

# A

## ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ

Έαρινό Έξάμηνο 2019

Καθηγητής Ν. Γ. Τζανάκης

Έξεταστική περίοδος Ίουνίου (30 Μαΐου 2019)

1. Άν οί  $a, b$  είναι πρώτοι μεταξύ τους και  $m, n \geq 1$ , δείξτε ότι  $(3a^m + 7b^n, 2a^m + 5b^n) = 1$ . **μον. 1**
2. Αποδείξτε ότι τὸ 11 διαιρεῖ τὸν ἀριθμὸ  $3 \cdot 5^{2n+1} + 2 \cdot 3^{n+2}$  γιὰ κάθε  $n \geq 0$ . **μον. 1.5**
3. Ὑπολογίστε ἓναν ἀκέραιο ἀριθμὸ μεταξύ 800 καὶ 900, ὁ ὁποῖος, διαιρούμενος διὰ 8 ἀφήνει ὑπόλοιπο 7, διαιρούμενος διὰ 9 ἀφήνει ὑπόλοιπο 2, καὶ διαιρούμενος διὰ 11 ἀφήνει ὑπόλοιπο 3. Γιὰ νὰ θεωρηθεῖ σωστὴ ἡ λύση σας **πρέπει νὰ κάνετε, ὅπωςδῆποτε, χρήση τοῦ «Κινέζικου Θεωρήματος Ὑπολοίπων»**. **μον. 1.5**
4. Ὑπολογίστε τὴν τιμὴ τοῦ συμβόλου Jacobi  $\left(\frac{598}{1267}\right)$ . **Δὲν ἐπιτρέπεται ἡ παραγοντοποίηση περιττῶν ἀριθμῶν**. Ἡ μόνη παραγοντοποίηση ποὺ ἐπιτρέπεται εἶναι, ὅταν ἔχετε ἄρτιο ἀριθμὸ, νὰ τὸν γράψετε ὡς γινόμενο δύναμης τοῦ 2 ἐπὶ περιττό. **μον. 1**
5. Πότε δύο λύσεις  $x_1, x_2$  τῆς ἰσοτιμίας  $12^x \equiv 7 \pmod{19}$  θεωροῦνται διαφορετικές; Ὁ παρακάτω πίνακας δίνει τὸν διακριτὸ λογάριθμο  $\text{ind}_a$  ὅλων τῶν  $a = 1, 2, \dots, 18$ . (Ὁ γεννήτορας, ὡς πρὸς τὸν ὁποῖο ἔχει ὑπολογισθεῖ ὁ διακριτὸς λογάριθμος, δὲν σᾶς χρειάζεται.)

$a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{ind}_a$	0	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Ὑπολογίστε ὅλες τὶς διαφορετικὲς λύσεις τῆς παραπάνω ἰσοτιμίας χρησιμοποιώντας αὐτὸν τὸν πίνακα. **Λύση μὲ δοκιμὲς ἀπορρίπτεται!** **μον. 1.5**

6. (α') Ἐστω  $n > 1$ . Ἄν  $(g, n) = 1$  καὶ  $g^d \not\equiv 1 \pmod{n}$  γιὰ κάθε **γνήσιο θετικὸ διαιρέτη**  $d$  τοῦ  $\phi(n)$ , δείξτε ὅτι ὁ  $g$  εἶναι γεννήτορας  $\text{mod } n$ . Μετὰ ἀποδείξτε ὅτι τὸ 5 εἶναι γεννήτορας  $\text{mod } 23$ . **μον. 1**  
(β') Μὲ τὴ βοήθεια **μόνο τῶν ὑπολογισμῶν τοῦ ἐρωτήματος (α')** καὶ τῆς σχέσης  $16 = 2^4$  ὑπολογίστε τὸν διακριτὸ λογάριθμο  $\text{ind}_5(16)$ . Ἐπίσης, **χωρὶς δοκιμὲς** ὑπολογίστε τὴν τάξη  $\text{ord}_{23}(16)$ . **μον. 1**
7. Ἐστω πρώτος  $p \equiv 7 \pmod{20}$ . Ἀποδείξτε ὅτι  $\left(\frac{-5}{p}\right) = +1$ . **μον. 1.5**  
(Ὑπόδειξη: Ὑπολογίστε πρώτα τὶς κλάσεις  $p \pmod{5}$  καὶ  $p \pmod{4}$ .)

### ΟΔΗΓΙΕΣ

- Διάρκεια τῆς ἐξέτασης 2 ὥρες.
- Δὲν ἐπιτρέπεται χρήση κανενὸς εἶδους ἠλεκτρονικῆς συσκευῆς. Οἱ πράξεις γίνονται ἄνετα μὲ τὸ χέρι.
- Δὲν ἐπιτρέπεται νὰ ἔχετε πάνω ἢ δίπλα σας, τσάντα, σημειώσεις, βιβλία, κινητὸ (ἔστω καὶ ἀπενεργοποιημένο) ἢ ἄλλη ἠλεκτρονικὴ συσκευὴ ποὺ μπορεῖ νὰ χρησιμοποιηθεῖ γιὰ ἀντιγραφή. Ὅλα τὰ παραπάνω πρέπει νὰ παραδίδονται στὴν ἔδρα ὑποχρεωτικὰ πρὶν τὴν ἔναρξη τῆς ἐξέτασης.