Универзитет у Београду
Математички факултет

МАСТЕР РАД

МЕРСЕНОВИ ПРОСТИ БРОЈЕВИ

Ментор:
Проф. др Миодраг Живковић

Студент:
Тамара Трифуновић
1026/2011

У Београду, мај 2015.

Садржај

1 Увод

Још око 300 година п.н.е. Еуклид (Euclid) је доказао да има бесконачно простих бројева. О расподели простих бројева међу природим бројевима говори тзв. теорема о простим бројевима доказана у 19. веку. На основу теореме о простим бројевима вероватноћа да је случајно изабрани цео број у опсегу $(1, n]$ прост је приближно једнака $1/\ln(n)$ за довољно велико n.

Многи од давнина познати нерешени проблеми везани за просте бројеве подстакли су развој теорије бројева. Неки од тих проблема су нпр. Голдбахова (Goldbach) хипотеза (сваки паран број већи од 2 се може написати као сума два проста броја) и хипотеза о простим бројевима близанацима (има бесконачно много парова простих бројва чија је разлика 2). Од круцијалног значаја у теорији бројева и математици генерално је основна теорема аритметике, тј. тврђење да се сваки природан број може на јединствен начин представити као производ својих простих чинилаца.

Дуго времена мислило се да прости бројеви имају изузетно ограничену примену ван чисте математике. То се променило седамдесетих година 20. века када су смишљени концепти криптографије са јавним кључем. Тежак проблем факторизације великих бројева на просте чиниоце довео је до проналажења метода за шифровање где прости бројеви заузимају значајно место. Криптосистеми са јавним кључем заснивају се на употреби два кључа, једним за шифровање и другим за дешифровање (због тога су и добили назив асиметрични). Асиметрични алгоритми своју тајност не заснивају на непознавању алгоритма, већ на употреби једносмерних функција. То су функције за које је ефективно израчунавање вредности инверзне функције тежак математички проблем, тешко решив рачунарским ресурсима у реалном времену. У већини асиметричних алгоритама за генерисање кључева се користе велики прости бројеви са стотину и више децималних цифара. Зато је у криптографији са јавним кључем изузетно важно имати метод за генерисање великог простог броја.

Постоје разне методе за проверу да ли је дати цео број прост. Основни метод састоји се у дељењу датог броја n могућим простим факторима који су већи од један, а мањи или једнаки квадратном корену од n и ако ниједан од ових количника није цео број, онда је дати број n прост. Иако једноставан, овај метод је врло непрактичан за тестирање великих бројева зато што број могућих фактора јако брзо расте са порастом n. Број простих фактора се може проценити на основу теореме о простим бројевима: број простих бројева мањих од $\sqrt{n}$ је приближно $\sqrt{n}/\ln(\sqrt{n})$. На пример за $n = 10^{20}$ овај број је око 450 милиона, што је превише за многе практичне примене.

Модерни тестови се деле у две групе: детерминистички и пробабилистички. Детерминистички засигурно тврде, док пробабилистички, који су често знатно бржи, не доказују потпуно да је дати број прост. Због тога се често прво примењују

пробабилистичке пре детерминистичких метода. Када је реч о детерминистичким методама, многи математичари су проучавали тестове за проверу великих бројева, али с ограничењем на бројеве одређеног облика. Алгоритми који раде са произвољним бројевима и даље заостају по ефикасности.

Тема овог рада су прости бројеви облика $h \cdot 2^n - 1$. Специјално за $h = 1$, прости бројеви облика $2^n - 1$ називају се Мерсенови прости бројеви. За овај рад инспирација је Х. Риселов (H. Riesel) рад *Lucasian criteria for the primality of* $h \cdot 2^n - 1$ [6]. У овом раду су описани најефикаснији алгоритами за проверу да ли је дати број прост. То су Лукас-Лемеров тест за Мерсенове бројеве [5], као и генерализација [6] овог теста за бројеве облика $h \cdot 2^n - 1$. Пажња је посвећена посебно теоријском делу Лукас-Лемеровог теста за Мерсенове просте бројеве, као и теоремама на којима се заснива генерализација овог теста за просте бројеве облика $h \cdot 2^n - 1$. Када су у питању бројеви $h \cdot 2^n - 1$, за h непарно и $h < 2^n$, критеријуми да је $N = h \cdot 2^n - 1$ прост број су следећег типа [6]: за одговарајуће u_0, број N је прост ако и само ако $u_{n-2} \equiv 0 \pmod{N}$, где је $u_{s+1} = u_s^2 - 2$. Дакле, проблем одређивања критеријума за дату комбинацију h и n састоји се у проналажењу одговарајућег u_0. Постоји једноставан резултат везан за u_0 када су у питању све непарне вредности h, осим ако 3 дели h. У раду је показано на који начин се u_0 може одредити за $h = 3A$. На основу тога је имплементиран тест, чији је опис дат у овом раду, који проверава да ли је број облика $3A \cdot 2^n - 1$ прост.

У поглављу *Неопходни појмови и тврђења* уводе се дефиниције и теореме на којима се базирају докази из следећих поглавља. За даља излагања у раду потребно је разумевање основних појмова и теорије о квадратним пољима. Наредно поглавље уводи појам Мерсенових простих бројева као посебног облика простих бројева. Приказан је историјат Мерсенових простих бројева, потом њихова веза са савршеним бројевима, као и тренутно најбољи алгоритам за проналажење ових бројева, Лукас-Лемеров тест. У 4. поглављу описана је генерализација Лукас-Лемеровог теста за просте бројеве облика $h \cdot 2^n - 1$ заједно са теоремама на којима се заснива. Поглавље *Имплементација, детаљи програма и резултати* садржи опис имплементације теста за бројеве облика $h \cdot 2^n - 1$ и резултате за $h = 3A, A \leq 45$ и $n \leq 1500$. За све друге непарне вредности h случај је једноставнији.

2 Неопходни појмови и тврђења

У овом поглављу наводе се дефиниције и теореме важне за разумевање теорема и њихових доказа из следећих поглавља. На почетку поглавља је део из теорије бројева који се односи на дефиницију Лагранжовог (Lagrange) и Јакобијевог (Jacobi) симбола, Ојлеров (Euler) критеријум и квадратни закон реципроцитета. Потом следе основе из теорије о квадратним пољима на којима се базирају будући докази у раду. Дефинисано је квадратно поље, цели бројеви у квадратном пољу, јединице и фундаменталне јединице, дељивост и факторизација у квадратном пољу. Наведене су и две теореме које важе у квадратним пољима значајне за даља доказивања.

Теорема 2.1. (мала Фермаова (Fermat) теорема) [9] Нека је p прост број, a природан број и $p \nmid a$. Тада важи:

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

Дефиниција 2.1. (квадратни остатак) Нека је m природан број већи од 1. Уколико једначина $x^2 \equiv a \pmod{m}$ има решења, онда се број a назива *квадратним остатком по модулу* m, док у супротном кажемо да је a *квадратни неостатак по модулу* m.

Дефиниција 2.2. (Лежандров симбол) Нека је p прост број већи од 2 и a цео број. *Лежандров симбол* (Legendre symbol) се дефинише на следећи начин:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако је } a \text{ квадратни остатак по модулу } p \\ -1, & \text{ако је } a \text{ квадратни неостатак по модулу } p \\ 0, & \text{ако } p|a \end{cases}.$$

Дефиниција 2.3. (Јакобијев симбол) Нека је m непаран цео број чији је канонски облик $m = \prod_{i=1}^{k} p_i^{e_i}$ и a цео број такав узајамно прост са m. Онда је *Јакобијев симбол* $(\frac{a}{m})$ дефинисан са

$$\left(\frac{a}{m}\right) = \left(\frac{a}{\prod_{i=1}^{k} p_i^{e_i}}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

где је $(\frac{a}{p_i})$ Лежандров симбол.

Теорема 2.2. (Ојлеров критеријум) Нека је p непаран прост број, и a цео број узајамно прост са p. Тада важи једнакост:

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

Доказ. Према малој Фермаовој теореми, с обзиром да су a и p узајамно прости, важи:

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

тј.

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Претходно може се написати у облику:

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}. \quad (1)$$

Како је p прост, ако је производ два броја по модулу p конгруентан са нулом по модулу p, онда бар један од тих бројева мора бити нула по модулу p. Значи, у (1) бар један од фактора $(a^{\frac{p-1}{2}} - 1)$, $(a^{\frac{p-1}{2}} + 1)$ мора бити конгруентан нули по модулу p.

Нека је a квадратни остатак по модулу p, тј. $a \equiv x^2 \pmod{p}$ за неки цео број $0 \leq x \leq p-1$. Применом мале Фермаове теореме добија се

$$a^{\frac{p-1}{2}} - 1 = (x^2)^{\frac{p-1}{2}} - 1 = x^{p-1} - 1 \equiv 1 - 1 = 0 \pmod{p},$$

односно

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Дакле, ако a јесте квадратни остатак по модулу p, (1) је задовољена, а тиме и тај део доказа завршен.

