二次域及有理逼近相关问题

引言

二次域是初等数论中篇幅很大的一部分，主要集中在不定方程篇章。

这里采用了较高一点的观点统一了这些简单的二次不定方程。希望读者在阅读之前，已经提前了解了简单的代数学。

绪论

定义

首项系数为1的整系数二次多项式$x^2+px+q=0$的零点是：

$$\frac{-p±\sqrt{p^2-4q}}{2}$$

称为“含有根号d的二次整数”，全体记作二次整环$Z(\sqrt{d})$对于加减乘封闭。不同的d对应于不同的整环。普通的整数环是每一个二次整环的理想。

第一种情况：对于所有的d$a+b\sqrt{d}$一定是二次整数。

第二种情况：当d模4余1a与b是奇数的时候$\frac{a+b\sqrt{d}}{2}$也是二次整数。因为这种情况也是首系数为1的整系数多项式的零点：

$$x^2-ax+\frac{a^2-db^2}{4}=0$$

奇数的一半称半整数。两个半整数配上除以4余1的d开二次根号，也是二次整数。

以上的d全部可正可负。当d为正时就是普通意义的二次根号，当d为负的时候可以理解成对绝对值开根号，并乘以虚数单位i

二次整数有两个线性无关的分量，因此二次整数是二维的。

同类二次整数的比构成二次有理数，全体构成二次域$Q(\sqrt{d})$

若d为正，集合中所有数均为实数，称为实二次整环或者实二次域。若d为负，集合中除了一般的有理数以外全部不是实数，称为虚二次整环或虚二次域。

范数与单位数

对于同一个整系数二次方程，有两个根。如果它们不是一般的有理数，那么它们在形式上只在二次根号前相差一个正负号。

如果两个二次有理数只在二次根号之前相差正负号，称它们互为**共轭**关系。因为一般的有理数在二次根号前面的系数是0，因此一般的有理数与它自身为共轭关系。

显然，在虚二次域中，某数的共轭的概念，与复数共轭的概念一致。但是在实二次域中这两个概念不一致。

在二次域中，由加减乘除（非0）四则运算产生的等式，无法区分共轭关系。也就是说，在等式中将每一个数换成它的共轭数，即将每一个二次根号的符号改变，等式仍然成立。

二次有理数与它的共轭的和称为**迹**。某数的迹就是它的有理数部分的2倍，形式简单，因此很少研究迹。

二次有理数与它的共轭的积称为**范数**

$$N(a+b\sqrt{d})=a^2-db^2$$

显然，在虚二次域中，范数的概念，与复数的模的平方的概念一致。但是在实二次域中这两个概念不一致。由于d不含平方因子，不可能是平方数，因此只有0的范数是0。

范数具有保持乘法和除法（非0）的良好性质。

$$N(a_1+b_1\sqrt{d})N(a_2+b_2\sqrt{d})=N((a_1+b_1\sqrt{d})(a_2+b_2\sqrt{d}))$$

$$\frac{N(a_1+b_1\sqrt{d})}{N(a_2+b_2\sqrt{d})}=N\left(\frac{a_1+b_1\sqrt{d}}{a_2+b_2\sqrt{d}}\right)$$

一个二次有理数与它的共轭相乘为这个数的范数，因此它的倒数就是它的共轭与范数之比。

$$a+b\sqrt{d}=\frac{a-b\sqrt{d}}{N(a+b\sqrt{d})}$$

如果一个二次整数的倒数还是二次整数，称这个二次整数为**单位数**。二次整数是单位数的充要条件是它的范数为1或-1。

单位数对于乘法封闭，构成单位群。有一个核心位置的定理（证明极难）：

狄利克雷单位定理：数域的单位群是有限生成阿贝尔群。

狄利克雷单位定理表明：单位群维数有限，存在一组基。所有的单位数可以由基的乘积表示。这组基（不含1和-1）称为**基本单位数**

虚二次域

简介

在虚二次域中，仅当d为-1和-3的时候，存在除了1和-1以外的单位数。当d为负数且不为-1或-3的时候，单位数只有1和-1。

当d为-1的时候，单位数有4个1-1i-i当d为-3的时候，单位数有6个1-1$\frac{1+\sqrt{3}i}{2}$$\frac{1-\sqrt{3}i}{2}$$\frac{-1+\sqrt{3}i}{2}$$\frac{-1-\sqrt{3}i}{2}$

