Φυλ 9 ασκ.

Έστω $a, n \in \mathbb{Z}$ με $n \geq 1$ κ' $ΜΚΔ(a,n)=1$

Έστω $x \geq 1$ ακέραιος. Ν.δ.ο $a^x \equiv 1 \bmod n$ αν $ord_n(a) \mid x$

Σαν εφαρμογή, να βρεθούν όλες οι θετικές λύσεις x της ισοτιμίας $2^x \equiv 1 \pmod 7$

<u>Λύση</u>: Θέτουμε $d = ord_n(a)$. Από θεωρία, για $k, k' \geq 0$ έχουμε $a^k \equiv a^{k'} \bmod n$ αν $k \equiv k' \bmod d$. Από ορισμό τάξης $a^d \equiv 1 \bmod n$. Άρα $a^x \equiv 1 \bmod n \Leftrightarrow$ $a^x \equiv a^d \bmod n \Leftrightarrow x \equiv d \bmod d \Leftrightarrow x \equiv 0 \bmod d \Leftrightarrow d \mid x$

Υπολογίζουμε $d = ord_7(2)$. $2^1 = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1 \bmod 7$. Συνεπώς $d = 3$. Άρα $2^x \equiv 1 \pmod 7$ κ' $x \geq 1$, αν $3 \mid x$

Φυλ 9 ασκ 2

Έστω $n \in \mathbb{Z}$ με $n \geq 3$. Ν.δ.ο για $a = n-1$ έχουμε $ΜΚΔ(a,n)=1$ κ' $ord_n(a) = 2$

Σαν συνέπεια, το $\phi(n)$ άρτιος.

<u>Λύση</u>:

$ΜΚΔ(a,n) = ΜΚΔ(n-1, n) = ΜΚΔ(n-1, n-(n-1)) = ΜΚΔ(n-1, 1) = 1$

Αφού $n \geq 3$, $[n-1]_n \neq [1]_n$ (γιατί $n \nmid n-2$, όταν $n \geq 3$)

Έχουμε $([n-1]_n) = [-1]_n$, άρα $([n-1]_n)^2 = ([-1]_n)^2 = [(-1)^2]_n = [1]_n$

Συνεπώς, $ord_n(a) = 2$

Από θεωρία, αν $n \geq 2$, $ΜΚΔ(a, n) = 1$, τότε $ord_n(a) \mid \phi(n)$

Άρα για $a = n-1$ κ' $n \geq 3$ έπεται $2 \mid \phi(n)$

Φυλ 9 ασκ 7

(i) Δο το 3 είναι αρχική ρίζα mod17

(ii) Για οποιονδήποτε ακέραιο a με $1 \leq a \leq 17$ κ' $ΜΚΔ(a, 17) = 1$ υπολογίστε τον ελάχιστο θετικό ακέραιο k με $3^k \equiv a \pmod{17}$

(iii) Λύστε για $x \in \mathbb{Z}$ την ισοδυναμία $x^4 \equiv 13 \pmod{17}$

δεν είναι γραμμική ως προς x

Λύση: (i) Έχουμε 17 πρώτος (με τα γνωστά με τις Γ), άρα $\phi(17) = 17\left(1 - \frac{1}{17}\right) = 17 - 1 = 16$

Φανερά $ΜΚΔ(3, 17) = 1$

Αφού $ord_{17}(3) \mid 16$ έχουμε $ord_{17}(3) \in \{1, 2, 4, 8, 16\}$

Συνεπώς αρκεί ισο $[3^m]_{17} \neq [1]_{17}$, για $m \in \{1, 2, 4, 8\}$. Επειδή $1 \mid 8$ κ' $2 \mid 8$ κ' $4 \mid 8$, αρκεί ισο $[3^8]_{17} \neq [1]_{17}$

Λόγω του (ii) θα υπολογίσουμε $[3^m]_{17}$ $\forall\, 1 \leq m \leq 16 = \phi(17)$