Нека сада a није квадратни остатак по модулу p. На основу мале Фермаове теореме,

$$a^{\frac{p-1}{2}} = (a^{p-1})^{\frac{1}{2}} \equiv (1)^{\frac{1}{2}} \equiv q \pmod{p}$$

где је q цео број такав да је $q^2 \equiv 1 \pmod{p}$. Према томе, два кандидата за q су ± 1. q не може бити $+1$, јер је тада $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, односно a је квадратни остатак по модулу p, што је супротно претпоставци. Дакле $q = -1 \pmod{p}$ тј. $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ и тиме је доказ завршен.

Лема 2.1. (Гаус (Gauss)) Нека је p непаран прост број и $(a, p) = 1$. Нека је μ број остатака у скупу ak, $1 \leq k \leq \frac{p-1}{2}$, чија је вредност већа од $\frac{p-1}{2}$. Тада је

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

Доказ. Нека је $la \equiv \pm m_l \pmod{p}$, где је $1 \leq m_l \leq \frac{p-1}{2}$. Како је $k \pm l \not\equiv 0 \pmod{p}$, за $1 \leq k < l \leq \frac{p-1}{2}$, то је $m_l \neq m_k$ за све $1 \leq k < l \leq \frac{p-1}{2}$. Дакле, $\{1, 2, \ldots, \frac{p-1}{2}\} = \{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\}$, па множењем конгруенција $la \equiv \pm m_l \pmod{p}$ добијамо

$$\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! \cdot (-1)^{\mu} \pmod{p}.$$

Тврђење леме сада следи из Ојлеровог критеријума.

Теорема 2.3. (квадратни закон реципроцитета) Ако су p и q различити непарни прости бројеви, тада важи

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Доказ. На основу Гаусове леме важи $\left(\frac{q}{p}\right) = (-1)^{\nu}$, где је ν број целих бројева x таквих да је $1 \leq x \leq \frac{p-1}{2}$ и $qx = py + r$ где је $-\frac{p}{2} < r < 0$, и y цео број. Такође важи да је $1 \leq y \leq \frac{q-1}{2}$, јер је y ненегативан и

$$py = xq - r < \frac{p-1}{2}q + \frac{p}{2} < \frac{p}{2}(q+1)$$

одакле следи $y < \frac{q+1}{2}$ односно $y \leq \frac{q-1}{2}$.

Слично, $\left(\frac{p}{q}\right) = (-1)^{\mu}$, где је μ број целих бројева y таквих да је $1 \leq y \leq \frac{q-1}{2}$, тако да је $py = qx + s$ где је $-\frac{q}{2} < s < 0$ и x је цео број. Сада је поново $1 \leq x \leq \frac{p-1}{2}$. Зато је $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\nu+\mu}$.

Закључује се да је $\nu + \mu$ број уређених парова целих бројева (x, y) таквих да је $1 \leq x \leq \frac{p-1}{2}$, $1 \leq y \leq \frac{q-1}{2}$ и $-\frac{p}{2} < qx - py < \frac{q}{2}$.

Посматрају се следећи скупови уређених парова целих бројева:

$S = \{(x, y) | 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}$
$S_1 = \{(x, y) \in S | qx - py \leq -\frac{p}{2}\}$
$S_0 = \{(x, y) \in S | -\frac{p}{2} < qx - py < \frac{q}{2}\}$
$S_1' = \{(x, y) \in S | \frac{q}{2} \leq qx - py\}$.

Пресликавање $\Theta : S \to S$, дефинисано са $\Theta(x, y) = (x', y')$, где су $x' = \frac{p+1}{2} - x$, $y' = \frac{q+1}{2} - y$ је бијекција, Θ^2 је идентитет, $\Theta(S_1) = S_1'$, $\Theta(S_1') = S_1$, $\Theta(S_0) = S_0$.

Дакле, $|S| = |S_1| + |S_0| + |S_1'| \equiv |S_0| \pmod{2}$ и следи

$$\frac{p-1}{2} \cdot \frac{q-1}{2} \equiv \mu + \nu \pmod{2}.$$

Зато је

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

У наставку се наводе основни појмови и неопходне теореме из теорије о квадратним пољима.

За цео број D без квадратних фактора и $D \neq 0, 1$, скуп $K = \mathbb{Q}(\sqrt{D}) = \{x + y\sqrt{D} : x, y \in \mathbb{Q}\}$ чини *квадратно поље* степена 2 над Q. Ако је $D > 0$, онда је то *реално квадратно поље*, у супротном *имагинарно*. Слично, $\mathbb{Z}(\sqrt{D}) = \{x + y\sqrt{D} : x, y \in \mathbb{Z}\}$ и представља потпрстен поља $\mathbb{Q}(\sqrt{D})$.

Посматрајмо бројеве z облика $z = r + s\sqrt{D}$, где су r, s рационални бројеви, а D цео број без квадратног фактора.

Дефиниција 2.4. (цео број у квадратном пољу) За број z се каже да је *цео број* у квадратном пољу $\mathbb{Q}(\sqrt{D})$ ако задовољава квадратну једначину облика

$$z^2 + pz + q = 0$$

где су p и q рационални цели бројеви.

Како је z решење квадратне једначине

$$(z - r)^2 = Ds^2 \text{ тј. } z^2 - 2rz + r^2 - Ds^2,$$

онда да би z био цео број у $\mathbb{Q}(\sqrt{D})$, неопходан и довољан услов је да $-2r$ и $r^2 - Ds^2$ буду рационални цели бројеви. Нека је $r = a/2$ за рационални цео број a, тада је $2r$ увек рационални цео број, а $r^2 - Ds^2$ је рационални цео број у два случаја:

1. a је паран (тј. r је рационални цео број) и s је рационални цео број

или

2. a је непаран (у том случају $a^2/4 \equiv 1/4 \pmod 1$) и $Ds^2 \equiv 1/4 \pmod 1$. Друго важи ако и само ако $s \equiv 1/2 \pmod 1$ и $D \equiv 1 \pmod 4$.

Ова два случаја се могу преформулисати:

Цели бројеви у $\mathbb{Q}(\sqrt{D})$ су бројеви облика $z = r + s\rho$, где је

$$\rho = \begin{cases} \sqrt{D}, & \text{ако је } D \equiv 2, 3 \pmod 4 \\ \dfrac{-1 + \sqrt{D}}{2}, & \text{ако је } D \equiv 1 \pmod 4 \end{cases}.$$

Дефиниција 2.5. (конјугати у квадратном пољу) Бројеви $x = r + s\sqrt{D}$ и $\overline{x} = r - s\sqrt{D}$ називају се *конјугати* у $\mathbb{Q}(\sqrt{D})$.

Дефиниција 2.6. (норма броја у квадратном пољу) Рационални број $x\overline{x} = N(x) = N(\overline{x})$ назива се *норма* броја x.

Дефиниција 2.7. (јединица у квадратном пољу) Ако је x цео број у $\mathbb{Q}(\sqrt{D})$ и $N(x) = \pm 1$, онда се x назива *јединицом* у $\mathbb{Q}(\sqrt{D})$.

У реалном квадратном пољу постоји специјална јединица ϵ, звана *фундаментална јединица*, таква да су све јединице у $\mathbb{Q}(\sqrt{D})$ обухваћене са $\pm\epsilon^n$ за $n \in \mathbb{Z}$. Фундаментална јединица се може израчунати решавањем Пелове (Pell) једначине $T^2 - DU^2 = \pm 4$, где се

знак узима тако да решење (T, U) буде са најмањим могућим позитивним T. За такво минимално (T, U), ϵ је дато са $\epsilon = \frac{1}{2}(T + U\sqrt{D})$.

Дефиниција 2.8. (придружени бројеви у квадратном пољу) За целе бројеве α и β у $\mathbb{Q}(\sqrt{D})$ се каже да су *придружени* ако је њихов количник јединица у $\mathbb{Q}(\sqrt{D})$.

Дефиниција 2.9. (дељивост у квадратном пољу) Ако је $\alpha = \beta\gamma$, где су α, β и γ цели бројеви у $\mathbb{Q}(\sqrt{D})$, онда се каже да је α *дељиво* са β (и са γ). Ознака: $\beta|\alpha$ (β дели α).

Дефиниција 2.10. (прост број у квадратном пољу) Ако се цео број α у $\mathbb{Q}(\sqrt{D})$ не може представити као $\alpha = \beta\gamma$, где су β и γ цели у $\mathbb{Q}(\sqrt{D})$ осим ако један од њих није јединица у $\mathbb{Q}(\sqrt{D})$, онда се за α каже да је *прост* у $\mathbb{Q}(\sqrt{D})$. У супротном, α је *сложен* у $\mathbb{Q}(\sqrt{D})$.

Сваки цео број α у $\mathbb{Q}(\sqrt{D})$ се може представити као производ простих фактора из $\mathbb{Q}(\sqrt{D})$. За разлику од факторизације код рационалних целих бројева, ова факторизација је јединствена само у неким случајевима.

