ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

8ο Εξάμηνο 2022 – 2023

Assignment – Solutions

Ζαρίφης Στέλιος – el20435 Email: el20435@mail.ntua.gr

Contents

1. Δείξτε ότι το γινόμενο n το πλήθος διαδοχικών ακεραίων είναι πολλαπλάσιο του n.

Θεωρούμε το εν λόγω γινόμενο: $P = a(a+1)(a+2)\dots(a+n-1), a \in \mathbb{Z}$

Έστω ότι δεν ισχύει η πρόταση, δηλαδή έστω ότι το γινόμενο n το πλήθος διαδοχικών ακεραίων <u>δεν</u> είναι πολλαπλάσιο του n.

Έστω επίσης x ο μέγιστος ακέραιος που διαιρείται από το n και είναι μικρότερος του a.

Αρχικά, ο x δε γίνεται να απέχει από τον a περισσότερο από n μονάδες γιατί προφανώς αν ίσχυε αυτό, θα υπήρχε $k \in \mathbb{N}^*$ ώστε ο $x+kn > x$ να είναι επίσης μικρότερος του a και να διαιρείται από το n. Συνεπώς ο $x+kn$ θα έπαιρνε τη θέση του x. Άρα δείξαμε ότι $a - x < n$

Η τελευταία σχέση, όμως, μας δίνει $x + n > a\ (1)$

Επιπλέον, είναι $x < a \Rightarrow x + n < a + n\ (2)$

Από τις σχέσεις $(1, 2)$ έχουμε ότι $a < x + n < a + n$.

Αυτό μας δείχνει ότι υπάρχει ακέραιος μεγαλύτερος του a και μικρότερος του $a+n$ που γράφεται ως $x+n$. Όμως από την υπόθεση έχουμε ότι $n|x$ και προφανώς $n|(x+n)$.

Άρα ένας από τους παράγοντες $a, a+1, \dots, a+n-1$ γράφεται ως $x+n$ και άρα διαιρείται από το n. Αφού ένας εκ των παραγόντων του γινομένου είναι πολλαπλάσιος του n, έχουμε ότι όλο το γινόμενο είναι πολλαπλάσιο του n. Συνεπώς καταλήξαμε σε ΑΤΟΠΟ!

Άρα η πρόταση αληθεύει.

2. Δείξτε ότι αν $p > 1$ και ο p διαιρεί τον $(p-1)! + 1$, τότε ο p είναι πρώτος.

Έστω ότι δεν ισχύει η πρόταση, δηλαδή έστω ότι αν ο $p > 1$ διαιρεί τον $(p-1)! + 1$ είναι σύνθετος.

Αυτό σημαίνει ότι υπάρχει ακέραιος $d, 1 < d < p$ ώστε $d|p$. Από τη μεταβατική ιδιότητα, θα είναι επίσης $d|p|(p-1)! + 1\ (1)$

Ακόμα, επειδή $1 < d < p$, ισχύει $(p-1)! = 1 \cdot \dots \cdot (d-1) \cdot d \cdot (d+1) \cdot \dots \cdot (p-1)$. Αφού ο d είναι παράγων, θα είναι ακόμα $d|(p-1)!\ (2)$

Από ιδιότητα, συμπεραίνουμε από τις $(1, 2)$ ότι ο d θα διαιρεί και το $(p-1)! + 1 - (p-1)!$, αφού διαιρεί κάθε γραμμικό συνδυασμό των $(p-1)! + 1$ και $(p-1)!$. Άρα δείξαμε ότι $d|1$.

Όμως, ο μοναδικός ακέραιος που διαιρεί το 1 είναι ο 1 και ξεκινήσαμε με την υπόθεση ότι ο d είναι ένας παράγων μεγαλύτερος του 1. Συνεπώς καταλήξαμε σε ΑΤΟΠΟ!

Άρα η πρόταση αληθεύει.

3. Δείξτε ότι $12|p+q$ και $6|p+1$ όπου $p>3$ και p,q δυο δίδυμοι πρώτοι (δηλαδή έχουν διαφορά 2).

Χωρίς βλάβη της γενικότητας, θεωρούμε $p>3$ και $q=p+2$.

Θα αποδείξουμε ότι $12|p+q$. Είναι $12=2^2\cdot 3$. Αρκεί να δείξουμε ότι $2^2|p+q \wedge 3|p+q$

1. $q=p+2 \Rightarrow p+q=2p+2=2(p+1)$. Επειδή $p>3$ πρώτος, θα είναι και περιττός. Άρα, ο επόμενός του, $p+1$, θα είναι άρτιος, δηλαδή θα μπορεί να γραφτεί στη μορφή $p+1=2k$. Συνολικά είναι $p+q=2(p+1)=4k$. Συμπεραίνουμε ότι $2^2|p+q$
2. Ας δούμε τι ισχύει για το υπόλοιπο της διαίρεσης του p με το 3: $p\ mod\ 3 \in \{1,0,-1\}$
   a. $p\ mod\ 3=1$. Άρα $p=3k+1>3, k\in\mathbb{N}$. Άρα, ο $q=p+2$ γράφεται $q=3k+1+2=3(k+1)$, δηλαδή $3|q$, το οποίο είναι άτοπο αφού q είναι πρώτος. Άρα αυτή η περίπτωση ισχύει.
   b. $p\ mod\ 3=0$. Σε αυτήν την περίπτωση, αφού $3|p$ σημαίνει πως ο $p>3$ <u>δεν</u> είναι πρώτος, το οποίο είναι άτοπο. Άρα ούτε αυτή η περίπτωση ισχύει.
   c. $p\ mod\ 3=-1$. Είναι η τελευταία περίπτωση που ισχύει υποχρεωτικά!

