VALIKOITUJA KOHTIA LUKUTEORIASTA

ARI LEHTONEN

1. Laajennettu Eukleideen algoritmi

1.1. **Jakoyhtälö.** Olkoot r_0, $r_1 \in \mathbb{Z}$, $r_0 \geq r_1 > 0$. Tällöin on olemassa yksikäsitteiset luvut q_1 ja $r_2 \in \mathbb{Z}$ siten, että

$$r_0 = q_1\, r_1 + r_2 \quad \text{ja} \quad 0 \leq r_2 < r_1.$$

Luku q_1 on lukujen r_0 ja r_1 *kokonaislukuosamäärä* ja r_2 (*kokonaisluku-*)*jakojäännös*.

Otetaan käyttöön seuraavat funktiot: Olkoot x, $y \in \mathbb{R}$, $y \neq 0$. Asetetaan (ks. [**?**, §1.2.4] tai [**?**, §3.1])

$$\begin{aligned} \lfloor x \rfloor &:= \text{suurin kokonaisluku } n \text{ siten, että } n \leq x \ (x\text{:n } \textit{lattia}); \\ \lceil x \rceil &:= \text{pienin kokonaisluku } n \text{ siten, että } n \geq x \ (x\text{:n } \textit{katto}); \\ x \bmod y &:= x - y\lfloor x/y \rfloor; \\ x \bmod 0 &:= x. \end{aligned}$$

Helposti nähdään, että kun $y > 0$, on $0 \leq x \bmod y < y$.

Jakoyhtälön osamäärä ja jakojäännös voidaan nyt ilmaista $q_1 = \lfloor r_0/r_1 \rfloor$ ja $r_2 = r_0 - q_1\, r_1 = r_0 - r_1 \lfloor r_0/r_1 \rfloor = r_0 \bmod r_1$.

1.2. **Eukleideen algoritmi.** Kun jakoyhtälöä toistetaan, löydetään luvut ℓ, q_i, $r_i \in \mathbb{N}$, $1 \leq i \leq \ell$, siten, että $0 \leq r_{i-1} < r_i$, kun $1 \leq i \leq \ell$, ja

$$\text{(1.1)} \qquad \begin{cases} r_0 = q_1\, r_1 + r_2, \\ r_1 = q_2\, r_2 + r_3, \\ \quad \vdots \\ r_{\ell-2} = q_{\ell-1}\, r_{\ell-1} + r_\ell, \\ r_{\ell-1} = q_\ell\, r_\ell + 0. \end{cases}$$

1.3. **Laajennettu Eukleideen algoritmi.** Olkoot luvut ℓ, q_i ja r_i kuten Eukleideen algoritmissa (**??**). Pyritään etsimään luvut s_i ja t_i siten, että $s_i\, r_0 + t_i\, r_1 = r_i$ kaikille $0 \leq i \leq \ell$. Oletetaan aluksi, että tällaiset luvut ovat olemassa. Kun tätä oletusta sovelletaan indekseihin $i-1$, i ja $i+1$, saadaan Eukleideen algoritmin avulla

$$\text{(1.2)} \qquad \begin{aligned} r_{i+1} &= r_{i-1} - q_i\, r_i = (s_{i-1}\, r_0 + t_{i-1}\, r_1) - q_i\, (s_i\, r_0 + t_i\, r_1) \\ &= (s_{i-1} - q_i\, s_i)\, r_0 + (t_{i-1} - q_i\, t_i)\, r_1. \end{aligned}$$

Toisaalta $r_{i+1} = s_{i+1}\, r_0 + t_{i+1}\, r_1$. Valitaan kertoimet seuraavan palautuskaavan mukaisesti

$$\text{(1.3)} \qquad \begin{aligned} s_{i+1} &= s_{i-1} - q_i\, s_i, \\ t_{i+1} &= t_{i-1} - q_i\, t_i. \end{aligned}$$

Päiväys: 1.11.2011.

