پردیس علوم
دانشکده ریاضی ، آمار و علوم کامپیوتر

الگوریتم‌های تشخیص اعداد اول و تجزیه اعداد مرکب

نگارنده

محمدرضا معتبر

استاد راهنما: امیر قادرمرزی

پایان‌نامه برای دریافت درجه کارشناسی
در رشته علوم کامپیوتر

تاریخ: اسفند ۱۴۰۲

چکیده

این پایان نامه به بررسی الگوریتم‌های تشخیص اعداد اول[1] و تجزیه اعداد مرکب[2] می پردازد که در شاخه نظریه اعداد، رمزنگاری و علوم کامپیوتر بسیار دارای اهمیت هستند.
ما روش‌های کلاسیک مانند تقسیم آزمایشی[3]، الگوریتم‌های احتمالی مانند آزمون میلر-رابین[4]، و تکنیک‌های پیشرفته‌تر ازجمله الگوریتم‌های فروبینس[5]وAKS[6] و روش‌های مبتنی بر خم‌های بیضوی[7]و ... را تجزیه و تحلیل می‌کنیم.همچنین مبانی نظری، پیچیدگی های محاسباتی، و پیاده سازی های عملی مورد بررسی قرار می‌دهیم.

[1]Ptimality Tests

[2]Factorization methods

[3]Trivial Division

[4]Miller–Rabin

[5]Frobenius test

[6]Agrawal–Kayal–Saxena

[7]Elliptic Curves

فهرست مطالب

فصل ۱

مقدمه

از دیرباز اعداد اول برای ریاضیدانان از اهمیت خاصی برخوردار بوده است، حتی تعمیم این مفهوم در جای جای ریاضی قابل مشاهده است. در دوران مدرن، در حالی که ریاضیدانان همچنان با ژرفای اعداد اول دست و پنجه نرم می کنند، تلاش و منابع گسترده ای به سمت جنبه محاسباتی، تشخیص و شناسایی و به کار بردن اعداد اول در حوزه های دیگر به کار برده شده است.

اگر بخواهیم دقیق باشیم، اعداد بزرگ واقعا وجود ندارند چرا که تمام اعداد را می‌توان کوچک در نظر گرفت. در واقع هیچ اهمیتی ندارد که شما چند رقم یا توان‌های متوالی روی کاغذ بنویسید، قطعا تعداد متناهی عدد از آن عدد کوچک‌تر و نامتناهی عدد از آن بزرگ‌تر هستند. اگر چه با این تعبیر همیشه با اعداد کوچک سر و کار داریم، مداوم در تلاش هستیم تا توان کار کردن با اعدادی را پیدا کنیم که شاید قبلا این کار امکان پذیر نبوده است و پیشرفت چشمگیری داشته باشیم. به طور مثال تعداد ارقام عددی که اکنون توانایی تجزیه آن را داریم در مقایسه با ۳۰ سال گذشته ۸ برابر شده است و تعداد ارقام عددی که می‌توانیم نشان دهیم که آن عدد، عددی اول است ۵۰۰ برابر شده است. توجه کنید که تعداد رقم‌ها چندین برابر شده است یعنی اگر ۳۰ سال پیش می‌توانستیم تشخیص دهیم یک عدد ۱۰ رقمی اول است یا خیر اکنون توانایی تشخیص اول بودن اعداد ۵۰۰۰ رقمی را داریم.

لازم به ذکر است که این پیشرفت هم به دلیل پیشرفت‌های تکنولوژی است و هم به دلیل پیشرفت در طراحی الگوریتم‌ها. قطعا پیشرفت در کیفیت و کمیت ابزارهای سخت افزاری که در اختیار داریم نقش پر رنگی داشته‌اند اما قطعا پیشرفت‌های اخیر فقط به این دلایل نبوده است. اگر مجبور بودیم از الگوریتمی که پیش از سال ۱۹۷۵ میلادی استفاده کنیم حتی با استفاده از بهترین

و قویترین و مجهزترین کامپیوترهای امروزی شاید توانایی تجزیه یک عدد ۴۰ رقمی و یا حتی تشخیص مرکب یا اول بودن آن عدد را نداشتیم.

