arXiv:2602.06538v1 [math.NT] 6 Feb 2026

范数欧几里得实二次域的除法算法——第一部分

FRANC.OIS MORAIN

Abstract. 我们为实二次域$\mathbb{Q}(\sqrt{m})$（其中 $m \in \{2,3,6,7,11,19\}$）给出一种欧几里得除法算法，其余数的范数取决于该域的第一欧几里得极小值。对于每种情况，我们用双曲线覆盖正方形 $[-1/2,1/2]\times[-1/2,1/2]$，并列出这些双曲线及其覆盖的区域。我们尽可能将证明形式化，并使用精确计算，以便能够复现这些证明。

1. Introduction

设 $\mathrm{K}/\mathbb{Q} = \mathrm{K}(\theta)$ 是一个次数为 d 的数域，其定义多项式为 $f(X)$，判别式为 D_K；$\mathrm{Norm}(x)$ 表示 $x \in \mathrm{K}$ 的范数；我们用 $\mathcal{O}_K$ 表示 K 的整数环。

$\xi \in \mathrm{K}$ 的欧几里得极小值为

$$m_{\mathbf{K}}(\xi) = \inf\{\mathrm{Norm}(\xi-\gamma), \gamma \in \mathcal{O}_K\}.$$

K 的欧几里得极小值为

$$M_1(\mathbf{K}) = \sup\{m_{\mathbf{K}}(\xi), \xi \in \mathbf{K}\}.$$

临界点（如果存在）ξ 满足 $m_{\mathbf{K}}(\xi) = M_1(\mathrm{K})$。参见 [5, 9]，了解理论结果以及计算次数较高的域的欧几里得极小值的高效算法。显然，$M_1(\mathrm{K}) < 1$（分别为 > 1）时，$\mathcal{O}_K$ 是范数欧几里得的（分别为非范数欧几里得的）。如果 $M_1(\mathrm{K}) = 1$，则情况取决于具体情形（例如，参见 [4]）。关于该问题的历史以及该领域成果的近乎完整列表（包括若干有关 Barnes 和 Swinnerton-Dyer 在这一主题上的工作的参考文献），请参阅这部代表作 [8]。

命题 1.1. $\mathcal{O}_K$ 是范数欧几里得的，当且仅当对每个 $\xi \in \mathrm{K}$，都存在$\gamma \in \mathcal{O}_K$ 使得

$$|\mathrm{Norm}(\xi-\gamma)| < 1. \tag{1}$$

我们来定义几类欧几里得除法算法：1-除法表示一种生成 γ 的算法，如式（1）所示。这种类型的算法并不能令人满意，例如，它无法为最大公因数提供有用的界。M-除法算法则对应于生成 γ，使得 $|\mathrm{Norm}(\xi-\gamma)| \le M$。例如，$M_1$-除法算法可确保最大公因数序列快速收敛。已知的 M_1-算法很少，因为欧几里得性的证明并不总能给出有用的算法，但某些分圆域是个例外 [15, 3, 7]（这与寻找高阶互反律的显式形式有关

Date: 2026年2月9日。LIX、法国国家科学研究中心、法国国家信息与自动化研究院、´巴黎综合理工学院、巴黎理工学院，法国帕莱索。

）。理论上，如果我们能找到一种显式算法来计算$m_K(x)$，就能得到一种最优的欧几里得除法算法。

本文旨在介绍适用于满足 $m \not\equiv 1 \bmod 4$ 条件的范数欧几里得实二次域 $\mathbb{Q}(\sqrt{m})$ 的 M_1-算法。满足 $m \equiv 1 \bmod 4$ 条件的情形将在 [11] 中讨论。关于虚二次域的情形，另请参见 [10] 。

第2节介绍精确计算，尤其是在某些情况下确定代数表达式的符号；这些计算是后文证明所必需的。第3节利用这些计算处理实二次域。证明具有几何性质：使用由范数定义的双曲线覆盖平面中的某个正方形。请注意，我们没有试图为给定的 m 寻找最少覆盖数。我们关注的是不使用浮点数进行精确计算，从而得到可复现的证明。值得一提的是，我们的 Maple 程序可在 https://gitlab.inria.fr/morain/euclid 获取，其中还提供了每种情形的结果，格式便于阅读。

2. Tools

2.1. 舍入。我们先给出一个简单的引理。

引理2.1. 对所有 $a_0 \in \mathbb{Q}$，存在 $\varepsilon \in \{\pm 1\}$和 $x \in \mathbb{Z}$，使得 $a_0 = x + \varepsilon a$且 $0 \le a \le 1/2$。

证明：取 $x = \lfloor a_0 \rceil$，使得 $|a_0 - x| \le 1/2$ 和 $\varepsilon = sign(a_0 - x)$。 □

2.2. 求二次多项式的符号。

引理2.2. 设 $P(X) = \alpha X^2 + \beta X + \gamma \in \mathbb{Q}[X]$ 且 $\alpha \neq 0$。对于实数 $x \in [x_{\min}, x_{\max}]$， $P(x)$ 的符号为：

$$\begin{cases} sign(\alpha) & \text{if } \operatorname{disc}(P) < 0 (case -); \\ sign(\alpha) & \text{if } \operatorname{disc}(P) = 0 case\ 0:\ but\ for\ x_0 = -\beta/(2\alpha) \\ & where\ it\ is\ 0\ in\ case\ x_0\ belongs\ to\ the\ interval; \\ see\ proof & \text{if } \operatorname{disc}(P) > 0. \end{cases}$$

证明：在最后一种情形中， P 有两个根 $x_\pm = (-\beta \pm \sqrt{\operatorname{disc}(P)})/(2\alpha)$。我们可以集中考虑情形 $\alpha > 0$，因为在这种情形下， $P(x)$的符号与 $-P(x)$的符号相反。有若干情形，如图1所示。

情形 a：若 $x_{\max} \le x_-$ （相应地 $x_+ \le x_{\min}$），则 $P(x)$从 $x_{\min}$ 递减（相应地递增）至 $x_{\max}$ ，且其值为正数。前一子情形标记为 a_1，前者 a_2。情形 b：

$[x_{\min}, x_{\max}] \subset [x_-, x_+]$： $sign(P(x)) \le 0$，见图1。情形 c：

$[x_-, x_+] \subsetneq [x_{\min}, x_{\max}]$： $sign(P(x))$在区间上不是常数：情形 d：

$x_{\min} < x_- < x_{\max} < x_+$： $P(x_{\min}) > 0$， $P(x_{\max}) < 0$。情形 e：

$x_- < x_{\min} < x_+ < x_{\max}$： $P(x_{\min}) < 0$， $P(x_{\max}) > 0$。

□

在我们的实践中， $x_\pm$、 $x_{\min}$ 和 $x_{\max}$ 的值都是精确数，因此我们可以精确地检验等式与不等式。

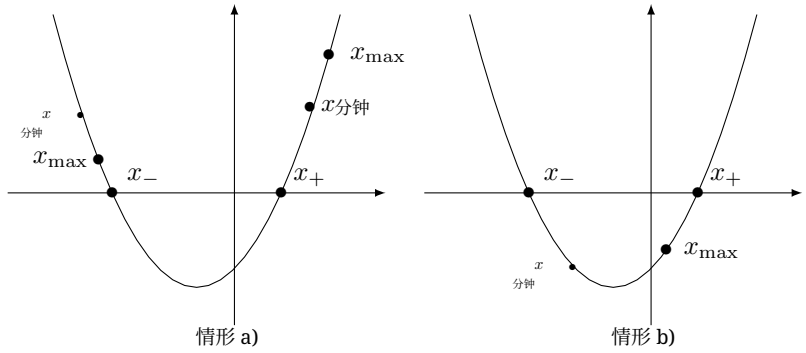

FIGURE 1. $[x_{\min}, x_{\max}]$上的二次多项式的符号。

2.3. 计算精确数的符号。精确数可以是整数、有理数、它们的平方根，或它们的和。例如

$$1, 1/2, \sqrt{2}, (1+\sqrt{5})/2, \sqrt{1+\sqrt{2}}$$

是精确数。（在本文中，所有平方根均假定为正数。）对这些数进行的计算都是精确的。根据我们的需要，我们能够在完全不使用浮点计算的情况下进行符号计算。这是获得正确且可验证证明的关键。

命题2.3。设 $t \geq 1$ 为整数。设$(x_i)_{0\leq i\leq t}$ 为严格正的有理整数，$(\epsilon_i)_{1\leq i\leq t}$ 为符号 ± 1，且$(y_i)_{1\leq i\leq t}$ 为精确数。我们要确定下列表达式的符号

$$x = x_0 + \sum_{i=1}^{t} \epsilon_i x_i \sqrt{y_i}.$$

记函数 ABS 为

$$ABS(x) = x_0 + \sum_{i=1}^{t} x_i \sqrt{y_i}.$$

1) 若对所有 i都有 $\epsilon_i = 1$，则 $sign(x) = +1$。

2) 若 $t = 1$ 且 $\epsilon_1 = -1$，则有

$$sign(x) = sign((xABS(x)) = sign(x_0^2 - x_1^2 y_1).$$

3) 若 $t = 2$，则 $sign(x) = sign(xABS(x))$，并且我们减少根式的数量。

4) 若 $t = 3$，则 $sign(x) = sign(xABS(x))$，并且我们减少根式的数量，但仅在以下情形：

$$x = x_0 + x_1\sqrt{y_1} - x_2\sqrt{y_2} - x_3\sqrt{y_3}.$$

证明：对于 2)，只需注意到 $x_0 + x_1\sqrt{y_1} > 0$，根据假设，因此通过乘法不会改变 x 的符号。

3）当 $t = 2$ 时，我们将问题归约为两种情况（必要时重新排序）

$$x = x_0 + x_1\sqrt{y_1} - x_2\sqrt{y_2}$$

or

$$x = x_0 - x_1\sqrt{y_1} - x_2\sqrt{y_2}.$$

在第一种情况下，我们使用

$$sign(x) = sign(xABS(x)) = sign(x_0^2 + x_1^2 y_1 - x_2^2 y_2 + 2x_0 x_1\sqrt{y_1})$$