   Δείξαμε λοιπόν ότι $p\ mod\ 3=-1 \Rightarrow p+1\ mod\ 3=0 \overset{\times 2}{\Rightarrow} 2(p+1)\ mod\ 3=0$.
   Θυμόμαστε όμως ότι $2(p+1)=p+q$. Άρα βρήκαμε ότι $p+q\ mod\ 3=0 \Rightarrow 3|p+q$.

Συνολικά, δείξαμε ότι $2^2|p+q \wedge 3|p+q$, άρα και $12|p+q$!

Έχοντας αποδείξει το πρώτο ζητούμενο, εύκολα μπορούμε να δούμε για το δεύτερο ότι

$$12|p+q \Rightarrow 12|2(p+1) \Rightarrow 2\cdot 6|2(p+1) \Rightarrow 6|p+1$$

Αποδείξαμε και τις 2 προτάσεις!

4. Να βρεθούν όλοι οι φυσικοί διαιρέτες των αριθμών 140 και 2023, και να βρεθούν όλοι οι φυσικοί αριθμοί που έχουν ακριβώς 3 διαιρέτες.

Αναλύουμε τους αριθμούς 140 και 2023 σε γινόμενα πρώτων παραγώντων:

$$\begin{array}{r|l} 140 & 7 \\ 20 & 5 \\ 4 & 2 \\ 2 & 2 \\ 1 & \end{array} \quad \textit{και} \quad \begin{array}{r|l} 2023 & 17 \\ 119 & 17 \\ 7 & 7 \\ 1 & \end{array}$$

Άρα γράφουμε $140=2^2\cdot 5\cdot 7$ και $2023=7\cdot 17^2$ και όλοι οι φυσικοί διαιρέτες, εφόσον περιλαμβάνουν του πρώτους παράγοντες, γράφονται για τους 2 αριθμούς:

140: $1\cdot 2^{\alpha}\cdot 5^{\beta}\cdot 2^{\gamma}, 0\le\alpha\le 2, 0\le\beta\le 1, 0\le\gamma\le 1$
2023: $1\cdot 7^{\alpha}\cdot 17^{\beta}, 0\le\alpha\le 1, 0\le\beta\le 2$

Οπότε για να δώσουμε όλους τους φυσικούς διαιρέτες των, αρκεί να υπολογίσουμε τα ανωτέρω γινόμενα για κάθε (μοναδικό) συνδυασμό των α, β, γ και α, β. Οι tuples είναι:

α	β	γ	*Διαιρέτης του* 140	*Διαιρέτης του* 2023
0	0	0	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 1$	$1 \cdot 7^{\alpha} \cdot 17^{\beta} = 1$
0	0	1	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 7$	
0	1	0	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 5$	$1 \cdot 7^{\alpha} \cdot 17^{\beta} = 17$
0	1	1	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 35$	
1	0	0	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 2$	$1 \cdot 7^{\alpha} \cdot 17^{\beta} = 7$
1	0	1	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 14$	
1	1	0	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 10$	$1 \cdot 7^{\alpha} \cdot 17^{\beta} = 119$
1	1	1	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 70$	
2	0	0	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 4$	$1 \cdot 7^{\alpha} \cdot 17^{\beta} = 49$
2	0	1	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 28$	
2	1	0	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 20$	$1 \cdot 7^{\alpha} \cdot 17^{\beta} = 2023$
2	1	1	$1 \cdot 2^{\alpha} \cdot 5^{\beta} \cdot 7^{\gamma} = 140$	

1. Κάθε αριθμός n μεγαλύτερος του 1 έχει για διαιρέτες τον εαυτό του και το 1.
2. Αν ο n είναι τετράγωνο πρώτου αριθμού, τότε ο τρίτος διαιρέτης που ψάχνουμε είναι ο πρώτος αυτός αριθμός. Οπότε βλέπουμε πως τα τετράγωνα πρώτων αριθμών ανήκουν στην κατηγορία που αναζητούμε.
3. Έστω ότι ο n δεν είναι τετράγωνο πρώτου αριθμού. Τότε ο n είναι σύνθετος (όχι πρώτος αφού θα είχε μόνο 2 διαιρέτες). Άρα ο n μπορεί να αναλυθεί σε γινόμενο πρώτων παραγόντων και επειδή δεν είναι τετράγωνο πρώτου (θα είχε μοναδικό παράγοντα τον ίδιο τον πρώτο), αναγκαστικά θα έχει 2 ή περισσότερους πρώτους παράγοντες. Αυτό σημαίνει ότι για διαιρέτες, εκτός από τον εαυτό του και το 1 θα είχε και τους περισσότερους από 1 πρώτους παράγοντές του, άρα θα είχε περισσότερους από 3 διαιρέτες. Συνεπώς, δεν υπάρχει άλλος αριθμός που να ανήκει στη ζητούμενη κατηγορία.

Αποδείξαμε ότι μόνο τα τετράγωνα πρώτων αριθμών έχουν ακριβώς τρεις διαιρέτες, το 1, τον εαυτό τους και την τετραγωνική τοτς ρίζα (τον πρώτο αριθμό).

