ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΟΜΕΑΣ ΜΑΘΗΜΑΤΙΚΩΝ

Οι Πρώτοι Αριθμοί

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
της

ΛΑΡΕΝΤΖΑΚΗ ΕΥΑΓΓΕΛΙΑ

Επιβλέπουσα : Λαμπροπούλου Σοφία
Αν. Καθηγήτρια Ε.Μ.Π.

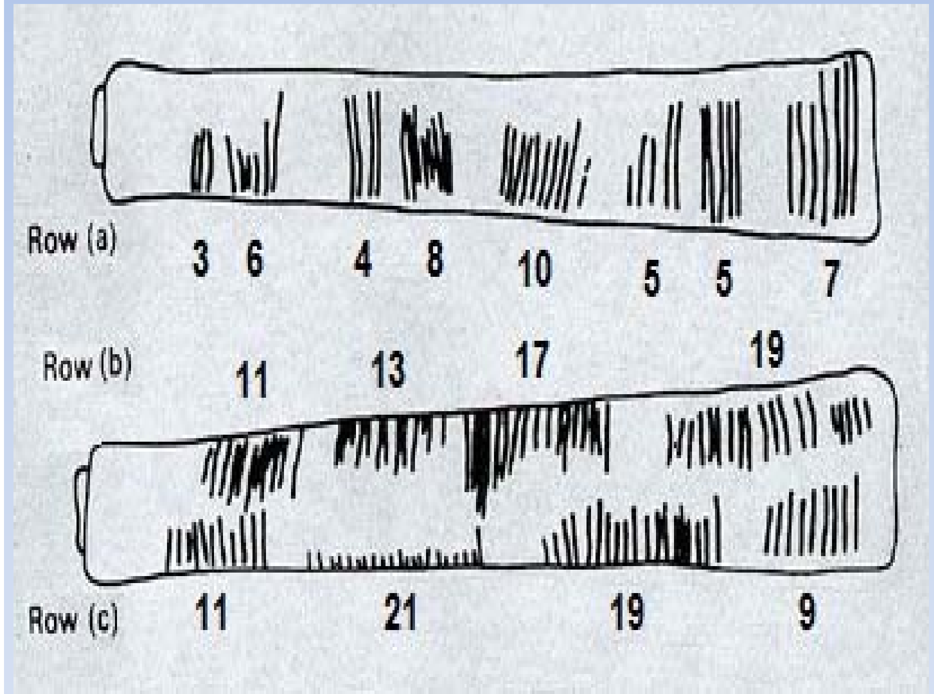
Αθήνα, Ιούνιος 2012

Ορισμός 1:

Ένας ακέραιος αριθμός μεγαλύτερος του ένα λέγεται *πρώτος αριθμός*,
αν οι μόνοι θετικοί διαιρέτες του (παράγοντες) είναι το ένα και ο ίδιος ο αριθμός.
Για παράδειγμα, οι πρώτοι πρώτοι αριθμοί είναι οι 2, 3, 5, 7, 11, 13...

Παλαιολιθική Εποχή

Οστό Ishango



Αιγύπτιοι-Βαβυλώνιοι

- Πάπυρος του Rhynd
- Βαβυλωνιακά δισκία με πίνακες πρώτων αριθμών

Αρχαίοι Έλληνες

- **Ορισμός 2:**

Τέλειος αριθμός ονομάζεται
ο αριθμός που το άθροισμα των διαιρετών του
ισούται με τον ίδιο τον αριθμό.
Για παράδειγμα ο αριθμός 6 έχει διαιρέτες του τους 1,2,3 και 1+2+3=6.

- **Ορισμός 3:**

Ένα ζεύγος *φιλικών αριθμών*
είναι ένα ζεύγος αριθμών που οι διαιρέτες του ενός
έχουν ως άθροισμα τον άλλο και αντίστροφα.
Για παράδειγμα οι αριθμοί 220 και 284.

Ευκλείδης

Θεώρημα 1 (Ευκλείδης 400 π.Χ.)**:**

Το σύνολο των πρώτων αριθμών είναι άπειρο.

Θεώρημα 3 (Το ΘεμελιώδεςΘεώρημα της Αριθμητικής):

Κάθε φυσικός αριθμός $n \neq 0$ *εκφράζεται μονοσήμαντα ως γινόμενο πρώτων αριθμών, όχι κατ' ανάγκη διαφόρων μεταξύ τους. Η σειρά των παραγόντων δεν λαμβάνεται υπόψη.*

•Ορισμός 4:

Οι αριθμοί της μορφής $F_n = 2^{2^n} + 1$ όπου $n = 0, 1, 2, \ldots$ ονομάζονται *αριθμοί του Fermat.*

•Ορισμός 5:

Ορίζουμε την συνάρτηση $\pi : \mathbb{R} \to \mathbb{N}$ ως: $\pi(x) := \#\{p \leq x : p \in P\}$ τον αριθμό των πρώτων αριθμών που είναι μικρότεροι ή ίσοι από τον πραγματικό αριθμό x .

Ερατοσθένης

Ρωμαίοι- Άραβες

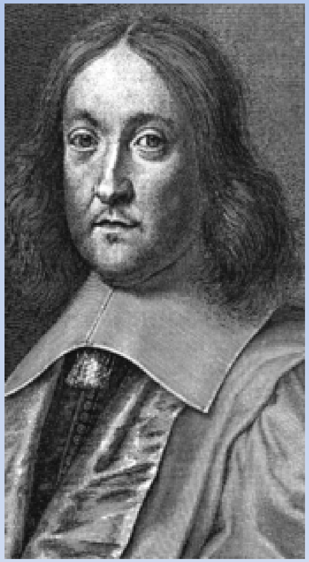
•Ορισμός 6:

Πρώτοι Thabit αριθμοί ονομάζονται οι αριθμοί της μορφής $p_n = 3 \times 2^n - 1$ και ονομάστηκαν έτσι από τον Thabit ibn Qurra που ήταν ο πρώτος που τους μελέτησε.

