Euclidean Ideals in Imaginary Quadratic Fields

by

Hester Graves & Nick Ramsey

Talk Structure

1. Review Euclidean domains

2. Introduce Euclidean Ideals

3. Euclidean Ideals in Imaginary Quadratic Fields

Section 1

Definition Let R be a domain. If $\varphi : R \setminus 0 \longrightarrow W$, W a well-ordered set, is a function such that for all $a, b \in R$, $b \neq 0$, there exist some $q, r \in R$ for which

$$a = bq + r, \text{ where } \varphi(r) < \varphi(b) \text{ or } r = 0,$$

then we say φ is a *Euclidean algorithm* and R is a *Euclidean domain*.

Fact Every Euclidean domain is a PID

For the rest of the talk, we will assume all Euclidean algorithms are $\mathbb{N}$-valued, where $\mathbb{N}$ includes 0.

When people think of Euclidean domains and algorithms, they usually think of the ring of integers of a number field and the norm.

Ex. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right]$

Def. Let K be a number field. If the norm is a Euclidean algorithm for $\mathcal{O}_K$, we say $\mathcal{O}_K$ is *norm-Euclidean*.

Thm (Clark 1994) $\mathbb{Z}\left[\frac{1+\sqrt{69}}{2}\right]$ is a Euclidean domain, but it is not norm-Euclidean

Thm (Harper 2004) $\mathbb{Z}[\sqrt{14}]$ is Euclidean (but not norm-Euclidean)

Thm (Motzkin 1949) Let R be a domain. We define

$$A_0 := \{0 \cup R^\times\} \text{ and}$$

$$A_i := A_{i-1} \cup \{\beta \in R : A_{i-1} \twoheadrightarrow R/\beta\} \text{ for } i > 0.$$

We further define A to be $\bigcup_{i=0}^{\infty} A_i$.

$A = R \iff R$ has a $\mathbb{N}$-valued Euclidean algorithm.

Example $R = \mathbb{Z}$

$A_0 = 0, \pm 1$

$A_1 = 0, \pm 1, \pm 2, \pm 3$

$A_2 = 0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7$

Thm (Weinberger 1973) If K is a number field with $|\mathcal{O}_K^\times| = \infty$ and one assumes the generalized Riemann hypothesis, then

$\mathcal{O}_K$ is a PID

$\Updownarrow$

$\mathcal{O}_K$ is a Euclidean domain.

Note this theorem refers to K such that $|\mathcal{O}_K^*| = \infty$, so it does not apply to imaginary quadratic fields.

Fact: If K is an imaginary quadratic field and $\mathcal{O}_K$ is Euclidean, then K is $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, or $\mathbb{Q}(\sqrt{-11})$. In each of these cases, the ring of integers is norm-Euclidean

Section 2: Euclidean Ideals

Motivation for the Definition:

Let K be a number field. If $\mathcal{O}_K$ is norm-Euclidean, then for all $a, b \in \mathcal{O}_K$, $b \neq 0$, there exist some $q, r \in \mathcal{O}_K$ such that

$a = qb + r$, where $Nm(r) < Nm(b$

In other words, $Nm\left(\frac{a}{b} - q\right) = Nm\left(\frac{r}{b}\right) < 1$.

$\mathcal{O}_K$ is norm-Euclidean if for all x in K, there exists some y such that $Nm(x-y) < 1 = Nm(\mathcal{O}_K)$.

What if we replaced $\mathcal{O}_K$ by some ideal C?

Let R be a Dedekind domain.

Def $E := \{\text{ideals } I : R \subset I\}$

Def Suppose that C is an ideal in R and that $\psi : E \longrightarrow W$, W a well-ordered set. We say ψ is a *Euclidean algorithm for* C if for all $I \in E$ and all $x \in IC \setminus C$, there exists some $y \in C$ such that

$$\psi((x+y)^{-1} I C) < \psi(I).$$

If such a ψ exists, we say that C is a *Euclidean Ideal*.

Note that if

① if C is a Euclidean ideal, then so is every J st. $[J] = [C]$.

② the domain R is Euclidean $\iff$ $[R]$ is Euclidean

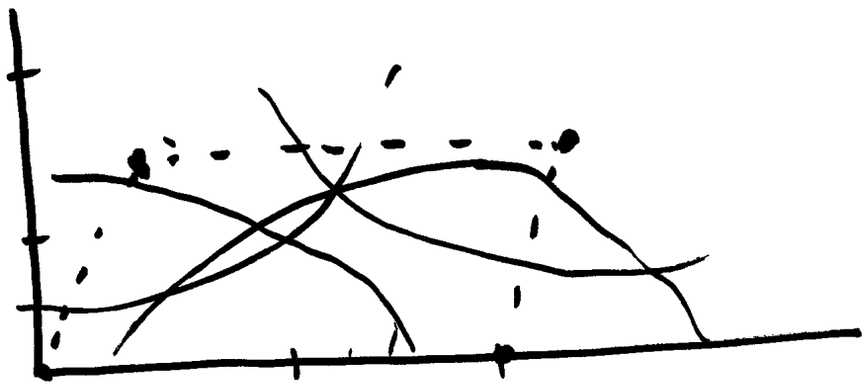
③ Fact: If C is Euclidean, then $Cl_R = \langle [C] \rangle$

④ If $\psi(I) = Nm(I^{-1})$, then this reduces to $Nm(x+y) < Nm(C)$

Example:

Let $K = \mathbb{Q}(\sqrt{-5})$

$C = (2, \frac{1+\sqrt{-5}}{2})$



So given any point x in $\mathbb{Q}(\sqrt{5})$, it is within $\sqrt{2}$ of a point in C.

Theorem (Lenstra 1979)

Suppose that K is a number field, $|\mathcal{O}_K^\times| = \infty$, and that C is an ideal in $\mathcal{O}_K$, $C \neq 0$. If one assumes the generalized Riemann hypothesis, then

$$Cl_K = \langle [C] \rangle \iff C \text{ is a Euclidean ideal.}$$

Note that this does not apply to imaginary quadratic fields.

Theorem (2009)

Let R be a Dedekind domain and let C be an ideal of R, $C \neq 0$.

We define $A_{0,C} := \{R\}$

$$A_{i,C} := A_{i-1,C} \cup \{I \in E : \forall\, x \in IC \setminus C,\ \exists\, y \in C \text{ s.t. } (x+y)^{-1} IC \in A_{i-1,C}\}$$

for $i > 0$

and $A_C := \bigcup_{i=0}^{\infty} A_{i,C}$.

The ideal C has a Euclidean algorithm mapping to $\mathbb{N} \iff E \in A_C = E$.

Note that $I \in A_{1,C} \setminus A_{0,C}$

$\Rightarrow [I^{-1}] = [C]$.

Section 3:

We know that $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$ have Euclidean ideals since their rings of integers are norm-Euclidean.

All other imaginary quadratic fields K ~~satisfy~~ have only two units (± 1) in $\mathcal{O}_K$. $\Rightarrow$

$$A_{0,C} = \{\mathcal{O}_K\}$$

$$A_{1,C} = \left\{ I \in E : \begin{array}{l} \forall\, x \in IC \setminus C, \exists \\ y \in C \text{ s.t.} \\ (x+y)^{-1} IC = \mathcal{O}_K \end{array} \right\}$$

We know that $IC/C \cong R/I^{-1}$.

$\mathcal{O}_K$ has only 2 generators $\Rightarrow$ $\mathrm{Nm}(I^{-1}) = 2$ or 3 for $I \in A_{1,C} \setminus A_{0,C}$

Using this method and SAGE, we were able to determine whether or not K has a Euclidean ideal ——

unless $K = \mathbb{Q}(\sqrt{-23})$.

Back to the Drawing Board!

For the following, let K be an imaginary quadratic field and fix an embedding of $K \hookrightarrow \mathbb{C}$.

Let C be a non-zero fractional ideal of $\mathcal{O}_K$; the image of C forms a lattice.

Around each point in C, make an open disk of radius $\sqrt{Nm(C)}$. We shall call the union of these ~~points~~ disks U.

If U covers all of $\mathbb{C}$, then C is norm-Euclidean.

Lemma Let $\varepsilon > 0$. There exists some M such that for all $z \in K$ and all fractional ideals I, $Nm(I) > M$, there exists some $x \in I^{-1}$ such that $Nm(x - z) < \varepsilon$.

pf. Let $I_1, \ldots, I_k$ be representatives of the classes in Cl_K.

Each ideal I_i can be viewed as a lattice under the embedding. For each, there exists some M_i such that disks of radius $\sqrt{M_i}$ centered at the elements of I_i covers $\mathbb{C}$.

$\Rightarrow$ If $z \in K$, there exists some $x \in I_i$ such that $Nm(x - z) = |x - z| < M_i$.

Choose $M > \max_i \left(\frac{M_i \, Nm(I_i)}{\varepsilon} \right)$.

Let $z' \in K$ and let J be an ideal such that $Nm(J) > M$. $\Rightarrow \frac{1}{Nm(J)} < \frac{\varepsilon}{M \, Nm(I_i)}$ for all i

We can write $J = gI_i$ for some $g \in K^*$. $\Rightarrow Nm(g^{-1}) = \frac{Nm(I_i)}{Nm(J)}$

There exists some $x' \in I_i^{-1}$ such that

$$Nm(x' - gz') < M_i$$

$$Nm(g^{-1}x' - z') = Nm(g^{-1}) \, Nm(x' - gz')$$

$$< \frac{Nm(I_i)}{Nm(J)} \, M_i < \frac{\cancel{Nm(I_i)} \cdot \varepsilon}{M \, \cancel{Nm(I_i)}} \, M_i$$

$$< \varepsilon .$$

Prop If the complement of U contains a non-empty open set, then U is not a Euclidean ideal.

Proof.

Since K is dense in $\mathbb{C}$, there exists some $z \in K$ such that $B_{\sqrt{\varepsilon}}(z)$ is contained in the complement of U.

