



Tarinoita polynomeista (osa 1)

Jukka Tuomela

Itä-Suomen yliopisto, Joensuu

jukka.tuomela@uef.fi

Lähtökohtia

Polynomeja esiintyy kaikkialla matematiikassa, joten polynomeihin liittyviä kysymyksiä voi tulla esille osatehtävinä hyvin monissa eri yhteyksissä. Ei siis ole ihme, että lukiossa käsitellään polynomeja, ja matematiikkakilpailuissakin usein on polynomeihin liittyviä tehtäviä. Nämä tehtävät ovat kuitenkin usein jotenkin kummallisia, ja niihin liittyvät mallivastauksetkin ovat joskus hiukan erikoisia. Ei kuitenkaan ole ihan yksinkertaista selittää, missä mielessä minusta tehtävät ovat joskus hassuja, ja mikä sitten olisi ”luonnollisempi” tapa tarkastella polynomitehtäviä.

Tämä kirjoitus lähtikin liikkeelle yrityksestä selventää tätä asiaa, mutta huomasin, että asiaa tulikin helposti aika paljon, joten oli sitten parasta jakaa tämä kirjoitus osiin. Katsotaan sitten montako osaa tarvitaan.

Ehkäpä lyhyesti voisi sanoa, että polynomitehtävät usein perustuvat johonkin näppärään kikkaan, joka toimii, kun tehtävän polynomi on huolellisesti valittu. Toisaalta monesti tehtävän voisi ratkaista algoritmisesti aivan yleisessäkin tapauksessa. Mutta asia varmaankin selkenee, kun katsotaan tarkemmin joitain esimerkkejä. Käytän seuraavassa esimerkkinä tehtäviä, jotka ovat joko ylioppilaskirjoituksista¹ tai matematiikkakilpailusivuilta².

¹<https://matta.hut.fi/matta/yoteht/>

²<https://matematiikkakilpailut.fi/>

Tässä kirjoituksessa ei oleteta mitään erityisiä lukion ulkopuolen esitietoja. Jotkut termit ja merkinnät voivat olla uusia, mutta tämän ei pitäisi olla ongelmallista. Esitiedoiksi riittää, että tietää, mikä on polynomi ja miten polynomeja lasketaan yhteen ja kerrotaan. Jos sitten haluaa syvällisemmin perehtyä polynomeihin voi aloittaa erinomaisesta kirjasta [2].

Perusasiat

Lähdetään liikkeelle yhden muuttujan polynomeista, jotka ovat muotoa

$$f = a_0 + a_1x + \dots + a_nx^n = \sum_{j=0}^n a_jx^j. \quad (1)$$

Jos $a_n \neq 0$, niin sanotaan, että polynomien aste on n ja merkitään $\deg(f) = n$. Tällöin sanotaan, että $\text{LT}(f) = a_nx^n$ on f :n isoin termi (leading term).

Usein tehtävissä esiintyvissä polynomeissa kertoimet a_j ovat rationaalilukuja, mutta ne voisivat myös olla reaali- tai kompleksilukuja.

Olkoon nyt \mathbb{Q} rationaalilukujen joukko; jos on annettu polynomi (1), missä $a_j \in \mathbb{Q}$, niin merkitään $f \in \mathbb{Q}[x]$. Hyvin usein tehtävissä esiintyy kuitenkin ”parametreja”; tavallaan ne ovat muuttujia, kuten ”varsinainen”

muuttuja x , mutta kuitenkin tehtävän kannalta jotenkin eri asemassa.

Esimerkki 1. Keväällä 2014 ylioppilaskirjoituksissa ky-
syttiin, millä parametrin arvolla a polynomilla

$$f = ax^2 - 5x + 2$$

on kaksinkertainen nollakohta. Tehtävä ratkeaa helpos-
ti, kun kirjoitetaan

$$f = ax^2 - 5x + 2 = a(x - b)^2 = ax^2 - 2abx + ab^2.$$

Vertaamalla kertoimia nähdään, että $a = 25/8$ ja
 $b = 4/5$. ☆

Kun kertoimissa on parametreja, on usein kätevää aja-
tella, että kertoimet ovat parametrien rationaalifunk-
tioita:

h on a :n rationaalifunktio, $h \in \mathbb{Q}(a)$, jos $h = f/g$,
missä $f, g \in \mathbb{Q}[a]$.

