העולם העתיק והקלאסי

לפה"ס ועד המאה ה-5

מספרים – 2

נאסף ונערך בעברית ע"י פרופ' צבי קם

אלגוריתמים

אלגוריתמים

כתוב מירשם (אלגוריתמים) לשימוש בחשבוניה לחיבור ולחיסור
רשום אלגוריתם לחיבור, לחיסור, לכפל ולחילוק שני מספרים

אלגוריתם הכפלה: פיבונצי, (מכונות הכפלה - בהמשך)

דוגמא **לאלגוריתם איטרטיבי** לחישוב שרש ריבועי בכל דיוק רצוי:

$$x^{1/2} = 1 + \frac{x-1}{1+x^{1/2}}$$

ולכן

$$x^{1/2} = 1 + \cfrac{x-1}{2 + \cfrac{x-1}{2 + \cfrac{x-1}{2 + \cfrac{x-1}{\cdots}}}}$$

למשל: $\sqrt{2} \sim 1.5$ קירוב א: $1+1/2.5=1.4$ קירוב ב: $1+1/2.4=1.4167$ קירוב ג: $1+1/2.4167=1.4138$
כאשר: $\sqrt{2} = 1.41421356$

אלגוריתם בבלי לקירוב שרש ריבועי:

אם A הוא קירוב ל- $\sqrt{Q}$ כי אז $B=(A+Q/A)/2$ הוא קירוב טוב יותר
האם תוכלו להוכיח?

נניח כי A קטן מ- $\sqrt{Q}$
$\sqrt{Q}-B=\sqrt{Q}-(A+Q/A)/2 < \sqrt{Q}-A$
$-Q/A/2 < -A/2$
$Q < A^2$

נניח כי A גדול מ- $\sqrt{Q}$
$B-\sqrt{Q}=(A+Q/A)/2-\sqrt{Q} < A-\sqrt{Q}$
$Q/A/2 < A/2$
$Q < A^2$

למשל: $\sqrt{2} \sim 1.5$ קירוב א: $(1.5+2/1.5)/2=1.41667$ קירוב ב: $(1.4166+2/1.4166)/2=1.4142156$

אלגוריטם להוצאת שרש מסדר שני ושלישי

בכל שלב התוצאה מדוייקת עד לספרה שחושבה

חלוקה לזוגות (שלישיות) , שרש של הקבוצה השמאלית

ואח"כ תוצאה כפול20 או 30 (+ x כפול x עבור x הכי גדול, וחוזר חלילה)

http://www.mathpath.org/Algor/squareroot/algor.square.root.htm

שרש ריבועי

```
7. 3  3  4  8

  \/53.80 00 00 00
 7   49
 -   __
      4 80
 143  4 29
 -    _____
        51 00
1463       43 89

 -          ______
             7 11 00
14664         5 86 56
 -           ________
             1 24 44 00
```

שרש שלישי

```
5.  1   3   9   9

\3/135.790 000 000 000
5   125
      ____
                10 790
       7500
       (151)
 -
151
          -----
7651    7  651
       _______
          3  139 000
780300
 (1533)
          -
        4599
        -------
       784899     2 354 697
                  __________
                   784 303 000
     78950700
      (15399)
          -
      138591
      ---------
     79089291           711 803 619
                        ____________
                         72 499 381 000
```

מספרים ראשוניים

מספרים ראשוניים

מספרים שלמים המתחלקים רק ב-1 ובעצמם
התיאורמה הבסיסית של האריטמטיקה - כל מספר ניתן לבטא כמכפילת אחד או יותר מספרים ראשוניים באופן אחד בלבד (עד כדי סדר הכופלים)

אוקלידס 325-265 לפה"ס **Euclid**
הוכיח שיש אין-סוף מספרים ראשוניים

נניח ש-p_m הוא המספר הראשוני הגדול ביותר (את הקטנים ממנו נסמן p_1,p_2,p_3 ...)
המספר $P=1+p_1*p_2*p_3*....*p_m$ הוא או ראשוני, או מתחלק במספר ראשוני-q
אם P ראשוני הוא גדול מכל הראשוניים שלנו ולכן מצאנו ראשוני נוסף
אם הוא אינו ראשוני הוא מתחלק ב-q שאינו יכול להיות אחד מהמספרים הראשוניים שלנו:
הפרש בין שני מספרים המתחלקים ב- q גם הוא מתחלק ב- q
אבל ההפרש הוא $1= p_1*p_2*p_3*....*p_m - P$ ואינו יכול להתחלק ב-q שאינו 1
ולכן q הוא מספר ראשוני נוסף וכך נמשיך עד אינסוף

איך נמצא אם מספר n הוא ראשוני:
נבדוק אם הוא מתחלק בכל המספרים הקטנים ממנו
2. נבדוק אם הוא מתחלק בכל המספרים עד שרש- n (למה?)
3. נייצר את טבלת הראשוניים עד שרש- n
תרגיל פשוט: בצע את הסריקה בטבלא עד 120

אלגוריתם הסריקה (ניפוי) של ארטוסטנס 276-194 BC (Sieve of Eratosthenes)

אלגוריתם למציאת כל הראשוניים עד למספר כלשהו

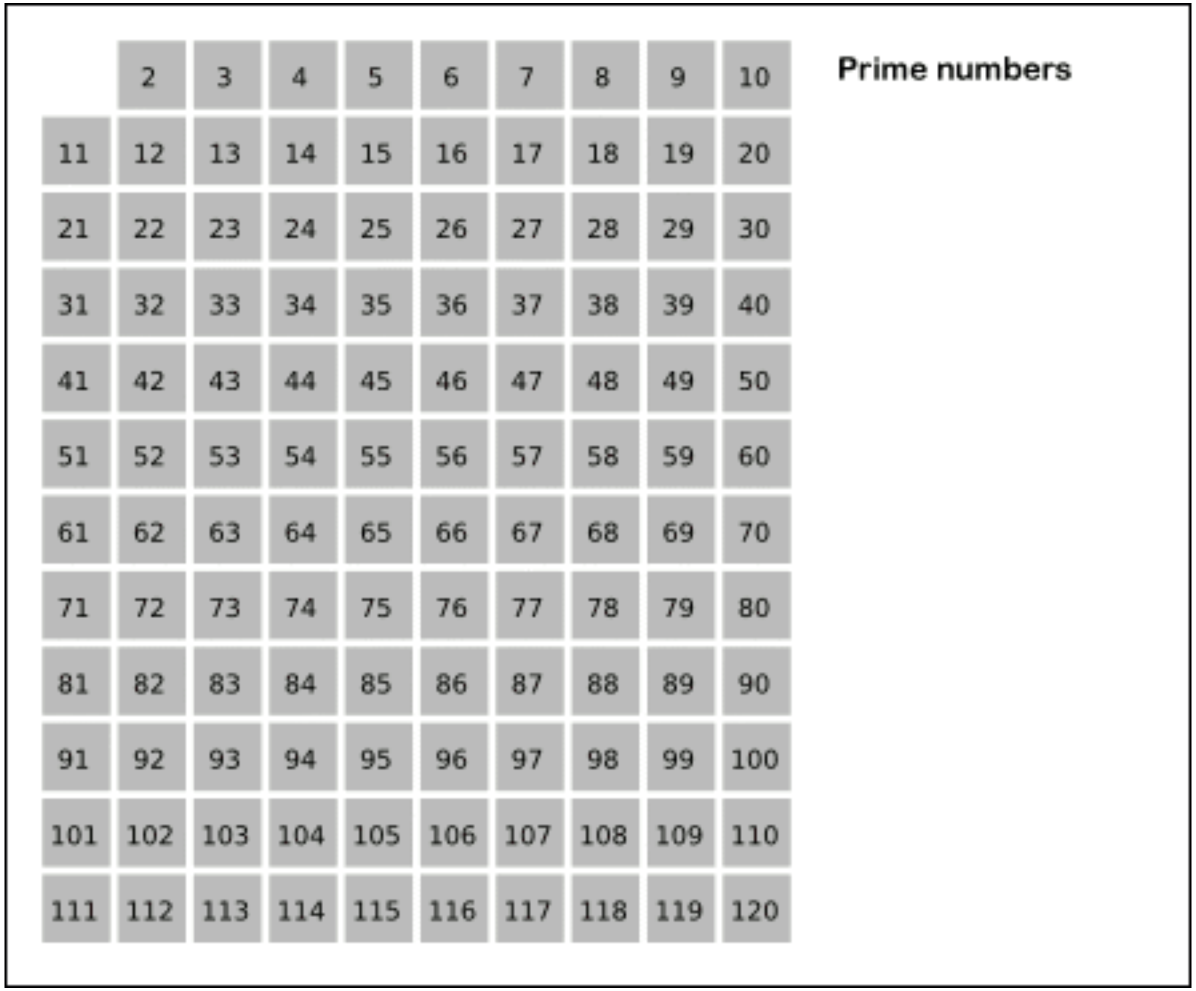
רשום כל המספרים 2 ... N

איתחול- ראשוני מספר 1= p

לולאה על p – סמן כפולות p ברשימה (3p, 5p, 7p...) אולי בחלקם כבר סומנו

מצא את המספר הראשון הגדול מ-p^2 שלא סומן – זה הראשוני הבא בלולאה

הפסק אם אין מספר שלא סומן

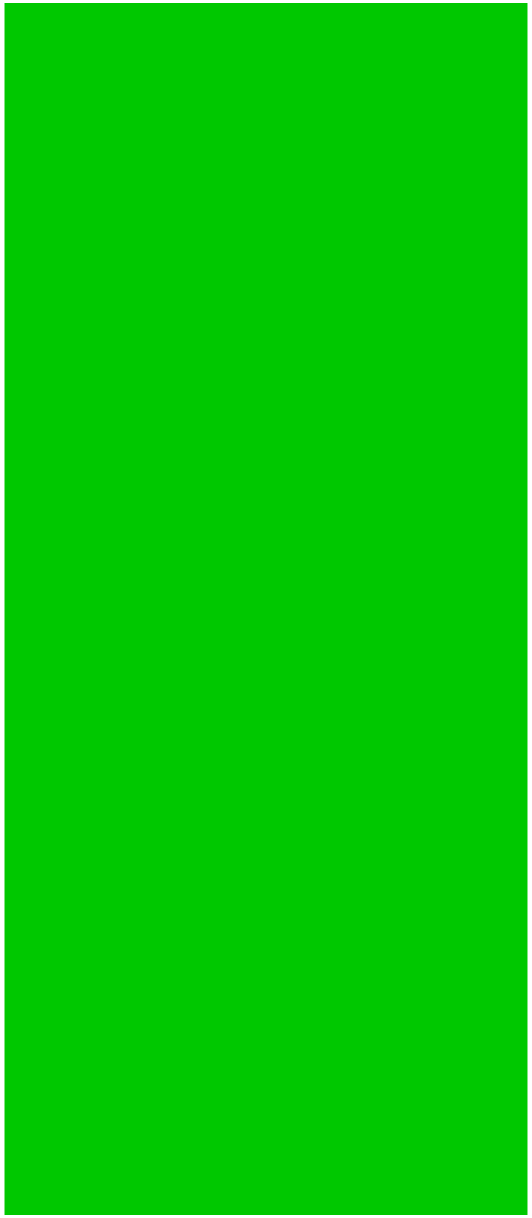


חישוב הגורם המשותף הגדול ביותר GCD לשני מספרים -

שיטה ישירה: נמצא את כל הגורמים לשני המספרים ונשווה את הרשימה.

יותר טוב: נמצא את כל הגורמים מ-1 עד למספר הקטן בין השניים.

עוד יותר טוב: נמצא את הגורמים הראשוניים עד לשרש המספר הקטן.



שיטה חכמה במיוחד: האלגוריטם של אוקלידס

אם A>B אז GCD(A,B)=GCD(A-B,B)

A=G*X B=H*X => (A-B)=(G-H)*X

אם היה Y>X המקיים (A-B)=M*Y B=N*Y

אזי בניגוד להנחתנו A=(M+N)*Y

<u>למשל 1989 ו-7</u>

GCD(1989,867)=GCD(1989-867,867)=

=GCD(1122,867)=GCD(1122-867,867)=

=GCD(255,867)=GCD(255,867-255)=

=GCD(255,612)=GCD(255,612-255)=

=GCD(255,357)=GCD(255,102)=

=GCD(255-102,102)=GCD(153,102)=

=GCD(153-102,102)=GCD(51,102)=

=GCD(51,102-51)=GCD(51,51)=51

ואכן: 51X17=867 51X39=1989

<u>באופן ציורי לדוגמא</u>- 1071 ו-462: מציירים 1071 462 (ירוק).

בתוכו נכנסים שני ריבועים 462x462 (צהוב)

נשאר 462x147 שלתוכו נכנסים שלושה ריבועים 147x147 (כחול)

נשאר 21x147 שלתוכו נכנסים שבע ריבועים 21x21 (אדום)

21 הוא הגורם המשותף הגדול ביותר של 1071 ו-462

שימושים למספרים ראשוניים:

למרות שתורת המספרים נחשבה עד לזמן האחרון כמתמטיקה טהורה, עידן המחשבים יצר לה שני שימושים חשובים ביותר:

1. שיטות ליצירת מספרים פסיבדו-אקראיים – ז"א סידרה סופית ארוכה ומחזורית של מספרים אקרעיים התלויה באיתחול "הגרעין" seed שלה

דוגמא עבור מספרים אקרעיים של 15 ביטים:

random() in range [0 ... 65535] = 256*256-1 (15 bits)

ע"י הנוסחא הרקורסיבית: (כאשר סימן האחוזים % אומר השארית מהחלוקה ב-65536)

iseed=(iseed*5761+999)%65536

כאשר 5761 הוא מספר ראשוני גדול

מנרמלים אם רוצים שיהיה בתחום [0 , 1] random=(float)(iseed)/65536.0

```
a=(float)(random()%987654)/987654.0;
```

בדיוק גבוה יותר:

random() in range [0 ... 2147483647] = 256*256*256*128-1 (31 bits)

iseed=(iseed*16807)%2147483647

תרגיל: בדוק את הפילוג של התוצאות – האם הוא אחיד? האם שווה לכל "גרעין" התחלה?

2. קריפטוגרפיה – דוגמא:
שיטת ההצפנה RSA, (עדי שמיר רונלד ריבסט ולאונרד אדלמן)

גם באלגוריטם חסכוני לא ניתן למצוא בזמן סביר אם מספר גדול הוא ראשוני או לא
על זה מבוססת שיטת RSA לקריפטוגרפיה – שימוש למפתח דיגיטאלי לבנק או לטלויזיה לווינית

http://he.wikipedia.org/wiki/
פרוטוקול דיפי הלמן – המצאת המפתח הציבורי
http://he.wikipedia.org/wiki/RSA
ריבסט, שמיר ואדלמן

אם נשלח מכפילה של שני מספרים ראשוניים מאד גדולים – איש לא יוכל בזמן סביר לפרק אותה

אניגמה – מכונת הקידוד של הגרמנים במלחמת העולם השניה, שפוענך ע"י הבריטים, מבוסס על תרגום כל אות לאות אחרת – מאחר וכבר בימי הבינים אל_קינדי הראה שטקסט מספיק ארוך אפשר לפענח לפי תדירות השימוש של אותיות בשפה, לאניגמה נבנה מנגנון מכאני שמשנה אחרי כל אות את התרגום.

הצפנת ריבסט, שמיר ואדלמן http://he.wikipedia.org/wiki/RSA

בגרסת RSA הבסיסית, תחילה להכנה:

1. בוחרים שני מספרים ראשוניים גדולים p ו– q
2. מחשבים =pq
3. מחשבים $\phi=(p-1)(q-1)$.
4. בוחרים את המפתח הפומבי: e שלם וזר ל– ϕ המקיים $\phi>e>1$
   זר: משמעותו שאין ל– e ו– ϕ מחלק משותף, או $GCD(e,\phi)=1$ שמבטיח התמרה חד ערכית
   להקלת הפיענוח e צריך להיות מספר קטן
5. מחשבים את המפתח הפרטי: $d.e= 1 \mod(\phi)$ וניתן להשמיד את p,q

א׳ משדר לב׳ את מפתחות ההצפנה e,n ושומר בסוד את d
ב׳ משדר ל–א׳ את $c=m^e \mod(n)$ המקודד את – m
א׳ מפענחת את המסר ע״י $m=c^d \mod(n)$

דוגמה במספרים "קטנים":

נניח שא' בוחר $q=8059$, $p=5581$, $n=5581.8059=4497727$, $\phi=(5580\ 8058)=7493940$
ובוחר $e=257$ המקיים $gcd(7493940,257)=1$
ו– $d=291593$ המקיים $(291593\cdot 257)=1 \mod (7493940)$
א׳ שולח לב׳ $n=4497727$ ו– $e=257$ ושומר בסוד $d=291593$
ב׳ רוצה לשלוח לא׳ $m=123456$ המקודד ל– $c=123456^{257} \mod(44977279) = 10526715$
א׳ משחזר את m בעזרת d,n :

$$m=c^d \mod(n)=10526715^{291593} \mod 44977279=123456$$

בווריאציות על שיטה זו משיגים יעילות גדולה יותר במהירות החישובים של מספרים גדולים

במשלוח מסרים דיגיטאליים ייתכנו טעויות הנובעות מרעשים בקוי התמסורת ו/או הפחתת הסיגנאל לאורך הקוים.

תיקון טעויות במשלוח מסרים: מבוסס על משלוח של סכומים sums

למשל: בנוסף ל-64 ביטים נשלחים עוד 16 ביטים לזוגיות שורות ועמודים –

כמה טעויות מכסימום נוכל לתקן?

```
1 0 1 1 0 1 0 0   0
1 1 0 1 0 0 1 1   1
1 0 1 1 0 1 0 1   1
1 0 0 0 0 1 0 0   0
1 1 0 1 0 0 1 0   0
1 0 1 1 0 1 1 0   1
0 1 1 1 0 1 1 1   0
1 1 1 1 1 1 1 1   0

1 0 1 1 1 0 1 0   .
```

נסו 2, 3, 4 טעויות!

```
1 0 1 1 0 1 0 0   0
1 1 0 1 0 0 1 1   1
1 0 1 1 0 1 0 1   1
1 0 0 0 1 1 0 0   0
1 1 0 1 0 0 1 0   0
1 0 1 1 0 1 1 0   1
0 1 1 1 0 1 1 1   0
1 1 1 1 1 1 1 1   0

1 0 1 1 1 0 1 0   .
```

למשל זה לא ניתן לתקן

```
1 0 1 1 0 1 0 0   0
1 1 0 1 0 0 1 1   1
1 0 1 1 0 1 0 1   1
1 0 0 0 1 0 0 0   0
1 1 0 1 1 1 1 0   0
1 0 1 1 0 1 1 0   1
0 1 1 1 0 1 1 1   0
1 1 1 1 1 1 1 1   0

1 0 1 1 1 0 1 0   .
```

מספרים מעניינים, לפי סדרת הטלויזיה של ה–BBC

שרש 2

מספרים אירציונאליים מענינים

$\sqrt{2}$

היונים אהבו גיאומטריה וסימטריה, וגילו שארכים בצורות גיאומטריות "יפות" אינם מבוטאים ע"י מספרים "פשוטים" (כמו מספרים שלמים או יחסים ביניהם=מספרים רציונאליים). האלכסון של ריבוע הוא דוגמא. הם מצאו קירובים הולכים ומשתפרים למספרים לא רציונאליים.

