Az euklideszi algoritmusról

Ivanyos Gábor

2012 március 12

Fazekas 1969–77

Seress Ákos, IG

Tanárok a 70-es évekből

Surányi László gyűjteményéből

Elekes György

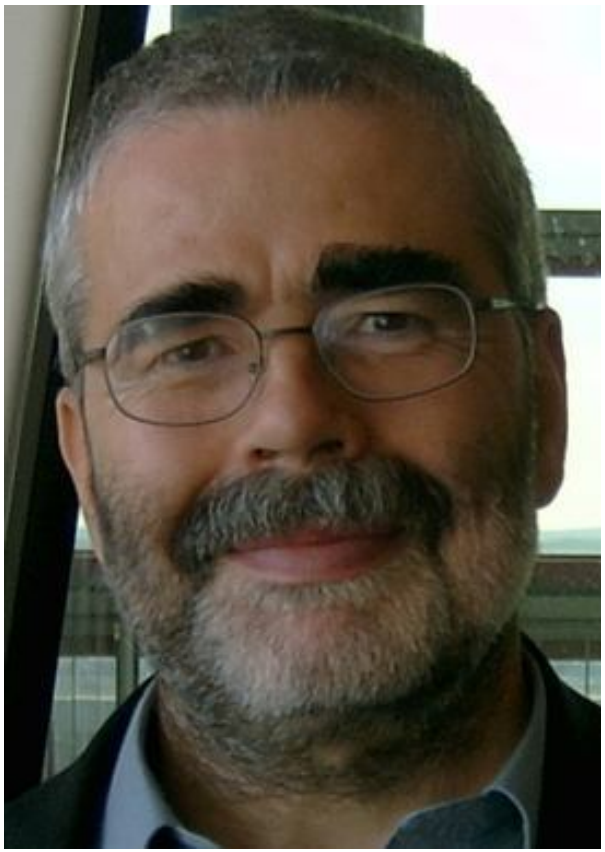
Tablókép

ELTE 1978–83

Lovász László

Pelikán József

MTA SZTAKI 1983–



Turchányi Gyula

iwiw

MTA SZTAKI 1991–; BME 1992–

Babai László

cs.uhicago.edu

Sántha Miklós

Algoritmus - mi is az

- (számítási) módszer, eljárás

Algoritmus - mi is az

- (számítási) módszer, eljárás
- (számítógépes) program, programrészlet "lényege"

Algoritmus - mi is az

- (számítási) módszer, eljárás
- (számítógépes) program, programrészlet "lényege"
- Rokonok:
  - geometriai szerkesztés
  - stratégia játékban, Rubik-kocka kirakása, papírhajtogatás, kijutás labirintusból, stb...
  - konyhai vagy kémiai recept (pl. aranycsinálás)
  - összeszerelési útmutató (pl. bútoré), gyártási eljárás, stb...

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

  Harun al-Rashid uralkodása: 786–809

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

  Harun al-Rashid uralkodása: 786–809
- Egy könyve latin átiratának (12. sz.) címe az első két szava után: *Dixit Algorizmi* = *Al Khwarizmi mondta*

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

  Harun al-Rashid uralkodása: 786–809
- Egy könyve latin átiratának (12. sz.) címe az első két szava után: *Dixit Algorizmi* = *Al Khwarizmi mondta*
- Másik cím: *Algoritmi de numero Indorum*

Algoritmus - a névadó

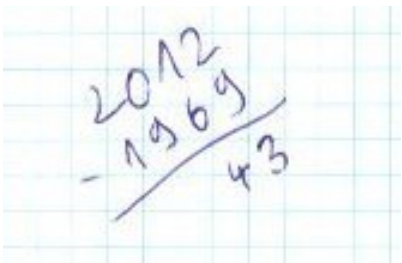
- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

  Harun al-Rashid uralkodása: 786–809
- Egy könyve latin átiratának (12. sz.) címe az első két szava után: *Dixit Algorizmi* = *Al Khwarizmi mondta*
- Másik cím: *Algoritmi de numero Indorum*
  $\approx$ *Al Khwarizmi a hindu számolás művészetéről*

Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

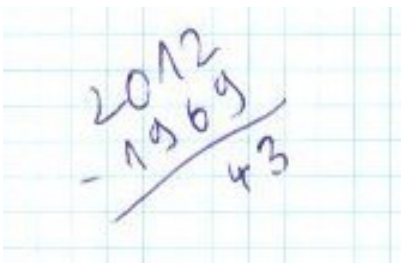
  Harun al-Rashid uralkodása: 786–809
- Egy könyve latin átiratának (12. sz.) címe az első két szava után: *Dixit Algorizmi* = *Al Khwarizmi mondta*
- Másik cím: *Algoritmi de numero Indorum*
  $\approx$ *Al Khwarizmi a hindu számolás művészetéről*



Algoritmus - a névadó

- Abu Dzsafar Muhammed ibn Musza **al-Khwarizmi**
- **Khwarezm:** tartomány $\subset$ Kelet-Perzsia (ma Üzbegisztán)
- Élt kb. 780–850-ig Bagdadban

  Harun al-Rashid uralkodása: 786–809
- Egy könyve latin átiratának (12. sz.) címe az első két szava után: *Dixit Algorizmi* = *Al Khwarizmi mondta*
- Másik cím: *Algoritmi de numero Indorum*
  $\approx$ *Al Khwarizmi a hindu számolás művészetéről*



A tízes számrendszerben történő
(hindu eredetű) számolásról
($\approx$ az iskolában tanult módszerek)

A helyiértékes számábrázolásról

- Lehetővé teszi igen nagy számok leírását

A helyiértékes számábrázolásról

- Lehetővé teszi igen nagy számok leírását
  és a velük való számolást

A helyiértékes számábrázolásról

- Lehetővé teszi igen nagy számok leírását

  és a velük való számolást
- Egy 100 jegyű szám akkora, ameddig el sem tudunk számlálni

A helyiértékes számábrázolásról

- Lehetővé teszi igen nagy számok leírását

  és a velük való számolást
- Egy 100 jegyű szám akkora, ameddig el sem tudunk számlálni
  - Az univerzum atomjainak a száma: 10^{78} és 10^{82} között

A helyiértékes számábrázolásról

- Lehetővé teszi igen nagy számok leírását

  és a velük való számolást
- Egy 100 jegyű szám akkora, ameddig el sem tudunk számlálni
  - Az univerzum atomjainak a száma: 10^{78} és 10^{82} között
  - Az univerzum kora: $< 10^{18}$ másodperc

A helyiértékes számábrázolásról

- Lehetővé teszi igen nagy számok leírását

  és a velük való számolást
- Egy 100 jegyű szám akkora, ameddig el sem tudunk számlálni
  - Az univerzum atomjainak a száma: 10^{78} és 10^{82} között
  - Az univerzum kora: $< 10^{18}$ másodperc
  - Várható leggyorsabb számítógép 2020-ban: 10^{18} lebegőpontos művelet/másodperc

Az iskolai módszerek költsége

- a, b: n jegyű számok: $n \approx \log_{10} a$

Az iskolai módszerek költsége

- a, b: n jegyű számok: $n \approx \log_{10} a$
- $a + b$ és $a - b$ számolása: n-nel arányos

Az iskolai módszerek költsége

- a, b: n jegyű számok: $n \approx \log_{10} a$
- $a + b$ és $a - b$ számolása: n-nel arányos számú művelet számjegyekkel

Az iskolai módszerek költsége

- a, b: n jegyű számok: $n \approx \log_{10} a$
- $a + b$ és $a - b$ számolása: n-nel arányos számú művelet számjegyekkel
- $a \cdot b$ és $a : b$ számolása: n^2-tel arányos

Az iskolai módszerek költsége

- a, b: n jegyű számok: $n \approx \log_{10} a$
- $a + b$ és $a - b$ számolása: n-nel arányos számú művelet számjegyekkel
- $a \cdot b$ és $a : b$ számolása: n^2-tel arányos

- (vannak elvileg gyorsabb szorzó-osztó módszerek; ezek csak nagyon nagy számokra jobbak a gyakorlatban)

Az euklideszi algoritmus - lelőhely

- Euklidesz: Elemek *(Sztoicheia)* (Alexandria, kb. i.e. 300)

Az euklideszi algoritmus - lelőhely

- Euklidesz: Elemek *(Sztoicheia)* (Alexandria, kb. i.e. 300)

- Az Elemek 7. (és 11.) könyvében szerepel az eukl. alg.

Az euklideszi algoritmus - lelőhely

- Euklidesz: Elemek *(Sztoicheia)* (Alexandria, kb. i.e. 300)

- Az Elemek 7. (és 11.) könyvében szerepel az eukl. alg.
- Jó on-line kiadás: David Joyce "fordítása":
  http://aleph0.clarku.edu/~djoyce/java/elements/elements.html

  (a kép forrása: Bill Casselman:

  http://www.math.ubc.ca/~cass/Euclid/papyrus/papyrus.html)

A legnagyobb közös osztó

Legnagyobb közös osztó $\sim$ a legnagyobb közösen kiemelhető tényező

A legnagyobb közös osztó

Legnagyobb közös osztó $\sim$ a legnagyobb közösen kiemelhető tényező

Definíció:

A legnagyobb közös osztó

Legnagyobb közös osztó $\sim$ a legnagyobb közösen kiemelhető tényező

Definíció: legyenek $a, b > 0$ egészek

A legnagyobb közös osztó

Legnagyobb közös osztó $\sim$ a legnagyobb közösen kiemelhető tényező

Definíció: legyenek $a, b > 0$ egészek
$\mathrm{lnko}(a, b) =$ a legnagyobb olyan $d > 0$ egész, amelyre $d|a$ és $d|b$.

Kiszámolható törzstényezős felbontás segítségével

A legnagyobb közös osztó

Legnagyobb közös osztó $\sim$ a legnagyobb közösen kiemelhető tényező

Definíció: legyenek $a, b > 0$ egészek
$\mathrm{lnko}(a, b) =$ a legnagyobb olyan $d > 0$ egész, amelyre $d|a$ és $d|b$.

Kiszámolható törzstényezős felbontás segítségével

Ez rossz esetben igen lassú

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával

- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával

- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

  200-nál több jegyű N-re $\sqrt{N} > 10^{100}$, **ennyi időnk nincs!**

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával

- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

  200-nál több jegyű N-re $\sqrt{N} > 10^{100}$, **ennyi időnk nincs!**

- **Nem ismert** $(\log N)^{1000}$-nel arányos idejű módszer sem

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával
- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

  200-nál több jegyű N-re $\sqrt{N} > 10^{100}$, **ennyi időnk nincs!**
- **Nem ismert** $(\log N)^{1000}$-nel arányos idejű módszer sem
- Feltételezett nehézség kihasználása: RSA titkosírás

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával
- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

  200-nál több jegyű N-re $\sqrt{N} > 10^{100}$, **ennyi időnk nincs!**
- **Nem ismert** $(\log N)^{1000}$-nel arányos idejű módszer sem
- Feltételezett nehézség kihasználása: RSA titkosírás

- 2007-ig díjak kitűzve nagy konkrét N-ek felbontására

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával
- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

  200-nál több jegyű N-re $\sqrt{N} > 10^{100}$, **ennyi időnk nincs!**
- **Nem ismert** $(\log N)^{1000}$-nel arányos idejű módszer sem
- Feltételezett nehézség kihasználása: RSA titkosírás

- 2007-ig díjak kitűzve nagy konkrét N-ek felbontására
- Felbontó projektek:
  számítógépek önkéntes hálózatán+szuperszámítógépeken

Nagy N törzstényezős felbontása nehéz (?)

- Érdemi rész: valódi osztó keresése

  $M|N$ esetén tovább M és N/M felbontásával
- Naiv módszer: $\sqrt{N}$-ig próbálkozás (osztás):

  200-nál több jegyű N-re $\sqrt{N} > 10^{100}$, **ennyi időnk nincs!**
- **Nem ismert** $(\log N)^{1000}$-nel arányos idejű módszer sem
- Feltételezett nehézség kihasználása: RSA titkosírás

- 2007-ig díjak kitűzve nagy konkrét N-ek felbontására
- Felbontó projektek:
  számítógépek önkéntes hálózatán+szuperszámítógépeken
- 2009-es rekord: 235 jegyű szám felbontása
  (két kb. 120 jegyű prímszám szorzata)

Az lnko a legjobb felbontó algoritmusokban

- a munka nehéz része: keressünk olyan N-nél kisebb M-et, amelyre $\text{lnko}(N, M) > 1$

Az lnko a legjobb felbontó algoritmusokban

- a munka nehéz része: keressünk olyan N-nél kisebb M-et, amelyre $\text{lnko}(N, M) > 1$
- a próbálgatásnál sokkal okosabb és gyorsabb módszerek vannak "szerencsés" M keresésére

Az lnko a legjobb felbontó algoritmusokban

- a munka nehéz része: keressünk olyan N-nél kisebb M-et, amelyre $\text{lnko}(N, M) > 1$
- a próbálgatásnál sokkal okosabb és gyorsabb módszerek vannak "szerencsés" M keresésére
- "szerencsés" M birtokában
  az euklideszi algoritmussal kiszámoljuk $\text{lnko}(N, M)$-et

Az lnko a legjobb felbontó algoritmusokban

- a munka nehéz része: keressünk olyan N-nél kisebb M-et, amelyre $\text{lnko}(N, M) > 1$
- a próbálgatásnál sokkal okosabb és gyorsabb módszerek vannak "szerencsés" M keresésére
- "szerencsés" M birtokában

  az euklideszi algoritmussal kiszámoljuk $\text{lnko}(N, M)$-et

  $\text{lnko}(M, N)$ valódi osztója N-nek

Az euklideszi algoritmus alapötlete

Legyenek a és b egészek.

Észrevétel: Ha d közös osztója a-nak és b-nek, akkor d közös osztója a-nak és $b \pm a$-nak.

Az euklideszi algoritmus alapötlete

Legyenek a és b egészek.

Észrevétel: Ha d közös osztója a-nak és b-nek, akkor d közös osztója a-nak és $b \pm a$-nak.

Biz.: Tegyük fel, hogy $b = db'$, $a = da'$. Ekkor $b \pm a = d(b' \pm a')$.

Az euklideszi algoritmus alapötlete

Legyenek a és b egészek.

Észrevétel: Ha d közös osztója a-nak és b-nek, akkor d közös osztója a-nak és $b \pm a$-nak.

Biz.: Tegyük fel, hogy $b = db'$, $a = da'$. Ekkor $b \pm a = d(b' \pm a')$.

Következmény: $\{a \text{ és } b \text{ közös osztói}\} = \{a \text{ és } b - a \text{ közös osztói}\}$

Az euklideszi algoritmus alapötlete

Legyenek a és b egészek.

Észrevétel: Ha d közös osztója a-nak és b-nek, akkor d közös osztója a-nak és $b \pm a$-nak.

Biz.: Tegyük fel, hogy $b = db'$, $a = da'$. Ekkor $b \pm a = d(b' \pm a')$.

Következmény: $\{a \text{ és } b \text{ közös osztói}\} = \{a \text{ és } b - a \text{ közös osztói}\}$

Következmény: $\text{lnko}(a, b) = \text{lnko}(a, b - a)$.

