Carmichaelin lukujen konstruktioista
Esitelmä lukuteorian päivillä 1995

Matti K. Sinisalo

1995

Fermat'n pienen lauseen mukaan jokaisella alkuluvulla p ja jokaisella kokonaisluvulla a, jolla $\gcd(p, a) = 1$ (ts. a ei ole jaollinen luvulla p), on

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Kääntäen, jos n on positiivinen kokonaisluku, a sellainen kokonaisluku, että $\gcd(n, a) = 1$ ja $a^{n-1} - 1$ ei ole tasan jaollinen luvulla n, niin n on yhdistetty luku. Fermat'n pientä lausetta voidaan siis käyttää luvun osoittamiseen yhdistetyksi luvuksi.

On kuitenkin olemassa sellaisia yhdistettyjä lukuja, joita ei voida osoittaa yhdistetyiksi Fermat'n pientä lausetta käyttäen. Näitä lukuja sanotaan *Carmichaelin luvuiksi*.

Äskettäin on todistettu, että Carmichaelin lukuja on ääretön määrä [**Alford**]. Tässä esitelmässä tarkastelemme todistuksessa käytettyä Carmichaelin lukujen konstruktiota.

1. Carmichaelin funktiosta

Kokonaisluvun b kertalukua modulo $n > 0$ merkitsemme $\mathrm{ord}_n(b)$.

Carmichaelin funktiolla $\lambda : \mathbb{Z}^+ \to \mathbb{Z}^+$ tarkoitamme ryhmän $\mathbb{Z}_n^*$ yleistä kertalukua ts. pienintä sellaista kokonaislukua k, että $b^k \equiv 1 \pmod{n}$ kaikilla b, $\gcd(b, n) = 1$.

Carmichaelin funktiolle pätee $\lambda(n) = \mathrm{lcm}_{\gcd(b,n)=1}(\mathrm{ord}_n(b))$.

Edelleen funktiolle saadaan seuraavat laskusäännöt:

$$\lambda(2) = 1,$$

$$\lambda(4) = 2,$$

$$\lambda(2^k) = \frac{1}{2}\varphi(2^k) = 2^{k-2}, \text{ kun } k \geq 3,$$

$$\lambda(p^k) = \varphi(p^k) = p^{k-1}(p-1), \text{ kun } p \geq 3,$$

$$\lambda(n) = \mathrm{lcm}_i(\lambda(p_i^{k_i})), \text{ kun } n = \prod_{i=1}^{r} p_i^{k_i}.$$

Carmichaelin funktio toteuttaa Eulerin lausetta vastaavan tuloksen:

LAUSE 1 (Carmichaelin lause). Olkoot $n > 0$ ja b kokonaislukuja ja $\gcd(n, b) = 1$. Tällöin $b^{\lambda(n)} \equiv 1 \pmod{n}$.

Erityisesti $\lambda(n)|\varphi(n)$ kaikilla $n > 0$.

2. Pseudoalkuluvuista

Pseudoalkuluvuilla tarkoitetaan yhdistettyjä lukuja, joilla on tiettyjä alkulukujen ominaisuuksia.

Määritelmä. Yhdistettyä lukua $n > 0$ sanomme *kannan* $b > 0$ *pseudoalkuluvuksi*, mikäli $b^{n-1} \equiv 1 \pmod{n}$.

Yhdistetty luku $n > 0$ on siis kannan b, $\gcd(b, n) = 1$ pseudoalkuluku jos ja vain jos $\mathrm{ord}_n(b)|(n-1)$.

Selvästi jokainen kannan b pseudoalkuluku n toteuttaa ehdon $\gcd(b, n) = 1$.

3. Carmichaelin luvuista

Carmichaelin luvut ovat sellaisia yhdistettyjä lukuja $n > 1$, jotka ovat kaikkien kantojen b, missä $\gcd(b, n) = 1$, pseudoalkulukuja.

Korselt esitti vuonna 1899 kriteerin, jota voidaan käyttää luvun osoittamiseen Carmichaelin luvuksi. Carmichaelin funktiota käyttäen tämä tulos voidaan kirjoittaa seuraavaan muotoon.

