Φυλλάδιο #6 16/12/2016

Άσκηση 3 : $n = 2k+1 \Rightarrow 2^n + 3^n \not\equiv 0 \mod 17$

Υποθέτουμε ότι $2^n \equiv (-3)^n \mod 17$ για κάποιο $n$

$(-3)^n \equiv (14)^n \mod 17$

$2^n \equiv 14^n \mod 17$

$2^n \equiv (2 \cdot 7)^n \mod 17$

$2^n \equiv 2^n \cdot 7^n \mod 17$

$(2,7) = 1$

$\left.\begin{array}{l} 7^n \equiv 1 \mod 17 \\ \varphi(17) = 16 \text{ άρτιος} \\ n \not\equiv 0 \mod 16 \\ \text{Euler} \end{array}\right\}$ $7^n \equiv 1 \mod 17$ Άτοπο

Άσκηση 4 : $p, q$ πρώτοι διαφορετικοί

$p, q$ περιττοί

$a \in \mathbb{Z}$ με $(a, pq) = 1$

$(a, p) = 1 = (a, q)$

$a^{\frac{\varphi(pq)}{2}} \equiv 1 \mod pq$

$\varphi(pq) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1) \geq 4$ $p, q$ περιττοί

$a^{\frac{\varphi(pq)}{2}} \mod p \equiv a^{\frac{(p-1)(q-1)}{2}} \mod p \equiv (a^{p-1})^{\frac{q-1}{2}} \mod p \equiv 1$ (+)

Το ίδιο

$a^{\frac{\varphi(pq)}{2}} \mod q \equiv 1$ (++)

$x - y = pk \Leftarrow x \equiv y \mod p$

$x - y = q\,l \Leftarrow x \equiv y \mod q$

$x \equiv y \mod pq$

(+) και (++) $\Rightarrow$ (*)

$p, q \mid x - y \Rightarrow \left.\begin{array}{l} q \mid pk \\ q \nmid p \end{array}\right\} \Rightarrow q \mid k$

$\rightarrow$

$x - y = pqk' \Leftrightarrow x \equiv y \mod pq$

⊛ Άρα $a^{\frac{\varphi(pq)}{2}} \equiv 1 \bmod pq$

Άσκηση 5

$3x \equiv 7 \bmod 17 \Rightarrow 6\cdot 3x \equiv 6\cdot 7 \bmod 17$

$3\cdot 6 \equiv 1 \bmod 17 \qquad x \equiv 8 \bmod 17$

Επαλήθευση $3\cdot 8 = 24 \equiv 7 \bmod 17$

$Ord_{17}(3) = \varphi(17) = 16$

$\exists k : 3^k \equiv 7 \bmod 17$

$3x \equiv 3^k \bmod 17$

$x \equiv 3^{k-1} \bmod 17$

Άσκηση 6

$5x \equiv 3 \bmod 7 \Rightarrow 3\cdot 5x \equiv 3\cdot 3 \bmod 7 \Rightarrow x \equiv 9 \bmod 7$

$4x \equiv 2 \bmod 5 \Rightarrow 4\cdot 4x \equiv 4\cdot 2 \bmod 5 \Rightarrow x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 3 \Rightarrow x \equiv 2 \bmod 3$

Κινέζος

Λύση $\bmod (7\cdot 5\cdot 3) = \bmod 105$

Άσκηση 7 : a) $n$;; $\in \mathbb{N}$

$\varphi(n) = \frac{1}{2} n$

$n = 2^k m \quad m$ περιττός

$\phi(n) = \varphi(2^k m) = \varphi(2^k)\cdot\varphi(m) = 2^{k-1}\cdot\varphi(m)$ (+)

$m =$ περιττός $\Rightarrow \exists\, p | m \Rightarrow p^r | m$ μέγιστος

Άρα $\varphi(m) = p^{r-1}(p-1)\varphi(m')$

$m = p^r \cdot m'$, $p$ ελάχιστος πρώτος

$p^r | m$ και $p^r \nmid \varphi(m)$

Άρα $\varphi(m) < m \overset{(+)}{\Rightarrow} \varphi(2^k)\cdot\varphi(m) = 2^{k-1}\cdot\varphi(m) = \frac{1}{2}\cdot 2^k m$ θέλαμε

Αλλά $\varphi(m) < m \quad$ Άρα $n = 2^k$

β) $\varphi(n)=\varphi(2n)$ Το κάναμε!

γ) $\varphi(n)=2n$

Αδύνατο από το α).