Дефиниција 2.11. (највећи заједнички делилац у квадратном пољу) Нека су α, β и γ цели бројеви у $\mathbb{Q}(\sqrt{D})$. Ако је α заједнички делилац β и γ и сваки заједнички делилац β и γ дели α, онда се α назива *највећи заједнички делилац* β и γ и означава се (β, γ).

Највећи заједнички делилац није јединствен с обзиром да је сваки придружени број највећем заједничком делиоцу такође највећи заједнички делилац.

Теорема 2.4. (Фермаова теорема у $K(\sqrt{D})$) Ако је α цео број у $K(\sqrt{D})$, D није дељив квадратом неког броја, p непаран прост број, и ако је $(\alpha, p) = 1$ у $K(\sqrt{D})$, онда је

$$\alpha^{p-1} \equiv 1 \pmod{p}, \text{ ако је } \left(\frac{D}{p}\right) = 1,$$

$$\alpha^{p+1} \equiv \alpha\overline{\alpha} \pmod{p}, \text{ ако је } \left(\frac{D}{p}\right) = -1.$$

Овде је $\left(\frac{D}{p}\right)$ Лежандров симбол.

Теорема 2.5. (корен из -1) Ако постоји природан број K, такав да је

$$\alpha^K \equiv -1 \pmod{p},$$

онда постоји најмањи природан број k, такав да је

$$\alpha^k \equiv -1 \pmod{p},$$

при чему је K/k непаран цели број. Даље, $e = 2k$ је најмањи природан број такав да је

$$\alpha^e \equiv +1 \pmod{p}.$$

.

3 Мерсенови прости бројеви

Поставља се питање за које целе бројеве a је $a^n - 1$, $n \geq 2$ прост број. Растављањем

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1)$$

види се да $a-1|a^n-1$, што значи да је a^n-1 сложен осим ако је $a-1 = 1$, односно $a = 2$. Дакле, довољно је проучавати бројеве облика $2^n - 1$. Такође, довољно је испитивати само случај када је n прост број. У супротном, ако је n сложен, нпр. $n = mk$, онда је

$$2^n - 1 = 2^{mk} - 1 = (2^m)^k - 1 = (2^m - 1)((2^m)^{k-1} + (2^m)^{k-2} + \ldots + 2^m + 1),$$

односно $2^n - 1$ има фактор $2^m - 1$. $2^n - 1$ може бити прост ако је $2^m - 1 = 1$, тј. $m = 1$. То значи, ако је n сложен, онда је и $2^n - 1$ сложен број. Према томе, довољно је проучавати бројеве облика $2^p - 1$, где је p прост број. Број $M_p := 2^p - 1$ не мора бити прост ($2^{11} - 1 = 2047 = 23 \cdot 89$), а ако јесте прост, онда се назива Мерсенов прост број.

Уопште, Мерсенови бројеви су цели бројеви облика $2^s - 1$, $s \geq 2$, а Мерсенови бројеви који су прости, зову се Мерсенови прости бројеви.

Ови бројеви добили су име по француском математичару Марину Мерсену (фр. Marin Mersenne, 1588-1648). Мерсен је проучавао просте бројеве покушавајући да нађе израз који би их све објединио. У томе није успео, али је његов рад подстакао многе да наставе оно што је он започео.

3.1 Историја и преглед до сада откривених Мерсенових простих бројева

Када је у питању најранија историја, дуго се сматрало да су бројеви облика $2^n - 1$ прости за све просте n [4]. Х. Региус (H. Regius)[1] је 1536. године показао да је $2^{11} - 1$ сложен. До 1603. П. Каталди (P. Cataldi)[2] је установио да су $2^{17} - 1$ и $2^{19} - 1$ оба прости, а потом тврдио и да су $2^n - 1$ за $n = 23, 29, 31$ и 37 прости. Ферма је 1640. показао да је Каталди погрешио у вези са бројевима 23, 37, а онда је Ојлер 1738. показао да је Каталди погрешио и у вези са бројем 29. Нешто касније Ојлер доказује да је Каталдијева тврдња за број 31 тачна.

Марин Мерсен је навео у својој Cogitata Physica-Mathematica (1644) да су бројеви

[1] Hudalrichus Regius (XVI век) је грчки математичар који је у свом делу *Utriusque Arithmetices* показао да бројеви облика $2^n - 1$ нису прости за све n као што се до тада сматрало.

[2] Pietro Antonio Cataldi (15. април 1548 – 11. фебруар 1626.) је био италијански математичар. Предавао је математику и астрономију и бавио се војним проблемима.

$2^n - 1$ прости за $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ и 157 и сложени за све остале позитивне целе бројеве $n < 257$. Иако је Мерсенова претпоставка била нетачна, његово име је остало везано за ове бројеве. Његовим колегама је било очигледно да он није могао проверити све ове бројеве, што је и сам признавао, али нису могли ни они.

Око 100 година касније, Ојлер је овој листи додао следећи прост број $2^{31} - 1$. Након још једног века, 1876. године Е. Лукас (E. Lucas) је потврдио да је $2^{127} - 1$ прост. Седам година касније, Первушин (I. M. Pervushin)[3] је показао да је Мерсен у својој листи изоставио број $2^{61} - 1$. Такође је изоставио бројеве $2^{89} - 1$ и $2^{107} - 1$, што је Р. Е. Пауерс (R. E. Powers)[4] показао раних 1900-тих. Коначно, до 1947. Мерсенова листа је комплетно проверена и утврђено је да су бројеви $2^n - 1$ прости за $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107$ и 127.

Са појавом електронских дигиталних рачунара настала је револуција у потрази за Мерсеновим простим бројевима. Алан Тјуринг (Alan Turing) је Мерсенове просте бројеве тражио 1949. године на Manchester Mark 1 рачунару. Међутим, први следећи успешни резултат је број M_{521} 30. јануара 1952. Пројектом је управљао Д. Х. Лемер (D. H. Lehmer) на Универзитету у Калифорнији у Лос Анђелесу (УКЛА). Коришћен је рачунар U.S. National Bureau of Standards Western Automatic Computer (SWAC), а програм за пројекат је писао Робинсон (R. M. Robinson)[5]. После мање од два сата пронађен је следећи број M_{607}, такође коришћењем тог рачунара. У следећих неколико месеци коришћењем истог програма откривена су још три броја M_{1279}, M_{2203} и M_{2281}. M_{4253} је први откривени број са најмање 1000 децималних цифара, M_{44497} са најмање 10000 цифара, а $M_{6972593}$ са најмање 1000000 цифара.

Great Internet Mersenne Prime Search (GIMPS) [3] је заједнички пројекат добровољаца који користе јавно доступан софтвер за проналажење Мерсенових простих бројева. Пројекат је основао Џорџ Волтман (George Woltman)[6] у јануару 1996. године. Он је за потребе овог пројекта написао софтвер Prime95 и MPrime. Скот Куровски (Scott Kurowski)[7] је 1997. године написао PrimeNet сервер који преко интернета управља задацима и резултатима добровољаца без људске интервенције. Куровски је на тај начин омогућио пораст пројекта у целини. За GIMPS се каже да је један од првих пројеката дистрибуираног рачунарства великих размера преко интернета за истраживачке сврхе.

[3] Ivan Mikheevich Pervushin (21. јануар 1827 – 29. јун 1900.) је био руски свештеник и математичар, посебно заинтересован за теорију бројева.

[4] Ralph Ernest Powers (27. април 1875 – 31. јануар 1952.) је био амерички математичар који се бавио простим бројевима.

[5] Raphael M. Robinson (1911-1995.) је био амерички математичар. Бавио се теоријом бројева, математичком логиком, теоријом низова, геометријом и комбинаториком. Искодирао је Лукас-Лемеров тест за SWAC и открио највеће Мерсенове просте бројеве познате у то време.

[6] George Woltman (рођен 10. новембра 1957.), оснивач GIMPS пројекта, студирао је рачунарство на Масачусетском институту за технологију (МИТ).

[7] Scott Kurowski је 1997. основао компанију Entropia у Калифорнији која се бави дистрибуираним рачунарством. GIMPS је заправо доказ концепта пројекта, да покаже инвеститорима да дистрибуирано програмирање има комерцијалну будућност.

У септембру 2008. године, математичари из УКЛА су учествујући у GIMPS пројекту освојили $100000 вредну награду од Electronic Frontier Foundation (EFF) за проналажење простог броја са најмање 10000000 цифара. Овај прост број има око 13 милиона цифара и пронађен је на Dell OptiPlex 745 крајем августа 2008.

У јуну 2009. године, помоћу GIMPS пројекта откривен је 47. Мерсенов прост број $M_{242643801}$. Иако је 47. хронолошки откривен број, није највећи. Мањи је од највећег познатог у то време, 45. откривеног.

К. Купер (Curtis Cooper)[8] је 25. јануара 2013. открио 48. и највећи до сада Мерсенов прост број $M_{57885161}$, број са 17425170 цифара, као резултат претраге помоћу GIMPS мреже. То је трећи Мерсенов прост број који су Купер и његов тим открили у последњих седам година. Уједно, то је и до сада највећи познат прост број уопште. За запис овог броја у основи 10 потребно је 4647 страница са 75 цифара по линији и 50 линија по страни.

