Κινέζικο Θεώρημα Υπολοίπων (CRT)

Το Κινέζικο Θεώρημα Υπολοίπων (**C**hinese **R**emainder **T**heorem) μάς παρέχει, κατ' αρχήν, μια μέθοδο επίλυσης συστημάτων γραμμικών ισοτιμιών. Οι λύσεις μπορούν να βρεθούν χρησιμοποιώντας έναν εύκολο και αποδοτικό αλγόριθμο.

Θεώρημα

Έστω $m_1, \ldots, m_r \in \mathbb{N}$ ανά δύο σχετικώς πρώτοι ακέραιοι, δηλ.

$$\gcd(m_i, m_j) = 1, \text{ για } i \neq j.$$

Έστω επίσης $a_1, a_2, \ldots, a_r$ ακέραιοι. Τότε υπάρχει ακέραιος x τέτοιος, ώστε

$$x \equiv a_i \pmod{m_i}, \; i = 1, \ldots, r.$$

Επιπλέον, το υπόλοιπο $x \bmod M$ είναι μοναδικό, όπου $M = m_1 \cdot \ldots \cdot m_r$. □

Η πρόταση αυτή σημαίνει ότι υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των κλάσεων καταλοίπων modulo M και των πλειάδων κλάσεων καταλοίπων modulo $m_1, \ldots, m_r$. Αυτή η αμφιμονοσήμαντη αντιστοιχία διατηρεί την προσθετική και πολλαπλασιαστική δομή. Επομένως, έχουμε την ακόλουθη δακτυλιο-θεωρητική διατύπωση του παραπάνω Θεωρήματος.

Θεώρημα 5.18 (Κινέζικο Θεώρημα Υπολοίπων)

Έστω $m_1,\ldots, m_r \in \mathbb{N}$ ανά δύο σχετικώς πρώτοι ακέραιοι,, δηλ.

$$\gcd(m_i, m_j) = 1, \text{ για } i \neq j.$$

Έστω $M = m_1 \cdot \ldots \cdot m_r$. Τότε η απεικόνιση

$$\begin{aligned} f:\ \mathbb{Z}_M &\to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \\ [x] &\mapsto ([x \bmod m_1], \ldots, [x \bmod m_r]) \end{aligned}$$

είναι ένας ισομορφισμός δακτυλίων. □

Από την απόδειξή του, την οποία παραλείψαμε, προκύπτει το εξής γεγονός (που μας δίνει έναν αποδοτικό αλγόριθμο υπολογισμού των λύσεων ενός συστήματος ισοτιμιών):

Έστω $m_1,\ldots, m_r \in \mathbb{N}$ με $\gcd(m_i, m_j) = 1$, αν $i \neq j$. Έστω επίσης $a_1, \ldots, a_r \in \mathbb{Z}$ τέτοιοι, ώστε

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad\vdots \\ x \equiv a_r \pmod{m_r} \end{cases} \qquad \textbf{(1)}$$

Τότε το σύστημα **(1)** έχει μία μόνο λύση modulo $M = m_1 \ldots m_r$, η οποία δίνεται από τον τύπο

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

όπου $M_i = M/m_i$ και $y_i = M_i^{-1} \bmod m_i$, $1 \leq i \leq r$.

Ισομορφισμοί:

- $f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r}$

  $f(x) = (x \bmod m_1, \ldots, x \bmod m_r)$

  (όπου παραλείπουμε τον συμβολισμό κλάσεων αναφερόμενοι στους φυσικούς αντιπροσώπους τους)

Παραδείγματος χάρη, αν

$$r = 2,\ m_1 = 5,\ m_2 = 3 \quad (M = 5 \cdot 3 = 15)$$

τότε είναι

$$\mathbb{Z}_{15} \to \mathbb{Z}_5 \times \mathbb{Z}_3:\ \begin{array}{lll} f(0) = (0, 0) & f(1) = (1, 1) & f(2) = (2, 2) \\ f(3) = (3, 0) & f(4) = (4, 1) & f(5) = (0, 2) \\ f(6) = (1, 0) & f(7) = (2, 1) & f(8) = (3, 2) \\ f(9) = (4, 0) & f(10) = (0, 1) & f(11) = (1, 2) \\ f(12) = (2, 0) & f(13) = (3, 1) & f(14) = (4, 2) \end{array}$$

- $\rho = f^{-1}:\ \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_r} \to \mathbb{Z}_M$

$$\rho(a_1, \ldots, a_r) \equiv \sum_{i=1}^{r} a_i M_i y_i \bmod M$$

Παράδειγμα

Έστω $r = 3$ και $m_1 = 7$, $m_2 = 11$, $m_3 = 13$, οπότε $M = 7 \cdot 11 \cdot 13 = 1001$ και $M_1 = 143$, $M_2 = 91$, $M_3 = 77$.

