11-5-2017

Σε όλα τα πρωτόκολλα που έχουμε δει μέχρι τώρα, το πρώτο βήμα είναι να επιλέξουμε δύο μεγάλους πρώτους p και q. Πώς όμως τους επιλέγουμε;

- 1η προσέγγιση: διαλέγουμε έναν τυχαίο αριθμό και ελέγχουμε αν είναι πρώτος.
- 2η προσέγγιση: διαλέγω από ένα κατάλογο πρώτων αριθμών.

Η 2η προσέγγιση είναι ευάλωτη σε επιθέσεις στον κατάλογο. Αν δηλαδή κάποιος αποκτήσει πρόσβαση στον κατάλογο από τον οποίο διαλέγουμε τους p και q, τότε θα μπορεί να αποκρυπτογραφήσει τα μηνύματά μας οποιοδήποτε πρωτόκολλο και αν χρησιμοποιήσουμε.

Η 1η προσέγγιση γεννά δύο ερωτήματα:

- Τι σημαίνει ότι ένας αριθμός είναι τυχαίος;
- Πώς μπορούμε να ελέγξουμε σε πολυωνυμικό χρόνο ότι ένας αριθμός είναι πρώτος;

Έστω ότι έχουμε να λύσουμε το παρακάτω πρόβλημα:

Έχουμε μια σειρά από n bits, από τα οποία τα n/2 είναι 0 και τα υπόλοιπα n/2 είναι 1. Σε πόσο χρόνο θα βρούμε τον πρώτο άσσο;

Οι ντετερμινιστικοί αλγόριθμοι που γνωρίζουμε μέχρι τώρα χρειάζονται χρόνο n/2+1 για να επιλύσουν το πρόβλημα, με την παροχή του κατάλληλου στιγμιότυπου. Αν δηλαδή ο αντίπαλος που παρέχει τη σειρά γνωρίζει ποιόν αλγόριθμο θα χρησιμοποιήσουμε, θα μπορεί πάντα να μας δώσει μια σειρά για την οποία ο αλγόριθμος θα χρειαστεί χρόνο n/2+1 για να λύσει το πρόβλημα.

Αν χρησιμοποιήσουμε ένα πιθανοτικό αλγόριθμο, εισάγεται η έννοια της **μέσης περίπτωσης**, δηλαδή το μέσο πλήθος των bit που πρέπει να εξετάσουμε για να βρούμε 1. Η **χειρότερη περίπτωση** δεν αλλάζει και είναι n/2+1. Για το πρόβλημα αυτό, η μέση περίπτωση είναι 2.

Επιτυχής Πιθανοτικός Αλγόριθμος

Ένας πιθανοτικός αλγόριθμος θεωρείται επιτυχής αν έχει πιθανότητα επιτυχίας

$$Pr(success) \geq 1 - \frac{1}{n^c}, \quad \text{όπου } c \geq 1 \text{ σταθερά}$$

Χρησιμοποιώντας έναν πιθανοτικό αλγόριθμο θα πρέπει να εξετάσουμε τουλάχιστον $\log_2 n$ για να λύσουμε το πρόβλημα.

Τι σημαίνει ότι ένας αριθμός είναι τυχαίος;

Σημαίνει ότι αν παρατηρήσουμε n εξόδους, τότε δεν μπορούμε να αυξήσουμε την πιθανότητα να μαντέψουμε σωστά την επόμενη.

Πρόβλημα

Έστω ότι έχουμε ένα κέρμα που φέρνει κορώνα με πιθανότητα p και γράμματα με πιθανότητα 1-p. Πώς θα δημιουργήσουμε ένα τίμιο κέρμα (με p=0,5) χρησιμοποιώντας αυτό που έχουμε;

2 ρίψεις του κέρματος που διαθέτουμε αντιστοιχούν σε μία του τίμιου, και κωδικοποιούνται ως εξής:

ΚΚ αγνοείται, ξαναρίχνουμε το κέρμα

ΓΚ 0

ΚΓ 1

ΓΓ αγνοείται, ξαναρίχνουμε το κέρμα

Πρόβλημα ΠΡΩΤΟΣ(n)
Είσοδος: n
Έξοδος: είναι το n πρώτος;

Το πρόβλημα ανήκει στο σύνολο P, δηλαδή υπάρχουν αλγόριθμοι που το λύνουν σε πολυωνυμικό χρόνο. Όμως για να βρούμε από ποιούς p και q παραγοντοποιείται ο n, θα πρέπει να λύσουμε το πρόβλημα ΠΑΡΑΓΟΝΤΟΠΟΙΗΣΗ(n) το οποίο δεν λύνεται σε πολυωνυμικό χρόνο.