اما امروزه چه توانایی داریم؟ در حال حاضر قادریم هر عدد ۱۷۰ رقمی دلخواهی را با موفقیت تجزیه کنیم در حالی که می‌توانیم اول بودن یا نبودن اعداد ۱۵۰۰۰ رقمی را مشخص کنیم. یکی از مشهور ترین تجزیه‌ها چالش تجزیه عدد ۱۲۹ رقمی بود که در ستون "بازی‌های ریاضی" آقای مارتین گاردنر[1] در مجله "آمریکایی علمی[2]" بود [۱]. عدد این چالش

$$\begin{aligned}\mathrm{RSA129} = &\text{۱۱۴۳۸۱۶۲۵۷۵۷۸۸۸۸۶۷۶۶۹۲۳۵۷۷۹۹۷۶۱۴۶۶}\backslash\\ &\text{۱۲۰۱۰۲۱۸۲۹۶۷۲۱۲۴۲۳۶۲۵۶۲۵۶۱۸۴۲۹۳۵۷۰}\backslash\\ &\text{۶۹۳۵۲۴۵۷۳۳۸۹۷۸۳۰۵۹۷۱۲۳۵۶۳۹۵۸۷۰۵۰۵۸}\backslash\\ &\text{۹۸۹۰۷۵۱۴۷۵۹۹۲۹۰۰۲۶۸۷۹۵۴۳۵۴۱}\end{aligned}$$

بود که بعدها به عنوان مورد آزمایشی[3] برای سیستم رمز[4] RSA[5] مورد استفاده قرار گرفت. برخی پیشبینی می‌کردند که ۴۰ کوادریلیون[6] سال طول خواهد کشید که عدد RSA129 تجزیه شود. با این حال، در سال ۱۹۹۴ میلادی با استفاده از الگوریتم غربال درجه دوم[7] توسط آتکینز[8]، گراف[9]، لنسترا[10] و لیلند[11] تجزیه شد. تجزیه بدست آمده برای عدد RSA129

---

[1] Martin Gardner

[2] Scientific American

[3] Test case

[4] Cryptosystem

[5] برای اطلاعات بیشتر در مورد این سیستم رمز می‌توانید به فصل ۸ [۲] رجوع کنید.

[6] Quadrillion

[7] Quadratic sieve (QS)

[8] D. Atkins

[9] M. Graff

[10] A. Lenstra

[11] P. Leyland

$$۳۴۹۰۵۲۹۵۱۰۸۴۷۶۵۰۹۴۹۱۴۷۸۴۹۶۱۹۹۰۳۸۹۸۱۳۳۴۱۷۷۶۴۶۳۸۴۹۳۳۸۷۸۴۳۹۹۰۸۲۰۵۷۷$$

$$\times$$

$$۳۲۷۶۹۱۳۲۹۹۳۲۶۶۷۰۹۵۴۹۹۶۱۹۸۸۱۹۰۸۳۴۴۶۱۴۱۳۱۷۷۶۴۲۹۶۷۹۹۲۹۴۲۵۳۹۷۹۸۲۸۸۵۳۳،$$

و پیام "THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE." که توسط سیستم رمز RSA و این عدد رمز شده بود رمز گشایی شد.