Let M be as in our Lemma for K & ε.

Suppose $I_0 \in E$ and $Nm(I_0^{-1}C^{-1}) > M$.

By our Lemma, there exists $x \in I_0 C$ such that $Nm(x - z) < \varepsilon$, so

$$|x - z| < \sqrt{\varepsilon}.$$

Suppose, leading to $\Rightarrow\Leftarrow$, that $\psi : E \longrightarrow \mathbb{N}$ is a Euclidean algorithm for C, so $A_C = \bigcup_{i=0}^{\infty} A_{i,C} = E$.

Since $x \in I_0 C \setminus C$ and $I_0 \in E = A$, $\exists\ y \in C$ such that

$$\psi((x+y)^{-1} I_0 C) < \psi(I_0).$$

$I_1 := (x+y)^{-1} I_0 C$

$I_1 \in E$ and $\psi(I_1) < \psi(I_0)$

$$Nm(I_1) = \frac{Nm(I_0)Nm(C)}{Nm(x+y)} = \frac{Nm(I_0)Nm(C)}{|x+y|^2}$$

$$\leq Nm(I_0)$$

Iterate to get a sequence of ideals $I_0, I_1, I_2, \ldots\ldots$

such that $Nm(I_0) \geq Nm(I_1) \geq \ldots\ldots$

and $\psi(I_0) > \psi(I_1) > \psi(I_2) > \ldots$

$\Rightarrow\Leftarrow$ Since $\mathbb{N}$ is well-ordered

□

Putting It All Together

If K is imaginary & quadratics $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, then $A_{1,c}$ contains an inverse of a prime $\mathfrak{p}$ of norm 2 or 3.

And $[\mathfrak{p}] = [C]$.

So, if K has a Euclidean ideal, then $\mathfrak{p}$ is Euclidean.

So let us look at such ideals in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-D})$

Case 1:

$Nm(\mathfrak{p}) = 2$

(a) 2 ramifies, $D \equiv 1 \pmod 4$

$\mathfrak{p} = (2, \sqrt{-D} + 1)$

$D = 1 \quad , \quad 5 \quad , \quad 13$

(b) 2 ramifies, $D \equiv 2 \pmod 4$

$\mathfrak{p} = (2, \sqrt{-D})$

$D = 2 \quad , \quad$ ~~6~~.