Θεώρημα 4 (Thabit):

Για $n > 1$ *, θεωρούμε* $p_n = 3 \times 2^n - 1$ *και* $q_n = 9 \times 2^{2n-1}$*. Αν* p_{n-1}, p_n $\kappa\alpha\iota$ q_n *είναι πρώτοι αριθμοί, τότε οι* $\alpha = 2^n p_{n-1} p_n$ *και* $b = 2^n q_n$ *είναι φιλικοί αριθμοί.*

Pierre de Fermat



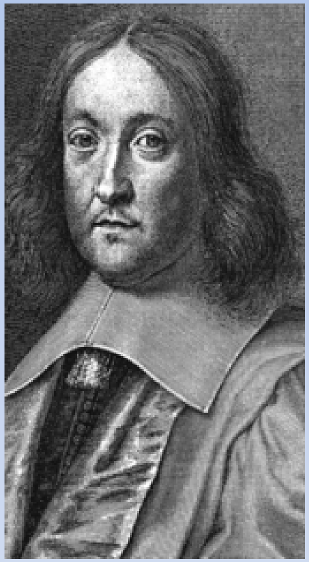
•***<u>Θεώρημα 5</u>***
<u>(μικρό Θεώρημα του Fermat):</u> *Έστω p πρώτος αριθμός. Τότε για κάθε ακέραιο a έχουμε $a^p = a \bmod p$.*

•***<u>Εικασία του Fermat:</u>*** *Για όλους τους φυσικούς αριθμούς n, οι αριθμοί $2^{2^n}+1$ είναι πρώτοι.*

•***<u>Θεώρημα 6 (Gauss):</u>*** *Ένα κανονικό ν-γωνο, όπου ν πρώτος αριθμός, μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν και μόνο αν ο ν είναι πρώτος αριθμός του Fermat!*

•***<u>Θεώρημα 7:</u>*** *Ένα κανονικό m-γωνο μπορεί να κατασκευαστεί με κανόνα και διαβήτη αν και μόνο αν $m = 2^s \times p_1 p_2 ... p_l$, όπου $p_1, p_2, ..., p_l$ είναι πρώτοι αριθμοί του Fermat διαφορετικοί μεταξύ τους.*

Pierre de Fermat



<u>***Θεώρημα 8 (Fermat, 1640):***</u>

Ένας περιττός p πρώτος αριθμός μπορεί να γραφτεί ως

$$p = x^2 + y^2$$

όπου x, y ακέραιοι αν και μόνο αν $p \equiv 1 \bmod 4$.

Marin Mersenne

Οι αριθμοί του τύπου $p = 2^n - 1$ ονομάζονται ‘*αριθμοί Mersenne*’ και συμβολίζονται M_n .

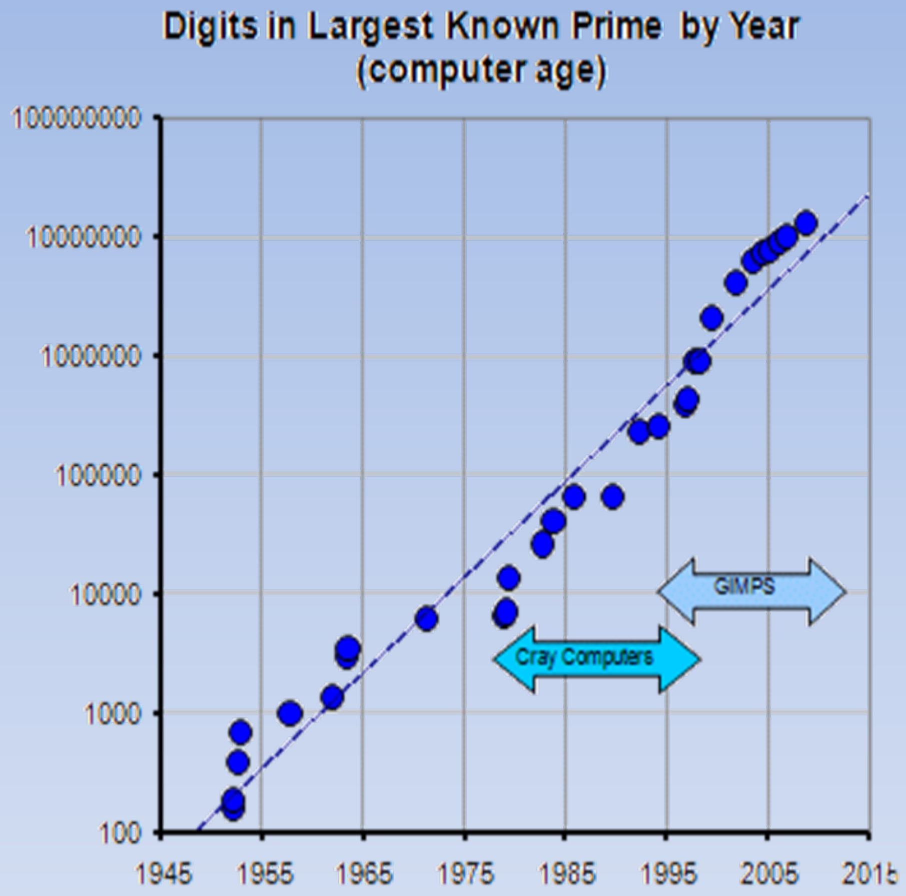
Ρεκόρ πρώτων αριθμών πριν την εποχή των ηλεκτρονικών υπολογιστών				
Αριθμός	**Ψηφία**	**Χρονιά**	**Μαθηματικός**	**Μέθοδος**
$2^{17}-1$	6	1588	Cataldi	δοκιμαστικές διαιρέσεις
$2^{19}-1$	6	1588	Cataldi	δοκιμαστικές διαιρέσεις
$2^{31}-1$	10	1772	Euler	δοκιμαστικές διαιρέσεις
$(2^{59}-1)/179951$	13	1867	Landry	δοκιμαστικές διαιρέσεις
$2^{127}-1$	39	1876	Lucas	ακολουθίες Lucas
$(2^{148}+1)/17$	44	1951	Ferrier	Θεώρημα του Proth (1878)