EFF нуди награду од $150000 ономе ко открије прост број са најмање 100000000 децималних цифара.

Следи листа свих познатих Мерсенових простих бројева [3]:

#	p	M_p	број цифара	датум открића	проналазач	коришћена метода и рачунар
1	2	3	1	око 430. пне	антички грчки математичари	
2	3	7	1	око 430. пне	антички грчки математичари	
3	5	31	2	око 430. пне	антички грчки математичари	
4	7	127	3	око 430. пне	антички грчки математичари	
5	13	8191	4	1456.	непознат	проста провера
6	17	131071	6	1588.	P. Cataldi	проста провера
7	19	524287	6	1588.	P. Cataldi	проста провера
8	31	2147483647	10	1722.	L. Euler	оптимизована провера
9	61	2305843009213693951	19	новембар 1883.	I. M. Pervushin	Лукасов низ
10	89	618970019642...137449562111	27	јун 1911.	R. E. Powers	Лукасов низ
11	107	162259276829...578010288127	33	1. јун 1914.	R. E. Powers	Лукасов низ
12	127	170141183460...715884105727	39	10. јануар 1876.	E. Lucas	Лукасов низ
13	521	686479766013...291115057151	157	30. јануар 1952.	R. M. Robinson	LLT[9] / SWAC
14	607	531137992816...219031728127	183	30. јануар 1952.	R. M. Robinson	LLT / SWAC
15	1279	104079321946...703168729087	386	25. јун 1952.	R. M. Robinson	LLT / SWAC
16	2203	147597991521...686697771007	664	7. октобар 1952.	R. M. Robinson	LLT / SWAC
17	2281	446087557183...418132836351	687	9. октобар 1952.	R. M. Robinson	LLT / SWAC
18	3217	259117086013...362909315071	969	8. септембар 1957.	H. Riesel	LLT / BESK
19	4253	190797007524...815350484991	1281	3. новембар 1961.	A. Hurwitz	LLT / IBM 7090
20	4423	285542542228...902608580607	1332	3. новембар 1961.	A. Hurwitz	LLT / IBM 7090

[8] Curtis Cooper (рођен 27. децембра 1915.) је амерички математичар, професор на Универзитету у Централном Мисурију

[9] Лукас-Лемеров тест, поглавље 3.3

21	9689	478220278805...826225754111	2917	11. мај 1963.	D. B. Gillies	LLT / ILLIAC II
22	9941	346088282490...883789463551	2993	16. мај 1963.	D. B. Gillies	LLT / ILLIAC II
23	11213	281411201369...087696392191	3376	2. јун 1963.	D. B. Gillies	LLT / ILLIAC II
24	19937	431542479738...030968041471	6002	4. март 1971.	B. Tuckerman	LLT / IBM 360/91
25	21701	448679166119...353511882751	6533	30. октобар 1978.	L. C. Noll, L. Nickel	LLT / CDC Cyber 174
26	23209	402874115778...523779264511	6987	9. фебруар 1979.	L. C. Noll	LLT / CDC Cyber 174
27	44497	854509824303...961011228671	13395	8. април 1979.	H. L. Nelson, D. Slowinski	LLT / Cray 1
28	86243	536927995502...209433438207	25962	25. септембар 1982.	D. Slowinski	LLT / Cray 1
29	110503	521928313341...083465515007	33265	29. јануар 1988.	W. Colquitt, L. Welsh	LLT / NEC SX-2
30	132049	512740276269...455730061311	39751	19. септембар 1983.	D. Slowinski	LLT / Cray X-MP
31	216091	746093103064...103815528447	65050	1. септембар 1985.	D. Slowinski	LLT / Cray X-MP/24
32	756839	174135906820...328544677887	227832	17. фебруар 1992.	D. Slowinski, P. Gage	LLT / Harwell Lab's Cray-2
33	859433	129498125604...243500142591	258716	4. јануар 1994.	D. Slowinski, P. Gage	LLT / Cray C90
34	1257787	412245773621...976089366527	378632	3. септембар 1996.	D. Slowinski, P. Gage	LLT / Cray T94
35	1398269	814717564412...868451315711	420921	13. новембар 1996.	GIMPS/ J. Armengaud	LLT / Prime95 on 90 MHz Pentium PC
36	2976221	623340076248...743729201151	895932	24. август 1997.	GIMPS/ G. Spence	LLT / Prime95 on 100 MHz Pentium PC
37	3021377	127411683030...973024694271	909526	27. јануар 1998.	GIMPS/ R. Clarkson	LLT / Prime95 on 200 MHz Pentium PC
38	6972593	437075744127...142924193791	2098960	1. јун 1999.	GIMPS/ N. Hajratwala	LLT / Prime95 on 350 MHz Pentium II IBM Aptiva
39	13466917	924947738006...470256259071	4053946	14. новембар 2001.	GIMPS/ M. Cameron	LLT / Prime95 on 800 MHz Athlon T-Bird
40	20996011	125976895450...762855682047	6320430	17. новембар 2003.	GIMPS/ M. Shafer	LLT / Prime95 on 2 GHz Dell Dimension
41	24036583	299410429404...882733969407	7235733	15. мај 2004.	GIMPS/ J. Findley	LLT / Prime95 on 2.4 GHz Pentium 4 PC
42	25964951	122164630061...280577077247	7816230	18. фебруар 2005.	GIMPS/ M. Nowak	LLT / Prime95 on 2.4 GHz Pentium 4 PC
43	30402457	315416475618...411652943871	9152052	15. децембар 2005.	GIMPS/C. Cooper, S. Boone	LLT / Prime95 on 2 GHz Pentium 4 PC
44	32582657	124575026015...154053967871	9808358	4. септембар 2006.	GIMPS/C. Cooper, S. Boone	LLT / Prime95 on 3 GHz Pentium 4 PC
45*	37156667	202254406890...022308220927	11185272	6. септембар 2008.	GIMPS/ H.-M. Elvenich	LLT / Prime95 on 2.83 GHz Core 2 Duo PC
46*	42643801	169873516452...765562314751	12837064	12. април 2009.	GIMPS/ O. M. Strindmo	LLT / Prime95 on 3 GHz Core 2 PC
47*	43112609	316470269330...166697152511	12978189	23. август 2008.	GIMPS/ E. Smith	LLT / Prime95 on Dell Optiplex 745
48*	57885161	581887266232...071724285951	17425170	25. јануар 2013.	GIMPS/ C. Cooper	LLT / Prime95 on 3 GHz Intel Core2 Duo E8400

Није познато да ли има неоткривених Мерсенових простих бројева између 44. и 48. броја у претходној табели. Из тог разлога знак * поред бројева у табели означава да је рангирање привремено. Сви Мерсенови бројеви испод 47. су тестирани барем једном, али неки нису два пута проверени, а изнад 47. неки нису ни тестирани.

3.2 Веза Мерсенових простих бројева са парним савршеним бројевима

Интересантна чињеница у вези са Мерсеновим простим бројевима је њихова коресподенција са савршеним бројевима. Савршени бројеви су цели бројеви који су једнаки збиру својих делилаца (у делиоце не спада сам тај број, нпр. $6 = 1 + 2 + 3$). У IV веку п.н.е. Еуклид је показао да ако је $2^p - 1$ прост, онда је $2^{p-1}(2^p - 1)$ савршен број. Ојлер је у XVIII веку доказао да је сваки паран савршен број тог облика.

Теорема 3.1. (Ојлер) Нека је n позитиван, паран број. Тада,

$$n \text{ је савршен ако и само ако је } n = 2^{p-1}(2^p - 1),$$

где су p и $2^p - 1$ прости бројеви.

Доказ. Нека је $\sigma(n) = \sum_{d|n} d$ (тј. $\sigma(n)$ је сума свих делилаца од n). Тада важе следеће особине за σ:

1. $\sigma(1) = 1$
2. n прост ако и само ако $\sigma(n) = n + 1$
3. ако је p прост, $\sigma(p^j) = 1 + p + \ldots + p^j = \frac{p^{j+1}-1}{p-1}$
4. мултипликативност - ако је $(n_1, n_2) = 1$, онда је $\sigma(n_1)\sigma(n_2) = \sigma(n_1 n_2)$ ((a, b) означава највећи заједнички делилац бројева a и b).

Број u савршен ако је $u = \sigma(u) - u$, тј. $\sigma(u) = 2u$.

$\Leftarrow$: Нека је $n = 2^{p-1}q$, где је $q = 2^p - 1$ Мерсенов прост број. Треба показати да је n савршен, односно да је $\sigma(n) = 2n$.