于是我们又回到了情形 $t = 1$。

在第二种情形下，我们同样

$$sign(x) = sign(xABS(x)) = sign((x_0^2 - x_1^2 y_1 - x_2^2 y_2) - 2x_1 x_2\sqrt{y_1 y_2})$$

这样一来，我们以增加平方根内部的内容为代价，减少了平方根的数量。这使我们又回到了情形 $t = 1$。

4) 当 $t = 3$ 时，我们从

$$x_0 + x_1\sqrt{y_1} - x_2\sqrt{y_2} - x_3\sqrt{y_3}$$

通过相乘可得:

$$xABS(x) = (x_0 + x_1\sqrt{y_1})^2 - (x_2\sqrt{y_2} + x_3\sqrt{y_3})^2 = X_0 + X_1\sqrt{Y_1} - X_2\sqrt{Y_2}.\square$$

数值示例见第3.6节中的 $m = 7$ 。

注2.1。在某些情况下，我们可以运用一些技巧，例如将 $x = x_0 + X_0 - Y$写成 X_0 和 Y，且二者均为正数。如果 $X_0 - Y$更容易处理，并且 $sign(X_0 - Y) \geq 0$，那么显然 $x > 0$。如果 $X_0 - Y < 0$，我们可以得到 $x_0 \leq X_0$；如果 $2X_0 - Y \leq 0$，那么 $x \leq 0$。我们可以用$x_0 \leq x_1\sqrt{y_1}$和 $X_0 + x_1\sqrt{y_1} \leq Y$进一步改进；或者甚至尝试 X的所有子集的和。还有一些情况下，平方根的数量并未减少，但乘积 $xABS(x)$给出了符号。例如，当$x = x_0 + x_1\sqrt{y_1} + x_2\sqrt{y_2} - x_3\sqrt{y_3}$时，我们计算

$$xABS(x) = (x_0^2 + x_1^2 y_1 + x_2^2 y_2 - x_3^2 y_3) + 2(x_0 x_1\sqrt{y_1} + x_0 x_2\sqrt{y_2} + x_1 x_2\sqrt{y_1 y_2})$$

如果首项为正数，我们就得到正号。

注 2.2。前面的结果可以很容易地推广到这样的情形：对于某个定义在 $\mathbb{Q}[X]$ 上、且在区间 $\mathcal{A} = [a_{\min}, a_{\max}]$ 上为正的多项式，有 $y_k = P_k(a)$。当我们要比较第3节中的两段双曲线时，就会遇到这种情形。

3. Real quadratic fields $\mathbb{Q}(\sqrt{m})$, $m \not\equiv 1 \bmod 4$

设 $m \not\equiv 1 \bmod 4$ 是一个无平方因子整数。令 $\mathrm{K} = \mathbb{Q}(\sqrt{m})$；其整数环为 $\mathcal{O}_K = \mathbb{Z}[\omega]$，其中 $\omega = \sqrt{m}$，且 K 的定义多项式为 $X^2 - m$。K 的判别式 D_K 等于 $4m$，并且

$$f_m(x, y) := \mathrm{Norm}(x + y\omega) = x^2 - my^2.$$

实数 x, y 对应的数 $x + y\omega$ 可视为平面上的点 (x, y)。

下表列出了相应的欧几里得数域，以及最小值和临界点集（其中一些来自 P. Lezowski 非常宝贵的程序，参见 https://www.math.u-bordeaux.fr/~plezowsk/tables/result.php）。

m	M_1	C_1
2	$1/2$	$\{(0, 1/2)\}$
3	$1/2$	$\{(1/2, 1/2)\}$
6	$3/4$	$\{(1/2, 1/2)\}$
7	$9/14$	$\{(1/2, 5/14), (1/2, 9/14)\}$
11	$19/22$	$\{(1/2, 15/22), (1/2, 7/22)\}$
19	$170/171$	$\{(0, 20/57), (0, 37/57)\}$

3.1. 准备工作。

3.1.1. 双曲线与覆盖。设 $0 < M < 1$ 为一个实数（通常为有理数）。由于范数形式为 $f_m(a,b) = a^2 - mb^2$，我们考虑方程为

$$H^+_{u,v} : (a+u)^2 - m(b+v)^2 = M, \quad H^-_{u,v} : (a+u)^2 - m(b+v)^2 = -M$$

对于 u 和 v 有理整数，并注意 $\mathcal{H}_{u,\ v}$ 两者之间的区域:

$$\mathcal{H}_{u,v} = \{(a,b) \in \mathcal{S}, -M \le f_m(a+u, b+v) \le M\}.$$

对于 $(a,b) \in \mathcal{S}$，由于关于坐标轴对称，这形成了 2 个部分。由于 $f_m(a+u,b+v) = f_m(-a-u,-b-v)$，我们将研究范围缩小到 $(a,b) \in \mathcal{S}_0 = [0,1/2] \times [0,1/2]$。

考虑满足 $-M \le f_m(a,b) \le +M$ 的 $\mathcal{S}_0$ 集合 $\mathcal{H}$。如果 $\mathcal{H}_{u,v}$ 覆盖 (a,b)，则称之为覆盖；若 $(a,b) \in \mathcal{H}_{u,v}$。我们将这一概念扩展到区域 $\mathcal{R} \subset \mathcal{S}_0$。简言之，我们说 (u,v) 覆盖一个点（或一个区域）。

最后，我们以一条与临界点有关的性质结束这份列表。这条性质往往会使覆盖变得复杂，因为它们会被临界点吸引。

命题 3.1. 若 $P = (x_0, y_0)$ 是临界点，且被 (u,v) 覆盖，则

$$f_m(x_0+u, y_0+v) = \pm M.$$

3.1.2. 计算。

定义 3.2. 对于有理整数 u 和 v，以及 θ、$\epsilon \in \{\pm 1\}$，定义

$$B^{\theta,\epsilon}_{u,v}(a) := -v + \theta\sqrt{((a+u)^2 - \epsilon M)/m}.$$

这些曲线的绘图示例将在下文的诸多情形中给出，先从图 2 开始。另请注意，对于 $0 \le a \le 1/2$，以及可能相当大的整数 u，我们需要绘制函数 $B^{\theta,u\ \epsilon}_{,v}(a)$ 的部分曲线。在这种情况下，我们很乐意采用近似

$$B^{\theta,\epsilon}_{u,v}(a) \approx -v + \frac{\theta}{\sqrt{m}}\,|a+u|.$$

引理3.3. 当 $u \ge 0$, $B^{+,u\ \mp}_{\ \ v,}$（分别为 $B^{-,u\ \mp}_{\ \ v,}$）在$\mathcal{S}_0$上递增（分别递减）时；当 $u < 0$, $B^{+,u\ \mp}_{\ \ v,}$（分别为 $B^{-,u\ \mp}_{\ \ v,}$）在 $\mathcal{S}_0$ 上递减（分别递增）时。

证明：因为

$$B^{\theta,\epsilon}_{u,v}(a)' = \frac{\theta}{m}\,\frac{a+u}{\sqrt{((a+u)^2 - \epsilon M)/m}},$$

待证性质取决于 $a+u$ 在 $\mathcal{S}_0$ 上的符号，因此结论成立。 □我们的任务是证明，对于 $a \in \mathcal{A} = [a_{\min}, a_{\max}] \subset [0,1/2]$，有 $B^{\theta_1,u_1\ \epsilon_1}_{\ \ v_1,}(a) \ge B^{\theta_2,u_2\ \epsilon_2}_{\ \ v_2,}(a)$。这将通过注 2.2 来完成，同时还要证明，对于某个固定值 b_0，有 $B^{\theta,u\ \epsilon}_{\ \ v,}(a) \ge b_0$。

3.2. 计算一列范数。我们展开

$$f_m(a+u, b+v) = f_m(a,b) + f_m(u,v) + 2(au - mbv).$$

在某些情况下（计算下面的 $\mathcal{C}(p,B)$、测试它，或在实际除法中使用它），a和 b 是固定的，但有理整数 u 和 v 会变化。我们可以预先计算所有的 $f_m(u,v)$（也许还会预先计算所有 mv，或至少计算 mb）。

3.3. 非正式算法。我们的目标是证明，对于所有 $(a,b) \in \mathcal{S}_0$，都存在一个由 $\mathcal{H}_{u,v}$ 覆盖 (a,b) 的覆盖，其中 u, v 是某些整数。为此，我们对点 p 定义：

$$\mathcal{C}(p,B) = \{(u,v) \in \mathbb{Z}, |u|, |v| \leq B, p \text{ is covered by } H^{\pm}_{u,v}\},$$

对于某个整数 B。在实际计算中，取值为 $B = 10^2$ 或 $B = 10^3$。显然，更大的 B并不会产生很多覆盖。

我们以算法1给出我们方法的概要。我们无法证明该算法在所有情况下都会终止，也无法对其复杂度作任何说明（但请注意，这是一次性计算）。其中某些部分相当模糊，但将在下文的情形中加以说明。使用重心的想法基于这样一种思路：帮助覆盖某个子区域，从而有助于覆盖整个区域。