Pietro Cataldi

Edouard Lucas

Ρεκόρ πρώτων αριθμών την εποχή των ηλεκτρονικών υπολογιστών				
Αριθμός	**Ψηφία**	**Χρονιά**	**Η/Υ**	**Μαθηματικός**
$180(M_{127})^2+1$	79	1951	EDSAC1	Miller&Wheeler
M_{521}	157	1952	SWAC	Robinson(Jan30)
M_{607}	183	1952	SWAC	Robinson(Jan30)
M_{1279}	386	1952	SWAC	Robinson(June25)
M_{2203}	664	1952	SWAC	Robinson (Oct 7)
M_{2281}	687	1952	SWAC	Robinson (Oct 9)
M_{3217}	969	1957	BESK	Riesel
M_{4423}	1332	1961	IBM7090	Hurwitz
M_{9689}	2917	1963	ILLIAC 2	Gillies
M_{9941}	2993	1963	ILLIAC 2	Gillies
M_{11213}	3376	1963	ILLIAC 2	Gillies
M_{19937}	6002	1971	IBM360/91	Tuckerman
M_{21701}	6533	1978	CDC Cyber 174	Noll & Nickel
M_{23209}	6987	1979	CDC Cyber 174	Noll
M_{44497}	13395	1979	Cray 1	Nelson&Slowinski
M_{86243}	25962	1982	Cray 1	Slowinski
M_{132049}	39751	1983	Cray X-MP	Slowinski
M_{216091}	65050	1985	Cray X-MP/24	Slowinski
$391581 \times 2^{216193}-1$	65087	1989	Amdahl 1200	Amdahl Six

M_{756839}	227832	1992	Cray-2	Slowinski & Gage
M_{859433}	258716	1994	Cray C90	Slowinski & Gage
$M_{1257787}$	378632	1996	Cray T94	Slowinski & Gage
$M_{1398269}$	420921	1996	Pentium(90Mhz)	Armengaud,Woltman
$M_{2976221}$	895932	1997	Pentium(100Mhz)	Spence, Woltman
$M_{3021377}$	909526	1998	Pentium(200Mhz)	Clarkson,Woltman, Kurowski
$M_{6972593}$	2098960	1999	Pentium(350Mhz)	Hajratwala,Woltman, Kurowski
$M_{13466917}$	4053946	2001	AMDT-Bird(800 Mhz)	Cameron,Woltman, Kurowski
$M_{20996011}$	6320430	2003	Pentium (2 GHz)	Shafer,Woltman, Kurowski
$M_{24036583}$	7235733	2004	Pentium4(2.4GHz)	Findley,Woltman, Kurowski
$M_{25964951}$	7816230	2005	Pentium4(2.4GHz)	Nowak,Woltman, Kurowski
$M_{30402457}$	9152052	2005	Pentium 4(2GHz upgraded to3GHz)	Cooper,Boone, Woltman, Kurowski
$M_{32582657}$	9808358	2006	Pentium 4 (3 GHz)	Cooper,Boone, Woltman, Kurowski
$M_{43111609}$	12978189	2008	Intel Core 2Duo E6600CPU(2.4GHz)	E_Smith,Woltman, Kurowski



οι αριθμοί των ψηφίων γνωστών πρώτων αριθμών μετά την ανακάλυψη του ηλεκτρονικού υπολογιστή

Τύποι παραγωγής Πρώτων Αριθμών

«Οι μαθηματικοί έχουν προσπαθήσει μάταια μέχρι σήμερα να ανακαλύψουν κάποια τάξη στην ακολουθία των πρώτων αριθμών, και έχουμε λόγους να πιστεύουμε πως αυτό είναι ένα μυστήριο στο οποίο ο ανθρώπινος νους δεν πρόκειται να διεισδύσει ποτέ.»

Euler

Η συνάρτηση *π(x)*

- Η συνάρτηση που δίνει το πλήθος των πρώτων αριθμών των μικρότερων ή ίσων ενός αριθμού x συμβολίζεται $\pi(x)$.
- $\lim_{x \to +\infty} \pi(x) = +\infty$

Carl Friedrich Gauss

x	$\pi(x)$	$\frac{x}{\log(x)}$	$\pi(x)/\frac{x}{\log(x)}$
10	4	4,3	0,93
10^2	25	21,7	1,15
10^3	168	144,8	1,16
10^4	1229	1086	1,13
10^5	9592	8686	1,10
10^6	78498	72382	1,08
10^7	664579	620420	1,07
10^8	5761455	5428681	1,06
10^9	50847534	48254942	1,05
10^{10}	455052511	434294482	1,048

πίνακας της συνάρτησης $\pi(x)$ εν συγκρίσει με την $\frac{x}{\log(x)}$ όπου $\log(x)$ ο φυσικός λογάριθμος του x .

