ANCIENT AND CLASSIC WORLS

Until the 5-th Century

NUMBERS

Collected and edited by Prof. Zvi Kam,
Weizmann Institute, Israel

SCRIPTS

Types of Scripts

Hieroglyphs vs. Alphabetical: Pictographic vs. logographic

Consonants, Syllables. Vowels or added signs for vowels (e.g. Hebrew “punctuations”).

Text direction: right to left(Arabic, Hebrew, Aramaic),
left to right (Greek, Latin, English),
up to down (Chinese)

Letters shapes (squared, curved, uniform or variable thickness,
continuation between letters – English lower-case writing),
shape is reflecting the tools of scripting (pegs, chisels, tips, brushes)
and writing medium (clay, stone, papyrus, skins, paper).

Complexity of the scripts: Pictographic - elaborate pictures (Hieroglyphs, Maya scripting)
or letters: logographic - for fast scripting (Lower vs. Upper-case}.
complex: Specialized class of literate people, simple: widely-spread literacy.

Scripting Music

Encodes tone pitch (frequency), length (rhythm), atmosphere (sad, jolly).
Mono-sonic or polyphonic, harmonies, orchestration.

Dance

Scripting choreography: body and limbs gesture (smooth, rounded, vigorous)

Facial expressions (Shamans), finger formations (Indian, Tai).

Dynamics of movements: slow-fast, flowing-abrupt,

Numbers

Base (60-too many signs, 10-decimal, 2-binary)

Roman (I II V X C) vs. positional system (zero)

Integers, fraction (¼), powers (10^7), decimal point.

Development of writing scripts

4000th BC – peg script in Sumer

4000th BC – Egyptian Hieroglyphs

1500-100 BC – Hieroglyphs, brought from Crete: Linear A & B

1700 BC – Proto-Canaan script spread by the Phoenicians all over the Mediterranean. Synthesis of Egyptian and Babylonian scripts.
The source of Greek scripts: 1500 BC and Hebrew 1400 BC.

1200 BC Chinese script

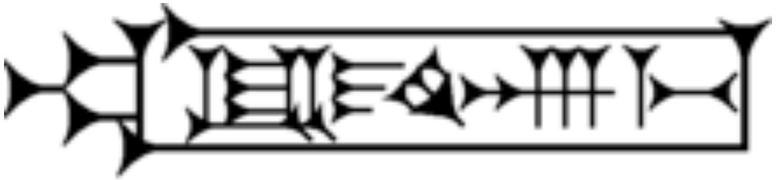
Center America Maya scripts developed independently.

Aztec used some pictorial script.

Inca is a unique culture with an empire that did not develop writing script.

Sumer – pegs script:

Writing by embedding pegs in soft clay.

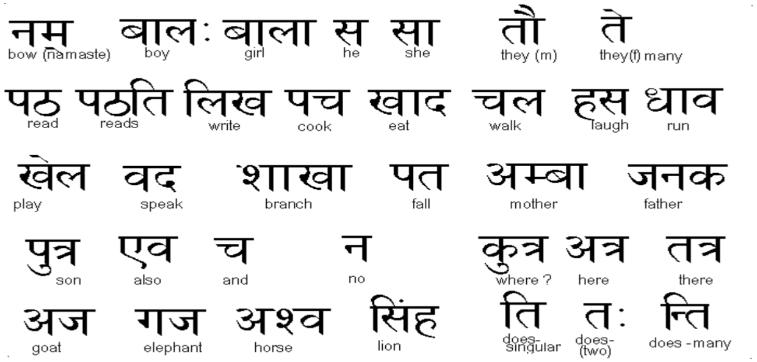


Greek: **αβγδηεκλμνυθψϕφωϖρστιοπζξχ**

Written with calamus on skins.

Latin: **ABCDEFGHIJKLMNOPQRSTUVWXYZ**

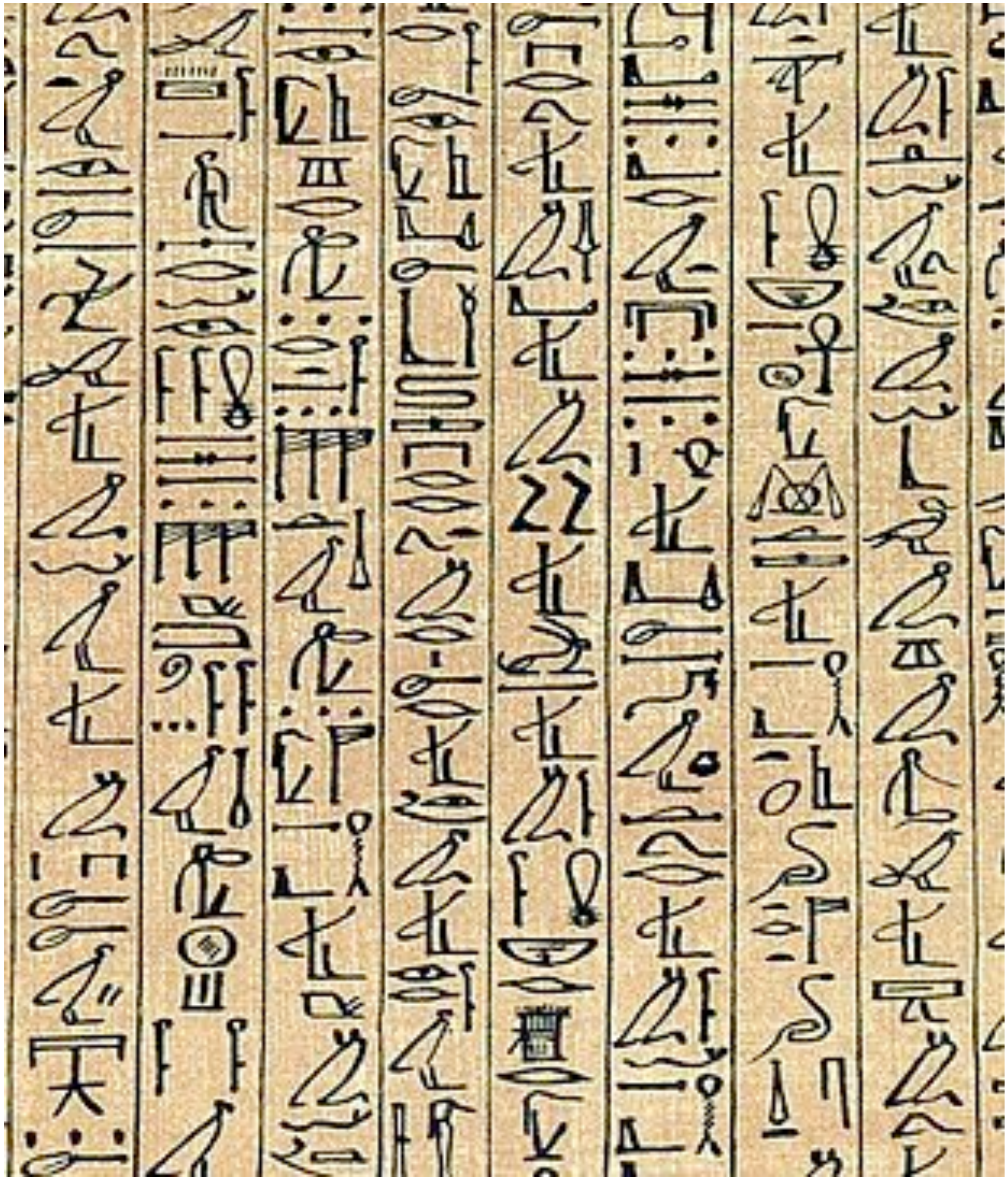
Sanskrit (India):



नम	bow (namaste)
बाल:	boy
बाला	girl
स	he
सा	she
तौ	they (m)
ते	they(f) many
पठ	read
पठति	reads
लिख	write
पच	cook
खाद	eat
चल	walk
हस	laugh
धाव	run
खेल	play
वद	speak
शाखा	branch
पत	fall
अम्बा	mother
जनक	father
पुत्र	son
एव	also
च	and
न	no
कुत्र	where ?
अत्र	here
तत्र	there
अज	goat
गज	elephant
अश्व	horse
सिंह	lion
ति	does-singular
त:	does-(two)
न्ति	does -many

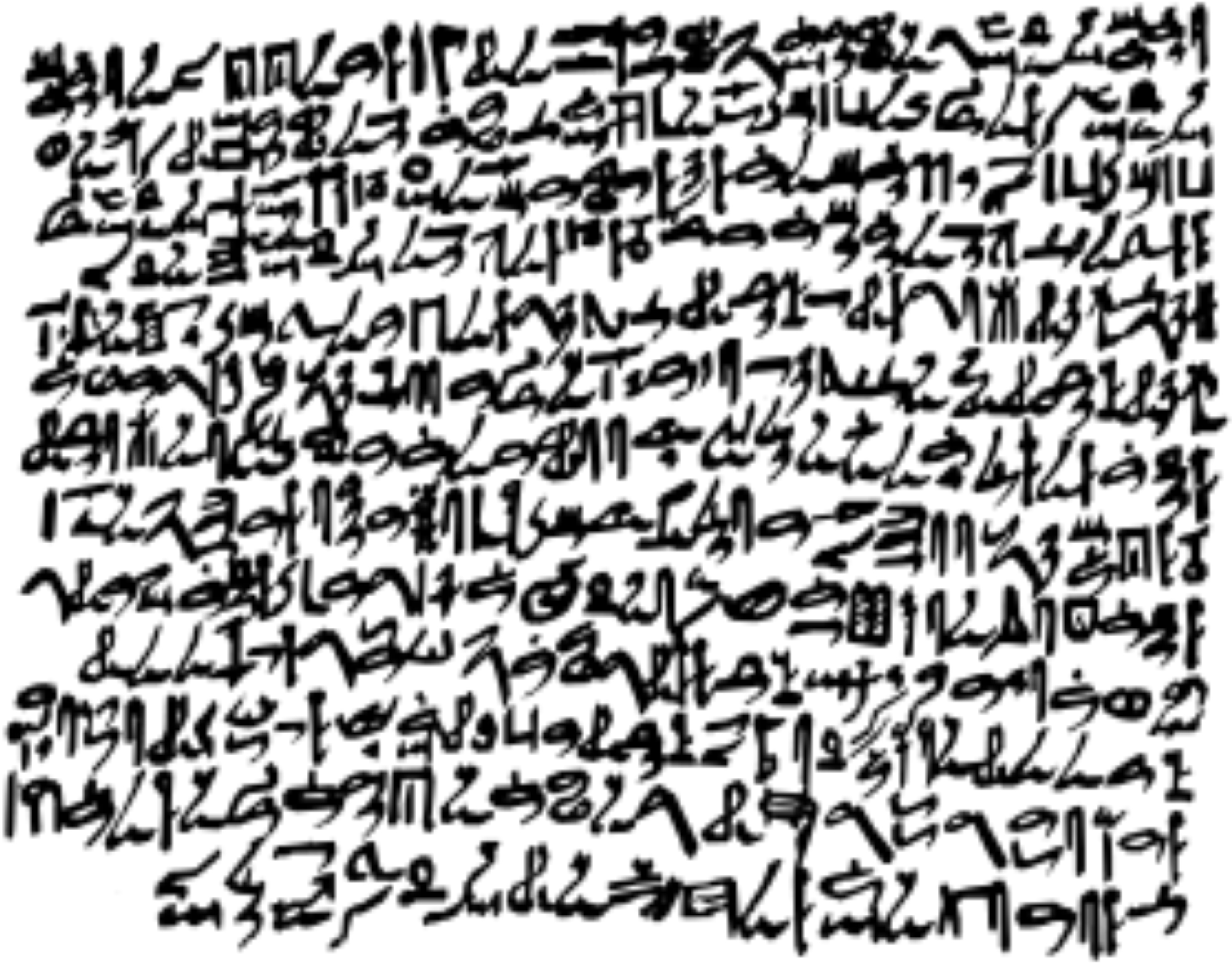
Egypt: Hieroglyphs

Scribed on lime stones and marble plates, Simplified for writing with tips on papyrus (demotic script)

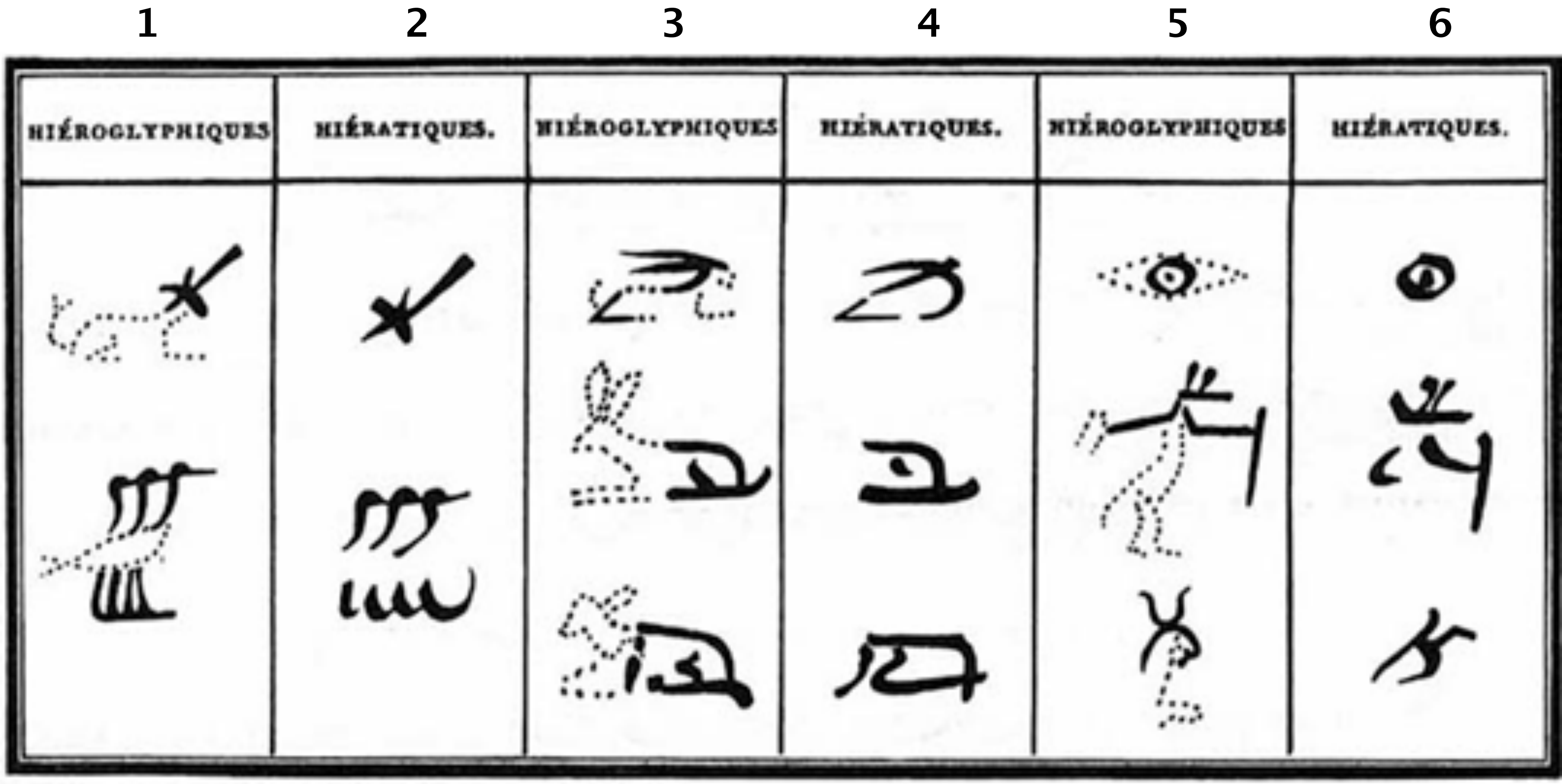


Egypt: Hieratic script

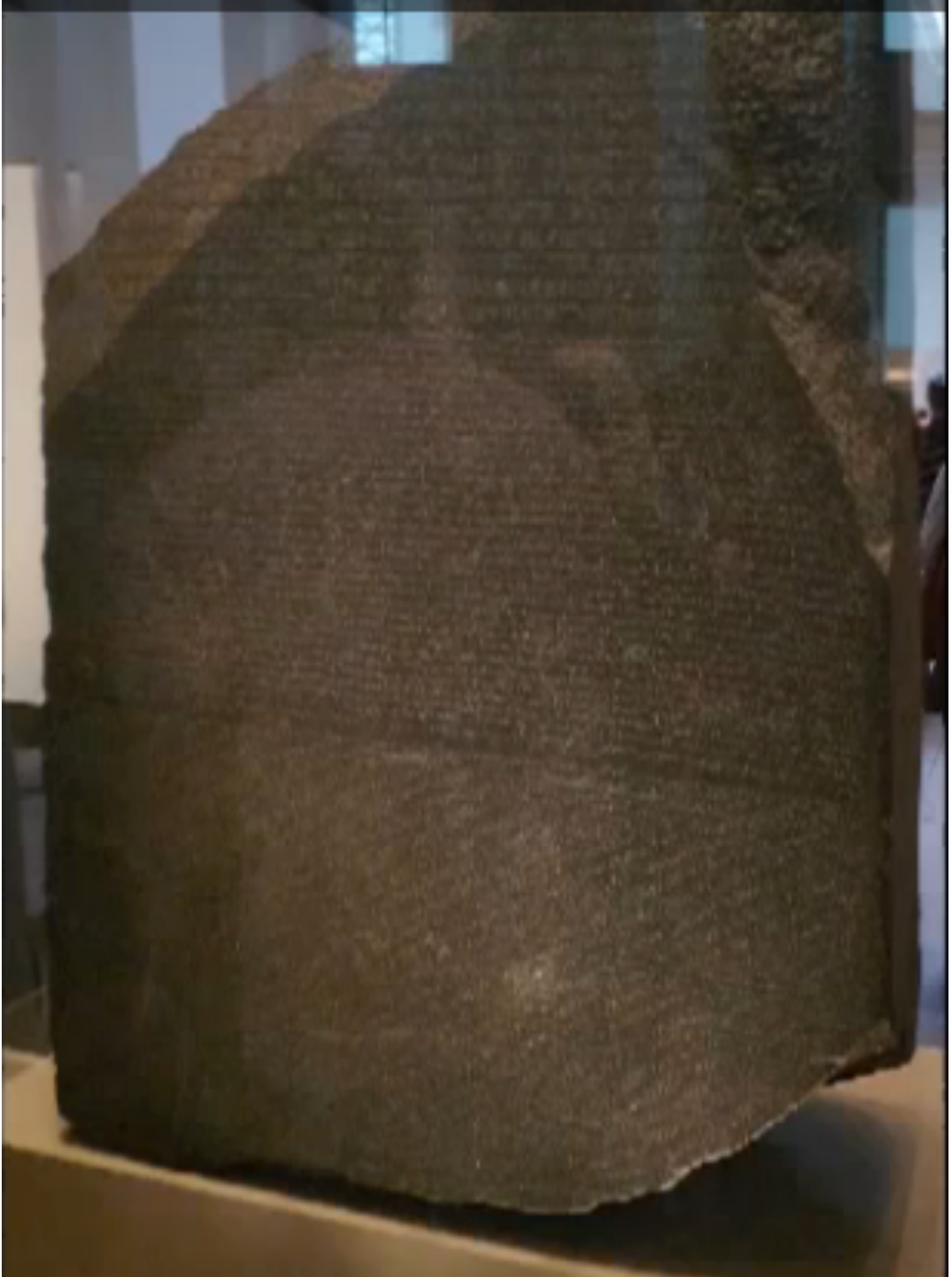
Similar to Hieroglyphs, but adapted simplicity for fast writing with ink on papyrus.



Comparison of Hieroglyphs (columns 1,3,5) to the Heratic script (2,4,6)



Alan Henderson Gardiner1879–1963 was the English expert who translated many important papyruses, as well as the Proto-Sinai script (based on key words such as god names). The use of letters to replace signs for words indicates Babylonian influence. Letters signs of this script originate from the first vowel of the hieroglyphic word.



The Rosetta stone:

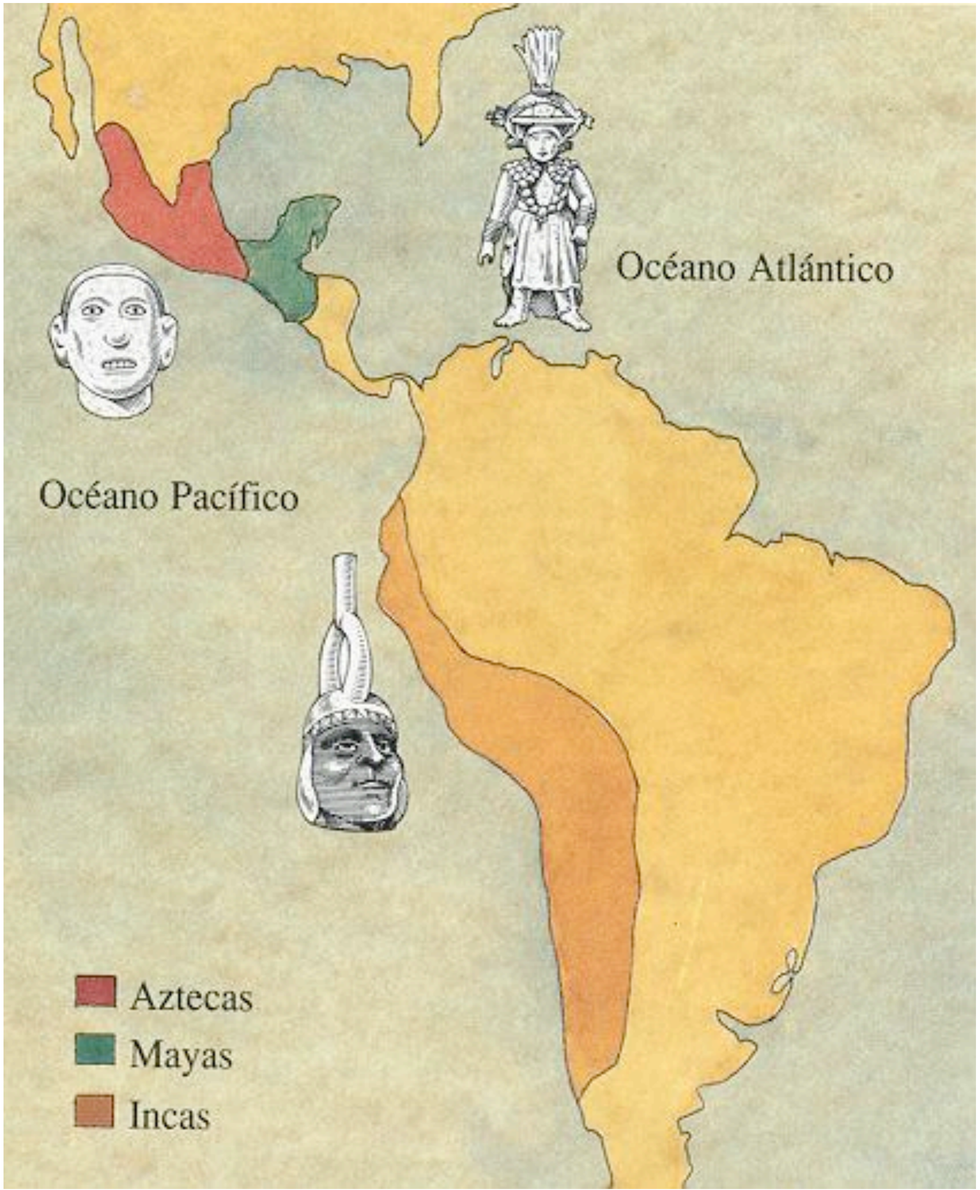
A granite stele written by the Ptolemy's in three scripts: Hieroglyphs, demotic script, and ancient Greek, which made it possible to interpret Egyptian Hieroglyphs by Champollion and Young.

Americas: Aztecs Maya & Inca

Maya- in Yucatan, Honduras, Guatemala: 2000-900 BC cities: Copan, Tikal,

Inca – in Peru: cities: Cusco, Machu-Picchu. No writing script.

Aztecs – in Mexico: some writing.

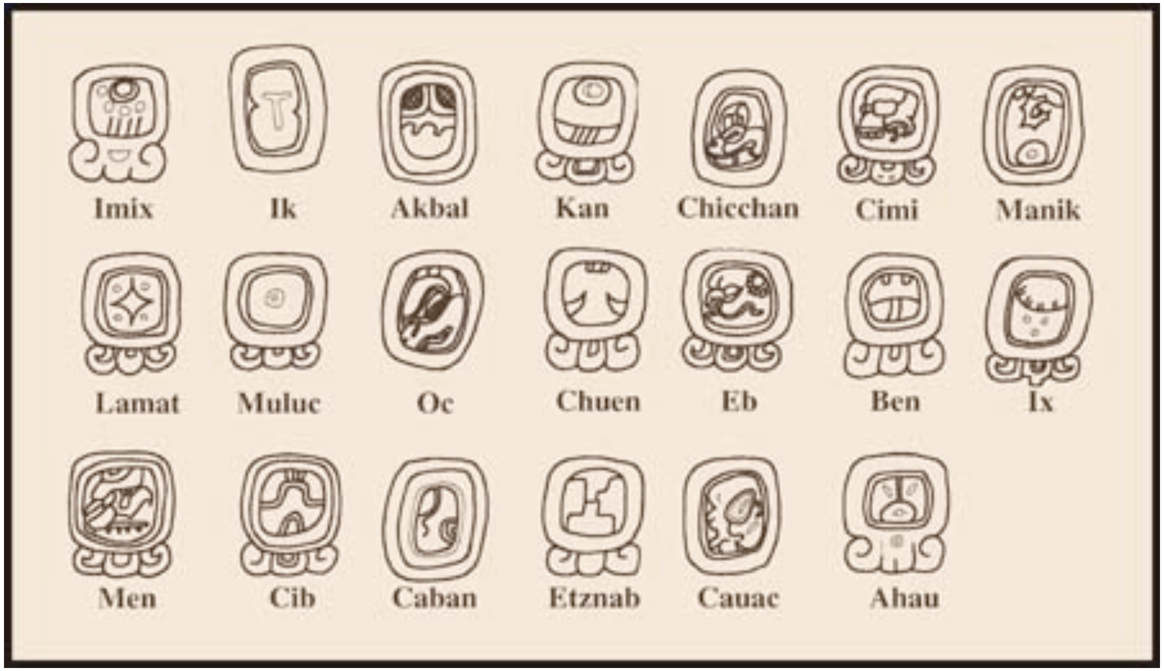


Maya script

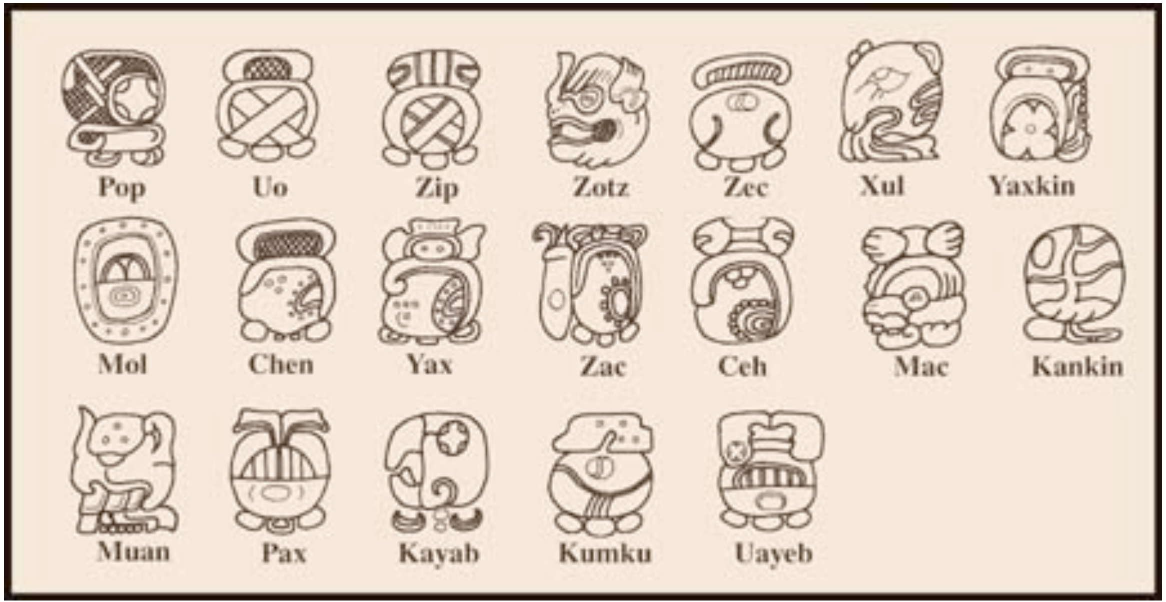
Important for governmental control on astronomy, religion and agriculture
Agricultural year: 20 days/month, 18 months+5 festive months/year 365 days/year
Religious year: 365.2420 days/year moon month=29.52 days
Agricultural and religious years met every 5 years.
Calendar count years since the creation of the world, date: 12 August 3113 BC

Maya script

Names of 20 days in a month

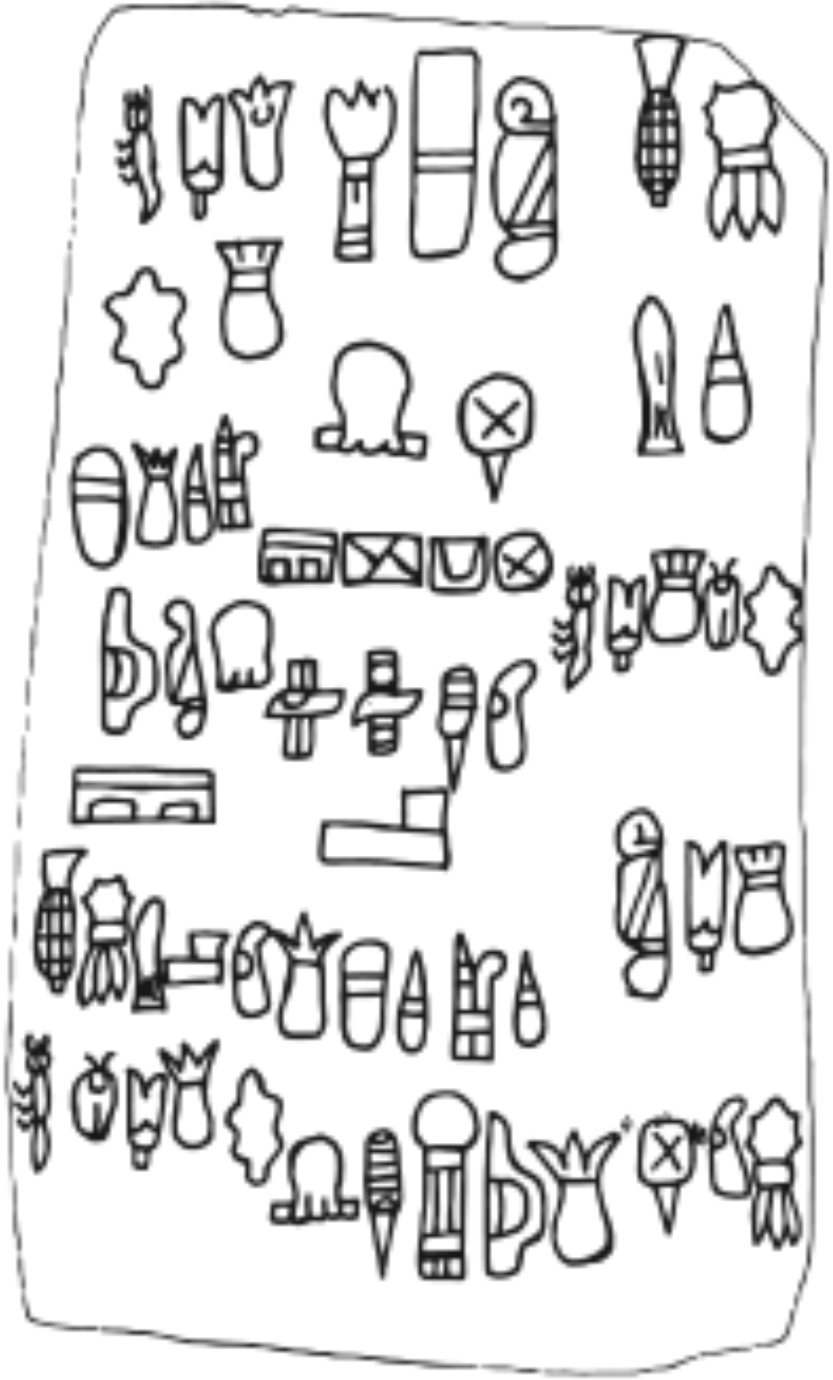


Names of 19 months per year



Aztec script

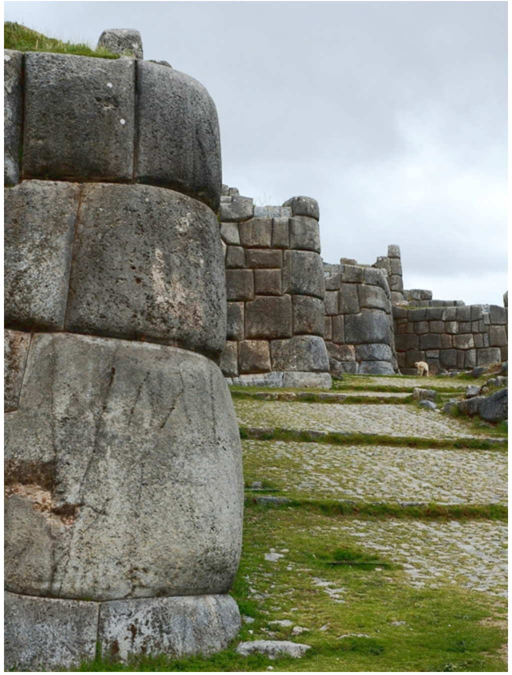
Cascajal block **900 BC**
Indicative of Aztec writing script



Inca – advanced culture with impressive constructions (Cusco, Machu-Picchu) possibly built by human slaves without animal chariots (not applicable in mountain paths).
It is told that the Spanish cavalry was seen as gods. Sun god, painting and sculptures.
Huge empire administered without iron or swards. Lack of scripts. Administrative accounting using Quipu – rope numbering system.