Ennen kuin päästään asiaan, otetaan vielä pari termiä.
Joukko $\mathbb{Q}[x]$ on *renkas*, mikä tarkoittaa, että voidaan
laskea yhteen ja kertoa, mutta käänteisalkiota ei ole:
jos f on polynomi, niin $1/f$ ei ole polynomi (paitsi jos
 f on vakio). Sen sijaan \mathbb{Q} ja $\mathbb{Q}(a)$ ovat *kuntia*; näissä
myös käänteisalkio on olemassa, joten jos h on ratio-
naalifunktio, niin myös $1/h$ on rationaalifunktio. Nyt
voidaan kirjoittaa

$$f = ax^2 - 5x + 2 \in \mathbb{Q}(a)[x].$$

Samoin voidaan merkitä monen muuttujan tapaukses-
sa, esimerkiksi

$$f = \frac{b}{a^2}x^2 + \frac{a^3b^2}{a-b^4}y^3 - \frac{1}{a+b}xy + \frac{2ab}{a^2+2b^2} \in \mathbb{Q}(a,b)[x,y].$$

Tässä ajatellaan, että f on polynomi muuttujien x ja
 y suhteen, ja kertoimet ovat parametrien a ja b ratio-
naalifunktioita.

Jos sitten \mathbb{R} on reaaliluvut, niin periaatteessa voitai-
siin tarkastella reaalkertoimisia polynomeja: $f \in \mathbb{R}[x]$.
Tässä kirjoituksessa ei kuitenkaan tehdä näin. Syy on
se, että tarkoituksena on ottaa algoritmisen näkökul-
ma; katsotaan mitä oikeasti voidaan käsin laskea, tai
mitä tietokoneelle voi ohjelmoida. Reaaliluvuilla ei voi
laskea, sillä niille ei ole äärellistä esitysmuotoa. Muis-
tetaan, että tietokoneet käyttävät liukulukuja (floating
point numbers), kun ne approksimoivat reaalilukuja.
Toisaalta jos jossain laskussa esiintyy vaikkapa luku π ,
niin sehän on laskun kannalta kuten mikä tahansa pa-
rametri, joten voitaisiin kirjoittaa

$$f = x^3 + 2\pi x + 3\pi^3 \in \mathbb{Q}(\pi)[x].$$

Jatkossa polynomien kertoimet ovat pääasiassa joko ra-
tionaalilukuja tai rationaalifunktioita.

Algebran peruslause

Olkoon f kuten yhtälössä (1) ja oletetaan nyt, että
 $a_j \in \mathbb{Q}$ ja $a_n \neq 0$. Algebran peruslauseen mukaan f
voidaan kirjoittaa muodossa

$$f = a_n(x - b_1)^{\ell_1} \dots (x - b_k)^{\ell_k}, \quad (2)$$

missä $b_i \neq b_j$, kun $i \neq j$, ja $\ell_1 + \dots + \ell_k = n$. Lu-
vut b_j , jotka ovat f :n nollakohdat, ovat yleisesti ottaen
kompleksilukuja. Jos siis tiedetään nollakohdat b_j ja
niitten kertaluvut ℓ_j , niin polynomi voidaan aina jakaa
lineaarisiin tekijöihin. Termi lineaarinen viittaa siihen,
että $x - b_j$ on ensimmäisen asteen polynomi. Sanotaan
vielä, että nollakohta on yksinkertainen, jos sen kerta-
luku on yksi.