Tällöin yhtälöstä (**??**) seuraa, että jos $s_k\,r_0 + t_k\,r_1 = r_k$ arvoilla $k = i-1$ ja $k = i$ ja kertoimet s_k ja t_k on määrätty palautuskaavojen (**??**) avulla, niin yhtälö $s_k\,r_0 + t_k\,r_1 = r_k$ on voimassa myös, kun $k = i+1$. Riittää siis löytää sopivat aloitusarvot. Tällaiset ovat

$$s_0 = 1, \quad t_0 = 0, \quad s_1 = 0, \quad t_1 = 1.$$

Laajennetussa Eukleideen algoritmissa määrätään luvut ℓ, q_i, $r_i \in \mathbb{N}$, s_i, $t_i \in \mathbb{Z}$, $1 \leq i \leq \ell$, siten, että $0 \leq r_{i-1} < r_i$, kun $1 \leq i \leq \ell$, ja

$$\begin{cases} s_0 = 1, \quad t_0 = 0 \\ s_1 = 0, \quad t_1 = 1 \\ r_{i-1} = q_i\,r_i + r_{i+1} \\ s_{i-1} = q_i\,s_i + s_{i+1} \\ t_{i-1} = q_i\,t_i + t_{i+1} \end{cases} \tag{1.4}$$

Tällöin $s_i\,r_0 + t_i\,r_1 = r_i$ kaikille $0 \leq i \leq \ell$ ja $r_\ell = \operatorname{syt}(r_0, r_1)$.

Lisätietoa laajennetusta Eukleideen algoritmista löytyy kirjoista [**?**, §3.2], [**?**, §4.5.2].

Huomautus 1.1. Suurimman yhteisen tekijän määrääminen Eukleideen algoritmilla vaatii enintään $1 + \log r_1 / \log \Theta$ jakoyhtälöä, missä $\$\Theta := (1+\sqrt{5})/2$. "Hitain" tapaus syntyy Fibonaccin lukujen kohdalla. Laajennettu Eukleideen algoritmi on laskennallisesti tehokas tapa laskea $\operatorname{syt}(r_0, r_1)$ ja samalla ratkaista Diofantoksen yhtälö $x\,r_0 + y\,r_1 = \operatorname{syt}(r_0, r_1)$. [**?**, §1.10], [**?**, §1.2.1].

Esimerkki 1.2. Laajennetun Eukleideen algoritmi voidaan kirjata taulukoksi:

i	r_i	s_i	t_i
0	126	1	0
1	35	0	1
2	21	1	−3
3	14	−1	4
4	7	2	−7
5	0	−5	18

Riviltä $i = 4$ saadaan
$r_4 = \operatorname{syt}(r_0, r_1) = s_4 r_0 + t_4 r_1$, eli
$7 = \operatorname{syt}(126, 35) = 2 \cdot 126 - 7 \cdot 35$.

2. Toistettu neliöinti

Jos potenssin a^n lasketaan potenssin määrittelevän rekursion $a^n := a \cdot a^{n-1}$, $a^1 := a$, avulla, tarvitaan $n-1$ kertolaskua. Laskemista voidaan nopeuttaa huomattavasti seuraavasti ([**?**, §4.3]):

1° Esitetään luku $n \in \mathbb{Z}_+$ kaksikantaisena muodossa $n = 2^k + d_{k-1}\,2^{k-1} + \cdots + d_1\,2 + d_0$, missä $d_{k-1}, \ldots, d_1, d_0 \in \{0, 1\}$.

2° Asetetaan $b_k := a$.

3° Kun $j = k-1,\ k-2, \ldots,\ 1,\ 0$, asetetaan

$$\begin{cases} b_j := b_{j+1}^2\,a, & \text{jos } n_j = 1, \\ b_j := b_{j+1}^2, & \text{muuten.} \end{cases}$$

Edellä lasketun jonon viimeinen alkio $b_0 = a^n$ (todistus jätetään lukijan tehtäväksi).

Kun potenssi a^n lasketaan tällä algoritmilla, tarvitaan $k = \lfloor \log_2 n \rfloor$ neliöintiä ja enintään yhtä monta kertolaskua ($\log_2 n$ on luvun n kaksikantainen logaritmi). Kaikenkaikkiaan kertolaskujen lukumäärä on enintään $2\,\lfloor \log_2 n \rfloor$.

3. Äärellisen kunnan primitiivinen elementti

Ryhmän G *alkion* a *kertaluku* on pienin positiivinen kokonaisluku k siten, että $a^k = 1$, jos tällainen luku on olemassa. Alkion a kertalukua merkitään $\operatorname{ord}(a)$. *Alkion* a *virittämä syklinen aliryhmä* on $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$. Jos alkion a kertaluku k on äärellinen, niin $\langle a\rangle = \{1, a, a^2, \ldots, a^{k-1}\}$.