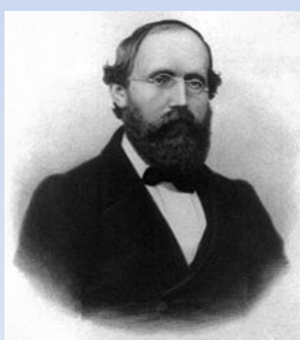
Το Θεώρημα Πρώτων Αριθμών

<u>Θεώρημα 11(Θεώρημα των πρώτων αριθμών):</u>

Ισχύει ότι:

$$\pi(x) \sim \frac{x}{\log(x)}$$

Pafnuty Chebyshev

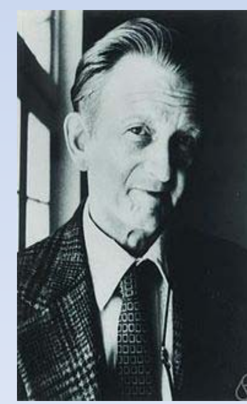


Bernhard Riemann

J.Hadamard

De Vallee Poussin

P.Erdos



A.Selberg

Θεώρημα Bertrand

<u>Θεώρημα 13 (Θεώρημα Bertrand):</u> *Για κάθε* $n \geq 1$, *υπάρχει κάποιος πρώτος αριθμός* p *με* $n < p \leq 2n$.

Θεώρημα Wilson

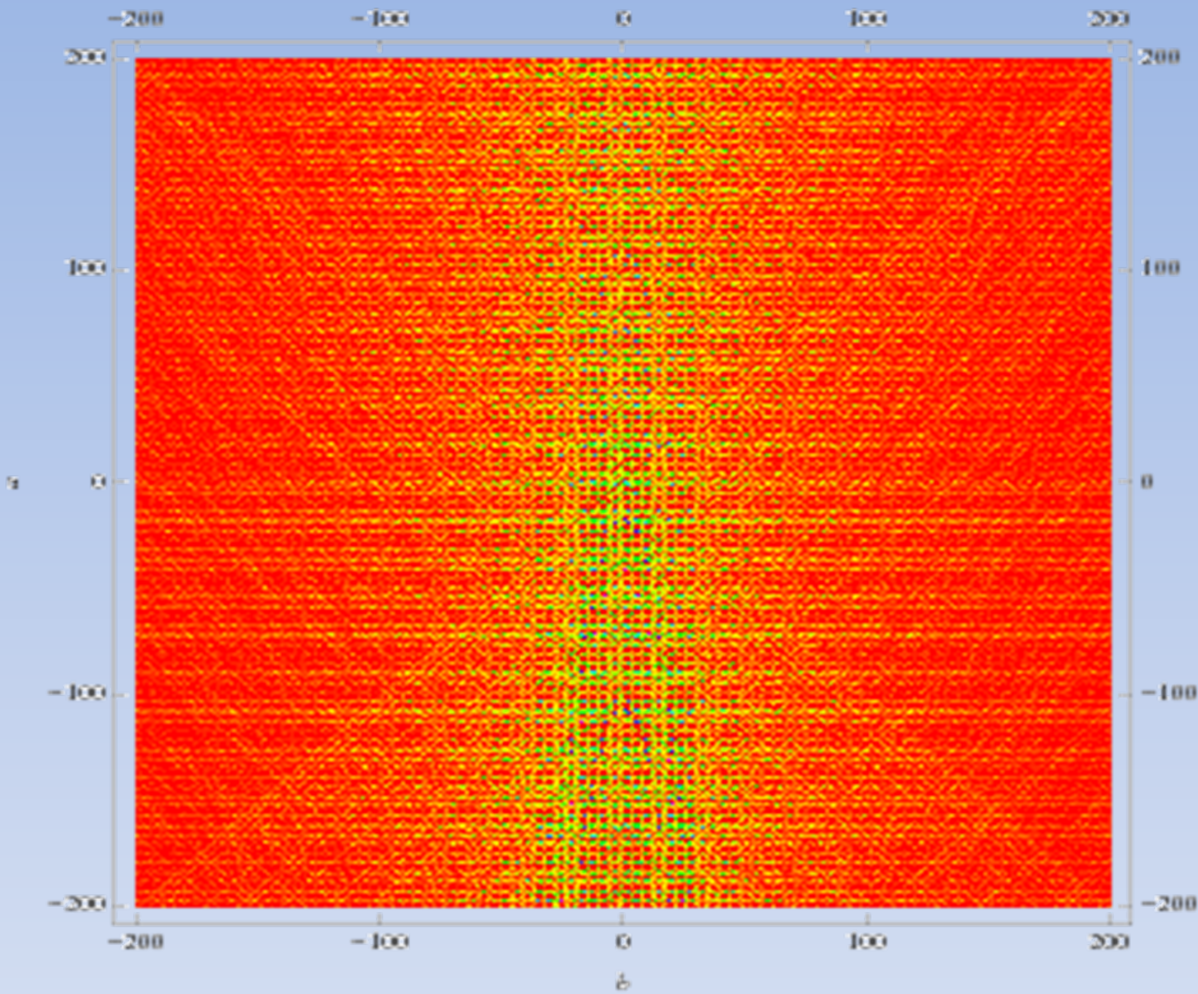
<u>Θεώρημα 14 (Θεώρημα Wilson) (John Wilson,1770):</u> *Ένας φυσικός αριθμός* $p > 1$ *είναι πρώτος αριθμός αν και μόνο αν* $(p-1)! \equiv -1 \bmod p$ *.*

Πολυώνυμα και πρώτοι αριθμοί

<u>Θεώρημα 16 (Christian Goldbach,1752):</u> *Δεν υπάρχει μη σταθερό πολυώνυμο με ακέραιους συντελεστές που να μπορεί να δώσει πρώτους αριθμούς για όλες τις ακέραιες τιμές της μεταβλητής.*

- Το πιο γνωστό πολυώνυμο που παράγει (ενδεχομένως κατά απόλυτη τιμή) μόνο πρώτους αριθμούς είναι το n^2+n+41, το βρήκε ο Euler και δίνει διακριτούς πρώτους αριθμούς για 40 συνεχόμενους ακεραίους.

