Αλγόριθμος AKS και πολυωνυμική πολυπλοκότητα

Ν. Λυγερός

Στον τομέα της πιστοποίησης πρώτου στη θεωρία αριθμών υπάρχουν οι εργασίες του Atkin και του Morain, οι οποίες παραμένουν αποτελεσματικές στις πρακτικές εφαρμογές. Όμως στον καθαρά θεωρητικό τομέα, ο αλγόριθμος AKS έλυσε οριστικά το πρόβλημα της πολυπλοκότητας εφόσον απέδειξε ότι η πιστοποίηση πρώτου είναι πολυωνυμική.
Ο αλγόριθμος AKS αποτελείται από τα εξής βήματα:

1. Αν υπάρχουν ακέραιοι $\alpha \geq 2$ και $\kappa \geq 2$ με $n = \alpha^{\kappa}$, τότε ο n είναι σύνθετος.

$O((\log n)^4)$

Πολυπλοκότητα :

2. Να βρεθεί ο μικρότερος πρώτος r έτσι ώστε η τάξη του n modulo r να είναι μεγαλύτερη από $4(\log_2 n)^2 + 2$. Θέτουμε $l = 2\sqrt{r}\log_2 n + 1$

Πολυπλοκότητα : $O((\log n)^8)$

3. Αν κάποιος από τους ακεραίους *2, 3, ..., l* διαιρεί τον *n*, τότε ο *n* είναι σύνθετος.

Πολυπλοκότητα : $O((\log n)^5)$

4. Αν ισχύει $(X-\alpha)^n \neq X^n - \alpha$ modulo $R_{n,r}$
όπου $R_{n,r}$ συμβολίζει τη σχέση ισοδυναμίας που ορίζεται
επί του *Z[X]* από το ιδεώδες $I_{m,r} = (m, X^r - 1)$
με τον εξής τρόπο: $\alpha(X) \equiv \beta(X)$ modulo $R_{m,r} \Leftrightarrow \alpha(X) - \beta(X) \in I_{m,r}$

για κάποιο $\alpha \in [1,....,l]$, τότε ο *n* είναι σύνθετος.

Πολυπλοκότητα : $O\left((\log n)^{17}\right)$

5. Αν ο *n* δεν έχει βρεθεί σύνθετος σε κάποιο από τα προηγούμενα βήματα, τότε αυτός είναι πρώτος.

Συμπεραίνουμε, λοιπόν, ότι η συνολική πολυπλοκότητα του αλγορίθμου AKS είναι $O\left((\log n)^{17}\right)$. Και αυτή είναι η θεωρητική καινοτομία του αλγορίθμου AKS, διότι πρακτικά δεν αλλάζει ουσιαστικά την προσέγγιση του προβλήματος της πιστοποίησης πρώτου εφόσον η αποτελεσματικότητα των εκθετικών αλγορίθμων είναι ισχυρότερη. Παρ' όλα αυτά, ο αλγόριθμος AKS θα είναι πια ένα σημείο αναφοράς για τη βαθιά γνώση μας στον τομέα όπως ο αλγόριθμος του Shor για την

επίλυση του διακριτού λογαρίθμου μέσω κβαντικών υπολογιστών. Η αξία του είναι η ύπαρξή του και όχι η χρήση του.