17/01/2017

Αριθμητικές Συναρτήσεις

$F : \mathbb{N} \to K$ αριθμητική, εαν

$f(m,n) = f(m) \cdot f(n)$ όταν $(m,n) = 1$

Π.χ. ϕ Euler
σ άθροισμα των Διαιρετών
μ Möbius

Να ξέρω να εφαρμόζω τον τύπο!

f αριθμητική $\Rightarrow F(n) = \sum_{d|n} f(d)$ αριθμ.

$F(n) = \sum_{d|n} f(d) \xrightarrow[\text{αντιστροφής}]{\text{Τύπος}}$

$$f(n) = \sum_{d|n} \mu(d) \, F\left(\frac{n}{d}\right)$$

Π.χ.

$$\sigma(n) = \sum_{d|n} d \iff n = \sum_{d|n} \mu(d) \, \sigma\left(\frac{n}{d}\right)$$

ταυτοτική

~~Τέλειοι Αριθμοί!~~

~~Ευκλείδης: ο φυσικός σ(n)=2n~~

ΤΕΛΕΙΟΙ ΑΡΙΘΜΟΙ

Ευκλείδης : n φυσικό $\sigma(n)=2n$;;

$\sigma(1)=1<2\cdot 1$

$\sigma(2)=1+2<2\cdot 2$

$\sigma(3)=1+3<2\cdot 3$

$\sigma(4)=1+2+4<2\cdot 4$

$\sigma(5)=1+5<2\cdot 5$

$\sigma(6)=1+2+3+6=2\cdot 6$ $\boxed{6}$ τέλειος

$\sigma(p)=1+p<2p$

$\sigma(8)=1+2+4+8<2\cdot 8$

$\sigma(10)=1+2+5+10<2\cdot 10$

$\sigma(12)=1+2+3+4+6+12>2\cdot 12$

$\sigma(28)=2\cdot 28$

$\sigma(496)=2\cdot 496$

$\sigma(8.128)=2\cdot 8128$

$\sigma(33550336)$

Οι πέντε πρώτοι τέλειοι είναι άρτιοι.

Υπάρχουν περιττοί; Δεν ξέρουμε

$2^{\alpha}-1$ πρώτος $\Rightarrow$ α πρώτος

$(2^{10}-1)=(2^5)^2-1=(2^5-1)(2^5+1)$

Θεώρημα

Εάν ο φυσικός $2^{n+1}-1$ είναι πρώτος (τότε $n+1$ = πρώτος), τότε ο φυσικός $2^n(2^{n+1}-1)$ είναι τέλειος και καλείται τέλειος του Ευκλείδη. Ο Gauss απέδειξε και το αντίστροφο.

"$\Rightarrow$" $2^{n+1}-1=p$ πρώτος

$\sigma(2^{n+1}-1)=1+(2^{n+1}-1)=2^{n+1}$

$\sigma(2^n)=2^0+2^1+2^2+\ldots+2^n=$
$=1+2+\ldots+2^n$

$\sigma\left(2^n(2^{n+1}-1)\right)=\sigma(2^n)\,\sigma(2^{n+1}-1)=(1+2+\ldots+2^n)(2^{n+1}$ (+)

Θέλουμε $\sigma(2^n(2^{n+1}-1))=2\cdot 2^n(2^{n+1}-1)=2^{n+1}(2^{n+1}-1)=$

$2^{n+1}-1=(2-1)(2^n+2^{n-1}+\ldots+1)=2^n+2^{n-1}+\ldots+1$

$=2^{n+1}(2^n+2^{n-1}+\ldots+1)$ (++)

Άρα, (+) = (++)

Έστω p πρώτος. Αν ο $2^n p$ είναι τέλειος, τότε
$p=2^{n+1}-1$

$2^n p$ πρώτος $\Leftrightarrow$ $\sigma(2^n p)=2\cdot 2^n\cdot p=2^{n+1}\cdot p$ (+)

$p>2$ περιττός

$\sigma(2^n)\sigma(p)=(1+2+\ldots+2^n)(1+p)$ (++)

(+) και (++) $2^{n+1}\cdot p=\underbrace{(1+2+\ldots+2^n)}_{2^{n+1}-1}(1+p)$

$2^{n+1}\cdot p=2^{n+1}-1+2^{n+1}\cdot p-p \Rightarrow p=2^{n+1}-1.$

Ερωτήματα

α) Υπάρχουν φυσικοί n με $\sigma(n) < 2n$;
Ναι, και είναι άπειροι

β) Υπάρχουν φυσικοί n με $\sigma(n) > 2n$;
Ναι, και είναι άπειροι
Για $n = 2^k \cdot 3$ ισχύει

γ) Υπάρχουν φυσικοί n με $\sigma(n) = 2n$;
Ναι, και είναι άπειροι σύμφωνα με τον Ευκλείδη

δ) Υπάρχει τέλειος περιττός;
Δεν γνωρίζουμε

1908	Αν ο n	τέλειος	περιττός	$n > 2 \cdot 10^6$
1955	"	"	"	$n > 10^{20}$
1973	"	"	"	$n > 10^{50}$
Σήμερα,	"	"	"	$n > 10^{100}$

ε) Υπάρχουν άπειροι πρώτοι τύπου Mersenne $2^p - 1$;
Κανείς δεν ξέρει.