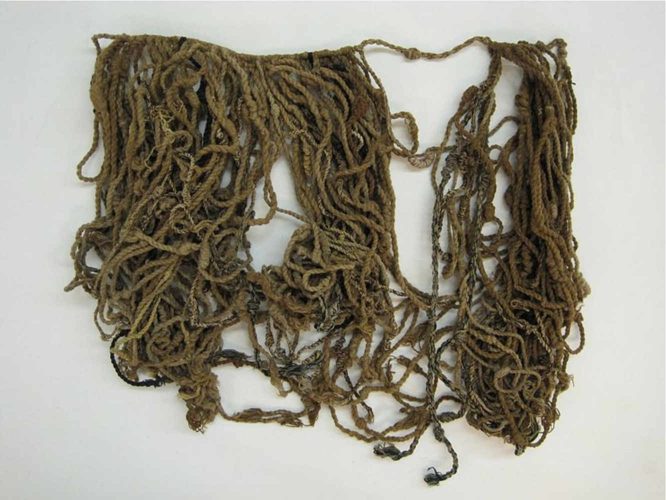
Embroidery

Sun god with snakes



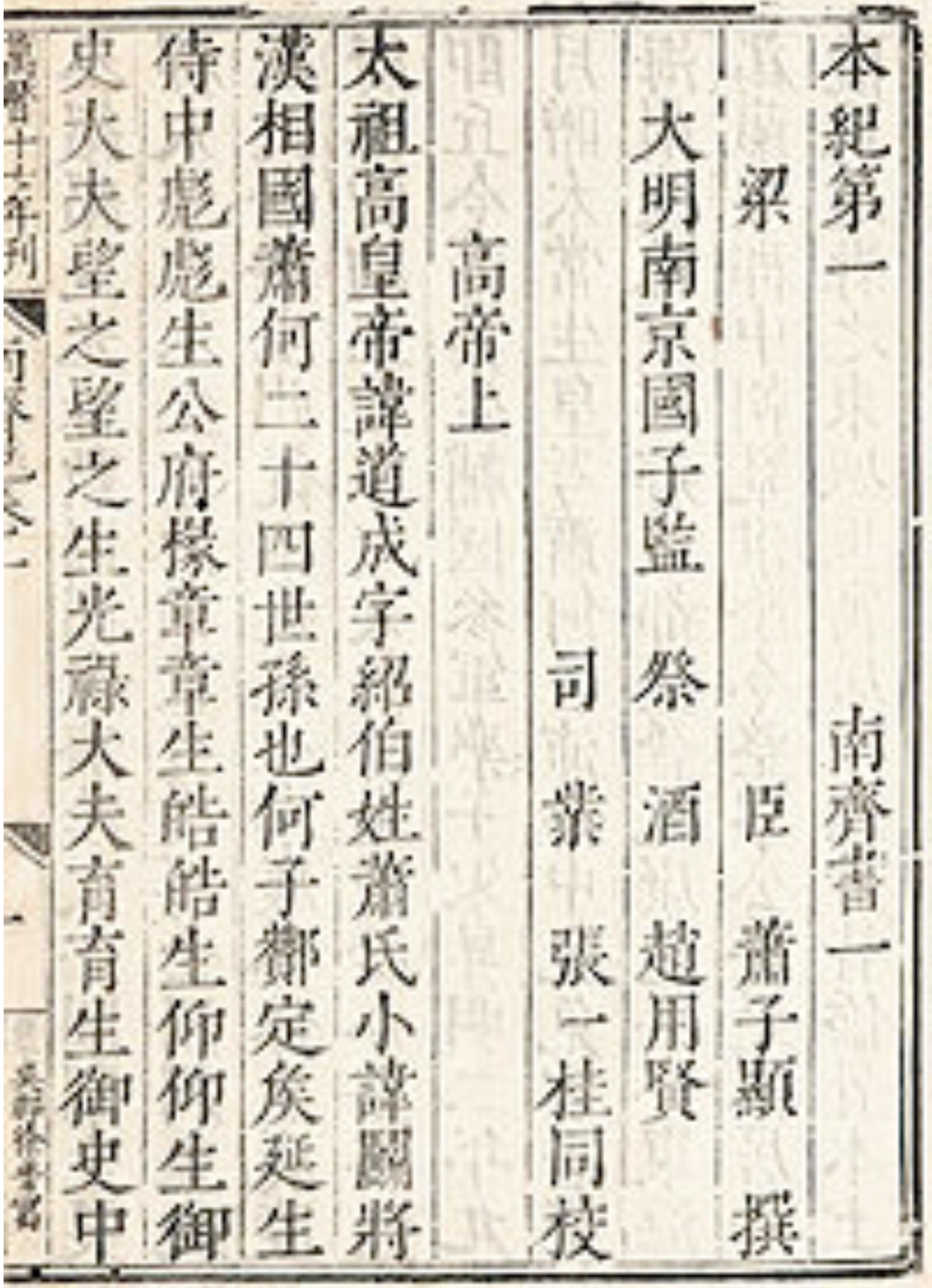
Cusco

Machu-Picchu



Quipu

Chinese script



本紀第一　南齊書一

梁　臣蕭子顯　撰

大明南京國子監祭酒趙用賢

司業張一桂同校

高帝上

太祖高皇帝諱道成字紹伯姓蕭氏小諱鬬將

漢相國蕭何二十四世孫也何子酇定侯延生

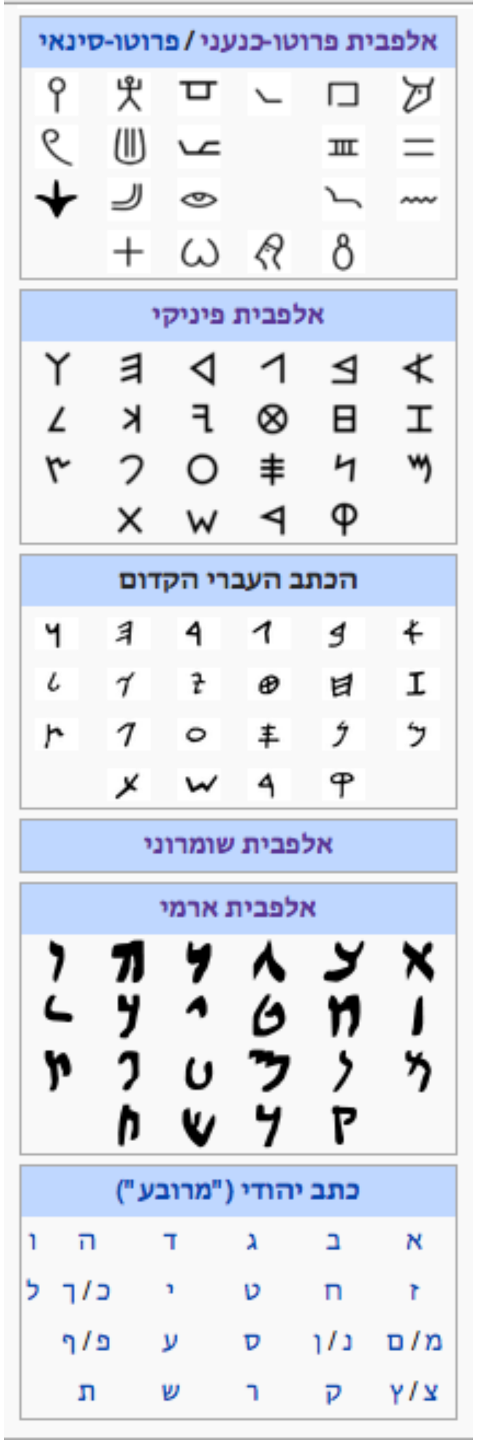
侍中彪彪生公府掾章章生皓皓生仰仰生御

史大夫望之望之生光祿大夫育育生御史中

萬曆十六年刊　南齊書卷一　一　吳郡徐本富

為此所能兼

Hebrew Alphabet development



אלפבית פרוטו-כנעני / פרוטו-סינאי

אלפבית פיניקי

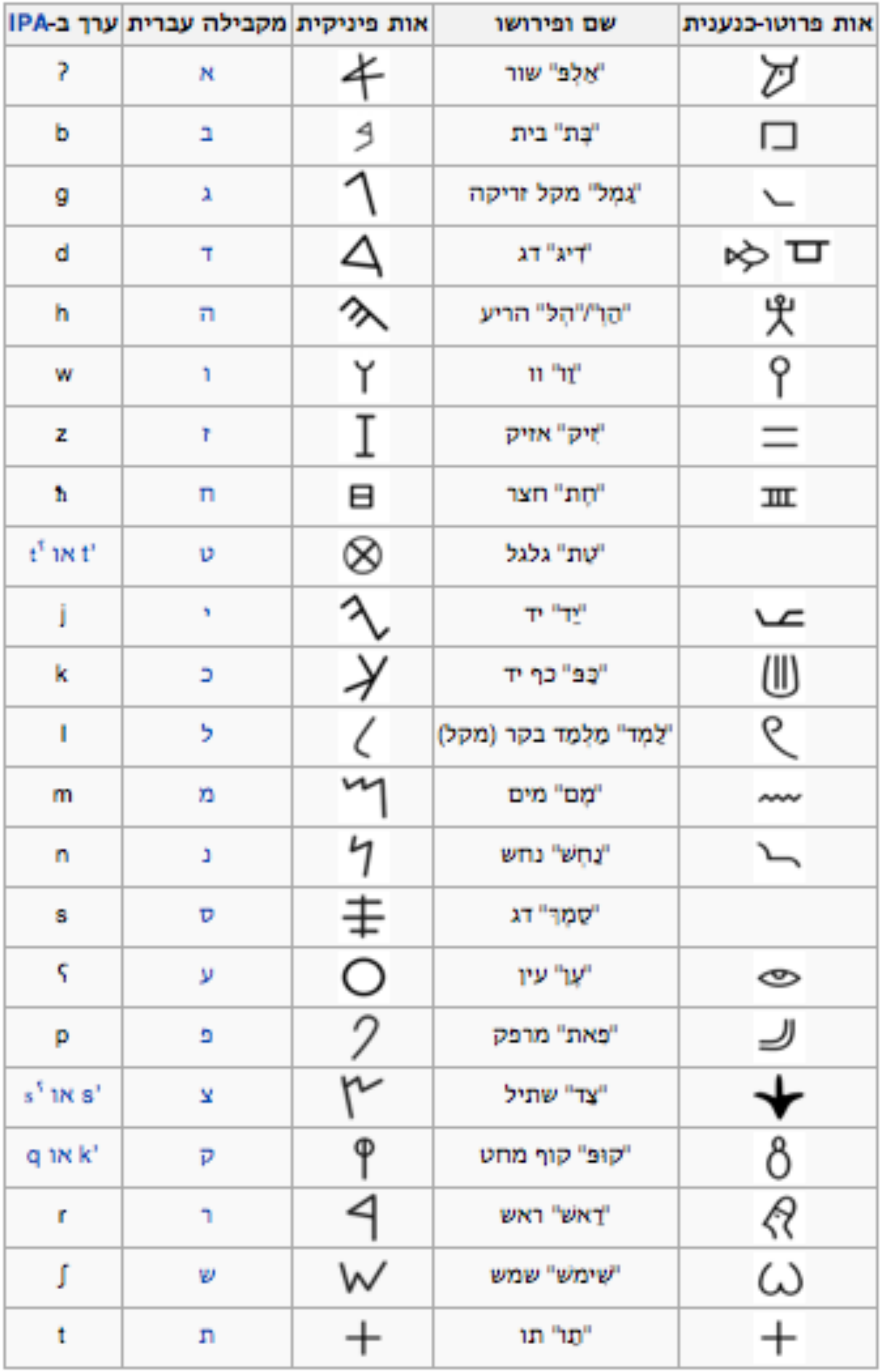
הכתב העברי הקדום

אלפבית שומרוני

אלפבית ארמי

כתב יהודי ("מרובע")

א ב ג ד ה ו
ז ח ט י כ/ך ל
מ/ם נ/ן ס ע פ/ף
צ/ץ ק ר ש ת

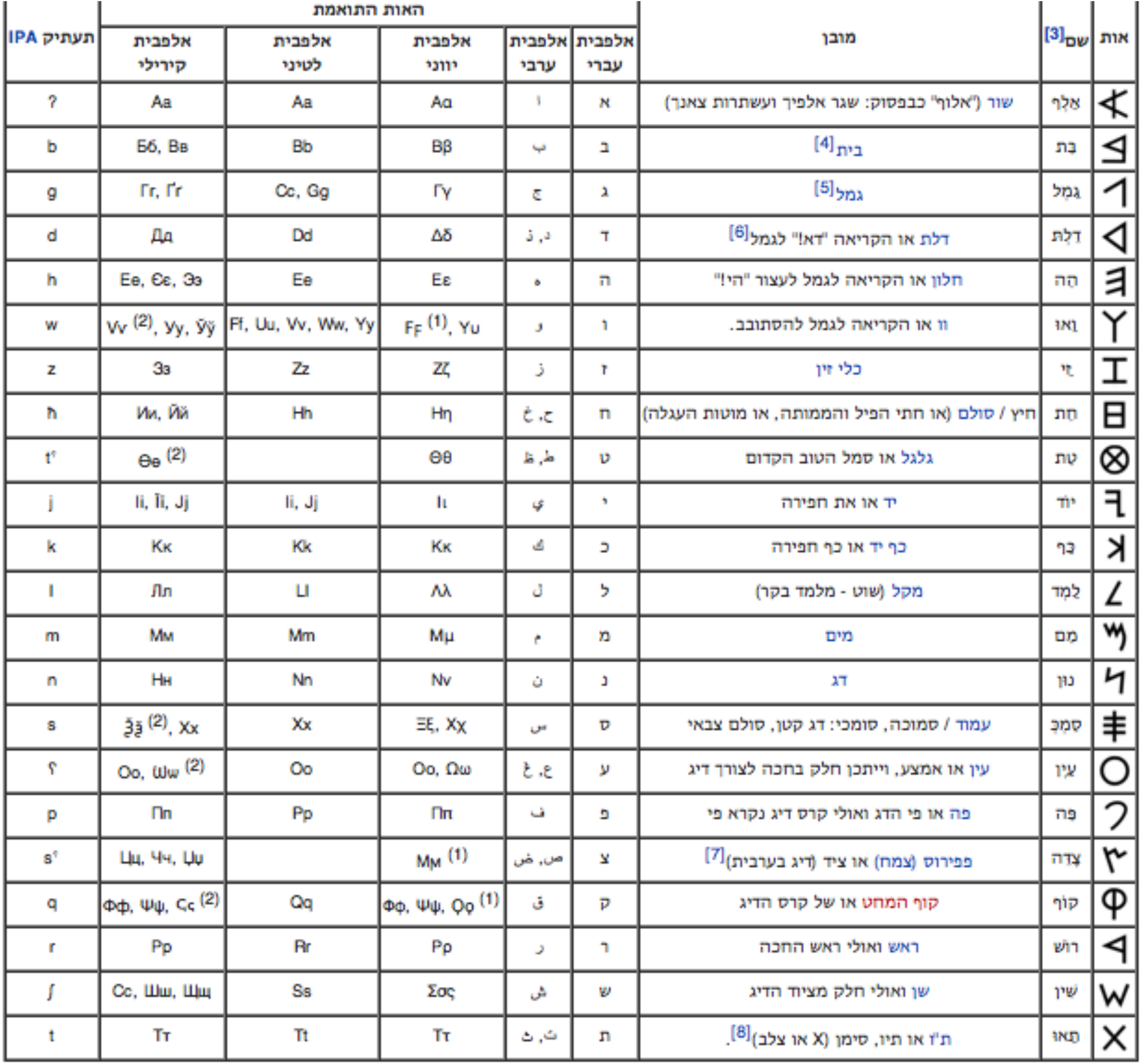


ערך ב-IPA	מקבילה עברית	אות פיניקית	שם ופירושו	אות פרוטו-כנענית
ʔ	א	𐤀	"אָלֶף" שור	
b	ב	𐤁	"בֵּת" בית	
g	ג	𐤂	"גִּמֶל" מקל זריקה	
d	ד	𐤃	"דִיג" דג	
h	ה	𐤄	"הֵן"/"הֵל" הריע	
w	ו	𐤅	"וָו" וו	
z	ז	𐤆	"זִיק" אזיק	
ħ	ח	𐤇	"חֵת" חצר	
t' או tˤ	ט	𐤈	"טֵת" גלגל	
j	י	𐤉	"יַד" יד	
k	כ	𐤊	"כַּף" כף יד	
l	ל	𐤋	"לָמֶד" מְלַמֵּד בקר (מקל)	
m	מ	𐤌	"מֵם" מים	
n	נ	𐤍	"נַחַשׁ" נחש	
s	ס	𐤎	"סָמֶךְ" דג	
ʕ	ע	𐤏	"עֵן" עין	
p	פ	𐤐	"פאת" מרפק	
s' או sˤ	צ	𐤑	"צדי" שתיל	
k' או q	ק	𐤒	"קופ" קוף מחט	
r	ר	𐤓	"רֵאשׁ" ראש	
ʃ	ש	𐤔	"שִׁימְשׁ" שמש	
t	ת	𐤕	"תָו" תו	

Proto-Canaan script – migration from pictographic hieroglyphs to letters.

The deciphering of this script was enabled by Egyptian text in both hieroglyphs and Proto-Canaan scripts on the Amanmakhat III sphinx.

These scripts were found in the Sinai desert.



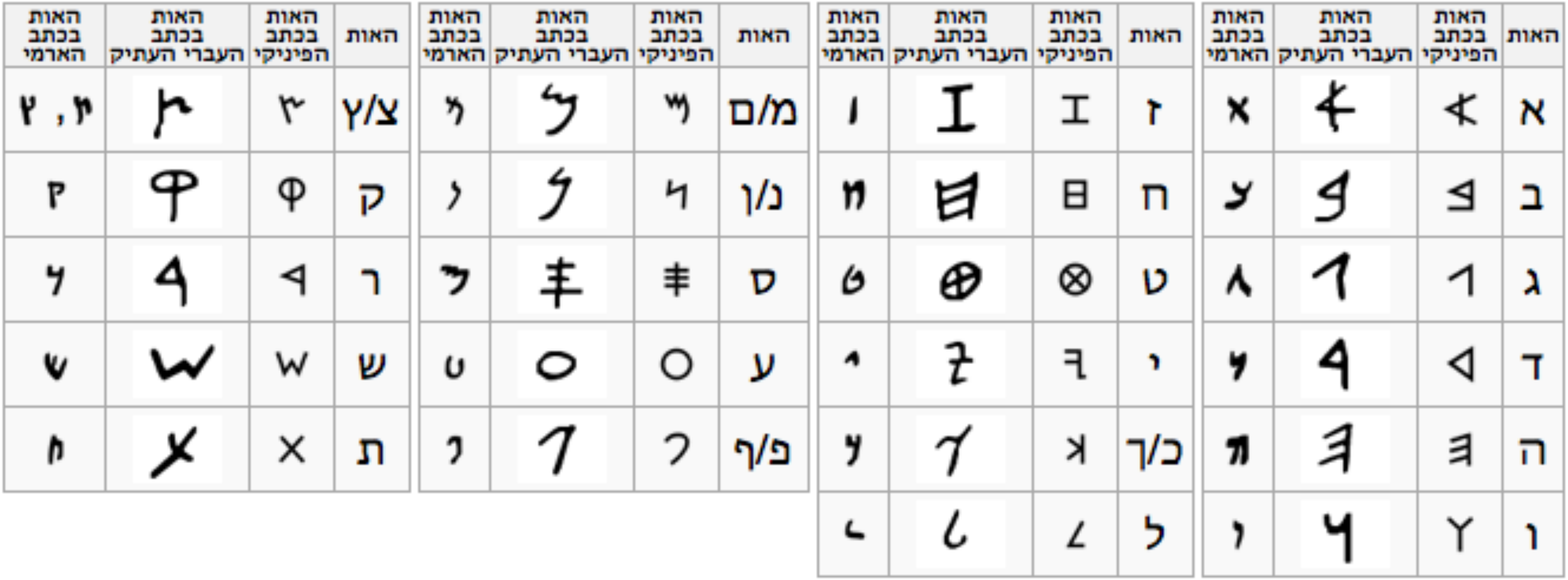
תעתיק IPA	האות התואמת					מובן	שם[3]	אות
	אלפבית קירילי	אלפבית לטיני	אלפבית יווני	אלפבית ערבי	אלפבית עברי			
ʔ	Aa	Aa	Aα	ا	א	שור ("אלוף" כבפסוק: שגר אלפיך ועשתרות צאנך)	אָלֶף	𐤀
b	Бб, Вв	Bb	Bβ	ب	ב	בית[4]	בֵּת	𐤁
g	Гг, Ґґ	Cc, Gg	Γγ	ج	ג	גמל[5]	גִּמֶל	𐤂
d	Дд	Dd	Δδ	د, ذ	ד	דלת או הקריאה "דא!" לגמל[6]	דֶּלֶת	𐤃
h	Ее, Єє, Ээ	Ee	Eε	ه	ה	חלון או הקריאה לגמל לעצור "הי!"	הֵה	𐤄
w	Vv (2), Уу, Ўў	Ff, Uu, Vv, Ww, Yy	Ϝϝ (1), Υυ	و	ו	וו או הקריאה לגמל להסתובב.	וָאו	𐤅
z	Зз	Zz	Ζζ	ز	ז	כלי זין	זַי	𐤆
ħ	Ии, Йй	Hh	Hη	ح, خ	ח	חיץ / סולם (או חתי הפיל והממותה, או מוטות העגלה)	חֵת	𐤇
tˤ	Ѳѳ (2)		Θθ	ط, ظ	ט	גלגל או סמל הטוב הקדום	טֵת	𐤈
j	Ii, Її, Jj	Ii, Jj	Iι	ي	י	יד או את חפירה	יוֹד	𐤉
k	Кк	Kk	Kκ	ك	כ	כף יד או כף חפירה	כַּף	𐤊
l	Лл	Ll	Λλ	ل	ל	מקל (שוט - מלמד בקר)	לָמֶד	𐤋
m	Мм	Mm	Mμ	م	מ	מים	מֵם	𐤌
n	Нн	Nn	Nν	ن	נ	דג	נוּן	𐤍
s	Ѯѯ (2), Хх	Xx	Ξξ, Xχ	س	ס	עמוד / סמוכה, סומכי: דג קטן, סולם צבאי	סָמֶךְ	𐤎
ʕ	Оо, Ѡѡ (2)	Oo	Oo, Ωω	ع, غ	ע	עין או אמצע, וייתכן חלק בחכה לצורך דיג	עַיִן	𐤏
p	Пп	Pp	Ππ	ف	פ	פה או פי הדג ואולי קרס דיג נקרא פי	פֵּה	𐤐
sˤ	Цц, Чч, Џџ		Ϻϻ (1)	ص, ض	צ	פפירוס (צמח) או ציד (דיג בערבית)[7]	צָדֵה	𐤑
q	Фф, Ψψ, Ҁҁ (2)	Qq	Φφ, Ψψ, Ϙϙ (1)	ق	ק	קוף המחט או של קרס הדיג	קוֹף	𐤒
r	Рр	Rr	Pρ	ر	ר	ראש ואולי ראש החכה	רוֹשׁ	𐤓
ʃ	Сс, Шш, Щщ	Ss	Σσς	ش	ש	שן ואולי חלק מציוד הדיג	שִׁין	𐤔
t	Тт	Tt	Tτ	ت, ث	ת	ת'ו או תיו, סימן (X או צלב)[8].	תָּאו	𐤕

Phoenician script

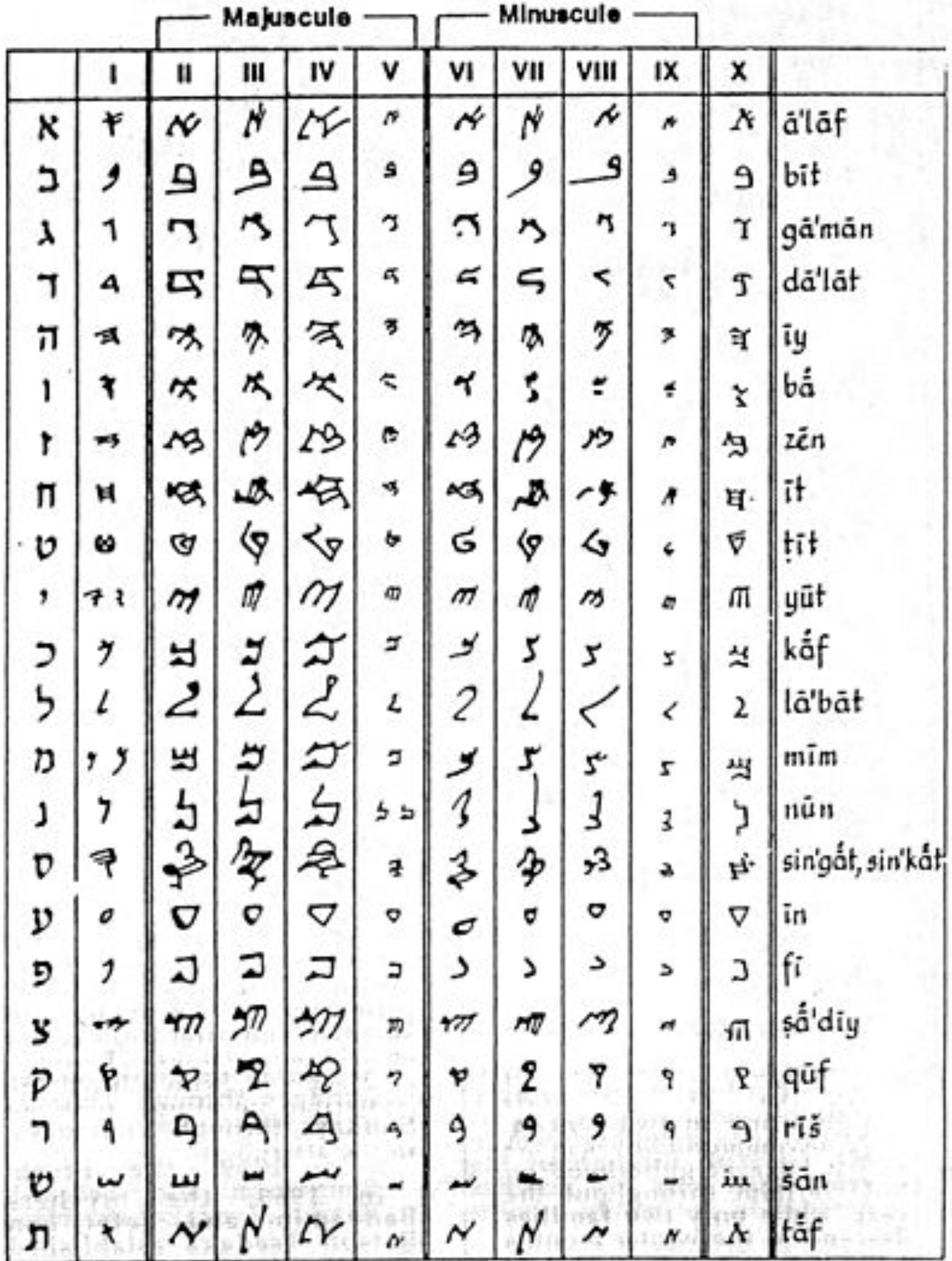
Gezer tablet

The source of Aramaic, Hebrew and Greek scripts.

Old Hebrew letters



האות	האות בכתב הפיניקי	האות בכתב העברי העתיק	האות בכתב הארמי
א	𐤀	𐤀	𐡀
ב	𐤁	𐤁	𐡁
ג	𐤂	𐤂	𐡂
ד	𐤃	𐤃	𐡃
ה	𐤄	𐤄	𐡄
ו	𐤅	𐤅	𐡅
ז	𐤆	𐤆	𐡆
ח	𐤇	𐤇	𐡇
ט	𐤈	𐤈	𐡈
י	𐤉	𐤉	𐡉
כ/ך	𐤊	𐤊	𐡊
ל	𐤋	𐤋	𐡋
מ/ם	𐤌	𐤌	𐡌
נ/ן	𐤍	𐤍	𐡍
ס	𐤎	𐤎	𐡎
ע	𐤏	𐤏	𐡏
פ/ף	𐤐	𐤐	𐡐
צ/ץ	𐤑	𐤑	𐡑 , 𐡑
ק	𐤒	𐤒	𐡒
ר	𐤓	𐤓	𐡓
ש	𐤔	𐤔	𐡔
ת	𐤕	𐤕	𐡕


Majuscule
Minuscule
I
II
III
IV
V
VI
VII
VIII
IX
X
א ā'lāf
ב bīt
ג gā'mān
ד dā'lāt
ה īy
ו bā́
ז zēn
ח īt
ט ṭīt
י yūt
כ kā́f
ל lā'bāt
מ mīm
נ nūn
ס sin'gā́t, sin'kā́t
ע īn
פ fī
צ ṣā́'dīy
ק qūf
ר rīš
ש šān
ת tā́f

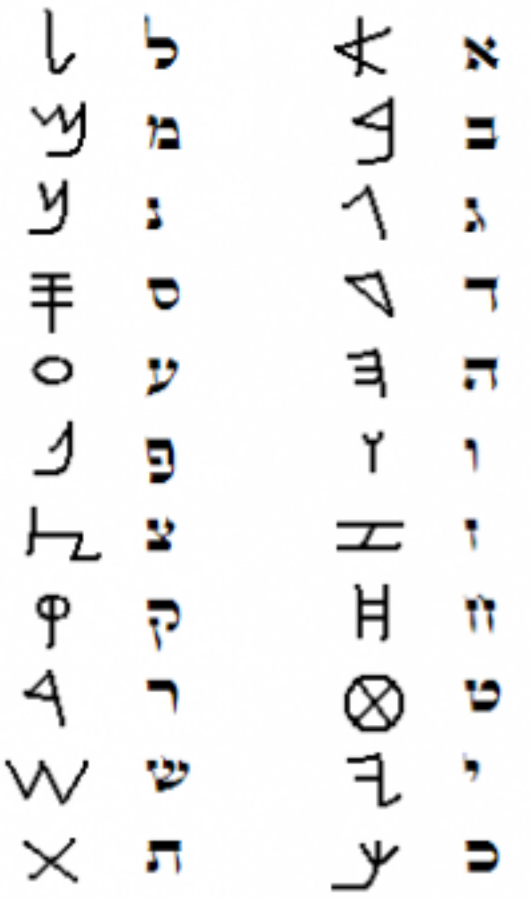
Samaritan script

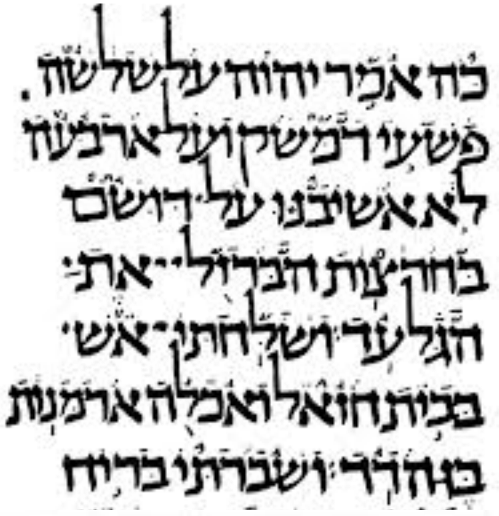
Probably the script of the Judea and Israel kingdoms of the first temple.

Aramaic and modern Arabic & Hebrew scripts

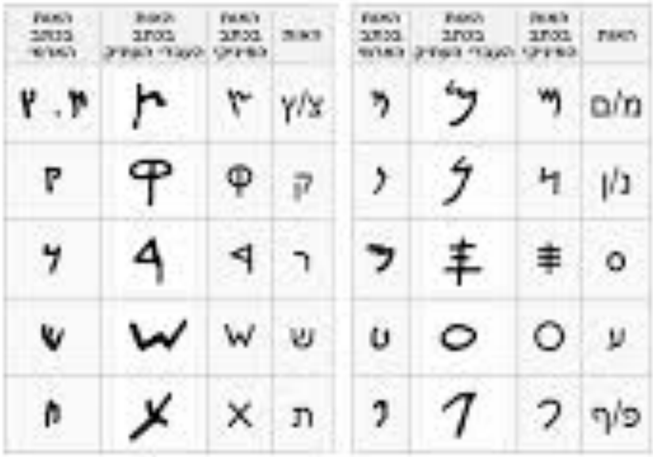
Sound		Syriac	Arabic	Hebrew	Aramaic	Sound	Syriac	Arabic	Hebrew	Aramaic
/l/		ܠ	ل	ל	𐡋	/ʔ/; /aː/, /eː/	ܐ	أ	א	𐡀
/m/		ܡ	م	מ ם	𐡌	/b/, /v/	ܒ	ب	ב	𐡁
/n/	□	ܢ	ن	נ ן	𐡍	/g/, /ɣ/	ܓ	ج	ג	𐡂
/s/		ܣ	·	ס	𐡎	/d/, /ð/	ܕ	د، ذ	ד	𐡃
/ʕ/		ܥ	ع، غ	ע	𐡏	/h/	ܗ	ه	ה	𐡄
/p/, /f/		ܦ	ف	פ ף	𐡐	w/; /oː/, /uː//	ܘ	و	ו	𐡅
/sˤ/ נחצי		ܨ	ص، ض	צ ץ	𐡑 . 𐡑	/z/	ܙ	ز	ז	𐡆
/q/		ܩ	ق	ק	𐡒	/ħ/	ܚ	ح، خ	ח	𐡇
/r/		ܪ	ر	ר	𐡓	/tˤ/ נחצי	ܛ	ط، ظ	ט	𐡈
/ʃ/, /ɬ/		ܫ	ش، س	ש	𐡔	j/; /iː/, /eː//	ܝ	ي	י	𐡉
/t/, /θ/		ܬ	ت، ث	ת	𐡕	/k/, /x/	ܟ	ك	כ ך	𐡊

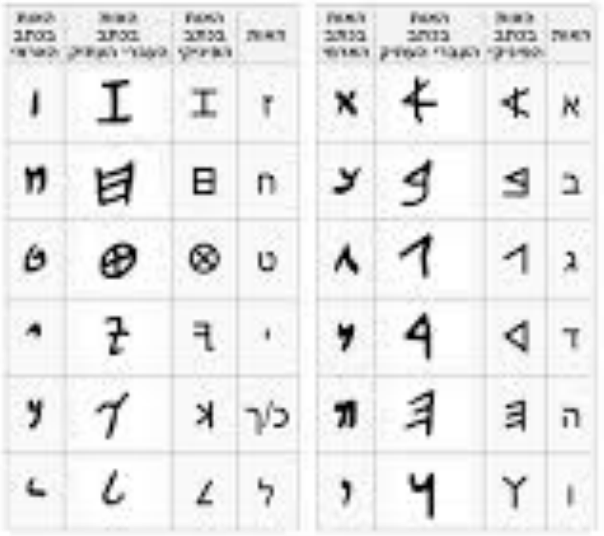
Hebrew on stone & calf skin

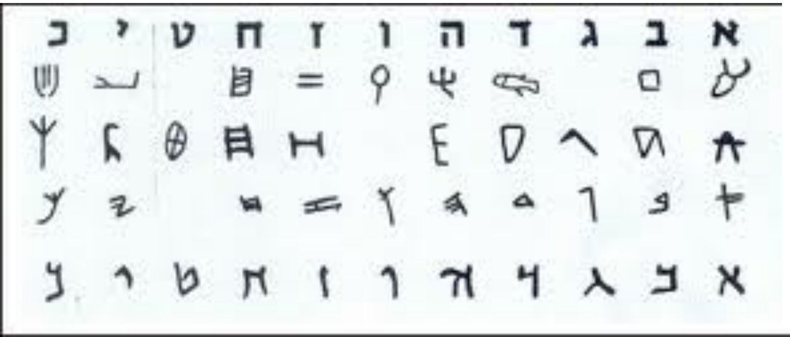




כה אמר יהוה על שלשה.
פשעי דמשק ועל ארבעה
לא אשיבנו על דושם
בחרצות הברזל את
הגלעד ושלחתי אש
בבית חזאל ואכלה ארמנות
בןהדד ושברתי בריח


צ/ץ
ק
ר
ש
ת
מ/ם
נ/ן
ס
ע
פ/ף


ז
ח
ט
י
כ/ך
ל
א
ב
ג
ד
ה
ו



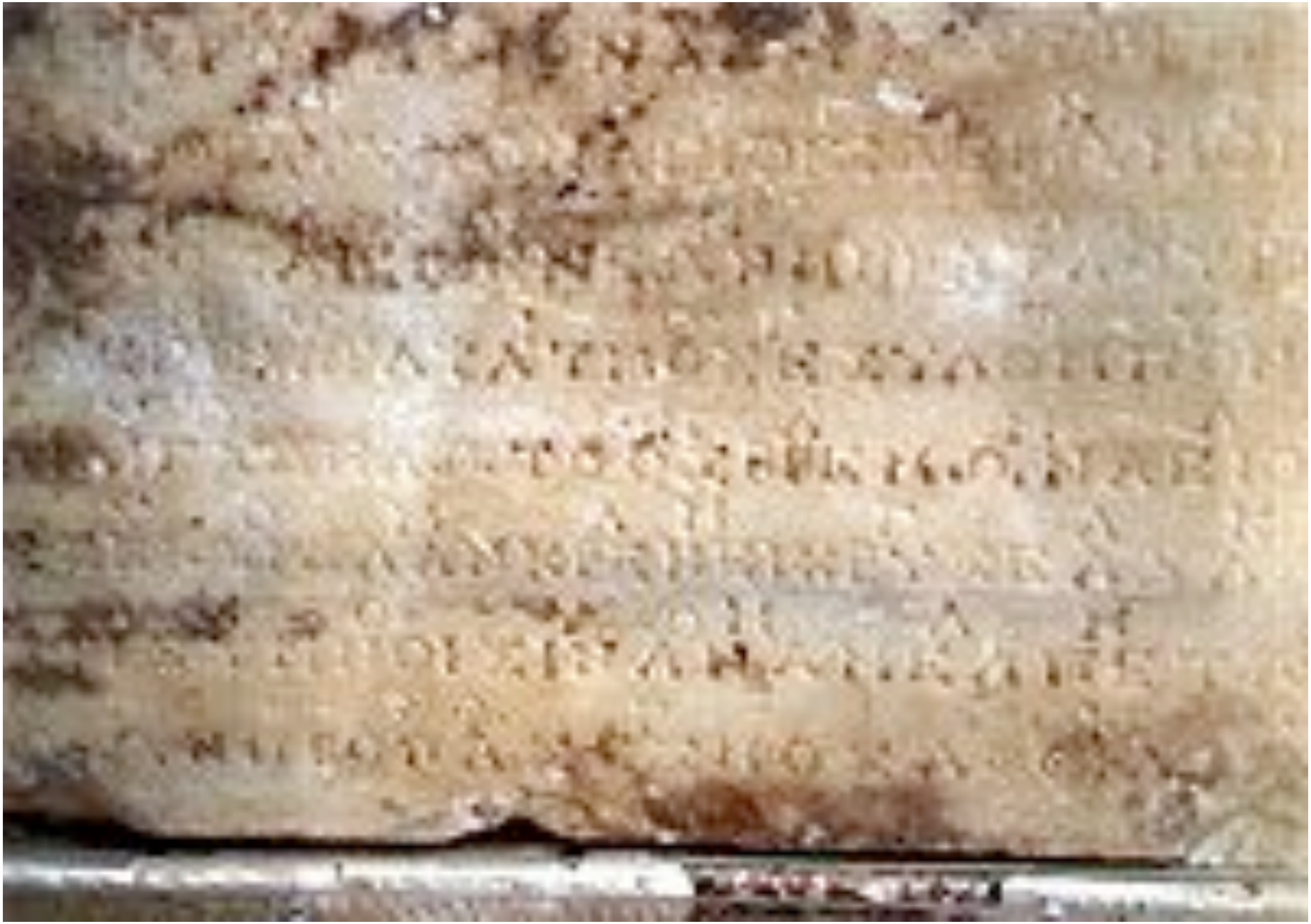
Present
Canaan
Proto-Canaan
Hebrew seals
Squared Hebrew

SUMMARY:

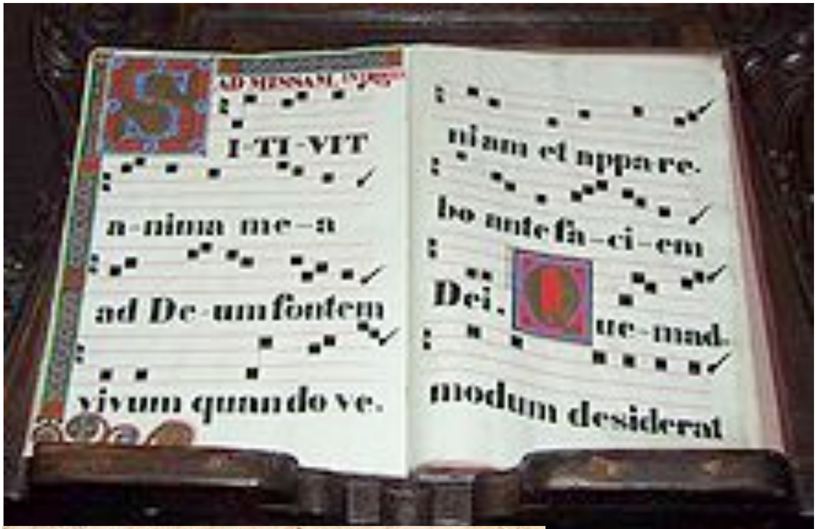
Writing probably started with pictorial signs. The enriching of the spoken languages with the expansion of the literal population (from priests in temples, to administrators and merchants), was probably the reason to develop simpler signs, and to move from Pictographic toward Logographic scripts. Letters, often a first sound or vowel in the pictorial name, provided flexibility of writing words without extending the “dictionary”. At different sites of human settlement the evolution of scripting was different. Interactions between cultures created fusions and similarities, nevertheless, hundreds of distinct languages and scripts exist today, and ethnic pride to keep their heritage invest efforts to preserve them, side by side with global communication languages.

