20/12/2016

Τετραγωνικά Υπόλοιπα

Ο α καλείται τετραγωνικό υπόλοιπο mod m αν $\exists\ b \in \mathbb{Z}$ $b^2 \equiv a \bmod m$ Τ.Υ.

Αν δεν υπάρχει καλείται Τετρ. μη-υπόλοιπο (ΤΜΥ) mod m

α ΤΥ $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \bmod p$

Λύση: $x^2 \equiv a \bmod m$

Η λύση αν υπάρχει εξαρτάται από το α και m.

Π.Χ. $x^2 \equiv 5 \bmod 19$

$5^{\frac{19-1}{2}} \equiv 5^9 = 25 \equiv 1 \bmod p \Rightarrow$ έχει λύση

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

αν γράφεται

$4+1$

$5 = 25 \cdot 25 \cdot 5 = 6 \cdot 6 \cdot 5 \equiv -10 \bmod 19 \equiv 9 \bmod 19$

$9^2 = 81 \bmod 19 = 5$

Άρα, η λύση είναι $\boxed{5^{4+1} \bmod 19}$

Γενικά a^{k+1} λύση της $x^2 \equiv a \bmod p$

$(a^{k+1})^2 \equiv a^{2k+2}$

$p-1 = 4k+2 \Rightarrow \frac{p-1}{2} = 2k+1$

$a^{\frac{p-1}{2}} \equiv 1 \bmod p \Leftrightarrow a^{2k+1} \equiv 1 \bmod p$

$a^{2k+2} \equiv a \bmod p$

$(a^{k+1})^2 \equiv a \bmod p$

Γενικά Αν $p=4k+3$ και η $x^2 \equiv a \bmod p$ έχει λύση ($a^{\frac{p-1}{2}} \equiv 1 \bmod p$) τότε η λύση δίνεται από $a^{k+1} \bmod p$.

Π.χ.

$x^2 \equiv 5 \bmod 77 \qquad 77 = 7 \cdot 11$

$x^2 \equiv 5 \bmod 7$
$x^2 \equiv 5 \bmod 11$

Θεώρημα

Έστω p πρώτος και a ακέραιος με $(p,a)=1$.
Αν η $x^2 \equiv a \bmod p$ έχει λύσεις τότε και η $x^2 \equiv a \bmod p^2$ έχει επίσης λύσεις (οι λύσεις είναι δύο)
Αν η $x^2 \equiv a \bmod p$ δεν έχει λύση τότε αυτή και η $x^2 \equiv a \bmod p^2$ έχει λύση.

(χωρίς απόδειξη)

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

$x^2 \equiv 15 \bmod 7^2$ (+) $\quad (15, 49) = 1$

Αν x_0 είναι λύση $x_0^2 \equiv 15 \bmod 7^2$

$x_0^2 - 15 = m7^2 \bmod 7$

$\bmod 7$: $0, 1, \dots, 6$ ↓

$\bmod 7^2$: $0, 1, 2, \dots, 48$

$u + 7n$ | $0 \le u \le 6$, $0 \le n \le 6$

$x_0 = u + 7n$ (++)

$x_0 = (v+7n)^2$

$x_0^2 - 15 = (v+7n)^2 - 15 \bmod 7 \Rightarrow v^2 - 15 \equiv 0 \bmod 7$

αρα, ν λύση της $x^2 \equiv 15 \bmod 7$

$x^2 \equiv 15 \bmod 7 \Rightarrow x^2 \equiv 1 \bmod 7 \Leftrightarrow v = \pm 1$.

Η λύση x_0 της αρχικής (+) θα είναι της μορφής

(++) $x_0 = v + 7n = 1 + 7n$ ή $-1 + 7n'$

Πρέπει να βρούμε το π ή π'

$(1+7n)^2 \equiv 15 \bmod 7^2$

$1 + 2 \cdot 7n + \cancel{7^2 \cdot n^2} \equiv 15 \bmod 7^2$

$2 \cdot 7\pi \equiv 14 \bmod 7^2 \xrightarrow{:7}$

$\Rightarrow 2\pi \equiv 2 \bmod 7$

$\Rightarrow \pi \equiv 1 \bmod 7$.

Η λύση $x_0 \equiv 1 + 1 \cdot 7 \bmod 7^2$

$x_0 \equiv 8 \bmod 7^2$

Επαλήθευση: $8^2 = 64 \bmod 49 \equiv 15$.