LAUSE 2 (Korseltin kriteeri). Luku $n > 1$ on Carmichaelin luku, jos ja vain jos $\lambda(n)|(n-1)$.

Todistus. Oletetaan, että luku $n > 1$ on Carmichaelin luku. Koska $\mathrm{ord}_n(b)|(n-1)$ kaikilla b, $\gcd(b, n) = 1$, niin $\mathrm{lcm}_b(\mathrm{ord}_n(b)) = \lambda(n)|(n-1)$.

Oletetaan toisaalta, että $\lambda(n)|(n-1)$. Tällöin kaikilla b, $\gcd(b, n) = 1$, on $b^{n-1} = (b^{\lambda(n)})^{(n-1)/\lambda(n)} \equiv 1 \pmod{n}$. Siis n on Carmichaelin luku. QED

Korseltin kriteeristä seuraa, että jokainen Carmichaelin luku on pariton.

LAUSE 3 [Carmichael 1912]. Jokainen Carmichaelin luku on neliövapaa.

Todistus. Olkoon $n = p^k m$ Carmichaelin luku, $k \geq 2$, $p > 2$ alkuluku ja luku m ei ole jaollinen luvulla p. Carmichaelin funktion laskusäännöistä ja Korseltin kriteeristä seuraa, että $p|\lambda(p^k)|\lambda(n)|(n-1)$. Tämä on ristiriita. QED

Edelleen Korseltin kriteeristä seuraa, että jokainen Carmichaelin luku on vähintään kolmen erisuuren parittoman alkuluvun tulo.

LAUSE 4 [Carmichael 1912]. Jos alkuluku p jakaa Carmichaelin luvun n, niin $n \equiv 1 \pmod{p-1}$ ja siten $n \equiv p \pmod{p(p-1)}$.

Todistus. Nyt $(p-1)|\lambda(n)|(n-1)$.

Koska $n \equiv 0 \pmod{p}$, $n \equiv 1 \pmod{p-1}$ ja $\gcd(p, p-1) = 1$, niin $n \equiv p \pmod{p(p-1)}$. QED

Chernick esitti vuonna 1939 seuraavaa menettelytapaa Carmichaelin lukujen konstruoimiseksi.

LAUSE 5 [Chernick 1939]. Olkoot n ja k sellaisia positiivisia kokonaislukuja, että $n = (6k+1)(12k+1)(18k+1)$. Jos $6k+1$, $12k+1$ ja $18k+1$ ovat alkulukuja, niin n on Carmichaelin luku.

Todistus. Lauseen oletuksista seuraa, että $n - 1 = (6k+1)(12k+1)(18k+1) - 1 = 36k(36k^2 + 11k + 1)$ ja toisaalta λ-funktion laskusääntöjen mukaan $\lambda(n) = \mathrm{lcm}(\lambda(6k+1), \lambda(12k+1), \lambda(18k+1)) = \mathrm{lcm}(6k, 12k, 18k) = 36k$. Siten $\lambda(n)|(n-1)$ ja n on Carmichaelin luku. QED

Tämä kaava antaa meille mahdollisuuden toteuttaa helposti Eratostheneen seulan tyyppisen seulan (kolminkertainen seula), jonka avulla voimme muutamassa minuutissa tuottaa kymmeniä tuhansia kolmen alkulukutekijän Carmichaelin lukuja.

Seulamenetelmää kokeiltiin kirjoittamalla lyhyt FORTRAN-ohjelma WAGON 486/33 MHz -mikrotietokoneelle. Väliltä $1 \le k \le 3 \cdot 10^6$ löytyi 12306 yo. tyyppiä olevaa Carmichaelin lukua. Ohjelman ajo kesti noin 3 minuuttia.

Vastaavan tyyppisiä parvia voidaan konstruoida myös muilla kertoimien valinnoilla. Granville [Granville 1992] antaa seuraavat esimerkit:

$$(12k+5)(36k+13)(48k+17),$$

$$(28k+5)(112k+17)(196k+29),$$

$$(30k+7)(60k+13)(150k+31),$$

$$(180k+7)(300k+11)(360k+13)(1200k+41).$$

Yleisemmin toteutuu seuraava tulos.

