Τμήμα Μαθηματικών ΕΚΠΑ
Θεωρία Αριθμών 532
18 Σεπτεμβρίου 2017
Ομάδα Α

1. (3,-1) Έστω a, m θετικοί ακέραιοι. Αν ισχύει $a^m \neq a \mod m$ τότε ο m είναι σύνθετος.

    - Σ, Λ

2. (3,-1) Έστω p πρώτος αριθμός τέτοιος ώστε $p \equiv (-1) \mod 4$. Τότε ισχύει $x^2 \equiv (p-1) \mod p$.

    - Σ, Λ

3. (3,-3) Ο Ερατοσθένης όρισε πρώτος στην ιστορία της ανθρωπότητας τους πρώτους αριθμούς.

    - Σ, Λ

4. (3,-2) Ισχύει $-65 \equiv 3 \mod 6$.

    - Σ, Λ

5. (3,-2) Το σύνολο $\{15, 24, -3, -22, -11\}$ είναι ένα πλήρες σύστημα υπολοίπων *modulo* 5.

    - Σ, Λ

6. (5) Να βρεθεί ο $\mu.\kappa.\delta.(1769, 2378)$ και να εκφραστεί ως γραμμικός συνδυασμός αυτών.

7. (5) Έστω x, y ακέραιοι τέτοιοι ώστε $\mu.\kappa.\delta.(x, 3) = \mu.\kappa.\delta.(y, 3) = 1$. Να δείξετε ότι ο θετικός ακέραιος $x^2 + y^2$ δεν είναι τέλειο τετράγωνο.

8. (5) Έστω α ακέραιος. Να δείξετε ότι $\alpha^{21} \equiv \alpha \mod 15$.

9. (5) Να βρεθούν όλες οι αρχικές ρίζες $\mod 17$.

10. (5) Έστω **P** το σύνολο των πρώτων αριθμών. Θεωρήστε ότι ο ακέραιος αριθμός 1 ανήκει στο **P**. Υπάρχουν άπειροι πρώτοι οι οποίοι ανήκουν στο **P**; Δικαιολογήστε την απάντησή σας.

11. (7) Να λυθεί η γραμμική ισοδυναμία $30x \equiv 12 \mod 102$.

12. (7) Να βρεθούν, εάν υπάρχουν, οι λύσεις της ισοδυναμίας $x^2 \equiv 257 \mod 269$.

13. (7) Να βρεθούν οι περιττοί πρώτοι p ώστε $x^2 \equiv (-7) \mod p$.

14. (11) Να λυθεί η πολυωνυμική ισοδυναμία $7x^4 + 19x + 25 \equiv 0 \mod 135$.

15. (11) Να λυθεί η διοφαντική εξίσωση $101x + 37y = 3819$ και στη συνέχεια να βρεθούν οι θετικές της λύσεις.

16. (13)* Να ορίσετε τους τύπους που προκύπτουν από τα μοτίβα τα οποία υπάρχουν στον παρακάτω πίνακα για το σύμβολο *Legendre* $(\frac{q}{p})$.

$p \setminus q$	3	5	7	11	13	17	19
3		$\heartsuit$	$\sharp$	$\sharp$	$\heartsuit$	$\heartsuit$	$\sharp$
5	$\heartsuit$		$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
7	$\sharp$	$\heartsuit$		$\sharp$	$\heartsuit$	$\heartsuit$	$\sharp$
11	$\sharp$	$\heartsuit$	$\sharp$		$\heartsuit$	$\heartsuit$	$\sharp$
13	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$		$\heartsuit$	$\heartsuit$
17	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$		$\heartsuit$
19	$\sharp$	$\heartsuit$	$\sharp$	$\sharp$	$\heartsuit$	$\heartsuit$	

17. (17)* Έστω $\Phi = (1+\sqrt{5})/2$ και n το πλήθος των βημάτων όπου χρειάζεται για να τερματίσει ο Ευκλείδειος Αλγόριθμος κατά τη διάρκεια υπολογισμού του Μέγιστου Κοινού Διαιρέτη d των $(a,\ b) = (r_0,\ r_1)$. Να δείξετε ότι :
(i) για κάθε $k = 0, 1, ..., n$ ισχύει

$$r_{n-k} \geq \Phi^k,$$

όπου r_{n-k} το υπόλοιπο του $n-k-1$ βήματος του Ευκλειδείου Αλγορίθμου
(ii) ισχύει

$$n \leq \frac{\log b}{\log \Phi} + 1.$$

Υπόδειξη: Θεωρήστε γνωστή την σχέση $\Phi = 1 + \frac{1}{\Phi}$.

Σύνολο μονάδων: 113.
Τα θέματα με το διακριτικό * είναι υποχρεωτικά.
Διάρκεια εξέτασης 179 λεπτά.
Καλή επιτυχία.