Titokmegosztás

Titokmegosztás

Adva van a titok

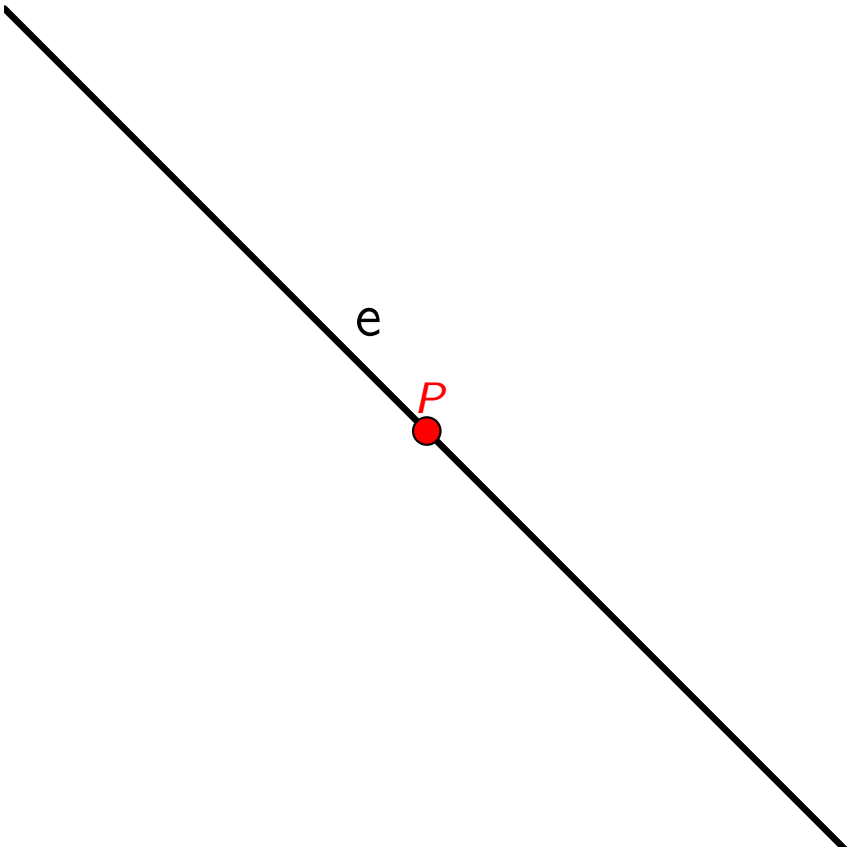
Titokmegosztás

Adva van a titok
Erről akarunk információt szétosztani emberek között

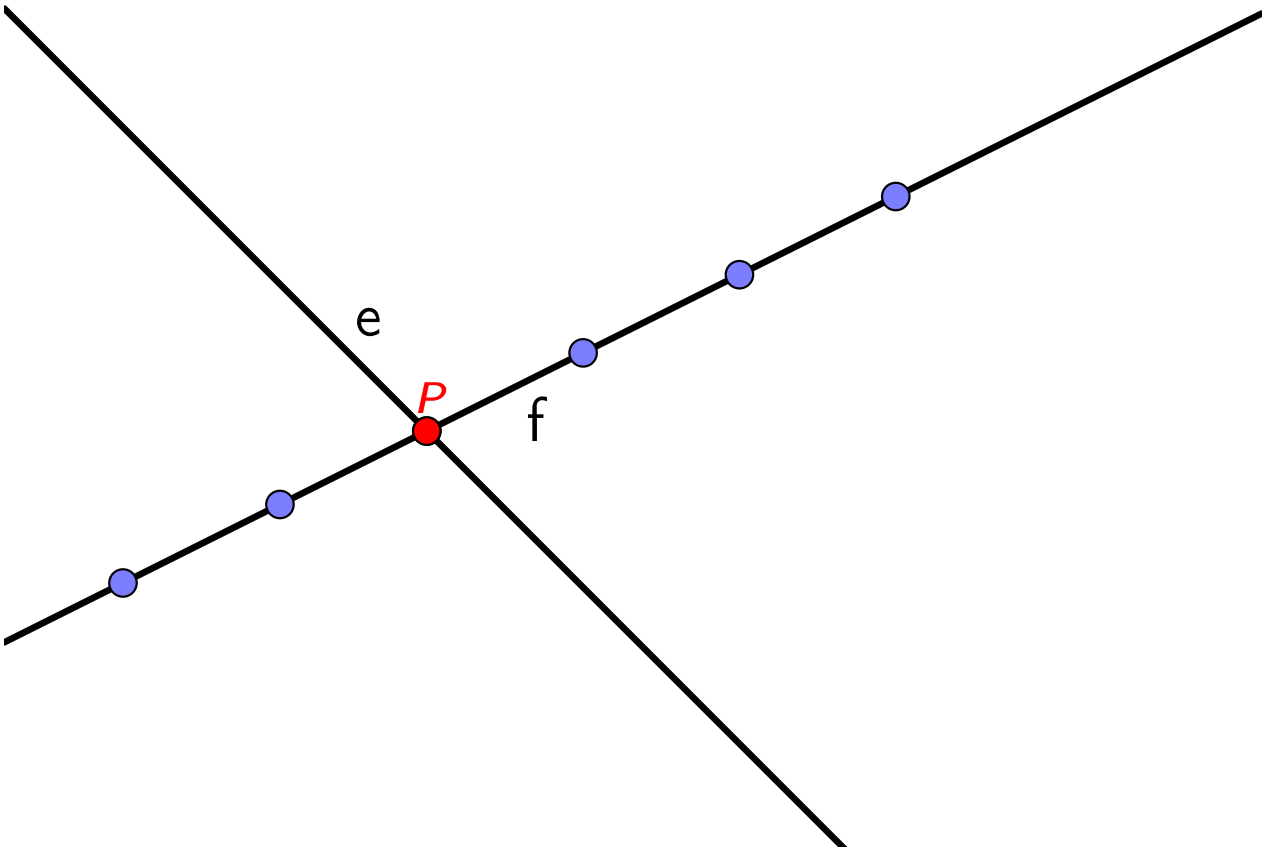
Titokmegosztás

Adva van a titok