LAUSE 6. Olkoot $1 \ge a_1 < a_2 < ... < a_r$ sellaisia kokonaislukuja, että

$$\mathrm{lcm}(a_1, a_2, ..., a_r) \left| \left(2^{s-1} \sum_{1 \le j_1 < j_2 < ... < j_s \le r} a_{j_1} a_{j_2} \cdots a_{j_s} \right) \right.$$

kaikilla $s = 1, 2, ..., r$. Olkoon m sellainen positiivinen kokonaisluku, että $2a_k m + 1$ on alkuluku jokaisella $k = 1, 2, ..., r$. Tällöin $n_m = \prod_{i=1}^{r}(2a_i m + 1)$ on Carmichaelin luku.

Todistus. Koska luvut $2a_1m+1, 2a_2m+1, ..., 2a_rm+1$ ovat erisuuria parittomia alkulukuja, on λ-funktion laskusääntöjen mukaan $\lambda(n_m) = 2m\text{lcm}(a_1, a_2, ..., a_m)$. Toisaalta

$$n_m - 1 = \sum_{s=1}^{r} \left(\sum_{1 \le j_1 < j_2 < \ldots < j_s \le r} a_{j_1} a_{j_2} \cdots a_{j_s} \right) 2^s m^s$$

$$= 2m \sum_{s=1}^{r} \left(2^{s-1} \sum_{1 \le j_1 < j_2 < \ldots < j_s \le r} a_{j_1} a_{j_2} \cdots a_{j_s} \right) m^{s-1}.$$

Siis $\lambda(n_m)|(n_m - 1)$, joten n_m on Carmichaelin luku. QED

Lausetta 6 käyttäen voidaan todistaa:

LAUSE 7. Olkoot $r \ge 4$ ja $m \ge 1$ kokonaislukuja ja

$$n_m = (2^{r-3}3m + 1)(2^{r-2}3m + 1) \prod_{i=3}^{r} (2^{r-6+i}9m + 1).$$

Jos kaikki r oikean puolen tekijää ovat alkulukuja, niin n_m on Carmichaelin luku.

M. Yorinaga [Yorinaga 1978] ja S. Wagstaff [Wagstaff 1980] ovat käyttäneet tätä menetelmää suurten Carmichaelin lukujen konstruoimiseen.

Tiettyä rajaa x pienempien Carmichaelin lukujen lukumäärää $C(x)$ esittää seuraava taulukko [Granville 1992]:

x	$C(x)$	$\frac{\log(C(x))}{\log(x)}$	Vuosi	Tutkijat
10^3	1		1910	Carmichael
10^4	7	0.211	1912	Carmichael
10^5	16	0.241		
10^6	43	0.272		
10^7	105	0.289		
10^8	255	0.301	1938	Poulet
10^9	646	0.312	1975	Swift
10^{10}	1547	0.319		
$2.5 \cdot 10^{10}$	2163	0.321	1980	Pomer., Selfr., Wagst.
10^{11}	3605	0.323		
10^{12}	8241	0.326	1990	Jaeschke
10^{13}	19279	0.330		
10^{14}	44706	0.332		
10^{15}	105212	0.335	1993	Pinch

Taulukon perusteella näyttää ilmeiseltä, että Carmichaelin lukuja on olemassa äärettömän paljon, joskin ne ovat melko harvinaisia. Erdös osoitti vuonna

1949, miten harvinaisia Carmichaelin luvut ovat. Hän todisti nimittäin, että Carmichaelin lukujen käänteislukujen summa suppenee.

Edellä olevaan taulukkoon on laskettu myös luvun $\log(C(x))/\log(x)$ likiarvot. Erdös esitti tarkastelujensa perusteella konjektuurin, jonka mukaan tämä suhde lähestyy lukua 1, kun x lähestyy ääretöntä.

Erdös vuonna 1956 esittämä uusi tapa Carmichaelin lukujen konstruoimiseksi on seuraava.