$x \equiv 2 \bmod 6$
$x \equiv 4 \bmod 20$
$x = 4 + 20k$

$4 + 20k \equiv 2 \bmod 6$
$2k \equiv -2 \bmod 6$
$2k \equiv 4 \bmod 6$
$k \equiv 2 \bmod 3$
$k = 2 + 3l$.

16/12/2016

Να λυθεί το σύστημα

$2x \equiv 4 \bmod 12 \Rightarrow 2x = 4 + 12k \Rightarrow x = 2 + 6k$
$2x \equiv 8 \bmod 20$

$x \equiv 2 \bmod 6$

Στο mod12 έχουμε 2 λύσεις
Αυτή που βρίσκαμε 2, $2 + \frac{12}{2} = \underline{8}$

$2x \equiv 4 \bmod 12$
$x \equiv 2 \bmod 12$ ή $x \equiv 8 \bmod 12$
$2x \equiv 8 \bmod 20 \Rightarrow x \equiv 4 \bmod 10$ λύσεις στο mod20
$4,\ 4 + 10 = 14$
$2x \equiv 8 \bmod 20 \quad x \equiv 4 \bmod 20$ ή $x \equiv 14 \bmod 20$

Το αρχικό σύστημα γίνεται:

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

---

$x \equiv 2 \bmod 12$
$x \equiv 14 \bmod 20$

---

$x \equiv 8 \bmod 12$
$x \equiv 4 \bmod 20$

---

$x \equiv 8 \bmod 12$
$x \equiv 14 \bmod 20$

πχ.

$3x \equiv 7 \bmod 8$
$3x \equiv 7 \bmod 14$
$x \equiv 91 \bmod 35$

$3 \cdot 3x \equiv 3 \cdot 7 \bmod 8 \Leftrightarrow x \equiv 5 \bmod 8$
$5 \cdot 3x \equiv 5 \cdot 7 \bmod 14 \Leftrightarrow x \equiv 7 \bmod 14$
$x \equiv 91 \bmod 35$

1η λύση

Επειδή $(8, 35) = 1$ μπορούμε να εφαρμόσουμε το Κινέζο στο
$$\left.\begin{array}{l} x \equiv 5 \bmod 8 \\ x \equiv 21 \bmod 35 \end{array}\right\} \Rightarrow x_0 \bmod (8 \cdot 35)$$

Το αρχικό σύστημα γίνεται $x \equiv x_0 \bmod 280$
$x \equiv 7 \bmod 14$

Εξετάζουμε εάν έχει λύση

Αν και $x = 7 + 14k$ ή $x = x_0 + 280l$ και να αντικαταστήσουμε στην άλλη με άγνωστο το $k$ ή το $l$. Και το λύνουμε...

2η λύση:

$x \equiv 5 \bmod 8$
$x \equiv 7 \bmod 14 \longrightarrow x \equiv 1 \bmod 2$, $x \equiv 7 \bmod 7$
$x \equiv 21 \bmod 35 \Leftrightarrow x \equiv 21 \bmod 5$, $x \equiv 21 \bmod 7$

$x \equiv 5 \bmod 8$
$x \equiv 1 \bmod 2 \Leftrightarrow$ x περιττός
$x \equiv 0 \bmod 7$
$x \equiv 1 \bmod 5$
~~$x \equiv 0 \bmod 7$~~

$$\left.\begin{array}{l} x \equiv 5 \bmod 8 \\ x \equiv 0 \bmod 7 \\ x \equiv 1 \bmod 5 \end{array}\right\} \text{Κινέζο} \Rightarrow \ldots$$

# Συστήματα ισοτιμιών

$a_1 x \equiv b_1 \bmod m_1$
$a_k x \equiv b_k \bmod m_k$

Κάθε μια εξίσωση $a_i x \equiv b_i \bmod m_i$ έχει λύση ανν $(a_i, m_i) | b_i$

Αν $(a_i, m_i) = 1 \Rightarrow$ έχει μοναδική λύση $x \equiv a_i^{-1} \bmod m_i$

Αν $(a_i, m_i) = \delta_i > 1$, $\delta_i | b_i$. Λύνουμε την $\frac{a_i}{\delta_i} x \equiv \frac{b_i}{\delta_i} \bmod \frac{m_i}{\delta_i}$

η οποία έχει μοναδική λύση $x_0 \bmod \frac{m_i}{\delta_i}$

Η $a_i x_i \equiv b_i \bmod m_i$ έχει λύσεις:

$$x_0,\ x_0 + \frac{m_i}{\delta_i},\ x_0 + 2\frac{m_i}{\delta_i}, \ldots, x_0 + (\delta - 1)\frac{m_i}{\delta_i} \bmod m_i$$