Како је $(2^{p-1}, q) = 1$, онда је

$$\sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)(q + 1) = 2n.$$

$\Rightarrow$: Нека је n паран, савршен број. С обзиром да је n паран, може се написати у облику

$$n = 2^j m, \quad j \geq 1, \; m \text{ непаран и } m \neq n.$$

Одатле следи да је

$$\sigma(n) = \sigma(2^j)\sigma(m) = (2^{j+1} - 1)\sigma(m).$$

А како је n савршен,

$$\sigma(n) = 2n = 2^{j+1}m.$$

Дакле,

$$(2^{j+1} - 1)\sigma(m) = 2^{j+1}m,$$

из чега следи $2^{j+1}|\sigma(m)$, тј. за неко $r \geq 1$ је

$$r2^{j+1} = \sigma(m)$$

Такође,

$$2^{j+1}m = (2^{j+1} - 1)r2^{j+1},$$

односно

$$m = (2^{j+1} - 1)r.$$

Претпоставимо да је $r > 1$. Тада, на основу претходне једначине, m има 3 различита делиоца: 1, r и m (по хипотези $r \neq 1$ и, $r \neq m$, јер ако је $r = m$, онда је $j = 0$ и самим тим $n = m$, тј. n би био непаран). Отуда,

$$\sigma(m) \geq 1 + r + m = 1 + r + (2^{j+1} - 1)r = 1 + 2^{j+1}r = 1 + \sigma(m),$$

што је контрадикција. Значи, $r = 1$ и тако

$$\sigma(m) = 2^{j+1} \text{ i } m = 2^{j+1} - 1.$$

Како је $\sigma(m) = m + 1$, закључује се да је m прост број, а с обзиром и да је $n = 2^j m$, доказ је завршен.

Другим речима, постоји бијекција између парних савршених бројева и Мерсенових простих бројева. Иначе, није познато да ли постоји непаран савршен број [10].

3.3 Лукас-Лемеров тест

Лукас-Лемеров (Lucas-Lehmer) тест је најбољи тренутно познати алгоритам за проверу да ли је Мерсенов број сложен или прост. Француски математичар Е. Лукас (Lucas, 1842 - 1891) развио је потпуно нов начин провере да ли је број прост, без тражења фактора тог броја. Уместо тога, показао је да ако је $p \equiv 1 \pmod 4$ и $2^p - 1$ прост, тада и само тада $2^p - 1$ дели број, назван Лукас - Лемеров број, S_{p-2} дефинисан са $S_0 = 4, S_{n+1} = S_n^2 - 2$. Амерички математичар Д. Лемер (Lehmer, 1905 - 1991) дао је 1930. комплетан доказ претходног показујући да важи и за све непарне просте бројеве, не само за $p \equiv 1 \pmod 4$. Стога тест носи име оба ова математичара.

Теорема 3.2. (Лукас-Лемер) Ако је $p > 2$ прост број и Лукасов низ дефинисан са $S_0 = 4, S_{n+1} = S_n^2 - 2$, тада је $M_p = 2^p - 1$ прост ако и само ако $M_p | S_{p-2}$.

Доказ. Нека је $\omega = 2 + \sqrt{3}$ і $\overline{\omega} = 2 - \sqrt{3}$. Индукцијом се показује да је $S_i = \omega^{2^i} + \overline{\omega}^{2^i}$, за свако $i \geq 0$. Заиста,

$$S_0 = \omega^{2^0} + \overline{\omega}^{2^0} = 2 + \sqrt{3} + 2 - \sqrt{3} = 4$$

и

$$S_n = S_{n-1}^2 - 2 = (\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}})^2 - 2 = \omega^{2^n} + \overline{\omega}^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} - 2 = \omega^{2^n} + \overline{\omega}^{2^n},$$

јер је $\omega\overline{\omega} = 1$.

$\Leftarrow$: (Ако је $M_p | S_{p-2}$, онда је $2^p - 1$ прост број)

Претпоставка је да је $S_{p-2} \equiv 0 \pmod{M_p}$. То значи да је

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = kM_p$$

за неки цео број k, тј.

$$\omega^{2^{p-2}} = kM_p - \overline{\omega}^{2^{p-2}}.$$

Множењем целе једначине са $\omega^{2^{p-2}}$, добија се

$$(\omega^{2^{p-2}})^2 = kM_p\omega^{2^{p-2}} - (\omega\overline{\omega})^{2^{p-2}},$$

односно

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1 \ (3).$$

Претпоставимо да је M_p сложен број и q његов најмањи прост фактор. С обзиром да су Мерсенови бројеви непарни, онда је $q > 2$.

Нека је X скуп дефинисан са $X = \{a + b\sqrt{3} \mid a, b \in Z_q\}$. Како је $q > 2$, $\omega \in X$. Скуп X има q^2 елемената, у њему је дефинисана операција множења на следећи начин:

$$(a+b\sqrt{3})(c+d\sqrt{3}) = ((ac+3bd) \mod q) + ((ad+bc) \mod q)\sqrt{3}.$$

Производ два броја из X је у X, али овај скуп није мултипликативна група, јер нема сваки његов елемент мултипликативни инверз у X. Ако се посматрају само елементи из X који имају инверз у X, тај скуп је група у односу на множење и обележава се са X^*. X^* има највише q^2-1 елемената с обзиром да 0 нема инверз.

Како је $M_p \equiv 0 \pmod q$ и $\omega \in X$, онда је $kM_p\omega^{2^{p-2}} \equiv 0 \pmod q$ у X, па конгруенција (3) постаје

$$\omega^{2^{p-1}} \equiv -1 \pmod q.$$

Квадрирањем се добија $\omega^{2^p} \equiv 1 \pmod q$.

Из ове једнакости следи да је ω инвертибилан (инверз је ω^{2^p-1}), дакле спада у X^* и још, ред овог елемента дели 2^p (ред елемента a групе $(G,*,e)$ је најмањи природан број n такво да је $a^n = e$, уколико такво n постоји, а у супротном елемент a је бесконачног реда). Тачније, како је $\omega^{2^{p-1}} \neq 1$, ред не дели 2^{p-1}, што значи да је баш једнак 2^p. С обзиром да важи да је ред елемента мањи или једнак од реда групе, онда је $2^p \leq q^2-1 < q^2$, а како је q најмањи фактор сложеног броја M_p, онда је $q^2 \leq M_p = 2^p - 1$. Дакле, због контрадикције $2^p < 2^p - 1$, закључује се да је M_p прост број.

$\Rightarrow$: (Ако је 2^p-1 прост број, онда $M_p | S_{p-2}$)

У овом делу доказа користи се Ојлеров критеријум:

Ако је a узајамно прост са непарним простим бројем q, онда је

$$\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}} = \begin{cases} 1 \pmod q & \text{ако постоји цео број } x \text{ такав да је } a \equiv x^2 \pmod q \\ -1 \pmod q & \text{иначе} \end{cases}.$$

Разматрају се бројеви облика $a+b\sqrt{3} \pmod{M_p}$.
Применом биномног развоја на $(1+\sqrt{3})^{M_p} \pmod{M_p}$, с обзиром да је M_p прост фактор сваког биномног коефицијента осим првог и последњег, добија се

$$(1+\sqrt{3})^{M_p} \equiv 1 + (\sqrt{3})^{M_p} \equiv 1 + (\sqrt{3})3^{\frac{M_p-1}{2}} \pmod{M_p}.$$

На основу Ојлеровог критеријума $3^{\frac{M_p-1}{2}} \equiv \pm 1 \pmod{M_p}$. Како су M_p и 3 оба конгруентни $-1 \pmod 4$, закон квадратног реципроцитета каже да је или 3 квадратни остатак по модулу M_p или M_p квадратни остатак по модулу 3, али не и оба случаја. Али како је лако проверити да је $M_p \equiv 1 \pmod 3$, а тиме је M_p квадратни остатак по модулу 3, следи да 3 није квадратни остатак по модулу M_p. Дакле,

$$3^{\frac{M_p-1}{2}} \equiv -1 \pmod{M_p},$$

па је

$$(1+\sqrt{3})^{M_p} = 1 - \sqrt{3} \pmod{M_p}.$$

Множењем обе стране са $1+\sqrt{3}$, добија се

$$(1+\sqrt{3})^{M_p+1} \equiv -2 \pmod{M_p}.$$

Користећи једнакост $(1+\sqrt{3})^2 = 2\omega$, добија се

$$(2\omega)^{\frac{M_p+1}{2}} \equiv -2 \pmod{M_p}.$$

Лева страна једначине једнака је

$$2^{\frac{M_p+1}{2}}\omega^{\frac{M_p+1}{2}} = 2 \cdot 2^{\frac{M_p-1}{2}}\omega^{\frac{M_p+1}{2}}.$$

На основу закона реципроцитета, 2 је квадратни остатак простог броја конгруентног са $\pm 1 \pmod 8$ и пошто M_p јесте овог облика, следи $2^{\frac{M_p-1}{2}} \equiv 1 \pmod{M_p}$, што омогућава да претходна једначина добије облик

$$2 \cdot \omega^{\frac{M_p+1}{2}} = -2 \pmod{M_p}.$$

2 има инверз по модулу M_p, па се множењем једначине тим инверзом добија

$$\omega^{\frac{M_p+1}{2}} \equiv -1 \pmod{M_p}.$$

Како је $\omega^{\frac{M_p+1}{2}} = \omega^{2^{p-1}} = \omega^{2^{p-2}}\omega^{2^{p-2}} \equiv -1 \pmod{M_p}$, множењем обе стране са $\overline{\omega}^{2^{p-2}}$ и пребацивањем на леву страну добија се

$$\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} \equiv 0 \pmod{M_p}$$

тј. $S_{p-2} \equiv 0 \pmod{M_p}$. Лева страна је цео број, па је S_{p-2} дељиво са M_p.