πολυώνυμο	πρώτοι αριθμοί από 0 έως n	διαφορετικοί μεταξύ τους πρώτοι αριθμοί	αναφορές
$\frac{1}{4}(n^5 - 133n^4 + 6729n^3 - 158379n^2 + 1720294n - 6823316)$	56	57	Dress and Landreau (2002), Gupta (2006)
$\frac{1}{36}(n^6 - 126n^5 - 153066n^3 + 1987786n^2 - 13055316n + 34747236)$	54	55	Wroblewski and Meyrignac (2006)
$n^4 - 97n^3 + 3294n^2 - 45458n + 213589$	49	49	Beyleveld (2006)
$n^5 - 99n^4 + 3588n^3 - 56822n^2 + 348272n - 286397$	46	47	Wroblewski and Meyrignac (2006)
$-66n^3 + 3845n^2 - 60897n + 251831$	45	46	Kazmenko and Trofimov (2006)
$36n^2 - 810n + 2753$	44	45	Fung and Ruby(A050268)
$3n^3 - 183n^2 + 3318n - 18757$	46	43	S. M. Ruiz (pers. comm., Nov. 20, 2005)
$47n^2 - 1701n + 10181$	42	43	Fung and Ruby(A050267)
$103n^2 - 4707n + 50383$	42	43	Speiser (pers. comm., Jun. 14, 2005)
$n^2 - n + 41$	40	40	Euler(A005846)
$42n^3 + 270n^2 - 26436n + 250703$	39	40	Wroblewski and Meyrignac
$43n^2 - 537n + 2971$	34	35	J. Brox (pers. comm., Mar. 27, 2006)
$8n^2 - 488n + 7243$	61	31	F. Gobbo (pers. comm., Dec. 27, 2005)
$6n^2 - 342n + 4903$	57	29	J. Brox (pers. comm., Mar. 27, 2006)
$2n^2 + 29$	28	29	Legendre (1798) (A007641)
$7n^2 - 371n + 4871$	23	24	F. Gobbo (pers. comm., Dec. 26, 2005)
$n^4 + 29n^2 + 101$	19	20	E. Pegg, Jr. (pers. comm., Jun. 14, 2005)
$3n^2 + 39n + 37$	17	18	A. Bruno (pers. comm., Jun. 12, 2009)
$n^2 + n + 17$	15	16	Legendre(A007635)
$4n^2 + 4n + 59$	13	14	Honaker(A048988)
$2n^2 + 11$	10	11	(A050265)
$n^3 + n^2 + 17$	10	11	(A050266)



Διάγραμμα που απεικονίζει τον αριθμό των πρώτων αριθμών που παράγονται από τετραγωνικά πολυώνυμα της μορφής $x^2 + ax + b$ από το -200 ως το 200.

Leonhard Euler

- Επέκτεινε το ‘μικρό Θεώρημα του Fermat’
- Εισήγαγε την ‘φ-συνάρτηση Euler’
- Παραγοντοποίησε τον 5ο αριθμό του Fermat
- Βρήκε 60 ζευγάρια φιλικών αριθμών
- Διατύπωσε αυτό που ονομάζεται ‘Law of Quadratic Reciprocity’
- Ίδρυσε την Αναλυτική Θεωρία Αριθμών
- Απέδειξε πως ο $2^{31}-1$ είναι πρώτος

Johann Lejeune Dirichlet και αριθμητικοί πρόοδοι

<u>Θεώρημα του Dirichlet:</u> *Αν* a *και* b *είναι θετικοί ακέραιοι που είναι πρώτοι μεταξύ τους, το πολυώνυμο* $ax+b$ *δίνει άπειρους πρώτους αριθμούς καθώς το* x *διατρέχει όλους τους θετικούς ακεραίους*

- 17 Μαΐου 2008: εύρεση της 1ης γνωστής αριθμητικής προόδου 25 πρώτων αριθμών από τους Wróblewski και Raanan Chermoni
- 12 Απριλίου 2010: εύρεση της 1ης γνωστής αριθμητικής προόδου 26 πρώτων αριθμών από τον Benoãt Perichon με λογισμικό των Wróblewski και Geoff Reynolds

Τύποι παραγωγής πρώτων που χρησιμοποιούν την συνάρτηση ‘ακέραιο μέρος’ (floor function)

<u>Θεώρημα 17</u> *<u>(William H. Mills, 1947):</u>* *Υπάρχει πραγματικός αριθμός* λ *τέτοιος ώστε για όλα τα* $n=1,2,...$ *ο αριθμός* $\lfloor \lambda^{3^n} \rfloor$ *είναι πρώτος.*
(όπου $\lfloor a \rfloor$ *το ακέραιο μέρος του* a*).*

<u>Θεώρημα 18</u> *<u>(E. M. Wright):</u>* *Υπάρχει πραγματικός αριθμός* μ *τέτοιος ώστε κάθε αριθμός της μορφής*

$$\left\lfloor 2^{2^{\cdot^{\cdot^{2^{\mu}}}}} \right\rfloor$$

είναι πρώτος αριθμός .

