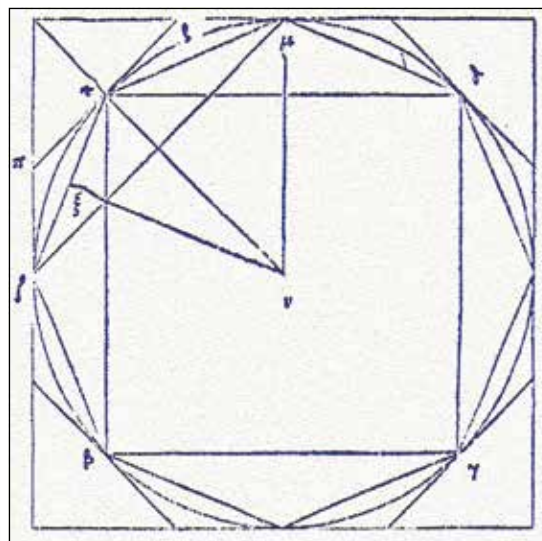
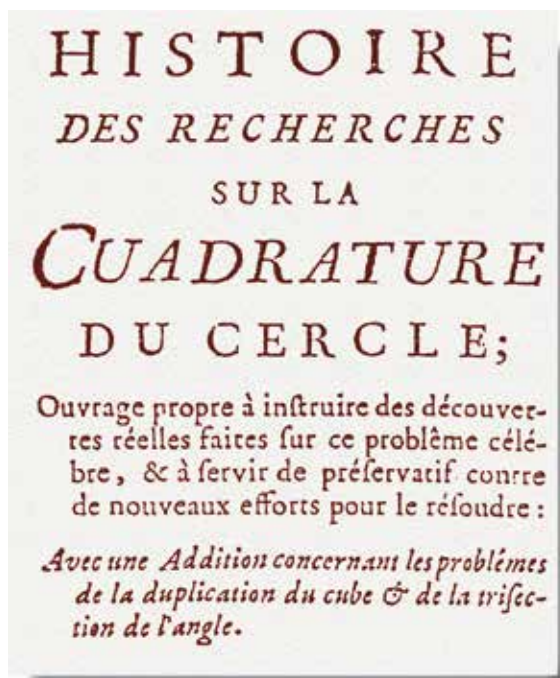


A PROBLÉMA BONYOLULTSÁGA ANNYIRA HÍRESSÉ VÁLT,
HOGY HA VALAKI LEHETETLEN FELADATOT KAP, AZT MONDJA:
„EZ NEHEZEBB, MINT A KÖR NÉGYZETRE VONÁSA.”

• A kör négyzetre vonása A kiméra története



◀ Bal oldalon látható Jean-Étienne Montucla könyvének borítója, amelyben a 18. századig a kör négyzetre vonásának legérdekesebb megoldási kísérleteit írja le. Mellette látható Euklidész által javasolt „megoldás”. A kör négyzetre vonása, az szög háromszögelése és a kocka megkétszerezése az ókori görög matematikusok három legnagyobb problémája volt; egyikre sem volt megoldás, de akkoriban ezt még nem tudták.

Az a probléma, amely évszázadok óta foglalkoztatja a legjobb matematikusokat, így hangzik: „Ha adott egy kör, akkor lehet-e csak vonalzó és körző segítségével olyan négyzetet rajzolni, amelynek területe megegyezik a körével?” A vonalzó és a körző használata nagyon fontos, mert természetesen nem milliméteres vonalóról van szó, különben minden gyermek, aki rendelkezik a szükséges ismeretekkel, könnyedén megoldaná a feladatot. Mindig akad valaki, aki megméri a kör sugarát, kiszámítja annak területét, majd megrajzol egy azonos méretű négyzetet, és utána csodálkozik, hogy lehetséges-e, hogy valami ilyen egyszerű

