ΜΑΘΗΜΑΤΙΚΑ ΠΛΗΡΟΦΟΡΙΚΗΣ και ΤΗΛΕΠΙΚΟΙΝΩΝΙΏΝ

Εξέταση 14 Σεπτεμβρίου 2005

ΟΔΗΓΙΕΣ: ΔΙΑΒΑΣΤΕ ΠΡΟΣΕΚΤΙΚΑ

- Λύστε όλα τα θέματα. Η βαθμολογία είναι 50-50% για τα δυο μέρη (ένα για κάθε διδάσκοντα). Οι απαντήσεις σας να είναι σαφείς και σύντομες. Μακροσκελείς απαντήσεις κινδυνεύουν να πάρουν μικρό βαθμό.
- Σας έχουν δοθεί 3 κόλλες. Η πρώτη για το μέρος Α, η δεύτερη για το μερος Β και η τρίτη για πρόχειρο. Γράψτε πριν αρχίσει η εξέταση (δηλαδή τώρα!) το όνομα σας σε κάθε κόλλα που σας έχει δοθεί. Γράψτε στην πρώτη κόλλα 'ΜΕΡΟΣ Α', στη δεύτερη κόλλα 'ΜΕΡΟΣ Β' και στην τρίτη κόλλα 'ΠΡΌΧΕΙΡΟ'. Οι επιτηρητές θα περάσουν να το ελέγξουν. Είναι σημαντικό να ακολουθήσετε τις οδηγίες για να μας διευκολύνετε και να βαθμολογηθεί σωστά το γραπτό σας.
- Γράψτε πάνω στα θέματα το όνομά σας. Πρέπει να τα επιστρέψετε με όλες τις κόλλες (και το πρόχειρο). Τα θέματα θα αναρτηθούν στη σελίδα του μαθήματος.
- Δεν επιτρέπονται σημειώσεις, βιβλία, αριθμομηχανές, κλπ. Απομακρύνετε τα κινητά σας.
- Αντιγραφή συνεπάγεται μηδενισμό για **όλους** τους συμμετέχοντες.
- Μπορείτε να σημειώσετε πάνω στο γραπτό σας αν επιθυμείτε να μην περαστεί η βαθμολογία σας όταν είναι κάτω από κάποιο ελάχιστο. Οι διδάσκοντες επιφυλάσσονται για το αν θα δεχθούν τέτοιο αίτημα.

ΜΕΡΟΣ Α': ΜΑΘΗΜΑΤΙΚΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
Διδάσκων: Η.Κουτσουπιάς

1. **[50%]** Θεωρήστε το υποσύνολο T των φυσικών αριθμών που ορίζεται με τον εξής αναδρομικό ορισμό:

- $1 \in T$.
- Αν $n \in T$, τότε $2n \in T$.
- Αν $n \in T$, τότε $n + 3 \in T$.

1. Δώστε τα 10 μικρότερα στοιχεία του συνόλου T;
2. Αποδείξτε προσεκτικά ότι το σύνολο T είναι το

$$\{3k + a \,:\, k \in \mathbb{N} \text{ και } a = 1, 2\}.$$

2. **[40%]** Έστω ότι έχουμε ένα πιθανοτικό αλγόριθμο A που για κάθε είσοδο x:

- Αν η σωστή απάντηση για την είσοδο x είναι 'ναι', τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά 'ναι') με πιθανότητα $1/2$.
- Αν η σωστή απάντηση για την είσοδο x είναι 'όχι', τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά 'όχι') με πιθανότητα $9/10$.

