Εξισώσεις Α' Βαθμού

Να βρεθούν οι ακέραιες λύσεις της $ax \equiv b \bmod n$ με $a, b \in \mathbb{Z}$. Στους πραγματικούς $ax+b=0 \Leftrightarrow ax=-b$

Αν $a \neq 0 \Rightarrow \exists a^{-1} \Rightarrow a^{-1} \cdot ax = a^{-1} b \Rightarrow x = \frac{b}{a}$.

Στο $\bmod n$:

$ax \equiv b \bmod n$

Υποθέτουμε ότι $\exists x_0 \in \mathbb{Z}$ ώστε

$ax_0 \equiv b \bmod n \Leftrightarrow ax_0 - b \equiv 0 \bmod n \Leftrightarrow ax_0 - b = kn$

άρα αν $\delta = (a,n) \Rightarrow \delta | b$

Πρέπει $\delta | b$ για να έχουμε λύση το x_0

Αναρωτηθήκατε ποτέ αν υπάρχει ο αντίστροφος του $a \bmod n \Leftrightarrow$ η κλάση $[a]_n$ είναι αντιστρέψιμη; $\Leftrightarrow (a,n)=1$. Υποθέτουμε ότι $(a,n)=1$ και τότε υπάρχει $[\gamma]_n$ με $[\gamma]_n \cdot [a]_n = 1$

$ax \equiv b \bmod n \Rightarrow \gamma a x \equiv \gamma b \bmod n \Rightarrow x \equiv \gamma b \bmod n$.

ΘΕΩΡΗΜΑ: Η εξίσωση $ax \equiv b \bmod n$ έχει λύση στους ακεραίους αν $(a,n) | b$. Τότε, οι λύσεις θα δίνονται από

$x_0, x_0 + \frac{n}{\delta}, x_0 + \frac{2n}{\delta}, \dots, x_0 + \frac{(\delta-1)n}{\delta}$. Όπου x_0 λύση και $\delta = (a,n)$

Απόδειξη

$(\Rightarrow)$ $\exists x_0 : ax_0 \equiv b \bmod n \Leftrightarrow ax_0 - b \equiv kn \Rightarrow \delta = (a,n) | b$

$(\Leftarrow)$ $ax \equiv b \bmod n \Rightarrow \frac{a}{\delta} x \equiv \frac{b}{\delta} \bmod \frac{n}{\delta}$ (1)

Επίσης $\delta=(a,n) \Rightarrow \left(\frac{a}{\delta}, \frac{n}{\delta}\right)=1 \Rightarrow 1 \mid \frac{b}{\delta}$ (2)

καθώς το ότι:

$\left(\frac{a}{\delta}, \frac{n}{\delta}\right)=1 \Rightarrow \exists$ γνωστό $\frac{\alpha}{\delta}\gamma \equiv 1 \bmod \frac{n}{\delta}$ (3)

Από (1), (2) και (3) $\rightsquigarrow x \equiv \gamma \frac{b}{\delta} \bmod \frac{n}{\delta} \Leftrightarrow x=\gamma\frac{b}{\delta}+k\frac{n}{\delta}$, $k=0,1,\dots,\delta-1$

Υπολογίσαμε $(a,n)=1$ και τότε υπάρχει $[\gamma]_n$ με $[\gamma]_n \cdot [a]_n = 1$: $ax \equiv b \bmod n \Rightarrow \gamma a x \equiv \gamma b \bmod n$

$\Rightarrow x \equiv \gamma b \bmod n$

Έστω $x_0 = \gamma\frac{b}{\delta}$ τότε

$\left(\gamma\frac{b}{\delta}+i\frac{n}{\delta}\right) \bmod \frac{n}{\delta} \equiv \left(\gamma\frac{b}{\delta}+j\frac{n}{\delta}\right) \bmod \frac{n}{\delta}$, $i \neq j$

$(i-j)\frac{n}{\delta} \equiv 0 \bmod \frac{n}{\delta}$ άρα βρήκαμε δ διαφορετικές $\bmod \frac{n}{\delta}$