在虚二次域中，仅当d为-1和-3时，存在基本单位数i和$\frac{1+\sqrt{3}i}{2}$其他情况不存在1和-1以外的其他单位数，也就不存在基本单位数。

因此，两个整环$Z(i)$和$Z(\sqrt{3}i)$是特殊的整环，称为高斯整环和艾森斯坦整环。它们直观上分别构成复平面上正方形点阵和正六边形点阵（正三角形格点），研究虚二次域的时候最经常用到这两个整环。

虚二次域中对范数的研究可以转化为**椭圆上整点问题**，有名的“圆上整点问题”可以转化为对d为-1的虚二次域的研究。

高斯整数与圆上整点问题

占坑

勾股方程

占坑

艾森斯坦整数

占坑

实二次域

简介

对于每一个实二次域，单位数有无限个。

对于实二次域，基（不含1和-1）只有一个。因此有如下结论：取ε为正的单位数中除了1以外两分量（任一）最小的，那么全体单位数可以表示成：

$$±\varepsilon ^n \quad n\in Z$$

研究实二次域的结构，首先就要求解基本单位数，因此就有了Pell方程（佩尔方程）。佩尔方程的解法已经被研究透彻，可以采用连分数算法。

连分数

连分数是一种记号。例如，长为4的连分数：

$$<a_0,a_1,a_2,a_3>=a_0+\frac{1}{a_1+\frac{1}{a_2+\frac{1}{a_3}}}$$

只是为了形式上简洁，才记成等号左边的样子。这里的四个变元可以任意取值。

连分数中，从前面一直到第k个变元构成的连分数，是它的**第k渐进分数**。连分数各变元的下标从0开始。

渐进分数有递推关系：

$$\frac{p_n}{q_n}=\frac{x_np_{n-1}+p_{n-2}}{x_nq_{n-1}+q_{n-2}}$$

这个式子和下面的Farey数列的递推关系很像。

上面的例子是有限连分数。如果分式无限地写下去，有无限个变元，就得到无限连分数。无限连分数收敛等价于渐进分数收敛。

有定理：

无限连分数，如果各变元均大于等于1，那么一定收敛。

因为只要各变元为正，无限连分数的偶渐进分数单调递增（都比它小），奇渐进分数单调递减（都比它大）。而在均大于等于1时，相邻（奇偶间）两个渐进分数之间距离可以给出估计式，趋于0，因此收敛。

