

Παράδειγμα Αλγορίθμου του Shanks

Ας πάρουμε $p=809$. Επιθυμούμε να υπολογίσουμε το $\log_3 525$.

1. Το $a=3$ είναι πρωταρχική ρίζα $\text{mod } 809$ και $b=525$. Είναι $m=\lceil p-1 \rceil = \lceil 808 \rceil = 29$
2. Υπολογίζουμε το $a^m \text{ mod } p = 3^{29} \text{ mod } 809 = 99 \text{ mod } 809$.
3. Στη συνέχεια υπολογίζουμε τα ζευγάρια $(j, 99^j \text{ mod } 809)$, $0 \leq j \leq m-1=28$ και σχηματίζουμε τον πίνακα L1.
Είναι:
(0,1), (23,15), (12,26), (28,81), (2,93), (1,99), (13,147), (8,207), (6,211), (9,268), (19,275), (27,295), (3,308), (5,329), (17,464), (21,496), (20,528), (4,559), (22,564), (26,575), (25,586), (18, 638), (10, 644), (11,654), (7, 664), (24,676), (15,725), (16,781), (14,800)
4. Υπολογίζουμε στη συνέχεια τα ζευγάρια $(i, 525 \cdot 3^{-i} \text{ mod } 809)$, $0 \leq i \leq m-1=28$ και σχηματίζουμε τον πίνακα L2.
Είναι:
(6,44), (5,132), (17,133), (28,163), (1,175), (13,256), (24,259), (18,314), (2,328), (14,355), (25,356), (3,379), (15,388), (4,396), (16,399), (10,440), (27,489), (9,511), (21,521), (0,525), (7,554), (19,644), (26,658), (11,686), (22,713), (8,724), (20,754), (23,777)
5. Παρατηρούμε ότι $(10,644) \in L1$ και $(19,644) \in L2$.
Επομένως $\log_3 525 = 29 \cdot 10 + 19 = 309$.
6. Επαλήθευση: Πρέπει $3^{309} = 525 \pmod{809}$ που ισχύει πράγματι.