Βρίσκουμε τους αντίστροφους, $y_1 = 5$, $y_2 = 4$, $y_3 = 12$.

(Οι τιμές αυτές βρίσκονται με τον διευρυμένο αλγόριθμο του Ευκλείδη)

Άρα,

$$f^{-1}(a_1, a_2, a_3) = (715a_1 + 364a_2 + 924a_3) \bmod 1001$$

και για $a_1 = 5$, $a_2 = 3$, $a_3 = 10 \;\Rightarrow\; x = (715 \cdot 5 + 364 \cdot 3 + 924 \cdot 10) \bmod 1001 = 894.$ ■

Ο αλγόριθμος υπολογισμού που αναφέραμε παραπάνω είναι άμεση υλοποίηση των όσων ήδη είπαμε και είναι ο ακόλουθος:

Αλγόριθμος CRT($m_1,\ldots, m_r$; $a_1, \ldots, a_r$)

$M \leftarrow m_1 \cdot \ldots \cdot m_r$

for $i \leftarrow 1$ **to** r

$M_i \leftarrow M/m_i$

$b_i \leftarrow M_i \bmod m_i$

$t_i \leftarrow b_i^{-1} \bmod m_i$

$e_i \leftarrow M_i t_i$

$x \leftarrow \sum_{i=1}^{r} a_i e_i \bmod M$

return x

Παράδειγμα

Ας βρούμε τους δύο μικρότερους θετικούς ακεραίους οι οποίοι έχουν υπόλοιπα 1, 2 και 6 όταν διαιρεθούν με τους 3, 5 και 7 αντιστοίχως. Πρέπει

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

Είναι

$$\begin{cases} a_1 = 1 \\ a_2 = 2 \\ a_3 = 6 \end{cases}, \quad \begin{cases} m_1 = 3 \\ m_2 = 5 \\ m_3 = 7 \end{cases} \text{ (ανά δύο σχετικώς πρώτοι) και}$$

$$M = m_1 m_2 m_3 = 105.$$

Βρίσκουμε

$$\begin{cases} M_1 = M/m_1 = 35 \\ M_2 = M/m_2 = 21 \\ M_3 = M/m_3 = 15 \end{cases} \text{ και } \begin{cases} b_1 = M_1 \bmod m_1 = 35 \bmod 3 = 2 \\ b_2 = M_2 \bmod m_2 = 25 \bmod 5 = 1 \\ b_3 = M_3 \bmod m_3 = 15 \bmod 7 = 1 \end{cases}$$

Επίσης βρίσκουμε τους

$$\begin{cases} t_1 = b_1^{-1} \bmod m_1 = 2^{-1} \bmod 3 = 2 \\ t_2 = b_2^{-1} \bmod m_2 = 1^{-1} \bmod 2 = 1 \\ b_3 = b_3^{-1} \bmod m_3 = 1^{-1} \bmod 7 = 1 \end{cases} \text{ και } \begin{cases} e_1 = M_1 t_1 = 35 \cdot 2 = 70 \\ e_2 = M_2 t_2 = 21 \cdot 1 = 21 \\ e_3 = M_3 t_3 = 15 \cdot 1 = 15 \end{cases}$$

οπότε

$$x = (a_1 e_1 + a_2 e_2 + a_3 e_3) \bmod M = (1 \cdot 70 + 2 \cdot 21 + 6 \cdot 15) \bmod 105 = 202 \bmod 105 = 97.$$

Άρα οι ζητούμενοι ακέραιοι είναι οι 97 και $97 + 105 = 202$. ■

❖ Το CRT μπορεί να χρησιμοποιηθεί ώστε να γίνουν οι αριθμητικοί υπολογισμοί modulo M (δηλ. στο $\mathbb{Z}_M$), όπου M ένας μεγάλος ακέραιος, ευκολότεροι και (πολύ) περισσότερο αποδοτικοί.

Στηριζόμαστε στο γεγονός ότι η απεικόνιση

$$f: \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$$

$$[x] \mapsto ([x \bmod m_1], \ldots, [x \bmod m_r])$$

είναι ένας ισομορφισμός δακτυλίων.

