Ameerika Matemaatika Seltsi Cole'i preemiast arvuteooria alal

Ellen Redi
Tallinna Ülikool

Sissejuhatus

Aastal 2002 jagati järjekordne, arvult neljateistkümnes, Frank Nelson Cole'i preemia arvuteooria alal kahe matemaatiku vahel. Nendeks olid Rutgersis asuva New Jersey Riikliku ülikooli professor Henryk Iwaniec ja Harvardi ülikooli professor Richard Taylor. Viieteistkümnendat korda anti see preemia välja 6. jaanuaril 2005 Princetoni ja New Yorgi ülikoolide professorile Peter Sarnakile.

Nimetatud preemia on üks Ameerika Matemaatika Seltsi (edaspidi AMSi[1]) poolt regulaarselt väljaantavatest preemiatest. Teised AMSi poolt omistatavad (praegu suurusega 5000 $) preemiad on:

- George David Birkhoffi preemia rakendusmatemaatika alal,
- Maxime Bôcheri preemia matemaatilise analüüsi alal,
- Frank Nelson Cole'i preemia algebra alal,
- Ruth Lyttle Satteri preemia parimale naismatemaatikule,
- Leroy P. Steele'i preemia elutöö eest,
- Leroy P. Steele'i preemia matemaatika esituse eest,
- Leroy P. Steele'i preemia teedrajava uurimuse eest,
- Oswald Veblen preemia geomeetria alal,

[1] AMSi puudutavad materjalid on võetud nende kodulehestikust.

- Norbert Wieneri preemia tööstus- ja rakendusmatemaatika alal.

Alustuseks tutvustame lühidalt arvuteooriaalase Frank Nelson Cole'i preemia saamislugu ja varasemaid laureaate.

Pisut ajaloost

Frank Nelson Cole (1861–1926) oli Ameerika Matemaatika Seltsi sekretär 25 aastat (1896–1920) ja ajakirja *Bulletin of AMS* peatoimetaja 20 aastat (1897–1926). Tema põhilised uurimused on seotud arvuteooriaga, sealhulgas algarvudega, ja rühmateooriaga. Arvuteooria alal tõstetakse esile seda, et ta oli esimene, kes tegurdas (ruutjääkide meetodil) arvu $2^{67} - 1$.

Teatavasti arve kujul $2^n - 1$ nimetatakse *Mersenne'i arvudeks* ja tähistatakse M_n. Nende hulgast otsitakse suuri algarve, millel on tänapäeval infoturbe tagamisel oluline roll. Marin Mersenne (1588–1648) väitis, et arv $2^n - 1$, kus $n \leq 257$, on algarv vaid siis, kui

$$n = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257.$$

Tegelikult ta eksis: sellesse nimekirja ei kuulu $n = 67$ ja $n = 127$ ning omakorda väärtused $n = 61$, $n = 89$ ja $n = 107$ tuleks sellesse lisada. Näiteks,

$$2^{67} - 1 = 147573952589676412927 = 761838257287 \cdot 193707721.$$

G. M. Phillps kirjutab (vt [5], lk 169), et E. T. Bell kirjeldab oma raamatus [1], kuidas 1903. aastal ühel AMSi koosolekul korrutas F. N. Cole, sõnagi lausumata, need kaks arvu ning näitas, et saadud arv on $2^{67} - 1$. Tänapäeval leiab arvuti arvu M_{67} tegurid mõne sekundiga.

Hetkel suurim teadaolev algarv on Josh Findley poolt 2004. aastal leitud Mersenne'i arv $2^{24036583} - 1$, mis on 7 235 733-kohaline (vt [2]). On olemas projekt GIMPS suurte algarvude leidmiseks. See käivitus 1996. aastal ja selle käigus on leitud 7 seni teadaolevast 41st Mersenne'i algarvust. Välja on kuulutatud 100000 $ suurune preemia sellele, kes esimesena leiab kümne miljoni kohalise algarvu.