LAUSE 8 (Erdösin konstruktio Carmichaelin luvuille). Olkoon L positiivinen kokonaisluku. Olkoot $p_1, p_2, ..., p_s$ sellaisia erisuuria parittomia alkulukuja, että kaikilla $i = 1, 2, ..., s$ $(p_i - 1)|L$. Jos $n = p_1 p_2 \cdots p_s \equiv 1 \pmod{L}$, niin n on Carmichaelin luku.

Todistus. Nyt jokaisella $i = 1, 2, ..., s$ on $(p_i - 1)|L|(n-1)$, joten $(p_i - 1)|(n-1)$. Siten $\text{lcm}(p_1 - 1, p_2 - 1, ...p_s - 1)|(n-1)$ ts. $\lambda(n)|(n-1)$ ja n on Carmichaelin luku. QED

Lähtiessämme soveltamaan tätä lausetta Carmichaelin lukujen konstruoimiseen voimme lukuja $p_1, p_2, ...p_r$ valitessamme hylätä ensimmäiseksi sellaiset ehdon $(p-1)|L$ toteuttavat alkuluvut p, joilla myös $p|L$. Tällöin nimittäin ehto $n \equiv 1 \pmod{L}$ ei voi toteutua.

Käytämme Erdösin konstruktiota siis seuraavasti:
(i) Valitsemme kokonaisluvun L (joka hajoaa pieniin tekijöihin).
(ii) Muodostamme kaikkien sellaisten alkulukujen p joukon P, joilla $(p-1)|L$, mutta p ei jaa lukua L.
(iii) Valitsemme joukon P alkuluvuista sellaisen osajoukon, että niiden tulo $\equiv 1 \pmod{L}$.
Tällöin ko. tulo on Carmichaelin luku.

Alford ilmoitti [Granville 1992] vuoden 1991 alussa osoittaneensa olevan olemassa vähintään 2^{128} Carmichaelin lukua. Tulos perustui laskennallisesti tehokkaaseen muunnelmaan Erdösin konstruktiosta.

Alfordin konstruktio on seuraava.

LAUSE 9. Muodostamme luvun L ja alkulukujoukon P kuten Erdösin konstruktion kohdissa (i) ja (ii). Tämän jälkeen
(iii') etsimme sellaisen sellaisen joukon P osajoukon Q, jonka alkioiden erilaisia neliövapaita tuloja vastaavat jäännösluokat modulo L peittävät multiplikatiivisen ryhmän $\mathbf{Z}_L^*$.
Tällöin jokaista joukon $R = P \setminus Q$ alkioiden erilaista neliövapaata tuloa vastaa erilainen Carmichaelin luku.

Todistus. Olkoot $q_1, q_2, \cdots q_r \in R$ erisuuria. Tällöin on olemassa sellainen joukon Q alkioiden osajoukko $\{p_1, p_2, ..., p_k\}$, että $p_1 p_2 \cdots p_k \equiv (q_1 q_2 \cdots q_r)^{-1} \pmod{L}$ ja siten $n = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_r \equiv 1 \pmod{L}$. Erdösin konstruktiosta seuraa, että n on Carmichaelin luku.

Selvästi jokaista joukon R alkioiden erilaista neliövapaata tuloa vastaa erilainen Carmichaelin luku. QED

Tuloksena saamme siis $2^{|R|} - 1$ erisuurta Carmichaelin lukua.

Menetelmän etu on siinä, että meidän ei tarvitse kirjoittaa jokaista näin saatavaa Carmichaelin lukua eksplisiittisesti.

Vaikeutena on joukon Q löytäminen kohdassa (iii'). Joukko Q voidaan muodostaa lähtemällä tyhjästä joukosta ja lisäämällä siihen yksitellen joukon P alkioita, kunnes multiplikatiivinen ryhmä $\mathbf{Z}_L^*$ on peitetty.

Käytännössä tämä voidaan suorittaa käsittelemällä sopivasti tietokoneen muistista varattua L-pituista bittivektoria, jonka kukin bitti vastaa yhtä jäännösluokkaa modulo L.

Joukon Q muodostaminen on puhtaasti ryhmäteoreettinen ongelma. Joukon P alkioita vastaavat jäännösluokat modulo L ovat nimittäin multiplikatiivisen ryhmän $\mathbf{Z}_L^*$ alkioita. Tehtävänä on siis muodostaa erään multiplikatiivisen Abelin ryhmän osajoukon alkioista sellainen osajoukko, jonka neliövapaat tulot peittävät ko. Abelin ryhmän.