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ
ΤΜΗΜΑ Α
ΕΠΑΝΑΛΗΠΤΙΚΕΣ ΑΣΚΗΣΕΙΣ

1) Να λυθεί το σύστημα $2x \equiv 10 \bmod 12$
$4x \equiv 12 \bmod 20$

2) Να λυθεί το σύστημα $x \equiv 3 \bmod 7$ $\quad 2x \equiv 6 \bmod 7$
$x \equiv 9 \bmod 11$ $\quad 5x \equiv 1 \bmod 11$
$x \equiv 5 \bmod 13$ $\quad x \equiv 5 \bmod 13$

$x = 3\cdot 5 \frac{M}{7} + 9\cdot 4 \frac{M}{11} + 5\cdot 12 \frac{M}{13} \bmod M$

3) Να λυθούν οι εξισώσεις α) $x^2 \equiv 23 \bmod 11^2$
β) $3x^2 + 6x \equiv 66 \bmod 11^2$

4) Αν το γινόμενο δύο πρώτων είναι $n = 1147$ και $\varphi(1147) = 1080$,

να βρεθούν οι πρώτοι

5) Να λυθεί η εξίσωση $x^{25} \equiv 3 \bmod 37$

6) Να βρεθούν n ώστε $3^{6n} + 3^n + 2 \equiv 0 \bmod 7$

7) Έχει λύση η $x^2 \equiv -1 \bmod 19$;
Βρείτε τις λύσεις της $x^4 \equiv 1 \bmod 19$

8) Να βρεθεί η τάξη του 3 στο mod 11 και mod 22
Βρείτε τις δυνάμεις του 6 στο mod 15 και του 3

9) Να γράψετε το 320 στη δυαδική και δεκαδική αναπαράσταση

10) Να δείξετε ότι αν το 7 διαιρεί το $2m+n$, τότε διαιρεί και το $10m+n$.

β) $5 \mid 3\cdot 7^n + 2\cdot 2^n$ για $n \geq 0$ $\qquad$ δ) $10 \nmid (n-1)! + 1$ για $n \geq 1$

γ) $15 \mid 3n^5 + 5n^3 + 7n$ για $n \geq 1$

11) Να βρεθούν ακέραιοι α και β με $a6 + \beta 14 = 2$. Πόσα ζευγάρια υπάρχουν;

Επαναληπτικές Ασκήσεις

17/01/2017

Άσκηση 1

$2x \equiv 10 \bmod 12$
$4x \equiv 12 \bmod 20$

$2x \equiv 10 \bmod 12 \Rightarrow$ $(2,12)=2 \mid 10 \Rightarrow$ έχει λύση όχι μονή
$x \equiv 5 \bmod 6$ Λύσεις: 5,
$5+\frac{12}{2} = 11 \bmod 12$

Τέσσερα συστήματα: Πιθανόν να μην είναι όλα συμβιβαστά (να μην έχουν λύση)

Λύνουμε αυτά για τα οποία υπάρχουν

$x \equiv 5 \bmod 12$ $\Leftrightarrow$ $x \equiv 5+12k$ $\Rightarrow$ να βρούμε το k
$x \equiv 3 \bmod 20$ $\quad 5+12k \equiv 3 \bmod 20$
$5+12k = 3+20\lambda$.

Άσκηση 2 : Κινέζικο Θεώρημα

Άσκηση 3

a) $x^2 \equiv 23 \bmod 11$

$x^2 \equiv 23 \bmod 11 \equiv 1 \bmod 11^2 \Rightarrow x \equiv \pm 1 \bmod 11$

$(1+11k)^2 \equiv 23 \bmod 11^2$
$1 + 2 \cdot 11k + \cancel{11^2 k^2} \equiv 23 \bmod 11^2$
$2 \cdot 11k \equiv 22 \bmod 11^2$
$11k \equiv 11 \bmod 11^2 \Rightarrow k \equiv 1 \bmod 11^2$

$x \equiv (1+1\cdot 11) \bmod 11^2$
$x \equiv 12 \bmod 11^2$
$\left(\begin{matrix} 12^2 = 144 \bmod 121 \\ 23 \end{matrix} \right) \rightarrow$ Επαλήθευση

Αν $x^2 \equiv 23 \bmod 3 \cdot 11^2$
$(3,11)=1 \rightarrow x^2 \equiv 23 \bmod 3 \Rightarrow x^2 \equiv 2 \bmod 3$ Δεν έχει λύση
$\rightarrow x^2 \equiv 23 \bmod 11^2 \Rightarrow x \equiv 12 \bmod 11^2$

Έστω $\left. \begin{matrix} x \equiv 2 \bmod 3 \\ x \equiv 12 \bmod 11^2 \end{matrix} \right\}$ τότε λύνω με Κινέζικο Θεώρημα β) $3x^2 + 6x \equiv 66 \bmod 11^2$