<u>Θεώρημα 19</u> *<u>(E. M. Wright 1951, Ribenboim 1996):</u>* *Υπάρχει πραγματικός αριθμός* $\omega \approx 1,9287800$ *τέτοιος ώστε για όλα τα* $n=1,2,...$ *ο αριθμός* $\lfloor 2\,\omega\, n \rfloor$ *είναι πρώτος αριθμός.*

Τύποι παραγωγής πρώτων που χρησιμοποιούν την συνάρτηση ‘ακέραιο μέρος’ (floor function)

Ένας σημαντικός τύπος που δημοσιεύτηκε το 1964 από τον Willans:

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{n} \left(\sum_{x=1}^{m} \left\lfloor \cos^2 \pi \frac{(x-1)!+1}{x} \right\rfloor \right)^{-\frac{1}{n}} \right\rfloor$$

Μερικά ακόμη άλυτα προβλήματα πρώτων αριθμών

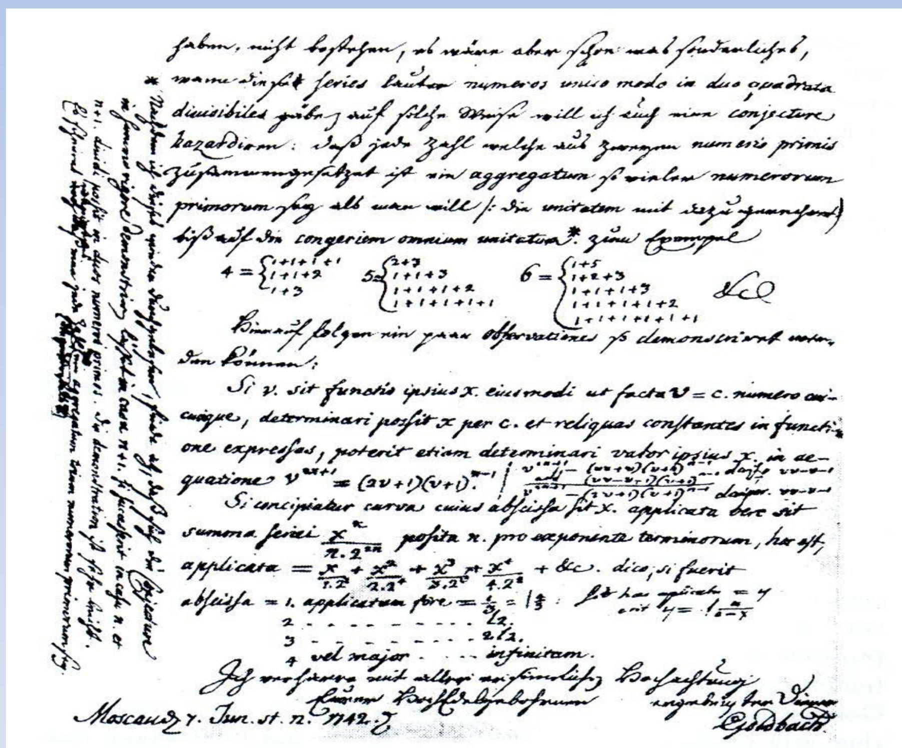
1. Υπάρχει ζυγός αριθμός >2 που να μην εκφράζεται ως άθροισμα δύο περιττών πρώτων αριθμών; (εικασία του Goldbach)
2. Υπάρχουν άπειροι δίδυμοι πρώτοι αριθμοί;
3. Υπάρχει ζυγός αριθμός >2 που να μην εκφράζεται ως διαφορά δύο πρώτων αριθμών;
4. Υπάρχουν άπειροι πρώτοι 'αριθμοί Mersenne';
5. Υπάρχουν άπειροι 'πρώτοι αριθμοί του Fermat';
6. Υπάρχουν άπειροι πρώτοι αριθμοί της μορφής x^2+1 όπου x ακέραιος;
7. Υπάρχουν άπειροι πρώτοι της μορφής x^2+k (k γνωστό);
8. Υπάρχει πάντα τουλάχιστον ένας πρώτος αριθμός μεταξύ των n^2 και $(n+1)^2$ για κάθε ακέραιο $n \geq 1$;
9. Υπάρχει πάντα τουλάχιστον ένας πρώτος αριθμός μεταξύ των n^2 και n^2+n για κάθε ακέραιο $n \geq 1$;
10. Υπάρχουν άπειροι πρώτοι των οποίων όλα τα ψηφία να είναι 1; (για παράδειγμα δύο τέτοιοι πρώτοι είναι οι: 11 και 11.111.111.111.111.111.111.111)