Κάθε μία θα δίνει ένα σύστημα
Το αρχικό μπορούμε να το γράψουμε για να μας βοηθήσει για τη γενική λύση

$$\left.\begin{aligned} \frac{a_1}{\delta_1} x &\equiv \frac{b_1}{\delta_1} \bmod \frac{m_1}{\delta_1} \\ &\vdots \\ \frac{a_k}{\delta_k} x &\equiv \frac{b_k}{\delta_k} \bmod \frac{m_k}{\delta_k} \end{aligned}\right) \Rightarrow \begin{aligned} x &\equiv \left(\frac{a_i}{\delta_i}\right)^{-1} \frac{b_i}{\delta_1} \bmod \frac{m_1}{\delta_1} \\ &\vdots \\ x &\equiv \left(\frac{a_k}{\delta_k}\right)^{-1} \frac{b_k}{\delta_k} \bmod \frac{m_k}{\delta_k} \end{aligned}$$

Αυτό έχει λύση αν $\left(\frac{m_i}{\delta_i}, \frac{m_j}{\delta_j}\right) \Big| \left(\frac{a_i}{\delta_i}\right)^{-1} \frac{b_i}{\delta_i} - \left(\frac{a_j}{b_j}\right)^{-1} \frac{b_j}{\delta_j}$

Αν τα $\left(\frac{m_i}{\delta_i}, \frac{m_j}{\delta_j}\right) = 1$ για όλα τα i και j $(i \neq j)$

τότε έχουμε λύση με το Θ. κινέζικο.

# Τετραγωνικά Υπόλοιπα

$ax \equiv b \bmod n$ $\quad ax = b \quad$ αν $x^2 = k \Leftrightarrow x^2 - k = 0$

$$ax^2 + bx + \gamma = 0 \Rightarrow a\left(x^2 + \frac{bx}{a} + \frac{\gamma}{a}\right) =$$

$$= a\left(x^2 + \frac{3b}{2a}x + \left(\frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{\gamma}{a}\right)$$

$$= a\left(\left(x + \frac{b}{2a}\right)^2 - \underbrace{\frac{b^2 - 4a\gamma}{4a^2}}_{D}\right)$$

Αν $D<0 \Rightarrow$ δεν έχει πραγματική λύση

Θέλουμε $\varepsilon^2 = \dfrac{b^2 - 4a\gamma}{4a^2}$ ώστε να γράψουμε

$$= a\left(x + \frac{b}{2a} - \varepsilon\right)\left(x + \frac{b}{2a} + \varepsilon\right) = 0$$

Λύσεις $x = -\dfrac{b}{2a} + \varepsilon$ και $x = -\dfrac{b}{2a} - \varepsilon$

Εξετάζαμε αντίστοιχα την
$ax^2 + bx + \gamma \equiv 0 \bmod p$ με $p$ πρώτος

Επειδή $p$ πρώτος και $(a,p)=1$ για να έχει έννοια η εξίσωση δευτέρου βαθμού πολ/μου με τον $a^{-1} \bmod p$

$x^2 + a^{-1}bx + a^{-1}\gamma \equiv 0 \bmod p$ για $p>2$ έχουμε

$(x + a^{-1}b)^2 - (2a)^{-1}(b^2 - 4a\gamma) \equiv 0 \bmod p$

Θέτουμε $y = x + a^{-1} b \bmod p$ και
$\varepsilon = (2a)^{-1}(b^2 - 4ay) \bmod p$

Η αρχική εξίσωση γίνεται
$y^2 - \varepsilon \equiv 0 \bmod p \Leftrightarrow y^2 \equiv \varepsilon \bmod p$

__Π.χ.__

$x^2 \equiv 2 \bmod 3$ (δοκιμάζω)

$1^2 \not\equiv 2 \bmod 3$
$(-1)^2 \equiv 2^2 \not\equiv 2 \bmod 3$

Δεν έχει λύση

Η $y^2 \equiv \varepsilon \bmod p$ θα έχει λύση
αν για το $\varepsilon$ $\exists\, \delta$ ώστε $\varepsilon \equiv \delta^2 \bmod p$
Τότε το $\varepsilon$ θα λέγεται τετραγωνικό υπόλοιπο.

p

3 $\quad \underset{0^2}{\overset{0}{\equiv}}, \quad \underset{1^2 \equiv (-1)^2}{\overset{1}{\equiv}}, \quad \overset{2}{\uparrow}$ όχι Τ.Υ.

