Αριθμοί Mersenne - Πρώτοι Mersenne

Σωτήριος Καλπάκογλου

Ημερομηνία Παράδοσης: 29/10/2014

1 Ιστορική Αναδρομή

Για πολλά χρόνια πολλοί μαθηματικοί, θεωρούσαν ότι οι αριθμοί της μορφής $2^n - 1$ είναι πρώτοι, για κάθε αριθμό $n \in \mathbb{N}$. Το 1536, ο Hudalricus Regius έδειξε για πρώτη φορά ότι ο αριθμός $2^{11} - 1$ είναι σύνθετος αριθμός, και μάλιστα $2^{11} - 1 = 2047 = 23 \cdot 89$.

Το 1603 ο Pietro Cataldi διαπίστωσε ορθά, ότι οι αριθμοί $2^{17} - 1$ και $2^{19} - 1$ είναι πρώτοι, αλλά ωστόσο ανέφερε εσφαλμένα ότι το $2^n - 1$ είναι πρώτος και για τους πρώτους αριθμούς $n = 23, 29, 31, 37$. Το 1640, ο Fermat απέδειξε το σφάλμα του Cataldi για τους πρώτους 23 και 37. Το σφάλμα για τον πρώτο 29 απέδειξε το 1738 ο Euler, ενώ λίγο αργότερα, απέδειξε την ορθότητα του ισχυρισμού του Cataldi για τον αριθμό 31.

Οι αριθμοί Mersenne, πήραν το όνομά τους από το Γάλλο μοναχό, Marin Mersenne (1588 - 1648) ο οποίος ασχολήθηκε με την εικασία του Pietro Cataldi και δήλωσε ότι ο αριθμός $2^n - 1$ είναι πρώτος για τους $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$, και είναι σύνθετος για κάθε άλλο ακέραιο μικρότερο του 257. Αν και δεν είναι σωστός αυτός ο ισχυρισμός, το όνομά του συνδέθηκε με τους πρώτους αριθμούς με αυτήν την ιδιότητα.

Όταν ένας αριθμός είναι της μορφής $2^n - 1$ τότε είναι αριθμός Mersenne.
Όταν ο αριθμός $2^n - 1$ είναι πρώτος, τότε καλείται πρώτος Mersenne.

Εκατό χρόνια αργότερα, το 1750, ο Euler έδειξε ότι ο αριθμός $2^{31} - 1$ είναι πρώτος, ενώ ακόμη έναν αιώνα αργότερα, το 1876, ο Lucas έδειξε ότι ο $2^{127} - 1$ είναι επίσης πρώτος. Αυτός είναι ο μεγαλύτερος πρώτος Mersenne που υπολογίστηκε χωρίς τη βοήθεια υπολογιστή. Επτά χρόνια αργότερα ο Pervouchine έδειξε ότι ο $2^{61} - 1$ είναι πρώτος, έτσι διαπιστώνουμε ότι αυτός είναι ένας από τους αριθμούς που ο Mersenne παρέλειψε. Αργότερα, στις αρχές του $19^{ου}$ αιώνα, ο Powers διαπίστωσε και άλλες ελλείψεις στη λίστα του Mersenne, που ήταν οι αριθμοί $2^{89} - 1$ και $2^{107} - 1$. Μέχρι το 1947 η λίστα του Mersenne, για τους πρώτους $n \leq 257$ οι οποίοι δημιουργούν

πρώτους της μορφής $M_n = 2^n - 1$ έχει ελεγχθεί και διαμορφωθεί ως εξής: $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$.

2 Προκαταρκτικά

Σε αυτή την ενότητα θα παρουσιάσουμε την πολλαπλασιαστική συνάρτηση $\sigma(n)$, την οποία θα χρησιμοποιήσουμε για τον ορισμό των τέλειων αριθμών, καθώς και για κάποιες από τις αποδείξεις των ιδιοτήτων τους.

2.1 Πολλαπλασιαστικές συναρτήσεις, η $\sigma(n)$

Ορισμός 2.1. *Πολλαπλασιαστική συνάρτηση*

Μία συνάρτηση $F : \mathbb{N} \to \mathbb{C}$ καλείται πολλαπλασιαστική, αν και μόνο εάν ισχύουν:

1. $F(1) = 1$
2. $F(n \cdot m) = F(n) \cdot F(m)$ για κάθε $n, m \in \mathbb{N}$ με $(n, m) = 1$.

Ορισμός 2.2. *Έστω αριθμός $n \in \mathbb{N}$. Τότε ορίζουμε τη συνάρτηση $\sigma(n)$ να ισούται με το άθροισμα των διαιρετών του n.*

Θεώρημα 2.1. *Αν $n \in \mathbb{N}$, και $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ η ανάλυσή του σε πρώτους, τότε*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Απόδειξη. Έστω $n \in \mathbb{N}$, και $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ η ανάλυσή του σε πρώτους παράγοντες.

Τότε το άθροισμα των διαιρετών του n, είναι το ανάπτυγμα του γινομένου

$$\sigma(n) = (1 + p_1 + p_1^2 + \ldots + p_1^{a_1}) \cdots (1 + p_k + p_k^2 + \ldots + p_k^{a_k}) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

□

Θεώρημα 2.2. *Η συνάρτηση $\sigma(n)$ είναι πολλαπλασιαστική.*

Απόδειξη. Αρχικά, για $n = 1$, ο μοναδικός διαιρέτης του 1 είναι το 1, οπότε $\sigma(1) = 1$.

Επιπλέον, εάν θεωρήσουμε δύο αριθμούς $n, m \in \mathbb{N}$ με $(n, m) = 1$, θα αποδείξουμε ότι $\sigma(n \cdot m) = \sigma(n) \cdot \sigma(m)$.

Έχουμε την ανάλυση των n, m, με $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ και $m = q_1^{b_1} q_2^{b_2} \dots q_\ell^{b_\ell}$. Δεδομένου ότι $(n, m) = 1$, έχουμε $p_i \neq q_j$, $\forall\, 1 \leq i \leq k$, $1 \leq j \leq \ell$. Έτσι $n \cdot m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \cdot q_1^{b_1} q_2^{b_2} \dots q_\ell^{b_\ell}$.