5. Να βρεθούν όλες οι θετικές ακέραιες λύσεις (n, m) της εξίσωσης $m^n = n^m$.

Θεωρούμε ότι m, n αναφέρονται σε διαφορετικούς ακεραίους γιατί αλλιώς οι λύσεις είναι άπειρες αν $m = n$.

Εύκολα βρίσκουμε δύο προφανείς λύσεις: $(m, n) \in \{(2, 4), (4, 2)\}$. Θα αποδείξουμε ότι είναι οι μοναδικές. Κάνουμε κάποιους μετασχηματισμούς:

$$m^n = n^m \overset{\log(\cdot)}{\Longleftrightarrow} n \log m = m \log n \Leftrightarrow \frac{\log n}{n} = \frac{\log m}{m}$$

Θεωρούμε τη συνάρτηση

$$f: \mathbb{R} \mapsto \mathbb{R}, f(x) = \frac{\log x}{x}$$

Βρίσκουμε τη μονοτονία της:

$$f'(x) = \frac{1 - \log x}{x^2} \Rightarrow f: \nearrow \ \alpha\nu\ x \in (0, e)\ \kappa\alpha\iota\ f: \searrow \ \alpha\nu\ x \in (e, +\infty)$$

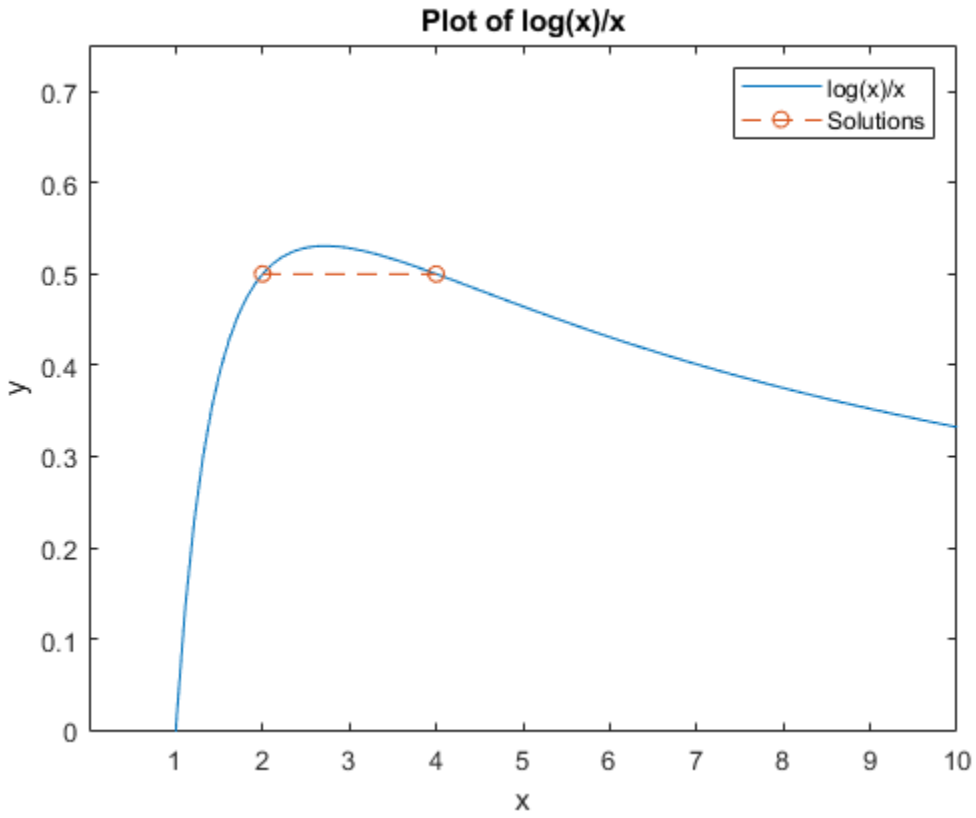
Θεωρούμε για τώρα ότι $m < n$ και ό,τι βρούμε εφαρμόζεται και συμμετρικά για $m < n$. Εξετάζουμε τις περιπτώσεις:

1. $0 < m < n < e$: Σε αυτήν την περίπτωση, λόγω της μονοτονίας της f στο διάστημα αυτό, είναι $m < n \Rightarrow f(m) < f(n) \Rightarrow f(m) \neq f(n)$, άρα δεν υπάρχουν λύσεις της μορφής $0 < m < n < e$.
2. $e < m < n$: Και πάλι, λόγω της μονοτονίας της f στο διάστημα, είναι $m < n \Rightarrow f(m) > f(n) \Rightarrow f(m) \neq f(n)$, άρα δεν υπάρχουν λύσεις της μορφής $e < m < n$.
3. $0 < m < e < n$: Είναι η τελευταία περίπτωση και είναι δυνατόν να υπάρξουν λύσεις αυτής της μορφής. Επειδή m, n ακέραιοι και $0 < m < e$, σημαίνει ότι υποχρεωτικά $m = 1$ ή $m = 2$. Όμως απορρίψαμε στην αρχή την $m = 1$ διότι δίνει $n = 1$ και θεωρήσαμε ότι $m \neq n$ για να αποφύγουμε την απειρία των λύσεων. Αυτό που απομένει είναι $m = 2$ ως *μοναδική* περίπτωση για λύση του προβλήματος. Συμμετρικά, αν ήταν $n < m$ θα καταλήγαμε πάλι στη *μοναδική* περίπτωση $n = 2$

Αποδείξαμε λοιπόν ότι έχουμε μοναδικές λύσεις $(m, n) \in \{(2, 4), (4, 2)\}$.

