p$ 称为 p—adic 赋值. 值得注意的是，p 在 m 中出现的幂次愈高，$|m|_p$ 就愈小. 从孙子定理可以推出

逼近定理 设 $p_1, p_2, \cdots, p_r$ 是 r 个两两相异的素数，$a_1, a_2, \cdots, a_r$ 是 r 个整数. 任给 $\varepsilon > 0$, 总有一个整数 x 使

$$|x-a_i|_{p_i}<\varepsilon,\quad i=1,2,\cdots,r.$$

证明 选正整数 $e_1,e_2,\cdots,e_r$ 使 $p^{-e_i}<\varepsilon$，$i=1,2,\cdots,r$. 根据孙子定理，有整数 x 使

$$x\equiv a_i \pmod{p_i^{e_i}},\quad i=1,2,\cdots,r.$$

于是 $p_i^{e_i}\mid x-a_i$，因此 $|x-a_i|_{p_i}\leqslant p_i^{-e_i}<\varepsilon$，$i=1,2,\cdots,r$.

逼近定理是近代赋值论的基本工具，它的思想也来源于孙子定理.

8. “大衍求一术”和连分数

上一节，我们讲了孙子定理对近代数学的影响. “大衍求一术”与近代数学也有关系，这里我们介绍它与连分数理论的密切关系.

设 q_1 是整数，$q_2, q_3, \cdots, q_N$ 是正整数. 形如

$$q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{q_4+\ddots+\cfrac{1}{q_N}}}} \tag{1}$$

的繁分数叫做有限连分数. 显然有限连分数都是有理数，例如

$$1+\cfrac{1}{2+\cfrac{1}{3}}=1+\cfrac{1}{\cfrac{7}{3}}=1+\frac{3}{7}=\frac{10}{7},$$

$$3+\cfrac{1}{7+\cfrac{1}{15+\cfrac{1}{1}}}=3+\cfrac{1}{7+\cfrac{1}{16}}$$

$$=3+\cfrac{1}{\cfrac{113}{16}}=3+\frac{16}{113}=\frac{355}{113}.$$

反过来，可以把任一有理数表成有限连分数. 设 $\frac{a}{b}$ 是个有理数，这里 a 是整数而 b 是正整数. 令 $r_{-1}=a$，$r_0=b$. 对 r_{-1} 和 r_0 进行辗转相除. 各次除法的商依序记作 $q_1, q_2, \cdots$，而余

数依序记作 $r_1, r_2, \cdots$. 我们有

$$r_{k-2}=q_k r_{k-1}+r_k,\quad 0<r_k<r_{k-1},\quad k=1,2,3,\cdots. \tag{2}$$

设 n 使 $r_n \mid r_{n-1}$，这时 $r_{n-1}=q_{n+1} r_n$，$r_{n+1}=0$，即(2)式中的 k 终止于 n，而当 $k=n+1$ 时有

$$r_{n-1}=q_{n+1} r_n,\qquad r_{n+1}=0. \tag{3}$$

显然 $q_2, q_3, \cdots, q_{n+1}$ 都是正整数，而 $q_{n+1}>1$. 用 r_{k-1} 去除(2)式就得到

$$\frac{r_{k-2}}{r_{k-1}}=q_k+\frac{1}{\frac{r_{k-1}}{r_k}},\quad \frac{r_{k-1}}{r_k}>1,\quad k=1,2,\cdots,n \tag{4}$$

再用 r_n 去除(3)式就得到

$$\frac{r_{n-1}}{r_n}=q_{n+1},\qquad q_{n+1}>1. \tag{5}$$

利用(4)式和(5)式就可以把 $\frac{a}{b}$ 表成有限连分数

$$\frac{a}{b}=\frac{r_{-1}}{r_0}=q_1+\frac{1}{\frac{r_0}{r_1}}=q_1+\cfrac{1}{q_2+\cfrac{1}{\frac{r_1}{r_2}}}$$

$$=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\cfrac{1}{\frac{r_2}{r_3}}}}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+\ddots+\cfrac{1}{q_{n+1}}}} \tag{6}$$

其中 q_1 是整数，$q_2, q_3, \cdots, q_{n+1}$ 都是正整数，而 $q_{n+1}>1$.