Az euklideszi algoritmus - elegáns változat

Tudjuk: $b > a$ esetén $\text{lnko}(a, b) = \text{lnko}(a, b - a)$

Az euklideszi algoritmus - elegáns változat

Tudjuk: $b > a$ esetén $\text{lnko}(a, b) = \text{lnko}(a, b - a)$

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

Az euklideszi algoritmus - elegáns változat

Tudjuk: $b > a$ esetén $\text{lnko}(a, b) = \text{lnko}(a, b - a)$

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

Az euklideszi algoritmus - elegáns változat

Tudjuk: $b > a$ esetén $\text{lnko}(a, b) = \text{lnko}(a, b - a)$

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

(2) Legyen $b \longleftarrow b - a$

Az euklideszi algoritmus - elegáns változat

Tudjuk: $b > a$ esetén $\text{lnko}(a, b) = \text{lnko}(a, b - a)$

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

(2) Legyen $b \longleftarrow b - a$

(3) Ha $a > b$, akkor $a \longleftrightarrow b$

Az euklideszi algoritmus - elegáns változat

Tudjuk: $b > a$ esetén $\text{lnko}(a, b) = \text{lnko}(a, b - a)$

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

(2) Legyen $b \longleftarrow b - a$

(3) Ha $a > b$, akkor $a \longleftrightarrow b$

Újra (1)-től.

Az euklideszi algoritmus - elegáns változat

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

(2) Legyen $b \longleftarrow b - a$

(3) Ha $a > b$, akkor $a \longleftrightarrow b$

Újra (1)-től.

Az euklideszi algoritmus - eredeti változat

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

(3') $a \longleftrightarrow b$

Újra (1)-től.

Az eredeti változat lassú lehet

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

Az eredeti változat lassú lehet

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

Előfordulhat, hogy a sokkal kisebb lesz, mint b

Az eredeti változat lassú lehet

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

Előfordulhat, hogy a sokkal kisebb lesz, mint b

Például $a \approx \sqrt{b}$ és b 200 jegyű

Az eredeti változat lassú lehet

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

Előfordulhat, hogy a sokkal kisebb lesz, mint b

Például $a \approx \sqrt{b}$ és b 200 jegyű

Ekkor kb. $b/a \approx 10^{100}$ kivonás lenne

Az eredeti változat lassú lehet

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

Előfordulhat, hogy a sokkal kisebb lesz, mint b

Például $a \approx \sqrt{b}$ és b 200 jegyű

Ekkor kb. $b/a \approx 10^{100}$ kivonás lenne

Ez reménytelenül sok!

Az euklideszi algoritmus - eredeti változat

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény a.

(2') Ameddig $b \geq a$, legyen $b \longleftarrow b - a$

(3') $a \longleftrightarrow b$

Újra (1)-től.

Az euklideszi algoritmus - maradékos osztással

Ciklus:

Feltételek: $0 \leq a \leq b$ egészek

(1) Ha $a = 0$, akkor kész; az eredmény b.

(2") Legyen $b \longleftarrow b\%a$ $\qquad (b\%a = b - a\lfloor b/a \rfloor)$

(3') $a \longleftrightarrow b$

Újra (1)-től.

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1}$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell$,

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$

  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$
  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér
- **Két lépés után** (ha $a_{\ell+1} \neq 0$):

$$a_{\ell+2}$$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$
  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér
- **Két lépés után** (ha $a_{\ell+1} \neq 0$):

$$a_{\ell+2} \quad = \quad b_{\ell+1} \% a_{\ell+1}$$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$
  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér
- **Két lépés után** (ha $a_{\ell+1} \neq 0$):

$$\begin{aligned} a_{\ell+2} &= b_{\ell+1} \% a_{\ell+1} \\ &= a_\ell \% a_{\ell+1} \end{aligned}$$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$
  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér
- **Két lépés után** (ha $a_{\ell+1} \neq 0$):

$$\begin{aligned} a_{\ell+2} &= b_{\ell+1} \% a_{\ell+1} \\ &= a_\ell \% a_{\ell+1} \\ &\leq a_\ell - a_{\ell+1} \end{aligned}$$

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$
  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér
- **Két lépés után** (ha $a_{\ell+1} \neq 0$):

$$\begin{aligned} a_{\ell+2} &= b_{\ell+1} \% a_{\ell+1} \\ &= a_\ell \% a_{\ell+1} \\ &\leq a_\ell - a_{\ell+1} \end{aligned}$$

- Tehát $a_{\ell+2} \leq a_\ell - a_{\ell+1}$,

Az euklideszi algoritmus elemzése

- **Jelölés:** a_ℓ, b_ℓ az "a, b" értéke ℓ lépés után.
  (Mostantól a, b az eredeti (a bemenő) a, b-t jelöli!)
  $a_0 = a,\ b_0 = b$
- **Feltétel:** $0 < a_\ell \leq b_\ell$
- **Egy lépés eredménye:** $a_{\ell+1} = b_\ell \% a_\ell < a_\ell,\ b_{\ell+1} = a_\ell.$
  $a_{\ell+1} < a_\ell$, tehát előbb-utóbb véget ér
- **Két lépés után** (ha $a_{\ell+1} \neq 0$):

$$\begin{aligned} a_{\ell+2} &= b_{\ell+1} \% a_{\ell+1} \\ &= a_\ell \% a_{\ell+1} \\ &\leq a_\ell - a_{\ell+1} \end{aligned}$$

- Tehát $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.
- Innen $a_\ell \geq a_{\ell+1} + a_{\ell+2} \geq a_{\ell+2} + a_{\ell+2} = 2a_{\ell+2}$,

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.
- Innen $a_\ell \geq a_{\ell+1} + a_{\ell+2} \geq a_{\ell+2} + a_{\ell+2} = 2a_{\ell+2}$,
- Azaz: $a_{\ell+2} \leq \frac{1}{2} a_\ell$.

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.
- Innen $a_\ell \geq a_{\ell+1} + a_{\ell+2} \geq a_{\ell+2} + a_{\ell+2} = 2a_{\ell+2}$,
- Azaz: $a_{\ell+2} \leq \frac{1}{2} a_\ell$.
- a_ℓ két lépésben feleződik (vagy még kisebb lesz)

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.
- Innen $a_\ell \geq a_{\ell+1} + a_{\ell+2} \geq a_{\ell+2} + a_{\ell+2} = 2a_{\ell+2}$,
- Azaz: $a_{\ell+2} \leq \frac{1}{2} a_\ell$.
- a_ℓ két lépésben feleződik (vagy még kisebb lesz)
- Ebből: $a_{2\ell} \leq \frac{1}{2^\ell} a_0$.

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.
- Innen $a_\ell \geq a_{\ell+1} + a_{\ell+2} \geq a_{\ell+2} + a_{\ell+2} = 2a_{\ell+2}$,
- Azaz: $a_{\ell+2} \leq \frac{1}{2} a_\ell$.
- a_ℓ két lépésben feleződik (vagy még kisebb lesz)
- Ebből: $a_{2\ell} \leq \frac{1}{2^\ell} a_0$.
- Innen: a ciklus lefutásainak száma
  $\leq 2 \cdot \log_2 a = \text{konstans} \cdot \log_{10} a$

Az euklideszi algoritmus elemzése

- Előző oldalról: $a_\ell \geq a_{\ell+1} + a_{\ell+2}$.
- Innen $a_\ell \geq a_{\ell+1} + a_{\ell+2} \geq a_{\ell+2} + a_{\ell+2} = 2a_{\ell+2}$,
- Azaz: $a_{\ell+2} \leq \frac{1}{2} a_\ell$.
- a_ℓ két lépésben feleződik (vagy még kisebb lesz)
- Ebből: $a_{2\ell} \leq \frac{1}{2^\ell} a_0$.
- Innen: a ciklus lefutásainak száma
  $\leq 2 \cdot \log_2 a = \text{konstans} \cdot \log_{10} a$
- Összköltség: $(\log_{10} a)^3$-nel arányos

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$,

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz

  $$a_\ell \geq a_{\ell+1} + a_{\ell+2}$$

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz

  $$a_\ell \geq a_{\ell+1} + a_{\ell+2}$$

- Leglassabban csökken, ha egyenlőség teljesül:

  $$a_\ell = a_{\ell+1} + a_{\ell+2}$$

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz

  $$a_\ell \geq a_{\ell+1} + a_{\ell+2}$$

- Leglassabban csökken, ha egyenlőség teljesül:

  $$a_\ell = a_{\ell+1} + a_{\ell+2}$$

- a Fibonacci-sorozat rekurziója, csak fordítva indexelve

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz

  $$a_\ell \geq a_{\ell+1} + a_{\ell+2}$$

- Leglassabban csökken, ha egyenlőség teljesül:

  $$a_\ell = a_{\ell+1} + a_{\ell+2}$$

- a Fibonacci-sorozat rekurziója, csak fordítva indexelve
- Fibonacci-számok: $F_1 = 1$, $F_2 = 2$,

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz

  $$a_\ell \geq a_{\ell+1} + a_{\ell+2}$$

- Leglassabban csökken, ha egyenlőség teljesül:

  $$a_\ell = a_{\ell+1} + a_{\ell+2}$$

- a Fibonacci-sorozat rekurziója, csak fordítva indexelve
- Fibonacci-számok: $F_1 = 1$, $F_2 = 2$, $F_\ell = F_{\ell-2} + F_{\ell-1}$ $(\ell > 2)$

Pontosabb elemzés: a Fibonacci-számok

- **Tudjuk:** $a_{\ell+2} \leq a_\ell - a_{\ell+1}$, azaz

  $$a_\ell \geq a_{\ell+1} + a_{\ell+2}$$

- Leglassabban csökken, ha egyenlőség teljesül:

  $$a_\ell = a_{\ell+1} + a_{\ell+2}$$

- a Fibonacci-sorozat rekurziója, csak fordítva indexelve
- Fibonacci-számok: $F_1 = 1$, $F_2 = 2$, $F_\ell = F_{\ell-2} + F_{\ell-1}$ $(\ell > 2)$
- Belátható, hogy $a_\ell \leq \frac{1}{F_{\ell+1}} a_0$.

Lánctörtbe fejtés

Elemek 11. könyv:

Euklideszi algoritmus tetszőleges $0 < a \leq b$-re

(1) $b \longleftarrow b - a \cdot \lfloor b/a \rfloor$

(2) Ha $b = 0$, akkor kész.

(3) Különben $b \longleftrightarrow a$ és folytatjuk (1)-től

Lánctörtbe fejtés

Elemek 11. könyv:

Euklideszi algoritmus tetszőleges $0 < a \leq b$-re

(1) $b \longleftarrow b - a \cdot \lfloor b/a \rfloor$

(2) Ha $b = 0$, akkor kész.

(3) Különben $b \longleftrightarrow a$ és folytatjuk (1)-től

$\gamma = b/a$-val

Lánctörtbe fejtés

Elemek 11. könyv:

Euklideszi algoritmus tetszőleges $0 < a \leq b$-re

(1) $b \longleftarrow b - a \cdot \lfloor b/a \rfloor$

(2) Ha $b = 0$, akkor kész.

(3) Különben $b \longleftrightarrow a$ és folytatjuk (1)-től

$\gamma = b/a$-val

(1) $\gamma \longleftarrow \{\gamma\}$

(2) Ha $\gamma = 0$, akkor kész

(3) Különben $\gamma \longleftarrow 1/\gamma$ és folytatjuk (1)-től

Lánctörtbe fejtés

Az előző eljárás átszervezve és

tartalommal megtöltve

(1) $\gamma = \lfloor\gamma\rfloor + \{\gamma\}$

(*) feljegyezzük $\lfloor\gamma\rfloor$-t

(2) Ha $\{\gamma\} = 0$, akkor kész

(3) Különben folytatjuk γ helyett $1/\{\gamma\}$-val

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma \quad = \quad 1 +$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma \quad = \quad 1 + \frac{1}{\gamma_1}$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma = 1 + \frac{1}{\gamma_1} = 1 + \cfrac{1}{2 + }$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma \quad = \quad 1 + \frac{1}{\gamma_1} = 1 + \cfrac{1}{2 + \cfrac{1}{\gamma_2}}$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma = 1 + \frac{1}{\gamma_1} = 1 + \frac{1}{2 + \frac{1}{\gamma_2}} = 1 + \frac{1}{2 + \frac{1}{2 + }}$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma = 1 + \frac{1}{\gamma_1} = 1 + \frac{1}{2 + \frac{1}{\gamma_2}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\gamma_3}}}$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma = 1 + \frac{1}{\gamma_1} = 1 + \frac{1}{2 + \frac{1}{\gamma_2}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\gamma_3}}}$$

$$= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\gamma_4}}}}$$

Példa: $\sqrt{2}$ lánctört alakja

$$\sqrt{2} = \gamma = 1 + \frac{1}{\gamma_1} = 1 + \frac{1}{2 + \frac{1}{\gamma_2}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\gamma_3}}}$$

$$= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\gamma_4}}}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}}}$$

$\sqrt{2}$ lánctört alakja - bizonyítás

- Trükk: $\sqrt{2}$ helyett $1 + \sqrt{2}$-re bizonyítunk.

$\sqrt{2}$ lánctört alakja - bizonyítás

- Trükk: $\sqrt{2}$ helyett $1+\sqrt{2}$-re bizonyítunk.
- Legyen $x = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}$

$\sqrt{2}$ lánctört alakja - bizonyítás

- Trükk: $\sqrt{2}$ helyett $1+\sqrt{2}$-re bizonyítunk.
- Legyen $x = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}$
- Be kéne látni, hogy $x = 1 + \sqrt{2}$.

$\sqrt{2}$ lánctört alakja - bizonyítás

- Trükk: $\sqrt{2}$ helyett $1+\sqrt{2}$-re bizonyítunk.
- Legyen $x = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}$
- Be kéne látni, hogy $x = 1 + \sqrt{2}$.
- Észrevétel: $x = 2 + \frac{1}{x}$,

$\sqrt{2}$ lánctört alakja - bizonyítás

- Trükk: $\sqrt{2}$ helyett $1+\sqrt{2}$-re bizonyítunk.
- Legyen $x = 2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}}}$
- Be kéne látni, hogy $x = 1 + \sqrt{2}$.

- Észrevétel: $x = 2 + \frac{1}{x}$,
- amiből $x^2 = 2x + 1$.