אם נביט במשוואה $m^2 = 2n^2$ ובטבלת הריבועים השלמים נראה שיש זוגות ריבועים ההולכים ומתקרבים לשויון הנ"ל ולכן m/n מהוים קירובים משתפרים לשרש 2

$2^2 \cdot 2 + 1 = 3^2$	3	2
$2 \cdot 5^2 + 1 = 7^2$	7	5
$2 \cdot 12^2 + 1 = 17^2$	17	12
$2 \cdot 29^2 + 1 = 41^2$	41	29
$2 \cdot 70^2 + 1 = 99^2$	99	70

$3 + 2 = 5$ $7 + 5 = 12$ המספרים בטור הימני סכום שני המספרים בשורה מעל

$2 + 5 = 7$ $5 + 12 = 17$ המספרים בטור השמאלי סכום המספר מימינו ושמעליו

הוכחה: אם $m^2 = 1+2n^2$ אז גם $(m+2n)^2 \overset{?}{=} 1+2(n+m)^2$

$$m^2+4nm+4n^2 \overset{?}{=} 1+2n^2+4nm+2m^2$$

$$2n^2 = 1+m^2$$

וזה נכון, ומוכיח שלמספר לא רציונאלי אפשר להתקרב למרחק קטן ככל הרצוי

המושג של סידרה מתכנסת (ראה בהמשך "הפרדוקס של זינו") הוא הבסיס לאינפי.

נוכיח ששרש של 2 אינו רציונאלי על דרך השלילה (פיתגורס והיפרכוס)

אם ניתן לבטא כשבר $a/b = \mathrm{sqrt}(2)$

נצמצם את השבר עד שלפחות אחד מהמונה או המכנה יהיו איזוגיים

נזכור שריבוע כל מספר זוגי גם הוא זוגי ולהפך כי אם ריבוע הוא איזוגי אין לו גורם 2

$a^2/b^2=2$

ולכן $a^2=2*b^2$ זוגי

ולכן גם a זוגי

מכאן $b^2=a^2/2$

ולכן b^2 זוגי b

אך זה בניגוד להנחתנו.

חתף זהב

חתך זהב $\varphi = 1.618034...$

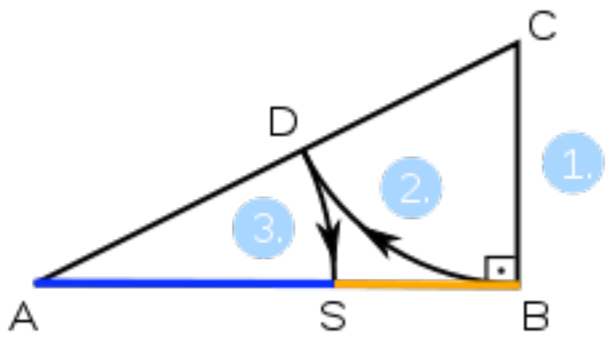
יחס בין ממדי מיבנים שנחשב אסטטי – לדוגמא מקדש אתנה באקרופוליס – הפרתנון

ככה משערים שנראה תוכו של מקדש אתינה

היונים קבעו את חתך הזהב באופן גיאומטרי– כי לא אהבו לחשב חישובים...

הגדרתו היחס בין גדלים A,B המקיימים– $(A+B)/A = A/B = B/(A-B)$

$\varphi = A/B = 1/(\varphi - 1)$



הבניה הגיאומטרית:

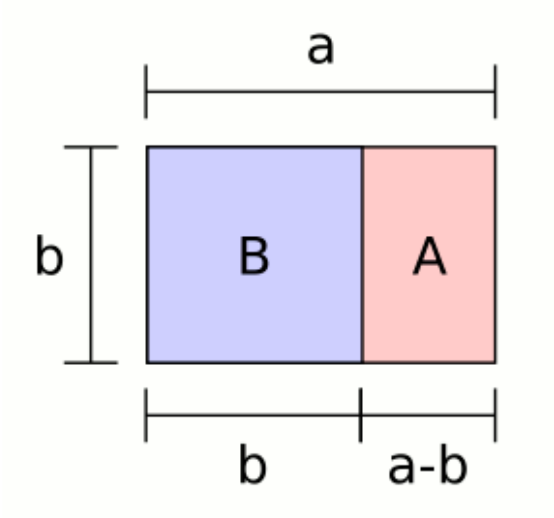
1. צייר זוית ישרה ABC הניצב BC כפול באורכו מ–AB
2. חבר AC וקבע D במרחק מ–C השווה ל–BC
3. קבע S במרחק מ–A השווה ל– AD והוא מחלק את AB ביחס זהב

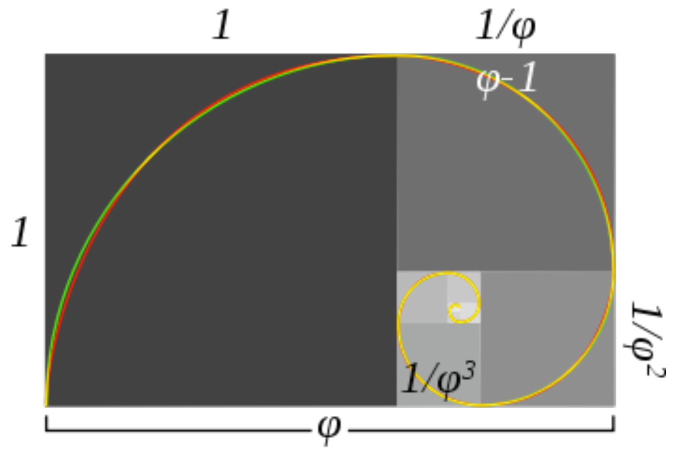
הוכחה:

BC=1 AB=2 AC=√5 CD=1 AD=√5-1=AS SB=3-√5

AS/SB=SB/(AS-SB) (√5-1)/(3-√5)=(3-√5)/(√5-1-3+√5)

$(\sqrt{5}-1)\ (\sqrt{5}-2)2 = (3-\sqrt{5})^2 \quad 2(5-3\sqrt{5}+2)=9-6\sqrt{5}+5$





אם נוציא מהמרובע axb עם צלעות a,b המקיימות יחס חתך זהב את הריבוע bxb בצבע תכילת ישאר מרובע b,a–b בצבע ורוד ששוב מקיים יחס חתך זהב
זה העקרון בבנית השבלול

בעזרת אלגברה נוכל לפתור את ערכו של φ

$$\frac{r}{s} = \frac{r+s}{r}$$

$$r^2 = rs + s^2$$

$$r^2 - rs - s^2$$

משוואה ריבועית ל- r

$$r = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-s \pm \sqrt{s^2 - 4(1)(-s^2)}}{2(10)}$$

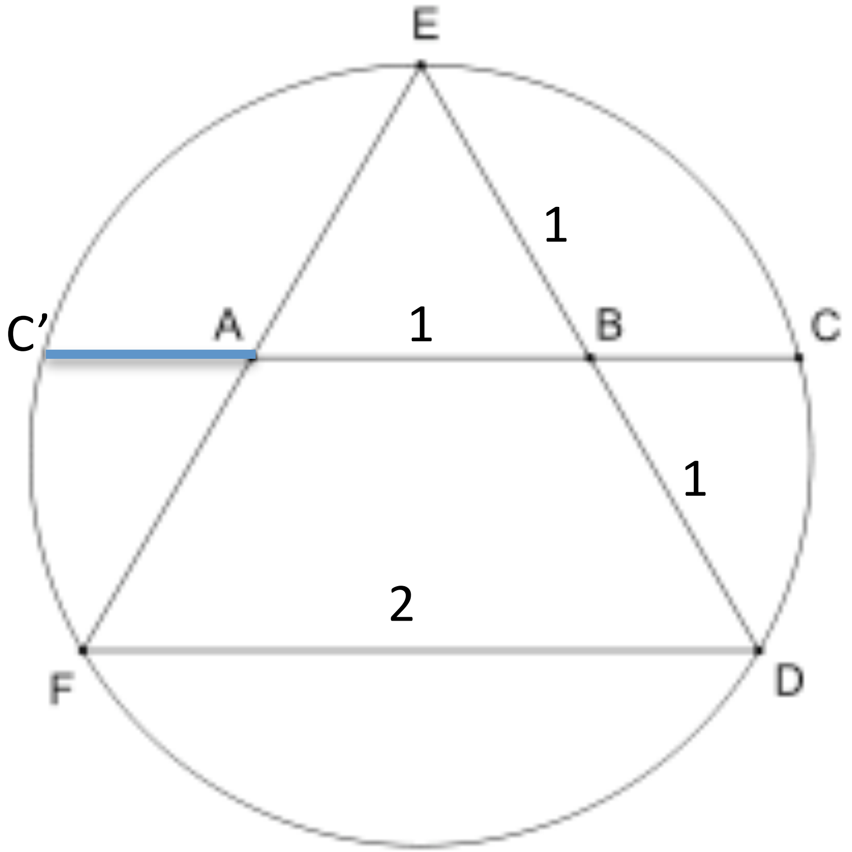
$$r = \frac{s+s\sqrt{5}}{2}$$

$$\frac{r}{s} = \frac{1+\sqrt{5}}{2} \approx 1.61803398874989.$$

דרך אחרת (**<u>פיתגורס</u>**):

<u>ממשפט המיתרים החוצים</u> $BE*BD=BC*BC'=BC*(1+BC)=BC+BC^2$

או באופן כללי ($1 \leftarrow x$ $\varphi \leftarrow a$) $x2 = a(a+x)$



$\varphi=1/(\varphi-1)$

ולכן $\varphi^2-\varphi-1=0$

מפתרונות משוואה ריבועית:

$\phi=(1\pm\sqrt{5})/2 \sim 1.618034$ a=1, b=-1, c=-1 $\phi^2-\phi-1=0$

הפתרון עם מינוס הוא שלילי ולא מתאים.

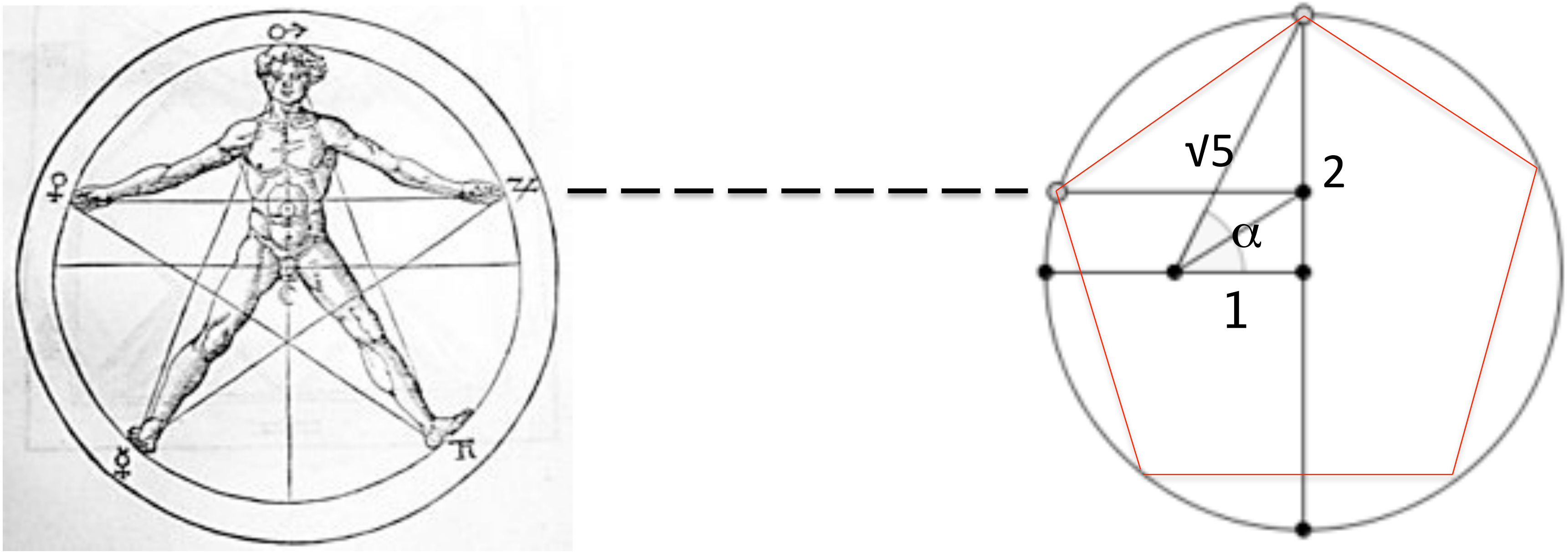
ואכן $(\sqrt{5}-1)/2=2/(\sqrt{5}+1)$

הפתרון $\Phi=(1+\sqrt{5})/2=2\cos(\pi/5)$

קשור למחומש שווה צלעות:

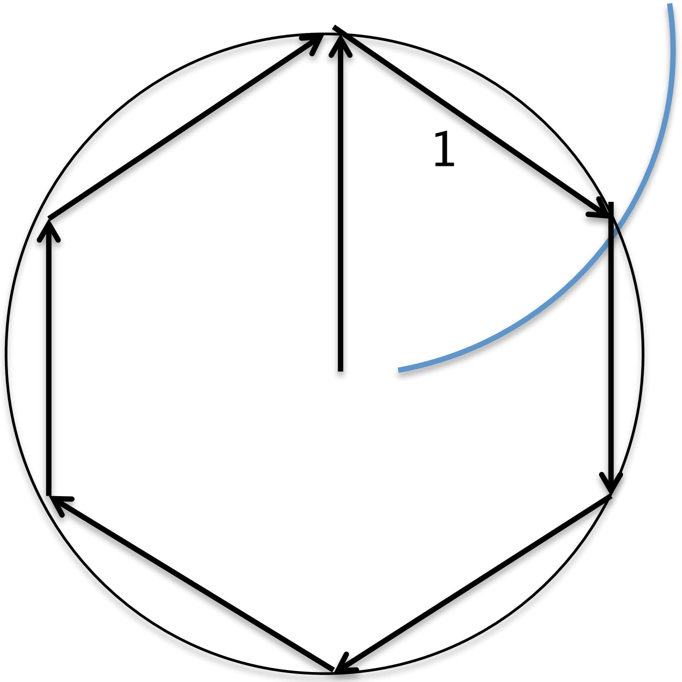
נבנה עיגול ברדיוס 2 , המשולש צלעות 1,2 ואלכסון $\sqrt{5}$

חוצה הזוית הוא גובה צלע המחומש: למחומש שווה צלעות (זויות פנימיות בקדקדים $=108^0$)

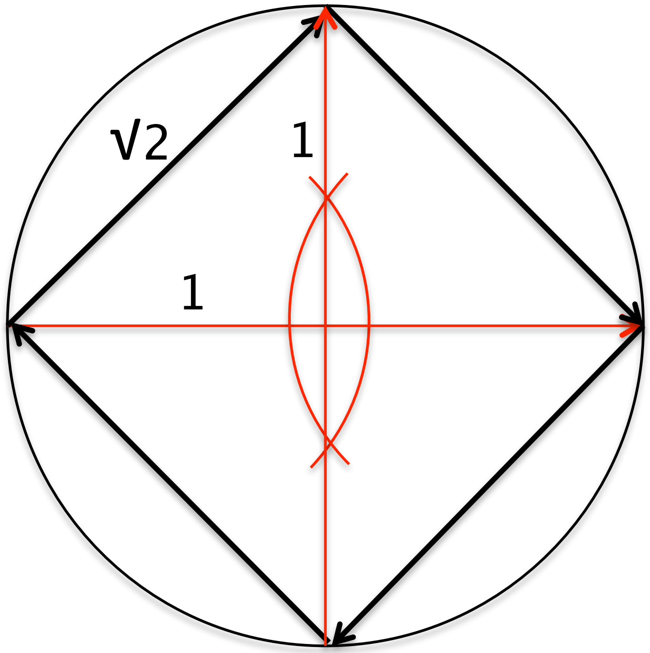


בנית פוליגונים משוכללים מסדר n :

בנית משולש ומשושה – (וממנו 12, 24 וכו)



בנית ריבוע – (ו- 8, 16, ...)



בנית 7 צלעות – אין פתרון. בעיה שלא נפתרה 2000 שנים. גאוס 1777-1855 Carl Friedrich Gauss הוכיח (בגיל 19) שלא ניתן לבנות עם מחוגה וסרגל בלבד.

הראה שבנית צלעון שוה-צלעות וזויות בעזרת מחוגה וסרגל אפשרית רק ל-n המקיים

$n=2^m*F_m$ F_m=Ferma prime=2^k+1; $k=2^m$

כיום מספרי פרמה הראשוניים הידועים הם רק: 3,5,17,257,65537

האם תוכל לבנות פוליגון משוכלל בן 17 צלעות?

הבניה של גאוס ל-17 צלעון משוכלל:

האפס והאינסוף

ברהמגופטה Brahmagupta 598-668

נתן לראשונה את <u>החוקים לאריתמטיקה של האפס</u>:

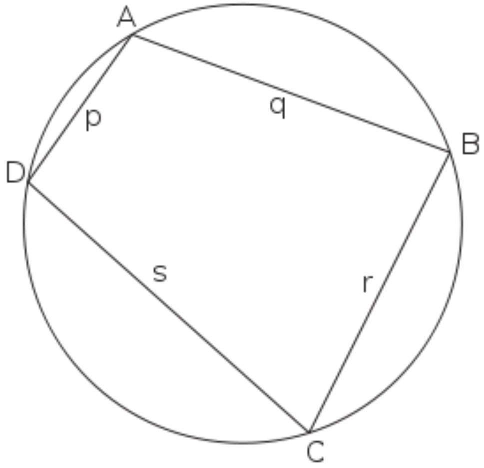
1. בחיבור או חיסור אפס ממספר הוא אינו משתנה
2. הכפלת מספר באפס נותנת אפס

<u>ואת החוקים למספרים שליליים (קרא להם "חובות"):</u>

1. חוב פחות אפס הוא חוב
2. זכות פחות אפס היא זכות
3. אפס פחות אפס נותן אפס
4. אפס פחות חוב נותן זכות
5. אפס פחות זכות נותן חוב
6. מכפלת אפס בחוב או זכות נותנת אפס
7. מכפלת אפס באפס נותנת אפס
8. מכפילת או מנת זכויות נותן זכות
9. מכפילת או מנת חובות נותן זכות
10. מכפילת או מנת חוב וזכות נותן חוב
11. מכפילת או מנת זכות וחוב נותן חוב

הוא היה חכם ונמנע מלדון בחלוקת אפס באפס...