算法1：覆盖一个区域。

函数 COVERING$(m, M, \mathcal{R})$输入： M 是 $\mathbb{Q}(\sqrt{m})$中范数的一个界 输出： $\mathcal{R}$ 的一个覆盖 对 $p \in \mathcal{R}$ 执行$UV[p] = \mathcal{C}(p, B)$；如果 $\exists (u, v)$为所有 $UV[p]$ 所共有，则返回$\mathcal{R}_{u,v}$ 由 $\mathcal{R}$构造。否则如果 $\exists (u, v)$覆盖多于两个点，则构造 $\mathcal{R}_{u,v}$ 即 $\mathcal{R}$ 中由(u, v)覆盖的子区域及其补集 $\mathcal{R}'$；返回$\mathcal{R}_{u,v} \cup Covering($ $m, M, \mathcal{R}')$ 否则计算 $\mathcal{R}$ 的重心 q，并尝试覆盖 $\mathcal{R} \cup \{q\}$的各个部分。

我们的方法构造一个点序列 P_i，始终从由其四个角点表示的 $\mathcal{S}_0$ 开始：

$$P_0 = (0,0), P_1 = (1/2, 0), P_2 = (1/2, 1/2), P_3 = (0, 1/2).$$

临界点将记为 P_c或 P_{c_1}、 P_{c_2}.....；（此类临界点在我们的图中将以符号 $\circ$ 印出）。该算法的输出是覆盖正方形 $\mathcal{S}_0$ 的一组区域 $\mathcal{R}_{u_i,v_i}$。一个典型区域由通过直线或双曲线片段相关联的点（的指标） $B^{\theta}{}_{,u}{}^{\epsilon}{}_{,v}$ 组成。关于区域的例子，见第3.5节中的情形$m = 6$。

3.4. 情形 $m = 2$、3。这三个情形的范数欧几里得性证明由 Perron [13], 2 完成，而 3 已由 Dedekind [6]完成。情形 2 在 [16] 中得到仔细考察。对于这些情形，我们直接进行，但查看图 2 是值得的。

命题3.4. 设 $0 \leq a$、 $b \leq 1/2$。
i) 对于 $m = 2$, $|f_m(a, b)| \leq M(f_m) = 1/4$。ii) 对于 $m = 3$, 存在 $(u, v) \in \{(0, 0), (-1, 0)\}$ 使得

$$|f_m(a + u, b + v)| \leq M(f_m).$$

证明：

i) 对于 $0 \le a$、$b \le 1/2$，我们得到 $-m/4 \le f_m(a,b) \le 1/4$，因此 $|f_m(a,b)| \le m/4$。参见图 2。

ii) 对于 $m = 3$，假设 $a^2 - 3b^2 < -1/2$。我们推出 $3b^2 > 1/2$，结合 $-1 \le a - 1 \le -1/2$ 可得

$$-\frac{1}{2} \le \frac{1}{4} - 3b^2 \le (a-1)^2 - 3b^2 < 1 - \frac{1}{2}.$$

见图 2。

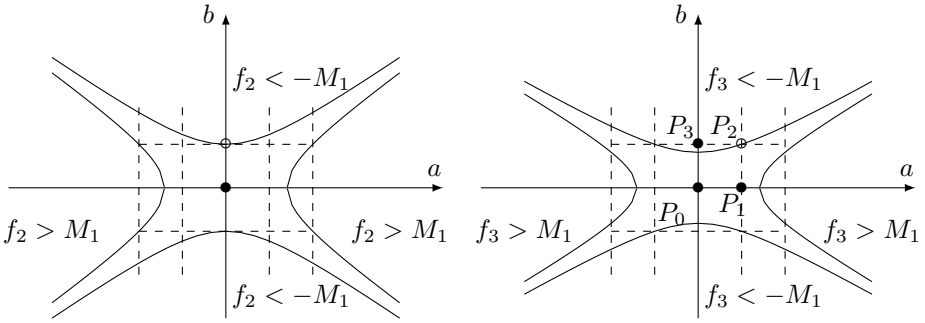

FIGURE 2. 情形 $m = 2$（左）和 $m = 3$（右）。

3.5. 情形 $m = 6$。Perron [13]证明了此情形下的范数欧几里得性。

定理 3.5. 对于 $m = 6$，正方形 $\mathcal{S}_0$ 可由这些对覆盖

$$(0,0), (1,0), (-2,-1).$$

证明： $\mathcal{S}_0$ 中有一个临界点，即 $P_c = (1/2, 1/2)$。我们从以 (0, 0) 为覆盖开始，得到点

$$P_4 = \left(0, 1/4\sqrt{2} \approx 0.353553\right).$$

第一个区域为

$$\mathcal{R}_{0,0} = (0, 1, c, [0, 0, 1, -1], 4, 0),$$

这表明 (0,0) 覆盖了由 $\overline{P_0P_1P_c}$ 界定的区域，接着是 $B^{+-}_{0\,0}$，连接 P_c 和 P_4，再接着是直线 $\overline{P_4P_0}$。

我们添加以 (1, 0) 为覆盖，以处理 $P_2P_3P_4$，并引入点

$$P_5 = B^{++}_{1,0} \cap B^{+-}_{0,0} = \left(1/4, 1/24\sqrt{78} \approx 0.367990\right).$$

我们证明（使用注 2.2）对 $P_2P_3P_4$ 的覆盖，其中

$$B^{+-}_{1,0} \ge B^{+-}_{0,0} \text{ for } a \in [0, 1/2], \text{i.e.}, 2\,a + 1 \ge 0;$$

$$B^{+-}_{0,0} \ge B^{++}_{1,0} \text{ for } a \in [0, x(P_5)], \text{i.e.}, 1 - 4\,a \ge 0.$$

我们证明， P_2P_3 可通过以下方式覆盖

$$B^{+-}_{1,0} \ge 1/2 \text{ for } a \in [0, 1/2], \text{i.e.}, 4\,a^2 + 8\,a + 1 \ge 0 : \text{case } a_2;$$

$$B^{++}_{1,0} \le 1/2 \text{ for } a \in [0, 1/2], \text{i.e.}, 4\,a^2 + 8\,a - 5 \ge 0 : \text{case b}.$$

这得出了该区域

$$\mathcal{R}_{1,0} = (2, 3, 4, [0, 0, 1, -1], 5, [1, 0, 1, 1], 2).$$

最后，我们以带有证明的（$-2, -1$）作结

$$B^{-+}_{-2,-1} \geq B^{+-}_{0,0} \text{ for } a \in [x(P_5), 1/2], \text{i.e.}, -32\,a^2 + 112\,a - 23 \geq 0 : \text{case b};$$

$$B^{+-}_{0,0} \geq B^{--}_{-2,-1} \text{ for } a \in [1/4, 1/2], \text{i.e.}, 4\,a^2 - 8\,a + 7 \geq 0 : \text{case -}.$$

而该区域为

$$\mathcal{R}_{-2,-1} = (c, 2, [-2, -1, -1, 1], 5, [0, 0, 1, -1], c).$$

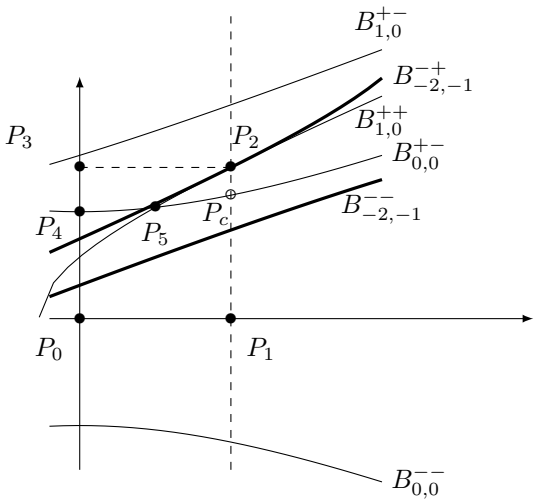

FIGURE 3. 情形 $m = 6$ （右）。

3.6. 情形 $m = 7$。欧几里得性的第一个证明由 Perron [13] 给出。第一个极小值是在 [17] 中计算的。

定理3.6. 对于 $m = 7$，正方形 $\mathcal{S}_0$ 可以由以下四对覆盖

$$(0, 0), (1, 0), (-4, 1), (-2, -1).$$

证明： $\mathcal{S}_0$ 中有一个临界点，即 $P_c = (1/2, 5/14)$，我们计算

$$\mathcal{C}(P_c, 10^2) = \{[-57, 21], [-26, -10], [-12, 4], [-4, 1], [-2, -1], [-1, 0], [0, 0], [1, -1], [3, 1], [11, 4], [25, -10], [56, 21]\},$$

我们来看看图 4，其中

$$P_4 = \left(0, 3\sqrt{2}/14 \approx 0.3030\right),$$

它自然地表现为 $B^{+-}_{0},_{0}$ 与 b-轴的交点。曲线 $B^{+-}_{0},_{0}$ 和 $B^{--}_{0},_{0}$ 之间的点位于 $\mathcal{H}$中。这就得到了我们的第一个区域：

$$\mathcal{R}_{0,0} = (0, 1, c, [0, 0, 1, -1], 4, 0),$$

也就是说，(0, 0) 覆盖 $\overline{P_0P_1P_c} \cup B^{+-}_{0},_{0} \cup \overline{P_4P_0}$。

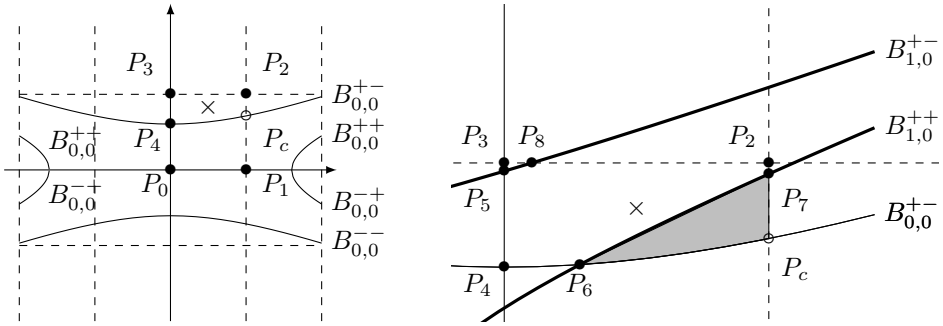

FIGURE 4. 情形 $m = 7$：步骤1（左）与步骤 2（右）。

我们必须找到其他区域$\mathcal{H}_{u,\ v}$，以覆盖 $\mathcal{S}_0$ 的剩余部分，也就是区域 $P_4P_c \cup \overline{P_cP_2P_3P_4}$。

