GENERATORJI PRAŠTEVIL

JANKO BRAČIČ

Naravoslovnotehniška fakulteta
Univerza v Ljubljani

Math. Subj. Class. (2010): 11A41

Generator praštevil je postopek, ki nam na vsakem koraku vrne praštevilo oziroma množico praštevil. V članku predstavimo nekaj znanih in manj znanih generatorjev praštevil.

PRIME NUMBER GENERATORS

A prime generator is an algorithm which on each step returns a prime number or a set of prime numbers. In this paper we present some known and less known prime generators.

Uvod

Množica naravnih števil $\mathbb{N}$ ima po eni strani preprosto strukturo, ki se nanaša na seštevanje. Do vsakega naravnega števila pridemo z enostavnim postopkom: začnemo s številom 1, prištejemo 1 in dobimo 2, spet prištejemo 1 in dobimo 3 itd. Rečemo lahko, da ima aditivna struktura v $\mathbb{N}$ en sam osnovni gradnik, število 1. Tesno povezana z aditivno strukturo v $\mathbb{N}$ je dobra urejenost te množice.

Po drugi strani je multiplikativna struktura množice $\mathbb{N}$ manj enostavna. Potrebujemo veliko osnovnih gradnikov – praštevil, da lahko vsako naravno število izrazimo kot njihov produkt. Že starogrški matematiki so vedeli, da za vsako naravno število $n \geq 2$ obstajajo takšna enolično določena praštevila $p_1 < \cdots < p_k$ in naravna števila $e_1, \ldots, e_k$, da je $n = p_1^{e_1} \cdots p_k^{e_k}$. Na tem *osnovnem izreku aritmetike* sloni Evklidov dokaz, da je praštevil neskončno mnogo. Idejo njegovega dokaza lahko uporabimo za konstrukcijo generatorja praštevil. Z generatorjem praštevil imamo v mislih postopek, ki nam ob ustreznih začetnih podatkih da eno ali več praštevil. Iz Evklidovega dokaza lahko izluščimo naslednji postopek za generiranje praštevil.

- Naj bo $\{q_1, \ldots, q_l\}$ poljubna množica praštevil;
- produktu $q_1 \cdots q_l$ prištejemo 1, da dobimo število $n = q_1 \cdots q_l + 1 > 2$;
- osnovni izrek aritmetike zagotavlja obstoj takšnih enolično določenih praštevil $p_1 < \cdots < p_k$ in naravnih števil $e_1, \ldots, e_k$, da je $n = p_1^{e_1} \cdots p_k^{e_k}$;
- dobili smo množico praštevil $\{p_1, \ldots, p_k\}$ in vsako od njih je različno od praštevil v začetni množici.

Ker je $\{q_1, \ldots, q_l\}$ prava podmnožica v $\{q_1, \ldots, q_l, p_1, \ldots, p_k\}$, lahko sklepamo, da je praštevil neskončno mnogo.

K pravkar opisanemu generatorju praštevil se bomo vrnili pozneje, ko bomo govorili o njegovih variantah, celi družini generatorjev praštevil, ki jim rečemo evklidski generatorji praštevil.

Obrazci za računanje praštevil

Že Euler je opazil, da je vrednost polinoma $f(n) = n^2 + n + 41$ praštevilo za vse $n = 0, 1, \ldots, 39$. Ker je $f(40) = 1681 = 41^2$, ta kvadratni polinom ni generator praštevil. Seveda lahko z interpolacijo za vsak nabor praštevil $p_1, \ldots, p_k$ najdemo takšen polinom f, da je $f(n) = p_n$ za vse $n = 1, \ldots, k$. Na žalost pa pri interpolaciji stopnja polinoma f narašča s k. Green in Tao [5] sta dokazala zelo globok izrek o praštevilih. Pokazala sta, da so v množici praštevil poljubno dolga aritmetična zaporedja. Z drugimi besedami, za vsako naravno število k obstajata takšni naravni števili u_k, v_k, da je vrednost linearne funkcije $l(n) = u_k n + v_k$ praštevilo za vse $n = 1, 2, \ldots, k$. Števili u_k in v_k sta si seveda tuji, zato je po Dirichletovem izreku o praštevilih v aritmetičnem zaporedju $l(n)$ neskončno mnogo praštevil. A že zelo enostaven argument nas prepriča, da $l(n)$ ne more biti praštevilo za vse $n \in \mathbb{N}$. Namreč, za $n = u_k + v_k + 1$ je $l(n) = (u_k + 1)(u_k + v_k)$. Pravzaprav ni takšnega nekonstantnega polinoma f, katerega vrednost $f(n)$ bi bila praštevilo za vsako naravno število n. Dokažemo lahko še več.