Πόρισμα: Αν $(a,n)=1$, τότε η εξίσωση $ax \equiv b \bmod n$ έχει μοναδική λύση $\bmod n$

Πχ

Να λυθεί η εξίσωση $540x \equiv 18 \bmod 462$

Λύση

Για να έχει λύση θα πρέπει $(540,462) \mid 18$

$540 = 1\cdot 462 + 78 \Rightarrow 462 = 5\cdot 78 + 72 \Rightarrow 78 = 1\cdot 72 + 6$ (6 | 18)

$6 = 78 - 72 = 78 - (462 - 5\cdot 78) = -462 - 6\cdot 78 =$

$= -462 + 6(540 - 462) = 6\cdot 540 - 7\cdot 462 \Rightarrow \boxed{6 = 6\cdot 540 - 7\cdot 462}$

$\Leftrightarrow 3\cdot 6 = 3\cdot 6\cdot 540 - 3\cdot 7\cdot 462 \Rightarrow$

$\Rightarrow 18 \equiv 540\cdot 18 - 462\cdot 21 \Rightarrow 18 \equiv 540 \cdot \underbrace{18}_{\text{(μια λύση)}} \bmod 462$

Για να βρούμε και τις υπόλοιπες λύσεις εφαρμόζουμε το προηγούμενο θεώρημα

$\left(18, 18+\frac{462}{6}, 18+\frac{2\cdot 462}{6}, \dots, 18+\frac{5\cdot 462}{6}\right) \bmod 462$

⊛ Πως θα βρούμε τον αντίστροφο [γΙη;

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

Ένα πιθανό γ είναι το $a^{\varphi(n)-1} \bmod n$

ΘΕΩΡΗΜΑ: Αν $(a,n)=1$, τότε η μοναδική λύση της $ax \equiv b \bmod n$ θα δίνεται από $x \equiv b \cdot a^{\varphi(n)-1} \bmod n$

Πχ

$5x \equiv 3 \bmod 24$

$(5,24) = 1 \mid 3$ έχουμε μοναδική λύση

$x \equiv 3 \cdot 5^{\varphi(24)-1} \bmod 24$

$\varphi(24) = \varphi(2^3 \cdot 3) = \varphi(2^3) \cdot \varphi(3) = 2^2(2-1) \cdot 2 = 8$

$\varphi(24) = 8$

$5^{\varphi(24)} \equiv 1 \bmod 24$

$5^8 \equiv 1 \bmod 24$

$5 \cdot 5^7 \equiv 1 \bmod 24$

$5^7 \equiv ; \bmod 24$

$5^7 = (5^2)^3 \cdot 5 \equiv (25)^3 \cdot 5 \bmod 24 \equiv 1^3 \cdot 5 \bmod 24 \equiv 5 \bmod 24$

$x \equiv 3 \cdot 5^{\varphi(24)-1} \bmod 24 \equiv 3 \cdot 5^7 \bmod 24 \equiv 3 \cdot 5 \bmod 24 \equiv 15 \bmod 24$

$x^2+1=0$ έχει λύση στο $\mathbb{R}$; ← ΟΧΙ

$x^2+1=0$ έχει λύση στο $\mathbb{C}$

Η $x^2 \equiv -1 \bmod p$ έχει λύση p: πρώτος

ΘΕΩΡΗΜΑ:

Έστω p πρώτος περιττός

Υπάρχει $a \in \mathbb{Z}$ με $a^2 \equiv -1 \bmod p$ αν-ν $p \equiv 1 \bmod 4$

ΑΠΟΔΕΙΞΗ

($\Leftarrow$) $p=4k+1 \Leftrightarrow p-1=4k \Leftrightarrow \frac{p-1}{2}=2k$

$1\cdot 2\cdot 3\cdot \ldots \cdot 2k(2k+1)\ldots 4k \equiv -1 \bmod p$ (Wilson)

$(2k+i) \equiv -(2k-i+1) \bmod p$

Άρα, $1\cdot 2\cdot 3\cdot \ldots \cdot 2k\,(-1)(2k)\ldots(-1)\cdot(2k-2k+1) \equiv$