$\sqrt{2}$ lánctört alakja - bizonyítás

x olyan pozitív szám, amelyre

$$x^2 = 2x + 1$$

$\sqrt{2}$ lánctört alakja - bizonyítás

x olyan pozitív szám, amelyre

$$x^2 = 2x + 1$$

$$x^2 - 2x + 1 = 2$$

$$(x-1)^2 = 2$$

$$x - 1 = \pm\sqrt{2}$$

$$x = 1 \pm \sqrt{2}$$

$1 - \sqrt{2}$ negatív, tehát

$\sqrt{2}$ lánctört alakja - bizonyítás

x olyan pozitív szám, amelyre

$$x^2 = 2x + 1$$

$$x^2 - 2x + 1 = 2$$

$$(x-1)^2 = 2$$

$$x - 1 = \pm\sqrt{2}$$

$$x = 1 \pm \sqrt{2}$$

$1 - \sqrt{2}$ negatív, tehát

$$x = 1 + \sqrt{2}.$$

Véges és periodikus lánctörtek

- γ lánctörtalakja véges $\Leftrightarrow$ γ racionális

Véges és periodikus lánctörtek

- γ lánctörtalakja véges $\Leftrightarrow$ γ racionális
- **Periodikus lánctört:** $\sqrt{2}$ vagy pl.

$$1+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{4+\cdots}}}}}}}$$

Véges és periodikus lánctörtek

- γ lánctörtalakja véges $\Leftrightarrow$ γ racionális
- **Periodikus lánctört:** $\sqrt{2}$ vagy pl.

$$1+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{3+\cfrac{1}{4+\cdots}}}}}}}$$

- **Tétel:** γ lánctörtalakja periodikus $\Leftrightarrow$ γ pozitív kvadratikus szám: egy racionális együtthatós másodfokú egyenlet pozitív gyöke

$\sqrt{2}$ közelítése csonkított lánctörtekkel

$$\sqrt{2} \approx 1.41421$$

$$1 + \frac{1}{2} = \frac{3}{2} = 1.50000$$

$\sqrt{2}$ közelítése csonkított lánctörtekkel

$$\sqrt{2} \approx 1.41421$$

$$1 + \cfrac{1}{2 + \cfrac{1}{2}} = \frac{7}{5} = 1.40000$$

$\sqrt{2}$ közelítése csonkított lánctörtekkel

$$\sqrt{2} \approx 1.41421$$

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}} = \frac{17}{12} \approx 1.41666$$

$\sqrt{2}$ közelítése csonkított lánctörtekkel

$$\sqrt{2} \approx 1.41421$$

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}}} = \frac{41}{29} \approx 1.41379$$

$\sqrt{2}$ közelítése csonkított lánctörtekkel

$$\sqrt{2} \approx 1.41421$$

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2}}}}} = \frac{99}{70} = \approx 1.41428$$

Nicsak: $\frac{99}{70} = \frac{297}{210}$ és 210x297mm: az A4-es lap mérete

A leglassabban közelítő lánctört

$$1 + \frac{1}{1} = \frac{2}{1} = 2$$

A leglassabban közelítő lánctört

$$1 + \cfrac{1}{1 + \cfrac{1}{1}} = \frac{3}{2} = 1.5$$

A leglassabban közelítő lánctört

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}} = \frac{5}{3} \approx 1.66666$$

A leglassabban közelítő lánctört

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1}}}} = \frac{8}{5} = 1.60000$$

A leglassabban közelítő lánctört

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{1}}}}}} = \frac{13}{8} = 1.62500$$

A leglassabban közelítő lánctört

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}}}}} = \frac{21}{13} \approx 1.61538$$

A leglassabban közelítő lánctört

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{1}}}}}}}} = \frac{34}{21} \approx 1.61905$$

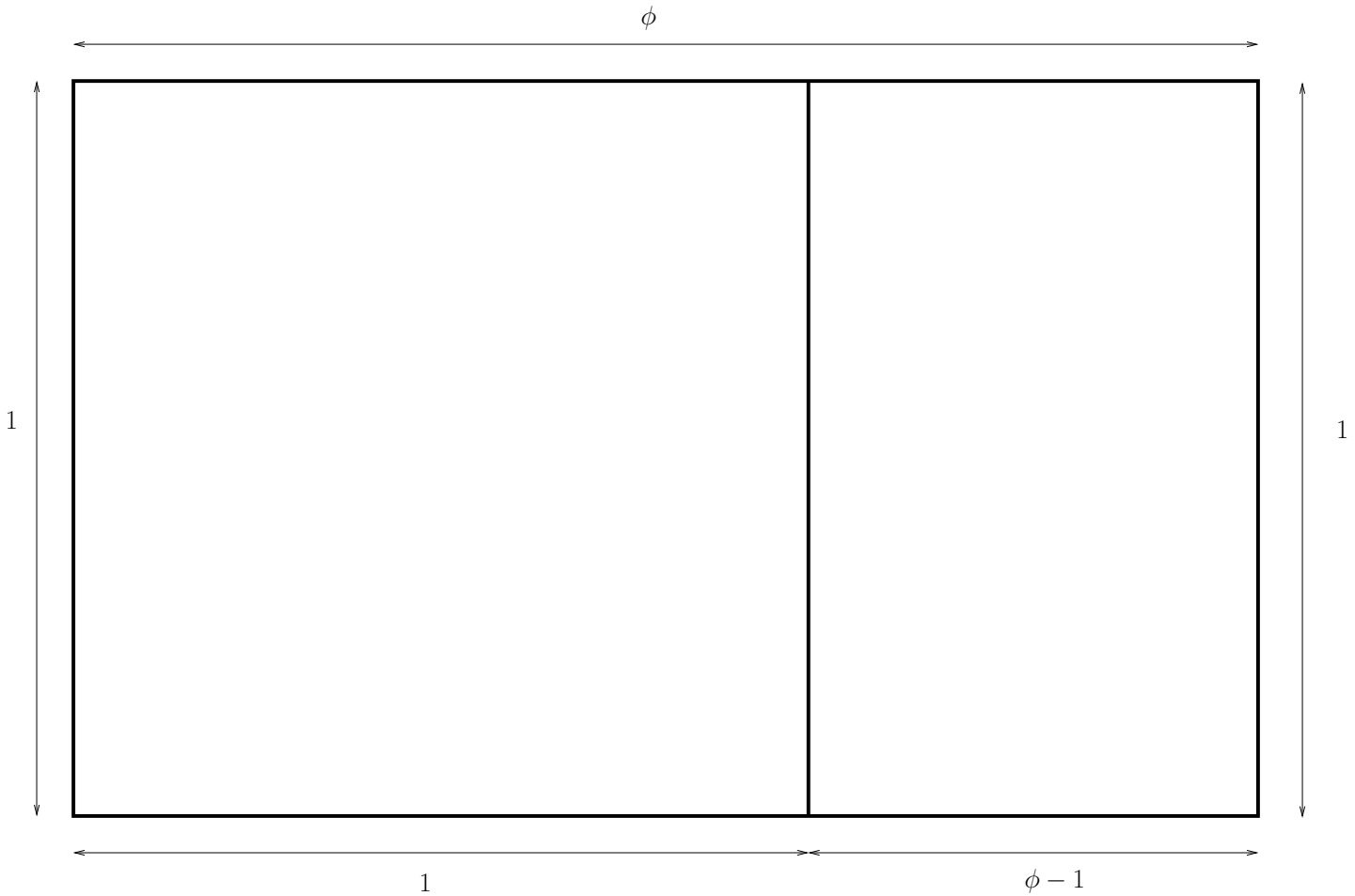
A leglassabban közelítő lánctört

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}}}}}}}=\frac{55}{34}\approx 1.61765$$

A leglassabban közelítő lánctört

$$1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1}}}}}}}}}}=\frac{89}{55}\approx 1.61818$$

