06/12/2018

Φυλλάδιο 6 - Άσκηση 8:

Δείξτε ότι:

(α) $2^{20} - 1 \equiv 0 \mod 41$

Λύση: Έχουμε $\sqrt{41} < 7$ και 2,3,5 δεν διαιρούν το 41. Άρα 41 πρώτος $\Rightarrow \varphi(41) = 40$. Από Θ. Fermat $2^{40} \equiv 1 \mod 41$

Αλλά εμείς θέλουμε ν.δ.ο. $2^{20} \equiv 1 \mod 41$

Επομένως κάνουμε πράξεις

$[2^2]_{41} = [4]_{41}$ $\qquad [2^6]_{41} = [(2^2)^3]_{41} \cancel{= ([2^2]_{41})^3 =}$

$= [4^3]_{41} = [64]_{41} = [23]_{41}$

Συνεπώς $[2^{10}]_{41} = [2^4 \cdot 2^6]_{41} = [2^4]_{41} [2^6]_{41} = [16]_{41} [23]_{41} =$

$= [368]_{41} = [41 \cdot 8 + 40]_{41}$

Συνεπώς $[2^{20}]_{41} = [(2^{10})^2]_{41} = ([2^{10}]_{41})^2 = ([-1]_{41})^2 =$

$= [1]_{41}$

(b) $2^{50} \equiv 4 \mod 7$

Έχουμε 7, πρώτος. ~~Συνεπώς από προηγούμενο έχουμε~~

$\Rightarrow \varphi(7) = 6$

Συνεπώς, αφού ΜΚΔ$(2,7)=1$ από Θ. Euler-Fermat

$[2^6]_7 = [1]_7$ (1)

Κάνουμε ευκλείδεια διαίρεση του 50 με το 6

$50 = 8 \cdot 6 + 2$

Συνεπώς, $[2^{50}]_7 = [2^{8\cdot 6+2}]_7 = [2^{8\cdot 6} \cdot 2^2]_7 = [2^{6}]_7^{8} [2^2]_7 =$

$= ([2^6]_7)^8 \cdot [2^2]_7 = ([1]_7)^8 [4]_7 = [1^8]_7 [4]_7 =$

$= [1]_7 [4]_7 = [4]_7$

Παρατήρηση: Αν ΜΚΔ$(a,n)=1$ και $k \in \mathbb{N}$ ~~έχουμε~~ και r το υπόλοιπο της ευκλ. διαίρεσης του n με το $\varphi(n)$, έχουμε από το Θ. Euler-Fermat $[a^k]_n = [a^r]_n$.

Παράδειγμα: Βρείτε το υπόλοιπο της διαίρεσης του 61^{97} με το 65.

Λύση:

Βήμα - 1ο: Αρκεί να βρω a με $0 \le a < 65$ ώστε $[61^{97}]_{65} = [a]_{65}$

Τότε το a είναι το ζητούμενο υπόλοιπο.

Βήμα - 2ο: $65 = 5 \cdot 13 \Rightarrow \varphi(65) = (5-1)(13-1) = 48$

Κάνουμε Ευκλ. διαίρ. του 97 με το 48

Έχουμε $97 = 2 \cdot 48 + 1$.

Βήμα 3ο: Δείχνουμε ΜΚΔ$(61,65)=1$

$(61,65) = (61, 65-61) = (61,4) = (61-4\cdot 15, 4) = (1,4) = 1$

Βήμα 4ο. Αφού δείξαμε ΜΚΔ$(61, 65) = 1$ από την παρατήρηση και την $(*) \Rightarrow [61]^{97}_{65} = [61^1]_{65} = [61]_{65}$

Αφού $0 \leq 61 \leq 65$, έχουμε ότι το υπόλοιπο της Ευκλ. Διαίρεσης του 61^{97} με το 65 είναι 61.