Παρακάτω, φαίνεται και εποπτικά η λύση. Βλέπουμε πως είναι ανάγκη να οι λύσεις m, n να βρίσκονται εκατέρωθεν του e και σε αυτήν την περίπτωση, επειδή η αριστερή είναι φραγμένη και από το 0, έχει περιθώριο, ως ακέραια, να είναι μόνο 1 ή 2.

```
% Define the range of x
x = linspace(0, 10);

% Calculate the values of the function
y = log2(x)./x;

% Calculate the values of the horizontal line segment
y_line = [log2(2)/2, log2(4)/4];

% Define the x-coordinates of the line segment
x_line = [2, 4];

% Plot the function and the line segment
plot(x, y, x_line, y_line, '--o')

% Label the plot
title('Plot of log(x)/x')
xlabel('x')
ylabel('y')

% Add a legend for the line segment
legend('log(x)/x', 'Solutions')
```



6. Δείξτε ότι για κάθε ακέραιο k ισχύει ότι $(7k+5, 11k+8) = 1$, και για ακεραίους $a_1, \dots, a_n$ και b με $(a_i, b) = 1, \forall i$ ισχύει ότι $(a_1 a_2 \dots a_n, b) = 1$.

Έστω $(k, d) \in \mathbb{Z}^2$ και ότι υπάρχει $d > 1$ ώστε $(7k+5, 11k+8) = d$. Αυτό σημαίνει ότι ο d διαιρεί και τους δύο αιρθμούς. Από την ιδιότητα, ξέρουμε ότι ο d θα διαιρεί και οποιονδήποτε γραμμικό συνδυασμό αυτών. Σκοπός μας είναι να καταλήξουμε σε άτοπο, δηλαδή ότι $d \leq 1$. Σίγουρα θέλουμε να «απελευθερωθούμε» από τα k. Έχουμε:

$$(7k+5, 11k+8) = d \Rightarrow \begin{cases} d|7k+5 \\ d|11k+8 \end{cases} \Rightarrow d|7(11k+8) - 11(7k+5) \Rightarrow$$
$$\Rightarrow d|77k + 56 - 77k - 55 \Rightarrow d|1 \Rightarrow d \equiv 1$$

Αφού ο d είναι διαιρέτης και του 1, τότε υποχρεωτικά είναι ο 1. Καταλήξαμε σε άτοπο!

Άρα δεν υπάρχει τέτοιος d, οπότε η πρόταση $\forall k\ (7k+5, 11k+8) = 1$ είναι αληθής.

Για το δεύτερο μέρος, έστω $d \in \mathbb{Z}$ και ότι υπάρχει $d > 1$ ώστε $(a_1 a_2 \dots a_n, b) = d > 1$. Αυτό σημαίνει ότι ο d διαιρεί και τους δύο αιρθμούς. Είναι δηλαδή:

$$\begin{cases} d|a_1 a_2 \dots a_n \\ d|b \end{cases} (1)$$

Το $d|a_1 a_2 \dots a_n$ δηλώνει ότι το d διαιρεί τουλάχιστον έναν παράγοντα του γινομένου. Υπάρχει, δηλαδή, $i \in \{1, 2, \dots, n\}$ για το οποίο είναι $d|a_i$ (2).

Από τις $(1, 2)$, όμως, έχουμε ότι υπάρχει ένας κοινός διαιρέτης των a_i, b, ο d, ο οποίος είναι μεγαλύτερος από τον μέγιστο κοινό διαιρέτη, που είναι 1, από τα δεδομένα. Καταλήξαμε λοιπόν σε άτοπο. Άρα η πρόταση $\forall i\ a_i \in \mathbb{Z} \wedge b \in \mathbb{Z} \wedge (a_i, b) = 1 \Rightarrow (\prod_{i=1}^{n} a_i, b) = 1$ αληθεύει.

7. Για τη συνάρτηση μ του Möbius, δείξτε ότι για κάθε φυσικό $n \geq 1$ ισχύει $\mu(n) \cdot \mu(n+1) \cdot \mu(n+2) \cdot \mu(n+3) = 0$ και ότι για κάθε φυσικό $n \geq 3$ ισχύει $\sum_{k=1}^{n} \mu(k!) = 1$.

Θα αποδείξουμε ότι

$$\mu(n) \cdot \mu(n+1) \cdot \mu(n+2) \cdot \mu(n+3) = 0, \forall n \geq 1$$

Ένας από τους αριθμούς $n, n+1, n+2, n+3$, ως 4 διαδοχικοί, διαιρείται με το 4.

Απόδειξη: Έστω ότι κανένας δε διαιρούταν με το 4. Τότε $n \; mod \; 4 = k, k \in \{1, 2, 3\}$.