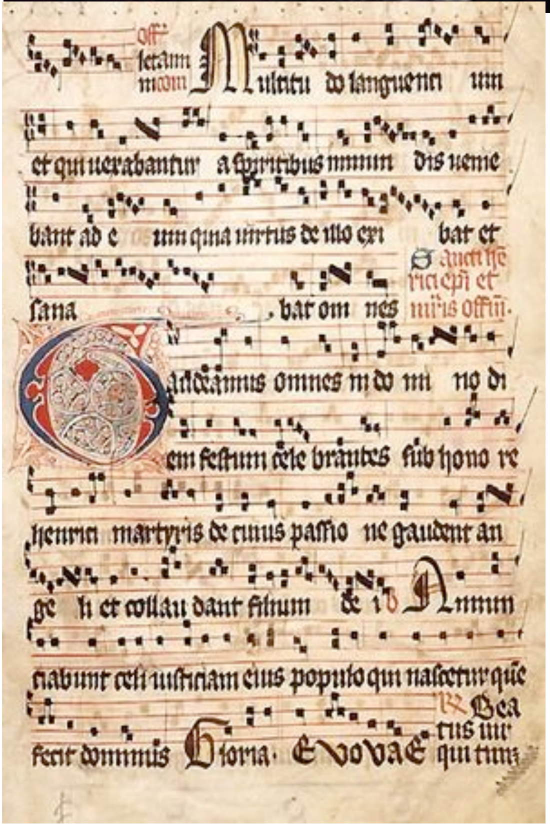
WRITTEN MUSIC

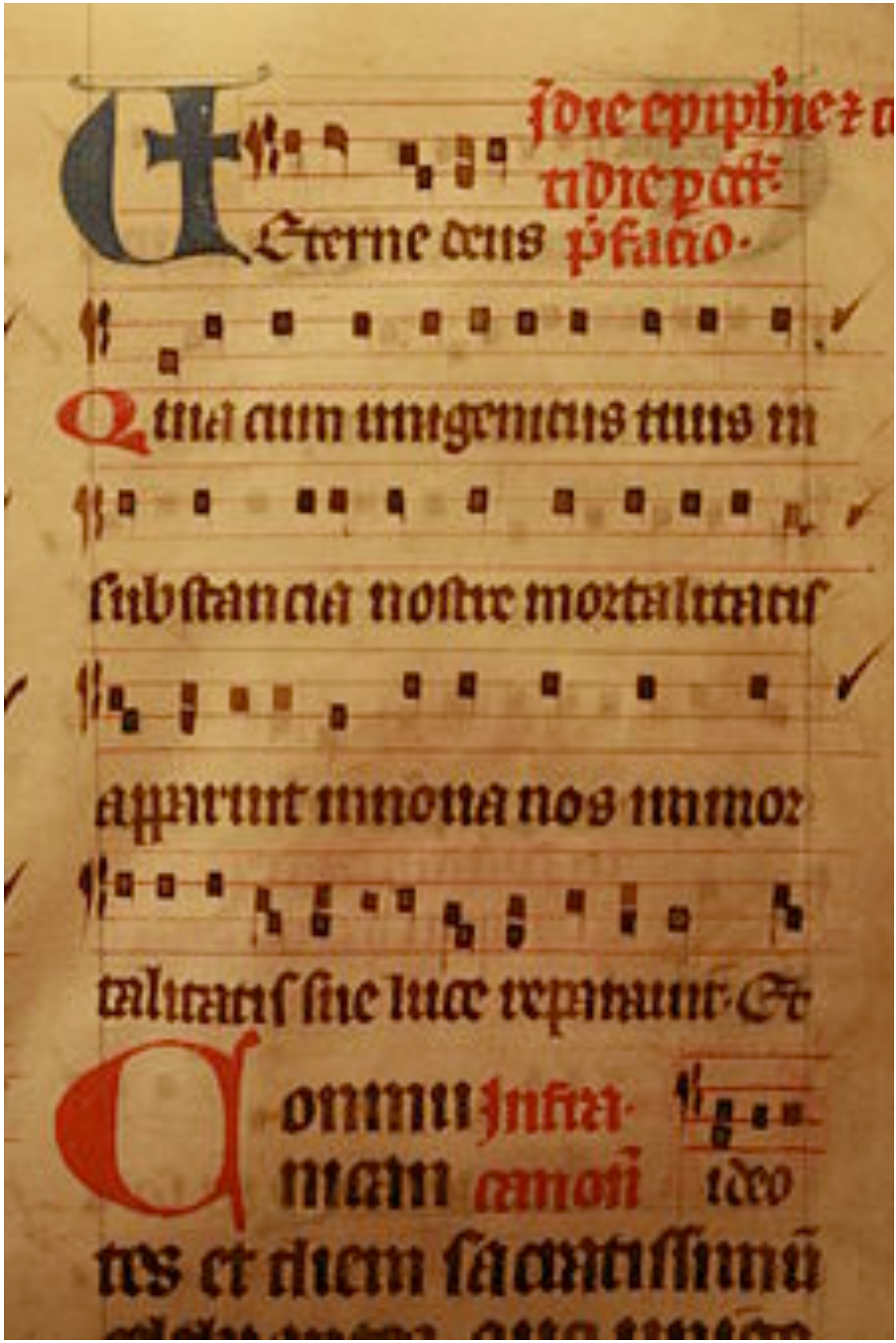
Song of praise to Apollo



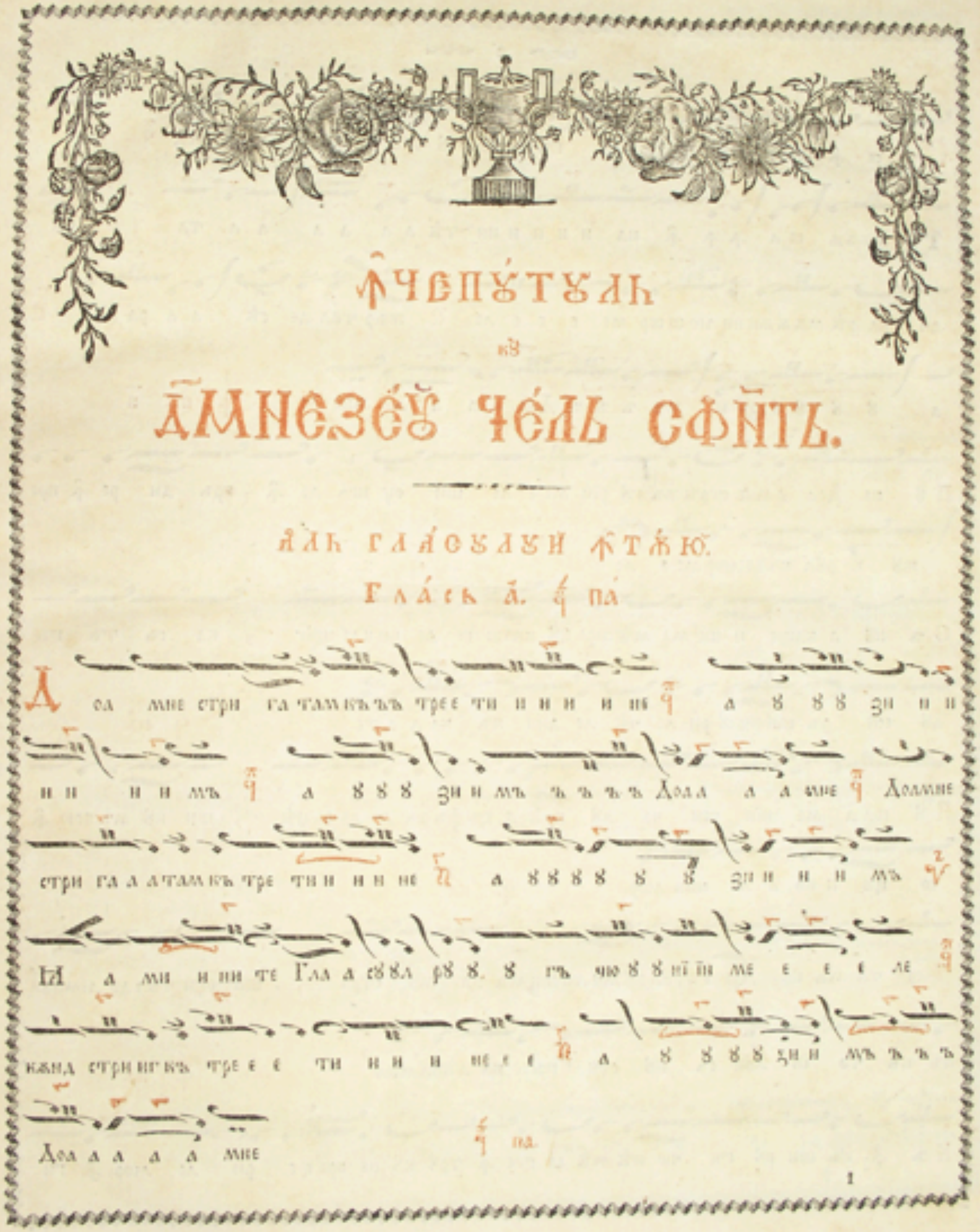
Gregorian chants – medieval era




Offeram
Multitu do languenti
et qui uexabantur a spiritibus
Gaudeamus omnes in domino
em festum celebrantes sub hono re
henrici martyris de cuius passio ne gaudent an
Gloria. Euouae


Eterne deus
Quia cum unigenitus tuus in
substancia nostre mortalitatis
apparuit in nova nos immor
talitatis sue luce reparavit. Et
Communicantes
tes et diem sacratissimu

Byzantine chants



Ѫнчепꙋтꙋлъ

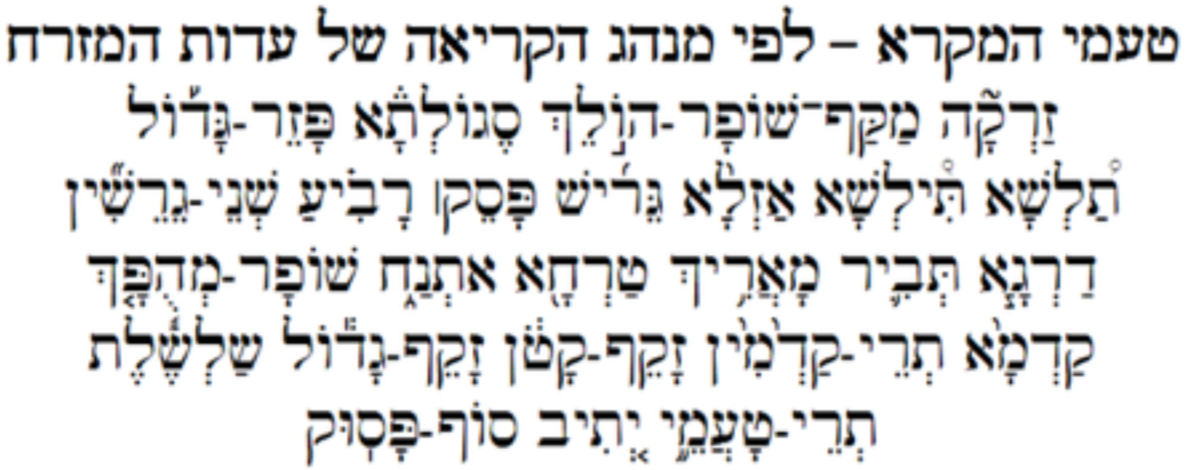
кꙋ

Дмнезеꙋ чел сфнтъ.

Ал гласꙋлꙋи ѫнтѫю.

Гласъ а. па

Д оа мне стри га тамкъ къ тре ти и и и и не а ꙋ ꙋ ꙋ зи и и
и и и и мъ а ꙋ ꙋ ꙋ зи и мъ ъ ъ ъ Доа а а мне Доамне
стри га а а тамкъ тре ти и и и и не а ꙋ ꙋ ꙋ ꙋ ꙋ ꙋ зи и и и мъ
И а ми и ни те Гла а сꙋꙋа рꙋ ꙋ ꙋ гъ чю ꙋ ꙋ ни ми ме е е е ле
кѫнд стри иг къ тре е е ти и и и не е е а ꙋ ꙋ ꙋ ꙋ зи и мъ ъ ъ ъ
Доа а а а а мне
па
1

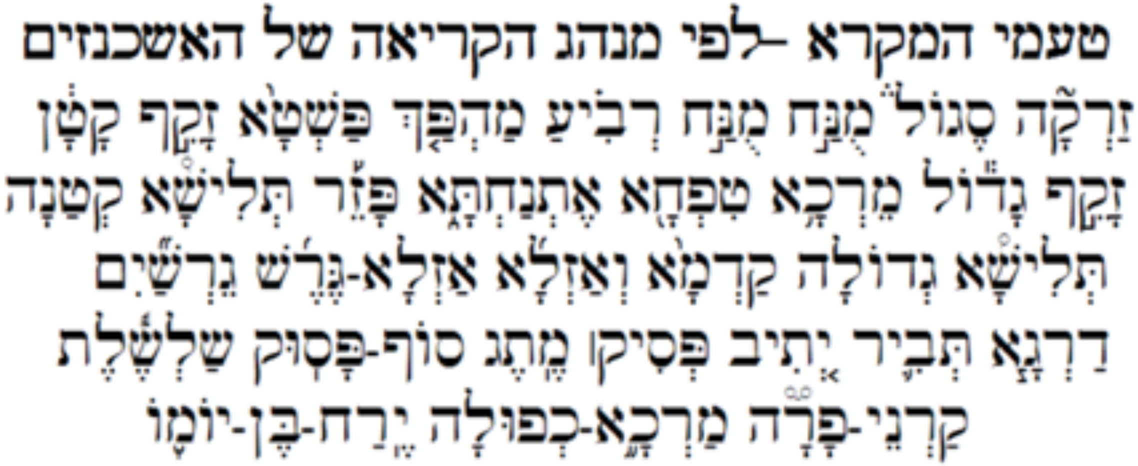


טעמי המקרא – לפי מנהג הקריאה של עדות המזרח

זַרְקָ֮ה מַקַּף־שׁוֹפָר-הוֹלֵ֣ךְ סֶגוֹלְתָּא֒ פָּזֵ֡ר-גָּד֟וֹל
תַּלְשָׁ֨א תִּ֩לְשָׁא אַזְלָ֨א גֵּרִ֜ישׁ פָּסֵקוּ רָבִ֗יעַ שְׁנֵי-גְרִישִׁ֞ין
דַּרְגָּ֧א תְּבִ֛יר מָאֲרִ֥יךְ טַרְחָ֖א אתְנָ֑ח שׁוֹפָר-מְהֻפָּ֤ךְ
קַדְמָ֨א תְּרֵי-קַדְמִ֨ין זָקֵף-קָטֹ֔ן זָקֵף-גָּד֕וֹל שַׁלְשֶׁ֓לֶת
תְּרֵי-טַעֲמֵ֦י יְתִ֚יב סוֹף-פָּסֽוּק

Cantillation

Musical signs for the cantor
Reading the bible

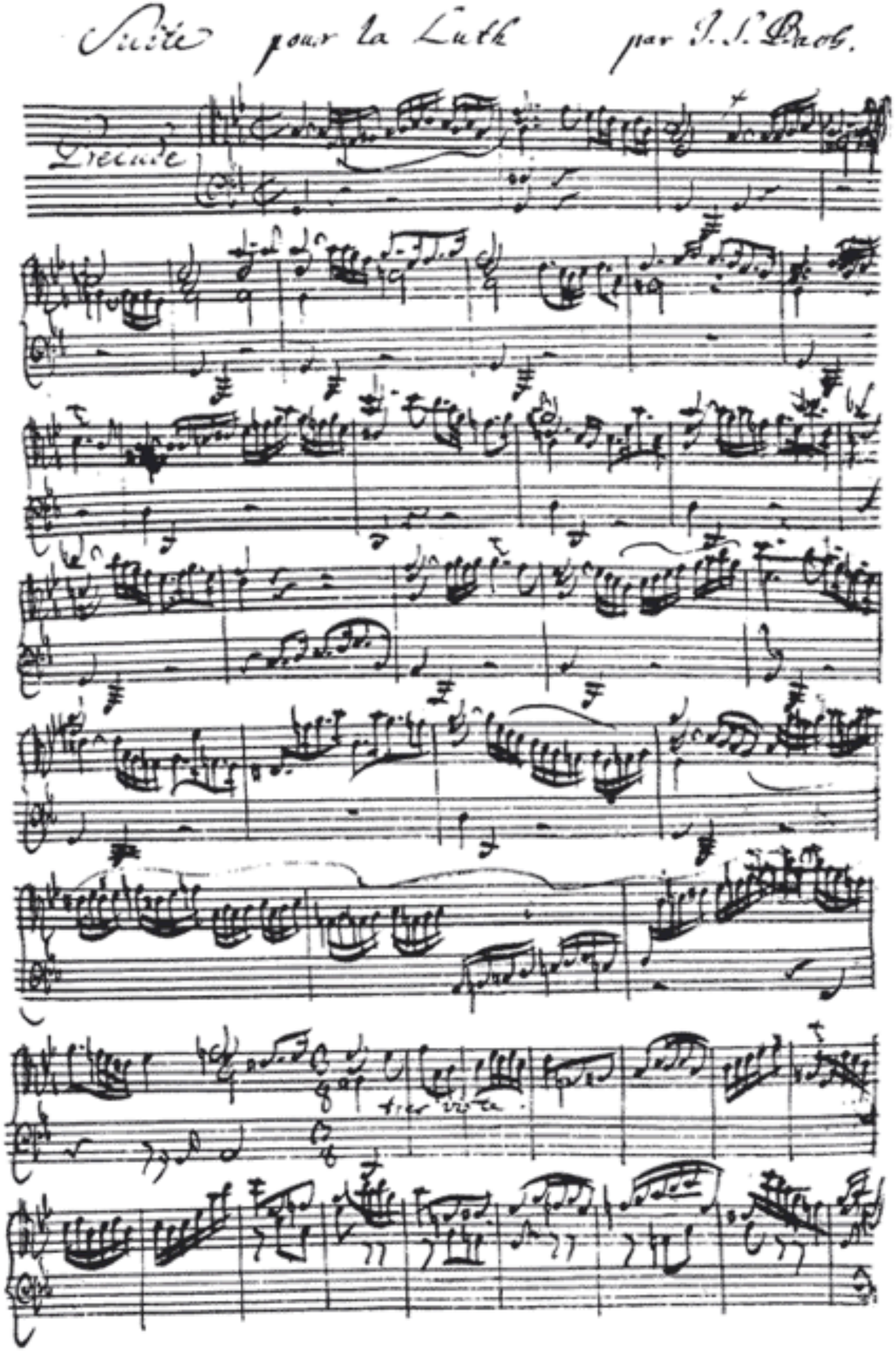


טעמי המקרא –לפי מנהג הקריאה של האשכנזים

זַרְקָ֮ה סֶגוֹל֒ מֻנַּ֣ח מֻנַּח֙ רְבִ֗יעַ מַהְפַּ֤ךְ פַּשְׁטָא֙ זָקֵף קָטֹ֔ן
זָקֵף גָּד֕וֹל מֵרְכָ֥א טִפְּחָ֖א אֶתְנַחְתָּ֑א פָּזֵ֡ר תְּלִישָׁא֠ קְטַנָּה
תְּ֠לִישָׁא גְדוֹלָה קַדְמָ֨א וְאַזְלָ֨א אַזְלָא-גֵּ֜רֵשׁ גֵּרְשַׁ֞יִם
דַּרְגָּ֧א תְּבִ֛יר יְתִ֚יב פְּסִיקו מֵֽתֶג סוֹף-פָּסֽוּק שַׁלְשֶׁ֓לֶת
קַרְנֵי-פָרָ֟ה מֵרְכָא-כְפוּלָ֦ה יֶרַח-בֶּן-יוֹמ֪וֹ

So far, musical writing in unisono – melody in one voice, no signs for dynamics or tempo.

Gregorian chants have sometimes canons (two voices)

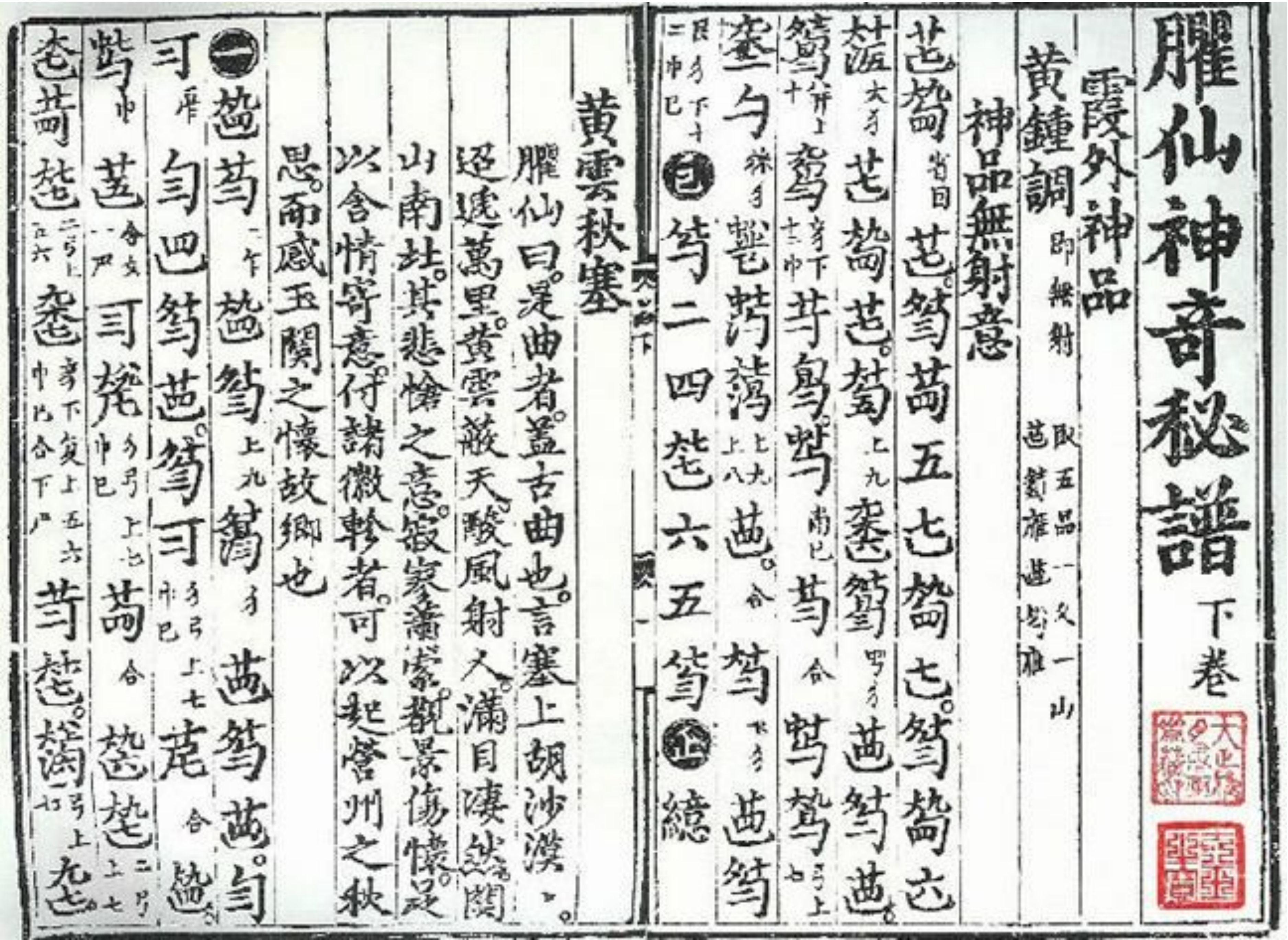


Bach
Harpsichord (two hands)

Bach composed using
"harmonic chords"

In contrast to "dissonances"

Chinese music: symbols similar to text scripts



臞仙神奇秘譜 下卷

霞外神品

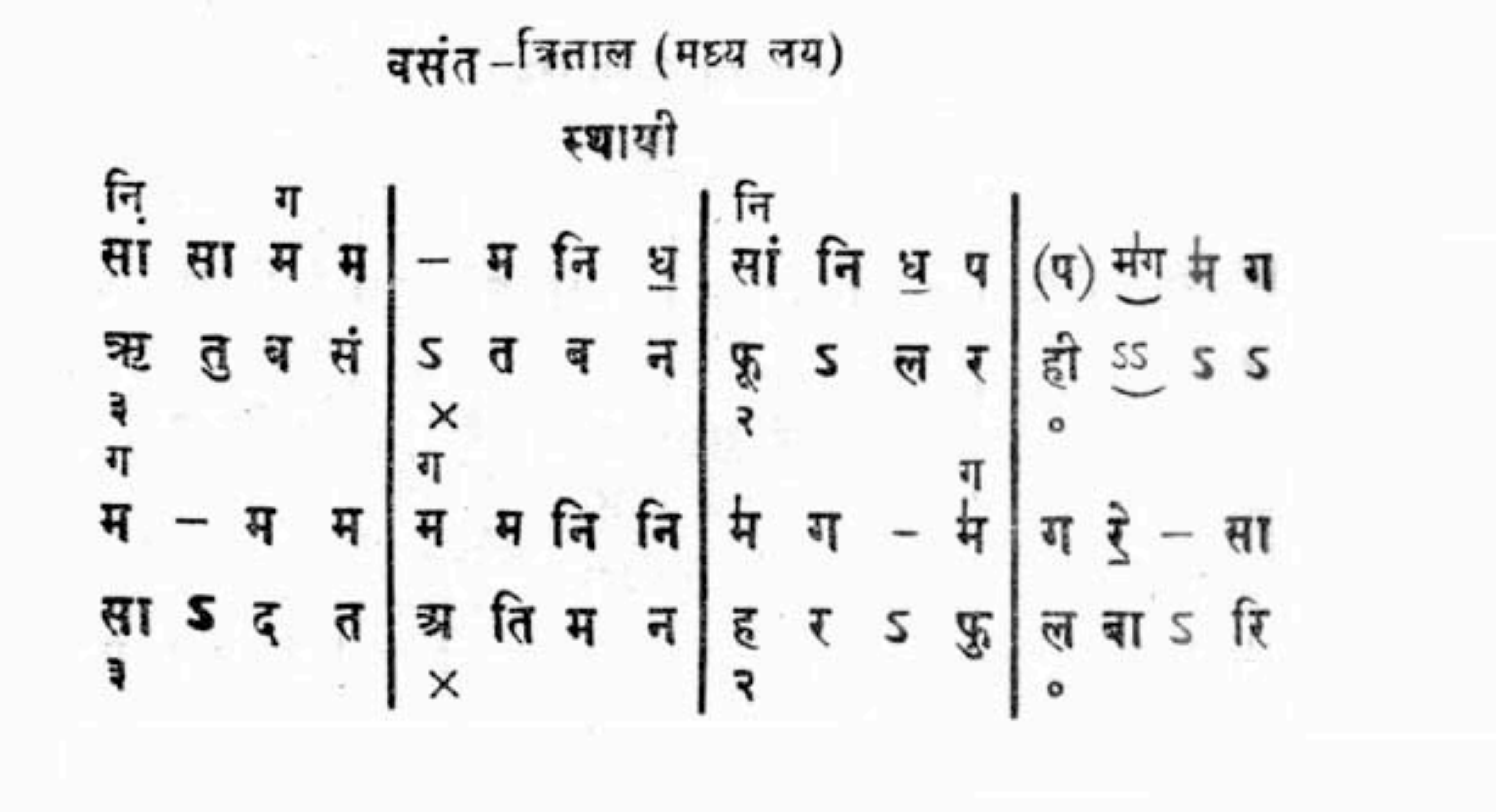
黃鍾調 即無射

神品無射意

黃雲秋塞

臞仙曰。是曲者。蓋古曲也。言塞上胡沙漠〻。逕遠萬里。黄雲蔽天。酸風射人。滿目淒然。關山南北。其悲愴之意。寂寥蕭索。觀景傷懷。是以含情寄意。付諸徽軫者。可以起營州之秋思。而感玉關之懷故鄉也

Modern Indian music

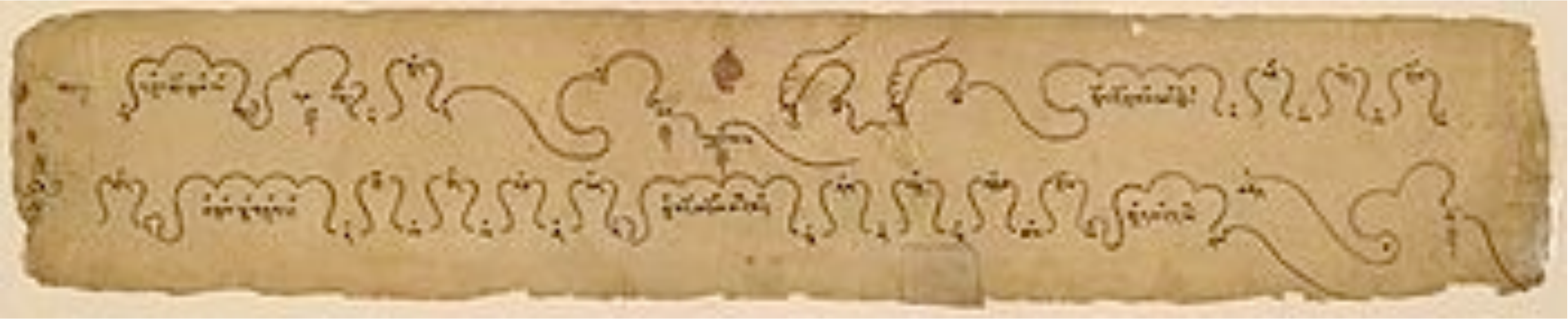


वसंत-त्रिताल (मध्य लय)

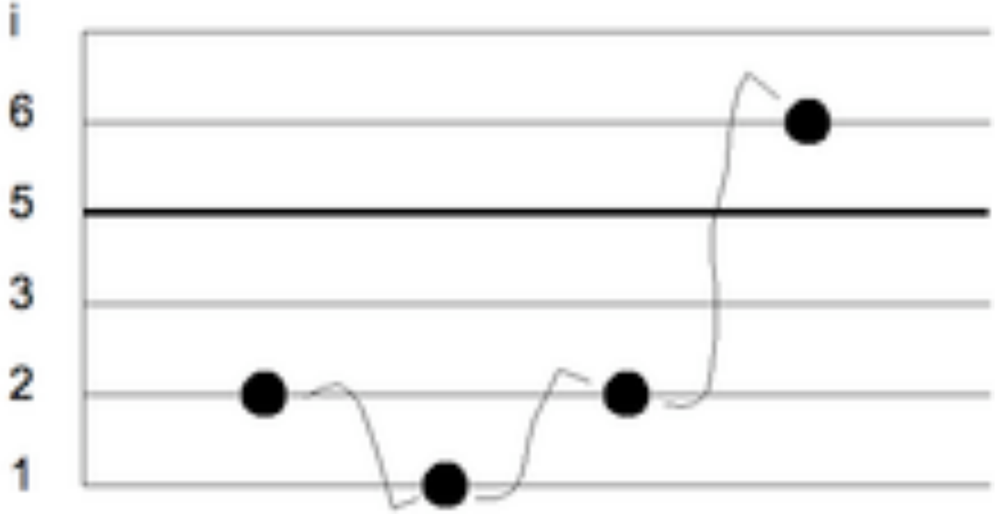
स्थायी

नि़		ग						नि							
सा	सा	म	म	–	म	नि	ध॒	सां	नि	ध॒	प	(प)	म॑ग	म॑	ग
ऋ	तु	ब	सं	ऽ	त	ब	न	फू	ऽ	ल	र	ही	ऽऽ	ऽ	ऽ
३				×				२				०			
ग				ग							ग				
म	–	म	म	म	म	नि	नि	म॑	ग	–	म॑	ग	रे॒	–	सा
सा	ऽ	द	त	अ	ति	म	न	ह	र	ऽ	फु	ल	बा	ऽ	रि
३				×				२				०			

Indonesian Gamelan music – two groups of instruments



Freedom of interpretation to the performer



Music writing

A strong resemblance between the notations for writing text and music.

Is music writing more or less complex than text?

Depends on the music:

Gregorian chants: include information on pitch sometimes length of the sound. No dynamics, tempo. Not polyphonic- one line.

Similarly cantillation: emphasizes textural content, music is just decorating.

Classical orchestral music: many parallel lines create harmonies. Music is written in different scales for different instruments, and includes note lengths, dynamics (piano, forte), tempo and mood indications (allegro maestoso, adagio cantabile) as well as sound effects (tremolo, pizzicato, sul-ponticello, sul-tasto, mute or sordino, harmonic or flageolett etc.).

