Πανεπιστημιο Κρητης — Τμημα Μαθηματικων
Θεωρια Αριθμων — Εαρινο Εξαμηνο 2012–13

Μάνος Λυδάκης 29 Μαίου 2013

Διάλεξη 1: Διαιρετότητα, διαιρέτες, πολλαπλάσια, στοιχειώδεις ιδιότητες. Θεωρήσαμε το σύνολο $< a >$ των πολλαπλασίων του a. Θεωρήσαμε και τα S που είναι τα σύνολα ακεραίων που είναι κλειστά ως προς το 0, το $-$, και το $+$. Είδαμε ότι κάθε $< a >$ είναι ένα από αυτά τα S.

Διάλεξη 2: Κάθε S όπως παραπάνω είναι ένα από τα $< a >$. Κοινά Πολλαπλάσια (ΚΠ) και το Ελάχιστο Κοινό Πολλαπλάσιο (ΕΚΠ), το ΕΚΠ διαιρεί κάθε ΚΠ. Μετά θεωρήσαμε ακόμη περισσότερα S από πριν, δηλαδή, δεδομένων ακεραίων $a_1, \ldots, a_n$, θεωρήσαμε το σύνολο S των Γραμμικών Συνδυασμών (ΓΣ) αυτών των ακεραίων. Αυτό το S το συμβολίσαμε με $< a_1, \ldots, a_n >$, και, αν $n = 1$, είναι το ίδιο με το $< a_1 >$ της προηγούμενης διάλεξης. Γενικότερα, για $n \geq 1$, το S αποτελείται από τους ΓΣ των $a_1, \ldots, a_n$, όπου για μας αυτοί οι «ΓΣ» είναι οι ακέραιοι c που γράφονται στη μορφή $c = m_1 a_1 + \cdots + m_n a_n$ (με $m_1, \ldots, m_n \in \mathbb{Z}$). Αποδείξαμε ότι και αυτά τα S είναι κλειστά ως προς το 0, το $-$, και το $+$. Κοινοί Διαιρέτες (ΚΔ), ο Μέγιστος Κοινός Διαιρέτης (ΜΚΔ), «ΚΔ+ΓΣ⇔ΜΚΔ», ο ΜΚΔ διαιρείται από κάθε ΚΔ, «$\text{ΜΚΔ}(ca, cb) = c \cdot \text{ΜΚΔ}(a, b)$».

Διάλεξη 3: «$\text{ΜΚΔ}(\frac{a}{c}, \frac{b}{c}) = \frac{1}{c}\text{ΜΚΔ}(a, b)$», σχέση μεταξύ ΕΚΠ και ΜΚΔ, ο Ευκλείδειος Αλγόριθμος, πρώτοι και σχετικά πρώτοι αριθμοί, το Λήμμα του Ευκλείδη, κάθε αριθμός μεγαλύτερος του 1 έχει κάποιο πρώτο διαιρέτη.

Διάλεξη 4: Υπάρχουν άπειροι πρώτοι, το Κόσκινο του Ερατοσθένη, σύντομα σχόλια πάνω στη συνάρτηση $p(n)$ (όπου το σύνολο $\mathbb{P}$ των πρώτων είναι $\{p(1) < p(2) < p(3) < \ldots\}$), στην «αντίστροφη» συνάρτηση $\pi(x)$, στο Θεώρημα των Πρώτων Αριθμών, και στην Εικασία του Riemann, το Θεμελιώδες Θεώρημα της Αριθμητικής (ΘΘΑ).

Διάλεξη 5: Απόδειξη του ΘΘΑ, ο εκθέτης $m = v_p(a)$ του πρώτου p στον αριθμό a που χαρακτηρίζεται από το ότι p^m είναι η μέγιστη δύναμη του p που διαιρεί τον a και από το ότι $a = p^m a'$ με $p \not| a'$, $v_p(ab) = v_p(a)v_p(b)$, $a|b \Leftrightarrow (\forall p)[v_p(a) \leq v_p(b)]$.