Δουλεύουμε mod17 $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv \underset{[27]_{17}}{10}$, $3^4 \equiv 3^3 \cdot 3 \equiv 10 \cdot 3 \equiv \underset{\text{mod}17}{13} \equiv -4$

$3^5 \equiv -12 \equiv 5$, $3^6 \equiv 15 \equiv -2$, $3^7 \equiv -6 \equiv 11$, $3^8 \equiv -18 \equiv -1 \equiv 16$

$3^9 \equiv -3 \equiv 14$, $3^{10} \equiv -9 \equiv 8$, $3^{11} \equiv -10 \equiv 7$, $3^{12} \equiv 21 \equiv 4$, $3^{13} \equiv 12 \equiv -5$, $3^{14} \equiv -15 \equiv 2$

$3^{15} \equiv 6$, $3^{16} \equiv 1$

Επομένως, 3 η αρχική ρίζα mod 17

(ii)

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
k	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

διακριτός λογάριθμος του a ως προς 3

(Παρατήρηση: Πιο γενικά, αν $n \geq 2$ κ' a αρχική ρίζα mod n, έχουμε $U(\mathbb{Z}/n) = \{[a]_n, [a^2]_n, \dots, [a^d]_n\}$, όπου $d = \#U(\mathbb{Z}/n) = \phi(n) = ord_n(a)$)

Άρα $\forall b \in \mathbb{Z}$ με $1 \leq b \leq n$ κ' $ΜΚΔ(b,n) = 1$, $\exists$ ελάχιστος θετικός ακέραιος m, ώστε $b \equiv a^m \bmod n$

Εξήγηση Πίνακα) Έαν $a \in \mathbb{Z}$ με $1 \leq a \leq 16$. Ο ελάχιστος θετικός ακέραιος k με $3^k \equiv a \bmod 17$ είναι ο ακέραιος κάτω από το a. π.χ. Αν $a = 15$, τότε $k = 6$

(ιι) Έαν $x \in \mathbb{Z}$ με $x^4 \equiv 13 \bmod 17$ τότε $ΜΚΔ(x^4, 17) = ΜΚΔ(13, 17) = 1$,
άρα $ΜΚΔ(x, 17) = 1$

Βήμα 1ο: $\exists$ (μοναδικό) $y \in \{1, 2, \dots, 16\}$ ώστε $[x]_{17} = ([3]_{17})^y$

Ο λόγος είναι ότι 3 είναι αρχική ρίζα mod 17 κ' $ΜΚΔ(x, 17) = 1$

Επομένως, $[x^4]_{17} = [13]_{17} \iff ([3^y]_{17})^4 = [13]_{17} \iff [3^{4y}]_{17} = [13]_{17} \iff$
$3^{4y} \equiv 13 \bmod 17 \underset{\text{πίνακα}}{\iff} 3^{4y} \equiv 3^4 \bmod 17 \iff 4y \equiv 4 \bmod ord_{17}(3)$

$\iff 4y \equiv 4 \bmod 16 \iff y \equiv 1 \bmod 4$. Αφού $1 \leq y \leq 16$, έχουμε $y \in \{1, 5, 9, 13\}$

Άρα για $y = 1$, $[x]_{17} = [3^y]_{17} = [3]_{17}$
$y = 5$, $[x]_{17} = [3^y]_{17} = [3^5]_{17} = [5]_{17}$
$y = 9$, $[x]_{17} = [3^y]_{17} = [3^9]_{17} = [14]_{17}$
$y = 13$, $[x]_{17} = [3^y]_{17} = [3^{13}]_{17} = [12]_{17}$

Επομένως, το $x \in \mathbb{Z}$ λύση της $x^4 \equiv 13 \bmod 17$ αν $[x]_{17} \in \{[3]_{17}, [5]_{17}, [12]_{17}, [14]_{17}\}$
Με άλλα λόγια αν το υπόλοιπο της Ευκλ. Διαιρ. του x με 17 είναι 3 ή 5 ή 12 ή 14