Alford käytti esimerkkiä $L = 23284800 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11$. Hän löysi kaikkiaan 155 joukkoon P kuuluvaa alkulukua ts. alkulukua $p \geq 13$, joka toteuttaa ehdon $(p-1)|L$. Joukkoon Q tarvittiin näistä 27 pienintä. Joukkoon R jäi $155 - 27 = 128$ lukua ja siten tulokseksi saamme $2^{128} - 1$ erisuurta Carmichaelin lukua.

Alfordin valinta luvun L arvoksi on tietysti vain eräs esimerkki. Muilla valinnoilla voimme päästä yhä suurempiin Carmichaelin lukujen lukumääriin.

Alfordin valintaa paremman tuloksen antaa luku $L = 21621600 = 2^5 \cdot 3^3 \cdot 5^2 7 \cdot 11 \cdot 13$. Tälle luvulle löydämme 186 joukkoon P kuuluvaa alkulukua. Nämä luvut ovat

17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 101, 109, 113, 127, 131, 151, 157, 181, 199, 211, 241, 271, 281, 313, 331, 337, 353, 379, 397, 401, 421, 433, 463, 521, 541, 547, 601, 617, 631, 661, 673, 701, 757, 859, 881, 911, 937, 991, 1009, 1051, 1093, 1171, 1201, 1249, 1301, 1321, 1801, 1873, 1951, 2003, 2017, 2081, 2161, 2311, 2341, 2377, 2521, 2731, 2801, 2861, 2971, 3121, 3169, 3301, 3361, 3433, 3511, 3697, 3851, 4159, 4201, 4621, 4951, 5281, 5851, 6007, 6301, 6553, 7151, 7393, 7561, 7723, 8009, 8191, 8317, 8581, 8737, 9241, 9829, 9901, 11551, 11701, 12601, 13729, 14561, 14851, 15121, 15401, 15601, 16381, 16633, 17551, 18481, 19801, 20021, 20593, 21601, 21841, 23761, 24571, 25741, 26209, 28081, 30241, 34651, 36037, 38611, 39313, 42901, 47521, 48049, 50051, 51481, 54601, 55441, 65521, 66529, 70201, 72073, 79201, 81901, 92401, 93601, 96097, 103951, 108109, 109201, 110881, 118801, 120121, 123553, 131041, 140401, 150151, 151201, 180181, 193051, 196561, 200201, 216217, 218401, 257401, 270271, 300301, 332641, 393121, 415801, 432433, 450451, 540541, 600601, 617761, 800801, 982801, 1029601, 1201201, 2402401, 2702701, 3088801

ja 4324321.

Vaiheen (iiia) toteuttamiseen riittävät näistä alkuluvuista 28 ensimmäistä. Tämä todettiin lyhyellä Oulun Yliopiston IBM-keskustietokoneelle kirjoitetulla Alfordin menetelmää käyttävällä FORTRAN-ohjelmalla. Ohjelman suoritus vaati n. 15 minuuttia keskusyksikköaikaa. Joukko R sisältää siis tässä esimerkissä kaikkiaan $186-28 = 158$ alkulukua ja Carmichaelin lukuja on siis olemassa vähintään $2^{158} - 1 \approx 3.65 \cdot 10^{47}$ kappaletta.

Käytetyillä FORTRAN-ohjelmilla tarkistettiin myös Alfordin esimerkin laskut.

Tutustuttuaan Alfordin ideaan eräät Georgian yliopiston tutkijat arvelivat, että sitä käyttäen voitaisiin myös osoittaa, että on olemassa ääretön määrä Carmichaelin lukuja ja vieläpä saada hyviä asymptoottisia alarajoja näiden lukujen lukumäärille. Menetelmä johtikin näiden vanhojen ongelmien ratkaisuun.

LAUSE 10 (Alford, Granville ja Pomerance 1992). $C(x) > x^{2/7}$, kun x on riittävän suuri kokonaisluku.