上面介绍的把有理数 $\frac{a}{b}$ 表成有限连分数的算法实际上就是

辗转相除法.

立即发生把有理数表成有限连分数的表法是否唯一的问题. 显然有

$$7\frac{1}{2}=7+\frac{1}{2}=7+\frac{1}{1+\frac{1}{1}}.$$

因此表法不唯一，但是如果在有限连分数(1)中，当 $N>1$ 时限定最后一个整数 $q_N>1$，那么把一个给定的有理数 $\frac{a}{b}$ 表成有限连分数时表法是唯一的. 实际上，用符号 $[x]$ 表示不超过实数 x 的最大整数；例如

$$[7]=7,\quad [101\frac{1}{2}]=101,\quad [4.72]=4$$

$$[-5]=-5,\quad [-2.3]=-3,$$

等等. 那么由(6)式容易看出

$$q_1=[\frac{a}{b}],\ q_2=\left[\frac{1}{\frac{a}{b}-q_1}\right],\ q_3=\left[\frac{1}{\frac{1}{\frac{a}{b}-q_1}-q_2}\right],\cdots$$

等等. 因此 q_1，q_2，$\cdots$，q_{n+1} 都由 $\frac{a}{b}$ 唯一确定. 表面上，这又给出了将 $\frac{a}{b}$ 表成有限连分数的一个算法，但这实际上仍是辗转相除法，只是写法不同而已.

习题 1 把 $\frac{333}{106}$ 表成有限连分数.

习题 2 把 $\frac{6188}{4709}$ 表成有限连分数.

由于有限连分数的记号(1)太占篇幅，今后我们把(1)简记作 $[q_1, q_2, \cdots, q_N]$. 我们再放宽 N 必需是正整数的限制. 当 $N=\infty$ 时，$[q_1, q_2, q_3, \cdots]$ 叫做无限连分数(自然仍假定 q_1 是整数，$q_2, q_3, \cdots$ 都是正整数)，把它看作有限连分数序列

$$[q_1], [q_1, q_2], [q_1, q_2, q_3], \cdots$$

的极限；这个极限一定存在，将在下面证明.

暂时把 $q_1, q_2, q_3, \cdots, q_N$ 都看作无关未定元. 由计算易得

$$[q_1]=\frac{q_1}{1}, \quad [q_1, q_2]=\frac{q_2q_1+1}{q_2},$$

$$[q_1, q_2, q_3]=\frac{q_3q_2q_1+q_3+q_1}{q_3q_2+1},$$

等等. 通常写

$$[q_1, q_2, \cdots, q_k]=\frac{P_k}{Q_k} \qquad 1\leqslant k\leqslant N, \tag{7}$$

其中 P_k 和 Q_k 都是 $q_1, q_2, \cdots, q_k$ 的多项式，它们对每一个 q_i 都是一次的，其中分母 Q_k 与 q_1 无关. $\frac{P_k}{Q_k}$ 叫做 $[q_1, q_2, \cdots, q_N]$ 的第 k 个渐近分数. 置初值

$$P_{-1}=0, \quad P_0=1; \qquad Q_{-1}=1, \quad Q_0=0, \tag{8}$$

用归纳法可以证明

$$\begin{aligned} P_k&=q_kP_{k-1}+P_{k-2}\\ Q_k&=q_kQ_{k-1}+Q_{k-2} \end{aligned} \qquad k=1, 2, \cdots, N \tag{9}$$

实际上，当 $k=1$ 时，(9)式可直接从计算得证. 设 $1\leqslant k<N$，并假定

$$[q_1, q_2, \cdots, q_k] = \frac{P_k}{Q_k} = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}}.$$