Preemiad algebras ja arvuteoorias rajas F. N. COLE siis, kui ta jäi pensionile. Alus selle preemia fondile tekkis sellest, et professor COLE pani siia temale määratud pensioni ja lisaks annetasid ka teised AMSi liikmed. Hiljem tema poeg CHARLES A. COLE kahekordistas selle raha.

Preemia määratakse viimase kuue aasta jooksul avaldatud silmapaistva artikli eest arvuteooriast. Siinjuures peab autor olema AMSi liige või artikkel peab olema avaldatud Põhja-Ameerika mõnes tuntud ajakirjas. Neid preemiaid loetakse ka tänapäeval väga prestiižikateks.

Cole'i preemiat arvuteooria alal on välja antud alates aastast 1931 algul kümne, siis kuue, hiljem viie aasta järel. Hiljuti hakati neid (praeguseks 5000 $ suurusi) preemiaid välja andma iga kolme aasta järel.

Lühiülevaade preemia saajatest

Cole'i preemiat arvuteooria alal on antud viieteistkümnel korral ja laureaate on kokku 22 (vt [3]).

1. (1931) preemia sai ameerika arvuteoreetik HARRY SCHULTZ VANDIVER (1882–1973) mitmete artiklite eest Fermat' suure teoreemi kohta, mis olid avaldatud ajakirjades *Trans. AMS* ja *Annals of Math.* viimase viie aasta jooksul. Eriti tõsteti seejuures esile artiklit

   On Fermat's last theorem, *Trans. AMS*, **31** (1929), 613–642.

2. (1941) preemia sai vahepeal ameerikas elanud prantsuse matemaatik CLAUDE CHEVALLEY (1909–1984) artikliga

   La théorie du corps de classes, *Annals of Math.*, Series 2, **41** (1940), 394–418.

3. (1946) preemia sai H. B. MANN tunnustust väärinud artikliga

   A proof of the fundamental theorem on the density of sums of sets of positive integers, *Annals of Math.*, Series 2, **43** (1942), 523–527.

4. (1951) preemia sai ungari matemaatik Paul Erdös (1913–1996) oma paljude arvuteoreetiliste artiklite eest. Põhiliseks peeti siinjuures artiklit

   On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, *Proc. National Acad. Sci.*, **35** (1949), 374–385.

5. (1956) preemia sai Texase Austini ülikooli professor John T. Tate, kusjuures auhinnatuks osutus artikkel

   The higher dimensional cohomology groups of class field theory, *Annals of Math.*, Series 2, **56** (1952), 294–297.

6. (1962) preemia said jaapani matemaatik Kenkichi Iwasawa (1917–1998) oma auhinnatud artikliga

   Gamma extensions of number fields, *Bull. AMS*, **65** (1959), 183–226,

   ja ameerika arvuteoreetik Bernard M. Dwork (1923–1998) auhinda väärinud artikliga

   On the rationality of the zeta function of an algebraic variety, *Amer. Journ. Math.*, **82** (1960), 631–648.

7. (1967) preemia said ameerika matemaatik James B. Ax ja Princetoni ülikooli professor Simon Bernard Kochen kolmeosalise ühisartikliga

   Diophantine problems over local fields. I, *Amer. Journ. Math.*, **87** (1965), 605–630; II, 631–648; III, *Annals of Math.*, Series 2, **83** (1966), 437–456 .

8. (1972) preemia sai Colorado ülikooli professor Wolfgang M. Schmidt. Preemia kindlustasid järgmised neli artiklit:

   On simultaneous approximation of two algebraic numbers by rationals, *Acta Mathematica* (Uppsala), **119** (1967), 27–50;

   T-numbers do exist, in *Symposia Mathematica*, **IV**, Academic Press, 1970, 1-26;

Simultaneous approximation to algebraic numbers by rationals, *Acta Mathematica* (Uppsala), **125** (1970), 189–201;

On Mahler's T-numbers, in *Proc. Symp. in Pure Math.*, **20**, AMS, 1971, 275–286.