Πως μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο A ώστε να κατασκευάσουμε ένα αλγόριθμο που δίνει την σωστή απάντηση—ανεξάρτητα αν η σωστή απάντηση είναι 'ναι' ή 'όχι'—με πιθανότητα τουλάχιστον $3/4$;

3. [10%] Κάποιος που θέλει να 'σπάσει' ένα σύστημα RSA κατάφερε να βρει ένα κατάσκοπο και με πολλές προσπάθειες να αποκτήσει ένα αποκρυπτογραφημένο μήνυμα του συστήματος. Έχει λοιπόν στη διάθεση του ένα μήνυμα στην κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή. Ελπίζει ότι με αυτή την πληροφορία θα καταφέρει να 'σπάσει' το σύστημα και να μπορεί να αποκρυπτογραφεί κάθε μήνυμα γρήγορα· χωρίς τη βοήθεια του κατασκόπου φυσικά. Τι λέτε, μπορεί; Εξηγείστε.

Υποθέστε βέβαια ότι το σύστημα RSA χρησιμοποιεί πάντα τα ίδια ιδιωτικά και δημόσια κλειδιά.

ΜΕΡΟΣ Β': ΣΤΟΙΧΕΙΑ ΣΥΝΗΘΩΝ ΔΙΑΦΟΡΙΚΩΝ ΕΞΙΣΩΣΕΩΝ ΚΑΙ ΜΙΓΑΔΙΚΗΣ ΑΝΑΛΥΣΗΣ

Διδάσκων: Ι. Στρατής

1. (α) Να λυθεί η δ.ε. $y' = \frac{t+y}{t-y}$.

(β) Να δειχθεί, με τη μέθοδο των ολοκληρωτικών υπολοίπων, ότι

$$I = \int_0^\infty \frac{2x^2-1}{x^4+5x^2+4}dx = \frac{\pi}{4}.$$

2. (α) Να λυθεί η δ.ε. $\boldsymbol{y}'(t) = A\boldsymbol{y}(t)$, όπου

$$A = \begin{bmatrix} -1 & -1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & -1 \end{bmatrix}.$$

(β) Να υπολογισθεί το $\int_C \overline{z}\,dz$ όπου C ο θετικά προσανατολισμένος μοναδιαίος κύκλος του μιγαδικού επιπέδου.

ΜΑΘΗΜΑΤΙΚΑ ΠΛΗΡΟΦΟΡΙΚΗΣ και ΤΗΛΕΠΙΚΟΙΝΩΝΙΏΝ
ΜΕΡΟΣ Α΄: ΜΑΘΗΜΑΤΙΚΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
Διδάσκων: Η.Κουτσουπιάς
Λύσεις εξέτασης 14 Σεπτεμβρίου 2005

Πρόβλημα 1. Θεωρήστε το υποσύνολο T των φυσικών αριθμών που ορίζεται με τον εξής αναδρομικό ορισμό:

- $1 \in T$.
- Αν $n \in T$, τότε $2n \in T$.
- Αν $n \in T$, τότε $n + 3 \in T$.

1. Δώστε τα 10 μικρότερα στοιχεία του συνόλου T;
2. Αποδείξτε προσεκτικά ότι το σύνολο T είναι το

$$\{3k + a \ : \ k \in \mathbb{N} \text{ και } a = 1, 2\}.$$

Λύση. Τα 10 μικρότερα στοιχεία του συνόλου T είναι 1,2,4,5,7,8,10,11,13,14.

Ας ορίσουμε το σύνολο $S = \{3k + a \ : \ k \in \mathbb{N} \text{ και } a = 1, 2\}$. Θέλουμε να δείξουμε ότι $T = S$. Για να το δείξουμε αυτό θα δείξουμε ότι $T \subseteq S$ και ότι $S \subseteq T$.

Πρόταση 1. *Κάθε στοιχείο του συνόλου T είναι της μορφής $3k+1$ ή της μορφής $3k + 2$, για κάποιο φυσικό αριθμό k. Ισοδύναμα, τα στοιχεία του συνόλου T δεν διαιρούνται με το 3.*

Απόδειξη. Με δομική επαγωγή.

Βάση δομικής επαγωγής: Το 1 προφανώς δεν διαιρείται με το 3 (είναι της μορφής $3k + 1$).