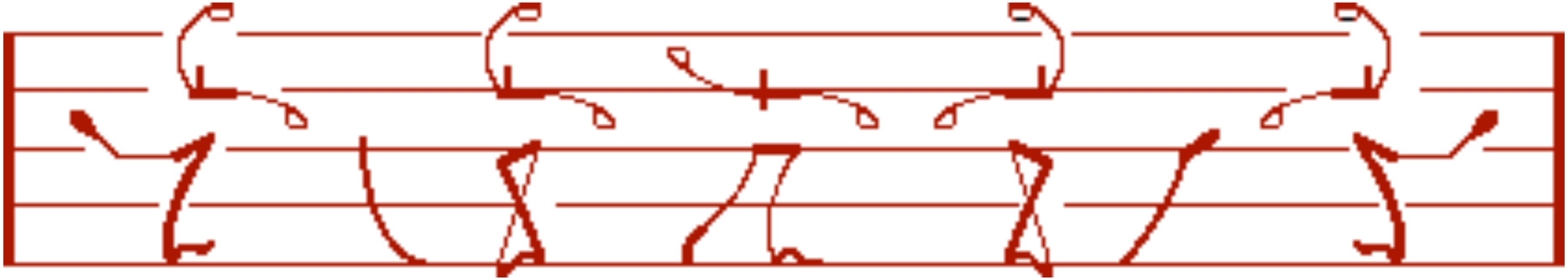
Much like different interpretations of reading poetry or acting plays in theaters, the interpretation of playing orchestral music is at the hands of the conductor, that vary in their performances. This is in contrast to mathematical scripts, that must express the same precise quantitative relations for all readers…

DANCE

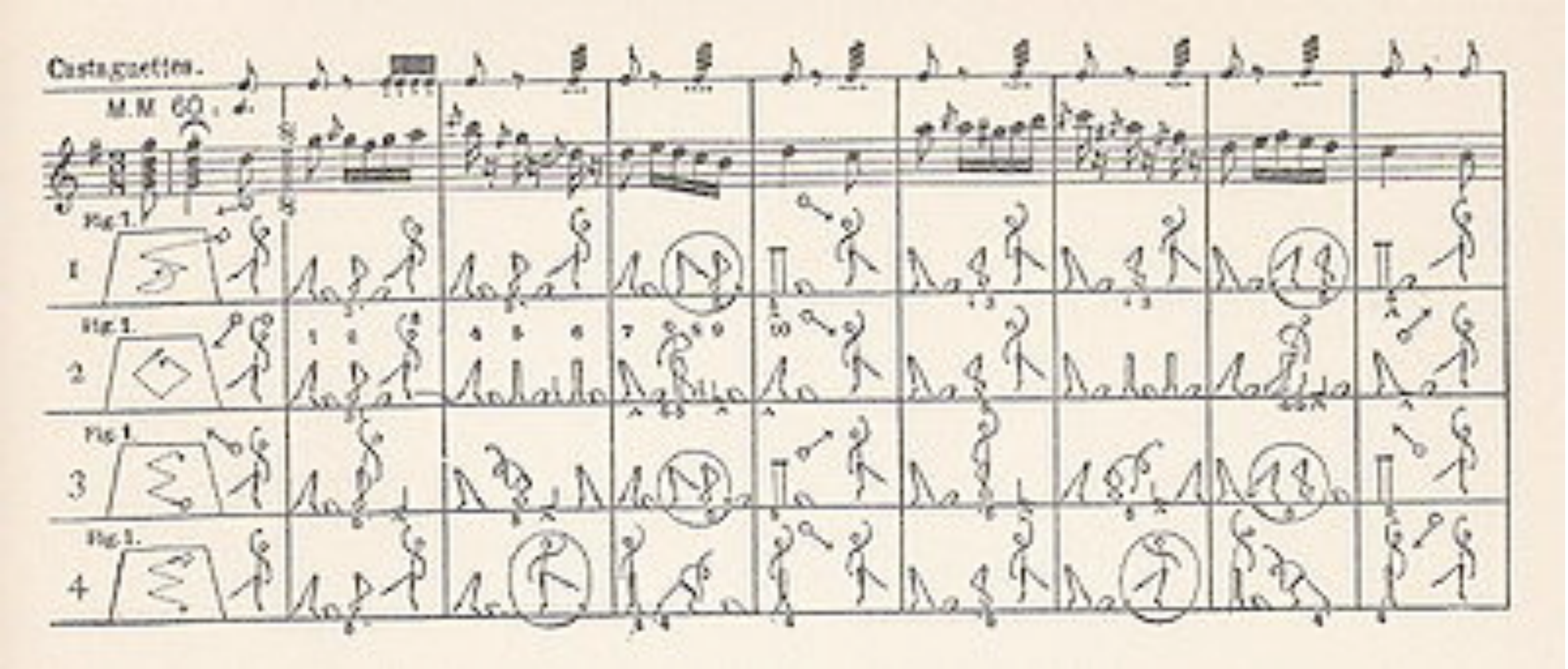
(CHOREOGRAPHY)

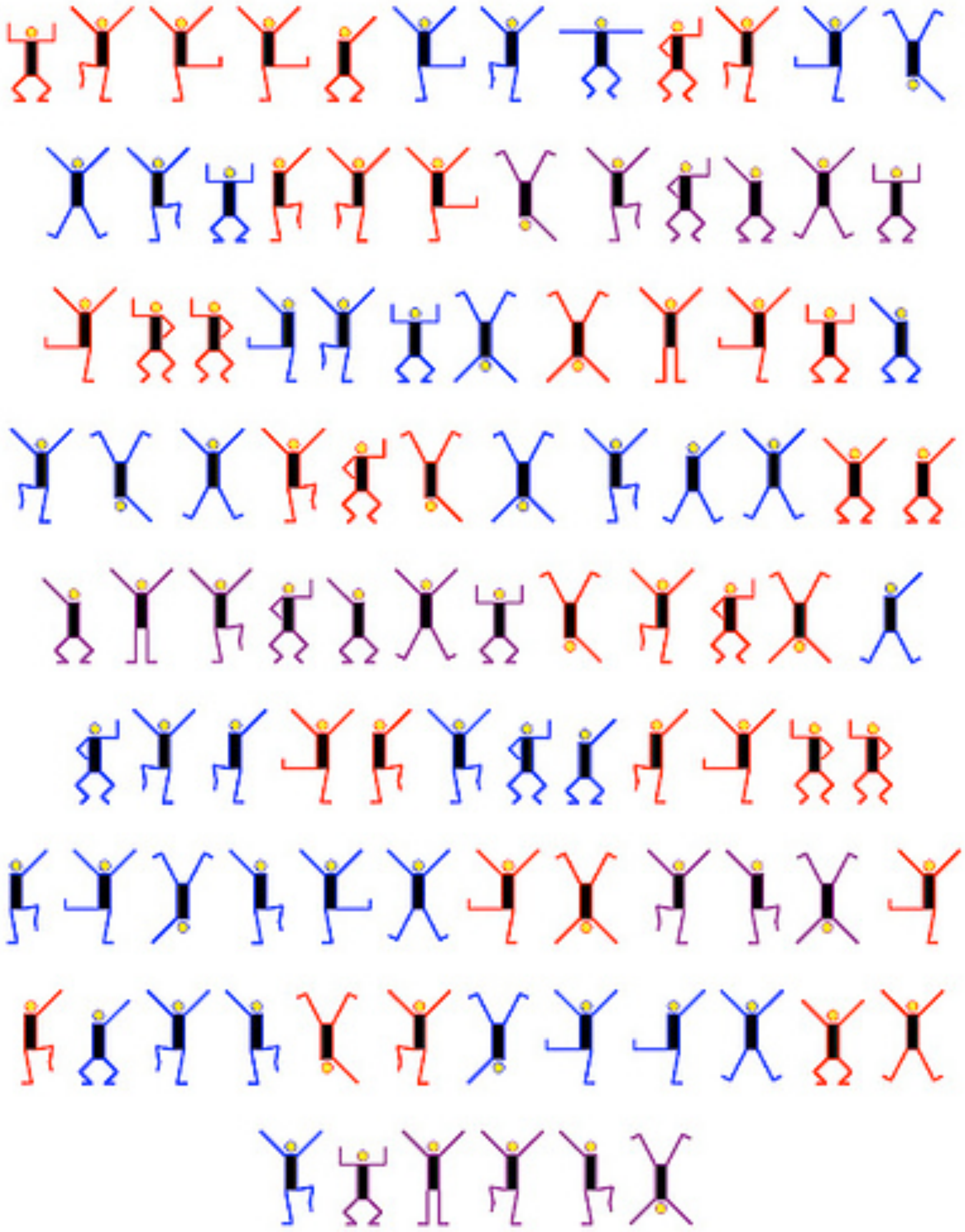
RECORDING CHOREOGRAPHIC INSTRUCTIONS

Classical ballet – sets of dancing postures.
Less structured in 20th century ballets (e.g. Stravinsky)
Modern ballet (Pinna Bausch, Ohad Naharin) passed on by teachers.



The scripts are pictorial, and indicate body postures,
yet also highly dependent on additional information, passed from teacher to students





Choreographic documentation reminding of hieroglyphs or Semaphore,
but no uniform signs system established.
Each choreographer has personal nuances understood by his coworkers, and the scripts are more like a reminder.

ENCRYPTION

TRANSLATION,
ENCODING & DECODING

ENCRYPTION (cryptography)
and translation between languages

Writing is the encryption of speech. Interpreting text of unknown language is therefore challenging. It is required for understanding archeological scripts, and typically starts by recognizing repetitive words which meanings are guessed, and from it continue to expand the “dictionary”. Steles that scripted the same “message” in several writings helped decipher ancient scripts.

Cicero’s secretary was first known stenographer, a fast “short hand” scripting of talk.

Encryption of text to keep it secret from unwanted readers was commonly used during wars (sending secret messages). The Enigma machine was a modern method to transfer openly on radio encrypted messages with changing letter mixing. Encryptology became a vivid field with many applications in our digital world, for commerce, banking, information security etc.

From Simon Singh’s book “the Code”

Stenography – concealing a message

Xerxes, the Persian king, drafts a huge army and builds a large fleet in order to evade Salamis bay near Athens. Demaratus, a Greek that evidenced Xerxes preparations, scrapes a message in wood covered with bee’s wax, and sends to Athens, where they melted the wax, read the warning, and started to build their defense ships. Silver mines profits, at peace time donated to all citizens of Athens, were confiscated for the war efforts, and a fleet of small and fast ships was built. They attracted the heavy Persian boats into the bay, and sunk them.

Pliny describe secret ink, prepared from the plant Thithymallus that is unseen, but turn brown while heated.

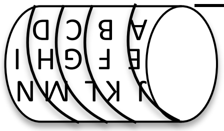
Chinese scripted messages on silk, squeezed to a small ball coated with wax and swallowed by the messenger.

Giovanni Porta wrote on egg shell with a solution of salt and acetic acid. The script can be read on the hard-cooked egg after pealing the shell.

During the second world war messages were shrunk to a point by microphotography, and read under a microscope.

Transposition - is a common encryption method: e.g. inverse letter order in each word, or sentence, and listing even then odd letters.

Spartan Scytale – writing on leather cylinder and cutting it to make a belt.



Substitution – exchange each letter with another, either in pairs, or group of n-letters (used by Julius Caesar).

Al Kindi – describes deciphering codes by the frequency of letter usage. Need long text to establish statistical significance.

Willingham, Elisabeth security minister, decodes letters from Marry, queen of Scotts, and she is accused of treasury and prosecuted.

Leon Batista Alberti of Florence – double encoding

Blaise de Vigenére , 1543 – invents encoding using Vigenére square.

Charles Babbage wrote a computer program that decoded Vigenére square.

Morse telegraph and **Marconi** radio brought encryption art to the front.

Alan Turing decoded the Enigma messages through the repeated “Heil Hitler”

Encryption by computers (details in 20th century chapter)

Lucifer – a mincing machine

Dipi & Helman –

Rivest–Shamir–Adleman - public key for code encryption

Digital signature

Computer viruses, Trojan horses,

Encoding computer data and demanding ransom for decoding back.

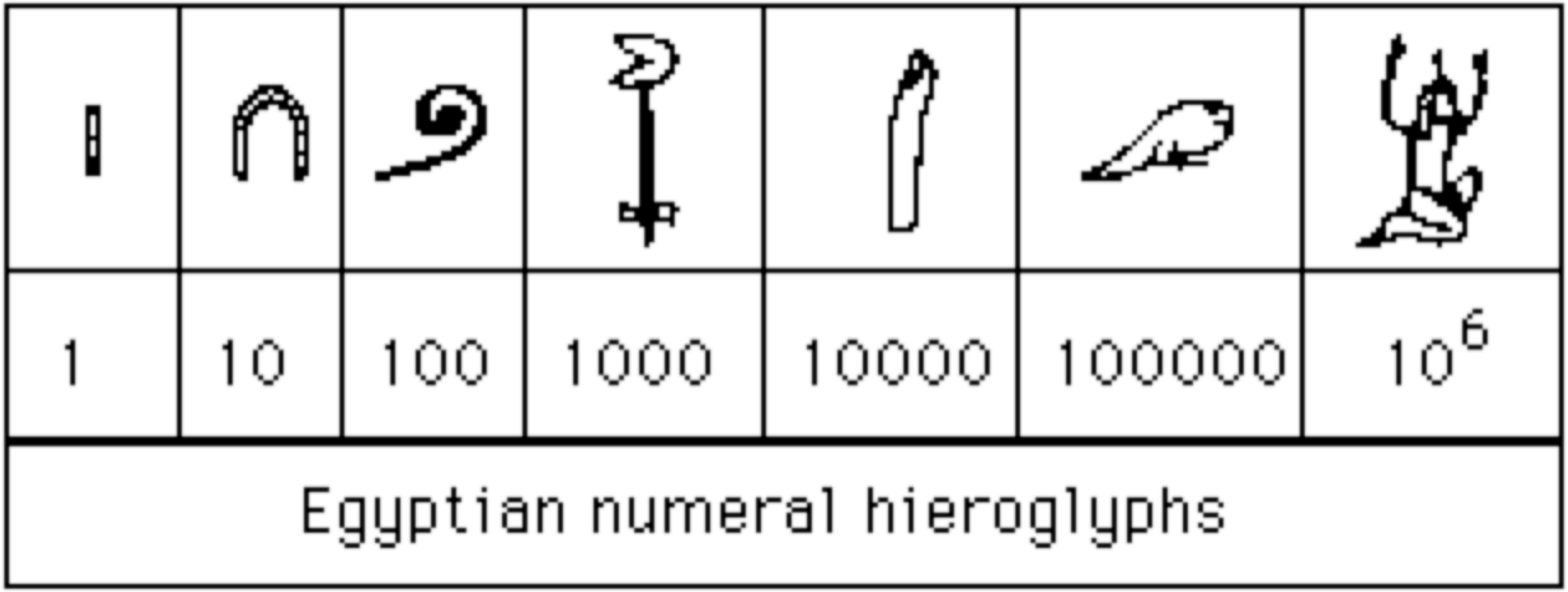
Enigma – the Nazi encoding machine, was decoded by the British (in fact by Alan Turing in the British team).

It is based on letter-to-letter transformation, but the changed the letter transformation after each transmitted letter, using a gear mechanism.

WRITING NUMBERS

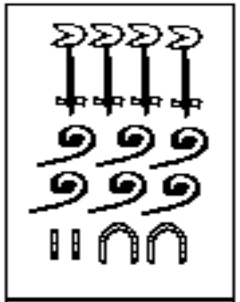
Egypt

Counting integer numbers. Simple duplication I II III IIII
Becomes difficult to read, therefore signs were defined for decimal powers
Probably motivated by counting with 10 fingers.
As seen in the lower tables, there is no significance to positions.

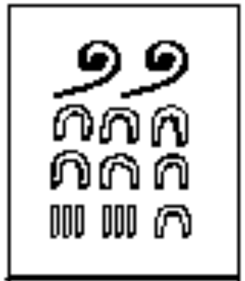


𓏺	𓎆	𓍢	𓆼	𓂭	𓆐	𓁨
1	10	100	1000	10000	100000	10^6

Egyptian numeral hieroglyphs

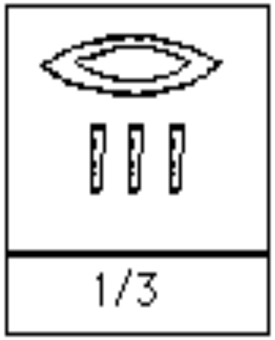


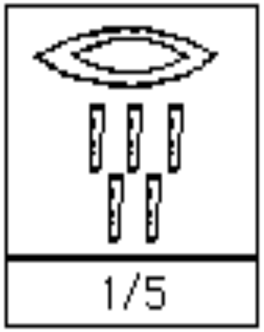
4622

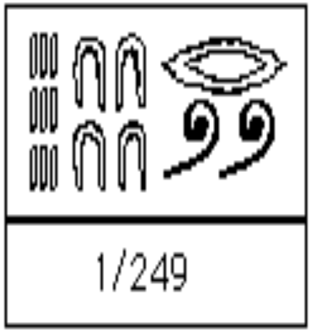


276

SIGNS FOR FRACTIONS

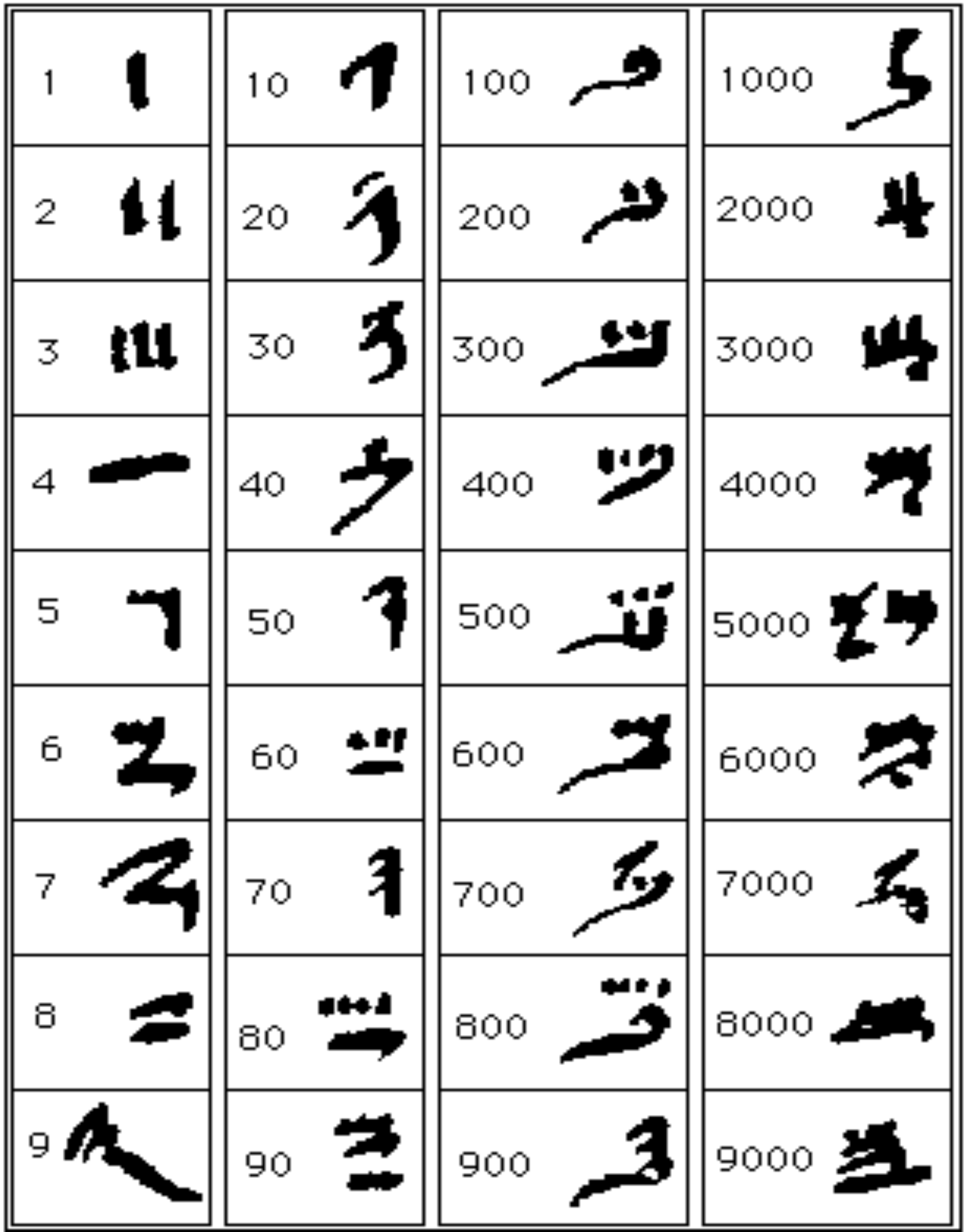




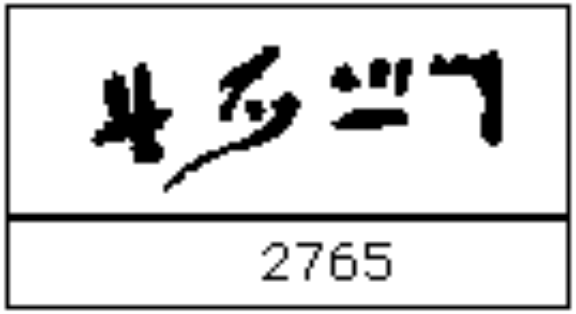


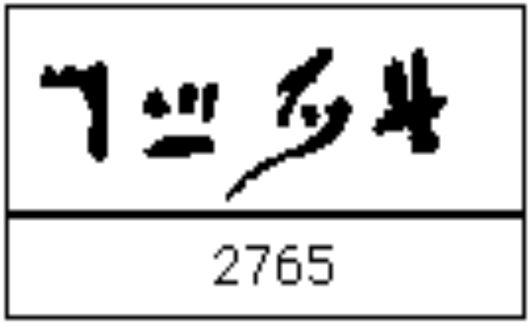
How a pile of wheat grains is divided into 5 ?
Iterative guesses, much like one adds or deletes tomatoes from a balance in the market…
Iterative method was also used as division algorithm: guess the answer to the quotient, e.g. 358/17, and multiply by 17, incrementing or decrementing the answer multiplying with the nominator, until closest to the denominator.
Multiplication algorithm is by repeated addition.

Scripting numbers on papyrus:
9 signs for each decade.
What is missing ?


1
2
3
4
5
6
7
8
9
10
20
30
40
50
60
70
80
90
100
200
300
400
500
600
700
800
900
1000
2000
3000
4000
5000
6000
7000
8000
9000

Hieratic numerals





Arbitrary order

Rhind papyrus - aka the Aumes 1680-1620 BC

Includes division algorithms and 87 numerical problems, including solution of equations: Volume of wheat silos, and approximation (progression) methods.

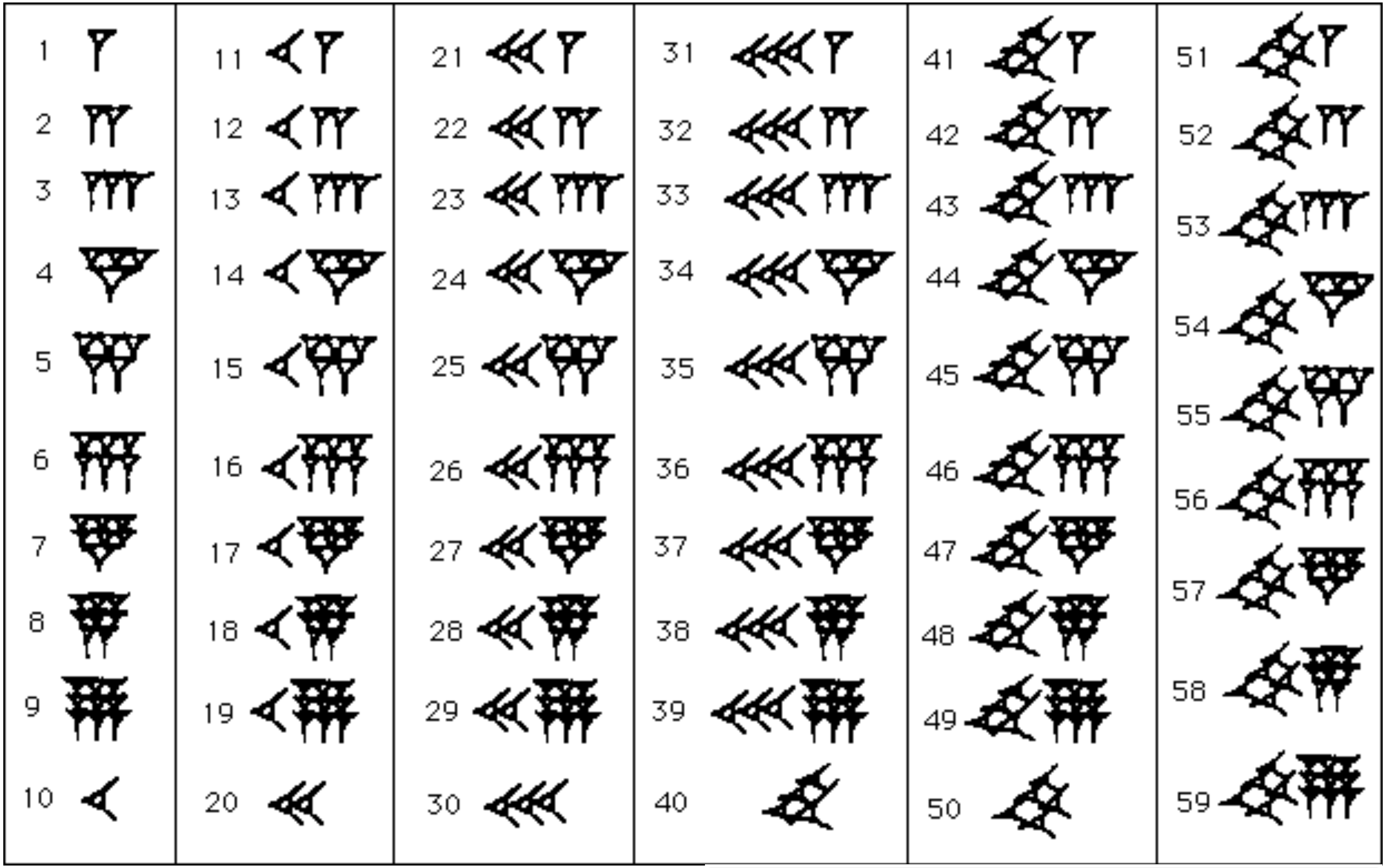
MESOPOTAMIA

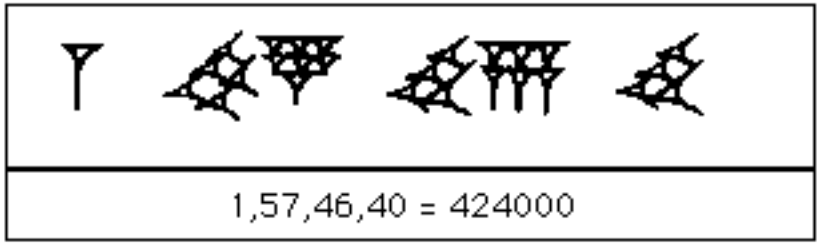
Pegs script on soft clay that dries and solidifies. Here listings of irrigation channels, quantities delivered in convoys, number of workers and their fees, taxes & mailed letters.

Sumer – 3500 BC
Accad – 2300 BC
Babylon – 2000 BC

Number scripting with **base of 60**: 59 signs

Position-significance: Right: units, Left to it: multiples of 60, then multiples of 3600 etc.





1,57,46,40 = 424000

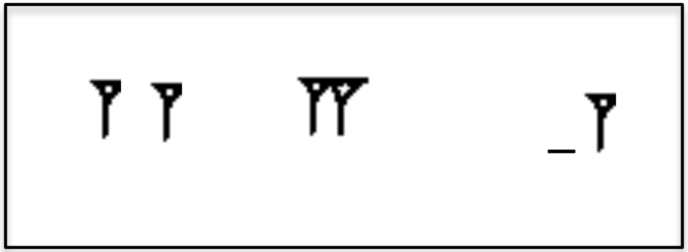
1*216000 + 57*3600 + 46*60 + 40 = 424000

Problems:

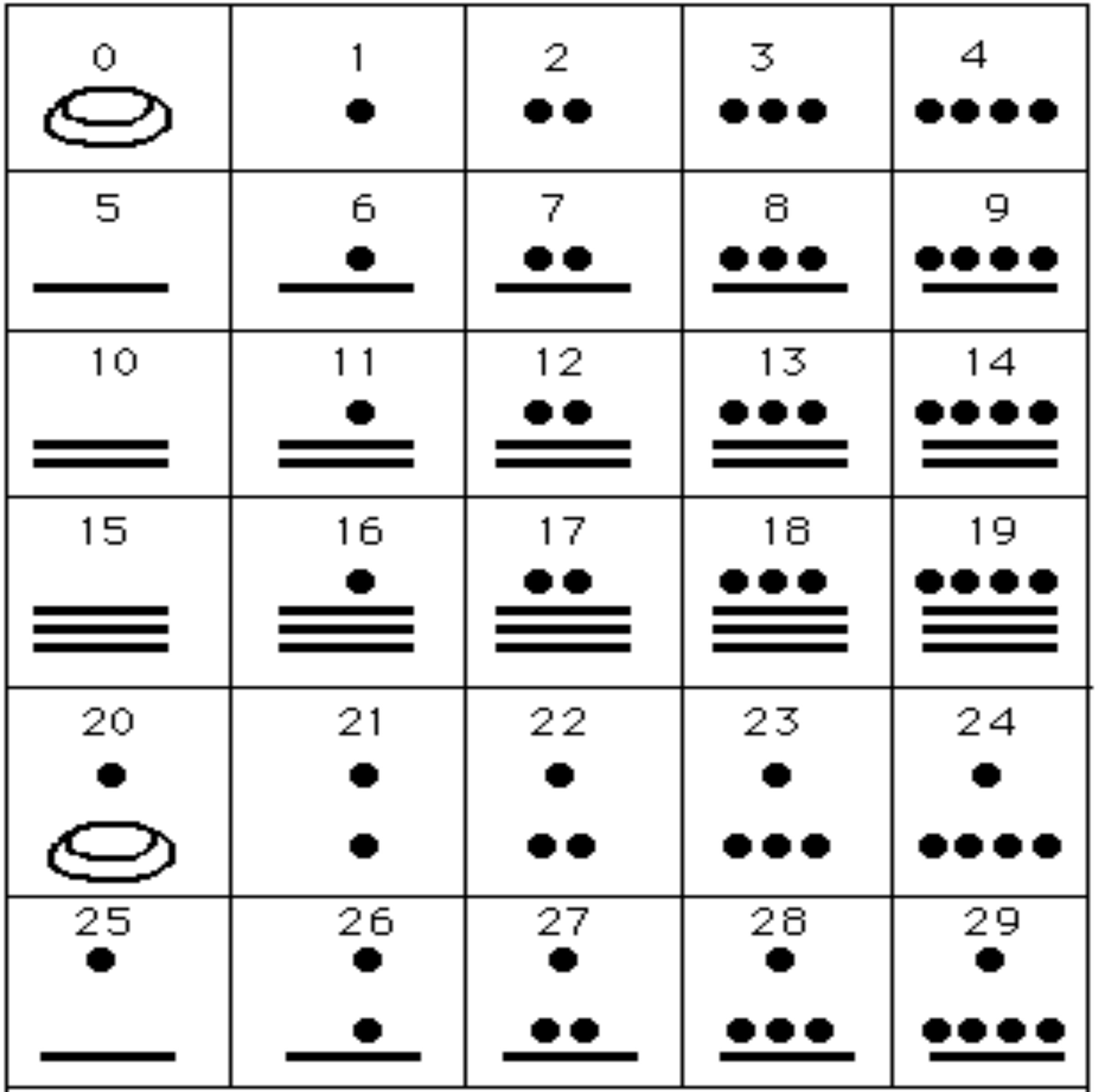
When there are no units (e.g. 60) a line is added left of the 60 sign.

Still: hard to discriminate between 2 and 61

Try to solve by spaces:



MAYA – Numbers base 20, including zero, and position-significant system.
Written up-down. Simplifies adding numbers.
But no fractions. Puzzling: how did they calculate year length with such high accuracy?



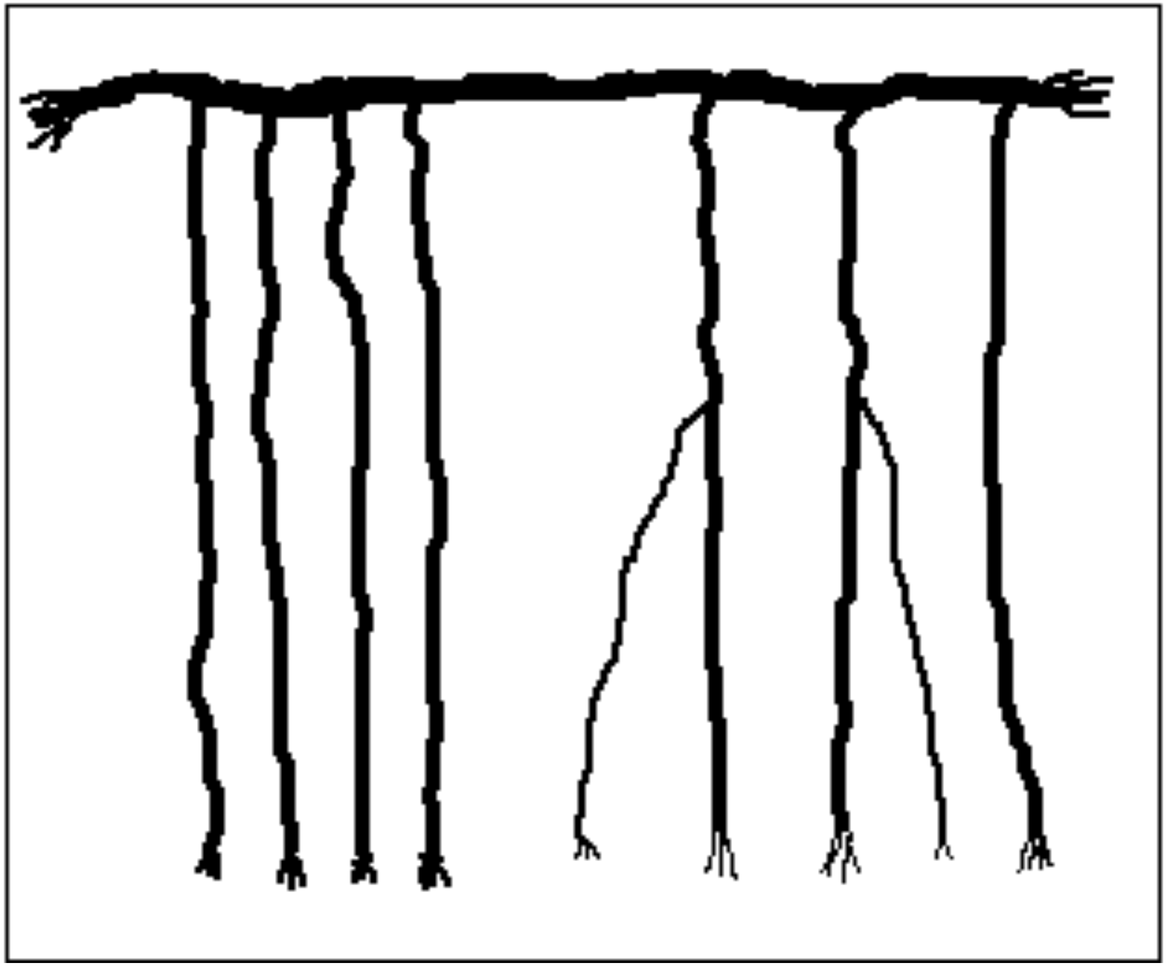
Mayan positional number system

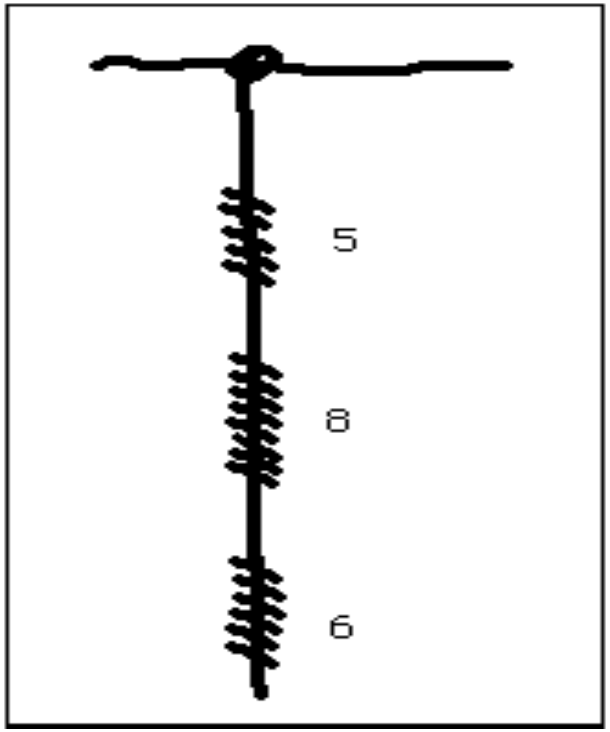
INCA

Spaniard found a well organized empire, central government, communication roads, agriculture, textile industry, but no script !!!