步骤 2：首先，我们添加区域$\mathcal{H}_{1,0}$，它覆盖平行四边形 $P_cP_2P_3P_4$的重心（绘制为 $\times$），见图 4，从而得到区域 $\overline{P_5P_4} \cup P_4P_6P_7 \cup P_7P_2P_8 \cup P_8P_5$ 的覆盖，其中

$$P_5 = B_{1,0}^{+-} \cap \{x = 0\} = \left(0, 1/14\sqrt{46} \approx 0.484452\right),$$

$$P_6 = B_{1,0}^{++} \cap B_{0,0}^{+-} = \left(1/7 \approx 0.142857, \frac{\sqrt{910}}{98} \approx 0.307818\right),$$

$$P_7 = B_{1,0}^{++} \cap \{x = 1/2\} = \left(1/2, 3/14\sqrt{6} \approx 0.479157\right),$$

$$P_8 = B_{1,0}^{+-} \cap \{y = 1/2\} = \left(-1 + 1/14\sqrt{217} \approx 0.052209, 1/2\right).$$

结果表明，双曲线弧 P_4P_6 也被覆盖。为此，利用引理3.3和注 2.2，我们必须证明对于 $0 \le a \le 1/7$

$$B_{1,0}^{+-} \ge B_{0,0}^{+-} \text{ for } a \in [0, 1/7], \text{i.e.}, 2\,a + 1 \ge 0;$$

$$B_{0,0}^{+-} \ge B_{1,0}^{++} \text{ for } a \in [0, 1/7], \text{i.e.}, 1 - 7\,a \ge 0.$$

我们还需要利用注 2.2证明直线 P_8P_2 被覆盖：

$$B_{1,0}^{+-} \ge 1/2 \text{ for } a \in [x(P_8), 1/2], \text{i.e.}, 28\,a^2 + 56\,a - 3 \ge 0 : \text{case } a_2;$$

$$B_{1,0}^{++} \le 1/2 \text{ for } a \in [x(P_8), 1/2], \text{i.e.}, 28\,a^2 + 56\,a - 39 \ge 0 : \text{case b.}$$

这给出了区域

$$\mathcal{R}_{1,0} = (7, 2, 8, [1, 0, 1, -1], 5, 4, [0, 0, 1, -1], 6, [1, 0, 1, 1], 7).$$

步骤3：尚待覆盖 $P_5P_8 \cup \overline{P_8P_3P_5}$，这通过对这些点的可能覆盖求交来完成，得到 $\{(-4, 1), (-4, -2)\}$。我们选择第一个以得到图5。为证明$\mathcal{H}_{-4,1}$ 覆盖弧 P_4P_8，我们需要证明：

$$B_{-4,1}^{+-} \ge B_{1,0}^{+-} \text{ for } a \in [0, x(P_8)],$$

换句话说：$4a^2 - 12a + 1 \ge 0$，$-392a^2 + 1036a + 5 \ge 0$，对于 $0 \le a \le x(P_8)$，这由引理2.2可知成立。我们还需要证明 P_3P_8 的覆盖：

$$B_{-4,1}^{+-} \ge 1/2 \text{ for } a \in [0, x(P_8)], \text{i.e.}, 28\,a^2 - 224\,a + 25 \ge 0 : \text{case } a_1;$$

$$B^{++}_{-4,1} \le 1/2 \text{ for } a \in [0, x(P_8)], \text{i.e.}, 28\,a^2 - 224\,a - 11 \ge 0 : \text{case b.}$$

该区域为 $\mathcal{R}_{-4,1} = (c, 5, [1, 0, 1, -1], 8, 3)$。

$\overset{\frown}{}$对弧 $P_6P_cP_7$ 也进行同样的处理，找到一对 $(-2, -1)$，将其添加到图5中，并首先证明

$$B^{-+}_{-2,-1} \ge B^{++}_{1,0} \text{ for } a \in [0, 1/2], \text{i.e.}, 4\,a^2 - 4\,a + 3 \ge 0 : \text{case -;}$$

$$B^{++}_{1,0} \ge B^{--}_{-2,-1} \text{ for } a \in [0, 1/2], \text{i.e.}, -392\,a^2 + 1148\,a + 129 \ge 0 : \text{case b.}$$

我们还需要

$$B^{+-}_{0,0} \ge B^{--}_{-2,-1} \text{ for } a \in [0, 1/2], \text{i.e.}, 4\,a^2 - 8\,a + 3 \ge 0 : \text{case } a_1,$$

由此完成证明。最后一个区域是

$$\mathcal{R}_{-2,-1} = (c, 7, [1, 0, 1, 1], 6, [0, 0, 1, -1], c).$$

□

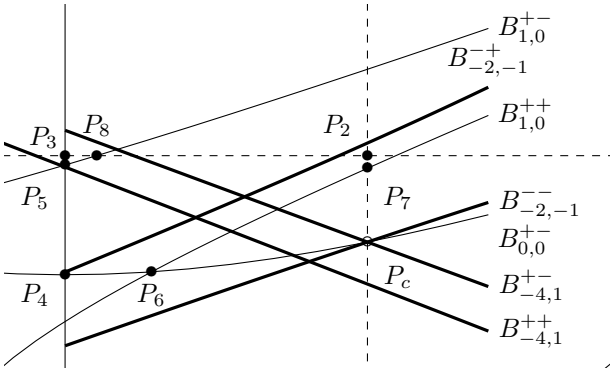

FIGURE 5. 情形 $m = 7$：步骤3。

3.7. 情形 $m = 11$。此情形已在 [13, 12, 14] 中处理过，并在[1, 定理 1] 中再次讨论（其中给出了一个连续极小值序列及其临界点和许多性质），另见 [18]。

对于最后两种情况，我们不提供区域，因为数量很多。对应的数据文件请参见作者的 Git 网站。

定理 3.7. 对于 $m = 11$，正方形 $\mathcal{S}_0$ 可以由以下六对覆盖

$$(0, 0), (1, 0), (-6, -2), (-5, 1), (5, -2), (25, -8).$$

证明： $\mathcal{S}_0$ 中有一个临界点，即 $P_c = (1/2, 7/22)$。我们计算

$$\mathcal{C}(P_c, 10^2) = \{[-16, -5], [-6, -2], [-1, 0], [0, 0], [5, -2], [15, -5]\}.$$

我们来看图6，其中 $P_4 = (0, 1/22\sqrt{38})$。曲线 $B^{+-}_{0\,0}$, 和 $B^{--}_{0\,0}$, 之间的点位于 $\mathcal{H}$ 中。我们必须找到其他区域 $\mathcal{H}_{u,\,v}$，以覆盖 $\overset{\frown}{}$ 的剩余部分，即区域 $P_4P_c \cup \overline{P_cP_2P_3P_4}$。

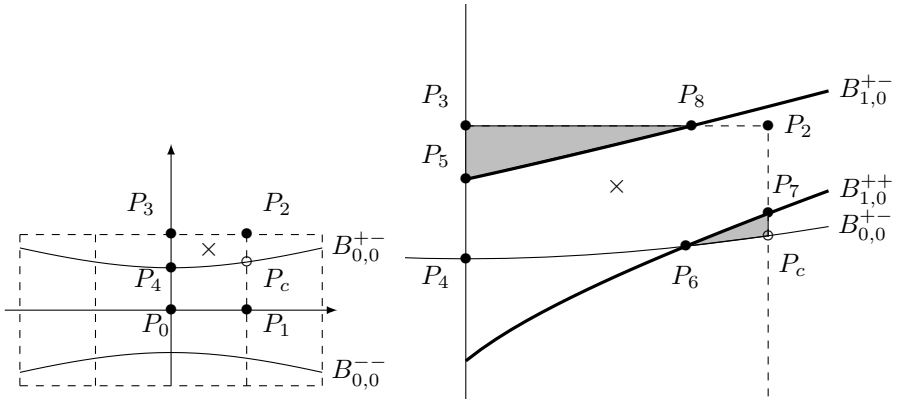

FIGURE 6. 情形 $m = 11$: 步骤1（左），步骤 2（右）。

步骤 2: 我们添加区域$\mathcal{H}_{1,\ 0}$，以覆盖平行四边形$\overset{\frown}{\quad}\ \overline{\quad}\ \overset{\frown}{\overline{P_4P_cP_2P_3}}$的重心，见图6，这样便得到 $\overline{P_5P_4}\cup P_4P_6P_7\cup P_7P_2P_8\cup P_8P_5$ 的一个覆盖，其中

$$P_5 = B^{+-}_{1,0}\cap\{x=0\} = (0, 1/22\sqrt{82}\approx 0.4116),$$
$$P_6 = B^{++}_{1,0}\cap B^{+-}_{0,0} = \left(4/11, \frac{\sqrt{5302}}{242}\approx 0.3009\right),$$
$$P_7 = B^{++}_{1,0}\cap\{x=1/2\} = \left(1/2, 1/22\sqrt{61}\approx 0.3550\right),$$
$$P_8 = B^{+-}_{1,0}\cap\{y=1/2\} = \left(-1+1/22\sqrt{913}\approx 0.3734, 1/2\right).$$