Trditev 1. *Ne obstaja takšen nekonstanten polinom f, katerega vrednosti $f(n)$ so praštevila za vsa naravna števila n iz nekega aritmetičnega zaporedja naravnih števil.*

Dokaz. Ideja dokaza je iz [6]. Vzemimo, da obstajata takšen nekonstanten polinom f in takšno aritmetično zaporedje $A = \{dk + e;\ k = 0, 1, 2 \ldots\}$, da je $f(n)$ praštevilo za vse $n \in A$. Potem je $f(e) = p$ praštevilo. Ker je $dpj + e \in A$ za vse $j \in \mathbb{N}$, je tudi vsako od števil $f(dpj + e)$ praštevilo. Iz $dpj+e \equiv e \pmod p$ sledi $(dpj+e)^m \equiv e^m \pmod p$ za vsako naravno število m, kar nam da $f(dpj + e) \equiv f(e) \equiv 0 \pmod p$ za vse $j \in \mathbb{N}$. To pomeni, da je praštevilo $f(dpj + e)$ enako p. Toda to je nemogoče, saj nekonstanten polinom ne more zavzeti iste vrednosti neskončnokrat. ∎

Zdaj, ko vemo, da ni takšnega polinoma f, pri katerem bi bilo $f(n)$ praštevilo za vsa števila n iz nekega aritmetičnega zaporedja naravnih števil, se postavlja vprašanje, ali sploh obstaja takšna nekonstantna funkcija f, katere vrednosti $f(n)$ so praštevila za vse n iz neke neskončne množice naravnih števil. Preden odgovorimo na to vprašanje, dokažimo naslednjo trditev.

Lema 2. *Naravno število $n \neq 4$ je praštevilo natanko tedaj, ko n ne deli števila $(n-1)!$.*

Dokaz. Če je n praštevilo, potem število $(n-1)!$ ni deljivo z n. Za dokaz obrata moramo pokazati, da vsako naravno število $n \neq 4$, ki ni praštevilo, deli število $(n-1)!$. Ker za $n = 1$ to očitno velja, lahko predpostavimo, da je n sestavljeno število. Vzemimo najprej, da obstaja razcep $n = uv$, kjer sta $1 < u < v < n$. Potem seveda u in v nastopata v produktu $(n-1)! = 1 \cdot 2 \cdots u \cdots v \cdots (n-1)$ in zato $n|(n-1)!$. Razcep $n = uv$ z $1 < u < v < n$ obstaja za vsako sestavljeno število n, razen za števila oblike $n = p^2$, kjer je p praštevilo. Predpostavimo torej, da je $n = p^2$ za neko praštevilo p. Ker je $n \neq 4$, je p liho praštevilo. Iz $(p^2-1)! = 1 \cdot 2 \cdots p \cdot (p+1) \cdots (2p) \cdot (2p+1) \cdots (p^2-1)$ vidimo, da $p^2|(p^2-1)!$. ∎

Za realno število x označimo z $\lfloor x \rfloor$ največje celo število, ki ne presega x, in z $\lceil x \rceil$ najmanjše celo število, ki ga x ne presega. Na primer, $\lfloor 2{,}4 \rfloor = 2$ in $\lceil 2{,}4 \rceil = 3$. Če je x celo število, potem je $\lfloor x \rfloor = \lceil x \rceil = x$.

Poglejmo zdaj funkcijo

$$f(n) = \left\lceil \frac{2(n-1)!}{n} - \left\lfloor \frac{2(n-1)!}{n} \right\rfloor \right\rceil (n-2) + 2.$$

Izračunamo lahko, da je $f(1) = 2$, $f(2) = 2$, $f(3) = 3$, $f(4) = 2$, $f(5) = 5$, $f(6) = 2$ itd.