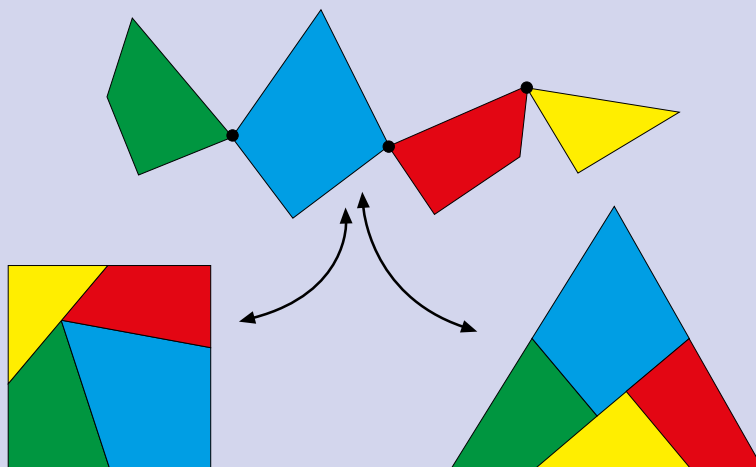
feladat évszázadokig foglalkoztatta a legjelentősebb matematikusokat. Tehát ez egy tisztán geometriai konstrukció, amelyben nincs szükség semmilyen számításra.

•Vonalzóval és körzővel

A vonalzó és a körző segítségével történő konstrukciót görög geometrikusok találták ki, és ezek a megoldások olyan problémák halmazát alkotják, amelyek matematikai szempontból nagyon érdekesek. Néhány nagyon egyszerű, mint például egy szög tengelyének megrajzolása. Mások nehezebbek, mint például három másik körhöz érintő kör megrajzolása.

A háromszög négyzete

A kvadráturák világa nem feltétlenül végződik körrel: mindenféle sokszög is négyzetre alakítható. Könnyen elkészíthetünk egy kis négyzet alakú játékot összekapcsolt faelemekből, amely néhány mozdulattal háromszöggé alakítható (és fordítva). Ebben az esetben nem kétséges, hogy a négyzet és a háromszög területe megegyezik.





◀ A kocka megkettőzésének problémája „a Delphoi jósa” problémájaként is ismert. A legenda szerint Apollón isten többször is haragudott az egész világra. A delphoi jósa úgy döntött, hogy azt tanácsolja az athéniaknak, hogy építsenek az istennek egy új oltárt, amely kétszer akkora lesz, mint az előző. Abban az időben a matematikát néha arra is használták, hogy megnyugtassák a haragos isteneket. Amikor azonban a geometerek munkához láttak, rájöttek, hogy az oltár kocka alakú. Olyan problémával szembesültek, amelyet nem tudtak megoldani.

ÉRDEKESSEGEK

Még mindig vannak olyanok, akik úgy vélik, hogy megoldották a kör négyzetre vonásának problémáját (és az állandó mozgás problémáját is). Becslések szerint minden tanévben világszerte 50 és 100 közötti ilyen típusú „megoldás” jelenik meg az összes egyetemen.

Napoleon nagy szerelmese volt a matematikának, és hadjáratai között problémák megoldásával foglalkozott. Arról, hogy a lelkesedésén kívül tehetsége is volt hozzá, tanúskodik az a tény, hogy a problémákat nemcsak megoldotta, hanem ki is találta őket. Az egyik, az úgynevezett „Napoleon-probléma” így hangzik: Találd meg a kör középpontját csak körző segítségével. Ennek a problémának van megoldása.

A pitagoreusok iskolái a kör négyzetre vonásának metafizikai jelentőséget tulajdonítottak, amelyet később az európai okkult irányzatok is átvettek: a probléma megoldhatatlan, mert a matematikából az okkult szimbolikába lefordítva ez ugyanazt jelenti, mint pontosan tudni egy ember halálának helyét és idejét, ami nyilvánvalóan lehetetlen.