9. (1977) preemia sai Princetoni ülikooli emeriitprofessor GORO SHIMURA artiklitega

   Class fields over real quadratic fields and Hecke operators, *Annals of Math.*, Series 2, **95** (1972), 130–190;

   On modular forms of half integral weight, *Annals of Math.*, Series 2, **97** (1973), 440–481.

10. (1982) preemia said Princetoni Matemaatika Uurimisinstituudi professor ROBERT P. LANGLANDS automorfsete vormide, Eisensteini jadade ja korrutamisvalemite kohta käivate teedrajavate tööde eest, eriti oli aluseks raamat

    Base change for GL(2), *Annals of Math. Studies*, **96**, Princeton Uni. Press, 1980, 237 p;

    ja Harvardi ülikooli professor BARRY MAZUR elliptiliste kõverate ja Abeli muutkondade, sealhulgas ratsionaalsete punktide järgu lõplikkuse kohta käivate silmapaistvate tööde eest. Eelkõige nimetati mahukat artiklit

    Modular curves and the Eisenstein ideal, *Publ. Math. de l'Institut des Hautes Etudes Sci.*, **47** (1977), 33–186.

11. (1987) preemia said Columbia ülikooli professor DORIAN M. GOLDFELD auhinda vääriva artikliga

    Gauss's class number problem for imaginary quadratic fields, *Bull. AMS*, **13**, (1985), 23–37,

    ja Harvard ülikooli professor BENEDICT H. GROSS koos DON B. ZAGIERiga. Siinjuures oli preemiat vääriv nende ühisartikkel

    Heegner points and derivatives of L-Series, *Inventiones Math.*, **84** (1986), 225–320.

12. (1992) preemia said California Irvine'i ülikooli professor KARL RUBIN elliptiliste kõverate ja Iwasawa teooria kohaste tööde eest, eriti tõsteti siinjuures esile kahte artiklit:

    Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. In: *Algebraic number theory in honor of K. Iwasawa, Advanced Studies in Pure Math.* **17** (1989), Acad. Press, 409–419;

    The "main conjectures" of Iwasawa theory for imaginary quadratic fields, *Inventiones Math.*, **103** (1991), 25–68,

    ning California Berkeley ülikooli professor PAUL VOJTA diofantiliste ülesannete kohaste tööde eest, põhiartikliga

    Siegel's theorem in the compact case, *Annals of Math.*, Series 2, **133** (1991), 509–548.

13. (1997) preemia sai Princetoni ülikooli professor ANDREW J. WILES Shimura-Taniyama hüpoteesi ja Fermat' suure teoreemi kohaste tulemuste eest, mis sisaldusid mahukas artiklis

    Modular elliptic curves and Fermat's Last Theorem, *Annals of Math.*, Series 2, **141** (1995), 443–551.

14. (2002) preemia said H. IWANIEC fundamentaalse panuse eest analüütilisse arvuteooriasse ja R. TAYLOR mitmete väljapaistvate edasiarenduste eest algebralises arvuteoorias. Nende preemiatöid tutvustame järgnevates osades pikemalt.

15. (2005) preemia sai Princetoni ülikooli ja New Yorgi ülikooli matemaatika instituudi professor PETER SARNAK fundamentaalse panuse eest arvuteooriasse. Eriti oli aluseks Princetoni kolleegi NICHOLAS KATZiga kaasautorluses kirjutatud raamat

    Random Matrices, Frobenius Eigenvalues and Monodromy. Colloquium Publications. AMS. 45 (1999). Providence, RI: AMS. xi, 419 p.

Selle raamatu filosoofia esitleb teda kui analüütilise arvuteooria töösuundade põhilist mõjutajat. Nimetatud filosoofiat on kontrollitud (ühel raskematest erijuhtudest) kahes preemiat väärinud artiklis

> (kaasautor H. Iwaniec) "The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros". *Isr. J. Math.* **120** (2000), Pt. A, 155–177;
>
> (kaasautorid H. Iwaniec ja W. Luo) "Low lying zeros of families of L-functions". In *Publ. Math., Inst. Hautes Étud. Sci.* **91** (2000), 55–131.