ב-773 הגיע סיפרו לבגדד וחנך את המתמטיקה הערבית



<u>אגב: נוסחת ברהמגופטה</u>

לשטח מרובע החסום במעגל

S=(p+q+r+s)/2

$$K = \sqrt{(S-p)(S-q)(S-r)(S-s)}.$$

האפס: מאפשר לתת ערך לפי מקום במספר: כמו 20 מול 2, ומבטל צורך באותיות מיוחדות לעשרות, מאות וכו'.
הובא מהודו לפרס, מיוחס לאל–בירוני 973–1048 – מתמטיקאי ואסטרונום פרסי

בולים לציון 1000 שנים לאל–בירוני מפקיסטן, סוריה ואירן
מדוע כולן מייחסות אותו לעצמן???
הובא לספרד המאורית על ידי אברהם בן מאיר אבן עזרה 1092–1167 מטודלה וסרגוסה ויושם ע"י המתמטיקאי פיבונצ'י 1170–1250 באיטליה.
"**שיטת המספרים הערבים**" – בה אנו משתמשים היום.

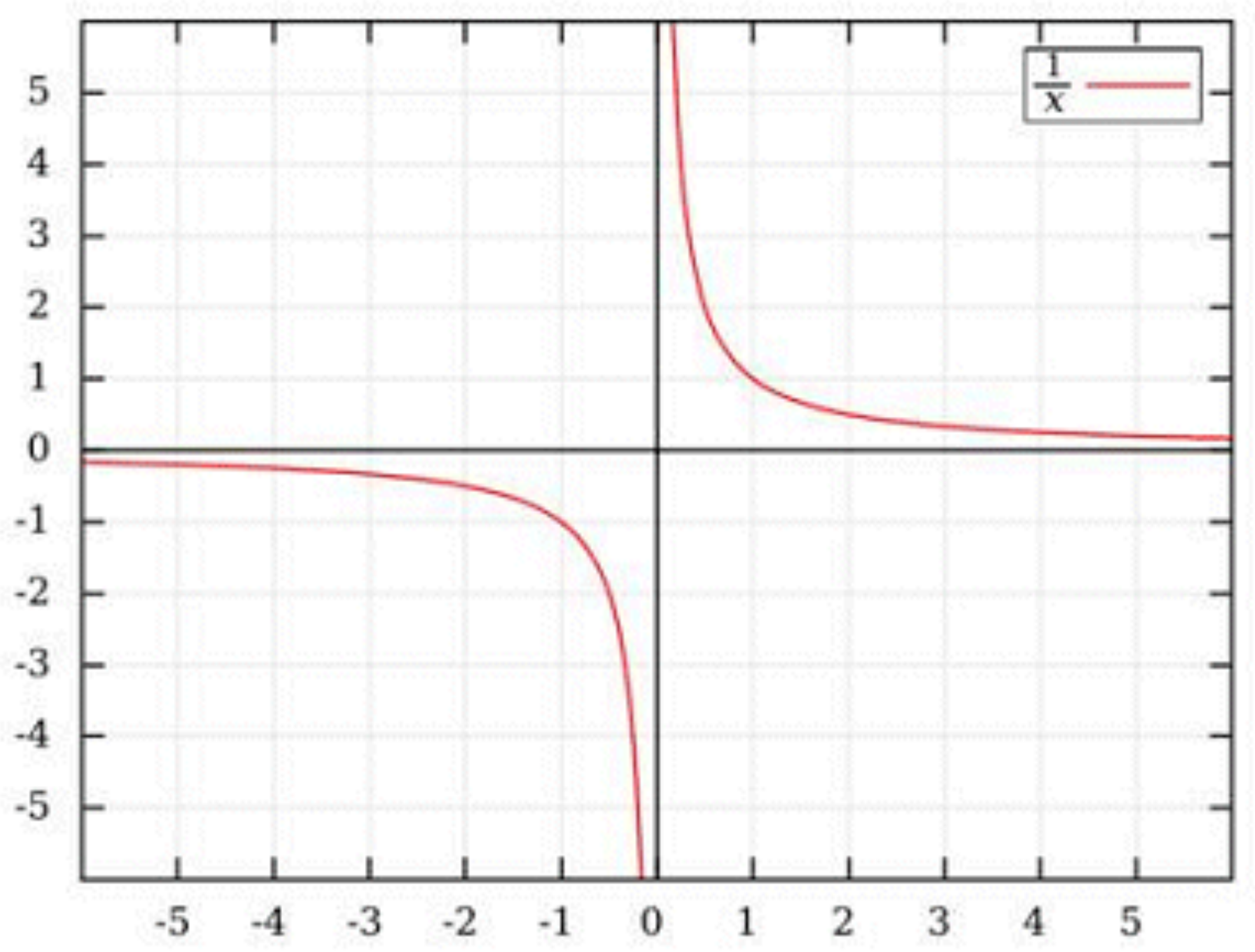
האפס דורש הרחבת תחום המספרים:

מספרים שליליים בחיסור – $-5 = 0-5$

מספר גדול אינסופי (∞) בחלוקה – אינסוף = $0/5$

כאשר x הולך וגדל $1/x$ הולך וקטן (ולהפך)

המושג של ערך "השואף לאפס" ("אפסילוני קטן") הוא הבסיס ל-calculus – חשבון דיפרנציאלי ואינטגראלי ("אינפי")



שיטת המיקום

50 לפה"ס הודים מפתחים כתיבת מספרים בשיטת המיקום תוך שימוש באפס

האינסוף ומספרים גדולים

"כחול אשר על שפת הים, ככוכבים בלילה"

ברגע שהוספנו את החילוק לפעולות בין מספרים, האפס מביא איתו את האינסוף.

אריסטו תאר אינסוף מספרים – לכל r נוכל לקבל r+1

אוקלידס הוכיח כי יש אינסוף מספרים ראשוניים: (מספרים המתחלקים רק בעצמם וב-1)

ההוכחה קונסטרוקטיבית – אם יש לנו את כל r המספרים הראשוניים $p_1, p_2, \ldots, p_r$
המספר P השוה ל-(מכפלת כולם + 1) הוא או ראשוני או שאינו ראשוני. אם ראשוני-הוא אינו ברשימה שלנו (כי גדול מכולם). אם אינו ראשוני הוא מתחלק במספר ראשוני כלשהו-q. אם היה אחד מהרשימה היה מחלק את P ואת המכפלה $p_1p_2\ldots p_r$ ולכן את ההפרש $P-p_1p_2\ldots p_r$ אך ההפרש הוא 1 ולכן q אינו יכול להיות ברשימה. בשני במיקרים קבלנו מספר ראשוני חדש – או P או q

וודה הודית (900 לפה"ס) מתארת אינסוף כמספר שאפשר להוסיף או לגרוע ממנו והוא נשאר אינסוף.

ארכימדס (287-121 לפה"ס) שתי קבוצות אינסופיות שוות בגדלן אם נוכל להתאים בזוגות את כל אבריהן.

המציא שיטה לכתיבת מספרים גדולים המבוססת על $100000000 = 10^8$

האוקטט הראשון של מספרים $1-10^8$

האוקטט השני של מספרים 10^8-10^{16} וכו

כך חישב את מספר גרגרי החול שמכיל כדור הארץ 10^{64}

אלקרזי al-Karaji הציג טיעונים של אינדוקציה החוזרת עד אינסוף

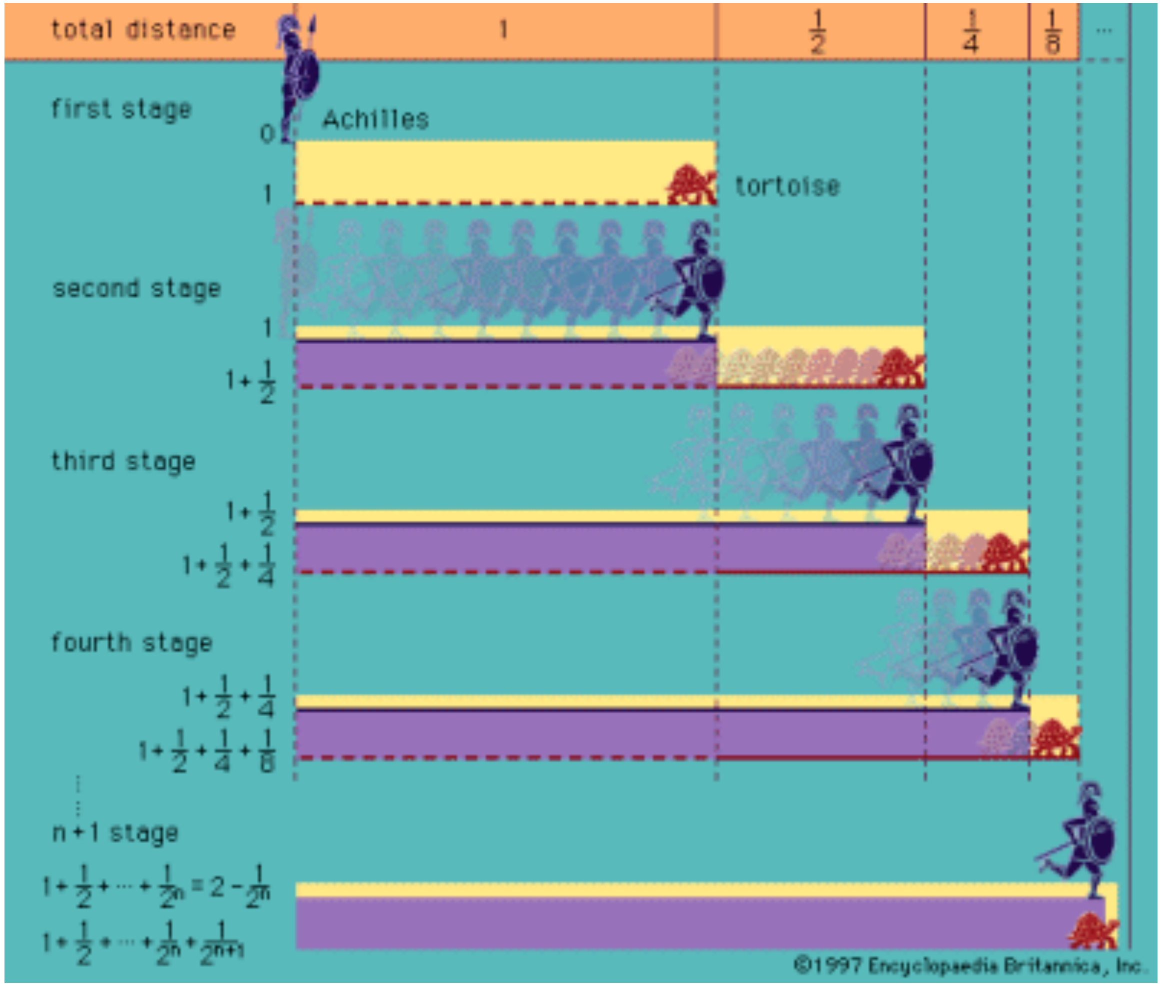
גלילאו GALILEO: אותו מספר מספרים שלמים וריבועים, למרות שהריבועים הם רק חלק מהשלמים: אין מגבלה באינסוף להתאמה בזוגות של קבוצה על חלק ממנה.
לכן גדול וקטן <> אינו ישים לאינסוף

בולצאנו Bolzano הגדיר קבוצות עם אינסוף אלמנטים

בחשבון איפניטסימאלי אם בגבול $\varepsilon \to 0$ אז $1/\varepsilon \to \infty$
ובכל זאת ניתן במקרים מסויימים להגדיר את הגבול עבור $0 * \infty$
כאשר $x \to 0$ האינסוף של $1/x^2$ "חזק" יותר מזה של $1/x$
(ראה בהמשך משפט לופיטל)

פרדוקס של זינו – אכילס והצב: יסודות האינפי (Calculus)

אכילס רץ במהירות 2 מטר לשניה והצב במהירות 1 מטר לשניה
אכילס מתחיל 2 מטר מקו המטרה ונותן לצב יתרון להתחיל 1 מטר מקו המטרה
הם מתחילים לרוץ: כשאכילס רץ 1 מטר הוא הגיע לנקודת המוצא של הצב, אך הצב התקדם 1/2 מטר כשאכילס ירוץ עוד 1/2 מטר הצב יתקדם עוד 1/4 מטר וכך עד אינסוף – כל פעם שאכילס יגיע לנקודה בה היה הצב – הצב יזוז קדימה – ולכן אכילס מעולם לא ישיג את הצב...
האכן? איפה הטעות? הרי אנו יכולים לחשב שאכילס והצב בדיוק יפגשו בקו הסיום כעבור שניה אחת!



סדרות אינסופיות, סכומים אינסופיים

אורך קו = 1

אורך שני חצאים = ½+½ = 1

אורך ארבעה רבעים = ¼ + ¼+ ¼ + ¼ = 1

...

ארך N שברים כ"א באורך $N * 1/N = 1$

$N \to \infty$ $\quad$ $\infty * 0 = 1$

כך גם הסכום עם מספר רב של אברים "שואף" לגבול 2 $\quad 1+1/2+1/4+1/8+ \ldots \Rightarrow 2$

יסודות האינפי – התכנסות ורציפות

אנו אומרים כי $\lim_{x \to a} f(x) = L$

אם ורק אם לכל $\epsilon > 0$ קיים $\delta > 0$ כך שאם $|x - a| < \delta$ אז $|f(x) - L| < \epsilon$

הדרך להוכחה הוא חילוץ x מהאי שוויון

דרך עם הסבר גיאומטרי: נקרב את f סביב $f(a)=L$ בקו המשיק. שיפועו של הקו הוא הנגזרת של

$f(x)$ במקום $x=a$ שתסומן $f'(a)$

עבור δ קטן $\quad f(a+\delta)+\varepsilon=L+f'(a)*\delta = L$

ולכן $\quad \delta*f(a) = \varepsilon$

מה מיוחד בפונקציות בעלות נגזרת? רציפות!

דוגמא לפונקציה פשוטה אך ללא נגזרת ב- $x=0$

$f(x)=1/x$

π

π = 3.14159265…

מה ערכו של π בתנ"ך?

תאור ים הנחושת בבית המקדש: קוטר=10, הקף=30, גובה=5,
נפח=2000 בת: אם היה צילינדרי נפחו היה 390 "אמות מעוקבות"
אך אם היה חצי כדור נפחו 260 אמות מעוקבות. מה נפח בת?

<u>וַיַּעַשׂ</u> אֶת הַיָּם מוּצָק; עֶשֶׂר בָּאַמָּה מִשְּׂפָתוֹ
עַד שְׂפָתוֹ, עָגֹל סָבִיב, וְחָמֵשׁ בָּאַמָּה
קוֹמָתוֹ; שְׁלֹשִׁים בָּאַמָּה יָסֹב אֹתוֹ סָבִיב.
וּפְקָעִים מִתַּחַת לִשְׂפָתוֹ סָבִיב סֹבְבִים אֹתוֹ
עֶשֶׂר בָּאַמָּה מַקִּפִים אֶת הַיָּם סָבִיב; שְׁנֵי
טוּרִים הַפְּקָעִים יְצֻקִים בִּיצֻקָתוֹ. עֹמֵד עַל
שְׁנֵי עָשָׂר בָּקָר שְׁלֹשָׁה פֹנִים צָפוֹנָה וּשְׁלֹשָׁה
פֹנִים יָמָּה וּשְׁלֹשָׁה פֹּנִים נֶגְבָּה וּשְׁלֹשָׁה
פֹּנִים מִזְרָחָה וְהַיָּם עֲלֵיהֶם מִלְמָעְלָה; וְכָל
אֲחֹרֵיהֶם בָּיְתָה. וְעָבְיוֹ טֶפַח וּשְׂפָתוֹ
כְּמַעֲשֵׂה שְׂפַת כּוֹס פֶּרַח שׁוֹשָׁן – אַלְפַּיִם בַּת
יָכִיל.

– מלכים א ז, 6–23

במצרים 1650 לפה"ס Rhind Papyrus $\pi=4(8/9)^2=3.16$

ובמקום אחר $\pi=25/8=3.125$

במסופוטמיה $\pi=\sqrt{10}=3.162$ or $\pi=25/8=3.1250$

בהודו קבעו כי יחס הקף המעגל לקטרו שונה מיחס השטח לריבוע הרדיוס

מה מראים הקירובים הנ"ל?