Mások pedig megrajzolhatatlanok, mint például a kör négyzetre osztása. Csak 1882-ben bizonyította Ferdinand Lindemann matematikus, hogy egy körrel azonos területű négyzet megrajzolása csak vonalzó és körző segítségével megoldhatatlan feladat. Több mint 23 évszázadnyi kimerítő kísérletnek kellett eltelnie, mert a matematikában gyakran nehezebb bizonyítani, hogy egy probléma megoldhatatlan, mint megtalálni a megoldást egy olyan problémára, amelynek van megoldása.

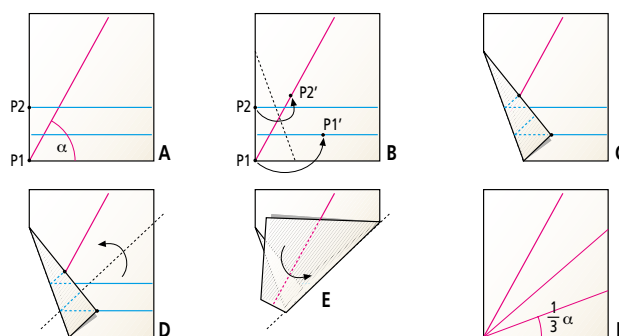
A fenti probléma a három klasszikus vonalzóval és körzővel megoldható probléma közül a legismertebb. A másik kettő a „szög háromszögelése” és a „kocka megkettőzése”, amelyek nagyon hasonlítanak ehhez. Az első a szög három részre osztásában, a második pedig egy adott kocka térfogatának kétszeresére történő megkettőzésében áll. Természetesen csak vonalzó és körző használatával.

•Zárásként

Sokáig tartott, mire kielégítő megoldást találtak erre a problémára. Ez részben annak volt köszönhető, hogy nem lehetett tisztán geometriai fogalmakkal megfogalmazni, hanem bele kellett merülni abba a területbe, amelyet sokkal később csoportelméletnek neveztek el, vagyis abba a tudományágba, amelynek alapjait a 19. század közepén a francia matematikus Évariste Galois fektette le.

A megoldás az, hogy kizárólag vonalzó és körző segítségével nem lehet megoldani a kör négyzetre vonását, a szög háromszögelését és a kocka megkettőzését.

Triszekció és origami



A papír hajtogatásával, az origami nevű művészettel, amelyben a geometria mély titkai rejlenek, elvégezhető a szög háromszögelése. Vegyünk egy tetszőleges papírlapot, jelöljük meg az α szöget, és rajzoljunk két egyenlő párhuzamot a lap alsó részére (A). Hajtsuk át az alsó sarok P1-et az első párhuzamos vonalra úgy, hogy a második csúcs P2 vége érintse a szög oldalát (B és C). Hozzunk létre egy új hajtást az első párhuzamos vonalon, amely a lap felső csúcsától a szög csúcsáig (D) vezet. Osszuk el ezt a szöget két részre (E), és kapunk egy olyan szöget, amely harmadokra van osztva (F).

• *Kódok és kulcsok*

Üzenetek titkosítása és visszafejtése

► A Rosette-i kő, amelyet 1799-ben egy napóleoni katona véletlenül talált meg, kulcsfontosságú volt az egyiptomi hieroglifák megfejtésében. Ugyanaz a szöveg szerepel rajta hieroglif, démotikus és görög írással.



▲ Csak 1822-ben sikerült Champollionnak megfejtenie a hieroglif írást. A fenti ábrán néhány hieroglif jel látható a kartusban.