Θέμα (Ιανουαρίου 2018)

Βρείτε όλες τις ακέραιες λύσεις της Διοφαντικής εξίσωσης $42x - 93y = 123$ (*) ή αποδείξτε ότι $\nexists$ ακέραιες λύσεις

(Υπενθύμιση: Έαν $c, a, b \in \mathbb{Z}$ με $a \neq 0$ κ' $ax + by = c$ (**)

Βήμα 1ο: Θέτουμε $d = ΜΚΔ(a, b)$

Βήμα 2ο: Αν $d \nmid c$, η (**) ΔΕΝ έχει ακέραιες λύσεις

Βήμα 3ο: Υποθέτουμε ότι $d \mid c$. Με Ευκλ. Αλγόριθμο υπολογίζουμε $z_1, z_2 \in \mathbb{Z}$ με $d = z_1 a + z_2 b$. Τότε, το σύνολο λύσεων της (**) είναι το εξίσ

$A = \{ (x,y) = (z_1 \frac{c}{d} + t\frac{b}{d}, z_2 \frac{c}{d} - \frac{a}{d}) \mid t \in \mathbb{Z} \}$

Θέτουμε $a = 42$, $b = -93$, $c = 123$, $d = ΜΚΔ(a,b)$

Έχουμε $d = ΜΚΔ(a,b) = ΜΚΔ(a,-b) = ΜΚΔ(42, 93)$

Υπολογίζουμε

$93 = 2 \cdot 42 + 9$ $\qquad$ $6 = 2\cdot 3 + 0$

$42 = 4 \cdot 9 + 6$

$9 = 6 + 3$ $\qquad$ Επομένως $d = 3$

Έχουμε $3 \mid 123 = c$, γιατί $3 \mid (1+2+3) = 6$

Υπάρχουν z_1, z_2 με $d = z_1 a + z_2 b$

$3 = 9 - 6 = 9 - (42 - 4\cdot 9) = 5\cdot 9 - 1\cdot 42 = 5(93 - 2\cdot 42) - 1\cdot 42 =$

$= (-11)\cdot 42 + (-5)(-93)$

Θέτουμε $z_1 = -11$, $z_2 = -5$

Επομένως, το σύνολο λύσεων της διοφαντικής (*) είναι

$\{(-11 \frac{123}{3} + t\frac{(-93)}{3}, (-5)\frac{123}{3} - t\frac{42}{3}) \mid t \in \mathbb{Z}\} =$

$= \{(-11\cdot 41 + t(-31), (-5)41 - t14) \mid t \in \mathbb{Z}\} =$

$= \{(-451 + t(-31), -205 - t14) \mid t \in \mathbb{Z}\}$

ΠΑΠΙ θέμα (Ιαν 2018)

Βρείτε όλα τα $a \in \mathbb{Z}$, για τα οποία $ΜΚΔ(3a+2, 7a+1) = 11$

Λύση:

$ΜΚΔ(3a+2, 7a+1) = ΜΚΔ(3a+2, (7a+1) - 2(3a+2)) =$

$= ΜΚΔ(3a+2, a-3) = ΜΚΔ((3a+2) - 3(a-3), a-3) =$

$= ΜΚΔ(11, a-3)$

Συνεπώς $ΜΚΔ(3a+2, 7a+1) = 11 \Leftrightarrow ΜΚΔ(11, a-3) = 11$

$\Leftrightarrow 11 \mid a-3 \Leftrightarrow a \equiv 3 \bmod 11 \Leftrightarrow \exists k \in \mathbb{Z}$ με $a = 11k+3$

$\Leftrightarrow a \in \{\ldots, -30, -19, -8, 3, 14, 25, 36, 47, \ldots\}$