המצרים מציגים את π כמספר רציונאלי – לא הכירו מספרים אירציונאליים

הבבלים ידעו לחשב שרשים ולכן קרבו את π בשרש

ההודים ידעו לעשות חישובים מדוייקים אך בגלל טעות מדידה של שטח כנראה הסיקו הנ"ל

ארכימדס 212–287 לפה"ס Archimedes of Syracuse הוכיח באופן גיאומטרי שהיחסים בין הקף לקוטר ושטח עיגול לריבוע הרדיוס שווים. שימוש ראשון באינפי (שיטת המיצוי). ראה להלן

קבע גבול עליון ותחתון $223/71 < \pi < 22/7$

קירובים אחרים:

Wallis (1616-1703) $2/\pi = (1.3.3.5.5.7.\ldots)/(2.2.4.4.6.6.\ldots)$

James Gregory (1638- 1675) $\tan^{-1} x = x - x^3/3 + x^5/5 - \ldots$

$\pi/4 = \tan^{-1}(1/2) + \tan^{-1}(1/3)$

Leibniz (1646-1716) $\pi/4 = 1 - 1/3 + 1/5 - 1/7 + \ldots$

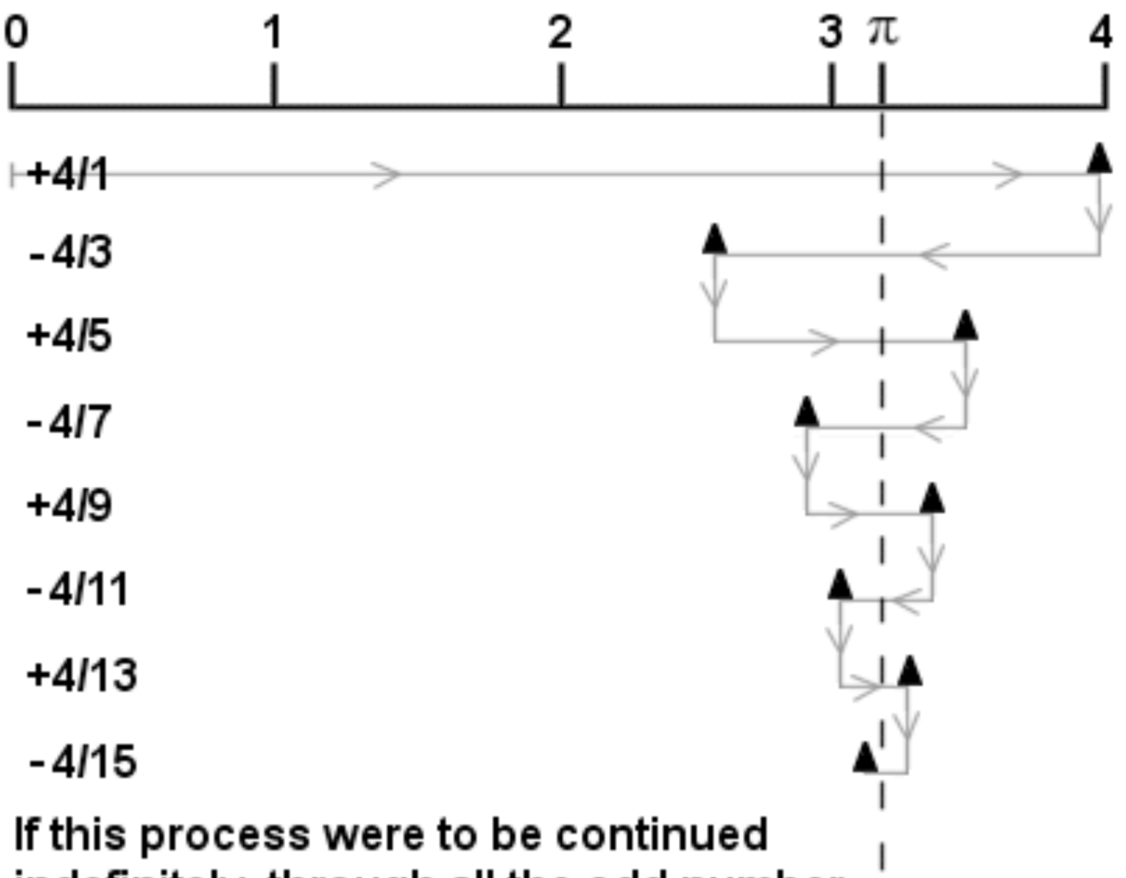
הוכחה כי π אירציונאלי: 1761 Lambert

מעניין: זרוק מחט באורך k על שריג עם מרווח = 1. הסיכוי למחט ליפול על קו מהשריג $\mathbf{2k/\pi}$

מדוע חיכינו עד כאן כדי לספר על π ? בגלל התלות באינפי.

מדהבה מסנגמגרמה (c. 1350–1425) Madhava of Sangamagrama מצא קירוב ל – π

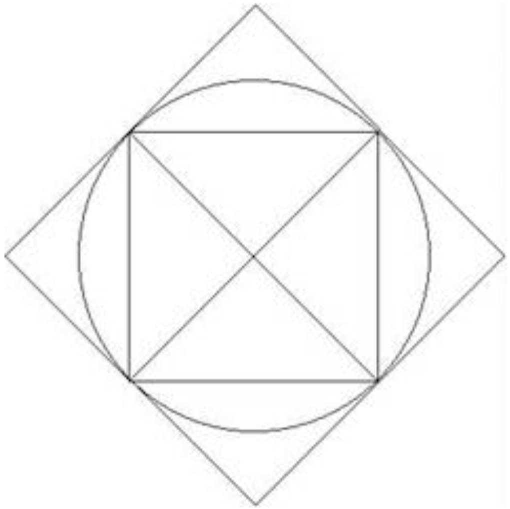
$$\pi = 4 - 4/3 + 4/5 - 4/7 + 4/9 - 4/11 + 4/13 - 4/15 \ldots 4/\infty$$

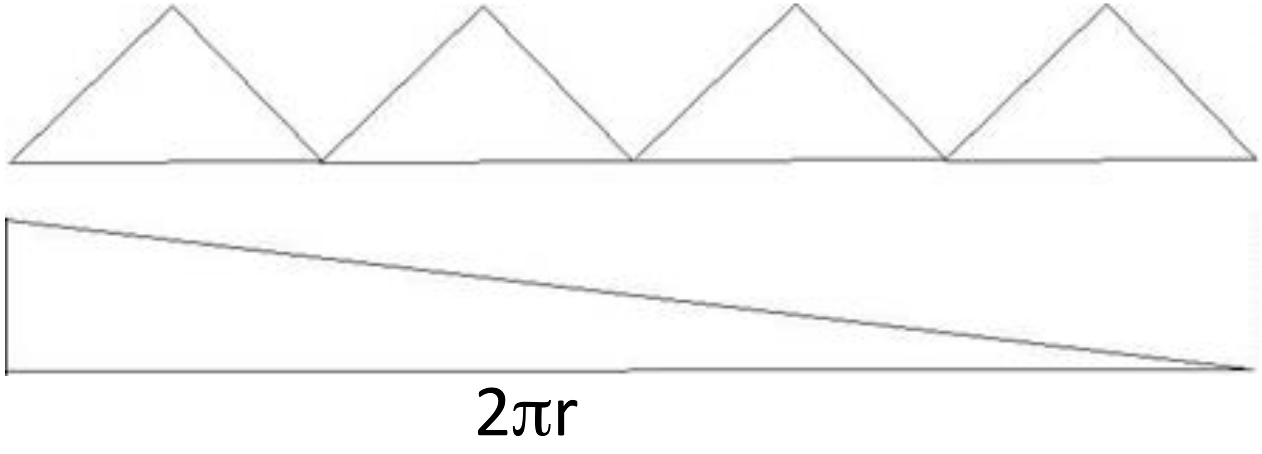


If this process were to be continued indefinitely, through all the odd number fractions to infinity, the approximation would hit π exactly

ארכימדס הוכיח **<u>ששטח המעגל</u>** שוה לשטח משולש ישר זוית עם צלעות האנכים באורך הרדיוס ובאורך הקפו בהתאמה.
רעיון ההוכחה הוא:
ריבוע החסום בכדור מחולק ל-4 משולשים ישרי זוית עם צלע h ובסיס b=2h
שטח הריבוע החסום = 4 פעמים שטח המשולש = 2hb
שטח זה שוה לשטח משולש בגובה h ובסיס 4b שהוא הקף הריבוע החסום.
קירוב טוב יותר - אוקטגון. גם האוקטגון מתחלק למשולשים ישרי זוית שגבהם כמרחק בין המרכז לאמצע צלעות האוקטגון. גם שטחם הוא גובה המשולשים כפול הקף האוקטגון.
נוכל כך להמשיך בפוליגון חסום עם 16 צלעות וכו.
אם אנו בשלב של פוליגון עם n צלעות עבור n מאד גדול גובה המשולשים מתקרב לרדיוס המעגל, והקף הפוליגון מתקרב להקף המעגל. ולכן:

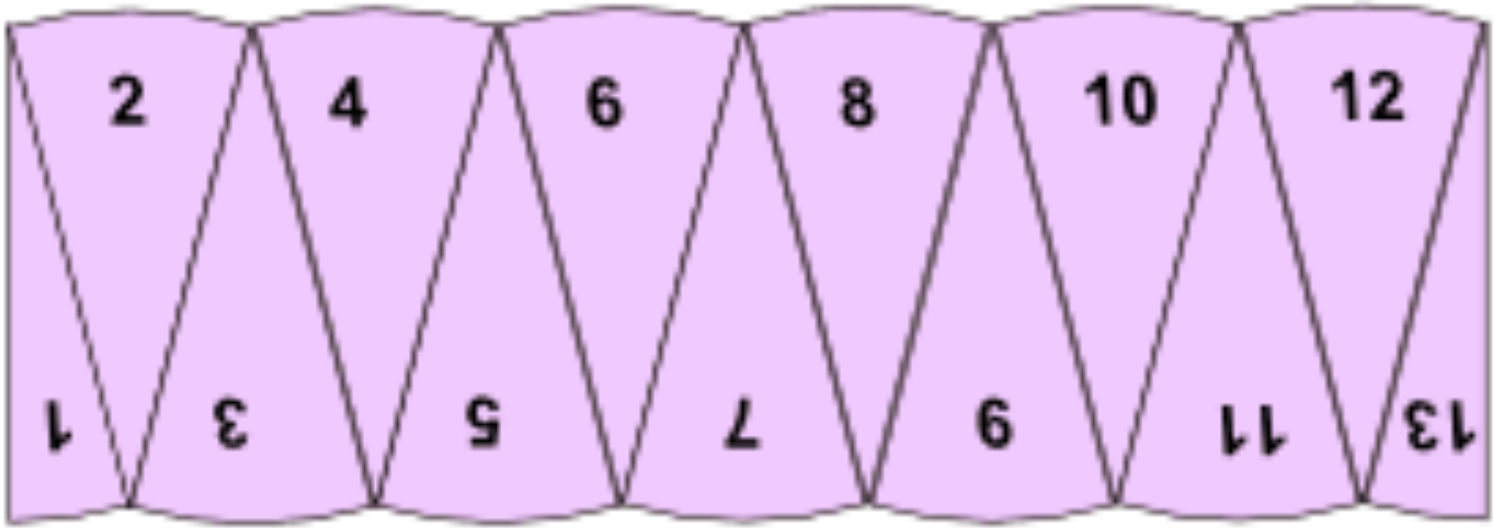
$$\tfrac{1}{2}\times\text{base(perimeter)}\times\text{height(radius)} = \tfrac{1}{2}\times 2\times\pi\times r\times r = \pi\times r^2$$





בצורה אחרת:

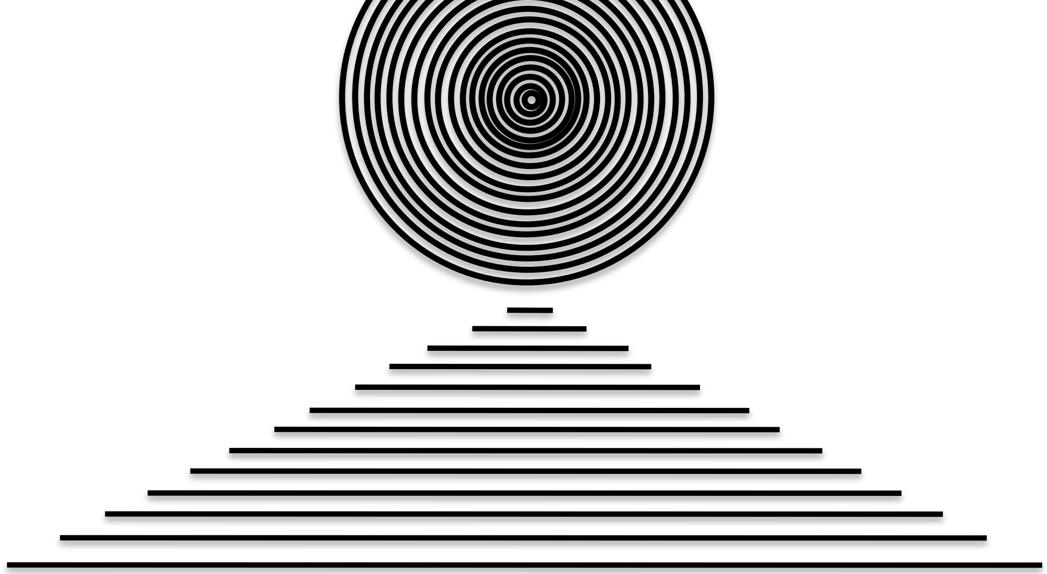
הקשר בין רדיוס R שטח המעגל A והקפו S הוא: $A=RS/2$



הסבר אחר נתן רבי אברהם בר חיא הנשיא (בסיפרו "חבור המשיחה והתשברת" הוצאת חברת מקיצי נרדמים, תרע"ג ברלין) וזה לשון ההוכחה:

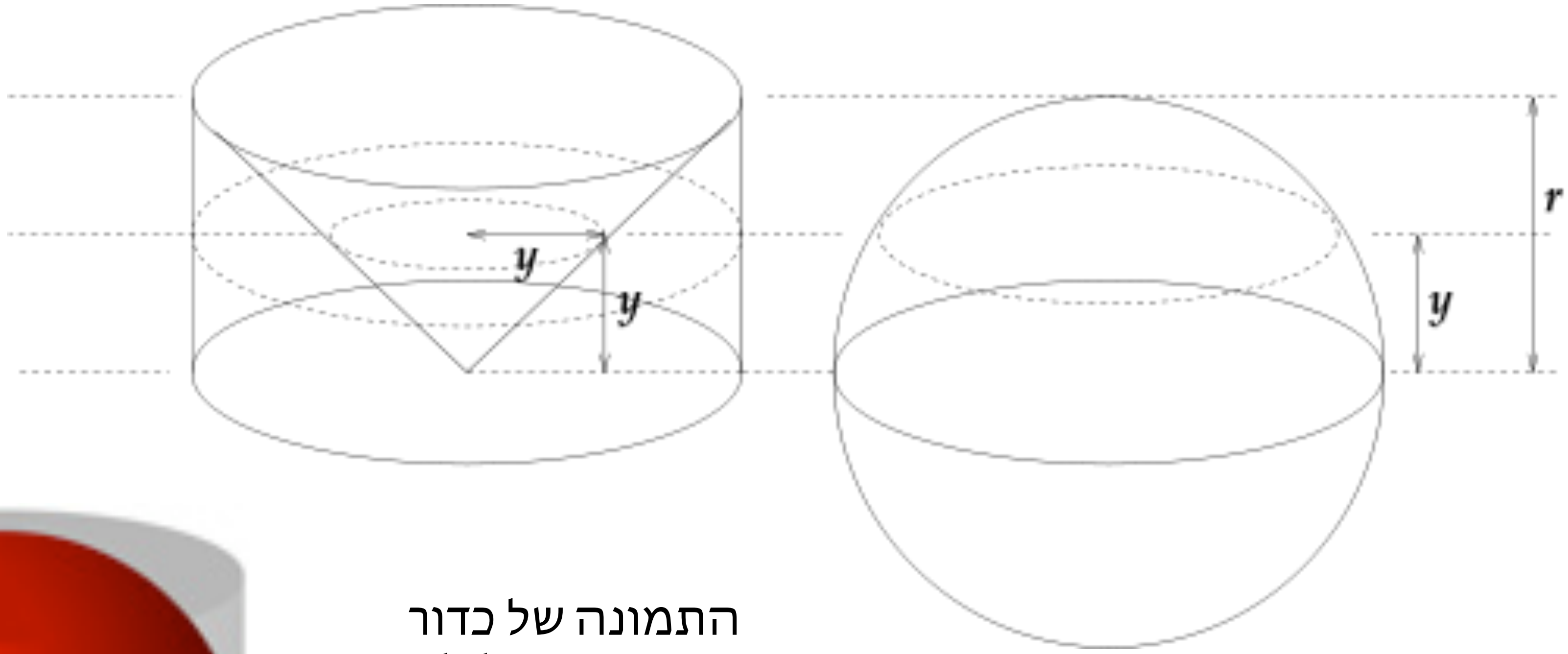
"והאות [=הוכחה] על התשבורת [=מידת השטח] הזה ידענו: אם תפתח שטח העיגול מצד אחד ותיישר כל הקוים הסובבים מקו החיצוני עד המרכז, יתפשטו המקיפים שטח העיגול ויחזרו לקוים מתמעטים והולכים עד שחוזרים אל נקודה אחת, והיא נקודת המרכז – החיצון גדול מכולם, ואשר לפנים ממנו קטן ממנו וגדול מאשר לפנים ממנו, וכן הולכים עד הנקודה, ובזה נולדה לנו צורת המשולש, ותשבורת המשולש כבר בארנו, היא כדי העמוד [=גובה] בחצי התושבת [=בסיס], וזה מחצית הקוטר [=רדיוס] במחצית הקו המקיף [=הקף]"

אנו נכתוב: $\pi R^2 = 2\pi R * R/2$



כך גם הקשר בין שטח פני הכדור וניפחו, המורכב מפירמידות בגובה הרדיוס שסכום שטח בסיסם הוא שטח פני הכדור. אנו נכתוב: $4/3\pi R^3 = 4\pi r^2 * R/3$

שטח ונפח כדור הוא 2/3 משטח (כולל בסיסיו) ונפח הצילינדר החוסם אותו
הוכחה: (ראה משפט קבאליירי ב"גיאומטריה")
נפח כדור שוה לנפח גליל להוציא חרוט שרדיוס בסיסו וגובהו שוים לרדיוס הכדור:
בכל חתך שטח חתך הכדור $\pi(r^2-y^2)$ וזה גם שטח חתך הגליל בלי הקונוס.
נפח הקונוס $\pi r^3/3$ לכן נפח הכדור $r^3(1-1/3)2=4/3\pi r^3$



התמונה של כדור
החסום בגליל
שארכימדס ביקש לצייר
על קיברו, עדות
לחשיבות ממצא זה
בעיניו
(לפי ציצרו 75 לפה"ס)

הנ"ל קושר את נוסחאות השטח וההקף לאותו יחס גודל π

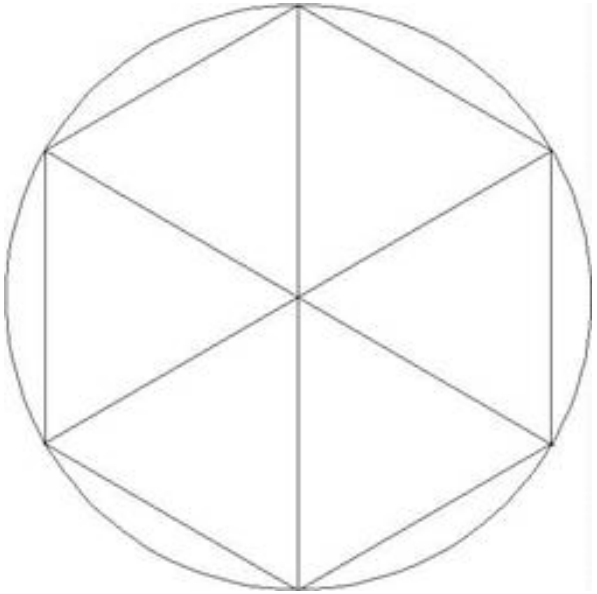
אך ארכימדס גם חישב ערך של π בדיוק רב מהקף פוליגון עם $n \to \infty$