Champollion úgy vélte, hogy ezek a jelek a fáraó nevét fejezhetik ki. A görög szövegben megjelent Ptolemaiosz király neve, és Champollion

felvetette a hipotézist, hogy ez a fent írt név. Ez volt az első lépés a megfejtés felé, amely mögött hatalmas munka állt, és amely végül feltárta a kő titkát.

kifejezés, amelyek a köznyelvben ugyanazt jelentik, vagy pontosabban, ugyanazt a szándékot fejezik ki, nevezetesen, hogy valamilyen módon elrejtsek egy adott üzenetben szereplő információkat. Ahhoz, hogy a címzett megfejtse annak jelentését, ismernie kell azt a mechanizmust, amelyet *kulcsnak* neveznek, és amelynek segítségével az eredeti szót titkosították. Ebben az esetben az ábécé minden betűjét három hellyel arrébb található betűvel helyettesítették. A dekódoláshoz tehát minden betűt három hellyel hátrébb található betűvel kell helyettesíteni, így kapjuk meg a SOK szót. Ez az egyszerű titkosítási rendszer a rómaiak idején volt használatos, és *Caesar*-módszerként ismert. A kriptográfia, azaz a bizonyos üzenetekben rejlő rejtett információkkal foglalkozó tudomány vagy művészet, ugyanolyan régi, mint maga az írás. Bizonyos értelemben már az ókori egyiptomiak is használtak kriptográfiai módszereket írásukban; ezt bizonyítja, hogy míg a nép a démotikus írást használta, a papok hieratikus (hieroglifikus) írással írtak, amely a laikusok számára érthetetlen volt.

• Jó zár

A titkosítási rendszer akkor működik, ha mind a feladó, mind a címzett ismeri:

1. *Algoritmus*. Ez egy számítási módszer, amelyet üzenetek titkosítására vagy visszafejtésére használnak.
2. *Kulcs*. Ez egy titkos információ, amelyet az algoritmus az üzenet titkosításához és visszafejtéséhez használ.
3. *Határidő*. Ez az az időtartam, amely alatt a kulcs érvényes.

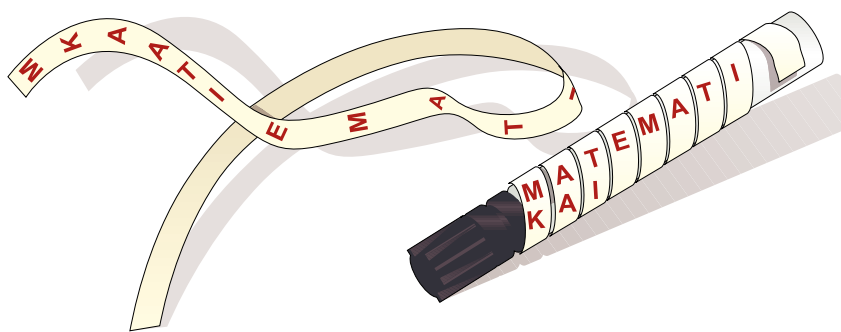
Tegyük fel, hogy egy épületben található lakásokat rendszeresen használják egy vállalat vezetői. Az apartmanokat biztonsági rendszer védi, amely megköveteli, hogy a felhasználó számkódot adjon meg az ajtó kinyitásához. Ebben a példában az *algoritmus* egy utasítások sorozata, amely kinyitja vagy nem nyitja ki az ajtót. A helyes kód egy titkos kulcsot jelent. A *határidő* az az időtartam, amely alatt a vezető használja az apartmant. Ezen időtartam letelte után a kulcsot meg kell változtatni, hogy más felhasználó ne tudja használni.

•Szkütale

A legrégebbi ismert mechanikus titkosítási módszer a szkütale, amelyet katonai célokra használtak az Athén és Spárta közötti háborúban az i. e. 5. században. Ehhez két azonos méretű hengerre volt szükség; az egyiket a küldő, a másikat a címzett kapta meg. A hengerre hosszú papirusz- vagy bőrszalagot tekertek. Ezután megírták az üzenetet. A szalag letekeredése után az üzenet olvashatatlanná vált, és csak akkor lehetett elolvasni, ha a második, az elsővel megegyező hengerre tekerték. Minél bonyolultabb volt a henger alakja, annál biztonságosabb volt a rendszer. A hírnök általában a csomagot a derekán, az övé mögött rejtve hordta. Hogy az üzenet még jobban megzavarja a nem kívánt címzetteket, az üres helyekre betűket írtak.

