

Μέγιστος κοινός διαιρέτης πολυωνύμων

Το πολυώνυμο $d(x)$ είναι ΜΚΔ των πολυωνύμων $d_1(x)$, $d_2(x)$ αν:
το $d(x)$ διαιρεί τα $d_1(x)$, $d_2(x)$ και έχει τον ελάχιστο δυνατό βαθμό.

Ταυτότητα για τον ΜΚΔ πολυωνύμων

Αν το πολυώνυμο $d(x)$ είναι ΜΚΔ των πολυωνύμων $d_1(x)$, $d_2(x)$:
θα υπάρχουν πολυώνυμα $A(x)$, $B(x)$ ώστε $d(x) = A(x) \circ d_1(x) + B(x) \circ d_2(x)$.

Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο

Εστω πολυώνυμο $d_K(x)$, $0 \leq K \leq N-1$, όπου:
κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$, $j \neq K$, είναι σταθερά.

Εστω $P(x)$, $Q(x)$ πολυώνυμα όπου $P(x) = Q(x) \bmod d_K(x)$, $0 \leq K \leq N-1$.

Τότε $P(x) = Q(x) \bmod \prod_{0 \leq K \leq N-1} d_K(x)$.

Chinese Remainder Theorem για πολυώνυμα

Δίνονται πολυώνυμα $d_K(x)$, $u_K(x)$, $0 \leq K \leq N-1$, ώστε:

Κάθε πολυώνυμο $u_K(x)$ έχει βαθμό μικρότερο από τον βαθμό του $d_K(x)$.

Κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$, $j \neq K$ είναι σταθερά.

Θα υπάρχει πολυώνυμο $P(x)$ ώστε:

$$P(x) \bmod d_K(x) = u_K(x), \quad 0 \leq K \leq N-1.$$

Σημείωση Από την Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο :

το πολυώνυμο $P(x) \bmod \prod_{0 \leq K \leq N-1} d_K(x)$ θα είναι μοναδικό.

ΑΠΟΔΕΙΞΗ

Θεωρούμε ένα τυχαίο K , $0 \leq K \leq N-1$:

Για κάθε $j \neq K$, κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$ είναι σταθερά:
επομένως θα υπάρχουν πολυώνυμα $A_{j,K}(x)$, $B_{j,K}(x)$ ώστε

$$1 = A_{j,K}(x) \circ d_K(x) + B_{j,K}(x) \circ d_j(x),$$

$$\text{οπότε} \quad B_{j,K}(x) \circ d_j(x) = 1 \bmod d_K(x) \quad \text{για κάθε } j \neq K$$

Θέτουμε $g_K(x) = \prod_{0 \leq j \leq N-1, j \neq K} B_{j,K}(x) \circ d_j(x)$:

$$\text{Από τα παραπάνω} \quad g_K(x) = 1 \bmod d_K(x) \quad (\text{I})$$

$$g_K(x) = 0 \bmod d_j(x), \quad \text{για κάθε } j \neq K \quad (\text{II})$$

Σημείωση Από την Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο :

το πολυώνυμο $g_K(x) \bmod \prod_{0 \leq K \leq N-1} d_K(x)$ θα είναι μοναδικό.

Θέτουμε $P(x) = \sum_{0 \leq \Lambda \leq N-1} g_\Lambda(x) \circ u_\Lambda(x)$:

Έχουμε $P(x) \bmod d_K(x) = \sum_{0 \leq \Lambda \leq N-1} [g_\Lambda(x) \circ u_\Lambda(x) \bmod d_K(x)]$

Από τις (I, II) : $P(x) \bmod d_K(x) = u_K(x)$, $0 \leq K \leq N-1$.

Άσκηση 1 Ιδιότητες των πολυωνύμων $g_K(x)$, $0 \leq K \leq N-1$.

Εστω $D(x) = \prod_{0 \leq K \leq N-1} d_K(x)$, όπου για κάθε $j \neq K$,
κάθε πολυώνυμο που είναι ΜΚΔ των $d_K(x)$, $d_j(x)$ είναι σταθερά.