显然可以看到，连分数关于下标为偶数的变元单调递增，关于下标为奇数的变元单调递减。这无论它有限或无限都成立。

还有一个事实，对于有限连分数，全体结尾为1的有限连分数和全体结尾不为1的有限连分数一一对应，即同一个连分数有两种表示：

$$<a_0,a_1,a_2,a_3>=<a_0,a_1,a_2,a_3-1,1>$$

简单连分数：连分数从第1项开始全都是正整数。如果有限，要求最后一项不为1。（第0项可以任意）

简单连分数的值，一定大于偶数的渐进分数，一定小于奇数的渐进分数。无限简单连分数一定收敛。

仿照一般分数的概念，第0项是0的连分数称为“ 真分数 ”。显然如果这之后的所有变元都大于等于1，那么得到的真分数一定落在0到1之间。

如果“ 规定第0项是该数的取整 ”，那么全体实数都有“ 唯一的简单连分数表示 ”。其中：

如果两个无限简单连分数的值相等，必然逐项相等。

如果两个有限简单连分数的值相等，不仅要逐项相等，而且必然项数也相同。

无限简单连分数不能与有限简单连分数值相等。有理数与有限简单连分数具有一一对应关系，因此无限简单连分数全都是无理数。

如果要求0、1区间内某个数的简单连分数表示（第0项为0），只需：

第一步：取倒数，得到的数大于1。

第二步：取整，得到的数在0到1之间。这个数称为余数。

第三步：对余数重复上述操作。

这样就得到了相应的表示。

循环连分数

仿照循环小数的概念，如果在连分数后面形成了循环，则形成**循环连分数**。如果循环节从第0项开始，称为**纯循环连分数**，否则称为**混循环连分数**。例如纯循环连分数：

$$<a_0,a_1,a_2,a_3,a_0,a_1,a_2,a_3,...>=<\overline{a_0,a_1,a_2,a_3}>$$

混循环连分数:

$$<a_0,a_1,a_2,a_3,a_1,a_2,a_3,...>=<a_0,\overline{a_1,a_2,a_3}>$$

混循环连分数后面循环的部分，一般要找最早循环的部分，称为它的“ 纯循环部分 ”。循环节一般取最小正整数。

对二次有理数执行“ 无限简单连分数 ”计算，即取倒数、取整交替，得到的余数还是二次有理数。

这里考虑一类特殊形式的二次有理数。

设ξ是如下形式的二次有理数□d只需是正数：

$$\xi_k=\frac{1}{q_k}\left(c_k+\sqrt{d}\right)=<a_k,a_{k+1},a_{k+2},a_{k+3},...>\quad q_k|N(c_k-\sqrt{d})$$

称ξ_k为**第k余数**

只要让分母整除分子的范数，取倒数、取整的交替过程会变得简单很多。事实上如果这条件不成立，只要分子分母同时乘以分母的绝对值，并强行压入根号，条件就成立了。因此，任何二次有理数都能写成这形式。

如果这条件成立，那么每个余数都满足这条件。

根据上文的简单连分数算法：对余数取整可以得到a进而得到新的c

$$a_k=\frac{c_{k+1}+c_k}{q_k}$$

取整后得到的新的c为负数，且绝对值一定比根号d小，因此范数为负。取倒数，得到新的分母q，q总是正的。

$$q_k q_{k+1}=-N(c_{k+1}-\sqrt{d})$$

由于范数为负，取倒数之后根号d前面的符号不变，而c的符号由负变正（负数前面加负号变为正数）。

余数循环显然是循环连分数的循环条件。由于计算方法固定，只要余数重复必循环。

余数ξ里面，每个c都为负数，且绝对值一定比根号d小，因此c的个数有限。每个q都整除对应c构成二次整数的范数，因此q的个数有限。

余数有限必重复。因此**所有二次有理数都可以写成循环连分数**。反过来容易证明**循环连分数一定是二次有理数**

由于无限简单连分数写法唯一，因此就找到了二次有理数的一种唯一表示。

Stern-Brocot树

Stern-Borcot树从两个简单的分数开始：0和无穷。

$$\frac{0}{1}\quad\frac{1}{0}$$

每次我们在相邻的两个分数$\frac{a}{b}$，$\frac{c}{d}$中间插入一个分数$\frac{a+c}{b+d}$，这样就完成了一次迭代，得到下一个序列。

$$\frac{0}{1}\quad\frac{1}{1}\quad\frac{1}{0}$$

$$\frac{0}{1}\quad\frac{1}{2}\quad\frac{1}{1}\quad\frac{2}{1}\quad\frac{1}{0}$$

将每一层新加入的数写在上一层下面，最终形成树状结构：

每一个序列都是 Stern-Brocot 树的中序遍历。在每一层的序列中，真分数是单调递增的，并且序列中的分数都是最简分数。因此Stern-Borcot树可以当成一棵平衡树，建立和查询就向平衡树一样做就行了。