$x^2 + 2x \equiv 22 \bmod 11^2$

$x^2 + 2x + 1 \equiv (22+1) \bmod 11^2$

$(x+1)^2 \equiv 23 \bmod 11^2$

$y^2 \equiv 23 \bmod 11^2$

Από το προηγούμενο

Άσκηση 4

p, q $\quad pq = 1147$

$\varphi(1147) = 1080 = (p-1)(q-1) \Rightarrow \overbrace{pq}^{1147} - q - p + 1 = 1080$

$p + q = 68$

$pq = 1147$ $\quad$ Με τριώνυμο $\Rightarrow$ $p = 31$, $q = 37$

Άσκηση 5

$x^{35} \equiv 3 \bmod 37$

37 πρώτος $\Rightarrow \varphi(37) = 36$

$x \cdot x^{35} \equiv 3x \bmod 37 \Rightarrow 3x \equiv 1 \bmod 37$

$12 \cdot 3x \equiv 12 \bmod 37 \Rightarrow x \equiv -12 \bmod 37$

Άσκηση 6

$3^{6n} + 3^n + 2 \equiv 0 \bmod 7$

$(3^{\varphi(7)})^n + 3^n + 2 \equiv 0 \bmod 7$

$1 + 3^n + 2 \equiv 0 \bmod 7$ $\quad$ $3, 3^2 \equiv 2, 3^3 = 27 \equiv 6$

$3^n \equiv -3 \bmod 7$

$3^{n-1} \equiv -1 \bmod 7$

$3^{n-1} \equiv 6 \bmod 7 \equiv 3^3 \bmod 7 \Rightarrow n-1 \equiv 3 \bmod 6$

$\Rightarrow n \equiv 4 \bmod 6$

Άσκηση 7

$x^2 \equiv -1 \bmod 19$
$\equiv 18 \bmod 19$

Δεν έχει λύση

1	
2	4
3	9
4	16
5	6
6	-2
7	11
8	7
9	5
10	5

$x^4 \equiv 1 \bmod 19$
$(x^2)^2 \equiv 1 \bmod 19$
$x^2 \equiv 1 \bmod 19$ → $x \equiv 1$, $x \equiv -1$

$\cancel{x^2 \equiv -1 \bmod 19}$

Άσκηση 8

Τάξη του $3 \bmod 11$

$3, \ 9 \equiv -2, \ -6, \ 7, \ -1 \Rightarrow ord_{11}(3) = \varphi(11) = 10$
1 2 3 4 5

Τάξη του $3 \bmod 22$

$3, \ 9, \ 27 \equiv 5, \ 15 \equiv -7, \ -21 \equiv 1$
1 2 3 4 5

$ord_{22}(3) = 5$

$6 \bmod 15$ $\quad 36 \equiv 6$
Δεν έχει τάξη
Έχει 1 δυνάμη

$3 \bmod 15$ $\quad 9, \ 27 \equiv -3, \ -9, \ 3$
Δεν έχει τάξη, Έχει 4 δυνάμεις

Άσκηση 9

$310 \to 3\cdot 10^2 + 1\cdot 10 + 0\cdot 10^0$

$(3,1,0)_{10}$

$310 \,|\, 256 = 2^8$, $54 \,|\, 1$; $54 \,|\, 32 = 2^5$, $22 \,|\, 1$; $22 \,|\, 16 = 2^4$, $6 \,|\, 1$; $6 \,|\, 4 = 2^2$, $2 \,|\, 1$; $2 \,|\, 2$, $0 \,|\, 1$

$310 = 1\cdot 2^8 + 1\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^2 + 1\cdot 2$

Άρα, $(1,0,0,1,1,0,1,1,0)_2$

Άσκηση 10

α) Αν $7 / 2m+n$ τότε $7 / 100m+n$

$7 / 2m+n \Rightarrow 7 / 50(2m+n) = 100m + 50n$

$7 / 100m + 50n - 49n \Rightarrow 7 / 100m + n$

β) $5 / 3\cdot 7^n + 2\cdot 2^n$ για $n \geq 0$

α' τρόπος Αρκεί $3\cdot 7^n + 2\cdot 2^n \equiv 0 \bmod 5$

$3\cdot 7^n \bmod 5 + 2\cdot 2^n \bmod 5$

$\equiv$

$3\cdot 2^n \bmod 5 + 2\cdot 2^n \bmod 5 \equiv 5\cdot 2^n \bmod 5 \equiv 0$

β' τρόπος: Με επαγωγή: $n=0$, $n=1$ $3+2=5$ ισχύει

$3\cdot 7 + 2\cdot 2 = 25$ ισχύει

Θέλαμε $3\cdot 7^{k+1} + 2\cdot 2^{k+1} = 3\cdot 7^k \cdot 7 + 2\cdot 2^k \cdot 2 =$

$= 21\cdot 7^k + 4\cdot 2^k$

$= (3+3+15)\cdot 7^k + 2\cdot 2^k + 2\cdot 2^k$

$= \underbrace{3\cdot 7^k + 2\cdot 2^k} + \underbrace{3\cdot 7^k + 2\cdot 2^k} + 15\cdot 7^k = 5\lambda$