ΚΟΣΚΙΝΟ ΤΟΥ ΕΡΑΤΟΣΘΕΝΗ

Έστω $N \geq 2$ ακέραιος. Εύρεση όλων των πρώτων $p \leq N$

Βήμα 1ο: Γράφουμε όλους τους ακέραιους από το 2 εώς το N.

$N=25$ ~~2~~ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13
~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~

Βήμα 2ο: Υπογραμμίζουμε τον πρώτο 2. Διαγράφουμε τα γνήσια πολλ/σια του 2. Δηλαδή 4, 6.

Βήμα 3ο: Επαναλαμβάνουμε το βήμα 2 για τον πρώτο μετά τον 2 αριθμό που δεν έχει ήδη υπογραμμιστεί ή διαγραφεί. Διαγράφουμε τα γνήσια πολλ/σια του.

Συνεχίζουμε όπως στο Βήμα 3.

Οι υπογραμμισμένοι αριθμοί είναι ακριβώς όλοι οι πρώτοι $\leq N$

ΠΑΡΑΤΗΡΗΣΗ: Έστω $a = p_1 p_2 \cdots p_t$ όπως στο προηγούμενο θεώρημα της Αριθμητικής Θεμελίωσης των πρώτων που διαιρούσαν τουλάχιστον δύο φορές, μετακαλούμε τη γραφή

$a = q_1^{r_1} q_2^{r_2} \cdots q_s^{r_s}$ όπου $q_1 < q_2 < \cdots < q_s$ πρώτοι

κ' $r_1, \ldots, r_s$ θετικοί ακέραιοι. Αυτή η γραφή λέγεται **ΠΡΩΤΟΓΕΝΗΣ ανάπτυξη** του ακεραίου $a \geq 2$

π.χ. $8 = 2^3$, $15 = 3^1 5^1$, $45 = 3^2 5$, $2019 = 3 \cdot 673$

2019	3
21	673

$\sqrt{673}$ ~~26~~ $27^2 > 673$

Άρα ελέγχουμε αν το 673 έχει πρώτο διαιρέτη ≤ 26

Οι πρώτοι ≤ 25 είδαμε ότι είναι 2, 3, 5, 7, 11, 13, 17, 19, 23.

Με πράξεις κανένα δεν διαιρεί το 673, άρα 673 πρώτος κ' $2019 = 3^1 \cdot 673^1$ η πρωτογενής ανάπτυξη του 2019

π.χ 2017 πρώτοι

ΠΑΡΑΤΗΡΗΣΗ: Έστω $a \geq 2$ κ' $p_1, p_2, \dots, p_N$ πρώτοι, ώστε κάθε πρώτος που διαιρεί το a να είναι κάποιο p (Αλλά μπορεί να $\nexists j$, ώστε $p_j \nmid a$).

Επίσης υποθέτουμε $p_i \neq p_j$ για $i \neq j$. Τότε υπάρχουν μοναδικοί $d_i \geq 0$, ώστε
$a = p_1^{d_1} p_2^{d_2} \cdots p_N^{d_N}$

π.χ $a = 8$, $p_1 = 2$, $p_2 = 3$, $p_3 = 11$
$a = 2^3$, άρα ο μόνος πρώτος διαιρέτης του a είναι το p_1
Έχουμε $a = p_1^3 p_2^0 p_3^0$

π.χ $a = 50$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$
Έχουμε ότι η πρωτογενής ανάλυση του a είναι $a = 2 \cdot 5^2$

Συνεπώς, $a = p_1^{d_1} p_2^0 p_3^0 p_4^0$
Παρόμοια, αν $p_1, \dots, p_N$ διαφορετικοί πρώτοι χρειάζονται $b = p_1^{c_1} p_2^{c_2} \cdots p_N^{c_N}$

ΣΤΟΧΟΣ: ΜΚΔ $(p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}, p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}) = p_1^{\min(c_1,d_1)} p_2^{\min(c_2,d_2)} \cdots p_r^{\min(c_r,d_r)}$

όταν $p_1, \dots, p_r$ πρώτοι με $p_i \neq p_j$ για $i \neq j$ κ' $r_1 \geq 0, d_1 \geq 0$ ακέραιοι.

Στόχος 2: Εύρεση όλων των θετικών διαιρετών του $p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, όπου p_i, c_i όπως παραπάνω.