Trditev 3. *Funkcija f je generator praštevil. Če je n praštevilo, je $f(n) = n$, za druga naravna števila n pa je $f(n) = 2$.*

Dokaz. Če je n liho praštevilo, potem po lemi 2 število $\frac{2(n-1)!}{n}$ ni celo, kar pomeni, da je $\frac{2(n-1)!}{n} - \left\lfloor \frac{2(n-1)!}{n} \right\rfloor$ število z intervala $(0, 1)$ in zato $\left\lceil \frac{2(n-1)!}{n} - \left\lfloor \frac{2(n-1)!}{n} \right\rfloor \right\rceil = 1$. Ker že vemo, da je $f(2) = 2$, lahko zaključimo, da je $f(n) = n$, če je n praštevilo. Po drugi strani, če je $n \neq 4$ sestavljeno število ali enako 1, je po lemi 2 $\frac{2(n-1)!}{n}$ celo število in zato $\frac{2(n-1)!}{n} - \left\lfloor \frac{2(n-1)!}{n} \right\rfloor = 0$. Ker je $f(4) = 2$, vidimo, da je $f(n) = 2$, če n ni praštevilo. ∎

Naša konstrukcija funkcije f iz trditve 3 temelji na funkciji, ki je predstavljena na spletni strani [10].

Bertrandov postulat (včasih imenovan tudi izrek Bertrand-Čebiševa) pravi, da za vsako število $x > 1$ obstaja na intervalu $[x, 2x]$ vsaj eno praštevilo. Odkar je leta 1852 Čebišev dokazal ta izrek, so ga matematiki precej izboljšali. Tako so, na primer, leta 2001 Baker, Harman in Pintz v članku [1] pokazali, da obstaja takšno število $x_0 > 0$, da za vsak $x \geq x_0$ interval $[x, x + x^{21/40}]$ vsebuje vsaj eno praštevilo. Avtorji v svojem članku trdijo, da je mogoče število x_0 efektivno izračunati, a ne navajajo nobene ocene za velikost števila x_0.

Označimo s p_n n-to praštevilo. Torej, $p_1 = 2, p_2 = 3, p_3 = 5$ itd. Iz rezultata, ki so ga dokazali Baker, Harman in Pintz, sledi, da obstaja takšen indeks n_0, da je

$$p_n < p_{n+1} < p_n + p_n^{21/40} < p_n + p_n^{2/3} \qquad \text{za vse} \quad n \geq n_0.$$

Lema 4 ([7]). *Če je N takšno naravno število, za katerega velja $p_{n_0} < N^3$, potem obstaja takšno praštevilo q, da je $N^3 < q < (N+1)^3 - 1$.*

Dokaz. Naj bo p_n največje praštevilo, za katerega velja $p_n < N^3$. Potem je $n \geq n_0$ in torej velja $N^3 < p_{n+1} < p_n + p_n^{2/3} < N^3 + N^2 < (N+1)^3 - 1$. ■

Cheng [4] je pokazal, da lema 4 velja za vsako število $N > e^{e^{15}}$. Se pravi, da lahko za p_{n_0} vzamemo najmanjše praštevilo, ki presega $e^{3e^{15}}$.

Naj bo zdaj $q_0 > e^{3e^{15}}$ poljubno praštevilo. S pomočjo leme 4 lahko dobimo neskončno zaporedje praštevil $q_0 < q_1 < q_2 < \ldots$, za katerega velja

$$q_n^3 < q_{n+1} < (q_n + 1)^3 - 1 \qquad (n \in \mathbb{N}).$$

Definirajmo zaporedji

$$u_n = q_n^{3^{-n}} \qquad \text{in} \qquad v_n = (q_n + 1)^{3^{-n}} \qquad (n \in \mathbb{N}).$$

Lema 5 ([7]). *Zaporedje u_n je monotono naraščajoče, zaporedje v_n je monotono padajoče in pri vsakem n je $u_n < v_n$.*

Dokaz. Očitno je $u_n < v_n$. Pri vsakem n velja $u_{n+1} = q_{n+1}^{3^{-n-1}} > (q_n^3)^{3^{-n-1}} = q_n^{3^{-n}} = u_n$ in $v_{n+1} = (q_{n+1}+1)^{3^{-n-1}} < ((q_n+1)^3-1+1)^{3^{-n-1}} = (q_n+1)^{3^{-n}} = v_n$. ■

Trditev 6 ([7]). *Obstaja takšno število $\alpha > 1$, da je funkcija*

$$g(n) = \lfloor \alpha^{3^n} \rfloor \qquad (n \in \mathbb{N})$$

generator praštevil.

