信息安全数学基础 第七次作业

BY 18340087 李晨曦

(1)

令

$$\begin{aligned} p_n &= \frac{a}{(a,b)} \\ q_n &= \frac{b}{(a,b)} \end{aligned}$$

那么我们有:

$$\begin{aligned} p_n q_{n-1} - q_n p_{n-1} &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - (a_n q_{n-1} + q_{n-2}) p_{n-1} \\ &= -(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}) \\ &= \ldots \\ &= (-1)^{n-1} \\ &= (-1)^{n+1} \end{aligned}$$

所以,

$$\frac{a}{(a,b)} q_{n-1} - \frac{b}{(a,b)} p_{n-1} = (-1)^{n+1}$$

故:

$$a q_{n-1} - b p_{n-1} = (-1)^{n+1} (a,b)$$

(2)

这个所谓的新方法是, 如果我们知道了p_{n-1}、q_{n-1}的值和n的值, 那么我们立刻就可以算出(a, b):

$$(a,b) = (a q_{n-1} - b p_{n-1}) (-1)^{n+1}$$

但是如何得到这些信息呢? 我们不得不算出$\frac{a}{b}$的有限简单连分数表示。

- 如果有了$\frac{a}{b}$的一个有限简单连分数表示$[a_0, a_1, \ldots a_n]$, 自然地就会有n的值了;
- 如果有了$\frac{a}{b}$的一个有限简单连分数表示$[a_0, a_1, \ldots a_n]$, 那么$[a_0, a_1, \ldots a_{n-1}]$也自然地得到了, 进而可以得到$p_{n-1}$和$q_{n-1}$的值。

对于不定方程$ax + by = c$, 我们可以通过这个方法得到一个特解:

$$\begin{aligned} a q_{n-1} - b p_{n-1} &= (-1)^{n+1} (a,b) \\ a (q_{n-1} c) + b(-p_{n-1} c) &= (-1)^{n+1} (a,b) c \\ a ((-1)^{n+1} q_{n-1} c) + b((-1)^{n+2} p_{n-1} c) &= (a,b) c \end{aligned}$$

如果有

$$\begin{array}{rcl}(a,b) & \mid & (-1)^{n+1}q_{n-1}c\\(a,b) & \mid & (-1)^{n+2}p_{n-1}c\end{array}$$

因为$(q_{n-1},p_{n-1})=1$， 实际上要使上面的两个式子成立当且仅当

$$(a,b)|c$$

那么， 一个特解为

$$\begin{array}{rcl}x_0 & = & \frac{q_{n-1}c}{(aq_{n-1}-bp_{n-1})}\\y_0 & = & -\frac{p_{n-1}c}{(aq_{n-1}-bp_{n-1})}\end{array}$$

(i)

首先我们求出$\frac{7696}{4144}$的连分数表示：

$$\frac{7696}{4144}=1+\frac{1}{1+\frac{1}{6}}$$

可知:

$$\begin{array}{rcl}n & = & 2\\q_{n-1} & = & 1\\p_{n-1} & = & 2\\(a,b) & = & (7696\times1-4144\times2)\times(-1)^3\\ & = & 592\end{array}$$

(ii)

首先我们求出$\frac{77}{63}$的有限简单连分数表示：

$$\frac{77}{63}=1+\frac{1}{4+\frac{1}{2}}$$

即$[1,4,2]$,
所以

$$\begin{array}{rcl}n & = & 2\\q_{n-1} & = & 4\\p_{n-1} & = & 5\end{array}$$

那么,

$$(a,b)=-77\times4+63\times5=7$$

我们有

$$7\nmid40$$

所以这个方程无解。

(3)

按照最简单的算法：

$$\frac{-97}{73}=-2+\frac{1}{1+\frac{1}{2+\frac{1}{24}}}$$

把这个数变为正数， 再次计算得到：

$$\frac{97}{73}=1+\frac{1}{3+\frac{1}{24}}$$

那么它的相反数为：

$$\frac{-97}{73}=-1+\frac{1}{-3+\frac{1}{-24}}$$

这样一来就得到了两种有限简单连分数。

同理，

$$\frac{5391}{3976}=1+\frac{1}{2+\frac{1}{4+\frac{1}{3+\frac{1}{1+\frac{1}{5+\frac{1}{2+\frac{1}{1+\frac{1}{3}}}}}}}}$$

把它变为负数， 再计算其相反数得到：

$$\frac{5391}{3976}=[2,-1,-1,-1,-4,-3,-1,-5,-2,-1,-3]$$