Henryk Iwaniecile preemia toonud töödest

Aastal 2002 omistati *Cole*'i arvuteooria preemia (vt [3]) HENRYK IWANIECile Rutgersi ülikoolist tema fundamentaalse panuse eest analüütilisse arvuteooriasse, kusjuures aluseks olid mitmed artiklid. Eelkõige oli selleks koostöös Toronto ülikooli professori JOHN B. FRIEDLANDERiga valminud artikkel

> The polynomial X^2+Y^4 captures its primes, *Annals of Math.*, Series 2, **148** (1998), No.3, 945–1040.

See on üleüldse esimene artikkel, mis näitab, et täisarvuliste kordajatega polünoomil saab olla lõpmatult palju algarvulisi väärtusi. Siin näitab väljatöötatud meetodi tugevust see, et Oxfordi ülikooli professor ROGER HEATH-BROWN on juba laiendanud seda meetodit teatud kuuppolünoomidele artiklis

> *Counting rational points on cubic surfaces,* In: Peyre, Emmanuel (ed.), Nombre et répartition de points de hauteur bornée. Paris: Société Mathématique de France, Astérisque. **251** (1998), 13–29.

Preemia määramisel oli aluseks ka California ülikooli (Los Angeles) professori WILLIAM D. DUKEiga ja J. FRIEDLANDERiga kaasautorluses kirjutatud artiklite seeria:

> Bounds for automorphic L-functions, *Invent. Math.*, **112** (1993), No.1, 1-8;

Bounds for automorphic L-functions II, *Invent. Math.*, **115** (1994), No.2, 219–239;

Bounds for automorphic L-functions III, *Invent. Math.* **143** (2001), No.2, 221–248;

ja Ameerika Matemaatika Instituudi professori ja juhataja Brian J. Conreyga kaasautorluses avaldatud artikkel

The cubic moment of central values of automorphic L-functions, *Annals of Math.*, Series 2, **151** (2000), No.3, 1175–1216.

Need artiklid käsitlevad automorfsete L-funktsioonide joonkriitilisi tõkkeid, mis on seotud teatud modulaarsete vormidega ning on oluliselt parendatud uute meetodite abil. Tuletame meelde, et *automorfseks* (vt [7]) nimetatakse kompleksmuutuja z- funktsiooni $f(z)$, mis on analüütiline oma määramispiirkonna igas punktis (poolused välja arvatud) ja mis on invariantne murdlineaarsete teisenduste (ehk Möbiuse teisenduste) rühma suhtes.

Nendes sisalduva tehnika laiendus lõi lähtekoha, millele toetudes õnnestus Ohio Riikliku ülikooli professoril James Wesley Cogdellil, Princetoni ülikooli professoril I. Piatetskii-Shapirol ja Peter Sarnakil lõpuks lahendada Hilberti üheteistkümnes probleem. (**Laiendada ruutkorpuste kohta saadud tulemused suvalistele täisarvuliselt algebraliste arvude korpustele** (vt [8])).

Veel on aluseks koos P. Sarnakiga avaldatud artikkel (vt 15. preemiat), mis on sissejuhatuseks automorfsete L-funktsioonide perede uurimisel rakendatavale keskmiste ja silumistehnikale (ing. k. *mollification*).

Henryk Iwanieci elukäigust

Henryk Iwaniec sündis Elblagis, Poolas, 9. oktoobril 1947. aastal. Ta lõpetas Varssavi Ülikooli 1971. aastal ja kaitses järgmisel aastal samas doktorikraadi.