Υπολογίζουμε λοιπόν,

$$\sigma(n \cdot m) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{a_k+1} - 1}{p_k - 1} \cdot \frac{q_1^{b_1+1} - 1}{q_1 - 1} \cdot \ldots \cdot \frac{q_\ell^{b_\ell+1} - 1}{q_\ell - 1} = \sigma(n) \cdot \sigma(m)$$

. □

2.2 Τετραγωνικά ισοϋπόλοιπα

Ο αριθμός a καλείται *τετραγωνικό ισοϋπόλοιπο* $\bmod m$, εάν η ισοτιμία

$$x^2 \equiv a \pmod{m},$$

με $m \geq 1$ και $(a, m) = 1$ έχει λύση. Εάν η ίδια ισοτιμία δεν έχει λύση, τότε καλείται *τετραγωνικό ανισοϋπόλοιπο* $\bmod m$.

Θεώρημα 2.3. *Έστω περιττός πρώτος p. Τότε υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα* $\bmod p$, *ανά δύο ανισότιμα* $\bmod p$.

Απόδειξη. Ένας αριθμός a είναι τετραγωνικό ισοϋπόλοιπο $\bmod p$, αν και μόνο αν είναι ισότιμος με έναν από τους αριθμούς $1^2, 2^2, \ldots (p-2)^2, (p-1)^2$. Ωστόσο για κάθε αριθμό ξ ισχύει $\xi^2 \equiv (p-\xi)^2 \pmod{p}$, έτσι

$$1^2 \equiv (p-1)^2, 2^2 \equiv (p-2)^2, \ldots, \left(\frac{p-1}{2}\right)^2 \equiv \left(\frac{p+1}{2}\right)^2 \pmod{p}.$$

Οπότε τα στοιχεία του συνόλου $A = \{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$ είναι τετραγωνικά ισοϋπόλοιπα $\bmod p$. Έτσι υπάρχουν το πολύ $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα ανάμεσα στους αριθμούς $1, \ldots, p-1$.

Από την άλλη, θα αποδείξουμε ότι τα στοιχεία του συνόλου A είναι ανά δύο ανισότιμα $\bmod p$. Θα υποθέσουμε λοιπόν ότι υπάρχουν δύο αριθμοί k, ℓ με $1 \leq \ell < k \leq \frac{p-1}{2}$ και έστω ότι $k^2 \equiv \ell^2 \pmod{p}$. Έτσι έχουμε $k^2 - \ell^2 \equiv 0 \pmod{p}$, δηλαδή $(k-\ell)(k+\ell) \equiv 0 \pmod{p}$, το οποίο είναι αδύνατο, αφού τότε το p θα έπρεπε να διαιρεί είτε το $k+\ell$ είτε το $k-\ell$, οι οποίοι είναι μικρότεροι από p. Έτσι εάν θεωρήσουμε R ένα περιορισμένο σύστημα υπολοίπων μέτρου p τότε κάθε αριθμός του συνόλου A είναι ισότιμος με έναν διαφορετικό αριθμό του R ο οποίος φυσικά είναι τετραγωνικό ισοϋπόλοιπο $\bmod p$. Οπότε υπάρχουν τουλάχιστον $\frac{p-1}{2}$ διαφορετικοί αριθμοί ανά δύο ανισότιμοι που είναι τετραγωνικά ισοϋπόλοιπα.

□

Για την απόδειξη του επόμενου θεωρήματος θα χρειαστούμε ένα γνωστό θεώρημα των ισοτιμιών, το οποίο είναι το εξής:

Θεώρημα 2.4. *Κάθε πολυώνυμο $f(x) \in \mathbb{Z}_p[X]$ με βαθμό $\deg f(x) = n$, έχει το πολύ n ρίζες στο $\mathbb{Z}_p$.*

Απόδειξη. Η απόδειξη του θεωρήματος αυτού είναι άμεση συνέπεια του γενικότερου αλγεβρικού θεωρήματος, ότι ένα μη μηδενικό πολυώνυμο με συντελεστές από ένα σώμα δεν μπορεί να έχει περισσότερες ρίζες από το βαθμό του. □

Θεώρημα 2.5. *Έστω ένας πρώτος $p > 2$ και $p \nmid a$. Τότε ο αριθμός a είναι τετραγωνικό ισοϋπόλοιπο* $\bmod p$, *αν και μόνο αν $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

Απόδειξη. Από το Θεώρημα του Fermat έχουμε ότι για κάθε a με $p \nmid a$ ισχύει:

$$a^{p-1} \equiv 1 \pmod{p}$$

και επομένως

$$p \mid a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \Rightarrow p \mid a^{\frac{p-1}{2}} - 1 \text{ ή } p \mid a^{\frac{p-1}{2}} + 1.$$

Τα δύο τελευταία ενδεχόμενα δεν συμβαίνουν ταυτόχρονα, διότι αλλιώς θα είχαμε:

$$p \mid (a^{\frac{p-1}{2}} + 1) - (a^{\frac{p-1}{2}} - 1) = 2$$

το οποίο είναι άτοπο.
Άρα για κάθε a με $p \nmid a$ ισχύει ακριβώς μία από τις ισοτιμίες:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Απομένει, λοιπόν, να αποδείξουμε ότι:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow \text{ το } a \text{ είναι τετραγωνικό ισοϋπόλοιπο} \pmod{p}$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \Leftrightarrow \text{ το } a \text{ είναι τετραγωνικό ανισοϋπόλοιπο} \pmod{p}$$

Τώρα θεωρούμε την ισοτιμία: $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Από το Θεώρημα (2.4) συνεπάγεται ότι η παραπάνω εξίσωση έχει το πολύ $\frac{p-1}{2}$ λύσεις ανά δύο διαφορετικές $\bmod p$. Από την άλλη μεριά, κάθε τετραγωνικό ισοϋπόλοιπο $\bmod p$ είναι λύση της εξίσωσης. Διότι αν ισχύει $\xi^2 \equiv a \pmod{p}$ για κάποιο ξ, τότε, σύμφωνα με το Θεώρημα του Fermat $a^{\frac{p-1}{2}} \equiv \xi^{p-1} \equiv 1 \pmod{p}$. Βασισμένοι στο Θεώρημα (2.3) διαπιστώνουμε ότι υπάρχουν ακριβώς $\frac{p-1}{2}$ τετραγωνικά ισοϋπόλοιπα $\bmod p$, ανά δύο ανισότιμα $\bmod p$. Άρα η ισοτιμία έχει ακριβώς $\frac{p-1}{2}$ λύσεις ανά δύο διαφορετικές $\bmod p$ και αυτές είναι τα τετραγωνικά ισοϋπόλοιπα $\bmod p$. □

