16/12/15

Τετραγωνικά Υπόλοιπα

$ax \equiv b \bmod p$

$ax^2 \equiv b \bmod p$, p = πρώτος

$(a,p)=1 \Rightarrow \nexists\ a^{-1} \Rightarrow a^{-1} \cdot a \cdot x^2 \equiv a^{-1} b \bmod p$

$\boxed{x^2 \equiv c \bmod p}$

π.χ $Z_5 = \{[0], [1], [2], [3], [4]\} \rightsquigarrow \{0, 1, 4\}$

Παρατηρούμε ότι

$1 \equiv 1 \bmod 5$

$4 = 2 \cdot 2 \bmod 5$

Άρα $3 \neq x^2 \bmod 5$

1 και 4 είναι Τ.Υ

2 και 3 είναι Τ.Μ.Υ

$x^2 \equiv 2 \bmod 5$ δεν έχει λύση

Παρατήρηση:

Αν a είναι λύση της $x^2 \equiv c \bmod p$, τότε και $p-a$ είναι επίσης λύση

Λύσεις: Ζεύγαρια ή Καμία

Θεώρημα (Euler)

- Αν $(a,p)=1$ τότε ο a είναι Τ.Υ. $\bmod p$ αν $a^{\frac{p-1}{2}} \equiv 1 \bmod p$
- Ο a είναι Τ.Μ.Υ αν $a^{\frac{p-1}{2}} \neq 1 \bmod p$

Π.χ Εξετάστε αν έχει λύση η $x^2 \equiv 5 \bmod 19$ ⊕

$\{0,1,2 \dots 18\} = Z_{19} \xrightarrow{\text{Τετράγωνα}} \{0,1,4 \dots\}$

Αν 5 ∈ "Τετράγωνα" τότε είναι Τ.Υ και η ⊕ έχει λύση.

Να ελέγξουμε αν $5^{\frac{p-1}{2}} \equiv 1 \bmod p$
Δηλαδή $5^{\frac{19-1}{2}} \equiv 1 \bmod 19$;;;

$5^9 \equiv 1 \bmod 19$ (το δείξαμε)
Άρα η ⊕ έχει λύση. Ποια είναι η λύση;

$p = 19 = 4 \cdot 4 + 3$

$(5^4)^2 = 5^8$ ή $5^5 = 5^{4+1}$

$(5^5)^2 = 5^{10} = 5^9 \cdot 5 \equiv 1 \cdot 5 \bmod 19$
Άρα μια λύση είναι η $5^5 \bmod 19$

Πρόταση: Έστω ότι ο p γράφεται $p = 4k+3$ και ισχύει ότι $a^{\frac{p-1}{2}} = a^{2k+1} \equiv 1 \bmod p$, τότε το $a^{k+1} \bmod p$ αποτελεί λύση της $x^2 \equiv a \bmod p$

Π.χ. $x^2+2x+15 \equiv 0 \bmod 19$

$x^2+2x+1^2-1^2+15 \equiv 0 \bmod 19$

$(x+1)^2+14 \equiv 0 \bmod 19$

$(x+1)^2 \equiv -14 \bmod 19$

$(x+1)^2 \equiv 5 \bmod 19$

Άρα $x+1 \equiv 5^5 \bmod 19$

$x+1 \equiv (19-5^5) \bmod 19$

ΠΡΟΤΑΣΗ: Έστω p πρώτος και α ακέραιος με $(\alpha,p)=1$. Αν η εξίσωση $x^2 \equiv \alpha \bmod p$ έχει λύση, τότε η εξίσωση $x^2 \equiv \alpha \bmod p^2$ έχει επίσης λύση.

Χωρίς απόδειξη!

ΕΡΩΤΗΜΑ: ΠΩΣ ΘΑ ΒΡΕΘΕΙ Η ΛΥΣΗ?!

Π.χ. Να λυθεί η $x^2 \equiv 15 \bmod 7^2$

Εξετάζουμε αν η $x^2 \equiv 15 \bmod 7$ έχει λύση

$x^2 \equiv 15 \bmod 7 \Rightarrow x^2 \equiv 1 \bmod 7$

$x \equiv 1, 7-1=6$

Ξεκινάμε με τον $x \equiv 1 \bmod 7$. Δοκιμάζουμε το $(1+7k)^2 \equiv 15 \bmod 7^2$. Να βρεθεί το k;;;

$1+2\cdot 7k+7^2 \cdot k^2 \equiv 15 \bmod 7^2$

$2 \cdot 7k \equiv 14 \bmod 7^2 \Rightarrow$

$2k \equiv 2 \bmod 7 \Rightarrow k=1$

Άρα μία λύση του αρχικού είναι $1+7 \cdot 1 = 8 \bmod 7^2$

$8^2 \equiv 15 \bmod 7^2$

$64 \equiv 15 \bmod 49$.