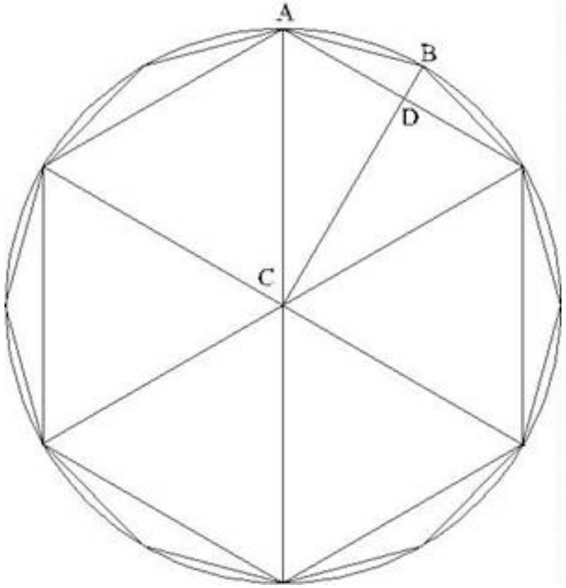
נובע מנוסחת **אינדוקציה** המבוססת על משפט פיטגורס:

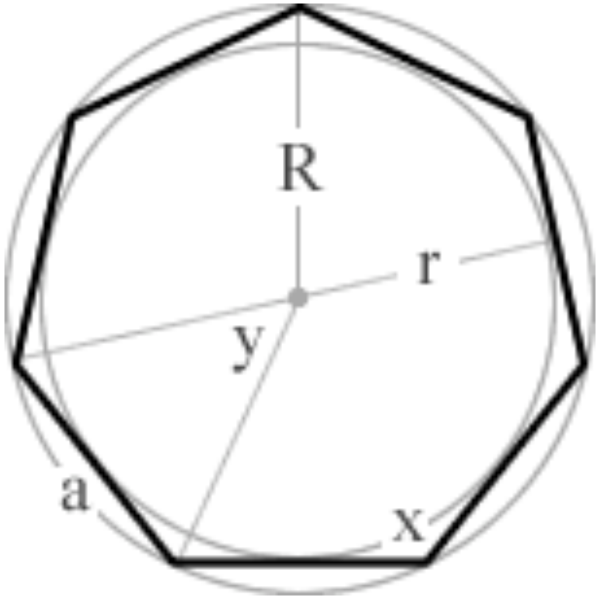
ידוע צלעות משושה

מתוך הצלעות של פוליגון עם 6 צלעות

חישב צלעות פוליגון של 12 צלעות







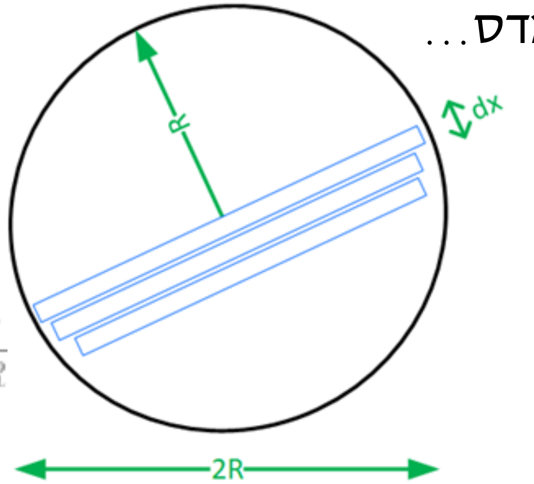
מה החשיבות של חישוב מדוייק של π היום בעולם ממוחשב?
חישובי קואורדינטות וזויות לחריטת חלקים מכאניים
חישובי מיקום למשל ב-GPS מתוך חישובי פזות
חישובי נפחים ושטחים לאריזה של מזון (בקבוקים) או כל חומר אחר
חישוב חמרי בנין (בטון ליציקת עמודים)

נחזור לחישוב **π** בפרק על גיאומטריה

מעניין: אם שטח המעגל (דו ממדי) יחסי ל-**π**, וגם נפח כדור (תלת ממדי), מה היפר-נפח של כדור ארבע ממדי?
התשובה: יחסי ל-**π**^{2} וכך לכדור חמש ממדי.
כל שני ממדים החזקה עולה ב-1.
נוכל להסביר בעזרת חשבון אינטגראלי:

הבה נחשב נפח היפר–כדור ב–n ממדים

נלך בעקבות ארכימדס...



שטח עיגול (n=2)

$$\begin{aligned}
V_2(R) &= \int_{-R}^{R} V_1(\sqrt{R^2-x^2})dx \\
&= \int_{-R}^{R} 2\sqrt{R^2-x^2}dx \\
&= 2R^2\int_{-R}^{R}\sqrt{1-(\frac{x}{R})^2}d\frac{x}{R} \\
&= 2R^2\int_{-\pi/2}^{\pi/2}\sqrt{1-\sin^2\theta}\, d(\sin\theta) \text{ where } \sin\theta=\frac{x}{R} \\
&= 2R^2\int_{-\pi/2}^{\pi/2}\cos^2\theta\, d\theta \\
&= 2R^2\cdot\frac{1}{2}[\theta+\sin 2\theta]_{-\pi/2}^{\pi/2} \\
&= \pi R^2
\end{aligned}$$

נפח כדור (n=3)

$$\begin{aligned}
V_3(R) &= \int_{-R}^{R} V_2(\sqrt{R^2-x^2})dx \\
&= \int_{-R}^{R} \pi(\sqrt{R^2-x^2})^2 dx \\
&= \pi(2R^3-\int_{-R}^{R}x^2dx) \\
&= \pi(2R^3-\frac{2R^3}{3}) \\
&= \frac{4}{3}\pi R^3
\end{aligned}$$

היפר–נפח כדור (n=4)

$$\begin{aligned}
V_4(R) &= \int_{-R}^{R} V_3(\sqrt{R^2-x^2})dx \\
&= \int_{-R}^{R} \frac{4}{3}\pi(\sqrt{R^2-x^2})^3 dx \\
&= \frac{4}{3}\pi R^4\int_{-R}^{R}(1-(\frac{x}{R})^2)^{\frac{3}{2}}d(\frac{x}{R}) \\
&= \frac{4}{3}\pi R^4\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}(1-\sin^2\theta)^{\frac{3}{2}}d(\sin\theta) \text{ where } \sin\theta=\frac{x}{R} \\
&= \frac{4}{3}\pi R^4\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\cos^3\theta\cdot\cos\theta d\theta \\
&= \frac{4}{3}\pi R^4\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\cos^4\theta d\theta \\
&= \frac{4}{3}\pi R^4([\frac{\cos^3\theta\sin\theta}{4}]_{-\frac{\pi}{2}}^{\frac{\pi}{2}}+\frac{3}{4}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}\cos^2\theta d\theta) \\
&= \frac{4}{3}\pi R^4(0+\frac{3}{4}\frac{1}{2}[\theta+\sin 2\theta]_{-\frac{\pi}{2}}^{\frac{\pi}{2}}) \\
&= \frac{\pi^2}{2}R^4
\end{aligned}$$

המשך 1 ...

נוסחא רקורסיבית לנפח היפר_נפח כדור בממד n כאינטגראל על ממד n-1

$$V_N(R) = \int_{-R}^{R} V_{N-1}(\sqrt{R^2 - x^2})dx \qquad V_N(R) = K_N R^N$$

$$\begin{aligned}
V_N(R) &= \int_{-R}^{R} V_{N-1}(\sqrt{R^2 - x^2})dx \\
&= K_{N-1} \int_{-R}^{R} (R^2 - x^2)^{\frac{N-1}{2}} dx \\
&= K_{N-1} R^N \int_{-R}^{R} (1 - (\frac{x}{R})^2)^{\frac{N-1}{2}} d(\frac{x}{R}) \\
&= K_{N-1} R^N \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^{N-1}\theta \cdot \cos\theta d\theta \text{ where } \sin\theta = \frac{x}{R} \\
&= K_{N-1} R^N \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^N \theta d\theta
\end{aligned}$$

$$\begin{aligned}
V_N(R) \quad &= \quad K_N R^N = C_N K_{N-1} R^N \text{ where } C_N = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^N \theta d\theta \\
\implies &\quad K_N = C_N K_{N-1} \\
\implies &\quad K_N = (\prod_{i=2}^{N} C_i) K_1 = 2 \prod_{i=2}^{N} C_i \text{ (since } K_1 = 2)
\end{aligned}$$

$$C_N = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^N \theta d\theta = \frac{N-1}{N} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^{N-2} \theta d\theta \implies C_N = \frac{N-1}{N} C_{N-2}$$

המשך 2...

$$
\begin{aligned}
C_N C_{N-1} &= \frac{N-1}{N} C_{N-2} \frac{N-2}{N-1} C_{N-3} \\
&= \frac{N-2}{N} C_{N-2} C_{N-3} \\
&= \frac{N-2}{N} \frac{N-4}{N-2} C_{N-4} C_{N-5} \\
&= \frac{N-4}{N} C_{N-4} C_{N-5} \\
&= \begin{cases} \frac{2}{N} C_2 C_1 & \text{if N is even} \\ \frac{1}{N} C_1 C_0 & \text{if N is odd} \end{cases} \\
&= \begin{cases} \frac{2\pi}{N} & \text{if N is even} \\ \frac{2\pi}{N} & \text{if N is odd} \end{cases} \\
&= \frac{2\pi}{N}
\end{aligned}
$$

$$
\begin{aligned}
C_0 &= \pi \\
C_1 &= 2 \\
C_2 &= \frac{\pi}{2}
\end{aligned}
$$

$$
\begin{aligned}
K_N &= 2 \prod_{i=2}^{N} C_i \\
&= \begin{cases} 2 \cdot \frac{2\pi}{N} \frac{2\pi}{N-2} \ldots \frac{2\pi}{4} C_2 & \text{if N is even} \\ 2 \cdot \frac{2\pi}{N} \frac{2\pi}{N-2} \ldots \frac{2\pi}{3} & \text{if N is odd} \end{cases} \\
&= \begin{cases} \pi \cdot \frac{2\pi}{N} \frac{2\pi}{N-2} \ldots \frac{2\pi}{4} & \text{if N is even} \\ 2 \cdot \frac{2\pi}{N} \frac{2\pi}{N-2} \ldots \frac{2\pi}{3} & \text{if N is odd} \end{cases}
\end{aligned}
$$

$$
V_N(R) = \begin{cases} \pi \cdot \frac{2\pi}{N} \frac{2\pi}{N-2} \ldots \frac{2\pi}{4} \cdot R^N & \text{if N is even} \\ 2 \cdot \frac{2\pi}{N} \frac{2\pi}{N-2} \ldots \frac{2\pi}{3} \cdot R^N & \text{if N is odd} \end{cases}
$$

רואים לכן שנפח היפר–כדור בממד $n>6$ הולך וקטן: תכונה לא אינטואיטיבית לממדים גבוהים !!!

חישוב אחר (עבור כדור יחידה r=1)

עבור קו

$$V_0 = 1$$

$$S_0 = 2$$

$$V_{n+1} = \int_0^1 S_n r^n \, dr \quad \longrightarrow \quad V_{n+1} = \frac{S_n}{n+1}.$$

$$S_{n+2} = \int_0^{\frac{\pi}{2}} S_1 r.\, S_n R^n \, d\theta$$

$$= \int_0^{\frac{\pi}{2}} S_1 \cdot S_n R^n \cos\theta \, d\theta$$

$$= \int_0^1 S_1 \cdot S_n R^n \, dR$$

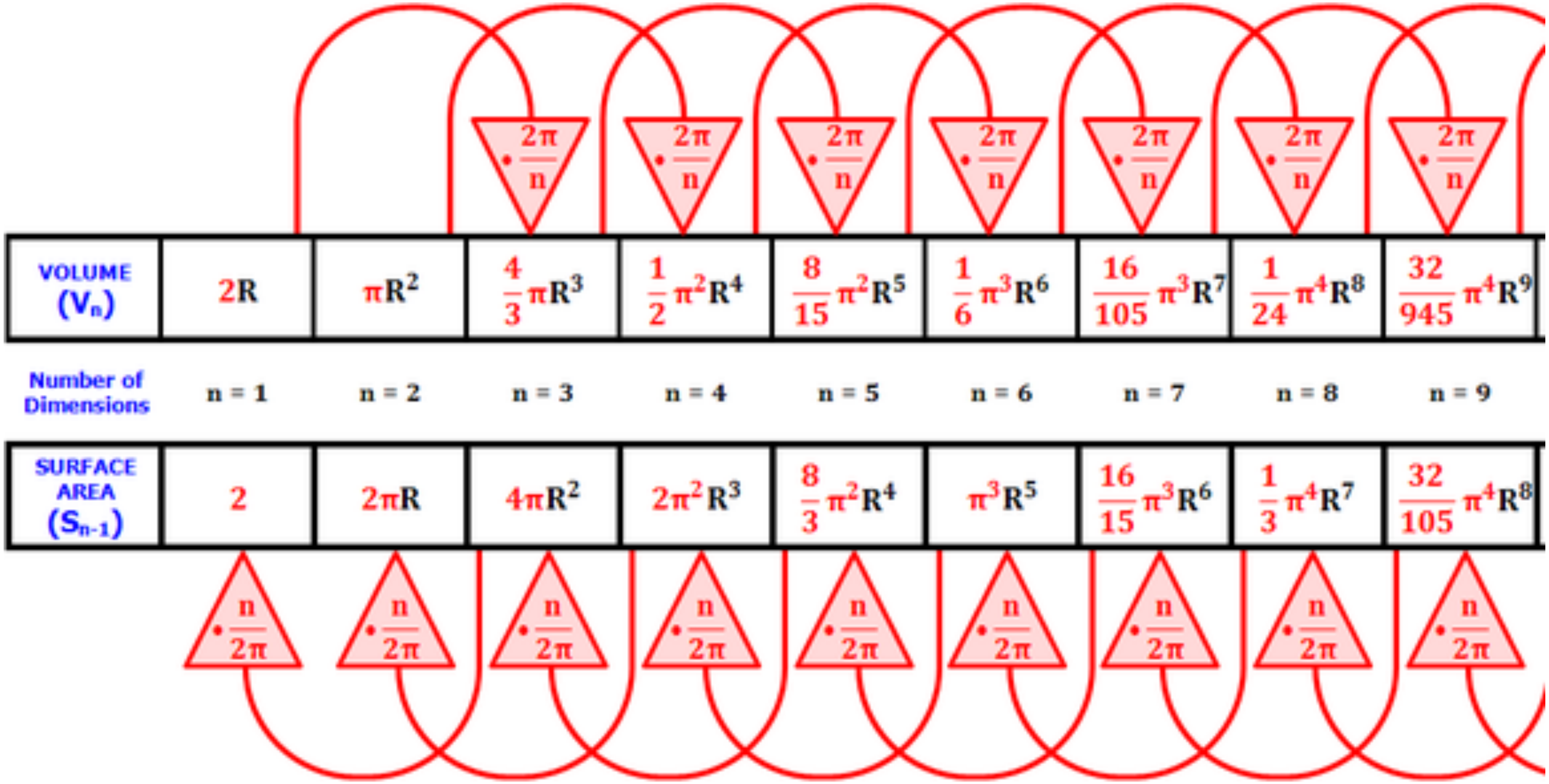
$$= S_1 \int_0^1 S_n R^n \, dR$$

$$= 2\pi V_{n+1} \quad \longrightarrow \quad S_{n+1} = 2\pi V_n$$

$$V_{n+2} = 2\pi \frac{V_n}{n+2}.$$

$$V_{2k} = \frac{\pi^k}{k!}$$

$$V_{2k+1} = \frac{2(2\pi)^k}{(2k+1)!!} = \frac{2k!(4\pi)^k}{(2k+1)!}$$



VOLUME (V_n)	$2R$	πR^2	$\frac{4}{3}\pi R^3$	$\frac{1}{2}\pi^2 R^4$	$\frac{8}{15}\pi^2 R^5$	$\frac{1}{6}\pi^3 R^6$	$\frac{16}{105}\pi^3 R^7$	$\frac{1}{24}\pi^4 R^8$	$\frac{32}{945}\pi^4 R^9$
Number of Dimensions	n = 1	n = 2	n = 3	n = 4	n = 5	n = 6	n = 7	n = 8	n = 9
SURFACE AREA (S_{n-1})	2	$2\pi R$	$4\pi R^2$	$2\pi^2 R^3$	$\frac{8}{3}\pi^2 R^4$	$\pi^3 R^5$	$\frac{16}{15}\pi^3 R^6$	$\frac{1}{3}\pi^4 R^7$	$\frac{32}{105}\pi^4 R^8$

חזקות

כוחן של חזקות

סדרות גיאומטריות

צייר 1.2^n 1.4^n 2^n

כמו ...... $(2^{1/2})^{2n}$ $((2^{1/2})^{2})^{n}$

הגבול $2^{n/m} = (2^{1/m})^{mn}$

סכום סידרה גיאומטרית (אם $n \to \infty$ מתכנס רק אם $q<1$)

$1+q+q^2+q^3+ \ldots q^n =(1-q^n)/(1-q)$

חלוקה של בקטריות – כל כשעה. מספרן גדל אקפוננציאלית (מדוע לא יכול להמשיך לתמיד?)

