Εδώ Σελ 18

Άσκηση 1: Αποδείξτε ότι το 53 είναι πρώτος αριθμός.

Λύση $7^2 \leq 53 \leq 8^2 \Rightarrow 7 \leq \sqrt{53} \leq 8$ Έστω ότι το 53 είναι σύνθετο.

$\Rightarrow$ Τότε έχει έναν τουλάχιστον πρώτο διαιρέτη μικρότερο του $\sqrt{53}$. Άρα, έχει διαιρέτη έναν από τους πρώτους αριθμούς 2, 3, 5, 7.

Όμως: $2 \nmid 53$

$3 \nmid 53$

$5 \nmid 53$

$7 \nmid 53$ αφού $53 = 7 \cdot 7 + 4$.

Άτοπο! Άρα ο 53 είναι πρώτος αριθμός

β) Αποδείξτε ότι το 3 είναι αρχική ρίζα modulo 53 ενώ το 7 δεν είναι

Λύση $\varphi(53) = 53 - 1 = 52$, διότι το 53 είναι πρώτος

$\mu\kappa\delta(53, 3) = 1$. Άρα το 3 έχει τάξη modulo 53.

$\text{ord}_{53}(3) \mid \varphi(53) = 52$

Άρα $\text{ord}_{53}(3) \in \{1, 2, 4, 13, 26, 52\}$

$3^1 \equiv 3 \bmod 53$ $\quad \text{ord}_{53}(3) \neq 1$

$3^2 \equiv 9 \bmod 53$ $\quad \text{ord}_{53}(3) \neq 2$

$3^4 \equiv 81 \bmod 53$

$\equiv 28 \bmod 53$ $\quad \text{ord}_{53}(3) \neq 4$

$3^{13} \equiv 3^4 \cdot 3^4 \cdot 3^4 \cdot 3 \bmod 53$

$\equiv 28 \cdot 28 \cdot 28 \cdot 3 \bmod 53$

$\equiv 784 \cdot 84 \bmod 53$ αφαιρώ από τα 784 και 84 από 53-άρια

$\equiv (-11) \cdot 31 \bmod 53$

$\equiv -341 \bmod 53$

$\equiv 30 \bmod 53$ $\quad \text{ord}_{53}(3) \neq 13$

$3^{26} \equiv 3^{13} \cdot 3^{13} \bmod 53$

$\equiv 30 \cdot 30 \bmod 53$

$\equiv 900 \bmod 53$

$\equiv -2 \bmod 53$ $\quad \text{ord}_{53}(3) \neq 26$

Άρα η τάξη του 3 είναι 52
$ord_{53}(3) = 52$
Άρα, το 3 είναι αρχική ρίζα modulo 53.

$\mu\kappa\delta(7, 53) = 1 \Rightarrow$ το 7 έχει τάξη και $ord_{53}(7) / \varphi(53) = 52$
$= 4 \cdot 13$

$\Rightarrow ord_{53}(7) \in \{1, 2, 4, 13, 26, 52\}$

$7^2 \equiv 7 \bmod 53 \neq 1 \bmod 53 \quad ord_{53}(7) \neq 1$
$7^2 \equiv 49 \bmod 53 \neq 1 \bmod 53 \quad ord_{53}(7) \neq 2$
$7^4 \equiv 49 \cdot 49 \bmod 53$
$\equiv (-4)(-4) \bmod 53$
$\equiv 26 \bmod 53 \neq 1 \bmod 53 \quad ord_{53}(7) \neq 4$
$7^{13} \equiv 7^4 \cdot 7^4 \cdot 7^4 \cdot 7 \bmod 53$
$\equiv 16 \cdot 16 \cdot 16 \cdot 7 \bmod 53$
$\equiv 256 \cdot 16 \cdot 7 \bmod 53$
$\equiv 256 \cdot 112 \bmod 53$
$\equiv 44 \cdot 6 \bmod 53$
$\equiv (-9) \cdot 6 \bmod 53$
$\equiv -54 \bmod 53$
$\equiv -1 \bmod 53 \neq 1 \bmod 53 \quad ord_{53}(7) \neq 13$
$7^{26} \equiv 7^{13} \cdot 7^{13} \bmod 53$
$\equiv (-1)(-1) \bmod 53$
$\equiv 1 \bmod 53$
Άρα $ord_{53}(7) = 26$
Άρα το 7 δεν είναι αρχική ρίζα modulo 53. Αν ήταν θα είχε τάξη $52 = \varphi(53)$

4) Βρείτε όλους τους φυσικούς x ώστε $x \leq 70$ και $ord_{53}(3^x) = 26$
$1 \leq x \leq 70$

Λύση $ord(a^s) = \frac{ord(a)}{\mu\kappa\delta(s, ord(a))}$

$26 = ord_{53}(3^x) = \frac{ord(3)}{\mu\kappa\delta(x, ord(3))} = \frac{52}{\mu\kappa\delta(x, 52)} \Rightarrow \mu\kappa\delta(x, 52) = \frac{52}{26} = 1$

