Katedra Informatiky
Fakulta Matematiky, Fyziky a Informatiky
Univerzita Komenského, Bratislava

Testovanie prvočíselnosti

Ondrej Pašuth

bakalárska práca

9.2.1 Informatika

Vedúci: RNDr. Martin Sleziak, PhD.

Bratislava, 2009

Čestne prehlasujem, že som túto bakalársku prácu vypracoval samostatne s použitím citovaných zdrojov a literatúry.

Bratislava, dňa 11. 6. 2009 Ondrej Pašuth

Poďakovanie

Chcem na tomto mieste vyjadriť úprimnú vďaku vedúcemu mojej bakalárskej práce RNDr. Martinovi Sleziakovi, PhD. za jeho ochotu, námahu, za jeho čas a trpezlivosť, s akou mi vysvetľoval veci, ktoré sa týkali mojej bakalárskej práce. Tiež mu chcem poďakovať za výber zaujímavej témy, za zabezpečenie študijných materiálov a za to, že si na mňa vždy našiel čas. Ďalej by som sa chcel poďakovať svojim rodičom a súrodencom, bez ktorých by som sa určite na Matfyz nikdy nedostal.

Abstrakt

Autor: Ondrej Pašuth
Názov bakalárskej práce: Testovanie prvočíselnosti
Škola: Univerzita Komenského v Bratislave
Fakulta: Fakulta matematiky, fyziky a informatiky
Katedra: Katedra informatiky
Vedúci bakalárskej práce: RNDr. Martin Sleziak, PhD.
Bratislava, jún 2009

Cieľom tejto bakalárky je rozobrať rôzne prvočíselné testy a dokázať ich správnosť. Množstvo z nich je v konečnej podobe jednoduchým algoritmom, ku ktorého zostrojeniu však vedie dlhá cesta v podobe netriviálneho matematického dôkazu. Zameral som sa na niektoré testy, pričom tieto testy majú rozličné vlastnosti a aj ich podstata je rôzna. V práci sme tiež popísali rôzne druhy pseudoprvočísel, pre ktoré sú jednotlivé testy určené. V tejto bakalárskej práci som sa venoval pravdepodobnostným testom (Rabin-Millerov test, pravdepodobnostný pseudoprvočíselný test), ďalej som rozobral testy pre rôzne druhy čísel špeciálneho tvaru (Pepinov test a Lucas-Lehmerov test), ukázal som však aj možnosť postupného zlepšovania testov (test pre Lucasove pseudoprvočísla a Frobeniove pseudoprvočísla). V práci je množstvo rôznych viet a tvrdení, ktoré sú základom pre jednotlivé testy, vysvetlených a dokázaných tak, aby mohol byť tento text nápomocný aj pre samoštudujúcich nadšencov, ktorých zaujala táto vzrušujúca oblasť matematiky.

KĽÚČOVÉ SLOVÁ: prvočísla, pseudoprvočísla, testy na overovanie pseudoprvočísel, Lucasova postupnosť, Malá Fermatova veta, zvyškové triedy, pravdepodobnostný test, Frobeniov automorfizmus

Obsah

Úvod

Prvočísla, teda čísla, ktoré sú deliteľné iba jednotkou a sebou, očarovali ľudí už od matematického praveku. Už starovekí Gréci sa snažili zistiť o nich čo najviac informácií a študovali prvočíselné vlastnosti. Už okolo roku 300 pred Kristom dokázal Euklid, že takýchto tajomných čísel je nekonečne veľa. Prvočísla boli, sú a vždy aj budú fascinujúcim objektom záujmu mnohých významných matematikov. Stoja v strede najrozličnejších matematických disciplín a napriek tomu, že im boli venovaná nekončiaca sa pozornosť, ešte stále je množstvo otvorených otázok súvisiacich s prvočíslami. Samotné prvočísla majú však aj veľké praktické využitie, v súčasnom technologickom svete sú práve oni tým pravým kľúčom ku kryptografii, kryptológii a kódovaniu.

Časom sa však ľudia začali sami seba pýtať, aké najväčšie prvočíslo sú schopní vyprodukovať. Známa je iniciatíva istej americkej spoločnosti, ktorá za objavenie doteraz najdlhšieho objaveného prvočísla ponúka odmenu 100 tisíc dolárov. Ľudia v snahe rozhodnúť, či je nejaké číslo aj prvočíslom, začali vymýšľať rôzne testy, ktorými priamo nedokázali prvočíselnosť daného čísla, vďaka takýmto testom sa však veľakrát dokázalo práve to, že dané číslo prvočíslom nie je. Pri takomto vymýšľaní sa zistilo a dokázalo aj mnoho iných vecí, ktoré pomohli k rozvoju ďalších a ďalších oblastí matematiky.

Práve tejto oblasti sa týka moja bakalárska práca. Rozoberá a dokazuje rôzne tzv. prvočíselné testy, ktoré dávnejšie alebo nie až tak dávno vymysleli rôzni slávni matematici a informatici. Testy vychádzajú z toho, že ak je dané číslo prvočíslom, platí pre neho nejaká dokázateľná vlastnosť. Teda ak nejaké číslo túto vlastnosť nemá, môžeme o ňom s určitosťou tvrdiť, že prvočíslom nie je. Danú vlastnosť však môžu mať aj zložené čísla, preto sa tieto testy snažia nájsť čo najoptimálnejšiu vlastnosť pre prvočísla. Toto je základom pre tzv. testovanie prvočíselnosti. Naproti tomu stojí ďalšia rodina testov, tzv. pravdepodobnostné testy. Tie tiež povedia o danom čísle, či je prvočíslom alebo zloženým číslom, mýlia sa však s istou pravdepodobnosťou, ktorá je však menšia ako $1/2$. Preto pri ich dostatočnom opakovaní môžeme takmer s istotou tvrdiť, že ak dané číslo prešlo cez všetky testy, jedná sa o prvočíslo.

V jednotlivých kapitolách rozoberám rôzne testy, ktoré vychádzajú z rôznych matematických viet a rôznych vlastností prvočísel. Niektoré z týchto testov dopomohli objaviť obrovské prvočísla, iné nemali veľkú životnosť. Samotné testy nie sú väčšinou komplikované, za nimi však stojí množstvo matematických viet a tvrdení. Práve o takéto rozbitie a rozanalyzovanie týchto testov som sa pokúšal v tejto práci. Základným prameňom bola pre mňa kniha od autorov Crandalla a Pomeranca Prime Numbers, a Computational Perspective. Túto náročným štýlom písanú knihu sme využili ako zdroj mnohých poznatkov, ktoré sme sa snažili podať zrozumiteľným štýlom.

Kapitola 1

Základné pojmy a definície

1.1 Základné definície využívané v ďalšej časti

Definícia 1.1.1 (Lucasove postupnosti)**.** Majme ľubovoľné $a, b \in \mathbb{Z}$. Lucasove postupnosti U_j a V_j sú postupnosti rekurentne dané nasledovne:

$$\begin{aligned} U_j(a,b) &= aU_{j-1}(a,b) - bU_{j-2}(a,b) \\ V_j(a,b) &= aV_{j-1}(a,b) - bV_{j-2}(a,b), \end{aligned} \tag{1.1}$$

kde $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = a$.

Z predpisu je jasné, že obe postupnosti závisia od premenných a a b. V ďalšej časti preto nebudeme vypisovať $U_j(a,b)$, resp. $V_j(a,b)$, ale iba skrátenú formu U_j, reps. V_j.

Definícia 1.1.2 (Kvadratické zvyšky)**.** Nech $n \nmid q$. Potom sa číslo q nazýva *kvadratický zvyšok* $\pmod n$, ak existuje také $x \in \mathbb{Z}$, že $x^2 \equiv q \pmod n$. V opačnom prípade hovoríme, že q je *kvadratický nezvyšok* $\pmod n$.

My budeme používať aj stručnejší zápis: qRn znamená, že q je kvadratický zvyšok modulo n a $q\overline{R}n$ znamená, že q je kvadratický nezvyšok modulo n.

Definícia 1.1.3 (Legendrov symbol)**.** Ak p je prvočíslo a a je celé číslo, tak *Legendrov symbol* $\left(\frac{a}{p}\right)$ definujeme nasledovne:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ak } aRp, \\ -1 & \text{ak } a\overline{R}p, \\ 0 & \text{ak } p \mid a. \end{cases}$$

Definícia 1.1.4 (Eulerova funkcia)**.** Nech $m \in \mathbb{N}$. Ako $\varphi(m)$ označíme počet čísel z množiny {1,2,. . . ,m } nesúdeliteľných s m. Funkciu φ nazývame *Eulerova funkcia.*[1]

[1] Leonhard Paul Euler (15. apríla 1707 - 18. septembra 1783) bol švajčiarsky matematik a fyzik, ktorý strávil väčšinu svojho života v Rusku a Nemecku. Euler bol významným vedcom svojej doby, ktorý sa zaoberal rôznymi oblasťami matematiky a fyziky, napr. teóriou grafov. Zaviedol množstvo matematických znakov, označení pre rôzne funkcie a veľa pojmov zo súčasnej matematickej terminológie sa tiež objavilo práve v jeho dielach. Je známa jeho práca v oblastiach mechaniky, dynamiky, optiky a astronómie. Tzv. Eulerova konštanta nesie práve jeho meno.

Definícia 1.1.5. Funkcia σ v poli F_{p^2}, ktorá každému prvku z poľa priradí jeho p-tu mocninu, sa nazýva Frobeniov[2] automorfizmus.

1.2 Niektoré vety využívané v ďalších kapitolách

1.2.1 Teória čísel

Veta 1.2.1 (Gaussov zákon kvadratickej reciprocity, [B]). *Ak p a q sú rôzne nepárne prvočísla, tak*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}. \tag{1.2}$$

Predchádzajúca veta je dosť dôležitá v teórii čísel. Ako zaujímavosť môžeme spomenúť, že je známych cez 200 dôkazov tejto vety. [3]

Lema 1.2.1. *Nech p je prvočíslo a nech $1 \leq i \leq p$. Potom $p \mid \binom{p}{i}$, čiže $\binom{p}{i} \equiv 0 \pmod{p}$.*

Dôkaz. Kombinatorický význam matematického zápisu $\binom{p}{i}$ hovorí, že ide o počet i-prvkových podmnožín z n-prvkovej množiny. Z toho jasne vidno, že $\binom{p}{i}$ je celé číslo. Jeho presné vyjadrenie (či už podľa definície alebo z kombinatorického významu) je

$$\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{1.2.\dots.i}.$$

Už z rozpísaného čísla $\binom{p}{i}$ vidno, že čitateľ obsahuje vo svojom kanonickom rozklade na prvočísla aj p. Naopak, menovateľ p neobsahuje, pretože v menovateli sú všetky čísla menšie ako prvočíslo p a nijakým súčinom dvoch čísel nedostaneme prvočíslo (samozrejme okrem súčinu samotného prvočísla s jednotkou). Z toho vyplýva, že dané celé číslo $\binom{p}{i}$ je deliteľné prvočíslom p. □

Veta 1.2.2. *Nech p je prvočíslo. Potom*

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

Dôkaz. Pre ľubovoľné prvočíslo môžeme písať, že $(-a)^p \equiv -a^p \pmod{p}$, pretože $(-a)^p = (-1)^p(a)^p$ a ak je p nepárne, tak sa výraz rovná $-a^p$. Ak je naopak párne (čiže 2), potom $-x \equiv x \pmod{2}$. Z tohto vyplýva, že nám stačí overiť danú kongruenciu pre $a \geq 0$. Kongruenciu dokážeme matematickou indukciou. Uvedená kongruencia zjavne platí pre $a = 0$ a $a = 1$ (báza indukcie). Nech pre a platí, že $a^p \equiv a \pmod{p}$. My dokážeme uvedenú kongruenciu aj pre $a+1$, čím na základe princípu matematickej indukcie vetu dokážeme. Z binomickej vety platí, že $(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^i$. Využitím lemy 1.2.1 dostávame nasledovné:

$$(a+1)^p \equiv a^p + 1 \overset{ip}{\equiv} a + 1 \pmod{p}.$$

[2] Ferdinand Georg Frobenius (26. októbra 1849 - 3. augusta 1917) bol nemeckým matematikom, známy najmä svojím prínosom v oblasti diferenciálnych rovníc a teórie grúp. Narodil sa na predmestí Berlína, vyštudoval Berlínsku univerzitu. Niekoľko rokov vyučoval v rodnom Berlíne, potom však odišiel do Švajčiarska, kde bol učiteľom na Polytechnickej univerzite. V roku 1893 sa vrátil do Berlína a stal sa členom Pruskej akadémie vied.

[3] Presne 224 rôznych dôkazov od rozličných matematikov, ktorí túto vetu dokazovali už od roku 1788, je popísaných na stránke www.rzuser.uni-heidelberg.de/ hb3/fchrono.html. Dosť veľa rôznych dôkazov je tiež spísaných v [L].

□

Nasledujúca veta sa dá chápať ako dôsledok predchádzajúcej vety, no je aj mnoho iných spôsobov, ako ju dokázať.

Veta 1.2.3 (Malá Fermatova veta). *Nech p je prvočíslo a nech a je celé číslo také, že $p \nmid a$. Potom*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1.3}$$

Veta 1.2.4 (Eulerova veta). *Nech $a, n \in \mathbb{N}$ sú také čísla, že $(a, n) = 1$. Potom*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Symbol $\varphi(n)$ v tejto vete je Eulerova funkcia zadefinovaná v definícii 1.1.4. Dôkaz tejto vety tu nebudem uvádzať, nakoľko jej dôkaz možno nájsť v [S2] a samotný dôkaz ani nie je cieľom tejto práce.

Veta 1.2.5 (Eulerovo kritérium). *Nech $p > 2$ je prvočíslo. Potom pre všetky n platí*

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}. \tag{1.4}$$

Dôkaz tejto vety sa nachádza v knihe [S2, Veta 4.2.3].

Veta 1.2.6. *Nech $p > 2$ je prvočíslo. Potom*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Teda 2 je kvadratický zvyšok pre prvočísla tvaru $8k \pm 1$ a kvadratický nezvyšok pre prvočísla tvaru $8k \pm 3$.[4]

Veta 1.2.7 (Čínska veta o zvyškoch). *Nech $m_1, m_2, \ldots, m_n$ sú po dvoch nesúdeliteľné čísla. Nech $b_1, b_2, \ldots, b_n \in \mathbb{Z}$. Potom systém kongruencií*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\ldots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

má práve jedno riešenie modulo $m_1 m_2 \ldots m_n$ (čiže existuje práve jedno $x \in \{0, 1, \ldots, m_1 \ldots m_n - 1\}$ vyhovujúce všetkým uvedeným kongruenciám).[5]

Veta 1.2.8 (Bézoutova identita). *Nech $a, b \in \mathbb{Z}$, aspoň jedno z nich je nenulové. Nech $d = NSD\,(a, b)$. Potom existujú čísla $u, v \in \mathbb{Z}$ také, že $d = au + bv$. Navyše d je najmenšie prirodzené číslo, ktoré sa dá zapísať takýmto spôsobom.*[6]

Veta 1.2.9. *Kongruencia*

$$ax \equiv b \pmod{n} \tag{1.5}$$

má riešenie práve vtedy, keď $d \mid b$, kde $d = NSD(a, n)$.

Navyše, ak kongruencia (1.5) má riešenie, tak počet (navzájom nekongruentných) riešení je d.

[4] Dôkaz tejto vety nájdete v [S2, Tvrdenie 4.2.8].

[5] Dôkaz tejto vety sa dá nájsť napr. v [S2, Veta 3.1.18].

[6] Dôkaz tejto vety nie je veľmi zložitý, ale uvádzať ho tu nebudeme. Čitateľ si ho v prípade záujmu môže pozrieť v [S2, Veta 2.1.7].

Pekný dôkaz tejto vety sa uvádza v [S2, Veta 3.1.16].

Veta 1.2.10. *Nech $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ je kanonický rozklad čísla n. Potom*

$$\varphi(n) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

Jeden zo spôsobov, ako dokázať danú vetu, je použiť princíp zapojenia a vypojenia.

Tvrdenie 1.2.1. *Pre Legendrove symboly 1.1.3 platia nasledujúce vzťahy*[7]*:*

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \ \left(\frac{a^2}{n}\right) = 1.$$

1.2.2 Algebra a teória polí

Lema 1.2.2. *Nech F je pole a F' je jeho nadpole. Nech $f(x) \in F[x]$. Potom $c \in F'$ je koreňom $f(x)$ práve vtedy, keď $x - c \mid f(x)$ v $F'[x]$, t.j. existuje polynóm $g(x)$ taký, že $f(x) = g(x)(x - c)$.*[8]

Lema 1.2.3. *Nech F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3. Polynóm $f(x)$ je ireducibilný práve vtedy, keď $f(x)$ nemá koreň v F.*

Dôkaz. Ak by sme chceli rozložiť polynóm stupňa 2 alebo 3 rozložiť na súčin polynómov nižších stupňov, určite sa tam vyskytne aj minimálne jeden polynóm stupňa 1. Ako však vidno podľa lemy 1.2.2, takýto polynóm stupňa 1 by musel obsahovať koreň. Ten však podľa predpokladov lemy nemáme, teda polynóm $f(x)$ musí byť ireducibilný. □

Veta 1.2.11. *Ak $f : G \to H$ je surjektívny homomorfizmus okruhov, tak okruh H je izomorfný s faktorovým okruhom $G/\operatorname{Ker} f$.*

Túto vetu uvádzame bez dôkazu, nakoľko jej dôkaz je v [S1] dôsledne popísaný a pri jej dokazovaní by sme museli vysloviť a dokázať ďalšie potrebné vety a lemy, čo nie je úlohou tejto práce.