Aastatel 1971–1983 oli ta mitmetel ametikohtadel Poola Teaduste Akadeemia Matemaatika Instituudis. Habilitatsioonitöö kaitses ta 1976. aastal. Aastatel 1976–77 oli ta uurijaks Itaalias Pisa Accademia Nazionale dei Lincei Normaalkooli juures. Aastatel

1979–80 külastas ta USA Bordeaux' Ülikooli. Professoriks promoveeriti H. IWANIEC 1983 aastal ja kohe sai temast ka Poola Teaduste Akadeemia korrespondentliige.

H. IWANIEC lahkus Poolast veel samal aastal külalisteadlaseks üheks õppeaastaks (1983–84, hiljem veel 1985–86) USA Princetoni Matemaatika Uurimisinstituuti. Õppejõuks on ta olnud ka Michigani Ann Arbori ülikoolis (suvel 1984) ja Boulderi ülikoolis (sügisel 1984). Jaanuaris 1987 asus ta oma praegusele ametipostile Rutgersis asuva New Jersey Riiklikus ülikoolis. Ameerika Kunstide ja Teaduste Akadeemia akadeemikuks valiti H. IWANIEC 1995. aastal. Õppeaastal 1999–2000 oli ta taas külalisprofessor Princetoni (New Jersey) Matemaatika Uurimisinstituudi juures. Praeguseks on temast saanud USA kodanik.

HENRYK IWANIEC on pälvinud mitmeid autasusid:

Marcinkiewiczi preemia üliõpilastööde eest õppeaastatel 1968–69 ja 1969–70;
Poola valitsuse riiklik preemia (1978);
Jurzykowski preemia New Yorgi fondilt;
Sierpinski medal, Poola TA (1996).

Professor H. IWANIECit on kutsutud esinema Rahvusvahelistele Matemaatika Kongressidele Helsingis 1978 teemal *Sieve methods.* (Proc. Int. Congr. Math., Helsinki 1978, Vol. 1 (1980), 357–364) ja Berkley's 1986 teemal *Spectral theory to automorphic functions and recent developments in analytic number theory.* (Proc. Int. Congr. Math., Berkeley/Calif. 1986, Vol. 1 (1987), 444–456).

Richard Taylori preemiatöödest

Cole'i preemia arvuteooria alal anti Harvardi ülikooli professorile RICHARD TAYLORile mitmete väljapaistvate edasiarenduste eest algebralises arvuteoorias. R. TAYLOR on oluliselt laiendanud oma varasemat, kaasautorluses A. J. WILESiga, avaldatud tööd

> Ring-theoretic properties of certain Hecke algebras, *Annals of Math.*, Series 2, **141** (1995), No.3, 553–572.

Selles oli tõestatud, et kõik elliptilised kõverad üle $\mathbb{Q}$ on modulaarsed, täpsemini öeldes, nad on modulaarsete kõverate jakobiaanide

faktorid.

Selgitame nüüd siin esinevat elliptilise kõvera mõistet.

Elliptiliseks kõveraks (vt [4], lk 117) üle korpuse K nimetatakse siledat joont võrrandiga

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Siledus (ing. k. *smoothness*) tähendab, et joonel ei tohi leiduda punkte, milles mõlemad osatuletised on nullid. Teiste sõnadega, võrrandid

$$a_1y = 3x^2 + 2a_2x + a_4 \quad \text{ja} \quad 2y + a_1x + a_3 = 0$$

ei tohi kehtida korraga elliptilise kõvera üheski punktis.

Kui korpuse K karakteristika ei ole 2 ega 3, siis saab antud võrrandi sobiva muutujate vahetusega lihtsustada kujule

$$y^2 = x^3 + ax + b.$$

Tekkinud joone siledust saab viimase võrrandi korral väljendada nõudega, et tema paremal poolel oleval kuuppolünoomil ei ole kordseid juuri. Teatavasti kehtib see siis ja ainult siis, kui diskriminant $D = -(4a^3 + 27b^2)$ erineb nullist.

Kõigi viimast võrrandit rahuldavate punktide $(x, y) \in K^2$ hulka koos nn *lõpmatuspunktiga* O tähistame $E(K)$.