Πρόταση: Έστω $a, b \geq 1$ ακέραιοι κ' $a = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$ $b = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}$

όπου p_i πρώτοι $p_i \neq p_j$ για $i \neq j$, $c_i, d_i \geq 0$ ακέραιοι. Τότε $a | b$ αν $c_i \leq d_i$ $\forall i$

(π.χ $2^5 7^3 | 2^5 7^4$, αλλά $2^5 7^3 \nmid 2^4 7^3$

Απόδειξη: Υποθέτουμε $c_i \le d_i$ $\forall i$. Θέτουμε $u = p_1^{d_1-c_1} p_2^{d_2-c_2} \cdots p_r^{d_r-c_r} \in \mathbb{Z}$.
Τότε $au = p_1^{c_1} \cdots p_r^{c_r} \cdot p_1^{d_1-c_1} p_2^{d_2-c_2} \cdots p_r^{d_r-c_r} = p_1^{c_1} p_1^{d_1-c_1} \cdots p_r^{c_r} p_r^{d_r-c_r} =$

$= p_1^{c_1+(d_1-c_1)} \cdots p_r^{c_r+(d_r-c_r)} = p_1^{d_1} \cdots p_r^{d_r} = b$. Άρα $a \mid b$.

Αντίστροφα, υποθέτουμε $a \mid b$. Άρα $\exists u \in \mathbb{Z}, u > 0$ ώστε $au = b$. Έστω p πρώτος με $p \mid u$. Τότε $p \mid au = b \Rightarrow p \mid p_1^{d_1} \cdots p_r^{d_r}$. Άρα το p είναι ένα από τα p_i.
Συνεπώς, $\exists e_i \in \mathbb{Z}$ με $e_i \ge 0$, ώστε $u = p_1^{e_1} \cdots p_r^{e_r}$.
Άρα $au = b \Rightarrow p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r} \cdot p_1^{e_1} \cdots p_r^{e_r} = p_1^{d_1} \cdots p_r^{d_r} \Rightarrow$
$p_1^{c_1+e_1} p_2^{c_2+e_2} \cdots p_r^{c_r+e_r} = p_1^{d_1} \cdots p_r^{d_r} \xrightarrow[\text{ΑΡΙΘΜ}]{\text{ΘΕΩΡΗΜΑ}}$ $c_i + e_i = d_i$ $\forall i$. Άρα αυτού $e_i \ge 0$

$\forall i$ έπεται $c_i \le d_i$ $\forall i$

Πόρισμα: Έστω $a \in \mathbb{Z}$ με $a \ge 2$ και πρωτογενή ανάλυση $a = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, όπου p_i πρώτοι $p_i \ne p_j$ για $i \ne j$ και $c_i > 0$. Τότε, το σύνολο των θετικών διαιρετών του a είναι το $S = \{ p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \mid 0 \le d_i \le c_i \ \forall i \}$. Άρα $\#S = (c_1+1)(c_2+1) \cdots (c_r+1)$

Απόδειξη: Άμεση από την προηγούμενη πρόταση.

π.χ. Πόσους θετικούς διαιρέτες έχει ο $2^{15} 7^{21}$;
Απάντηση: Έχουμε $2, 7$ πρώτοι. $2 \ne 7$. Άρα από την πρόταση ο $2^{15} 7^{21}$ έχει $(15+1)(21+1) = 16 \cdot 3 = 48$ θετικούς διαιρέτες.

6) $7^2 \cdot 10$: Έχουμε $7^2 \cdot 10 = 2^1 \cdot 5^1 \cdot 7^2$. Άρα έχει $(1+1)(1+1)(2+1) = 12$ θετικοί διαιρέτες.

Πίνακας: Το σύνολο $S = \{ 2^{d_1} 5^{d_2} 7^{d_3} \mid 0 \le d_1 \le 1, 0 \le d_2 \le 1, 0 \le d_3 \le 2 \} =$

$= \{ 2^0 5^0 7^0 = 1, 2^0 5^0 7^1 = 7, 2^0 5^0 7^2 = 49, 2^0 5^1 7^0 = 5, 2^0 5^1 7^1 = 35, 2^0 5^1 7^2 = 5 \cdot 49 = 245,$
$2^1 5^0 7^0 = 2, 2^1 5^0 7^1 = 14, 2^1 5^0 7^2 = 2 \cdot 49 = 98, 2^1 5^1 7^0 = 10, 2^1 5^1 7^1 = 70,$
$2^1 5^1 7^2 = 490 \}$

ΠΑΡΑΤΗΡΗΣΗ: Έστω $p_1, p_2, \dots, p_r$ πρώτοι με $p_1 < p_2 < \dots < p_r$ και $a \in \mathbb{Z}$ με $a \neq 0$. Από το πόρισμα έχουμε ότι το σύνολο των διαιρετών του a είναι το $S = \{ p_1^{d_1} p_2^{d_2} \dots p_r^{d_r} : 0 \le d_i \le c_i, d_i \in \mathbb{N} \}$

Πρόταση: Έστω $p_1, p_2, \dots, p_r$ πρώτοι με $p_1 < p_2 < \dots < p_r$, και $a, b \in \mathbb{Z}$ με $a \neq 0$ και $b \neq 0$.