Arany téglalap

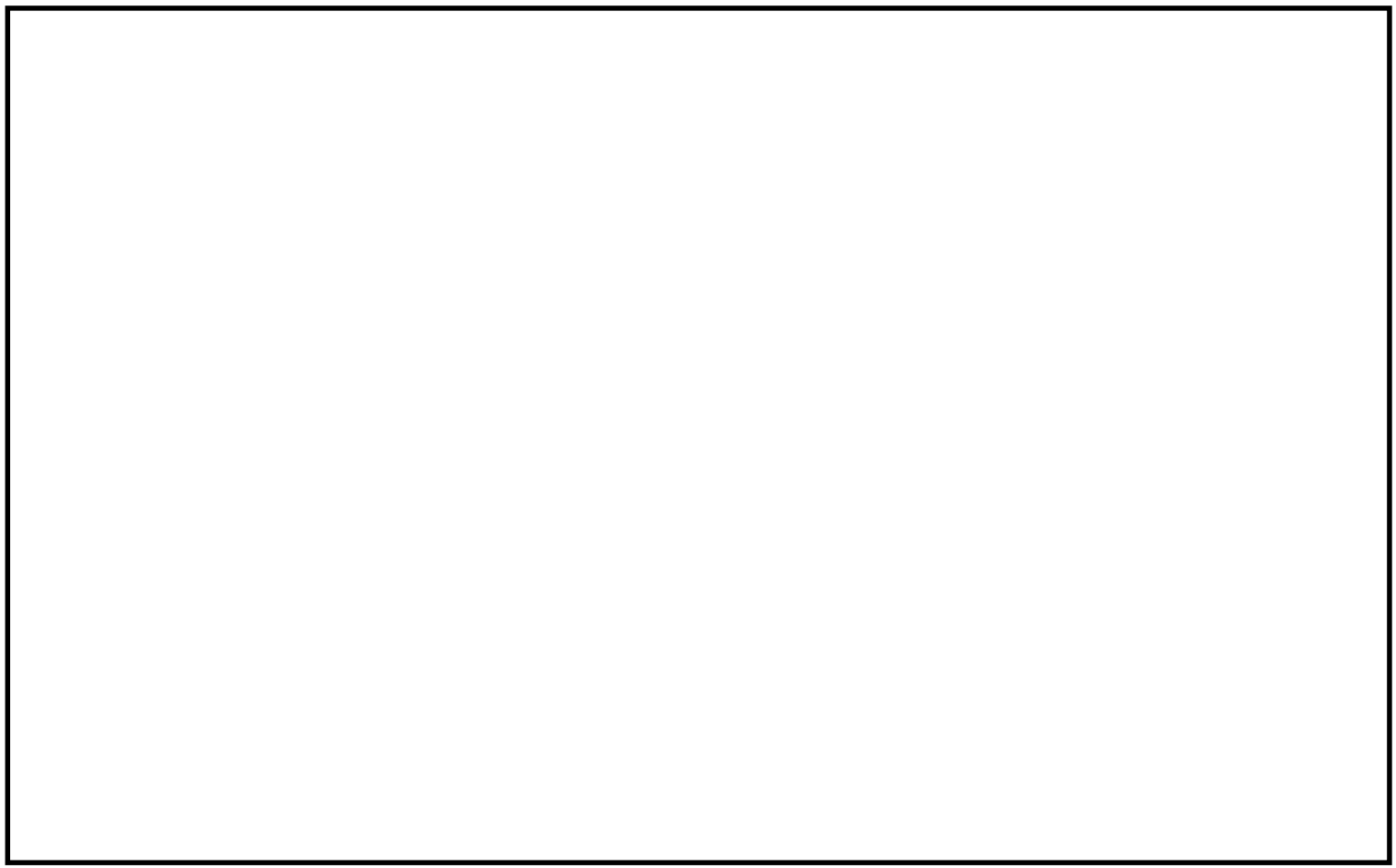


$$\frac{\phi}{1} = \frac{1}{\phi - 1}$$

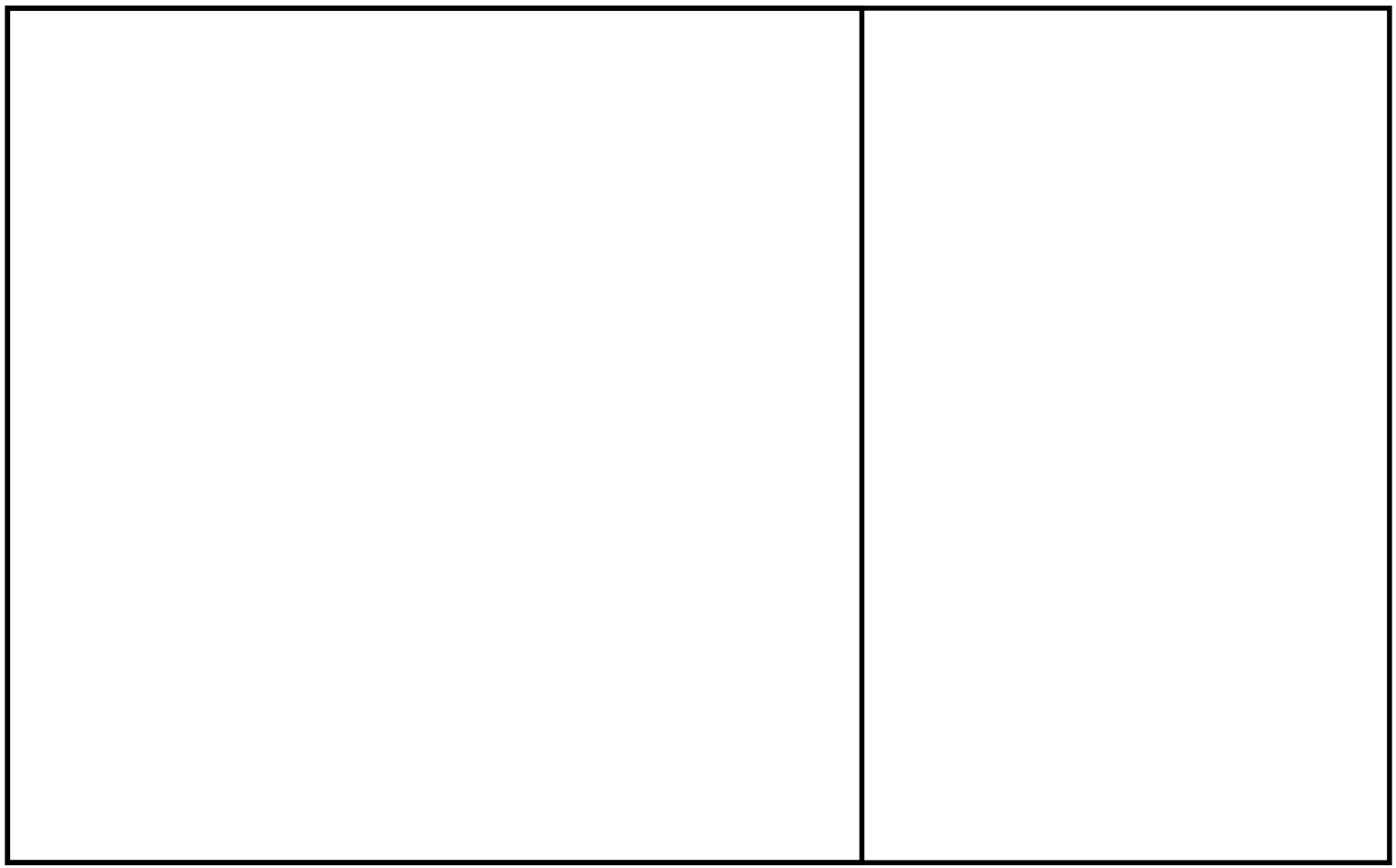
Az e szám lánctört-alakja

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{8 + \ldots}}}}}}}}}}}$$

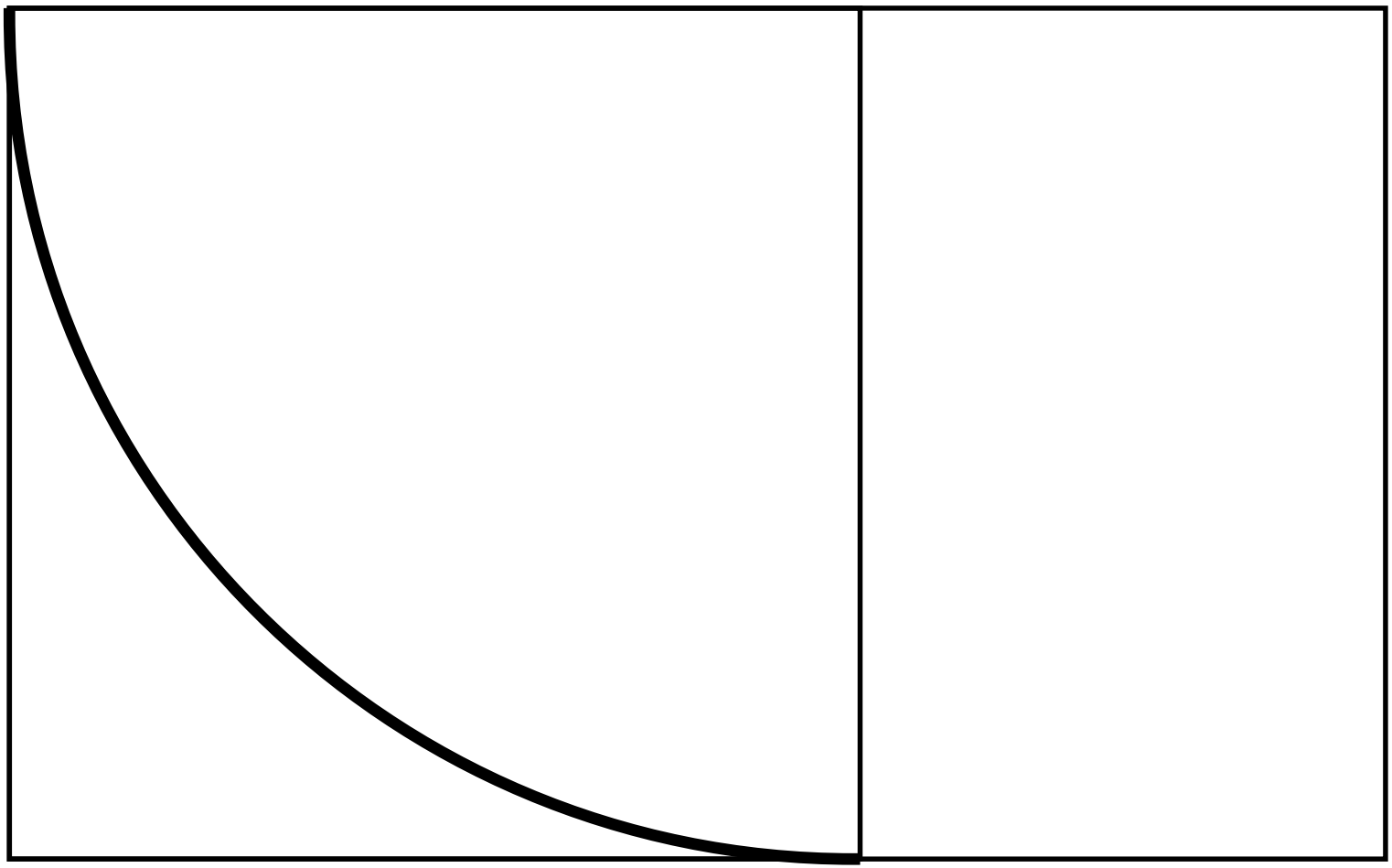
A Fibonacci-spirál



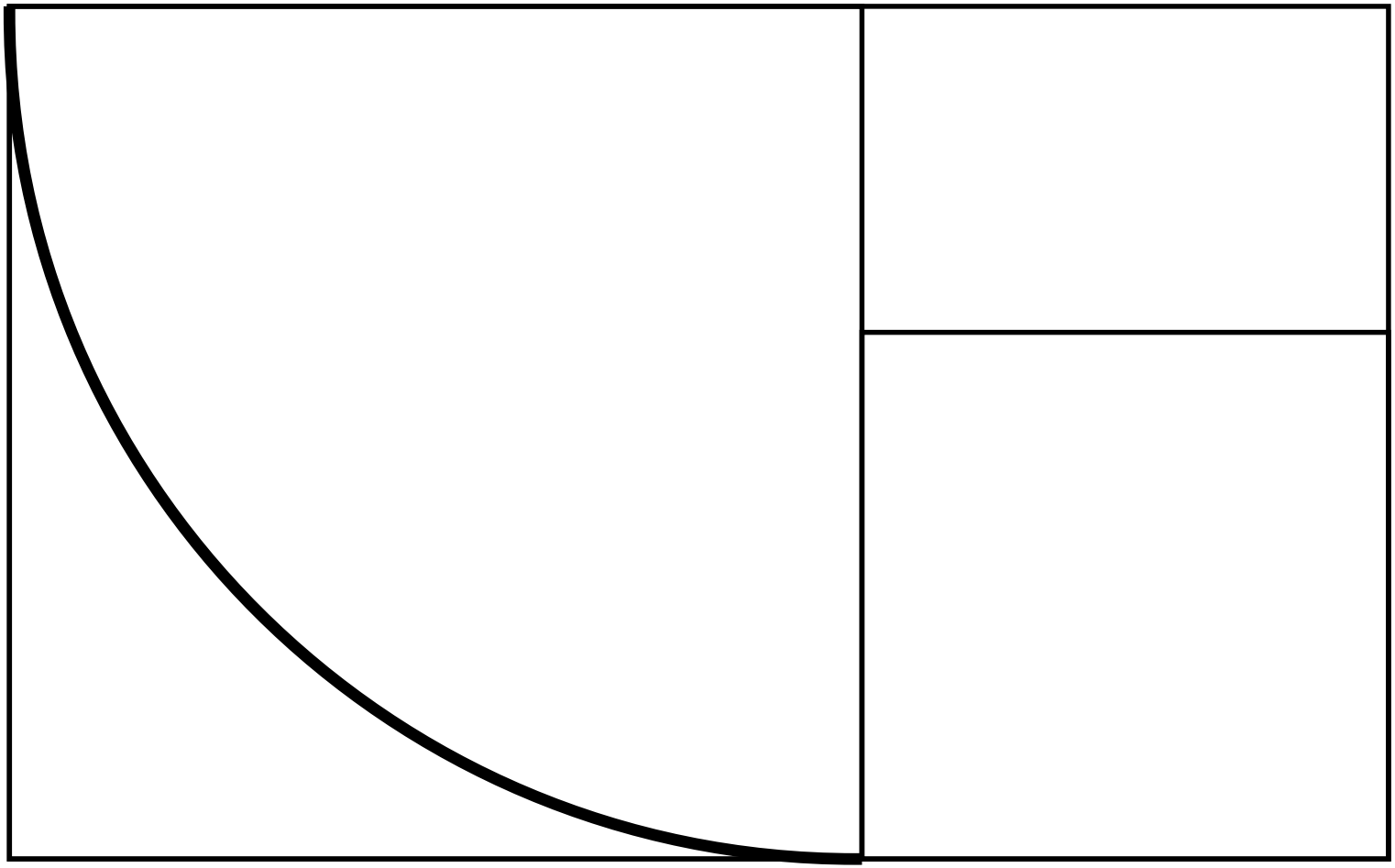
A Fibonacci-spirál



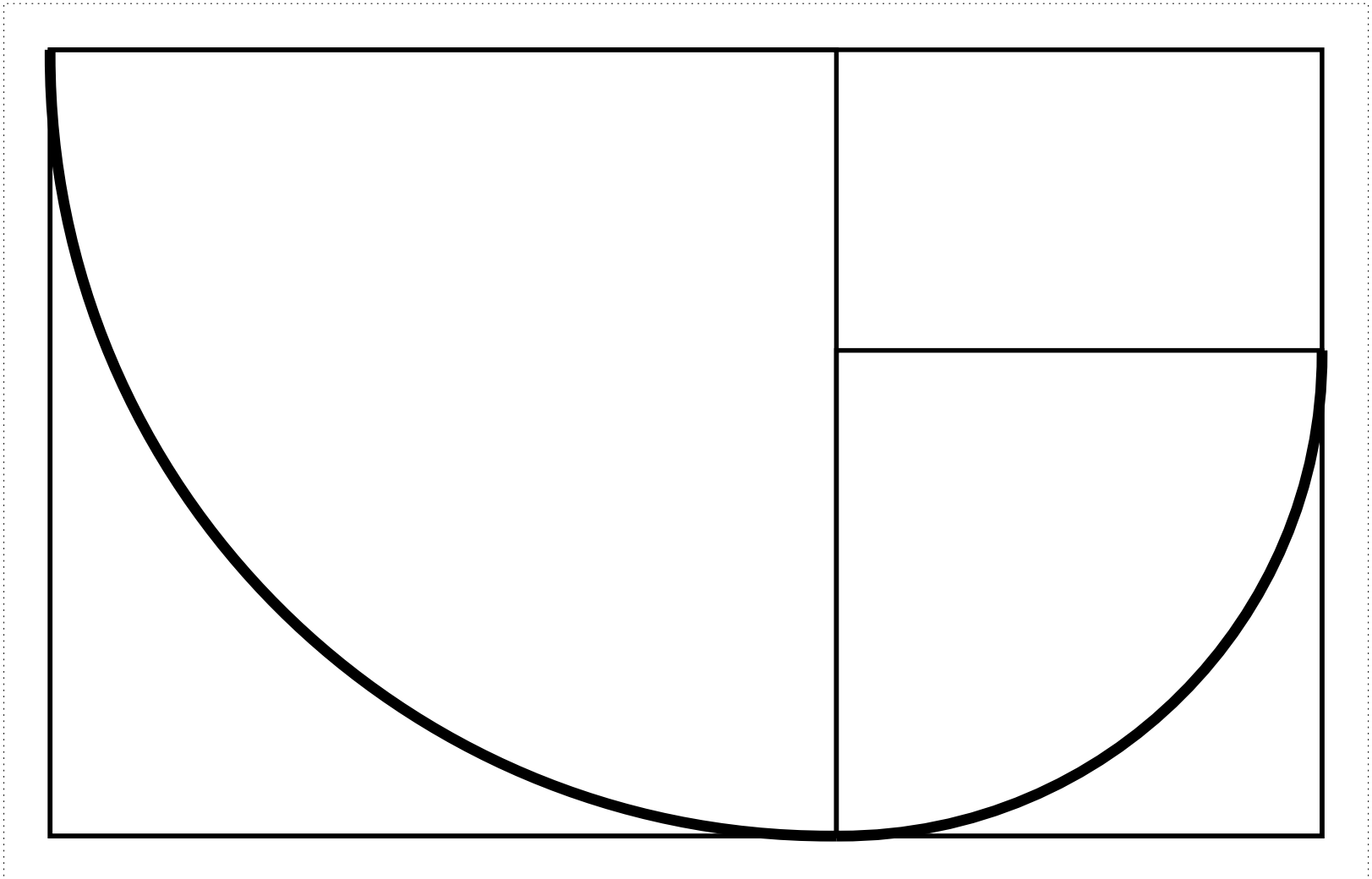
A Fibonacci-spirál



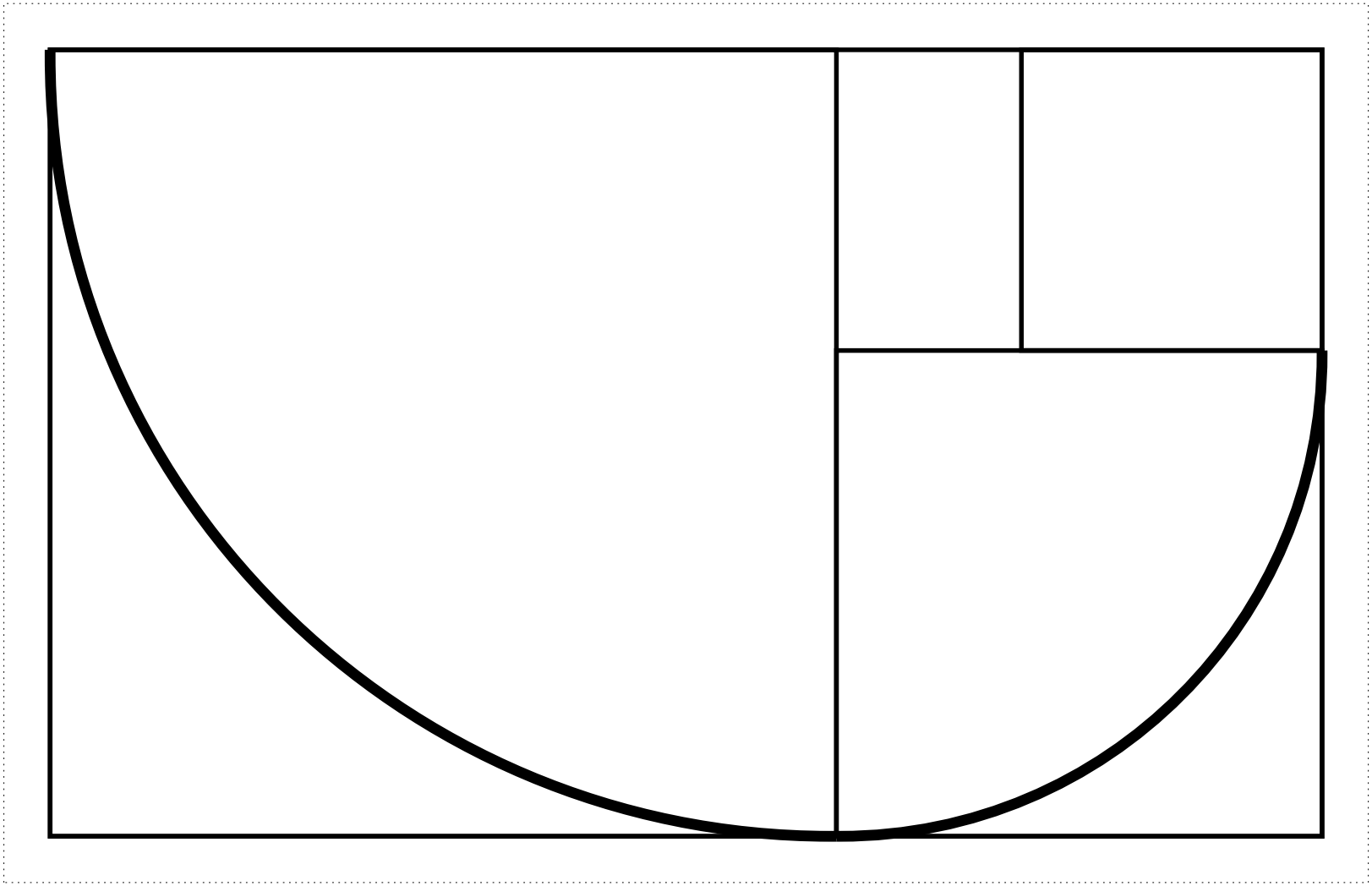
A Fibonacci-spirál



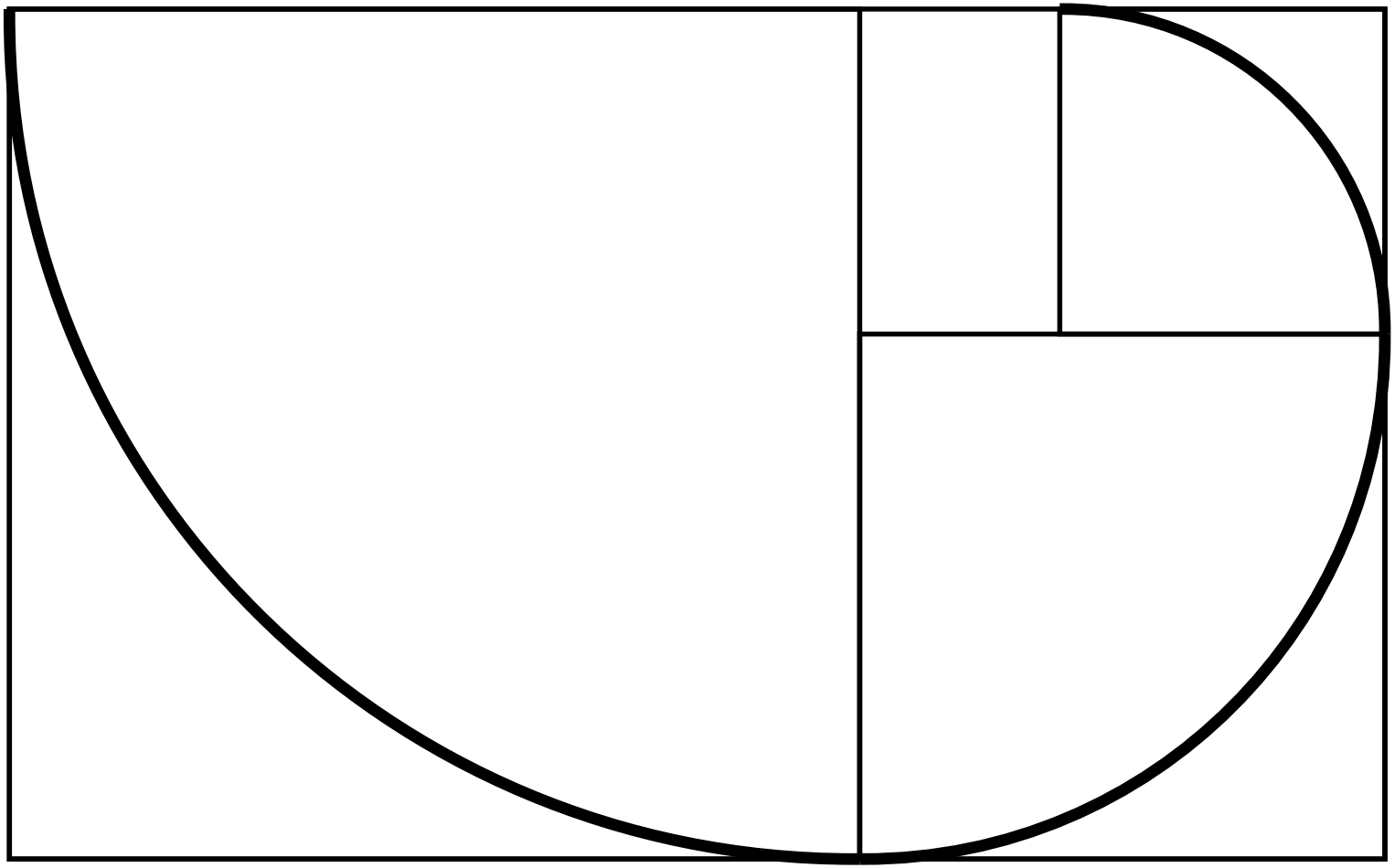
A Fibonacci-spirál



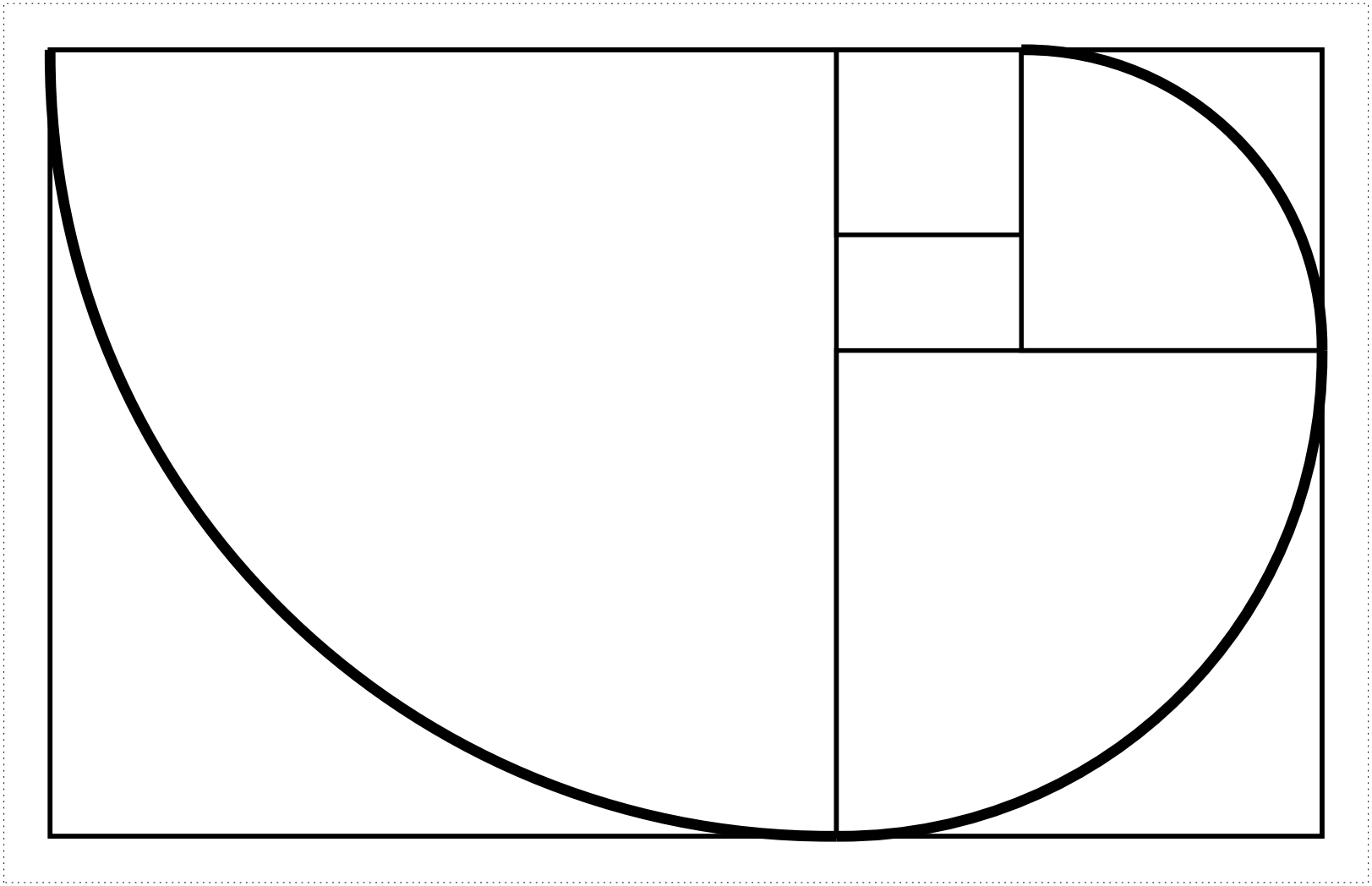
A Fibonacci-spirál



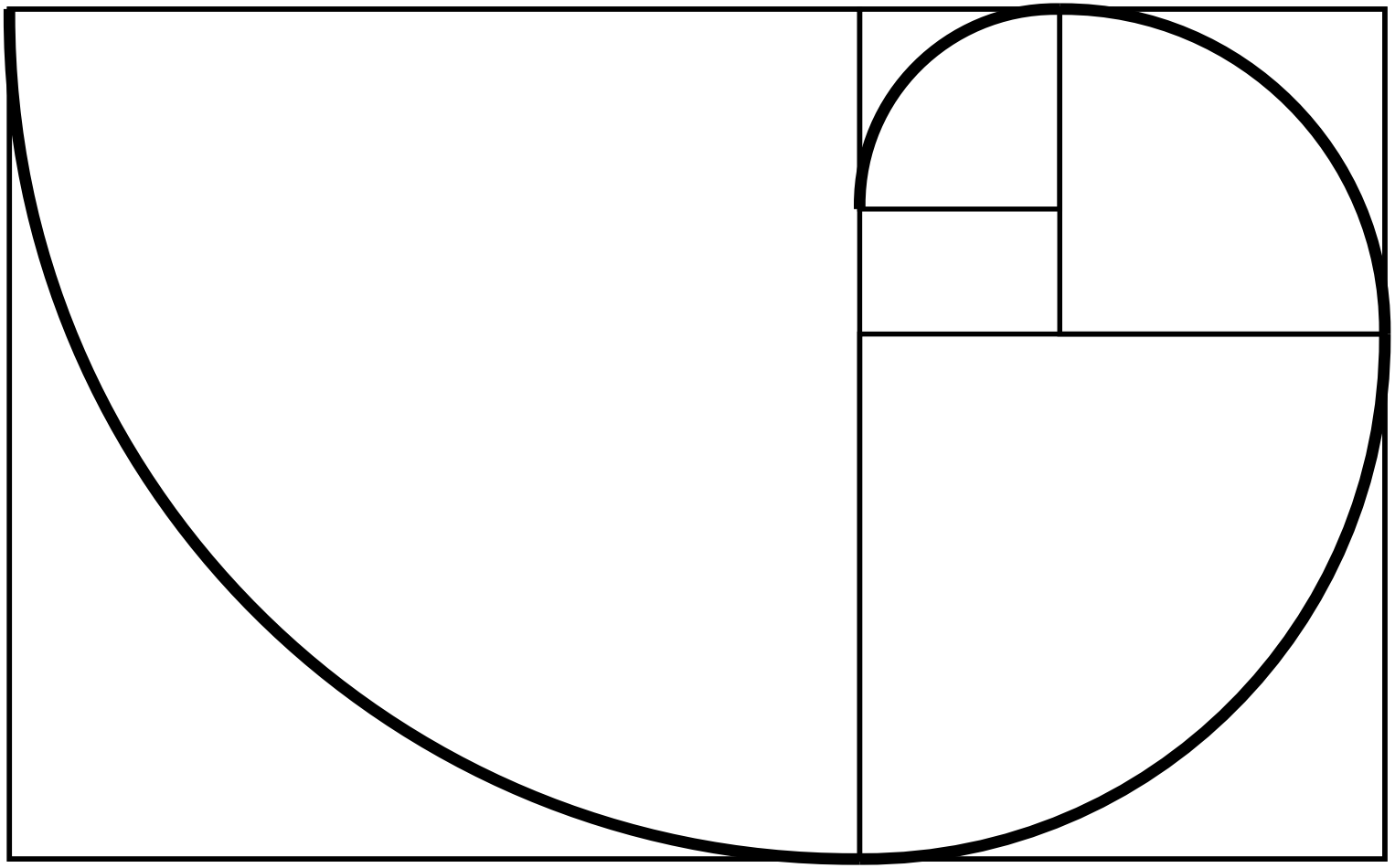
A Fibonacci-spirál



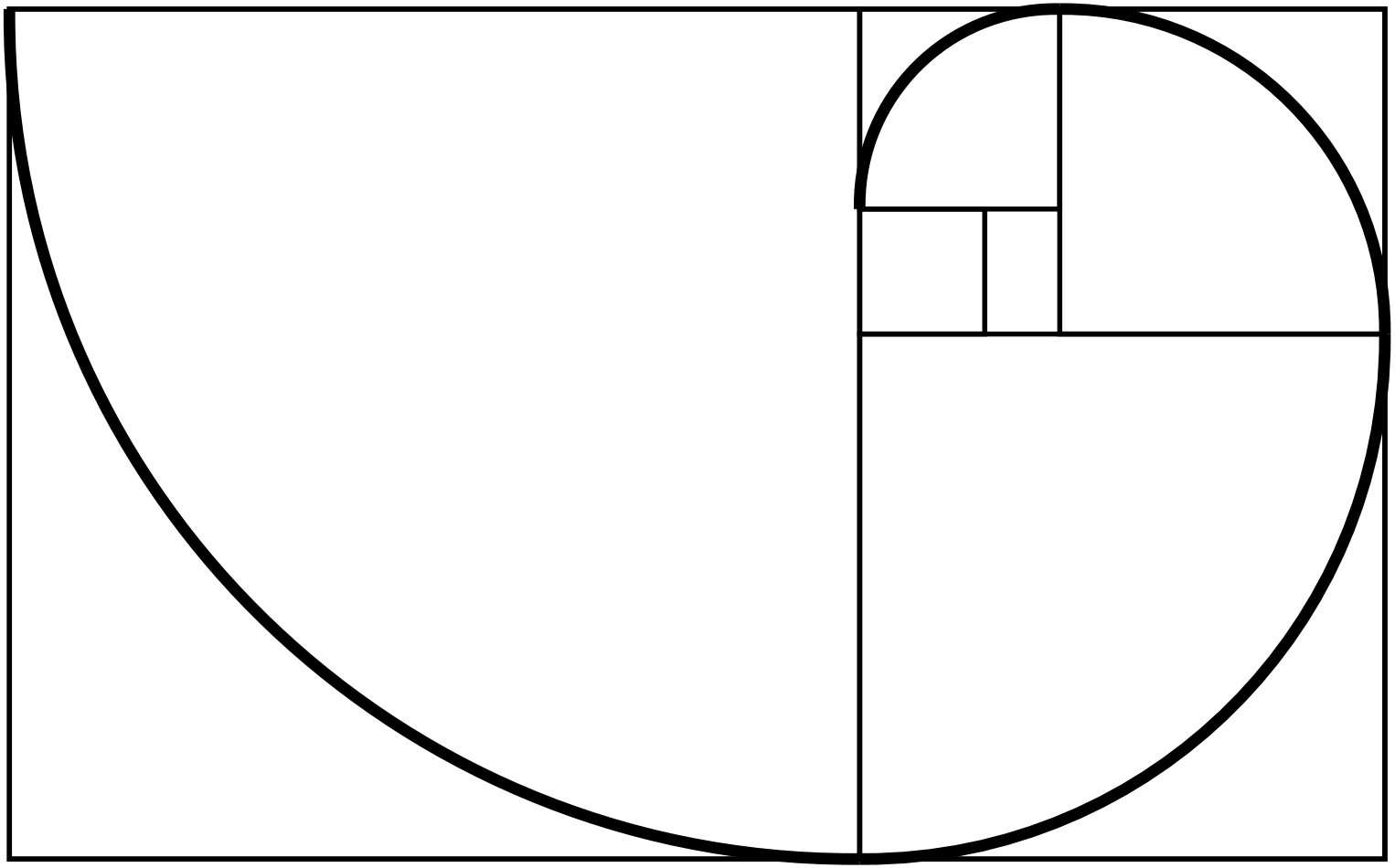
A Fibonacci-spirál