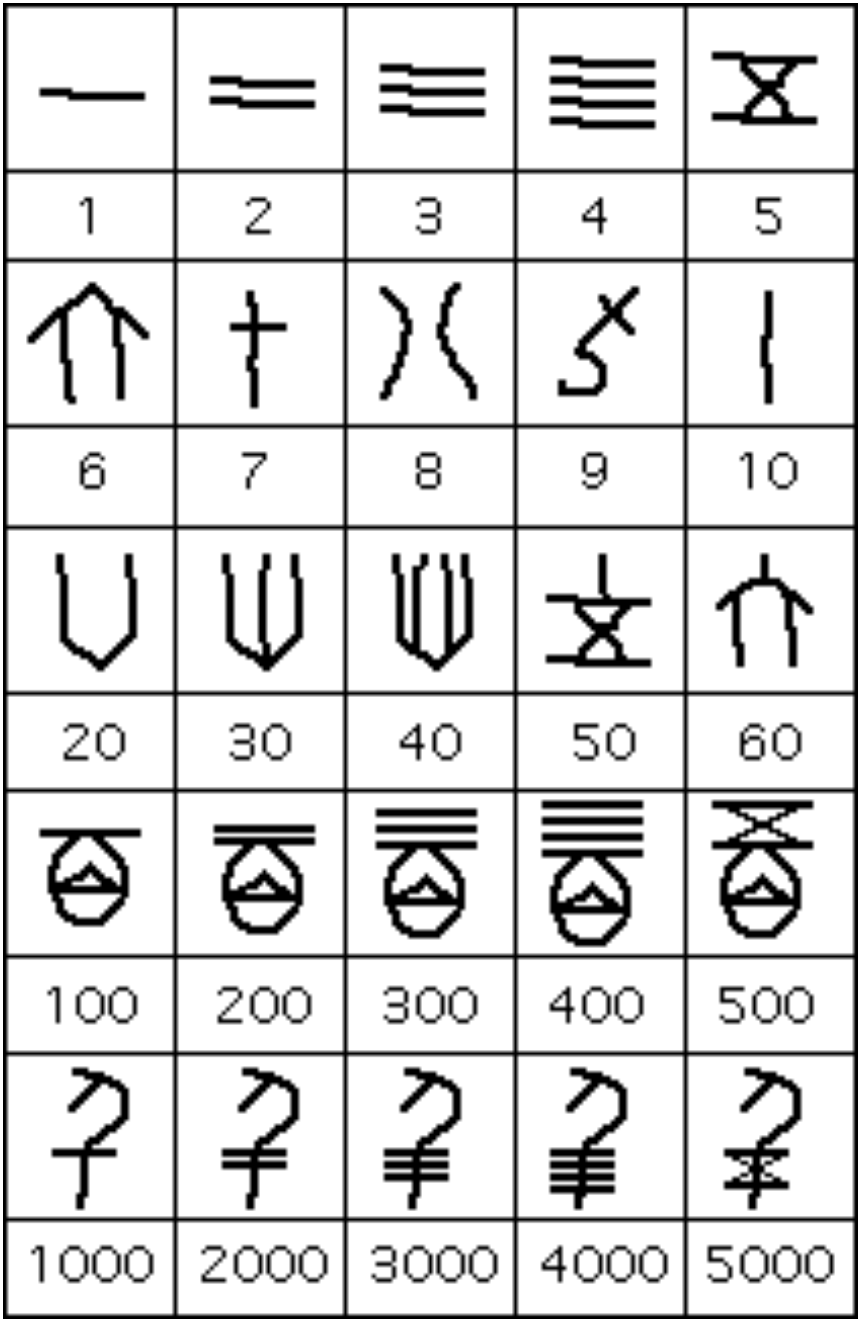
Administrative listing used **Quipu**, string knots system: Each knot is a number, position significant, and zero is space.

The color of the string encodes the objects counted: Animals, weapons, money.





Chinese number system – similar to Greek-Roman



1	2	3	4	5
6	7	8	9	10
20	30	40	50	60
100	200	300	400	500
1000	2000	3000	4000	5000

Zhu Shijie Imported zero from India . It is included in a mathematics book by **Ch'in** from **1303 AC**

Chinese mathematics discussed lot measurements, grain commerce, direct and inverse proportions between length measurements, area and volume calculations (applied Cavaliery's principle to calculate the volume of a sphere), civil engineering of channels, bridges, astronomical pyramids, quadratic interpolation of star locations.

See: Chinese problems

NUMBERS IN THE CLASSICAL WORLD have almost not changed from ancient Greece to Rome. Basis 10 (decimal system), position-significant (IV vs. VI) and minimal number of signs

IV=4 VI=6 IX=9 XI=11 XC=90 CX=110

1= I 5= V 10=X 50=L 100=C 500=D 1000=M

I	II	III	IIII	𐅃	𐅃I	𐅃II	𐅃III	𐅃IIII	Δ
1	2	3	4	5	6	7	8	9	10

1 - 10 in Greek acrophonic numbers

𐅃	Δ	Η	Χ	Μ
Pente	Deka	Hekaton	Khilioi	Murioi
Πεντε	Δεκα	Ηεκατον	Χιλιοι	Μυριοι
5	10	100	1000	10000

Δ	𐅄	Η	𐅅	Χ	𐅆	Μ	𐅇
10	50	100	500	1000	5000	10000	50000

Higher numbers and combining acrophonic numerals

170 BC – **Pergamum**- writing on processed leather skins replace papyrus: better preserved. Hebrew scripts on skins have preceded Pergamum.
105 AC – **Tsai Lun**, in the court of the emperor **Han Ho Ti**, China: invention of paper.
1150AC – First **paper mill** in Europe.

INDIA

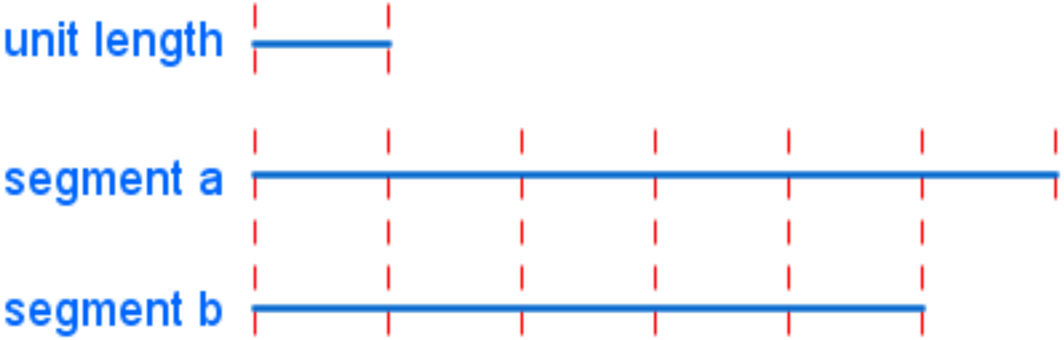
300 BC – Pingala describes binary number system
1854 AC – Boolean algebra in Europe
260 BC – Arabic numerals from India adopted by the Arabs, and moved to Europe by **Fibonacci**
150 BC – Sthananga Sutra - an extensive mathematical composition (sutra=idea)
3 AC – Invention of the Zero

It took 1000 years of European mathematics to adopt the zero from other cultures, while Babylonians, Indians and Maya, undoubtedly independent culture, applied zero early in their development of mathematic. Why?

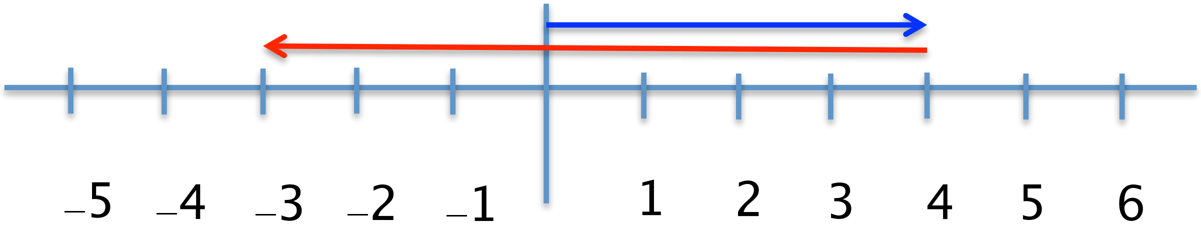
The reason must come from the practical use of mathematics: While the Babylonians and the Indians applied mathematical calculations (mainly for Astronomy), the Classical mathematicians considered their art as logical philosophical contribution, (e.g. axiomatic geometry). They used calculations with integers mainly for commerce and administration, and used geometry for multiplications and divisions.

EXTENSION OF NUMBER SYSTEMS:

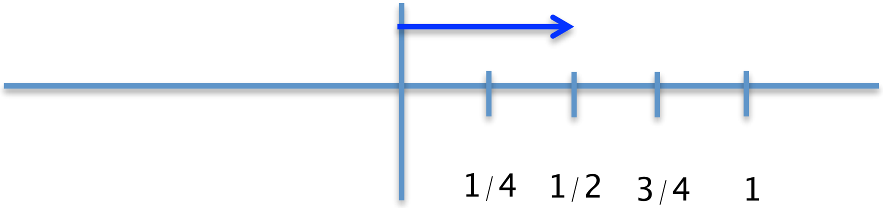
Integers: positive numbers for counting objects



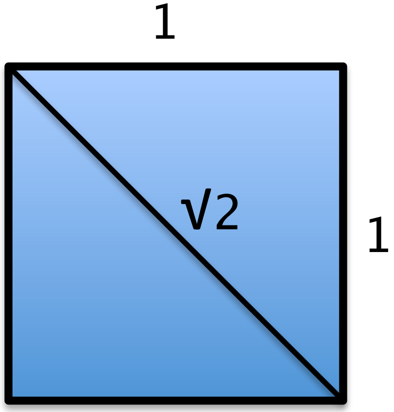
Negative integers: **100 BC in China**- first used to indicate debts of a number of objects. **Diaphanous** ignored negative solution to equations

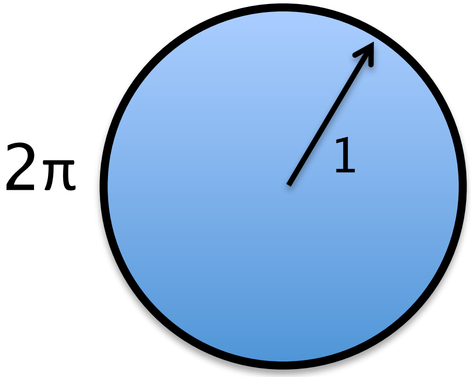


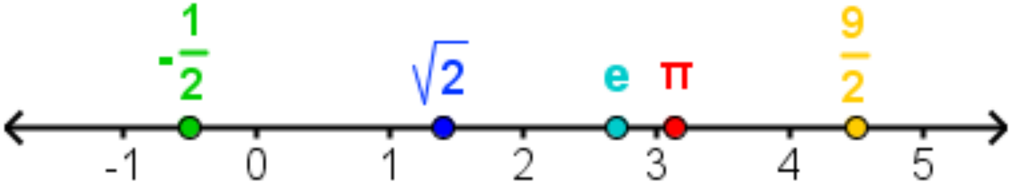
Fractions (rational numbers): indicating parts of a whole object, such as half length etc.



Irrational numbers: emerged from the length of the hypotenuse in right angle triangles, or the perimeter and area of circles. Such numbers got increasingly accurate values, but the proof that the value cannot be presented by rational numbers was only given during the middle ages







Very large and very small (infinitesimal) numbers: Archimedes devised a method to write large numbers base on 10^8 , see following slides.

In a computer, “floating point format” allows to express numbers larger than permitted by a finite number of digits: the computer word is segmented into two groups of numbers: the basis and the exponent.

1110110 | 10010110010100

The basis is always scaled to start with 1.

We shall come back to the concept of infinitesimal values in “calculus”.

Algebraic presentation: an expression of symbols that can be substituted by any number, e.g.2x+3

Transcendental numbers: numbers that cannot be a solution of an algebraic equation with rational numbers. They are typically calculated by infinite sums.

Complex numbers: numbers that come up from fractional powers (such as square root) of rational numbers.

We see that fields of number must be extended in order to solve problems defined inside the field:
Subtraction of integers creates negative numbers.
Division of integers create rational numbers.
Fractional powers and geometry creates irrational and complex numbers.
Arbitrarily large or small values and infinite sums converge to transcendental numbers.

SUMMARY

Integers
1,2,3, ...

Negative numbers

Zero

Positive numbers

Real numbers

Rational numbers
342 / 1673

Irrational numbers
$\sqrt{2}$

Transcendental numbers
$e \quad \pi$

Imaginary numbers
$\sqrt{(-1)}$

IMAGINARY NUMBERS

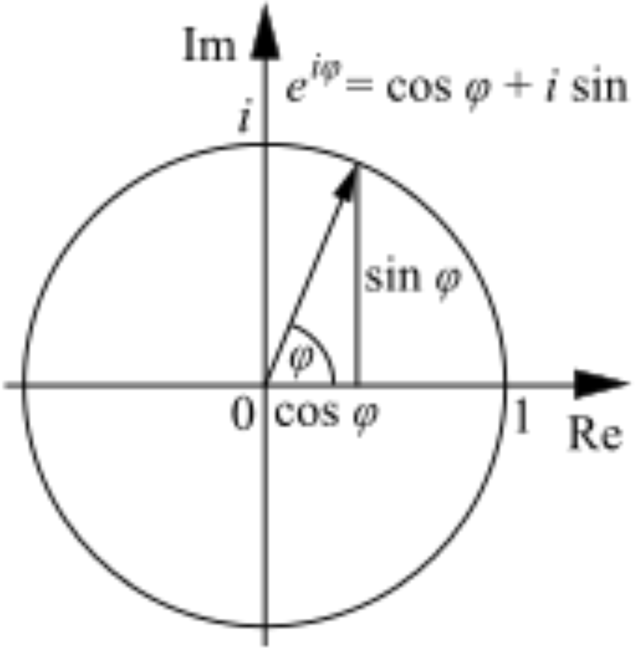
$$e^{ix} = \cos x + i \sin x,$$

$$\sqrt{(1)} = \pm 1$$

The sign i was first used by **Rafaello Bombelli**

$$\sqrt{(-1)} = \pm i$$

Imaginary numbers can be presented as
2D vector with length R and angle φ



$$e^{i\pi} = -1$$

$$\log_e(-1) = i\pi.$$

De Moivre’s formula

$$(\cos x + i \sin x)^n = \left(e^{ix}\right)^n = e^{inx} = \cos(nx) + i \sin(nx),$$

BABYLONIAN CALCULATION ALGORITHMS

Area of a lot = length * width

Multiplication tables are replaced with an algebraic equation and tables of squares:

$$ab = [(a + b)^2 - a^2 - b^2]/2$$

$$ab = [(a + b)^2 - (a - b)^2]/4$$

The advantage is that from a list of 10 squares of the numbers 1-10
we can calculate the products of all 100 pairs of these numbers

The square of the diagonal of a rectangular lot was calculated by: $a^2 + b^2$
Proceeding Pythagoras law by 1000 years

Table of fractional numbers help calculations:
The adaptation of the basis of 60 may come from the factors to 60: 1,2,3,4,5,6
making their fractions simple:

1/2 = 0.3
1/3 = 0.2
1/4 = 0.15
1/5 = 0.12
1/6 = 0.1
but not 7 1/7 = 0.0834....
1/8 = 0.075

Irrational numbers were approximated by two numbers whose squares are above and below: e.g. : $c^2 = 2$ for 1.4142…

A value presented by periodic digits following the decimal point is rational: How can we find out the ratio?

$0.33333\ldots == 3/9 = 1/3$
$0.181818\ldots == 18/99$
$0.0018 == 18/9900$
$0.38181818\ldots == 38/100 + 18/9900 = 19/50 + 1/550 = (209+1)/550 = 210/550 = 21/55$

The proof is from the sum of an infinite geometrical series:

For every q: $1 + q + q^2 + \ldots q^{n-1} = (1-q^n)/(1-q)$
For q<1, $n \rightarrow \infty$: $= 1/(1-q)$

For example:

$$0.333\ldots = 3/10 + 3/100 + \ldots = 3/10/(1-1/10)] = 3/9 = 1/3$$

Exercise: show that 0.999… = 1

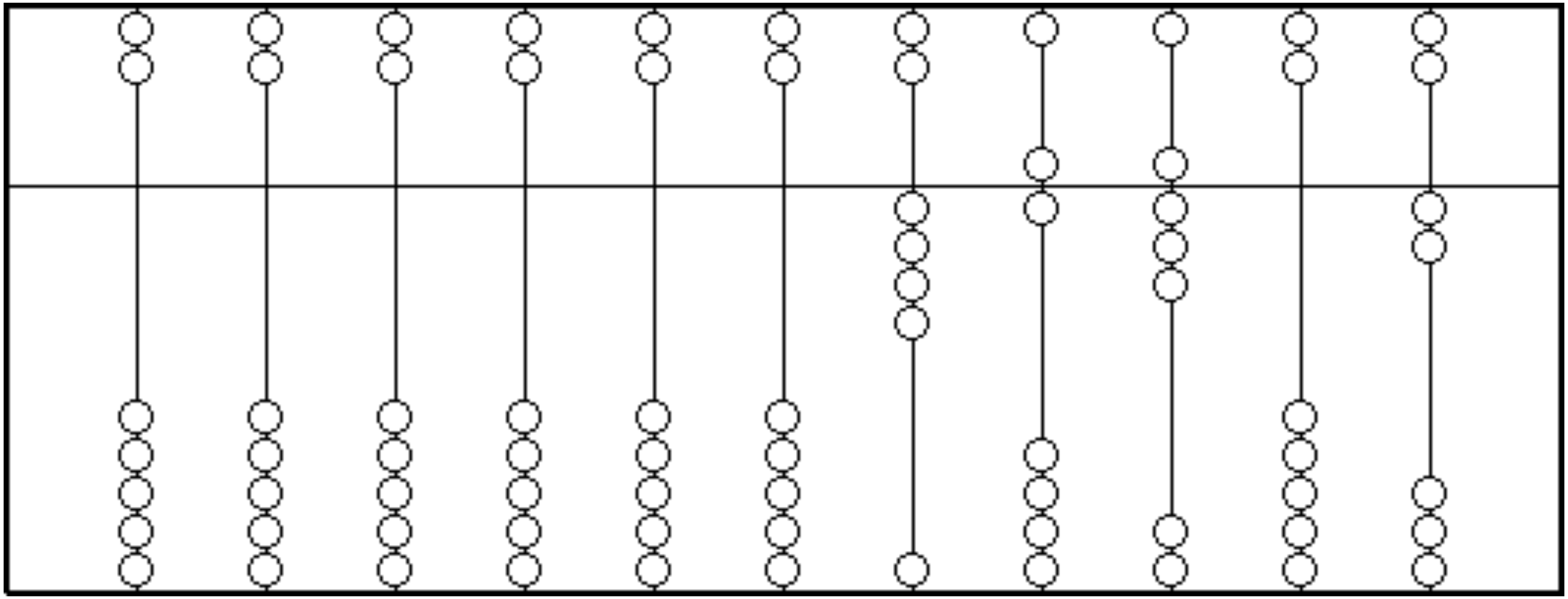
Therefore irrational values are not presented by periodic numbers.

THE ABACUS today: beads on strings in a wooden frame

Has a finite number of digits (like the computer).

What is the largest number that can be displayed with 11 rows?

How are negative numbers displayed?



What is the base for the above (Japanese) abacus?

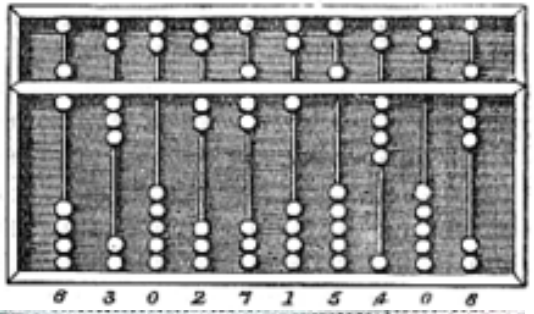
Can you define the rules for additions and subtractions?

Herodotus tells that the **Egyptians** manipulated pebbles from right to left, opposite to the Greeks. He may have referred to their Abacus, probably constructed from depressions in a stone wood or clay table. Wooden table with depressions and light & dark pebbles or stone figurines were Egyptian game structures, and are found in drawings.

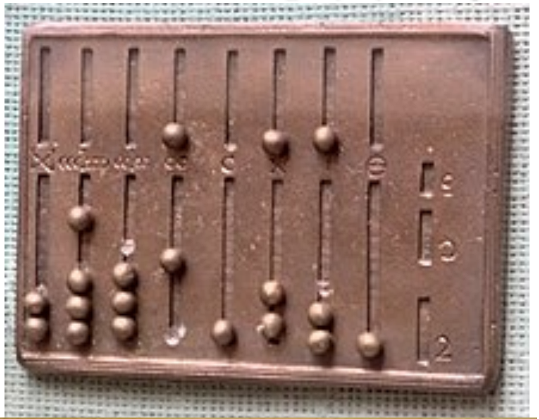
600 BC Persians started to use Abacus, and via trading spread its use to India, China and Rome.

Demosthenes 384 BC–322 BC in Athens discusses the need to “use pebbles in calculations too difficult for the head”

Chinese from ~200BC widely use abacus made of bamboo frame with 2 beads in the top part and 5 in the bottom

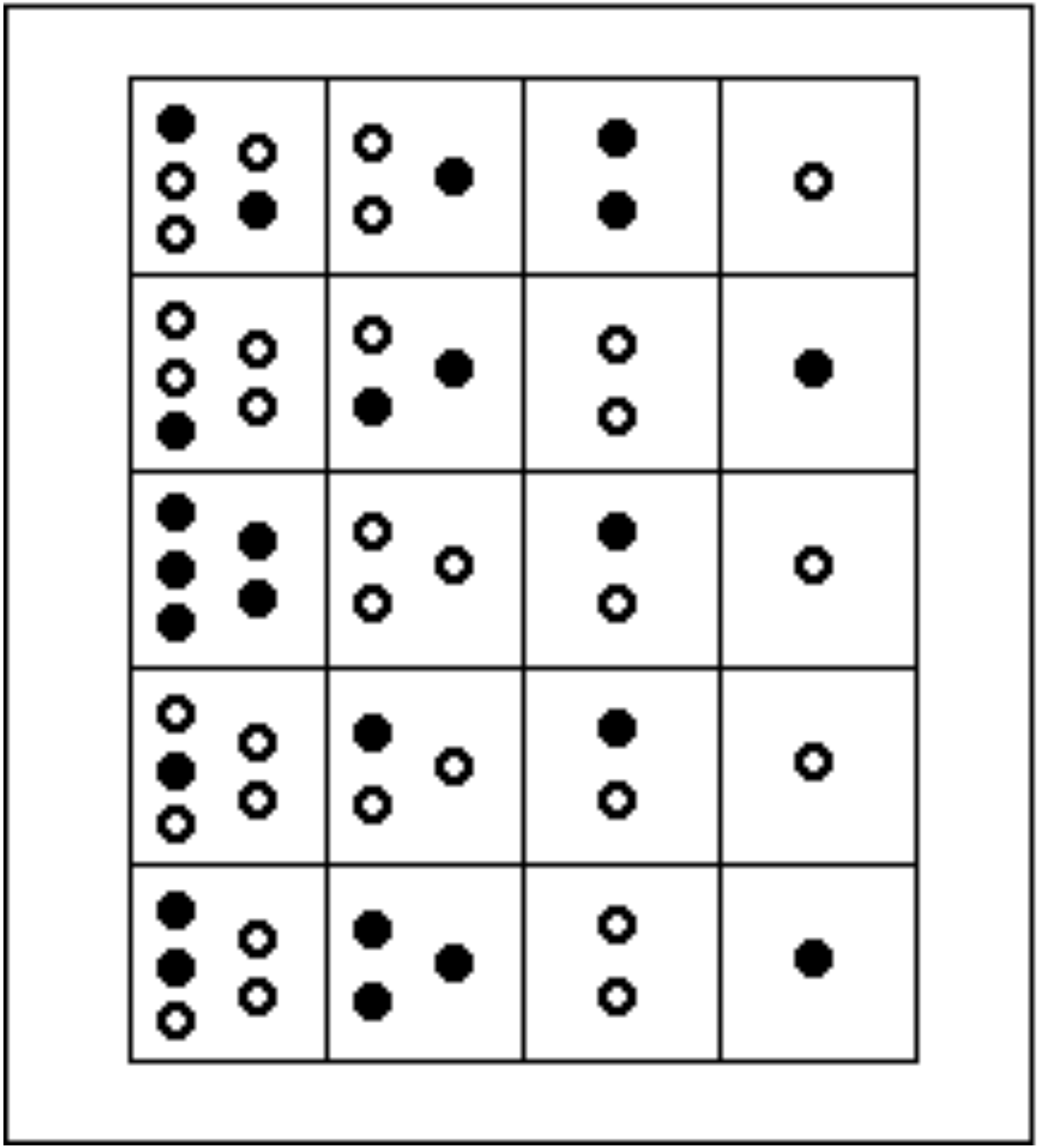


Romans made extensive use of abacus in commerce and Science. Pope Sylvester II reintroduced a modified abacus which spread its use in the whole of Europe.



The use of Abacus in **India and Japan (Soroban)** was documented from the 2nd century, and in Japan and Korea they are still used skillfully by school kids

Quipu, the Inca number register is a kind of abacus.



Maya abacus,
Corn grains on wood plate.
basis 20.
Can you describe the rules?

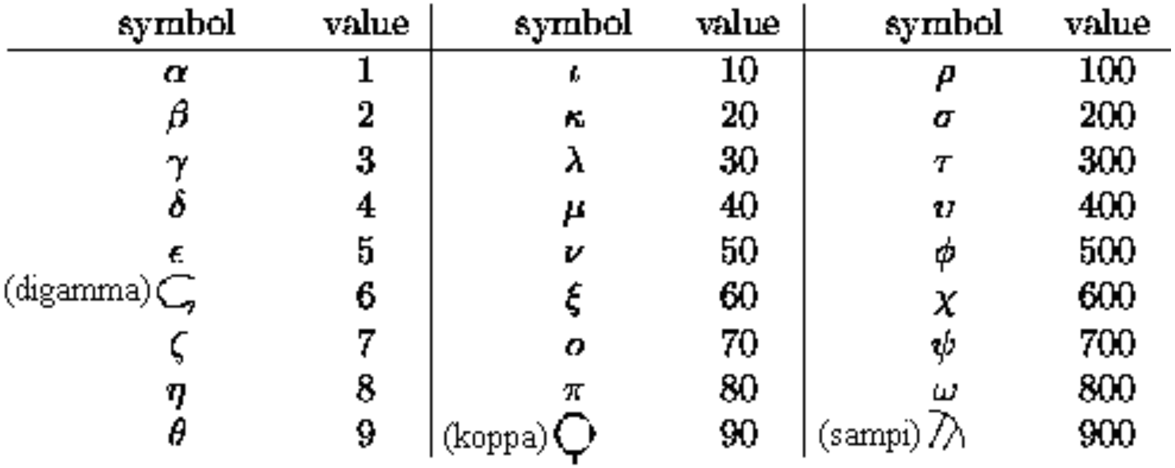
WRITING LARGE NUMBERS:

Based on $10^a * 10^b = 10^{a+b}$
The Greeks defined letters up to M=10,000 (M for Myriad meaning uncountable, like infinity).
Archimedes assigned the 1st myriad to numbers in the range 1-10^8

2nd myriad to the range $(10^8)^{(10^8)} = 10^{8 \cdot 10^8}$

3rd myriad to $\left((10^8)^{(10^8)}\right)^{(10^8)} = 10^{8 \cdot 10^{16}}.$

He used these assignments to write the number of sand grains in the world, in terms of our present notation:
$8x10^{63}$



symbol	value	symbol	value	symbol	value
α	1	ι	10	ρ	100
β	2	κ	20	σ	200
γ	3	λ	30	τ	300
δ	4	μ	40	υ	400
ϵ	5	ν	50	ϕ	500
(digamma) ϛ	6	ξ	60	χ	600
ζ	7	o	70	ψ	700
η	8	π	80	ω	800
θ	9	(koppa) ϙ	90	(sampi) ϡ	900

$$\sigma\pi\zeta = 287$$

$${}^{\prime}\gamma\sigma\pi\zeta = 3287$$

$$M^{\epsilon} = 50,000$$

$$M^{\alpha\beta}\sigma\pi\zeta = 120,287$$

ALGORITHMS

ALGORITHM (and ALGEBRA)

Are named after Al-Jabr (الجبر), an Arabic composition on algebra written by **Muhammad ibn Musa al-Khwarizmī 820 AC**

An algorithm is a prescription for carrying a specific calculation, applicable to any number.
e.g.: addition, multiplication or division of two numbers.

Here is an iterative algorithm for calculation of the square root, based on the equation:

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

By inserting the result of the previous step in this equation repeatedly, an improving solution is obtained:

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

For example, start with the approximation: √ 2 ~ 1.5

1.4 =2.5/ 1+1

1.4167=2.4/ 1+1

1.4138=2.4167/ 1+1

Where the value is:

√2 = 1.41421356

A Babylonian iterative algorithm for square root:

If A is an approximation for $\sqrt{Q}$ then $B=(A+Q/A)/2$ is a better approximation.

If $A<\sqrt{Q}$ then $\sqrt{Q}-A > \sqrt{Q}-B=\sqrt{Q}-(A+Q/A)/2$ and $-A/2 > -Q/A/2$ therefore $A^2 < Q$

If $A>\sqrt{Q}$ then $A-\sqrt{Q} > B-\sqrt{Q}=(A+Q/A)/2-\sqrt{Q}$ and $A/2 > Q/A/2$ therefore $A^2 > Q$

Same example: $\sqrt{2}$~1.5

1.41667=2/(1.5+2/1.5)

1.4142156=2/(1.4166+2/1.4166)

Closer to the true value after 2 iterations than the previous algorithm:

$\sqrt{2} =$ 1.41421356

Algorithm for square and cube roots:

At any stage the number of digits after the point are correct.

Segment the number into pairs (triples for cube root) from the least significant.

First square (cube) root of most significant pair (triplet), and subtract. Then repeatedly, add next pair (triplet) and subtract largest possible x*[20 (or 30)*the last result + x]. Add digit x to last result and repeat.

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

Square root

```
 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
```

Cube root

```
  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
```

PRIME NUMBERS

Primes are integers with only 1 and themselves as factors.
Factor of an integer is a divider with no remnant.

The basic theorem of arithmetic: Every integer can be uniquely factored (ignore order of factors).

325-265 BC Euclid – proved that there are an infinite number of primes.
Here is the proof: It is an example of the mathematical logics perfected by Euclid:

Assume p_m is the largest prime, the preceding primes are: $p_1,p_2,p_3 \dots$ The number $P=1+p_1*p_2*p_3*\dots.*p_m$ is a prime, or has a factor q. If a prime, it is larger than p_m denying our assumption. If q is a factor, it cannot be one of our m primes, because the difference between two integers with factor q is also divisible by q, but the difference $P-p_1*p_2*p_3*\dots.*p_m=1$ has no other factors than 1, therefor P is a prime.
This can be repeated infinitely.

How can we find out if a number P is a prime?

1. Check if it divides with all smaller integers.
2. Sufficing to check till √P

Facilitated if you generate a list all primes till √P

Sieve of Eratosthenes(276–194 BC

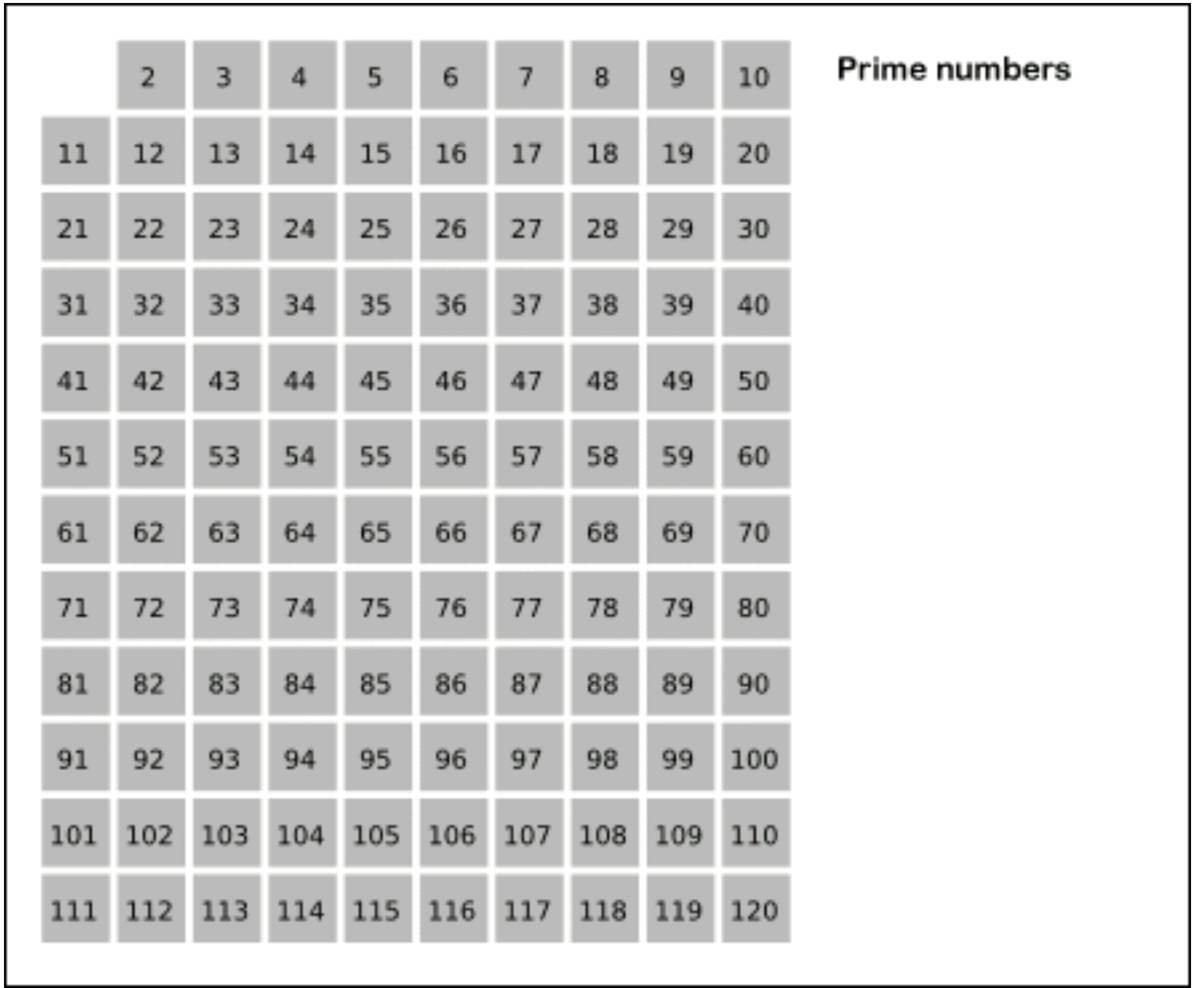
An efficient method to list all primes up to N:

Write all numbers 1 till N.

loop on P_m=2 … √N that was not yet erased.

Erase all numbers $P_m P_m$, (P_m+1) … in the list,

the closest number larger than P_m that was not erased is the next prime number.



	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

The largest common factor (GCD) of two integers

1. Brute force: list all factors for the two integers A & B and compare.
2. Better: Find all factors up to the smaller of the two integers.
3. Even better: Find the common factors up to the square root of the smaller integer.
1. Specially smart: Euclid’s algorithm.

If A>B than GCD(A,B)-GCD(A-B,B) (prove!)

Use this iteratively.

For example: 867 & 1989:

$$GCD(1989,867)=GCD(1989-867,867)=$$
$$=GCD(1122,867)=GCD(1122-867,867)=$$
$$=GCD(255,867)=GCD(255,867-255)=$$
$$=GCD(255,612)=GCD(255,612-255)=$$
$$=GCD(255,357)=GCD(255,102)=$$
$$=GCD(255-102,102)=GCD(153,102)=$$
$$=GCD(153-102,102)=GCD(51,102)=$$
$$=GCD(51,102-51)=GCD(51,51)=51$$

Indeed:

867=51x17 1989=51x39

Graphically the process is clearer:

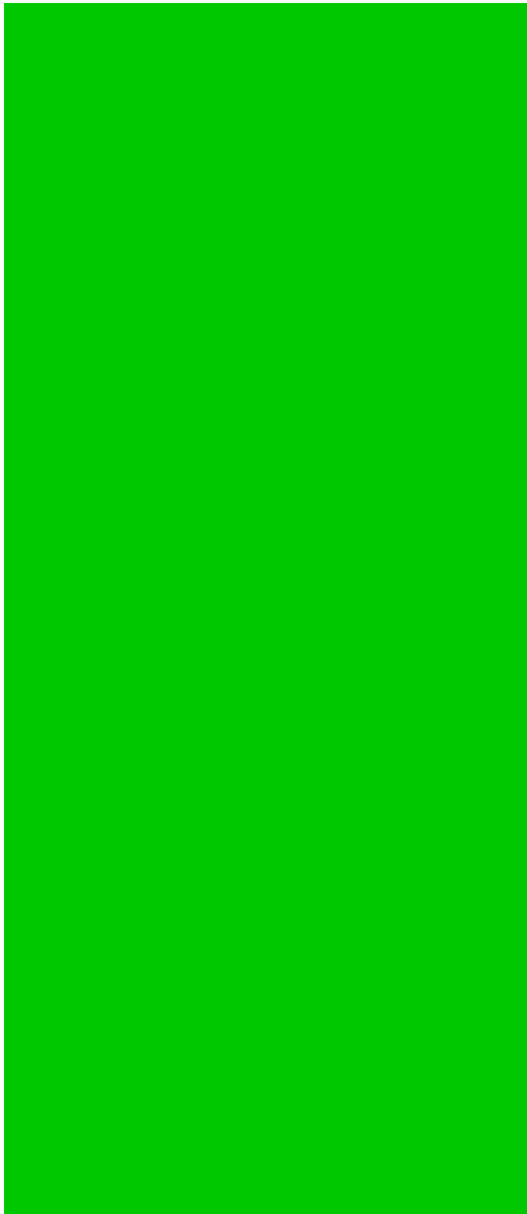
Rectangle edges 1071 & 462 (green)

Fit inside two yellow 462x462 squares

Remaining 462x147 fits in three blue 147x147 squares

remaining 21x147 fits in seven red 21x21 squares

Therefore 21 = GCD(1071,462)



APPLICATIONS FOR PRIMES:

Although number theory was considered pure mathematics, computer age brought two very important applications: 1. pseudo-random numbers, and 2. cryptographic keys.