$\Rightarrow \mu\kappa\delta(x, 52) = 2$

Οπότε $x$: $\{2, 6, 10, 14, 18, 22, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 70\}$

5) Βρείτε όλους τους φυσικούς αριθμούς $y$ τέτοιους ώστε το

$3^{4y} \equiv 1 \bmod 53$

Λύση $\left( \begin{array}{l} ord(a) = s \\ a^k \equiv a^\lambda \bmod n \end{array} \middle| \Rightarrow k \equiv \lambda \bmod s \right)$

$ord_{53}(3) = 52$

$3^{4y} \equiv 3^0 \bmod 53$

$4y \equiv 0 \bmod 52$

$4y \equiv 4 \cdot 0 \bmod 4 \cdot 13 \Leftrightarrow y \equiv 0 \bmod 13$, $y$ πολλαπλάσιο του 13

Άσκηση: Να δειχθεί ότι $(a,b) = (a+b, [a,b])$

Λύση $(a,b)[a,b] = ab$ (ο τύπος ισχύει μόνο για 2 αριθμούς)

Θέλω να δείξω ότι $d = \left(a+b, \frac{ab}{d}\right)$

$a = da'$

$b = db'$

$d = (a,b) = (da', db') = d(a', b') \Rightarrow (a', b') = 1$

Θέλω να δείξω ότι $d = \left(a+b, \frac{ab}{d}\right) \Leftrightarrow$

$\Leftrightarrow d = \left(da'+db', \frac{da' \cdot db'}{d}\right) \Leftrightarrow d = (d(a'+b'), d(a'b'))$

$\Leftrightarrow 1 = (a'+b', a'b')$ Δείξτε ότι αν $(a',b') = 1 \Rightarrow (a'+b', a'b') = 1$

Έστω ότι $\mu\kappa\delta(a'+b', a'b') = d' > 1$

Άρα υπάρχει $p$: πρώτος τέτοιος ώστε $p \mid d', \; \begin{matrix} d' \mid a'+b' \\ d' \mid a'b' \end{matrix} \Rightarrow$

$\left. \begin{array}{l} \Rightarrow p \mid a'+b' \\ p \mid a'b' \\ p: \text{πρώτος} \end{array} \right\} \Rightarrow p \mid a' \text{ ή } p \mid b'$

1η περίπτωση: $\left.\begin{matrix} p \mid a' \\ p \mid a'+b' \end{matrix}\right\} \Rightarrow p \mid \boxed{-1} a' + \boxed{1}(a'+b') \Rightarrow p \mid b'$

$\Rightarrow p \mid a'$ $\Rightarrow p \mid \text{μκδ}(a',b') = 1$ Άτοπο!

$p \mid b'$

2η περίπτωση: $\left.\begin{matrix} p \mid b' \\ p \mid a'+b' \end{matrix}\right\} \Rightarrow p \mid \boxed{1}(a'+b') + \boxed{-1} b' \Rightarrow p \mid a'$

Άρα $\left.\begin{matrix} p \mid a' \\ p \mid b' \end{matrix}\right\} \Rightarrow p \mid \text{μκδ}(a',b') = 1$ Άτοπο!

Συνεπώς $d' = 1$

Άσκηση: Πόσοι αριθμοί μεταξύ του 1 και το 50 είναι πρώτοι με το 50?

Λύση $\phi(50) = \phi(2 \cdot 25) = \phi(2 \cdot 5^2) = 2^{1-1}(2-1) \cdot 5^{2-1}(5-1) =$

$= 5 \cdot 4 = 20 \Rightarrow$

$\Rightarrow \phi(50) = 20$

Άσκηση: Πόσοι αριθμοί μεταξύ του 51 και του 100 είναι πρώτοι με το 50?

Λύση $\phi(50) = 20$

Άσκηση: Πόσοι αριθμοί μεταξύ του 1 και του 100 είναι πρώτοι με το 50?

Λύση $2\phi(50) = 2 \cdot 20 = 40$

Άσκηση: Πόσοι αριθμοί μεταξύ του 1 και του 1200 είναι πρώτοι με το 50?

Λύση $24\phi(50) = 24 \cdot 20 = 480$

Άσκηση: Πόσοι ακέραιοι μεταξύ του 3 και του 1202 είναι πρώτοι με το 50?

Λύση $24\phi(50) = 480$

Άσκηση: Πόσοι ακέραιοι μεταξύ του 103 και του 1202 είναι πρώτοι με το 50?

Λύση $22\phi(50) = 22 \cdot 20 = 440$

Άσκηση: Πόσοι ακέραιοι μεταξύ του 1 και του 53 είναι πρώτοι με το 50?

Λύση $\phi(50) + 2 = 22$

Άσκηση: Πόσοι ακέραιοι μεταξύ του 3 και του 50 είναι πρώτοι με το 50?

Λύση $\phi(50) - 1 = 19$