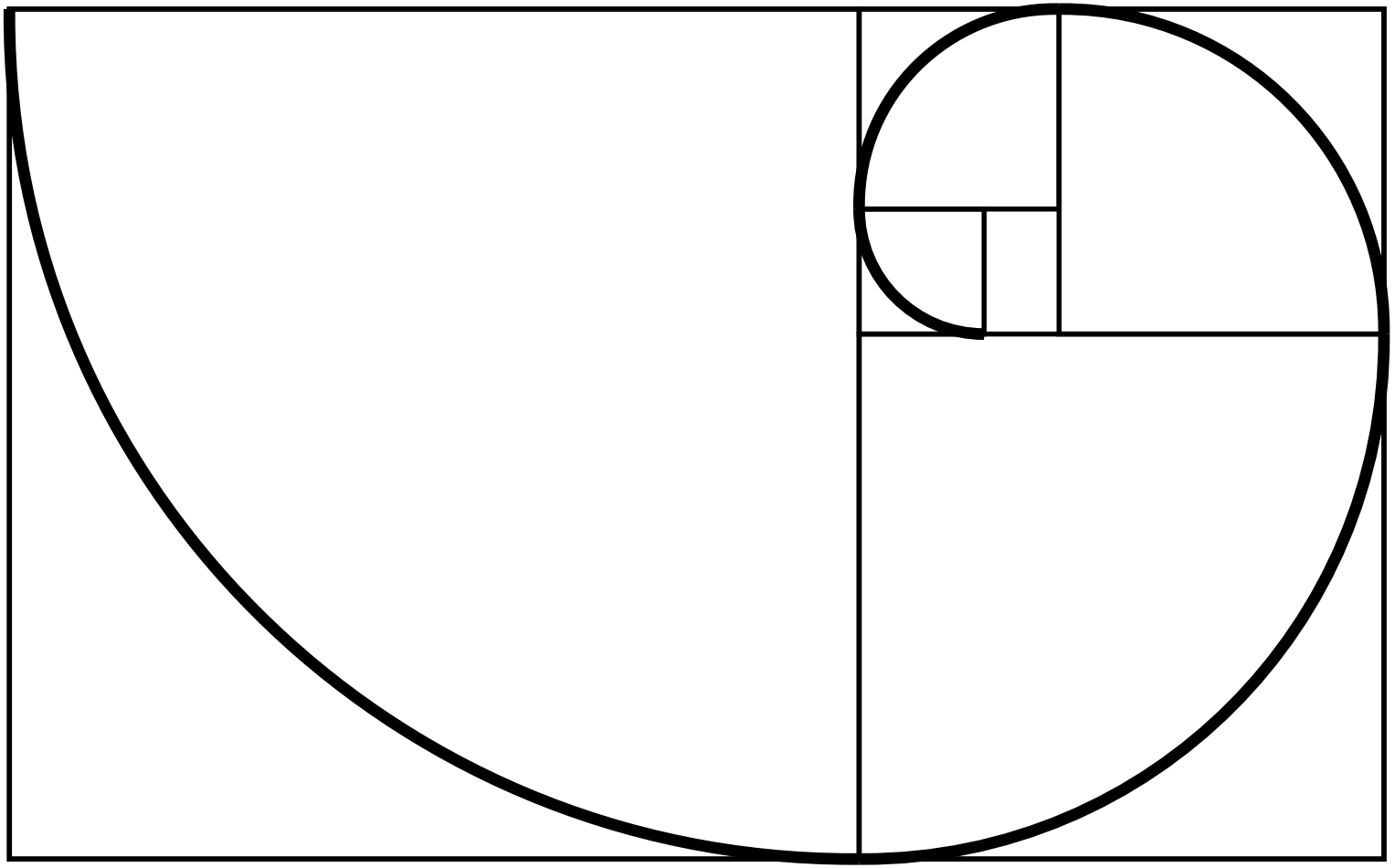
A Fibonacci-spirál



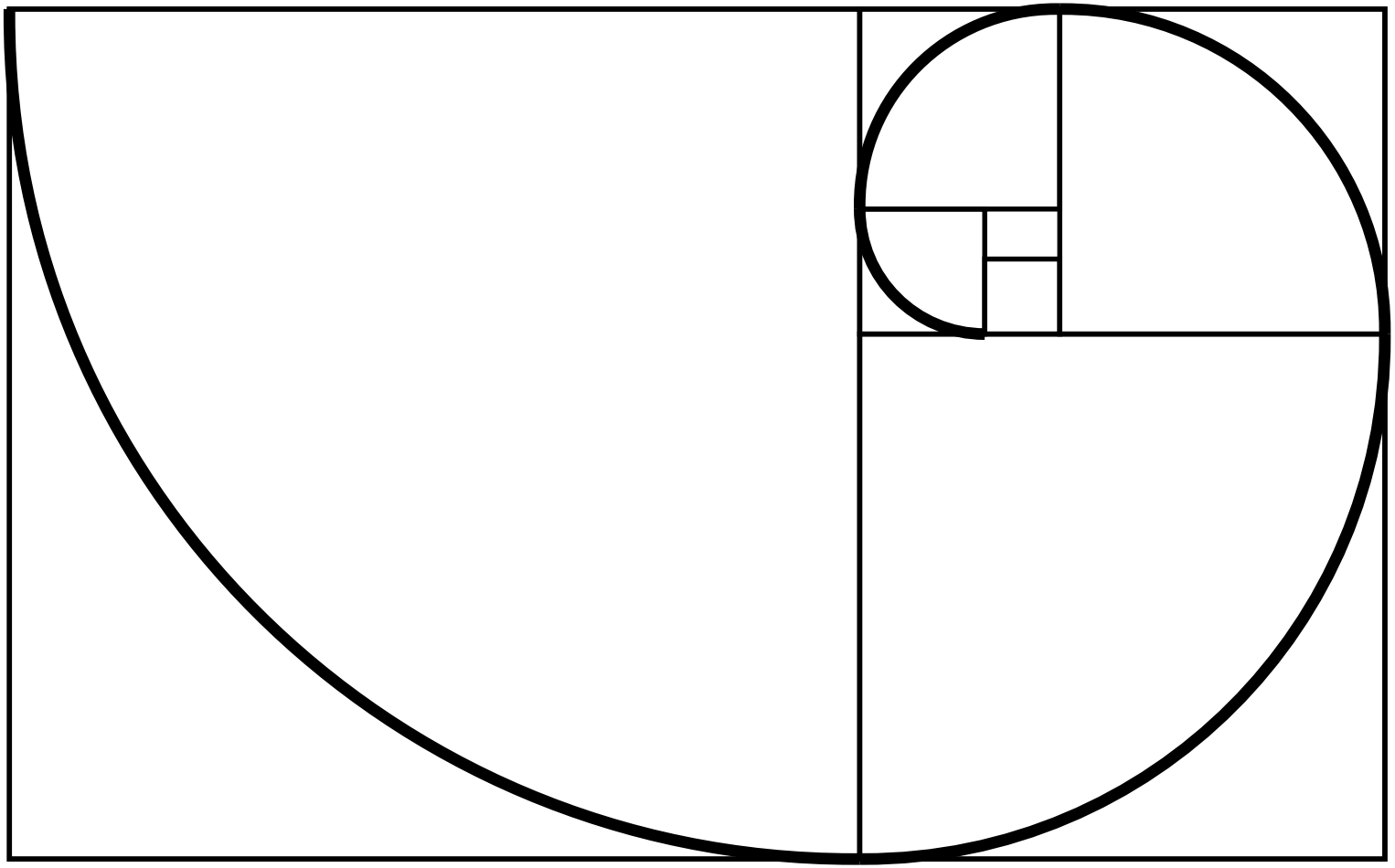
A Fibonacci-spirál



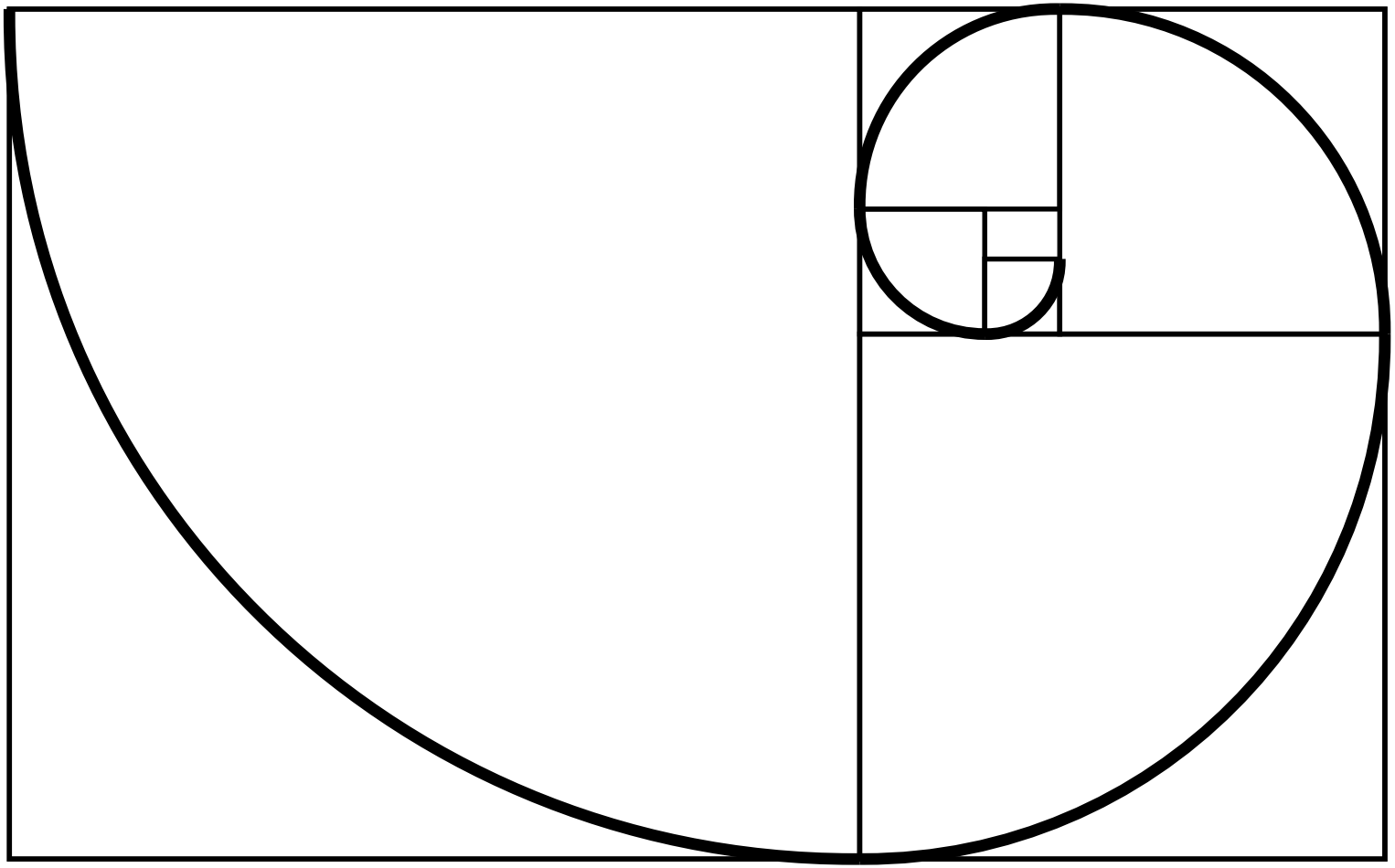
A Fibonacci-spirál



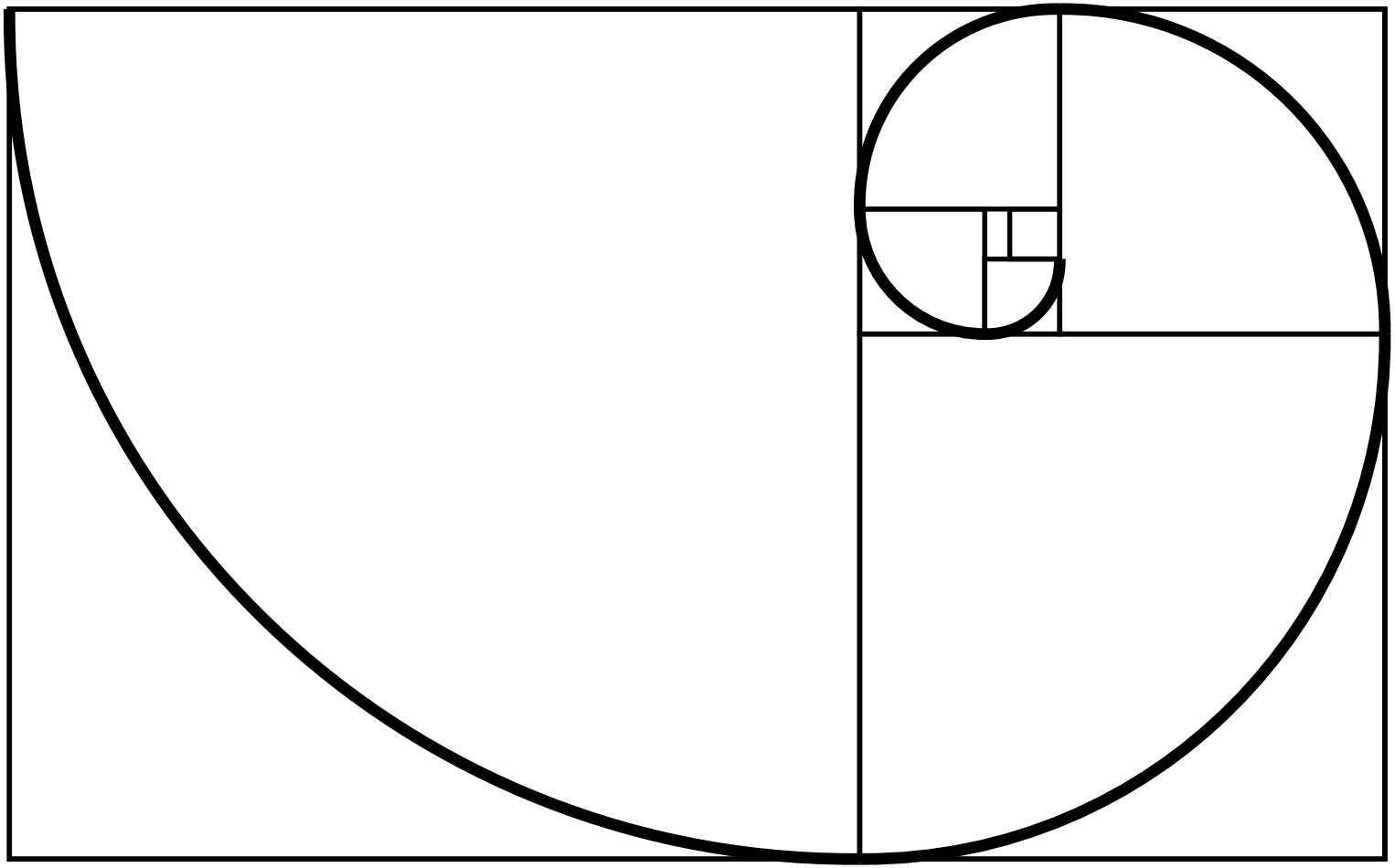
A Fibonacci-spirál



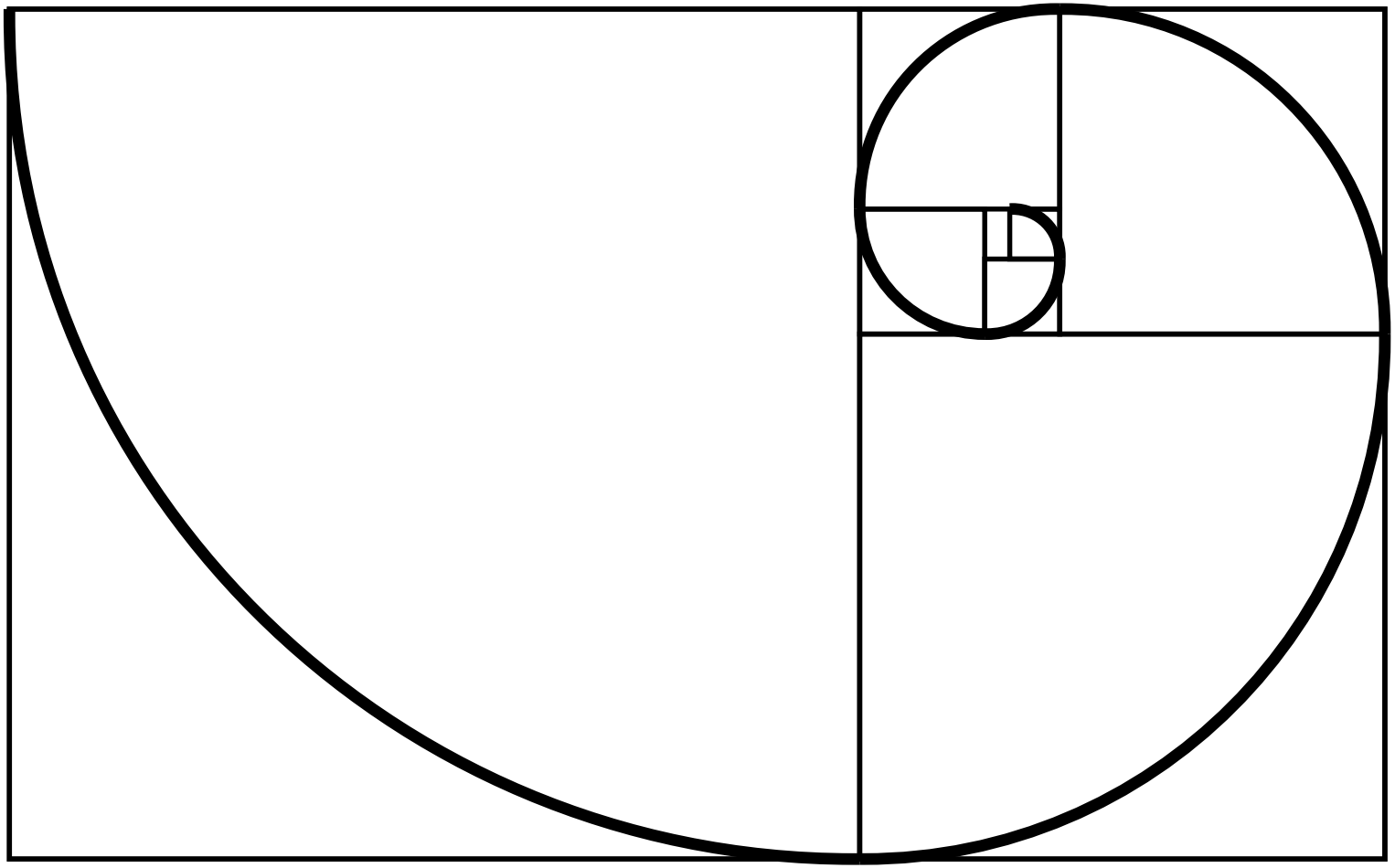
A Fibonacci-spirál



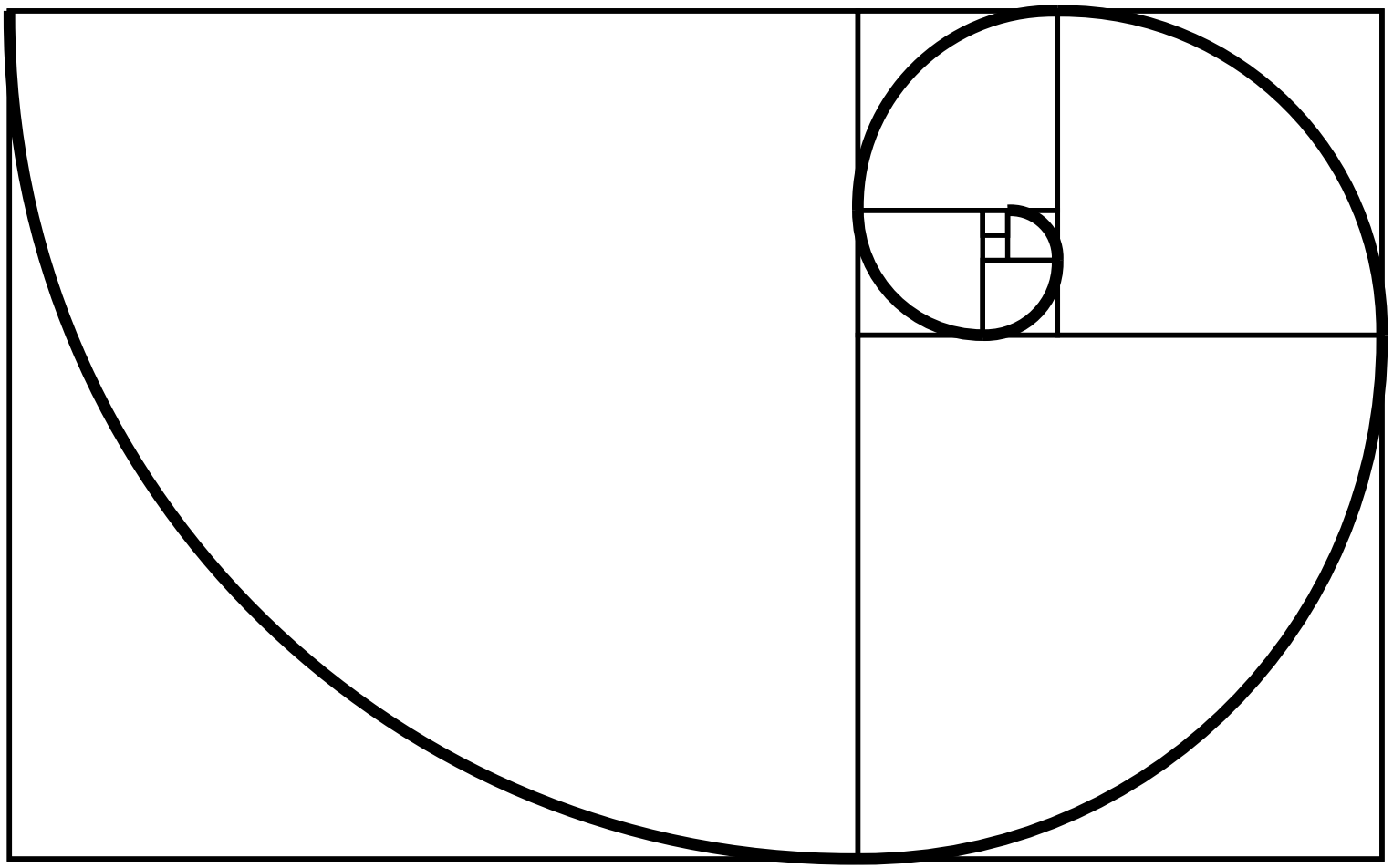
A Fibonacci-spirál



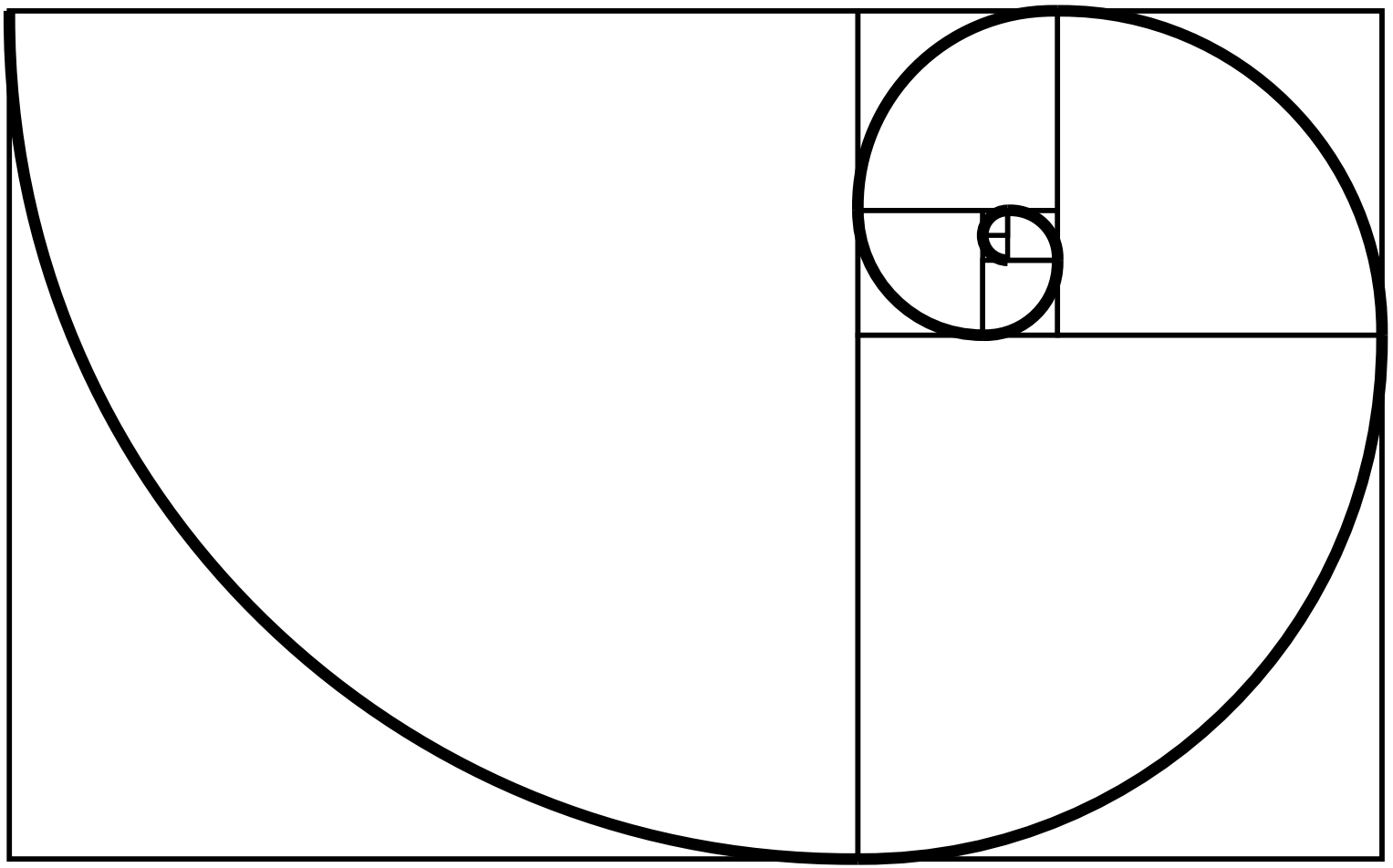
A Fibonacci-spirál



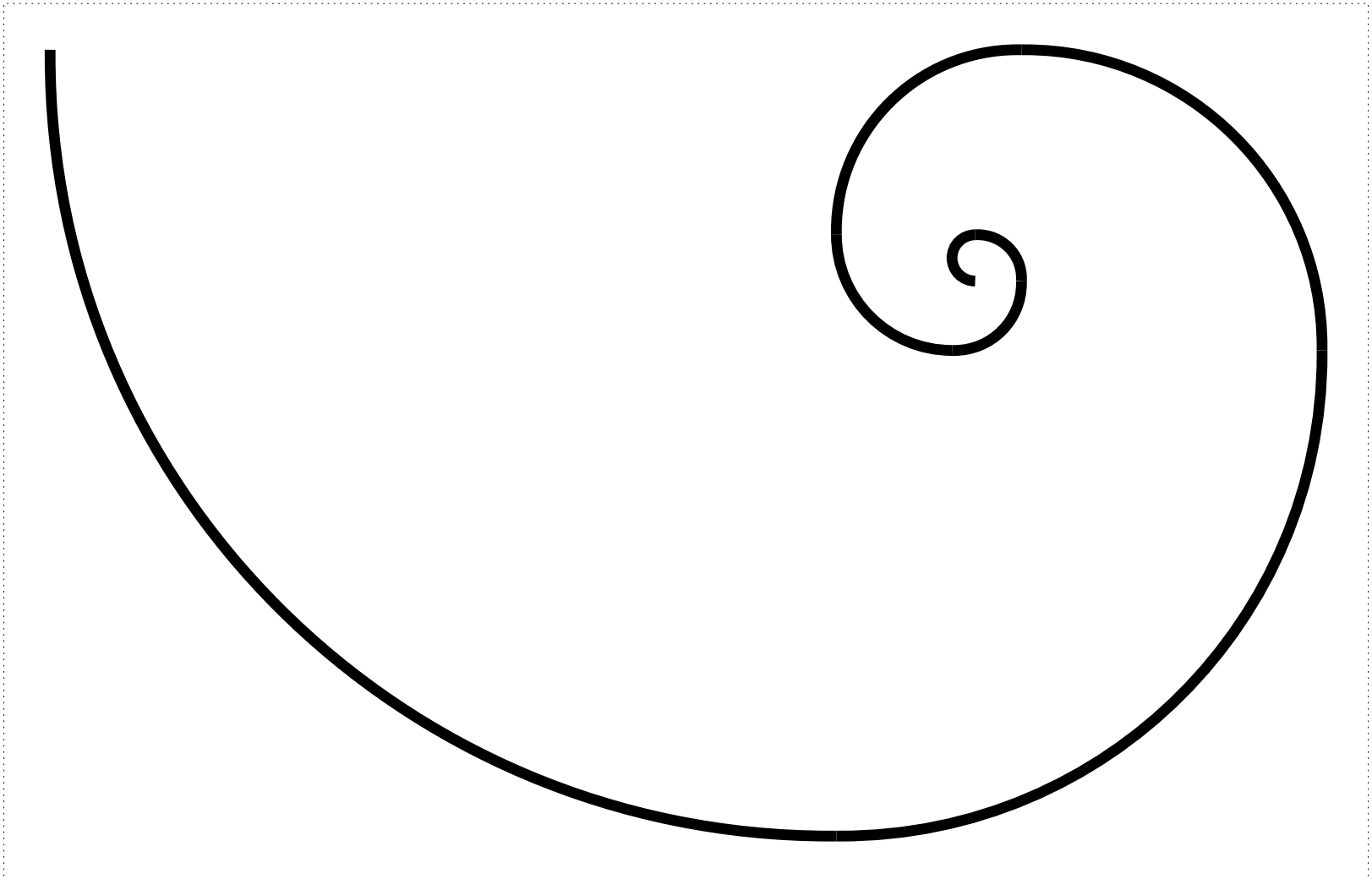
A Fibonacci-spirál



A Fibonacci-spirál



A Fibonacci-spirál



Az lnko egy fontos tulajdonsága

Tétel: Legyenek $0 < a, b$ egészek. Ekkor

$$\{ax + by \text{ alakú számok } (x, y \text{ egészek})\} = \{\text{lnko}(a, b) \text{ többszörösei}\}.$$

Az lnko egy fontos tulajdonsága

