29/11/2018

Ορισμός Ονομάζουμε ένα σύνολο από $\phi(n)$ σε πλήθος ακεραίους $[a_1, \dots, a_{\phi(n)}]$ ένα περιορισμένο σύστημα υπολοίπων modulo n αν

i) $a_i \not\equiv a_j \bmod n$

ii) $\text{μκδ}(a_i, n) = 1$ για κάθε $i \in \{1, \dots, \phi(n)\}$

Παράδειγμα : $n = 10$

$\phi(10) = \phi(2^1 \cdot 5^1) = 2^{1-1}(2-1)5^{1-1}(5-1) = 2^0 \cdot 1 \cdot 5^0 \cdot 4 = 4$

ϕ: συνάρτηση του Euler

$\phi(1) = 1$

$\phi(p_1^{a_1} \dots p_s^{a_s}) = p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\dots p_s^{a_s-1}(p_s-1)$

Πλήρες σύστημα υπολοίπων modulo 10: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Περιορισμένο σύστημα υπολοίπων modulo 10: $\{1, 3, 7, 9\}$

n $\{11, 1243, -3, -111\}$

n_2 $\{13, 247, -121, -99\}$

Πρόταση Αν το σύνολο $\{a_1, a_2, \dots, a_{\phi(n)}\}$ είναι ένα περιορισμένο σύστημα υπολοίπων modulo n και $\text{μκδ}(a, n) = 1$, τότε και το σύνολο $\{aa_1, aa_2, \dots, aa_{\phi(n)}\}$ είναι ένα περιορισμένο σύστημα υπολοίπων modulo n

Παράδειγμα : $\text{μκδ}(3, 10) = 1$

$\{11, 53, 17, 9\}$ $\{33, 159, 51, 27\}$

Απόδειξη $\{aa_1, aa_2, \dots, aa_{\phi(n)}\}$ είναι $\phi(n)$ σε πλήθος

Ισχυριζόμαστε ότι $aa_i \not\equiv aa_j \bmod n$

Έστω $aa_i \equiv aa_j \bmod n$, $i \neq j$ $\overset{\text{πρ}}{\Rightarrow}$ $a_i \equiv a_j \bmod n$

$\text{μκδ}(a, n) = 1$ $i \neq j$ Άτοπο

Ισχυριζόμαστε ότι $\text{μκδ}(aa_i, n) = 1$

Έστω ότι $\text{μκδ}(aa_i, n) = d > 1$

Αρα υπάρχει p πρώτος τέτοιος ώστε $p|d \Rightarrow$

$$\left.\begin{array}{l} \Rightarrow p|d \quad d|aai \\ \qquad\quad d|n \end{array}\right\} \Rightarrow \left.\begin{array}{l} p|aai \\ p|n \\ p: \text{πρώτος} \end{array}\right\} \Rightarrow \begin{array}{l} p|a \quad \text{ή} \quad p|ai \\ p|n \end{array}$$

1η περίπτωση: $\left.\begin{array}{l} p|a \\ p|n \end{array}\right\} \Rightarrow p|\text{μκδ}(a,n)=1$ Άτοπο
(το 1 είναι μόνο ένα διαιρέτη του 1 και το 1 δεν είναι πρώτος)

2η περίπτωση: $\left.\begin{array}{l} p|ai \\ p|n \end{array}\right\} \Rightarrow p|\text{μκδ}(ai,n)=1$ Άτοπο

Επομένως, $\text{μκδ}(aai,n)=1$

Θεώρημα Euler Αν ο n είναι φυσικός αριθμός και a ακέραιος με $\text{μκδ}(a,n)=1$ τότε:

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Παράδειγμα $n=1000$

$(12743, 1000)=1$ $\qquad \varphi(1000)=\varphi(2^3\cdot 5^3)=2^{3-1}(2-1)5^{3-1}(5-1)=1$

$\Rightarrow \varphi(1000)=400$

$12743^{\varphi(1000)} \equiv 1 \bmod 1000 \Leftrightarrow 12743^{400} \equiv 1 \bmod 1000$

Απόδειξη Έστω $\{a_1, a_2 \ldots, a_{\varphi(n)}\}$ ένα περιοριστικό σύστημα υπολοίπων modulo n.