Διάλεξη 6: Το πλήθος των διαιρετών του $b = p_1^{m_1} p_2^{m_2} \ldots p_k^{m_k}$ είναι $(1+m_1)(1+m_2)\ldots(1+m_k)$ αν $m_i = v_{p_i}(b)$. Η σχέση των $\text{ΜΚΔ}(a, b)$ και $\text{ΕΚΠ}(a, b)$ με τους πρώτους παράγοντες των a, b. Η κλάση $\bmod n$ του ακεράιου a, που θα τη συμβολίζουμε με $[a]_n$ ή με $\overline{a}$ (στην αίθουσα: και με a), και που είναι απλώς το υπόλοιπο της διαίρεσης του a δια n. Το σύνολο $\mathbb{Z}_n$ των ακεραίων $\bmod n$, που είναι απλώς το σύνολο που αποτελείται από όλα τα πιθανά $\overline{a}$, δηλαδή το σύνολο που αποτελείται από τα $0, 1, \ldots, n-1$. Ισοτιμία $\bmod n$. Πρόσθεση και πολλαπλασιασμός $\bmod n$ και η σχέση τους με την πρόσθεση και τον πολλαπλασιασμό ακεραίων. (Στην αίθουσα χρησιμοποιούμε το $+$ για την πρόσθεση $\bmod n$ και το $\cdot$ για τον πολλαπλασιασμό $\bmod n$. Με αυτό το συμβολισμό, η σχέση των «καινούργιων» πράξεων με τις «παλιές» είναι $a + b = c \Rightarrow a + b = c$ και $a \cdot b = c \Rightarrow a \cdot b = c$, όπου συμφωνούμε ότι το $=$ απλώς σημαίνει $=$)

Διάλεξη 7: Στοιχειώδεις ιδιότητες των ακεραίων $\bmod n$ και των ισοτιμιών $\bmod n$. Παραδείγματα που δείχνουν πως οι ακέραιοι $\bmod n$ μας βοηθούν να λύσουμε προβλήματα που, εκ πρώτης όψεως, έχουν να κάνουν μόνο με τους (συνήθεις) ακεραίους. (Ανάμεσα στα παραδείγματα είναι και μια εισαγωγή στους «Πρώτους του Mersenne».) Η εξίσωση $ax = 0$ στους ακεραίους $\bmod n$.

Διάλεξη 8: Η εξίσωση $ax = 0$ στους ακεραίους $\bmod n$ (συνέχεια). Ορίσαμε την προσθετική τάξη m του a στους ακεραίους $\bmod n$ ως τον ελάχιστο αριθμό (για μας «αριθμός» σημαίνει «θετικός ακέραιος») k με το άθροισμα k όρων $a + a + \cdots + a$ στους ακεραίους $\bmod n$ να είναι μηδέν. Είδαμε ότι αυτό το m ισούται με n/d όπου d είναι ο ΜΚΔ των a και n, και ότι τα παραπάνω k είναι ακριβώς τα πολλαπλάσια του m. Ορίσαμε τα «πολλαπλάσια $\bmod n$» του a, είδαμε ότι το πλήθος τους είναι m (με m όπως παραπάνω), ότι ταυτίζονται με τα πολλαπλάσια $\bmod n$ του d, και τα υπολογίσαμε ως $0, d, 2d, \ldots, (m-1)d$.

Διάλεξη 9: Η εξίσωση $ax = b$ στους ακεραίους $\bmod n$, η ισοτιμία $ax \equiv b \pmod n$ και πως αυτά τα δυό προβλήματα είναι ουσιαστικά το ίδιο πρόβλημα. Κλάσεις ισοτιμίας. Πολυωνυμικές ισοτιμίες και πως συμφωνούμε να παρουσιάζουμε τις λύσεις τους ως κλάσεις ισοτιμίας.