Farey数列

第k层Farey数列，是分母小于等于k的所有最简真分数按大小顺序排列形成的序列，即满足单调性。可以理解为上面的树的左半分支的变形。

$$\frac{0}{1}\quad\frac{1}{2}\quad\frac{1}{1}$$

$$\frac{0}{1}\quad\frac{1}{3}\quad\frac{1}{2}\quad\frac{2}{3}\quad\frac{1}{1}$$

$$\frac{0}{1}\quad\frac{1}{4}\quad\frac{1}{3}\quad\frac{1}{2}\quad\frac{2}{3}\quad\frac{3}{4}\quad\frac{1}{1}$$

$$\frac{0}{1}\quad\frac{1}{5}\quad\frac{1}{4}\quad\frac{1}{3}\quad\frac{2}{5}\quad\frac{1}{2}\quad\frac{3}{5}\quad\frac{2}{3}\quad\frac{3}{4}\quad\frac{4}{5}\quad\frac{1}{1}$$

区别在于，仅当满足分母条件，需要插入特定的分数的时候，才在这个位置插入这个特定的分数。由于第n层插入的均为分母为n的最简分数，第n层插入的分数总共有$\varphi(n)$个。

最佳有理逼近

讨论如何用有理数“最佳地”逼近无理数，不妨假设无理数落入0、1区间。

“最佳”一词的概念：选定的有理数必须保证，比它与无理数的距离更近的有理数，分母都比它大。不存在分母比它小的有理数，到给定无理数的距离更近。

最佳有理数：在法雷数列的某一行中，与给定无理数距离最近的那个有理数。

这个有理数可能在下面几行依旧与无理数“距离最近”，但一定有某一行，会找到一个新的有理数，与无理数距离更近。因此去重复后可以得到**最佳逼近有理数列**，分母严格递增，距离递减。

比无理数大的称为上逼近，否则为下逼近。由于无理数和有理数之间一定有有理数，最佳逼近有理数列必然为若干个上逼近，之后若干个下逼近，交替进行的形式。

有结论：

渐进分数必然为最佳逼近。偶项渐进分数全都是下逼近，奇项渐进分数全都是上逼近。渐进分数列是下上交错的逼近。

在最佳逼近有理数列中，渐进分数是下上关系改变之前的倒数第一个数。如果将最佳逼近有理数列都写成有限简单连分数，那么在渐进分数之后（下上关系改变之后），连分数长度加一。

例如，$<0,2,4,2>$是根号6减去2的一个渐进分数。那么它的渐进分数列是：

$$<0,2>=\frac{1}{2},<0,2,4>=\frac{4}{9},<0,2,4,2>=\frac{9}{20}...$$ 它的最佳逼近有理数列是
$$<0,1>=1,<0,2>=\frac{1}{2},<0,2,1>=\frac{1}{3},<0,2,2>=\frac{2}{5},<0,2,3>=\frac{3}{7},<0,2,4>=\frac{4}{9},<0,2,4,1>=\frac{5}{11},<0,2,4,2>=\frac{9}{20}...$$

从每个渐进分数（不包含）开始，到下一个渐进分数（包含）为止，同为上逼近，或同为下逼近。

在最佳逼近列中，每一个最佳分数是上一个最佳分数与再往前一个渐进分数的分子分母对应求和。

Dirichlet逼近定理

Dirichlet（狄利克雷）逼近定理是说，对于任意的一个无理数θ，均能找到无穷个有理数逼近它，满足不等式：

$$\left|\frac{p}{q}-\theta\right|\leqslant\frac{1}{q^2}$$

更强的结论是，在右边的分母上能放一个$\sqrt{5}$，这个$\sqrt{5}$是最优的，在无理数为黄金分割的时候取等。因此，在上式中的小于等于号事实上也可以是小于号。