Επαγωγικό βήμα: Έστω $m \in T$. Από την επαγωγική υπόθεση το m δεν διαιρείται με το 3. Αρκεί να δείξουμε ότι τα $2m$ και $m + 3$ δεν διαιρούνται με το 3. Αλλά αυτό είναι σχεδόν προφανές (γιατι $\gcd(2m, 3) = \gcd(m, 3)$ και $\gcd(m + 3, 3) = \gcd(m, 3)$).

Η απόδειξη τελείωσε αλλά αν θέλουμε μια εξαντλητική λύση μπορούμε να σκεφτούμε ως εξής:

- αν $m = 3k + 1$ τότε $2m = 3(2k) + 2$ και $m + 3 = 3(k + 1) + 1$ που είναι της κατάλληλης μορφής.
- αν $m = 3k + 2$ τότε $2m = 3(2k + 1) + 1$ και $m + 3 = 3(k + 1) + 1$ που είναι επίσης της κατάλληλης μορφής.

□

Θα δείξουμε τώρα το αντίστροφο:

Πρόταση 2. *Κάθε φυσικός που δεν διαιρείται με το 3 μπορεί να παραχθεί με τους κανόνες που ορίζουν το σύνολο T.*

Απόδειξη. Ας θεωρήσουμε ένα φυσικό αριθμό m της μορφής $3k+1$. Αυτός μπορεί να παραχθεί με μια εφαρμογή του πρώτου κανόνα (που μας δίνει 1) και στη συνέχεια k εφαρμογές του τρίτου κανόνα (που μας δίνει $1+3+3+\cdots+3 = 1+3k$).

Ας θεωρήσουμε τώρα ένα φυσικό αριθμό m της μορφής $3k+2$. Αυτός μπορεί να παραχθεί με μια εφαρμογή του πρώτου κανόνα (που μας δίνει 1), μια εφαρμογή του δεύτερου κανόνα (που μας δίνει 2) και στη συνέχεια k εφαρμογές του τρίτου κανόνα (που μας δίνει $2+3+3+\cdots+3 = 2+3k$).

Στη συνέχεια δίνω μια εναλλακτική απόδειξη με μαθηματική επαγωγή.

Βάση επαγωγής: Το 1 και το 2 παράγονται με τους κανόνες (το 1 με τον πρώτο κανόνα και το 2 με χρήση του δεύτερου κανόνα).

Επαγωγικό βήμα: Ας θεωρήσουμε τώρα ένα φυσικό $m > 3$ που δεν διαιρείται με το 3. Η επαγωγική υπόθεση λέει ότι κάθε φυσικός μικρότερος του m που δεν διαιρείται με το 3 μπορεί να παραχθεί από τους κανόνες που ορίζουν το σύνολο T. Ειδικότερα ο $m-3$ είναι φυσικός γιατί $m-3 \geq 0$ και δεν διαιρείται με το 3, αφού υποθέσαμε ότι ο m δεν είναι πολλαπλάσιο του 3. Άρα μπορεί να παραχθεί με του κανόνες. Αλλά τότε με εφαρμογή του τρίτου κανόνα και ο $(m-3)+3 = m$ παράγεται με τους κανόνες. □

Πρόβλημα 2. Έστω ότι έχουμε ένα πιθανοτικό αλγόριθμο A που για κάθε είσοδο x:

- Αν η σωστή απάντηση για την είσοδο x είναι 'ναι', τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά 'ναι') με πιθανότητα $1/2$.
- Αν η σωστή απάντηση για την είσοδο x είναι 'όχι', τότε ο αλγόριθμος απαντά σωστά (δηλαδή απαντά 'όχι') με πιθανότητα $9/10$.

