Primitiivijuurista

Tässä lyhyessä koosteessa kerrotaan, että jokaiseen alkulukuun $p > 2$ liittyy ainakin yksi *primitiivijuuri*. Se on p:llä jaoton luku a, jolle kongruenssi $a^b \equiv 1 \bmod p$ ei päde millään $b < p - 1$. Asia ei ole aivan triviaali, mutta sen tunteminen näkyy olevan oletuksena joissakin matematiikkakilpailutehtävissä. – Seikkaperäisemmin tästä on esityksessä `http://matematiikkakilpailut.fi/kirjallisuus/laajalukuteoriamoniste.pdf`.

Kongruenssiyhtälön juurien lukumäärä

Olkoon p alkuluku ja

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \tag{1}$$

koknaislukukertoiminen n:nnen asteen polynomi sekä s.y.t.$(a_n, p) = 1$. Yhtälö $f(x) \equiv 0 \bmod p$ on *n:nnen asteen kongruenssiyhtälö.* Osoitetaan induktiolla n:n suhteen, että tällaisella yhtälöllä on enintään n keskenään modulo p epäkongruenttia ratkaisua. Jos $n = 1$, asia on selvä. Jos $ax_1 + b \equiv 0 \bmod p$ ja $ax_2 + b \equiv 0 \bmod p$, niin $a(x_1 - x_2) \equiv 0 \bmod p$, ja koska s.y.t.$(a, p) = 1$, niin $x_1 \equiv x_2 \bmod p$. Oletetaan sitten, että väite on tosi astetta $k < n$ oleville kongruenssiyhtälöille. Oletetaan, että f on niin kuin kaavassa (1) ja että on $n + 1$ keskenään modulo p epäkongruenttia lukua $x = x_1, x_2, \ldots, x_n, x_{n+1}$, jotka toteuttavat kongruenssiyhtälön $f(x) \equiv 0 \bmod p$. Silloin

$$g(x) = f(x) - a_n(x - x_1)(x - x_2) \cdots (x - x_n)$$

on astetta $n - 1$ oleva polynomi, ja kongruenssiyhtälöllä $g(x) \equiv 0 \bmod p$ on n keskenään epäkongruenttia ratkaisua. Induktio-oletuksen mukaan tämä on mahdollista vain, jos $g(x)$:n korkeimmanasteisen termin kerroin on jaollinen p:llä. päättelyä jatkamalla tullaan siihen, että polynomin $g(x)$ kaikki kertoimet ovat p:llä jaollisia, joten $g(x) \equiv 0 \bmod p$ kaikilla x. Siis erityisesti $g(x_{n+1}) \equiv 0 \bmod p$. Mutta koska myös $f(x_{n+1}) \equiv 0 \bmod p$, on $a_n(x_{n+1} - x_1)(x_{n+1} - x_2) \cdots (x_{n+1} - x_n) \equiv 0 \bmod p$. Tämä on mahdollista vain, jos jokin tulon tekijä on jaollinen p:llä eli $x_{n+1} \equiv x_j \bmod p$ jollain j. Tämä on ristiriidassa luvuista x_j tehdyn epäkongruenttisuusoletuksen kanssa, joten induktioaskel on otettu ja väite todistettu.

Edellisestä tuloksesta seuraa, että kongruenssilla $x^n - 1 \equiv 0 \bmod p$ on enintään n keskenään epäkongruenttia ratkaisua.

Primitiivijuuren määritelmä

Eulerin funktio ϕ määritellään niin, että $\phi(m)$ on niiden kokonaislukujen a, $1 \le a \le n - 1$, lukumäärä, joille s.y.t.$(a, m) = 1$. *Eulerin lause* sanoo, että $a^{\phi(m)} \equiv 1 \bmod m$ aina, kun s.y.t.$(a, m) = 1$.

Olkoon $a > 1$ ja s.y.t.$(a, m) = 1$. On olemassa lukuja γ, joille $a^\gamma \equiv 1 \bmod m$. Yksi tällainen on $\phi(m)$, mutta pienempikin luku voi tulla kyseeseen. Esimerkiksi $2^3 \equiv 1 \bmod 7$.

Pienin γ, jolle $a^\gamma \equiv 1 \bmod m$ on *a:n indeksi modulo m*. Olkoon tämä pienin luku δ. Sanotaan, että *a kuuluu eksponenttiin δ* mod m.

Jos a kuuluu eksponenttiin δ mod m ja jos $0 \leq p < q < \delta$, niin ei voi olla $a^p \equiv a^q \bmod m$. Jos näin olisi, olisi $a^p(a^{q-p}-1) \equiv 0 \bmod m$, ja koska s.y.t.$(a,\, m) = 1$, olisi $a^{q-p} \equiv 1 \bmod m$, mikä olisi ristiriidassa δ:n minimiominaisuuden kanssa.