Kuna kõver $E(K)$ on x-telje suhtes sümmeetriline, siis selle punkti $P = (x_p, y_p)$, kus $P \neq O$, *vastandelemendiks* nimetatakse punkti $-P = (x_p, -y_p)$. Lõpmatuspunkti O loetakse iseenda vastandelemendiks.

Elliptilise kõvera $E(K)$ punktide $P = (x_p, y_p)$ ja $Q = (x_q, y_q)$, kui $P \neq -Q$, *summaks* nimetatakse neid läbiva sirge ja kõvera $E(K)$ (kolmandat) lõikepunkti $R = (x_r, y_r)$, mida saab leida valemitega

$$\begin{cases} x_r = \lambda^2 - x_p - x_q, \\ y_r = \lambda(x_p - x_r) - y_q, \end{cases} \qquad \text{kus} \qquad \lambda = \frac{y_p - y_q}{x_p - x_q}.$$

Täiendavalt defineeritakse

$$P + (-P) = O, \qquad O + P = P + O = P.$$

Nii konstrueeritud algebraline struktuur $(E(K),\ +)$ on Abeli rühm, mis on osutunud kasulikuks krüpteerimisel. Tüüpiliselt on siinjuures korpuseks K kas $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, korpuse $\mathbb{Q}$ mingi algebraline laiend, p-aadiliste arvude korpus $\mathbb{Q}_p$ või mingi lõplik korpus.

R. Taylori preemiatöödest nimetagem koos Dresdeni Tehnikaülikooli professori Michael Harrisega kirjutatud raamatut

The geometry and cohomology of some simple Shimura varieties. Ann. Math. Studies **151** (2001), Princeton: Princeton Uni Press, 276 p.,

millele on väikese lisa koostanud Iisraeli Weizmanni Teadusliku Instituudi professor VLADIMIR BERKOVICH. Raamatus esitatakse Langlandsi hüpoteesi tõestus lokaalsel juhul ning antakse lokaalse korpuse Galois' rühma n-mõõtmelise esituse täielik parametrisatsioon. Teatavasti püstitas LANGLANDS pööratavuse hüpoteesi, *et ratsionaalarvude korpuse* $\mathbb{Q}$ *lõpliku laiendi* $\mathbb{A}$ *Galois' rühma iga n-mõõtmelise kompleksse esituse Artini L-funktsioon on L-funktsioonina saadav üldisest lineaarsest rühmast* $GL_n(\mathbb{A})$ (vt [9]). Meenutame, et *lokaalseks* nimetatakse korpust, mis on täielik diskreetse normi suhtes ja mille jäägiklassikorpus on lõplik.

R. TAYLOR on saavutanud olulist edu 2-mõõtmeliste Galois' esituste uurimisel ja süvendanud arusaamu Fontaine-Mazuri ja Serre'i hüpoteesidest. Viimane neist tähendab väidet, et *Iga vaba moodul on projektiivne.*

R. TAYLORi töödest, mis jäävad preemia omistamisel aluseks oleva kuueaastase perioodi sisse, mainime veel järgmisi:

(kaasautorid C. BREUIL, B. CONRAD, F. DIAMOND) On the modularity of elliptic curves over **Q**: wild 3-adic exercises, *J. Amer. Math. Soc.*, **14** (2001), no. 4, 843–939 (electronic);

(kaasautorid K. BUZZARD, M. DICKINSON, N. SHEPARD-BARRON) On icosahedral Artin representations, *Duke Math. J.*, **109** (2001), 283–318;

(kaasautorid B. CONRAD, F. DIAMOND) Modularity of certain potentially Barsotti-Tate Galois representations, *J. Amer. Math. Soc.*, **12** (1999), 521–567;

(kaasautorid C. BREUIL, B. CONRAD, F. DIAMOND) Mod 2 and mod 5 icosahedral representations, *J. Amer. Math. Soc.*, **14** (2001), 843–939;

(kaasautorid H. DARMON, F. DIAMOND) *Fermat's last theorem.* In: Current Developments in Mathematics, 1995 (Cambridge, MA), 1–154.