$\overset{\frown}{\quad}$我们必须证明双曲线弧 P_4P_6 也被覆盖。为此，利用引理3.3和注 2.2，我们证明

$$B^{+-}_{1,0}\ge B^{+-}_{0,0}\ \text{for}\ a\in[0,1/2], \text{i.e.}, 2\,a+1\ge 0;$$
$$B^{+-}_{0,0}\ge B^{++}_{1,0}\ \text{for}\ a\in[0,x(P_6)], \text{i.e.}, 4-11\,a\ge 0.$$

我们还需要证明 P_8P_2 的覆盖:

$$B^{+-}_{1,0}\ge 1/2\ \text{for}\ a\in[x(P_8),1/2], \text{i.e.}, 44\,a^2+88\,a-39\ge 0 : \text{case } a_2;$$
$$B^{++}_{1,0}\le 1/2\ \text{for}\ a\in[x(P_8),1/2], \text{i.e.}, 44\,a^2+88\,a-115\ge 0 : \text{case b.}$$

$\overset{\frown}{\quad}$步骤3: 为了覆盖 $P_6P_cP_7$，我们对这些点可能的覆盖取交集，得到 $(-6,-2)$ 和图7。

我们需要证明

$$B^{-+}_{-6,-2}\ge B^{++}_{1,0}\ \text{for}\ a\in[x(P_6),1/2], \text{i.e.}, 20\,a^2-100\,a+57\ge 0 : \text{case } a_1;$$
$$B^{++}_{1,0}\ge B^{--}_{-6,-2}\ \text{for}\ a\in[x(P_6),1/2], \text{i.e.}, -605\,a^2+4488\,a-874\ge 0; \text{case b.}$$

$\overset{\frown}{\quad}$对于 P_3、 P_5、 P_8，没有共同的对，但$(-2,-1)$覆盖了我们添加到图7中的 P_5P_8。这样就剩下两个新的点

$$P_9 = B^{-+}_{-2,-1}\cap\{y=1/2\} = \left(2-1/22\sqrt{1749}\approx 0.099043, 1/2\right),$$
$$P_{10} = B^{-+}_{-2,-1}\cap\{x=0\} = \left(0, 1-1/22\sqrt{138}\approx 0.466030\right).$$

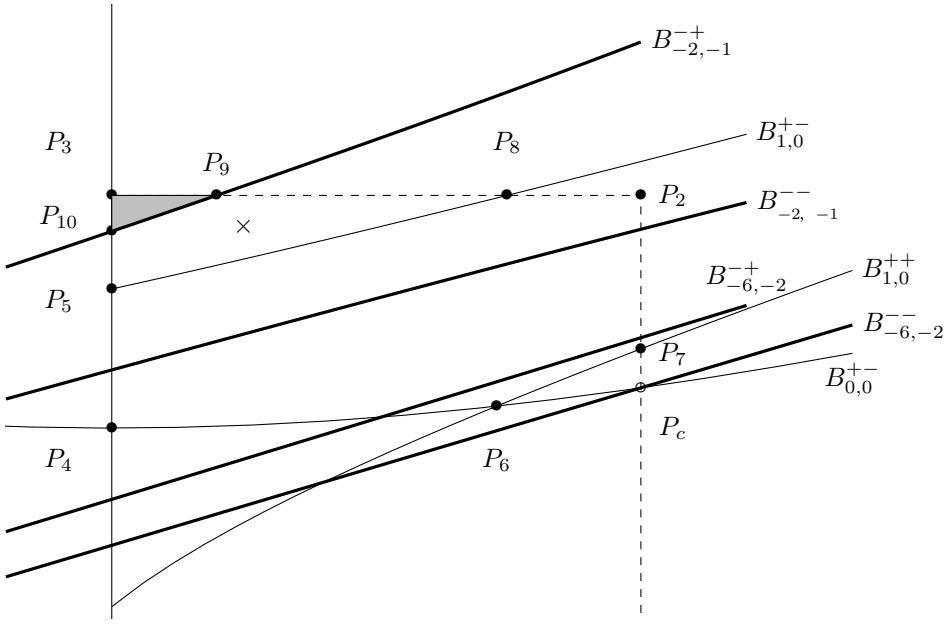

FIGURE 7. 情况 $m = 11$: 步骤3。

我们需要证明

$$B^{-+}_{-2,-1} \geq B^{+-}_{1,0} \text{ for } a \in [0, 1/2], \text{i.e.}, -968\,a^2 + 3476\,a + 1527 \geq 0 : \text{ case b;}$$

$$B^{+-}_{1,0} \geq B^{--}_{-2,-1} \text{ for } a \in [0, 1/2], \text{i.e.}, 4\,a^2 - 4\,a + 9 \geq 0 : \text{case } -.$$

步骤4: 还剩下对 $\overline{P_9P_3P_{10}} \cup P_{10}P_9$ 的覆盖。

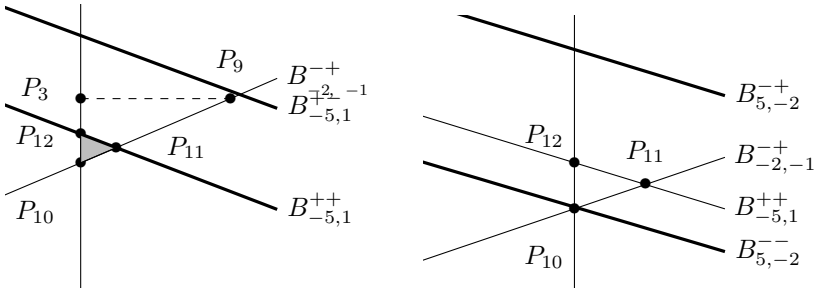

FIGURE 8. 情况 $m = 11$: 步骤4（左），步骤 5（右）。

我们可以使用 $(-5, 1)$，并找到两个新的点

$$P_{11} = B^{++}_{-5,1} \cap B^{-+}_{-2,-1} = \left(7/2 - \frac{3\sqrt{1645}}{35} \approx 0.0235, \frac{9\sqrt{1645}}{770} \approx 0.4741\right),$$

$$P_{12} = B^{++}_{-5,1} \cap \{x = 0\} = \left(0, -1 + \frac{3\sqrt{118}}{22} \approx 0.4813\right),$$

⌒见图 8。首先，我们证明它们用以下方式覆盖 $P_{11}P_9$

$B^{+-}_{-5,\,1} \geq B^{-+}_{-2,\,-1}$ 对于 $a \in [x(P_{11}, x(P_9)]$, 即 $4235\,a^2 - 29018\,a + 3009 \geq 0$: 情形 a_1;

$B^{-+}_{-2,\,-1} \geq B^{++}_{-5,\,1}$ 对于 $a \in [x(P_{11}, x(P_9)]$, 即 $-140\,a^2 + 980\,a - 23 \geq 0$: 情形 b。对于 P_3P_9，我们得到

$$B^{+-}_{-5,1} \geq 1/2 \text{ for } a \in [0, x(P_9)], \text{i.e.}, 44\,a^2 - 440\,a + 49 \geq 0 : \text{case } a_1;$$

$$B^{++}_{-5,1} \leq 1/2 \text{ for } a \in [0, x(P_9)], \text{i.e.}, 44\,a^2 - 440\,a - 27 \geq 0 : \text{case b.}$$

⌒步骤 5：剩下的区域是 $P_{10}P_{11}\overline{P_{11}P_{12}P_{10}}$。

我们决定用 $(5, -2)$ 覆盖 P_{11} 和 P_{12} （再次覆盖），见图 8。这留下了一个未覆盖的极小区域： $P_{10}P_{13}P_{14}$ （注意， P_{10} 未被覆盖），其中

$$P_{13} = B^{--}_{5,-2} \cap \{x = 0\} = \left(0, 2 - 1/22\,\sqrt{1138} \approx 0.4666\right),$$

$$P_{14} = B^{--}_{5,-2} \cap B^{-+}_{-2,-1} = \left(-\frac{73}{44} + 1/44\,\sqrt{5335} \approx 0.0009, \frac{67}{44} - \frac{7\sqrt{5335}}{484} \approx 0.4663\right).$$

为了证明该覆盖，我们需要

$$B^{-+}_{5,-2} \geq B^{++}_{-5,1} \text{ for } a \in [0, x(P_{11})], \text{i.e.}, 4\,a^2 + 243 \geq 0 : \text{case } -;$$

$$B^{++}_{-5,1} \geq B^{--}_{5,-2} \text{ for } a \in [0, x(P_{11})], \text{i.e.}, -242\,a^2 - 4180\,a + 5809 \geq 0 : \text{case b.}$$

⌒步骤 6：我们需要覆盖区域 $P_{10}P_{14}P_{13}\overline{P_{13}P_{10}}$，见图 9。我们可以使用

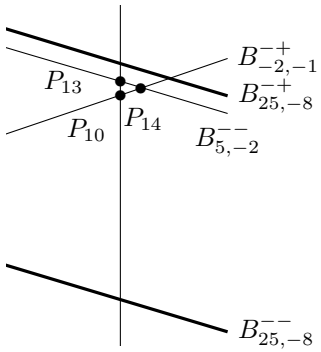

FIGURE 9. 情形 $m = 11$: 步骤 6。

$(25, -8)$，这是通过计算得出的，还需要证明

$B^{-+}_{25,-8} \geq B^{--}_{5,-2}$ for $a \in [0, x(P_{14})]$, i.e., $-1936\,a^2 - 41360\,a + 6503 \geq 0$: case b;

$B^{-+}_{5,\,-2} \geq B^{--}_{25,\,-8}$ 对于 $a \in [0, x(P_{14})]$, 即 $1936\,a^2 + 74800\,a + 495097 \geq 0$: 情形 a_2.至此定理的证明结束。 □