4 Прости бројеви облика $h \cdot 2^n - 1$

Нека је $u_0 \geq 3$ дати цео број и нека је $u_\nu = u_{\nu-1}^2 - 2, \nu = 1, 2, 3, \ldots$. Бројеви u_ν чине *Лукасов низ* са почетним елементом u_0. Ако је h непарно и $h < 2^n$, онда се за многе вредности h и n знају неки неопходни и довољни услови да је $N = h \cdot 2^n - 1$ прост број. Ови критеријуми су следећег типа:

$$\text{За одговарајуће } u_0, \text{ број } N \text{ је прост ако и само ако } u_{n-2} \equiv 0 \pmod{N}. \quad (2)$$

У наредној табели [6] се налазе познати услови за које је (2) тачно:

h	u_0	$N = h \cdot 2^n - 1$
1	4	n непарно
1	3	$n \equiv 3 \pmod 4$
3	5778	$n \equiv 0, 3 \pmod 4$
$6a \pm 1$	$(2+\sqrt{3})^h + (2-\sqrt{3})^h$	$3 \not\mid N$; произвољно n

За поменуте критеријуме за просте бројеве облика $N = h \cdot 2^n - 1$ каже се да су Лукасовог типа. Њихова важност лежи у чињеници да су то најефикаснији критеријуми за просте бројеве до сада изучавани.

Захваљујући данашњим рачунарима проблем налажења Лукасовог критеријума за дату комбинацију h і n, с обзиром на то да се заснива на великом обиму израчунавања потребних за проверу разних вредности за u_0, постаје остварљив задатак. Даљи део рада показује како се то може урадити.

Лукасов критеријум заснива се на наредне две теореме [6]:

Теорема 4.1. (основна теорема 1) Нека су a, b и r су рационални цели бројеви, нека је D цео број који није дељив квадратом неког броја и α цео број у $K(\sqrt{D})$. Ако је N прост број, $\left(\frac{D}{N}\right) = -1, \quad \alpha = \frac{(a+b\sqrt{D})^2}{r}$ и $\left(\frac{r}{N}\right) \cdot \frac{a^2 - b^2 D}{r} = -1$, онда је $\alpha^{\frac{N+1}{2}}$ цели број и

$$\alpha^{\frac{N+1}{2}} \equiv -1 \pmod{N}.$$

Доказ.

Према Теореми 2.4:

$$\alpha^{\frac{N+1}{2}} = \frac{(a+b\sqrt{D})^{N+1}}{r^{\frac{N+1}{2}}}$$

$$\equiv \frac{(a+b\sqrt{D})(a-b\sqrt{D})}{r^{\frac{N-1}{2}}\cdot r} = \frac{a^2-b^2D}{r}\left(\frac{r}{N}\right)$$
$$\equiv -1 \pmod{N}.$$

Теорема 4.2. (основна теорема 2) Ако је $N = h\cdot 2^n - 1$, $h < 2^n$, $n \geq 2$, h је непаран, α цео број у $K(\sqrt{D})$ облика $\alpha = \dfrac{(a+b\sqrt{D})^2}{|a^2-b^2D|}$, $(\alpha, N) = 1$ у $K(\sqrt{D})$ и $\alpha^{\frac{N+1}{2}} \equiv -1 \pmod{N}$, онда је N прост број.

Доказ. Нека је p произвољан прост фактор броја N. Тада је очигледно

$$\alpha^{\frac{N+1}{2}} \equiv -1 \pmod{p}.$$

Према Теореми 2.5, $(N+1)/2 = h\cdot 2^{n-1} = k\cdot u$, где је k најмањи позитиван експонент такав да је $\alpha^k \equiv -1 \pmod{p}$, а u непаран цео број. Дакле, $k = 2^{n-1}\delta$, где $\delta | h$. Најмање позитивно e, такво да је $\alpha^e \equiv 1 \pmod{p}$, онда биће $e = 2k = 2^n\cdot\delta \geq 2^n$.

Сада, према Теореми 2.4:

$$\alpha^{\frac{p-1}{2}} = \frac{(a+b\sqrt{D})^{p-1}}{|a^2-b^2D|^{\frac{p-1}{2}}}$$
$$\equiv \left(\frac{|a^2-b^2D|}{p}\right) \pmod{p}, \quad \text{ako je } \left(\frac{D}{p}\right) = 1$$
$$\alpha^{\frac{p+1}{2}} = \frac{(a+b\sqrt{D})^{p+1}}{|a^2-b^2D|^{\frac{p+1}{2}}}$$
$$\equiv \frac{a^2-b^2D}{|a^2-b^2D|}\left(\frac{|a^2-b^2D|}{p}\right) \pmod{p}, \quad \text{ako je } \left(\frac{D}{p}\right) = -1.$$

Квадрирањем, добија се

$$\alpha^{p\pm 1} \equiv 1 \pmod{p}.$$

Даље, како је $e \geq 2^n$, онда је $p \pm 1 \geq 2^n$ за било који прост фактор p од N. Најмање могуће p ће онда бити $p = 2^n - 1$. Како N није квадрат неког броја (с обзиром да $N \equiv 3 \pmod{4}$, јер је $n \geq 2$), факторизација N даје

$$N = p\cdot q \geq p(p+2) \geq (2^n-1)(2^n+1) = 2^n\cdot 2^n - 1 > h\cdot 2^n - 1 = N,$$

што је контрадикција. Дакле, N је прост број.

Теореме 4.1 и 4.2 чине базу за неопходан и довољан Лукасов критеријум за просте бројеве облика $h\cdot 2^n - 1$, где је h непарно и $h < 2^n$, и $n \geq 2$.

Претпоставка је да су нађени бројеви D, a, b и $r = |a^2 - b^2D|$ такви да задовољавају услове Теореме 4.1. Потом, из

$$(\alpha^{h\cdot 2^s}+\alpha^{-h\cdot 2^s})^2=\alpha^{h\cdot 2^{s+1}}+\alpha^{-h\cdot 2^{s+1}}+2$$

налази се рекурентна једначина

$$u_{s+1}=u_s^2-2,\quad \text{где је } u_s=\alpha^{h\cdot 2^s}+\alpha^{-h\cdot 2^s}.$$

Даље,

$$u_{n-2}=\alpha^{h\cdot 2^{n-2}}+\alpha^{-h\cdot 2^{n-2}}=\alpha^{-h\cdot 2^{n-2}}(\alpha^{h\cdot 2^{n-1}}+1)\equiv 0 \pmod N$$

ће бити неопходан и довољан услов да је N прост број, јер је $\alpha^{-h\cdot 2^{n-2}}$ јединица у $K(\sqrt{D})$. ($N(\alpha)=\alpha\overline{\alpha}=\frac{(a^2-b^2D)^2}{|a^2-b^2D|^2}=1$, и тако су α и $\alpha^{-h\cdot 2^{n-2}}$ јединице у $K(\sqrt{D})$).

Дакле, како је $u_0=\alpha^h+\alpha^{-h}$, долази се до следеће теореме:

Теорема 4.3. (Лукасов критеријум за просте бројеве облика $h\cdot 2^n-1$) Претпроставка је да је $n\geq 2$, h непаран и $h<2^n$, $N=h\cdot 2^n-1$, $r=|a^2-b^2D|$ где D није дељив квадратом неког броја, $\alpha=\frac{(a+b\sqrt{D})^2}{r}$, $\left(\frac{D}{N}\right)=-1$ и $\left(\frac{r}{N}\right)\frac{a^2-b^2D}{r}=-1$. Нека је $u_\nu=u_{\nu-1}^2-2$, $u_0=\alpha^h+\alpha^{-h}$. Тада је неопходан и довољан услов да N буде прост број:

$$u_{n-2}\equiv 0 \pmod N.$$

Како је α јединица у $K(\sqrt{D})$, следи да је $\alpha=\epsilon^s$, где је $s=1,2,3,\ldots$ и ϵ је фундаментална једница у $K(\sqrt{D})$. Ако је ϵ облика $\epsilon=\dfrac{(a+b\sqrt{D})^2}{r}$, s мора бити непарно, јер парно s ће у том случају дати $\alpha^{\frac{N+1}{4}}\equiv -1 \pmod N$ у Теореми 4.1 и тако $u_{n-3}\equiv 0 \pmod N$. Најједноставнији избор за α је, према томе, $\alpha=\epsilon$, ако је $\epsilon=\dfrac{(a+b\sqrt{D})^2}{r}$, и $\alpha=\epsilon^2$, ако ϵ нема такву репрезентацију.