Έστω $\text{μκδ}(a,n)=1$. Τότε $\{aa_1, aa_2, \ldots, aa_{\varphi(n)}\}$ περιοριστικό σύστημα υπολοίπων

$aa_1 \cdot aa_2 \cdots aa_{\varphi(n)} \equiv a_1 a_2 \ldots a_{\varphi(n)} \bmod n$

$a_1 a_2 \ldots a_{\varphi(n)} a^{\varphi(n)} \equiv a_1 a_2 \ldots a_{\varphi(n)} \bmod n$

$\cdot \text{μκδ}(a_2,n)=1 \rightarrow a_2 \ldots a_{\varphi(n)} a^{\varphi(n)} \equiv a_2 \ldots a_{\varphi(n)} \bmod n$

$\cdot \text{μκδ}(a_2,n)=1$

$\vdots$

$a_{\varphi(n)} a^{\varphi(n)} \equiv a_{\varphi(n)} \cdot 1 \bmod n$

$\cdot \text{μκδ}(a_{\varphi(n)},n)=1 \rightarrow a^{\varphi(n)} \equiv 1 \bmod n$ Euler.

Θεώρημα Fermat Έστω p: πρώτος και a ακέραιος τέτοιος ώστε $p \nmid a$, τότε $\boxed{a^{p-1} \equiv 1 \bmod p}$

$n = p$ πρώτος

$(p \nmid a) \Rightarrow \mu\kappa\delta(a,p) = 1$ η p (δεκτή, απορρίπτεται)

$\left.\begin{array}{l} \mu\kappa\delta(a,p)=1 \overset{\text{Euler}}{\Rightarrow} a^{\varphi(p)} \equiv 1 \bmod p \\ \varphi(p^1) = p^{1-1}(p-1) = 1(p-1) = p-1 \end{array}\right\} \Rightarrow a^{p-1} \equiv 1 \bmod p$

Παράδειγμα: Βρείτε το υπόλοιπο της διαίρεσης του 1613^{665} με το 7

Λύση $1613^{665} \equiv (7 \cdot 230 + 3)^{665} \bmod 7$

$\equiv 3^{665} \bmod 7$

Fermat: $\mu\kappa\delta(3,7) = 1$

$3^6 \equiv 1 \bmod 7 \Rightarrow (3^6)^k \equiv 1^k \bmod 7 \Rightarrow 3^{6k} \equiv 1 \bmod 7$

$\equiv 3^{660+5} \bmod 7$

$\equiv 3^{660} \cdot 3^5 \bmod 7$

$\equiv 3^{6 \cdot 110} \cdot 3^5 \bmod 7$

$\equiv (3^6)^{110} \cdot 3^5 \bmod 7$

$\equiv 1^{110} \cdot 3^5 \bmod 7$

$\equiv 3^5 \bmod 7$

$\equiv 33333 \bmod 7$

$\equiv 9 \cdot 9 \cdot 3 \bmod 7$

$\equiv 2 \cdot 2 \cdot 3 \bmod 7$

$\equiv 12 \bmod 7$

$\equiv 5 \bmod 7$

Επομένως, τα 1613^{665} και 5 αφήνουν το ίδιο υπόλοιπο αν διαιρεθούν με το 7.

Άρα, το υπόλοιπο είναι 5.

