Svarīgākās pārbaudāmās zināšanas un prasmes studiju kursā "Skaitļu teorija", 2009./2010.st.gads

1. (*Veselo skaitļu pamatīpašības, dalāmība, Eiklīda algoritms*) Dalīšana ar atlikumu, dalāmības īpašības, kopīgie dalītāji, LKD, Eiklīda algoritms.
2. (*Eiklīda algoritma sekas un lietojumi, pirmskaitļi un aritmētikas pamatteorēma*) Dalāmības īpašības, MKD, lineārās kombinācijas īpašība, pirmskaitļu īpašības, aritmētikas pamatteorēma, LKD un MKD atrašana izmantojot aritmētikas pamatteorēmu.
3. (*Kongruence, atlikumu klases un to īpašības*) Kongruence, kongruences īpašības - ar fiksētu moduli, ar mainīgu moduli, aritmētiskās īpašības. Atlikumu klases, kanoniskā atlikumu klašu pārstāvju kopa.
4. (*Atlikumu klašu gredzens, modulārās aritmētikas lietojumi*) Operācijas ar atlikumu klasēm, operāciju īpašības. Pozicionārais pieraksts.
5. (*Ķīniešu atlikumu teorēma un tās pastiprinājumi*) Noteiktā veida modulāro vienādojumu sistēmu risināšana visos gadījumos.
6. (*Atlikumu gredzeni un algebriskās struktūras*) Atlikumu aditīvā un multiplikatīvā grupa, atlikumu gredzens.
7. (*Atlikumu aditīvās grupas īpašības*) Atlikumu aditīvās grupas ciklisko apakšgrupu pārskaitīšana.
8. (*Atlikumu multiplikatīvās grupas īpašības*) Eilera funkcijas un vispārinātās Eilera funkcijas aprēķināšana. Fermā un Eilera teorēmas. Elementa multiplikatīvā kārta un tās īpašības.
9. (*Skaitļu teorijas lietojumi informācijas aizsardzībā*)
10. (*Primitīvās saknes un indeksi*) Primitīvā sakne, indekss, primitīvās saknes atrašana un lietojumi.
11. (*Modulāro vienādojumu risināšana, modulārie vienādojumi ar pirmskaitļa moduli*) Modulāro vienādojumu ekvivalentie pārveidojumi, modulāro vienādojumi mod p risināšana.
12. (*Modulārie vienādojumi ar saliktu moduli, kvadrātiskie modulārie vienādojumi*) Modulāro vienādojumu risināšana mod p^n un izmantojot ķīniešu atlikumu teorēmu. Kvadrātisko modulāro vienādojumu risināšana mod p - kvadrātiskie atlikumi, Eilera kritērijs, Ležandra simbols, kvadrātiskā reciprocitāte.
13. (*Lineāru vienādojumu ar diviem nezināmajiem risināšana*) Homogēnu un nehomogēnu lineāru vienādojumu ar diviem nezināmajiem risināšana.
14. (*Lineāru Diofanta sistēmu risināšana*) LDVS risināšana ar matricu metodi.