更进一步的定理是Kronecker（克罗内克）的逼近定理。

如果θ为无理数，α为实数，则对任意正数ε, 存在整数n和整数m，使得:

$$\left|n\theta-m-\alpha\right|<\varepsilon$$

这两个定理都可以用抽屉原理来解决。事实上，历史上第一次正式提出抽屉原理，就是Dirichlet为了解决Pell方程而研究这个有理数逼近条件才正式提出来抽屉原理的。

当然，采用抽屉原理的证明可以发现，上文中提到的最佳逼近有理数列，每项满足定理中右边改成分母为一次式的不等式。

进一步有结论，渐进有理数列中，每一项均满足Dirichlet逼近定理的不等式。

我们用Dirichlet逼近定理来逼近二次根式$\sqrt{d}$，即有无穷个有理数（显然为正有理数）满足：

$$\left|\frac{x}{y}-\sqrt{d}\right|\leqslant\frac{1}{y^2}$$

于是，下面的范数就有：

$$\left|N(x+y\sqrt{d})\right|=|x-y\sqrt{d}||x+y\sqrt{d}|\leqslant\frac{1}{y}(\frac{1}{y}+2y\sqrt{d})\leqslant2\sqrt{d}+1$$

这是对范数拆出的两项进行估值。这也直观地说明只要有理数与根号d越接近，范数越小。

因此，范数较小的二次整数有无限个，进而采用一些手段，就可以推出范数为正负1的单位数存在，也存在无限个。

进而可以发现，对于所有$\sqrt{d}$的渐进分数，配上系数之后得到的二次整数的范数都落在非常小的区间。由于$\sqrt{d}$的渐进分数是余数循环的，只要其中出现使得范数为正负1的渐进分数，经过一个循环之后新的渐进分数凑成的二次整数也应当满足范数为正负1，即这个新渐进分数也是单位数。由于第-1个渐进分数规定为$\frac{1}{0}$对应的二次整数范数为1，那么只要计算每个循环节处前一个渐进分数即可。

根据上逼近与下逼近的结论，第奇数个渐进分数得到的范数为负，偶数个为正。即是否存在范数为负1的二次整数取决于循环连分数的循环节长度是否为奇数。

最后还有一个结论，每经过一个循环，相当于旧的二次整数乘上了一个单位数，得到新的二次整数。因此上面得到的单位数是基本单位数。

Pell方程

实二次域中，对范数的研究最终可以转化为如下形式的二元二次不定方程，称为佩尔方程：

$$x^2-dy^2=k$$

其中d和k是给定的整数，并且d是正数，要求x和y的整数解。显然x和y与符号无关，将x与y均为正的解，称为**正解**

和二次域略有区别的是，这里d并没有要求“不含平方因子”的限制，但是可以将d的平方因子并入y中，变为某种特殊类型的解。

佩尔方程也可以理解成**双曲线上整点问题**，考虑双曲线上有没有整点，有多少个整点。

佩尔方程等价于，在实二次域中，求范数为k的两分量均为整数的特殊形式二次整数。

$$N(x+y\sqrt{d})=k$$

只要这样的二次整数存在，佩尔方程就有解，并且不同类型的二次整数对应不同类型的解。

对于上面的单位数求解问题，可以化为以下的**四个佩尔方程**

$$x^2-dy^2=1$$

对应于范数为1的一种情况。

$$x^2-dy^2=-1$$

对应于范数为-1的一种情况。

$$x^2-dy^2=4$$

这里d除4余1，x和y的奇偶性必然相同。当x和y均为偶数时，两边同时除以4，方程与第一个方程等价。当x与y均为奇数时，对应于范数为1，并且x与y均为半整数的情况。

$$x^2-dy^2=-4$$

这里d除4余1，x和y的奇偶性必然相同。当x和y均为偶数时，两边同时除以4，方程与第二个方程等价。当x与y均为奇数时，对应于范数为-1，并且x与y均为半整数的情况。