Για τα πολυώνυμα $g_K(x)$, $0 \leq K \leq N-1$, έχουμε ότι:

$$g_K(x) = 1 \pmod{d_K(x)} \quad (I)$$

$$g_K(x) = 0 \pmod{d_j(x)}, \text{ για κάθε } j \neq K. \quad (II)$$

Αποδείξτε ότι:

α Για $0 \leq K \leq N-1$, $d_K(x) \circ g_K(x) = 0 \pmod{D(x)}$

$$g_K(x) \circ g_K(x) = g_K(x) \pmod{D(x)}$$

Για κάθε $j \neq K$, $g_j(x) \circ g_K(x) = 0 \pmod{D(x)}$.

β $\sum_{0 \leq j \leq N-1} g_j(x) = 1 \pmod{D(x)}$.

Απάντηση

Για το (α) : Εφαρμόζουμε την Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο,
στα πολυώνυμα που αναφέρονται.

Για το (β) : Αναπτύσσουμε το γινόμενο $\prod_{0 \leq j \leq N-1} (1 - g_j(x))$,
και εφαρμόζουμε το (α) .

ΕΦΑΡΜΟΓΗ του Chinese Remainder Theorem

Δίνονται πολυώνυμα $d_K(x) = x - \rho_K$, $0 \leq K \leq N-1$, όπου $\rho_j \neq \rho_K$ για $j \neq K$.

Δίνονται σταθερές v_K , $0 \leq K \leq N-1$.

Θα υπάρχει πολυώνυμο $P(x)$ ώστε: $P(x) \bmod x - \rho_K = v_K$, $0 \leq K \leq N-1$.

Το πολυώνυμο $P(x) \bmod \prod_{0 \leq K \leq N-1} x - \rho_K$ θα είναι μοναδικό.

ΚΑΤΑΣΚΕΥΗ

Θεωρούμε ένα τυχαίο K , $0 \leq K \leq N-1$:

Για κάθε $j \neq K$, θέτουμε $A_{j,K}(x) = (\rho_j - \rho_K)^{-1}$ $B_{j,K}(x) = -(\rho_j - \rho_K)^{-1}$.

Θα έχουμε $1 = A_{j,K}(x) \circ d_K(x) + B_{j,K}(x) \circ d_j(x)$,

οπότε $B_{j,K}(x) \circ d_j(x) = 1 \bmod d_K(x)$ για κάθε $j \neq K$.

Θέτουμε $f_K(x) = \prod_{0 \leq j \leq N-1, j \neq K} B_{j,K}(x) \circ d_j(x)$
 $= \prod_{0 \leq j \leq N-1, j \neq K} (\rho_K - \rho_j)^{-1} \circ (x - \rho_j)$.

Θα έχουμε $f_K(x) = 1 \bmod d_K(x)$

$f_K(x) = 0 \bmod d_j(x)$, για κάθε $j \neq K$.

Θέτουμε $P(x) = \sum_{0 \leq K \leq N-1} v_K \cdot f_K(x)$.

Άσκηση 2 Εστω $m(x) = \prod_{0 \leq K \leq N-1} x - \rho_K$, ρ_K σταθερά, $\rho_j \neq \rho_K$ για $j \neq K$.

Έστω ένα πολυώνυμο $h(x)$.

α Ελέγξτε ότι $h(x) \bmod x - \rho_K = h(\rho_K)$, $0 \leq K \leq N-1$.

β Αποδείξτε ότι: αν $H(x) \bmod x - \rho_K = h(\rho_K)$, $0 \leq K \leq N-1$,

θα είναι $H(x) = h(x) \bmod m(x)$.

Απάντηση

Για το (β): Εφαρμόζουμε την Ιδιότητα πολυωνύμων πρώτων μεταξύ τους ανά δύο, στα πολυώνυμα $H(x)$, $h(x)$.