其中 P_{k-1}, Q_{k-1}, P_{k-2}, Q_{k-2} 只与 $q_1, q_2, \cdots, q_{k-1}$ 有关. 那么由归纳法假设有

$$\frac{P_{k+1}}{Q_{k+1}} = [q_1, q_2, \cdots, q_k, q_{k+1}] = [q_1, q_2, \cdots, q_{k-1}, q_k + \frac{1}{q_{k+1}}]$$

$$= \frac{(q_k + \frac{1}{q_{k+1}})P_{k-1} + P_{k-2}}{(q_k + \frac{1}{q_{k+1}})Q_{k-1} + Q_{k-2}} = \frac{q_{k+1}(q_k P_{k-1} + P_{k-2}) + P_{k-1}}{q_{k+1}(q_k Q_{k-1} + Q_{k-2}) + Q_{k-1}}$$

$$= \frac{q_{k+1} P_k + P_{k-1}}{q_{k+1} Q_k + Q_{k-1}}.$$

这就证明了(9)式.

现在再把 q_1 看作整数, $q_2, q_3, \cdots, q_N$ 看作正整数. 那么 P_k 和 Q_k ($k = -1, 0, 1, 2, \cdots$)就是由(8)式和(9)式所定义的两个整数序列, 而(7)式仍成立. 非常有趣的是, 序列 P_k ($k = -1, 0, 1, 2, \cdots$)和"大衍求一术"中的序列 d_k ($k = -1, 0, 1, 2, \cdots$)有相同的初值和递推关系式(比较§5中的(3)式和本节(9)式中的第一行的式子), 而序列 Q_k ($k = -1, 0, 1, 2, \cdots$)和"大衍求一术"中的序列 c_k ($k = -1, 0, 1, 2, \cdots$)有相同的初值和递推关系式(比较§5中的(2)式和本节(9)式中第二行的式子). 因此

$$\begin{aligned} P_k &= d_k \\ Q_k &= c_k \end{aligned} \quad (k = -1, 0, 1, 2, \cdots),$$

这就是说"大衍求一术"中出现的 c_k 和 d_k 的商 $\frac{d_k}{c_k}$ 恰是有

理数 $\frac{a}{b}$ 的有限连分数表示(6)的第 k 个渐近分数($k=1,2,\cdots,n+1$).值得指出的是,秦九韶是公元十三世纪的我国数学家,而连分数理论中渐近分数 $\frac{P_k}{Q_k}$ 的递推关系式(9)最早出现在公元十七世纪英国数学家 John Wallis 的著作中(见他的 *Opera Mathematica*, Ⅰ, 1695).

为了讨论无限连分数 $[q_1, q_2, q_3, \cdots]$ 还需要 P_k 和 Q_k 所适合的一些关系式,我们把它们编成下面的习题:

习题 3 用归纳法证明

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k, k=0,1,2,\cdots \qquad (10)$$

由此导出 $\frac{P_k}{Q_k}$ 是既约分数(即 $(P_k, Q_k)=1$ 的分数),且

$$\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{(-1)^k}{Q_k Q_{k-1}}, k=0,1,2,\cdots. \qquad (11)$$

我们在这里顺便指出,利用(10)式可以重新导出§5中的基本公式(4)式.实际上,把 $\frac{a}{b}$ 表成有限连分数(6),并假定 $\frac{P_k}{Q_k}$ 是 $\frac{a}{b}$ 的有限连分数表示(6)的第 k 个渐近分数($k=1,2,\cdots,n+1$). 这时 $(a,b)=r_n$. 于是 $(\frac{a}{r_n}, \frac{b}{r_n})=1$. 由

$$\frac{a}{b} = \frac{a/r_n}{b/r_n} = [q_1, q_2, \cdots, q_{n+1}] = \frac{P_{n+1}}{Q_{n+1}},$$

推出 $P_{n+1}=a/r_n$, $Q_{n+1}=b/r_n$. 在(10)式中取 $k=n+1$ 就有

$$P_{n+1}Q_n - P_n Q_{n+1} = (-1)^{n+1}.$$

又因为 $Q_n=c_n$, $P_n=d_n$, 因此有

$$r_n = (-1)^{n-1} c_n a + (-1)^n d_n b,$$

这就是 §5 中的(4)式.

