Πανεπιστήμιο Κρήτης, Τμήμα Μαθηματικών **Θεωρία Αριθμών (Μ 202)**

Εξέταση Ιανουαρίου 2010 **Εξεταστής: Δημήτριος Νταής**

ΘΕΩΡΗΤΙΚΑ ΘΕΜΑΤΑ

ΘΕΜΑ 1ο Να διατυπωθεί και να αποδειχθεί το *θεμελιώδες θεώρημα τής Αριθμητικής*.

ΘΕΜΑ 2ο Εάν $n \in \mathbb{N}$, $n \geq 2$, και οι $a_1, \ldots, a_n$ είναι μη μηδενικοί ακέραιοι με

$$|a_1| = p_1^{\alpha_{1,1}} \cdots p_k^{\alpha_{1,k}}, \ldots\ldots, \; |a_n| = p_1^{\alpha_{n,1}} \cdots p_k^{\alpha_{n,k}},$$

όπου οι $p_1, \ldots, p_k$ ($k \in \mathbb{N}$) είναι πρώτοι αριθμοί και οι $\alpha_{j,l}$, $j \in \{1, ..., n\}$, $l \in \{1, ..., k\}$, μη αρνητικοί ακέραιοι αριθμοί, να αποδειχθεί ότι

$$\text{μκδ}(a_1, \ldots, a_n) = \prod_{l=1}^{k} p_l^{\min\{\alpha_{1,l}, \ldots, \alpha_{n,l}\}}.$$

ΘΕΜΑ 3ο Να αποδειχθούν τα εξής:

(i) Δοθέντων ενός $m \in \mathbb{N}$ και δυο ακεραίων a, b, $a \neq 0$, η γραμμική ισοτιμία

$$ax \equiv b (\mathrm{mod}\, m) \qquad (\star)$$

διαθέτει λύσεις $x \in \mathbb{Z}$ κατά μόδιο m εάν και μόνον εάν μκδ $(a, m) | \, b$.

(ii) Όταν μκδ $(a, m) | \, b$, η ισοτιμία $(\star)$ διαθέτει ακριβώς μκδ(a, m) σαφώς διακεκριμένες λύσεις $x \in \mathbb{Z}$ κατά μόδιο m, οι οποίες είναι τής μορφής

$$x = x_0 + k \, \frac{m}{\text{μκδ}\,(a, m)}, \quad k \in \{0, 1, \ldots, \text{μκδ}\,(a, m) - 1\},$$

όπου x_0 μια ειδική λύση τής $(\star)$.

(iii) Μία ειδική λύση τής $(\star)$ είναι η $x_0 := a^{\varphi(m)-1} b$, όπου φ η συνάρτηση τού Euler.

ΘΕΜΑ 4ο Εάν η f είναι μια αριθμητική συνάρτηση και $F(n) := \sum_{d|n} f(d)$ για κάθε $n \in \mathbb{N}$, να αποδειχθούν τα εξής:

(i) Οι τιμές τής f προσδιορίζονται μέσω τού λεγομένου *τύπου αντιστροφής τού Möbius*:

$$f(n) = \sum_{d|n} \mu\,(d)\, F\left(\frac{n}{d}\right),$$

όπου

$$\mu\,(n) := \begin{cases} 1, & \text{όταν } n = 1, \\ 0, & \text{όταν } \exists p \text{ πρώτος: } p^2 \mid n, \\ (-1)^k & \begin{cases} \text{όταν } \nexists p \text{ πρώτος: } p^2 \mid n \text{ και } n = p_1 p_2 \cdots p_k, \\ \text{όπου } k \in \mathbb{N} \text{ και } p_1, \ldots, p_k \text{ (κατ' ανάγκην διακεκριμένοι) πρώτοι,} \end{cases} \end{cases}$$

η συνάρτηση τού Möbius.

(ii) Εάν η F είναι πολλαπλασιαστική, τότε και η f είναι πολλαπλασιαστική.

ΘΕΜΑ 5ο Εάν ο a είναι ένας ακέραιος και ο p ένας περιττός πρώτος αριθμός με μκδ$(a, p) = 1$, τότε το *σύμβολο τού Legendre* είναι το

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{όταν ο } a \text{ είναι τετραγωνικό υπόλοιπο } \mathrm{mod}\, p, \\ -1, & \text{όταν ο } a \text{ δεν είναι τετραγωνικό υπόλοιπο } \mathrm{mod}\, p. \end{cases} \qquad (1)$$

Σύμφωνα με ένα λήμμα τού Euler,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\operatorname{mod} p), \tag{2}$$

και, σύμφωνα με ένα λήμμα τού Gauss,

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{2ai}{p} \right\rfloor}, \tag{3}$$

(όπου $\lfloor x \rfloor := \max\{m \in \mathbb{Z} | \, m \leq x\}$ για οιονδήποτε $x \in \mathbb{Q}$). Με τη βοήθεια των (1), (2) και (3) να αποδειχθούν τα ακόλουθα:

(i) Για κάθε περιττό πρώτο αριθμό p και $a_1, a_2 \in \mathbb{Z}$, όπου μκδ$(a_1, p) =$ μκδ$(a_2, p) = 1$ και $a_1 \equiv a_2 (\operatorname{mod} p)$, ισχύουν οι ισότητες

$$\left(\frac{1}{p}\right) = 1 \;\; \text{και} \;\; \left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right).$$

(ii) Για κάθε περιττό πρώτο αριθμό p και $a_1, \ldots, a_k \in \mathbb{Z}$, όπου $k \in \mathbb{N}$, $k \geq 2$, και μκδ$(a_j, p) = 1$, $\forall j \in \{1, \ldots, k\}$, ισχύει η ισότητα

$$\left(\frac{a_1 a_2 \cdots a_k}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \cdots \left(\frac{a_k}{p}\right).$$

(iii) Για κάθε περιττό πρώτο αριθμό p ισχύει η ισότητα

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

ΘΕΜΑΤΑ ΣΧΕΤΙΖΟΜΕΝΑ ΜΕ ΤΙΣ ΕΦΑΡΜΟΓΕΣ

ΘΕΜΑ 6ο Εάν $a, b, c \in \mathbb{Z} \setminus \{0\}$, να αποδειχθεί ότι

$$\frac{\text{μκδ}(a,b)\text{μκδ}(b,c)\text{μκδ}(c,a)}{\text{μκδ}(a,b,c)^2} = \frac{\text{εκπ}(a,b)\text{εκπ}(b,c)\text{εκπ}(c,a)}{\text{εκπ}(a,b,c)^2}.$$

ΘΕΜΑ 7ο (i) Εάν οι p, q είναι περιττοί πρώτοι με $p \neq q$, και a ένας ακέραιος για τον οποίο ισχύει μκδ$(a, pq) = 1$, να αποδειχθεί ότι

$$a^{\frac{\varphi(pq)}{2}} \equiv 1 \, (\operatorname{mod} pq).$$

(ii) Να προσδιορισθούν οι λύσεις τής γραμμικής ισοτιμίας

$$6x \equiv 3 (\operatorname{mod} 21).$$

ΘΕΜΑ 8ο (i) Εάν ο p είναι ένας πρώτος αριθμός, να αποδειχθεί ότι για κάθε φυσικό αριθμό $n < p$ αληθεύει η ισοτιμία

$$(n-1)!(p-n)! \equiv (-1)^n (\operatorname{mod} p).$$

(ii) Να προσδιορισθεί ο μκδ$(n! + 1, (n + 1)!)$ για οιονδήποτε φυσικό αριθμό n.

<u>ΘΕΜΑ 9ο</u> Εάν ως φ, μ συμβολισθούν οι συναρτήσεις των Euler και Möbius, αντιστοίχως, να αποδειχθεί ότι για κάθε φυσικό αριθμό n ισχύουν οι ισότητες

$$\sum_{d|n} \frac{\mu\left(d\right)^2}{\varphi\left(d\right)} = \frac{n}{\varphi\left(n\right)} \quad \text{και} \quad \sum_{d|n} \mu\left(d\right)\varphi\left(d\right) = \prod_{p|n}\left(2-p\right),$$

όπου ο d διατρέχει τους φυσικούς αριθμούς και ο p τους πρώτους αριθμούς που διαιρούν τον n.

<u>ΘΕΜΑ 10ο</u> Να προσδιορισθεί η τιμή τού συμβόλου τού Legendre $\left(\frac{3}{p}\right)$ για οιονδήποτε πρώτο αριθμό $p > 3$.

- **Να απαντηθούν το πολύ 3 θέματα ανήκοντα σε μία εκ των δύο παρατιθέμενων κατηγοριών θεμάτων και το πολύ 2 θέματα ανήκοντα στην άλλη.**
- **Κάθε ορθώς απαντηθέν θέμα θα λαμβάνει 2 μονάδες**.
- **Κατά τη διάρκεια τής εξετάσεως οι σημειώσεις θα παραμείνουν κλειστές.**
- **Εντός τού γραπτού οι εξεταζόμενοι οφείλουν να αναγράφουν ρητώς σε ποιο εκ των δοθέντων θεμάτων απαντούν.**
- **Η χρήση πολύ δυσανάγνωστης γραφής ή/και μη αναγνωρίσιμων μαθηματικών συμβόλων ενδέχεται να οδηγήσει σε μείωση τού βαθμού (λόγω αδυναμίας διορθώσεως εκ μέρους τού εξεταστού).**
- **Κατά τη διάρκεια τής εξετάσεως δεν επιτρέπονται συζητήσεις μεταξύ των εξεταζομένων, αντιγραφή ή αδικαιολόγητη υπέρβαση τού ορισθέντος χρόνου για την απάντηση των θεμάτων. (Κάτι τέτοιο θα είχε ως συνέπεια ειδική μονογραφή σημάνσεως τού γραπτού και συνακόλουθο μηδενισμό του.)**

ΚΑΛΗ ΕΠΙΤΥΧΙΑ!