Ορισμός 2.3. *Σύμβολο Legendre*
Το σύμβολο Legendre του a ως προς p, ορίζεται ως εξής:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{αν } a \text{ τετραγωνικό ισοϋπόλοιπο} \bmod p \\ -1 & \text{αν } a \text{ τετραγωνικό ανισοϋπόλοιπο} \bmod p \end{cases}$$

Θεώρημα 2.6. *Έστω πρώτος $p > 2$ και ακέραιος a με $p \nmid a$. Για συντομία συμβολίζουμε $p' = \frac{p-1}{2}$.*

Τότε $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'} \left[\frac{2ak}{p}\right]}$.

Απόδειξη. Με τη χρήση του συμβολισμού $p' = \frac{p-1}{2}$, θεωρώ το σύνολο $R = \{-p', \ldots, -1, 1, \ldots p'\}$ το οποίο είναι ένα περιορισμένο σύστημα ισοϋπολοίπων. Αν λοιπόν $k \in \{1, 2, \ldots p'\}$, τότε $(ak, p) = 1$, οπότε ο ak είναι ισότιμος με κάποιον από τους αριθμούς του συνόλου R. Ο αριθμός αυτός του R είναι της μορφής $\sigma_k r_k$ όπου $\sigma_k \in \{-1, 1\}$ και $r_k \in \{1, 2, \ldots p'\}$. Άρα έχουμε τις σχέσεις

$$\begin{aligned} 1 \cdot a &\equiv \sigma_1 r_1 \pmod{p} \\ 2 \cdot a &\equiv \sigma_2 r_2 \pmod{p} \\ &\vdots \\ p' \cdot a &\equiv \sigma_{p'} r_{p'} \pmod{p} \end{aligned}$$

Επιπλέον, οι αριθμοί $r_1, r_2, \ldots, r_{p'}$ είναι όλοι διαφορετικοί μεταξύ τους. Πράγματι, έστω $1 \leq k < \ell \leq p'$. Γνωρίζουμε ότι το ak είναι ανισότιμο $a\ell \pmod{p}$, άρα αν ήταν $r_k = r_\ell$, αυτό θα συνεπαγόταν ότι, το ένα από τα σ_k, σ_ℓ θα ήταν 1 και το άλλο -1. Αυτό θα σήμαινε ότι $ak \equiv -a\ell \pmod{p}$, δηλαδή $(k + \ell)a \equiv 0 \pmod{p}$, αδύνατο, αφού $(a, p) = 1$.

Πολλαπλασιάζοντας τις σχέσεις παραπάνω κατά μέλη, έχουμε

$$(1 \cdot 2 \cdots p')a^{p'} \equiv (r_1 r_2 \cdots r_{p'})\sigma_1\sigma_2 \cdots \sigma_{p'} \pmod{p}.$$

Σύμφωνα με τα παραπάνω, οι αριθμοί $r_1, r_2, \ldots r_{p'}$ είναι μία μετάθεση των $1, 2, \ldots p'$, άρα, $r_1 r_2 \cdots r_{p'} = 1 \cdot 2 \cdots p'$, οπότε η προηγούμενη σχέση γίνεται

$$a^{p'} \equiv \sigma_1\sigma_2 \cdots \sigma_{p'} \pmod{p}.$$

Το αριστερό μέλος, ισούται με το $\left(\frac{a}{p}\right)$ και έτσι καταλήγουμε σε μία ισοτιμία που έχει και στα δύο μέλη είτε τον αριθμό 1, είτε τον -1. Έτσι έχουμε πλέον την ισότητα

$$\left(\frac{a}{p}\right) = \sigma_1\sigma_2 \cdots \sigma_{p'}. \tag{1}$$

Αν συμβολίσουμε με $[a]$ το ακέραιο μέρος του αριθμού a και $\{a\}$ το κλασματικό μέρος του αριθμού a, έχουμε $a = [a] + \{a\}$. Είναι σαφές ότι για οποιουσδήποτε αριθμούς a, b με $a \in \mathbb{R}$ και $b \in \mathbb{Z}$ έχουμε $[b + a] = b + [a]$.

Θεωρώ λοιπόν τον θετικό ακέραιο a, πρώτο ως προς τον p. Αν $1 \leq k \leq p'$, τότε

$$\left[\frac{2ak}{p}\right] = \left[2\left[\frac{ak}{p}\right] + 2\left\{\frac{ak}{p}\right\}\right] = 2\left[\frac{ak}{p}\right] + \left[2\left\{\frac{ak}{p}\right\}\right].$$

Αν το ν_k είναι το υπόλοιπο της ευκλείδειας διαίρεσης του ak δια p, τότε $\left\{\frac{ak}{p}\right\} = \frac{\nu_k}{p}$ και το τελευταίο κλάσμα είναι ένας αριθμός είτε του διαστήματος $[\,0, 0.5\,)$ αν $\nu_k \leq p'$,

είτε του διαστήματος $(0.5, 1)$ αν $\nu_k > p'$. Επίσης παρατηρούμε ότι $\nu_k \leq p' \Leftrightarrow \sigma_k = 1$ ενώ $\nu_k > p' \Leftrightarrow \sigma_k = -1$.

$$\text{Έτσι } \left[2\left\{\frac{ak}{p}\right\}\right] = \begin{cases} 0 & \text{αν } \sigma_k = 1 \\ 1 & \text{αν } \sigma_k = -1. \end{cases}$$

Έτσι συνδυάζοντας τα παραπάνω καταλήγουμε στο εξής:

$$\left[\frac{2ak}{p}\right] = \begin{cases} \text{άρτιος} & \text{αν } \sigma_k = 1 \\ \text{περιττός} & \text{αν } \sigma_k = -1. \end{cases}$$

οπότε

$$\sigma_k = (-1)^{\left[\frac{2ak}{p}\right]}. \tag{2}$$

Από τις ισότητες (1) και (2) έχουμε το ζητούμενου, $\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{p'}\left[\frac{2ak}{p}\right]}$.

