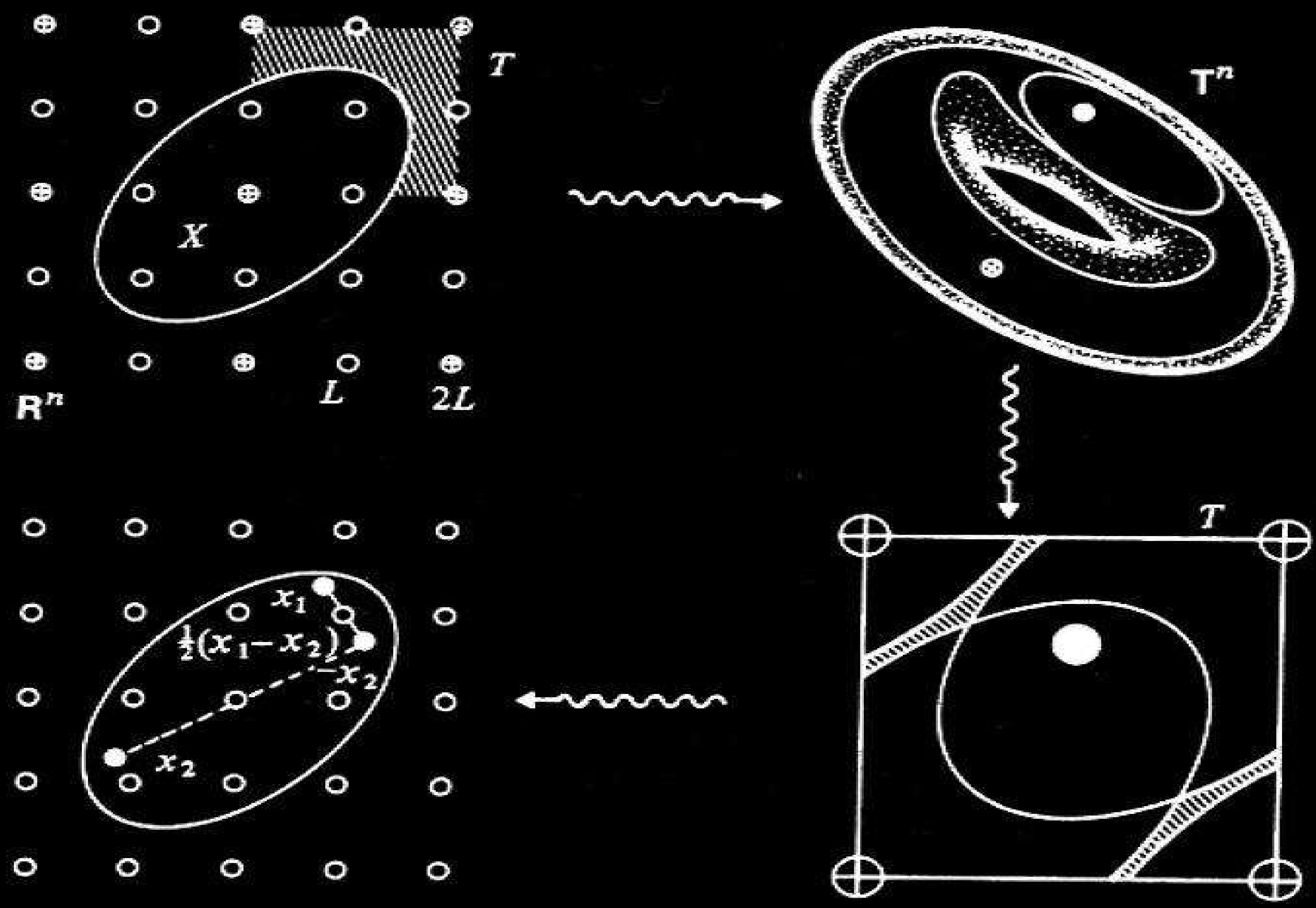
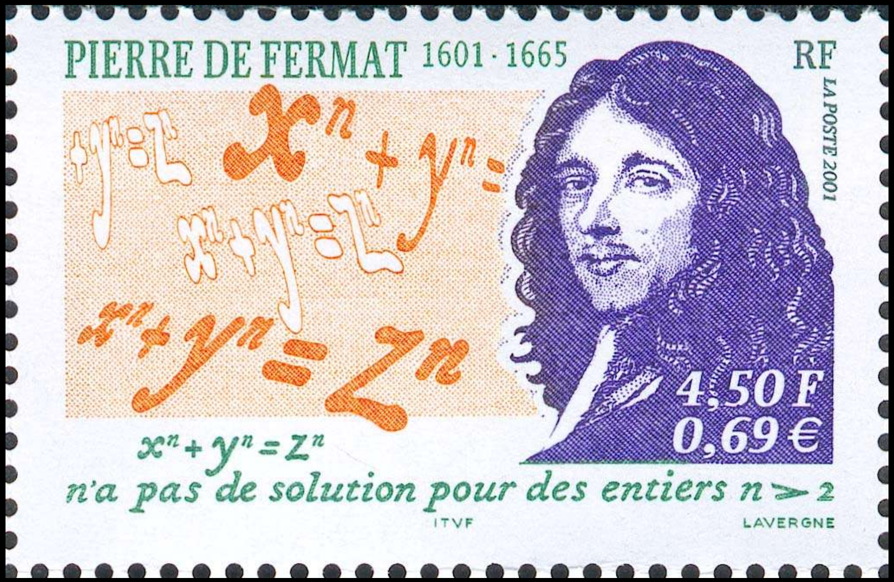
The Geometry of Numbers



The Prince of Amateurs



- Fermat was a lawyer by profession and indulged in number theory as a hobby.
- Formulated the two and four squares theorems
- Was in the habit of communicating theorems but not their proofs