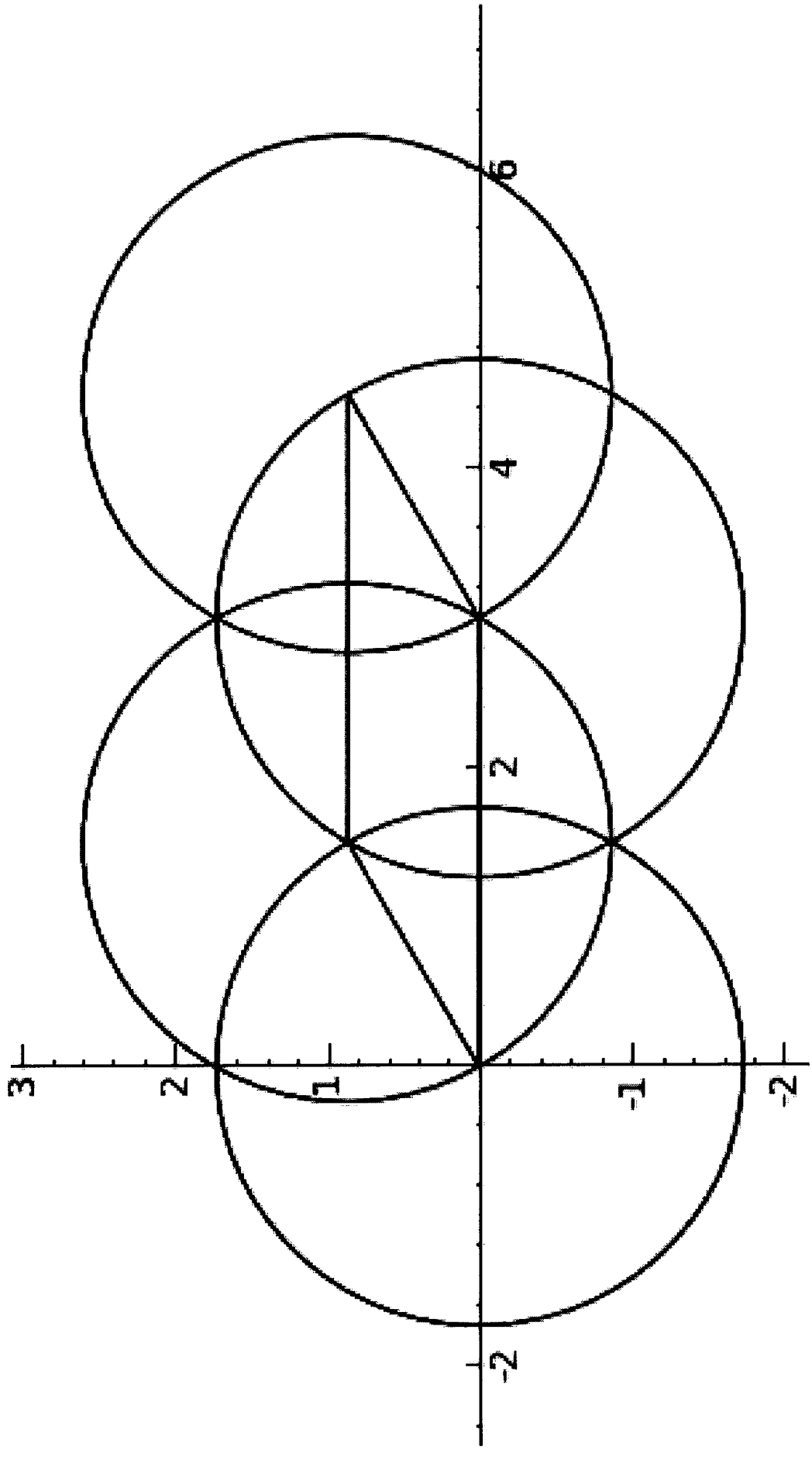
(c) 2 splits, $D \equiv 7 \pmod 8$

$\mathfrak{p} = (2, \frac{1+\sqrt{-D}}{2})$ or $(2, -\frac{1+\sqrt{-D}}{2})$

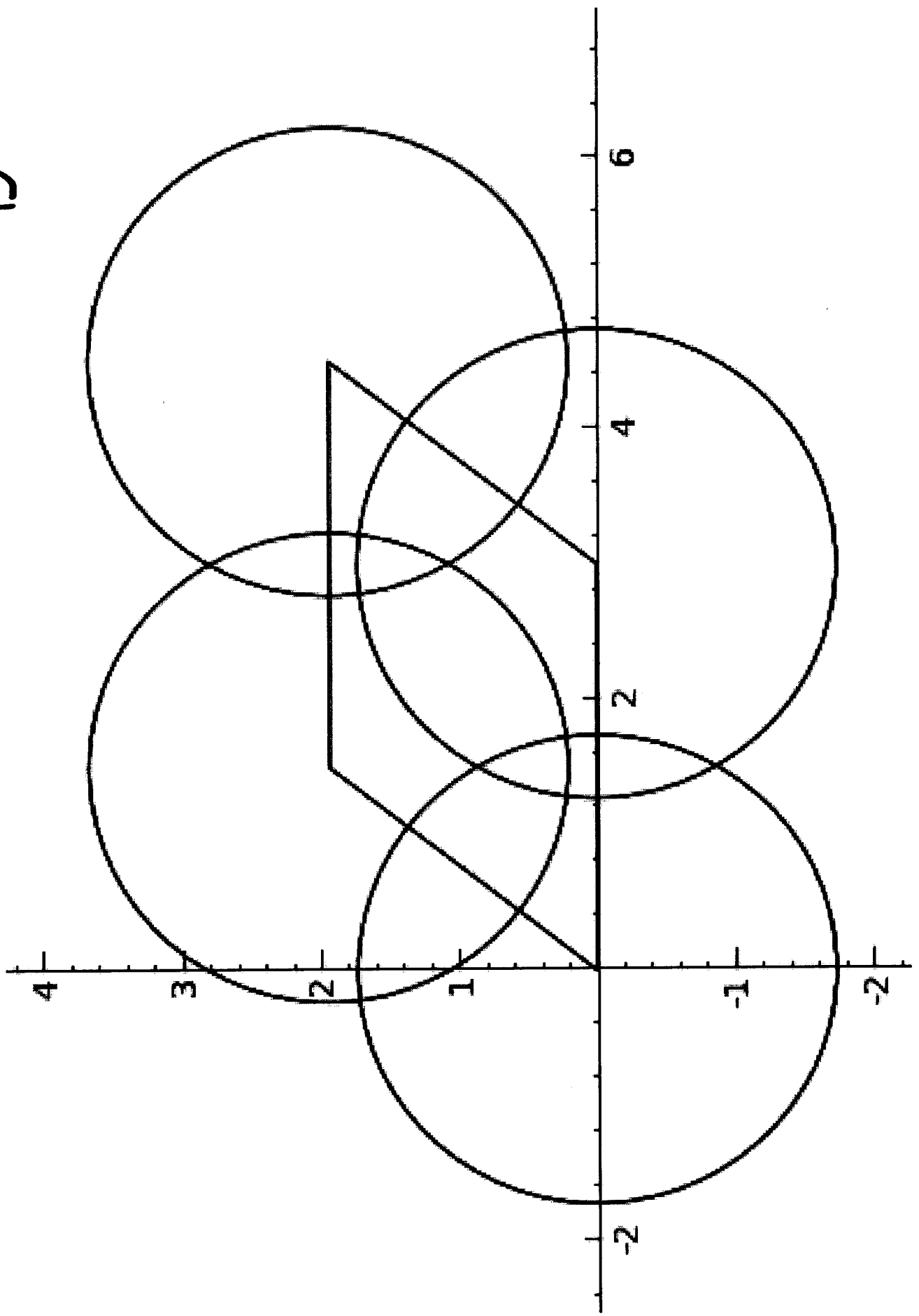