Lemma 3.1. *Olkoot G äärellinen syklinen ryhmä ja a, $b \in G$ siten, että niiden kertaluvut ovat keskenään jaottomat,* $\operatorname{syt}(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$.

Tällöin $\operatorname{ord}(a\,b) = \operatorname{ord}(a)\,\operatorname{ord}(b)$.

Olkoon K äärellinen kunta, jossa on p^n alkiota ($K = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, p alkuluku[1], tai $K = \mathbb{F}_{p^n} =$ *Galois'n kunta*, jossa on p^n alkiota, $n \in \mathbb{Z}_+$). Fermat'n pienen lauseen nojalla jokainen $a \in K^\times := K \setminus \{0\}$ toteuttaa yhtälön $a^{q-1} = 1$. Tästä seuraa, että jokaisen alkion $a \in K^\times$ kertaluku on luvun $q-1$ tekijä. Alkio $g \in K^\times$ on *kunnan* K *primitiivinen elementti*, jos sen kertaluku on $q-1$. Tällöin siis $K^\times = \langle g\rangle$.

Äärellisellä kunnalla on aina primitiivinen elementti. Ryhmäteorian kielellä ilmaistuna: multiplikatiivinen ryhmä $K^\times$ on syklinen. Itse asiassa, jokaiselle luvun $q-1$ tekijälle k kunnassa K on täsmälleen $\varphi(k)$ alkiota, jonka kertaluku on k (ks. [**?**, §2.8, 2.20, 2.21]). Tässä φ on Eulerin φ-funktio, $\varphi(n) :=$ joukon $\{k \in \mathbb{Z} \mid 1 \le k \le n$ ja $\operatorname{syt}(k, n) = 1\}$ alkioiden lukumäärä. Erityisesti q-alkioisessa kunnassa primitiivisiä elementtejä on $\varphi(q-1)$ kappaletta. Nämä tulokset todistetaan usein kauniin φ-funktiokaavan avulla:

$$\sum_{d|n} \varphi(d) = n.$$

Gaussin algoritmi primitiivisen elementin määräämiseksi:

1° Valitaan $a_1 \in K$, $a_1 \neq 0$. Olkoon $t_1 := \operatorname{ord}(a_1)$.
2° Jos $t_1 = q-1$, niin a_1 on kunnan K primitiivinen elementti.
3° Jos $t_1 < q-1$, valitaan $b \in K \setminus \langle a_1\rangle$. Olkoon $s := \operatorname{ord}(b)$. Jos $s = q-1$, niin b on kunnan K primitiivinen elementti.
4° Jos $s < q-1$, määrätään luvut d ja $e \in \mathbb{Z}_+$ siten, että $d|t_1$, $e|s$, $\operatorname{syt}(d, e) = 1$ ja $d\,e = \operatorname{pyj}(t_1, s)$. Asetetaan $a_2 := a_1^{t_1/d}\, b^{s/e}$ ja $t_2 := \operatorname{pyj}(t_1, s)$. Vaihdetaan edellä alion a_1 tilalle a_2 ja luvun t_1 tilalle t_2, ja toistetaan kohdasta 2°.

Todistuksen sijasta annamme muutaman kommentin:

(i) Alkion b kertaluku ei voi olla luvun tekijä; muutoin olisi $b^{t_1} = 1$, jolloin b olisi yhtälön $x^{t_1} - 1 = 0$ juuri. Mutta tällä yhtälöllä on jo t_1 eri juurta a_1^j, $1 \le j \le t_1$. Tästä seuraa myös, että $\operatorname{pyj}(t_1, s) > t_1$.
(ii) Kohdan 4° väite luvuille d ja e on yleinen: Kun $m \in \mathbb{Z}_+$ ja $n \in \mathbb{Z}_+$, niin on olemassa luvut d ja e siten, että $d|m$, $e|n$, $\operatorname{syt}(d, e) = 1$ ja $d\,e = \operatorname{pyj}(m, n)$. Väite on helppo todistaa esimerkiksi aritmetiikan peruslauseen avulla (ja jätetään lukijan tehtäväksi).
(iii) Kohdassa 4° alkion $a_1^{t_1/d}$ kertaluku on d ja alkion $b^{s/e}$ kertaluku on e. Edellisen lemman nojalla näiden tulon kertaluku on $d\,e = \operatorname{pyj}(t_1, s) > t_1$.