Veta 1.2.12. *Redukované zvyškové triedy $\mathbb{Z}_n^*$, t.j. pre dané n všetky zvyškové triedy, ktoré sú s n nesúdeliteľné*[9]*, tvoria vzhľadom na násobenie so zvyškom $\odot$ grupu.*

Dôkaz. Overme najprv, či je v $\mathbb{Z}_n^*$ operácia $\odot$ binárnou operáciou. Ak máme k, l také, že $\mathrm{NSD}(k, n) = 1$ a $\mathrm{NSD}\ (l, n) = 1$, potom $\mathrm{NSD}(k.l, n) = 1 \Rightarrow \mathrm{NSD}(k \odot l, n) = 1$. Z tohto vyplýva, že $\odot$ je v $\mathbb{Z}_n^*$ naozaj binárnou operáciou.

Asociatívnosť operácie $\odot$ v $\mathbb{Z}_n^*$ platí, pretože $\odot$ je asociatívna operácia aj napr. v $\mathbb{Z}$.

Neutrálny prvok vzhľadom na násobenie, a teda aj na násobenie so zvyškom $\odot$ je číslo 1. Keďže $\mathrm{NSD}(1, n) = 1$, patrí číslo 1 do $\mathbb{Z}_n^*$.

Poslednou podmienkou, ktorú musíme overiť, aby sme mohli tvrdiť, že $(\mathbb{Z}_n^*, \odot)$ je grupa, je ukázať existenciu inverzného prvku pre ľubovoľný prvok $\in \mathbb{Z}_n^*$ vzhľadom na násobenie so zvyškom $\odot$. Na základe Bézoutovej identity 1.2.8 existujú

[7] [KLS, Veta 2.30]

[8] Dôkaz tejto vety a tiež ďalšie veci z teórie polí sú v skriptách [S1]

[9] Môžeme to zapísať takto: $\mathbb{Z}_n^* = \{1 \leq m \leq n; \mathrm{NSD}\ (m, n) = 1\}$

také celé čísla u, v, že pre nesúdeliteľné m, n platí $u.m + v.n = 1$. To môžeme napísať aj takto $u \odot m = 1$. Také u musí navyše patriť do $\mathbb{Z}_n^*$, pretože v opačnom prípade by sa $\mathrm{NSD}(u \odot m, n)$ nemohlo rovnať 1. To preto, lebo nech $u \notin \mathbb{Z}_n^* \Rightarrow \mathrm{NSD}(u \odot m, n) = z > 1$. Predchádzajúca implikácia je zrejmá po rozpísaní danej situácie: $u \odot m = m.u - t.n$ a nech $z = \mathrm{NSD}\ (u, n)$. Potom pre nejaké o, p platí $u \odot m = m.o.z - t.p.z = z(m.o - t.p) \Rightarrow \mathrm{NSD}(u \odot m, n) =$ minimálne z. □

Veta 1.2.13. *Pre ľubovoľné nepárne prvočíslo p a ľubovoľné prirodzené číslo j platí, že grupa $\mathbb{Z}_{p^j}$ redukovaných zvyškových tried* $(\mathrm{mod}\ p^j)$ *je cyklická, pričom rád grupy je $p^{j-1}(p-1)$.*

Dôkaz tejto vety tiež neuvádzame, je však spomínaná v rôznych učebniciach elementárnej teórie čísel, napr. aj v [CP, Veta 2.2.5, časť 6].

Tvrdenie 1.2.2. *Ak p je ireducibilný prvok v okruhu hlavných ideálov R, potom (p) je prvoideál.*

Tvrdenie 1.2.3. *Ak $I = (m)$ je prvoideál v okruhu hlavných ideálov R, tak I je maximálny.*

Lema 1.2.4 (Veta o Frobeniovom automorfizme)**.** *Frobeniov automorfizmus σ (Definícia 1.1.5) v poli F_{p^2} je homomorfizmom* [10] *a navyše platí, že $\sigma(u) = u$ práve vtedy, keď $u \in \mathbb{Z}_p$.*

Dôkaz.

$$\sigma : x \to x^p$$

Binomická veta funguje aj v poli, takže

$$\sigma(u+v) = (u+v)^p = \sum_{k=0}^{p} \binom{p}{k} u^k v^{p-k}.$$

Podľa lemy 1.2.1 sa ale táto suma rovná $u^p + v^p = \sigma(u) + \sigma(v)$.

$\sigma(uv) = (uv)^p = u^p v^p = \sigma(u)\sigma(v)$.

Pri dokazovaní posledného tvrdenia musíme dokázať dve implikácie:
"$\Leftarrow$": Táto implikácia vyplýva priamo z vety 1.2.2.
"$\Rightarrow$": Rovnica $u^p - u = 0$ má maximálne p koreňov. My sme však už daných p koreňov našli. Sú to práve $u \in \mathbb{Z}_p$. Takže aj táto implikácia je pravdivá. □

Lema 1.2.5. *Ak nejaké u je koreňom rovnice $a_n x^n + \ldots + a_1 x + a_0 = 0$, pričom $a_n, \ldots, a_0 \in \mathbb{Z}_p$, tak potom obraz prvku u vo Frobeniovom automorfizme $\sigma(u)$ je tiež koreňom danej rovnice.*

Dôkaz. Nech $a_n u^n + \ldots + a_1 u + a_0 = 0,\ a_n, \ldots, a_0 \in \mathbb{Z}_p$.
Keďže sa jedná o homomorfizmus, použitím jeho vlastností (ktoré sme si ukázali a dokázali v predošlej leme 1.2.4) dostávame nasledovné:

$$a_n \sigma(u)^n + \ldots + a_1 \sigma(u) + a_0 = 0.$$

□

[10] Teda $\sigma(u+v) = \sigma(u) + \sigma(v)$ a $\sigma(uv) = \sigma(u)\sigma(v)$

Táto lema nám vlastne hovorí, že obraz koreňa nejakého polynómu zo $\mathbb{Z}_p[x]$ vo Frobeniovom automorfizme je opäť koreňom.

Z oboch vyslovených tvrdení teda dostávame nasledujúci dôsledok:

Dôsledok 1.2.1. *Aj je nejaké u koreňom rovnice $a_n x^n + \ldots + a_1 x + a_0 = 0$, $a_n, \ldots, a_0 \in \mathbb{Z}_p$ a $u \notin \mathbb{Z}_p$, tak potom ho $\sigma(u)$ zobrazí na nejaký* iný *koreň, ktorý tiež nie je z poľa $\mathbb{Z}_p$.*

1.3 Lucasove postupnosti

Lucasove postupnosti (1.1) sú lineárne homogénne rekurencie druhého rádu, pre ktoré je známa rozsiahla teória a venovala i venuje sa im veľká pozornosť matematikov. Tieto postupnosti majú veľa prekvapivých vlastností a veľa aplikácií. Sú pomenované po francúzskom matematikovi Édouardovi Lucasovi [11], ktorý je známy najmä pre veľký prínos pri vyriešení explicitného vyjadrenia n-tého člena Fibonacciho postupnosti a ďalších problémov súvisiacich s Fibonacciho postupnosťou. Práve táto, ale napr. aj Pellova, či Jacobsthalova postupnosť sú iba konkrétnym prípadom Lucasovej postupnosti.

Dá sa ľahko explicitne vyjadriť n-tý člen tejto Lucasovej postupnosti. To aj spravíme, v ďalšej časti si tiež ukážeme niekoľko výsledkov, ktoré platia pre Lucasovu postupnosť (1.1).

Pozrime sa, ako súvisia korene polynómu $f(x) = x^2 - ax + b$ s Lucasovými postupnosťami (1.1).

Veta 1.3.1. *Majme polynóm $f(x) = x^2 - ax + b$, ktorý má korene φ_1 a φ_2 (to znamená, že pre dané korene φ_1, φ_2 platí $\varphi_1 + \varphi_2 = a$ a zároveň $\varphi_1 \varphi_2 = b$). Potom postupnosti $(\varphi_1)^n$ a $(\varphi_2)^n$ vyhovujú uvedenej Lucasovej rekurencii* (1.1).

Dôkaz. Majme Lucasovu postupnosť $U_{n+2} - aU_{n+1} + bU_n = 0$ a nech φ_1 a φ_2 sú korene rovnice $f(x) = x^2 - ax + b$. Dosaďme hociktorý z týchto dvoch koreňov do našej rekurencie:

$$\varphi_1{}^{n+2} - a\varphi_1{}^{n+1} + b\varphi_1{}^{n} = \varphi_1^n(\varphi_1^2 - a\varphi_1 + b)$$

Ako jasne vidno, výraz v zátvorke je vlastne polynóm $f(x)$ v premennej φ_1, ktorá je koreňom tohto polynómu, takže celý výraz sa rovná nule. □

Rovnakým spôsobom, by sme vetu dokázali aj pre druhý koreň daného polynómu. Vidíme teda, že oba korene v príslušnej mocnine vyhovujú danej Lucasovej rekurencii. Ich lineárna kombinácia (a tiež ľubovoľná iná kombinácia členov vyhovujúcich rekurencii) opäť vyhovuje Lucasovej rekurencii:

Tvrdenie 1.3.1. *Ak nejaké φ_1^n a φ_2^n vyhovujú uvedenej Lucasovej postupnosti* (1.1)*, potom aj ich "lineárna kombinácia" vyhovuje danej postupnosti.*

Dôkaz.

$$(\alpha_1\varphi_1{}^{n+2} + \alpha_2\varphi_2{}^{n+2}) - a(\alpha_1\varphi_1{}^{n+1} + \alpha_2\varphi_2^{n+1}) + b(\alpha_1\varphi_1{}^{n} + \alpha_2\varphi_2{}^{n}) =$$
$$= \varphi_1^n\alpha_1 \underbrace{(\varphi_1^2 - a\varphi_1 + b)}_{0} + \varphi_2^n\alpha_2 \underbrace{(\varphi_2^2 - a\varphi_2 + b)}_{0} = 0.$$

[11] François Édouard Anatole Lucas (4. apríla 1842 - 3. októbra 1891) študoval na parížskej univerzite École Normale Supérieure. Istý čas pracoval v parížskom observatóriu, neskôr sa stal profesorom matematiky a vyučoval v Paríži. Nejakú dobu pracoval aj pre armádu.

□

Dostali sme teda, že n-tý člen (pre U_j, V_j) môžeme vyjadriť ako $\alpha_1(\varphi_1)^n + \alpha_2(\varphi_2)^n$. Podľa začiatočných podmienok dorátame neznáme α_1 a α_2 pre obe Lucasove postupnosti.

Dostávame sústavu rovníc (spôsob výpočtu si tentokrát ukážeme pre postupnosť V_j - pre U_j by bol postup podobný):

$$\begin{aligned} \alpha_1 + \alpha_2 &= 2 \\ \alpha_1\varphi_1 + \alpha_2\varphi_2 &= a, \text{ pričom } a = \varphi_1 + \varphi_2 \end{aligned}$$

Z toho už ľahko dorátame hodnoty α_1 a α_2, pričom nám vyjde $\alpha_1 = \alpha_2 = 1$ a teda postupnosť V_n môžeme explicitne vyjadriť ako

$$V_n = \varphi_1^n + \varphi_2^n. \tag{1.6}$$

Rovnako ľahko sa dá vyjadriť aj postupnosť U_n:

$$U_n = \frac{\varphi_1^n - \varphi_2^n}{\varphi_1 - \varphi_2}. \tag{1.7}$$

Kapitola 2

Fermatove pseudoprvočísla

2.1 Pseudoprvočísla

Uvažujme nejakú matematickú vetu alebo tvrdenie pre prvočísla: "Ak je číslo n prvočíslo, potom pre neho platí vlastnosť S". Vlastnosť S je pritom ľahko overiteľná, t.j. pre dané číslo n vieme rýchlo overiť (napr. v rozumnom polynomiálnom čase), či danú vlastnosť má. Vlastnosť S je teda nutnou podmienkou pre to, aby bolo dané číslo n prvočíslom. Ak n danú vlastnosť nemá, môžeme so stopercentnou istotou tvrdiť, že n nie je prvočíslo. V opačnom prípade, ak n danú vlastnosť S má, nemôžeme tvrdiť prakticky nič. Vlastnosť S je totiž iba nutnou podmienkou pre prvočíselnosť čísla n, nie však postačujúcou podmienkou, teda ju môžu mať aj niektoré zložené čísla. V súvislosti s takýmito nutnými podmienkami pre prvočíselnosť hovoríme o tzv. S-pseudoprvočíslach, pričom táto trieda čísel v sebe obsahuje všetky prvočísla, no ako "odpad" môže obsahovať aj zložené čísla. Našou úlohou teda je nájsť takú vlastnosť S, ktorá je na jednej strane ľahko overiteľná, no na druhej je trieda S-pseudoprvočísel čo najmenšia, teda popri prvočíslach obsahuje čo najmenej zložených čísel.

Jedným z príkladov takej "prvočíselnej vety" je nasledovné veľmi triviálne tvrdenie: Ak je číslo n prvočíslom, potom je n dvojka alebo nepárne číslo. Vidíme, že táto vlastnosť je triviálne overiteľná (v konštantnom čase), nehovorí nám však veľa o tom, či je dané číslo prvočíslo alebo zložené číslo, nakoľko v tejto triede je veľké množstvo (nekonečne veľa) zložených čísel. Preto nejaký test využívajúci toto tvrdenie nie je veľmi efektívny.

2.2 Fermatove pseudoprvočísla

Vieme veľmi rýchlo vypočítať hodnotu výrazu $a^b \pmod n$ a tento poznatok sa využíva v mnohých algoritmoch v teórii čísel. Celkovo sa pri overovaní, či v prípade nejakého čísla ide o prvočíslo alebo zložené číslo, využíva v hojnom počte počítanie mocnín v zvyškovej aritmetike. Veľmi veľa akýchsi prvočíselných testov využíva tiež vetu, ktorú sme si už uviedli v zozname na začiatku tejto práce. Je to veta 1.2.2, ktorá hovorí, že ak je n prvočíslo, potom platí

$$a^n \equiv a \pmod n. \tag{2.1}$$

Ak sú čísla a, n nesúdeliteľné, potom navyše platí Malá Fermatova veta 1.2.3:

$$a^{n-1} \equiv 1 \pmod{n}. \tag{2.2}$$

Na základe vzťahu (2.1) môžem zadefinovať triedu čísel, ktoré spĺňajú závery vety 1.2.2.

Definícia 2.2.1. Ľubovoľné číslo n nazveme *Fermatovým pseudoprvočíslom* pri základe a, ak spĺňa podmienku (2.1).

Teda napr. $n = 91$ je Fermatovým pseudoprvočíslom pri základe 3, pretože platí, že $3^{91} \equiv 3 \pmod{91}$. Rovnako tak platí, že číslo 341 je Fermatovým pseudoprvočíslom pri základe 2. Pri našich úvahách neberieme základ $a = 1$, pretože veta 1.2.2 je v takom prípade splnená pre ľubovoľné číslo. Preto predpokladáme, že $a > 1$.

Nasledujúca veta, ktorú si uvedieme bez dôkazu, hovorí o vzťahu medzi počtom prvočísel a zložených čísel, ktoré sú zároveň Fermatovými pseudoprvočíslami.

Veta 2.2.1. *Pre každé pevné $a \geq 2$ označme $\tau(x)$ počet zložených čísel menších alebo rovných ako x, ktoré sú zároveň Fermatovými pseudoprvočíslami pri základe a. Potom $\lim_{x\to\infty} \tau(x) = o(\pi(x))$, pričom $\pi(x)$ označuje počet prvočísel menších ako x.*

Vidíme teda, že počet zložených pseudoprvočísel pri základe a je menší než počet prvočíselných pseudoprvočísel pri základe a (keďže každé prvočíslo je pri ľubovoľnom základe Fermatovým pseudoprvočíslom), teda tento test má svoju opodstatnenosť.

Ekvivalent predchádzajúcej vety dokázal pre pseudoprvočísla zadefinované spôsobom (2.2) už v roku 1950 maďarský matematik Pál Erdős. Pre Fermatove pseudoprvočísla zadefinované spôsobom (2.1) to dokázal až v roku 1997 Li.

2.3 Pravdepodobnostné pseudoprvočísla

Ešte jedno obmedzenie základu a si môžeme dovoliť v prípade podmienky (2.2). Pre $a = n-1$ totiž podmienka platí pre ľubovoľné nepárne číslo, teda nám veľa o tom, či nejaké číslo je prvočíslo alebo zložené číslo, nepovie.

Definícia 2.3.1. Ak nejaká dvojica čísel n, a, pričom $1 < a < n-1$, spĺňa podmienky Malej Fermatovej vety 1.2.3, potom hovoríme, že n je pravdepodobnostné pseudoprvočíslo pri základe a.

Ak je nejaké číslo n prvočíslo, potom môžeme hneď tvrdiť, že je pravdepodobnostné pseudoprvočíslo pri ľubovoľnom základe. Ako sa ukázalo vo vete 2.2.1, počet zložených pseudoprvočísel je menší než počet prvočíselných prvočísel, teda nasledujúci test má ozajstné opodstatnenie:

Algoritmus 2.3.1 (Pravdepodobnostný pseudoprvočíselný test)**.**

1. Vypočítaj danú mocninu
   $b = a^{n-1} \pmod{n}$

2. Vráť výsledok
   if ($b == 1$) return "n je pravdepodobnostné pseudoprvočíslo pri základe a" else return "n je zložené číslo"

Aj keď je predchádzajúci test potenciálne dobrý, v nasledujúcej vete si dokážeme, že pre ľubovoľný základ existuje nekonečne veľa zložených pseudoprvočísel.