□

Θεώρημα 2.7. *Ο αριθμός* 2 *είναι τετραγωνικό ισοϋπόλοιπο* $\bmod p$, *αν για το* p *ισχύει,* $p \equiv \pm 1 \pmod 8$.

Απόδειξη. Η απόδειξη της πρόταση αυτής, στηρίζεται πλήρως στο θεώρημα (2.6). θα κάνουμε λοιπόν χρήση του τύπου $\frac{a+p}{2}$ στη θέση του a.

$$\begin{aligned}\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) \\ = (-1)^{\sum_{k=1}^{p'}\left[\frac{(a+p)k}{p}\right]} \\ = (-1)^{\sum_{k=1}^{p'}\left[\frac{ak}{p}\right]+\sum_{k=1}^{p'}k} \\ = (-1)^{\sum_{k=1}^{p'}\left[\frac{ak}{p}\right]+\frac{p^2-1}{8}}.\end{aligned}$$

Αν στην παραπάνω σχέση θέσουμε $a = 1$, το πρώτο άθροισμα στον εκθέτη του -1 είναι 0, αφού $\left[\frac{k}{p}\right]$ για $k = 1, \ldots, p'$. Άρα παίρνουμε τη σχέση $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Έτσι αν $p \equiv \pm 1 \pmod 8$, έχουμε τον εκθέτη να ισούται με $\frac{p^2-1}{8} = \frac{(8n\pm1)^2-1}{8} = 8n^2 \pm 2n$, δηλαδή άρτιος. Άρα το 2 είναι τετραγωνικό ισοϋπόλοιπο $\bmod p$. □

3 Τέλειοι αριθμοί και Πρώτοι Mersenne

Πολλοί αρχαίοι πολιτισμοί ασχολήθηκαν με τη σχέση που έχει ένας αριθμός με το άθροισμα των διαιρετών του, δίνοντας συχνά μία μυστική σημασία. Για παράδειγμα, ο αριθμός 6 είναι ο πρώτος τέλειος αριθμός διότι $6 = 1 + 2 + 3$, όπου $1, 2, 3$ είναι οι διαιρέτες του χωρίς το 6. Ο επόμενος τέλειος αριθμός είναι ο $28 = 1 + 2 + 4 + 7 + 14$. Οι επόμενοι δύο είναι οι 496 και 8128.

Η ανακάλυψη αυτών των αριθμών χρονολογείται πριν τη γέννηση του Χριστού. Είναι γνωστό ότι οι τέλειοι αριθμοί και οι μυστικές ιδιότητές τους έχουν μελετηθεί από τους Πυθαγόρειους περίπου στα 525 π.Χ. Οι μελέτες συνεχίστηκαν από το Νικόμαχο το Γερασηνό, ο οποίος χώρισε τους αριθμούς σε τρεις κατηγορίες. Κάθε αριθμός n είναι είτε μεγαλύτερος, είτε ίσος, είτε μικρότερος από το άθροισμα των διαιρετών του (εκτός του ιδίου). Εκείνος λοιπόν, μίλησε για την τελειότητα του αριθμού 28, στηριζόμενος στο γεγονός ότι το φεγγάρι χρειάζεται 28 μέρες για να κάνει μία πλήρη περιστροφή γύρω από τη γη . Το διασημότερο παράδειγμα για τη φύση των τέλειων αριθμών είναι εκείνο του Αγίου Αυγουστίνου, ο οποίος έγραψε χαρακτηριστικά: ''Το έξι δεν είναι τέλειος αριθμός επειδή ο Θεός δημιούργησε τον κόσμο σε έξι ημέρες, αλλά ο Θεός δημιούργησε τον κόσμο σε έξι ημέρες επειδή το έξι είναι τέλειος αριθμός.''

Ορισμός 3.1. *Τέλειος αριθμός*

Ένας θετικός ακέραιος n λέγεται τέλειος αριθμός αν είναι ίσος με το άθροισμα όλων των θετικών διαιρετών του, εκτός του ιδίου.

Για τον πλήρη ορισμό των τέλειων αριθμών, θα χρησιμοποιήσουμε τη συνάρτηση $\sigma(n)$, η οποία έχει οριστεί παραπάνω.

Ορισμός 3.2. *Ένας αριθμός n είναι τέλειος αν και μόνο αν*

$$\sigma(n) = 2n$$

.

Με βάση αυτόν τον ορισμό, στην παρακάτω ενότητα θα αποδείξουμε το θεώρημα των Ευκλείδη και Euler.

3.1 Θεώρημα Ευκλείδη - Euler

Παρατηρώντας προσεκτικότερα τους τέσσερις πρώτους τέλειους αριθμούς, διαπιστώνουμε ότι δίνονται από τον τύπο $2^{n-1}(2^n - 1)$ για $n = 2, 3, 5$ και 7 αντίστοιχα. Οι τέλειοι αριθμοί μελετούνται από την αρχαιότητα. Το επόμενο Θεώρημα είναι η πρόταση 36 από το ένατο βιβλίο των ''Στοιχείων'' του Ευκλείδη.

Σε ακριβή μετάφραση, λέει τα εξής:
Αν το άθροισμα ενός δεδομένου πλήθους αριθμών, που βρίσκονται σε συνεχή αναλογία,

η οποία ξεκινά από τη μονάδα και έχει λόγο 2, είναι πρώτος αριθμός, τότε το γινόμενο του αθροίσματος με τον τελευταίο αριθμό της συνεχούς αναλογίας θα είναι τέλειος αριθμός.