Έτσι, έστω η αντιστοιχία

$$a \leftrightarrow (a_1, a_2, \ldots, a_r)$$

όπου $a \in \mathbb{Z}_M$, $a_i \in \mathbb{Z}_{m_i}$ και

$$a_i = a \bmod m_i \quad \text{για } i = 1, 2, \ldots, r.$$

Η απεικόνιση f είναι μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των $\mathbb{Z}_M$ και $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$.

Οι πράξεις που εκτελούνται στα στοιχεία του $\mathbb{Z}_M$ μπορούν ισοδύναμα να γίνουν στις αντίστοιχες διατεταγμένες r – αδες εκτελώντας τις πράξεις ανεξάρτητα σε κάθε συνιστώσα: αν

$$a \leftrightarrow (a_1, a_2, \ldots, a_r),$$
$$b \leftrightarrow (b_1, b_2, \ldots, b_r),$$

τότε

- $(a + b) \bmod n \leftrightarrow ((a_1 + b_1) \bmod n_1, (a_2 + b_2) \bmod n_2, \ldots, (a_r + b_r) \bmod n_r)$

  $(ab) \bmod n \leftrightarrow ((a_1 b_1) \bmod n_1, (a_2 b_2) \bmod n_2, \ldots, (a_r b_r) \bmod n_r)$

  $k^t \bmod M \leftrightarrow \left(a_1^t \bmod m_1, a_2^t \bmod m_2, \ldots, a_r^t \bmod m_r\right)$

Απεικονίζουμε τους τελεστέους στο $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ με την f και κάνουμε εκεί τους υπολογισμούς μας.

Το $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ είναι ένα Καρτεσιανό γινόμενο δακτυλίων.

Η πρόσθεση και ο πολλαπλασιασμός γίνονται κατά τις συνιστώσες, δηλ. εκτελούμε τους υπολογισμούς modulo m_i, για $i = 1, \ldots, r$.

Έτσι δουλεύουμε με πολύ μικρότερους αριθμούς.

Στο τέλος, απεικονίζουμε το αποτέλεσμα πίσω στο $\mathbb{Z}_M$ με την αντίστροφη απεικόνιση f^{-1} (που γίνεται εύκολα με τον τύπο του CRT).

Παράδειγμα

(Εφαρμογή σε πράξεις με μεγάλους αριθμούς)

Έστω ότι ο Η/Υ μας μπορεί να κάνει πράξεις με ακέραιους στο διάστημα [0, 10000].

Μπορούμε χρησιμοποιώντας το CRT να επεκτείνουμε αυτό το διάστημα.

Αν πάρουμε $m_1 = 10000$, $m_2 = 9999$, είναι $\gcd(m_1, m_2) = 1$ και $m_1 \cdot m_2 = 99.990.000$.

Έστω ότι θέλουμε να προσθέσουμε:

$$25108735 + 13869131$$

στον υποθετικό Η/Υ μας.

Για να δούμε πως αποθηκεύει ο Η/Υ μας κάθε αριθμό εφαρμόζουμε τη συνάρτηση

$$f(\alpha) = (\alpha \bmod 10000, \alpha \bmod 9999)$$

στον καθένα:

$$f(25108735) = (8735, 1246)$$
$$f(13869131) = (9131, 518)$$

Για το $\alpha = 25108735 + 13869131$ παρατηρούμε:

- $\alpha \equiv 25108735 + 13869131 \equiv 8735 + 9131 \equiv 17866$
  $\equiv 7866 \pmod{10000}$
- $\alpha \equiv 25108735 + 13869131 \equiv 1246 + 518$
  $\equiv 1764 \pmod{9999}$

Εν συντομία:

$$\begin{aligned} 25108735 + 13869131 \rightarrow (8735, 1246) + (9131 + 518) &= \\ (8735 + 9131, 1246 + 518) &= \\ (17866, 1764) = (7866, 1764). \end{aligned}$$

Ευκλείδης:

$$10000 - 9999 = 1 \Rightarrow$$
$$f^{-1}(a_1, a_2) = (10000a_2 + 9999a_1) \Rightarrow$$
$$\begin{aligned} \alpha = f^{-1}(7866, 1764) &= 10000 \cdot 1764 - 9999 \cdot 7866 \\ &= -61012134 \\ &\equiv 38977866 \pmod{99990000}. \end{aligned}$$

■

Άσκηση

Να υπολογίσετε το 263790^{216491} mod 265651 γνωρίζοντας ότι 265651 = 631·421, όπου οι ακέραιοι 631, 421 είναι πρώτοι.