در طول دهه گذشته، توانستم تجزیه‌های بسیار دیگری انجام دهیم و به نقاط عطف مرتبط به آن‌ها دست یابیم. به طور مثال با استفاده از الگوریتم NFS[۱۲] توانسته‌ایم عدد RSA-526 که یک عدد ۱۷۴ رقمی است را تجزیه کنیم و توسط یکی از نسخه‌های خاص این الگوریتم[۱۳] عددی ۲۴۸ رقمی را تجزیه کنیم. تعداد این دستاوردها بسیار زیاد است که بیان تمام آن‌ها ممکن نیست. اما خوب است که اشاره کنیم روشی جدید بر پایه خم‌های بیضوی به نام ECM[۱۴] که اکنون قادر است اعدادی که دارای عامل اول حداکثر ۵۹ رقمی هستند را تجزیه کند. سوابق این دستاوردها در [۳] قابل مشاهده هستند و این سایت به طور مداوم بروز رسانی می‌شود.

باز هم، چنین دستاوردهایی تا حدی به دلیل پیشرفت در ماشین آلات و نرم افزار و بخشی به پیشرفت های الگوریتمی است. یکی از فناوری‌های احتمالی آینده - محاسبات کوانتومی[۱۵] - ممکن است منجر به پیشرفت ماشین‌آلات فوق‌العاده‌ای شود که می‌توان تصور کرد در چند دهه آینده، تجزیه اعداد به طور غیرقابل تصوری سریع‌تر از امروز باشد.

اشاره کردیم که اعداد اول در رمزنگاری مدرن[۱۶] - علم رمزگذاری و رمزگشایی پیام‌ها - کاربرد دارند. از آنجایی که بسیاری از سیستم های رمزنگاری به مطالعات اعداد اول، تجزیه اعداد، و مسائل نظریه اعداد مرتبط، وابسته هستند، پیشرفت تکنولوژیکی و الگوریتمی بسیار مهم شده است. توانایی ما برای کشف اعداد اول بزرگ و اثبات اول بودن آن‌ها از توانایی ما برای تجزیه اعداد پیشی گرفته است. این وضعیت به این دلیل برای فعالان حوزه امنیت دارای اهمیت است که تجزیه اعداد به تعبیری به معنای رمزگشایی و اعداد اول بزرگ به معنای رمزگذاری هستند

[12] Number field sieve

[13] SNFS

[14] Elliptic curve method

[15] Quantum computation

[16] Modern cryptography

و از آنجا که تاکنون تواناییمان برای پیدا کردن و ساختن اعداد اول بیشتر از تجزیه اعداد است یعنی می‌توانیم سیستم‌های امنی طراحی کنیم که شاید شکستنشان غیر در حال حاضر غیر ممکن باشد.

در ادامه سعی داریم روی الگوریتم‌های شناخته شده‌تر و پایه‌ای تر در حوزه تشخیص اعداد اول و تجزیه اعداد تمرکز کنیم. اما برای روشن کردن، توجیه و تأکید بر اهمیت عملی الگوریتم‌های محاسباتی، اغلب در حوزه نظری نیز عمیق می‌شویم و الگوریتم ها را همراه با اثبات درستی، تحلیل و مطالب مورد نیاز بررسی می‌کنیم.

فصل ۲

شناسایی اعداد اول و مرکب

احتمالا بارها پیش آمده است که به عددی برخورد کرده باشید و برایتان سوال شده باشد که آیا این عدد اول است یا خیر. اگر آن عدد کوچک باشد به راحتی می‌توان اول بودنش را بررسی کرد ولی اگر آن عدد بسیار بزرگ باشد، چگونه می‌توان اول یا مرکب بودن ععد مدنظرمان را بررسی کنیم؟

۲-۱ تقسیم آزمایشی

با توجه به تعریف اعداد اول شاید اولین و ساده ترین روشی که به ذهن برسد تقسیم عدد داده شده بر تمام اعداد کوچک تر از آن باشد. در این صورت اگر هیچ ،مقسوم علیهی به جز خودش و عدد یک برای عدد داده شده یافت نشود آنگاه آن عدد، عددی اول است.

