22/10/2015

ΕΥΚΛΕΙΔΕΙΑ ΔΙΑΙΡΕΣΗ: Έστω $a, b \in \mathbb{Z}$, $b \neq 0$, τότε υπάρχουν μοναδικοί ακέραιοι $q, r \in \mathbb{Z}$: $a = bq + r$, $0 \leq r < |b|$

ΠΑΡΑΔΕΙΓΜΑ: Έστω $k \in \mathbb{Z}$, και θεωρούμε τους διαδοχικούς ακεραίους:
$k, k+1, k+2, \ldots, k+n-1$ (n το πλήθος διαδοχικοί ακέραιοι)
Αν $A = k(k+1)(k+2)\ldots(k+n-1)$, τότε: $n \mid A$
Από την Ευκλείδεια Διαίρεση, θα έχουμε:
$k = n \cdot q + r$, όπου: $0 \leq r < n$
- Αν $r = 0$, τότε: $k = n \cdot q \Rightarrow n \mid k$ επειδή $k \mid A$, θα έχουμε $n \mid A$
- Έστω ότι $r \neq 0$. Τότε: $1 \leq r \leq n-1 \Rightarrow 1 \leq n-r \leq n-1$

$n - r < 1 \Rightarrow n < r + 1 \Rightarrow n < r$
$n - r > n - 1 \Rightarrow -r > -1 \Rightarrow r < 1$

$A = k(k+1)\ldots(k+n-r)\ldots(k+n-1) =$
$= k(k+1)\ldots(nq+r+n-r)\ldots(k+n-1) =$
$= k(k+1)\ldots n(q+1)\ldots(k+n-1) \Rightarrow n \mid A$

ΠΡΩΤΟΙ ΑΡΙΘΜΟΙ: Ο θετικός ακέραιος p καλείται πρώτος $\Leftrightarrow$ ο p έχει ως μοναδικούς διαιρέτες (θετικούς διαιρέτες) μόνο το 1 και τον εαυτό του, και $p \neq 1$. Ο θετικός ακέραιος $p > 1$ καλείται σύνθετος $\Leftrightarrow$ δεν είναι πρώτος $\Leftrightarrow$ $\Leftrightarrow p = a \cdot b$, όπου $1 < a, b < p$

1 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

ΘΕΩΡΗΜΑ: Κάθε θετικός ακέραιος $a > 1$ έχει τουλάχιστον έναν πρώτο διαιρέτη.
Απόδειξη: Θεωρούμε το σύνολο $S = \{m \in \mathbb{N} \mid m \mid a \text{ και } m > 1\} \subseteq \mathbb{N}$. Τότε $S \neq \emptyset$ διότι $a \in S$ (διότι $a \mid a$ και $a > 1$). Από την ΑΡΧΗ ΚΑΛΗΣ ΔΙΑΤΑΞΗΣ το S έχει ένα ελάχιστο στοιχείο, έστω $p = \min S$. Τότε $p \mid a$ και $p > 1$. Θα δείξουμε ότι p: πρώτος:

Έστω ότι ο P δεν είναι πρώτος $\Rightarrow p=r\cdot s$, όπου $1<r,s<p$
Τότε $r|p$. Επειδή $p|a \Rightarrow r|a$ και επειδή $r>1$, έπεται ότι $r\in S$
Επειδή $r\in S$, $r<p=\min S$ καταλήξαμε σε άτοπο. Άρα p: πρώτος

□

ΘΕΩΡΗΜΑ ΤΟΥ ΕΥΚΛΕΙΔΗ: Το πλήθος των πρώτων αριθμών είναι άπειρο.

Απόδειξη: Υποθέτουμε ότι το πλήθος των πρώτων αριθμών είναι πεπερασμένο, έστω ότι οι πρώτοι αριθμοί είναι: $P_1, P_2, \dots, P_n$.
Θεωρούμε τον αριθμό: $A=P_1P_2\cdots P_n+1>1$
Από το προηγούμενο θεώρημα, ο A έχει έναν πρώτο διαιρέτη p, δηλαδή $p|A$ και p: πρώτος.
Επειδή όλοι οι πρώτοι αριθμοί είναι οι $P_1, P_2, P_3, \dots, P_n$, έπεται ότι ο p είναι κάποιος από τους $P_1, P_2, \dots, P_n$.
Έστω ότι: $p=P_k$, $1\le k\le n$

Προφανώς $\left.\begin{array}{l} p=P_k \mid P_1P_2\cdots P_k\cdots P_n \\ p|A=P_1P_2\cdots P_k\cdots P_{n+1} \end{array}\right| \Rightarrow P_k=p|1 \Rightarrow p\le 1$ άτοπο, διότι ο P_k πρώτος $\neq 1$.