Usein on kuitenkin mukavampi kirjoittaa

$$f = a_n(x - b_1) \dots (x - b_n), \quad (3)$$

missä kaikki nollakohdat eivät välttämättä ole erisuu-
ria, vaan niitä toistetaan kertaluvun ilmoittama määrä.
Huomaa, että yleisesti ottaen nollakohdat ovat yksin-
kertaisia, jos polynomien kertoimet valitaan ”satunnai-
sesti”.

Kertomalla auki nähdään, että

$$\begin{aligned} b_1 \dots b_n &= (-1)^n \frac{a_0}{a_n} \\ b_1 + \dots + b_n &= -\frac{a_{n-1}}{a_n}, \end{aligned} \quad (4)$$

mikä on joskus hyödyllistä.

Jos ei haluta kompleksilukuja, niin voidaan jakaa reaali-
siin tekijöihin. Muistetaan, että jos polynomien kertoi-
met ovat reaalisia, niin kompleksiset nollakohdat esiin-
tyvät liittolukupareina. Jos b on kompleksinen nolla-
kohta, niin

$$(x - b)(x - \bar{b}) = x^2 - 2\Re b x + |b|^2.$$

Saadaan siis toisen asteen tekijä $x^2 + cx + d$, missä
 $c^2 - 4d < 0$. Tämä johtaa ”reaaliseen algebran pe-
ruslauseeseen”. Tällöin polynomi (1) voidaan kirjoittaa
muodossa

$$f = a_n(x - b_1) \dots (x - b_\ell)(x^2 + c_1x + d_1) \dots (x^2 + c_kx + d_k),$$

missä b_j, c_j ja d_j ovat reaalisia, $\ell + 2k = n$ ja $c_j^2 - 4d_j < 0$.
Esimerkiksi

$$\begin{aligned} x^4 + 4 &= (x^2 + 2x + 2)(x^2 - 2x + 2) \\ &= (x + 1 + i)(x + 1 - i)(x - 1 + i)(x - 1 - i). \end{aligned}$$

Reaalinen perusmuoto voi joskus olla kätevämpi. Hyvin
usein tehtävissä tarkastellaan vain reaalista tapausta,
jolloin kompleksiset nollakohdat tyypillisesti ovat epä-
oleellisia ratkaisun kannalta.

Koska $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, niin sanotaan, että \mathbb{R} on kunnan \mathbb{Q} kuntalaaajennus, ja samoin \mathbb{C} on sekä \mathbb{Q} :n että \mathbb{R} :n kuntalaaajennus. Ideana on, että koska yleensä polynomeilla $f \in \mathbb{Q}[x]$ ei ole nollakohtia \mathbb{Q} :ssa, niin yritetään löytää ne nollakohdat jostain isommasta joukosta. Algebran peruslause siis sanoo, että \mathbb{C} on ”riittävän” iso: aina löytyy tarpeeksi nollakohtia.

Jossain mielessä tämä intuitiivisesti selittää, miksi reaali- ja kompleksiluvuilla ei voi olla äärellistä esitysmuotoa: joukkojen \mathbb{R} ja \mathbb{C} täytyy olla valtavan isoja, jotta siellä olisi nollakohdat kaikille polynomeille, jopa reaali- ja kompleksikertoimisille, joten tällaisia joukkoja ei voi algoritmisesti käsitellä.

Tunnetusti ei ole mitään algoritmia, millä nollakohdat b_j voitaisiin tarkasti laskea. Palataan myöhemmin tarkemmin siihen, mitä johtopäätöksiä tästä pitäisi vetää.

Lukiot tehtävissä ja kilpailutehtävissä esiintyvät polynomit eivät kuitenkaan missään mielessä ole ”satunnaisia”, vaan päinvastoin ne on varta vasten valittu siten, että niillä on joitain erityisominaisuuksia. Esimerkiksi näissä tehtävissä polynomeilla on usein nollakohtana 0 , ± 1 tai ± 2 . Oletetaan siis, että tehtävän ratkaisija löytää tämän kokeilemalla, ja pääsee sitten tämän avulla tehtävässä eteenpäin.

