ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
Τμήμα Μαθηματικών και
Εφαρμοσμένων Μαθηματικών

Μαΐος 2018
Θ. Γαρεφαλάκης

ΘΕΩΡΙΑ ΑΡΙΘΜΩΝ
ΤΕΛΙΚΗ ΕΞΕΤΑΣΗ

Η διάρκεια της εξέτασης είναι 2 ώρες και 15 λεπτά. Φεύγοντας, παραδίνετε τα γραπτά, το πρόχειρο και τα θέματα. Επίσης, δε θα πρέπει να έχετε κοντά σας τσάντα ή κινητό τηλέφωνο (έστω και απενεργοποιημένο).

Θέμα 1 (20 μ.)

1. Έστω $p = 2^n + 1$ πρώτος αριθμός. Δείξτε ότι $n = 2^k$ για κάποιο $k \in \mathbb{N}$.
2. Έστω $p = 2^n - 1$ πρώτος αριθμός. Δείξτε ότι ο n είναι πρώτος.

Θέμα 2 (20 μ.) Ορίζουμε την αριθμητική συνάρτηση

$$f(n) = \sum_{d|n} \mu(d) \cdot d.$$

1. Δείξτε ότι
$$f\left(p_1^{e_1} \cdots p_k^{e_k}\right) = (-1)^k (p_1 - 1) \cdots (p_k - 1).$$
2. Εάν ο n διαιρείται από το p^2 για κάποιο πρώτο p, δείξτε ότι
$$\sum_{d|n} f(d) \cdot \mu\left(\frac{n}{d}\right) = 0.$$

Θέμα 3 (20 μ.) Για κάθε μία από τις παρακάτω ισοτιμίες, εξετάστε εάν έχει λύση. Για όποια ισοτιμία έχει λύση, υπολογίστε όλες τις λύσεις (τις ανισότιμες modulo το αντίστοιχο μέτρο).

$$x^2 \equiv 53 \pmod{101}, \quad x^2 \equiv 11 \pmod{35}.$$

Θέμα 4 (20 μ.) Έστω p, q δίδυμοι πρώτοι (δηλαδή $q = p + 2$). Δείξτε ότι είτε καμία είτε και οι δύο ισοτιμίες

$$x^2 \equiv q \pmod{p}, \;\; x^2 \equiv p \pmod{q}$$

έχουν λύση και δώστε ένα παραδείγμα για κάθε μία από τις δύο περιπτώσεις.

Θέμα 5 (20 μ.) Έστω q περιττός πρώτος αριθμός, τέτοιος ώστε $p = 4q + 1$ είναι επίσης περιττός πρώτος.

1. Δείξτε ότι η ισοτιμία $x^2 \equiv -1 \pmod{p}$ έχει δύο (ανισότιμες modulo p) λύσεις, οι οποίες είναι τετραγωνικά μη υπόλοιπα modulo p.
2. Δείξτε ότι κάθε τετραγωνικό μη υπόλοιπο modulo p, εκτός των δύο λύσεων της παραπάνω ισοτιμίας, είναι πρωταρχικές ρίζες modulo p.