Erről akarunk információt szétosztani emberek között
Úgy, hogy pont azok a részhalmazaik tudják meghatározni a titkot, amiket előre kijelöltünk.

Példa



Példa

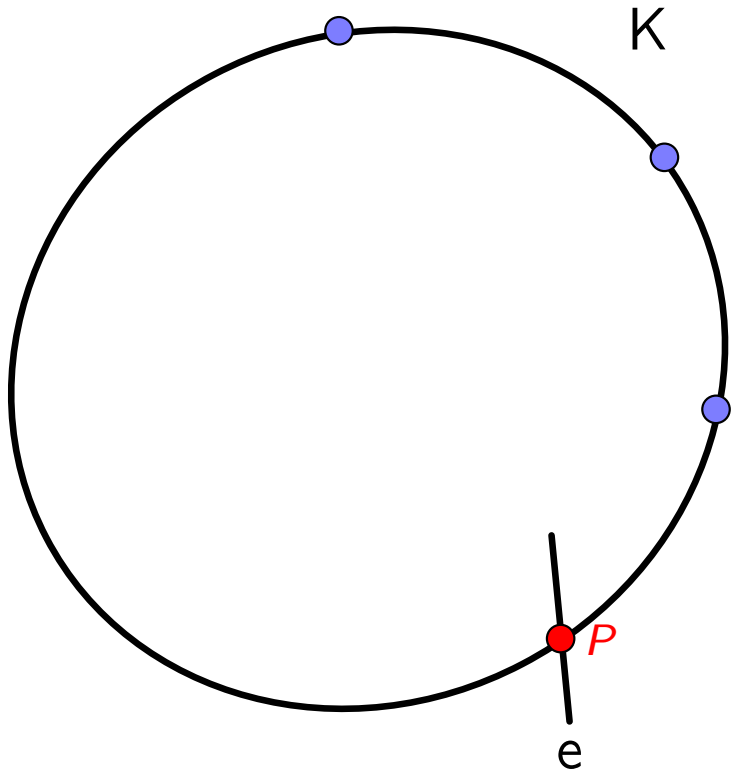


Példa 2

2 helyett n emberrel:

Példa 2

2 helyett n emberrel:

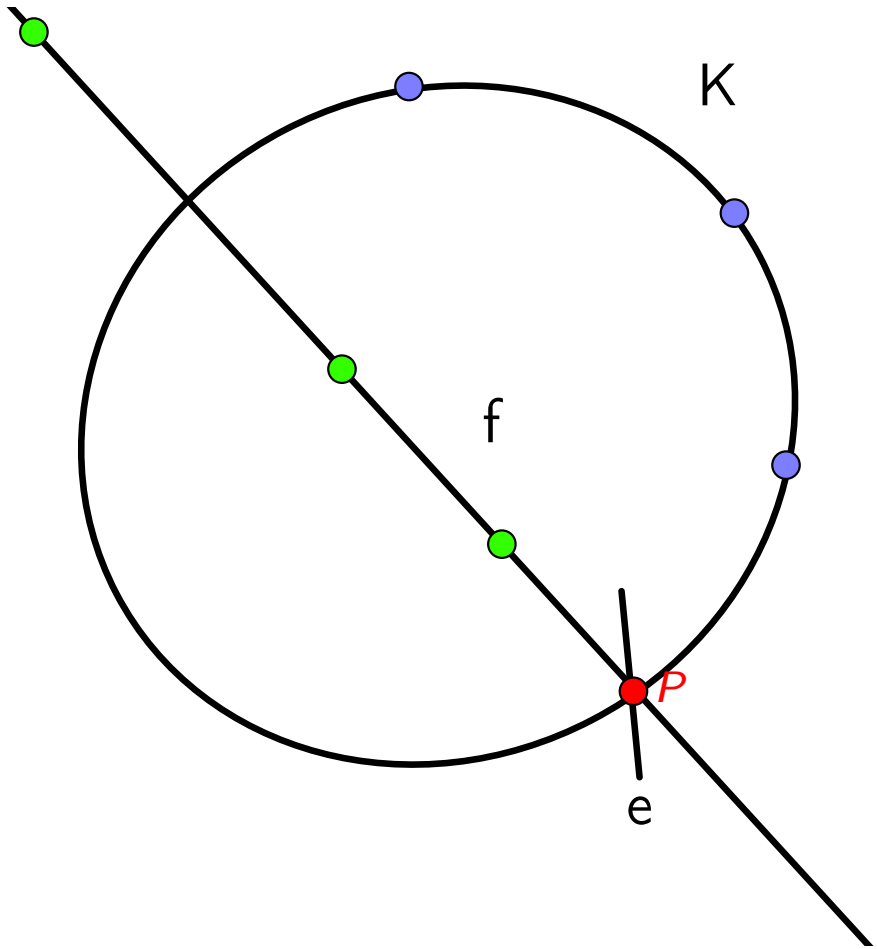


2 szintű titokmegosztás

Itt az emberek 2 részre vannak osztva, és a cél az, hogy akkor lehessen megfejteni a titkot, ha vagy az első típúsból van 2, vagy a másikból n.

2 szintű titokmegosztás

Itt az emberek 2 részre vannak osztva, és a cél az, hogy akkor lehessen megfejteni a titkot, ha vagy az első típusból van 2, vagy a másikból n.



Eredmény

$q-1$, q és $q+1$ bármely k osztójához választható olyan K és f, amelyre $|K| = k$, és f-en van mellé $q-k$ jó pont.

Eredmény

$q-1$, q és $q+1$ bármely k osztójához választható olyan K és f, amelyre $|K| = k$, és f-en van mellé $q-k$ jó pont.

$n = 3$

$n = 3$

a síkból f-et elhagyva egy affin síkot kapunk

$n = 3$

a síkból f-et elhagyva egy affin síkot kapunk

olyan K-t keresünk, aminek a pontjai között futó egyenesek kevés irányt határoznak meg

$n = 3$

a síkból f-et elhagyva egy affin síkot kapunk

olyan K-t keresünk, aminek a pontjai között futó egyenesek kevés irányt határoznak meg

affin szabályos sokszögek