Πως μπορούμε να χρησιμοποιήσουμε τον αλγόριθμο A ώστε να κατασκευάσουμε ένα αλγόριθμο που δίνει την σωστή απάντηση—ανεξάρτητα αν η σωστή απάντηση είναι 'ναι' ή 'όχι'—με πιθανότητα τουλάχιστον $3/4$;

Λύση. Η απάντηση είναι πολύ απλή: Τρέχουμε τον αλγόριθμο A με είσοδο x δυο φορές: Απαντάμε 'όχι' αν και μόνο αν η απάντηση που πήραμε και τις δυο φορές είναι 'όχι'. Αλλιώς απαντάμε 'ναι'.

Γιατί είναι σωστή αυτή η λύση; Ας εισάγουμε λίγο συμβολισμό για να είμαστε πιο σαφείς. Θα χρησιμοποιήσουμε την αντιστοιχία

$$0 = \text{όχι} \qquad 1 = \text{ναι}.$$

Έστω $f(x)$ συμβολίζει τη σωστή απάντηση για την είσοδο x, και έστω ότι $A_1(x)$ και $A_2(x)$ συμβολίζουν τα αποτελέσματα που παίρνουμε όταν τρέχουμε τον αλγόριθμο A με είσοδο x δυο φορές. Οι $A_1(x)$ και $A_2(x)$ είναι τυχαίες μεταβλητές.

Τότε από την εκφώνηση έχουμε

$$\Pr[A_1(x) = 0] = \Pr[A_2(x) = 0] = \begin{cases} 9/10 & \text{αν } f(x) = 0 \\ 1/2 & \text{αν } f(x) = 1 \end{cases}$$

και

$$\Pr[A_1(x) = 1] = \Pr[A_2(x) = 1] = \begin{cases} 1/10 & \text{αν } f(x) = 0 \\ 1/2 & \text{αν } f(x) = 1 \end{cases}$$

Στον παρακάτω πίνακα η πρώτη στήλη έχει το αποτέλεσμα των δυο εκτελέσεων του αλγόριθμου A. Η δεύτερη και τρίτη στήλη έχει την πιθανότητα να συμβεί το αντίστοιχο γεγονός της πρώτης στήλης όταν η σωστή απάντηση είναι 0 και 1 αντίστοιχα.

$A_1(x)A_2(x)$	$f(x) = 0$		$f(x) = 1$	
00	$\frac{9}{10}\frac{9}{10}$	$\surd$	$\frac{1}{2}\frac{1}{2}$	
01	$\frac{9}{10}\frac{1}{10}$		$\frac{1}{2}\frac{1}{2}$	$\surd$
10	$\frac{1}{10}\frac{9}{10}$		$\frac{1}{2}\frac{1}{2}$	$\surd$
11	$\frac{1}{10}\frac{1}{10}$		$\frac{1}{2}\frac{1}{2}$	$\surd$

Αν η σωστή απάντηση είναι 0 (δηλαδή αν $f(x) = 0$) τότε η πιθανότητα να δώσουμε απάντηση 0 είναι $81/100 \geq 3/4$ (αυτή είναι η πιθανότητα να έρθουν δυο 0). Αν η σωστή απάντηση είναι 1 (δηλαδή αν $f(x) = 1$) τότε η πιθανότητα να δώσουμε απάντηση 1 είναι $1/4+1/4/1/4 \geq 3/4$ (αυτή είναι η πιθανότητα να μην έρθουν δυο 0). Και στις δυο περιπτώσεις η πιθανότητα ορθής απάντησης είναι τουλάχιστον $3/4$.

Πρόβλημα 3. Κάποιος που θέλει να 'σπάσει' ένα σύστημα RSA κατάφερε να βρει ένα κατάσκοπο και με πολλές προσπάθειες να αποκτήσει ένα αποκρυπτογραφημένο μήνυμα του συστήματος. Έχει λοιπόν στη διάθεση του ένα μήνυμα στην κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή. Ελπίζει ότι με αυτή την πληροφορία θα καταφέρει να 'σπάσει' το σύστημα και να μπορεί να αποκρυπτογραφεί κάθε μήνυμα γρήγορα· χωρίς τη βοήθεια του κατασκόπου φυσικά. Τι λέτε, μπορεί; Εξηγείστε.