На основу претходног долази се до закључка да за дато h и n, једина ствар коју треба урадити је покушати са различитим вредностима за D и проверити да ли фундаментална јединица ϵ (некад и ϵ^2) у $K(\sqrt{D})$ задовољава услове Теореме 4.3. Када се пронађу D и α, може се израчунати u_0 (односно $u_0 \pmod N$ ако је N велико) коришћењем рекурзије за $v_\nu=\alpha^\nu+\alpha^{-\nu}$ [1]:

$$v_0=2,\quad v_1=\alpha^1+\alpha^{-1},\quad v_\nu=(\alpha^1+\alpha^{-1})v_{\nu-1}-v_{\nu-2}.$$

Када је проблем $\left(\frac{D}{N}\right)$ у питању, тражи се D за сваку комбинацију h и n у одређеној области. С обзиром да у општем случају за D није ништа познато, пробају се вредности D у растућем реду према величини бројева $v_1=\alpha^1+\alpha^{-1}$. На тај начин се добијају и најмање вредности за u_0. Међутим, прво је неопходно наћи везу између D и v_1. Како је $v_1=\alpha^1+\alpha^{-1}$, онда је $\alpha^2-v_1\alpha+1=0$ и D је део од (v_1^2-4) без квадратних фактора. Онда за разне D наћи репрезентацију од $\epsilon=\frac{(a+b\sqrt{D})^2}{r}$, ако постоји. Резултати су дати у Табели 1 за све $v_1\leq 100$ [6].

Табела 1.

v_1	D	a	b	r	$(a^2-b^2D)/r$
3	5	1	1	4	$-1,\epsilon^2$
4	3	1	1	2	-1
5	21	3	1	12	-1
6	2	1	1	1	$-1,\epsilon^2$
8	15	3	1	6	-1
9	77	7	1	28	-1
10	6	2	1	2	-1
11	13	3	1	4	$-1,\epsilon^2$
12	35	5	1	10	-1
13	165	11	1	44	-1
15	221	13	1	52	-1
16	7	3	1	2	$+1$
17	285	15	1	60	-1
19	357	17	1	68	-1
20	11	3	1	2	-1
21	437	19	1	76	-1
22	30	5	1	5	-1
24	143	11	1	22	-1
25	69	9	1	12	$+1$
26	42	6	1	6	-1
27	29	5	1	4	$-1,\epsilon^2$
28	195	13	1	26	-1
29	93	9	1	12	-1
30	14	4	1	2	$+1$
31	957	29	1	116	-1
32	255	15	1	30	-1
33	1085	31	1	124	-1
35	1221	33	1	132	-1
36	323	17	1	34	-1
37	1365	35	1	140	-1
38	10	3	1	1	$-1,\epsilon^2$
39	1517	37	1	148	-1
40	399	19	1	38	-1
41	1677	39	1	156	-1
42	110	10	1	10	-1
43	205	15	1	20	$+1$
44	483	21	1	42	-1
45	2021	43	1	172	-1
46	33	6	1	3	$+1$
48	23	5	1	2	$+1$
49	2397	47	1	188	-1
50	39	6	1	3	-1
51	53	7	1	4	$-1,\epsilon^2$
53	2805	51	1	204	-1

v_1	D	a	b	r	$(a^2-b^2D)/r$
54	182	13	1	13	-1
55	3021	53	1	212	-1
56	87	9	1	6	-1
57	3245	55	1	220	-1
58	210	14	1	14	-1
59	3477	57	1	228	-1
60	899	29	1	58	-1
61	413	21	1	28	$+1$
63	3965	61	1	244	-1
64	1023	31	1	62	-1
65	469	21	1	28	-1
66	17	4	1	1	$-1,\epsilon^2$
67	4485	65	1	260	-1
68	1155	33	1	66	-1
69	4757	67	1	268	-1
70	34	6	1	2	$+1$
71	5037	69	1	276	-1
72	1295	35	1	70	-1
73	213	15	1	12	$+1$
74	38	6	1	2	-1
75	5621	73	1	292	-1
76	1443	37	1	74	-1
77	237	15	1	12	-1
78	95	10	1	5	$+1$
80	1599	39	1	78	-1
81	6557	79	1	316	-1
82	105	10	1	5	-1
83	85	9	1	4	$-1,\epsilon^2$
84	1763	41	1	82	-1
85	7221	83	1	332	-1
86	462	21	1	21	-1
87	7565	85	1	340	-1
88	215	15	1	10	$+1$
89	7917	87	1	348	-1
90	506	22	1	22	-1
91	8277	89	1	356	-1
92	235	15	1	10	-1
93	8645	91	1	364	-1
94	138	12	1	6	$+1$
95	9021	93	1	372	-1
96	47	7	1	2	$+1$
97	1045	33	1	44	$+1$
99	9797	97	1	388	-1
100	51	7	1	2	-1

5 Имплементација, детаљи програма и резултати

Даљи део рада описује имплементацију програма за генерализован Лукас-Лемеров тест, тј. проверу простости за бројеве облика $h \cdot 2^n - 1$. За дату комбинацију h и n потребно је наћи одговарајуће u_0, тачније одговарајуће D користећи табелу 1, које ће задовољити услове теореме 4.3. Фокус је на случај када 3 дели h, јер као што је раније речено $u_0 = (2+\sqrt{3})^h + (2-\sqrt{3})^h$ одговара за све друге непарне вредности h осим ако 3 дели N.

Да би се избегло непотребно тестирање, приметити да D не може делити $2h$, јер је у том случају $(D/N) = +1$. Такође, у табели 1 за $D = 5, 2, 13, 29, 10, 53, 17$ и 85, ϵ нема репрезентацију облика $\epsilon = \dfrac{(a+b\sqrt{D})^2}{r}$, већ се користи ϵ^2. Ови случајеви су посебно интересантни, јер како је $r = 1$ или $r = 4$, односно r је савршен квадрат, онда је за свако N, увек $(r/N) = +1$. Даље, у овим случајевима је $(a^2 - b^2D)/r = -1$, па је $(r/N)\dfrac{a^2-b^2D}{r} = -1$, услов из теореме 4.3. задовољен за свако N.

Такође је од значаја прелиминарна претрага малих простих фактора од N. Ако су почетни услови теореме 4.3 задовољени, за оне N без малог простог фактора, даље у програму следи провера да ли је број прост, односно да ли је $u_{n-2} \equiv 0 \pmod N$.

Програм је писан у *Java* програмском језику. Користи класу *LargeInteger* [11] која омогућава рад са произвољно великим бројевима и користи се углавном у научне сврхе. Побољшања у односу на класу *java.math.BigInteger* су оптимизација за 64-битну архитектуру, прилагођеност раду у реалном времену због бољих перформанси и предвиђања и унапређени алгоритми.

За дато h и n најпре се проверава дељивост N малим простим бројевима (простим бројевима мањим од 256). Уколико је N без малог простог фактора, пролазећи редом кроз табелу 1. бира се одговарајуће D које ће задовољити услове теореме 4.3 помоћу следећих метода:

- провера услова $\left(\frac{D}{N}\right) = -1$
  boolean checkFirstCondition(int current_h, int current_table1Index, LargeInteger N)
- ако је претходни услов задовољен, следи провера услова $\left(\frac{r}{N}\right)\frac{a^2-b^2D}{r} = -1$
  boolean checkSecondCondition(int current_table1Index, LargeInteger N)
- ако су оба услова теореме 4.3 задовољена, следи провера да ли је број прост рачунањем $u_0 = \alpha^h + \alpha^{-h} = v_h = v_1 v_{h-1} - v_{h-2}$
  LargeInteger calculate_u0(int current_h, int current_table1Index, LargeInteger N)
  и затим провером услова $u_{n-2} \equiv 0 \pmod N$ коришћењем $u_s = u_{s-1}^2 - 2$.

У табели 2 су приказани резултати програма, тј. прости бројеви за $A \leq 45$ и $n \leq 1500$:

Табела 2.