۲-۱-۱ تشخیص بخش پذیری

طبیعتاً برای این که بفهمیم عدد n بر عددی مثل a بخش پذیر است کافیست n را بر a تقسیم کنیم؛ اگر باقیماندهٔ تقسیم برابر صفر شود به این معناست که n بر a بخش پذیر است. ولی از آن جا که همیشه سعی بر آن است که پیچیدگی زمانی الگوریتم‌ها را به حداقل برسانیم این سوال پیش می‌آید که آیا روش سریع تری برای تشخیص بخش پذیری وجود دارد یا خیر.
به طور مثال برای تشخیص بخش پذیری بر عدد ۲ نیازی به انجام دادن عملیات تقسیم نیست و تنها

با بررسی زوجیت یکان عدد n بخش پذیری یا عدم بخش پذیری عدد n بر عدد ۲ نتیجه می‌شود. چنین روش‌های مشابه کوتاه و سریع برای تشخیص بخش پذیری بر اعداد ۳، ۵ و ۹ نیز مرسوم هستند ولی با بزرگ‌تر شدن مقسوم علیه پیچیدگی زمانی این روش ها نیز افزایش پیدا می‌کند و عملا از لحاض پیچیدگی نظری و زمانی، تفاوت چندانی با انجام کامل عملیات تقسیم ندارند.
از آنجا که انجام عملیات تقسیم جامع است به این معنا که روند مشخص و مستقلی نسبت به مقسوم علیه دارد، برتری قابل توجهی نسبت به استفاده از روش‌های خاص که مختص به هر عدد هستند، دارد.از این رو در پیاده سازی و چه بسا انجام تقسیم روی کاغذ استفاده از آن ارجحیت دارد.

۲-۱-۲ تقسیم آزمایشی

در روش تقسیم آزمایشی، با استفاده از تقسیم پیاپی عدد داده شده $n_۱$ بر اعداد اول کوچک تر از آن سعی می‌شود بخشی از تجزیه عدد $n_۱$ به عوامل اولش بدست آید.
فرض کنید اعداد اول به ترتیب $p_۱ = ۲, p_۲, p_۳, \dots$ مرتب شده باشند. در مرحله i، عدد n_i را بر عدد اول iام یعنی p_i آنقدر تقسیم می‌کنیم تا عدد n_i عامل p_i دیگری نداشته باشد یا به عبارت دیگر با انجام تقسیم‌های پیاپی بزرگترین عدد α_iای را می‌یابیم که عدد n_i بر $p_i^{\alpha_i}$ بخش پذیر باشد ولی بر $p_i^{\alpha_i+۱}$ بخش پذیر نباشد. در این صورت میتوان n_i را به صورت $p_i^{\alpha_i} \times n_{i+۱}$ نوشت که $n_{i+۱}$ بر p_i بخش پذیر نیست و الگوریتم را ادامه داد.
احتمالا شهود الگوریتم برایتان واضح است در هر مرحله سعی می‌شود تمام عامل اول متناظر با آن مرحله از بخش تجزیه نشده $n_۱$ استخراج شود. البته با کمک استقرا و نماد گذاری بالا این ادعا را می‌توان به طور دقیق اثبات کرد همچنین نشان داد در مرحله iام می‌توان عدد $n_۱$ را به صورت $n_۱ = p_۱^{\alpha_۱} \times p_۲^{\alpha_۲} \times \cdots \times p_i^{\alpha_i} \times n_{i+۱}$ نوشت. که $n_{i+۱}$ همان قسمت تجزیه نشده عدد $n_۱$ در انتهای مرحله iام است. علاوه بر این می‌توان نشان داد که عدد n_i هیچ عامل اولی بین اعداد $p_۱, \dots, p_{i-۱}$ ندارد چرا که اگر داشته باشد با خاصیت بزرگترین بودن α_iها در تناقض است.
حال روند الگوریتم به خوبی مشخص است اما سوال این جاست که این الگوریتم تا کجا باید ادامه پیدا کند و متوقف شود. برای جواب به این سوال لم زیر را ثابت می‌کنیم.