Η ίδια πρόταση διατυπωμένη σε σύγχρονη μαθηματική γλώσσα, είναι το παρακάτω Θεώρημα:

Θεώρημα 3.1. *Εάν ένας αριθμός έχει τη μορφή* $n = 2^{m-1}(2^m - 1)$ *και* $2^m - 1$ *είναι πρώτος, τότε ο αριθμός* n *είναι τέλειος.*

Απόδειξη. Ας υποθέσουμε ότι $p = 2^m - 1$ είναι ένας πρώτος αριθμός και ότι $n = 2^{m-1}(2^m - 1)$. Για να δείξουμε ότι ο n είναι τέλειος, αρκεί να δείξουμε ότι $\sigma(n) = 2n$. Αφού η συνάρτηση σ είναι πολλαπλασιαστική έχουμε

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1}) \cdot \sigma(2^m - 1) \\ &= \frac{2^{m-1+1} - 1}{2 - 1} \cdot [(2^m - 1) + 1] \\ &= (2^m - 1) \cdot 2^m \\ &= \left[(2^m - 1) \cdot 2^{m-1}\right] \cdot 2 \\ &= 2n\end{aligned}$$

Αυτό μας δείχνει ότι ο n είναι τέλειος αριθμός. □

Η απόδειξη του αντίστροφου ισχυρισμού, ήρθε από τον Euler τον 18ο αιώνα.

Θεώρημα 3.2. *Ένας άρτιος ακέραιος αριθμός* n *για να είναι τέλειος πρέπει να έχει τη μορφή* $n = 2^{k-1}(2^k - 1)$ *με* $2^k - 1 = p \in \mathbb{P}$.

Απόδειξη. Θεωρούμε ότι ο n είναι οποιοσδήποτε άρτιος τέλειος αριθμός. Συνεπώς, $\sigma(n) = 2n$, καθώς επίσης και $n = 2^{k-1}m$ με m περιττό ακέραιο και $k \geq 2$. Χρησιμοποιούμε ξανά ότι η συνάρτηση σ είναι πολλαπλασιαστική, οπότε έχουμε:

$$\begin{aligned}\sigma(n) = \sigma(2^{k-1}m) &= \sigma(2^{k-1}) \cdot \sigma(m) \\ &= (2^k - 1)\sigma(m)\end{aligned}$$

ενώ παράλληλα

$$\sigma(n) = 2n = 2 \cdot 2^{k-1}m.$$

Έτσι

$$2^k m = (2^k - 1) \cdot \sigma(m), \tag{3}$$

οπότε $2^k - 1 \mid 2^k m$, δηλαδή $2^k - 1 \mid m$, άρα $m = (2^k - 1)M$. Τώρα αντικαθιστώντας στη σχέση (3) έχουμε $2^k M = \sigma(m)$. Άρα $\sigma(m) = 2^k * M = m + M$. Αν ήταν $M > 1$, τότε ο m θα είχε τουλάχιστον τρεις διαιρέτες, τους 1, m και M, άρα θα ήταν $\sigma(m) \geq m + M + 1$, άτοπο. Συνεπώς, $M = 1$, άρα $\sigma(m) = m + 1$, που δείχνει ότι

ο m είναι πρώτος. Ως εκ τούτου $m = 2^k - 1$ είναι πρώτος και έχουμε αποδείξει ότι ο αριθμός n έχει την καθορισμένη μορφή.

□

Το ευθύ και το αντίστροφο του θεωρήματος αυτού λοιπόν, είναι η αιτία άμεσης αντιστοιχίας των τέλειων αριθμών με τους πρώτους Mersenne. Έχουμε λοιπόν

Ένας αριθμός $M_p = 2^p - 1$ είναι πρώτος Mersenne αν και μόνο αν ο αριθμός $n = 2^{p-1}(2^p - 1)$ είναι τέλειος.

Οπότε η αναζήτηση για τους πρώτους Mersenne είναι επίσης αναζήτηση για τέλειους αριθμούς.

3.2 Ιδιότητες Τέλειων Αριθμών - Αριθμών Mersenne

Θεώρημα 3.3. *Εάν οι a και p είναι φυσικοί αριθμοί τέτοιοι ώστε ο $a^p - 1$ να είναι πρώτος, τότε $a = 2$ ή $p = 1$.*

Απόδειξη. Για τους αριθμούς a και p έχουμε διαδοχικά τις συνεπαγωγές

- $a \equiv 1 \pmod{a-1}$
- $a^p \equiv 1 \pmod{a-1}$
- $a^p - 1 \equiv 0 \pmod{a-1}$.

Έτσι $a-1 \mid a^p-1$. Δεδομένου όμως ότι το a^p-1 είναι πρώτος, τότε είτε $a-1 = a^p-1$, είτε $a - 1 = 1$. Στην πρώτη περίπτωση έχουμε ότι $a = a^p$. Αυτό ισχύει είτε με $a = 0$, είτε με $a = 1$, είτε με $p = 1$. Στις περιπτώσεις για $a = 0$ και $a = 1$ καταλήγουμε στις αντιφάσεις ότι -1 και 0 είναι πρώτοι αντίστοιχα. Οπότε δεχόμαστε μόνο την περίπτωση $p = 1$. Στην περίπτωση όπου $a - 1 = 1$ καταλήγουμε ότι $a = 2$. □

Θεώρημα 3.4. *Εάν για κάποιο θετικό ακέραιο n, ο $2^n - 1$ είναι πρώτος, τότε και ο n είναι πρώτος. Άρα, για να είναι ο M_n πρώτος, πρέπει ο n να είναι πρώτος. Συνεπώς, τους πρώτους Mersenne θα τους αναζητήσουμε στους αριθμούς M_p, όπου p είναι πρώτος.*

Απόδειξη. Έστω r και s δύο θετικοί ακέραιοι, τότε ισχύει η ισότητα $x^{rs}-1 = (x^s-1)\cdot(x^{s(r-1)}+x^{s(r-2)}+\cdots+x^s+1)$. Αν στην ταυτότητα αυτή θέσουμε $x = 2, n = rs, s \leq 2$, οδηγούμαστε στο συμπέρασμα ότι 2^s-1 είναι γνήσιος διαιρέτης του 2^n-1, μεγαλύτερος του 1. Άρα, αν ο n είναι σύνθετος, θα είναι και ο $2^n - 1$ επίσης σύνθετος . □

Θεώρημα 3.5. *Έστω p και q περιττοί πρώτοι αριθμοί. Εάν το p διαιρεί το $M_q = 2^q - 1$,τότε $p \equiv \pm 1 \pmod{8}$ και $p = 2kq + 1$ για κάποιον ακέραιο k.*

Απόδειξη. Εάν p διαιρεί το M_q, τότε $2^q \equiv 1 \pmod{p}$ και η τάξη του $2 \pmod{p}$ διαιρεί το πρώτο q, οπότε πρέπει να είναι q. Από το μικρό θεώρημα του Fermat η τάξη του 2 διαιρεί επίσης και το $p-1$, έτσι $p-1 = 2kq$ από το οποίο παίρνουμε το εξής:

$$2^{\frac{(p-1)}{2}} = 2^{qk} \equiv 1 \pmod{p}$$

οπότε το 2 είναι τετραγωνικό ισοϋπόλοιπο $\mod p$ και έτσι $p \equiv \pm 1 \pmod{8}$. □

Θεώρημα 3.6. *Έστω ένας πρώτος αριθμός με* $p \equiv 3 \pmod{4}$. *Τότε ο αριθμός* $2p+1$ *είναι επίσης πρώτος αν και μόνο αν διαιρεί τον* M_p.