Прости бројеви облика $3A \cdot 2^n - 1$ *за* $A \leq 45, n \leq 1500$

$3A$	n
3	1, 2, 3, 4, 6, 7, 11, 18, 34, 38, 43, 55, 64, 76, 94, 103, 143, 206, 216, 306, 324, 391, 458, 470, 827, 1274
9	1, 3, 7, 13, 15, 21, 43, 63, 99, 109, 159, 211, 309, 343, 415, 469, 781, 871, 939
15	1, 2, 4, 5, 10, 14, 17, 31, 41, 73, 80, 82, 116, 125, 145, 157, 172, 202, 224, 266, 289, 293, 463, 1004, 1246
21	1, 2, 3, 7, 10, 13, 18, 27, 37, 51, 74, 157, 271, 458, 530, 891
27	1, 2, 4, 5, 8, 10, 14, 28, 37, 38, 70, 121, 122, 160, 170, 253, 329, 362, 454, 485, 500, 574, 892, 962, 1213
33	2, 3, 6, 8, 10, 22, 35, 42, 43, 46, 56, 91, 102, 106, 142, 190, 208, 266, 330, 360, 382, 462, 503, 815, 1038
39	3, 24, 105, 153, 188, 605, 795, 813, 839
45	1, 2, 3, 4, 5, 6, 8, 9, 14, 15, 16, 22, 28, 29, 36, 37, 54, 59, 85, 93, 117, 119, 161, 189, 193, 256, 308, 322, 327, 411, 466, 577, 591, 902, 928, 946, 1162, 1428
51	1, 9, 10, 19, 22, 57, 69, 97, 141, 169, 171, 195, 238, 735, 885, 1287, 1365
57	1, 2, 4, 5, 8, 10, 20, 22, 25, 26, 32, 44, 62, 77, 158, 317, 500, 713
63	2, 3, 8, 11, 14, 16, 28, 32, 39, 66, 68, 91, 98, 116, 126, 164, 191, 298, 323, 443, 714, 758, 759, 1059, 1168
69	1, 4, 5, 7, 9, 11, 13, 17, 19, 23, 29, 37, 49, 61, 79, 99, 121, 133, 141, 164, 173, 181, 185, 193, 233, 299, 313, 351, 377, 540, 569, 909, 1057, 1081, 1189
75	1, 3, 5, 6, 18, 19, 20, 22, 28, 29, 39, 43, 49, 75, 85, 92, 111, 126, 136, 159, 162, 237, 349, 381, 767, 969, 1247
81	3, 5, 11, 17, 21, 27, 81, 101, 107, 327, 383, 387, 941
87	1, 2, 8, 9, 10, 12, 22, 29, 32, 50, 57, 69, 81, 122, 138, 200, 296, 514, 656, 682, 778, 881, 1422, 1494
93	3, 4, 7, 10, 15, 18, 19, 24, 27, 39, 60, 84, 111, 171, 192, 222, 639, 954
99	1, 4, 5, 7, 8, 11, 19, 25, 28, 35, 65, 79, 212, 271, 361, 461, 1237, 1297
105	2, 3, 5, 6, 8, 9, 25, 32, 65, 113, 119, 155, 177, 299, 335, 426, 462, 617, 896, 1377
111	2, 3, 6, 7, 21, 22, 23, 26, 29, 31, 58, 59, 67, 78, 83, 146, 159, 162, 165, 183, 262, 511, 718, 815, 1181, 1255, 1422
117	1, 2, 4, 6, 12, 16, 18, 20, 22, 24, 37, 40, 48, 49, 57, 62, 154, 172, 184, 236, 265, 374, 409, 445, 478, 664, 718, 928, 1186, 1369
123	2, 3, 11, 15, 23, 24, 27, 35, 71, 84, 108, 122, 123, 138, 236, 242, 290, 392, 500, 611, 747, 771, 1106, 1490
129	1, 3, 4, 5, 8, 9, 12, 16, 28, 51, 56, 59, 72, 73, 88, 93, 105, 148, 165, 292, 368, 445, 635, 771, 773, 940, 1173
135	1, 9, 10, 13, 16, 21, 24, 34, 54, 153, 177, 184, 226, 238, 286, 334, 586, 618, 870

Део табеле 2 за $A \leq 35$ и $n \leq 1000$ се слаже са резултатима из [6].

Java пројекат *masterRadProgram* се састоји из три директоријума:

/bin - празан директоријум у коме ће бити смештен преведен *.class* фајл
/src - садржи изворни код, фајл *PrimalityTest.java*
/lib - садржи *jscience.jar* библиотеку

За превођење изворног кода у бајтни код користи се *javac* компајлер који долази уз *JDK*. Превођење из командне линије на *Windows* оперативном систему врши се командом (из кореног директоријума програма):

javac -d bin -cp lib/jscience.jar src/masterRadProgram/PrimalityTest.java

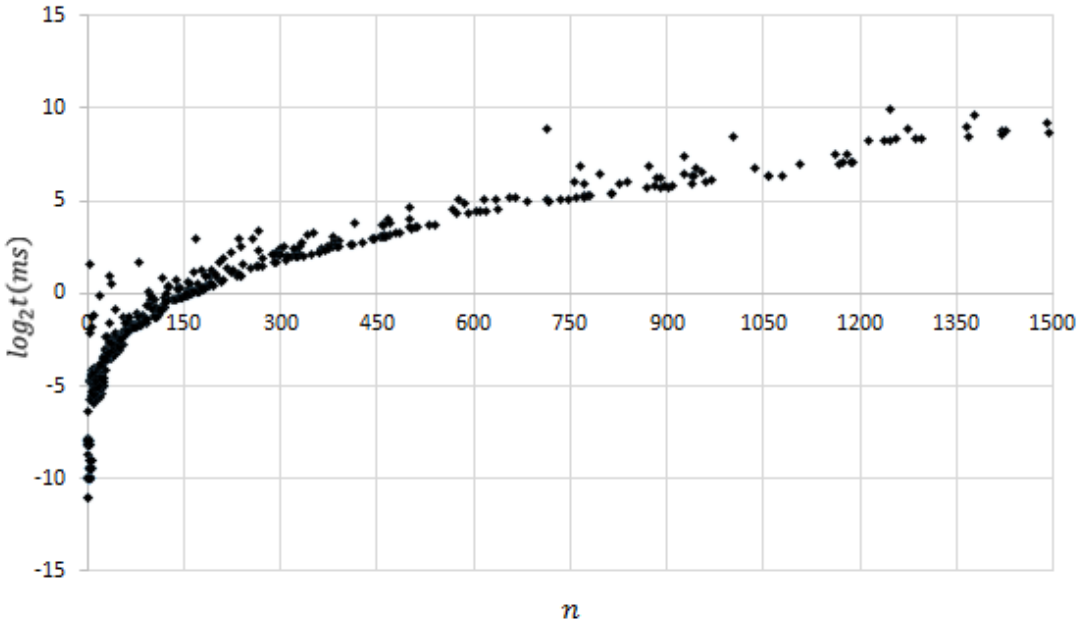
Покретање програма из командне линије врши се командом:

java -cp bin;lib/jscience.jar masterRadProgram/PrimalityTest

Време извршавања програма је $8h\ 49min\ 4sek$ на рачунару са следећим карактеристикама:

CPU Intel Core i7-3612QM 2.10 GHz 64-bit 4 cores
RAM 8GB
OS Windows 7 SP 1 64-bit
JDK version 1.7.0_51

Следећи график приказује време извршавања теста у зависности од n за свако N из табеле 2:



6 Закључак

У овом раду изучавани су бројеви облика $h \cdot 2^n - 1$. Објашњене су најефикасније детерминистичке методе за проверу да ли је број оваквог специјалног облика прост. Захваљујући Лукас-Лемеровом тесту (тесту специјализованом за Мерсенове бројеве, тј. бројеве облика $2^n - 1$) откривени су данас највећи познати прости бројеви. Неопходни и довољни услови да је број облика $h \cdot 2^n - 1$ прост, зависе од комбинација вредности h и n. За многе комбинације h и n познати су једноставни услови, осим када 3 дели h. Проблем налажења критеријума заснива се на великом броју израчунавања и коришћењем рачунара постаје остварљив задатак.

У раду је дат опис имплементације теста који проверава да ли је број облика $N = 3A \cdot 2^n - 1$ прост. За проналажење одговарајуће вредности за D које ће задовољити услове теореме 4.3, програм користи табелу 1 [6]. Међутим, у општем случају D не мора бити пронађено у табели. Како би се проширио скуп могућих вредности за D, од користи је имплементација рачунања фундаменталне јединице [8] квадратног поља за дато D. Описани програм у раду се извршава секвенцијално. Унапређење алгоритма које знатно убрзава програм могуће је паралелним тестирањем за различите h или паралелном провером различитих бројева из табеле 1 за проналажење одговарајућег D.

7 Литература

[1] H. Riesel, *Prime numbers and computer methods for factrorization*, Boston, Birkhäuser, 2011.

[2] R. A. Mollin, *Mathematics of computation*, Providence, American Mathematical Society, 1987.

[3] Great Internet Mersenne Prime Search, *http://www.mersenne.org/*

[4] Mersenne Primes, *http://primes.utm.edu/mersenne/index.html*

[5] Lucas Lehmer test, *http://www.mersennewiki.org/index.php/Lucas-Lehmer_ Test*

[6] H. Riesel, *Lucasian criteria for the primality of* $h \cdot 2^n - 1$, Mathematics of Computation 23 (108), 1969, стр. 869-875

[7] D. H. Lehmer, *An Extended Theory of Lucas' Functions*, Annals of Mathematics, 1930.

[8] E. W. Weisstein, *CRC Concise Encyclopedia of Mathematics*, CRC Press, 2002.

[9] T. Koshy, *Elementary Number Theory with Applications*, Academic Press, 2007.

[10] R. Guy, *Unsolved Problems in Number Theory*, Springer, 2004.

[11] JScience, *http://jscience.org/api/org/jscience/mathematics/number/LargeInteger.html*