Dokaz. Naj bosta u_n in v_n zaporedji, ki smo ju definirali prej. Ker je zaporedje u_n monotono naraščajoče in navzgor omejeno, je konvergentno. Naj bo $\alpha = \lim_{n\to\infty} u_n$. Ker je v_n monotono padajoče zaporedje in velja $u_n < v_n$, je $u_n < \alpha < v_n$ za vse $n \in \mathbb{N}$. Od tod sledi $q_n = u_n^{3^n} < \alpha^{3^n} < v_n^{3^n} = q_n + 1$ za vse $n \in \mathbb{N}$. Torej je $\lfloor \alpha^{3^n} \rfloor = q_n$. ∎

Obe funkciji, ki smo ju predstavili v tem razdelku, imata le teoretični pomen, za konkretno generiranje praštevil nista uporabni. Bolj ali manj je tako z vsemi funkcijami, ki generirajo praštevila. Funkcija f iz trditve 3 zahteva veliko računskih operacij za izračun vrednosti $f(n)$. Funkcija g iz trditve 6 pa ima to dodatno pomanjkljivost, da števila α ne poznamo, saj je definirano kot limita. V naslednjem razdelku bomo zato pogledali generatorje praštevil, ki so bolj priročni.

Sita

Sito je postopek, ki v dani neprazni končni množici naravnih števil poišče vsa praštevila. Najbolj znano je Eratostenovo sito. Postopek je naslednji. Naj bo M končna neprazna množica naravnih števil in naj bo m največje število v M. Množico M presejemo takole:

- naj bo $M_1 = M \setminus \{1\}$;
- za vsak $n = 2, \dots, \lfloor\sqrt{m}\rfloor$, naj bo $M_n = M_{n-1} \setminus \{kn;\ k = 2, \dots, \lfloor\frac{m}{n}\rfloor\}$.

Ko je postopek končan, dobimo množico $M_{\lfloor\sqrt{m}\rfloor}$, v kateri so natanko vsa praštevila iz množice M. Verjetno tega ni treba dokazovati, saj je Eratostenovo sito zelo znan generator praštevil.

Indijski matematik Sundaram je leta 1934 odkril zelo zanimivo sito. Naša predstavitev tega sita temelji na [11]. Začnimo z naslednjo tabelo naravnih števil.

$$\begin{array}{rrrrrrrrl}
4 & 7 & 10 & 13 & 16 & 19 & 22 & 25 & \dots \\
7 & 12 & 17 & 22 & 27 & 32 & 37 & 42 & \dots \\
10 & 17 & 24 & 31 & 38 & 45 & 52 & 59 & \dots \\
13 & 22 & 31 & 40 & 49 & 58 & 67 & 76 & \dots \\
16 & 27 & 38 & 49 & 60 & 71 & 82 & 93 & \dots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array} \tag{1}$$

Kaj je na tej tabeli zanimivega? Vidimo, da je v vsaki vrstici in vsakem stolpcu aritmetično zaporedje števil. V prvem stolpcu je v j-ti vrstici število $4+3(j-1)=3j+1$. To je prvi člen aritmetičnega zaporedja v j-ti vrstici. Razlika aritmetičnega zaporedja v j-ti vrstici je liho število $2j+1$. Se pravi, da je v j-ti vrstici in k-tem stolpcu število $3j+1+(k-1)(2j+1)=2jk+j+k$. Zdaj lahko razkrijemo najbolj zanimivo lastnost tabele (1).

Trditev 7. *Liho število $2n+1$ je praštevilo natanko tedaj, če število n ni v tabeli* (1)*.*

Dokaz. Videli smo, da so v tabeli (1) natanko vsa naravna števila oblike $n=2jk+j+k$ $(j,k\in\mathbb{N})$. Za takšno število n pa velja $2n+1=4jk+2i+2k+1=(2j+1)(2k+1)$, kar pomeni, da $2n+1$ ni praštevilo. Po drugi strani, če $2n+1$ ni praštevilo, je produkt dveh lihih števil $2j+1$ in $2k+1$. Iz $2n+1=(2j+1)(2k+1)$ sledi, da je $n=jk+j+k$, torej število iz tabele (1). ∎

S postopkom, ki mu rečemo Sundaramovo sito, lahko poiščemo vsa praštevila v neprazni končni množici števil M. Naj bo m najmanjše naravno število, za katerega velja $n\le 2m+2$ za vse $n\in M$. Postopek poteka takole:

- naj bo $M_0=M\setminus(\{2k;\ k=2,\dots,m+1\}\cup\{1\})$,
- za vsak $j=1,\dots,\lfloor\frac{2m-1}{6}\rfloor$, naj bo $M_j=M_{j-1}\setminus\{(2j+1)(2k+1);\ k=1,\dots,j\}$.

