

Εργασία 2

Κωσταντίνος Σαΐτας - Ζαρκιάς - 2406
Οδυσσεύς Κρυσταλάκος - 2362

26 Απριλίου 2016

Θέμα 1

Θέμα 2

(i)

Υλοποιώντας και χρησιμοποιώντας τον εκτεταμένο αλγόριθμο του Ευκλείδη για την εύρεση του GCD, βρέθηκε:

$$GCD(126048, 5050) = 202$$

$$-1 \cdot 126048 + 25 \cdot 5050 = 202$$

(ii)

Για τον υπολογισμό του αντίστροφου, υπολογίστηκαν όλα τα γινόμενα $809 * i$ όπου i παίρνει τιμές από 1 έως 1000. Βρέθηκε πως ο αντίστροφος είναι το 464.

(iii)

Καθώς το 2^{100} είναι δύσκολο να αποθηκευτεί και να χρησιμοποιηθεί σε πράξεις με ακρίβεια, χρησιμοποιήθηκε μία διαφορετική τεχνική. Υπολογίστηκε το 2 modulo 101 και το αποτέλεσμα πολλαπλασιάστηκε(modulo 101) με το 2. Αυτό έγινε επαναληπτικά 100 φορές και το αποτέλεσμα είναι 464.

(iv)

Ο αλγόριθμος υλοποιήθηκε στο αρχείο fast.py. Τα αποτελέσματα είναι:

$$2^{1234567} \bmod 12345 = 8648$$

$$130^{7654321} \bmod 567 = 319$$

Θέμα 3

Θέμα 4

Θέμα 5

Θέμα 6

Θέμα 7

Θέμα 8

Θέμα 9

(α)

Εφαρμόστηκε το τεστ του Fermat με τις συνθήκες που αναφέρονται στην εκφώνηση. Αυτό που παρατηρείται είναι ότι, κατά προσέγγιση, οι μισοί αριθμοί που παράγονται από την $f(x)$ είναι πρώτοι ενώ οι υπόλοιποι μισοί όχι.

(β)

Τα μόνα πολυώνυμα του Z που, για κάθε ακέραια τιμή, δίνουν πρώτο αριθμό είναι τα σταθερά πολυώνυμα με τιμή κάποιον πρώτο αριθμό.

$$P(x) = p$$

όπου p πρώτος αριθμός

Αντιθέτως, δεν υπάρχει μη σταθερό πολυώνυμο για το οποίο να ισχύει η παραπάνω συνθήκη.

Απόδειξη

Έστω ένα μη σταθερό πολυώνυμο $P(x)$ που μας δίνει πρώτο αριθμό για κάθε τιμή του $x \in Z$

Τότε ισχύει

$$P(1) = p$$

όπου p πρώτος αριθμός.

Επομένως ισχύει και

$$P(1 + np) \equiv 0 \pmod{p}, n \in Z$$

γιατί η παραπάνω τιμή του P διαιρείται με το p . Επομένως, αφού η τιμή του $P(1 + np)$ διαιρείται με το p , δεν είναι πρώτος αριθμός. Άτοπο, άρα η αρχική υπόθεση είναι εσφαλμένη και δεν υπάρχει τέτοιο μη σταθερό πολυώνυμο.