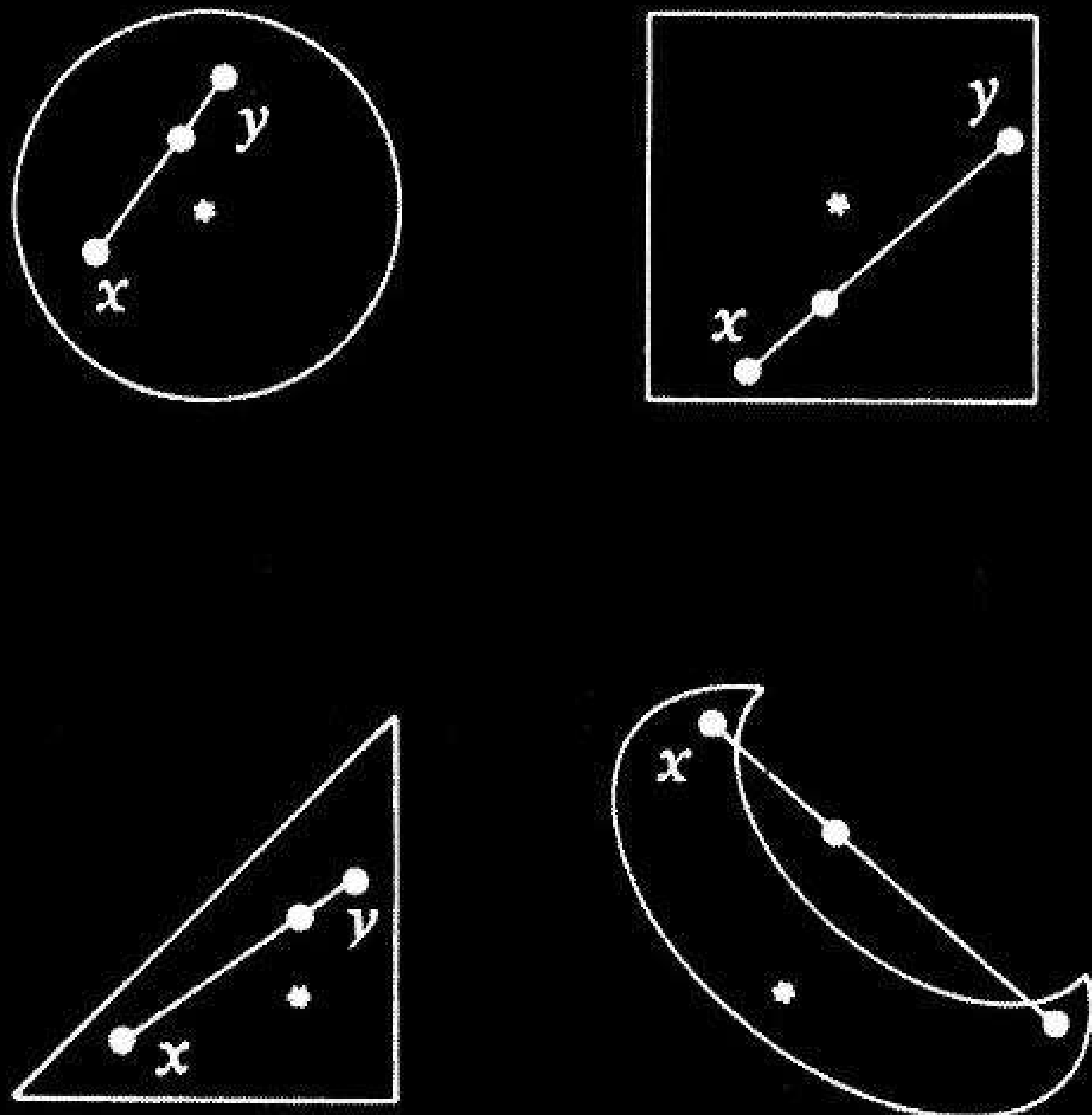
The 2 and 4 squares theorems

- (2 squares): Every prime of the form 4k+1 can be expressed as the sum of two squares.
- (4 squares): Every positive integer can be expressed as the sum of 4 squares.
- Euler (1707-1783) succeeded in proving the 2-squares theorem, but even after working on and off for 40 years on the 4-squares problem was not able to prove it conclusively.
- Lagrange (1736-1813) finally proved the 4-squares theorem in 1770.

Convex Regions

A convex region X is a set of points with the following two properties:

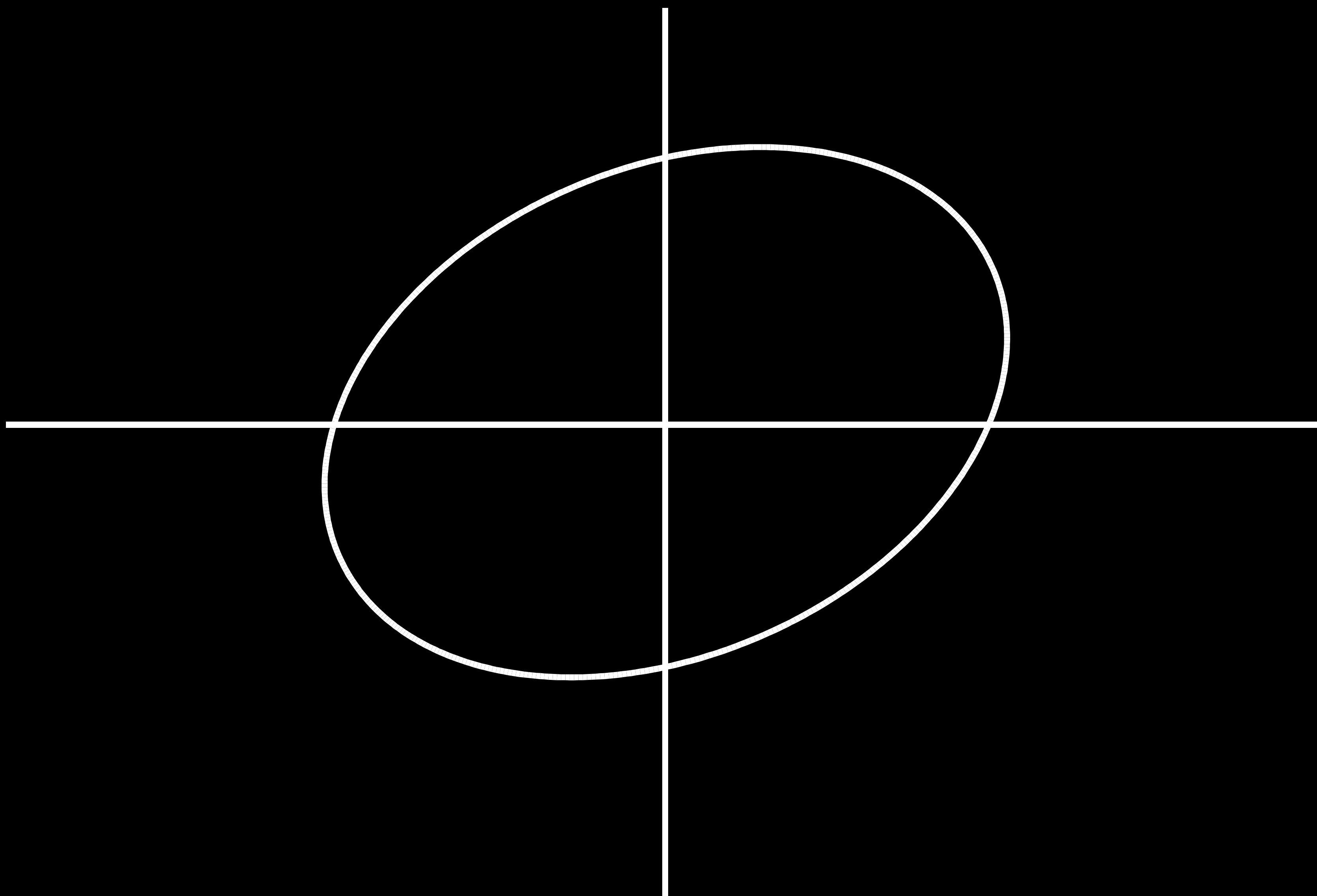
1) Every point of any chord of **X** belongs to **X**.
2) Any two points of **X** can be joined by a continuous curve lying entirely in **X**.