Μερικά ακόμη άλυτα προβλήματα πρώτων αριθμών

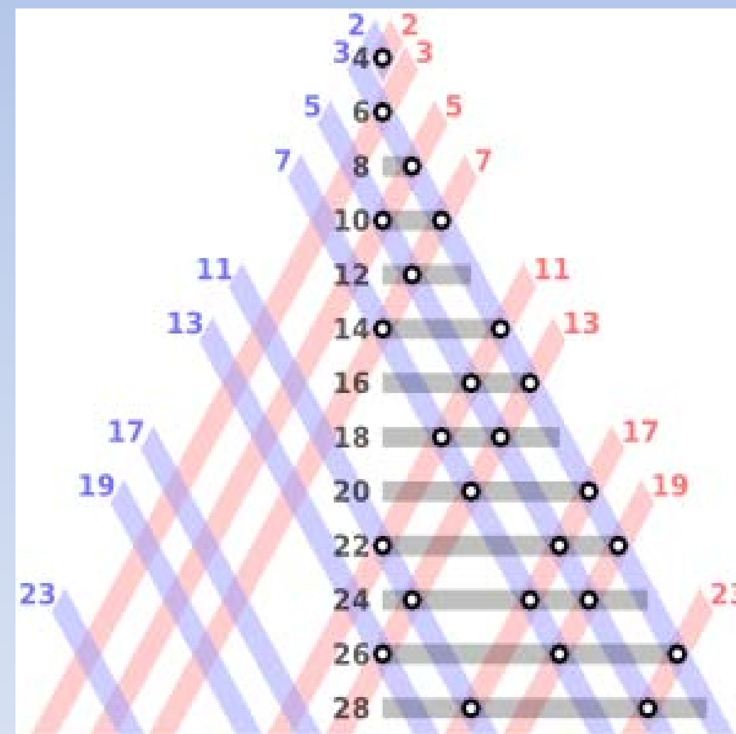
11. Υπάρχουν άπειροι πρώτοι της μορφής $n\#+1$ και $n\#-1$;
12. Υπάρχουν άπειροι πρώτοι της μορφής $n!+1$ και $n!-1$;
13. Περιέχει η ακολουθία Fibonacci (της οποίας κάθε όρος προκύπτει από το άθροισμα των δύο προηγούμενων : 1,1,2,3,5,8,13,…) άπειρους πρώτους αριθμούς;
14. Υπάρχει αριθμητική πρόοδος με διαδοχικούς πρώτους αριθμούς για κάθε πεπερασμένο μήκος αυτής; (για παράδειγμα η: 251,257,263,269 έχει μήκος 4 και το μεγαλύτερο γνωστό παράδειγμα έχει μήκος 10)
15. Υπάρχουν άπειρα σύνολα τριών διαδοχικών πρώτων αριθμών σε αριθμητική πρόοδο; (ισχύει για μη διαδοχικούς πρώτους αριθμούς)
16. Το πολυώνυμο n^2-n+41 δίνει πρώτους για $0 \le n \le 40$.Υπάρχουν άπειροι τέτοιοι πρώτοι αριθμοί; Το ίδιο ερώτημα ισχύει και για $n^2-79n+1601$ που δίνει πρώτους για $0 \le n \le 79$.

Η εικασία του Goldbach

‘Κάθε άρτιος ακέραιος μεγαλύτερος του 2 μπορεί να εκφραστεί ως το άθροισμα δύο πρώτων αριθμών’

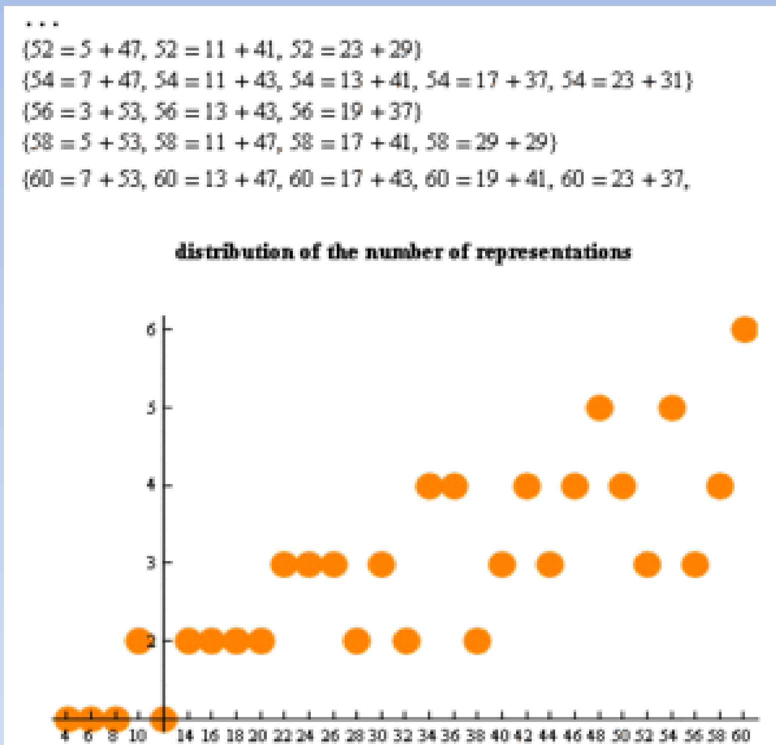


Το γράμμα από τον Goldbach προς τον Euler



Πώς γράφονται οι αριθμοί 4-28 ως άθροισμα δύο πρώτων αριθμών.