[1]Merkintää $\mathbb{Z}_n$ käytetään usein lyhenteenä kokonaislukujen jäännösluokkarenkaalle $\mathbb{Z}/n\mathbb{Z}$. Toisaalta, joissakin lukuteorian ja algebran esityksissä merkintä $\mathbb{Z}_p$, kun p on alkuluku, on varattu ns. *p-adisten lukujen kunnalle*, joka on täysin eri asia kuin kunta $\mathbb{Z}/p\mathbb{Z}$. Merkintä $\mathbb{F}_p$ ei aiheuta sekaannusta, mutta ei liene kovin yleisesti käytetty jäännösluokkakunnan $\mathbb{Z}/p\mathbb{Z}$ kohdalla.

3.1. Miten luvut d ja e valitaan, jos $m := 150$, $n := 225$, ja on oltava $d|m$, $e|n$, $\operatorname{syt}(d,e) = 1$ ja $d\,e = \operatorname{pyj}(m,n)$?

3.2. Jos et aiemmin ole osoittanut, niin osoita nyt: Kun $p_1, \ldots, p_k$ ovat keskenään erisuuria alkulukuja ja

$$m = p_1^{m_1} \ldots p_k^{m_k} \quad \text{ja} \quad n = p_1^{n_1} \ldots p_k^{n_k},$$

niin [2]

$$\operatorname{syt}(m,n) = p_1^{\min(m_1,n_1)} \ldots p_k^{\min(m_k,n_k)} \quad \text{ja} \quad \operatorname{pyj}(m,n) = p_1^{\max(m_1,n_1)} \ldots p_k^{\max(m_k,n_k)}.$$

3.3. Osoita aritmetiikan peruslauseen (tms) avulla, että kaikille m, $n \in \mathbb{Z}_+$ on olemassa luvut d ja e siten, että $d|m$, $e|n$, $\operatorname{syt}(d,e) = 1$ ja $d\,e = \operatorname{pyj}(m,n)$.

3.4. Olkoot a, b, $m \in \mathbb{Z}_+$, $m > 1$. Osoita, että yhtälöllä $a\,x \equiv b \bmod m$ on ratkaisu $x \in \mathbb{Z}$ jos ja vain jos $\operatorname{syt}(a,m) \mid b$.

3.5. Olkoon p pariton alkuluku ja g kunnan $\mathbb{Z}_p$ primitiivinen alkio. Olkoon $n \in \mathbb{N}$, $n > 0$. Selvitä miten yhtälö $x^2 = g^n$, $x \in \mathbb{Z}_p$, voidaan palauttaa kokonaislukujen kongruenssiyhtälöksi $2k \equiv n \bmod (p-1)$, $k \in \mathbb{Z}$. Millä ehdolla yhtälöllä $x^2 = g^n$ on ratkaisu?

4. Neliöjäännökset

Olkoon $p > 2$ alkuluku. Luku $a \in \mathbb{Z}$ on *neliöjäännös modulo* p, jos on olemassa $b \in \mathbb{Z}$ siten, että $a \equiv b^2 \bmod p$. *Legendren symboli* $\left(\frac{a}{p}\right)$ kertoo onko a neliöjäännös modulo p; tarkemmin

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{jos } a \equiv 0 \bmod p; \\ 1, & \text{jos } a \text{ on neliöjäännös modulo } p; \\ -1, & \text{jos } a \text{ ei ole neliöjäännös modulo } p. \end{cases}$$

Legendren symboli on helppo laskea toistetun neliöinnin avulla seuraavan tuloksen nojalla (todistus jää lukijan tehtäväksi):

Lause 4.1.

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p.$$

Yleisemmästä *Jacobin symbolista* käytetään samaa merkintää kuin Legendren symbolista, mutta Jacobin symbolissa luvun p ei tarvitse olla alkuluku. Jacobin symbolista ei toisaalta saa tärkeätä tietoa: jos $\left(\frac{a}{n}\right) = 1$, niin a on neliöjäännös modulo n.