1. Αν $k = 1$, τότε $n \; mod \; 4 = 1 \Rightarrow n + 3 \; mod \; k = 0$
2. Αν $k = 2$, τότε $n \; mod \; 4 = 2 \Rightarrow n + 2 \; mod \; k = 0$
3. Αν $k = 3$, τότε $n \; mod \; 4 = 3 \Rightarrow n + 1 \; mod \; k = 0$

Και στις 3 περιπτώσεις καταλήγουμε σε άτοπο. Άρα ένας από τους αριθμούς $n, n+1, n+2, n+3$ διαιρείται με το 4. Αυτό σημαίνει ότι έχει διαιρέτη τον $4 = 2^2$, λόγω του οποίου καθίσταται $non \; square - free$. Για αυτό, θα έχει τιμή συνάρτησης Möbius μηδέν. Αφού ο ένας εκ των παραγόντων $\mu(n), \mu(n+1), \mu(n+2), \mu(n+3)$ είναι μηδέν, το γινόμενο ισούται επίσης με μηδέν, για κάθε φυσικό $n \geq 1$. Άρα το πρώτο ζητούμενο αποδείχθηκε.

Για το δεύτερο μέρος, έχουμε:

$$\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!) + \mu(4!) + \cdots + \mu(n!)$$

Η Möbius function ορίζεται ως:

$$\mu(n) = \begin{cases} +1, n: \text{square} - \text{free θετικός ακέραιος με άρτιο αριθμό πρώτων παραγόντων} \\ -1, n: \text{square} - \text{free θετικός ακέραιος με περιττό αριθμό πρώτων παραγόντων} \\ 0, n: \text{όχι square} - \text{free θετικός ακέραιος} \end{cases}$$

Παρατηρούμε ότι για κάθε $n \geq 4$, είναι $n! = n(n-1) \cdots 4 \cdot 3 \cdot 2 \cdot 1 = 2^2 n(n-1) \cdots 3 \cdot 2 \cdot 1$. Δηλαδή, κάθε $n!, n \geq 3$ έχει έναν τετραγωνισμένο πρώτο παράγοντα.
Συνεπώς, $\mu(n!) = 0, \forall n \geq 4$. Άρα είναι:

$$\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!) + 0 + \cdots + 0$$

Επιπλέον,

$\mu(1!) \triangleq 1, \mu(2!) = \mu(2^1) = (-1)^1 = -1, \mu(3!) = \mu(2^1 \cdot 3^1) = (-1)^{1+1} = 1$, οπότε:

$$\sum_{k=1}^{n} \mu(k!) = \mu(1!) + \mu(2!) + \mu(3!) = 1 - 1 + 1 = 1, \forall n \geq 3$$

8.΄ Εστω η αριθμητική συνάρτηση λ του Liouville που ορίζεται ως

$$\lambda(n) = \begin{cases} 1, n = 1 \\ (-1)^{k_1+k_2+\cdots+k_r}, n = p_1^{k_1}p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \end{cases}$$

Να δειχθεί ότι είναι πολλαπλασιαστική και να υπολογιστεί το άθροισμα $\sum_{d|n} \lambda(d)$.

Ορίζουμε τη συνάρτηση $\Omega(n) = k_1 + k_2 + \cdots + k_r$, για κάθε φυσικό

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}, p_i : primes$$

Για τη συνάρτηση $\Omega(\cdot)$ ισχύει

$$\Omega(mn) = \Omega\left(p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r} \cdot q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots \cdot q_r^{l_s}\right) = k_1 + k_2 + \cdots + k_r + q_1 + q_2 + \cdots + q_s = \\ = \Omega(m) + \Omega(n)$$

Συνεπώς, αν $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}, n = q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots \cdot q_r^{l_s}, p_i, q_i : primes$, έχουμε:

$$\lambda(m \cdot n) = (-1)^{k_1+k_2+\cdots+k_r+q_1+q_2+\cdots+q_s} = (-1)^{\Omega(m)+\Omega(n)} = (-1)^{\Omega(m)}(-1)^{\Omega(n)} = \lambda(m)\lambda(n)$$

Άρα η $\lambda(\cdot)$ είναι πολλαπλασιαστική.

Το άθροισμα $\sum_{d|n} \lambda(d)$, ως άθροισμα πολλαπλασιαστικών συναρτήσεων είναι πολλαπλασιαστική συνάρτηση

Κάθε αριθμός n αναλύεται σε γινόμενο δυνάμεων πρώτων παραγόντων:

$$n = \prod_{i=1}^{k} p_i^{k_i}$$

Ας δούμε τη συμπεριφορά του αθροίσματος όταν το n είναι κάποια δύναμη πρώτου αριθμού:

$$\sum_{d|n=p^a} \lambda(d) = 1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a) = 1 - 1 + 1 - 1 + \cdots + (-1)^a = \begin{cases} 0, a : odd \\ 1, a : even \end{cases}$$

Αν θεωρήσουμε $f(n) = \sum_{d|n} \lambda(d)$, αφού η f είναι πολλαπλασιαστική, θα έχουμε:

$$f(n) = f\left(\prod_{i=1}^{k} p_i^{k_i}\right) = \prod_{i=1}^{k} f\left(p_i^{k_i}\right) = \begin{cases} 1, k_i : even \ \forall i \\ 0, else \end{cases}$$

Αρκεί δηλαδή ένας πρώτος να βρίσκεται σε περιττή δύναμη για να έχουμε έναν μηδενικό όρο στο γινόμενο.

Άρα, το άθροισμα $\sum_{d|n} \lambda(d)$ είναι 1 αν ο n είναι τετράγωνος και 0 διαφορετικά.