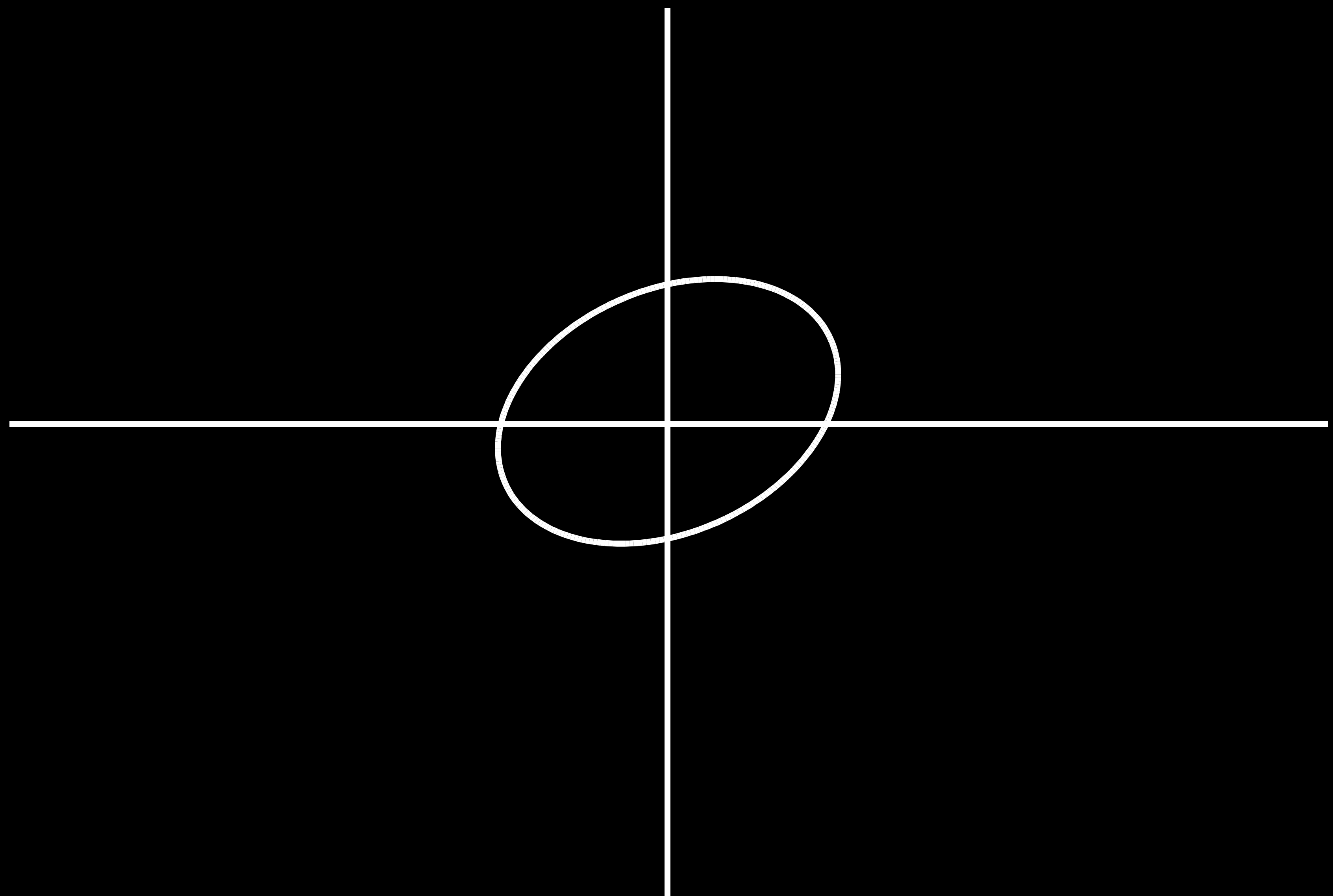

y
x
y
x
y
x
x

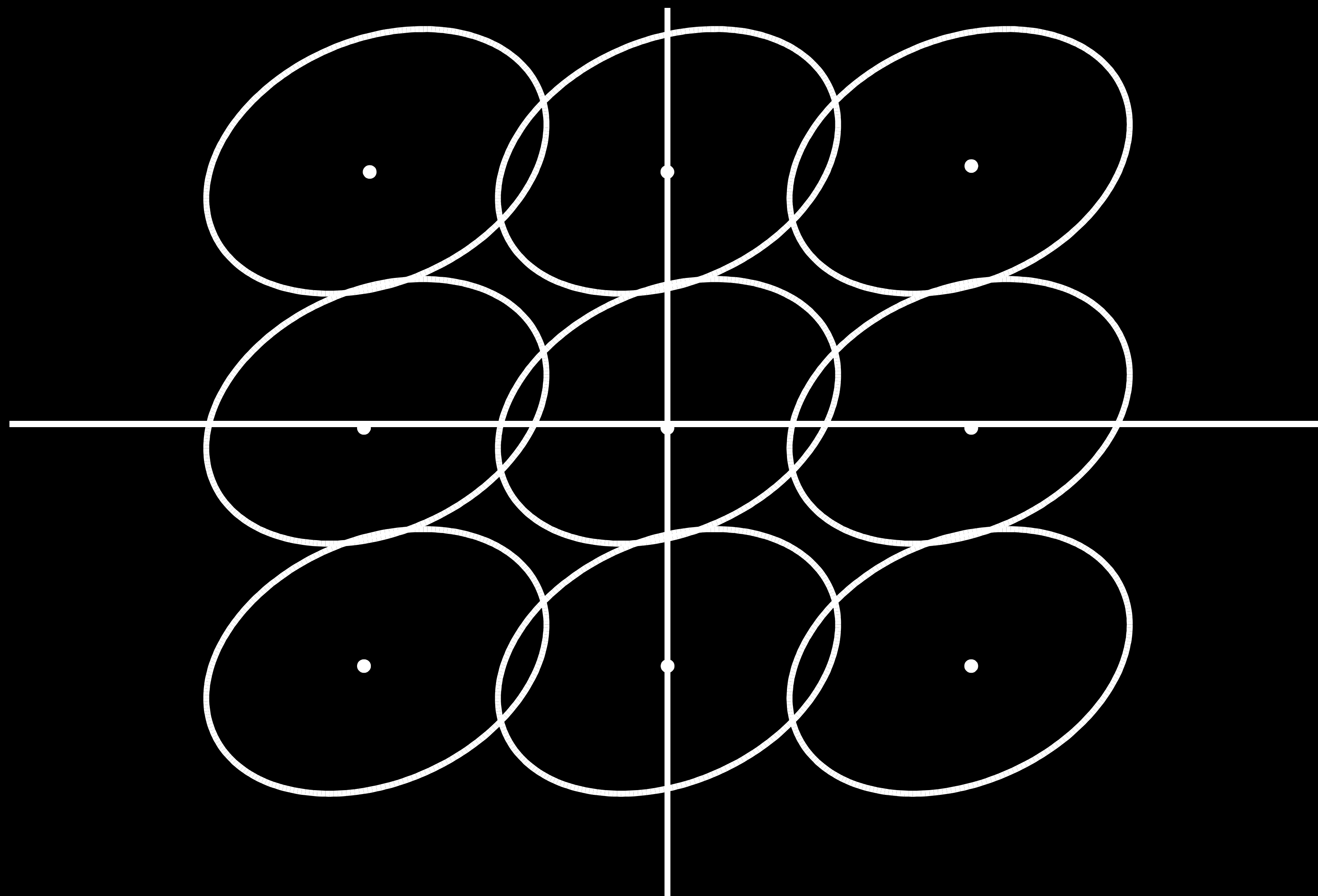
Minkowski's Theorem (simple)