Γράφουμε $a = p_1^{c_1} \dots p_r^{c_r}$, $b = p_1^{d_1} \dots p_r^{d_r}$. Τότε

(i) Το σύνολο των κοινών διαιρετών των a και b είναι $\{ p_1^{e_1} \dots p_r^{e_r} : 0 \le e_i \le \min(c_i, d_i), e_i \in \mathbb{N} \}$

(ii) $\text{ΜΚΔ}(a,b) = p_1^{\min(c_1,d_1)} p_2^{\min(c_2,d_2)} \dots p_r^{\min(c_r,d_r)}$

(όπου $\min(c_i, d_i)$ είναι ο ελάχιστος από τα c_i, d_i)

Απόδειξη: (i) Άμεσο από την πρόταση

(ii) Άμεσο από το (i)

π.χ $\text{ΜΚΔ}(2^5 3^2 7^3, 2 \cdot 3^5 7^4 10) = \text{ΜΚΔ}(2^5 3^2 7^3, 2 \cdot 3^5 7^4 2 \cdot 5) =$
$= \text{ΜΚΔ}(2^5 \cdot 3^2 \cdot 5^0 \cdot 7^3, 2^2 \cdot 3^5 \cdot 5^1 \cdot 7^4)$ πρόταση $2^{\min(5,2)} 3^{\min(2,5)} 5^{\min(0,1)} 7^{\min(3,4)} =$
$= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^3$

$\longleftrightarrow$

Ορισμός: Έστω $a, b \in \mathbb{Z}$ με $a \neq 2$ και $n \in \mathbb{Z}$. Ο n λέγεται άρτιος αν $\exists k \in \mathbb{Z}$ με $n = ka + b$

π.χ Ο 3 είναι "της μορφής $2k+1$", γιατί $3 = 2 \cdot 1 + 1$.
Ο 5 " -11- $3k+2$, γιατί $5 = 3 \cdot 1 + 2$
Ο 6 δεν -11- $3k+2$.

Απόδειξη: Έστω ότι είναι. Τότε $\exists k \in \mathbb{Z}$ με $6 = 3k + 2 \Rightarrow 4 = 3k \Rightarrow 3 | 4$, αντίφαση.

Παρατήρηση: Έστω $n \in \mathbb{Z}$

(i) Ο n είναι "της μορφής $k \cdot 2+0$", αυτός οι άρτιοι.

(ii) Ο n είναι "της μορφής $2k+1$", αυτός οι περιττοί

Απόδειξη: Άμεση

Πρόταση: Έστω $a \geq 2$, $n \in \mathbb{Z}$ και $b \in \mathbb{Z}$, $0 \leq b < a$.

Ο n "είναι της μορφής $ka+b$" αυτό το υπόλοιπο της Ευκλείδειας Διαίρεσης του n με το a είναι ίσο με b

Απόδειξη: Έστω ότι το υπόλοιπο της Ευκλείδειας Διαίρεσης του n με το a είναι b. Τότε $\exists k \in \mathbb{Z}$ με $n = k \cdot a + b$. Άρα n "της μορφής $ka+b$".

Αντίστροφα, υποθέτουμε ότι το n "της μορφής $ka+b$". Άρα $\exists k \in \mathbb{Z}$ με $n = ka+b$ (*)
Αφού $0 \leq b < a-1$, η (*) είναι η Ευκλείδεια Διαίρεση του n με το a. Άρα το αποτέλεσμα έπεται.

∴ $-7 = (-2) \cdot 5 + 3$ και $0 \leq 3 < 5$. Συνεπώς το -7 είναι "της μορφής $k \cdot 5 + 3$".

∴ Έχουμε $3 \mid 2019$. Όμως $3 \mid (2+0+1+9)$. Συνεπώς το 2019 είναι "της μορφής $3 \cdot k + 0$", ενώ δεν είναι "της μορφής $3k+1$", ούτε "της μορφής $3k+2$".

Πρόταση: Έστω $a \in \mathbb{Z}$ με $a \geq 2$ και $n \in \mathbb{Z}$. Τότε ο n είναι ακριβώς ένα από τα παρακάτω:

"της μορφής $k \cdot a + 0$", "της μορφής $k \cdot a + 1$", ...
"της μορφής $k \cdot a + (a-1)$"

Απόδειξη: Άμεσο από την πρόταση και την μοναδικότητα του υπολοίπου της Ευκλείδειας Διαίρεσης.

∴ Αν $a \leq 4$ και $n \in \mathbb{Z}$, τότε:

n "της μορφής $4k+0$", αν $n \in \{\ldots, -8, -4, 0, 4, 8, \ldots\}$
n "της μορφής $4k+1$", αν $n \in \{\ldots, -7, -3, 1, 5, 9, \ldots\}$
n "της μορφής $4k+2$", αν $n \in \{\ldots, -6, -2, 2, 6, 10, \ldots\}$
n "της μορφής $4k+3$", αν $n \in \{\ldots, -5, -1, 3, 7, 11, \ldots\}$