因此在后两个方程中，更注重讨论x与y的奇数解。

类似实二次域的基本单位数结论，可以给出这四类佩尔方程的“基本解”的概念。

有结论：只要d不是完全平方数，方程

$$x^2-dy^2=1$$

必然有解。并且记$\rho_1=x+y\sqrt{d}$为最小的正解，于是所有解都可以用

$$\{±\rho^n | n\in Z\}$$

表示。

在d不含平方因子，并且ε的范数是1，并且ε不是半整数形式的时候，这里的ρ(1)就是对应的实二次域中基本单位数ε此时对应的-1和-4的方程均无解，4的方程有解，但是无奇数解。

方程

$$x^2-dy^2=-1$$

很多时候无解。有解的时候，记$\rho_{-1}=x+y\sqrt{d}$为最小的正解，于是所有解都可以用

$${±\rho^n | n\equiv 1 \quad \mod 2}$$

表示。

在d不含平方因子，并且ε的范数是-1，并且ε不是半整数形式的时候，这里的ρ(-1)就是对应的实二次域中基本单位数ε□并且ε的平方范数为1，ρ(-1)的平方是对应的ρ(1)□此时对应的4和-4的方程均有解，但是均无奇数解。

方程

$$x^2-dy^2=4$$

总是有解，但是很多时候无奇数解。有奇数解的时候，记$\rho_4=\frac{x+y\sqrt{d}}{2}$为最小的正解，于是所有奇数解都可以用

$$\{±\rho^n | n\equiv 1 ,2 \quad \mod 3\}$$

的分子表示。

在d不含平方因子，并且ε的范数是1，并且ε是半整数形式的时候，这里的ρ(4)就是对应的实二次域中基本单位数ε□此时对应的-1与-4的方程均无解。可以发现，ε的立方恰好分母为1，范数为1，因此ρ(4)的立方恰好是对应的ρ(1)□

方程

$$x^2-dy^2=-4$$

有解等价于对应的-1的方程有解，在此基础上，有奇数解等价于对应的4的方程有解。此时，记$\rho_{-4}=\frac{x+y\sqrt{d}}{2}$为最小的正解，于是所有奇数解都可以用

$$\{±\rho^n | n\equiv 1 ,5 \quad \mod 6\}$$

的分子表示。

在d不含平方因子，并且ε的范数是-1，并且ε是半整数形式的时候，这里的ρ(-4)就是对应的实二次域中基本单位数ε□可以发现，ε的立方恰好分母为1，范数为-1，因此ρ(-4)的立方恰好是对应的ρ(-1)□同样有，ρ(-4)的平方是对应的ρ(4)□ρ(-4)的六次方是对应的ρ(1)□

综上，以上所有情况可以简记为-4基本解的若干次乘方，构成6循环的序列：

-4□4□-1□4□-4□1□-4□4□-1□4□-4□1……

只有1的情况是一定有解的，仅当-1有解并且4有奇数解，二者同时成立的时候，-4才有奇数解。

当d含有平方因子的时候，1的方程仍旧一定有解。这时如果将根号d中的平方因子全部提出来，依旧能对应于一个二次域。由范数为1，可以得到结论：

这时1方程的基本解是对应二次域基本单位数的若干次方。

同样地，-1和4和-4的方程如果有解，基本解也是对应二次域基本单位数的若干次方。因此解的情况和对应二次域的情况有关。

对于一定有解的1的方程，任意一个基本解的范数都是1。因此有结论：一般的佩尔方程

$$x^2-dy^2=k$$

一旦有解就一定有无数个解，即这样的双曲线上一旦有整点就一定有无数个整点。这是因为，将范数为k的对应的二次整数乘以范数为1的基本解对应二次整数，得到依然二次整数范数依然为k□而范数为1的基本解有无限个，相乘得到的范数为k的基本解不同。

依靠同一个解，与不同的单位数相乘，得到的全体解，称为“一族解”。同一个方程解的族数，可以大于1，也可以为1，也可以无解为0。

上面的讨论表明：方程-1的族数，为0或1，4的奇数解情形族数，为2或0，-4的奇数解情形族数，也为2或0。