习题 4. 利用(9)式和(10)式推出

$$P_k Q_{k-2} - P_{k-2} Q_k = (-1)^{k-1} q_k, \quad k = 1, 2, \cdots \tag{12}$$

即

$$\frac{P_k}{Q_k} - \frac{P_{k-2}}{Q_{k-2}} = \frac{(-1)^{k-1} q_k}{Q_k Q_{k-2}}, \quad k = 1, 2, \cdots \tag{13}$$

习题 5. 证明:

(i) 当 $k>1$ 时, $Q_k > Q_{k-1} + 1$ 以及 $Q_k > k$.

(ii) $\frac{P_{2k+1}}{Q_{2k+1}} > \frac{P_{2k-1}}{Q_{2k-1}}$, $\frac{P_{2k+2}}{Q_{2k+2}} < \frac{P_{2k}}{Q_{2k}}$, $k = 1, 2, \cdots$

现在利用这几个习题来证明 $\lim\limits_{k\to\infty} [q_1, q_2, \cdots, q_k]$ 一定存在. 我们已经引进了记号 $[q_1, q_2, \cdots, q_k] = \frac{P_k}{Q_k}$. 由习题 5 (ii) 知, 序列 $\frac{P_{2k-1}}{Q_{2k-1}}$, $k = 1, 2, \cdots$ 是一个单调递增序列

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \frac{P_5}{Q_5} < \cdots,$$

而序列 $\frac{P_{2k}}{Q_{2k}}$, $k = 1, 2, \cdots$ 是一个单调递减序列

$$\frac{P_2}{Q_2} > \frac{P_4}{Q_4} > \frac{P_6}{Q_6} > \cdots.$$

由习题 3 (11)式和习题 5 (i), 有

$$\frac{P_2}{Q_2} > \frac{P_{2k}}{Q_{2k}} > \frac{P_{2k-1}}{Q_{2k-1}} > \frac{P_1}{Q_1}.$$

因此 $\lim\limits_{k\to\infty}\dfrac{P_{2k-1}}{Q_{2k-1}}$ 存在，$\lim\limits_{k\to\infty}\dfrac{P_{2k}}{Q_{2k}}$ 也存在. 再次利用习题 3 (11)式和习题 5 (i)可推出，当 $k\to\infty$ 时

$$\left|\frac{P_{2k}}{Q_{2k}}-\frac{P_{2k-1}}{Q_{2k-1}}\right|=\frac{1}{Q_{2k}Q_{2k-1}}\leqslant\frac{1}{2k(2k-1)}\to 0.$$

因此

$$\lim_{k\to\infty}\frac{P_{2k-1}}{Q_{2k-1}}=\lim_{k\to\infty}\frac{P_{2k}}{Q_{2k}}.$$

这就证明了 $\lim\limits_{k\to\infty}[q_1,q_2,\cdots,q_k]$ 一定存在；我们把这个极限记作 $[q_1,q_2,q_3,\cdots]$，不难证明，它一定是一个无理数.

习题 6. 证明无限连分数 $[q_1,q_2,q_3,\cdots]$ 一定是无理数.

反过来，我们还可以证明无理数一定可以表成无限连分数. 设 α 是一个实数. 取 $q_1=[\alpha]$. 命 $\alpha_2=\dfrac{1}{\alpha-q_1}$，取 $q_2=[\alpha_2]$. 再命 $\alpha_3=\dfrac{1}{\alpha_2-q_2}$，取 $q_3=[\alpha_3]$，…，如此继续下去，命 $\alpha_k=\dfrac{1}{\alpha_{k-1}-q_{k-1}}$，取 $q_k=[\alpha_k]$，等等. 显然，如果这个算法经有限步停止(即有一个正整数 N 使得 α_N 是正整数，这时 $q_N=[\alpha_N]=\alpha_N$，这个算法就停止)，那么 α 一定是有理数. 因此当 α 是无理数时，这个算法就一直进行下去不能停止，这样就得到一个无限连分数 $[q_1,q_2,q_3,\cdots]$，而且 $[q_1,q_2,q_3,\cdots]=\alpha$.