↑ only need to examine the first

$D = 7, 15, 23$

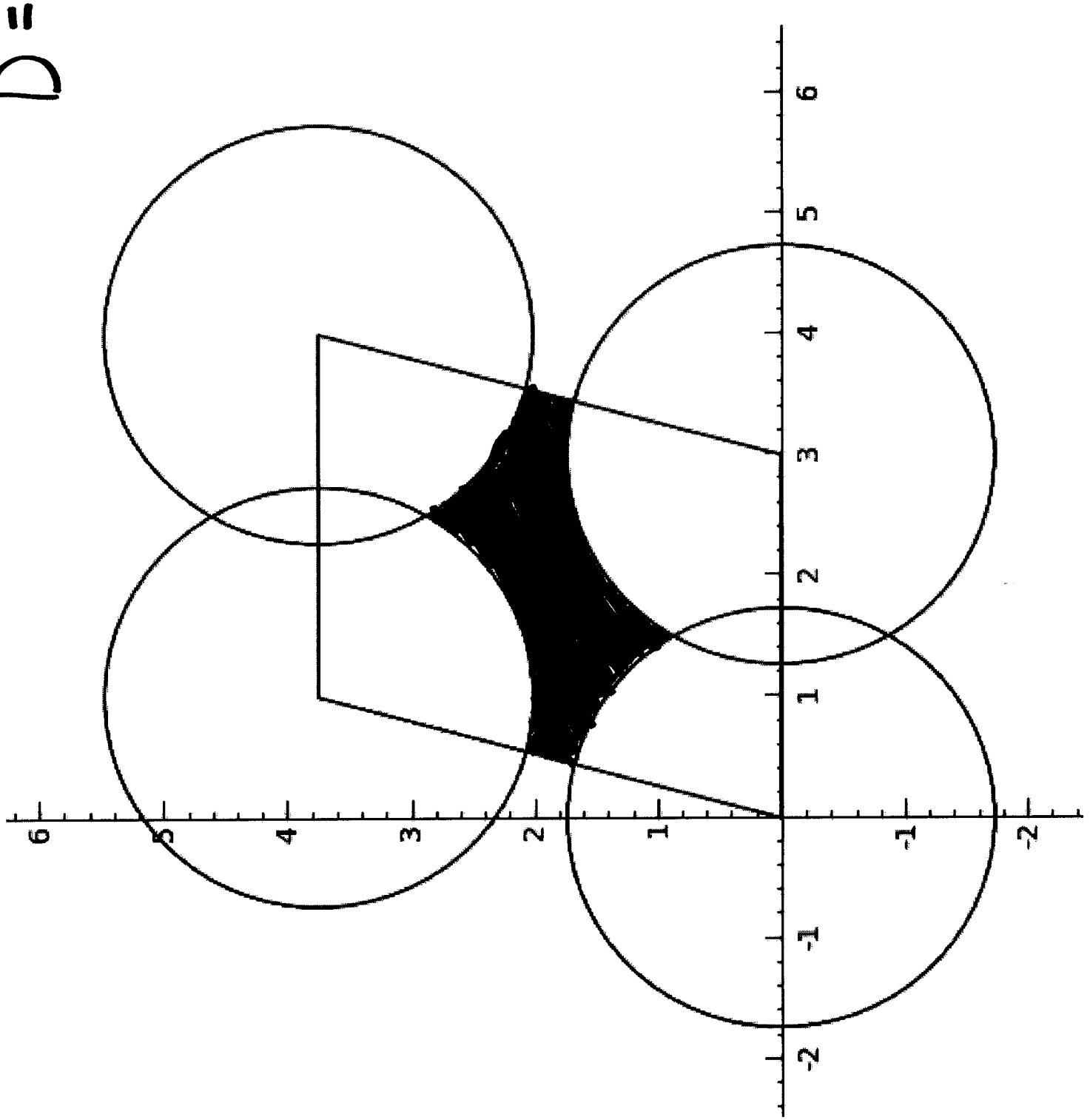
D=1



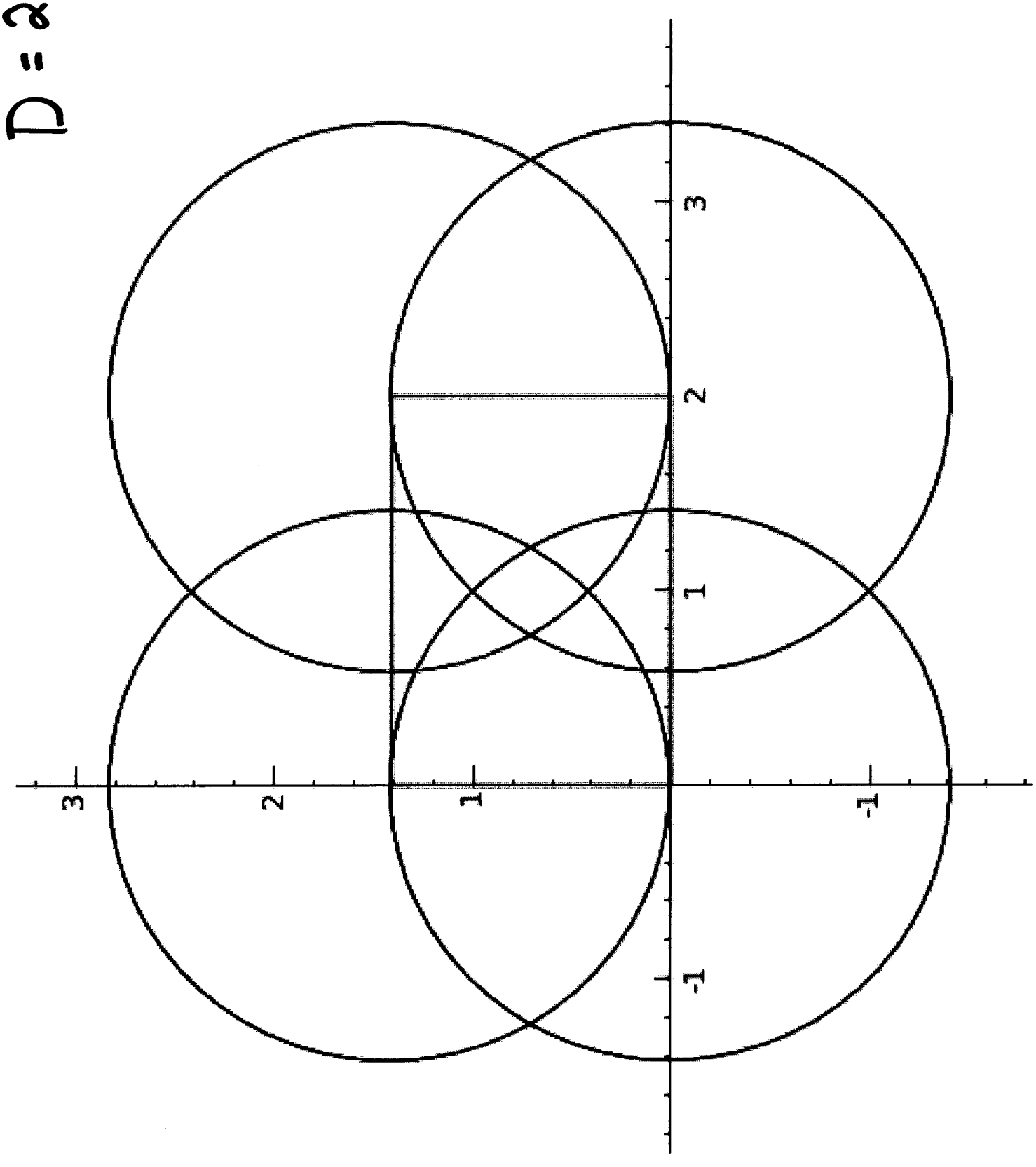
D = 5



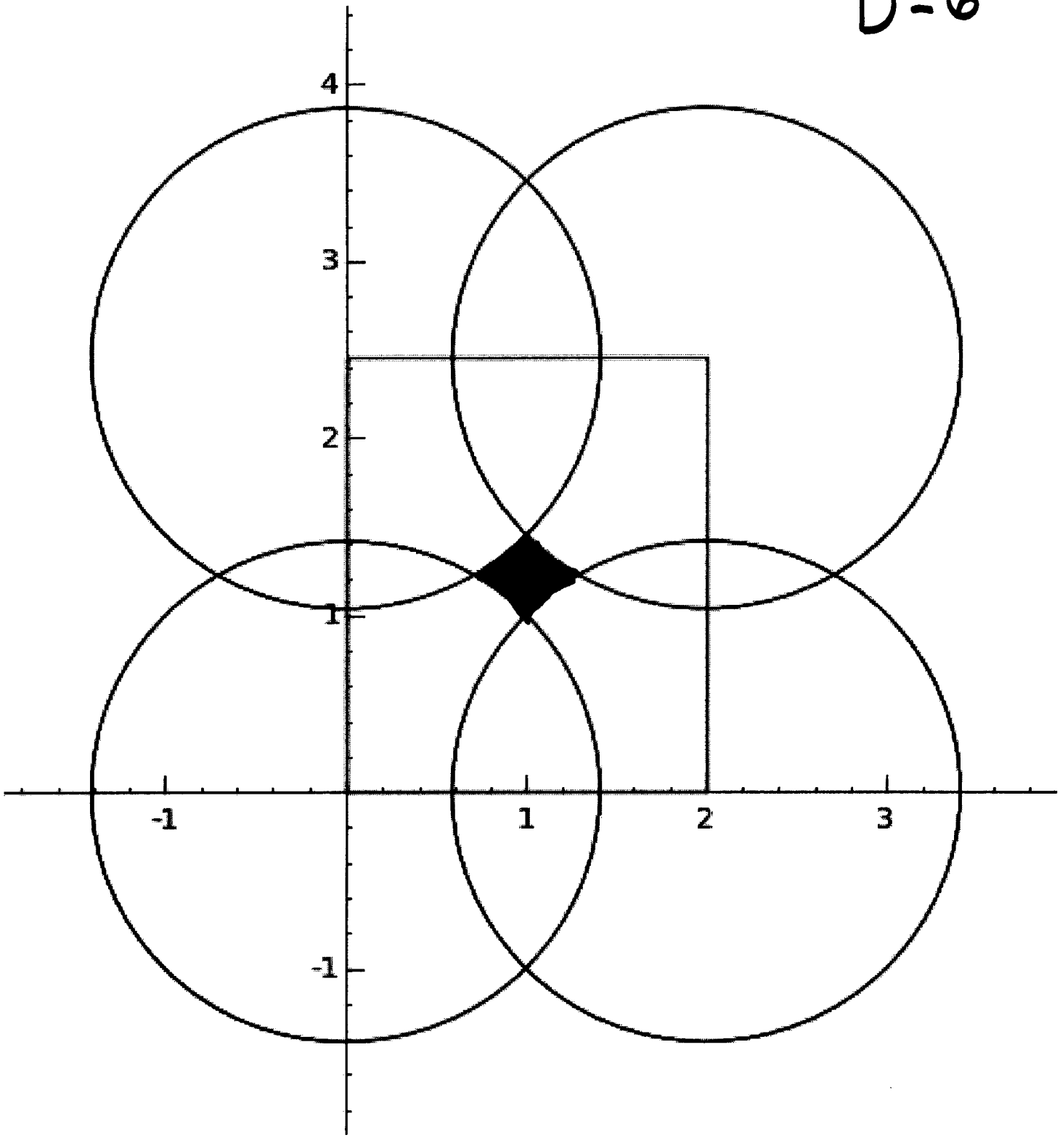