Διάλεξη 10: Πρώτα μελετήσαμε το Κινέζικο Θεώρημα Υπολοίπων (ΚΘΥ) και είδαμε εφαρμογές του ΚΘΥ. Μετά ορίσαμε ένα υποσύνολο U_n του $\mathbb{Z}_n$ που αποτελείται από αυτούς τους ακεραίους a στο $\mathbb{Z}_n$ που είναι σχετικά πρώτοι με το n. Παρατηρήσαμε ότι η εξίσωση $ax = 1$ στο $\mathbb{Z}_n$ έχει λύση αν και μόνο αν $a \in U_n$, στην οποία περίπτωση η λύση είναι μοναδική. Στην αίθουσα συμβολίζουμε αυτή τη λύση με $\frac{1}{a}$. Είδαμε πως λύνουμε την $ax = b$ όταν γνωρίζουμε το $\frac{1}{a}$. (Στην αίθουσα συμβολίζουμε με $ax = b$ την εξίσωση $ax = b$ όταν την θεωρούμε ως εξίσωση στο $\mathbb{Z}_n$.) Τέλος, ορίσαμε την συνάρτηση ϕ του Euler και είδαμε απλά παραδείγματα υπολογισμού του $\phi(n)$.

Διάλεξη 11: Αποδείξαμε δυό σημαντικές ιδιότητες της συνάρτησης ϕ. Η πρώτη είναι ότι η ϕ είναι «πολλαπλασι-

αστική», δηλ. $\phi(mn) = \phi(m)\phi(n)$ αν οι m και n είναι σχετικά πρώτοι. Η δεύτερη είναι ότι $\phi(p^m) = p^m - p^{m-1}$ αν ο p είναι πρώτος. Είδαμε πως οι δυό αυτές ιδιότητες κάνουν τον υπολογισμό του $\phi(n)$ πολύ εύκολο, για κάθε n που γνωρίζουμε την παραγοντοποίηση του σε πρώτους.

Διάλεξη 12: Το Θεώρημα των Fermat και Euler (ΘFE) και εφαρμογές στον υπολογισμό δυνάμεων στο $\mathbb{Z}_n$. (Το κομμάτι του ΘFE που βρήκε ο Fermat είναι γνωστό και ως Μικρό Θεώρημα του Fermat (ΜΘF).)

Διάλεξη 13: Πρώτα είδαμε την «κεντρική ιδέα» της Κρυπτογραφικής Μεθόδου RSA. Μετά αποδείξαμε το εξής θεώρημα, που πάνω του στηρίζεται αυτή η μέθοδος: Έστω $m = \phi(n)$. Είδαμε πως από το ΘFE προκύπτει ότι, για $a \in U_n$, αν $de \equiv 1 \bmod m$ τότε $a^{de} \equiv a \bmod n$. Το θεώρημα που αποδείξαμε εγγυάται πως αυτό ισχύει για τυχαίο ακέραιο a αρκεί ο n να είναι της μορφής $n = p_1 p_2 \cdots p_k$ με τους πρώτους $p_1, p_2, \ldots, p_k$ να είναι όλοι διαφορετικοί.

Διάλεξη 14: Τα δυαδικά ψηφία (bits) ενός αριθμού, «έξυπνη» ύψωση σε δύναμη, αριθμητικά παραδείγματα της «κεντρικής ιδέας» της RSA.

Διάλεξη 15: Οι «νόμοι των εκθετών» με τον «πολλλαπλασιαστικό συμβολισμό» και με τον «προσθετικό συμβολισμό». Διαισθητική εισαγωγή στους «διακριτούς λογαρίθμους». Η πολλαπλασιαστική τάξη n ενός στοιχείου γ του U_N.