Η εικασία του Goldbach

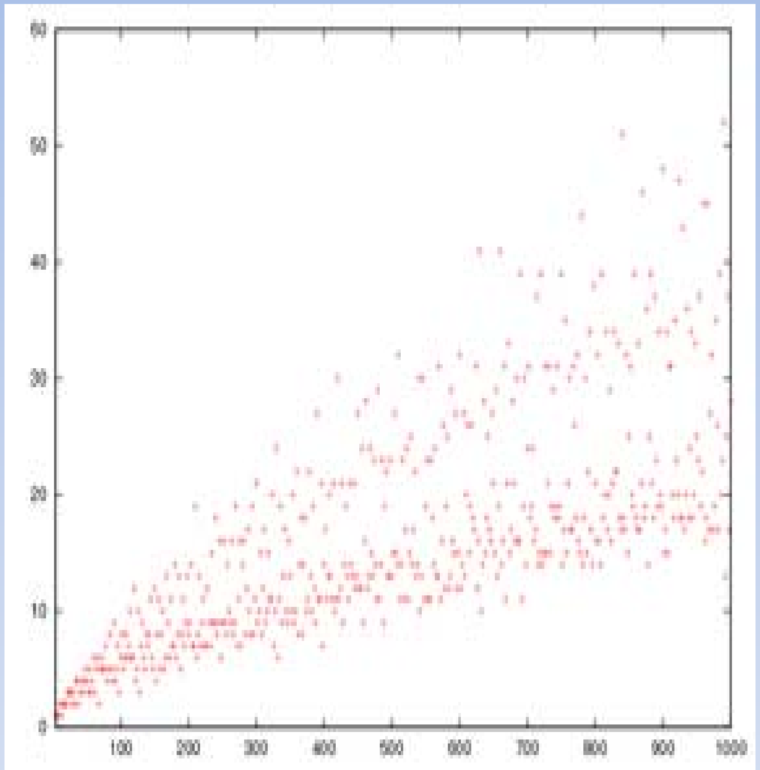


Ο αριθμός των τρόπων που ένας άρτιος αριθμός μπορεί να παρασταθεί ως το άθροισμα 2 πρώτων.

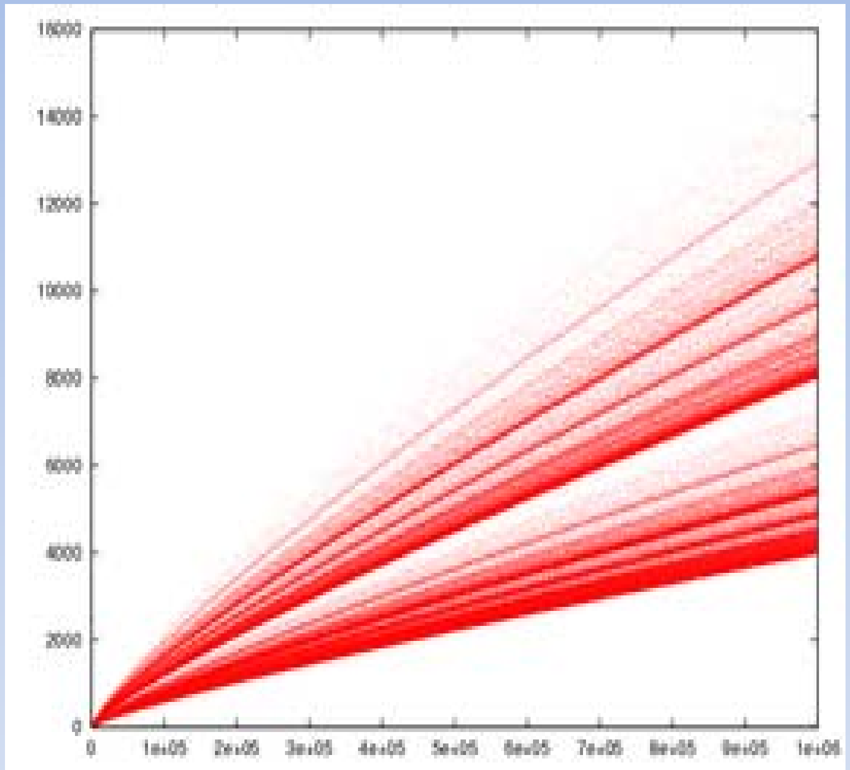
έλεγχος για $n \leq \cdots$	πηγή
1×10^{4}	Desboves 1885
1×10^{5}	Pipping 1938
1×10^{8}	Stein and Stein 1965
2×10^{10}	Granville et al. 1989
4×10^{11}	Sinisalo 1993
1×10^{14}	Deshouillers et al. 1998
4×10^{14}	Richstein 1999, 2001
2×10^{16}	Oliveira e Silva (Mar. 24, 2003)
6×10^{16}	Oliveira e Silva (Oct. 3, 2003)
2×10^{17}	Oliveira e Silva (Feb. 5, 2005)
3×10^{17}	Oliveira e Silva (Dec. 30, 2005)
12×10^{17}	Oliveira e Silva (Jul. 14, 2008)

Υπολογισμοί για την επαλήθευση της εικασίας του Goldbach

Η εικασία του Goldbach



$4 \leq n \leq 1000$



$4 \leq n \leq 1000000$

Δίδυμοι πρώτοι αριθμοί

<u>Ορισμός 9:</u> *Δίδυμοι πρώτοι αριθμοί* καλούνται οι πρώτοι αριθμοί της μορφής $(p, p+2)$

<u>Θεώρημα 20 (Θεώρημα Brun):</u> *Ο αριθμός που προκύπτει από την πρόσθεση των αντίστροφων των περιττών δίδυμων πρώτων αριθμών, συγκλίνει σε έναν συγκεκριμένο αριθμό (ο αριθμός αυτός έχει ονομαστεί σταθερά του Brun) που εκφράζει την σπανιότητα των δίδυμων πρώτων, ακόμα και αν υπάρχουν άπειροι από αυτούς.* $B = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\cdots,$

25 Δεκέμβρη του 2011: ρεκόρ δίδυμων πρώτων με 200700 ψηφία (υπολογιστικό πρόγραμμα PrimeGrid)

«…η πρόοδος της γνώσης μας ως προς τους αριθμούς εξελίσσεται όχι μόνο από αυτά που ήδη γνωρίζουμε για αυτούς, αλλά από το ότι συνειδητοποιούμε τι ακόμη δεν γνωρίζουμε γι’ αυτούς.»

Sierpinski