1. Generation of pseudo-random series of numbers:

Given a large prime (e.g. 5761) generate 15 bit pseudo-random integers by repeated use of the equation (% denoted the remnant of the division by 2^{15}=65536):

Iseed = (iseed*5761+999)%65536

For random numbers in range [0,1]: iseed/65536

or: iseed = (iseed*8253729+2396403)%32767

The series order depends on the initial value of the "seed"

For 31 bit numbers: (2147483647=2^{15}) (ignoring overflow)

iseed=(iseed*16807)%(2^{31})

2. Cryptographic keys, for example Diffie–Hellman and Rivest–Shamir–Adleman (RSA). The best algorithms cannot find if a large number is a prime within a short time.
This is the basis of its use as a public key in the RSA encryption method: if we use a key that equals the multiplication of two large primes, they could not be found in reasonable time.

https://en.wikipedia.org › wiki › Diffie–Hellman_key_exchange

https://simple.wikipedia.org › wiki › RSA_algorithm

RSA ENCRYPTION

1. Chose two large primers, p & q
2. Compute n=pq
3. Compute) f =(p-1)(q-1)
4. The public key, e, integer with no common factor with f : GCD(e, f)=1 guaranteeing one-to-one correspondence
5. The private key : d.e= 1 mod(f)
6. A sends B the keys e,n and saves d
7. B sends A $c=m^e$ mod(n) to code m
8. A decodes $m=c^d$ mod(n)

An example with small numbers:
A choses: P=5581 q=8059
Therefore: n=5581*8059=44977279 f =5580*8058=44963640
Chose e=257 so that GCD(257, 44963640)=1 and send e to B
d=1 mod (7493940) /257 = 291593 is kept by A
B wants to send A the number m=123456
It is encoded to: $c=123456^{257}$ mod(44977279) =10526715
A decodes $m=c^d$ mod(n) = 10526715^{291593} mod(44977279) = 123456

ERROR CORRECTION

Transmission of digits may be interpreted erroneously due to noise. If the error probability is small, adding “checksums” can uniquely correct errors.

For example, if, in addition to 64 bits, sent as 8x8 binary numbers, we send 16 additional bits with parity of 8 rows and 8 columns, the red error can be repaired.

```
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   .
```

```
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   .
```

But these 4 errors cannot be corrected:

```
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   .
```

The following slides summarize a BBC series
About the charm of 8 special numbers,
And is brought here to show the beauty in mathematics…

Square root of 2

$\sqrt{2}$

Greeks loved geometry and symmetry. Yet they realized that some “nice” shapes display length that cannot be presented by rational numbers. The diagonal of the square is such an example. They found though progressive approximations to such numbers.

Consider the equation $m^2 = 2n^2$: they searched through tables of squares, and found pairs n,m that come closer and closer to this quality, e.g

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

They realized that:

1. the right number in each pair equals the sum of the pair above, e.g. $3+2=5$ $7+5=12$
2. And the left left numbers are the sum of the right number of the pair and the number above it, e.g. $2+5=7$ $5+12=17$

Proof: if $m^2=1+2n^2$ then also $(m+2n)^2 =?= 1+2(n+m)^2$

$$m^2+4nm+4n^2 =?= 1+2n^2+4nm+2m^2$$

$2n^2 = 1+m^2$ which is correct

Therefore $\sqrt{2}$ can be approximated by a rational number to any required accuracy. The convergence of an infinite series is the basis of infinitesimal calculus. (see Zeno turtle problem in the following)

We can prove that √2 is not rational (Pythagoras & Hipparchus)

Suppose we can write $\sqrt{2} = a/b$

We can reduce a & b till at least one of them is odd.

The square of an odd number is odd. But $a^2 = 2*b^2$

this implies that a^2 is even thus also a is even: $a=2A$

$b^2 = a^2/2 = 2A^2$ implies that b^2 is even too.

But this means that our assumption is wrong.

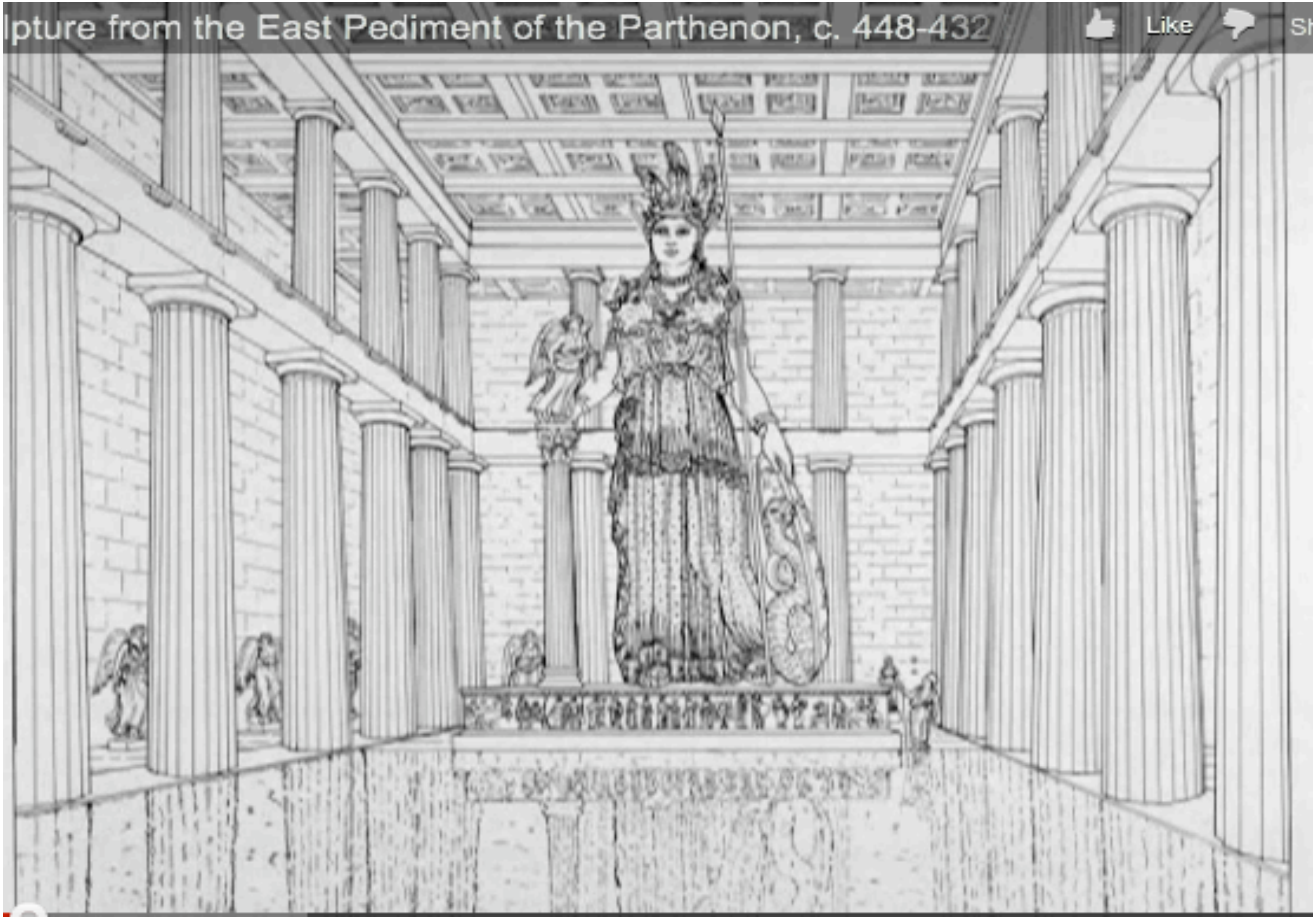
GOLDEN RATIO

GOLDEN RATIO φ = 1.618034…

Ratio between length and width or height of buildings that was considered esthetic by the Greeks. For example, the Parthenon in Athens, follows this rule.

Sculpture from the East Pediment of the Parthenon, c. 448-432 B

The assumed inside of the Parthenon, with a statue of Athens.



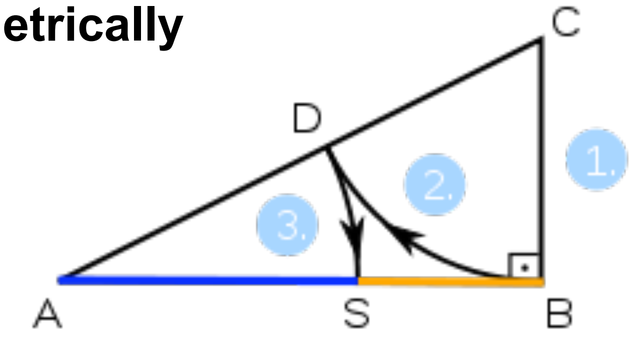
The golden ratio was defined geometrically

1. Right angle triangle with AB=2*BC
2. Using a compass, fix point D so that CB=CD
3. Fix point S so that AD=AS

S splits AB by the golden ratio.

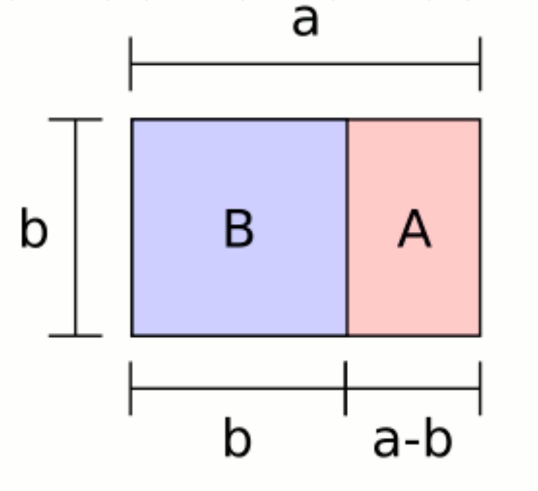
AB/AS=AS/SB=SB/(AS-SB)

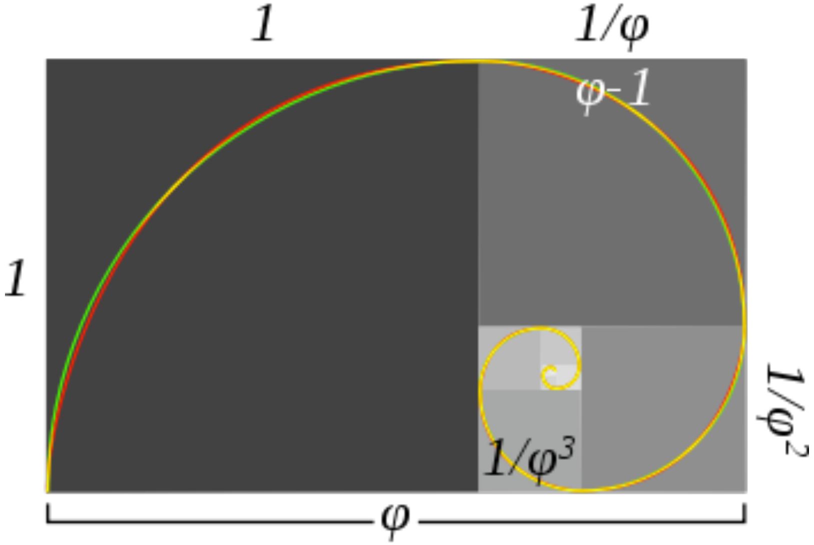
or: $\varphi = (a+b)/a=a/b=b/(a-b) = 1/(\varphi-1)$



Proof: $BC=1$ $AB=2$ $AC=\sqrt{5}$ $CD=1$ $AD=\sqrt{5}-1=AS$ $SB=3-\sqrt{5}$ $AS/SB=?=SB/(AS-SB)$

$(\sqrt{5}-1)/(3-\sqrt{5})=?=(3-\sqrt{5})/(\sqrt{5}-1-3+\sqrt{5})$ => $(\sqrt{5}-1)(\sqrt{5}-2)2 =?= (3-\sqrt{5})^2$ => $2(5-3\sqrt{5}+2)=9-6\sqrt{5}+5$: true





If a rectangle with edges a,b obeying $\varphi=a/b$ and we cut out the blue square bxb the remaining red square edges ratio is also golden

This is the basis of construction of the spiral linking circular arcs with radii $1/\varphi^n$

We can algebraically solve the value of φ=r/s

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

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

$$r^2 - rs - s^2$$ **=0** quadratic equation

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

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

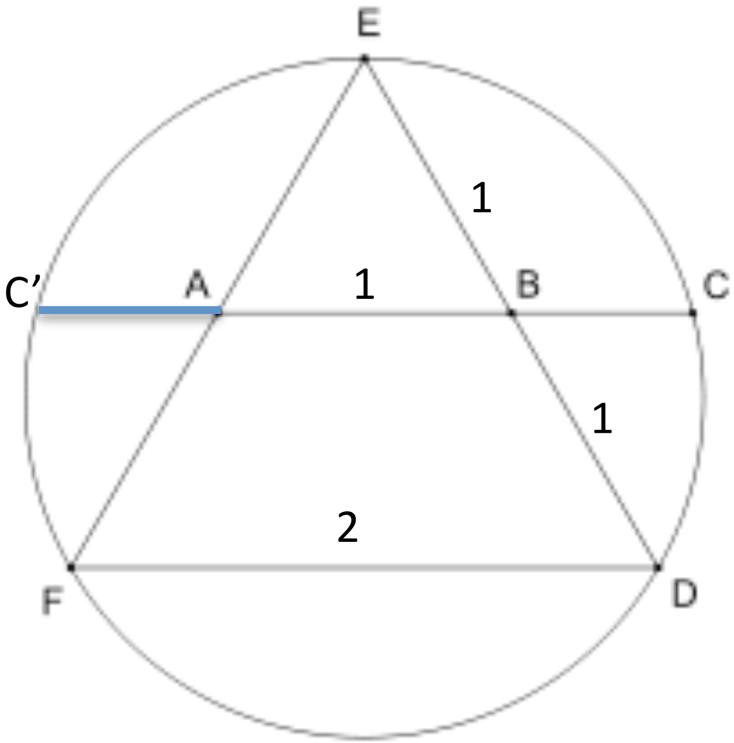
$$\frac{r}{s} = \frac{1+\sqrt{5}}{2} \approx 1.61803398874989.$$

We take the positive of the two solutions φ =(1 ± √5)/2

Pythagoras has a different geometrical construction

Draw the triangles with edges x=1 and the circumscribing circle.
The law of dissecting cords in a circle: BE*BD=BC*BC'=BC*(1+BC)
Or generally x=BE=BD a=BC=AC' $x^2=a*(a+x)$ $x^2-ax-a^2=0$
x/a=φ is the golden ratio, $\varphi^2-\varphi-1=0$ $\varphi=(1+\sqrt{5})/2 \sim 1.618034$
and $\varphi=1/(\varphi-1)$
indeed: $(1+\sqrt{5})/2 = 1/[(1+\sqrt{5})/2 -1] = 2/(-1+\sqrt{5})$ => $(5-1)/2=2$

Thus the ratio of lengths of the two sectors BE & BC is golden



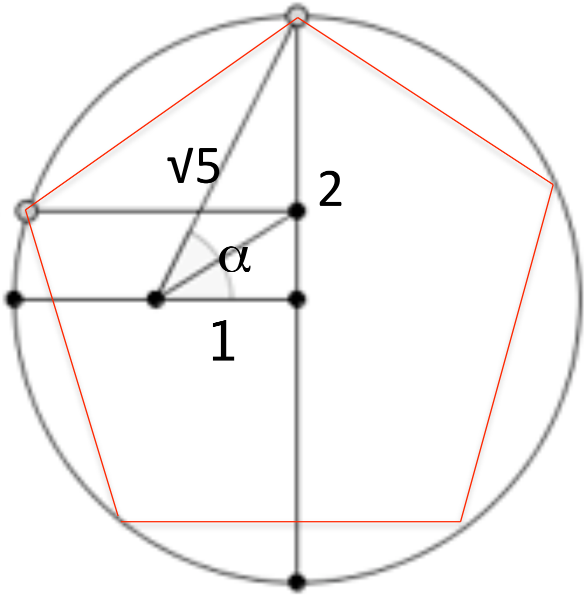
The golden ratio is connected to equal edges Pentagon

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

If we draw a circle of radius 2 and a right angle triangle with edges 1,2, √5
The bisector of angle α crosses the opposite edge at the height of the pentagon vertex.

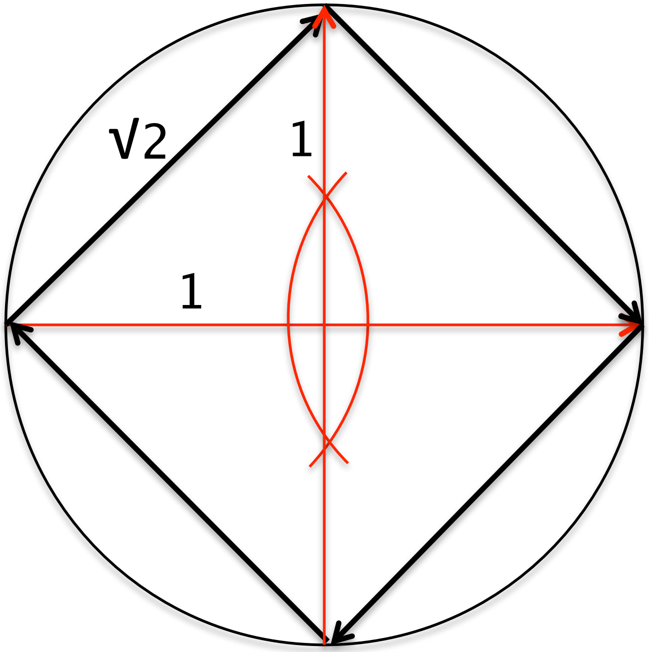
Leonardo da Vinci’s human dimensions logo use the pentagon due to this golden ratio.

The pentagon inner angle is 108^{o}

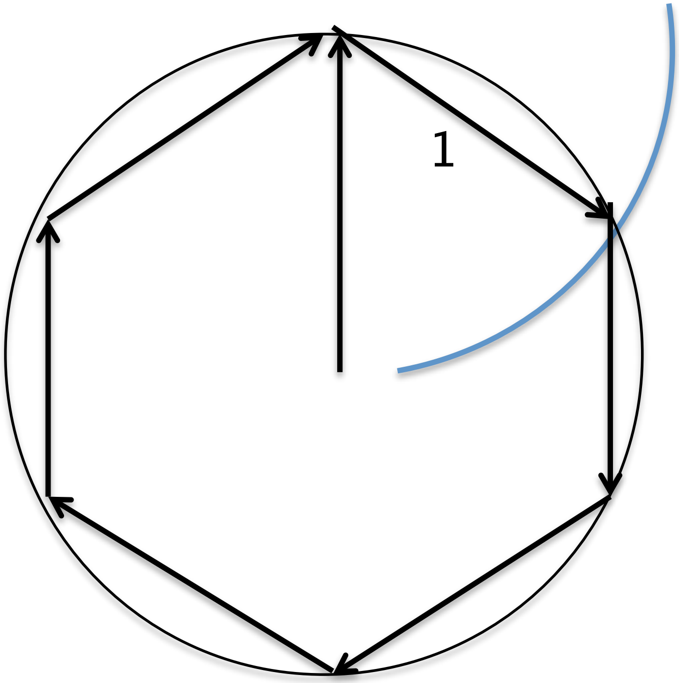


Construction of polygons with n equal edges – regular polygons

Square, and from it 8,16,... -gons



Hexagon, and from it 12,24,... -gons



Construction of Heptagon (7-sided polygon) was an unsolved problem for 2000 years **Carl Friedrich Gauss 1777–1855** proved at the age of 19 that such construction is impossible with compass and ruler alone. This is only possible for polygons with n edges where n = "Fermat Primes" = 2^k+1; $k=2^m$ and its multiples by 2^m m=1,2, ...

Today, known Fermat primes are: 3,5,17,257,65537

Gauss construction of 17-polygon: This is a vivid demonstration of Gauss’ ingenuity !

ZERO & INFINITY

Brahmagupta 598-668

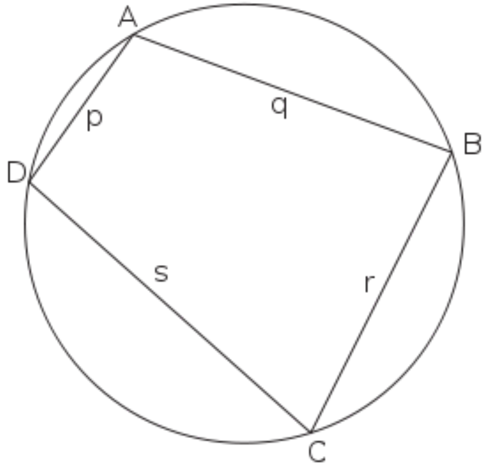
Was first to define the arithmetic rules for zero:

1. Adding or subtracting zero does not change a number
2. Multiplying a number by zero gives zero

And the rules for negative numbers (he called “debts”)

1. Debt minus zero = debt
2. Credit minus zero = credit
3. Zero minus zero = zero
4. Zero minus debt = credit
5. Zero minus credit = debt
6. Zero multiplied by credit or debt = zero
7. Zero multiplied by zero = zero
8. Multiplication or division of credits = credit
9. Multiplication or division of debts = credit
10. Multiplication or division of credit and debts = debt
11. Multiplication or division of debts and credit = debt

He “wisely” refrained from dealing with division by zero
773 BC Brahmagupta’s book reached Bagdad, and affected Arabic mathematics.



Brahmagupta wrote the formula for the area of a rectangle circumscribed in a circle:

$$K = \sqrt{(S-p)(S-q)(S-r)(S-s)}.$$ where S=(p+q+r+s)/2

The zero is a numerical value that enables in positional number system to attribute a value to a digit by its place: e.g. 2 vs. 20. This system does not require special signs for tens, hundreds etc.

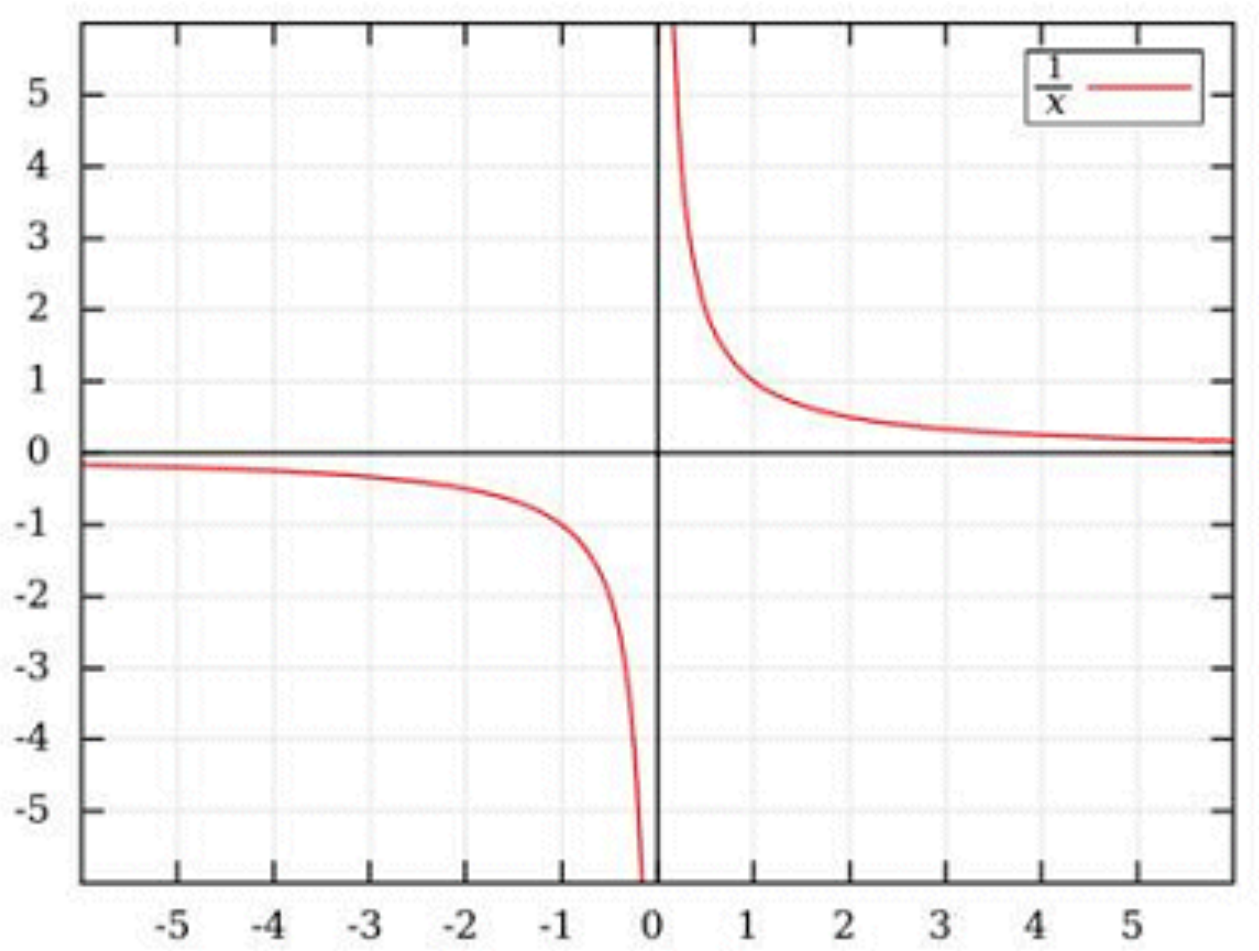
.The system was brought from India to Persia by the mathematician **Al Biruni 973-1048**

Stamps commemorating 1000 years for Al Biruni were issued by Pakistan, Syria and Iran, all adopting him to their national heritage, following his migrations.

The zero and the positional system, called “Arabic number system” spread into the Moorish Spain by **Ibn Ezra of Metudella and Saragossa 1092-1167** and into Europe by **Fibonacci 1170-1250**

Zero impose extension of the number system

Since division by zero is larger than any number: we need to add the infinity ∞.
When x grows, 1/x becomes small. The concept of a value “shrinking” towards zero (epsilon-small) is a basic concept of calculus.



Infinity has “strange” properties

Aristo – describe infinite numbers: for every number r we have r+1.

Euclid – proved that there is an infinite number of primes (see below).

Indian Veda 900 BC – defines infinity as a number that does not change when you add or subtract a number from it.

Archimedes 287-121 BC – defined equality between two infinite groups if we can pair all their members.

Al-Karaji – describe inductive algorithm that repeat infinitely.

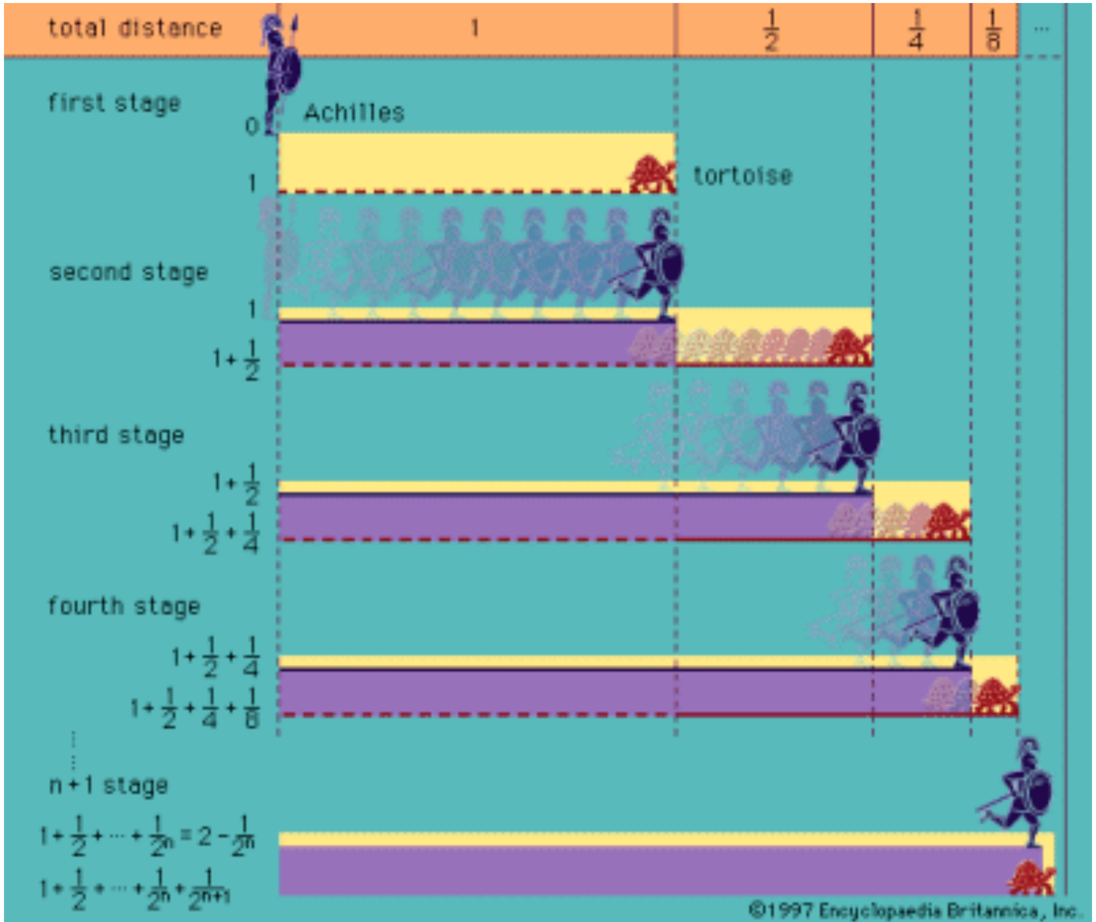
Galileo – the number of integers and squares is the same. Although the squares are a subgroup of all integers: one of the “strange” properties of infinite groups.

Bolzano – define groups with infinite number of elements.

if $\varepsilon \to 0$ then $1/\varepsilon \to \infty$ yet in some cases $0 * \infty$ can be finite (see L'Hôpital's rule)

Zeno’s paradox:

Achilles runs in a speed of 2 meters/second, and a turtle runs 1 meter/second.
Achilles starts 2 meters before the goal, and let the turtle start in front of him, 1 meter from the goal. When Achilles runs 1 meter, he is at the turtles start position, but the turtle moved ½ a meter forward. When Achilles runs ½ meter more, the turtle moves in front of him ¼ meters. So infinitely: whenever Achilles reach the previous position of the turtle, it will move forward from it, thus Achilles will never reach the turtle…
Where is the mistake? We know both Achilles and the turtle will meet after 1 second.


total distance
1
$\frac{1}{2}$
$\frac{1}{4}$
$\frac{1}{8}$
...
first stage
Achilles
0
1
tortoise
second stage
1
$1+\frac{1}{2}$
third stage
$1+\frac{1}{2}$
$1+\frac{1}{2}+\frac{1}{4}$
fourth stage
$1+\frac{1}{2}+\frac{1}{4}$
$1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}$
n+1 stage
$1+\frac{1}{2}+\cdots+\frac{1}{2^n}=2-\frac{1}{2^n}$
$1+\frac{1}{2}+\cdots+\frac{1}{2^n}+\frac{1}{2^{n+1}}$

©1997 Encyclopaedia Britannica, Inc.

Sums of infinite series

The total length of two half meter segments is 1 meter

The total length of four quarter meter segments is 1 meter

…

The total length of N segments each 1/N meters long is also 1 meter

for N->∞ $N * 1/N = 1$

But also $1+1/2+1/4+1/8+ \dots => 2$

We define limit of a function f(x) when x approaches a: $\lim_{x->a} f(x)=L$

The limit exists if for every $\delta>0$ there is $\varepsilon>0$

so that if $|x-a|<\delta$ then $|f(x)-L|<\varepsilon$

The geometrical meaning: if we draw the Tangential to f(x) at x=a with slope f’(a)

Then $\varepsilon = \delta * f'(a)$

For singular functions (e.g. f(x)=1/x) the tangential at x=0 does not exist, and f(x) has no limit.

The limit is the basis of infinitesimal calculus π

π = 3.14159265…

The bible, in the description of the round water container cast from copper that stood in King Solomon temple, specifies its diameter as 10 cubits length, and 30 cubits perimeter. Therefore π = 3.
The bible also specifies the volume: 2000 Bat, but we do not know the exact shape of the container (cylinder or half sphere) and also what is the definition of a Bat…

In Egypt 1560 BC in the Rhind Papyrus states: $\pi = 4(8/9)^2 = 3.16$
And in another script $\pi = 25/8 = 3.125$
Rational approximations were the only way Egyptians knew to write fractional numbers.
In Mesopotamia - $\pi = 25/8$ and also $\pi = \sqrt{10} = 3.162$
Since the Babylonians based their calculations on square tables, also π was so expressed.
In India –based on measurements, they determined that the ratio of the perimeter to diameter of circles is different than the ratio of circles to square of their radius. The measurement of perimeters could be quite accurate, but circles area were probably difficult to measure accurately.

Squaring the circle

The meaning for early and classical scientists was: a graphical method, preferably using only a compass and a ruler, to draw a square with area equals to that of a sphere. We now think that there is no solution to this problem, however, the value of π can be approximated to any degree of accuracy using various methods (see following).

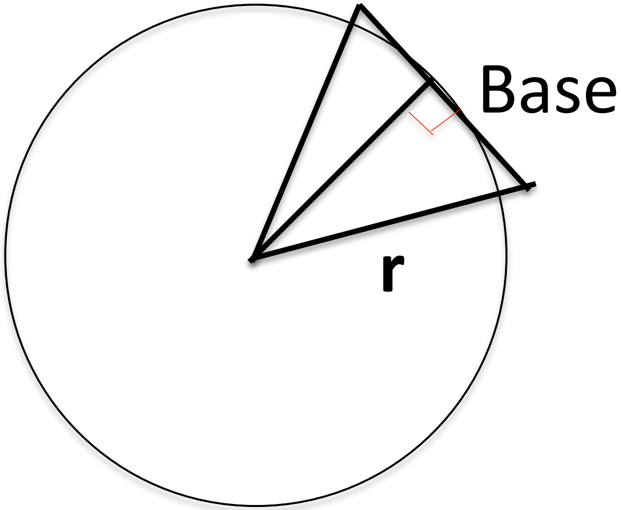
Archimedes of Syracuse 287-212 BC proved that the

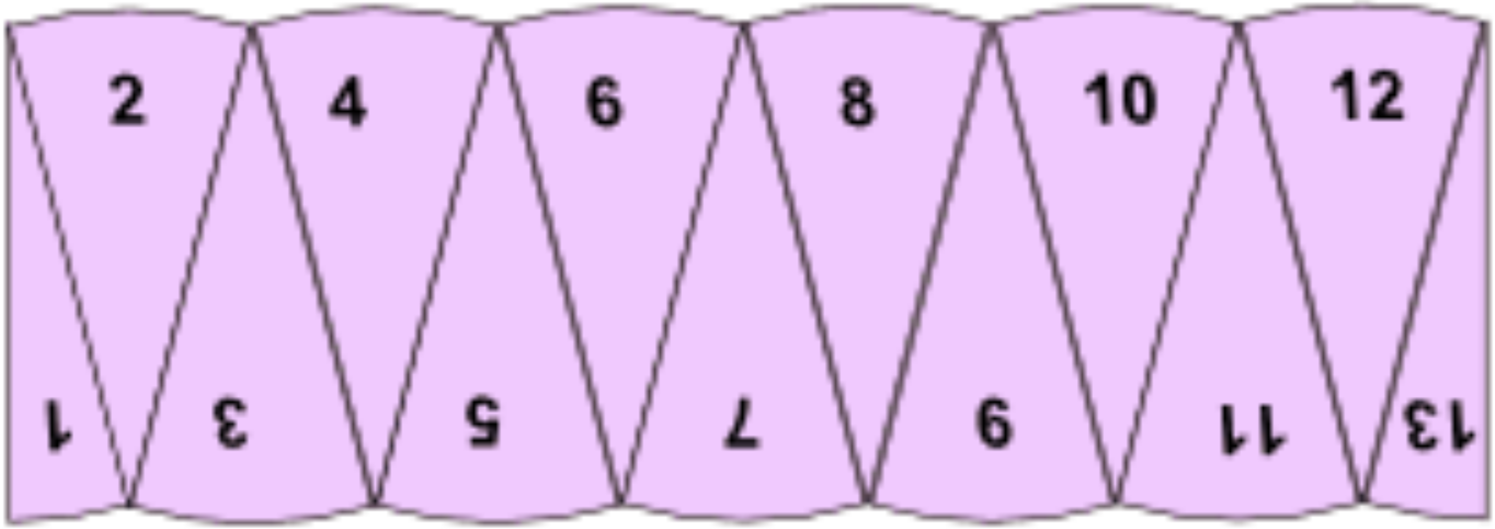
Circle area = Circle circumference * r/2

Therefore it is the same proportionality number π that appears in the circumference and the area of circles. He also showed that the same π also comes in the surface area and volume of the sphere (see following).