Veta 2.3.1. *Pre ľubovoľné $a \geq 2$ existuje nekonečne veľa Fermatových (rovnako tak pravdepodobnostných) zložených pseudoprvočísel pri základe a.*

Dôkaz. Ukážeme, že pre ľubovoľný základ a a ľubovoľné nepárne prvočíslo p, pre ktoré platí, že $p \nmid a^2 - 1$ je číslo $n = (a^{2p} - 1)/(a^2 - 1)$ zloženým pseudoprvočíslom pri základe a. Ako prvú skutočnosť ukážeme, že n je zložené číslo:

$$n = \frac{a^{2p} - 1}{a^2 - 1} = \frac{a^p - 1}{a - 1} . \frac{a^p + 1}{a + 1}.$$

Z toho, že p je nepárne vyplýva, že zlomky vystupujúce v predchádzajúcom výraze sú celé čísla (na základe poznatkov o možnosti rozloženia výrazov $A^n - B^n$ a $A^n + B^n$ pre n nepárne).

Na základe vety 1.2.2 platí, že $a^{2p} \equiv a^2 \pmod{p}$. Z toho vyplýva, že p delí výraz $a^{2p} - a^2$. V predpokladoch vety máme, že $p \nmid a^2 - 1$, z čoho vyplýva, že $p \mid n - 1$. To preto, lebo $n - 1 = \frac{a^{2p} - 1 - a^2 + 1}{a^2 - 1} = \frac{a^{2p} - a^2}{a^2 - 1}$. Keď si rozpíšeme $n - 1$, po predelení dostaneme, že $n - 1 = a^{2p-2} + a^{2p-4} + \ldots + a^2$. Teda $n - 1$ sme dostali ako súčet párneho počtu výrazov rovnakej parity $\Rightarrow n - 1$ je párne číslo, teda $2 \mid n - 1$. Dostali sme teda, že $2p \mid n - 1$ a teda $a^{2p} - 1$ je deliteľom $a^{n-1} - 1$. To preto, lebo $n - 1 = 2pl, l \in \mathbb{N}$ a $a^{n-1} - 1 = (a^{2p})^l - 1 = (a^{2p} - 1).Q$, pričom Q je prirodzené číslo, ktorého hodnota nás však momentálne nezaujíma. Máme však tiež, že $a^{2p} - 1 = n.(a^2 - 1)$, teda n je deliteľom $a^{2p} - 1$. Číslo n je teda deliteľom $a^{n-1} - 1$ a záver Malej Fermatovej vety 1.2.3, čiže aj vety 1.2.2 je splnený. □

Kapitola 3

Rabin-Millerov test

V nasledujúcej kapitole si ukážeme jeden z tzv. pravdepodobnostných algoritmov, ktorý nám povie, či je dané číslo pseudoprvočíslom (teda či spĺňa vlastnosti, ktoré určite spĺňajú aj prvočísla) alebo je zloženým číslom. Ide o tzv. Miller-Rabinov test. Ten má nasledujúce vlastnosti:

V prípade, že tento test "neprejde" (test skončí s odpoveďou, že nejde o pseudoprvočíslo), so stopercentou istotou vieme povedať, že pre dané číslo ide o zložené číslo.

Ak test "prejde" (test uvedie áno, teda číslo je pseudoprvočíslo), môžem o danom čísle tvrdiť, že je prvočíslo iba s istou pravdepodobnosťou.

Skúsme predpokladať, že Miller-Rabinov test sa pri druhom prípade pomýli (teda zložené číslo priradí ku pseudoprvočíslam) s pravdepodobnosťou menšou ako $1/2$. Potom opakovaním tohto testu môžeme dostať tvrdenie, že dané číslo je prvočíslo (ak test ani raz neodpovie "nie") s ľubovoľne malou pravdepodobnosťou. Práve toto bude hlavným cieľom kapitoly - dokázať, že Miller-Rabinov test sa pri svojom tvrdení, že dané číslo je prvočíslo, mýli iba s malou pravdepodobnosťou. V takom prípade by sme teoreticky po nekonečne veľa iteráciách mohli dané číslo, v prípade, že test stále ukázal hodnotu "áno", vyhlásiť za prvočíslo. Ako daný test funguje a kde je vlastne skrytá jeho pravdepodobnostná podstata, ukážeme si v ďalšej časti.

3.1 Silné pseudoprvočísla

Na začiatok si ukážeme pozmenenú verziu Malej Fermatovej vety 1.2.3.

Veta 3.1.1. *Nech n je nepárne prvočíslo. Zapíšme $n-1 = 2^s t$, kde t už je nepárne číslo. Ak nejaké a nie je deliteľné n, potom platí*

$$\begin{cases} \textit{buď } a^t \equiv 1 \pmod{n} \\ \textit{alebo } n^{2^i t} \equiv -1 \pmod{n} \textit{ pre nejaké } i, \textit{ pričom } 0 \leq i \leq s-1. \end{cases} \tag{3.1}$$

Dôkaz. Na dôkaz tohto tvrdenia nám poslúži Malá Fermatova veta 1.2.3 a fakt, že pre nepárne prvočíslo n sú jedinými riešeniami rovnice $x^2 \equiv 1 \pmod{n}$ v $\mathbb{Z}_n$ čísla $x = \pm 1 \pmod{n}$. To preto, lebo rovnicu $x^2 = 1$ si môžeme prepísať ako $x^2 - 1 = (x-1)(x+1) = 0$. v poli $\mathbb{Z}_n$ vzhľadom na násobenie nemáme deliteľov nuly, teda $(x-1)(x+1) = 0 \Rightarrow x = 1 \vee x = -1$.

Intuitívne je daná veta jasná, my si ju však dokážeme napr. sporom. Ak by totiž neplatila prvá podmienka, teda $a^t \not\equiv 1 \pmod{n}$ a ani druhá, teda $n^{2^i t} \not\equiv -1 \pmod{n}$ pre žiadne i, pričom $0 \leq i \leq s-1$, potom by podľa vysloveného tvrdenia, že jedinými riešeniami rovnice $x^2 \equiv 1 \pmod{n}$ v $\mathbb{Z}_n$ sú čísla $x = \pm 1 \pmod{n}$, nemohla platiť Malá Fermatova veta 1.2.3.

Tvrdenie môžeme dokázať aj matematickou indukciou vzhľadom na s, teda počet dvojok v kanonickom rozklade čísla $n-1$. Ak je $s = 0$, potom priamo z Malej Fermatovej vety 1.2.3 dostávame, že pre prvočíslo n platí $a^{n-1} = a^t \equiv 1 \pmod{n}$.

Nech tvrdenie platí pre nejaké $0 \leq i \leq s-1$. Chceme ukázať, že pre $i+1$ (a teda aj pre všetky ďalšie $i+2, \ldots, s$) už bude výsledok výrazu $a^{t.2^{i+1}} \pmod{n}$ iba 1. Začnime teda rozpisovať $a^{t.2^{i+1}} = (a^t)^{2^{i+1}} = (a^{2^i t})^2$. Z IP dostávame, že $a^{2^i t} = \begin{cases} \text{buď } -1 \pmod{n} \\ \text{alebo } 1 \pmod{n} \end{cases}$. Teda $(a^{2^i t})^2 = 1 \pmod{n}$.

□

Analogicky ku pravdepodobnostnému pseudoprvočíselnému testu 2.3.1 môžeme zadefinovať tzv. *silný pravdepodobnostný test*[1], ktorý vychádza z práve dokázanej vety. Za číslo a môžeme vziať ľubovoľné číslo a už dopredu môžeme prezradiť, že práve pri voľbe tohto základu a je skrytá pravdepodobnostná podstate celého testu.

Na upresnenie dodáme, že a je ľubovoľné prirodzené číslo $1 < a < n-1$. Prečo práve z takéhoto intervalu? To preto, lebo sa pohybujeme v grupe $\mathbb{Z}_p$. Pre $a = 1$ veta triviálne platí, pre $a = n-1 \equiv -1 \pmod{n}$ tiež veta triviálne platí.

Pred samotným testom sa ešte oplatí povedať, že vlastnosť (3.1), a teda aj tzv. silný pseudoprvočíselný test 3.1.1, je silnejšia ako Malá Fermatova veta 1.2.3. Je totiž viditeľné, že ak nejaké číslo (prvočíslo alebo pseudoprvočíslo) spĺňa podmienky (3.1), spĺňa aj podmienky vety 1.2.3. Z toho vyplýva, že každé pseudoprvočíslo, ktoré prejde cez nasledujúci test, prejde určite aj cez test 2.3.1.

Algoritmus 3.1.1 (Silný pseudoprvočíselný test)**.** Ako vstup zadáme nepárne číslo $n > 3$, o ktorom rozhodneme, či je zložené, alebo je to potenciálne (s istou pravdepodobnosťou) prvočíslo. Číslo n budeme reprezentovať ako $n = 1 + 2^s t$, kde t je nepárne číslo. Zvolíme si tiež základ a, pričom $1 < a < n-1$. Algoritmus odovzdá ako svoj výstup odpoveď, či je n zložené číslo alebo patrí do skupiny pseudoprvočísel.

1. Vyskúšame prvú nutnú podmienku vety 3.1
   $b = a^t \pmod{n}$
   if($b == 1$) or ($b == n-1$) return "n je pseudoprvočíslo pri základe a"

2. Skúsime otestovať aj druhú podmienku
   for (j=1..s-1) do {
   $b = b^2 \pmod{n}$
   if ($b == n-1$) return "n je pseudoprvočíslo pri základe a" }
   return "n je zložené číslo"

[1] Takto sa totiž nasledujúci test bude volať.

Tento test prvýkrát navrhol vo svojom článku Artjuhov v roku 1967. O niečo neskôr uzrel test zásluhou Johna Selfridgea [2] svetlo sveta opäť.

Pozrime sa ešte raz na tvrdenie, že silný pravdepodobnostný pseudotest je silnejší ako pravdepodobnostný pseudotest. Ukážeme si, že existuje číslo n so základom a, ktoré prešlo cez pravdepodobnostný test, ale neprešlo cez silný pravdepodobnostný test.

Za n dosaďme číslo 341, základom a bude 2. Test 3.1.1 odhalí, že ide o zložené číslo. Máme totiž, že $340 = 2^2.85, 2^{85} \equiv 32 \pmod{341}, 2^{170} \equiv 1 \pmod{341}$. Vidíme teda, že náš test odhalí, že v prípade čísla 341 nejde pri základe 2 o prvočíslo, ale zložené číslo, čo však test 2.3.1 neodhalil.

Ukážme si však, že existuje ale aj číslo, ktoré pri danom základe cez test prejde napriek tomu, že ide o zložené číslo. Dosaďme za $n = 91 = 7.13, a = 10$. Máme ďalej, že $90 = 2^1.45$, teda $10^{45} \equiv -1 \pmod{91}$.

Definícia 3.1.1. Vravíme, že n je *silné pseudoprvočíslo pri základe* a práve vtedy, keď n je nepárne číslo, ktoré spĺňa podmienky 3.1.

Z tejto definície dostávame, že napr. 341 nie je silné pseudoprvočíslo pri základe 2, číslo 91 však silným pseudoprvočíslom pri základe 10 je. Práve Johnovi Selfridgovi patrí pomenovanie takýchto pseudoprvočísel ako silné pseudoprvočísla. Už skôr sme si uviedli, že ak je číslo n silným pseudoprvočíslom pri základe a, tak je aj pseudoprvočíslom pri základe a. Z uvedeného príkladu pre $n = 341, a = 2$ vidno, že opačná implikácia neplatí, teda test na silné pseudoprvočísla je silnejší ako test na pseudoprvočísla 2.3.1.

3.2 Miller-Rabinov test

3.2.1 Veta o presnosti M-R testu

Definícia 3.2.1. Pre zložené nepárne číslo n definujeme

$$\mathbf{S}(n) = \{a \pmod{n} : n \text{ je silné pseudoprvočíslo pri základe } a\}. \tag{3.2}$$

Potom $S(n) = \sharp\mathbf{S}(n)$.

Nasledujúcu veľmi dôležitú vetu nezávisle na sebe dokázali v roku 1980 Monier a Rabin [3]. Hovorí o pravdepodobnosti pomýlenia testu 3.1.1.

Veta 3.2.1. *Pre každé nepárne zložené číslo $n > 9$ platí, že $S(n) \leq \frac{1}{4}\varphi(n)$, kde $\varphi(n)$ je Eulerova funkcia 1.1.4.*

Pripomeňme si, že Eulerova funkcia nám hovorí, koľko čísel menších ako n je nesúdeliteľných s n. Dokázali sme vo vete 1.2.12, že $\mathbb{Z}_n^*$, čo sú všetky takéto prvky nesúdeliteľné s n, je grupa vzhľadom na násobenie so zvyškom $\odot$ a táto grupa má práve $\varphi(n)$ prvkov. Ak poznáme kanonický rozklad n, vieme

[2] John L. Selfridge je americký matematik, ktorý sa preslávil najmä svojou prácou v oblasti analytickej teórie čísel. Selfridge študoval na Kalifornskej univerzite a v roku 1958 získal titul Ph.D. Bol jedným z vedcov, ktorý spolupracovali s vari najväčšou matematickou osobnosťou 20. storočia, maďarským matematikom Paulom Erdősom. V roku 1962 dokázal, že číslo 78 557 je tzv. Sierpinskeho číslo.

[3] Michael Oser Rabin (1. septembra 1931) sa narodil v nemeckom meste Breslau, ktoré v súčasnosti patrí Poľsku. Je židovským počítačovým expertom, ktorý si za svoju výnimočnú prácu vyslúžil aj Turingovu cenu.

presne určiť aj $\varphi(n)$: $\varphi(n) = n\prod_{p|n}(1-1/p)$, kde p ide cez všetky prvočísla nachádzajúce sa v kanonickom rozklade n.[4]

Vidíme, že veta 3.2.1 je kľúčovou v našich ďalších úvahách. Pred samotným dôkazom tejto dôležitej vety si ešte zadefinujeme a ukážeme niektoré veci a použitie danej vety.

Majme nepárne číslo n, o ktorom chceme rozhodnúť, či je zloženým číslom alebo prvočíslom. Vyskúšame test 3.1.1 pre nejaké $a, 1 < a < n-1$. Ak číslo n cez tento test neprejde, so stopercentnou istotou môžeme tvrdiť, že ide o zložené číslo. Ak však daný test prejde, báza a iba nemusela byť správnym výberom a my vieme iba s istou pravdepodobnosťou uviesť, že dané číslo by mohlo byť prvočíslom. Urobíme aj formálnu definíciu predchádzajúcej úvahy:

Definícia 3.2.2. Pre n nepárne zložené číslo nazveme bázu a $(1 < a < n-1)$, na ktorej test 3.1.1 zlyhá pre dané n, svedkom pre n. Svedok je teda báza, pre ktorú nie je n silným pseudoprvočíslom.

Taká báza a sa teda volá svedok preto, lebo "dosvedčuje", že ide o zložené číslo.

3.2.2 M-R test

Veta 3.2.1 hovorí o tom, že aspoň $3/4$ všetkých báz $\in \langle 1, n-1\rangle$ sú svedkami pre nejaké nepárne zložené číslo n. Na základe toho za chvíľu popíšeme pravdepodobnostný algoritmus, tzv. Miller-Rabinov test. Ten si najprv vyberie nejakú bázu a potom prevedie silný pravdepodobnostný test 3.1.1. Na základe vety 3.2.1 môžeme tvrdiť, že ak test pre nejaké nepárne číslo n prejde, dané číslo je prvočíslom s pravdepodobnosťou $3/4$. Opakovaním Miller-Rabinovho testu však môžeme túto pravdepodobnosť zväčšovať a získať ľubovoľnú pravdepodobnosť, akú len chceme.[5]

Algoritmus 3.2.1 (Miller-Rabinov test)**.** Ako vstup dostaneme nepárne číslo n. Pravdepodobnostný algoritmus sa v prípade, že ide o zložené číslo, pokúsi nájsť svedka a pre n. Ak sa tak stane, algoritmus ako svoj výstup vyhodí (a, ÁNO), v opačnom prípade (a, NIE).

1. Vyber potenciálneho svedka
   Vyber random $a \in < 2, n-2 >$
   Použi algoritmus 3.1.1

2. Rozhodovanie
   if (n je silné pseudoprvočíslo pri základe a) return (a, NO) else (a, YES)

Z vety 3.2.1 vidno, že pre $n > 9$ zložené nepárne číslo je pravdepodobnosť omylu $\leq \frac{1}{4}$. Ako sme však spomenuli skôr, môžeme tento test opakovať k-krát, pričom pravdepodobnosť omylu bude v takomto prípade $\leq \frac{1}{4^k}$. [6]

[4] Dôkaz tejto vety neuvádzame, nachádza sa napr. v [S2].

[5] Pôvodný test, ktorý publikoval Miller v roku 1976 bol o trochu viac komplikovaný a išlo o deterministický a nie pravdepodobnostný test. Bol to M. Rabin, ktorý v článkoch z roku 1976 a 1980 navrhol pravdepodobnostný test.

[6] Nie je to úplná pravda, pretože v prípade, že n je nepárne číslo, existuje medzi jeho svedkami, čiže bázami a, pre ktoré test 3.1.1 zlyhá, určitá závislosť, čiže korelácia. My však v našich úvahách budeme predpokladať, že korelácia je nulová a všetky výbery bázy a sú navzájom úplne nezávislé.