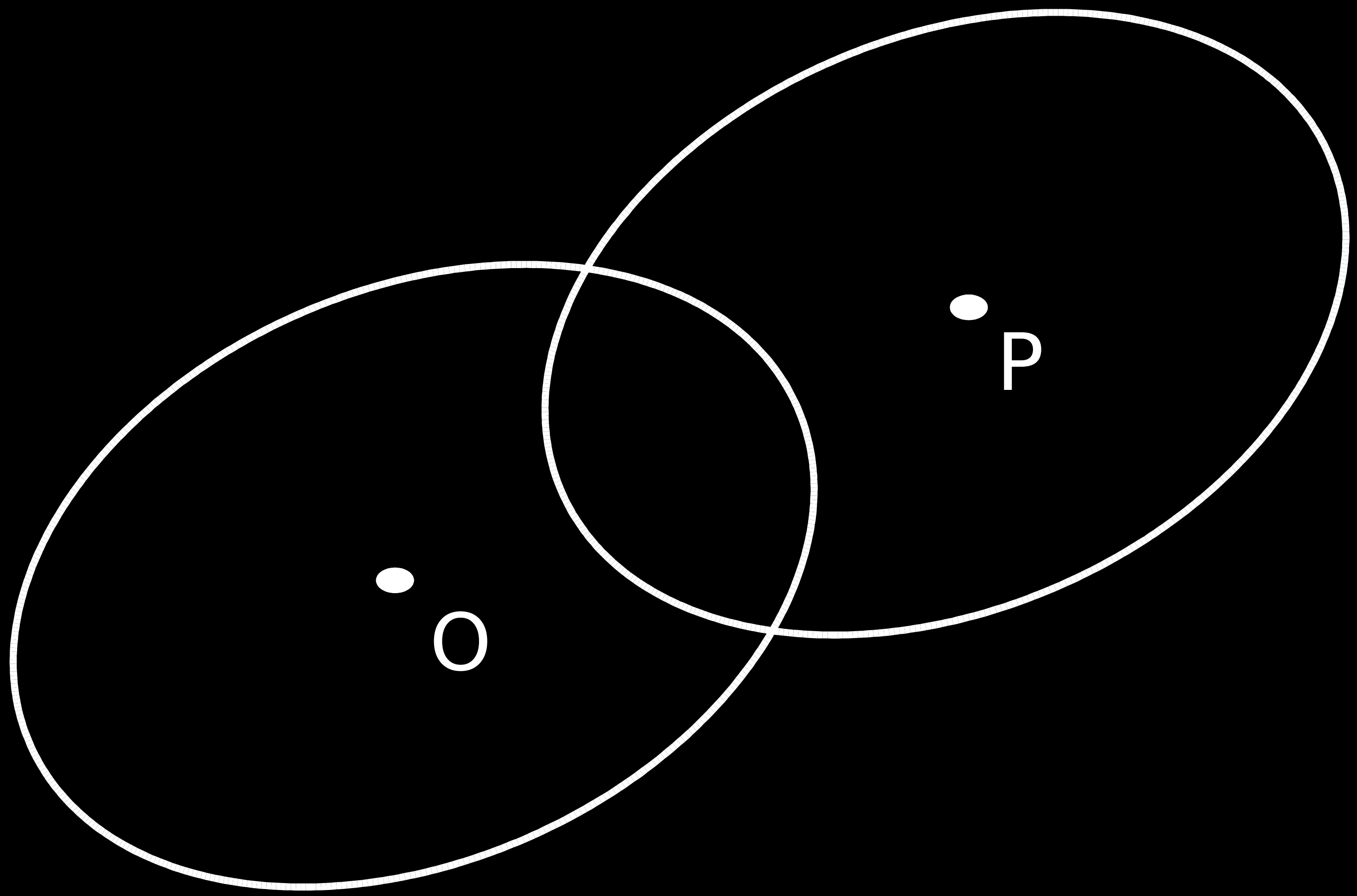
Any convex region **X** symmetrical about the origin, and of area greater than 4, includes integer lattice points other than the origin.

