Arvoisat vararehtorit, arvoisa dekaani, arvoisat kutsuvieraat, hyvät naiset ja herrat.

Roomalainen arkkitehti ja kirjailija Marcus Vitruvius Pollio kertoo teoksessaan ”De architectura libri decem” kreikkalaisesta filosofista Aristippoksesta, joka haaksirikkoutui Rhodoksen rannikolle. Kahlattuaan rantaan Aristippos huomasi, että rantahiekkaan oli piirretty geometrisia kuvioita. Aristippos huudahti kumppaneilleen: ”Älkää menettäkö toivoanne, näen merkkejä sivistyksestä”. Alun perin antiikin Kreikasta alkunsa saanut algebrallinen geometria on tällä hetkellä yksi modernin matematiikan keskeisistä osa-alueista. Haluan tässä luennossa paitsi esitellä tutkimusalaani myös pohtia yleisemminkin matematiikkaa ja sen olemusta.

Muinaiset kreikkalaiset tunsivat jo toisen asteen käyrät ellipsin, hyperbelin ja paraabelin. Kertomuksen mukaan ne keksittiin yritettäessä ratkaista ns. Deloksen ongelmaa. Ateenassa riehuvan ruton taltuttamiseksi Delfoin oraakkeli oli käskenyt kahdentaa Deloksen saarella sijaitsevan Apollon temppelin kuutionmuotoisen alttarin. Kreikkalaiset eivät kuitenkaan tunteneet koordinaatteja eivätkä tuntemattoman sisältävän yhtälön käsitettä.

Kehitys kohti modernia algebrallista geometriaa alkaakin varsinaisesti Descartesin ja Fermat’n keksinnöstä kuvata pisteen sijaintia euklidisessa avaruudessa sen koordinaattien avulla. Tämä keksintö synnytti analyyttisen geometrian. Se on jokaiselle koulusta tuttu. Analyyttisessa geometriassa geometrinen kuvio määritellään niiden pisteiden joukkona, joiden koordinaatit toteuttavat tietyt yhtälöt. Algebrallinen geometria keskittyy tutkimaan niitä geometrisia kuvioita, jotka voidaan määritellä käyttämällä polynomiyhtälöitä. Yksinkertainen esimerkki on paraabeli, jonka yhtälö on $y=x^2$. Yhden polynomiyhtälön tilalla on kuitenkin tavallisesti polynomiyhtälöistä koostuva yhtälöryhmä, jossa voi olla mikä tahansa määrä muuttujia. Näin saadaan paitsi algebrallisia käyriä myös pintoja sekä näiden korkeampiulotteisia vastineita.

Polynomien käytöstä on paljon etuja. Polynomit ovat säännöllisesti käyttäytyviä funktioita. Algebrallinen geometria on tässä mielessä hallittua geometriaa verrattuna esimerkiksi fraktaaligeometriaan. Mikä tärkeintä, algebra tarjoaa keinoja polynomiyhtälöiden muokkaamiseen. Voimme etsiä yhtälöryhmällemme ratkaisuja reaalilukujen joukon sijasta myös muista lukujoukoista kuten kompleksilukujen joukosta. Kompleksinen algebrallinen käyrä osoittautuu tällöin samaksi kuin kompleksianalyysin Riemannin pinta. Kokonais- tai rationaalilukuratkaisut antavat taas tietoa lukuteorian kysymyksistä. Nojautuminen algebraan mahdollistaa algeb-

rallisen geometrian menetelmien soveltamisen myös sellaisiin tapauksiin, joissa ei voida piirtää kuvaa.

Nykyaikaisen algebrallisen geometrian kehitys pääsi käyntiin 1800-luvun alussa, kun kompleksiluvut otettiin käyttöön Gaussin ja muiden toimesta. Algebrallisen geometrian läheinen yhteys kompleksianalyysiin paljastui. Tästä vuosisadasta muodostui klassisen algebrallisen geometrian kulta-aika. Todistettiin mm. kuuluisa lause tasan 27 suorasta kolmannen asteen pinnalla. Italialainen koulukunta ylti 1800-luvun lopussa merkittäviin saavutuksiin. Tarkkojen perustelujen sijasta maestrit nojautuivat kuitenkin todistuksissaan usein vain loistavaan geometriseen intuitioon.