3.2.3 Dôkaz vety o M-R teste

Teraz sa už dostaneme k samotnému dôkazu vety 3.2.1, ktorým si dokážeme oprávnenosť tohto naozaj silného nástroja na dokazovanie prvočíselnosti nepárnych čísel. Predtým si však ešte ukážeme nejaké pomocné tvrdenia:

Tvrdenie 3.2.1. *Majme grupu (G,*), ktorej prvok a má rád k.*[7] *Potom platí, že* $a^n = 1$ *práve vtedy, keď* $k \mid n$.

Dôkaz. "⇐":

$$n = k.l \Rightarrow a^n = (a^k)^l = 1^l = 1.$$

"⇒": Máme $a^n = 1$ a chceme dokázať, že $k \mid n$. Postupujme sporom a $n = k.q + r, 0 < r < k$. Potom $1 = a^n = a^{k.q+r} = (a^k)^q.a^r = a^r$, čo je spor, pretože $r < k$ a k je najmenšie prirodzené číslo také, že $a^k = 1$. □

Lema 3.2.1. *Nech je n nepárne zložené číslo,* $n - 1 = 2^s t$, *kde t je už nepárne číslo. Nech* $\nu(n)$ *označuje najväčšie prirodzené číslo také, že* $2^{\nu(n)}$ *delí* $p - 1$ *pre každé prvočíslo p nachádzajúce sa v kanonickom rozklade čísla n. Ak je n silné pravdepodobnostné pseudoprvočíslo pri základe a, tak potom* $a^{2^{\nu(n)-1}t} \equiv \pm 1 \pmod{n}$.

Dôkaz. Ak je nejaké číslo silným pravdepodobnostným pseudoprvočíslom, potom pre neho platia podmienky (3.1), a preto dostávame, že buď $a^t \equiv 1 \pmod{n}$ alebo $a^{2^i t} \equiv -1 \pmod{n}$. Ak zoberieme prvý prípad, teda $a^t \equiv 1 \pmod{n}$, tak závery uvedenej lemy jasne platia, pretože číslo 1 umocnené na čokoľvek nám dáva opäť 1.

Rozoberme si teraz druhý prípad, teda $a^{2^i t} \equiv -1 \pmod{n}$. Nech p je ľubovoľný prvočíselný faktor n. Potom je jasné, že $a^{2^i t} \equiv -1 \pmod{p}$.

Označme ako k rád a v poli $\mathbb{Z}_p$ (teda mod$p$). Potom podľa tvrdenia 3.2.1 k delí $2^{i+1}t$, ale nedelí $2^i t$. Preto mocnina čísla 2 v kanonickom rozklade k musí byť 2^{i+1}.Z Malej Fermatovej vety 1.2.3 však dostávame, že $a^{p-1} \equiv 1 \pmod{p} \Rightarrow k \mid p - 1 \Rightarrow 2^{i+1} \mid p - 1$. Predchádzajúci postup platí pre ľubovoľné prvočíslo p nachádzajúce sa v kanonickom rozklade n, z čoho dostávame $i + 1 \leq \nu(n)$. Potom $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$ alebo $\equiv -1 \pmod{n}$. Prvý prípad dostaneme, ak $i + 1 < \nu(n)$ a druhý, keď nastane rovnosť, čiže $i + 1 = \nu(n)$. □

Pred ďalšou lemou a jej dôkazom si zadefinujme jeden symbol, ktorý budeme používať:

Definícia 3.2.3. $\overline{\mathbf{S}}(n) = \{a \pmod{n} : a^{2^{\nu(n)-1}t} \equiv \pm 1 \pmod{n}\}$ a $\overline{S}(n) = \#\overline{\mathbf{S}}(n)$.

Lema 3.2.2. *Nech* $n - 1 = 2^s t$, *nech* $\omega(n)$ *je počet všetkých rôznych prvočíselných faktorov čísla n a nech funkcia* $\nu(n)$ *je zadefinovaná rovnako ako v predchádzajúcej leme 3.2.1. Potom platí*

$$\overline{S}(n) = 2.2^{(\nu(n)-1)\omega(n)} \prod_{p|n} NSD(t, p-1).$$

[7] Rád je najmenšie prirodzené číslo k také, že $a^k = 1$

Dôkaz. Označme $m = 2^{\nu(n)-1}t$. Pozrieme sa najprv na prípad, že $a^m \equiv 1 \pmod{n}$:

Nech $n = p_1^{j_1}p_2^{j_2}\dots p_k^{j_k}$ je kanonický rozklad čísla n, čiže $\omega(n) = k$. Z výpočtu a vety 1.2.7 dostávame, že platí $a^m \equiv 1 \pmod{n} \Leftrightarrow a^m \equiv 1 \pmod{p_i^{j_i}}$ pre $i = 1, \dots, k$.

Podľa vety 1.2.12 vieme, že redukované zvyškové triedy tvoria grupu. Na základe vety 1.2.13 tiež vieme, že pre prvočíslo p a prirodzené číslo j je grupa $\mathbb{Z}_{p^j}$ cyklickou grupou, ktorej rád sa rovná $p^{j-1}(p-1)$.

Keďže sa jedná o cyklickú grupu (má generátor g) s rádom $p^{j-1}(p-1)$, môžeme písať, že $\mathbb{Z}_{p^j} = \{g, g^2, \dots, g^{p^{j-1}(p-1)} = 1\}$. My vlastne teraz hľadáme počet riešení rovnice $a^m = (g^k)^m = g^{k.m} \equiv 1 \pmod{n}$, pričom neznáma je premenná k. To je podľa tvrdenia 3.2.1 práve vtedy, keď $p_i^{j_i-1}(p_i-1)) \mid k.m$. Úlohu sme teda pretransformovali na inú, a síce koľko je počet riešení rovnice $k.m \equiv 0 \pmod{p_i^{j_i-1}(p_i-1)}$. Na vyriešenie tohto problému nám pomôže veta 1.2.9. Tá hovorí o tom, že daná rovnica má riešenie, ak $d = \mathrm{NSD}(m, p_i^{j_i-1}(p_i-1)) \mid 0$, čo je splnené. Počet riešení takejto rovnice je potom práve d, čiže $\mathrm{NSD}(m, p_i^{j_i-1}(p_i-1))$. Z toho dostávame, že počet riešení sa rovná

$$\mathrm{NSD}(m, p_i^{j_i-1}(p_i-1)) = \mathrm{NSD}(m, p_i-1) = 2^{\nu(n)-1}.\mathrm{NSD}(t, p_i-1), \qquad (3.3)$$

pričom úvodnú rovnosť sme dostali, pretože $\mathrm{NSD}(m, p_i^{j_i-1}) = 1$. To platí na základe nasledujúcej úvahy:

$$1 = \mathrm{NSD}(n, n-1) \overset{m|n-1}{\geq} \mathrm{NSD}(n, m) \overset{p_i^{j_i-1}|n}{\geq} \mathrm{NSD}(p_i^{j_i-1}, m) \Rightarrow \mathrm{NSD}(p_i^{j_i-1}, m) = 1.$$

Ešte by sme si mali ukázať, prečo $m \mid n-1$. Vieme, že $m = 2^{\nu(n)-1}t$ a $n-1 = 2^s t$. Treba nám teda ukázať, že $\nu(n) - 1 \leq s$. Na to nám stačí rozpísať si danú situáciu:
$p_i - 1 = 2^{\nu(n)}.p_i'$ pre všetky $i \Rightarrow p_i = 2^{\nu(n)}.p_i' + 1$. Z toho si vyjadríme n:

$$n = \prod_{i=1}^{k} p_i^{j_i} = 2^{\nu(n)}[G] + 1 \Rightarrow n - 1 = 2^{\nu(n)}[G],$$

pričom G je nejaké prirodzené číslo, ktorého presnú hodnotu momentálne nepotrebujeme poznať. Ale už jasne vidno, že $s \geq \nu(n)$, takže naozaj je pravda, že $m \mid n-1$.

Opäť využijeme Čínsku vetu o zvyškoch 1.2.7, ktorá hovorí, že pre ľubovoľný konečný systém kongruencií (vzhľadom na jednotlivé prvočíselné mocniny $p_i^{j_i}$ v kanonickom rozklade čísla n), ktorých je podľa predchádzajúceho odvodenia $\prod_{i=1}^{k}(2^{\nu(n)-1}.\mathrm{NSD}(t, p_i-1))$, máme práve jedno riešenie $\pmod{p_1^{j_1}\dots p_k^{j_k}}$. Teda počet všetkých riešení sa rovná počtu všetkých kongruencií, ktorých je

$$\prod_{i=1}^{k}(2^{\nu(n)-1}.\mathrm{NSD}(t, p_i-1)) = 2^{(\nu(n)-1)\omega(n)} \prod_{i=1}^{k}(\mathrm{NSD}(t, p_i-1)).$$

Vidíme, že tento počet zodpovedá polovici počtu, o ktorom tvrdíme na začiatku. Teraz musíme ukázať, že počet riešení druhej kongruencie $a^m \equiv -1 \pmod{n}$ je rovnaký.

Pri dôkaze tohto tvrdenia si najprv všimnime, že $a^m \equiv -1 \pmod{p_i^{j_i}}$ práve vtedy, keď $a^{2m} \equiv 1 \pmod{p_i^{j_i}}$ a zároveň $a^m \not\equiv 1 \pmod{p_i^{j_i}}$. Z toho vyplýva, že počet riešení kongruencie $a^m \equiv -1 \pmod{p_i^{j_i}}$ dostaneme ako počet riešení kongruencie $a^{2m} \equiv 1 \pmod{p_i^{j_i}}$ mínus počet riešení kongruencie $a^m \equiv 1 \pmod{p_i^{j_i}}$.

Pri výpočte počtu riešení kongruencie $a^{2m} \equiv 1 \pmod{p_i^{j_i}}$ postupujeme rovnako ako v predchádzajúcej časti, až sa dostaneme k analógii výsledku (3.3):

$$\mathrm{NSD}(2m, p_i^{j_i-1}(p_i-1)) = \mathrm{NSD}(2m, p_i-1) = 2^{\nu(n)}.\mathrm{NSD}(t, p_i-1).$$

Počet výsledkov pre kongruenciu $a^m \equiv -1 \pmod{p_i^{j_i}}$ je teda

$$2^{\nu(n)}.\mathrm{NSD}(t, p_i-1) - 2^{\nu(n)-1}.\mathrm{NSD}(t, p_i-1) = 2^{\nu(n)-1}.\mathrm{NSD}(t, p_i-1).$$

Z tohto už vidno, že počet riešení oboch rekurencií je rovnaký, a síce

$$2^{(\nu(n)-1)\omega(n)} \prod_{i=1}^{k} (\mathrm{NSD}(t, p_i-1)).$$

Celkový počet riešení je teda

$$2.2^{(\nu(n)-1)\omega(n)} \prod_{i=1}^{k} (\mathrm{NSD}(t, p_i-1))$$

. □

Dôkaz vety 3.2.1. V leme 3.2.1 sme ukázali, čo platí pre každé zložené číslo n pri základe a, pričom táto dvojica je silným pravdepodobnostným pseudoprvočíslom. Množina $\overline{\mathbf{S}}(n)$ teda pre dané n v sebe obsahuje minimálne všetky a, pri ktorých je n silným pravdepodobnostným pseudoprvočíslom (samozrejme, daná vlastnosť môže byť splnená aj pre iné čísla). Nám teda stačí ukázať, že $\overline{\mathbf{S}}(n)/\varphi(n) \leq 1/4$ pre ľubovoľné nepárne zložené číslo $n > 9$. Z lemy 3.2.2 a vety 1.2.10 dostávame, že

$$\frac{\varphi(n)}{\overline{\mathbf{S}}(n)} = \frac{1}{2} \prod_{p^a \| n} p^{a-1} \frac{p-1}{2^{\nu(n)-1}\mathrm{NSD}(t, p-1)},$$

kde zápis $p^a \parallel n$ znamená, že p^a je presná mocnina prvočísla p v kanonickom rozklade zloženého čísla n. Všimnime si, že každý výraz $\frac{p-1}{2^{\nu(n)-1}\mathrm{NSD}(t,p-1)}$ je celé párne číslo. To preto. lebo $\frac{p-1}{2^{\nu(n)-1}} \geq 2$, $\frac{p-1}{\mathrm{NSD}(t,p-1)} \geq 1$ a v prvom zlomku robíme iba s mocninou dvojky, kým v druhom s nepárnymi číslami, keďže t je nepárne číslo. Z toho vyplýva, že celý výraz $\frac{\varphi(n)}{\overline{\mathbf{S}}(n)}$ je párne prirodzené číslo.

Teraz su rozlíšime rôzne prípady:

- Ak $\omega(n) \geq 3$, čiže v kanonickom rozklade zloženého čísla n máme aspoň tri prvočísla, potom $\frac{\varphi(n)}{\overline{\mathbf{S}}(n)} \geq \frac{1}{2}2^3$.
- Ak $\omega(n) = 2$ a n má aspoň jedno prvočíslo vo svojom kanonickom rozklade s mocninou aspoň 2. Potom násobok p^{a-1} je aspoň 3, čiže $\frac{\varphi(n)}{\overline{\mathbf{S}}(n)} \geq 6$.

- Predpokladajme, že $n = p.q$, pričom $p < q$ sú prvočísla a zároveň platí, že $2^{\nu(n)+1} \mid q-1$. Môžeme teda písať, že $q-1 = 2^{\alpha}.q', \alpha \geq \nu(n)+1$. Rozpíšme si menovateľ:

$$2^{\nu(n)-1} \underbrace{\mathrm{NSD}(t, q-1)}_{|q'} \leq 2^{\nu(n)-1}.q' \leq \frac{2^{\nu(n)+1}q'}{4} \leq \frac{q-1}{4}.$$

  Z toho už dostávame, že $\varphi(n)/\overline{\mathbf{S}} \geq 4$.

- Predpokladajme, že $n = p.q$, pričom $p < q$ sú prvočísla a zároveň neplatí, že $2^{\nu(n)+1} \mid q-1$, teda $2^{\nu(n)} \parallel q-1$.

  $$n = p.q = p(q-1) + p \equiv p \pmod{q-1} \Rightarrow n-1 \equiv p-1 \pmod{q-1},$$

  teda $q-1 \nmid n-1$. Z toho vyplýva, že v kanonickom rozklade čísla $q-1$ existuje nepárne prvočíslo vo väčšej mocnine ako je to u čísla $n-1$. Prečo takáto situácia nemôže nastať u čísla 2? Teda by $q-1$ malo vo vyššej mocnine dvojku. To uvidíme hneď po rozpísaní danej situácie:
  $p-1 = 2^{\nu(n)}p' \Rightarrow p = 2^{\nu(n)}p' + 1$
  $q-1 = 2^{\nu(n)}q' \Rightarrow q = 2^{\nu(n)}q' + 1$

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

  Z predchádzajúceho odvodenia teda jasne vidno, že dvojka nemôže byť v kanonickom rozklade $n-1$ vo vyššej mocnine ako v prvočíselnom rozklade $q-1$.

  Na základe predchádzajúcich úvah a toho, že $q-1 = 2^{\nu(n)}q'$ teda môžeme písať $2^{\nu(n)-1}\mathrm{NDS}(t, q-1) = 2^{\nu(n)-1}\mathrm{NSD}(t, q') \leq \frac{2^{\nu(n)q'}}{2.3} = \frac{q-1}{6}$.

- Posledným prípadom je možnosť, že $n = p^a$, kde $a \geq 2$. Potom $\frac{\varphi(n)}{\overline{\mathbf{S}}} \geq p^{a-1}$. Vo všetkých prípadoch okrem toho, že $p^a = 9$ potom dostávame $\frac{\varphi(n)}{\overline{\mathbf{S}}} \geq 5$.

□

3.3 Generátor pravdepodobnostných prvočísel

Miller-Rabinov test je veľmi užitočný v aplikáciách, kde sa narába s prvočíslami. Aj keď nie je úplne stopercentný, v mnohých praktických aplikáciách postačuje. Pravdepodobnosť, že dané číslo n, ktorého prvočíselnosť sme viackrát zdarne vyskúšali v teste 3.2.1, je totiž dostatočne veľká. Preto sa niekedy v prípade Miller-Rabinovho testu hovorí aj o "prvočíselnom teste". Tento názov celkom nezodpovedá realite, určite však nie je neoprávnený.

Henri Cohen[8] navrhol test založený na Miller-Rabinovom teste, ktorý generuje tzv. úrovňovo vygenerované pseudoprvočíslo.

[8] Henri Cohen (narodený v roku 1947) je známy francúzsky číselný teoretik, ktorý je profesorom na univerzite v Bordeaux. Preslávil sa najmä ako vedúci predstaviteľ tímu, ktorý vytvoril PARI/GP algebraický systém. Napísal niekoľko vedeckých kníh, ktoré mali vo svete veľký úspech. Zaoberal sa v nich najmä počítačovou a algebraickou teóriou čísel.

Algoritmus 3.3.1. Ako vstup dostaneme čísla $k \geq 3$ a $T \geq 1$, pričom $k, T \in \mathbb{N}$. Tento pravdepodobnostný algoritmus vytvorí náhodné k-bitové číslo[9], ktoré sme vyskúšali T iteráciami Miller-Rabinovho testu a žiadny z testov neodhalil, že by išlo o zložené číslo.