9. Αν n, k είναι θετικοί ακέραιοι αριθμοί, δείξτε ότι $\varphi(n^k) = n^{(k-1)}\varphi(n)$ και αν $d|n$, $\varphi(nd^k) = d^k\varphi(n)$.

Έστω $p_1, p_2, \dots, p_l$ οι prime factors του n. Τότε, για τη συνάρτηση $\varphi(\cdot)$ έχουμε:

$$\varphi(n) = n \cdot (1 - 1/p_1) \cdot (1 - 1/p_2) \cdot \dots \cdot (1 - 1/p_l)$$

Επίσης, μπορούμε να εκφράσουμε το n ως εξής:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$$

Άρα, για όρισμα n^k έχουμε:

$$n^k = \left(p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}\right)^k = p_1^{k \cdot k_1} p_2^{k \cdot k_2} \cdots p_l^{k \cdot k_l}$$

Το οποίο έχει τους ίδιους πρώτους παράγοντες με το n (προφανώς). Άρα:

$$\begin{aligned}\varphi(n^k) &= n^k \cdot (1 - 1/p_1) \cdot (1 - 1/p_2) \cdot \dots \cdot (1 - 1/p_l) = \\ &= n^{k-1} \cdot n \cdot (1 - 1/p_1) \cdot (1 - 1/p_2) \cdot \dots \cdot (1 - 1/p_l) = n^{k-1}\varphi(n)\end{aligned}$$

Αποδείξαμε το πρώτο ζητούμενο.

Επειδή $d|n$, κάποια δύναμη d^i θα είναι ο μέγιστος κοινός διαιρέτης των d^k και n.

Από θεώρημα έχουμε:

$$(d^k, n) = d^i \Rightarrow \varphi(d^k n) = \varphi(d^k)\varphi(n)\frac{d^i}{\varphi(d^i)}$$

Από το προηγούμενο ερώτημα έχουμε

$$\varphi(d^k) = d^{k-1}\varphi(d) \; \kappa\alpha\iota \; \varphi\left(d^i\right) = d^{i-1}\varphi(d)$$

Άρα έχουμε

$$\varphi(d^k n) = d^{k-1}\varphi(d)\varphi(n)\frac{d^i}{d^{i-1}\varphi(d)} = d^{k-1}\frac{d^i}{d^{i-1}}\varphi(n) \Rightarrow \varphi(d^k n) = d^k\varphi(n)$$

10. Έστω $\{a_1, \dots, a_p\}$ και $\{b_1, \dots, b_p\}$ δύο πλήρη συστήματα υπολοίπων $mod\ p$ όπου $p > 2$ πρώτος αριθμός. Δείξτε ότι το $\{a_1 b_1, \dots, a_p b_p\}$ δεν είναι πλήρες σύστημα υπολοίπων $mod\ p$.

Για τα 2 πλήρη συστήματα υπολοίπων έχουμε

$$\alpha_1 \alpha_2 \dots \alpha_{p-1} \equiv -1\ (mod\ p) \wedge b_1 b_2 \dots b_{p-1} \equiv -1\ (mod\ p)$$

Από το θεώρημα Wilson, για το γινόμενό αυτών έχουμε:

$$\left(\alpha_1 \alpha_2 \dots \alpha_{p-1}\right) \cdot \left(b_1 b_2 \dots b_{p-1}\right) \equiv (-1) \cdot (-1)\ (mod\ p) \equiv 1\ (mod\ p) \Rightarrow$$
$$\Rightarrow (\alpha_1 b_1) \cdot (\alpha_2 b_2) \cdot \dots \cdot \left(\alpha_{p-1} b_{p-1}\right) \equiv 1\ (mod\ p)$$

Το οποίο σημαίνει ότι το $\{a_1 b_1, \dots, a_p b_p\}$ δεν είναι πλήρες σύστημα υπολοίπων $mod\ p$

11. Υπολογίστε τα υπόλοιπα των διαιρέσεων $251^{143}: 7$, $5^{100}: 7$ και $16! : 19$

Εξετάζουμε τη διαίρεση $251^{143}: 7$. Κάνοντας τη διαίρεση $251: 7$ έχουμε υπόλοιπο 6, είναι δηλαδή:

$$251 \equiv 6\ (mod\ 7) \Rightarrow 251 \equiv -1\ (mod\ 7) \xrightarrow[\sigma\varepsilon\ \delta\acute{\upsilon}\nu\alpha\mu\eta]{I\delta\iota\acute{o}\tau\eta\tau\alpha\ \acute{\upsilon}\psi\omega\sigma\eta\varsigma} (251)^{143} \equiv (-1)^{143}\ (mod\ 7) \Rightarrow$$
$$\Rightarrow (251)^{143} \equiv -1\ (mod\ 7) \Rightarrow (251)^{143} \equiv 6\ (mod\ 7)$$

Άρα ο αριθμός 251^{143} δίνει επίσης υπόλοιπο 6 στη διαίρεσή του με το 7.