3.8. 情形 $m = 19$。伯格 [2] 通过列出一组不等式（未给出证明）给出了最小值；另见 [18]。我们可以预料到后面的情形会更难。

定理 3.8。对于 $m = 19$，正方形 $\mathcal{S}_0$ 可由以下各对覆盖

$$(0,0),(1,0),(-2,0),(2,-1),(-7,1),(-3,-1),(7,-2),(-6,1),(991,227),$$
$$(-19,4),(-80,18),(-430,-99),(90,-21).$$

有一个例外点 $P_c = (0, 20/57)$，它被弱覆盖：

$$C(P_c, 10^3) = \{[-991,227],[-29,-7],[-3,-1],[3,-1],[29,-7],[991,227]\}.$$

首先关注以下各点：

$$P_4 = \left(0, \frac{\sqrt{170}}{57} \approx 0.2287\right), P_5 = \left(1/2, \frac{\sqrt{851}}{114} \approx 0.2559\right)$$

其中 P_4 和 P_5 是与 $B^{+,\overline{0\,0}}$ 的交点，参见图 10。

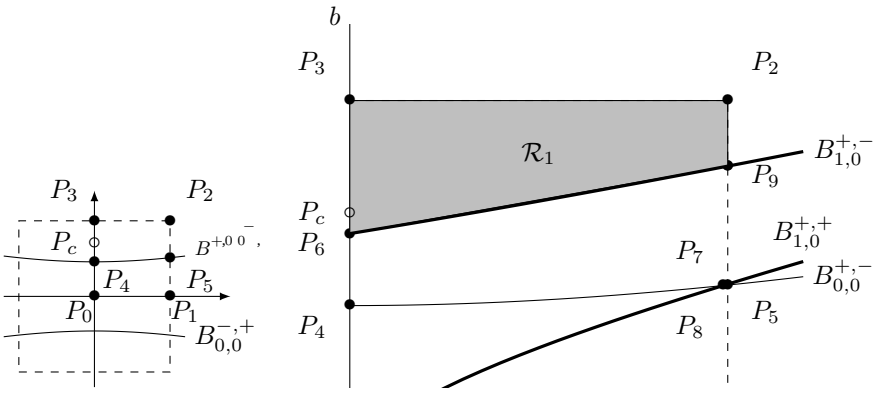

FIGURE 10. 情形 $m = 19$：步骤1（左），步骤 2（右）。

步骤 2：我们决定使用 (1, 0) 来覆盖 $\mathcal{S}_0$ 的更多部分，包括 P_4，见图 10。这会产生新的点

$$P_6 = B^{+-}_{1,0} \cap \{x = 0\} = \left(0, \frac{\sqrt{341}}{57} \approx 0.3240\right),$$

$$P_7 = B^{++}_{1,0} \cap \{x = 1/2\} = \left(1/2, \frac{\sqrt{859}}{114} \approx 0.2571\right),$$

$$P_8 = B^{++}_{1,0} \cap B^{+-}_{0,0} = \left(\frac{169}{342} \approx 0.4942, \frac{\sqrt{2751979}}{6498} \approx 0.2553\right),$$

$$P_9 = B^{+-}_{1,0} \cap \{x = 1/2\} = \left(1/2, \frac{\sqrt{2219}}{114} \approx 0.4132\right)$$

我们需要证明

$$B^{+,-}_{1,0} \geq B^{+,-}_{0,0} \geq B^{+,+}_{1,0}$$

对于 $a \in [0, x(P_8)]$，，即

$$2a + 1 \geq 0, 169 - 342a \geq 0.$$

我们需要覆盖区域 $\mathcal{R}_1 = P_2P_3P_6P_9$ 和非常小的区域 $P_5P_7P_8$。后者可由 (5, 1) 覆盖，见图11。我们必须证明

$B^{+-}_{5,1} \geq B^{++}_{10}$，对于 $a \in [0, 1/2]$，即 $-350892\,a^2 - 1175112\,a + 1415029 \geq 0$：情形 b；

$$B^{+-}_{5,1} \geq B^{+-}_{0,0} \text{ for } a \in [1/3, 1/2], \text{i.e.}, 54\,a^2 + 270\,a - 89 \geq 0 : \text{case } a_2;$$

$B^{+-}_{0,0} \geq B^{++}_{51}$，对于 $a \in [1/3, 1/2]$，即 $-175446\,a^2 - 586530\,a + 434681 \geq 0$：情形 b。（ 1/3 的值任意，且足以用于我们的证明。）

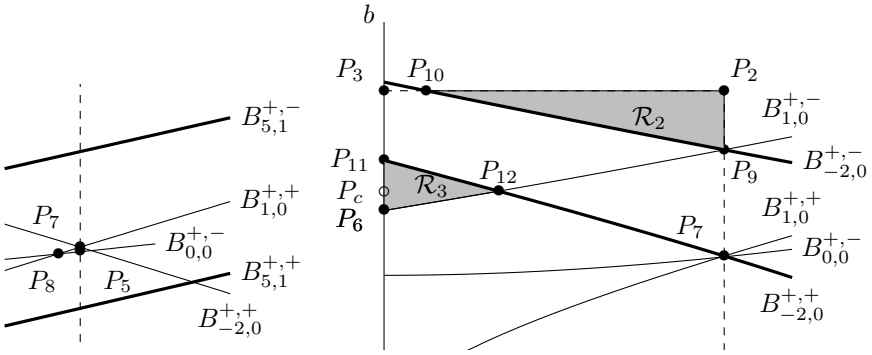

FIGURE 11. 情形 $m = 19$：步骤 2 结束（左），步骤3（右）。

步骤3： P_3、P_7 和 P_9 可由（-2，0）覆盖，见图11。这产生了新的点

$$P_{10} = B^{+-}_{-2,0} \cap \{y = 1/2\} = \left(2 - \frac{\sqrt{48811}}{114} \approx 0.0620, 1/2\right),$$

$$P_{11} = B^{++}_{-2,0} \cap \{x = 0\} = \left(0, \frac{\sqrt{514}}{57} \approx 0.3977\right),$$

$$P_{12} = B^{++}_{-2,0} \cap B^{+-}_{1,0} = \left(\frac{173}{1026} \approx 0.1686, \frac{\sqrt{47198299}}{19494} \approx 0.3524\right).$$

证明如下：

$$B^{+-}_{-2,0} \geq B^{+-}_{1,0} \text{ for } a \in [173/1026, 1/2], \text{i.e.}, -2\,a + 1 \geq 0;$$

$$B^{+-}_{1,0} \geq B^{++}_{-2,0} \text{ for } a \in [173/1026, 1/2], \text{i.e.}, 1026\,a - 173 \geq 0.$$

我们还需要证明 P_3P_{10} 的覆盖：

$$B^{+-}_{-2,0} \geq 1/2 \text{ for } a \in [0, x(P_{10})], \text{i.e.}, 684\,a^2 - 2736\,a + 167 \geq 0 : \text{case } a_1;$$

$$B^{++}_{-2,0} \leq 1/2 \text{ for } a \in [0, x(P_{10})], \text{i.e.}, 684\,a^2 - 2736\,a - 1193 \geq 0 : \text{case b}.$$

我们仍需覆盖 $\mathcal{R}_2 = \overline{P_9P_2P_{10}}P_{10}P_9$ 和 $\mathcal{R}_3 = P_{11}P_cP_6P_6P_{12}$。

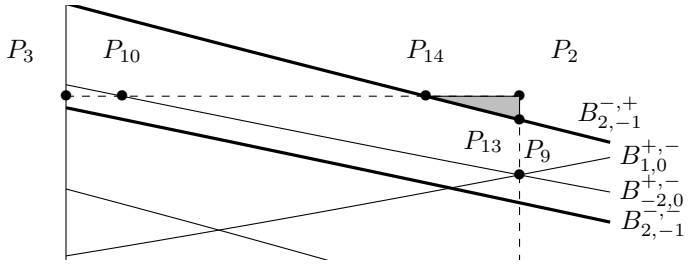

FIGURE 12. 情形 $m = 19$：步骤4。

3.8.1. 覆盖 $\mathcal{R}_2$。步骤4：$(2, -1)$ 覆盖 P_9 和 P_{10}，见图12。我们需要证明

$B_2^{-+}{}_{,\ -1} \geq B^{+-}_{-2,\ 0}$ </style}对于 $a \in [0, 1/2]$，即 $-350892\,a^2 - 930240\,a + 1782337 \geq 0$：情形 b；

$$B^{+-}_{-2,0} \geq B^{--}_{2,-1} \text{ for } a \in [0, 1/2], \text{i.e.}, 108\,a^2 + 167 \geq 0 : \text{case -}.$$

对于 $P_{10}P_{14}$ 的覆盖，我们得到

$$B^{-+}_{2,-1} \geq 1/2 \text{ for } a \in [x(P_{10}), x(P_{14})], \text{i.e.}, -684\,a^2 - 2736\,a + 1193 \geq 0 : \text{case b};$$

$B_2^{--}{}_{,\ -1} \leq 1/2$ 对于 $a \in [x(P_{10})\ x(P_{14})]$，即 $-684\,a^2 - 2736\,a - 167 \geq 0$：情形 a_2.我们找到两个新点

$$P_{13} = B^{-+}_{2,-1} \cap \{x = 1/2\} = \left(1/2, 1 - \frac{\sqrt{3595}}{114} \approx 0.4740\right),$$

$$P_{14} = B^{-+}_{2,-1} \cap \{y = 1/2\} = \left(-2 + \frac{\sqrt{74651}}{114} \approx 0.3967, 1/2\right).$$

