Αλγόριθμος Tonelli – Shanks

Εργασία στα πλαίσια του μαθήματος
«*Στοιχεία Θεωρίας Αριθμών*
και Εφαρμογές στην Κρυπτογραφία»

Νικολακόπουλος Θεόδωρος

Αθήνα, Φεβρουάριος 2012

Ο αλγόριθμος Tonelli – Shanks

- Δεδομένων ενός ακεραίου *n* και ενός πρώτου *p* > 2, επιστρέφει έναν ακέραιο *R*, ούτως ώστε:

$$R^2 \equiv n \pmod{p}$$

- Ο Alberto Tonelli ανέπτυξε το 1891 μια πιο αργή εκδοχή του αλγορίθμου
- Ο Daniel Shanks βελτίωσε τον αλγόριθμο το 1973

Βήματα του αλγορίθμου (1)

- Είσοδος: ακέραιος n, πρώτος $p > 2$.

  1. Εύρεση ακεραίων Q και S ούτως ώστε:

$$p-1 = Q \cdot 2^S$$

  2. Εύρεση ακεραίου z που να μην είναι τέλειο τετράγωνο modulo p.

  3. $c \leftarrow z^Q \bmod p$ $\quad R \leftarrow n^{\frac{Q+1}{2}} \bmod p$

     $t \leftarrow n^Q \bmod p$ $\quad M \leftarrow S$

Βήματα του αλγορίθμου (2)

4. Όσο $t \neg \equiv 1 \pmod{p}$ επανάλαβε:

α') Βρες το μικρότερο θετικό ακέραιο i ώστε:

$$t^{2^i} \equiv 1 \pmod{p}$$

β') $b \leftarrow c^{2^{M-i-1}} \bmod p$ $c \leftarrow b^2 \bmod p$ $R \leftarrow (R \cdot b) \bmod p$

$t \leftarrow (t \cdot b^2) \bmod p$ $M \leftarrow i$

- Έξοδος: R (η άλλη ρίζα είναι η $p - R \equiv R \pmod{p}$)

Βήμα 1ο: $p-1 = Q \cdot 2^S$

- Επιτυγχάνεται με συνεχείς διαιρέσεις δια 2

Βήμα 2ο: Εύρεση *z* ώστε: $\left(\frac{z}{p}\right) = -1$

- Επιλέγουμε τυχαίους αριθμούς και υπολογίζουμε το σύμβολο Lagrange.
- Ένας αριθμός έχει πιθανότητα να είναι τέλειο τετράγωνο modulo *p*: $\frac{p+1}{2p}$
- Απαιτούνται κατά μέσον όρο 2 δοκιμές

Βήμα 3ο: $c \leftarrow z^{Q} \bmod p \quad R \leftarrow n^{\frac{Q+1}{2}} \bmod p \quad t \leftarrow n^{Q} \bmod p \quad M \leftarrow S$

$$R \leftarrow n^{\frac{Q+1}{2}} \left(\bmod p\right) \Rightarrow$$

$$R^2 \equiv n^{Q+1} \equiv n^{Q} \cdot n \left(\bmod p\right) \overset{t \equiv n^{Q} \left(\bmod p\right)}{\Rightarrow}$$

$$R^2 \equiv t \cdot n \left(\bmod p\right)$$

- Θα δούμε ότι αυτό ισχύει και μετά από κάθε επανάληψη του 4ου βήματος

Βήμα 4ο: $b \leftarrow c^{2^{M-i-1}} \bmod p, c \leftarrow b^2 \bmod p, R \leftarrow (R \cdot b) \bmod p, t \leftarrow (t \cdot b^2) \bmod p, M \leftarrow i$

- Όπως είδαμε, ισχύει: $R^2 \equiv t \cdot n \pmod p$
- Προφανώς αν $t \equiv 1 \pmod p$ έχουμε το επιθυμητό R
- Σε κάθε επανάληψη έχουμε:

$$R' \equiv R \cdot b \pmod p \Rightarrow R'^2 \equiv R^2 \cdot b^2 \pmod p \overset{R^2 = t \cdot n \pmod p}{\Rightarrow}$$

$$R'^2 \equiv t \cdot n \cdot b^2 \overset{t' \equiv t \cdot b^2 \pmod p}{\Rightarrow} R'^2 \equiv t' \cdot n \pmod p$$

Ταχύτητα του αλγορίθμου

- Αν ο *p* έχει *m* bit, εκ των οποίων *k* είναι 1, το πλήθος των πολλαπλασιασμών modulo που απαιτούνται είναι:

$$2m+2k+\frac{S(S-1)}{4}+\frac{1}{2^{S-1}}-9$$