1. Výber nejakého kandidáta
   Vyber náhodné číslo nepárne číslo z intervalu $(2^{k-1}, 2^k)$

2. Preskúšaj ho Miller-Rabinovým testom 3.2.1
   for$(1 \leq i \leq T)$ {Pomocou algoritmu 3.2.1 skús nájsť svedka pre n;
   if(a je svedkom pre n) goto krok 1}
   return n;

Je naozaj veľká pravdepodobnosť, že takto vytvorené číslo je ozajstným prvočíslom, preto ho môžeme používať aj v rôznych praktických aplikáciách.

[9] Nejaké číslo z intervalu $<2^{k-1}, 2^k)$

Kapitola 4

Fibonacciho a Lucasove pseudoprvočísla

4.1 Fibonacciho pseudoprvočísla

Fibonacciho [1] postupnosť je veľmi dobre známa rekurentne zadaná postupnosť, pre ktorú platí:

$$F_n = F_{n-1} + F_{n-2}, \quad \text{pričom } F_0 = 0,\ F_1 = 1. \tag{4.1}$$

Ako vidno, táto Fibonacciho postupnosť je len konkrétnym príkladom Lucasovej postupnosti (1.1) $U_n(a,b)$ pre $a = 1$, $b = -1$.

Táto postupnosť (4.1) nám dáva jeden z nástrojov, ktorým sa pre nejaké prirodzené číslo n dá overiť, či sa jedná o prvočíslo. Platí totiž nasledujúca veta:

Veta 4.1.1. *Majme Fibonacciho postupnosť F_n zadanú obvyklým spôsobom* (4.1). *Ak číslo $n \in \mathbb{N}$ je prvočíslo, tak platí $F_{n-\varepsilon_n} \equiv 0 \pmod{n}$, kde*

$$\varepsilon_n = \begin{cases} 1 & ak\ n \equiv \pm 1 \pmod 5 \\ -1 & ak\ n \equiv \pm 2 \pmod 5 \\ 0 & ak\ n \equiv 0 \pmod 5 \end{cases} \tag{4.2}$$

Neznáma funkcia ε_n nie je nič iné ako Legendrov symbol - v našom prípade $\left(\frac{n}{5}\right)$ - zadefinovaný v úvodnej kapitole (Definícia 1.1.3).

Dôkaz tejto vety uvedieme trochu neskôr, nakoľko je iba konkrétnym príkladom oveľa všeobecnejšej vety.

Definícia 4.1.1. Ľubovoľné číslo $n \in \mathbb{N}$ nazveme Fibonacciho pseudoprvočíslom vtedy, ak pre neho platí, že $F_{n-\varepsilon_n} \equiv 0 \pmod{n}$.

Len pre zaujímavosť môžeme uviesť, že najmenšie také zložené Fibonacciho pseudoprvočíslo, ktoré je nesúdeliteľné s číslom 10, je číslo 323.

[1] Leonardo z Pisy (1190 - 1250), známy skôr pod menom Leonardo Fibonacci, bol taliansky matematik v súčasnosti považovaný za najtalentovanejšieho európskeho stredovekého matematika. Na začiatku 13. storočia napísal Knihu výpočtov, v ktorej sa zaoberal arabskými číslicami, ich použitím a vlastnosťami. Je známy aj vďaka tzv. Fibonacciho postupnosti, ktorou sa síce nezaoberal priamo, na základe nej však vysvetľoval vo svojej knihe mnohé javy.

4.2 Test využívajúci Lucasovu postupnosť

Pri dokazovaní vety 4.1.1 prišli matematici na oveľa všeobecnejší výsledok, ktorý sa viaže k Lucasovým postupnostiam (1.1). Fibonacciho postupnosť je vlastne rekurentnou postupnosťou zadanou ako $F_j = F_{j-1} + F_{j-2}$, ktorej prislúcha polynóm [2] $f(x) = x^2 - x - 1$.

Uvažujme lineárne rekurencie prislúchajúce polynómu $f(x) = x^2 - ax + b$, pričom platí, že $\triangle = a^2 - 4b$ nie je štvorec (t.j. nie je to druhá mocnina nejakého čísla).[3]

Nech

$$U'_j = U'_j(a,b) = \frac{x^j - (a-x)^j}{x - (a-x)} \pmod{f(x)} \tag{4.3}$$
$$V'_j = V'_j(a,b) = x^j + (a-x)^j \pmod{f(x)}.$$

Takéto značenie znamená, že my berieme zvyšky okruhu polynómov po delení polynómom $f(x)$.

Tvrdenie 4.2.1. *Obe postupnosti* (4.3) *sú ekvivalentné s nami uvedenými rekurentne zadanými postupnosťami* (1.1) *prislúchajúcimi polynómu* $f(x)$.

Dôkaz. Ukážeme to matematickou indukciou vzhľadom na parameter j (názornú ukážku uvedieme pre postupnosti V'_j a V_j, pre postupnosť U_j je však postup analogický).

Vidno, že báza indukcie je triviálne splnená, keďže V'_0 z postupnosti (4.3) $= x^0 + (a-x)^0 = 2 = V_0$ z postupnosti (1.1). Rovnako dostaneme aj $V'_1 = x^1 + (a-x)^1 = x + a - x = a = V_1$.

Nech tvrdenie platí pre všetky $k < j$:

$$V_j = aV_{j-1} - bV_{j-2} = a(x^{j-1} + (a-x)^{j-1}) - b(x^{j-2}a(a-x)^{j-2}) =$$
$$= ax^{j-1} - bx^{j-2} + a(a-x)^{j-1} - b(a-x)^{j-2} = x^{j-2}(ax-b) + (a-x)^{j-2}(a(a-x)-b) \equiv$$
$$\equiv x^{j-2}x^2 + (a-x)^{j-2}(a-x)^2 = x^j + (a-x)^j \pmod{f(x)}.$$

Platí totiž $x^2 \equiv ax - b \pmod{f(x)}$ a tiež:

$$a(a-x) - b = a^2 - b - ax \equiv a^2 - b - ax + x^2 - ax + b = a^2 - 2ax + x^2 = (a-x)^2 \pmod{f(x)}.$$

□

Analogicky k vete 4.1.1 máme oveľa všeobecnejšiu vetu, ktorá hovorí niečo o prvočíslach v spojení s rekurentnými postupnosťami U_n.

Veta 4.2.1. *Majme prirodzené čísla* a, b *a determinant* $\triangle = a^2 - 4b$. *Definujme postupnosti* U_j *a* V_j *podľa* (4.3). *Ak je nejaké číslo* p, *pričom NSD*$(p, 2b\triangle) = 1$, *prvočíslo, potom platí*

$$U_{p-\left(\frac{\triangle}{p}\right)} \equiv 0 \pmod{p}.$$

Pred samotným dôkazom vety 4.2.1 by som ešte chcel upriamiť pozornosť čitateľa na Frobeniov automorfizmus 1.1.5 a niekoľko pomocných tvrdení v úvodnej kapitole, ktoré o ňom hovoria viac. Tieto poznatky totiž využijeme pri samotnom dôkaze vety.

[2] Korene φ_1 a φ_2 tohto polynómu nám dajú explicitné riešenie danej rekurencie
[3] V našom prípade $\triangle$ zodpovedá determinantu kvadratickej rovnice $f(x)$.

Dôkaz vety 4.2.1. Na začiatok si všimnime, že redukujeme polynómy na zvyškové triedy, ktoré dostaneme po delení polynómom $f(x) = x^2 - ax + b$. Vo vete 4.2.1 tiež pracujeme so zvyškami modulo n. Preto sa budeme pohybovať v okruhu $\mathbf{R} = \mathbb{Z}_p[x]/(x^2 - ax + b)$. Budeme teda narábať so zvyškovými triedami tvaru $\{i + jx\colon\ i,\ j \in \mathbb{N}_0,$ pričom $0 \leq i, j \leq n-1\}$.

V okruhu $\mathbf{R}$ platí, že $x^2 = ax - b$. Preto môžeme písať pre súčet a súčin dvoch prvkov z okruhu R nasledujúce vzťahy:

$$(i_1 + j_1 x) + (i_2 + j_2 x) = i_3 + j_3 x$$
$$(i_1 + j_1 x)(i_2 + j_2 x) = i_4 + j_4 x,$$

kde

$$i_3 = i_1 + i_2 \pmod n, \qquad j_3 = j_1 + j_2 \pmod n$$
$$i_4 = i_1 i_2 - b j_1 j_2 \pmod n, \qquad j_4 = i_1 j_2 + i_2 j_1 + a j_1 j_2 \pmod n.$$

V dalšej časti dôkazu budeme rozlišovať dva prípady:

1. p je nepárne [4] prvočíslo, pričom platí $\left(\frac{\triangle}{p}\right) = -1$. Z tejto podmienky (z významu daného Legendrovho symbolu) dostávame, že $\triangle$, teda diskriminant kvadratickej rovnice $f(x)$ nie je štvorec v $\mathbb{Z}_p$, takže jeho odmocnením nedostanem prvok patriaci do $\mathbb{Z}_p$. Polynóm $x^2 - ax + b$ je teda ireducibilný nad $\mathbb{Z}_p$ (podľa lemy 1.2.3).

   Preto $\mathbf{R} = \mathbb{Z}_p[x]/(x^2 - ax + b) \cong$ konečné pole F_{p^2} s p^2 prvkami (Podľa viet 1.2.2 a 1.2.3). Podpole $\mathbb{Z}_p$ poľa $\mathbb{F}_{p^2}$ je vlastne zástupcom zvyškových tried tvaru $i + 0x$.

   Ktorý z reprezentantov $\{i + jx\}$ je koreňom polynómu $x^2 - ax + b$? Sú to práve x a $a - x$. Ako sme uviedli už vyššie, zvyškové triedy tvaru $i + 0x$ sú reprezentanti patriaci do $\mathbb{Z}_p$. Keďže x a ani $a - x$ nie sú tvaru $i + 0x$, nepatria ani do $\mathbb{Z}_p$. Podľa dôsledku 1.2.1 teda dostávame nasledovné:

   $$\text{pre prípad } \left(\frac{\triangle}{p}\right) = -1 : \begin{cases} x^p \equiv a - x \pmod{f(x), p}, \\ (a-x)^p \equiv x \pmod{f(x), p}. \end{cases} \tag{4.4}$$

   Označenie $\pmod{f(x), p}$ je pritom iba skrátený zápis toho, čo sme tu celý čas používali, a síce $\mathbb{Z}_p[x]/(x^2 - ax + b)$.

   V pokračovaní dôkazu už iba využijeme (4.4):

   $$x^{p+1} - (a-x)^{p+1} \equiv x(a-x) - (a-x)x \equiv 0 \pmod{f(x), p}, \tag{4.5}$$

   čo znamená, že $U_{p+1} \equiv 0 \pmod p$.

2. p je nepárne prvočíslo, pričom platí, že $\left(\frac{\triangle}{p}\right) = 1$. Teda $\triangle$ je štvorec a teda polynóm $x^2 - ax + b$ nie je ireducibilný. Neplatí teda, že okruh $\mathbf{R} = \mathbb{Z}_p[x]/(x^2 - ax + b) \cong$ konečné pole F_{p^2} s p^2 prvkami. Platí ale veta 1.2.11. Nech G je práve náš okruh $\mathbb{Z}_p[x]$ a H je okruh $(\mathbb{Z}_p \mathrm{x} \mathbb{Z}_p)$.

   Teda máme nejaké zobrazenie $\varphi : f(x) \to (f(a_1), f(a_2))$. Ak by boli splnené podmienky vety 1.2.11, mohli by sme podľa nej písať, že $G/Ker\varphi \cong H$,

[4] To, že musí byť nepárne, dostávame zo začiatočnej podmienky $\mathrm{NSD}(p, 2b\triangle) = 1$

čo v našom prípade dáva $\mathbb{Z}_p[x]/(x^2 - ax + b) \cong (\mathbb{Z}_p \mathrm{x} \mathbb{Z}_p)$. To preto, lebo ak $f(x) \in Ker\varphi$, tak potom musí platiť, že $(f(a_1), f(a_2)) = (0,0)$. Keďže $f(a_1) = 0 \overset{1.2.2}{\Rightarrow} x - a_1 \mid f(x)$. To isté platí pre $f(a_2)$. Teda $(x-a_1)(x-a_2) \mid f(x)$. K tomuto ešte treba pridať, že z toho, že $\mathrm{NSD}(\triangle, p) = 1$[5] vyplýva, že $\triangle \neq 0 \Rightarrow a_1 \neq a_2$. Preto horeuvedené veci s určitosťou platia. Dostali sme sa teda k výsledku, že $(x-a_1)(x-a_2) = x^2 - (a_1+a_2)x + a_1a_2 = a^2 - ax + b \mid f(x)$.

Našou najbližšou úlohou teda bude presvedčiť sa o tom, že $\varphi : f(x) \to (f(a_1), f(a_2))$ je surjekcia a navyše homomorfizmus.

- že dané zobrazenie je homomorfizmus v okruhu

$$\varphi(f(x) + g(x)) = ((f+g)(a_1), (f+g)(a_2)) =$$
$$= (f(a_1), f(a_2)) + (g(a_1), g(a_2)) = \varphi(f(x)) + \varphi(g(x))$$

$$\varphi(f(x)g(x)) = ((fg)(a_1), (fg)(a_2)) = (f(a_1)g(a_1), f(a_2)g(a_2)) =$$
$$= (f(a_1), f(a_2))(g(a_1), g(a_2)) = \varphi(f(x))\varphi(g(x))$$

- že dané zobrazenie je surjektívne
  Nech $(m,n) \in \mathbb{Z}_p^2$. Potom hľadáme polynóm $f(x)$ taký, pre ktorý platí

$$a_1^2 + aa_1 + b = m, \text{ z čoho dostávame } a_1a + b = m - a_1^2$$
$$a_2^2 + aa_2 + b = n, \text{ z čoho dostávame } a_2a + b = n - a_2^2$$

$$\text{Z podmienok vety } a_1 \neq a_2 \Rightarrow h \begin{pmatrix} a_1 & 1 \\ a_2 & 1 \end{pmatrix} = 2 \Rightarrow \text{ taká } f(x) \exists$$

Dostali sme teda, že $R = \mathbb{Z}_p[x]/(x^2 - ax + b) \cong \mathbb{Z}_p \mathrm{x} \mathbb{Z}_p$. Pre každý prvok v takomto okruhu podľa 1.2.2 platí, že $a^p = a$. Teda

$$\text{pre prípad } \left(\frac{\triangle}{p}\right) = +1 : \begin{cases} x^p \equiv x \pmod{f(x), p}, \\ (a-x)^p \equiv a - x \pmod{f(x), p}. \end{cases} \tag{4.6}$$

Pred poslednými úpravami v dôkaze ešte treba povedať, že z toho, že $\mathrm{NSD}(p, 2b\triangle) = 1$ vyplýva $\mathrm{NSD}(p,b) = 1 \overset{veta 1.2.8}{\Rightarrow} \exists u, v\colon\ u.p + b.v = 1 \Rightarrow b\ v \equiv 1 \pmod{p}$. A teda prvok b má inverzný prvok. Využijúc tento poznatok môžeme pokračovať:

$$x^2 - ax + b = 0 \Rightarrow x(a-x) = b \overset{b \text{ je invertovateľný}}{\Rightarrow} x[-(a-x)b^{-1}] = 1.$$

Vidíme teda, že v $\mathbb{Z}_p/(f(x))$ majú x aj $(a-x)$ inverzný prvok.

Z tohto dôvodu platí, že $x^{p-1} = x^p.x^{-1} \equiv x.x^{-1} = 1 \pmod{p, f(x)}$. Rovnako tak dostávame aj $(a-x)^{p-1} = (a-x)^p.(a-x)^{-1} = (a-x)(a-x)^{-1} = 1 \pmod{p, f(x)}$. Na základe toho dostávame výsledok $U_{p-1} \equiv 0 \pmod{p}$.

□

[5] Toto máme v podmienkach vety, a síce $\mathrm{NSD}(p, 2b\triangle) = 1$

Definícia 4.2.1. Ľubovoľné číslo n, pre ktoré platí $\mathrm{NSD}(n, 2b\triangle) = 1$, nazveme Lucasovým pseudoprvočíslom vzhľadom na polynóm $x^2 - ax + b$ práve vtedy, keď platí

$$U_{n-\left(\frac{\triangle}{n}\right)} \equiv 0 \pmod{n}.$$

Na záver si môžeme ukázať, ako vyplýva veta 4.1.1 zo všeobecnejšej vety 4.2.1. Ak totiž dosadíme $a = 1, b = -1$, dostaneme polynóm $f(x) = x^2 - x - 1$ a k nemu zodpovedajúcu Fibonacciho postupnosť (4.1). Diskriminant polynómu je $\triangle = 1 + 4 = 5$. Vidíme teda, že pre ľubovoľné prvočíslo p okrem prvočísel 5 a 2 platí, že $\mathrm{NSD}(p, 2.(-1).5) = 1$. Teda musí platiť, že $U_{p-\left(\frac{5}{p}\right)} \equiv 0 \pmod{p}$. Čísla 5 aj p sú nepárne a prvočísla, zo zákona kvadratickej reciprocity 1.2 teda dostávame, že $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. A keďže dávajú druhé mocniny prvkov poľa $\mathbb{Z}_5$ zvyšky iba ± 1, na základe definície Legendrovho symbolu 1.1.3 sme v podstate dostali presné znenie vety 4.1.1. Pre čísla 2 a 5 overíme platnosť vety napr. ručne.