Διάλεξη 16: Ιδιότητες της (πολλαπλασιαστικής) τάξης n ενός στοιχείου γ του U_N, ειδικότερα ότι μας επιτρέπει να ορίσουμε μια συνάρτηση, τον (διακριτό) λογάριθμο με βάση το γ, που είναι συνάρτηση της μορφής $\log_\gamma :< \gamma >\to \mathbb{Z}_n$, όπου $< \gamma >$ συμβολίζει το σύνολο όλων των δυνάμεων του γ. (Συμφωνούμε, όποτε χρησιμοποιούμε τα σύμβολα «$\alpha, \beta, \gamma, \delta$», τότε κάθε πολλαπλασιασμός μεταξύ τέτοιων συμβόλων θα είναι πάντα πολλαπλασιασμός $\bmod N$, ειδικότερα αυτό ισχύει για κάθε δύναμη του γ, αφού κάθε δύναμη του γ είναι γινόμενο της μορφής $\gamma\gamma\cdots\gamma$.) Ο ορισμός του $\log_\gamma$ είναι ο «προφανής», δηλαδή $\log_\gamma(\alpha) = a \Leftrightarrow \gamma^a = \alpha$. (Προσοχή στη διαφορά των «ελληνικών» γραμμάτων $\alpha, \beta, \gamma, \delta$ και των «λατινικών» γραμμάτων a, b, c, d, τα πρώτα «ζούνε στον πολλαπλασιαστικό κόσμο του modulo N» ενώ τα δεύτερα «ζούνε στον προσθετικό κόσμο του modulo n».)

Διάλεξη 17: Πρωταρχικές Ρίζες (ΠΡ) $\bmod N$, διατύπωση του Θεωρήματος Ύπαρξης Πρωταρχικών Ριζών (ΘΥΠΡ) $\bmod N$ του Gauss, παραδείγματα που καλύπτουν τις περιπτώσεις $2 \le N \le 8$. Στο υπόλοιπο της διάλεξης θεωρούμε δεδομένο κάποιο $\gamma \in U_N$ τάξης n. Η (πολλαπλασιαστική) τάξη του γ^a είναι η ίδια με την προσθετική τάξη του a στο $\mathbb{Z}_n$. Τάξη του γ^{-1}, ακριβώς $\phi(n)$ ανάμεσα στα γ^a έχουν ίδια τάξη με το γ, αν υπάρχει ΠΡ $\bmod N$ τότε υπάρχουν ακριβώς $\phi(\phi(N))$ ΠΡ $\bmod N$.

Διάλεξη 18: Η τάξη του γινομένου. Η μέγιστη τάξη. Η περίπτωση $N = p^s$. Η περίπτωση $N = 2p^s$.

Διάλεξη 19: Στοιχεία τάξης δύο. Η περίπτωση $N = 2^s$, $s > 2$. Οι υπόλοιπες περιπτώσεις.

Διάλεξη 20: Εφαρμογές των διακριτών λογαρίθμων στη λύση δυωνυμικών και εκθετικών ισοτιμιών.

Διάλεξη 21: Τετραγωνικά ισοϋπόλοιπα $\bmod n$, το σύμβολο του Legendre, που ορίζεται για p περιττό πρώτο και a ακέραιο που δεν διαιρείται με το p, και συμβολίζεται με $\left(\frac{a}{p}\right)$. Το Κριτήριο του Euler, που λέει ότι

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Διάλεξη 22: Ο Νόμος της Τετραγωνικής Αντιστροφής του Gauss, η πολλαπλασιαστικότητα του συμβόλου του Legendre, παραδείγματα.

Διάλεξη 23: Υπολογισμός «τετραγωνικών ριζών $\bmod p$» για $p \equiv 3 \bmod 4$. Για το υπόλοιπο της διάλεξης, επιλέγουμε τυχαίο γ που είναι Πρωταρχική Ρίζα $\bmod p$. Τα στοιχεία του $\mathbb{Z}_p$ που έχουν κάποια «τετραγωνική ρίζα $\bmod p$» είναι αυτά με άρτιο λογάριθμο (εννοείται, λογάριθμο με βάση το γ). Η ισότητα $\left(\frac{a}{p}\right) = (-1)^t$, όπου $t = \log_\gamma a$. Απόδειξη του Κριτηρίου του Euler.