Θεώρημα Έστω a ακέραιος και p πρώτος, τότε $a^p \equiv a \bmod p$

Απόδειξη $\mu\kappa\delta(a,p)=1$ ή $\mu\kappa\delta(a,p)=p$

1η περίπτωση: $\mu\kappa\delta(a,p)=1 \overset{\text{Fermat}}{\Rightarrow} a^{p-1} \equiv 1 \bmod p \Rightarrow$
$\Rightarrow p \mid a^{p-1}-1 \Rightarrow p \mid a(a^{p-1}-1) \Rightarrow p \mid a^p - a \Rightarrow a^p \equiv a \bmod p$

2η περίπτωση: $\mu\kappa\delta(a,p)=p \Rightarrow p \mid a \Rightarrow p \mid a-0 \Rightarrow a \equiv 0 \bmod p$
$a^p \equiv 0^p \bmod p \Leftrightarrow a^p \equiv 0 \bmod p \Leftrightarrow a^p \equiv a \bmod p$

Άσκηση Αν p περιττός πρώτος, τότε
α) $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \bmod p$ και
β) $1^p + 2^p + \dots + (p-1)^p \equiv 0 \bmod p$

Λύση

α) $1^{p-1} + 2^{p-1} + \dots + (p-1)^{p-1} \equiv 1+1+1\dots+1 \bmod p \equiv p-1 \bmod p \equiv -1 \bmod p$

(α) → Fermat: $\left.\begin{matrix}1 \le i \le p-1 \\ \mu\kappa\delta(i,p)=1\end{matrix}\right\} \Rightarrow i^{p-1} \equiv 1 \bmod p$

β) $1^p + 2^p + \dots + (p-1)^p \equiv 1 + 2 + \dots + (p-1) \bmod p$

$\equiv \dfrac{(p-1)(p-1+1)}{2} \bmod p$ ($\frac{p-1}{2}$ είναι ακέραιος → άρτιος καθώς το p είναι περιττός)

$\equiv \dfrac{(p-1)p}{2} \bmod p$

$\equiv \left(\dfrac{p-1}{2}\right) p \bmod p$

$\equiv 0 \bmod p$

Άσκηση Αν p άρτιος πρώτος, τότε
$29^{11} + 11^{2018} + 2018^{29} \equiv 0 \bmod p$
$11^{29} + 2018^{11} + 29^{2018} \equiv 0 \bmod p$
$29^{1071} + 11^{1204} + 2018^{1453} \equiv 0 \bmod p$

Λύση Μοναδικός άρτιος πρώτος είναι το 2 $\Rightarrow$ Άρα $p=2$

$29^{11} + 11^{2018} + 2018^{29} \equiv 1^{11} + 1^{2018} + 0^{29} \bmod 2 \equiv 0 \bmod 2$

$11^{29} + 2018^{11} + 29^{2018} \equiv 1^{29} + 0^{11} + 1^{2018} \bmod 2 \equiv 0 \bmod 2$

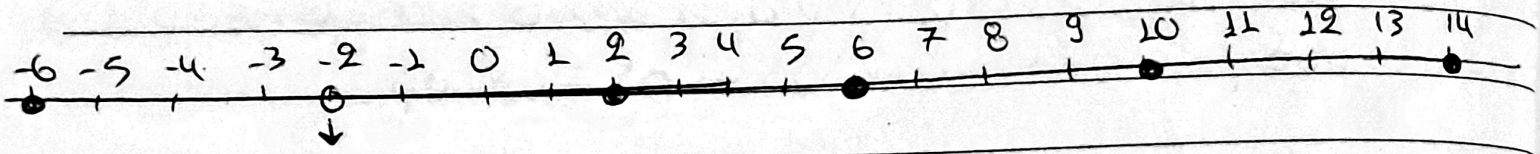
$29^{1071} + 11^{1204} + 2018^{1453} \equiv 1^{1071} + 1^{1204} + 0^{1453} \bmod 2 \equiv 0 \bmod 2$

- $ax \equiv b \pmod n$

$3x \equiv 5 \bmod 7$

$11x \equiv 3 \bmod 23$

$17x \equiv -4 \bmod 5$



$2 \bmod 4$ în $2 \bmod 8$ și $6 \bmod 8$

$x \equiv 2 \bmod 4$ în $2 \bmod 12$ și $6 \bmod 12$ și $10 \bmod 12$