Kapitola 5

Grantham-Frobeniov test

V celom Lucas-Lehmerovom teste hral dôležitú úlohu Frobeniov automorfizmus (ktorý nejakému prvku v poli priraďoval p-tu mocninu - 1.1.5). Tento zohrá kľúčovú rolu aj v nasledujúcom teste pochádzajúcom od Jona Granthama. Tento bude tiež narábať s funkciou $f(x)$, tá už ale nemusí byť iba kvadratická, ale môže to byť ľubovoľný polynóm. V prípade kvadratického polynómu je tento test silnejší ako Lucasovo testovanie, ktoré sme si predstavili už skôr. Aj preto si tento test ukážeme opäť v prípade, že za polynóm $f(x)$ dosadíme ľubovoľný kvadratický polynóm.

5.1 Frobeniove pseudoprvočísla a ich vzťah k Lucasovym pseudoprvočíslam

Definícia 5.1.1. Nech a, b sú prirodzené čísla, pre ktoré platí, že $\triangle = a^2 - 4b$ nie je štvorec. Nech n je ľubovoľné celé číslo, pre ktoré platí, že $\mathrm{NSD}(n, 2b\triangle) = 1$. Číslo n nazveme *Frobeniovo pseudoprvočíslo* vzhľadom na polynóm $f(x) = x^2 - ax + b$ práve vtedy, keď platí

$$x^n \equiv \begin{cases} a - x \pmod{f(x), n}, & \text{ak } \left(\frac{\triangle}{n}\right) = -1 \\ x \pmod{f(x), n}, & \text{ak } \left(\frac{\triangle}{n}\right) = 1. \end{cases}$$

Podobné výsledky sme už dostali pri dokazovaní vety 4.2.1, konkrétne podmienky (4.4) a (4.6). Pri zbežnom pohľade sa však zdá, že definícia hovorí iba o polovičných podmienkach prípadov (4.4) a (4.6). Nie je to však pravda, o čom sa presvedčíme v nasledujúcej vete. Ešte predtým si však uvedieme jedno pomocné tvrdenie.

Tvrdenie 5.1.1. *Nech m, n sú prirodzené čísla a $f(x), g(x), r(x) \in \mathbb{Z}[x]$. Ak $f(r(x)) \equiv 0 \pmod{n, f(x)}$ a $x^m \equiv g(x) \pmod{f(x), n}$, potom $r^m(x) \equiv g(r(x)) \pmod{n, f(x)}$.*[1]

Dôkaz. $x^m \equiv g(x) + f(x)h(x) \pmod{n}$ pre nejaké $h(x) \in \mathbb{Z}[x]$. Pretože x je premenná, môžeme za ňu dosadiť aj $r(x)$ a dostaneme $r^m(x) \equiv g(r(x)) +$

[1] Toto tvrdenie rovnako ako aj vzťah medzi Frobeniovými a Lucasovými pseudoprvočíslami je z [G]

$f(r(x))h(r(x)) \pmod n$. Z predpokladov tvrdenia však máme, že $f(r(x)) \equiv 0 \pmod{n, f(x)}$, a teda $r^m(x) \equiv g(r(x)) \pmod{n, f(x)}$. □

Lema 5.1.1. *Ak je nejaké číslo Frobeniovým pseudoprvočíslom, potom je aj Lucasovým pseudoprvočíslom.*

Dôkaz. Prípad, že $\left(\frac{\triangle}{n}\right) = -1$:

$$x^n \equiv a - x \pmod{f(x), n}$$
$$x^n = (a - x) + f(x)h(x) \pmod n$$

Posledná rovnosť je rovnosť 2 polynómov v $\mathbb{Z}_n[x]$; zostane v platnosti aj ak namiesto x dosadím $a - x$

$$(a - x)^n = x + f(a - x)h(a - x) \pmod n$$
$$(a - x)^n = x + f(x)h(a - x) \pmod n$$
$$(a - x)^n \equiv x \pmod{f(x), n}$$

Pričom sme využili fakt, že $f(a-x) = (a-x)^2 - a(a-x) + b = a^2 - 2ax + x^2 - a^2 + ax + b = x^2 - ax + b = f(x)$. (V podstate by nám stačilo aj to, že $a - x$ je koreň $f(x)$ v $\mathbb{Z}_n[x]/(f(x))$, nie je tam treba priamo rovnosť.)

Ďalej by sa už pokračovalo rovnako, ako v dôkaze vety 4.2.1, čiže by sme splnili podmienku pre Lucasove pseudoprvočíslo.
Prípad, že $\left(\frac{\triangle}{n}\right) = +1$:

Máme, že $x^n \equiv x \pmod{n, f(x)} \Rightarrow x^{n-1} \equiv 1 \pmod{n, f(x)}$. Predchádzajúca implikácia platí na základe podmienky $\mathrm{NSD}(n, b) = 1$, z ktorej vyplýva invertovateľnosť b v $\mathbb{Z}_n$. Z existencie inverzného prvku pre b už dostávame, že aj x má inverzný prvok. Takéto úvahy sme už využili na konci dôkazu vety 4.2.1. Keď do predchádzajúceho tvrdenia 5.1.1 dosadíme $r(x) = a - x, g(x) = 1, m = n - 1$, tak sú splnené jeho predpoklady: $f(r(x)) = f(a - x) \equiv 0 \pmod{n, f(x)}$ a $x^{n-1} \equiv g(r(x)) \pmod{n, f(x)} \equiv 1 \pmod{n, f(x)}$. Z tohto dôvodu môžeme písať, že $(a - x)^{n-1} \equiv 1 \pmod{n, f(x)}$. Teda sme dostali

$$U_{n-1} \equiv \frac{x^{n-1} - (a - x)^{n-1}}{x - (a - x)} \equiv 0 \pmod{n, f(x)}.$$

Ešte však treba ukázať, že menovateľ nie je nulový. To dostaneme z poznatku, že x a $a - x$ sú korene v $\mathbb{Z}[x]/(f(x))$ a toho, že $\mathrm{NSD}(n, \triangle) = 1$. Vieme totiž, že korene danej kvadratickej rovnice $f(x)$ môžeme vypočítať ako $\frac{a \pm \sqrt{\triangle}}{2}$. Treba ukázať, že $\triangle$ je nenulový prvok. To však plynie práve z toho, že $\mathrm{NSD}(n, \triangle) = 1$. Ak by totiž $\triangle = 0$, tak potom $\mathrm{NSD}(n, \triangle) = n$. □

Frobeniove pseudoprvočísla, ako sme videli v predchádzajúcej vete, obsahujú maximálne toľko zložených čísel ako Lucasove pseudoprvočísla. V skutočnosti ich je menej, čo si ukážeme neskôr.

5.2 Grantham-Frobeniov test

Teraz už pristúpme k vete, ktorá nám v istom zmysle hovorí, aký veľký je "odpad" zložených čísel pri Frobeniových pseudoprvočíslach. Predtým však opäť jedno celkom triviálne tvrdenie.

Tvrdenie 5.2.1. *Platí rovnosť* $2x^m = (2x-a)U_m + V_m \pmod{f(x), n}$.

Dôkaz.

$$(2x-a)U_m + V_m \equiv (2x-a)\frac{x^m-(a-x)^m}{x-(a-x)} + (x^m+(a-x)^m) =$$
$$= x^m - (a-x)^m + x^m + (a-x)^m = 2x^m \pmod{f(x), n}.$$

□

Veta 5.2.1. *Nech a, b sú prirodzené čísla, pre ktoré $\triangle = a^2 - 4b$ nie je štvorcom, teda druhou mocninou nejakého prirodzeného čísla. Nech n je ľubovoľné zložené prirodzené číslo, pre ktoré platí, že $NSD(n, 2b\triangle) = 1$. Potom je n Frobeniovým pseudoprvočíslom vzhľadom na polynóm $x^2 - ax + b$ práve vtedy, keď*

$$U_{n-\left(\frac{\triangle}{n}\right)} \equiv 0 \pmod{n} \quad a \quad V_{n-\left(\frac{\triangle}{n}\right)} \equiv \begin{cases} 2b, & ak \left(\frac{\triangle}{n}\right) = -1 \\ 2, & ak \left(\frac{\triangle}{n}\right) = +1. \end{cases}$$

Dôkaz. Opäť rozlíšime dve implikácie:

$''\Leftarrow''$: Máme dané nejaké kongruencie a chceme dokázať, že z nich vyplývajú kongruencie zadané v definícii Frobeniovych pseudoprvočísel 5.1.1.

- Ak $\left(\frac{\triangle}{n}\right) = -1$:

  $U_{n+1} \equiv 0 \pmod{n}$ a $V_{n+1} \equiv 2b$. Z tvrdenia 5.2.1 dostaneme $2x^{n+1} \equiv (2x-a).0+2b \pmod{f(x), n}$. Z toho vyplýva, že $x^{n+1} \equiv b \pmod{f(x), n}$. Keďže $x(a-x) \equiv b \pmod{f(x), n}$ a x má opäť inverzný prvok [2], dostávame teda $x^n \equiv (a-x) \pmod{f(x), n}$.

- Ak $\left(\frac{\triangle}{n}\right) = +1$:

  $U_{n-1} \equiv 0 \pmod{n}$ a $V_{n-1} \equiv 2$. Opäť využijeme tvrdenie 5.2.1 a dostávame $2x^{n-1} \equiv (2x-a).0 + 2 \Rightarrow x^{n-1} \equiv 1 \pmod{f(x), n}$. Z toho už jasne vidno, že $x^n \equiv x \pmod{f(x), n}$.

Boli splnené všetky podmienky a teda n je v takomto prípade Frobeniovo pseudoprvočíslo.

$''\Rightarrow''$: Predopkladajme, že n je Frobeniovo pseudoprvočíslo vzhľadom na $f(x)$. Ako sme už ukázali v leme 5.1.1, je zároveň aj Lucasovým pseudoprvočíslom, z čoho okrem iného vyplýva, že $U_{n-\left(\frac{\triangle}{n}\right)} \equiv 0 \pmod{n}$. Opäť z tvrdenia 5.2.1 dostávame $2x^{n-\left(\frac{\triangle}{n}\right)} \equiv V_{n-\left(\frac{\triangle}{n}\right)} \pmod{f(x), n}$. Ďalej teda rozlíšime dva prípady:

1. Nech $\left(\frac{\triangle}{n}\right) = -1$:

   Potom platí, ako sme ukázali v (4.4), že $x^n \equiv (a-x) \pmod{f(x), n}$, z čoho dostávame $x^{n+1} \equiv (a-x)x \equiv b \pmod{f(x), n}$. Takže $V_{n+1} \equiv 2b \pmod{n}$.

[2] Toto sme už ukázali v leme 5.1.1, pričom sme sa odvolali na dôkaz tvrdenia 4.2.1.

2. Nech $\left(\frac{\triangle}{n}\right) = +1$:

   Pretože x má inverzný prvok a platí (4.6), dostávame, že $x^{n-1} \equiv 1 \pmod{f(x), n}$. Z čoho vyplýva, že $V_{n-1} \equiv 2 \pmod{n}$.

Vidíme, že sme sa opäť dostali ku kongruenciám, ktoré sú uvedené v tejto vete. □

Už skôr sme si dokázali, že Frobeniových pseudoprvočísel, teda aj Frobeniových zložených čísel, je maximálne toľko, koľko je Lucasových pseudoprvočísel. Teraz si len na jednom praktickom príklade ukážeme, že ich je o dosť menej (čiže v tomto prípade je menší "odpad" zmiešaných čísel). Ak si totiž vezmeme polynóm $f(x) = x^2 - x - 1$, tak prvým Frobeniovým zmiešaným pseudoprvočíslom je 4181 (v poradí 19. Fibonacciho číslo) a prvým, pre ktoré platí $\left(\frac{5}{n}\right) = -1$ je 5777. Z tohto vidíme, že nie každé Lucasovo pseudoprvočíslo je aj Frobeniovo. Grantham-Frobeniov test je teda silnejší ako test, ktorý zisťuje príslušnosť k Lucasovým pseudoprvočíslam, pretože "ním prejde" menej zložených čísel.

Grantham-Frobeniov test môže byť veľmi efektívny. Napr. pre polynóm $x^2 + 5x + 5$ dodnes nepoznáme žiadny príklad zloženého Frobeniovho pseudoprvočísla n, pre ktoré platí $\left(\frac{5}{n}\right) = -1$. Predpokladá sa však, že minimálne jedno takéto číslo naozaj existuje.

Kapitola 6

Pepinov test

Prvočíselnosť menších čísel môžeme zistiť veľmi jednoducho (napr. predelením všetkých čísel menších ako odmocnica z daného čísla). Existuje však prah (takým je zhruba číslo 10^{12}, závisí však od rôznych špecifických vlastností počítača, na ktorom daný test prevedieme), pre ktorý už existujú aj lepšie metódy ako len "bezhlavé" skúšanie všetkých prípustných možností. Jednou z nich je aj tzv. Pepinov test, ktorý si predstavíme v nasledujúcej kapitole. Pomocou neho sa dá overiť alebo vyvrátiť prvočíselnosť tzv. Fermatových čísel. Pepinov test patrí medzi tzv. $n-1$- testy, pretože sa pri tomto teste nezaoberáme ani tak číslom n, ako skôr číslom $n-1$. Pepinov test je iba variantom Prothovho testu.

6.1 Lucasova veta

Aby sme sa dostali k vytúženému cieľu, potrebujeme si ešte predtým vysloviť a dokázať vetu, ktorá je známa ako Lucasova veta. Francúzsky matematik Édouard Lucas ju vyslovil ešte v roku 1876.

Veta 6.1.1 (Lucasova veta)**.** *Nech a, n sú prirodzené čísla, $n > 1$. Ak platí, že*

$$a^{n-1} \equiv 1 \pmod{n}, \text{ ale } a^{(n-1)/q} \not\equiv 1 \pmod{n} \text{ pre všetky prvočísla } q \mid (n-1),$$

potom je n prvočíslo.

Dôkaz. Sporom: Nech n je zložené číslo. Teda n má nejakého prvočíselného deliteľa p (je jasné, že p aj n sú celé čísla z množiny $\{1, 2, \ldots, n\}$). Podľa vety 1.2.12 vieme, že $\mathbb{Z}_n^*$, čo sú všetky čísla z tejto množiny nesúdeliteľné s n, tvoria vzhľadom na násobenie so zvyškom $\odot$ grupu. Využijúc už skôr vyslovené tvrdenie 3.2.1 môžeme tvrdiť, že prvá podmienka vety 6.1.1 hovorí, že stupeň a v $\mathbb{Z}_n$ je deliteľ čísla $n-1$. Z druhej podmienky však vyplýva, že stupeň a v $\mathbb{Z}_n$ nemôže byť menší ako $n-1$, teda je práve $n-1$.

Platí, že $\mathrm{NSD}(a, n) = 1$. Ukážeme to *sporom*. Nech a a n majú spoločného prvočiniteľa, nazvime ho p, t.j. $p \mid a$ a $p \mid n$. Keďže $p \mid n$, tak na základe prvej kongruencie z podmienok vety platí $a^{n-1} \equiv 1 \pmod{p}$. Súčasne však máme $p \mid a$, a teda $a^{n-1} \equiv 0 \pmod{p}$. Dostali sme však dva rozdielne výsledky, čo je spor.

Môžeme teda použiť Eulerovu vetu 1.2.4 a využitím ďalšej vety 3.2.1 dostávame nasledovné (stupeň a) $\mid \varphi(n)$. Z toho vyplýva, že $n - 1 \leq \varphi(n)$. Zároveň

však máme, vychádzajúc z toho, že n je zložené číslo a tiež z definície eulerovej funkcie $\varphi(n)$, že $\varphi(n) \leq n-2$. Toto je *spor*, teda n musí byť prvočíslom. □

Uvedená verzia vety 6.1.1 vďačí za svoje znenie Lehmerovi. Samotná Lucasova veta totiž uvažovala všetky možné delitele q čísla $n-1$.

6.2 Pepinov test

6.2.1 Fermatove čísla

Definícia 6.2.1. Fermatove[1] čísla sú tvaru $F_n = 2^{2^n}+1$ pre $n \in \mathbb{Z}, n \geq 0$.

O Fermatovych číslach sa dá napr. dokázať to, že ľubovoľné dve takéto čísla sú navzájom nesúdeliteľné[2]. Táto veta sa potom dá použiť na dôkaz o nekonečnosti množiny prvočísel.

Sám Fermat si myslel, že všetky čísla takéhoto tvaru sú prvočísla. Jeho hypotézu sa však podarilo vyvrátiť Eulerovi, ktorý dokázal rozložiť piate Fermatovo číslo $F_5 = 2^{32}+1 = 4294967297 = 641.6700417$, Dodnes nie je známe, či existuje nekonečne veľa Fermatovych prvočísel ani to, či vôbec existuje nekonečne veľa zložených Fermatovych čísel.

6.2.2 Pepinov test

Tvrdenie 6.2.1. *Ak je l kladné, tak* $2^l \equiv 1 \pmod 3$.

Dôkaz. Tvrdenie sa dá veľmi jednoducho dokázať *matematickou indukciou*. Báza indukcie triviálne platí.

Nech tvrdenie platí pre $\forall l \leq k$. Zoberieme 2^{k+2}:

$$2^{k+2} = 4.(2^k) = 4.(3m+1) = 12m+4 \equiv 1 \pmod 3.$$

□

V roku 1877 vyslovil Pepin tvrdenie podobné tomu nasledujúcemu:

Veta 6.2.1 (Pepinov test)**.** *Pre všetky $k \geq 1$ je Fermatovo číslo $F_k = 2^{2^k}+1$ prvočíslom práve vtedy, keď* $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.