5 $\quad \underset{0^2}{\overset{0}{\equiv}}, \quad \underset{1^2 \equiv (4)^2}{\overset{1}{\equiv}}, \quad \boxed{\underset{\text{όχι}}{\overset{2}{\uparrow}} \quad \underset{\text{όχι}}{\overset{3}{\uparrow}}} \quad \underset{2^2}{\overset{4}{\equiv}}$

$x^2 \equiv 2 \bmod 5$ ή $x^2 \equiv 3 \bmod 5$
Δεν έχουν λύση.

Ορισμός

Αν η εξίσωση $x^2 \equiv b \bmod p$, $p$ πρώτος, έχει λύση τότε το $b$ καλείται Τ.Υ. τετραγωνικό υπόλοιπο $\bmod p$.
Αν δεν έχει λύση καλείται Τ.Μ.Υ. τετραγωνικό μη υπόλοιπο $\bmod p$.

Π.Χ. Στο $\bmod 5$ το 3 είναι ΤΜΥ
το 4 είναι ΤΥ

Παρατήρηση: Έχουμε δει ότι η $x^2 \equiv -1 \bmod p$ έχει λύση αν $p = 4k+1$

Θεώρημα (Κριτήριο Euler)
Έστω $a \in \mathbb{Z}$ με $(a,p)=1$ και $p$ πρώτος.
a) ο $a$ είναι Τ.Υ. ανν $a^{\frac{p-1}{2}} \equiv 1 \bmod p$

β) ο $a$ δεν είναι ΤΥ ανν $a^{\frac{p-1}{2}} \equiv -1 \bmod p$

Απόδειξη

a) Αν ο $a$ είναι ΤΥ, τότε υπάρχει $b$ στο $\bmod p$ με $b^2 \equiv a \bmod p$

$(b^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p \Rightarrow b^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \bmod p$

Επειδή $b^{p-1} \equiv 1 \bmod p \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$

Αν ισχύει $a^{\frac{p-1}{2}} \equiv 1 \bmod p \Rightarrow a$ ΤΥ
Στο $\bmod p$ υπάρχει πρωταρχική ρίζα
g) Είναι το $c$ $1 < c < p-1$ με $ord_p(c) = \varphi(p) = p-1$

Άρα $c^k \equiv a \bmod p$ για κάποιο φυσικό $k$

Άρα, $ord_p(a) = ord_p(c^k)$

Προσοχή : Η σχέση $a^{\frac{p-1}{2}} \equiv 1 \bmod p \Rightarrow$
$ord_p(a) \mid \frac{p-1}{2} \Rightarrow ord_p(c^k) \mid \frac{p-1}{2}$

$ord_p(c^k) \underset{iii}{=} \frac{p-1}{(k, p-1)} \mid \frac{p-1}{2} \Rightarrow$

$\left(\frac{p-1}{2}\right) = \frac{(p-1)}{(k, p-1)} \ell \Rightarrow (k, p-1) = 2\ell \Rightarrow 2 \mid k \Rightarrow c^k \equiv (c^{\frac{k}{2}})^2 \bmod p \equiv$
$\equiv a \bmod p$

Άρα ο $c^{\frac{k}{2}} = d$ έχει την ιδιότητα
$d^2 \equiv a \bmod p \Rightarrow a$ είναι Τ.Υ.

β) $a$ ΤΜΥ $\Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \bmod p$
Οι λύσεις της $x^2 \equiv 1 \bmod p$ είναι 1 και $p-1$

$(a^{\frac{p-1}{2}})^2 \equiv a^{p-1} \equiv 1 \bmod p$

Άρα, το $a^{\frac{p-1}{2}} \bmod p$ είναι λύση της $x^2 \equiv 1 \bmod p$

$a^{\frac{p-1}{2}} \equiv 1 \bmod p$ ή $a^{\frac{p-1}{2}} \equiv -1 \bmod$
$\Updownarrow$
$a$ είναι ΤΥ τότε $a^{\frac{p-1}{2}} \equiv -1 \bmod p \Leftrightarrow a$ ΤΜΥ.

Π.Χ. Εξετάσετε αν το 5 είναι Τ.Υ. mod 19
Αν ναι, να λυθεί η $x^2 \equiv 5 \bmod 19$

$a=5$ $\quad 5^{\frac{p-1}{2}} = 5^{\frac{19-1}{2}} = 5^9$

$5,\ 5^2 \equiv 6,\ 5^3 \equiv 30 \equiv 11,\ 5^4 \equiv 55 \equiv 17$
$5^5 \equiv 85 \equiv 9,\ 5^6 \equiv 45 \equiv 7\ \ 5^7 \equiv 35 \equiv -3$
$5^8 \equiv (-15) \equiv 4,\ 5^9 \equiv 20 \equiv 1 \bmod 19$

Άρα, η $x^2 \equiv 5 \bmod 9$ έχει λύση.