Jos a on neliöjäännös modulo p ja $p \equiv 3 \bmod 4$, voidaan alkion a neliöjuuri modulo p määrätä helposti toistetun neliöinnin avulla; ks. **??**. Tarkastellaan seuraavaksi tapausta, missä n on kahden keskenään erisuuren alkuluvun p ja q tulo, $n = p\,q$.

Oletetaan, että a on neliöjäännös modulo n. Tällöin a on neliöjäännös modulo p ja modulo q. Olkoot c_p ja c_q luvut, joille

$$c_p^2 \equiv a \bmod p \quad \text{ja} \quad c_q^2 \equiv a \bmod q.$$

[2] Kirjassa [**?**, §4.5] ehdotetaan varsin nättiä merkintää $m \perp n$ tarkoittamaan lukujen m ja n keskenään jaottomuutta (eli sitä, että $\operatorname{syt}(m,n) = 1$)! Tämä tarkoittaisi siis alkulukujen $p_1, \ldots, p_k$ eksponenteille ehtoja $\min(m_1,n_1) = 0, \ldots, \min(m_k,n_k) = 0$, t.s. $m_1\,n_1 = 0, \ldots, m_k\,n_k = 0$.

Koska $\mathrm{syt}(p, q) = 1$, voidaan laajennetun Eukleideen algoritmilla avulla määrätä luvut x_p ja x_q siten, että

$$x_p\, p + x_q\, q = \mathrm{syt}(p, q) = 1.$$

Olkoot

$$r := c_q\, x_p\, p + c_p\, x_q\, q \bmod n \quad \text{ja} \quad s := c_q\, x_p\, p - c_p\, x_q\, q \bmod n$$

Harjoitustehtäväksi jää osoittaa, että luvut $\pm r \bmod n$ ja $\pm s \bmod n$ (kaikki neljä) ovat luvun a neliöjuuria modulo n.

4.1. Olkoon p alkuluku siten, että $p \equiv 3 \bmod 4$. Oletetaan, että a on neliöjäännös modulo p. Osoita, että $c := a^{(p+1)/4}$ on luvun a neliöjuuri modulo p, t.s. $c^2 \equiv a \bmod p$.

4.2. Olkoon p pariton alkuluku, ja $a \in \mathbb{Z}_p$, $a \not\equiv 0$. Osoita, että alkiolla a on neliöjuuri, jos ja vain jos

$$a^{(p-1)/2} = 1.$$

[Vihje: Osoita aluksi, että yhtälöllä $x^2 = 1$ on kunnassa $\mathbb{Z}_p$ täsmälleen kaksi ratkaisua, $x = 1$ ja $x = -1$; tehtävä **??** saattaa myös auttaa.]

4.3. Olkoon $p > 2$ alkuluku. Osoita, että kunnassa $\mathbb{Z}_p$ on tasan $(p-1)/2$ nollasta eroavaa alkiota, joilla on neliöjuuri kunnassa $\mathbb{Z}_p$, ja tasan $(p-1)/2$ alkiota, joilla ei ole.

Viitteet

[1] Johannes A. Buchmann: *Introduction to cryptography*, Undergraduate Texts in Mathematics, Springer, 2001.

[2] Joachim von zur Gathen ja Jürgen Gerhard: *Modern computer algebra*. Cambridge University Press, 1999.

[3] Ronald L. Graham, Donald E. Knuth ja Oren Patashnik: *Concrete mathematics: A foundation for computer science*. toinen laitos, Addison-Wesley, 1994.

[4] Lars Gårding ja Torbjörn Tambour: *Algebra for computer science*. Universitytext, Springer-Verlag, 1988.

[5] Donald E. Knuth: *The art of computer programming*, Vol. 1, *Fundamental algorithms*. Addison-Wesley, 1968; kolmas laitos, 1997.

[6] Donald E. Knuth: *The art of computer programming*, Vol. 2, *Seminumerical algorithms*. Addison-Wesley, 1969; kolmas laitos, 1998.

[7] Neal Koblitz: *A course in number theory and cryptography*, toinen laitos, Springer, 1994.

[8] Robert J. McEliece: *Finite fields for computer sciencists and engineers*, Kluwer Acaademic Publishers, 1987.

[9] Frithiof Nevanlinna: *Einführung in die Algebra und die Theorie der algebraischen Gleichungen*, Birkhäuser Verlag, 1965.