VÄLTTÄMÄTÖN LUKUTEORIA IMO:ON

1. Alkuluvut ja jaollisuus

- jaollisuuden määritelmä
- merkinnän || määritelmä ja mitä iloa siitä on
- alkulukujen määritelmä
- miksi alkulukuja on äärettömän paljon (ainakin yksi epätopologinen todistus)
- alkulukuhajotelman yksikäsitteisyys todistuksineen
- primitiiviset juuret
- neliönjäännökset, milloin -1 on neliönjäännös (ja milloin ei) ja Eulerin kriteerio neliönjäännöksille
- tekijäfunktioiden (eli tekijöiden summan ja lukumäärän kertovien funktioiden) määritelmä, multiplikatiivisuus ja kaava
- yksinkertaisimmat jaollisuussäännöt olisi hyvä olla aktiivimuistissa.

2. Kongruenssit

- määritelmä
- Fermat'n pieni lause todistuksineen
- Eulerin lause todistuksineen (lisäksi osattava Eulerin ϕ-funktion määritelmä sekä ideana että kaavana)
- kiinalainen jäännöslause
- Wilsonin lause
- Lagrangen lause polynomeista

3. Diofantoksen yhtälöt

3.1. **Ensimmäinen aste.**

- syt ja pyj
- Eukleideksen algoritmi
- kyky ratkaista täysin, tai osoittaa, että ratkaisuja ei ole

3.2. **Korkeammat asteet.**

- Pellin yhtälöt
- äärettömän laskeutumisen periaate
- Pythagoraan kolmikot
- huomattava, että Eukleideksen algoritmia voi käyttää myös korkeammissa asteissa, esimerkiksi eksponentin redusointiin

4. Temput

- havainnon, että jos $a|b$ ja $0 < a < b$, niin $b \geq 2a$ käyttäminen
- jos $a|b$, niin rajojen etsiminen luvulle $\frac{b}{a}$, sillä mikä nämä rajat ovat äärelliset, on ainoastaan äärellinen määrä erikoistapauksia käytävänä (koska osamäärän on oltava tällä välillä elävä kokonaisluku)
- Diofantoksen yhtälöön voi yrittää soveltaa jotain epäyhtälöä, ja sen jälkeen mietiskellä, josko tuloksena olisi jotain kahta edellistä kohtaa vastaavaa.
- Diofantoksen yhtälöitä tarkasteltaessa (ja miksei muulloinkin) lukujen neliöiden tarkasteleminen modulo 4 tai 8 tai 3 (tai muu vastaava), neljänsien potenssien tarkasteleminen modulo 16 (tai 5), jne. Joskus voi tuottaa iloa myös tarkastella esim. kolmansia ja neljänsiä potensseja modulo 13. Nämä ovat vain esimerkkejä, tilanteen mukaan on toimittava ja mietittävä Fermat'n pienen lauseen tai Eulerin lauseen perusteella eksponentteja ihmetellen mikä modulo tuottaisi eniten iloa.

5. Asiat, joita ilman voi ehkä selvitä hengissä, mutta itse en ottaisi riskiä

- Gaussin kokonaisluvut (näitä ei luultavasti tarvitse sellaisenaan, mutta nämä tuovat mukavasti lisää näkemystä)
- neliönjäännösten resiprookkilaki
- kahden neliön summat
- Lagrangen lause neljästä neliöstä