Esimerkki 2. Syksyn 2016 ylioppilaskirjoituksissa oli kaksikin tämäntyyppistä tehtävää. Toisessa tarvittiin tekijöihin jakoa

$$x^3 + 6x^2 - 7x = x(x-1)(x+7)$$

ja toisessa puolestaan

$$x^7 - 60x - 8 = (x-2)(x^6 + 2x^5 + 4x^4 + 8x^3 + 16x^2 + 32x + 4). \quad \star$$

Esimerkki 3. Pohjoismaisessa matematiikkakilpailussa vuonna 2003 tehtävä ratkesi, kun huomasi, että

$$\begin{aligned} f &= x^8 - x^7 + 2x^6 - 2x^5 + 3x^4 - 3x^3 + 4x^2 - 4x + \frac{5}{2} \\ &= x(x-1)(x^6 + 2x^4 + 3x^2 + 4) + \frac{5}{2}. \end{aligned}$$

Tehtävässä piti osoittaa, että $f \geq 0$ kaikilla x . \star

Esimerkki 4. Baltian tie -matematiikkakilpailuissa vuonna 1993 tehtävän ratkaisu edellytti, että jaetaan polynomi

$$f = x^{12} - x^8 - x^4 + 1$$

tekijöihin. Tässä $x^4 = \pm 1$ ovat nollakohtia, minkä jälkeen helposti löydetään

$$f = (x-1)^2(x+1)^2(x^2+1)^2(x^4+1).$$

Tässä piti osoittaa, että jos x on pariton, niin $f/512$ on kokonaisluku. \star

Näitten esimerkkien perusteella voidaan päätellä, että jos ylioppilaskirjoituksissa tai matematiikkakilpailuissa esiintyy polynomitehtäviä, on yllättävän suuri todennäköisyys, että tehtävä ratkeaa, kun kokeilee mitä tapahtuu, kun $x = \pm 1$ tai $x = \pm 2$.

Yritetään kuitenkin nyt katsoa systemaattisesti, mitä voidaan tehdä silloin kun arvaamalla ei päästä eteenpäin.

Jakolasku

Lähdetään liikkeelle jakolaskusta. Muistetaan ensin, että jos on annettu kokonaisluvut m ja k , niin on olemassa $0 \leq r < k$ ja q siten, että

$$m = qk + r.$$

Sanotaan, että q on osamäärä ja r on jakojäännös. Jos ei olla kiinnostuttu osamäärästä, on tapana merkitä

$$m = r \pmod k$$

Polynomeille voidaan määritellä samantapainen jakolasku:

Jos on annettu polynomit f ja g , niin on olemassa yksikäsitteiset polynomit q (osamäärä) ja r (jakojäännös) siten, että

$$f = qg + r$$

ja $\deg(r) < \deg(g)$.

Yksikäsitteisyyden osoittamisen jätän harjoitustehtäväksi. Seuraava algoritmi takaa olemassaolon. Olkoon annettu polynomit f ja g , ja $\text{LT}(f) = a_n x^n$ ja $\text{LT}(g) = c_m x^m$; tällöin merkintä $\text{LT}(g) \mid \text{LT}(f)$ (luetaan: $\text{LT}(g)$ jakaa $\text{LT}(f)$:n) tarkoittaa, että $n \geq m$, jolloin

$$\frac{\text{LT}(f)}{\text{LT}(g)} = \frac{a_n}{c_m} x^{n-m}$$

on hyvin määritelty termi. Seuraava algoritmi laskee osamäärän ja jakojäännöksen.

Algoritmi 1 OSAMÄÄRÄ JA JAKOJÄÄNNÖS

Input: polynomit f ja g , $g \neq 0$.