Απόδειξη. Έστω ότι ο $q = 2p+1$ είναι πρώτος. Δεδομένου ότι $p = 4r+3$, έχουμε $q = 2p+1 = 8r+7$, άρα $p \equiv 3 \pmod{4}$, άρα $q \equiv 7 \pmod{8}$. Έτσι ο αριθμός 2 είναι τετραγωνικό ισοϋπόλοιπο $\mod q$, δηλαδή υπάρχει κάποιος ακέραιος n ο οποίος επαληθεύει τη σχέση $n^2 \equiv 2 \pmod{q}$. Οπότε

$$2^p = 2^{\frac{q-1}{2}} \equiv n^{q-1} \equiv 1 \pmod{q},$$

δηλαδή $q \mid Mp$.

Για το αντίστροφο, υποθέτουμε ότι $2p+1 \mid M_p$ και θα αποδείξουμε ότι ο $2p+1$ είναι πρώτος. Θα υποθέσουμε λοιπόν ότι είναι σύνθετος και έστω k ο μικρότερος πρώτος παράγοντας του, οπότε $k \leq \sqrt{2p+1}$, άρα $2p+1 \geq k^2$. Έχουμε $2^p - 1 \equiv 0 \pmod{k}$. Οπότε $ord_k(2) \mid p$ και δεδομένου ότι $p \in \mathbb{P}$, έχουμε $ord_k(2) = p$, ενώ ταυτόχρονα, $ord_k(2) \mid k-1$, άρα $p \mid k-1$. Δηλαδή $k > p$ το οποίο συνεπάγεται $k^2 > p^2$. Όμως έχουμε και $2p+1 \leq k^2$, άρα $2p+1 > p^2$, άτοπο αφού $p > 2$. □

4 Τεστ Lucas–Lehmer

Σε αυτή την ενότητα θα ασχοληθούμε με το τεστ των Lucas–Lehmer που ισχύει μόνο για τους πρώτους Mersenne. Το τεστ αναπτύχθηκε αρχικά από τον Édouard Lucas το 1856 και στη συνέχεια βελτιώθηκε το 1878 από τον ίδιο. Η τελική βελτίωση έγινε από τον Derrick Henry Lehmer το 1930.

Το τεστ Lucas–Lehmer λειτουργεί ως εξής:
Έστω πρώτος $p > 2$ και ο αριθμός Mersenne $M_p = 2^p - 1$. Ορίζουμε την ακολουθία s_i αναδρομικά ως εξής:

$$s_i = \begin{cases} 4 & \text{αν } i = 0, \\ s_{i-1}^2 - 2 & \text{αλλιώς.} \end{cases}$$

Οι πρώτοι όροι αυτής της ακολουθίας είναι $4, 14, 194, 37634, \cdots$

> Έστω p περιττός πρώτος. Τότε ο M_p είναι πρώτος αν και μόνο αν $s_{p-2} \equiv 0 \pmod{M_p}$.

Ο αριθμός $s_{p-2} \pmod{M_p}$ ονομάζεται ο ισότιμος $\mod p$ κατά Lucas–Lehmer .

Απόδειξη. Θα εκφράσουμε με κλειστή μορφή τον γενικό όρο της αναδρομικής ακολουθίας. Ορίζουμε $\omega = 2 + \sqrt{3}$ και $\overline{\omega} = 2 - \sqrt{3}$, οπότε μπορούμε να επαληθεύσουμε ότι $s_i = \omega^{2^i} + \overline{\omega}^{2^i}$ για κάθε i. Πράγματι,

$$\begin{aligned} s_0 &= \omega^{2^0} + \overline{\omega}^{2^0} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4 \\ s_n &= s_{n-1}^2 - 2 \\ &= (\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}})^2 - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} \end{aligned}$$

όπου $\omega\overline{\omega} = (2 + \sqrt{3}) \cdot (2 - \sqrt{3}) = 1$.

Αυτό θα το χρησιμοποιήσουμε για την απόδειξη και των δύο κατευθύνσεων.
Για το ευθύ: Σε αυτή τη κατεύθυνση θα δείξουμε ότι αν $s_{p-2} \equiv 0 \pmod{M_p}$ τότε ο M_p είναι πρώτος.

Έστω $s_{p-2} \equiv 0 \pmod{M_p}$. Τότε $\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = kM_p$ για κάποιο ακέραιο k. Έτσι έχουμε διαδοχικά

- $\omega^{2^{p-2}} = kM_p - \overline{\omega}^{2^{p-2}}$

- $\left(\omega^{2^{p-2}}\right)^2 = kM_p\omega^{2^{p-2}} - (\omega\overline{\omega})^{2^{p-2}}$.

Έτσι έχουμε την εξίσωση:

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1 \tag{4}$$

Έστω λοιπόν ότι ο M_p είναι σύνθετος αριθμός και q ο μικρότερος πρώτος παράγοντάς του. Αφού οι αριθμοί Mersenne είναι περιττοί, έχουμε ότι $q > 2$.