$\equiv 1^2\cdot 2^2\cdot 3^2\cdot \ldots (2k)^2\cdot(-1)^{2k} \equiv -1 \bmod p$

$(\underbrace{1\cdot 2\cdot 3\ldots 2k}_{a})^2 \equiv -1 \bmod p$

($\Rightarrow$) Υποθέτουμε ότι υπάρχει $a \in \mathbb{Z}$ με $a^2 \equiv -1 \bmod p$ (⊕)

Θέλουμε $p=4k+1$ και $(p,a)=1 \Rightarrow a^{p-1} \equiv 1 \bmod p$ (Euler)

(Αν δεν ήταν πρώτος, $p \mid a \Rightarrow p \mid a^2$ και ⊕ $\Rightarrow p \mid 1$)

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

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

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

$p=4k+1 \leftrightarrow \frac{p-1}{2}=2k$ άρτιος $\Leftrightarrow (-1)^{\frac{p-1}{2}}=1$

$p=4k+3 \leftrightarrow \frac{p-1}{2}=2k+1$ περιτ. $\Leftrightarrow (-1)^{\frac{p-1}{2}}=1$

~~$p=4k$~~ $\leftrightarrow$

~~$p=4k+2$~~ $\leftrightarrow$ } ΟΧΙ γιατί p πρώτος

Για $p=4k+1$ ο $\left(\frac{p-1}{2}\right)!=a$ Δηλ. $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \bmod p$

Πρόταση: η συμπεριφορά των λύσεων δευτεροβάθμιων εξισώσεων εξαρτάται από το τίδος του p

Πχ

Ν.Δ.Ο η $x^2 \equiv -1 \bmod 29$ έχει λύση

Επειδή $29 = 4 \cdot 7 + 1 \Rightarrow \exists$ λύση με $\alpha \equiv 14! \bmod 29$

Αντιστρέψιμες κλάσεις - Πολλαπλικές κλάσεις-ρίζες.

Πχ

$p = 7$, $\mathbb{Z}_7 = \{[0]_7, [1]_7, \ldots, [6]_7\}$

$\mathbb{Z}^*_7 = \{[1]_7, [2]_7, \ldots, [6]_7\}$

Επειδή $(a,7) = 1$ με $1 \le a \le 6$, $a \in \mathbb{N}$

τότε κάθε κλάση είναι αντιστρέψιμη

Επίσης, εάν πολ/πο δύο στοιχεία του, θα παράγει πάλι στοιχείο του $\Leftrightarrow$ πολ/με 2 αντιστρέψιμες κλάσεις θα παράγει αντιστρέψιμη κλάση

(Συλ. το $\mathbb{Z}^*_p$ λέει ότι είναι ομάδα)

Επίσης γνωρίζαμε ότι $a^{p-1} \equiv 1 \bmod p$ (Euler)

Άρα, $[a]_p [a^{p-2}]_p = [1]_p$

$[a^k]_p = [a]_p^k$

$\varphi(p) = p-1$, $\varphi(7) = 6$ $\quad a^6 \equiv 1 \bmod 7$

$2 \to 2^2 = 4 \to 2^3 = 8 \equiv 1 \bmod 7$

Ορισμός: Έστω $n > 1$ και $a \in \mathbb{Z}^*$ με $(a,n) = 1$ ονομάζουμε τάξη του $a \bmod n$ τον μικρότερο φυσικό s ώστε $a^s \equiv 1 \bmod n$

Πρόταση: Πάντα ισχύει $a^{\varphi(n)} \equiv 1 \bmod n$

Μας ενδιαφέρει αν $s' < \varphi(n)$

Συμβολισμός: $s = \mathrm{ord}_n(a) = O_n(a)$

Αν λοιπόν $ord_n(a)=5$, τότε $a^k \equiv 1 \bmod y \Rightarrow k \geq 5$

Πχ1 $p=7=n$ $ord_7(2)=3 \leq \varphi(7)=6$

Πχ2 $p=7=n$ $ord_7(3)=6 \leq \varphi(7)=6$

(πρωταρχική ρίζα του 7)