习题 7 证明当 α 是无理数时，用以上算法所得到的无限连分数 $[q_1,q_2,q_3,\cdots]$ 确实等于 α. (提示：形式地记 $\alpha=[q_1,q_2,\cdots,q_k,\alpha_{k+1}]$，并定义 $P'_{k+1}=\alpha_{k+1}P_k+P_{k-1}$，$Q'_{k+1}=\alpha_{k+1}Q_k$

$+Q_{k-1}$，那么 $\alpha=\dfrac{P'_{k+1}}{Q'_{k+1}}$．仿照习题 3 证明 $P'_{k+1}Q_k-P_kQ'_{k+1}=(-1)^{k+1}$，再仿照习题 5 (i)证明 $Q'_{k+1}>Q_k+1$，然后再估算 $\left|\alpha-\dfrac{P_k}{Q_k}\right|$．）

同样会发生把无理数表示成无限连分数的表示是否唯一的问题．答案是肯定的．即

习题 8．用无限连分数表示无理数的方法是唯一的．

这样一来，如果在有限连分数 (1)中当 $N>1$ 时限定最后一个整数 $q_N>1$，那么实数与连分数一一对应；有理数与有限连分数一一对应，而无理数与无限连分数一一对应．

有了无理数 α 的连分数表示，就可以用这个连分数的渐近分数 $\dfrac{P_k}{Q_k}$ 来逼近这个无理数．我们还可以用习题 3 (11)式来估计 $\dfrac{P_k}{Q_k}$ 逼近 α 的程度．我们有

$$\left|\frac{P_{k+1}}{Q_{k+1}}-\frac{P_k}{Q_k}\right|=\frac{1}{Q_kQ_{k+1}}\ .$$

因为 α 位于 $\dfrac{P_k}{Q_k}$ 和 $\dfrac{P_{k+1}}{Q_{k+1}}$ 之间．所以

$$\left|\alpha-\frac{P_k}{Q_k}\right|\leqslant\frac{1}{Q_kQ_{k+1}}<\frac{1}{Q_k^2}\ . \tag{14}$$

更进一步，$\dfrac{P_k}{Q_k}$ 还是 α 的最佳渐近分数，即在分母不大于 Q_k 的各分数中，$\dfrac{P_k}{Q_k}$ 与 α 最接近．我们举出华罗庚《数论导引》，272 页上的一个例题作为本书的结束．

例. 作 $\pi=[3, 7, 15, 1, 292, 1, 1, \cdots]$ 的渐近分数，得

$$\frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \frac{103993}{33102}, \frac{104348}{33215}, \cdots$$

$\frac{3}{1}$ 这个 π 的近似分数在我国古书上记载为“径一周三”，即直径等于 1 的圆的圆周长近似等于 3. $\frac{22}{7}$ 这个 π 的近似分数是古希腊 Archimedes (公元前 287— 212 年)首先得到的，后来我国何承天 (公元 370 — 447 年)又独立地得到. $\frac{355}{113}$ 这个 π 的近似分数是我国南北朝时代的数学家祖冲之 (公元 429 — 500 年)首先得到的，德国 Valentinus Otto 也于 1573 年得到. 但比祖冲之晚了一千一百多年. 祖冲之把 $\frac{22}{7}$ 叫做约率，把 $\frac{355}{113}$ 叫做密率. 有趣的是祖冲之的约率 $\frac{22}{7}$ 和密率 $\frac{355}{113}$ 都是最佳渐近分数，即分母不超过 7 的分数中没有比 $\frac{22}{7}$ 更接近 π 的数，而分母不超过 113 的分数中没有比 $\frac{355}{113}$ 更接近 π 的数.

由(14)式可知

$$\left|\pi-\frac{355}{113}\right|<\frac{1}{113\times 33102}<\frac{1}{10^6}.$$

因此 $\frac{355}{113}$ 准确到第六位小数，这与实际计算的结果 $\frac{355}{113}=3.1415929$ 相符合.