Sivuutamme lauseen todistuksen, koska se perustuu pitkälle meneviin analyyttisen lukuteorian tuloksiin [Granville 1992].

Lähdeluettelo

[**Alford**] W. R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (to appear).

[**Beeger 1950**] N. G. W. H. Beeger, *On composite numbers n for which* $a^{n-1} \equiv 1$ *(*mod *n)*, Scripta math., **16**, (1950), 133-135.

[**Carmichael 1909**] R. D. Carmichael, *Note on a new number theory function*, Bulletin of the American Mathematical Society, **16**, (1909-1910), 232-238.

[**Carmichael 1912**] R. D. Carmichael: *On composite numbers P which satisfy the Fermat congruence* $a^{P-1} \equiv 1$ *(*mod *P)*, American Mathematical Monthly, **19**, (1912), 22-27.

[**Chernick 1939**] J. Chernick: *On Fermat's simple theorem*, Bulletin of the American Mathematical Society, **45**, (1939), 269-274.

[**Cipolla 1904**] M. Cipolla: *Sui numeri composti P, che verificano la congruenza di Fermat* $a^{p-1} \equiv 1$ *(*mod *P)*, Annali di Mathematica, **9 (3)**, (1904),

[**Dubner 1989**] H. Dubner: *A new method for producing large Carmichael numbers*, Mathematics of Computation, **53 (187)**, (1989), 411-414.

[**Duparc 1951**] H. J. A. Duparc: *On Carmichael numbers*, Simon Stevin, **29**, (1951/1952), 21-24.

[**Erdös 1949**] P. Erdös: *On the converse of Fermats theorem*, American Mathematical Monthly, **56**, (1949), 623-624.

[**Erdös 1950**] P. Erdös: *On almost primes*, American Mathematical Monthly, **57**, (1950), 404-407.

[**Erdös 1956**] P. Erdös: *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen, **4**, (1956), 201-206.

[**Granville 1992**] Andrew Granville: *Primality Testing and Carmichael Numbers*, Notices of the American Mathematical Society, **39**, (1992), 696-700.

[**Guillaume 1991**] D. Guillaume: *Table des nombres de Carmichael inférieurs à* 10^{12}, preprint, May 1991.

[**Guthmann 1992**] A. Guthmann: *On the computation of Carmichael numbers*, Universität Kaiserslautern, preprint 218, April 1992.

[**Jaeschke 1990**] Gerhard Jaeschke: *The Carmichael numbers to* 10^{12}, Mathematics of Computation, **55 (191)**, (1990), 383-389.

[**Keller 1988**] W. Keller: *The Carmichael numbers to* 10^{13}, Abstracts Amer. Math. Soc., **9**, (1988), 328-329.

[**Knödel 1953**] Walter Knödel: *Carmichaelsche Zahlen*, Mathematische Nachrichten, **9**, (1953), 343-350.

[**Lehmer 1974**] D. H. Lehmer: *Strong Carmichael Numbers*, Journal of the Australian Mathematical Society, **21**, (1974), 508-510.

[**Lehmer 1976**] D. H. Lehmer: *Strong Carmichael Numbers*, Journal of the Australian Mathematical Society, Series A, **21**, (1976), 508-510.

[**Pinch 1993**] R. G. E. Pinch: *The Carmichael numbers up to* 10^{15}, Mathematics of Computation, **61**, (1993), 381-391.

[**Pomerance 1980**] Carl Pomerance, J. L. Selfridge ja Samuel S. Wagstaff Jr.: *The Pseudoprimes to* $25 \cdot 10^9$, Mathematics of Computation, **35 (151)**, (1980), 1003-1026.

[**Swift 1975**] J. D. Swift: *Table of Carmichael Numbers to* 10^9 *(review)*, Mathematics of Computation, **29**, (1975), 338-339.

[**Wagstaff 1980**] S. S. Wagstaff Jr.:, *Large Carmichael Numbers*, Math. J. Okayama Univ., **22**, (1980), 33-41.

[**Yorinaga 1978**] M. Yorinaga: *Numerical computation of Carmichael numbers*, Math. J. Okayama Univ., **20**, (1978), 151-163; II, **21**, (1979), 183-205.