Richard Taylor on algebralise arvuteooria suur asjatundja ning ta töötab põhiliselt automorfsete vormide ja Galois' rühmade esituste vaheliste seoste temaatika kallal. Aastal 1994 töötas ta koos Andrew Wilesiga, tehes parandusi programmiga GAP Wilesi tõetuses Fermat' suure teoreemi kohta.

Richard Taylori elukäigust

Richard Taylor sündis 19. mail 1962. aastal Cambridge'is, Inglismaal. Kui ta oli kahene, kolis pere Oxfordi, kus möödus ta lapse- ja koolipõlv. Aastal 1980 läks ta tagasi Cambridge'i õppima. Ülikooliõpinguid alustas ta 1984. aastal Princetoni ülikoolis ja sealt sai ta ka dotorikraadi 1988. aastal modulaarsete vormide kongruentsuse teemalise töö eest, mida juhendas professor Andrew Wiles. Viimasel oligi suur mõju R. Taylori matemaatilisele arengule. Järeldoktori aasta läbis ta Pariisi lähistel Institut des Hautes Études Scientifiques'is.

Cambridge'i ülikooli Puhta Matemaatika ja Matemaatilise Statistika osakonna juhataja John Coatesi poolt julgustatuna tuli R. Taylor tagasi Cambridge'i (kuueks aastaks). Olles 1995. aastal abiellunud, lahkus ta sealt ja asus juhatama Savile'i nimelist geomeetria õppetooli Oxfordi ülikoolis. (Sir Henri Savile (1549–1622) oli tuntud inglise matemaatik, kes rajas 1619. aastal Oxfordi ülikoolis kaks uut õppetooli – geomeetria ja astronoomia.) Aasta hiljem kolis R. Taylor Harvardi ülikooli, kus ta on tööl ka praegu.

Richard Taylor on pälvinud mitmeid tunnustusi:

1990 Whiteheadi preemia noorteadlasele, Londoni MS;
1992 Franco-Brittanique'i preemia, Prantsuse TA;
1995 valiti ta Londoni Kuningliku Ühingu liikmeks.

Kirjandus

1. Bell, E. T. *Mathematics, Queen and Servant of Science*, G. Bell and Sons, London, 1952.

2. Caldwell, C. *The Largest Known Prime by Year / A Brief History*,
`http://www.utm.edu/research/primes/notes/by_year.html`

3. 2002 Cole Prize in Number Theory, *Notices of the AMS*, **49** (2002), N 4, 476–479.

4. Koblitz, N. *Algebraic Aspects of Cryptography*, Berlin, Springer, 1999.

5. Phillps, G. M. *Two Millennia of Mathematics / From Archimedes to Gauss.* – (CMS books in Mathemtaics: 6), 2002, Springer-Verlag, New York.

6. Weisstein, E. W. et al. *Artin's Conjecture*. From MathWorld,
`http://mathworld.wolfram.com/ArtinsConjecture.html`

7. Weisstein, E. W. *Automorphic Function.* From MathWorld,
`http://mathworld.wolfram.com/AutomorphicFunction.html`

8. Weisstein, E. W. *Hilbert's Problems.* From MathWorld,
`http://mathworld.wolfram.com/HilbertsProblems.html`

9. Weisstein, E. W. *Langlands Reciprocity.* From MathWorld,
`http://mathworld.wolfram.com/LanglandsReciprocity.html`

P.S. Selle artikli toimetamise aja jooksul avastati GIMPSi abiga veel kolm Mersenne'i algarvu (42.–44.). Seega oktoobrist 2006 on suurim algarv (Cooper, Boone, Woltman jt poolt 04.09.06 avastatud) $2^{32582657} - 1$, mis on 9808358- kohaline.

Autor