Algebrallisen geometrian saattaminen täsmälliselle perustalle onnistui viime vuosisadan alussa, kun saksalaisten Hilbertin ja Noetherin vaikutuksesta syntyi kommutatiiviseksi algebraksi kutsuttu matematiikan ala. Moderni algebrallinen geometria nojautuu kommutatiiviseen algebraan samalla tavalla kuin differentiaaligeometria differentiaalilaskentaan. Noin vuosina 1955–1970 ranskalainen koulukunta hallitsi algebrallisen geometrian kehitystä. Viime vuosisadan ehkä kaikkein merkittävimmän matemaatikon Alexander Grothendieckin toimesta algebrallinen geometria saavutti matematiikassa ennen näkemättömän abstraktioasteen. Vaikka tätä vaihetta seurasikin vastavaikutus konkreettisempaan suuntaan, Grothendieckin luoma koneisto on edelleen modernin algebrallisen geometrian perusta. Sitä hyödynsi myös englantilainen matemaatikko Andrew Wiles ratkaistessaan vuonna 1995 357 vuotta avoinna olleen Fermat’n suuren ongelman. Wiles todisti, että jos n on kahta suurempi kokonaisluku, ei ole mahdollista löytää sellaisia kokonaislukuja x, y ja z, että $x^n + y^n = z^n$.

Jokainen matemaatikko joutuu silloin tällöin kuulemaan maallikkojen ihmettelyä siitä, mitä uusia tuloksia matematiikassa muka voidaan enää keksiä: onhan peruslaskutoimitukset ja jopa prosenttilasku jo keksitty. Usein matematiikka myös nähdään vain pelkkänä kaavakielenä, jonka avulla erilaisia ongelmia voidaan esittää täsmällisessä muodossa. Itse asiassa viime vuosisata on kuitenkin ollut tuloksellisin koko matematiikan historiassa. Sen lisäksi, että lukuisia vanhoja ongelmia on ratkaistu – kuten edellä mainittu Fermat'n ongelma – on syntynyt paitsi uusia tuloksia ja teorioita myös useita kokonaan uusia matematiikan osa-alueita. Ymmärrämme myös entistä syvällisemmin matematiikan eri osa-alueiden välisiä yhteyksiä. Algebrallisen geometrian kannalta mielenkiintoisinta on sen välityksellä tällä hetkellä meneillään oleva geometrian ja lukuteorian synteesi. Myös uusia yllättäviä yhteyksiä matematiikan ulkopuolelle on paljastunut.

Laskevaksi geometriaksi kutsuttu algebrallisen geometrian osa-alue pyrkii selvittämään, kuinka monta tietyt ehdot täyttävää geometrista kuviota on olemassa. Jokainen tietää, että kahden pisteen kautta kulkee täsmälleen yksi suora eli ensimmäisen asteen tasokäyrä. Jo antiikin aikaan oltiin selvillä myös siitä, että viiden pisteen kautta kulkee täsmälleen yksi toisen asteen tasokäyrä. Mitä tapahtuu, jos tarkastellaan kolmannen tai korkeamman asteen tasokäyriä? Rajoitutaan ns. rationaalisiin tasokäyriin. 1800-luvulla todistettiin, että 8 pisteen kautta kulkee täsmälleen 12 kolmannen asteen käyrää ja 11 pisteen kautta 620 neljännen asteen käyrää. Tultaessa 1980-luvulle oli päästy ainoastaan siihen asti, että 14 pisteen kautta kulkee täsmälleen 87304 viidennen asteen käyrää. Apu löytyi erikoisesta suunnasta: nimittäin teoreettisen fysiikan jousiteoriasta. Jousiteoria auttoi venäläistä matemaatikkoa Maxim Kontsevichia keksimään 1994 yleisen kaavan, joka ratkaisi lopullisesti tämän ongelman. Englantilainen matemaatikko Sir Michael Atiyah kuvailee tämän yhteyden löytymistä algebrallisen geometrian ja fysiikan välillä ” 20. vuosisadan virkistävimmäksi tapahtumaksi matematiikan alalla”.

Matematiikka on yksi länsimaisen kulttuurin merkittävimmistä älyllisistä ja esteettisistä saavutuksista. Matematiikan kulttuuriarvoa ei ikävä kyllä nykyään aina tunnusteta. Matematiikka luetaan vain osaksi teknologiaa, joka tässä ajattelussa nähdään kaiken kulttuurin vastakohtana. Esteettisyyden tavoittelu on tärkeä matemaattisen teorian muodostusta ohjaava tekijä. Kuuluisan saksalaisen matemaatikon Weierstrassin kerrotaan sanoneen, että jos matemaatikossa ei ole vähän runoilijaa, hän ei voi koskaan tulla täydelliseksi matemaatikoksi. Englantilainen matemaatikko Hardy puolestaan kirjoittaa kirjassaan ”Matemaatikon apologia” seuraavaa: ”Taidemaalarin ja runoilijan tapaan matemaatikon on luotava kauniita hahmoja. Värien ja sanojen tapaan ideoiden on sovittava harmonisesti yhteen. Kauneus on ensimmäinen koe: maailmassa ei ole pysyvää paikkaa rumalle matematiikalle.” Toki matematiikan kauneus on abstraktia. Nykyaikainen tietokonegrafiikka voi kuitenkin välittää sen visuaalisen puolen myös maallikolle.