Here is a simple proof for the relation between circle circumference and area:
Cut the circle into small sections and stich back to make a rectangle
Its height is R, the circle radius, and its width = S/2 – half the circle circumference:
Therefor if S=2πR

$$A = RS/2 = \pi R^2$$

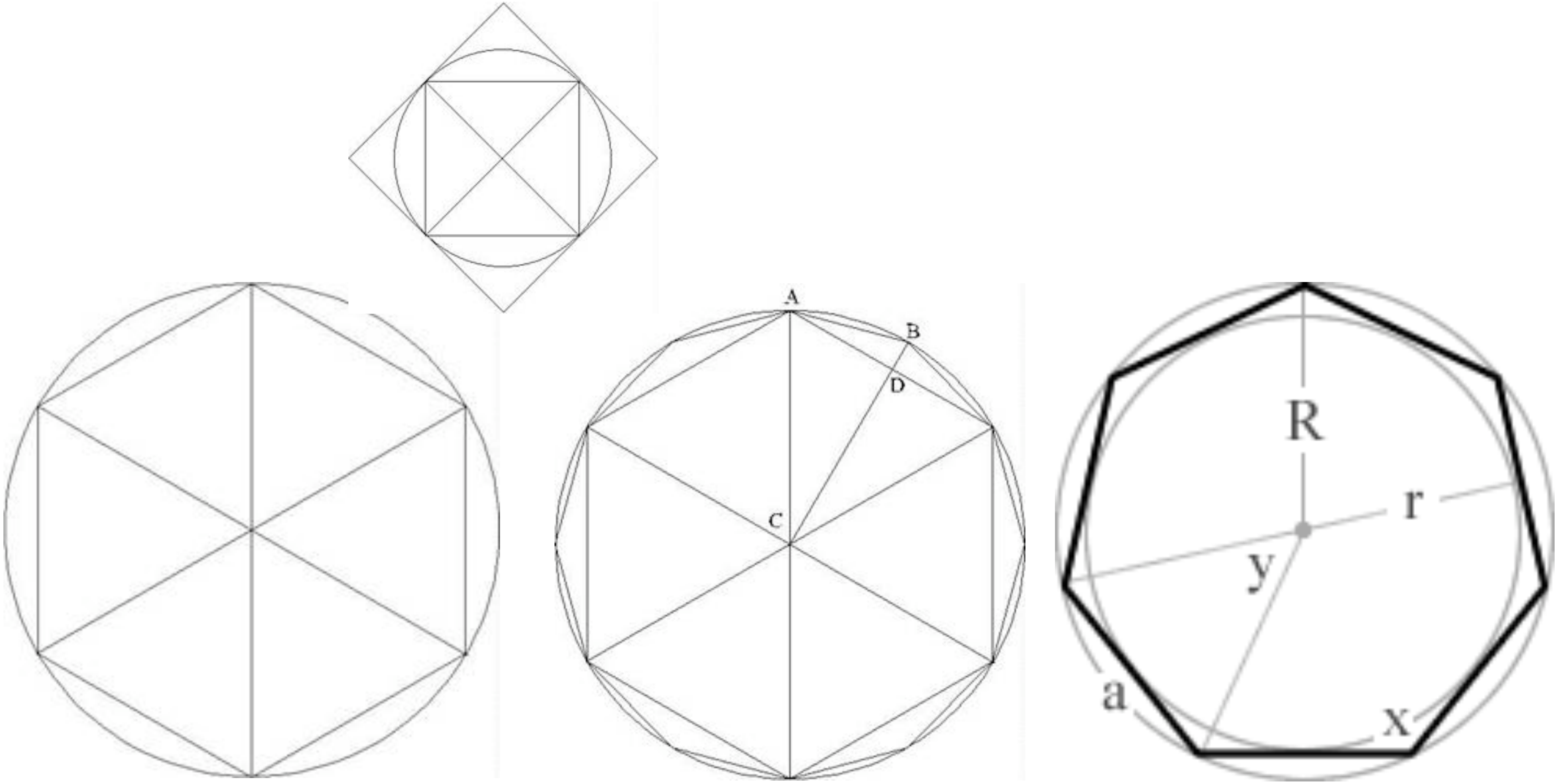


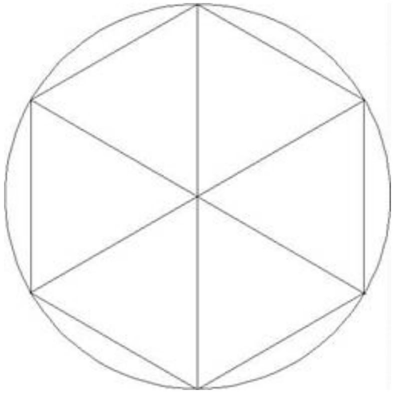


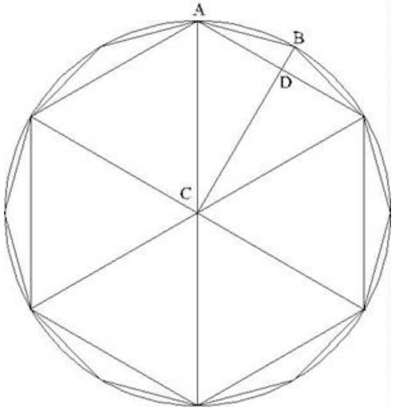
Archimedes - calculated the circumference (perimeter) of a circle from approximation by polygons with number of edges $6*2^N$ -> ∞

The perimeter of Hexagon is 6R, he calculated the edges of 12-gon 24-gons etc. using Pythagoras law and geometry.

In fact, inscribed and circumscribed polygons to a circle set upper and lower limits to the value of π . This was the first use of infinitesimal calculus:







From the hexagon, with edges = R, we conclude that 2π > 6, or **π>3**.

For dodecagon (12 edges) we can calculate the edge length from Pythagoras law:

AD=1/2

CD=sqrt(1-AD^2)=sqrt(3/4)=sqrt(3)/2

DB=1-CD=1-sqrt(3)/2

AB=sqrt(AD^2+DB^2)=sqrt(1/4+1+3/4-sqrt(3))=sqrt(2-sqrt(3))=0.517638…

2π ~< 12AB=6.211657…

For 24-edges polygon we use Pythagoras twice, giving **2π ~< 6.26**

Archimedes used the Babylonian tables to write his rational number limits,

e.g. 265/153 < sqrt3 < 1351/780

Archimedes reached 96-edge polygon and obtained: **3 10/71 < π < 3 1/7**

The average of the upper and lower limits is 3.14185 where the value of π is 3.14159

We can apply trigonometry to get a recursive formula for the edge of k-gon: ($k=3^n$)

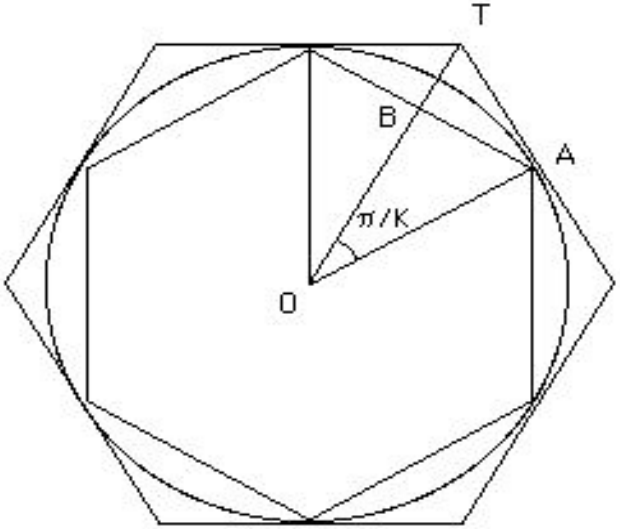
$a_n = K \tan(\pi/K)$, $b_n = K \sin(\pi/K)$,

$a_{n+1} = 2K \tan(\pi/2K)$, $b_{n+1} = 2K \sin(\pi/2K)$,

$a_1 = 3 \tan(\pi/3) = 3\sqrt{3}$ & $b_1 = 3 \sin(\pi/3) = 3\sqrt{3}/2$

$(1/a_n + 1/b_n) = 2/a_{n+1}$

$a_{n+1}\, b_n = (b_{n+1})^2$



OA = 1

AB = sin(π/K)

AT = tan(π/K)

where K = 3 x 2^{n-1}

Archimedes set upper and lower limits to π

$$223/71 < \pi < 22/7$$

Later approximation to the value of π were developed:

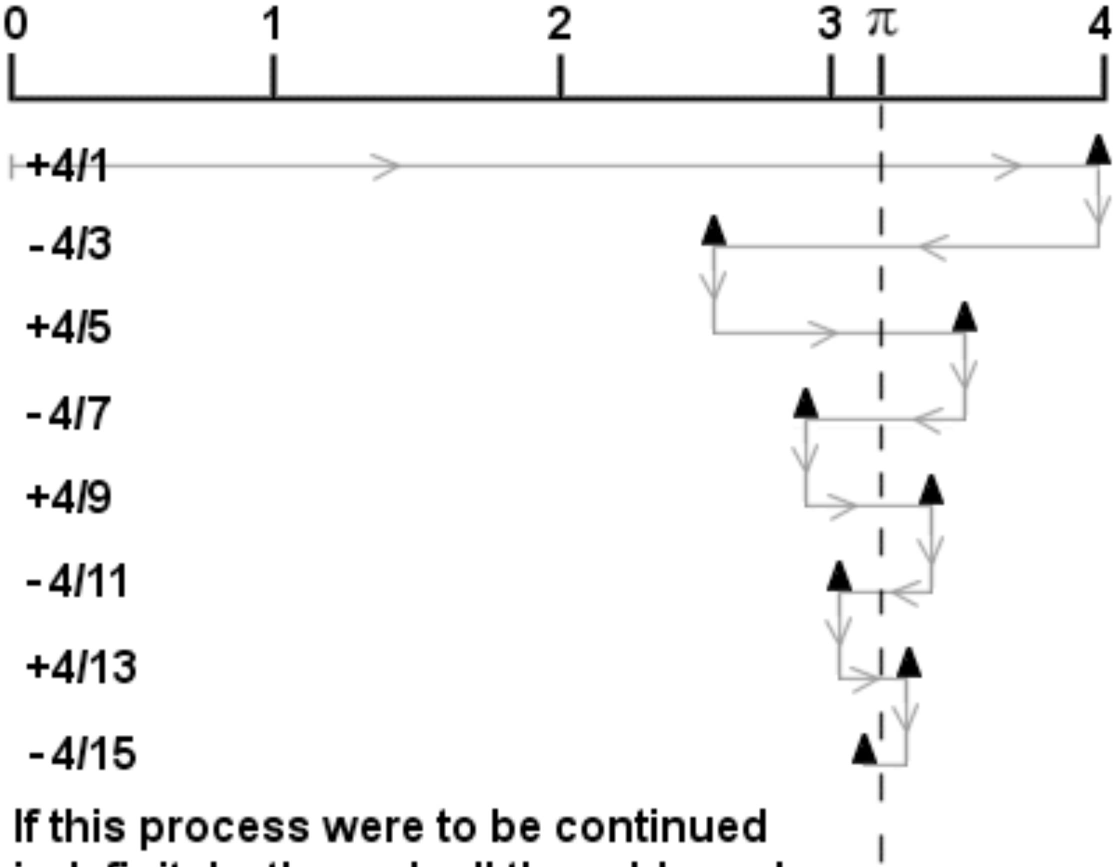
See next slide	**Madhava of Sangamagrama (1350–1425)**
$2/\pi = (1.3.3.5.5.7. ...)/(2.2.4.4.6.6. ...)$	**Wallis (1616-1703)**
$\tan^{-1} x = x - x^3/3 + x^5/5 - ...$	**James Gregory (1638- 1675)**
	$\pi/4 = \tan^{-1}(1/2) + \tan^{-1}(1/3)$
$\pi/4 = 1 - 1/3 + 1/5 - 1/7 + ...$	**Leibniz (1646-1716)**

But only **Lambert, 1761**, proved that π is an irrational number

Interesting property:
If we throw a needle of length k on a grid with spacing 1, the probability of the needle to fall on a grid line is **$2k/\pi$**

Madhava of Sangamagrama . 1350–1425 proposes an approximation for π at any required accuracy:

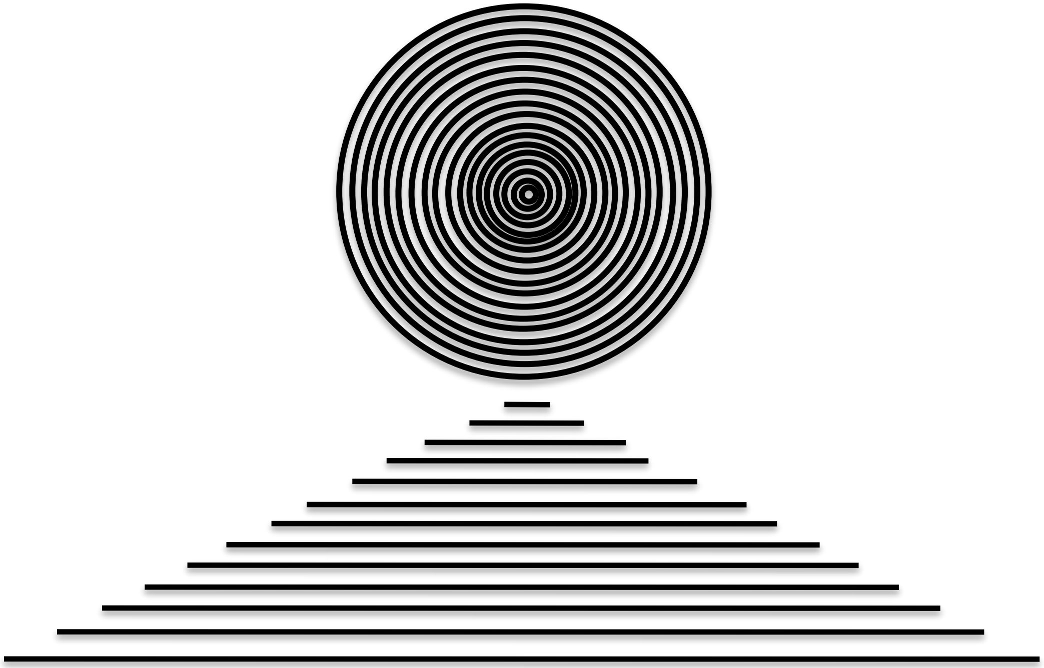
$$\pi = 4 - 4/3 + 4/5 - 4/7 + 4/9 - 4/11 + 4/13 - 4/15 \;.... \; 4/\infty$$



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

A different infinitesimal proof was described by the Jewish Rabi, **Abraham bar Hiyya Ha-Nasi 1070-1136 AC** (Barcelona and Provence).

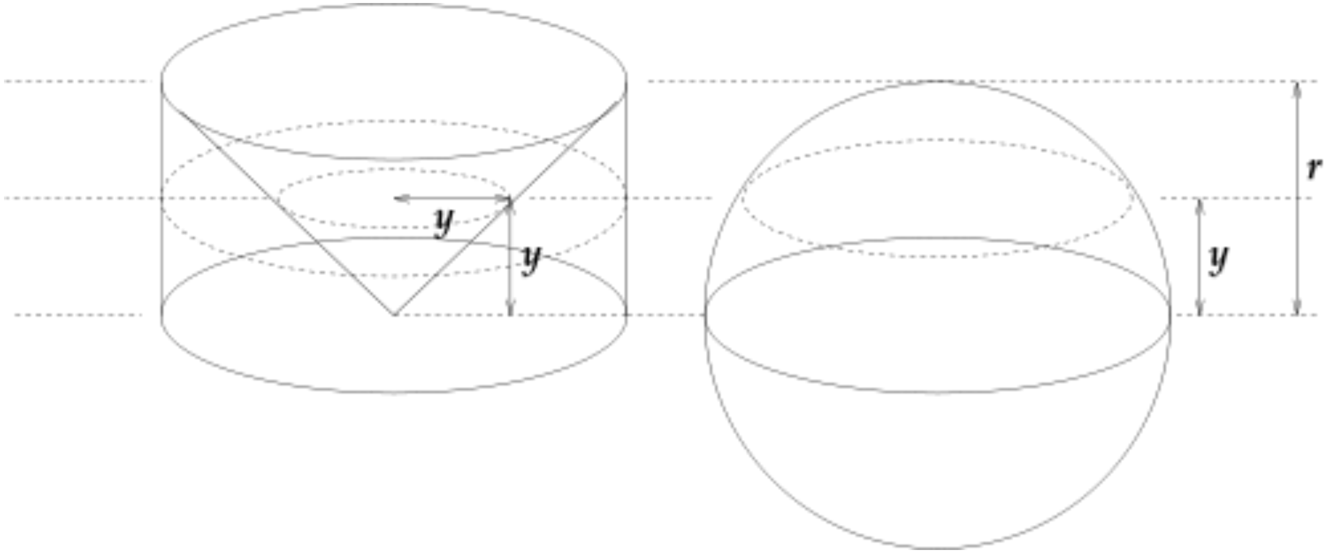
If you cut the area of the circle into N strips of perimeters with shrinking radius, up to the center point, straighten theses strips and pile them, we get a triangle with base $2\pi R$ and height R, therefore the circle area = $= 2\pi R*R/2 = \pi R^2$



Similarly, the relation between the surface area of a sphere and its volume is calculated by large number of infinitesimal pyramids with bases on the surface:

$$4\pi r^2 * R/3 = 4/3\pi R^3$$

Surface area and volume of a sphere is 2/3 of the surface area (including bases) of the circumscribing cylinder. The proof (given by Archimedes and known as Cavalieri's principle, **Bonaventura Francesco Cavalieri 1598–1647** , see Geometry):
The volume of the sphere = volume of the cylinder – volume of the cone with base & height equal to the cylinder.
Since for a section at any height y, the area of the sphere section is $\pi(r^2-y^2)$, and this is also cross area of the cylinder πr^2 minus the cross area of the cone πy^2
The volume of the cone $r^3/3\pi$, therefore the sphere volume is $r^3(1-1/3)2=4/3\pi r^3$



According to **Cicero, 75 BC**, Archimedes asked that the sphere circumscribed in the cylinder will be drawn on his grave, to emphasize the importance he attributed to this finding.

What is the significance of accurate value for π ?

Calculating coordinates and angles for machining parts.
Calculation position by GPS.
Calculating volumes and surface areas of packs for foods, materials, etc.
Calculations of quantities in building materials.

We saw the **π** appears in the ratio between a circle circumference to its radius, ratio between sphere area to its radius squared, and volume to its radius cube.

Is **π** also in the ratio between four-dimensional and higher dimensions hyper spheres?

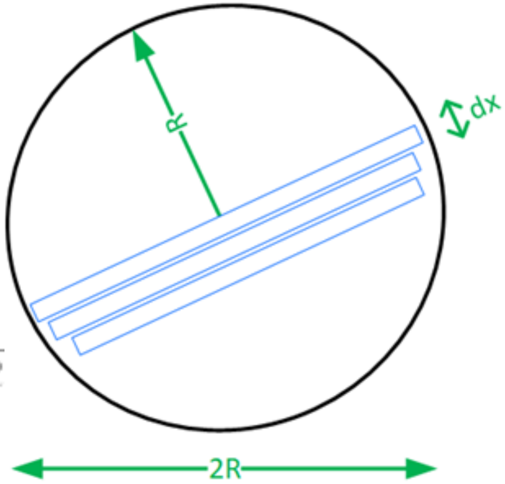
The answer is that for 4 & 5 dimensions the proportionality includes π^2
The power of **π** increase by 1 for every two dimensions.

The proof is by integral calculus:

Volumes of n-dimensional hyper spheres

Circle area n=2

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



Sphere volume n=3

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

Hyper-sphere n=4

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

Thus recursive calculation of the n-dimensional hyper sphere from n-1 dimensions

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

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

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

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

cont.…

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

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

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

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

We see that hyper volumes for n>6 decreases, a non-intuitive result for high dimensions!!!

Another calculation (for unit radius)

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

עבור קו

$$V_0 = 1$$

$$S_0 = 2$$

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

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

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

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

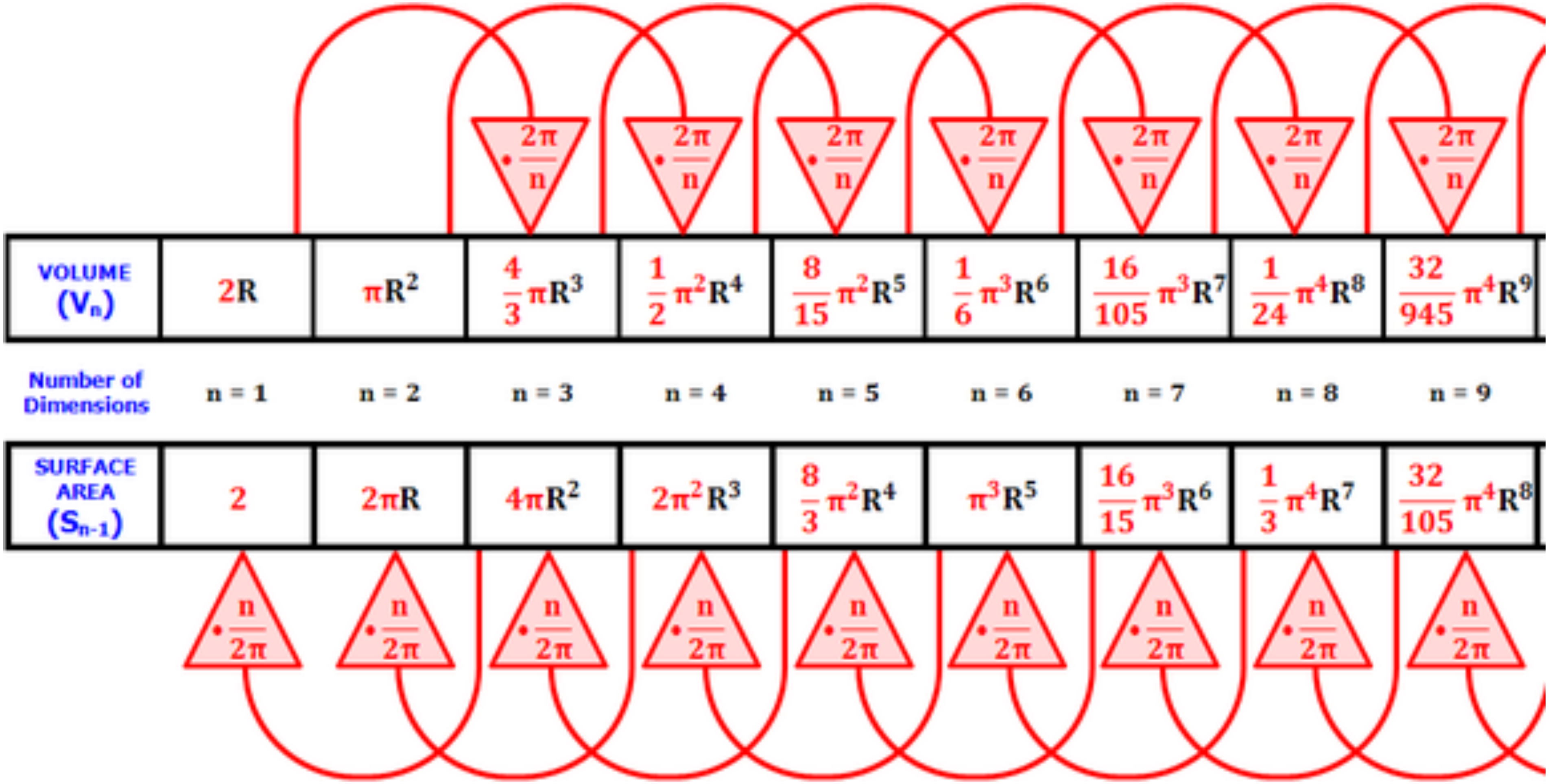
$$= 2\pi V_{n+1} \longrightarrow S_{n+1} = 2\pi V_n$$

$$\downarrow$$

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

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

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



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	$2\pi R$	$4\pi R^2$	$2\pi^2 R^3$	$\frac{8}{3}\pi^2 R^4$	$\pi^3 R^5$	$\frac{16}{15}\pi^3 R^6$	$\frac{1}{3}\pi^4 R^7$	$\frac{32}{105}\pi^4 R^8$

POWERS

The power of powers

The sum of geometric series $1+q+q^2+q^3+ \dots q^n =(1-q^n)/(1-q)$
converges for n->∞ if $q<1$

Multiplications of bacteria, dividing every hour - 2^T bacteria after T hours

Twice the rice grains on the next square of a chess board, on the last:

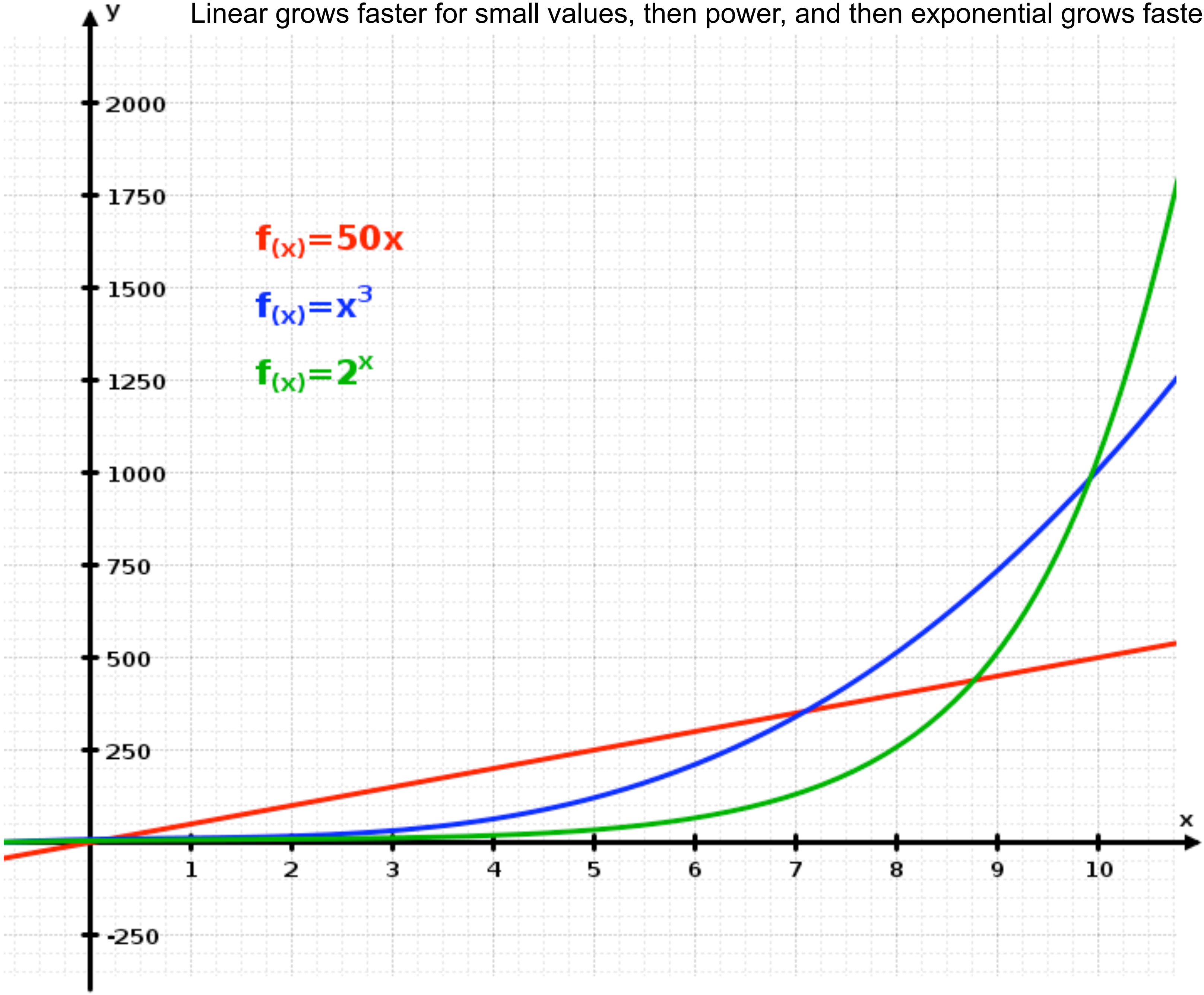
$$2^{64} = 18,446,462,598,732,800,000 \sim 0.18x10^{20}$$

their weight is 1/30,000 of earth weight ($5.974 \ x10^{24}$).

If each of us has 40 friends, at 6 level $4,000,000,000 \sim 40^6$ the whole world population is covered. (we assume the most friends of friends are not from the same circle).

Watch the growth of linear, power and exponential functions.

Linear grows faster for small values, then power, and then exponential grows fastest of all



<u>Gordon Moore</u> – predicted that computer processors speed will increase by a factor of 2 every 18 months. The prediction stayed valid for 40 years.

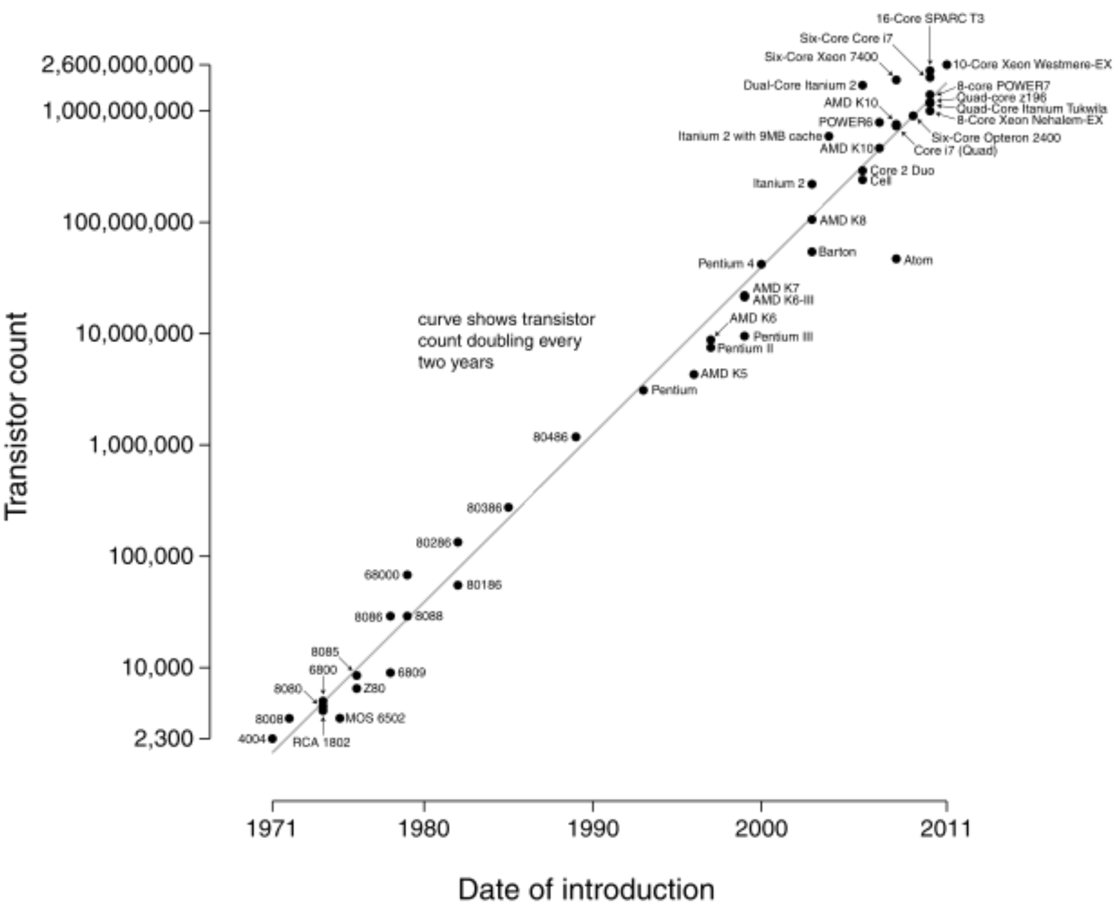
what are the physical limitations to speed, and possible solutions:

Speed of signal transfer (< speed of light): make processors smaller. ➔ Quantum computers.

Prevent heating: cooling sinks, ➔ immerse in superconducting liquid helium.

Limits of one processor: parallel computing, simpler but faster processors (GPU)

Microprocessor Transistor Counts 1971-2011 & Moore's Law



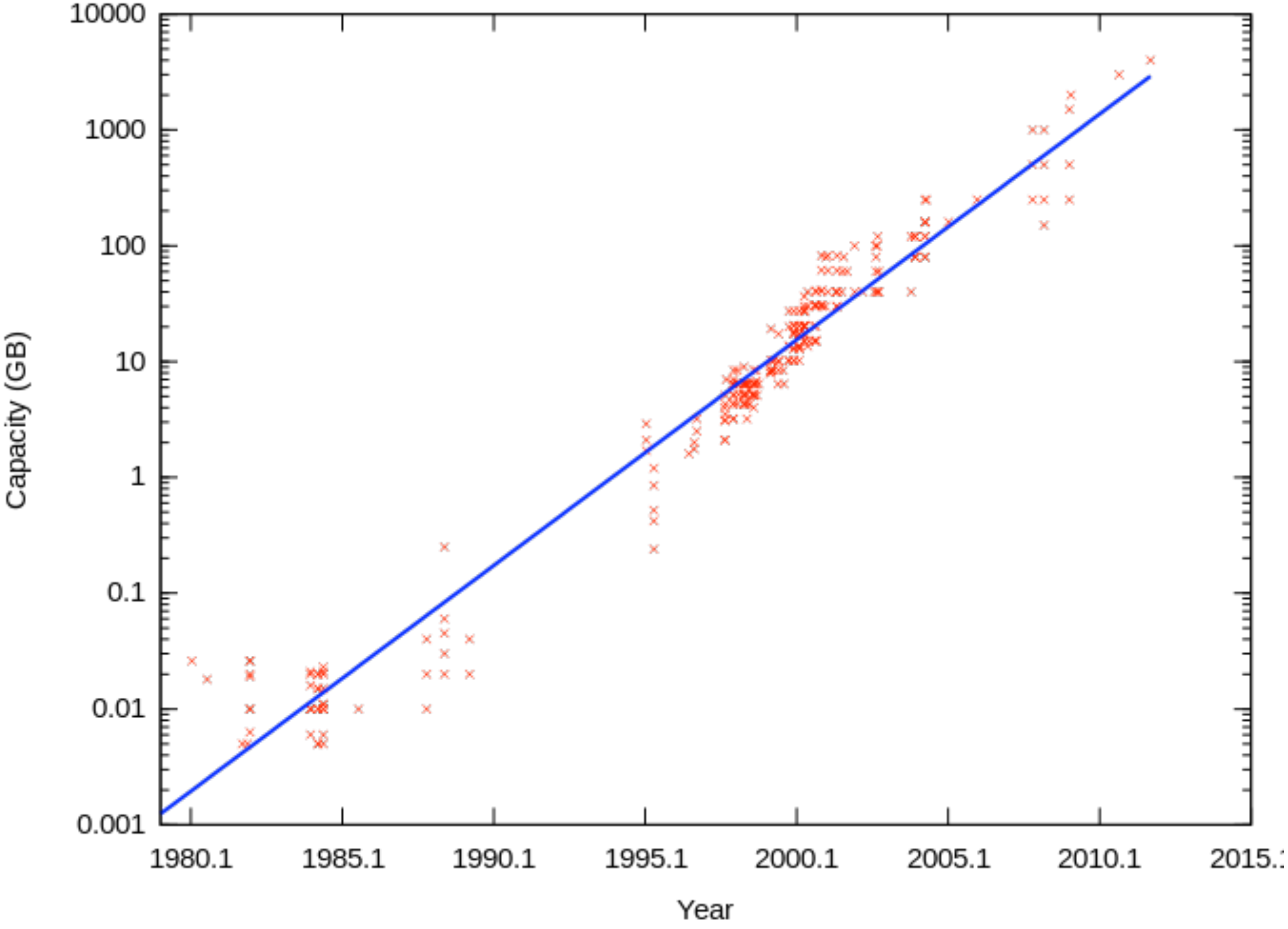
Also the capacity of digital information increases exponentially.

Limitations, and solutions:

Volume of storing a bit of information reliably: optical-diffraction limit. Magnetic: in principle one atom

Size of the reading head, its reading and writing speeds. For rotating disks: access time.

Surface or volume (3D) recording (e.g. multilayer disks).



e

e = 2.718281828...