Dôkaz. Keďže ide o ekvivalenciu, dostaneme nutnú a zároveň i postačujúcu podmienku pre prvočíselnosť Fermatových čísel. Musíme teda dokázať dve ekvivalencie.

$''\Leftarrow''$: Predpokladajme, že platí uvedená kongruencia. Potom ak dosadíme $n = F_k, a = 3$, tak F_k je podľa Lucasovej vety 6.1.1 prvočíslo. To preto, lebo

$$3^{(F_k-1)/2} \equiv -1 \pmod{F_k} \Rightarrow 3^{(F_k-1)/2}.3^{(F_k-1)/2} \equiv 1 \pmod{F_k}$$

a zároveň pre všetky prvočíselné deliteľe $F_k - 1$, ktorými je iba jediné číslo 2 (na základe tvaru Fermatových čísel $2^{2^k}+1$), sa $3^{(F_k-1)/2} \not\equiv 1 \pmod{F_k}$.

[1] Pierre de Fermat (žil začiatkom 17. storočia) bol francúzsky právnik a tiež matematik, ktorého výsledky sa využívajú v mnohých častiach matematiky i fyziky. Medzi jeho najznámejšie výsledky patrí dôkaz tzv. Malej Fermatovej vety a vyslovenie hypotézy, tzv. Veľkej fermatovej vety, ktorú sa matematikom podarilo dokázať az v posledných rokoch.

[2] Dôkaz nie je zložitý, dá sa nájsť napr. v [S2, Veta 2.4.4]

$''\Rightarrow''$: Predpokladáme, že pre nejaké k je Fermatove číslo F_k prvočíslom. Keďže 2^k je párne číslo, tak podľa tvrdenia 6.2.1 platí, že $2^{2^k} \equiv 1 \pmod 3$, teda $F_k \equiv 2 \pmod 3$. S odvolaním sa na tvar Fermatových čísel môžeme hneď tvrdiť, že pre $k \geq 1$ platí $F_k \equiv 1 \pmod 4$.

Keďže 3 aj F_k sú prvočísla, môžeme použiť rovnicu z Gaussovho zákona kvadratickej reciprocity (1.2):

$$\left(\frac{3}{F_k}\right) \cdot \left(\frac{F_k}{3}\right) = (-1)^{(3-1)(F_k-1)/4},$$

z ktorého vidíme, že $\left(\frac{3}{F_k}\right)$ aj $\left(\frac{F_k}{3}\right)$ majú rovnaké znamienka, pretože ich súčinom sme dostali 1 (platí totiž $F_k \equiv 1 \pmod 4$, čiže $4 \mid F_k - 1$).

Už sme si ukázali, že $F_k \equiv 2 \pmod 3$. Keď sa však pozrieme na zvyšky pri štvorcoch $\pmod 3$, vidíme, že tieto zvyšky sú v oboch možných prípadoch kongruentné s 1:

$$(3k+1)^2 = 9k^2 + 6k + 1 \qquad (3k+2)^2 = 9k^2 + 12k + 4.$$

Z toho teda vieme, že $\left(\frac{F_k}{3}\right) = -1 \Rightarrow \left(\frac{3}{F_k}\right) = -1 \Rightarrow 3$ nie je štvorec $\pmod{F_k}$. Podľa kongruencie v Eulerovom kritériu (1.4) teda platí

$$\left(\frac{3}{F_k}\right) = 3^{(F_k-1)/2} \equiv -1 \pmod{F_k}.$$

□

6.2.3 Pôvodný Pepinov test

Samotný Pepin používal pri tomto teste namiesto čísla 3 číslo 5 a v predpokladoch bolo $k \geq 2$. Až Proth a Lucas ukázali, že môže byť použité aj číslo 3. Samotná Pepinova veta znela takto:

Veta 6.2.2. *Pre všetky $k \geq 2$ je Fermatovo číslo $F_k = 2^{2^k} + 1$ prvočíslom práve vtedy, keď $5^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.*

Dôkaz. Dôkaz pre toto znenie sa iba v malých detailoch odlišuje od predchádzajúceho postupu:

$''\Leftarrow''$: Dôkaz tejto implikácie je prakticky totožný s dôkazom rovnakej implikácie v predchádzajúcej vete.

$''\Rightarrow:''$ Aj tu je postup v podstate veľmi podobný ako v predchádzajúcom prípade.

Keďže 5 aj F_k sú prvočísla, opäť použijeme zákon reciprocity (1.2):

$$\left(\frac{5}{F_k}\right) \cdot \left(\frac{F_k}{5}\right) = (-1)^{(5-1)(F_k-1)/4},$$

z ktorého vidíme, že $\left(\frac{5}{F_k}\right)$ aj $\left(\frac{F_k}{5}\right)$ majú rovnaké znamienka, pretože $F_k - 1$ je párne číslo.

Pozrime sa bližšie na zvyšok $F_k \pmod 5$. Indukciou sa dá dokázať, že pre $k \geq 2$ dá 2^{2^k} po delení číslom 5 zvyšok 1:

Báza indukcie je pre $k = 2$ splnená.
Nech tvrdenie platí pre všetky $l \leq k$. Vezmime číslo $2^{2^{(k+1)}} = 2^{2^k.2} = (2^{2^k})^2 \overset{ip}{\equiv} (5m+1)^2 = 25m^2 + 10m + 1 \equiv 1 \pmod 5$.

A teda číslo $F_k = 2^{2^k} + 1 \equiv 2 \pmod 5$. Ak by sme sa však opäť pozreli na zvyšky štvorcov zvyškových tried $\pmod 5$, číslo 2 by ste medzi nimi nenašli $\Rightarrow \left(\frac{F_k}{5}\right) = -1 \Rightarrow \left(\frac{5}{F_k}\right) = -1$. Opäť iba dosadíme do Euleroveho kritéria a dostaneme požadovanú kongruenciu. □

Kapitola 7

Lucas-Lehmerov test

Ďalší test prvočíselnosti jednej triedy čísel je prisudzovaný Édouardovi Lucasovi, ktorý ho vymyslel a dokázal v roku 1856. Tento test sa používa na dokazovanie prvočíselnosti tzv. Mersennových prvočísel. Sám francúzsky vedec ho ešte vylepšil v roku 1878 a po ňom doviedol celý test do súčasnej podoby v roku 1930 Derrick Henry Lehmer[1]. Tento test patrí medzi tzv. $n+1$-testy, pretože nás pri samotnom testovaní zaujíma skôr číslo $n+1$ a nie samotné n.

7.1 Morrisonova veta

V nasledujúcej kapitole budeme opäť pracovať s Lucasovými postupnosťami (1.1) a ekvivalentne zadanými postupnosťami (4.3).

Definícia 7.1.1. Všetky čísla tvaru $M_n = 2^n - 1$ sa nazývajú tzv. *Mersennove*[2] *pseudoprvočísla*[3].

Nevie sa, či je takýchto Mersennovych prvočísel (Mersennove pseudoprvočísla, ktoré sú aj naozaj prvočíslami) konečne alebo nekonečne veľa. Dá sa ale dokázať, že ľubovoľné dve Mersennove pseudoprvočísla M_n sú nesúdeliteľné. Taktiež nie je ťažké ukázať, že ak je M_n prvočíslo, tak aj n je prvočíslo[4].

Definícia 7.1.2. Pre $n \in \mathbb{N}, n \geq 0$, pričom platí $\mathrm{NSD}(n, 2b\triangle) = 1$, je tzv. *hodnosť výskytu* n, označovaná ako $r_{f(n)}$, také najmenšie r, pre ktoré platí $U_r \equiv 0 \pmod{n}$.

Tvrdenie 7.1.1. *Ak* $k \mid j$, *potom aj* $U_k \mid U_j$.

[1] Derrick Henry "Dick"Lehmer(23. februára 1905 - 22. mája 1991) bol americký matematik, ktorý nadviazal na prácu Édouarda Lucasa. On i jeho manželka sa výrazne podpísali pod mnohé objavy v oblasti výpočtovej techniky.

[2] Marin Mersenne (8. septembra 1588 - 1. septembra 1648) bol francúzsky matematik, filozof, teológ a hudobný teoretik. Je považovaný za otca fyzikálnej oblasti zaoberajúcej sa akustikou. Študoval v meste Le Mans a neskôr na jezuitskom kolégiu v La Fléche. Po štúdiách teológie a hebrejčiny sa stal Mersenne v roku 1613 mníchom.

[3] Ešte v apríli roku 2009 bolo známych iba 46 takýchto prvočísel.

[4] Viď skriptá [S2, Lema 2.4.5]

Dôkaz. Nech $j = n.k$ a $U_k = \frac{\varphi_1^k - \varphi_2^k}{\varphi_1 - \varphi_2}$. Potom

$$U_{n.k} = \frac{\varphi_1^{n.k} - \varphi_2^{n.k}}{\varphi_1 - \varphi_2} = \frac{(\varphi_1^k)^n - (\varphi_2^k)^n}{\varphi} = \\ = \frac{(\varphi_1^k - \varphi_2^k)(\varphi_1^{(n-1)k} + \varphi_1^{(n-2)k}\varphi_2 + \ldots + \varphi_1\varphi_2^{(n-2)k} + \varphi_2^{(n-1)k})}{\varphi_1 - \varphi_2}.$$

Vidíme, že prvá zátvorka nám dáva spoločne s menovateľom postupnosť U_k. Nám teda treba iba ukázať, že druhá zátvorka je celé číslo.

Keď však zoberieme postupne jednotlivé členy v zátvorke a im prislúchajúce členy idúce od konca, dostaneme:

$$\underbrace{(\varphi_1^{(n-1)k} + \varphi_2^{(n-1)k})}_{V_{(n-1)k}} + \underbrace{(\varphi_1^{(n-2)k}\varphi_2 + \varphi_2^{(n-2)k}\varphi_1)}_{bV_{(n-2)k-1}} + \ldots$$

Posledný "prostredný" člen (pre n-nepárne; pre n-párne by sme prostredné dva členy spárovali rovnako ako v predchádzajúcom prípade) je $\varphi_1^{\frac{(n-1)}{2}k}\varphi_2^{\frac{(n-1)}{2}k}$, čo je vlastne $b^{\frac{n-1}{2}k}$. Z tohto a z poznatku, že postupnosť V_n je postupnosť celých čísel, vidno, že v druhej zátvorke je celé číslo. □

Veta 7.1.1. *Ak NSD*$(n, 2b\triangle) = 1$ *potom platí nasledovné*

$$U_j \equiv 0 \pmod{n} \text{ práve vtedy, keď } j \equiv 0 \pmod{r_{f(n)}}.$$

Dôkaz. Implikácia $''\Leftarrow''$ je zrejmá. Jej dôkaz by sme previedli spôsobom takmer identickým tomu, ktorým sme dokázali predchádzajúce tvrdenie 7.1.1.

Dokážeme si obrátenú implikáciu:

$$\text{Ak } U_j \equiv 0 \pmod{n}, \text{ tak potom } j \equiv 0 \pmod{r_{f(n)}}.$$

Najprv si dôkaz ukážeme pre Fibonacciho postupnosť (4.1). Platí totiž nasledujúci vzťah[5]:

$$F_{m+n} = F_m F_{n-1} + F_{m+1}F_n. \tag{7.1}$$

Pre Fibonacciho postupnosť sa tiež napr. matematickou indukciou dá ukázať, že dva po sebe idúce členy Fibonacciho postupnosti sú navzájom nesúdeliteľné, teda $\text{NSD}(F_n, F_{n+1}) = 1$.

Poďme teda dokázať uvedenú implikáciu pre Fibonacciho postupnosť. Majme $U_j \equiv 0 \pmod{n}$. Zapíšme teda j ako $p.r_{f(n)} + z$, pričom našou úlohou bude ukázať, že zvyšok z je nulový. Využijeme teda (7.1):

$$\underbrace{F_{p.r_{f(n)}+z}}_{\text{deliteľné } n} = \underbrace{F_{p.r_{f(n)}}F_{z-1}}_{\text{deliteľné } n} + F_{p.r_{f(n)}+1}F_z.$$

Z tohto nám vyplýva, že aj $F_{p.r_{f(n)}+1}F_z$ musí byť deliteľné n.

$$\left.\begin{array}{l} n \mid U_{p.r_{f(n)}+1}U_z \\ \text{NSD}(U_{p.r_{f(n)}+1}, U_{p.r_{f(n)}}) = 1 \end{array}\right\} n \mid U_z \Rightarrow z = 0.$$

[5] Dôkaz pre Fibonacciho postupnosť je len na ilustráciu, tento vzťah si nebudeme dokazovať.

Keďže $z < r_{f(n)}$ a zároveň $r_{f(n)} = r$ je najmenšie také číslo (okrem nuly), že $U_r \equiv 0 \pmod{n}$, tak z musí byť nula.

Všeobecný dôkaz je dosť podobný.

$$U_{n+m} = U_n U_{m+1} - bU_m U_{n-1}, \text{ pretože}$$
$$U_n U_{m+1} - bU_m U_{n-1} = \frac{\varphi_1^n - \varphi_2^n}{\varphi_1 - \varphi_2}\frac{\varphi_1^{m+1} - \varphi_2^{m+1}}{\varphi_1 - \varphi_2} - b\frac{\varphi_1^m - \varphi_2^m}{\varphi_1 - \varphi_2}\frac{\varphi_1^{n-1} - \varphi_2^{n-1}}{\varphi_1 - \varphi_2} =$$
$$= \frac{\varphi_1(\varphi_1^{n+m} - \varphi_2^{n+m}) - \varphi_2(\varphi_1^{n+m} - \varphi_2^{n+m})}{(\varphi_1 - \varphi_2)^2} = U_{n+m}.$$

Ďalej matematickou indukciou ukážeme, že pre všetky $k \geq 0$ je $\mathrm{NSD}(U_k, U_{k+1}, n) = 1$. Pre $k = 0$ a tiež pre $k = 1$ tvrdenie triviálne platí.
Nech platí pre všetky $k < l$. Pozrime sa, či platí aj pre l:

Dôkaz prevedieme *sporom*: nech $\mathrm{NSD}(U_{l-1}, U_l, n) \neq 1$. Predpokladajme, že $\mathrm{NSD}(U_{l-1}, U_l, n) = m, m > 1$. Vieme ďalej, že $U_l = aU_{l-1} - bU_{l-2}$. Potom

$$\underbrace{\mathrm{NSD}(U_{l-1}, aU_{l-1} - bU_{l-2}, n)}_{=m} = \mathrm{NSD}(\underbrace{U_{l-1}}_{m.o}, \underbrace{aU_{l-1} - bU_{l-2}}_{m.p}, \underbrace{n}_{m.r}).$$

Z toho ale vyplýva, že aj bU_{l-2} je deliteľné číslom m. Keďže ale $\mathrm{NSD}(b, n) = 1$, čo vyplýva z podmienky, že $\mathrm{NSD}(n, 2b\triangle) = 1$, tak potom musí byť U_{l-2} deliteľné číslom $m \Rightarrow U_{n-2} = m.x$. Z toho ale vyplýva, že $\mathrm{NSD}(U_{l-2}, U_{l-1}, n) = m \neq 1$, čo je v spore s indukčným predpokladom a teda $(U_{l-1}, U_l, n) = 1$.

Teraz už máme vhodný aparát na dôkaz celej vety:
Nech $U_j = U_{p.r_{f(n)}+z} \equiv 0 \pmod{n}$. Teda

$$\underbrace{U_{p.r_{f(n)}+z}}_{\text{deliteľné } n} = \underbrace{U_{p.r_{f(n)}}U_{z+1}}_{\text{deliteľné } n} - bU_z U_{p.r_{f(n)}-1} \Rightarrow bU_z U_{p.r_{f(n)}-1} = n.z$$

Z toho, že $\mathrm{NSD}(U_k, U_{k+1}, n) = 1$ a $\mathrm{NSD}(n, 2b\triangle) = 1$ vyplýva, že $n \mid U_z$. Z tohto už podobne ako v predchádzajúcom dôkaze Fibonacciho postupnosti vyplýva, že $z = 0 \Rightarrow j \equiv 0 \pmod{r_{f(n)}}$. □

Na základe predchádzajúcich úvah a dôkazov dostávame vetu, ktorá súvisí s vetou 4.2.1:

Veta 7.1.2. *Majme funkciu $f = x^2 - ax + b$, jej determinant $\triangle = a^2 - 4b$ a prvočíslo p, ktoré nedelí $2b\triangle$. Potom $r_{f(p)} \mid p - \left(\frac{\triangle}{p}\right)$.*

Teraz sa dostávame k vete, ktorá bude veľmi dôležitá v ďalšej časti, resp. ktorá je dôležitým medzikrokom k tomu, aby sme sa dopracovali k Lucas-Lehmerovej vete a testu. Už pri tejto vete uvidíme, že sa nebudeme zaoberať ani tak číslom n, ako skôr $n + 1$.

Veta 7.1.3 (Morrisonova veta)**.** *Majme f a $\triangle$ zadefinované obvyklým spôsobom. Nech n je prirodzené číslo, pričom platí, že $NSD(n, 2b) = 1, \left(\frac{\triangle}{n}\right) = -1$. Ak je F ľubovoľným deliteľ čísla $n + 1$ a zároveň platia podmienky*

$$U_{n+1} \equiv 0 \pmod{n}, \quad NSD(U_{(n+1)/q}, n) = 1 \text{ pre všetky prvočísla } q \mid F, \quad (7.2)$$

potom pre ľubovoľné prvočíslo p deliace n platí, že $p \equiv \left(\frac{\triangle}{p}\right) \pmod{F}$. Navyše, ak $F > \sqrt{n} + 1$, tak číslo n je prvočíslo.