Λύση

Είναι

$$x \equiv 263790^{216491} \pmod{265651} \Leftrightarrow$$

$$\begin{cases} x \equiv 263790^{216491} \pmod{631}, & (1) \\ x \equiv 263790^{216491} \pmod{421}, & (2) \end{cases}$$

Είναι

$$263790 \equiv 32 \pmod{631} \Rightarrow$$

$$263790^{216491} \pmod{631} \equiv 32^{216491} \pmod{631}.$$

Επειδή ο 631 είναι πρώτος, από το θεώρημα Fermat έχουμε

$$32^{630} \equiv 1 \pmod{631} \Rightarrow$$

$$32^{216491} \equiv 32^{216491 \bmod 630} \equiv 32^{401} \pmod{631}.$$

Για τον υπολογισμό της δύναμης αυτής χρησιμοποιούμε τη μέθοδο των επανειλημμένων τετραγωνισμών (από αριστερά στα δεξιά εκθετοποίηση):

Είναι

$$401 = 110010001_2$$

και με τους υπολογισμούς να γίνονται στο $\mathbb{Z}_{631}$, βρίσκουμε

i	8	7	6	5	4	3	2	1	0
b_i	1	1	0	0	1	0	0	0	1
	32	$32^2 \cdot 32$	587^2	43^2	$587^2 \cdot 32$	114^2	376^2	32^2	$393^2 \cdot 32$
		$= 587$	$= 43$	$= 587$	$= 114$	$= 376$	$= 32$	$= 393$	$= 376$

Άρα, (1) $\Leftrightarrow$ $x \equiv 376 \pmod{631}$.

Παρόμοια, επειδή $263790 \equiv 244 \pmod{421}$ και $216491 \equiv 191 \pmod{420}$, έχουμε

$$263790^{216491} \equiv 244^{191} \pmod{421}$$

$$\equiv 102 \pmod{421}$$

οπότε

$$(2) \Leftrightarrow x \equiv 102 \pmod{421}.$$

Έτσι έχουμε καταλήξει στο εξής σύστημα ισοτιμιών

$$\begin{cases} x \equiv 376 \pmod{631} \\ x \equiv 102 \pmod{421} \end{cases}$$

Σύμφωνα με τη μέθοδο (αλγόριθμο) του Κινέζικου θεωρήματος υπολοίπων είναι:

$$\begin{cases} a_1 = 376 \\ a_2 = 102 \end{cases}, \quad \begin{cases} m_1 = 631 \\ m_2 = 421 \end{cases}$$ (ανά δύο σχετικώς πρώτοι) και

$$M = m_1 m_2 = 265651.$$

Βρίσκουμε

$$\begin{cases} M_1 = M/m_1 = 421 \\ M_2 = M/m_2 = 631 \end{cases} \quad \text{και} \quad \begin{cases} b_1 = M_1 \bmod m_1 = 421 \bmod 631 = 421 \\ b_2 = M_2 \bmod m_2 = 631 \bmod 421 = 210 \end{cases}$$

Επίσης βρίσκουμε

$$\begin{cases} t_1 = b_1^{-1} \bmod m_1 = 421^{-1} \bmod 631 = 3 \\ t_2 = b_2^{-1} \bmod m_2 = 210^{-1} \bmod 421 = 419 \end{cases}$$

και

$$\begin{cases} e_1 = M_1 t_1 = 421 \cdot 3 = 1263 \\ e_2 = M_2 t_2 = 631 \cdot 419 = 264389 \end{cases}$$

[στους υπολογισμούς για τους αντίστροφους χρησιμοποιήσαμε τον διευρυμένο αλγόριθμο του Ευκλείδη:

i	0	1	2	3	4
r_i	631	421	210	1	0
q_i		1	2	210	
s_i	1	0	1	–2	
t_i	0	1	–1	3	

$\Rightarrow$ gcd(631, 421) = 1, t = 3 $\Rightarrow$ 421^{-1} mod 631 = 3

και

i	0	1	2	3
r_i	421	210	1	0
q_i		2	210	
s_i	1	0	1	
t_i	0	1	–2	

$\Rightarrow$ gcd(421, 210) = 1, t = –2 $\equiv$ 419 (mod 421)

$\Rightarrow$ 210^{-1} mod 421 = 419.]

οπότε

$$x = (a_1 e_1 + a_2 e_2) \bmod M =$$

$$(376 \cdot 1263 + 102 \cdot 264389) \bmod 265651 = 80513.$$

Άρα,

$$263790^{216491} \bmod 265651 = 80513.$$