In order not to keep tables of powers of all numbers we can use logarithmic tables ln(x). For every y: $x^y = e^{\ln(x)*y}$ thus multiplying ln(x)*y and using the log table backwards (antilog) yields the value of x^y from e^y

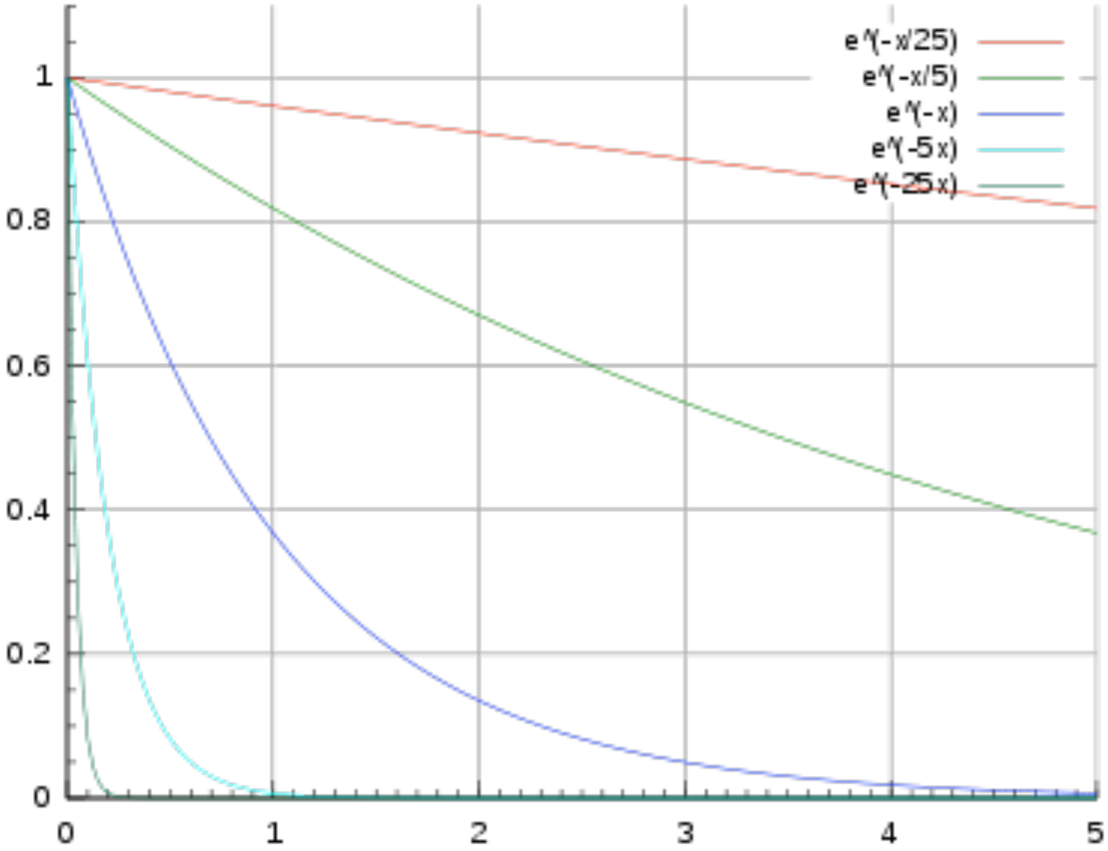
ברנולי

Jacob Bernoulli 1655–1705 – the Swiss mathematician, studies what would be the interest a bank would pay for a deposit of 1 Frank if the yearly interest rate is 100%.
If the interest is paid once a year: it will be 1 interest + 1 deposit = 2 Franks.
If the interest is paid twice a year the deposit + interest will be $1.5^2 = 2.25$
If paid 4 times a year: $1.25^4 = 2.44140625$
Every month: 2.613035
For n-times a year interest payment: $(1+1/n)^n$
and for continuous calculation and payment of the interest: $\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$ = e

Another example: A colored water in a cup is poured out through a pipe, and clear water is poured in at the same rate. What is the color concentration as a function of time:
The answer is $e^{-T/t}$

Since **e** comes up “naturally” in problems of multiplicative formulae, the logarithm on base **e** is called “natural logarithm”

Similar equations describe radioactivity, since the number of radioactive decay is proportional to the number of remaining intact atoms.



Also the probability to win the lottery after n times when n tickets are issued each time approaches 1/e=0.36787944…

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

The probability of winning k times out of n trials:

$$({}^{n}{}_{k})(1/n)^{k}(1-1/n)^{(n-k)}$$

Where

$$({}^{n}{}_{k}) = n!/(k!(n-k)!)$$

If n guests hang n hats numbered 1 to n randomly on collars numbered also 1 to n , What is the probability that not even one guest finds his hat on the right collar:

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

For large n the sum approaches **1/e.**

e also comes up in asymptotic formulae, e.g. Sterling approximation for factorials:

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

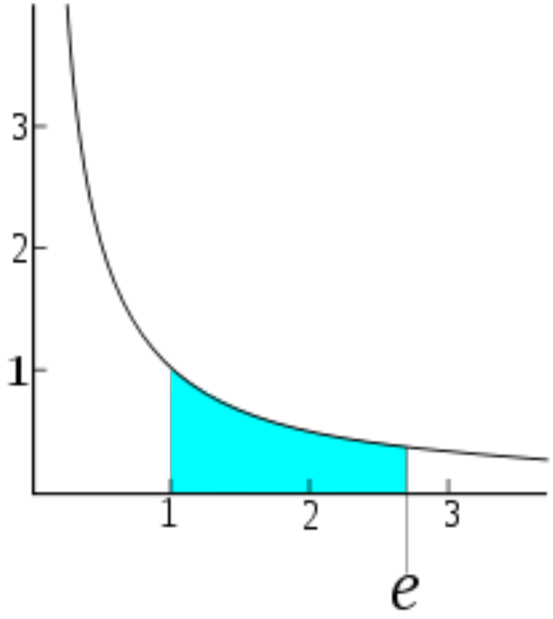
$$e = \lim_{n\to\infty} \frac{n}{\sqrt[n]{n!}}$$

Other properties:

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

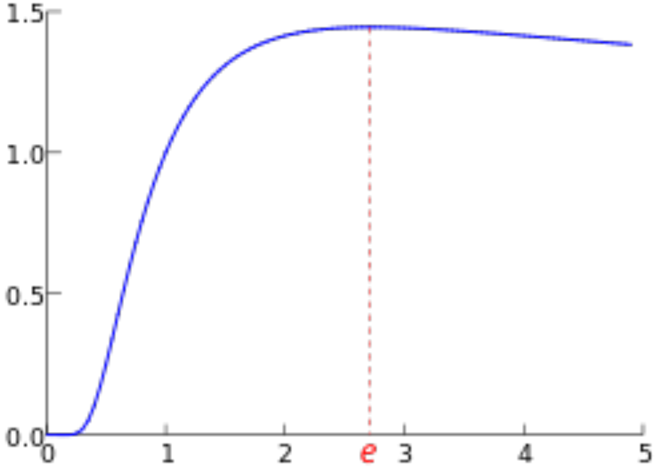
$$\frac{d}{dx}\log_e x = \frac{1}{x}.$$

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



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

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



The maximum of the function: $f(x) = \sqrt[x]{x}$
Is at x=e

The minimum of the function $f(x) = x^x$
Is at x=1/e

Probability
&
Combinatorics

OVERVIEW

Science attempts to describe natural phenomena by laws. Classically, these laws are deterministic, e.g. according to classical mechanics, given all positions and speeds of all bodies in the world the future can be predicted… The only classical limit is the errors associated with all measurements, (this was already recognized by the Greek philosophers and departed **Plato** from **Aristo**).

Probability theory developed from distribution of errors in measurements. **Gauss** developed best fitting of measurements and Gaussian distribution of random numbers carries his name. Probabilities were applied also to games (throwing a dice, or pulling a card), trying to help gamblers calculate their risks… Some results are counterintuitive: e.g. best bidding strategy is to put all your money if one bid, and not to distribute it over multiple bids. Combinatorial problems were studies by the Assyrians, Egyptians, Chinese, Arabs and middle age mathematicians.

The lack of practical capacity to know the positions and speeds of gas atoms in a container gave birth to thermodynamics, defining average properties that could be measured based on probabilistic distributions of molecules positions and speeds (e.g. volume, pressure, temperature). The conclusions reached by thermodynamics rose many debates, such as the problem of increasing entropy in systems governed by deterministic mechanics.

With the ability to perform measurements on small objects such as molecules, quantum mechanics emerged. Heisenberg’s uncertainty principle and Schrodinger’s probabilistic equation for the electron position created a huge “earthquake” in scientific thinking, and raised a lot of resistance before being accepted. Einstein, for example, claimed “God is not playing dice”.

RANDOM NUMBERS

We can simulate random behavior by throwing glass marbles into a field of nails. Initial small differences in the way we throw them is enhances by nails and their final position displays a Gaussian distribution:

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

The integral over all probabilities = 1,
the average = μ
and the distribution width (spread)= σ
Gaussian distribution characterize continuous random processes, x.

FIG.7.

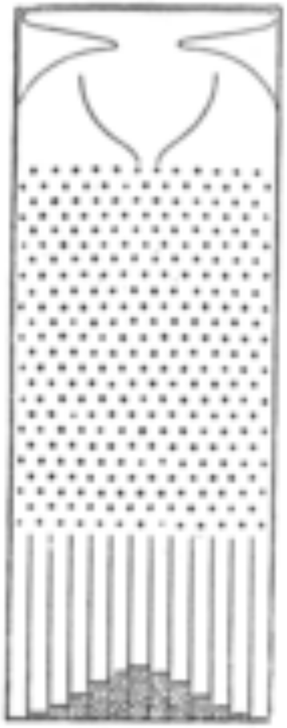


FIG.8.

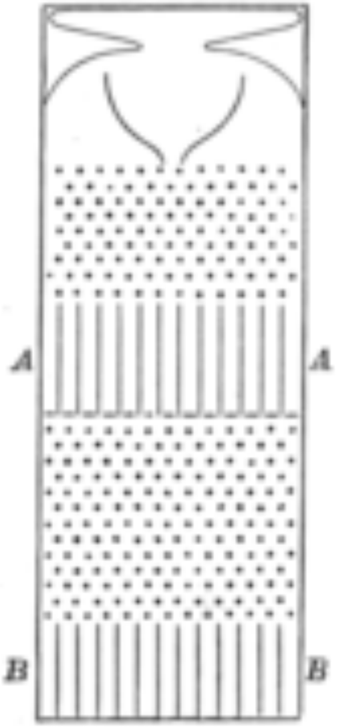
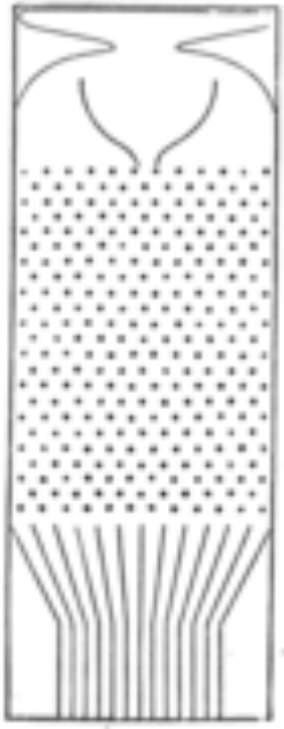
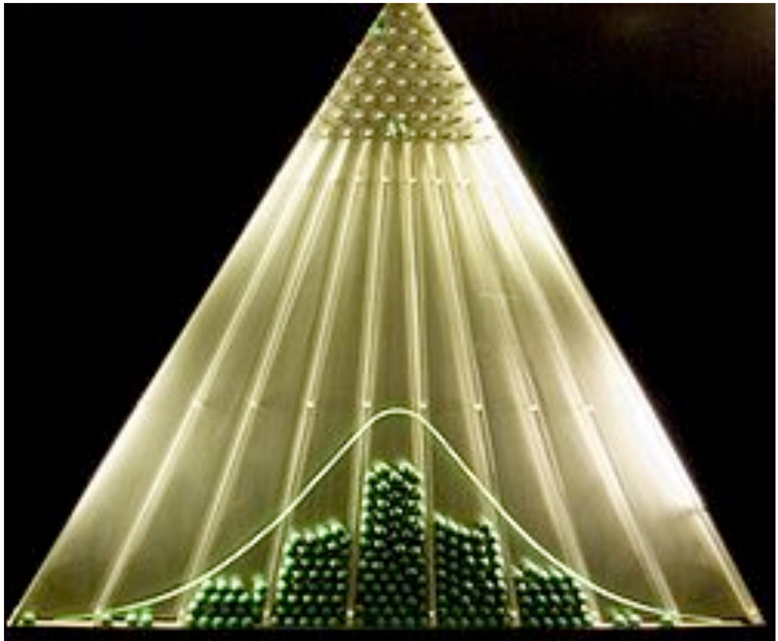


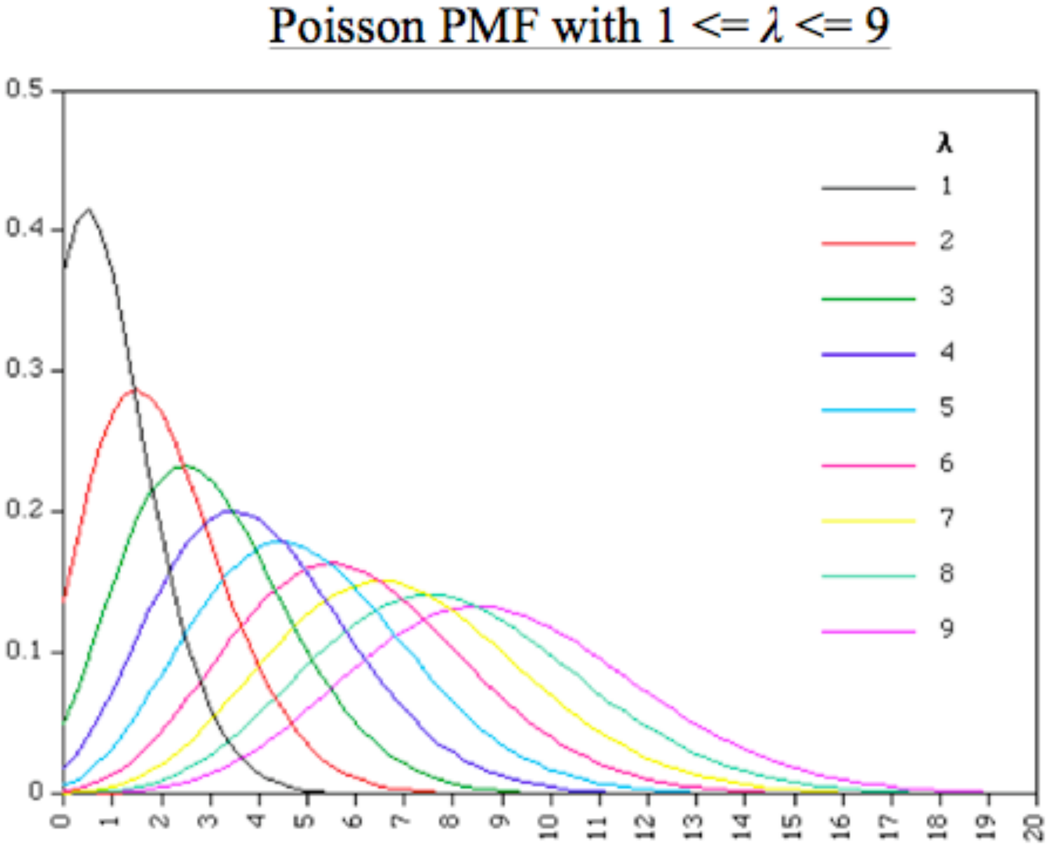
FIG.9.





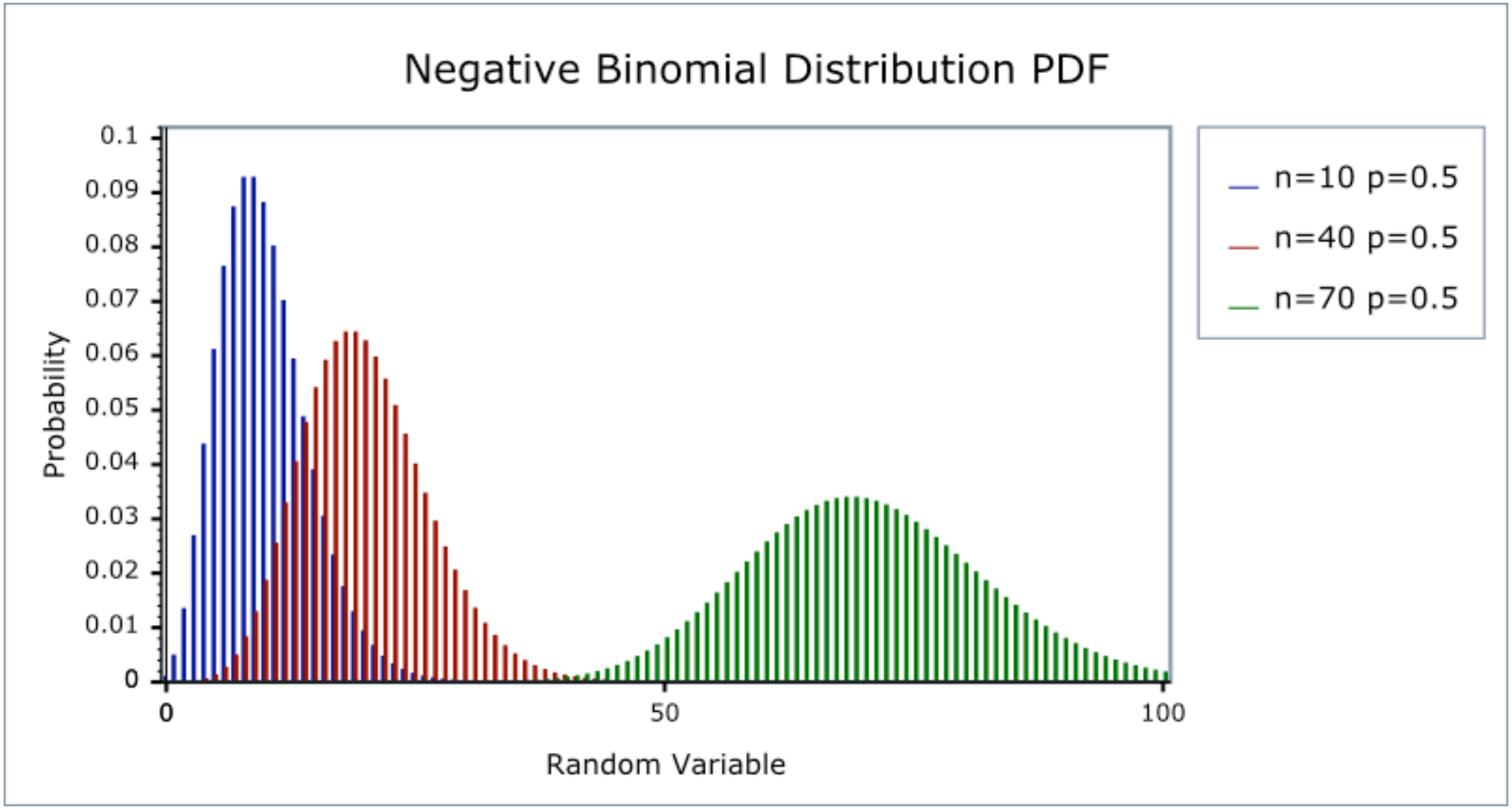
Other distributions characterize processes that are discrete, k:
e.g. **Poisson distribution**:

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



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

and **binomial distribution**



The **central limit theorem** defines that all probabilities approach Gaussian for large numbers (or close to continuous variables) (see the green binomial distribution for n=70)

Some problems:

What is the probability of getting a certain number of heads for 30 people each tossing a coin 100 times?

Since the number of possibilities is large, the probability will be Gaussian, averaged about 3000/2.

How many times one need to scramble 52 cards by splitting into two and mixing, in order to erase "memory" of their order.

The answer is: 7 times. If you do more – mixing is not improved.

How many communication lines are needed to guarantee that 75% of the times you try to call the line will be free.

The problem of number of radio lines needed in preparation for the landing in Normandy was studied in Bell Telephone Labs in New Jersey by a group whose research topics was random numbers.

Einstein connected the Brownian motion of small objects to the motion of gas molecules randomly impinging on them.

COMBINATORICS

DEFINITIONS:

N-factorial: $n! = n*(n-1)* \ldots 2*1$

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

In how many ways we can order 4 kids in a row?

Fist: any of 4 kids. Second: any of three left kids. Third: any of two. Last: the left kid.

4! = 4*3*2*1 = 24

In how many ways we can order 10 kids at a round table?

10! / 10

How many ways to arrange 5 boys and 5 girls in a row, no two of the same gender next to each other?

5! * 5!

Same at a round table?

5! * 5! / 5

How many words have 4 different letters?

26*25*24*23

How many 4 digit numbers? (numbers can repeat)

9*10*10*10 (cannot start with 0)

In how many ways a football team can be assembles in a class of 30?

$\binom{30}{11}$ = = 30!/11! (30-11)!

What is the chance to win the lottery, if 100,000 tickets were printed and half sold?

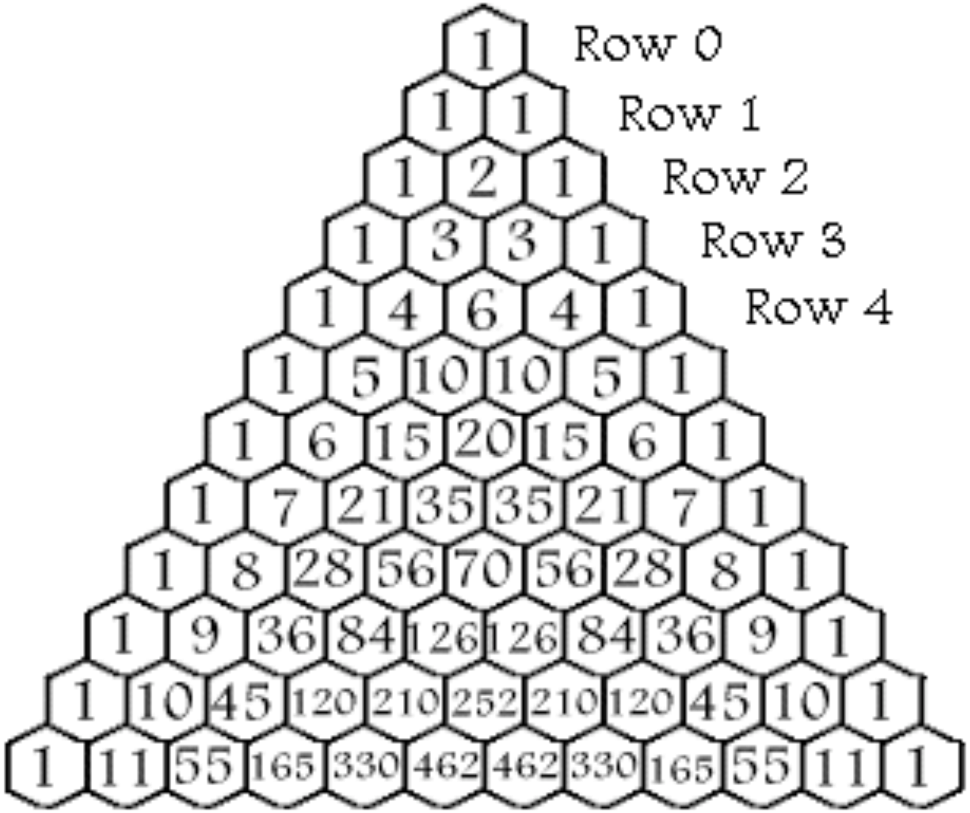
1/100,000

The number of ways k-times of a and n-k time of b appear in $(a+b)^n$?

The Binomial Theorem can be stated as:

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

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



1 Row 0
1 1 Row 1
1 2 1 Row 2
1 3 3 1 Row 3
1 4 6 4 1 Row 4
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1

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

Where: $$\binom{n}{i} = n! \;/\; [\, i! * (n-i)! \,]$$

The coefficients $\binom{n}{i}$ can be calculated from a recursive formula:

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

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

When is it advantageous to use a recursive over an explicit formula?

Explicit formulae take time to calculate. Thus if we want to fill a table for all numbers, the recursive equations would do the job much much faster.

Muhammad Al‒Karaji produced a proof to the recursive formula by **induction**:

"if the formula is true for n=1 we assume it is correct for any n, and prove it is correct for n+1"

For n=1: $(a+b)^1 = a + b$

Assume for n: $(a+b)^n = \Sigma ({}^{n}{}_{k})\, a^k\, b^{(n-k))}$ [k=0 .. N]

We prove for n+1: $(a+b)^{n+1} = \Sigma ({}^{n+1}{}_{k})\, a^k\, b^{(n+1-k)}$ [k=0 .. n+1]

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

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

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

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

$({}^{n}{}_{k-1}) + ({}^{n}{}_{k}) = ({}^{n+1}{}_{k})$

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)

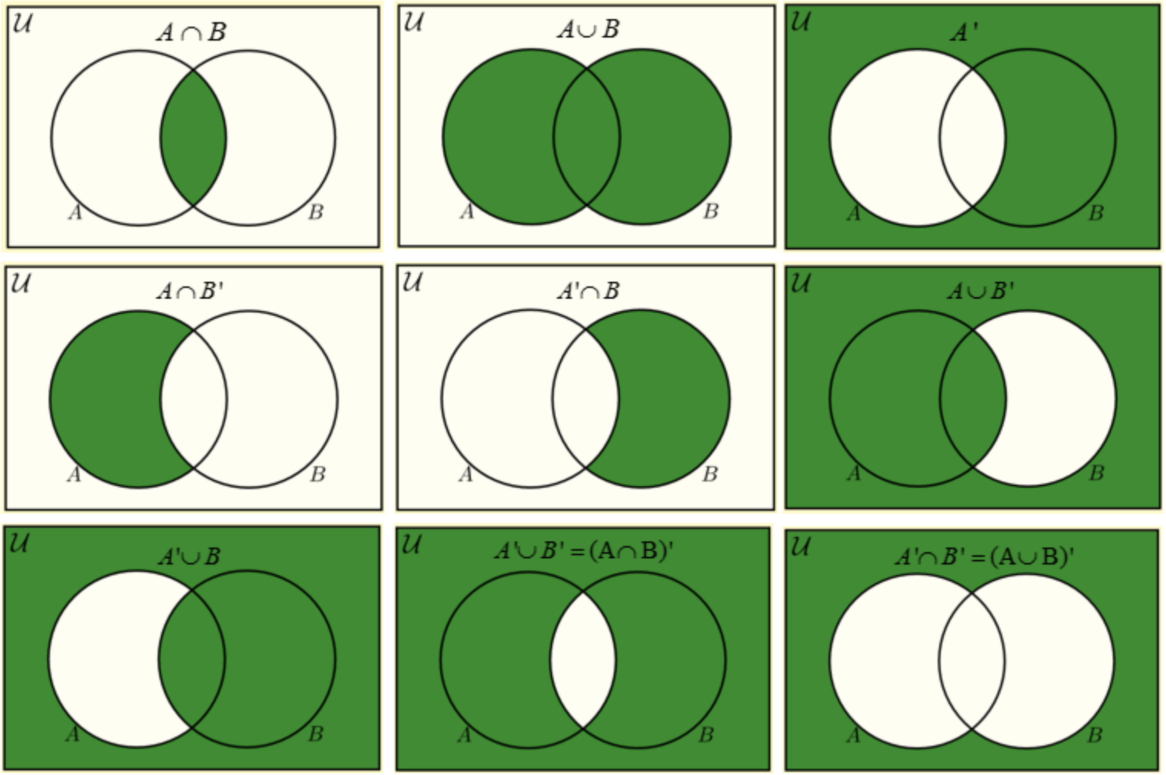
LOGICS

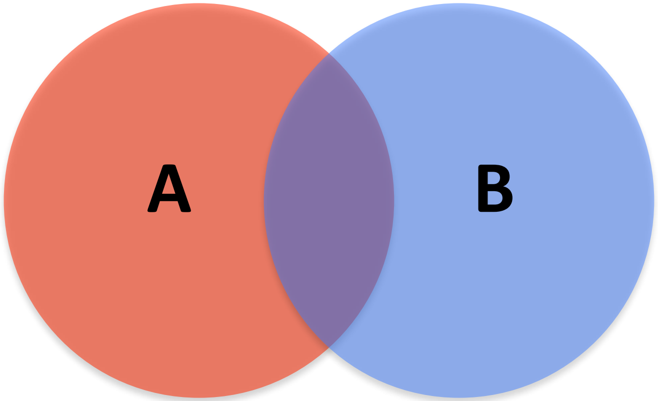
MATHEMATICAL LOGICS

Notations:

A=true [red] B=true [blue]	A or B true: A⋂B	Intersection: red **and** blue
	A and B true: AUB	Union: red **or** blue
A is untrue:	!A or A‘	Complement: all but red
A=true A’=false	A and only A is true	
A=true B=false	A⋂B’	
	AUB’	

The **Venn diagrams** display these logical notations:





MATHEMATICAL LOGICS

Truth table: is a table defining the results of logical operation on logical variables.

For example: the multiplication of p (positive) and n (negative) numbers:

	p	n
p	p	n
n	n	p

De Morgan's law:

$$(A \cap B)' = A' \cup B'$$

$$(A \cup B)' = A' \cap B'$$

Or

The complement of the union of two sets is the same as the intersection of their complements;

The complement of the intersection of two sets is the same as the union of their complements.

Equality:

If A then B implies that if B then A, therefore A=B

Logical operations are at the basis of computer hardware.

Logics expands mathematics of numbers

Gödel 1906–1976 proved that (roughly) any consistent set of axioms contains laws that are correct, but cannot be proven using these axioms alone. This means that every mathematical theory can be extended.

This theorem shook mathematicians, since it crumbled the old Euclid belief that Mathematics can be made a complete and self consistent logical field.

Fermat & integers

Number theory

Integers and their properties concerned people from the onset of mathematics. Some presumably simple problems they posed were found very difficult to solve.

The group of integers is an infinite group, displaying counterintuitive properties. For example, the number of integers, number of odds, evens and squares is the same.

Problems in number theory were studies until the 20th century, but were considered pure mathematics, interesting only to experts, but turned to be relevant to everyone in the digital world (e.g. encryption).

Problems in number theory

1. Arithmetic (linear) series, Ax+B
2. Powers and Geometrical series Aq^x (interest in banks, bacteria multiplication)
3. Sums of series
4. Ratio of numbers, common factors, primes
5. Algorithm for calculations (multiplication, division, roots)
6. Induction
7. Algebra in integers (Diophantine equations)

Pierre de Fermat 1601–1665 - Proposed a number of conjectures that concerned mathematicians till today (Fermat's last theorem, proposed by Diaphanous, that $C^n = A^n+B^n$ exists only for n=2, was found as a noted at the margin of a book that he claimed to prove but had no space to document the proof. This was only proven by Andrew Wiles at 1995).

Examples for some integer number hard-to-prove theorems:

- Every prime number of the form 4n+1 can be written uniquely as the sum of two squares
- Every number can be written as the sum of four squares.
- 1+2^(2^N) are primes. Fermat checked for n<5 and indeed 2,3,5,17,257,65537 are primes, but for N=5 Euler showed that $4294967297 = 2^{32}+1$ divides by 641
- N is a prime if and only if 2^N-2 divides by N

This is not true: 2^{341} -2 divides by 341 but 341=11*34 therefore not a prime.

- **Fermat** showed that sum of inverse integers from 1 till N grows infinitely, approximately as log(N)
- The sum of inverse primes till p grows to infinity as log(log(p)) (**Euler**)
- But the sum of inverse squares converges
- Fermat proposed that the density of primes near p is log(1/p)
  this was proven by **Jacques Salomon Hadamard** 1865 –1963.
- The number of primes till N is roughly $N/\ln(N)$

Open problems

- Is there an infinite number of primes of the form n^2+1
- Is there an infinite number of consecutive primes p,p+2
- Can we write every odd number (>2) as sum of two primes (**Goldbach’s** conjecture)

Fermat’s Little Theorem

If p is a prime and a does not have p as a factor, then a^p /p has as remnant of a

$$a^p = a \mod(p)$$

As often for true theorems, there have been a number of proofs proposed by different mathematicians since **Fermat** published his conjecture.

See:

https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem

A proof by induction:

For every 0<k<p the binomial coefficient $(^p{}_k)$=p!/k!/(p-k)! divides by p, since the nominator divides by p but not the denominator (both factors < p, and p is a prime).

Thus, for k=1 till p-1 $(^p{}_k)=0$ (mod p). For k=0 & k=p $(^p{}_k)=1$ (mod p)

Therefore:

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

Now prove by induction on a: a^p (mod p) = a (mod p)

True for a=1 . Assume true for a show true for (a+1): apply above for b=1:

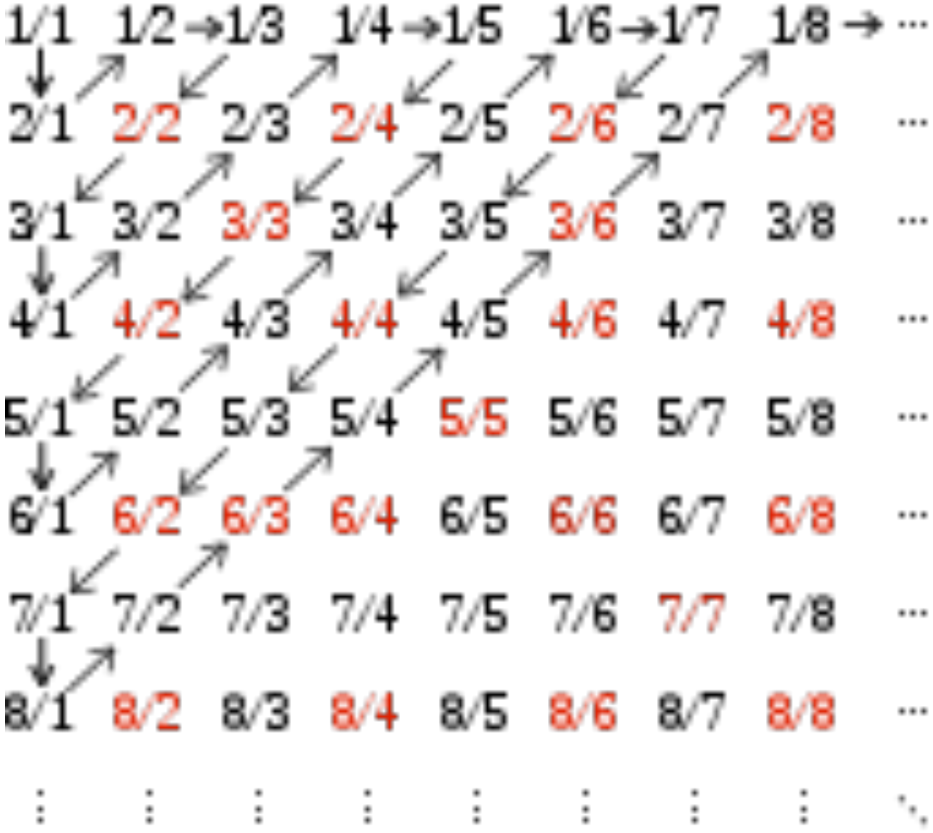
$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

GROUPS

George Cantor 1845-1918 Group theory

$\aleph_0$ is the sign for a countable group.

It is simple to understand that integers are countable. But Cantor showed that rational numbers are too countable. He proved it by one-to-one correspondence (constructive proof):



1/1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	···
2/1	2/2	2/3	2/4	2/5	2/6	2/7	2/8	···
3/1	3/2	3/3	3/4	3/5	3/6	3/7	3/8	···
4/1	4/2	4/3	4/4	4/5	4/6	4/7	4/8	···
5/1	5/2	5/3	5/4	5/5	5/6	5/7	5/8	···
6/1	6/2	6/3	6/4	6/5	6/6	6/7	6/8	···
7/1	7/2	7/3	7/4	7/5	7/6	7/7	7/8	···
8/1	8/2	8/3	8/4	8/5	8/6	8/7	8/8	···
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋱

On the other hand, the irrational numbers are not countable: the proof is a counter-example: Supposed we listed in order all irrational numbers between 0 and 1:

1 ↔ 0.112452...

2 ↔ 0.743212...

3 ↔ 0.213945...

4 ↔ 0.432912...

5 ↔ 0.394854...

...

If the list contains a line with a finite number of digits after the decimal point, we add zeroes. Now we create a value consisting of the first digit different from the first in the list (red), the second digit different from the corresponding digit in second (green) and so on. For example: 0.85863...

We are sure the value we created does not appear in the above list., since every line has at least one different digit.

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

But this contradicts our assumption that we listed all irrational numbers, implying that the Cardinality (extending the concept of “size” for infinite groups) of irrationals is bigger than of rationales, and is not countable. Cantor assumed that there is no group with intermediate cardinality, but this was never proved.

c