Tétel: Legyenek $0 < a, b$ egészek. Ekkor

$$\{ax + by \text{ alakú számok } (x, y \text{ egészek})\} = \{\text{lnko}(a, b) \text{ többszörösei}\}.$$

Biz.: $\subseteq$ könnyű: ha d osztója a, b-nek, akkor $ax + by$-nak is.

Az lnko egy fontos tulajdonsága

Tétel: Legyenek $0 < a, b$ egészek. Ekkor

$$\{ax + by \text{ alakú számok } (x, y \text{ egészek})\} = \{\text{lnko}(a, b) \text{ többszörösei}\}.$$

Biz.: $\subseteq$ könnyű: ha d osztója a, b-nek, akkor $ax + by$-nak is.
$\supseteq$, azaz $\text{lnko}(a, b)$ előáll $ax + by$ alakban:

Az lnko egy fontos tulajdonsága

Tétel: Legyenek $0 < a, b$ egészek. Ekkor

$$\{ax + by \text{ alakú számok } (x, y \text{ egészek})\} = \{\text{lnko}(a, b) \text{ többszörösei}\}.$$

Biz.: $\subseteq$ könnyű: ha d osztója a, b-nek, akkor $ax + by$-nak is.
$\supseteq$, azaz $\text{lnko}(a, b)$ előáll $ax + by$ alakban:
Azért, mert az euklideszi algoritmus során öröklődik, hogy a közbülső értékek (a_ℓ, b_ℓ) $ax + by$ alakúak.

Az lnko egy fontos tulajdonsága

Tétel: Legyenek $0 < a, b$ egészek. Ekkor

$$\{ax + by \text{ alakú számok } (x, y \text{ egészek})\} = \{\text{lnko}(a, b) \text{ többszörösei}\}.$$

Biz.: $\subseteq$ könnyű: ha d osztója a, b-nek, akkor $ax + by$-nak is.
$\supseteq$, azaz $\text{lnko}(a, b)$ előáll $ax + by$ alakban:
Azért, mert az euklideszi algoritmus során öröklődik, hogy a közbülső értékek (a_ℓ, b_ℓ) $ax + by$ alakúak.

Kiegészített euklideszi algoritmus: Az eukl. algoritmust kiegészítjük a közbülső számok (a_ℓ, b_ℓ) előállításával $ax + by$ alakban.