Το ίδιο μας για $v = -1$

ΙΙ.Χ. Βρείτε μια πρωταρχική ρίζα mod 8.

mod 8

$\varphi(8) = \varphi(2^3) = 2^{3-1}(2-1) = 4$

0 X 2 3 X 5 X 7

$3^2 \equiv 9 \equiv 1 \quad 5^2 \equiv 25 \equiv 1 \quad 7^2 = 49 \equiv 1.$

ΙΙ.Υ. Βρείτε την πρωταρχική ρίζα mod 27

Θεώρημα (χωρίς απόδειξη)

Έστω ότι το πολυώνυμο $f(x)$ έχει ακέραιους συντελεστές και $a \in \mathbb{Z}$. Με $f'(x)$ θα συμβολίζουμε την παράγωγο ως προς x. Τότε υπάρχει ακέραιο πολυώνυμο $g(x)$ ώστε $f(a+x) = f(a) + f'(a)x + g(x)x^2$

Θεώρημα

Έστω p πρώτος, $k \in \mathbb{N}^*$, $f(x)$ ακέραιο πολυώνυμο και η $f(x) \equiv 0 \bmod p^k$ έχει λύση x_0. Τότε

1) Αν $p \nmid f'(x_0)$, τότε η $f(x) \equiv 0 \bmod p^{k+1}$ έχει μοναδική λύση $b \equiv x_0 \bmod p^k$

   Η λύση δίνεται από $b = x_0 + p^k \cdot t$ με το t να είναι λύση της $f'(x_0)t \equiv -\frac{f(x_0)}{p^k} \bmod p$

2) Αν $p \mid f'(x_0)$ και $p^k \, p^{k+1} \mid f(x_0)$ τότε υπάρχουν p λύσεις στο $f(x) \equiv 0 \bmod p^{k+1}$

3) Αν $p \mid f'(x_0)$ και $p^{k+1} \nmid f(x_0)$ τότε η $f(x) \equiv 0 \bmod p^{k+1}$ ΔΕΝ έχει λύση.

ΠΧ a) $x^2 = 47 \bmod 11$ (++)

$x^2 = 47 \bmod 11 \equiv 3 \bmod 11$

$3^{\frac{p-1}{2}} = 3^5 = 9 \cdot 9 \cdot 3 = 5 \cdot 9 = 1$

$11 = 4 \cdot 2 + 3$

$3^{2+1} = 3^3 = 27 = 5$

Λύσεις τις $x^2 \equiv 3 \bmod 11$

5 και 6

Θέτουμε $x_0 = 5 + 11n$

$(5+11n)^2 \equiv 47 \bmod 11^2$

$25 + 2 \cdot 5 \cdot 11n + 11^2 n^2 \equiv 47 \bmod 11^2$

$\frac{2 \cdot 5 \cdot 11n}{11} \equiv \frac{22 \bmod 11^2}{11}$

$10n \equiv 2 \bmod 11$

$(-1)n \equiv 2 \bmod 11$

$(-1)(-1)n \equiv -2 \bmod 11 \equiv 9 \bmod 11$

$x_0 = 5 + 11 \cdot 9 = 104 \bmod 121$

β) $3x^2 \equiv 20 \bmod 11^2$

$(3, 11^2) = 1 \Rightarrow \exists\ 3^{-1} \bmod 11^2$

$11^2 = 121 = 120 + 1$

$3 \cdot 40 = 120 \equiv -1 \bmod 11^2$
$3^2 \cdot 40^2 \equiv 1 \bmod 11^2$
$3(3 \cdot 1600) \equiv 1 \bmod 11^2$
$3^{-1} \equiv 4800 \bmod 121 \equiv 81$ (+)

4800 | 121
1 2 f o | 39
= 81

$3x^2 \equiv 20 \bmod 11^2 \overset{(+)}{\Longrightarrow} x^2 \equiv 1620 \bmod 11^2$

1620 | 11
0410 | 13
47

$x^2 \equiv 47 \bmod 11^2$ (++)

Βλέπε ερώτημα α.

γ) $3x^2 + 60x + 38 \equiv 0 \bmod 121$

SOS
θέμα στην εξεταστική

$(3, 121) = 1$

$3(x^2 + 20x + 3^{-1} \cdot 38) \equiv 0 \bmod 121$
$3^{-1} \cdot 3 (x^2 + 20x + 81 \cdot 38) \equiv 0 \bmod 121$

$81 \times 38 = 3078$

3078 | 121
658 | 25
53

$x^2 + 20x + 53 \equiv 0 \bmod 121$

$2 \cdot 10x$

$x^2 + 2 \cdot 10x + 53 + 10^2 - 10^2 \equiv 0 \bmod 121$
$(x+10)^2 - 100 + 53 \equiv 0 \bmod 121$
$(x+10)^2 \equiv 47 \bmod 121$

Θέτουμε $x + 10 = y$
$y^2 \equiv 47 \bmod 121$ (++)
$y = 104 \bmod 121 \Rightarrow x + 10 \equiv 104 \bmod 121$

$\boxed{x \equiv 94 \bmod 121}$

Η μια λύση. Έχει και άλλη.

ΑΡΙΘΜΗΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ

Μια συνάρτηση $f: \mathbb{N}^* \to \mathbb{C}$ καλείται αριθμητική συνάρτηση

Π.Χ. $f(n)=a$ σταθερή $f(n)=0$ η 1 είναι πολ/κη
$f(n)=n$ ταυτοτική πολ/κη
$f(n)=n^i$
$f(n)=e^n$

$f(n)=\varphi(n)$ = πλήθος θετικών πρώτων με n
$f(n)=\sigma(n)$ = άθροισμα θετικών διαιρετών του n
$f(n)=\tau(n)$ = πλήθος θετικών διαιρετών του n

Ορισμός

Μια αριθμητική συνάρτηση $f: \mathbb{N}^* \to \mathbb{C}$ καλείται πολλαπλασιαστική, αν ισχύει:

$f(nm)=f(n)\cdot f(m)$ όταν $(n,m)=1$

Αν ισχύει $f(nm)=f(n)\cdot f(m)$ χωρίς περιορισμό, τότε καλείται πλήρως πολ/κη.

Π.Χ. $f(n)=n$, $f(n)=0$, $f(n)=1$ είναι πλήρως πολ/κες

$f(n)=\varphi(n)$, $f(n)=6(n)$ είναι απλά πολ/κες, όχι πλήρως

Συμβολισμός: $\sum_{d|n} f(d)$ = άθροισμα των εικόνων μέσω της f των διαιρετών του n

$$\sum_{d|12} f(d) = \boxed{f(1)} + \textcircled{f(2)} + \underline{f(3)} + \underline{f(4)} + \textcircled{f(6)} + \boxed{f(12)}$$

$\prod_{d|n} f(d)$ = γινόμενο των εικόνων μέσω της f των διαιρετών του n

$\prod_{d|12} f(d) = f(1)\, f(2)\, f(3)\, f(4)\, f(6)\, f(12)$

Π.χ $\sigma(n)$ = άθροισμα των διαιρετών $= \sum_{d|n} d$

Η f εδώ είναι ταυτοτική $f(d)=d$

$$n = \sum_{d|n} \varphi(d)$$

$g(n)=n$ ταυτοτική

$f(d)=\varphi(d)$ Euler

Παρατηρήσεις

1) Αν n f είναι πολ/κη, τότε $f(n)=f(n\cdot 1)=f(n)\,f(1)$
Άρα $f(1)=1$

2) Αν n f είναι πολ/κη, τότε αρκεί να υπολογίσουμε τα $f(p^k)$.
$$f(p_1^{k_1} \dots p_\ell^{k_\ell}) = f(p_1^{k_1}) \dots f(p_\ell^{k_\ell})$$

Ορισμός

Αν η f είναι πολλ/κη με F θα συμβολίζουμε την αριθμητική συνάρτηση $F: \mathbb{N}^* \to \mathbb{C}$ με τ.ο

$$F(n) = \sum_{d|n} f(d)$$

Πρόταση

Η F είναι πολλ/κη.

Απόδειξη

Έστω $(n,m)=1$, τότε $d|mn$
τότε $d=d_1d_2$ με $(d_1,d_2)=1$ και $d_1|m$, $d_2|n$ $(d_1,d_2)=1$

Έχουμε $F(m,n) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2) =$ f πολλ/κη

$$\sum_{d_1|m}\sum_{d_2|m} f(d_1)f(d_2) = \sum_{d_1|m} f(d_1) \sum_{d_2|m} f(d_2) = F(m).F(n)$$

Πόρισμα

1) Οι συναρτήσεις $\tau(n)$ και $\sigma(n)$ είναι πολλ/κες
2) Αν $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$ τότε $\tau(n) = \prod_{i=1}^{\ell}(k_i+1)$ και

$$\sigma(n) = \prod_{i=1}^{\ell} \frac{p_i^{k_i+1}-1}{p_i-1} \quad (+)$$

Απόδειξη

Οι αριθμητικές συναρτήσεις $g, f: \mathbb{N}^* \to \mathbb{C}$ με $g(n)=1$ και $f(n)=n$ είναι πλήρως πολλ/κες.

