Άσκηση 1.6

Σάββατο, 14 Μαρτίου 2020

36, 18, 9, 12,

Στον αλγόριθμο Baby step, Giant step, θέλουμε να λύσουμε την εξίσωση $g^x = h \bmod p$ «σπάζοντας» τον άγνωστο λογάριθμο $0 \le x < p - 1$ σε $x = b + S \cdot G$, όπου $S = \lceil \sqrt{(p-1)} \rceil$ και $b, G \le S$.

Έπειτα, ξαναγράφουμε την εξίσωση ως $g^{S \cdot G} \equiv h \cdot g^{-b}$. Έτσι, μπορούμε να εξαντλήσουμε όλες τις περιπτώσεις, με 2S υπολογισμούς (και O(n log n) συγκρίσεις για ταξινόμηση), αντί τους $p - 1 = S^2$ υπολογισμούς της προφανούς λύσης.

$\log_2 5 \bmod 37$

$2^x = 5 \bmod 37$

$x = 0, 1, 2, 3 \dots 35$

$x = b + 6 \cdot G$ όπου $b, G < 5$

$2^{b+6G} \equiv 5 \Leftrightarrow 2^b = 5 \cdot 2^{-6G}$

37 = 18·2 + 1

1 = 37 − 18·2

$2^{-1} = 19 \bmod 37$

$2^0 = 1$	$5 \cdot 2^{-0}$	$5 \quad 19^0 \quad 5 \cdot 11^0$
$2^1 = 2$	$5 \cdot 2^{-6}$	$5 \cdot 19^6 \quad 5 \cdot 11^1$
$2^2 = 4$	$5 \cdot 2^{-12}$	$5 \cdot 19^{12} \quad 5 \cdot 11^2$
$2^3 = 8$	$5 \cdot 2^{-18}$	⋮ ⋮
$2^4 = 16$	$5 \cdot 2^{-24}$	
$2^5 = 32$	$5 \cdot 2^{-30}$	

37 × 3 = 90 + 21 = 111 = 148

$19^6 = (19 \cdot 19)^3 = 361^3 = (-3)^3 = 81 \cdot (-3) = (81 - 74) \cdot (-3) = -21 \cdot 3 = 16 \cdot 3 = 48 = 11$

$2^5 = 5 \cdot 2^{-6(3)}$

$11^0 = 1$

$11^1 = 11$

$11^2 = 121 = 10$

$11^3 = 11 \cdot 10 = 110 = -1 = -5 = 32$

$11^4 = -11 = 26$ $\quad = 130 - 111 = 19$

$11^5 = -10 = 27$ $\quad = 135 - 111 = 24$

$x5 = 5$

$= 55 = 18$

$= 50 = 13$

$x = 5 + 3 \cdot 6 = 5 + 18 = 23$

$2^{23} = 8 \cdot (2^5)^4 = 8(-5)^4 = 8 \cdot 25^2 = 2 \cdot 50^2 = 2 \cdot 13^2 = 26 \cdot 13$

$= -11 \cdot 13$

$= -130 - 13 = -143$

$\equiv 5^{-143 + 148}$