Ας θεωρήσουμε ότι το σύνολο $\mathbb{Z}_q$ περιέχει τους ακεραίους $\mod q$, καθώς και το σύνολο $X = \{a + b\sqrt{3} | a, b \in \mathbb{Z}_q\}$, ορίζοντας σε αυτό το σύνολο τον πολλαπλασιασμό ως εξής:

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + \sqrt{3}(bc + ad) \pmod{q}.$$

Προφανώς το σύνολο X είναι κλειστό ως προς αυτόν τον πολλαπλασιασμό, ενώ για το πλήθος των στοιχείων του ισχύει $|X| \leq q^2$. Το σύνολο X δεν είναι ομάδα γιατί δεν περιέχει για κάθε στοιχείο και το αντίστροφό του. Ωστόσο μπορούμε να θεωρήσουμε το σύνολο X^*, που περιέχει τα αντιστρέψιμα στοιχεία του συνόλου X. Το σύνολο X^* έχει δομή ομάδας. Δεδομένου ότι το $0 \in X$ δεν είναι αντιστρέψιμο, $|X^*| \leq |X| - 1 \leq q^2 - 1$.

Τώρα, εφόσον $M_p \equiv 0 \pmod{q}$ και $\omega \in X$, λόγω της εξίσωσης (4) έχουμε στο σύνολο X τις παρακάτω συνεπαγωγές

$$kM_p\omega^{2^{p-2}} = 0 \Rightarrow \omega^{2^{p-1}} = -1 \Rightarrow \omega^{2^p} = 1.$$

Έτσι $\omega \in X^*$ και μάλιστα έχει αντίστροφο το ω^{2^p-1}. Επιπλέον, $ord(\omega) \mid 2^p$ και εφόσον $\omega^{2^{p-1}} \neq 1$, έχουμε ότι $ord(\omega) = 2^p$.

Όμως η τάξη κάθε στοιχείου μιας ομάδας δεν υπερβαίνει την τάξη της ομάδας, άρα

$$2^p \leq |X^*| \leq q^2 - 1 < q^2.$$

Έχουμε όμως θεωρήσει ότι ο q είναι ο μικρότερος πρώτος παράγοντας του σύνθετου M_p, οπότε $q^2 \leq M_p = 2^p - 1$, δηλαδή $2^p < 2^p - 1$, άτοπο. Έτσι ο αριθμός M_p είναι πρώτος.

Αντίστροφο:

Τώρα, θα υποθέσουμε ότι ο αριθμός M_p είναι πρώτος και θα αποδείξουμε ότι $s_{p-2} \equiv 0 \pmod{M_p}$.

Αρχικά κάνουμε την παρατήρηση ότι ο αριθμός 3 είναι τετραγωνικό ανισοϋπόλοιπο $(\mod M_p)$ εφόσον $2^p - 1 \equiv 7 \pmod{12}$ για περιττό $p > 1$. Έτσι από τις ιδιότητες του συμβόλου Legendre και τον νόμο της τετραγωνικής αντιστροφής, έχουμε ότι $\left(\frac{3}{M_p}\right) = \left(\frac{M_p}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{M_p-1}{2}} = \left(\frac{1}{3}\right)\cdot(-1) = -1$, οπότε και $3^{\frac{M_p-1}{2}} = -1 \pmod{M_p}$.

Από την άλλη μεριά ο αριθμός 2 είναι τετραγωνικό ισοϋπόλοιπο $\pmod{M_p}$ εφόσον $2^p \equiv 1 \pmod{M_p}$. Έτσι $2 \equiv 2^{p+1} = \left(2^{\frac{p+1}{2}}\right)^2 \pmod{M_p}$, οπότε $2^{\frac{M_p-1}{2}} = 1 \pmod{M_p}$.
Ορίζουμε λοιπόν τον αριθμό $\sigma = 2\sqrt{3}$ και το σύνολο X^* όπως και προηγουμένως, το σύνολο των μονάδων του συνόλου $X = \{a + b\sqrt{3} | a, b \in \mathbb{Z}_q\}$, όπου $q = M_p$.
Στις πράξεις παρακάτω, οι οποίες γίνονται στο δακτύλιο Q, χρησιμοποιούμε το Freshman's dream, δηλαδή την ισοτιμία $(x+y)^{M_p} \equiv x^{M_p} + y^{M_p} \pmod{M_p}$ και το μικρό θεώρημα του Fermat, δηλαδή την ισοτιμία $a^{M_p} \equiv a \pmod{M_p}$. Επειδή $q = M_p > 3$, τα στοιχεία 2 και 3 του X είναι αντιστρέψιμα (τα αντίστροφά τους ταυτίζονται με τα αντίστροφα των 2 και 3 στο σώμα $\mathbb{Z}_q$).

Έτσι στο δακτύλιο X έχουμε

$$\begin{aligned}(6+\sigma)^{M_p} &= 6^{M_p} + (2^{M_p})(\sqrt{3})^{M_p} \\ &= 6 + 2(3^{\frac{M_p-1}{2}})\sqrt{3} \\ &= 6 + 2(-1)\sqrt{3} \\ &= 6 - \sigma.\end{aligned}$$

Η επιλογή του σ έγινε έτσι ώστε $\omega = \dfrac{(6+\sigma)^2}{24}$ [1]. Οπότε μπορούμε να το χρησιμοποιήσουμε ώστε να υπολογίσουμε το $\omega^{\frac{M_p+1}{2}}$ στο δακτύλιο X.

$$\begin{aligned}\omega^{\frac{M_p+1}{2}} &= \frac{(6+\sigma)^{M_p+1}}{24^{\frac{M_p+1}{2}}} \\ &= \frac{(6+\sigma)^{M_p}(6+\sigma)}{24 \cdot 24^{\frac{M_p-1}{2}}} \\ &= \frac{(6-\sigma)(6+\sigma)}{-24} \\ &= -1.\end{aligned}$$

(χρησιμοποιήσαμε την ισότητα $24^{\frac{M_p-1}{2}} = (2^{\frac{M_p-1}{2}})^3(3^{\frac{M_p-1}{2}}) = (1)^3(-1) = -1$.)

Εφόσον $M_p \equiv 3 \pmod{4}$ το μόνο που απομένει είναι να πολλαπλασιάσουμε τα δύο μέλη της ισότητας με $\overline{\omega}^{\frac{M_p+1}{4}}$ και χρησιμοποιώντας τη γεγονός $\overline{\omega}\omega = 1$.