$\tau(n)$ = πλήθος των θετικών διαιρετών του $n = \sum_{d|n} 1(d) = 1$

Π.Χ.

$$\tau(12) = \underset{1}{1} + \underset{2}{1} + \underset{3}{1} + \underset{4}{1} + \underset{6}{1} + \underset{12}{1} =$$

$$= 1(1) + 1(2) + 1(3) + 1(4) + 1(6) + 1(12)$$

Άρα και η τ είναι πολ/κη

$$\tau(n) = \prod_{i=1}^{e} \tau(p_i^{k_i}) \qquad \tau(p^k) = ;;;$$

Ποιοι είναι οι διαιρέτες του p^k;

p^r με $0 \le r \le k$

$$\tau(p^k) = k+1$$

Άρα $\tau(n) = \prod_{i=1}^{e}(k_i+1)$

$\sigma(n)$ = Άθροισμα των διαιρετών του n

$= \sum_{d/n} d$ ← ταυτοτική συνάρτηση $F(d) = d$

n οποία είναι πολ/κη

Άρα, $\sigma(n)$ πολ/κη.

$$\sigma(p_1^{k_1} \dots p_e^{k_e}) = \prod_{i=1}^{e} \sigma(p_i^{k_i})$$

$$\left.\begin{array}{l} \sigma(p^k) = 1 + p + p^2 + \dots + p^k = \dfrac{p^{k+1} - 1^{k+1}}{p-1} \\ \text{Διαιρέτες του } p^k : 1, p, p^2, \dots, p^k \end{array}\right\} \Rightarrow \oplus$$

Παρατήρηση

$$F(n)=\sum_{d|n} f(d)$$

$F(1)=f(1)$
$F(2)=f(1)+f(2)$
$F(3)=f(1)+f(3)$
$F(4)=f(1)+f(2)+f(4)$
$F(5)=f(1)+f(5)$

Η F καθορίζει την f_{jj}

$f(n)=; \ \forall n\in\mathbb{N}^*$

Συνάρτηση του Mobius $\mu:\mathbb{N}^*\to\mathbb{C}$

$$\mu(n)=\begin{cases}1 & n=1\\ 0 & p^2\mid n\\ (-1)^\ell & n=p_1p_2\cdots p_\ell\end{cases}$$

$\mu(3\cdot11\cdot13\cdot17)=1 \qquad n=3\cdot11\cdot13\cdot17$
$\mu(3\cdot11^2\cdot13^3\cdot17)=0=\mu(3\cdot11\cdot13^3\cdot17)$

Πρόταση

Η συνάρτηση του Mobius είναι πολ/κη.

$$\sum_{d|n}\mu(d)=\begin{cases}1 & n=1\\ 0 & \text{διαφορετικά}\end{cases}$$

Απόδειξη

n,m με $(n,m)=1$

α) $n=m=1 \Rightarrow \mu(1\cdot1)=\mu(1)=1=\mu(1)\cdot\mu(1)$

β) $\exists\, p^2\mid n$ ή m. Ας πούμε ότι $p^2\mid n$ και $p^2\nmid m$ και $\mu(nm)=0$

$\mu(nm)=0=\mu(n)\cdot\mu(m)$

γ) κανένας δεν διαιρείται με τετράγωνο πρώτου

$n = p_1 p_2 \cdots p_\ell$ $\quad m = q_1 \cdots q_\epsilon$ με $p_1, p_2, \ldots, p_\ell, q_1, \ldots, q_\epsilon$ διαφορετικοί πρώτοι

$\mu(mn) = \mu(p_1 p_2 \cdots p_\ell q_1 \cdots q_\epsilon) = (1)^{\ell+\epsilon}$ διαφορετικοί πρώτοι,

$= (-1)^\ell (-1)^t = \mu(p_1 \cdot p_2 \cdots p_\ell)\, \mu(q_1 q_2 \cdots q_\epsilon) = \mu(m) \cdot \mu(n)$.

Άρα, μ πολ/κη $\Rightarrow F(n) = \sum_{d|n} \mu(d)$ πολ/κη.

$n = p_1^{k_1} \cdots p_\ell^{k_\ell} \Rightarrow F(n) = \prod_{i=1}^{\ell} F(p_i^{k_i})$

$F(p^k) = \sum_{d|p^k} \mu(d)$

αν $k=0$ τότε $F(1) = \mu(1) = 1$

αν $k=1$ τότε $F(p) = \sum_{d|p} \mu(d) = \mu(1) + \mu(p) = 1 + (-1) = 0$

$F(p^2) = \sum_{d|p^2} \mu(d) = \boxed{\mu(1) + \mu(p)} + \mu(p^2)^{\to 0}$

αν $k \geq 2$ τότε $F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2)^{\to 0} + \mu(p^3)^{\to 0} + \mu(p^k)^{\to 0}$

$= 1 + (-1) = 0$

Άρα $F(p^k) = \begin{cases} 1 & k = 0 \\ 0 & k > 0 \end{cases}$