Υποθέστε βέβαια ότι το σύστημα RSA χρησιμοποιεί πάντα τα ίδια ιδιωτικά και δημόσια κλειδιά.

Λύση. Το γεγονός ότι γνωρίζει ένα μήνυμα στην κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή δεν βοηθάει. Ο κατάσκοπος έδωσε κάποια πληροφορία που μπορούσε να αποκτήσει οποιοσδήποτε: ο τρόπος κωδικοποίησης είναι δημόσιος, γνωστός δηλαδή σε όλους. Θα μπορούσε λοιπόν κάποιος να πάρει οποιοδήποτε μήνυμα και να το κρυπτογραφήσει. Έτσι θα γνωρίζει και την κρυπτογραφημένη και στην αποκρυπτογραφημένη μορφή του.

Ας σημειωθεί ότι η απάντηση ισχύει για κάθε σύστημα δημόσιου κλειδιού, όχι μόνο για το RSA.

ΜΑΘΗΜΑΤΙΚΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΛΥΣΕΙΣ ΤΩΝ ΘΕΜΑΤΩΝ ΤΟΥ Β΄ ΜΕΡΟΥΣ ΤΗΣ ΕΞΕΤΑΣΗΣ ΣΕΠΤΕΜΒΡΙΟΥ 2005

Ι. ΣΤΡΑΤΗΣ

1. (α) Να λυθεί η δ.ε. $y' = \dfrac{t+y}{t-y}$

Λύση

Οι συναρτήσεις $t+y$ και $t-y$ είναι ομογενείς πρώτου βαθμού.

Ο μετασχηματισμός $v = \dfrac{y}{t}$, $t \neq 0$ μετατρέπει τη δ.ε. σε χωριζομένων μεταβλητών. Πράγματι

$$y = vt \Rightarrow \frac{t+y}{t-y} = \frac{1+v}{1-v}, \quad t \neq 0,$$

και

$$y' = v + tv',$$

οπότε η αρχική δ.ε. γίνεται

$$v + tv' = \frac{1+v}{1-v}$$

Ολοκληρώνουμε

$$\int \left(\frac{1}{1+v^2} - \frac{v}{1+v^2} \right) dv = \int \frac{dt}{t}$$

και έχουμε

$$\arctan v - \frac{1}{2} \ln(1+v^2) = \ln|t| + c_1$$

απ' όπου

$$2\arctan v = \ln t^2 (1+v^2) + c \qquad (c = 2c_1)$$

και, επιστρέφοντας στις αρχικές μας μεταβλητές, έχουμε τη λύση σε πεπλεγμένη μορφή

$$2\arctan \frac{y}{t} = \ln(t^2+y^2) + c \quad , t \neq 0.$$

---

1. (β) Να δειχθεί, με τη μέθοδο των ολοκληρωτικών υπολοίπων, ότι

$$I = \int_0^\infty \frac{2x^2-1}{x^4+5x^2+4} dx = \frac{\pi}{4}.$$

Λύση

Αρχικά παρατηρούμε ότι

$$I = \frac{1}{2} \int_{-\infty}^{\infty} \frac{2x^2-1}{x^4+5x^2+4} dx$$

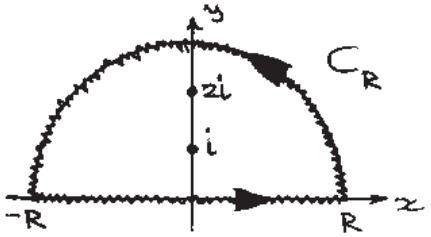
Ορίζουμε

$$f(z) := \frac{2z^2-1}{z^4+5z^2+4}$$

Η $f(z)$ έχει απλούς πόλους στα σημεία

$$z_1 = i \ , \ z_2 = -i \ , \ z_3 = 2i \ , \ z_4 = -2i .$$

Έστω $R > 2$ και C_R η κλειστή καμπύλη του σχήματος.