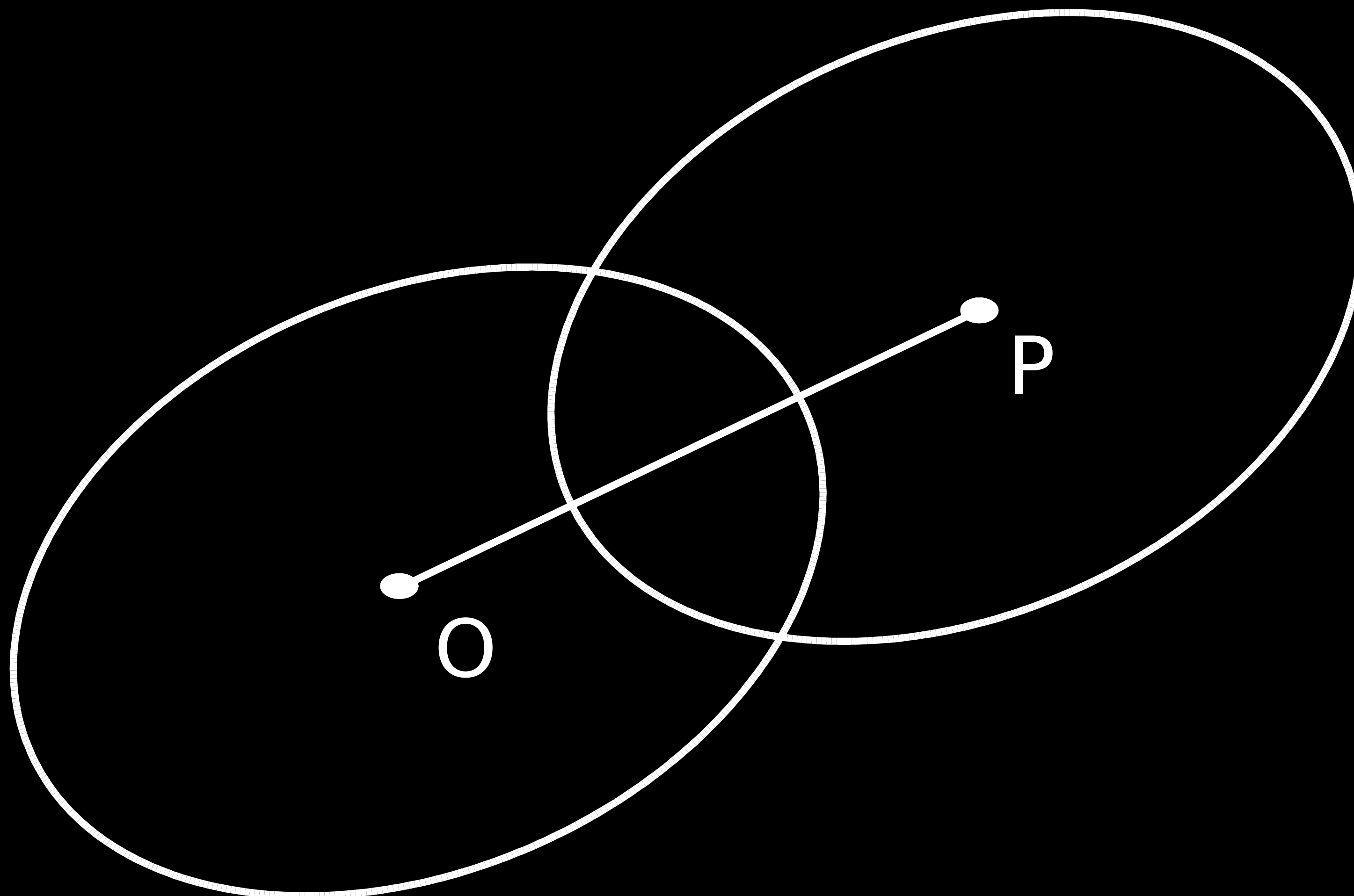
Proof

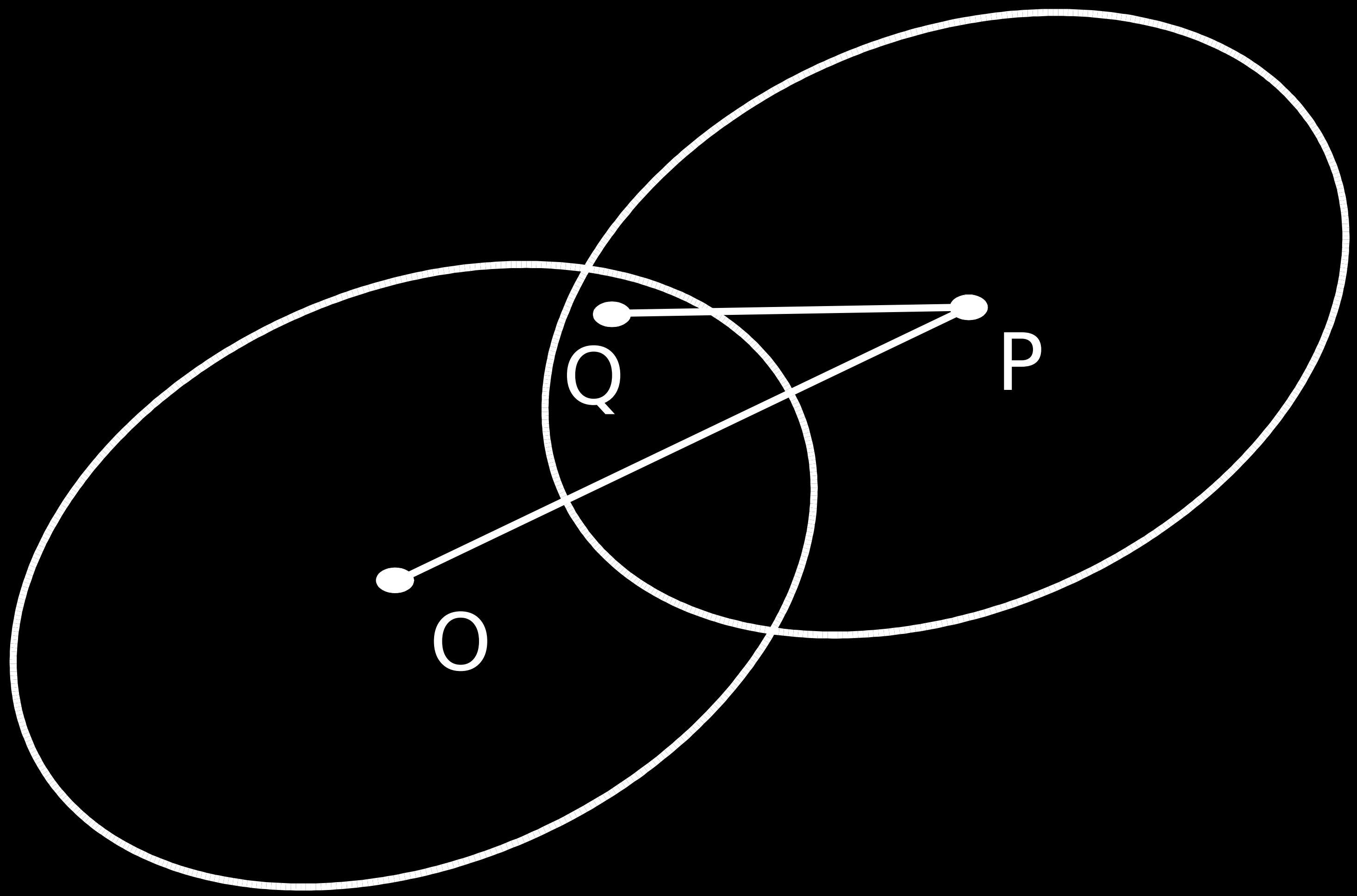


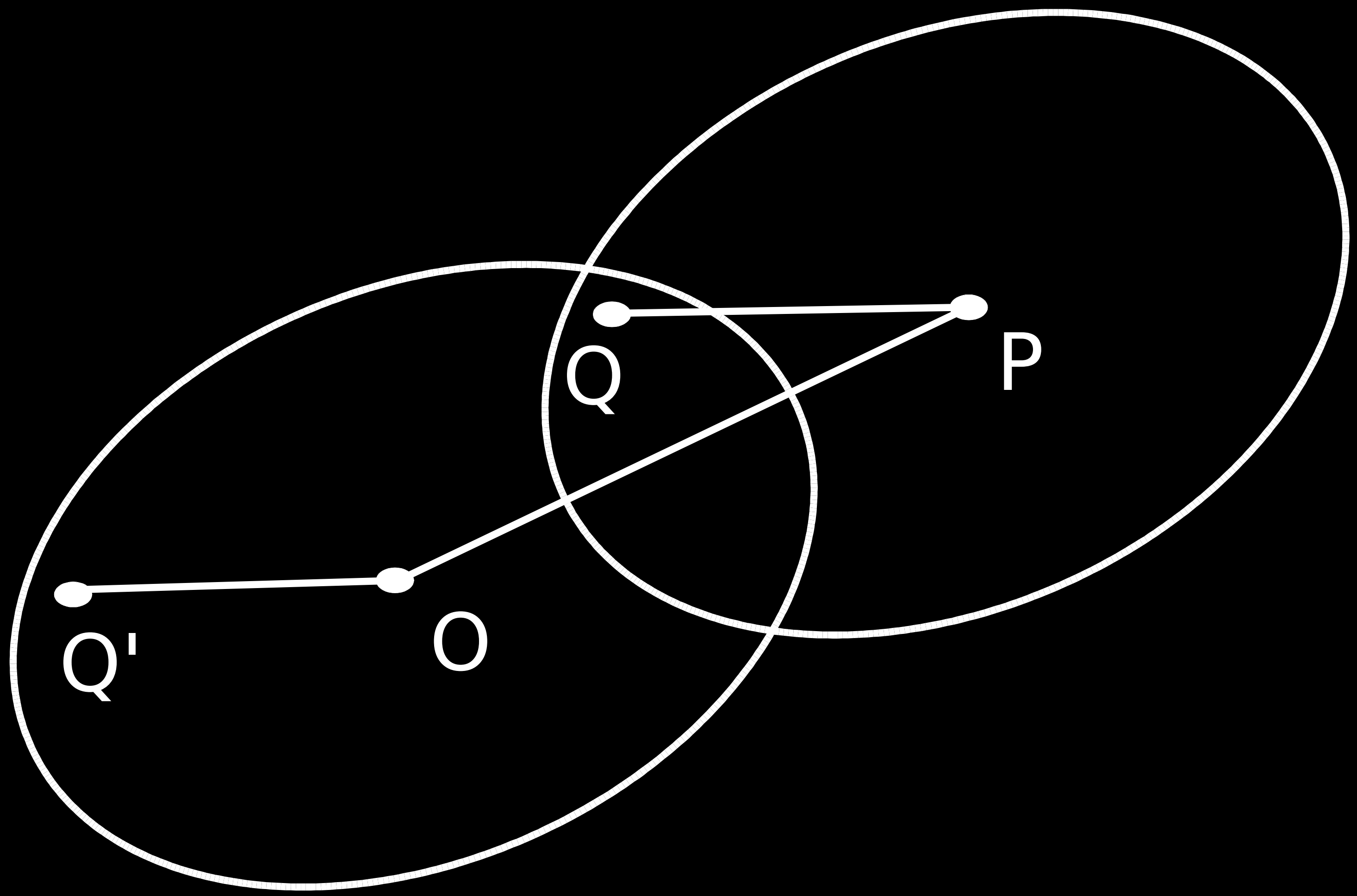




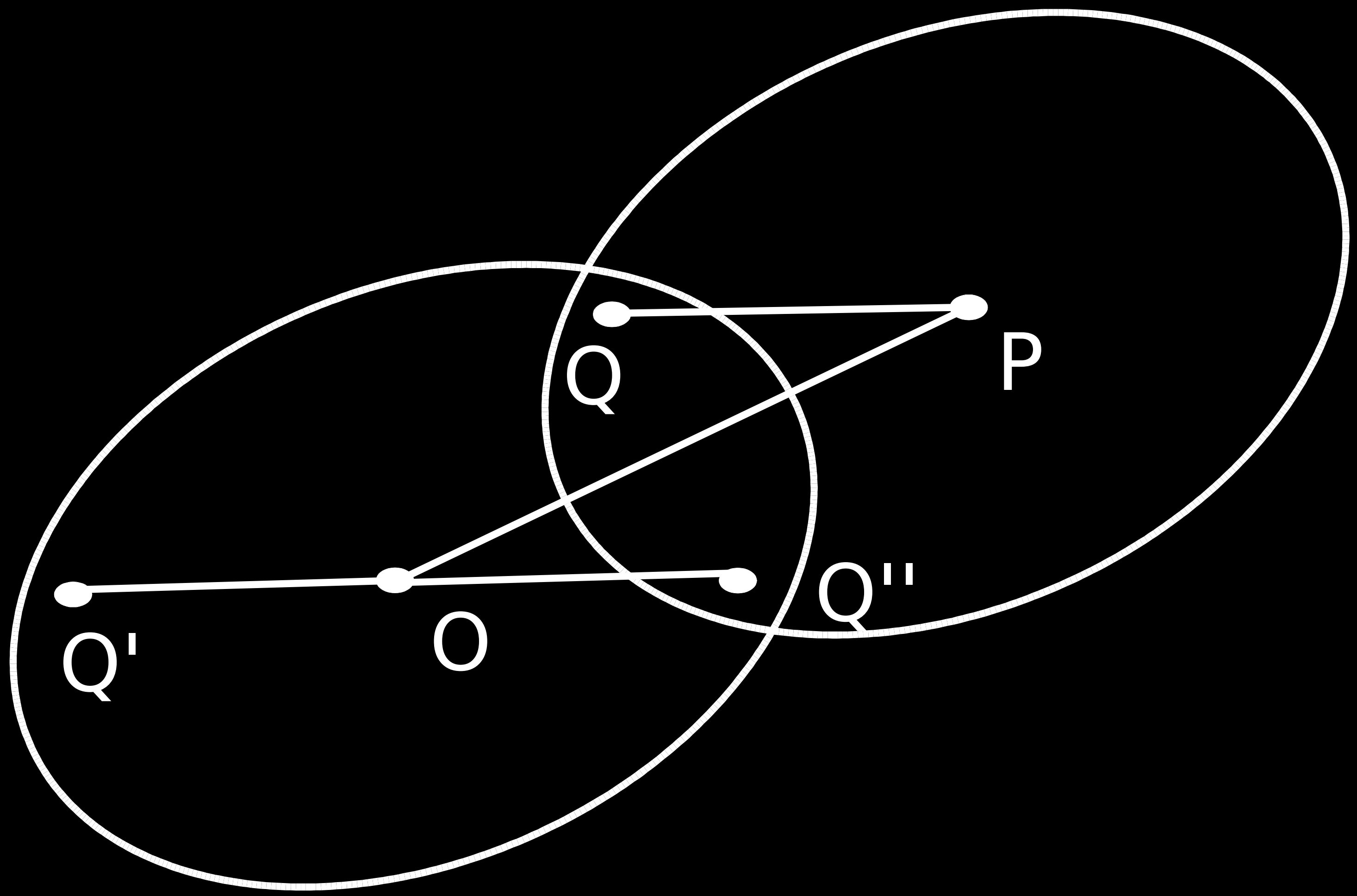

O
P


P
O

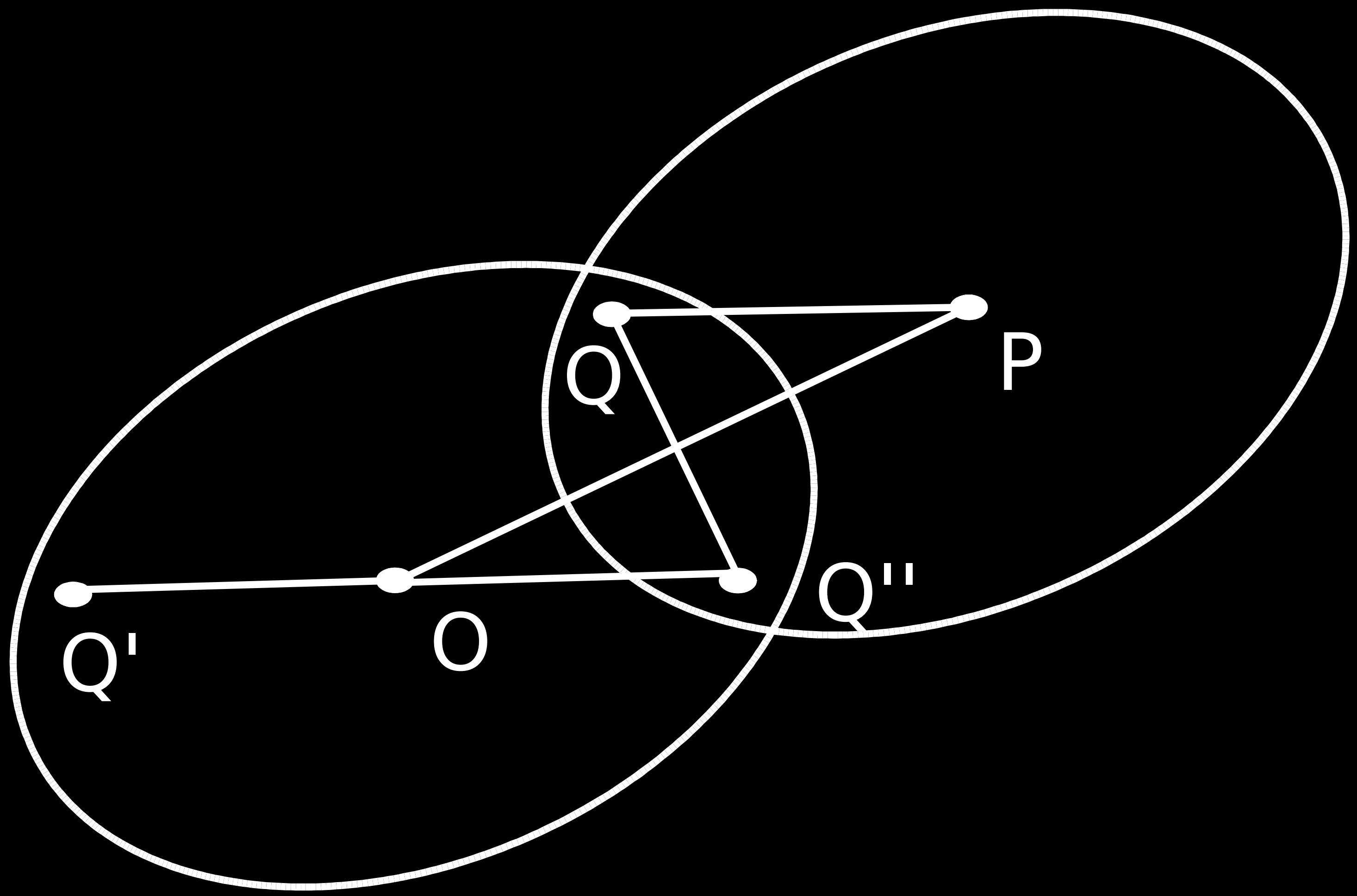

Q
P
O

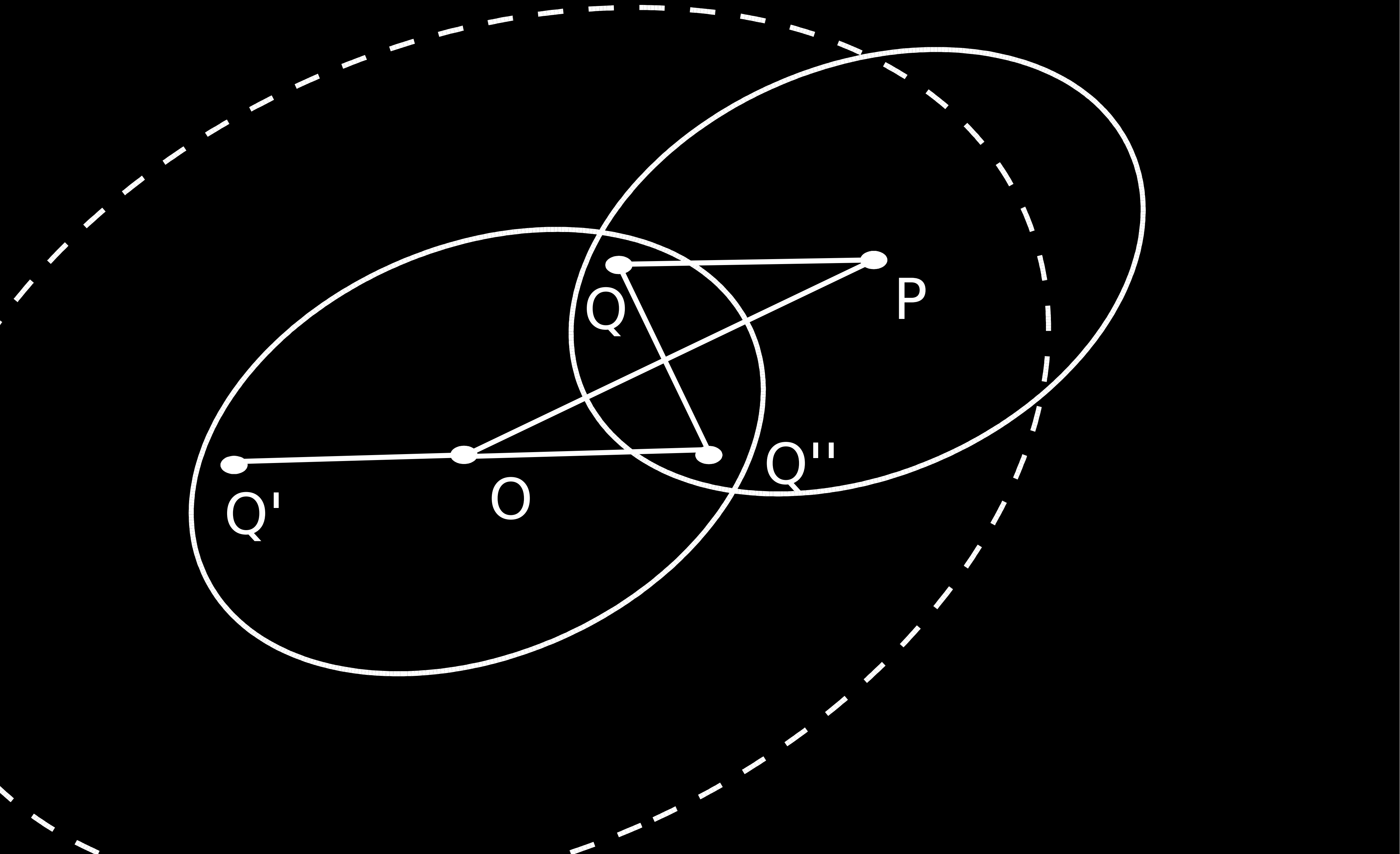


Q
P
Q'
O

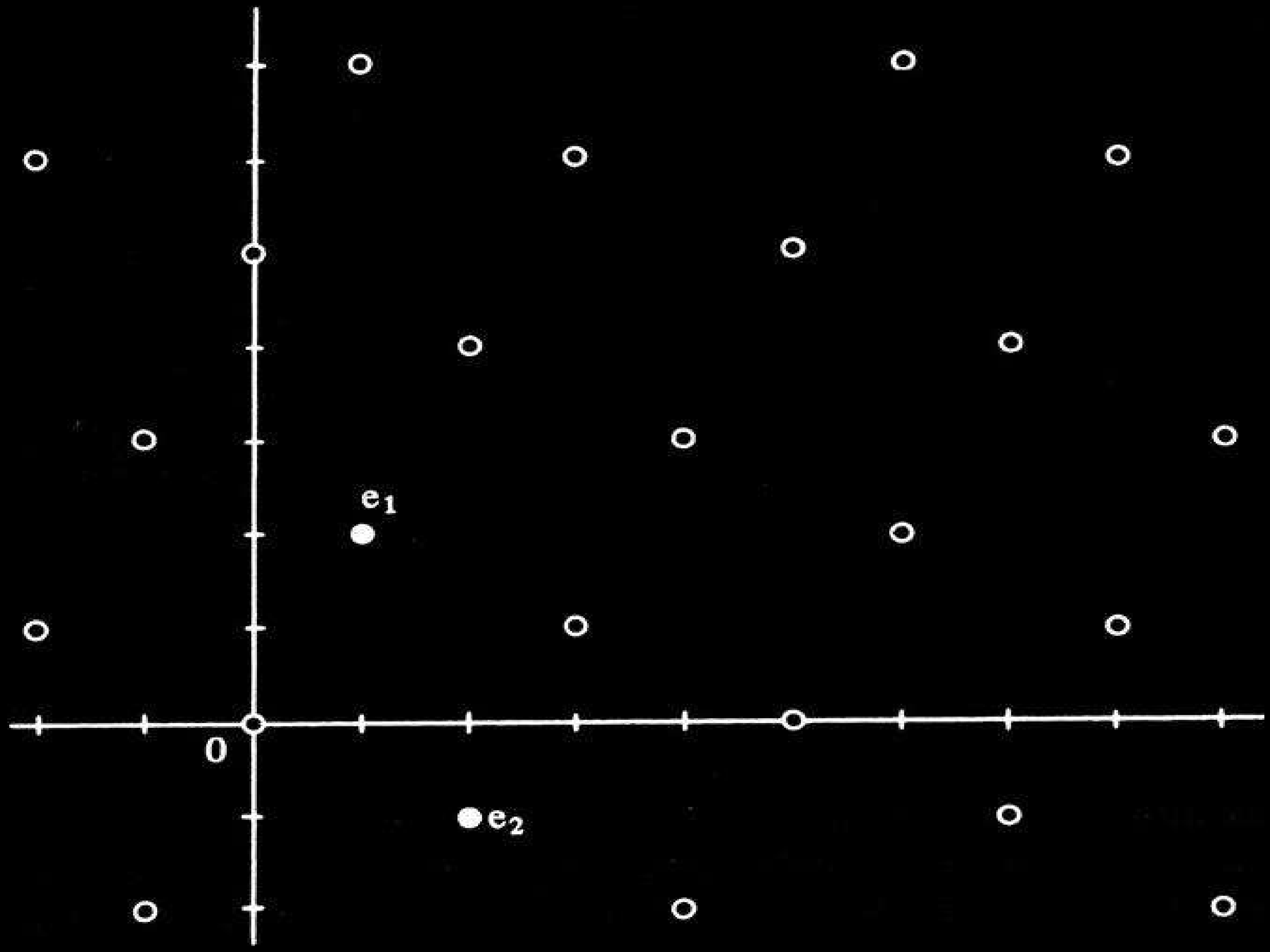


Q
P
Q''
Q'
O

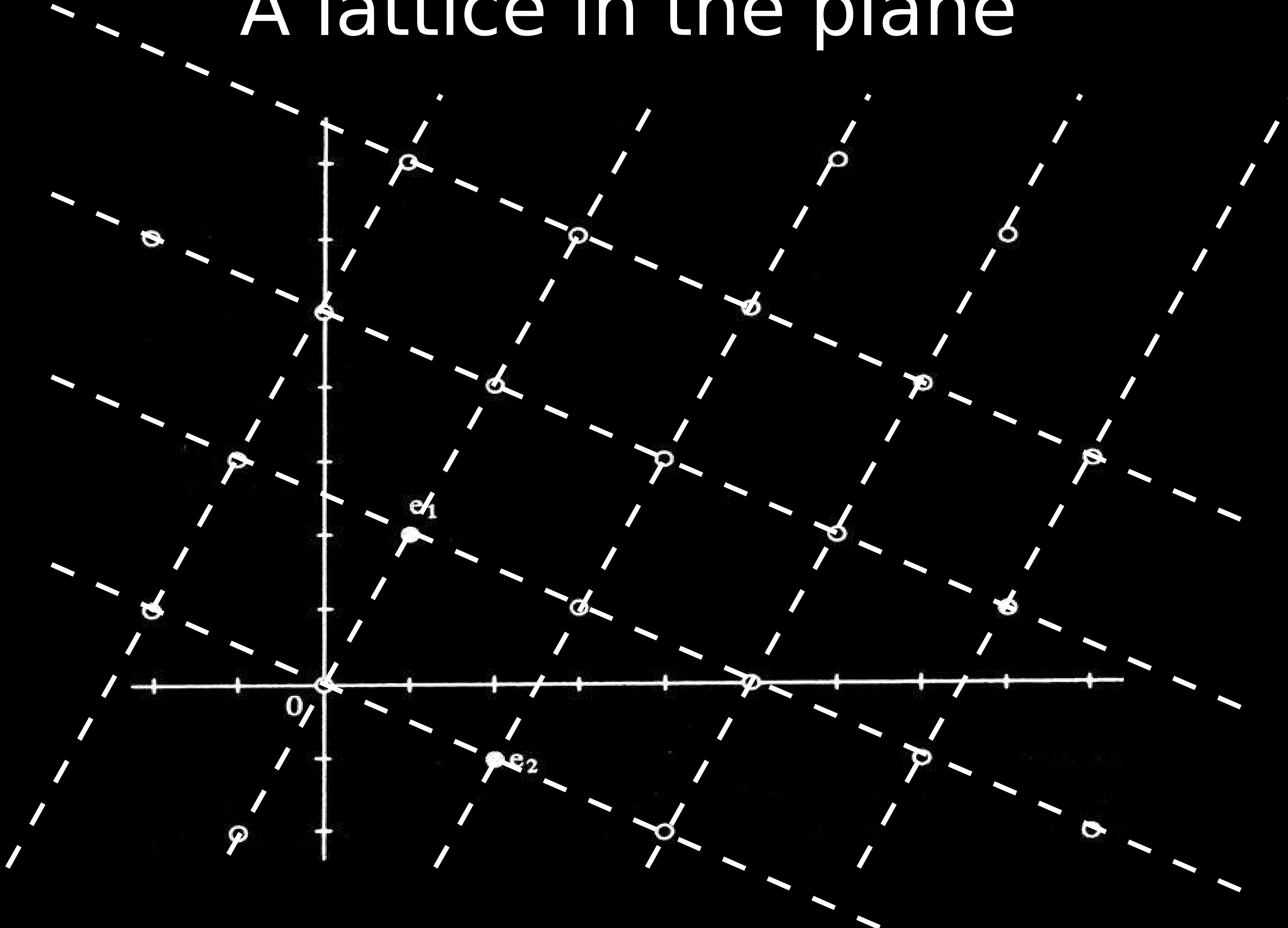

Q
P
Q''
O
Q'


Q
P
Q''
Q'
O

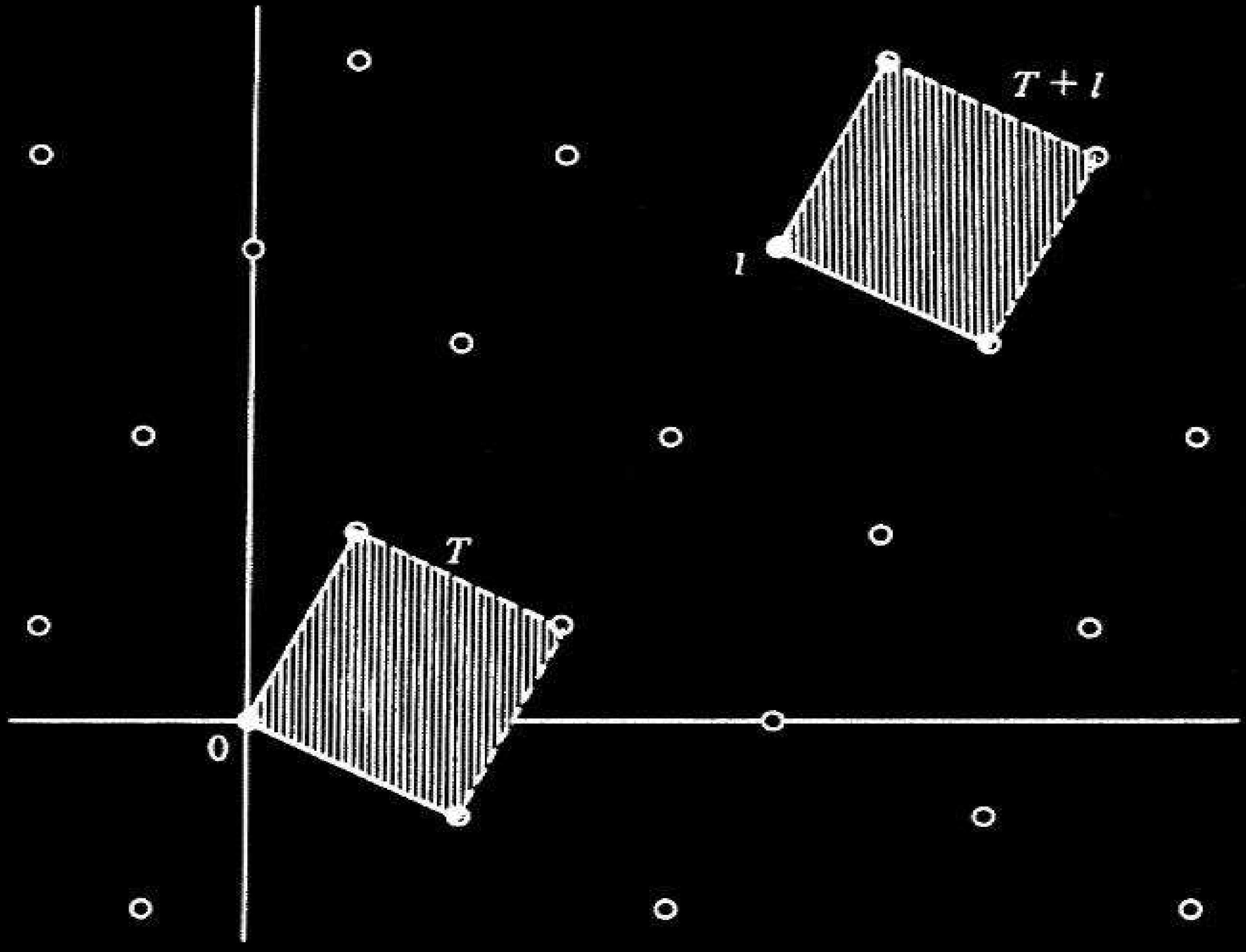
A lattice in the plane



A lattice in the plane



A Fundamental Domain **T**



Minkowski's Theorem

