19.11.2018

$a \equiv b \bmod n \iff n \mid a-b$

$a \equiv b \bmod n \iff$ Αν διαιρεθούν τα a, b με το n αφήνουν το ίδιο υπόλοιπο.

Παραδείγματα $13 = 1 \bmod 6$

$-3 = 4 \bmod 7$

Θεώρημα Έστω n φυσικός αριθμός και a, b, γ, δ ακέραιοι. Τότε:

(i) Αν $a \equiv b \bmod n$ και $\gamma \equiv \delta \bmod n$, τότε

$a+\gamma = b+\delta \bmod n$ και $a\gamma = b\delta \bmod n$

(ii) Αν $a \equiv b \bmod n$, τότε:

$a+\gamma = b+\gamma \bmod n$ και $a\gamma \equiv b\gamma \bmod n$

(iii) Αν $a \equiv b \bmod n$, τότε

$a^k \equiv b^k \bmod n$

(iv) Αν $f(x) = \gamma_0 + \gamma_1 x + \gamma_2 x^2 + \dots + \gamma_n x^m$, είναι πολυώνυμο με ακέραιους συντελεστές. Τότε αν:

$a \equiv b \bmod n \iff f(a) \equiv f(b) \bmod n$

Απόδειξη (i) $\Rightarrow$ (ii)

$a \equiv b \bmod n$
$\gamma \equiv \gamma \bmod n$
$\Big| \overset{(i)}{\Rightarrow}$ $a+\gamma \equiv b+\gamma \bmod n$
$a\gamma \equiv b\gamma \bmod n$

η σχέση ισοτιμίας είναι σχέση ισοδυναμίας

(iii) $a \equiv b \bmod n$ και $a \equiv b \bmod n \Rightarrow a \cdot a = b \cdot b \bmod n \Rightarrow$

$\Rightarrow a^2 \equiv b^2 \bmod n$

$a \equiv b \bmod n$ και $a^2 \equiv b^2 \bmod n \overset{(i)}{\Rightarrow} a \cdot a^2 \equiv b \cdot b^2 \bmod n \Rightarrow$

$\Rightarrow a^3 \equiv b^3 \bmod n$

Με τον ίδιο τρόπο επαγωγικά: $a^k \equiv b^k \bmod n$

(iv) $a \equiv b \bmod n$

$\overset{(ii)}{\Rightarrow} \gamma_1 a \equiv \gamma_1 b \bmod n$

$\overset{(iii)}{\Rightarrow} a^2 \equiv b^2 \bmod n$

$\overset{(ii)}{\Rightarrow} \gamma_2 a^2 \equiv \gamma_2 b^2 \bmod n$

$\overset{(i)}{\Rightarrow} a^m \equiv b^m \bmod n$

$\overset{(ii)}{\Rightarrow} \gamma_m a^m \equiv \gamma_m b^m \bmod n$

$\gamma_0 \equiv \gamma_0 \bmod n$

$\overset{(i)}{\Rightarrow} (+)$

Ιδ: $f_0+f_1a+f_2a^2+\dots+f_m a^m \equiv f_0+f_1b+f_2b^2+\dots+f_m b^m \bmod n$

$\Rightarrow f(a) = f(b) \bmod n$

Άσκηση Βρείτε το υπόλοιπο της διαίρεσης του 41^{2017} με το 7

$f(x) = x^{2017}$

$41^{2017} \equiv 48^{2017} \bmod 7$ (είναι χειρότερα)

$41^{2017} \equiv 34^{2017} \bmod 7$

(μπορώ να αφαιρώ 7 κάθε φορά)

$41^{2017} \equiv 6^{2017} \bmod 7$ (αφαιρώ 7)

$41^{2017} \equiv (-1)^{2017} \bmod 7$

$= (-1)$

$45^{2019} \equiv 3^{2019} \bmod 7$

$\equiv (-4)^{2019} \bmod 7$

Το (-1) δεν είναι πιθανό υπόλοιπο. Το ισοδύναμο του (-1) είναι το 6. Άρα, το υπόλοιπο του 41^{2017} και του 6 διαιρούμενα με το 7 είναι το ίδιο, το 6. Άρα, το υπόλοιπο της διαίρεσης του 41^{2017} με το 7 είναι το 6.

Άσκηση Βρείτε το υπόλοιπο της διαίρεσης του $a = 1! + 2! + 3! + \dots + 2018!$ με το 12. $(a \equiv (\ ) \bmod n)$

$1! \equiv 1 \bmod 12$

$2! \equiv 1 \cdot 2 \bmod 12 \Rightarrow 2! \equiv 2 \bmod 12$

$3! \equiv 1 \cdot 2 \cdot 3 \bmod 12 \Rightarrow 3! \equiv 6 \bmod 12$

$4! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \bmod 12 \Rightarrow 4! \equiv 24 \bmod 12 \Rightarrow 4! \equiv 0 \bmod 12$

$5! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \bmod 12 \Rightarrow 5! \equiv 0 \cdot 5 \bmod 12 \Rightarrow 5! \equiv 0 \bmod 12$

$5 \le k \le 2018 \equiv 0$

$k! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot \dots \cdot k \bmod 12 \Rightarrow k! \equiv 0 \cdot 5 \dots k \bmod 12 \Rightarrow$

$\Rightarrow k! \equiv 0 \bmod 12$

$a \equiv 1 + 2 + 6 + 0 + 0 + 0 \dots + 0 \bmod 12$

$a \equiv 9 \bmod 12$. Άρα, αν το a και το 9 διαιρεθούν με το 12, αφήνουν το ίδιο υπόλοιπο. Όμως, το υπόλοιπο της διαίρεσης του 9 με το 12 είναι 9 (αφού $9 = 0 \cdot 12 + 9$). Άρα το a αφήνει υπόλοιπο 9 αν διαιρεθεί με το 12.