Πώς μπορούμε λοιπόν να αποδείξουμε ότι ένας αριθμός είναι πρώτος;

Μικρό θεώρημα Fermat
Αυτή η προσέγγιση δεν δουλεύει.

Έστω p ένας πρώτος. Τότε για κάθε α ∈ {1, 2, ..., p-1} (δηλαδή το α είναι ένας αριθμός που παράγει κάποια από τις ομάδες του p) ισχύει ότι $\alpha^{p-1} \equiv 1 (\mod p)$.

FERMAT(n):
-διαλέγω ένα α ∈ {1, 2, ..., n-1}
-ελέγχω αν $\alpha^{n-1} \equiv 1 (\mod n)$
-αν “ΟΧΙ” τότε “ΣΥΝΘΕΤΟΣ”
-αν “ΝΑΙ”, επιστροφή στο πρώτο βήμα

Η προσέγγιση αυτή δεν δουλεύει επειδή υπάρχουν τιμές για το n για το οποίο δεν μπορούμε να έχουμε την απάντηση “ΟΧΙ”.

Αριθμοί Carmichael
Οι αριθμοί για τους οποίους ισχύει αυτό λέγονται αριθμοί Carmichael. Είναι σύνθετοι με gcd(a,n)=1, και $\alpha^{n-1} \equiv 1 (\mod n)$. Τους αριθμούς αυτούς θα πρέπει είτε να τους θεωρήσουμε πρώτους, είτε να τους χρησιμοποιήσουμε για να παραγοντοποιήσουμε το n.

Miller-Rabin
Αν ο p είναι πρώτος, τότε το $x^2 \equiv 1 (\mod p)$ έχει μόνο δυο ρίζες, 1 και p-1. Για παράδειγμα, το $x^2 \equiv 1 (\mod 15)$ έχει 4 ρίζες, άρα το 15 δεν είναι πρώτος.

```
MILLER-RABIN(n):
for i=1 to k {
    a←random
    witness(a,n)  //είναι το α μάρτυρας ότι ο n είναι σύνθετος;
    if “true”
        then return “COMPOSITE”
    }
return “PRIME”
```

Παρατήρηση: Το ότι ένας αριθμός είναι μάρτυρας σημαίνει ότι είναι παράγοντας του n και είναι διαφορετικός από το 1 και το n. Αν το n είναι όντως σύνθετος, τότε η

πιθανότητα το α να είναι μάρτυρας είναι 3/4. Η πιθανότητα να μην βρω κάποιο μάρτυρα σε k προσπάθειες είναι $(1/4)^k$.

```
WITNESS(a,n)
b_k, b_{k-1}, ...., b_1          //δυαδική αναπαράσταση n-1
d=1
/*Με αυτό το κομμάτι εξετάζουμε αν μπορούμε να βρούμε αντιπαράδειγμα για το Miller-Rabin*/
for i=k down to 1 {
    temp←d
    d←d^2 modn
    if d==1 AND temp≠{n-1, 1}
        return TRUE
    if b==1
        d←admodn
    }
/*Με αυτό το κομμάτι εφαρμόζουμε το μικρό θεώρημα Fermat. Η τελική τιμή του d θα είναι n-1.*/
if a^d≠1(modn)
    return TRUE
else
    return FALSE
```

Έτσι, αν το n είναι σύνθετος, τότε θα βρούμε 3n/4 μάρτυρες. Για k προσπάθειες, η πιθανότητα το τεστ να πει ότι ο αριθμός είναι πρώτος, ενώ στην πραγματικότητα είναι σύνθετος, είναι το πολύ $1/4^k$ ή $Pr(M-R\ \pi\rho\acute{\omega}\tau\sigma\varsigma | n\ \sigma\acute{\upsilon}\nu\theta\varepsilon\tau\sigma\varsigma) = \frac{1}{4^k}$ Η πιθανότητα μειώνεται επειδή αφαιρούμε το κάθε a από το σύνολο των αριθμών που δεν είναι μάρτυρες, ώστε να μην το επιλέξουμε ξανά. Θα είμαστε σίγουροι για την απάντηση αν δοκιμάσουμε $\left(\frac{n}{4}\right)^k$ φορές.