D = 13



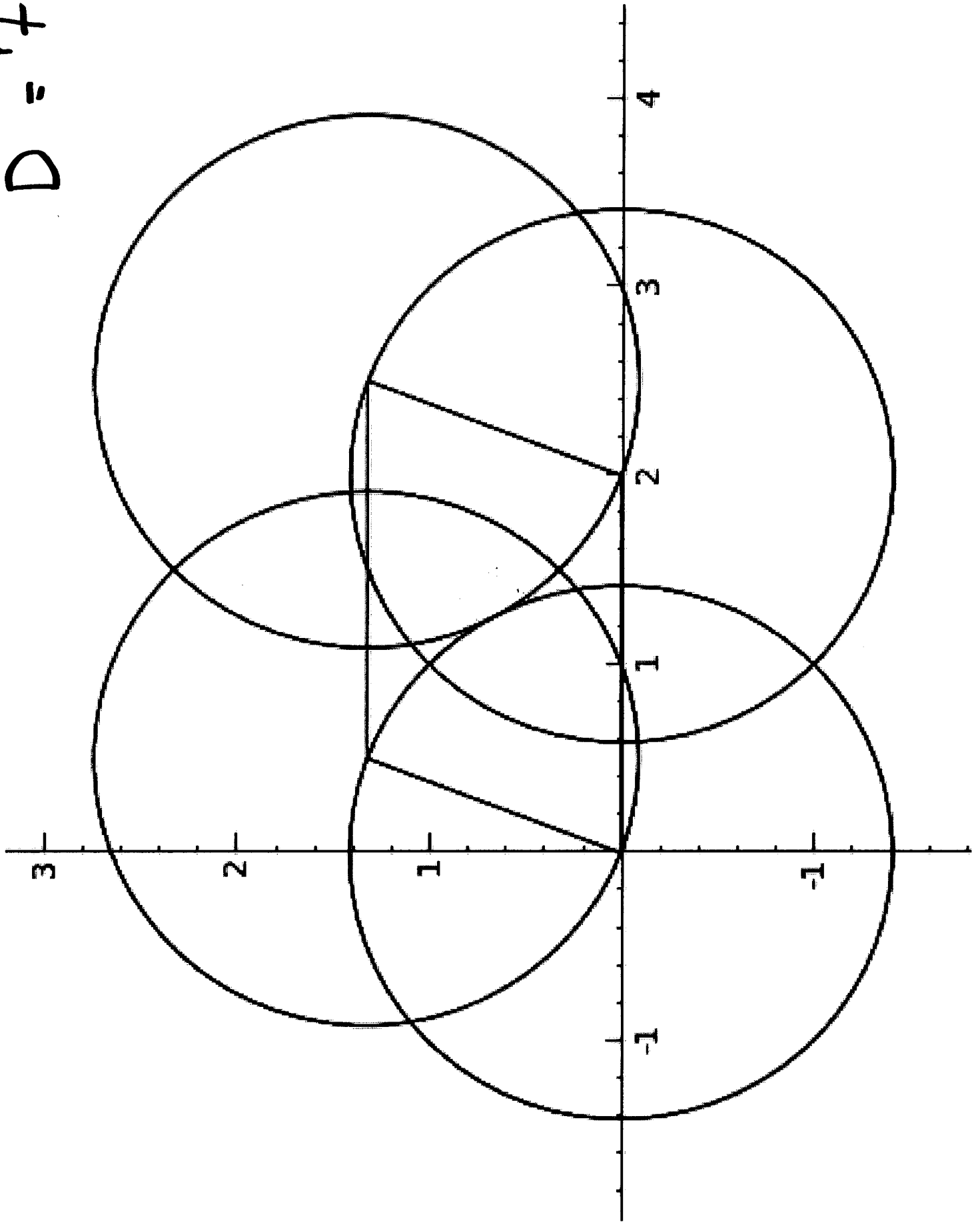
D = 2



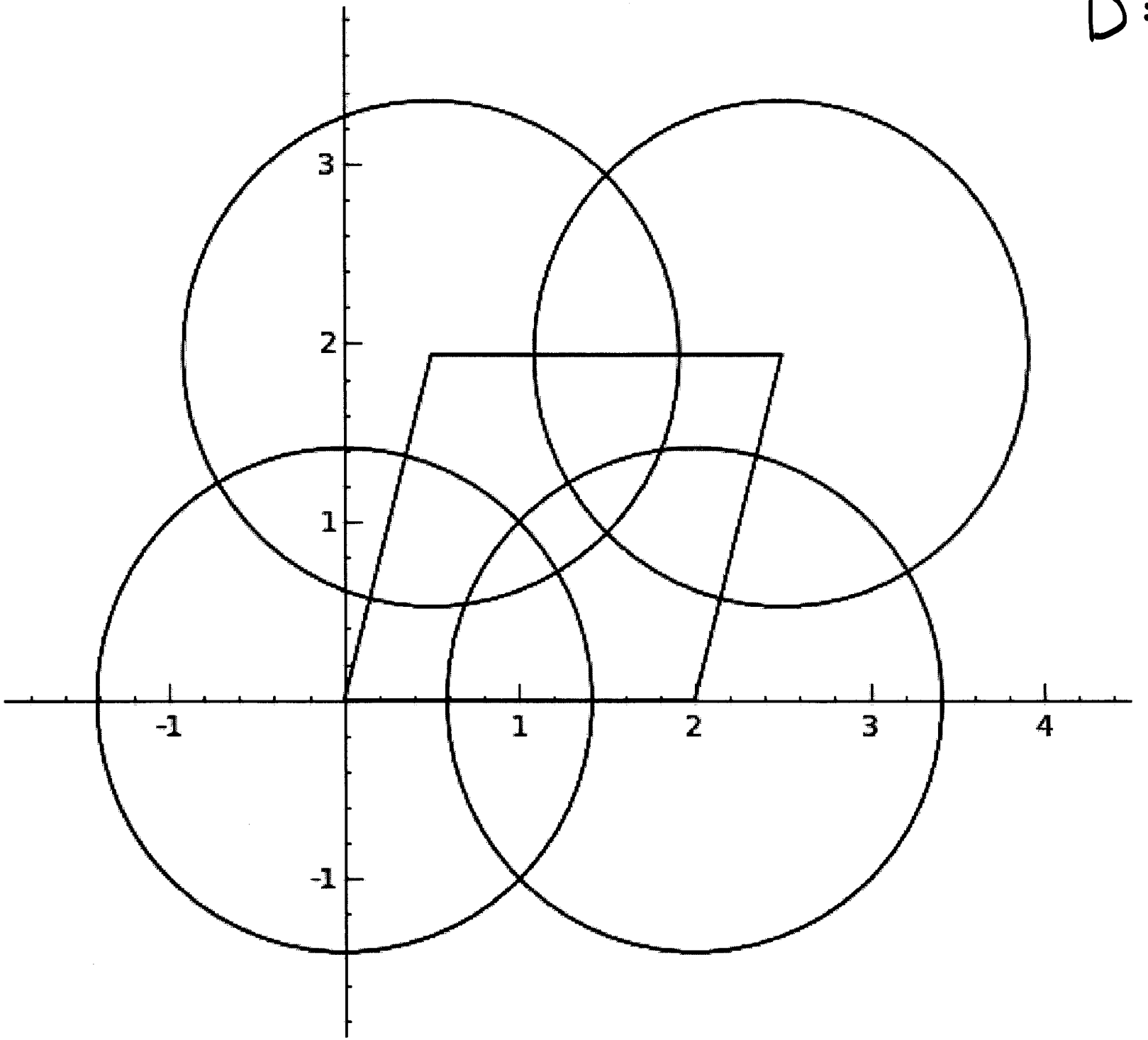
D=6



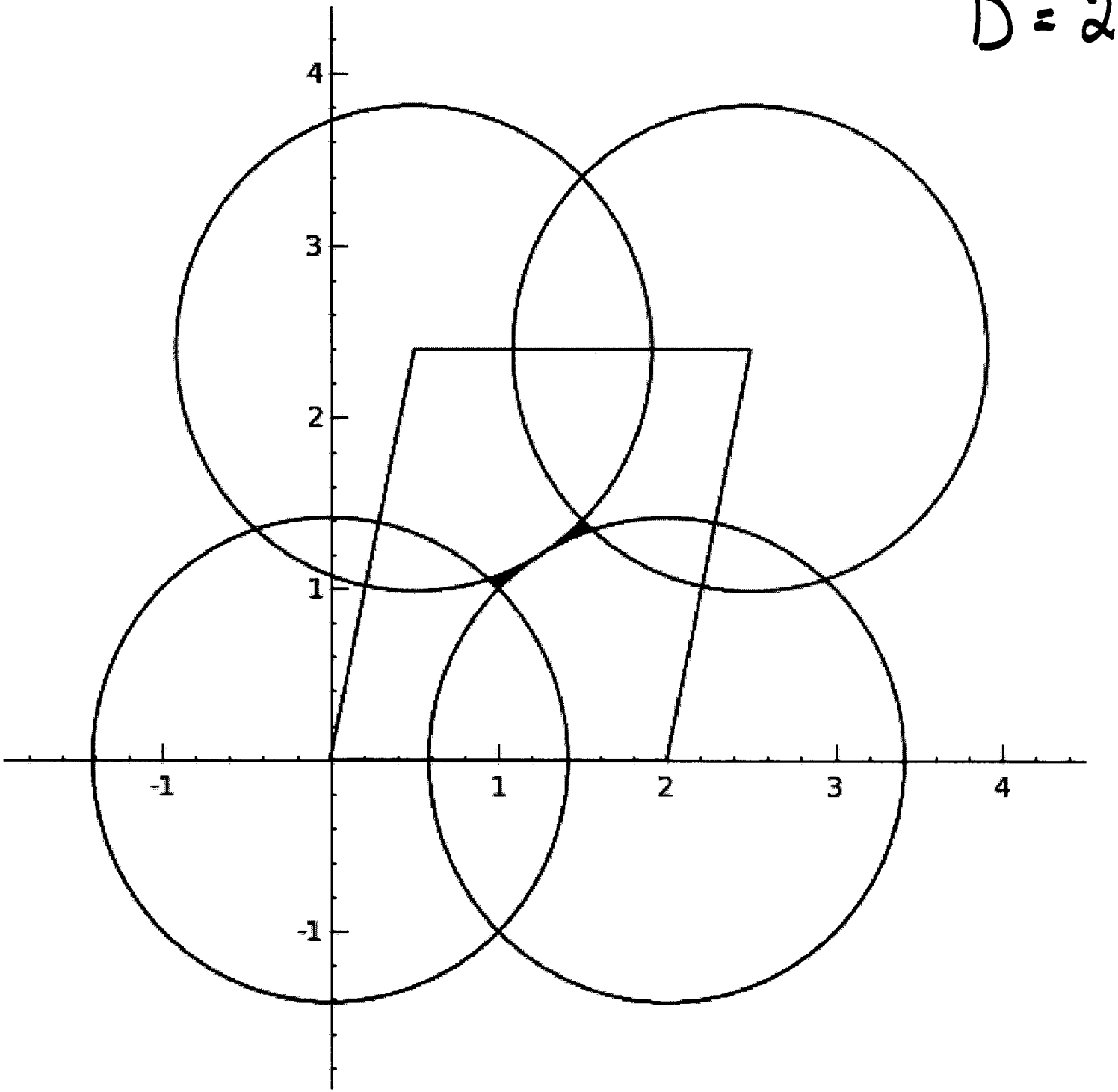
D - 4



D = 15



D = 23



Case 2:

$Nm(\mathfrak{p}) = 3$

(a) 3 ramifies, $D \equiv 1, 2 \pmod 4$

$\mathfrak{p} = (3, \sqrt{-D})$

$D = 6$

(b) 3 ramifies, $D \equiv 3 \pmod 4$

$\mathfrak{p} = (3, \frac{3+\sqrt{-D}}{2})$

$D = 3, 15, 39$

(c) 3 split, $D \equiv 1, 2 \pmod 4$

$\mathfrak{p} = (3, 1+\sqrt{-D})$ or $(3, 1-\sqrt{-D})$

↑ only need to consider one

$D = 2, 5, 14$

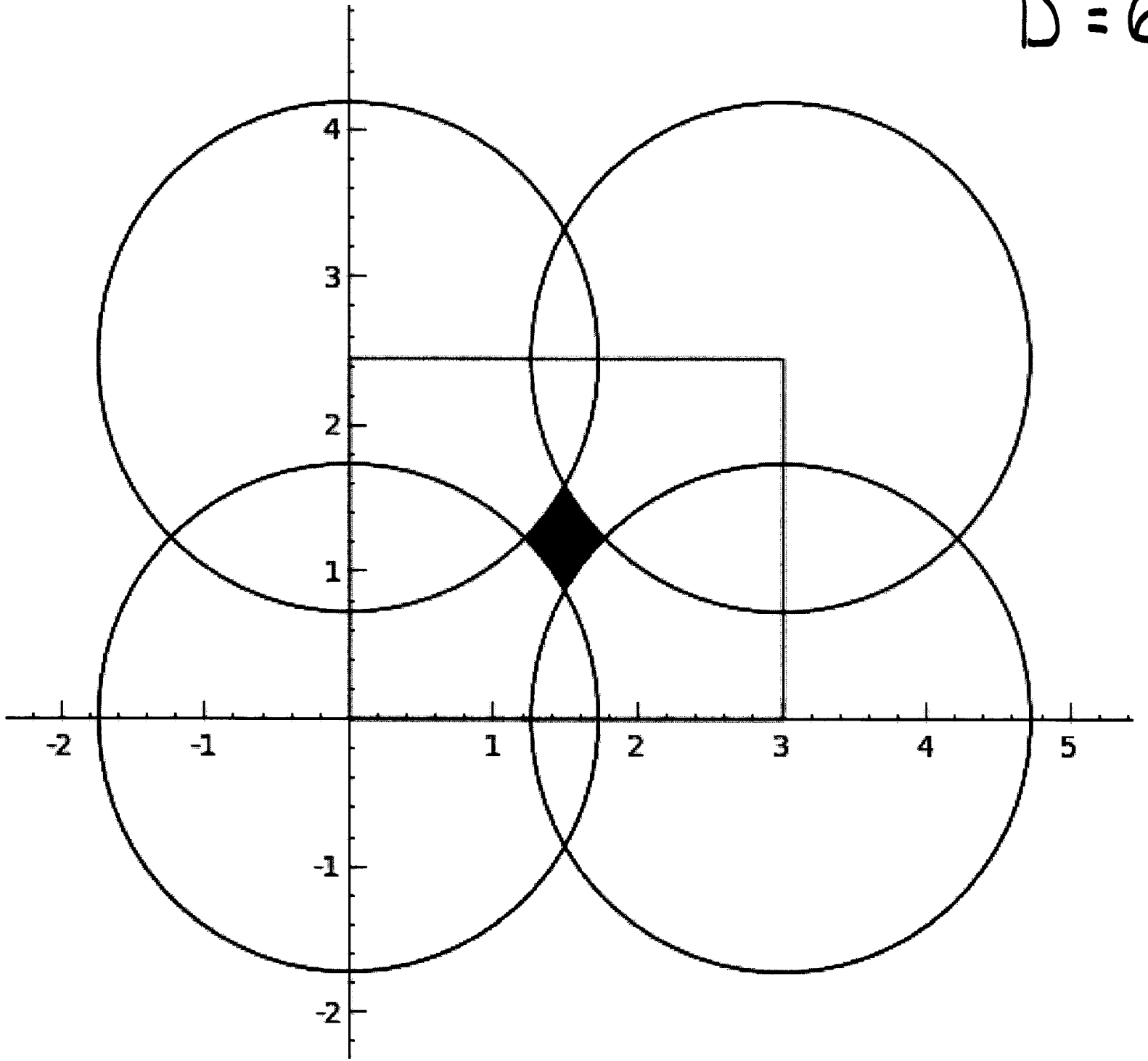