Η άλλη λύση θα βρεθεί με τον ίδιο τρόπο χρησιμοποιώντας τη δεύτερη λύση των αρχικών

ΑΡΙΘΜΗΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

$f: Z^* \to C$ συνάρτηση

Π.χ. α) $f(n)=n$ ταυτοτική

β) $f(n)=n^k$ $k \in \mathbb{N}$

γ) $f(n)=e^{in}$

Μας ενδιαφέρουν αυτές που έχουν τις εξής ιδιότητες.

Αν $(n,k)=1$, τότε $f(nk)=f(n)\cdot f(k)$. Σε αυτήν την περίπτωση η f καλείται πολλαπλασιαστική.

Αν ισχύει $f(nk)=f(n)\cdot f(k)$ για όλα τα n και k, τότε καλείται ολικά πολ/κή.

Π.χ. α) $g: \mathbb{N}^* \to \mathbb{C}$ με $g(1)=1$ και $g(n)=0$ αν $n>1$

Για τυχαίο $m \in \mathbb{N}^*$ ισχύει ότι $m=1$ ή $m>1$

$g'(1)=g(1\cdot 1)=1=1\cdot 1=g(1)\cdot g(1)$

$m>1$ $g(m)=0$

Αν $m=m_1 m_2 \Rightarrow m_1$ ή $m_2 > 1$

Για $m_1>1 \Rightarrow g(m_1)=0$ και $g(m)=g(m_1\cdot m_2)=$

$g(m_1)\cdot g(m_2)=0\cdot g(m_2)=0$ ολικά πολ/κή

β) $f: \mathbb{N}^* \to \mathbb{C}$ με $f(n)=n$ ολικά πολ/κή

γ) Η συνάρτηση του Euler $\varphi: \mathbb{N}^* \to \mathbb{N} \subseteq \mathbb{C}$ με τύπο $\varphi(n)=$ το πλήθος των φυσικών μικρότερων ή ίσων του n και πρώτων με το n.

$\varphi(p^k)=p^{k-1}\varphi(p)=p^{k-1}(p-1)$ και

$\varphi(p^k q^l)=p^{k-1}(p-1)\cdot q^{l-1}(q-1)=\varphi(p^k)\cdot\varphi(q^l)$

δ) $\sigma : \mathbb{N}^* \to \mathbb{N}$

$\sigma(n)$ = το άθροισμα των φυσικών διαιρετών του n

$$\sigma(n) = \sum_{d/n} d$$

τυπική

$$\sigma(12) = 1+2+3+4+6+12 = \sum_{d/12} d$$

Ο τύπος των Gauss

τυπική

$$n = \sum_{d/n} \varphi(d)$$ ← Euler

Θεώρημα: Εάν η $f : \mathbb{N}^* \to \mathbb{C}$ είναι πολ/κη και η $F : \mathbb{N}^* \to \mathbb{C}$ ορίζεται από τον τύπο

$F(n) = \sum_{d/n} f(d)$, τότε και η F είναι πολ/κη.

Απόδειξη

$n = 18$ 1, 2, 3, 6, 9, 18

$n = 36 = 2^2 \cdot 3^2$

1, 2, 3, 4, 6, 9, 12, 18, 36

2^2	1	2	4
3^2	1	3	9

Θέλουμε να δείξουμε ότι η F είναι πολ/κη.

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

$$F(n \cdot m) = \sum_{d/nm} f(d)$$

$$F(n) = \sum_{d_1/n} f(d_1)$$

$$F(m) = \sum_{d_2/m} f(d_2)$$

Αν $d \mid m \cdot n$ τότε θα γράφεται $d = d_1 \cdot d_2$ με $d_1 \mid m$ και $d_2 \mid n$. Θα δείξουμε ότι οι διαιρέτες του mn δίνονται από γινόμενα διαιρετών του n και m ανεξάρτητα και από μία φορά.
Αν $d_1 \mid m$ και $d_2 \mid n \Rightarrow d_1 d_2 \mid mn$
$(d_1, d_2) = 1$ διότι $(m, n) = 1$

Αν $d = (m, n) \Rightarrow d = (d, mn) = (d, m)(d, n) = d_1 \cdot d_2$

Άρα $F(mn) = \sum_{d \mid mn} f(d) = \sum_{\substack{d = d_1 d_2 / mn \\ (d_1, d_2) = 1}} f(d) =$ πολ. $\sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) \cdot f(d_2) =$

$= \sum_{d_1 \mid m} \cdot \sum_{d_2 \mid n} f(d_1, d_2)$

$\sum_{d_1 \mid m} f(d_1) \cdot \sum_{d_2 \mid n} f(d_2) = F(m) \cdot F(n)$