גרעיני אורז על לוח שחמט $0.18\times10^{20} \sim 2^{64} = 18,446,462,598,732,800,000$

ז"א שמשקל האורז 1/30000 ממשקל כדור הארץ שהוא 5.974×10^{24}

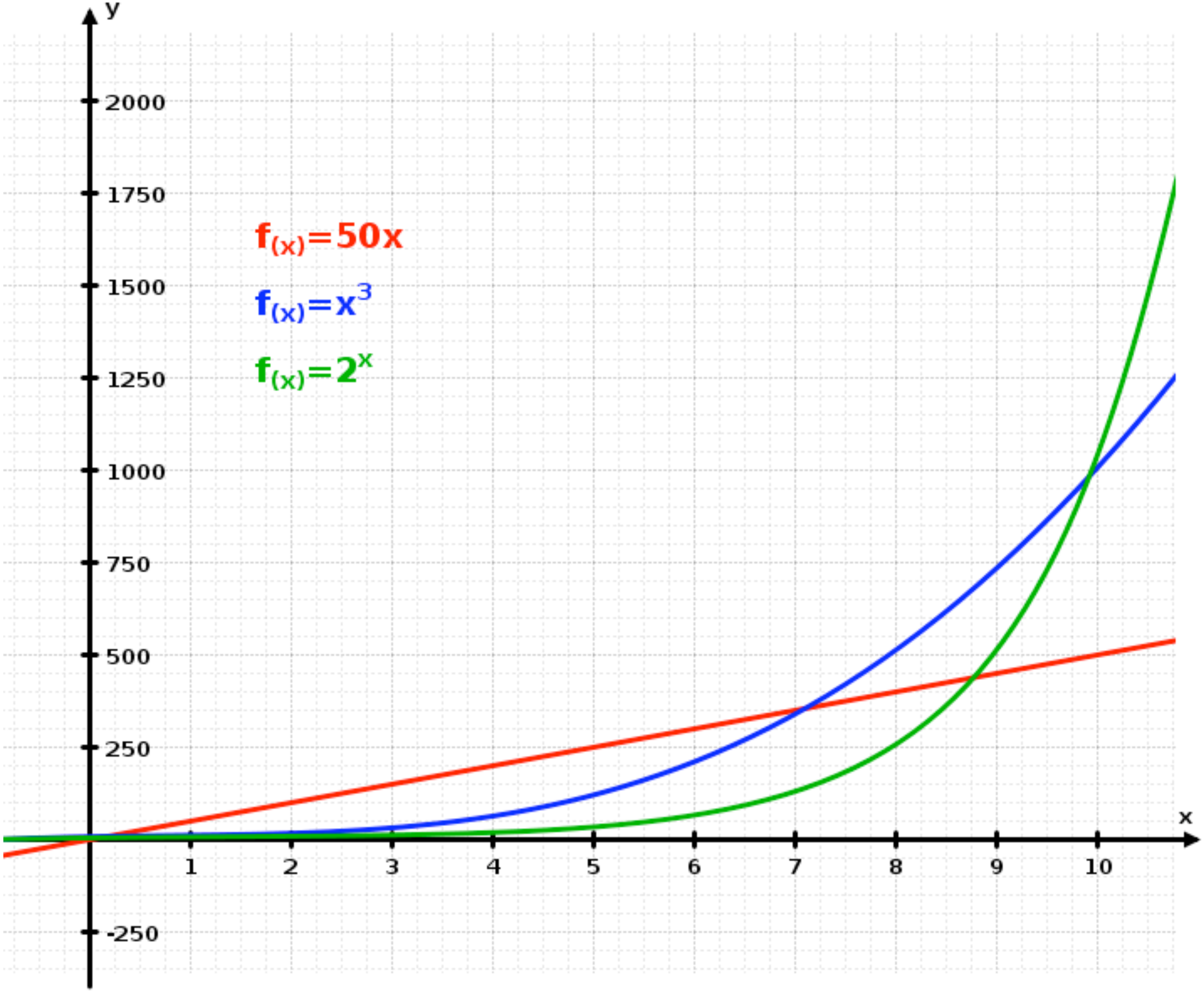
שיטחו 500,000,000 קמ"ר שטח מדינת ישראל 20,000

הינו האורז ישקול בערך כמשקל מדינת ישראל (פרוסה הממשיכה עד מרכז כדור הארץ)

אם נניח שלכל אחד מאיתנו 40 חברים. ב-6 דרגות של חברים לחברים נכסה את כל אוכלוסית העולם $40^6 \sim 4,000,000,000$

מה בכל זאת לא נכון בחישוב הנ"ל?

נביט בהתנהגות פונקציות– ליניארית, x^3 וחזקת x – מי עולה מהר יותר? (תלוי באיזה תחום)

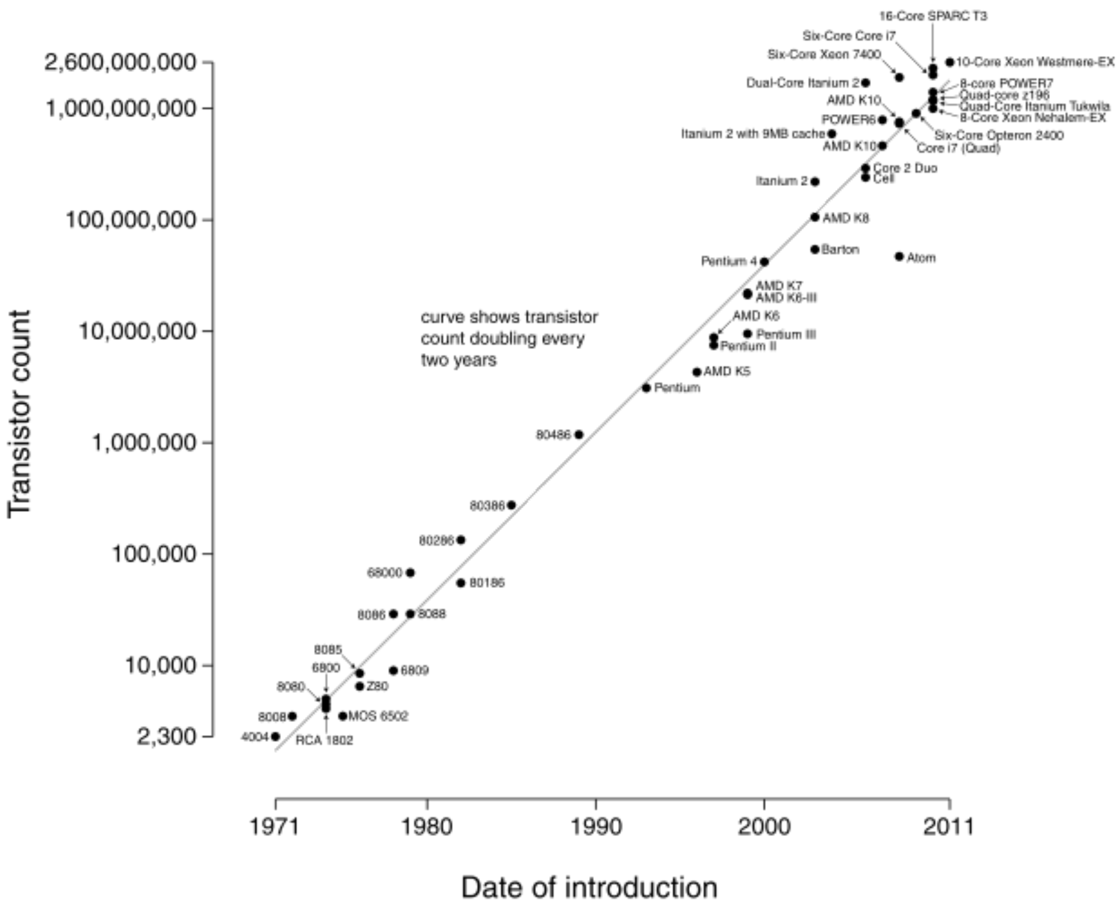


חוק מור Gordon Moore מנבא שמעבדי מחשב מכפילים את מהירותם כל 18 חדשים – זה תקף מזה 40 שנים. **מה המגבלות למהירות מחשבים (טכניות ועקרוניות)?**

מהירות העברת סיגנאל ← הקטנת המעבד
סילוק אנרגיה הנבלעת וגורמת לחימום ← קירור אפקטיבי
אלגוריטמים של חישוב מקבילי בכמה מעבדים ← לא מתאים לכל חישוב
מעבדים מהירים מיוחדים המיועדים לפעולות מסויימות ← מעבד גראפי

מחשבים קוונטיים - העברת אינפורמציה מיידית. (ראה בפרק על מכאניקה קוונטית במאה הדיגיטאלית)

Microprocessor Transistor Counts 1971-2011 & Moore's Law



קיבול האיכסון הדיגיטאלי עולה גם הוא אכספוננציאלית

מה המגבלות?

נפח לאיכסון ביט בודד -> אופטי – גודל נקודת המיקוד ללייזר.

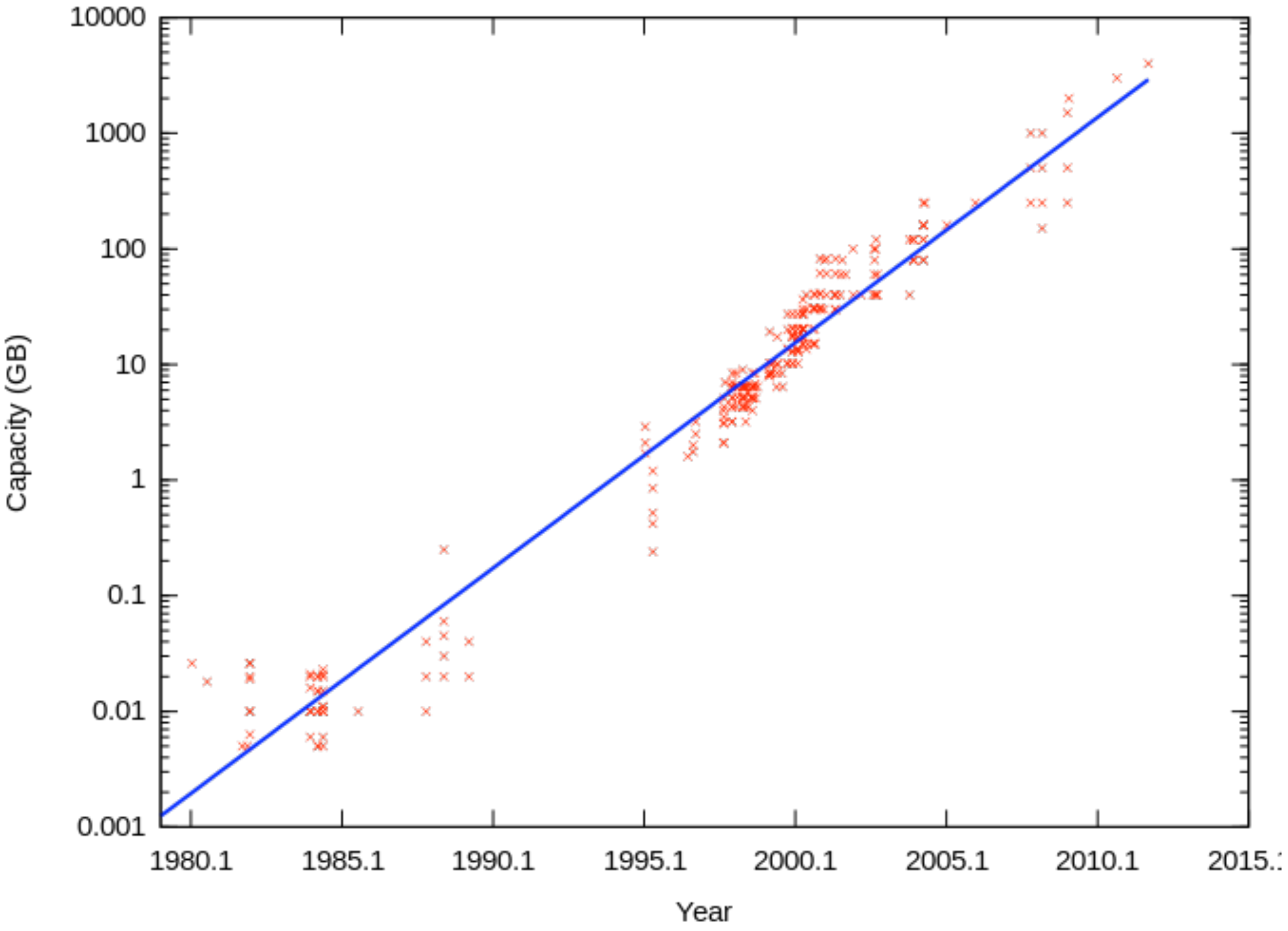
מגנטי – גודל מגנט: עקרונית יכול להיות אטום בודד

גודל (רזולוציה) של הראש הקורא – מוקד ליזר או סליל לקריאת מגנטיות

מהירות הכתיבה והקריאה –

מהירות סיבוב הדיסק – הזמן הנדרש לקרוא ביט או לכתוב ביט (לרוב איטי יותר בכתיבה)

הזמן הנדרש לייצוב הראש קרוב לדיסק אך בלי לשרוט אותו



e

e = 2.718281828...

במקום לערוך טבלאות של כל החזקות לכל המספרים – טבלאות לוגריטמיות ln(x),
ולכל מספר y אחר: $x^y = e^{\ln(x)*y}$ ומשתמשים בטבלא הפוך (אנטילוג) מ- ln(x)*y

ברנולי 1655-1705 **Jacob Bernoulli** השויצרי בדק כמה ריבית יקבל מהבנק אם הריבית השנתית היא 100%. אם הריבית תחושב בסוף שנה יקבל עבור כל פרנק עוד פרנק אחד. אם הריבית תחושב פעמיים בשנה כעבור חצי שנה ייתוסף 50% לקרן סה"כ 1.5 פרנק, ובסוף השנה שוב 50% על 1.5 פרנקים – הינו $1.5^2 = 2.25$ פרנקים. אם ארבע פעמים בשנה $1.25^4 =$ 2.44140625 כל חדש: 2.613035
באופן כללי – אם ריבית מחושבת n פעמים בשנה הסכום שיקבל על כל פרנק הוא $(1+1/n)^n$

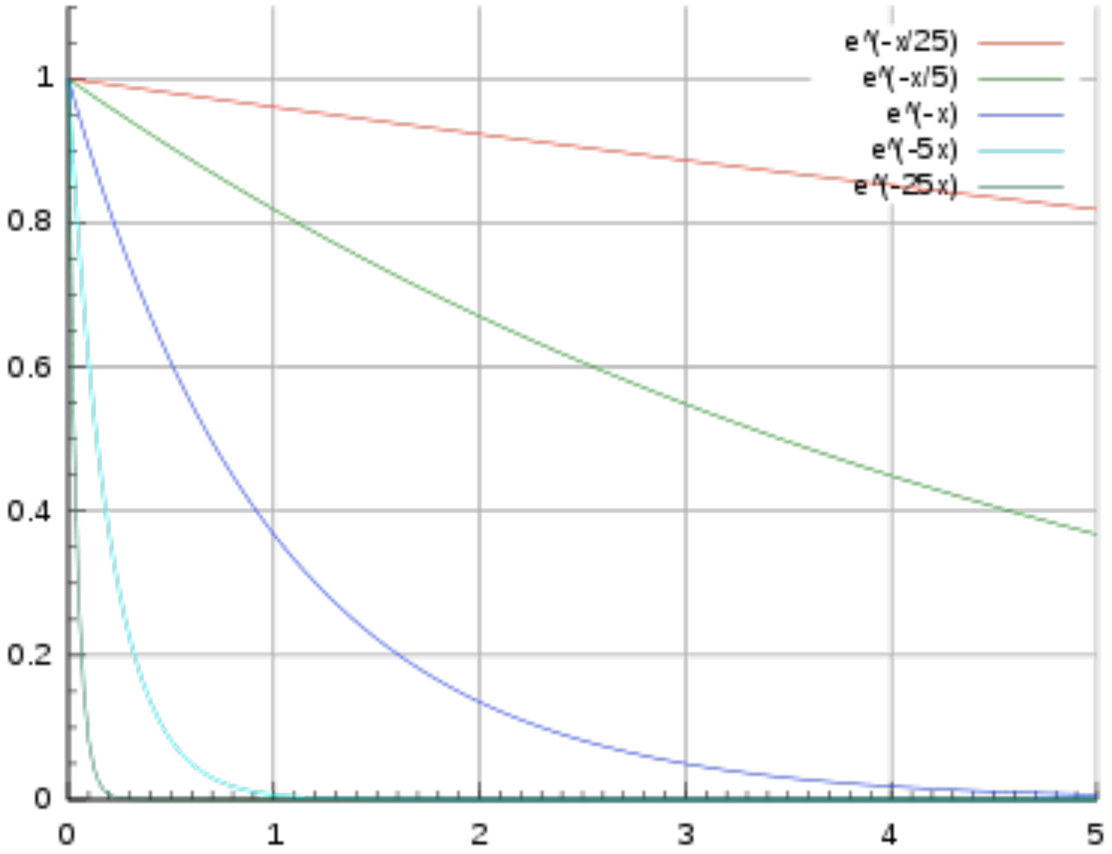
ואם הריבית מחושבת באופן רצוף – $n \to \infty$ נקבל פי e פרנקים, לפי $e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$

או, בריבית דריבית R המחושבת רצוף ל- t שנים נקבל eRt פרנקים.

בעיה אחרת: כוס מלאה במים צבועים. נוציא מהכוס בצינור זרם קבוע של מים צבועים, ונכניס זרם מים צלולים בקצב זהה – מה יהיה ריכוז הצבע בכוס: $e^{-T/t}$

בגלל ש-e מופיע "טיבעית" בתהליכים עם התנהגות מכפלתית הלוגריטם על בסיס e נקרא "לוגריטם טיבעי"

עקומות דומות מקבלים בדעיכה רדיואקטיבית, בה בכל רגע מספר ההתפרקויות יחסי למספר האטומים הרדיואקטיביים שנשארו



גם רלוונטי לסיכוי לזכות במפעל הפיס: אם הסיכוי לזכות בכל פעם הוא 1/n ומשחקים n פעמים, עבור n גדול הסיכוי לא לזכות אף פעם הוא 1/e

$$\frac{1}{e} = \lim_{n\to\infty} \left(1 - \frac{1}{n}\right)^n .$$

ה סיכוי לזכות k פעמים מתוך n הוא בינומיאלי: $\binom{n}{k}(1/n)^k(1-1/n)^{(n-k)}$

כאשר n על k מוגדר כ- $\binom{n}{k}=n!/(k!(n-k)!)$

אם n אורחים עם מספרים (1 ... n) תולים את כובעם על n קולבים הממוספרים באופן אקראי, מה הסיכוי שאף אורח לא ימצא את כובעו על מספר הקולב הנכון:

$$p_n = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!} = \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

ועבור n גדול ערך זה שואף ל $1/e$

e גם מופיע בנוסחות אסימפטוטיות - כגון נוסחת שטרלינג Stirling

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

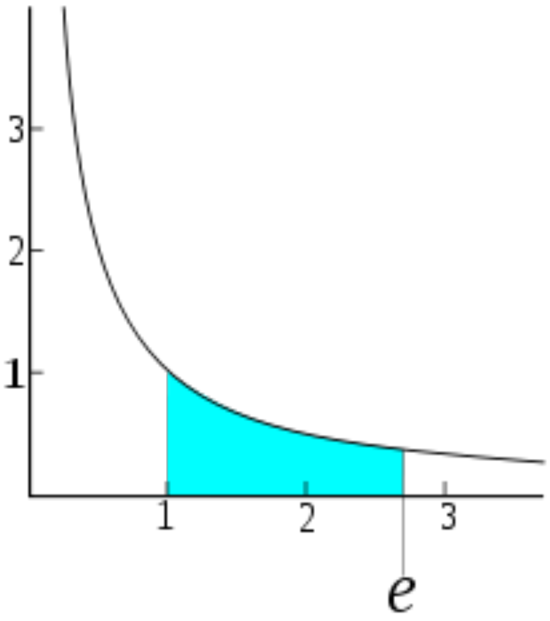
וכן

$$e = \lim_{n\to\infty} \frac{n}{\sqrt[n]{n!}}$$

תכונות ייחודית

$$\frac{d}{dx}e^x = e^x.$$

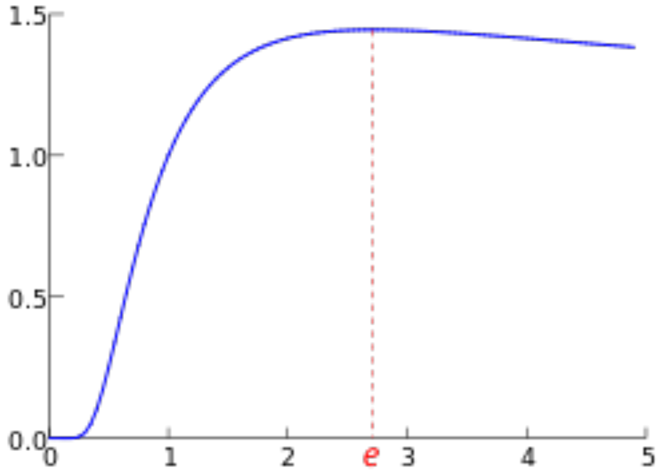
$$\frac{d}{dx}\log_e x = \frac{1}{x}.$$



$$\int_1^e \frac{1}{t}\,dt = 1.$$

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \cdots$$



$f(x) = \sqrt[x]{x}$ המכסימום של הפונקציה
הוא ב– x=e

$f(x) = x^x$ המינימום של הפונקציה
הוא ב– x=1/e

הסתברות וקומבינטוריקה

המדע מנסה לתאר את תופעות הטבע באמצעות חוקים דטרמיניסטים. למשל במסגרת המכאניקה הקלאסית: אם תיתנו לי את מיקומם ומהירויותיהם של כל האטומים ביקום אוכל לנבא את העתיד...