Let **L** be an n-dimensional lattice in $\mathbf{R}^n$ with fundamental domain **T**, and let **X** be a bounded symmetric (about the origin) convex subset of $\mathbf{R}^n$. If

$$\text{volume}(\mathbf{X}) > 2^n \,\text{volume}(\mathbf{T})$$

then **X** contains a non-zero point of **L**.

The 4-squares Theorem

Every positive integer is the sum of four squares.

Proof: We claim that the congruence

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

has a solution u,v in the integers. This is because both u^2 and $-1-v^2$ take on $(p+1)/2$ values as u,v run through $0,\ldots,p-1$;

So we have u,v that satisfy

$$u^2 + v^2 + 1 \equiv 0 \pmod{p}$$

Consider the lattice $\boldsymbol{L}$ in $\mathbf{R}^4$ consisting of a,b,c,d such that

$$c \equiv ua + vb, \quad d \equiv ub - va \quad \pmod{p}$$

It is easy to verify that the fundamental domain has volume p^2

Now a 4-dimensional sphere, center the origin, has volume $\pi^2 r^4/2$, and if we choose to make r^2 say $1.9p$, then this is greater than $16p^2$.

So there exists a non-zero lattice point (a,b,c,d) in this 4-sphere, so:

$$a^2 + b^2 + c^2 + d^2 \leq r^2 = 1.9p < 2p$$

Now modulo p, we have

$$a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2$$

$$\equiv a^2 + b^2 + u^2a^2 + v^2b^2 + 2uavb + u^2b^2 + v^2a^2 - 2ubva$$

$$\equiv (a^2 + b^2)(1 + u^2 + v^2) \equiv 0$$

Thus, we have that:

$$a^2 + b^2 + c^2 + d^2 = p$$

But now:

$$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)$$

$$= (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2$$

$$+ (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$$

Further Applications

- A similar (actually shorter and easier) argument hands us the 2-squares theorem.
- Paradise lost: when unique factorization fails. Finiteness of the class number. Excellent bounds on the same.