Példa: $a = 8, b = 13$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \qquad 8x + 13 \cdot 0$$

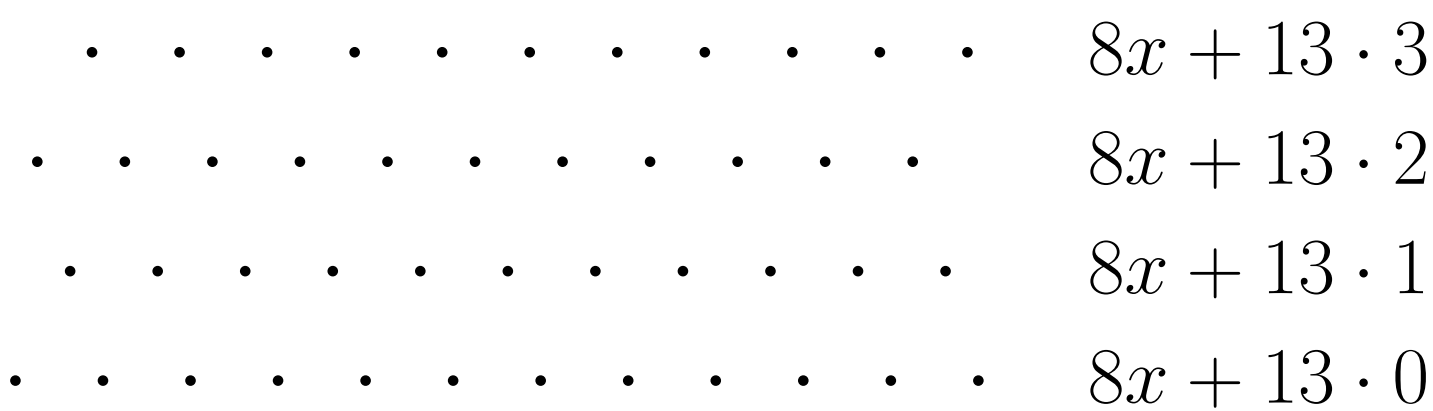
Példa: $a = 8, b = 13$

$$\cdots \quad 8x + 13 \cdot 1$$
$$\cdots \quad 8x + 13 \cdot 0$$

Példa: $a = 8, b = 13$

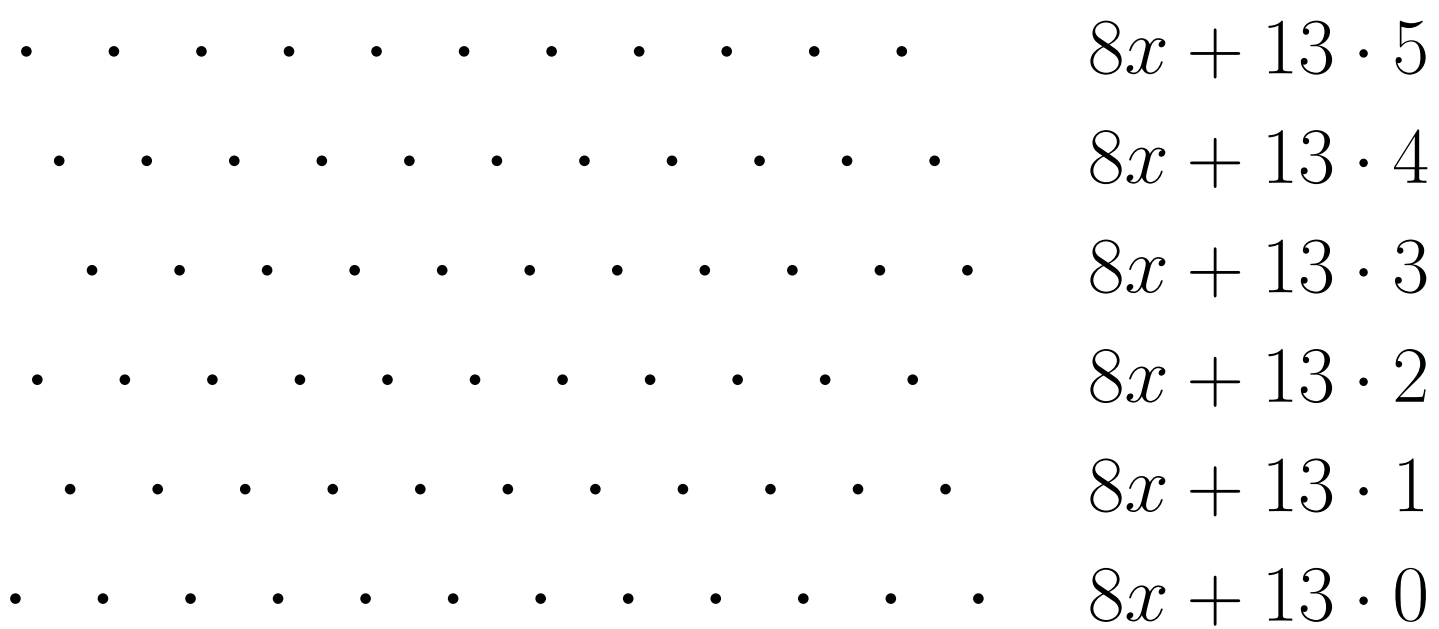
$$\begin{array}{ll} \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & 8x + 13 \cdot 2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & 8x + 13 \cdot 1 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & 8x + 13 \cdot 0 \end{array}$$

Példa: $a = 8, b = 13$



Példa: $a = 8, b = 13$

Példa: $a = 8, b = 13$



$8x + 13 \cdot 5$

$8x + 13 \cdot 4$

$8x + 13 \cdot 3$

$8x + 13 \cdot 2$

$8x + 13 \cdot 1$

$8x + 13 \cdot 0$

Példa: $a = 8, b = 13$

$8x + 13 \cdot 6$

$8x + 13 \cdot 5$

$8x + 13 \cdot 4$

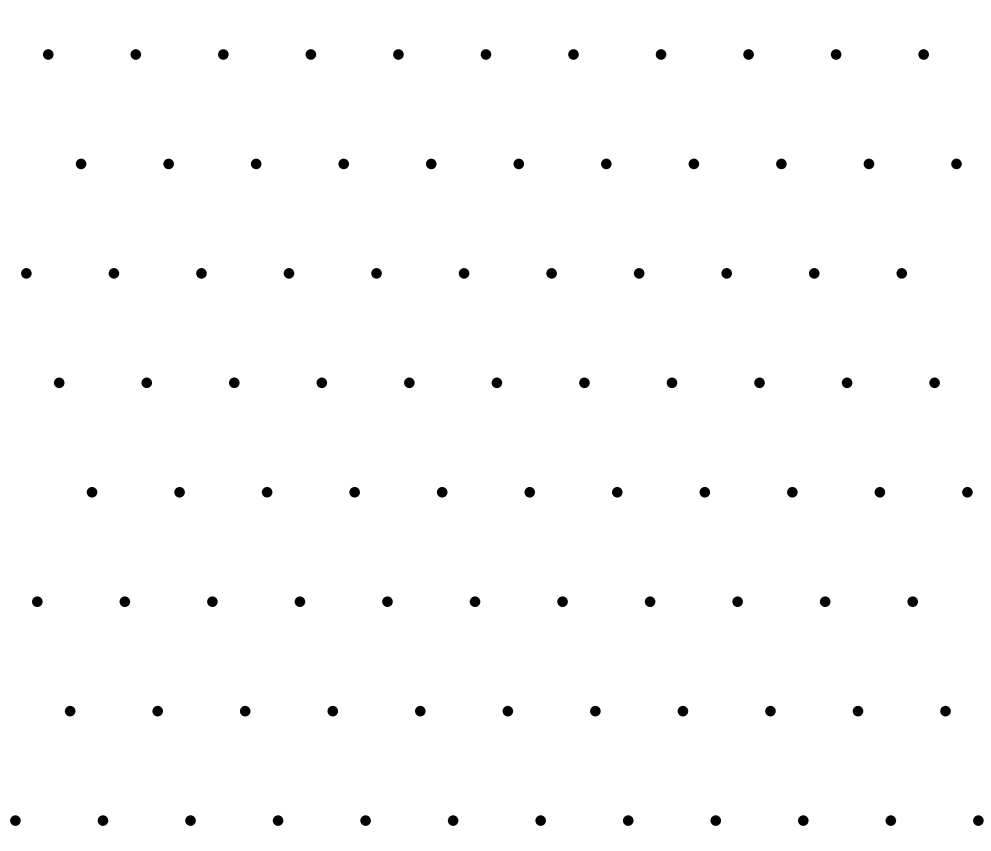
$8x + 13 \cdot 3$

$8x + 13 \cdot 2$

$8x + 13 \cdot 1$

$8x + 13 \cdot 0$

Példa: $a = 8, b = 13$



$8x + 13 \cdot 7$

$8x + 13 \cdot 6$

$8x + 13 \cdot 5$

$8x + 13 \cdot 4$

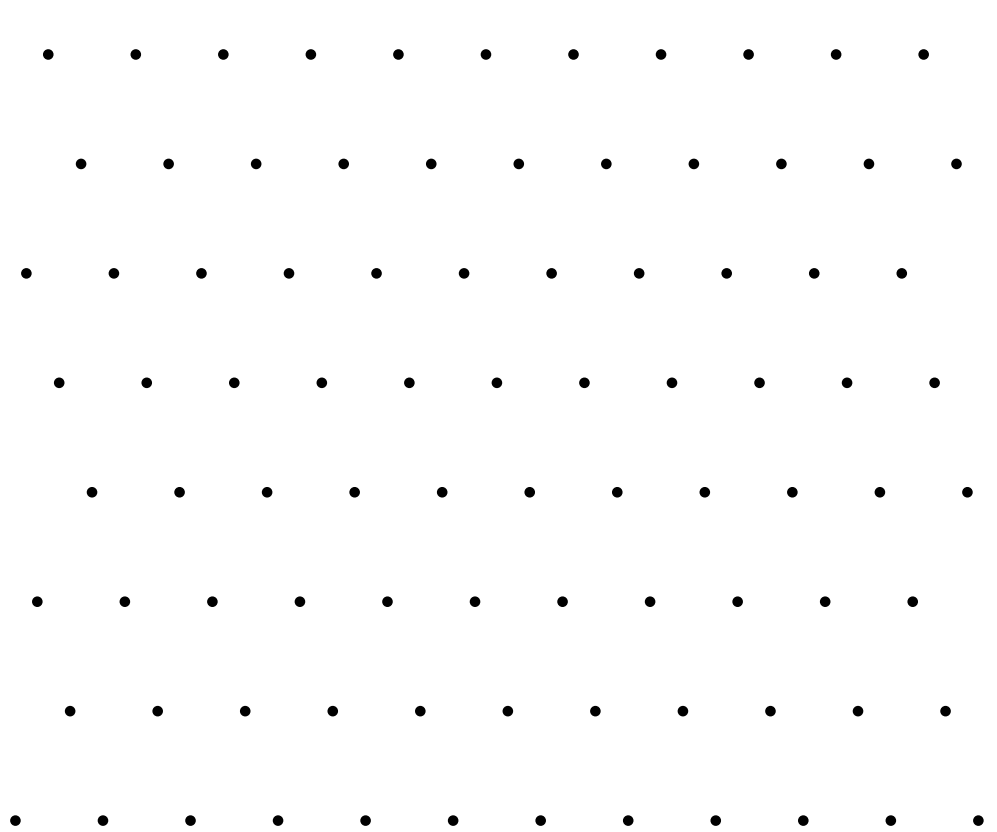
$8x + 13 \cdot 3$

$8x + 13 \cdot 2$

$8x + 13 \cdot 1$

$8x + 13 \cdot 0$

Példa: $a = 8, b = 13$



$8x + 13 \cdot 7$

$8x + 13 \cdot 6$

$8x + 13 \cdot 5$

$8x + 13 \cdot 4$

$8x + 13 \cdot 3$

$8x + 13 \cdot 2$

$8x + 13 \cdot 1$

Példa: $a = 8, b = 13$

$$8x + 13 \cdot 7$$
$$8x + 13 \cdot 6$$
$$8x + 13 \cdot 5$$
$$8x + 13 \cdot 4$$
$$8x + 13 \cdot 3$$
$$8x + 13 \cdot 2$$

Példa: $a = 8, b = 13$

$8x + 13 \cdot 7$

$8x + 13 \cdot 6$

$8x + 13 \cdot 5$

$8x + 13 \cdot 4$

$8x + 13 \cdot 3$

Példa: $a = 8, b = 13$

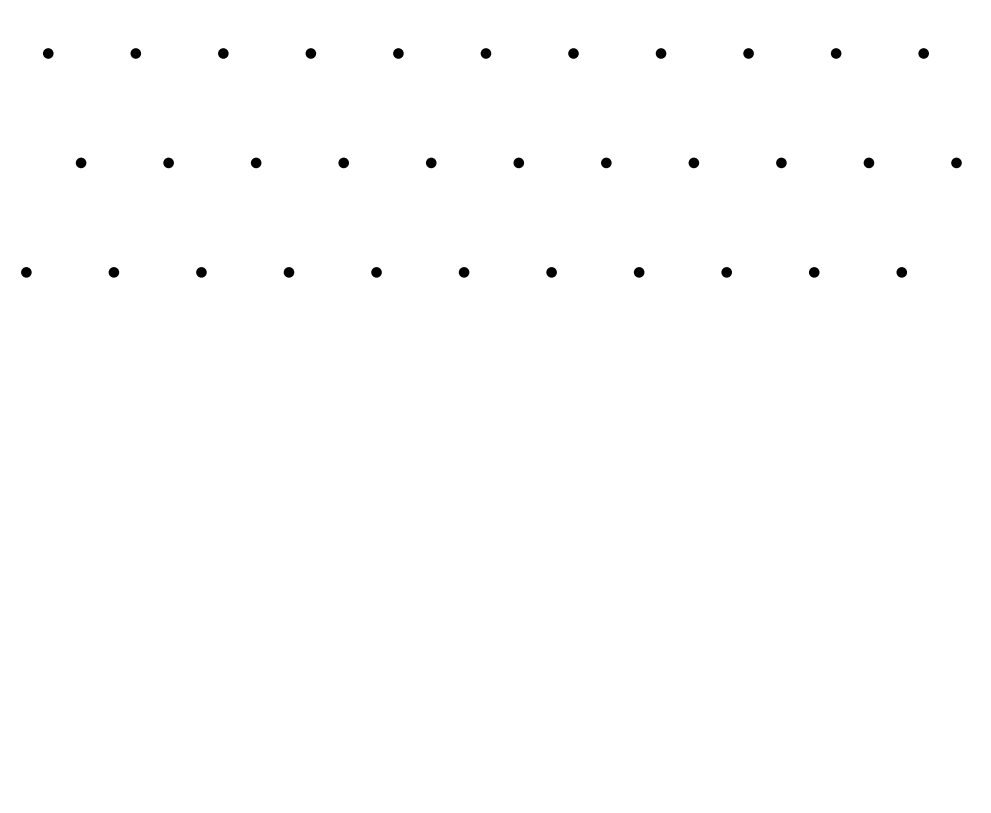
$8x + 13 \cdot 7$

$8x + 13 \cdot 6$

$8x + 13 \cdot 5$

$8x + 13 \cdot 4$

Példa: $a = 8, b = 13$

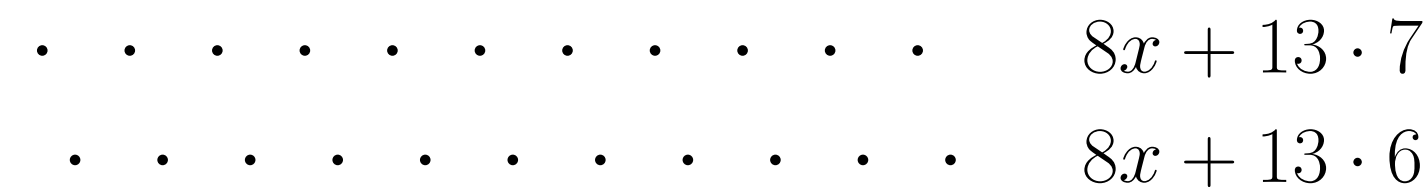


$8x + 13 \cdot 7$

$8x + 13 \cdot 6$

$8x + 13 \cdot 5$

Példa: $a = 8, b = 13$



Példa: $a = 8, b = 13$

$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$ $\qquad 8x + 13 \cdot 7$

$\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot\cdot\cdot \quad \cdot\cdot\cdot\cdot\cdot$

Példa: $a = 8, b = 13$

Az euklideszi játék (Cole–Davie 1969)

Adott két egész hosszúságú madzag és 2 játékos, akik felváltva lépnek.

Az euklideszi játék (Cole–Davie 1969)

Adott két egész hosszúságú madzag és 2 játékos, akik felváltva lépnek.

Egy lépés:

- a hosszabbik madzagból levágjuk a rövidebb egy többszörösét
- legalább 1-szeresét
- azért még maradjon valamennyi

Az euklideszi játék (Cole–Davie 1969)

Adott két egész hosszúságú madzag és 2 játékos, akik felváltva lépnek.

Egy lépés:

- a hosszabbik madzagból levágjuk a rövidebb egy többszörösét
- legalább 1-szeresét
- azért még maradjon valamennyi

Vesztes: aki nem tud lépni (azaz aki két egyforma madzagot kap).

Az euklideszi játék (Cole–Davie 1969)

Adott két egész hosszúságú madzag és 2 játékos, akik felváltva lépnek.

Egy lépés:

- a hosszabbik madzagból levágjuk a rövidebb egy többszörösét
- legalább 1-szeresét
- azért még maradjon valamennyi

Vesztes: aki nem tud lépni (azaz aki két egyforma madzagot kap).

Kérdés: a kezdeti hosszúságoktól függően a kezdőnek mikor van nyerő stratégiája?