Για τη διαίρεση $5^{100} = 5^{16\cdot 6+4} = 5^{16\cdot 6}5^4$ από το θεώρημα Euler Fermat έχουμε ότι:

Επειδή οι ακέραιοι 7 και 5 είναι coprime και $\varphi(7) = 6$, έχουμε ότι

$$5^6 \equiv 1\ (mod\ 7) \Rightarrow (251^6)^{16} = 5^{16\cdot 6} \equiv 1\ (mod\ 7)$$

Άρα μπορούμε να γράψουμε:

$$5^{100}\ (mod\ 7) = 5^{16\cdot 6} \cdot 5^4\ (mod\ 7) = 1 \cdot 5^4\ (mod\ 7)$$

Τέλος, έχουμε:

$$5 \equiv 2\ (mod\ 7) \xrightarrow[\sigma\varepsilon\ \delta\acute{\upsilon}\nu\alpha\mu\eta]{I\delta\iota\acute{o}\tau\eta\tau\alpha\ \acute{\upsilon}\psi\omega\sigma\eta\varsigma} 5^4\ (mod\ 7) \equiv 2^4\ (mod\ 7) \equiv 16\ (mod\ 7) \equiv 2\ (mod\ 7)$$

Οπότε βρήκαμε:

$$5^{100}\ mod\ 7 = 2\ (mod\ 7)$$

Οπότε το υπόλοιπο της διαίρεσης $5^{100}: 7$ είναι 2

Τέλος, για τη διαίρεση $16! = 16 \cdot 15 \cdot \ldots \cdot 2 \cdot 1$, από το θεώρημα Wilson, για τον πρώτο αριθμό 19 έχουμε ότι:

$$18! \equiv -1\ (mod\ 19) \Rightarrow 16! \cdot 17 \cdot 18 \equiv -1\ (mod\ 19) \Rightarrow 16! \cdot 17 \cdot (-1) \equiv -1\ (mod\ 19) \Rightarrow$$
$$\Rightarrow 16! \cdot 17 \equiv 1\ (mod\ 19)$$

Ο αντίστροφος του $17\ (mod\ 19)$ είναι ο x για τον οποίον: $2x \equiv 1\ (mod\ 19) \Rightarrow x = 9\ (mod\ 19)$

$$16! \cdot 17 \equiv 1\ (mod\ 19) \Rightarrow 16! \equiv 9\ (mod\ 19) \Rightarrow 16! \equiv 9\ (mod\ 19)$$

Άρα το υπόλοιπο της διαίρεσης $16!: 19$ είναι 9.

12. Να βρεθούν οι λύσεις (αν υπάρχουν) των ισοτιμιών $19x \equiv 30\ (mod\ 4)$ και $980x \equiv 1500\ (mod\ 1600)$.

Για την πρώτη ισοτιμία, $19x \equiv 30\ (mod\ 4)$, έχουμε:

$(19, 30) = 1$ σημαίνει ότι υπάρχει μοναδική λύση. Αυτή θα βρεθεί πολλαπλασιάζοντας με τον αντίστροφο του $19\ (mod\ 4)$ και τα 2 μέλη:

$$x \equiv 30 \cdot 19^{\varphi(4)-1}\ (mod\ 4) = 30 \cdot 19^{2-1}\ (mod\ 4) = 30 \cdot 19^{2-1}\ (mod\ 4) =$$
$$= 2 \cdot 3 \cdot 5 \cdot 19\ (mod\ 4) = 2 \cdot 3 \cdot 1 \cdot 3\ (mod\ 4) = 18\ (mod\ 4) \Rightarrow$$
$$\Rightarrow x \equiv 2\ (mod\ 4)$$

Για την ισοτιμία $980x \equiv 1500\ (mod\ 1600)$ είναι:

$(980, 1500) = 20$ άρα υπάρχει λύση. Η ισοτιμία, σε μορφή εξίσωσης, μας δίνει:

$$1500 - 980x = 1600n \Rightarrow 1500 = 980x + 1600n$$

Θα βρούμε τον μέγιστο κοινό διαιρέτη των $980, 1600$ με τον αλγόριθμο του Ευκλείδη:

$1600 = 1 \cdot 980 + 620$
$980 = 1 \cdot 620 + 360$
$620 = 1 \cdot 360 + 260$
$360 = 1 \cdot 260 + 100$
$260 = 2 \cdot 100 + 60$
$100 = 1 \cdot 60 + 40$
$60 = 1 \cdot 40 + \boxed{20} \leftarrow GCD$
$40 = 2 \cdot 20 + 0$

Ελέγχουμε ότι $20|1500$, αφού $1500 = 20 \cdot 75$, δηλαδή ότι υπάρχει η εγκύηση για μία λύση τουλάχιστον.

Θα βρούμε αρχικά μία λύση για την εξίσωση $20 = 980x + 1600n$, την $(x, n) = (x_1, n_1)$:

$$20 = 60 - 1 \cdot 40 =$$
$$= 60 - 1 \cdot (100 - 1 \cdot 60) = 2 \cdot 60 - 1 \cdot 100$$
$$= 2 \cdot (260 - 2 \cdot 100) - 1 \cdot 100 = 2 \cdot 260 - 5 \cdot 100 =$$
$$= 2 \cdot 260 - 5 \cdot (360 - 1 \cdot 260) = -5 \cdot 360 + 7 \cdot 260 =$$
$$= -5 \cdot 360 + 7 \cdot (620 - 1 \cdot 360) = 7 \cdot 620 - 12 \cdot 360 =$$
$$= 7 \cdot 620 - 12 \cdot (980 - 1 \cdot 620) = -12 \cdot 980 + 19 \cdot 620 =$$
$$= -12 \cdot 980 + 19 \cdot (1600 - 1 \cdot 980) = 19 \cdot 1600 - 31 \cdot 980$$

Βρήκαμε λοιπόν τη λύση $(x_1, n_1) = (-31, 19)$ και πολλαπλασιάζοντας με 75 προκύπτει η λύση στην αρχική εξίσωση: $(x, n) = (-2325, 1425)$.

