Εξεταζόμενη Ύλη Θεωρίας Αριθμών Χειμερινού Εξαμήνου 2008-2009.

Η ύλη είναι περίπου η ίδια με την ύλη που συμπεριλαμβάνεται στις περιλήψεις των μαθημάτων της Θεωρίας Αριθμών στο διαδίκτυο. Αυτή περιλαμβάνει τα παρακάτω με την σειρά που διδάχθηκαν φέτος:

Ευκλείδια διαίρεση(εύρεση πηλίκου, υπόλοιπου).

Διαιρετότητα, Μ.Κ.Δ. και ταυτότητα Bezout.Γενική λύση Διοφαντικών εξισώσεων με δύο αγνώστους.

Σχετικά πρώτοι αριθμοί.

Ε.Κ.Π. Σχέση του Ε.Κ.Π. με το Μ.Κ.Δ.

Τα συστήματα των αριθμών(δεκαδικό, δυαδικό, τριαδικό, κ.ο.κ.) και πως παριαστάνεται ένας αριθμός σε κάθε ένα αυτά.

Γενίκευση Ευκλείδιας Διαίρεσης. Κάποιες εφαρμογές.

Ισοτιμίες. Ιδιότητες και εφαρμογές.

Λύση μιας γραμμικής εξίσωσης με μόντουλα όταν έχουμε ένα άγνωστο(αν υπάρχουν λύσεις θα πρέπει να βρούμε μια ειδική λύση πρώτα και μετά τις άλλες απ΄ αυτήν). Εύρεση μιας ειδικής λύσης με χρήση της Bezout. Το πλήθος των ανισότιμων λύσεων για την $ax \equiv b(modn)$ με άγνωστο το x και με την προυπόθεση ότι Μ.Κ.Δ$(a, n)/b$. Πότε ένας αριθμός a αντιστρέφεται μόντουλο n(όταν Μ.Κ.Δ$(a, n) = 1$).

Κλάσεις ισοτιμίας $\bmod n$ και ο δακτύλιος $\mathbb{Z}_n$. Εφαρμογές. Η ομάδα των ενάδων U_n.

Πλήρη σύνολα καταλοίπων.

Γραμμικά συστήματα με ισοτιμίες. Κινεζικό Σύστημα. Γενίκευση Κινεζικού συστήματος(όπου τα μόντουλα δεν είναι κατ΄ ανάγκη σχετικά πρώτα μεταξύ τους). Επίλυση οποιασδήποτε εξίσωσης ή συστήματος με ισοτιμίες με ένα άγνωστο.(το μετατρέπουμε ισοδύναμα σε ένα ή περισσότερα Κινεζικά συστήματα και το λύνουμε)

Βασικές αριθμοθεωρητικές συναρτήσεις και ιδιότητές τους(συναρτήσεις $\pi(x), \phi(x), d(x), \sigma(x)$). Πολλαπλασιαστικές συναρτήσεις.

Αριθμοί του Fermat και Mersenne. Τέλειοι αριθμοί.

Το πλήθος των ανισότιμων λύσεων της εξίσωσης $x^2 \equiv 1 \bmod 2^e$. Όμοια της $x^2 \equiv 1 \bmod p^e$ για $p > 2$ πρώτο. Πώς λύνουμε τις δευτεροβάθμιες εξισώσεις $ax^2 + bx + c \equiv (\mathrm{mod} n)$. Ο τύπος του πλήθους N των λύσεων της εξίσωσης $x^2 \equiv 1(\mathrm{mod} n)$.

Το πλήθος των στοιχείων της πολλαπλασιαστικής ομάδος U_n. Το πλήθος των στοιχείων της πολλαπλασιαστικής ομάδος Q_n(τα Q_n είναι όλα τα στοιχεία του U_n τα οποία έχουν κάποια τετραγωνική ρίζα μόντουλο n).

Θεμελιώδες Θεώρημα της αριθμητικής με τις εφαρμογές του. Κόσκινο του Ερατοσθένη.

Θεώρημα του Euler, μικρού θεωρήματος Fermat(ειδική περίπτωση του προηγούμενου) και θεωρήματος Langrange(από την Άλγεβρα, αλλά είναι χρήσιμο και στην Θεωρία Αριθμών). Θεώρημα του πανεπιστημίου Αιγαίου ή με άλλα λόγια για κάθε $s \in U_n, s^{\frac{2\phi(n)}{N}} \equiv 1(\mathrm{mod} n)$.

Πως λύνουμε την ισοτιμία $f(x) \equiv 0(\mathrm{mod} p^e)$ γνωρίζοντας τις λύσεις της $f(x) \equiv 0(\mathrm{mod} p^{e-1})$, όπου p πρώτος.

Αρχικές ή πρωταρχικές ρίζες και ο ρόλος τους. Πότε ένας ακέραιος n έχει τέτοιες ή με άλλα λόγια πότε η ομάδα U_n είναι κυκλική. Πόσες τέτοιες υπάρχουν και πως τις βρίσκουμε. Διακριτός λογάριθμος του a με βάση την αρχική ρίζα g του n(συμβολικά $ind_{g,n}a$)και η χρήση του(ο διακριτός λογάριθμος έχει παρόμοιες ιδιότητες με τον κανονικό λογάρειθμο).

Πυθαγόρειες τριάδες.

Σας ευχόμαστε ολόψυχα καλή επιτυχία. Να θυμάστε η θεωρία(θεωρήματα, προτάσεις, ιδιότητες, κ.ο.κ) είναι ένα πανίσχυρο εργαλείο που κάνει εύκολη ακόμα και την πιο δύσκολη άσκηση. Να κοιτάτε όμως ακριβώς ποιές προυποθέσεις κρύβονται πίσω απ' αυτήν ώστε να μην γίνεται λάθος χρήση της θεωρίας. Τέλος να κάνετε δοκιμή στα αποτελέσματά σας. Π.χ. αν σας δίνουν να λύσετε μια ισοτιμία να δοκιμάζετε τις απαντήσεις σας δηλ. αν πράγματι ικανοποιούν την ισοτιμία. Ένα επιστημονικό ή μή κομπιουτεράκι είναι καλός συνεργάτης.