Output: polynomit q ja r siten, että $f = qg + r$ ja $\deg(r) < \deg(g)$

```

1: q:=0; r:=f;
2: while r ≠ 0 ja LT(g) | LT(r) do
3:   q := q + LT(r)/LT(g)
4:   r := r - LT(r)/LT(g) g
5: end while
```

Algoritmin rivillä 4 jakojäännöksen isoin termi kumoutuu, joten $\deg(r)$ pienenee joka askeleella. Tämän takia ennemmin tai myöhemmin joko $r = 0$ tai $\deg(r) <$

$\deg(g)$, jolloin algoritmi tulee ulos **while** silmukasta, mikä todistaa, että algoritmi päättyy. Algoritmi on itse asiassa käytännössä sama kuin kokonaislukujen jakaminen jakokulmassa.

Yksinkertainen jakolasku on yllättävän tehokas työkalu.

Esimerkki 5. Britannian matematiikkaolympialaisissa vuonna 2007 piti laskea

$$\frac{1 + 2007^4 + 2008^4}{1 + 2007^2 + 2008^2}.$$

Tietenkin tämän voi laskea suoraan, mutta osoittajaan tulee 14-numeroinen luku, joten tämä olisi hyvin työlästä käsin laskien. Olkoon $f = 1 + x^4 + (x + 1)^4$ ja $g = 1 + x^2 + (x + 1)^2$; jakolasku antaa

$$f = (x^2 + x + 1)g,$$

joten vastaus on $1 + 2007 + 2007^2 = 4030057$. ☆

Esimerkki 6. Baltian tie matematiikkakilpailussa vuonna 1992 oli seuraava tehtävä.

Oletetaan, että $a^2 + b^2 + (a + b)^2 = c^2 + d^2 + (c + d)^2$.

Todista, että $a^4 + b^4 + (a + b)^4 = c^4 + d^4 + (c + d)^4$.

Olkoon

$$\begin{aligned} f &= a^4 + b^4 + (a + b)^4 - c^4 - d^4 - (c + d)^4, \\ g &= a^2 + b^2 + (a + b)^2 - c^2 - d^2 - (c + d)^2. \end{aligned}$$

Tehtävä voidaan nyt muotoilla seuraavasti.

Jos $g = 0$, niin $f = 0$.

Mutta nythän ratkaisu saadaan heti: väite voi olla totta täsmälleen silloin kun g on f :n tekijä. Toisin sanoen kun f jaetaan g :llä, niin jakojäännöksen pitäisi olla nolla.

Nyt tietysti olisi luontevaa ajatella, että $f, g \in \mathbb{Q}[a, b, c, d]$, koska kaikki muuttujat ovat tavallaan samanarvoisessa asemassa. Mutta jakolaskualgoritmin kannalta voidaan yhtä hyvin ajatella vaikkapa, että a on ”muuttuja”, ja muut ovat ”parametreja”, jolloin voidaan ajatella, että $f, g \in \mathbb{Q}(b, c, d)[a]$.

Nyt jakolaskualgoritmi antaa

$$f = qg = (a^2 + ab + b^2 + c^2 + cd + d^2)g,$$

mikä todistaa väitteen. Vaikeaksi tarkoitettu tehtävä ratkeaa siis algoritmisesti suoraan laskemalla. Huomaa, että tässä tehtävän ainoa vaikeus oli siinä, että piti nimetä polynomit f ja g . ☆

Yleisesti ottaen polynomitehtävissä ongelma on tapana muotoilla yhtälöitten avulla, eikä oleellisia polynomeja suoraan mainita. Tehtävissä siis aina kannattaa nimetä

ne polynomit, joita tarkastellaan. Tuntuu ehkä hassulta, että asioitten nimeäminen ”oikein” ratkaisee tehtävän. Tämän voi mieltää niin, että kun polynomit on nimetty, niin automaattisesti tämä ohjaa ajattelua oikeaan suuntaan. Katsotaan vielä toinen esimerkki tällaisesta ilmiöstä.

Esimerkki 7. Matti Lehtisen tehtäväkokoelmassa *Kilpailumatematiikan lajeja ja periaatteita* oli seuraava tehtävä.

Oletetaan, että

$$\begin{aligned} abc &= 1, \\ a + b + c &= \frac{1}{a} + \frac{1}{b} + \frac{1}{c}. \end{aligned}$$

Osoita, että $a = 1$ tai $b = 1$ tai $c = 1$.