[1] Λόγω της παραπάνω παρατήρησης για τα $2, 3$, το 24 είναι αντιστρέψιμο στοιχείο του X.

$$\begin{aligned}
\omega^{\frac{M_p+1}{2}} \cdot \overline{\omega}^{\frac{M_p+1}{4}} &= -\overline{\omega}^{\frac{M_p+1}{4}} \\
\omega^{\frac{M_p+1}{4}} + \overline{\omega}^{\frac{M_p+1}{4}} &= 0 \\
\omega^{\frac{2^p-1+1}{4}} + \overline{\omega}^{\frac{2^p-1+1}{4}} &= 0 \\
\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} &= 0 \\
s_{p-2} &= 0.
\end{aligned}$$

Έτσι το s_{p-2} είναι ακέραιος και μηδενικό στο δακτύλιο X, οπότε ‘‘ μεταφραζόμενο ’’ αυτό το συμπέρασμα στο $\mathbb{Z}$, λέει ότι $s_{p-2} \equiv 0 \pmod{M_p}$. □

5 Εικασίες και άλυτα προβλήματα

Υπάρχει περιττός τέλειος αριθμός;

Γνωρίζουμε ότι όλοι οι τέλειοι αριθμοί είναι γινόμενο ενός πρώτου Mersenne και μίας δύναμης του 2. Αλλά τι γίνεται με τους περιττούς τέλειους αριθμούς; Αν υπάρχει ένας, τότε είναι γινόμενο ενός τέλειου τετραγώνου με μία περιττή δύναμη ενός πρώτου. Θα είναι διαιρετό από τουλάχιστον οκτώ πρώτους αριθμούς και έχει τουλάχιστον 75 πρώτους παράγοντες με τουλάχιστον 9 από αυτούς διακριτούς, έχει τουλάχιστον 300 δεκαδικά ψηφία, και έχει ένα πρώτο διαιρέτη μεγαλύτερο από 10^{20}.

Υπάρχουν άπειροι το πλήθος πρώτοι Mersenne;

Ισοδύναμα μπορούμε να αναρωτηθούμε: Υπάρχουν άπειροι το πλήθος άρτιοι τέλειοι αριθμοί; Η απάντηση είναι πιθανότατα ναι.

Υπάρχουν άπειροι το πλήθος σύνθετοι αριθμοί Mersenne;

Ο Euler έδειξε:

Θεώρημα: Αν $k > 1$ και $p = 4k + 3$ είναι πρώτος, τότε $2p + 1$ είναι πρώτος αν και μόνο αν $2^p \equiv 1 \pmod{2p+1}$.

Οπότε εάν $p = 4k + 3$ και ο $2p + 1$ είναι πρώτος, τότε ο αριθμός Mersenne $2^p + 1$ είναι σύνθετος.

Η νέα εικασία του Mersenne

Έστω p ένας περιττός φυσικός αριθμός. Αν ισχύουν δύο από τις επόμενες συνθήκες, τότε ισχύει και η τρίτη.

1. $p = 2^k \pm 1$ ή $p = 4^k \pm 3$
2. $2^p - 1$ είναι πρώτος, ειδικότερα πρώτος Mersenne
3. $\dfrac{2^p + 1}{3}$ είναι πρώτος.

Παρατηρήστε πώς αυτή η εικασία σχετίζεται με το θεώρημα στην προηγούμενη εικασία.

Είναι κάθε αριθμός Mersenne ελεύθερος τετραγώνου;

Αυτό θεωρείται ένα από τα ανοικτά ερωτήματα του οποίου δεν ξέρουμε την απάντηση και όχι εικασία.

Γνωστοί Πρώτοι Mersenne

Στον παρακάτω πίνακα παρατήθενται πληροφορίες για τους πρώτους Mersenne που είναι γνωστοί μέχρι σήμερα.

Πίνακας Πρώτων Mersenne

♯	Πρώτος p	Ψηφία του M_p	Ψηφία του P_p	Χρονολογία	Εξερευνητής
1	2	1	1	—-	Αρχαίοι Έλληνες Μαθηματικοί
2	3	1	2	—-	Αρχαίοι Έλληνες Μαθηματικοί
3	5	2	3	—-	Αρχαίοι Έλληνες Μαθηματικοί
4	7	3	4	—-	Αρχαίοι Έλληνες Μαθηματικοί
5	13	4	8	1456	anonymous
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll, Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson, Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt, Welsh
30	132049	39751	79502	1983	Slowinski

Πίνακας Πρώτων Mersenne (συνέχεια)

♯	Πρώτος p	Ψηφία του M_p	Ψηφία του P_p	Χρονολογία	Εξερευνητής
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski, Gage
33	859433	258716	517430	1994	Slowinski, Gage
34	1257787	378632	757263	1996	Slowinski, Gage
35	1398269	420921	841842	1996	Armengaud, Woltman, et. al. (GIMPS)
36	2976221	895932	1791864	1997	Spence, Woltman, et al. (GIMPS)
37	3021377	909526	1819050	1998	Clarkson,Woltman,Kurowski et al.(GIMPS)
38	6972593	2098960	4197919	1999	Hajratwala,Woltman,Kurowski et al.(GIMPS)
39	13466917	4053946	8107892	2001	Cameron,Woltman,Kurowski et al. (GIMPS)
40	20996011	6320430	12640858	2003	Shafer, Woltman, Kurowski et al. (GIMPS)
41	24036583	7235733	14471465	2004	Findley, Woltman, Kurowski et al. (GIMPS)
42	25964951	7816230	15632458	2005	Nowak, Woltman, Kurowski et al. (GIMPS)
43	30402457	9152052	18304103	2005	Cooper,Boone,Woltman,Kurowski et al.(GIMPS)
44*	32582657	9808358	19616714	2006	Cooper, Boone, Woltman, Kurowski et al. (GIMPS)
45*	37156667	11185272	22370543	2008	Elvenich, Woltman, Kurowski et al. (GIMPS)
46*	42643801	12837064	25674127	2009	Strindmo, Woltman, Kurowski et al. (GIMPS)
47*	43112609	12978189	25956377	2008	Smith, Woltman, Kurowski et al. (GIMPS)
48*	57885161	17425170	34850339	2013	Cooper, Woltman, Kurowski et al. (GIMPS)

Τα τελευταία πέντε στοιχεία είναι με αστερίσκο, διότι δεν έχει αποδεδειχθεί ακόμη, ότι δεν υπάρχουν πρώτοι Mersenne ανάμεσά τους.