ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Ἐαρινὸ Ἑξάμηνο 2019

Καθηγητὴς Ν. Γ. Τζανάκης

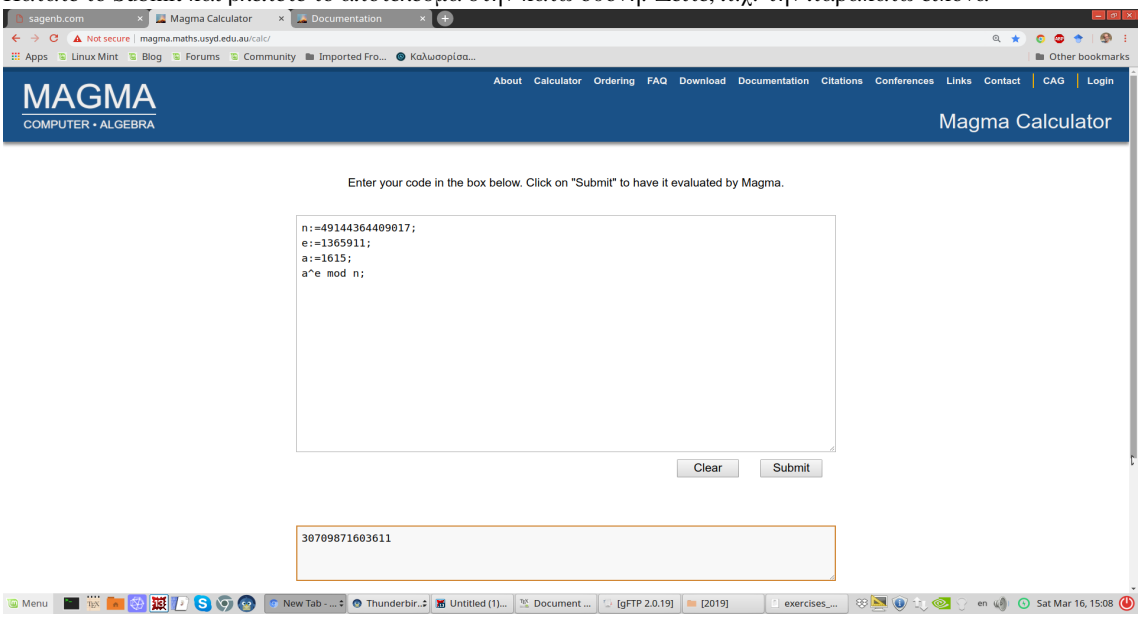
Ἀσκήσεις τῆς $6^{\eta\varsigma}$ ἑβδομάδας

1. Γιὰ ποιὲς ἀπὸ τὶς παρακάτω τριάδες (a, b, m) ἡ ἰσοτιμία $ax \equiv b \pmod m$ ἔχει λύση; Σὲ περίπτωση ποὺ ἡ ἰσοτιμία εἶναι ἐπιλύσιμη, ὑπολογῖστε ὅλες τὶς λύσεις της.

$$(a, b, m) = (15, 33, 168),\ (33, 10, 168),\ (17, 1, 168),\ (17, 1, 462),\ (35, 49, 462).$$

   Ὑπόδειξη-σχόλια. Στὸ μάθημα κάναμε τὶς ἑξῆς δύο ἁπλὲς παρατηρήσεις: (1) Ἂν $(a, m) = 1$ καὶ $x_0 \pmod m$ εἶναι ἡ μοναδικὴ λύση τῆς ἰσοτιμίας $ax \equiv 1 \pmod m$, τότε, γιὰ κάθε b καὶ τὰ ἴδια a, m, ἡ μοναδικὴ λύση τῆς ἰσοτιμίας $ax \equiv b \pmod m$ εἶναι $bx_0 \pmod m$. (2) Γιὰ τὴν ἐπίλυση τῆς ἰσοτιμίας $ax \equiv 1 \pmod m$ ὅταν $(a, m) = 1$, ἀρκεῖ νὰ ἐκφράσομε τὸ 1 ὡς γραμμικὸ συνδυασμὸ τῶν a, m κατὰ τὰ γνωστά, μὲ τὴ βοήθεια τοῦ εὐκλειδείου ἀλγορίθμου.

2. Ἐλέγξτε τὴν ὀρθότητα τοῦ ἀριθμητικοῦ παραδείγματος τῆς ἑνότητας 2.4 τῶν Σημειώσεων κάνοντας τὶς πράξεις μὲ τὴ βοήθεια τοῦ Magma Online Calculator.
   Ὑποδείξεις γιὰ τὴ χρήση του Magma. Γράφετε τὰ δεδομένα σας στὴν πάνω ὀθόνη ὡς ἑξῆς:
   $n := 49144364409017$; $e := 1365911$; κλπ, στὴν ἴδια ἢ σὲ διαφορετικὲς γραμμές. Τὸ ; εἶναι ἀπαραίτητο. Πατᾶτε τὸ Submit καὶ βλέπετε τὸ ἀποτέλεσμα στὴν κάτω ὀθόνη. Δεῖτε, π.χ. τὴν παρακάτω εἰκόνα



3. (α΄) Ἔστω ὅτι, σὲ κρυπτογραφικὸ σύστημα RSA, τὸ δημόσιο κλειδί σας εἶναι $(n, e) = (72731, 2155)$ (ἡ ἀνάλυση τοῦ n σὲ πρώτους εἶναι $72731 = 257 \cdot 283$). Ἡ Α κρυπτογράφησε μὲ αὐτὸ τὸ κλειδί σας ἕνα διψήφιο ἀριθμό, σᾶς τὸν ἔστειλε καὶ ὁ κρυπτογραφημένος ἀριθμὸς ποὺ λάβατε εἶναι ὁ 980. Ἀποκρυπτογραφῆστε τον καὶ βρεῖτε τὸν διψήφιο ἀριθμὸ ποὺ σᾶς ἔστειλε ἡ Α.

(β′) Ἀνάλογο πρόβλημα μὲ τὸ (α′) ἂν $(n, e) = (72731, 2977)$ καὶ τὸ κρυπτογραφημένο μήνυμα ποὺ λάβατε εἶναι τὸ 846.
(γ′) Ἀνάλογο πρόβλημα μὲ τὸ (α′) ἂν $(n, e) = (72731, 9119)$ καὶ τὸ κρυπτογραφημένο μήνυμα ποὺ λάβατε εἶναι τὸ 1055.

Ὑπόδειξη-σχόλια καὶ γιὰ τὰ τρία ἐρωτήματα. Ἀκολουθῆστε τὰ βήματα τῆς ἀποκρυπτογράφησης ποὺ περιγράφονται στὴν ἑνότητα 2.4 τῶν Σημειώσεων. Ὁ ὑπολογισμὸς τοῦ ἀντικλειδιοῦ d ἀπαιτεῖ ἐλάχιστες πράξεις. Τὶς ὑψώσεις σὲ δυνάμεις $\bmod n$ θὰ κάνετε ἀκολουθώντας τὰ βήματα τοῦ ἀλγορίθμου τῆς σελίδας 35 τῶν Σημειώσεων. Ὅλες οἱ πράξεις γίνονται μὲ κομπιουτεράκι τσέπης, ἀρκεῖ νὰ μπορεῖ νὰ ἐμφανίσει 10 ψηφία.