لم ۲-۱. *اگر عدد n هیچ عامل اول کوچک‌تر یا مساوی مجذورش نداشته باشد، عددی اول است.*

اثبات. برهان خلف، فرض کنید عدد n عددی اول نباشد و مقسوم علیه اول p داشته باشد. در این صورت طبق فرض خلف عدد n مرکب و با p برابر نیست. در نتیجه عامل اول دیگر بزرگتر از مجذورش مثل q باید داشته باشد. بدون از دست دادن کلیات مسئله فرض کنید $p \leq q$. در این

صورت از آنجا که $p > \sqrt{n}$ پس $n \geq pq \geq p^۲ > n$ و این تناقض است. در نتیجه فرض خلف باطل و حکم لم برقرار است. $\square$

با توجه به لم بالا و اینکه عدد n_i در مرحله iام هیچ عامل اولی کوچک تر از p_i ندارد هرگاه $p_i > \sqrt{n_i}$ می‌توان نتیجه گرفت که n_i اول است و تجزیه عدد داده شده $n_۱$ به طور کامل به دست آمده است. البته حالت دیگری برای اتمام الگوریتم وجود دارد و آن این است که در مرحله‌ای، n_i برابر ۱ شود.

به طور مثال فرض کنید می‌خواهیم تجزیه عدد $n_۱ = ۷۳۹۹$ را با این الگوریتم بدست آوریم. با بررسی اعداد ۲، ۳و ۵ (نخستین ۳ عدد اول) در می‌یابیم که عدد $n_۱$ بر این اعداد بخش پذیر نیست و درنتیجه $n_۱ = n_۲ = n_۳ = n_۴$.

عدد اول بعدی ۷ است. با تقسیم $n_۴$ بر ۷ خارج قسمت ۱۰۵۷ و باقیمانده ۰ حاصل می‌شود پس ۷ یکی از عوامل اول عدد $n_۴$ است. از آن جا که در این مرحله باید تمام عامل ۷ را استخراج کنیم باید دوباره ۷ را روی خارج قسمت بررسی کنیم. با بررسی مجدد ۷ مشاهده می‌شود که ۱۰۵۷ نیز بر ۷ بخش پذیر است و عامل ۷ دیگری در $n_۴$ وجود دارد. در تقسیم عدد ۱۰۵۷ بر ۷ خارج قسمت ۱۵۱ بدست می‌آید. در ادامه با تقسیم عدد ۱۵۱ بر ۷ متوجه می‌شویم که عدد ۱۵۱ بر ۷ بخش پذیر نیست و $n_۵ = ۱۵۱$ و $n_۴ = ۷^۲ \times n_۵$. حال با رفتن به مرحله بعد و در نظر گرفتن عدد اول بعدی یعنی ۱۱ الگوریتم را ادامه می دهیم. با انجام تقسیم متوجه می‌شویم که عدد ۱۵۱ بر ۱۱ نیز بخش پذیر نیست و $n_۶$ هم همان عدد ۱۵۱ است. عدد اول بعدی ۱۳ است که از مجذور عدد ۱۵۱ بیشتر است و بنا بر مطالب گفته شده عدد ۱۵۱ اول و الگوریتم به پایان رسیده است.

با کنار هم قرار دادن روابط بدست برای n_i ها تجزیه کامل عدد $n_۱$ به صورت $n_۱ = ۷^۲ \times ۱۵۱$ بدست می‌آید.

احتمالا برایتان سوال شده است که اعداد اول p_i چگونه بدست می‌آیند. با این که الگوریتم‌هایی برای این منظور وجود دارند که در ادامه آن ها را نیز بررسی می‌کنیم، ولی می‌توانیم در این الگوریتم مشکل بدست آوردن p_iها را به گونه‌ای دور بزنیم.