$3 \to 3^2 = 9 \equiv 2 \bmod 7 \to 3^3 = 2 \cdot 3 \bmod 7 \equiv 6 \bmod 7$

$3^4 \equiv 6 \cdot 3 \bmod 7 \equiv 18 \bmod 7 \equiv 4 \bmod 7$

$3^5 \equiv 4 \cdot 3 \bmod 7 \equiv 12 \bmod 7 \equiv 5 \bmod 7$

$3^6 \equiv 5 \cdot 3 \bmod 7 \equiv 15 \bmod 7 \equiv 1 \bmod 7$

(*) Οι δυνάμεις του 3 μας δίνουν όλους τους αριθμούς modulo 7.

$3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1$

$$\mathbb{Z}_7^* = \{[1],[2],[3],[4],[5],[6]\} = \{[3],[3^2],[3^3],[3^4],[3^5],[3^6]\}$$

Ορισμός: Έστω $a \in \mathbb{Z}^*$ και $n>1$ με $(a,n)=1$

Αν $ord_n(a) = \varphi(n)$ τότε ο a καλείται πρωταρχική ρίζα mod n.

Πχ

$2 \to 2^2 \equiv 4 \xrightarrow{\bmod 31} 2^3 \equiv 8 \xrightarrow{\bmod 31} 2^4 \equiv 16 \xrightarrow{\bmod 31} 2^5 = 32 \equiv 1 \bmod 31$

$ord_{31}(3) = 30$ άρα το 3 πρωταρχική ρίζα mod 31

Δηλ. θα υπάρχει φυσικός ώστε $3^k \equiv 2 \bmod 31$

ΠΡΟΤΑΣΗ: Έστω ότι $ord_n(a) = \varphi(n)$ τότε ένα σύστημα ανιπαραθέτων υπολοίπων mod n δίνεται από τις δυνάμεις του a:

$\{[a]_n, [a^2]_n, \ldots, [a^{\varphi(n)}]_n\}$

Πρόταση: Έστω $n>1$ και $a,b \in \mathbb{Z}^*$ με $(a,n)=1$
τότε $a \equiv b \bmod n \Rightarrow ord_n(a) = ord_n(b)$

ΑΠΟΔΕΙΞΗ

$(a,n)=1 \Rightarrow (b,n)=1 \Rightarrow a^k \equiv b^k \bmod n$, $\forall k \in \mathbb{Z}$ (*)

$a-b=nk$

Αν $(b,n)=\delta \Rightarrow \delta \mid b, nk \Rightarrow \delta \mid a \Rightarrow (a,n) \geq \delta$

Έστω $S = ord_n(a) \Rightarrow a^S \equiv 1 \bmod n$ (*) $\Rightarrow b^S \equiv 1 \bmod n$

Προσοχή: αυτό δεν δίνει $ord_n(b)=S$. Απλά, $ord_n(b) \leq S$. Εμείς θέλουμε να είναι S

Έστω ότι $ord_n(b) = t \leq S$

Γράφουμε $S = \pi t + u$, $0 \leq u < t$

$b^S = b^{\pi t + u} \equiv b^u \overset{(*)}{\equiv} a^u$ Άρα

$1 \equiv a^u \bmod n \Rightarrow ord_n(a) \leq u < t$

Αδύνατον. Άρα, $u=0$ και $S=t \Leftrightarrow ord_n(a) = ord_n(b)$

πχ

$ord_7(2) = ord_7(4) = 3$

$2 \to 2^2 = 4 \to 2^3 = 8 \equiv 1 \bmod 7 \Rightarrow ord_7(2) = 3$

$4 \to 4^2 = 16 \equiv 2 \bmod 7 \to 4^3 = 2 \cdot 4 \bmod 7 \equiv 8 \bmod 7 \equiv 1$

$\Rightarrow ord_7(4) = 3$

$4 \not\equiv 2 \bmod 7$

$2^2 \equiv 4 \to ord(2^2) = 3$

$2 \to ord_7(2) = 3$

Πρόταση: Έστω $a \in \mathbb{Z}^*$ και $n>1$ με $(a,n)=1$
τότε

i) $a^m \equiv a^k \bmod n \Leftrightarrow m \equiv k \bmod s$, $S = ord_n(a)$

ii) $a^m \equiv 1 \bmod n \Leftrightarrow S = ord_n(a) \mid m$

ΑΠΟΔΕΙΞΗ

Απόδειξη

i) ($\Rightarrow$): $m-k = \Pi S + U$ ← Διαιρούμε με το $S = ord_n(a)$ $0 \le U < S$