•Digitális hírnök

A titkosítás (a francia *chiffre* szóból, amely számot jelent) szó szerint azt jelenti, hogy a szöveget számokká alakítjuk át. Ebben az értelemben úgy titkosítjuk az üzenetet, hogy az egyik számot egy másikra cseréljük. Ha minden betűhöz egy számot rendelünk (01 az A-hoz, 02 a B-hez stb.), akkor bármely szó, például az ALICE, 01 12 09 03 05-re változik. Ha most minden számhoz hozzáadjuk a Caesar-módszer szerint hárommal nagyobb számot, az eredmény a következő lesz: 04 15 12 06 08. Ez



▲ A szkütalét vastag filccel lehet elkészíteni. Fontos megjegyezni azt a pontos helyet, ahol elkezdődik a szalag, amelyre az üzenet kerül.

▼ Stanley Kubrick 2001: Űrodüsszeia című filmjében a „gonosz” egy számítógép volt, amely az űrhajó sorsát irányította. Anélkül, hogy sok néző észrevette volna, a HAL név egy titkosított szó volt. A kulcs? Nagyon egyszerű: minden betűt az ábécé következő betűjével kell helyettesíteni. Miért volt a szó kódolva? Mert egy jelentős számítógépgyártó cégről volt szó, amely nem engedhette meg magának, hogy egyik legjobb terméke ne működjön megfelelően.

egy titkosított üzenet, amelyet eljuttathatunk valakinek, aki tudja, hogy az üzenet megfejtéséhez elegendő minden számból hárommal levonni; ez azt jelenti, hogy a „3” a titkos kulcs ehhez a titkosítási rendszerhez. Jelenleg a legvalószínűbb, hogy az üzenet az egyik számítógépről indul és a másikra érkezik, ami azt jelenti, hogy az üzenetet alkotó számok sora bináris rendszerre való átalakítás után egy hosszú „nulla” és „egy” (bit) listává alakul. Az ALICE szóra alkalmazott folyamat eredményeként a következő számok jönnek létre: 0100 1101 1100 0101 1100 1000, ami egy olyan üzenet, amely már készen áll a számítógépes hálózaton történő terjesztésre.

•Egy kis történelem

Leon Battista Alberti (1402-1472) tekinthető a nyugati kriptográfia atyjának, amelyhez a Vatikáni Kúrián belül a titkosításért felelős titkárként végzett munkájával járult hozzá. Alapvető műve a *Modus scribendi in ziferas* című értekezése, amelyben leírja a lemezek segítségével történő titkosítás módszerét, amely lehetővé tette az ábécé betűinek felcserélését. Alberti hírneve ellenére azonban a reneszánsz kriptográfia csak Trithemius apátnak köszönhetően érte el csúcspontját. Johann Heidenberg

Alapvető szókincs

Kriptográfia: a görög nyelvből származó szó, amely a *kryptos* (rejtett) és a *grafos* (írás) szavakból áll, és a titkos írásban alkalmazott művészetet, technikát vagy tudományt jelöli.

Kriptogram: titkosított üzenet.

Titkosítás: az eredeti üzenet titkosított üzenetté alakítása.

Dekódolás: a kriptogramból az eredeti üzenethez vezető folyamat.

Adatvédelem: az üzenet azon tulajdonsága, amely csak a feladó és a címzett számára teszi azt érthetővé.

Kulcs: a kommunikáló felek közötti megállapodás az üzenet titkosítására és visszafejtésére.

Hitelesítés: olyan üzenetalírás, amely megakadályozza, hogy egy harmadik fél a feladónak adja ki magát.

Titkosításelemzés: egy titkosított üzenet kulcsának visszafejtésére szolgáló technikák összessége.

Kriptológia: a kriptográfiát és a kriptanalízist magában foglaló tudományág.