Στο άτοπο καταλήξαμε υποθέτοντας το πλήθος των πρώτων αριθμών είναι πεπερασμένο. Άρα αυτό το πλήθος είναι άπειρο

□

Πρώτοι του Mersenne: πρώτοι αριθμοί της μορφής 2^p-1 (όπου p: πρώτος)

Μέχρι σήμερα υπάρχουν μόνο 48 πρώτοι του Mersenne, ο τελευταίος βρέθηκε το 2013
Οι 10 μεγαλύτεροι πρώτοι αριθμοί είναι πρώτοι του Mersenne.
Ο μεγαλύτερος μέχρι σήμερα πρώτος αριθμός είναι ο $2^{57.885.161}-1$
(έχει 17.425.170 ψηφία)

- (1876) $2^{127}-1$ πρώτος του Mersenne
- (1978) $2^{\text{γιγάντιος}}-1$ ΗΗ

$\pi : \mathbb{R} \to \mathbb{N}$, $\pi(x)$ το πλήθος των πρώτων αριθμών $\leq x$

ΘΕΩΡΗΜΑ ΤΩΝ ΠΡΩΤΩΝ ΑΡΙΘΜΩΝ: $\pi(x) \sim \frac{x}{\log x}$

Αν P_n : ο n-οστός στη σειρά πρώτος είναι: $P_n \sim n \log n$

ΠΡΟΤΑΣΗ: Υπάρχουν οσοδήποτε μεγάλα χάσματα στην κατανομή των πρώτων αριθμών, $\forall n \in \mathbb{N}$: οι αριθμοί: $(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1$: είναι σύνθετοι

Απόδειξη:

Για $k = 2, 3, \ldots, n+1$

$1 < k < (n+1)! + k$

και $k \mid (n+1)! + k$, διότι $k \mid k$ και $k \mid (n+1)!$, διότι $2 \leq k \leq n+1$

□

Παραγοντικό:
$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$
π.χ. $1! = 1$
$2! = 1 \cdot 2 = 2$
$3! = 1 \cdot 2 \cdot 3 = 6$

ΘΕΩΡΗΜΑ: Κάθε σύνθετος φυσικός αριθμός $a > 1$, έχει τουλάχιστον έναν πρώτο διαιρέτη P, έτσι ώστε: $P \leq \sqrt{a}$

Απόδειξη: Επειδή ο a είναι σύνθετος $\Rightarrow a=b\cdot c$, όπου $1<b, c<a$
Χωρίς βλάβη της γενικότητας, έστω $c\le b \Rightarrow c^2 \le b\cdot c = a \Rightarrow$
$\Rightarrow c \le \sqrt{a}$. Επειδή ο $c>1$, έχουμε αποδείξει ότι ο c έχει έναν πρώτο διαιρέτη, έστω p. Τότε p: πρώτος και $p|c$ $\Big| \rightarrow p|a$ και $p\le c \le \sqrt{a}$
Όμως $c|a$ $\Big|$ p: πρώτος

→ Συνέχεια από Θεώρημα.

ΠΟΡΙΣΜΑ: Έστω $a>1$ ένας φυσικός αριθμός και δεν υπάρχει πρώτος p έτσι ώστε: $p|a$ και $p\le\sqrt{a}$. Τότε ο a είναι πρώτος

ΠΑΡΑΔΕΙΓΜΑ: $a=643$ και $b=583$

(1) $25 < \sqrt{643} < 26$ Θεωρούμε αριθμούς ≤ 25
Οι πρώτοι αριθμοί ≤ 25 είναι: 2, 3, 5, 7, 11, 13, 17, 19, 23
Δοκιμάζοντας, βλέπουμε ότι κανένας από αυτούς τους πρώτους δεν διαιρεί το 643. Άρα το 643 είναι πρώτος

(2) $24 < \sqrt{583} < 25$. Όμως $11 | 583$ και άρα το 583 είναι σύνθετος.