Άσκηση Βρείτε το υπόλοιπο της διαίρεσης του
$a = 1^5 + 2^5 + 3^5 + \ldots + 100^5$ με το 4. ($a \equiv (\ ) \bmod 4$)

$1^5+2^5+3^5+4^5+5^5+6^5+7^5+8^5+\ldots+97^5+98^5+99^5+100^5 \equiv (\ ) \bmod 4$
$\equiv 1^5+0+(-1)^5+0+1^5+2^5+3^5+4^5+1^5+2^5+3^5+4^5 \equiv 0 \bmod 4$

Φυλλάδιο #4
Άσκηση 4 Δείξτε ότι $\mu\kappa\delta(9m+2, 9m+4) = 1$
Έστω $d = \mu\kappa\delta(9m+2, 9m+4)$
$d \mid 9m+2$ $\quad d \mid \boxed{-9}(9m+2) + \boxed{2}(9m+4) = -18m-9+18m+8$
$d \mid 9m+4$ $\quad = -1$
$d \mid -1 \Rightarrow d \mid 1 \Rightarrow d = 1$

Φυλλάδιο #4
Άσκηση 5 Δείξτε ότι $\mu\kappa\delta(6m+1, 6m+5) = 1$
Έστω $d = \mu\kappa\delta(6m+1, 6m+5)$
$d \mid 6m+1$ $\quad d \mid \boxed{-1}(6m+1) + \boxed{1}(6m+5)$
$d \mid 6m+5$
$d \mid -1+5 = 4 \Rightarrow d = 1$ ή $d = 2$ ή $d = 4$
Έστω $d = 2$
$d = 2 \mid \underbrace{6m+1}_{\text{περιττός}} \Rightarrow 2 \mid \boxed{1}(6m+1) + \boxed{-3}2m$
$= 6m+1-6m = 1 \Rightarrow 2 \mid 1$ άτοπο!

Έστω $d = 4$
$d = 4 \mid 6m+1 \Rightarrow 2 \mid 6m+1 \Rightarrow 2 \mid 1$

Άρα έχουμε άτοπο για τις περιπτώσεις όπου $d = 2$ και $d = 4$
Συνεπώς, προκύπτει ότι $d = 1$

Άσκηση Έστω ότι μκδ(α,β) = 1. Δείξτε ότι μκδ(α−β^17, α^3β^2) = 1

Έστω d = μκδ(α−β^17, α^3β^2)

Έστω d > 1. Τότε υπάρχει p: πρώτος τέτοιος ώστε p|d

p|d|α−β^17 ⇒ p|α−β^17 ⇒ p|α^3 ή p|β^3
p|d|α^3β^2 p|α^3β^2 ↓

p: πρώτος p|α·α·α ή p|β·β
p|α ή p|β

1η περίπτωση: p|α

p|α−β^17 ⇒ p|1·α + (−1)(α−β^17) ⇒

⇒ p|β^17 = β·β·...·β ⇒ p|β ⇒ p: κοινός διαιρέτης των α, β
(17 φορές)

⇒ p διαιρεί το μκδ(α,β) = 1 ⇒

p: πρώτος ⇒ άτοπο!

2η περίπτωση: p|β

p|α−β^17 ⇒ p|β^17·β + 1(α−β^17) ⇒ p|α

Άρα p|β, p|α } p: κοινός διαιρέτης, άρα p|μκδ(α,β) = 1 άτοπο!

Άρα d = 1

μκδ(α−β^17, α^3β^2) = 1
α = 2 β = 3
Οποιοιδήποτε δύο αριθμοί που είναι πρώτοι μεταξύ τους.

Φυλλάδιο #5

Άσκηση 4 Δείξτε ότι αν p·β = α^2, τότε p|β

p: πρώτος, α, β φυσικοί

p|β = α^2 ⇒ p|α^2 ⇒ p|α·α ⇒ p|α ⇒ α = pκ

p: πρώτος β = α^2 ⇒ (pκ)^2 = p^2κ^2

β = pκ^2 ⇒

⇒ p|β

Φυλλάδιο #5

Άσκηση 8 Να περιγραφούν όλοι οι φυσικοί αριθμοί που έχουν ακριβώς α) δύο φυσικούς διαιρέτες

β) τρεις -11- -11-

γ) τέσσερις -11- -11-

(α) Είναι οι πρώτοι αριθμοί

(β) Έστω n φυσικός αριθμός που έχει ακριβώς 3 φυσικούς διαιρέτες.

$n>1 \Rightarrow p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$

$\tau(n) = 3 \Rightarrow (a_1+1)(a_2+1)\dots(a_s+1) = 3, \quad a_i+1 > 1$

$a_1+1 = 3 \Rightarrow a_1 = 2$

$a_2+1 = 1$ $\Rightarrow n = p_1^2$

$a_3+1 = 1$

$\vdots$

$a_s+1 = 1$

Άρα οι φυσικοί άρτιοι που έχουν ακριβώς τρεις φυσικούς διαιρέτες είναι τετράγωνα πρώτων αριθμών, $p = n^2$