Λόγω του $mod\ 1600$, έχουμε τις εξής υπόλοιπες λύσεις:

$$x = -2325 + \frac{1600}{20}k, n = 1425 - \frac{980}{20}k,$$

Για τη λύση της ισοτιμίας μας ενδιαφέρουν μόνο οι λύσεις που βρήκαμε για το $x\ (mod\ 1600)$, άρα έχουμε:

$$x \equiv -2325 + 80k\ (mod\ 1600) \equiv 875 + 80k\ (mod\ 1600)$$

Και είναι στο πλήθος όσο και ο gcd των $980, 1500$, δηλαδή 20.

13. Βρείτε έναν αριθμό ο οποίος είναι πολλαπλάσιο του 11 και δίνει υπόλοιπο 1 όταν διαιρεθεί με τους αριθμούς $2, 3, 5, 7$.

Έστω υπάρχει τέτοιος αριθμός, ο n. Για να δίνει υπόλοιπο 1 όταν διαιρεθεί με τους αριθμούς $2, 3, 5, 7$, θα ισχύει $n = 1\ mod\ k \Rightarrow n - 1 = 0\ mod\ k, k = \{2, 3, 5, 7\}$. Αφού ο $n - 1$ διαιρείται με τους 4 αυτούς αριθμούς, τότε ο $n - 1$ θα έχει για παράγοντες όλους αυτούς, θα είναι δηλαδή κάποιο πολλαπλάσιο του ελάχιστου κοινού πολλαπλασίου των $2, 3, 5, 7$:

$$n - 1 = \lambda \cdot LCM(2, 3, 5, 7) = 210\lambda \Rightarrow n = 210\lambda + 1$$

Επιπλέον, θέλουμε ο n να διαιρείται ακριβώς με το 11, δηλαδή να ισχύει:

$$n|11 \Rightarrow 210\lambda + 1|11$$

Το κριτήριο διαιρετότητας με τον αριθμό 11 λέει ότι ένας αριθμός x sδιαιρείται με το 11 αν $(x\ mod\ 100 + x/100)|11$ (αν το άθροισμα του αριθμού που σχηματίζουν τα 2 τελευταία ψηφία με τον αριθμό που σχηματίζουν τα υπόλοιπα ψηφία διαιρούνται με το 11).

Παρατηρούμε ότι για $\lambda = 10$ έχουμε $n = 210 \cdot 10 + 1 = 2101$ που διαιρείται με το 11.

Άρα ο αριθμός 2101 είναι ένας αριθμός που ικανοποιεί το ζητούμενο!

14. Δείξτε ότι υπάρχουν άπειροι πρώτοι της μορφής $3k+2$, και ότι για κάθε $n \geq 3$ υπάρχουν άπειροι πρώτοι αριθμοί που δεν είναι της μορφής $nk+1$.

Για το πρώτο ζητούμενο, έστω οι πρώτοι της μορφής $3k+2$ είναι οι $p_1, p_2, \dots, p_n$, πεπερασμένοι. Θεωρούμε τον αριθμό $N = 3p_1p_2 \dots p_n + 2$.

Αφού p_i πρώτοι, κανένας από αυτούς δε διαιρεί τον N, αφού αφήνουν υπόλοιπο 2, ομοίως και για τον αριθμό 3. Επίσης, ούτε ο 2 διαιρεί τον N, αφού ο τελευταίος είναι άθροισμα άρτιου με γινόμενο περιττών, άρα περιττός.

- Έστω ότι οι πρώτοι διαιρέτες του N ήταν όλοι της μορφής $3k+1$. Τότε, θα ήταν
$$N = (3k_1+1)(3k_2+1)\cdots(3k_l+1) = 3\lambda + 1$$
*Αυτό ισχύει διότι, αν κάνουμε τους πολλαπλασιασμούς, ο μόνος όρος που δεν πολλαπλασιάζεται με 3 είναι εκείνος που προκύπτει από τον πολλαπλασιασμό $1 \cdot \dots \cdot 1$. Έχουμε λοιπόν την αντίφαση $N = 3\lambda + 1 \wedge N = 3k+2 \Rightarrow Άτοπο$.

- Ακόμα, ένας πρώτος διαιρέτης είναι αδύνατον να είναι της μορφής $3k+3$, αφού τότε θα ήταν σύνθετος.

- Άρα καταλήγουμε ότι θα υπάρχει τουλάχιστον ένας πρώτος διαιρέτης του N της μορφής $3k+2$.

Συνεπώς, βρήκαμε ότι θα υπάρχει ένας πρώτος της μορφής $3k+2$ που διαιρεί τον N. Άλλα ξεκινήσαμε με την υπόθεση ότι οι πρώτοι της μορφής $3k+2$ είναι πεπερασμένοι, n το πλήθος, και κανένας από αυτούς διαιρεί τον N. Βρήκαμε δηλαδή έναν επιπλέον πρώτο, άρα καταλήξαμε σε άτοπο! Άρα πράγματι, υπάρχουν άπειροι πρώτοι της μορφής $3k+2$.