Γνωρίζουμε ότι αν P και Q είναι πολυώνυμα με $Q \not\equiv 0$ στο $\mathbb{R}$ και $\deg Q \geq \deg P + 2$, τότε

$$\int_{-\infty}^{\infty} \frac{P(x)}{Q(x)} dx = 2\pi i \sum_{k} \operatorname{Res}\left(\frac{P}{Q}; z_k\right),$$

όπου z_k οι ρίζες του Q στο άνω ημιεπίπεδο.

Έτσι

$$I = \frac{1}{2} 2\pi i \left\{ \operatorname{Res}\left(f(z); z_1\right) + \operatorname{Res}\left(f(z); z_3\right) \right\}$$

αφού μόνο οι $z_1 = i$ και $z_3 = 2i$ βρίσκονται στο άνω ημιεπίπεδο.

Έχουμε

$$\operatorname{Res}\left(f(z); z_1\right) = \lim_{z \to i} (z - i) f(z) = \frac{i}{2}$$

$$\operatorname{Res}\left(f(z); z_3\right) = \lim_{z \to 2i} (z - 2i) f(z) = -\frac{3i}{4}$$

απ' όπου τελικά έπεται ότι

$$I = \frac{\pi}{4} .$$

2. (a) Να λυθεί η δ.ε. $\underset{\sim}{y}'(t) = A\,\underset{\sim}{y}(t)$, όπου

$$A = \begin{pmatrix} -1 & -1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix}.$$

Λύση

Ο Α έχει ιδιοτιμή το $\lambda = -1$ με αλγεβρική πολλαπλότητα 3.

Το αντίστοιχο ιδιοδιάνυσμα που αντιστοιχεί στην λ είναι το

$$\underset{\sim}{v}_1 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}.$$

Το γενικευμένο ιδιοδιάνυσμα $1^{ης}$ τάξης είναι το

$$\underset{\sim}{v}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

ενώ το γενικευμένο ιδιοδιάνυσμα $2^{ης}$ τάξης είναι το

$$\underset{\sim}{v}_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Οι αντίστοιχες λύσεις της δ.ε. είναι

$$\underset{\sim}{y}_1(t) = e^{-t}\,\underset{\sim}{v}_1 = e^{-t}\begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$$

$$\underset{\sim}{y}_2(t) = e^{-t}\left(t\,\underset{\sim}{v}_1 + \underset{\sim}{v}_2\right) = e^{-t}\begin{pmatrix} -t \\ 1 \\ t \end{pmatrix}$$

$$\underset{\sim}{y}_3(t) = e^{-t}\left(t^2\,\underset{\sim}{v}_1 + 2t\,\underset{\sim}{v}_2 + 2\,\underset{\sim}{v}_3\right) = e^{-t}\begin{pmatrix} 2-t^2 \\ 2t \\ t^2 \end{pmatrix}$$

και η γενική λύση της δ.ε. είναι

$$\underset{\sim}{y}(t) = c_1\,\underset{\sim}{y}_1(t) + c_2\,\underset{\sim}{y}_2(t) + c_3\,\underset{\sim}{y}_3(t), \quad c_1, c_2, c_3 \text{ σταθ.}$$

2. (β) Να υπολογιστεί το $\int_C \bar{z}\,dz$, όπου C ο δεξιά προσανατολισμένος μοναδιαίος κύκλος του μιγαδικού επιπέδου.

Λύση

Επί του $C: |z| = 1$ έχουμε

$z = e^{i\theta}$, $\theta \in [0, 2\pi]$

οπότε

$\bar{z} = e^{-i\theta}$ και $dz = ie^{i\theta}d\theta$.

Έτσι

$$\int_C \bar{z}\,dz = \int_0^{2\pi} e^{-i\theta} \cdot ie^{i\theta}\,d\theta = i\int_0^{2\pi} d\theta = 2\pi i$$