کافیست از مرحله ۱، با در نظر گرفتن عدد $i + ۱$ برای مرحله i الگوریتم را اجرا کنیم. از آن جا که هر عدد اول، قبل از تمام اعداد مرکب شامل آن (ضرایب آن عدد اول) ظاهر می‌شود تنها در مراحلی که عدد متناظرشان عددی اول است باقیمانده صفر می‌شود و عدد n_i با $n_{i+۱}$ متمایز می‌شود. پس الگوریتم دقیقا مشابه حالت قبل عمل میکند و تنها به واسطهٔ تست‌های بخش پذیری اضافه‌ای که برای اعداد مرکب انجام می‌شود کندتر است ولی دیگر نیازی به پیدا کردن اعداد اول نیست. البته می‌توان این روند را کمی بهبود بخشید؛ اینگونه که تنها عدد ۲ و اعداد فرد را در مراحل برسسی

کنیم چرا که می‌دانیم تمام اعداد زوج به جز ۲ مرکب هستند.

شبه کد این الگوریتم به صورت زیر است:

الگوریتم ۱ تقسیم آزمایشی

این الگوریتم برای عدد $n > 1$ داده شده، چندمجموعه $\mathcal{F}$ شامل تمام اعداد اولی که n را عاد می‌کنند را بدست می‌آورد (یک ”چند مجموعه“، یک مجموعه است با این تفاوت که اعضایش می‌توانند تکرار شوند).

[تقسیم بر دو]

$\mathcal{F} = \{\}$
$N = n$
while $2|N$ **do**
    $N = N/2$
    $\mathcal{F} = \mathcal{F} \cup \{2\}$

[حلقه اصلی تقسیم]

$d = 3$
while $d^2 \leq N$ **do**
    while $d|N$ **do**
        $N = N/d$
        $\mathcal{F} = \mathcal{F} \cup \{d\}$
    $d = d + 2$
if $N == 1$ **then return** $\mathcal{F}$
return $\mathcal{F} \cup \{N\}$

لازم به ذکر است که حذف اعداد زوج، پیچیدگی زمانی الگوریتم را تغییر نمی‌دهد و تنها تقریباً سرعت الگوریتم را دو برابر می‌کند. حذف اعداد زوج را می‌توان به این شکل تعمیم داد که باقیمنده تقسیم اعداد اول بزرگ تر از ۳ بر ۶ یا ۱ است یا ۵، پس می‌توانیم فقط اعداد به این فرم را بررسی کنیم و به جای این که متغیر d در شبه کد را هر بار ۲ واحد افزایش دهیم تا روی اعداد فرد حرکت کند با شروع از ۵ یکی در میان d را ۲ و ۴ واحد افزایش دهیم تا روی اعداد با باقیمانده ۱ و ۵ در تقسیم بر ۶ حرکت کند. این فرایند را میتوان به باقیمانده بر اعداد بزرگتر از ۶ نیز تعمیم داد اما پیچیدگی تحلیل باقیمانده اعداد اول بر اعداد بزرگ و پیچیدگی پیاده سازی آن به صورت بسیار سریعی رشد می‌کند که با توجه به مزیت کمی که دارد و تغییر نیافتن پیچیدگی زمانی الگوریتم، ارزش انجام و پیاده سازی ندارد.

۲-۱-۳ ملاحظات عملی

با این که این الگوریتم بسیار ابتدایی است، زمانی که n زیادی بزرگ نباشد استفاده از آن کاملا منطقی به نظر می‌رسد. اما بزرگ بودن یک عدد صفتی کیفیست و متناسب با قدرت پردازشی که در اختیار داریم و مدت زمانی که انتظار داریم که الگوریتم به ما پاسخ دهد سنجیده می‌شود. امروزه به نظر می‌رسد برای بدست آوردن تجزیه کامل اعداد حداکثر ۲۰ رقمی می‌توان از این الگوریتم استفاده کرد و این الگوریتم عملکردی قابل قبول دارد.
البته همان طور که در ابتدا گفته شد از این الگوریتم می‌توان به منظور بدست آوردن بخشی از تجزیه عدد داده شده n استفاده کرد به عبارت دیگر با محدود کردن تعداد مراحل الگوریتم تمام توان‌های اعداد اول ظاهر شده در تجزیه کامل عدد n تا آن مرحله را بدست می‌آورد.