Na prvem koraku smo izločili soda sestavljena števila in število 1, na drugem koraku pa liha sestavljena števila. V množici $M_{\lfloor\frac{2m-1}{6}\rfloor}$ so ostala le praštevila, ki so v M. Še pojasnilo, zakaj število j teče od 1 do $\lfloor\frac{2m-1}{6}\rfloor$. Namreč, vsako sestavljeno liho število v M je oblike $(2j+1)(2k+1)$, kjer je $j \geq k$. Ker je vedno $2k+1 \geq 3$, je dovolj, da je $j \leq \lfloor\frac{2m-1}{6}\rfloor$, saj za $\lfloor\frac{2m-1}{6}\rfloor + 1$ že velja $3\big(2(\lfloor\frac{2m-1}{6}\rfloor+1)+1\big) \geq 3\big(2\frac{2m-1}{6}+1\big) = 2m+2$. V nekaterih primerih je res potrebno, da j teče do $\lfloor\frac{2m-1}{6}\rfloor$. Naj bo na primer $p = 2t+1 > 3$ liho praštevilo in M poljubna množica naravnih števil, v kateri je $3p$ največje število. Ni težko videti, da je $m = \frac{3p-1}{2} = 3t+1$ najmanjše naravno število, pri katerem velja $n \leq 2m+2$ za vse $n \in M$. Število $3p$ je liho in sestavljeno, kot produkt dveh lihih naravnih števil različnih od 1 ga lahko zapišemo samo na en način: $3p = (2t+1)(2\cdot 1+1)$. Se pravi, da ga z zgornjim algoritmom izločimo iz množice M šele na koraku, ko je $j = t = \lfloor\frac{2m-1}{6}\rfloor$.

Evklidski generatorji praštevil

Na koncu se vrnimo k Evklidu in njegovemu dokazu, da je praštevil neskončno mnogo. Generator praštevil, ki smo ga opisali v uvodu, je Mullin [8] nekoliko spremenil in definiral dva generatorja praštevil. Prvo Mullinovo zaporedje praštevil dobimo takole:

- naj bo $q_1 = 2$,
- za vsak $k \in \mathbb{N}$ naj bo q_{k+1} najmanjše praštevilo, ki deli $q_1 \cdots q_k + 1$,

drugo Mullinovo zaporedje pa takole:

- naj bo $Q_1 = 2$,
- za vsak $k \in \mathbb{N}$ naj bo Q_{k+1} največje praštevilo, ki deli $Q_1 \cdots Q_k + 1$.

V naslednji tabeli, ki je povzeta po [2], je prvih deset členov obeh zaporedij

k	q_k	Q_k
1	2	2
2	3	3
3	7	7
4	43	43
5	13	139
6	53	50 207
7	5	340 999
8	6 221 671	2 365 347 734 339
9	38 709 183 810 571	4 680 225 641 471 129
10	139	1 368 845 206 580 129

Zelo malo je znanega o teh dveh zaporedjih praštevil. Tako je še vedno nerešen problem, ali se v zaporedju q_k pojavijo vsa praštevila. Za zaporedje Q_k je Booker [2] pokazal, da v njem manjka neskončno mnogo praštevil.

Za konec poglejmo nekoliko drugačen evklidski generator praštevil, ki ga je objavil Wooley leta 2017. Potrebujemo naslednjo lemo.

Lema 8 ([9]). *Za vsako naravno število n je najmanjše praštevilo, ki deli $n^{n^n} - 1$, enako najmanjšemu praštevilu, ki ne deli n.*

Dokaz. Za $n = 1$ trditev očitno velja, zato predpostavimo, da je $n \geq 2$. Če je n liho število, je 2 najmanjše praštevilo, ki ne deli n. Očitno 2 deli $n^{n^2} - 1$. Tudi obratno velja, če 2 deli $n^{n^n} - 1$, potem je n liho število in je torej 2 najmanjše praštevilo, ki ne deli n. Vzemimo zdaj, da je n sodo število. Naj bodo $q_1, \ldots, q_k$ vsa praštevila, ki delijo n in p najmanjše praštevilo, ki ne deli n. Torej je $p \geq 3$ in $q_1 \cdots q_k + 1 \leq n + 1$. Evklidov argument nam zagotavlja, da obstaja praštevilo q, ki deli $q_1 \cdots q_k + 1$. To praštevilo seveda ne deli n in je manjše kvečjemu enako $q_1 \cdots q_k + 1$. Ker pa je po predpostavki p najmanjše praštevilo, ki ne deli n, je $p \leq q$ in zato $p \leq q_1 \cdots q_k + 1 \leq n + 1$.

