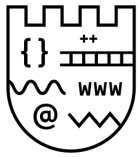
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Σχολή Θετικών Επιστημών



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Υλοποίηση Quadratic Sieve

Καλαθάς Μάνος - ΑΕΜ:101

7 Φεβρουαρίου 2022

Περιεχόμενα

1 Quadratic Sieve **2**

1.1 Περιγραφή προγράμματος 2

1.2 Αρχικοποίηση 2

1.3 Κοσκίνισμα 2

1.4 Γραμμική Άλγεβρα 2

1.5 Παραγοντοποίηση 3

1 Quadratic Sieve

1.1 Περιγραφή προγράμματος

Το πρόγραμμα δέχεται ως είσοδο από τον χρήστη τον αριθμό που επιθυμεί να παραγοντοποιήσει και ως μεταβλητές έχει ένα άνω όριο B και το μήκος του sieve. Ο χρήστης μπορεί να αλλάξει αυτές τις τιμές όπως επιθυμεί και κάθε φορά που ο αλγόριθμος αποτυγχάνει να βρει μία λύση διπλασιάζει το όριο B.

1.2 Αρχικοποίηση

Στην αρχικοποίηση του αλγορίθμου υπολογίζονται όλοι οι πρώτοι αριθμοί μικρότεροι του B για τους οποίους ισχύει η σχέση legendre $\frac{n}{p} = 1$.

1.3 Κοσκίνισμα

Βάση των πρώτων που βρήκαμε στο προηγούμενο βήμα, πραγματοποιείται τώρα ένα κοσκίνισμα των αριθμών $(x^2 - n)$ με το x να παίρνει τιμές από την ρίζα του αριθμού που θέλουμε να παραγοντοποιήσουμε μέχρι το διάστημα που ορίζει η μεταβλητή στην αρχή του προγράμματος. Οι αριθμοί που βρίσκουμε σε αυτό το στάδιο λέγονται B-ομαλοί και είναι σε πλήθος όσοι οι πρώτοι που αποτελούν τη βάση συν ένα.

1.4 Γραμμική ΄Αλγεβρα

Αρχικά φτιάχνουμε έναν πίνακα όπου κάθε γραμμή είναι ένα διάνυσμα των εκθετών όλων των πρώτων modulo 2. Στην συνέχεια φέρνουμε τον πίνακα σε reduced echelon form με την χρήση απαλοιφής του Gauss στο πεδίο GF(2) και βρίσκουμε ποιες γραμμές είναι γραμμικά εξαρτημένες μεταξύ τους.

1.5 Παραγοντοποίηση

Έχοντάς βρει ένα συνδυασμό εξαρτημένων γραμμών από το προηγούμενο βήμα, και έστω $x_1, x_2, .., x_k$) αυτές παίρνουμε την τιμή $x = x_1, x_2, .., x_k \pmod{n}$ και $y = \sqrt{(x_1^2 - n)(x_2^2 - n)...(x_k^2 - n)} \pmod{n}$. Βρίσκουμε το gcd(x-y, n) και αν αυτός έχει τιμή διάφορη από το n και το 1, έχουμε βρει μία παραγοντοποίηση του n.