$a^S \equiv 1 \bmod n \Rightarrow a^{\Pi S} \equiv 1 \bmod n \Rightarrow a^{m-k} = a^{\Pi \cdot S} \cdot a^U \bmod n$

$\Rightarrow a^{m-k} \equiv a^U \bmod n$ (*)

$a^m - a^k \equiv 0 \bmod n \Rightarrow n \mid a^m - a^k = a^k(a^{m-k}-1)$

$n \mid a^k(a^{m-k}-1)$ } $\Rightarrow n \mid a^{m-k}-1 \Leftrightarrow a^{m-k} \equiv 1 \bmod n$ (**)

$(a, n) = 1$

Από (*) και (**) $\Rightarrow a^U \equiv 1 \bmod n$ } $\Rightarrow$ Άδοναζο

Επί $U < S$ Άρα, $U = 0$

$m = k \bmod S$

($\Leftarrow$): Αν $m = k \bmod S \Rightarrow m - k + S\Pi \Rightarrow a^m = a^{k+S\Pi} =$

$= a^k \cdot a^{S\Pi} = a^k \cdot (a^S)^\Pi \equiv a^k \cdot 1 \bmod n$

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

ii) Χρήση του (i) για $k = 0$

Πόρισμα: $ord_n(a) \mid \varphi(n)$

Απόδειξη

Από πάνω $a^{\varphi(n)} \equiv 1 \bmod n$, Άρα $S \mid \varphi(n)$

Πρόταση: Οι τάξεις είναι διαιρέτες του $\varphi(n)$

Πχ 1) $ord_{36}(5)$

Αυτός πρέπει να διαιρεί το $\varphi(36) = \varphi(4 \cdot 9) = \varphi(4)\varphi(9)$

$= \varphi(2^2)\varphi(3^2) = 2^1(2-1)3^1(3-1) = 2^2 \cdot 3$

Το $ord_{36}(5)$ μπορεί να είναι $2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3$

$5 \to 5^2 = 25 \to 5^3 = 5 \cdot 25 = 125 \equiv 17 \bmod 36$

$36 \times 3 = 108$ $5^4 = 5^3 \cdot 5 \equiv 17 \cdot 5 \bmod 36 \equiv$

$\equiv 85 \bmod 36 \equiv 13 \bmod 36$.

$5^4 \equiv 13 \bmod 36$.

Επομένως δεν είναι $5^5 \equiv 1 \bmod 36$

$5^6 \equiv 5^4 \cdot 5^2 = 13 \cdot 25 \bmod 36 \equiv 325 \bmod 36 \equiv 1 \bmod 36$

ΠΡΟΤΑΣΗ

Αν $\text{ord}_n(a) = s$ και $\text{ord}_n(b) = t$
με $(s,t) = 1$, τότε $\text{ord}_n(ab) = st$

ΠΧ

$\text{ord}_{11}(30) = \text{ord}_{11}(8) = \text{ord}_{11}(2^3)$

$\varphi(11) = 10$ πιθανοί διαιρέτες $2, 5, 10$

$30 = 3 \cdot 10$

$10 \to 10^2 = 100 \equiv 1 \bmod 11 \Rightarrow \text{ord}(10) = 2$

$3 \to 3^2 = 9 \to (3^2) \cdot 3 = 9^2 3 = 81 \cdot 3 \equiv 4 \cdot 3 \equiv 12 \equiv 1 \bmod 11$

Άρα, η τάξη του 3 είναι 5 ($\text{ord}_{11}(3) = 5$)

$(\text{ord}_{11}(3), \text{ord}_{11}(10)) = (5,2) = 1$

$\text{ord}_{11}(30) = 2 \cdot 5 = 10 = \varphi(11)$.