התנהגות הסתברותית קיימת בבסיס מכאניקת הקוואנטים עקב חוק אי הוודאות של הייזנברג, הקובע שלא ניתן לדעת בו זמנית את המיקום והמומנטום המדוייק של חלקיקים. הקושי לקבל אי וודאות כזו בטבע גרם להתנגדות רחבה לתורת הקוונטים (איינשטיין אמר: "אלוהים לא משחק בקוביה")

קדם לתורת הקוונטים הניגוד בין דטרמיניזם בחוקי המכאניקה הקלאסית והתנהגות הסתברותית של גאזים הנובעת מחוקי הטרמודינאמיקה (למשל עליה באנטרופיה), ניגוד זה העסיק את המדענים במאה ה-19 והיה נושא לוויכוחים מרים.

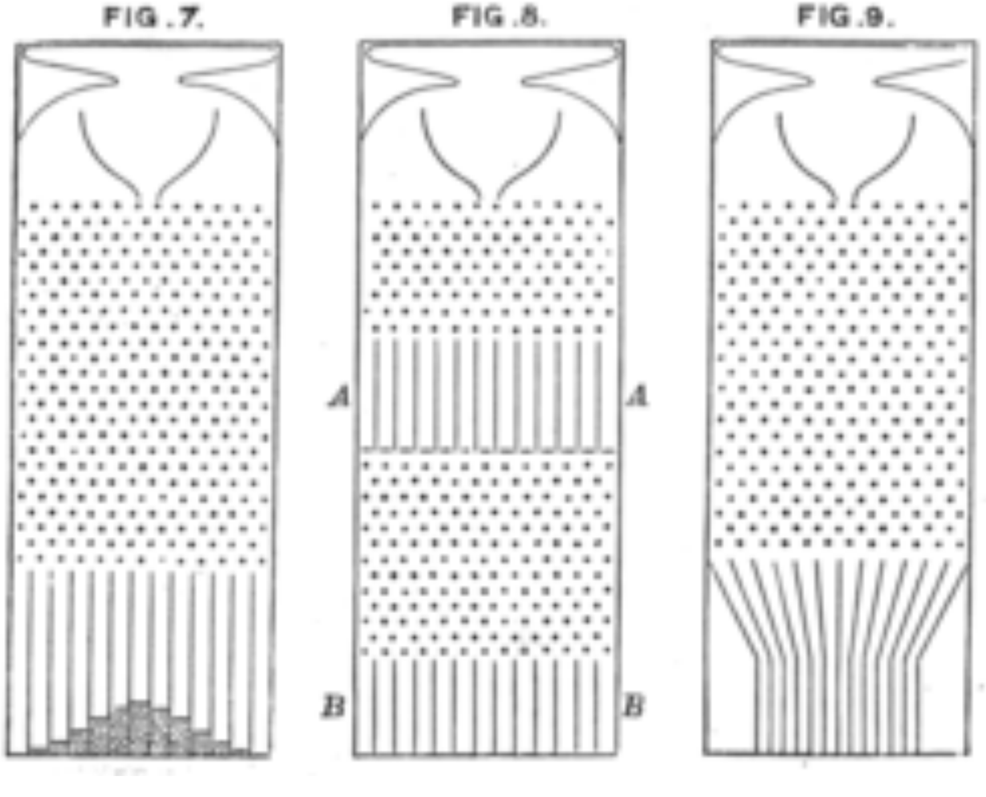
למרות שהביסוס המתמטי של תורת ההסתברות נעשה במאה ה-19, המושגים הרלוונטיים טופלו מוקדם בהרבה. חישוב סיכויי זכיה במשחקי קלפים, קוביה ומשחקי מזל אחרים, הבנת הקשר בין מספר האפשרויות השונות לקבל אותו מצב והסיכוי לראות מצב כזה (קומבינטוריקה), כל אלה הן בעיות שהוצגו ונפתרו מאז ומתמיד, ונשמרו בכתבים אשוריים ומצריים, סיניים, ערביים ומימי הביניים.

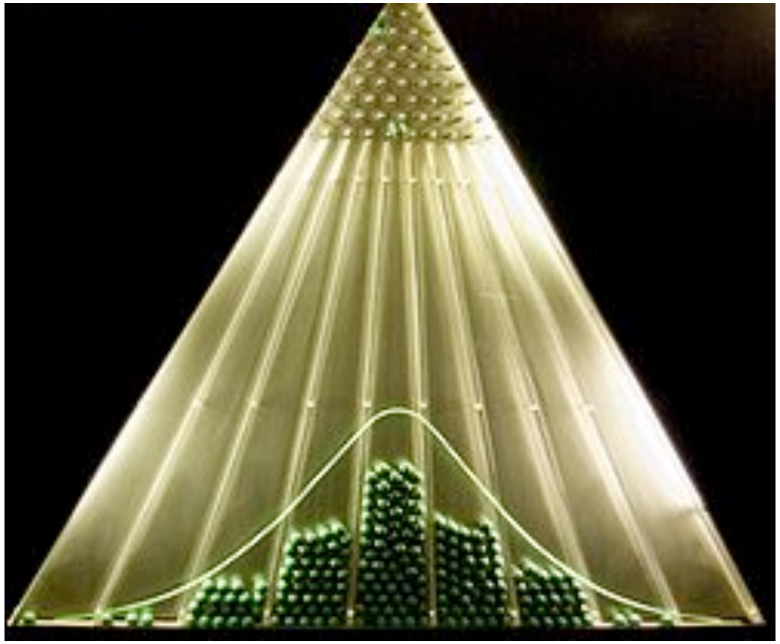
מעניין לציין שלתורת ההסתברות מסקנות לא אינטואיטיביות: למשל שסיכוי הגכיה בפיס בכל הגרלה קבוע, ואינו תלוי באם זכית בהגרלות קודמות. או שהאסטרטגיה הטובה ביותר להמר כשביידך סכום קבוע היא להמר על כל הסכום בהימור אחד, ולא לפצלו בין מספר הימורים רב.

מספרים אקראיים

$$f(x;\mu,\sigma^2)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^2}$$

זריקת כדורים דרך "שדה" מסמרים – התפלגות גאוסית
סכום (אינטגראל) ההסתברויות = 1
ממוצע ההתפלגות = μ
רוחב ההתפלגות = σ



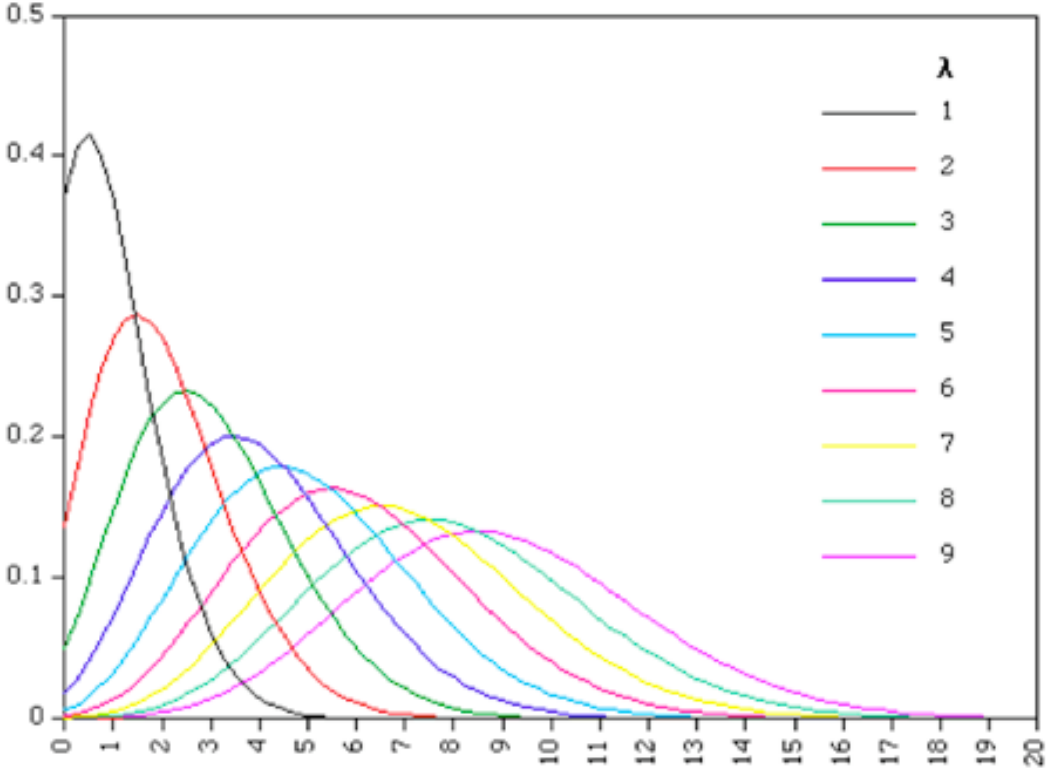


התפלגויות בינאריות, ופואסוניות לתהליכים בדידים (לא רצופים)

משפט הגבול המרכזי (central limit theorem) אומר שבמספרים גדולים
כל ההסתברויות שואפות לפילוג נורמאלי (גאוסיאניות)

$$f(k;\lambda) = \Pr(X = k) = \frac{\lambda^k e^{-\lambda}}{k!},$$

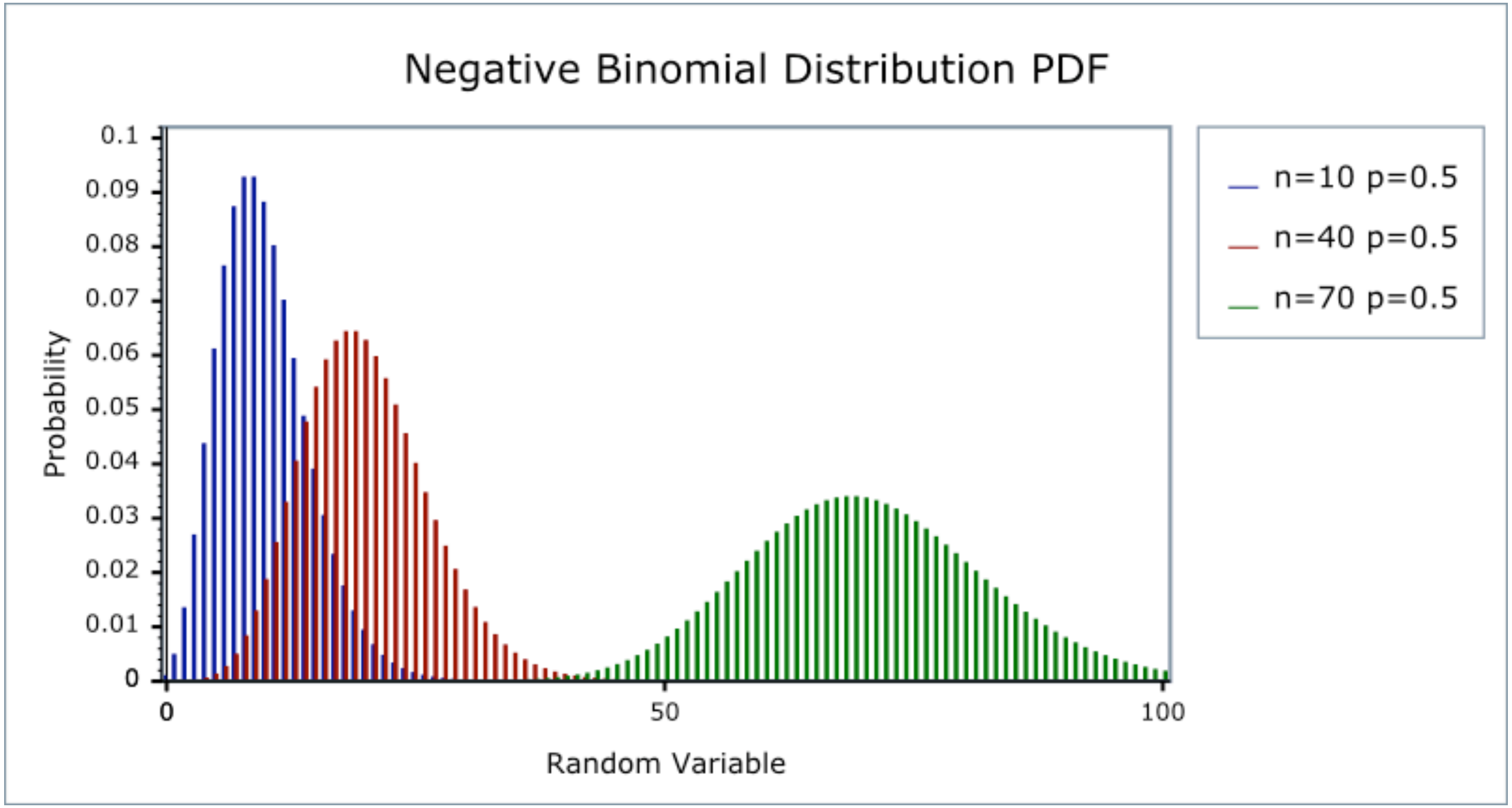
Poisson PMF with 1 <= λ <= 9



$$P(x,p,n) = \binom{n}{x} (p)^x (1-p)^{(n-x)} \quad \text{for } x = 0, 1, 2, \cdots, n$$

$$\binom{n}{x} = \frac{n!}{x!(n-x)!}$$

#


Negative Binomial Distribution PDF
Probability
0.1
0.09
0.08
0.07
0.06
0.05
0.04
0.03
0.02
0.01
0
0
50
100
Random Variable
n=10 p=0.5
n=40 p=0.5
n=70 p=0.5

מה הסיכוי לעץ או למספר בזריקת מטבע – אם 30 תלמידים יזרקו כל אחד 100 פעמים ונרשום כמה פעמים התקבלו עץ לכולם – נקבל התפלגות סביב 50.

כמה פעמים צריך לערבב 52 קלפים כדי שלא יהיה זכר לסדר הראשוני שלהם
הראו שצריך לפחות 7 פעמים
פחות מ-7: נשאר "זכרון" לסדר. יותר מ-7: אין רווח

מספר קווי תקשורת שיבטיחו ש-75% מהפעמים שתטלפן לכל מספר הקו יהיה פנוי
מספר ערוצי הרדיו שצריך כדי להבטיח תקשורת חירום לקראת הפלישה בנורמנדי
מעבדות Bell Telephone בניו ג'רסי הקימו קבוצה שחקרה בעיות של <u>אירועים אקראיים</u>

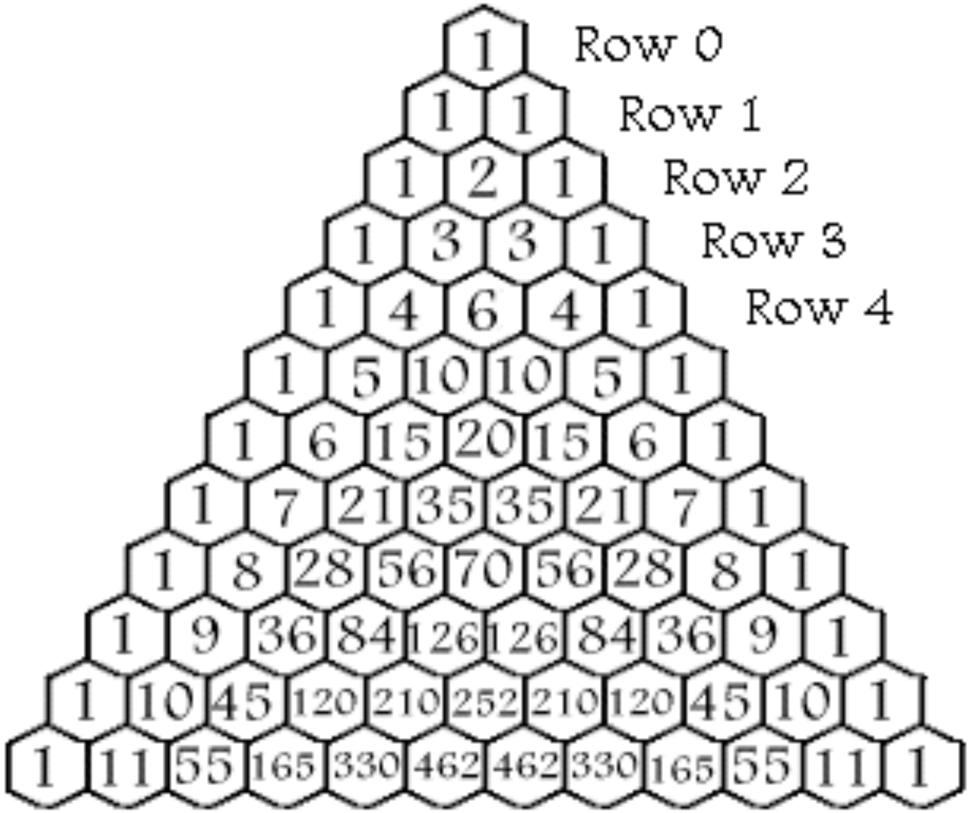
איינשטיין קישר את התנועה האקראית של אטומי המים לתנועה בראונית של חלקיקים במים