步骤 5：我们必须覆盖 $P_{13}P_2P_{14}$，这可以通过使用 $(-7, 1)$ 来完成，见图 13。我们需要证明 P_2P_{14} 已被覆盖：

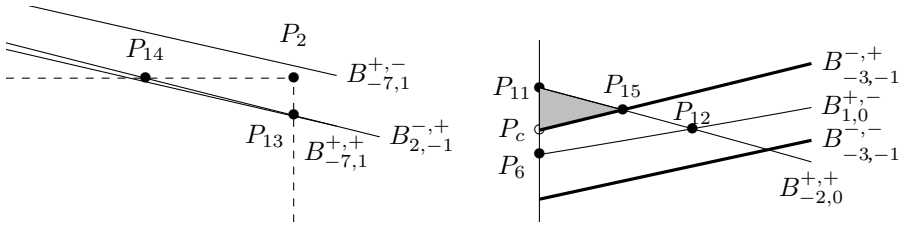

FIGURE 13. 情形 $m = 19$：步骤 5（左），步骤 6（右）。

$B^{+-}_{-7,\ 1} \geq 1/2$ 当 $a \in [x(P_{14})\ 1/2]$ 时，即 $684\,a^2 - 9576\,a + 4955 \geq 0$：情形 a_1；$B^{++}_{-7,\ 1} \leq 1/2$ 当 $a \in [x(P_{14})\ 1/2]$ 时，即 $684\,a^2 - 9576\,a + 3595 \geq 0$：情形 b。此外：

$B^{+-}_{-7,\ 1} \geq B_2^{-+}{}_{,\ -1}$ 对于 $a \in [0, 1/2]$，即 $-116964\,a^2 + 1003428\,a + 421651 \geq 0$：情形 b；$B_2^{-+}{}_{,\ -1} \geq B^{++}_{-7,\ 1}$ 对于 $a \in [0, 1/2]$，即 $36\,a^2 - 180\,a + 85 \geq 0$：情形 a_1.

3.8.2. 覆盖 $\mathcal{R}_3$。步骤 6：我们选择 $(-3,-1)$，得到图 13。这就形成了

$$P_{15}=B^{-+}_{-3,-1}\cap B^{++}_{-2,0}=\left(5/2-1/18\sqrt{1879}\approx 0.0918, 1/2-\frac{\sqrt{1879}}{342}\approx 0.3733\right).$$

我们需要证明

$B^{-+}_{-3,-1}\geq B^{+-}_{1\,0}$,对于 $a\in[0,1/2]$，即 $-350892\,a^2+1632024\,a+501205\geq 0$：情形 b；

$$B^{+-}_{1,0}\geq B^{--}_{-3,-1}\text{ for }a\in[0,1/2],\text{i.e.},108\,a^2-216\,a+275\geq 0:\text{case -}.$$

这样我们就只剩下 $P_{11}P_cP_{15}$。

第7步：为了覆盖 P_{15}，我们使用 $(7,-2)$ 来覆盖 $P_{11}P_{15}$，见图 14。这会产生

$$P_{16}=B^{--}_{7,-2}\cap\{x=0\}=\left(0,2-\frac{\sqrt{8549}}{57}\approx 0.3779\right),$$

$$P_{17}=B^{--}_{7,-2}\cap B^{-+}_{-3,-1}=\left(-\frac{29402}{13851}+\frac{\sqrt{3647350219}}{27702}\approx 0.0574,\right.$$

$$\left.\frac{41893}{27702}-\frac{5\sqrt{3647350219}}{263169}\approx 0.3648\right).$$

我们需要证明

$$B^{-+}_{7,-2}\geq B^{++}_{-2,0}\text{ for }a\in[0,2/5],\text{i.e.},36\,a^2+180\,a+85\geq 0:\text{case }a_2;$$

$B^{++}_{-2,\ 0}\geq B^{--}_{7,\ -2}$ 对于 $a\in[0,2/5]$，即 $-116964\,a^2-1003428\,a+421651\geq 0$：情形 b。

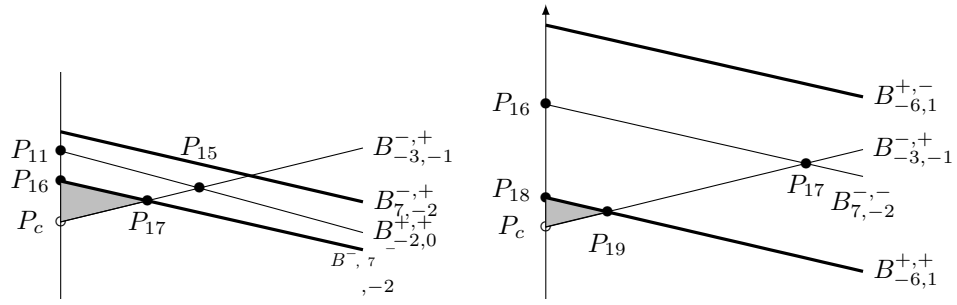

FIGURE 14. 情形 $m=19$：第7步（左），第8步（右）。

第8步：我们仍需覆盖 $P_cP_{17}P_{16}$。由于 P_c 的覆盖能力较弱，我们必须开始一个繁琐的过程来覆盖该区域。每一步都会留下一个较小的区域需要覆盖。这个过程在第7步时就已经开始。我们选择 $(-6,1)$，以至少覆盖 P_{16} 和 P_{17}，见图 14，这会产生两个点

$$P_{18}=B^{++}_{-6,1}\cap\{x=0\}=\left(0,-1+\frac{\sqrt{5986}}{57}\approx 0.3574\right),$$

$$P_{19}=B^{++}_{-6,1}\cap B^{-+}_{-3,-1}=\left(9/2-\frac{\sqrt{813179}}{201}\approx 0.0136,\frac{\sqrt{813179}}{2546}\approx 0.3542\right).$$

我们必须证明

$$B^{+-}_{-6,1} \geq B^{--}_{7,-2} \text{ for } a \in [0,2/5], \text{i.e.}, 2\,a^2+2\,a+85 \geq 0 : \text{case -;}$$

$B^{--}_{7,\,-2} \geq B^{++}_{-6,\,1}$对于 $a \in [0,2/5]$，即 $-58482\,a^2+697338\,a+2892295 \geq 0$： 情形 b。

第 9 步：我们计算

C[18]={[-321, -74], [-19, 4], [-6, 1], [6, 1], [19, 4],[321, -74]} C[19]={[-430, -99], [-19, 4], [-6, 1], [-3, -1], [321, -74], [991, 227]}

这表明 P_c 和 P_{19} 可由 (991, 227) 覆盖，而 P_{18} 和 P_{19}也可由 $\{(-19,4)、(321,-74)\}$ 中的任意一个覆盖。我们选择较大的 (991, 227) 和较小的 $(-19,4)$，得到图 15。我们得到三个新点

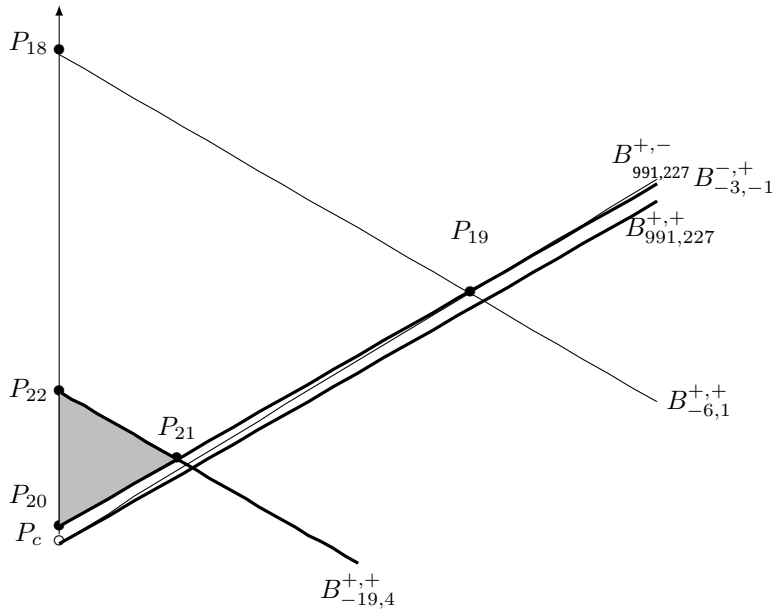

FIGURE 15. 情形 $m = 19$：第 9 步。

$$P_{20} = B^{+-}_{991,227} \cap \{x=0\} = \left(0, -227 + \frac{11\sqrt{1387901}}{57} \approx 0.3511\right),$$

第一部分中，以及

$$P_{21} = B^{++}_{-19,4} \cap B^{+-}_{991,227} = \left(-\frac{6253815094}{12867579} + \frac{\sqrt{156443316403988655691}}{25735158} \approx 0.0039\,,\right.$$

$$\left. -\frac{2972486569}{25735158} + \frac{505\sqrt{3145917199299979}}{244484001} \approx 0.3520\right),$$

$$P_{22} = B^{++}_{-19,4} \cap \{x=0\} = \left(0, -4 + \frac{\sqrt{61561}}{57} \approx 0.3529\right)$$

第二部分中。首先，我们必须证明

$$B^{+-}_{991,227} \geq B^{-+}_{-3,-1} \text{ for } a \in [0, x(P_{19})], \text{i.e.},$$

$$-29241\,a^2 - 29060082\,a + 480767 \geq 0 : \text{case b};$$

$$B^{-+}_{-3,-1} \geq B^{++}_{991,227} \text{ for } a \in [0, x(P_{19})], \text{i.e.}, a^2 + 988\,a \geq 0 : \text{case } a_2.$$

其次，我们需要

$B^{+-}_{-19,\ 4} \geq B^{++}_{-6,\ 1}$ 对于 $a \in [0, 2/5]$，即 $-58482\,a^2 + 706230\,a + 2838943 \geq 0$：情形 b；

$$B^{++}_{-6,1} \geq B^{++}_{-19,4} \text{ for } a \in [0, 2/5], \text{i.e.}, 2\,a^2 - 50\,a + 57 \geq 0 : \text{case } a_1.$$