Huomaa, että väite

$$a = 1 \text{ tai } b = 1 \text{ tai } c = 1$$

on ekvivalenttia sen kanssa, että

$$h = (a - 1)(b - 1)(c - 1) = 0.$$

Olkoon $f_0 = abc - 1$ ja

$$f_1 = abc(a + b + c) - ab - ac - bc.$$

Tehtävä voidaan nyt muotoilla seuraavasti.

Oletetaan, että $f_0 = f_1 = 0$. Osoita, että $h = 0$.

Olkoon edelleen $\hat{f}_1 = a + b + c - ab - ac - bc$. Jos $f_0 = 0$, niin $\hat{f}_1 = f_1$. Tästä saadaan muotoilu:

Oletetaan, että $f_0 = \hat{f}_1 = 0$. Osoita, että $h = 0$.

Mutta nyt heti nähdään, että

$$h = f_0 + \hat{f}_1,$$

mikä todistaa väitteen. ☆

SYT

Jakolaskun avulla voidaan helposti laskea suurin yhteinen tekijä (gcd, greatest common divisor) polynomeille; algoritmi on tuttu Eukleideen algoritmi, jolla lasketaan kokonaislukujen suurin yhteinen tekijä. Jos on annettu polynomit f ja g , niin merkitään äskeisen algoritmin antamaa jakojäännöstä $r = \text{rem}(f, g)$. Lisäksi on kätevää ottaa käyttöön seuraava merkintä: jos $\text{LT}(f) = a_n x^n$, niin isoimman termin kerroin (leading coefficient) on $\text{LC}(f) = a_n$.

Algoritmi 2 SUURIN YHTEINEN TEKIJÄ**Input:** polynomit f ja $g \neq 0$ **Output:** $\text{syt}(f, g)$ $a := f; b := g;$ **while** $b \neq 0$ **do** $r := \text{rem}(a, b)$ $a := b$ $b := r$ **end while** $\text{syt}(f, g) := a/\text{LC}(a)$

Koska jakojäännöksen aste pienenee joka askeleella, niin algoritmi päättyy.

Suurimman yhteisen tekijän avulla nähdään, onko kahdella polynomilla yhteisiä nollakohtia; f :llä ja g :llä on yhteisiä nollakohtia, jos $\deg(\text{syt}(f, g)) > 0$. Tämän selvittäminen on täysin algoritmista, eikä se riipu siitä, osataanko nollakohtia laskea. Jos siis ”unohdetaan” algebran peruslause, niin joka tapauksessa on voimassa seuraava tulos.

Olkoon $f, g \in \mathbb{Q}[x]$. Jos $\text{syt}(f, g) = 1$, niin tehtävällä $f = g = 0$ ei ole ratkaisuja.

Huomaa erityisesti, että tämä ei riipu siitä mistä \mathbb{Q} :n kuntalaajennuksesta ratkaisua etsitään.

Esimerkki 8. Kanadan matematiikkaolympialaisissa vuonna 1988 oli seuraava tehtävä.

Olkoon $f = 1988x^2 + bx + 8891$ ja $g = 8891x^2 + bx + 1988$; millä b :n arvoilla polynomeilla f ja g on yhteinen tekijä?

Tässäkin tehtävä ratkeaa heti, jos huomaa kokeilla, mitä tapahtuu, kun $x = \pm 1$. Tällöin nähdään heti, että $b = \pm 10879$ ja vastaava yhteinen tekijä on $x \pm 1$.

Jos edetään algoritmisesti, niin lasketaan ensin

$$r = \text{rem}(f, g) = \frac{6903}{8891}(bx + 10879)$$

ja sitten

$$r_0 = \text{rem}(g, r) = -\frac{8891}{b^2}(b^2 - 118352641).$$

Jos on yhteisiä tekijöitä, niin $r_0 = 0$, ja tästä saadaan arvaamalla löydetty ratkaisu. ☆

Esimerkki 9. Pohjoismaisessa matematiikkakilpailussa vuonna 2009 oli seuraava tehtävä.