Mutta matematiikan luonne on duaalinen. Älyllisen ja esteettisen puolensa lisäksi matematiikasta on myös käytännöllistä hyötyä ympäröivälle yhteiskunnalle. Matemaatikkojen keskuudessa ollaan nykyään yleisesti sitä mieltä, että aikanaan hyvin selvä raja puhtaan ja sovelletun matematiikan välillä on hämärtynyt. Algebrallinen geometria tarjoaa tästä hyvän esimerkin. Se on vuosisatoja ollut tyypillinen puhtaan matematiikan ala, jolla ei ole juurikaan ollut mitään käytännön sovelluksia. Viime vuosikymmeninä näitä on kuitenkin löytynyt runsaasti ennen kaikkea informaatioteoriasta ja tietojenkäsittelytieteestä.

Tietoverkkoja käytetään nykyään kaikkialla. Tietoturva askarruttaa meistä jokaista viimeistään silloin, kun käytämme sähköisiä pankkipalveluja tai teemme ostoksia verkkokaupassa. Tehokkaat salakirjoitusmenetelmät ovat tarpeen haluttaessa estää luottamuksellisen tiedon leviäminen vääriin käsiin. Ns. julkisen avaimen salakirjoitusmenetelmät ovat tällöin osoittautuneet tärkeiksi. Näistä tunnetuin eli RSA-menetelmä perustuu siihen, että jos kerromme kaksi esimerkiksi 100-numeroista alkulukua keskenään ja julkistamme tulon, ulkopuolisen on sen perusteella hyvin vaikea päätellä, mitkä olivat tulon alkuperäiset tekijät. Miten tämä liittyy algebralliseen geometriaan? Elliptinen käyrä on kolmannen asteen polynomiin liittyvä käyrä. Yksinkertainen esimerkki elliptisestä käyrästä on vaikkapa käyrä $y^2=x^3+x$. Ranskalainen matemaatikko Poincare havaitsi viime vuosisadan alussa, että elliptisen käyrän pisteitä voidaan laskea yhteen ja että tämä yhteenlasku antaa käyrälle ryhmäksi kutsutun matemaattisen struktuurin. 1980-luvun lopussa keksittiin, että tämä yhteenlasku tarjoaa keinon julkisen avaimen salakirjoitukseen. Lyhyen avaimensa takia se sopii mobiililaitteisiin kuten kännykkään paremmin edellä mainittu RSA-menetelmä.

Itävaltalainen matemaatikko Wolfgang Gröbner antoi 1964 oppilaalleen Bruno Buchbergerille väitöskirja-aiheeksi ongelman, joka liittyi polynomiyhtälöistä koostuvan yhtälöryhmän ratkaisemiseen. Gröbner on sittemmin kertonut, että hän tunsi itse ratkaisun. Väitöskirja valmistui 1965. Buchberger pääsi siinä pidemmälle kuin Gröbner oli aavistanut. Sen päätulos on ns. Buchbergerin algoritmi. Sitä voidaan pitää lineaaristen yhtälönryhmien ratkaisussa tutun Gaussin algoritmin yleistyksenä polynomiyhtälöiden ryhmiin. Buchbergerin algoritmi jäi pariksikymmeneksi vuodeksi unohduksiin, mutta tietokoneiden laskentatehon kehittymisen ansiosta sen käyttämisestä on tullut realistinen tapa ratkaista polynomiyhtälöistä koostuvia yhtälöryhmiä. Algebrallista geometriaa voidaan nyt hyödyntää esimerkiksi sellaisilla aloilla kuin kolmiulotteinen mallinnus, kuvankäsittely ja tietokonenäkö. Sovelluksia on vieläpä matemaattisessa biologiassakin. On myös syntynyt kokonaan uusi algebrallisen geometrian osa-alue, jota kutsutaan laskennalliseksi algebralliseksi geometriaksi.

Hämmästyttävää kyllä Buchbergerin keksintö on vaikuttanut algebrallisen geometrian tutkimukseen myös aivan konkreettisella tasolla. Uutta teoriaa kehittävä matemaatikko turvautuu aluksi arvauksiin ja esimerkkeihin. Buchbergerin algoritmia hyödyntävien symbolisen laskennan ohjelmistojen avulla tutkijan on nyt mahdollista laskea entistä realistisempia esimerkkejä ja muotoilla niiden perusteella otaksumia, joita hän sitten voi yrittää todistaa. Algebrallisen geometrian tutkimuksen voidaan täten sanoa saaneen kokeellisen ulottuvuuden.

Millaiseksi matematiikka muodostuu tietoyhteiskunnassa? Tietokoneen laskutoimitukset koostuvat aina vain äärellisestä määrästä askelia. Tällainen äärellisyys kuuluu luonnostaan algebraan. Uskallan väittää, että antiikin Kreikassa alkunsa saanut algebrallinen geometria tulee säilyttämään asemansa matematiikassa myös tulevaisuudessa.