步骤 10：剩下的就是覆盖 $\overline{P_{22}P_{20}}P_{20}P_{21}P_{22}$。我们用 $(-80, 18)$ 覆盖数对 (P_{21}, P_{22})，然后用 $(-430, -99)$ 覆盖 (P_{20}, P_{24})，得到图 16。

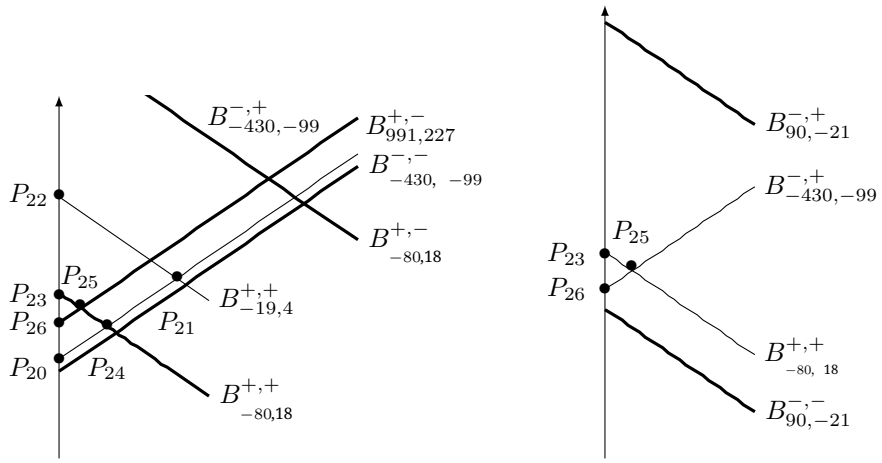

FIGURE 16. 情况 $m = 19$：步骤 10（左），步骤 11（右）。

我们得到四个新的点

$$P_{23} = B^{++}_{-80,18} \cap \{x = 0\} = \left(0, -18 + \frac{\sqrt{1094230}}{57} \approx 0.3518\right),$$

$$P_{24} = B^{++}_{-80,18} \cap B^{+-}_{991,227} = \left(-\frac{2744379489}{6024938} + \frac{11\sqrt{13966378024053079}}{2853918} \approx 0.001582,\right.$$

$$\left. -\frac{349606825}{2853918} + \frac{119\sqrt{13966378024053079}}{114473822} \approx 0.351470\right),$$

$$P_{25} = B^{-+}_{-430,-99} \cap B^{++}_{-80,18} = \left(255 - \frac{39\sqrt{3237343002931}}{275182} \approx 0.0007,\right.$$

$$\left. \frac{81}{2} - \frac{175\sqrt{3237343002931}}{7842687} \approx 0.3517\right),$$

$$P_{26} = B^{-+}_{-430,-99} \cap \{x = 0\} = \left(0, 99 - \frac{\sqrt{31617730}}{57} \approx 0.3515\right).$$

首先，我们需要证明

$$B^{+-}_{-80,18} \geq B^{++}_{-19,4} \text{ for } a \in [0, 2/5], \text{i.e.,}$$

$$-350892\,a^2 + 20552148\,a + 169237849 \geq 0 : \text{case b;}$$

$B^{++}_{-19,\ 4} \geq B^{++}_{-80,\ 18}$ 对于 $a \in [0, 2/5]$，即 $108\,a^2 - 10692\,a + 30799 \geq 0$: 情形 a_1.第二:

$$B^{-+}_{-430,-99} \geq B^{+-}_{991,227} \text{ for } a \in [0, 2/5], \text{i.e.,}$$

$$-350892\,a^2 + 133617348\,a + 242222193409 \geq 0 : \text{case b;}$$

$B^{+-}_{991,\ 227} \geq B^{--}_{-430,\ -99}$ 对于 $a \in [0, 2/5]$，即 $108\,a^2 + 60588\,a + 26245559 \geq 0$: 情形 -。

步骤 11：最后一步（！）是覆盖剩余的三个点 P_{23}, P_{26}, P_{25}。结果表明

C[23]={[-90,-21]，[-80，18]，[80，18]，[90，-21]} C[24]={[-90,-21]，[90，-21]} C[25]={[-90,-21]，[-80，18]，[90，-21]} Cinter={[-90, -21]，[90，-21]}

因此，我们可以使用 $(90, -21)$ 来完成这项任务。得到图 16。对于这种情况，我们最后的证明如下

$$B^{-+}_{90,-21} \geq B^{++}_{-80,18} \text{ for } a \in [0, 2/5], \text{i.e.,} 4\,a^2 + 40\,a + 86121 \geq 0 : \text{case -;}$$

$$B^{++}_{-80,18} \geq B^{--}_{90,-21} \text{ for } a \in [0, 2/5], \text{i.e.,}$$

$$-116964\,a^2 - 40704840\,a + 644319959 \geq 0 : \text{case b.}$$

最后

$$B^{-+}_{90,-21} \geq B^{-+}_{-430,-99} \text{ for } a \in [0, x(P_{25})], \text{i.e.,} 229\,a^2 - 77860\,a + 399 \geq 0 : \text{case } a_1;$$

$$B^{-+}_{-430,-99} \geq B^{--}_{90,-21} \text{ for } a \in [0, 2/5], \text{i.e.,}$$

$$-1131655941\,a^2 + 384755461740\,a + 153230834 \geq 0 : \text{case b.}$$

4. Computing the euclidean division

给定一个数 $\xi = a + b\omega$，其中 $0 \leq a, b \leq 1/2$（由两个二次数的中心除法得到），我们要找出两个有理整数 x 和 y，使得 $\gamma = x + y\omega$，且 $|\mathrm{Norm}(\xi - \gamma)| \leq M$。有两种可能的算法。第一种是从我们收集的区域中，找到一个覆盖区域，使其覆盖 (a, b)。从算法角度来看，这有些繁琐。第二种算法依次考察列表中的所有可能覆盖 (u, v)，并在 $|f_m(a + u, b + v)| \leq M$ 时立即停止。（可能有多个符合条件的对 (u, v)；对于我们的需求，一个就足够了，除非我们坚持要使范数尽可能小。）

5. Future work

首要任务是将这项工作推广到 $m \equiv 1 \bmod 4$的情形；这项工作已经开始，其中既突出了较易的情形（5、17、21、57），也有较难的情形，如13和29，参见即将发表的 [11]。我们可以尝试将我们的方法用于M_2-除法算法的情形，其中 M_2 为第二欧几里得极小值，又何尝不可用于某些已知情形下的其他 M_i。这可能会困难得多。在更一般的背景下，更高次数的 M_1-算法仍有发展空间，而对已知情形的研究工作可能更为困难。

References

[1] E. S. Barnes与H. P. F. Swinnerton-Dyer. 二元二次型的非齐次极小值. II. *Acta Math.*, 88:279–316, 1952年.[2] E. Berg. ¨论二次数域中欧几里得算法的存在性¨. *Kungl. Fysiografiska sällskapets i Lund förhandlingar*, 5(5):53–58, 1935年. [3] Perlas C. Caranay与Renate Scheidler. 一种高效的七次幂剩余符号算法. *Int. J. Number Theory*, 6(8):1831–1853, 2010年. [4] Jean-Paul Cerri. 单位秩严格大于 1 的数域的非齐次谱与欧几里得谱 . *J. Reine Angew. Math.*, 592:49–62, 2006年. [5] Jean-Paul Cerri. 全实数域的欧几里得极小值：算法确定. *Math. Comp.*, 76(259):1547–1575, 2007年. [6] P. G. Lejeune Dirichlet. *Vorlesungen über Zahlentheorie*. Vie weg, 不伦瑞克, 1893年. 编. R. Dedekind.[7] Marc Joye、Oleksandra Lapiha、Ky Nguyen与David Naccache. 十一次幂剩余符号. *J. Math. Cryptol.*, 15(1):111–122, 2021年. [8] Franz Lemmermeyer. 代数数域中的欧几里得算法. *Exposition. Math.*, 13 5 385 2004年 416, 1995年 ( ): – . 更新版本 , . [9] Pierre Lezowski. 代数数域欧几里得极小值的计算 . *Math.* , ( ): – *Comp.* 83 287 1397 1426, 2014 . [10] F. Morain. 欧几里得虚二次域的除法算法 . 预印本 , 2026 年 1 月 .[11] F. Morain. 范数欧几里得实二次域的除法算法——第二部分. 准备中, 2026年1月. [12] Alexander Oppenheim. 具有与不具有欧几里得算法的二次域. *Math. Ann.*, 109 1 349 352, 1934年 ( ): – . [13] Oskar Perron. 具有欧几里得算法的二次数域¨. *Math. Ann.*, 107 1 489 495, 1933年 ( ): – .[14] Robert Remak. ¨论实二次数域中的欧几里得算法¨. *Jahresbericht der Deutschen Mathematiker-Vereinigung*, 44:238–250, 1934年.[15] Renate Scheidler与Hugh C. Williams. 一种利用分圆域的公钥密码系统. *Des. Codes Cryptogr.*, 6(2):117–131, 1995年. [16] P. Varnavides. 非齐次二元二次型. I, II. *Nederl. Akad. Weten-* , , : – *sch. Proc.* 51 396 404, 470 481 = 10, 142 150, 164 175, 1948 – Indagationes Math. – – . 情形 Q(sqrt(2)). [17] P. Varnavides. 关于二次型 $x^2 - 7y^2$ *Proc. Roy. Soc. London Ser. A* 197 256 268, . , : – . 1949 [18] P. Varnavides. 型 $x^2 - 11y^2$的闵可夫斯基常数. *Bull. Soc. Math. Grèce*, 26:14– 23, 1952年.

Email address: morain@lix.polytechnique.fr