קומבינטוריקה

The Binomial Theorem can be stated as:

$$(a+b)^n = a^n + na^{n-1}b^1 + \frac{n(n-1)}{2}a^{n-2}b^2 + \dots + b^n$$

The co-efficients generated by expanding binomials of the form $(a+b)^n$ can be shown in the form of a symmetrical triangle:



הנוסחא $(a+b)^n = \sum_{i=0}^{i=n} \binom{n}{i} a^{n-i} b^i$

כאשר $\binom{n}{i} = n! / [i! * (n-i)!]$

אפשר לבנות את משולש המקדמים הבינאריים (משולש פסקל) באופן הדרגתי (רקורסיבי)

$$\binom{n+1}{i} = \binom{n}{i-1} + \binom{n}{i}$$

$$\frac{(n+1)\,n!}{i!\,(n+1-i)!} =V= \frac{n!}{(i-1)!(n-i+1} + \frac{n!}{i!(n-i)!} = \frac{n!\,(i+1+n-i)}{i!\,(n+1-i)!}$$

Muhammad Al_Karaji מוחמד אל_קרזי הוכחה באינדוקציה של הנוסחא הבינארית

$(a+b)^1 = a + b$

$(a+b)^n = \Sigma \binom{n}{k} a^k b^{(n-k)}$ $[k=0 .. n]$ נניח

$(a+b)^{n+1} = \Sigma \binom{n+1}{k} a^k b^{(n+1-k)}$ $[k=0 .. n+1]$ נוכיח

$(a+b)^{n+1} =(a+b) (a+b)^{n+1} =(a+b) \Sigma \binom{n}{k} a^k b^{(n-k)} =$

$\Sigma \binom{n}{k} a^{k+1} b^{(n-k)} + \Sigma \binom{n}{k} a^k b^{(n-k+1)} =v= \Sigma \binom{n+1}{k} a^k b^{(n+1-k)}$

$\Sigma \binom{n}{i-1} a^i b^{(n-i+1)}_{[i=1 ... n+1]} + \Sigma \binom{n}{k} a^k b^{(n-k+1)}_{[k=0 .. n]} =v= \Sigma \binom{n+1}{k} a^k b^{(n+1-k)}$

$\Sigma \binom{n}{k-1} a^k b^{(n-k+1)}_{[k=1 ... n]} + \Sigma \binom{n}{k} a^k b^{(n-k+1)}_{[k=1 .. N} =v= \Sigma \binom{n+1}{k} a^k b^{(n+1-k)}] + \binom{n}{n} a^{n+1} + \binom{n}{0} b^{n+1}$

$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$

$n!/(k-1)!/(n-k+1)! + n!/k!/(n-k)!=(n+1)!/k!/(n-k+1)!$

$1/(n-k+1) + 1/k = (n+1)/k/(n-k+1)$

הגדרות

n-עצרת $n! = n*(n-1)* \ldots 2*1$

n על k $\binom{n}{k} = n! / [k!(n-k)!] = n*(n-1)* \ldots *(n-k+1)/[k*(k-1)* \ldots *2*1]$

בכמה דרכים ניתן לסדר קבוצה של 4 ילדים בשורה $24 = 1*2*3*4 = 4!$

כמה מילים יש עם 4 אותיות לא חוזרות $21*22*23*24$

כמה מספרים בני 4 ספרות (חוזרות) $10*10*10*10$

בכמה דרכים ניתן לבחור קבוצת כדורגל (11 שחקנים) בכיתה של 30 ילדים $\binom{30}{11}$

קשר בין המקדמים הבינאריים לקומבינטוריקה –

מספר האפנים שניתן לקבץ מתוך n מכפילים

$(a+b)*(a+b)*(a+b)\ .....\ *(a+b)$

בעיות קומבינטוריות

בכמה אופנים ניתן לסדר 10 ילדים בשורה
בכמה אופנים ניתן לסדר 10 ילדים סביב שולחן עגול
בכמה אופנים ניתן לסדר 5 בנים ו–5 בנות בשורה כך שתמיד בן יהיה בין 2 בנות ולהפך
כנ"ל אבל סביב שולחן עגול
מה הסיכוי לזכות בפיס אם מפעל הפיס הדפיס 1,000,000 כרטיסים ומהם ניקנו 500,000

לוגיקה

נושאים בלוגיקה מתמטית

A=true B=true AÇB=? AUB=?

A=true !A=?

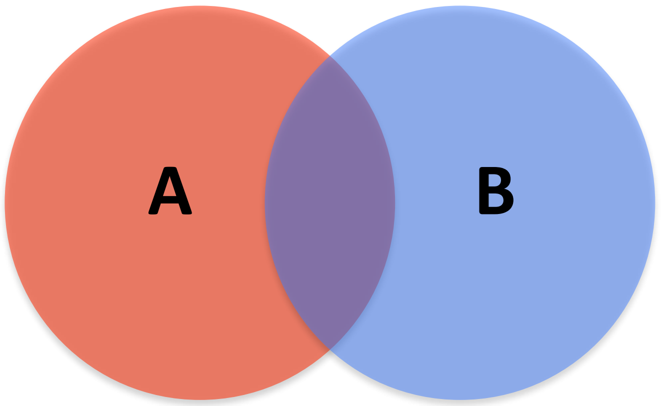
A=true B=false AÇB=? AUB=?

A=true !A=false (A and only A is true)

A>0 B>0 f(A,B) ?

Truth table ##################

De Morgan's law ###########

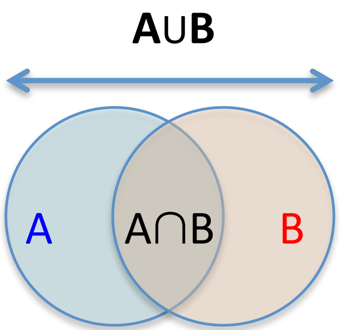


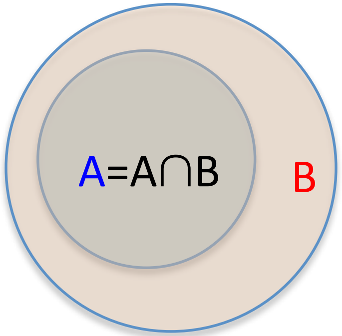
הוכחת משפט מתמטי מתבססת על כללי מחשבה – לוגיקה

שני מרחבי אפשרויות A,B שמקבלים רק שני ערכים – נכון-True ולא נכון-False

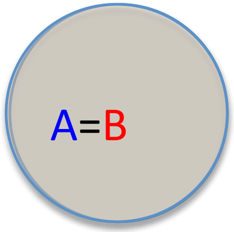
כל האפשרויות AUB A.or.B (איחוד, union), והמשותף (החיתוך) A.and.B

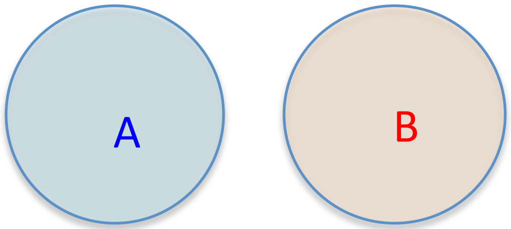
לא בהכרח – אם B אז A





אם ורק אם A אז B גורר בהכרח – אם B אז A ולכן A=B





אם A אז לא B

הלוגיקה מרחיבה את התחום לו הגדרנו כללים

מספרים שלמים   שברים   מספרים שאינם יכולים להתבטא כשברים – מספרים אירציונאליים
מספרים שליליים   מספרים מדומים

משפט גודל (Gödel   1906-1976)

טוען שבכל מערכת הנחות (אכסיומות) עיקבית יש חוק שהוא נכון אך לא ניתן להוכחה במסגרת המערכת הקיימת. מעין אפשרות להרחיב כל תורה מתמטית.
חוק זה גרם לזעזוע במתמטיקה, מאחר ועירער את השאיפה האוקלידית לבסס שטח מתמטי מושלם על אקסיומות.

פרמה ומספרים

תורת המספרים

המשחקים במספרים השלמים ותכונותיהם משכו מתמטיקאים מקדמת דנא מאחר והם גילו כי השאלות שצצות כמעט מעצמן ונראות מובנות וברורות אינן קלות לפתרון.

<u>קבוצת המספרים</u> היא אינסופית: מושג לא טיבעי לתפיסה ותכונותיו אינן אינטואיטיביות (כגון אותו מספר מספרים ומספרים זוגיים.)
<u>קבוצת המספרים הראשוניים</u> או <u>הריבועים השלמים</u> הציגו שאלות לא פתירות.

הבעיות של תורת המספרים נראו בעיות אקדמיות וללא השלכות מעשיות, עד למאה ה-20.
השימוש המתרחב בהצגות מספריות בעולם הדיגיטאלי ובתקשורת מצא שימושים מעניינים לתורת המספרים (למשל להצפנה).

תורת המספרים – נושאים ללימוד

1. סדרות אריטמתיות (ליניאריות) $Ax+B$
2. חזקות (q^k) וסדרות גיאומטריות [ריבית דריבית, התרבות בקטריות]
3. סכומי סדרות
4. יחסי מספרים, גורמים משותפים, מספרים ראשוניים
5. אלגוריתמים לחלוקה, להוצאת שרש
6. אינדוקציה
7. אלגברה
8. בניות גיאומטריות והוכחות

תרגיל: מצא את המספר הראשוני הגדול ביותר הקטן מ- 10,000

משפטי פרמה בתורת המספרים: (1601-1665) Fermat-

כל מספר ראשוני מהצורה 4n+1 יכול להכתב באופן אחד כסכום שני ריבועים

כל מספר יכול להכתב כסכום ארבעה ריבועים

פרמה הוכיח הנחה סינית עתיקה: מספר n הוא ראשוני אם 2^n-2 מתחלק ב- n

אם ורק אם לא נכון, דוגמא: $2^{341}-2$ מתחלק ב- 341 אך 341=34*11 אינו ראשוני

פרמה הניח כי (1+2^(2^n הם מספרים ראשוניים, ובדק עד n=4

אכן ראשוניים, (2,3,5,17,257,65537)

אך אוילר הראה עבור 5 כי $2^{32}+1 = 4294967297$ מתחלק ב-641

הראה כי סכום היפוכי המספרים השלמים sum(1/n) גדל לאינסוף כמו log(n)

סכום היפוכי המספרים הראשוניים sum(1/p) גדל לאינסוף כמו log(log(p))

הניח (אדמאר הוכיח) כי צפיפות המספרים הראשוניים ליד p היא ~ log(1/p)

בעיות פתוחות:

האם יש מספר אינסופי של מספרים ראשוניים מהצורה n^2+1

האם יש מספר אינסופי של שני מספרים ראשוניים "צמודים" (בהפרש 2)

האם כל מספר איזוגי גדול מ–2 יכול להכתב כסכום שני ראשוניים [סברת Goldbach]

Goldbach's Conjecture

משפט פרמה –

עבור $n>2$ לא קיימים מספרים שלמים המקיימים $C^n = A^n+B^n$

היה סברה מאז דיאופנטוס ובמשך 350 שנים, והוכח ע"י ויילס ב–1995:

המשפט הקטן של פרמה: אם p ראשוני ו-a זר לו: a^p מתחלק ב-p עם שארית a
$a^p=a*mod(p)$
הוכחה ע"י השוואה של מערכות שאריות
נסתכל על קבוצת כל השאריות (מלבד 0) מודולו : p נכפיל את כל האיברים בקבוצה ב-a, ונקבל
נראה שגם ב-B מופיעות אותן שאריות, כמו ב-A: הקבוצה אינה כוללת 0 , מכיוון שכל המספרים הם מכפלות של שני מספרים זרים ל-p, שהוא ראשוני, ולכן גם המכפלה זרה ל-p מלבד זה, אין בקבוצה שני מספרים זהים (הוכחה: נניח בשלילה ש-
מאחר ש-a זר ל-p, ניתן לחלק בו את שני צידי המשוואה
מתקבל ש-
מה שמוביל לסתירה . כעת, מאחר ששתי הקבוצות זהות, גם מכפלת איבריהן שווה

ומאחר ש- הוא מכפלת מספרים זרים ל-p, הרי שגם הוא זר ל-p (למעשה הוא שווה ל-1- לפי משפט וילסון), ולכן ניתן לחלק בו את שני צידי המשוואה ולקבל את המשפט:
מכאן נובע שלכל a,

הוכחה באינדוקציה:

לכל $0 < k < p$ במקדם הבינומי $\frac{p!}{k!(p-k)!}$ המונה מתחלק ב-p והמכנה לא, ולכן המנה מתחלקת ב-p. מכאן שלכל a,b מתקיים

$$(a+b)^p = \sum_{k=0}^{p} \frac{p!}{k!\,(p-k)!} a^k b^{p-k} \equiv a^p + b^p \pmod p$$

בפרט, באינדוקציה על a

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$$

מענין: סכום הפכי המספרים השלמים מתבדר (ז"א גדול מכל מספר נתון) $\sum(1/n) \Rightarrow \infty$

אוילר הוכיח שסכום הפכי המספרים הראשוניים p_n מתבדר $\sum(1/p_n) \Rightarrow \infty$

לעומת זאת סכום הפכי הריבועים מתכנס -

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} = \sum_{i=1}^{n} \frac{1}{i^2}$$

האם אפשר להגיד שיש "יותר" ריבועים מראשוניים?

נראה בהמשך שקבוצת הריבועים שוה בגדלה לקבוצת כל השלמים !!!

זו ההתנהגות ה"מוזרה" של קבוצות אינסופיות

ברון Brun הוכיח שסכום כל זוגות הראשוניים הנפרדים ב-2 מתכנס

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots = \sum_{\substack{p \text{ prime},\\ p+2 \text{ prime}}} \left(\frac{1}{p}+\frac{1}{p+2}\right),$$

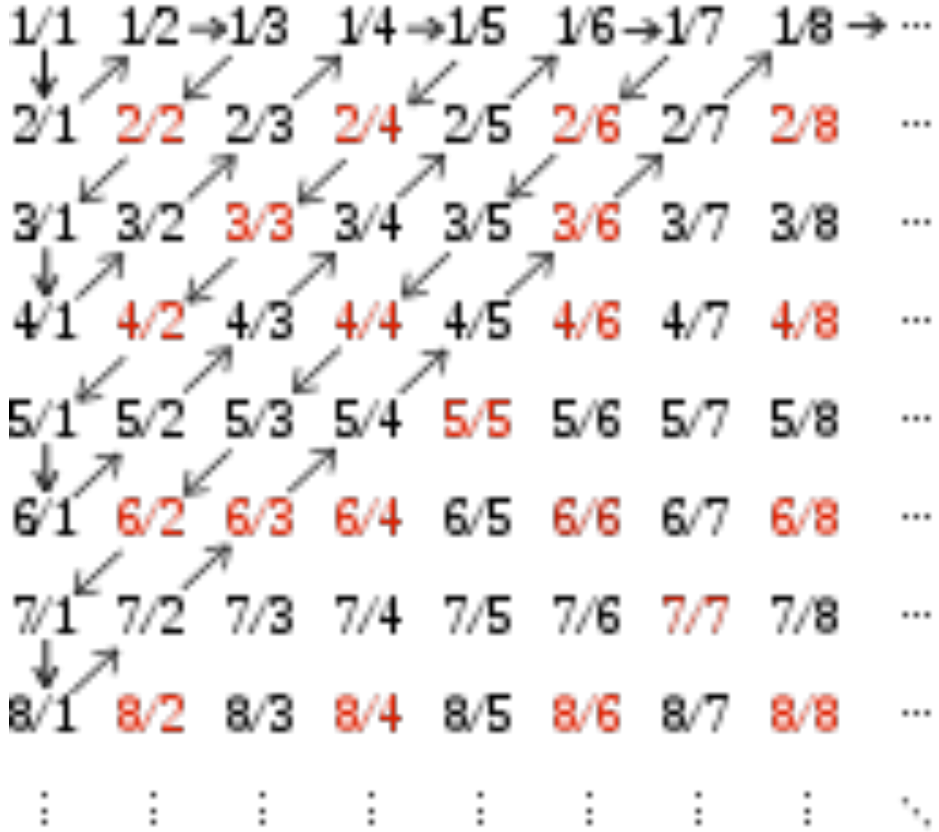
הראו שמספר המספרים הראשוניים עד n עולה כמו $n/\ln(n)$

קבוצות

<u>גיאורג קנטור (1845–1918) תורת הקבוצות</u>

$\aleph_0$ סימן לגודל קבוצה ספירה. למשל 1,2,3,4, ...

למרות שבין 1 ו- 2 יש אינסוף מספרים ראציונאליים ניתן לספור את כל המספרים הרציונאליים
נראה זאת בהוכחה "קונסטרוקטיבית" ע"י מיפוי כל מספר ראציונאלי למספר שלם.



לעומת זאת לא ניתן "לספור" את המספרים האירציונאליים. נוכיח על דרך השלילה בשיטת קנטור של אלמנטים אלכסוניים:

נניח שרשמנו וזיווגנו את כל אינסוף המספרים הממשיים בין 0 ל-1 למספרים השלמים. תחילת טבלת הזיווגים תיראה למשל כך

1 ↔ 0.112452...

2 ↔ 0.743212...

3 ↔ 0.213945...

4 ↔ 0.432912...

5 ↔ 0.394854...

...

אם ברשימה מספר ממשי עם מספר ספרות סופי אחרי הנקודה העשרונית נוסיף אינסוף אפסים. ניצור עכשיו מספר מהספרה הראשונה אחרי הנקודה השונה מהמספר הראשון ברשימה (אדום), הספרה השניה שונה מזו של המספר השני (ירוק) וכו למשל:

0.85863...

אנו בטוחים שמספר זה לא הופיע ברשימה: כי לכל מספר ברשימה יש לפחות ספרה אחת השונה מהספרה המתאימה במספר שיצרנו: הנה ההשואה לתחילת הטבלה:

0.11245...	0.74321...	0.21394...	0.43291...	0.39485...
0.85863...	0.85863...	0.85863...	0.85863...	0.85863...

זה נוגד את ההנחה שלנו, ולכן ההנחה אינה נכונה. המסקנה היא ש"חוזק" (cardinality) קבוצת המספרים הממשיים גדול מחזק קבוצת המספרים השלמים, ואינו ניתן לספירה.
קנטור הניח שאין קבוצה אינסופית שחוזקה הוא בין הקבוצה הספירה לקבוצת המספרים הממשיים (היפוטיזת הרצף) אך הנחה זו לא הוכחה עד היום.

c