Olkoon $f = x^{17} + x^{13} + x^5 - 90x^4 + x - 90$; tiedetään, että f :llä on tekijä $g = x^2 + x + a$. Mikä on a ?

Tässä vaiheessa lukija varmaankin jo arvaa, että $a = \pm 1$ tai $a = \pm 2$.

Jos g on tekijä, niin jakojäännös on nolla. Lasketaan jakojäännös:

$$f = qg + r, \quad \text{missä}$$

$$r = h_1x + h_0 \quad \text{ja}$$

$$h_0 = -8a^8 + 84a^7 - 258a^6 + 365a^5 - 276a^4 + 114a^3 - 116a^2 + 93a - 90,$$

$$h_1 = a^8 - 36a^7 + 211a^6 - 483a^5 + 565a^4 - 370a^3 + 137a^2 - 209a + 94.$$

Tässä ensin ajatellaan, että f ja g ovat x :n polynomeja ja a on parametri, eli $f, g \in \mathbb{Q}(a)[x]$, ja sovelletaan jakolaskualgoritmia x :n suhteen. Nyt jakojäännös on $r = h_1x + h_0$, missä h_j ovat polynomeja a :n suhteen, ja jakojäännös on nolla, jos polynomeilla h_0 ja h_1 on yhteisiä nollakohtia. Nyt suoraan laskemalla $\text{syt}(h_0, h_1) = a - 2$, joten vastaus on $a = 2$. Laskut ovat helpompia, jos huomaa, että

$$\begin{aligned} f &= x^{17} + x^{13} + x^5 - 90x^4 + x - 90 \\ &= (x^4 + 1)(x^{13} + x - 90). \end{aligned}$$

Selvästi g :n täytyy olla polynomien $\hat{f} = x^{13} + x - 90$ tekijä, ja jakolasku antaa nyt

$$\hat{f} = \hat{q}g + \hat{r}$$

$$\hat{r} = \hat{h}_1x + \hat{h}_0$$

$$\hat{h}_0 = -6a^6 + 35a^5 - 56a^4 + 36a^3 - 10a^2 + a - 90$$

$$\hat{h}_1 = a^6 - 21a^5 + 70a^4 - 84a^3 + 45a^2 - 11a + 2.$$

Luonnollisesti edelleen $\text{syt}(\hat{h}_0, \hat{h}_1) = a - 2$. ☆

Neliövapaa polynomi

Palataan sitten kaavaan (2). Jos ollaan ensisijaisesti kiinnostettu nollakohdista, ja kertaluvut eivät ole niinkään oleellisia, niin voisi olla mukavampi analysoida polynomia

$$f_{\text{red}} = (x - b_1) \cdots (x - b_k).$$

Sanotaan, että f_{red} on f :n reduktio, ja että f on *neliövapaa* (squarefree), jos $f = f_{\text{red}}$. Jos f ei ole neliövapaa, niin $\deg(f_{\text{red}}) < \deg(f)$, joten siirtyminen redusoituun polynomiin alentaa astetta, mikä puolestaan helpottaa tehtävän analyysiä. Mutta miten redusoitu polynomi voitaisiin laskea? Nollakohtiahan ei tunneta.

Jos b on f :n nollakohta, jonka kertaluku on ℓ , niin tällöin voidaan kirjoittaa

$$f = (x - b)^\ell h(x),$$

missä $h(b) \neq 0$. Mutta tällöin edelleen

$$f' = \ell(x - b)^{\ell-1}h + (x - b)^\ell h' = (x - b)^{\ell-1} \hat{h}.$$

Toisin sanoen $(x - b)^{\ell-1}$ on f :n ja f' :n tekijä, ja kun tämä tekijä poistetaan f :stä, saadaan