Naj bodo $p_1, \ldots, p_j$ praštevila, ki delijo $p-1$, velja naj $p-1 = p_1^{e_1} \cdots p_j^{e_j}$. Potem zaradi $p_j < p$ in predpostavke, da je p najmanjše praštevilo, ki ne deli n, sledi, da je vsako od praštevil $p_1, \ldots, p_j$ v množici praštevil $\{q_1, \ldots, q_k\}$, ki delijo n.

Za vsako praštevilo q_i velja $q_i^n \geq 2^n \geq n + 1 \geq p$. Med drugim to velja tudi za vsako praštevilo p_i, ki deli $p - 1$. Torej je $p_i^{e_i} \leq p - 1 < n + 1 \leq p_i^n$ oziroma $e_i < n$ za vse $i = 1, \ldots, j$. Od tod sklepamo, da $p - 1$ deli število $(p_1 \cdots p_j)^n$ in torej tudi število n^n. Naj bo $d \in \mathbb{N}$ takšno število, da je

$n^n = d(p-1)$. Ker p ne deli n, lahko uporabimo mali Fermatov izrek in dobimo $n^{n^n} = (n^d)^{p-1} \equiv 1 \pmod p$. Torej p deli $n^{n^n} - 1$. Vsako praštevilo, ki deli $n^{n^n} - 1$, seveda ne deli n in je zato večje kvečjemu enako praštevilu p, ki je najmanjše praštevilo, ki ne deli n. Se pravi, da je p najmanjše praštevilo, ki deli $n^{n^n} - 1$. Isti argument nam zagotavlja, da velja tudi obratna implikacija. Če je p najmanjše praštevilo, ki deli $n^{n^n} - 1$, potem p ne deli n. To praštevilo je najmanjše med tistimi, ki ne delijo n, saj smo že videli, da najmanjše praštevilo, ki ne deli n, deli $n^{n^n} - 1$. ∎

Wooleyev generator praštevil je naslednji postopek:

- naj bo $p_1 = 2$;
- za $k \in \mathbb{N}$, $k \geq 2$, naj bo $n = p_1 \cdots p_{k-1}$ in p_k najmanjše praštevilo, ki deli $n^{n^n} - 1$.

Z uporabo leme 8 vidimo, da nam algoritem na k-tem koraku vrne k-to najmanjše praštevilo. Se pravi, s tem postopkom dobimo natanko vsa praštevila, urejena po velikosti.

LITERATURA

[1] R. C. Baker, G. Harman in J. Pintz, *The difference between consecutive primes, II*, Proceedings of the London Mathematical Society **83** (2001), 532–562.

[2] A. R. Booker, *On Mullin's second sequence of primes*, Integers **12** (2012), 1167–1177.

[3] A. R. Booker in C. Pomerance, *Squarefree smooth numbers and Euclidean prime generators*, Proceedings of the American Mathematical Society **145** (2017), 5035–5042.

[4] Y. F. Cheng, *Explicit estimate on primes between consecutive cubes*, Rocky Mountain Journal of Mathematics **40** (2010), 117–153.

[5] B. Green in T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics (2) **167** (2008), 481–547.

[6] N. Mackinnon, *Prime number formulae*, The Mathematical Gazette **71** (1987), 113–114.

[7] W. H. Mills, *A prime-representing function*, Bulletin of the American Mathematical Society **53** (1947), 604.

[8] A. A. Mullin, *Recursive function theory. (A modern look at a Euclidean idea.)*, Bulletin of the American Mathematical Society **69** (1963), 737.

[9] T. D. Wooley, *A Superpowered Euclidean prime generator*, American Mathematical Monthly **124** (2017), 351–352.

[10] *Formula for primes*, dostopno na `en.wikipedia.org/wiki/Formula_for_primes`, ogled 22. 12. 2018.

[11] *Sieve of Sundaram*, dostopno na `en.wikipedia.org/wiki/Sieve_of_Sundaram`, ogled 22. 12. 2018.