Jos $a^\gamma \equiv a^{\gamma'} \bmod m$, niin $\gamma \equiv \gamma' \bmod \delta$. Olkoon nimittäin $\gamma = q\delta + r$ ja $\gamma' = q'\delta + r'$, $0 \leq r,\, r' < \delta$. Silloin $a^\gamma = \left(a^\delta\right)^q a^r \equiv a^r \bmod m$ ja vastaavasti $a^{\gamma'} \equiv a^{r'} \bmod m$. Edellisen kappaleen mukaan $a^r \equiv a^{r'} \bmod m$ on mahdollinen vain, jos $r = r'$ eli $\gamma - \gamma' \equiv 0 \bmod m$. – Jos $\gamma \equiv \gamma' \bmod \delta$, niin $\gamma = q\delta + r$ ja $\gamma' = q'\delta + r$, jolloin $a^\gamma = \left(a^\delta\right)^q a^r \equiv a^r \bmod m$ ja samoin $a^{\gamma'} \equiv a^r \bmod m$, joten $a^\gamma \equiv a^{\gamma'} \bmod m$.

Erityisesti $a^\gamma \equiv 1$ jos ja vain jos $\delta|\gamma$. Täten jokaisella a se eksponentti, johon a kuuluu mod m, on luvun $\phi(m)$ tekijä.

Luvut, jotka kuuluvat eksponenttiin $\phi(m)$ mod m ovat *primitiivijuuria* modulo m. Jos p on alkuluku, niin $\phi(p) = p - 1$.

Primitiivijuuret modulo alkuluku

Oletetaan, että x kuuluu eksponenttiin ab mod m. Silloin $x^{ab} \equiv 1 \bmod m$. Tarkastellaan lukua x^a. Oletetaan, että x^a kuuluu eksponenttiin δ mod m. Silloin $x^{a\delta} \equiv 1 \bmod m$. Yllä sanotuin nojalla $(ab)|(a\delta)$ joten $b|\delta$. Mutta koska $(x^a)^b \equiv 1 \bmod m$, niin $\delta|b$. Siis onkin $\delta = b$. Oletuksesta, että x kuuluu eksponenttiin ab seuraa, että x^a kuuluu eksponenttiin b modulo m.

Olkoot a ja b kaksi lukua, joille s.y.t.$(a,\, b) = 1$. Kuulukoon x eksponenttiin a ja y eksponenttiin b modulo m. Tarkastellaan lukua xy. Oletetaan, että se kuuluu eksponenttiin δ mod m. Silloin $x^\delta y^\delta \equiv 1 \bmod m$ ja edelleen $x^{b\delta}y^{b\delta} \equiv 1 \bmod m$. Mutta tästä seuraa, että $x^{b\delta} \equiv 1 \bmod m$ ja edelleen, että $a|b\delta$. Koska $(a,\, b) = 1$, on oltava $a|\delta$. Samoin osoitetaan, että $b|\delta$. Jos kaksi yheistekijätöntä lukua ovat δ:n tekijöitä, niiden tulokin on: $ab|\delta$. Mutta toisaalta $(xy)^{ab} = (x^a)^b(y^b)^a \equiv 1 \bmod m$, joten $\delta|(ab)$. Siis $ab = \delta$. Tulo xy kuuluu siis eksponenttiin ab.

Olkoon nyt $p > 2$ alkuluku. Luvut $1,\, 2,\, \ldots,\, p-1$ kuuluvat jokainen johonkin eksponenttiin mod p. Olkoot $\delta_1,\, \delta_2,\, \ldots,\, \delta_r$ tällaiset eksponentit. Jokainen δ_j on luvun $p-1$ tekijä. Olkoon sitten τ näiden lukujen pienin yhteinen monikerta. Luvulla τ on kanoninen alkulukuhajotelma $\tau = q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_k^{\alpha_k}$. Olkoon $1 \leq s \leq k$. Jokin luvuista δ_j on jaollinen luvulla $q_s^{\alpha_s}$; olkoon se luku δ. Siis $\delta = aq_s^{\alpha_s}$. Jos x on luku, joka kuuluu eksponenttiin δ, niin aikaisemmin sanotun perusteella x^a kuuluu eksponenttiin $q_s^{\alpha_s}$. Merkitään lukua x^a x_s:llä. Sama pätee kaikille $s = 1,\, \ldots,\, k$. Voidaan muodostaa luku $g = x_1x_2\cdots x_s$. Koska eri luvuilla x_s ei ole yhteisiä tekijöitä, g kuuluu eksponenttiin $q_1^{\alpha_1}\cdots q_k^{\alpha_k} = \tau$. Jokainen δ_j on τ:n tekijä. Jokaiselle luvuista $x = 1,\, 2,\, \ldots,\, p-1$ pätee $x^{\delta_j} \equiv 1 \bmod p$ jollain δ_j. Mutta silloin jokaiselle tällaiselle x pätee $x^\tau \equiv 1 \bmod p$.

Astetta τ olevalla kongruenssilla on enintään τ eri ratkaisua. Siis $p - 1 \leq \tau$. Mutta koska jokainen δ_j on $p-1$:n tekijä, on myös lukujen δ_i pienin yhteinen monikerta eli τ on $p-1$:n tekijä. Siis $\tau \leq p - 1$, ja g on primitiivinen juuri mod p.