(d) 3 split, $D \equiv 3 \pmod 4$

$\mathfrak{p} = (3, \frac{1+\sqrt{-D}}{2})$ or $(3, \frac{1-\sqrt{-D}}{2})$

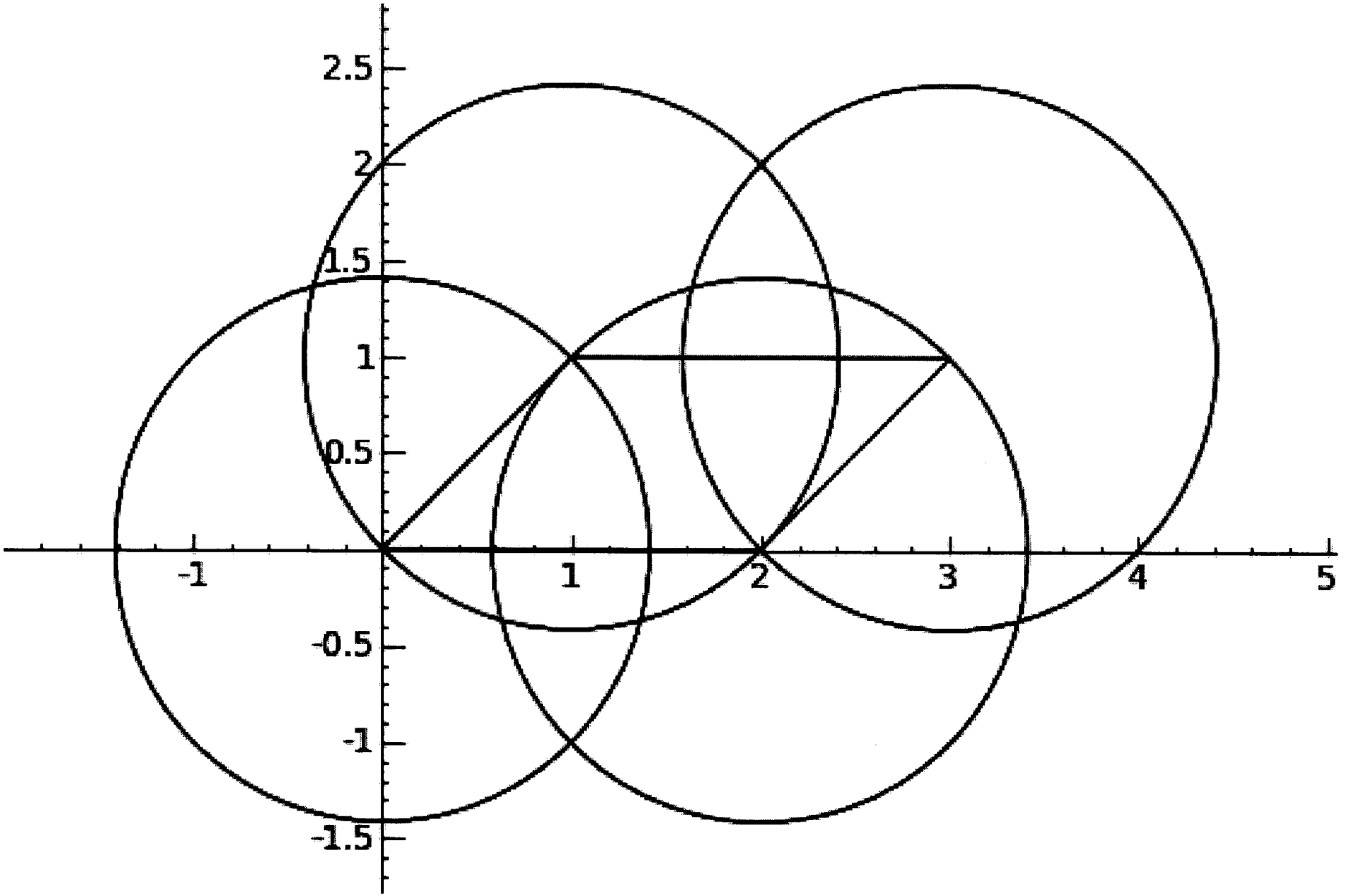
↑ only need to consider one

$D = 11, 23$

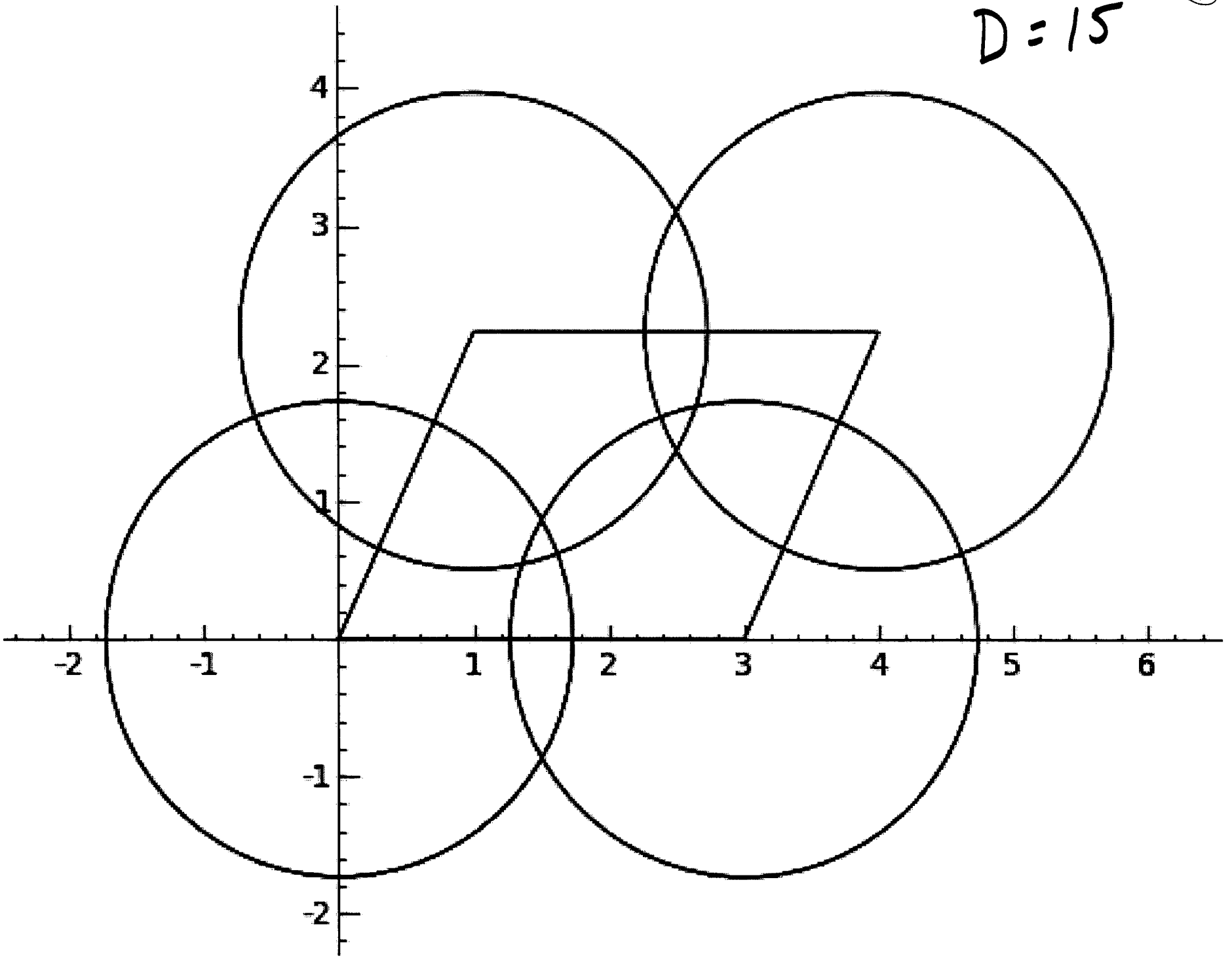
D = 6



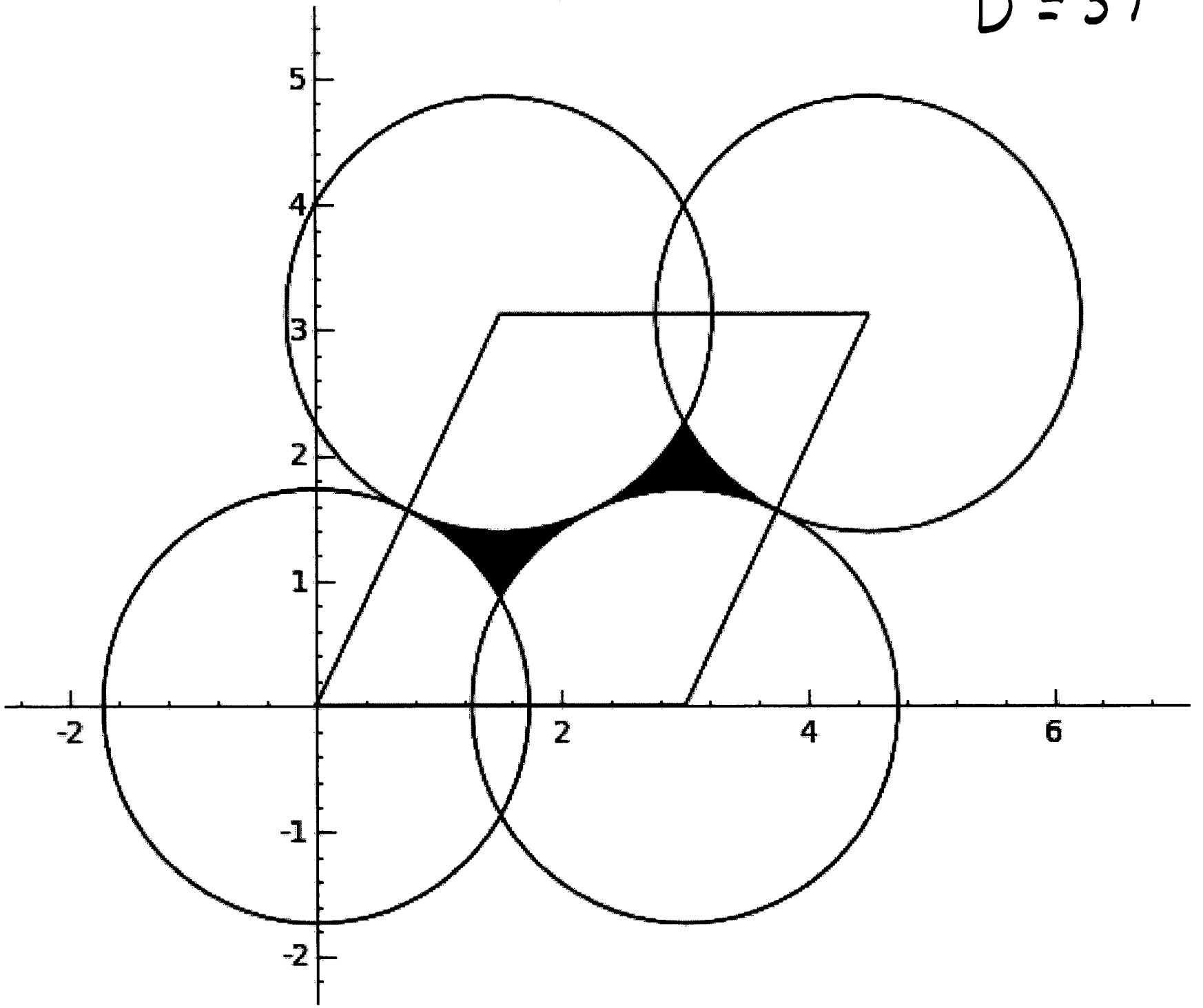
D = 3



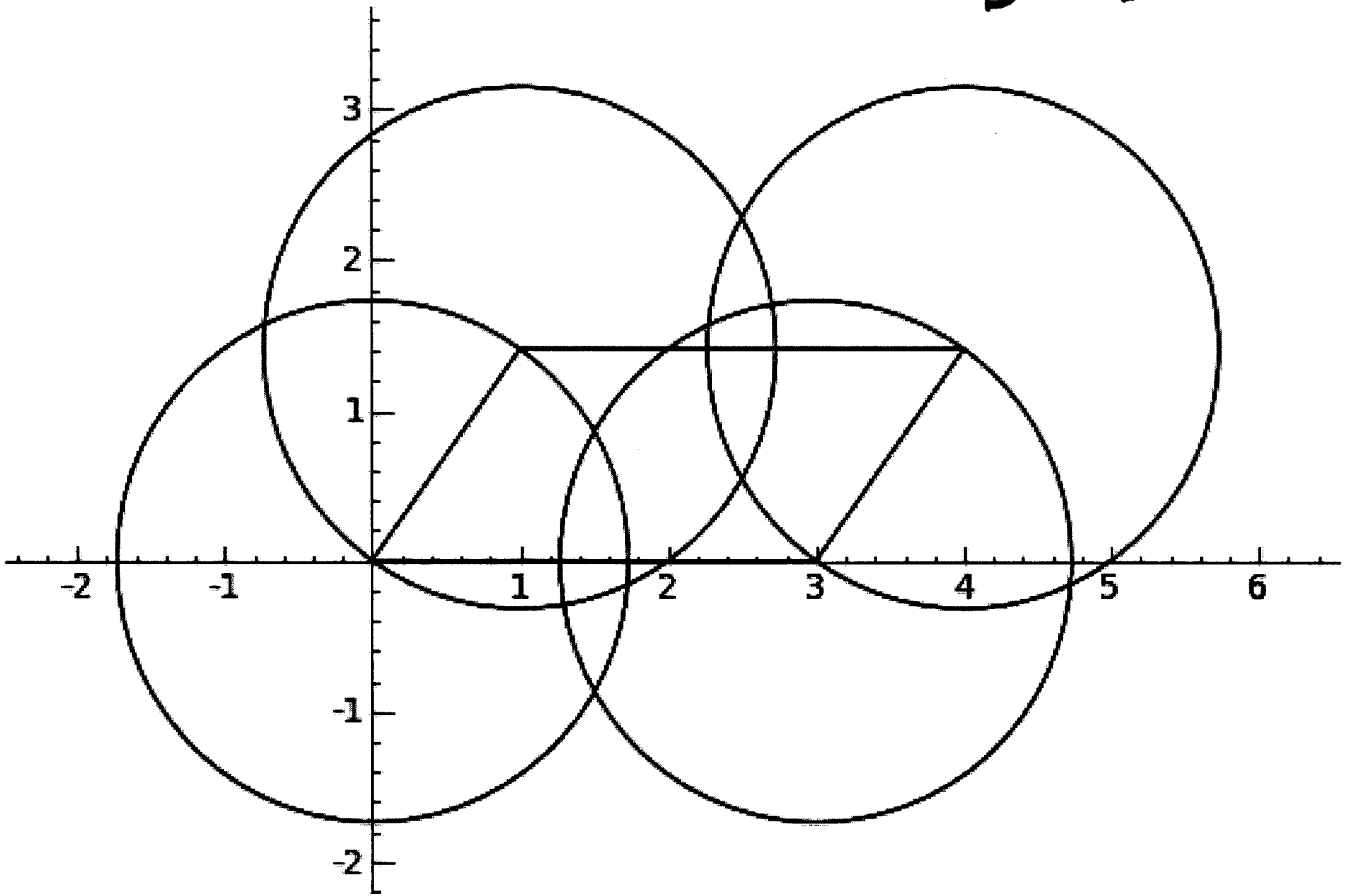
D = 15



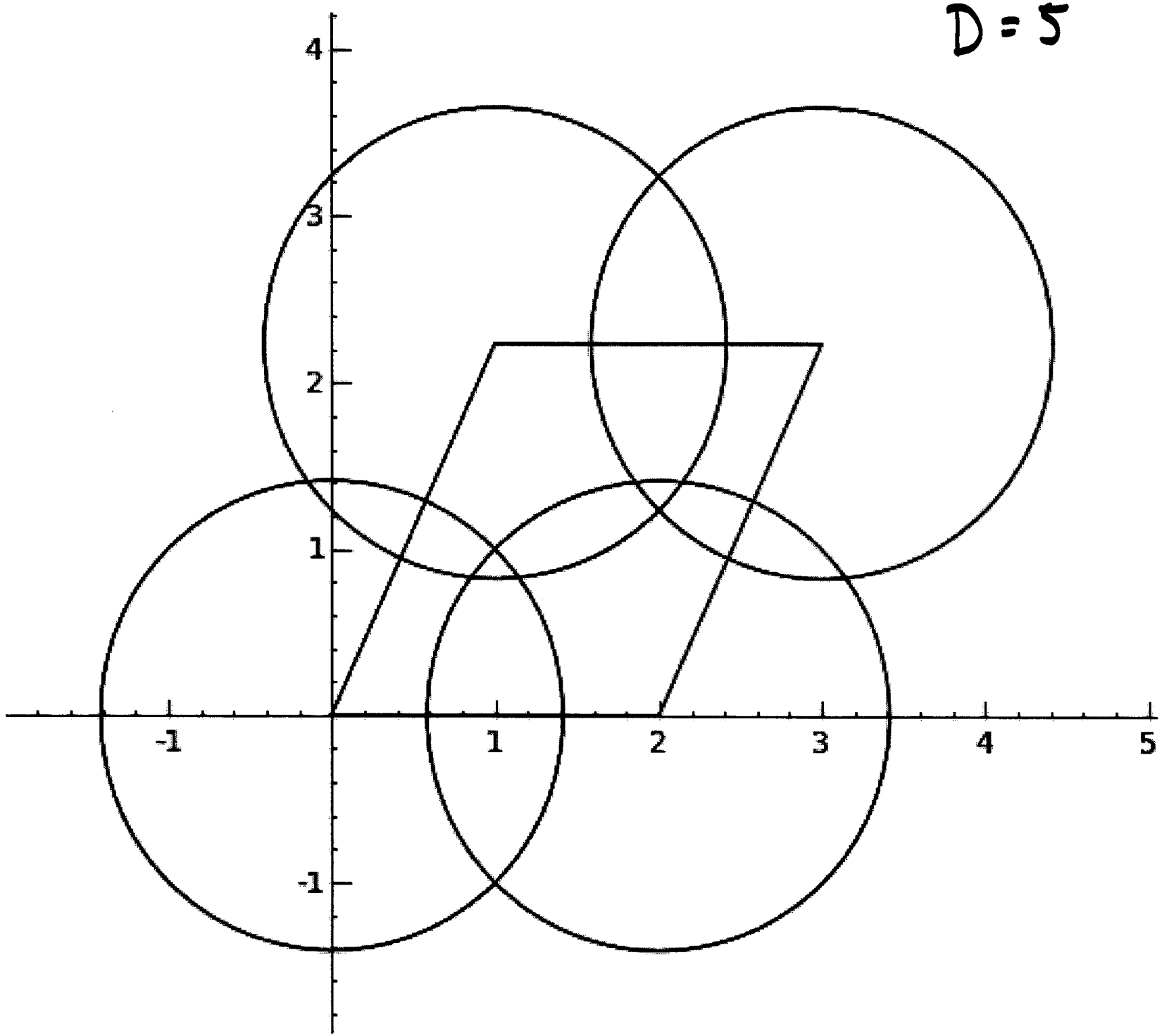
D = 39