Θεώρημα (Wilson): Έστω $n > 1$ ακέραιος. Τα ακόλουθα είναι ισοδύναμα:

(1) n πρώτος

(2) $(n-1)! \equiv -1 \bmod n$.

Απόδειξη

(1) $\Rightarrow$ (2) χωρίς απόδειξη

(2) $\Rightarrow$ (1) Υποθέτουμε ότι $n > 1$, $(n-1)! \equiv -1 \bmod n$ και n σύνθετος και θα βρούμε αντίφαση. Αφού $n > 1$ σύνθετος υπάρχουν r, s με $2 \leq r, s$ ώστε $n = r \cdot s$

Αφού $2 \leq s \Rightarrow r \leq n-1$. Συνεπώς $r \mid (n-1)!$ (1)

Αφού $(n-1)! \equiv -1 \bmod n \Rightarrow n \mid (n-1)! + 1$ (2)

Αφού $r \mid n \overset{(2)}{\Rightarrow} r \mid (n-1)! + 1$ (3)

Από (1) + (3) $\Rightarrow r \mid ((n-1)! + 1 - (n-1)!) \Rightarrow r \mid 1$ αντίφαση, αφού $r \geq 2$.

* **Παράδειγμα**: Αποδείξτε ότι ο 101 είναι πρώτος. Μετά βρείτε το υπόλοιπο της διαίρεσης του $97!$ με το 101.

Λύση: $\sqrt{101} < 11$. Οι πρώτοι < 11 είναι 2, 3, 5, 7.

$2 \nmid 101$ προφανώς, $3 \nmid 101$ γιατί $3 \nmid (1 + 0 + 1) = 2$

$5 \nmid 101$ προφανώς

$7 \nmid 101$ γιατί $101 = 14 \cdot 7 + 3$, άρα το υπόλοιπο της Ευκλ. διαίρ. του 101 με το 7 είναι $3 \neq 0$.

Βήμα 2ο: Αρκεί να βρούμε $a \in \mathbb{Z}$ με $0 \leq a < 101$ ώστε $[97!]_{101} = [a]_{101}$. Τότε a το υπόλοιπο που ψάχνουμε.

Βήμα 3ο: Αφού 101 πρώτος από Θ. Wilson
$100! \equiv -1 \mod 101$ άρα $[100!]_{101} = [-1]_{101}$
$\Rightarrow [(97!)(98)(99)(100)]_{101} = [-1]_{101}$
$\Rightarrow [97!]_{101}[98]_{101}[99]_{101}[100]_{101} = [-1]_{101}$
$\Rightarrow [97!]_{101}[-3]_{101}[-2]_{101}[-1]_{101} = [-1]_{101}$
$\Rightarrow [97!]_{101}[(-3)(-2)(-1)]_{101} = [-1]_{101} \Rightarrow$
$[97]_{101}[-6]_{101} = [-1]_{101}$
$\Rightarrow [97!]_{101}[-6]_{101}[-1]_{101} = [-1]_{101}[-1]_{101} \Rightarrow$
$\Rightarrow [97!]_{101}[6]_{101} = [1]_{101}$ $(*)$
Αφού 101 πρώτος και $1 \leq 6 < 101$ έχουμε ΜΚΔ$(6, 101) = 1$
Συνεπώς, το $[6]_{101}$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_{101}$
Υπολογίζουμε $c \in \mathbb{Z}$ με $([-6]_{101})^{-1} = [c]_{101}$ με το γνωστό αλγόριθμο. Μετά τις πράξεις έχουμε $([6]_{101})^{-1} = [17]_{101}$

Άρα $(*) \Rightarrow [97!]_{101}[6]_{101}[17]_{101} = [1]_{101} \cdot [17]_{101} \Rightarrow$
$[97!]_{101} \cdot [1]_{101} = [17]_{101} \Rightarrow [97!]_{101} = [17]_{101}$

Άρα το υπόλοιπο της Ευκλ. Διαιρ. του 97! με το 101 είναι το 17.