Dôkaz. Nech p je ľubovoľný prvočíselný deliteľ n. Z podmienok zadefinovaných v (7.2) dostávame, že F delí $r_{f(p)}$. To preto, lebo platí veta 7.1.1, teda $n-1 = r_{f(p)}.Q$, pričom hodnota Q nás teraz nezaujíma. Pre ľubovoľné prvočíslo, ktoré delí F však platí, že $\mathrm{NSD}(U_{(n+1)/q}, n) = 1$, teda prvočíslo muselo predeliť $r_{f(p)}$. Ak by tak totiž nespravilo, potom by $(U_{r_{f(p)}.z}, n) = n$ podľa vety 7.1.1. Využijúc vetu 7.1.2 teda dostávame, že $p \equiv \left(\frac{\triangle}{p}\right) \pmod F$.

Nech $F > \sqrt{n}+1$. Vieme, že $p \equiv \left(\frac{\triangle}{p}\right) \pmod F$, takže $p = F.m + \left(\frac{\triangle}{p}\right)$. Na pravej strane je $m > 0$, pretože v opačnom prípade by rovnosť nemohla platiť (prvočíslo p by totiž muselo byť $+1$ alebo -1). Takže určite platí, že $p \geq F - 1 > \sqrt{n}$. Keďže toto platí pre každé prvočíslo deliace n, musí byť prvočíslo p práve číslom n. □

7.2 Morrisonova veta pre postupnosť V_n

Nasledujúca veta je v istom zmysle analogická ku tej predchádzajúcej.

Veta 7.2.1. *Nech f a $\triangle$ sú zadefinované rovnako ako v predchádzajúcich prípadoch. Nech n je prirodzené číslo, pričom platí, že $NSD(n, 2b) = 1$ a $\left(\frac{\triangle}{n}\right) = -1$. Ak F je párny deliteľ čísla $n+1$ a navyše platia podmienky*

$$V_{F/2} \equiv 0 \pmod n \; NSD(V_{F/2q}, n) = 1 \text{ pre všetky nepárne prvočísla } q \mid F, \tag{7.3}$$

potom pre každé prvočíslo p deliace n platí $p \equiv \left(\frac{\triangle}{p}\right) \pmod F$. Navyše, ak $F > \sqrt{n}+1$, tak n je prvočíslo.

Pri dôkaze tejto vety využijeme jednoduchú rovnosť $U_{2m} = U_m V_m$. Rozpísaním pravej strany rovnice veľmi ľahko dôjdeme k dôkazu rovnosti:

$$\frac{x^m - (a-x)^m}{x-(a-x)}(x^m + (a-x)^m) = \frac{x^{2m} - (a-x)^{2m}}{x-(a-x)}.$$

Dôkaz vety 7.2.1. Nech p je nepárne prvočíslo, ktoré delí obe postupnosti U_m, V_m. Obe postupnosti (4.3) a (1.1) sú ekvivalentné a hneď vieme povedať, že $x^m \equiv (a-x)^m \pmod{f(x), p}$ a tiež $x^m \equiv -(a-x)^m \pmod{f(x), p}$. Z toho potom vyplýva (pretože sme v poli), že $x^m \equiv 0 \pmod{f(x), p}$. Potom aj $b^m = (x(a-x))^m \equiv 0(\pmod{f(x), p})$, z čoho dostávame, že $p \mid b$.

V nasledujúcej časti si ukážeme, že

$$\mathrm{NSD}(U_{2m}, n) = \mathrm{NSD}(U_m, n).\mathrm{NSD}(V_m, n), \tag{7.4}$$

čo vyplýva z toho, že $p \mid b$, $\mathrm{NSD}(n, 2b) = 1$ a $U_{2m} = U_m V_m$:
$\mathrm{NSD}(U_{2m}, n) = \mathrm{NSD}(U_m V_m, n)$. Nech

$$\begin{aligned} U_m &= p_1^{\alpha_1} \ldots . p_t^{\alpha_t} \\ V_m &= p_1^{\beta_1} \ldots . p_t^{\beta_t} \\ n &= p_1^{\gamma_1} \ldots . p_t^{\gamma_t}, \end{aligned}$$

pričom jednotlivé p_i sú všetky prvočísla, ktoré sa vyskytujú v kanonickom rozklade ľubovoľného výrazu.

Pre ľubovoľné prvočíslo $p_i, i \in \{1, \ldots, t\}$ zoberieme do $\mathrm{NSD}(U_{2m}, n)$ ako exponent $\min\{\alpha_i + \beta_i, \gamma_i\}$.
Ak je nejaké p_i v niektorej postupnosti U_m alebo V_m nulové, tak pre to p_i daná rovnosť (7.4) triviálne platí. Ak by však p_i v postupnosti U_m aj V_m bolo nenulové, potom by muselo byť nulové v n. To preto, lebo $p_i \mid U_m, U_n$. Z toho podľa vyššie uvedeného $p_i \mid b$. Ak by však p_i delilo aj n, tak je to spor s tým, že $\mathrm{NSD}(n, 2b) = 1$. Vidíme teda, že aj v takomto prípade uvedená rovnosť (7.4) platí.

Z prvej podmienky v (7.3) dostávame, že $U_F \equiv 0 \pmod{n}$, pretože $U_F = U_{F/2}V_{F/2} \Rightarrow U_{n+1} \equiv 0 \pmod{n}$.

Tiež platí, že $\mathrm{NSD}(U_{F/2}, n) = 1$, pretože $\mathrm{NSD}(U_{F/2}, n) \mid \mathrm{NSD}(U_{F/2}, V_{F/2})$. Ak by $\mathrm{NSD}(U_{F/2}, n) \neq 1$, potom by existovalo prvočíslo p nachádzajúce sa v kanonickom rozklade $U_{F/2}$ aj n. Teda $p \mid \mathrm{NSD}(U_{F/2}, V_{F/2})$. My sme si ale ukázali, že potom by platilo $p \mid b$, z čoho jasne vyplýva $p \mid 2b$. To by však bolo v spore s tým, že $\mathrm{NSD}(n, 2b) = 1$.

Nech q je ľubovoľný nepárny deliteľ F. Opäť využijeme poznatok, že $U_{F/q} = U_{F/2q}V_{F/2q}$. Podľa tvrdenia 7.1.1 vieme, že keďže $F/2q \mid F/2$, tak $U_{F/2q} \mid U_{F/2}$. Keďže $\mathrm{NSD}(U_{F/2}, n) = 1$, tak potom aj $\mathrm{NSD}(U_{F/2q}, n) = 1$. Z druhej podmienky (7.3) teda dostávame, že $\mathrm{NSD}(U_{F/q}, n) = 1$.

Splnili sme teda všetky podmienky vety Morrisonovej vety (7.2), teda platia jej závery. □

7.3 Lucas-Lehmerov test

Tvrdenie 7.3.1. *Platí nasledovná rovnosť:* $V_{2j} = V_j^2 - 2b^j$.

Dôkaz. Podľa Vietových vzťahov platí, že $\varphi_1\varphi_2 = b$. Z tohto dostaneme:

$$V_j^2 - 2b^j = (\varphi_1^j + \varphi_2^j)^2 - 2b^j = \varphi_1^{2j} + \varphi_2^{2j} + 2\varphi_1^j\varphi_2^j - 2b^j = V_{2j}.$$

□

Pred samotným testom si uvedieme vetu, ktorá je kľúčom k danému testu. Pri jej dokazovaní využijeme predchádzajúcu vetu 7.2.1.

Veta 7.3.1 (Lucas-Lehmerova veta pre Mersennove prvočísla)**.** *Uvažujme postupnosť* $v_k, k = 0, 1 \ldots$ *rekurentne zadanú takto:* $v_0 = 4, v_{k+1} = v_k^2 - 2$. *Ak je* p *nepárne prvočíslo, potom platí, že Mersennovo číslo* $M_p = 2^p - 1$ *je prvočíslo práve vtedy, keď* $v_{p-2} \equiv 0 \pmod{M_p}$.

Dôkaz. $''\Leftarrow''$: Majme funkciu $f(x) = x^2 - 4x + 1$, ktorej diskriminant $\triangle = 4^2 - 4 = 12$. Dá sa ľahko ukázať (napr. matematickou indukciou), že $M_p \equiv 3 \pmod 4$ a $M_p \equiv 1 \pmod 3$. V našom prípade platí, že $\left(\frac{\triangle}{M_p}\right) = \left(\frac{12}{M_p}\right) = \left(\frac{3}{M_p}\right)$, pretože platí veta 1.2.1 a $\left(\frac{4}{M_p}\right)$ je 1 (vďaka tomu, že $4 = 2^2$ je štvorec).

Opäť raz využijeme zákon o kvadratickej reciprocite (1.2), z ktorého dostávame nasledovné:

$$\left(\frac{3}{M_p}\right)\left(\frac{M_p}{3}\right) = (-1)^{\frac{(3-1)(M_p-1)}{4}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1.$$

Ako sme si už vyššie uviedli, $M_p \equiv 1 \pmod 3$ a $1 = 1^2$ je štvorec, teda $\left(\frac{3}{M_p}\right) = -1 \Rightarrow \left(\frac{\triangle}{M_p}\right) = -1$.

Použijeme vetu 7.2.1, v ktorej za F dosadíme $2^{p-1} = (M_p + 1)/2$. Musíme overiť, či pre takýto deliteľ spĺňa zadaná postupnosť podmienky danej vety. Druhú podmienku tejto vety overovať nemusím, pretože deliteľ $F = (M_p+1)/2$ nemá žiadnych nepárnych prvočíselných deliteľov. Stačí nám overiť, že $V_{2^{p-2}} \equiv 0 \pmod{M_p}$. Keďže máme funkciu $f(x) = x^2 - 4x + 1$, pre ktorú sa $a = 4$, tak $x(a-x) = x(4-x) \equiv 1 \pmod{f(x)}$.

$$V_{2m} \equiv x^{2m} + (4-x)^{2m} = (x^m + (4-x)^m)^2 - 2x^m(4-x)^m \equiv V_m^2 - 2 \pmod{f(x)}.$$

Máme zadefinované $V_1 = 4 = v_0$. Indukciou si ukážeme, že $V_{2^k} = v_k$:

$$V_{2^k} = V_{2.2^{k-1}} \overset{7.3.1}{\equiv} V_{2^{k-1}}^2 - 2 \overset{IP}{=} v_{k-1}^2 - 2 = v_k.$$

Keďže $v_{p-2} = V_{2^{p-2}} \equiv 0 \pmod{M_p}$, tak sú splnené všetky podmienky vety 7.2.1 a teda M_p je prvočíslo.

$''\Rightarrow''$:

Predpokladajme, že M_p je prvočíslo. Ako sme si ukázali v predchádzajúcom prípade, $\left(\frac{\triangle}{M_p}\right) = -1$. Rovnako ako v prvej časti pri dôkaze vety 4.2.1 teda môžeme písať, že $\mathbb{Z}[x]/(f(x), M_p) \cong$ konečné pole $F_{M_p^2}$. Od tohto momentu budeme používať namiesto označenia M_p už iba M (Spriehľadní nám to totiž zápis). Opäť použijeme Frobeniov automorfizmus a jeho vlastnosti [6] Použijúc ich dostávame, že $x^M \equiv (4-x) \pmod{f(x), M}$. Teraz vypočítame $(x-1)^{M+1}$ dvoma spôsobmi, ktorých výsledky neskôr porovnáme.

1. Máme $(x-1)^2 = x^2 - 2x + 1 = (x^2 - 4x + 1) + 2x \equiv 2x \pmod{f(x), M}$. Z Eulerovho kritéria (1.4) a podľa vetz 1.2.6 dostávame $\left(\frac{2}{M}\right) \equiv 2^{(M-1)/2} = 1 \pmod M$. Pokračujme:

$$(x-1)^{M+1} \equiv ((x-1)^2)^{\frac{M+1}{2}} \equiv (2x)^{(M+1)/2} = \\ = 2.2^{(M-1)/2} x^{(M+1)/2} \equiv 2x^{(M+1)/2} \pmod{f(x), M}.$$

2. Druhý spôsob výpočtu:

$$(x-1)^{M+1} = (x-1)(x-1)^M \overset{(1.2.2)}{\equiv} (x-1)(x^M - 1) \equiv \\ \equiv (x-1)(4-x-1) = (-x^2 + 4x - 3 + 2) - 2 \equiv -2 \pmod{f(x), M}.$$

Predchádzajúce vyjadrenia dáme do rovnosti a dostaneme, že $x^{(M+1)/2} \equiv -1 \pmod{f(x), M}$. Z toho vyplýva, že $x^{2^{p-1}} \equiv -1 \pmod{f(x), M}$ Využijeme náš automorfizmus 1.1.5 a môžeme písať, že $(4-x)^{2^{p-1}} \equiv -1 \pmod{f(x), M}$.

Z dvoch predchádzajúcich výsledkov teda dostávame, že $U_{2^{p-1}} \equiv 0 \pmod M$. Nemôže platiť $U_{2^{p-2}} \equiv 0 \pmod M$, potom by $x^{2^{p-2}} \equiv (4-x)^{2^{p-2}} \pmod{f(x), M}$, z čoho by sme dostali spor:

$$-1 \equiv x^{2^{p-1}} = x^{2^{p-2}}. \equiv x^{2^{p-2}} \equiv x^{2^{p-2}}(4-x)^{2^{p-2}} = (x(4-x))^{2^{p-2}} \equiv 1 \pmod{f(x), M}.$$

[6] Tieto veci sme už používali a dokazovali v 1.2.4, 1.2.5 a 1.2.1.

Už skôr sme ukázali, že platí nasledujúca rovnosť $U_{2^{p-2}} = U_{2^{p-2}}V_{2^{p-2}}$, z ktorej dostávame, že $V_{2^{p-2}} \equiv 0 \pmod{M}$. Už vyššie sme si však ukázali, že $V_{2^{p-2}} = v_{p-2}$, čím sme vlastne dokázali celú vetu. □

Nasleduje už samotný zápis Lucas-Lehmerovho testu:

Algoritmus 7.3.1. Na vstupe dostaneme nepárne prvočíslo p. Nasledujúci algoritmus rozhodne, či Mersennovo číslo $M_p = 2^p - 1$ je prvočíslo alebo je to zložené číslo:

1. Inicializácia
   $v = 4$

2. Lucas-Lehmerova postupnosť
   for $k = 1..p-2$ do $v = v^2 - 2 \pmod{2^p - 1}$

3. Kontrola výsledku
   if$(v == 0)$ return 1 else return 0.

Vidíme teda, že algoritmus vychádza z predchádzajúcej vety 7.3.1 a on len overí, či sú splnené všetky podmienky tejto vety. Tento test je veľmi efektívny a dosiahli sa pomocou neho pekné výsledky. Tento test je o to lepší, že nie iba povie, či je dané Mersennovo číslo pseudoprvočíslo, on dokonca povie, či je dané Mersennovo číslo prvočíslo alebo zložené číslo.

Záver

V práci sme sa snažili prísť na to, čo stojí za rôznymi testami, ktoré sa snažia rozhodnúť, či ide pri danom čísle o prvočíslo alebo zložené číslo. Skúmali sme matematické základy, na ktorých sú postavené jednotlivé testy. Tie využívajú veľké množstvo tvrdení a viet z teórie čísel a algebry. Každé jedno tvrdenie a vetu sme sa snažili dostatočne vysloviť a keď sme niečo nedokazovali, tak sme čitateľovi poskytli odkaz na dostupnú literatúru, v ktorej si dôkaz danej vety môže naštudovať dodatočne. Tvrdenia sme sa snažili sformulovať jasne a nezabúdať popritom ani na poriadne definície. Práca teda ponúka bohatý výklad matematiky v praxi, pričom žiadna využívaná veta nie je zbytočná. Chceli sme a dúfame, že sa nám to aj podarilo, dôsledne opísať aspoň časť z tejto bohatej oblasti matematiky. Keďže je však táto téma veľmi široká, do budúcnosti by sa dali naštudovať a vysvetliť ďalšie testy. Pri snahe o dokázanie niektorých vecí však môžeme prísť na ďalšie a ďalšie poznatky. Veď tak to v matematike chodí - človek pri skúmaní jednej disciplíny objaví množstvo vecí z inej, v ktorej možno ani nie je odborník. Téma prvočíselnosti ponúka širokú paletu možností. Kto však chce vojsť cez privreté dvere, musí si už čo-to s matematikou odžiť.

Literatúra

[B] P. Bachmann. *Niedere Zahlentheorie, 1. Teil.* B. G. Teubner, Leipzig, 1902.

[CP] R. Crandall and C. Pomerance. *Prime Numbers, a Computational Perspective.* Springer-Verlag, New York, 2001.

[G] Jon Grantham. Frobenius pseudoprimes. *Mathematics of Computation*, 70(234):873–891, 2000.

[KLS] M. Křížek, F. Luca, and L. Somer. *17 lectures on Fermat numbers. From number theory to geometry.* Springer, New York, 2001.

[L] F. Lemmermeyer. *Reciprocity laws. From Euler to Eisenstein.* Springer, Berlin, 2000.

[S1] M. Sleziak. *Algebra 2.* `http://thales.doa.fmph.uniba.sk/sleziak/vyuka`, poznámky k prednáške, verzia aktualizovaná 7. mája 2009.

[S2] M. Sleziak. *Teória čísel.* `http://thales.doa.fmph.uniba.sk/sleziak/vyuka`, poznámky k prednáške, verzia aktualizovaná 7. mája 2009.