$$f_0 = (x - b)h.$$

Tässä päästiin eroon moninkertaisesta nollakohdasta, kun jaettiin f :n ja f' :n tekijällä. Mutta edellä on esitetty algoritmi suurimmalle yhteiselle tekijälle, eikä algoritmissa tarvitse tietää nollakohtia. Siispä

$$f_{\text{red}} = \frac{f}{\text{syt}(f, f')}.$$

Toisella tavalla ajateltuna tässä f jaetaan kahteen tekijään:

$$f = \text{syt}(f, f')f_{\text{red}}.$$

Usein (tai aina) tehtävä helpottuu, jos löydetään jokin tekijöihin jako, sillä tällöin voidaan tutkia alempiasteisia tekijöitä erikseen.

Esimerkin 4 tapauksessa saadaan $\text{syt}(f, f') = x^4 - 1$, joten

$$x^{12} - x^8 - x^4 + 1 = (x^4 - 1)(x^8 - 1).$$

Tästä on sitten helppo jatkaa tekijöihin jakoa.

Redusoituun polynomiin siirtyminen helpottaa tehtävää jo siinä, että polynomien asteluku pienenee, mutta on itse asiassa toinenkin tärkeä syy, miksi tämä reduktio kannattaa tehdä. Palataan tähän sitten myöhemmin.

wxMaxima, Sage ja Wolfram Alpha

Edellä esitellyt algoritmit on toteutettu varmaankin kaikissa symbolisen laskennan ohjelmistoissa. Esimerkiksi wxMaximassa on komento `divide`, joka laskee osamäärän ja jakojäännöksen, ja komento `gcd`, joka laskee suurimman yhteisen tekijän.

Tarkemmin wxMaxima³ on käyttöliittymä Maximaan⁴. Nämä ovat vapaita ohjelmistoja, ja itse asiassa wxMaximaa voi käyttää ylioppilaskirjoituksissa. Siis kaikki edellä mainitut esimerkkitehtävät olisivat ratkenneet

parissa minuutissa, jos ne olisivat olleet ylioppilaskirjoitustehtäviä. Esimerkissä 7 ei tosin tarvinnut jakolaskua, mutta se olisi helposti ratkennut myös toisella tavalla muuttujia eliminoimalla, ja tämäkin onnistuu wxMaximalla. Palataan muuttujien eliminointiin tarkemmin myöhemmin.

Myös Sage on ilmainen ohjelmisto, jolla voi laskea sekä symbolisesti että numeerisesti [1].⁵ Sagea on ehkä kätevinä käyttää Jupyterin avulla.⁶

Netissä on lisäksi vapaasti käytettävissä Wolfram Alpha, jonka avulla voi helposti laskea tässä kirjoituksessa olleet esimerkit.⁷ Tässä on taustalla Mathematica⁸, joka on maksullinen ohjelma. Toinen hyvä maksullinen ohjelma on Maple.⁹

Jatkuu ensi numerossa

Ensi kerralla katsotaan tarkemmin polynomien nollakohtien ratkaisemista. Erityisesti tarkastellaan kriittisesti ratkaisukaavoja ja juurilausekkeita ja päädytään siihen, että jos ne eivät ehkä ole täysin hyödyttömiä, niin ainakin niitten merkitystä on vahvasti liioiteltu. Jakolaskualgoritmi sen sijaan osoittautuu edelleen hyödylliseksi työkaluksi.

Viitteet

- [1] G. V. Bard, *Sage for undergraduates*, American Mathematical Society, 2015.
- [2] D. A. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, 4th ed., Undergraduate Texts in Mathematics, Springer, Cham, 2015, An introduction to computational algebraic geometry and commutative algebra.

³<https://wxmaxima-developers.github.io/wxmaxima/>

⁴<https://maxima.sourceforge.io/>

⁵<https://www.sagemath.org/index.html>

⁶<https://jupyter.org/>

⁷<https://www.wolframalpha.com/examples/mathematics/algebra/polynomials>

⁸<https://www.wolfram.com/mathematica/>

⁹<https://www.maplesoft.com/>