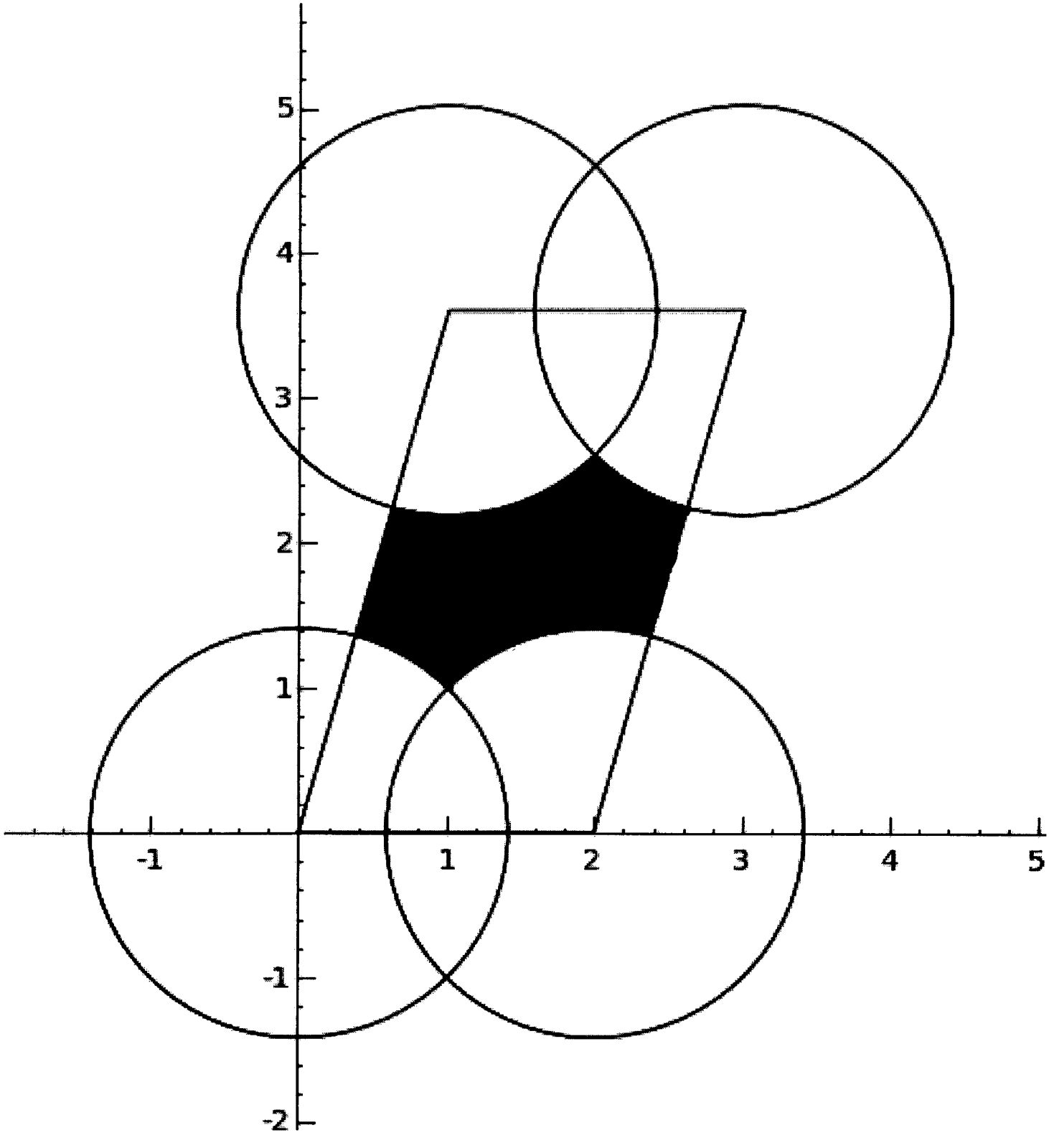
D = 2



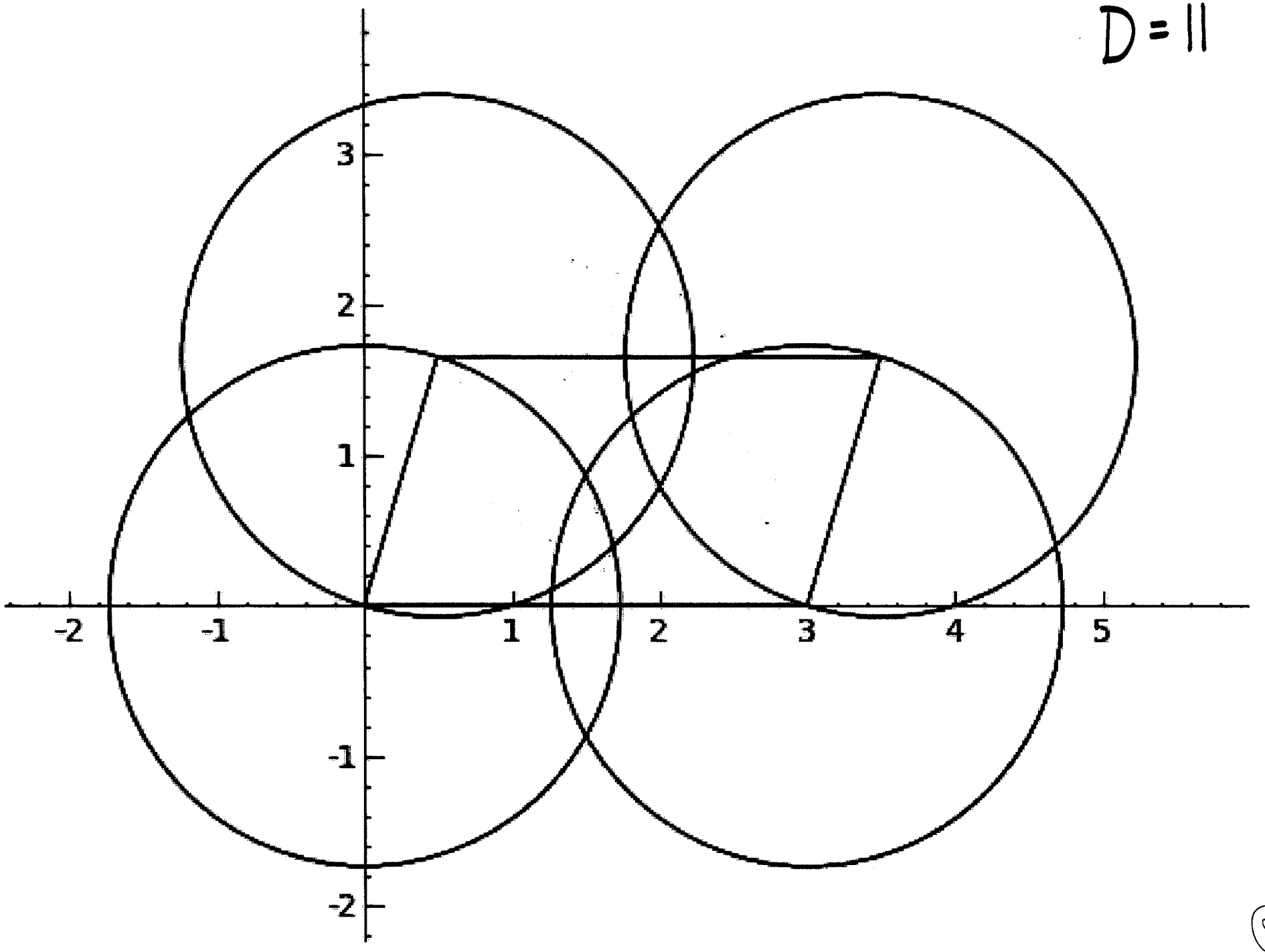
D = 5



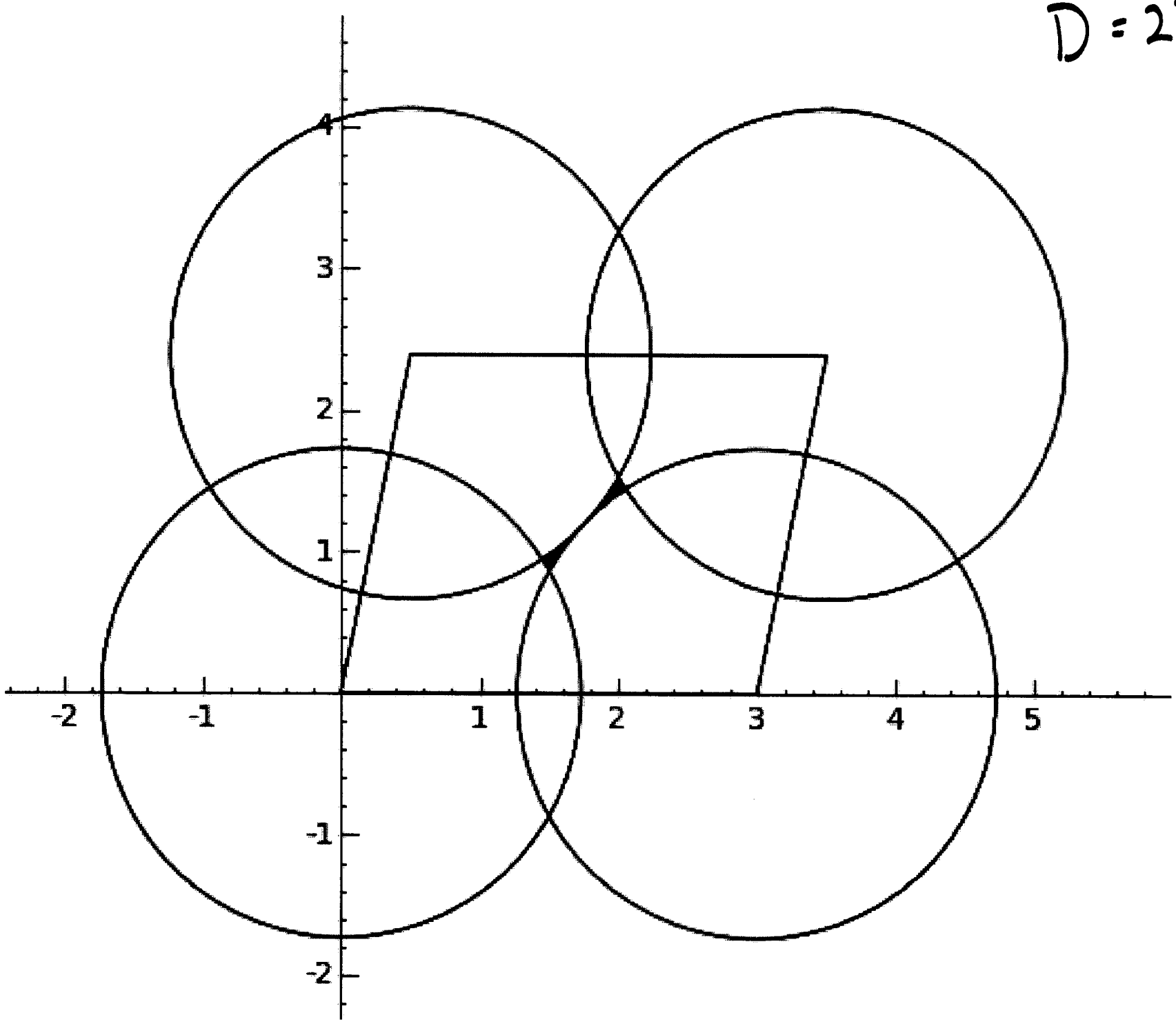
D = 14



D = 11



D = 23 (40)



Thm The quadratic imaginary fields with a Euclidean ideal are

$\mathbb{Q}(\sqrt{-D})$: $D = 1, 2, 3, 7, 11$ Class # 1

$\mathbb{Q}(\sqrt{-D})$: $D = 5, 15$.

In each case, Lenstra already proved ~~each~~ the Euclidean ideal is norm-Euclidean.