تعریف ۲-۲. *عدد طبیعی n را Bـ هموار[1] نامیم هرگاه تمام عامل های اول ظاهر شده در تجزیه عدد n به اعداد اول، کوچکتر یا مساوی B باشند.*

با توجه به تعریف اعداد Bـ هموار و مطالب بالا از این الگوریتم می‌توان برای مشخص کردن Bـ هموار بودن یا نبودن عدد داده شده استفاده کرد. برای این منظور می‌توان الگوریتم تقسیم آزمایشی را برای اعداد اول کوچک تر از B اجرا کنیم و اگر عدد داده شده به صورت کامل تجزیه شد، به این معناست که هیچ عامل اولی بزرگ تر از B ندارد و Bـ هموار است و در غیر این صورت اینگونه نیست. علاوه بر این، این الگوریتم نه تنها Bـ هموار بودن یا نبودن را مشخص می‌کند بلکه تجزیه آن بخش از عدد داده شده که شامل اعداد اول کوچک تر از B هست را نیز نتیجه می‌دهد.

۲-۱-۴ ملاحظات نظری

از الگوریتم تقسیم آزمایشی می‌توان برای مشخص کردن اول بودن یا نبودن عدد داده شده نیز استفاده کرد. کافیست الگوریتم را اجرا کنیم هر گاه عامل اولی برای عدد داده شده پیدا شد نتیجه می‌گیریم عدد داده شده مرکب بوده است و اگر الگوریتم بدون پیدا کردن عامل اولی برای عدد داده شده به پایان رسید به این معناست که آن عدد اول است.
ابتدا فرض کنید می‌خواهیم اول بودن یا نبودن عدد داده شده n را با استفاده از الگوریتم تقسیم آزمایشی مشخص کنیم. با توجه به مطالب گفته شده می‌دانیم این الگوریتم نهایتا اعداد اول کوچک‌تر یا مساوی مجذور n را بررسی می‌کند. در نتیجه بدترین حالت، زمانی اتفاق می‌افتد

[1] B-smooth

که دقیقا همه این اعداد بررسی شوند یا به صورت معادل، n خود عددی اول باشد.
اگر به جای بررسی تمام اعداد کوچک‌تر یا مساوی مجذور n تنها اعداد اول این بازه را بررسی کنیم تعداد بررسی‌های انجام شده با توجه به قضیه اعداد اول تقریباً برابر $2\sqrt{n}/\ln n$ است. و اگر تنها عدد ۲ و اعداد زوج را بررسی کنیم تعداد بررسی‌ها برابر $\frac{1}{2}\sqrt{n}$ می‌شود. همچنین اگر از تعمیم گفته شده استفاده کنیم، یعنی مانند آنچه که پیش‌تر گفته شد به جای بررسی عدد ۲ و اعداد فرد، بعد از عدد ۵ اعدادی که باقیمانده ۱ یا ۵ بر ۶ دارند را بررسی کنیم یا حتی این موضوع را به باقیمانده اعداد اول بر اعداد بزرگ‌تر تعمیم دهیم، ثابت $\frac{1}{2}$ در تعداد بررسی‌ها با ثابت کوچک‌تری جایگزین می‌شود.
حال اگر بخواهیم از این الگوریتم برای پیدا کردن تجزیه کامل عدد داده شده n استفاده کنیم پیچیدگی زمانی الگوریتم در بدترین حالت همچنان همان $\sqrt{n}$ باقی می‌ماند. به طور مثال باز هم اگر n اول باشد هیچ تقسیمی صورت نمی‌گیرد و تنها تمام اعداد کوچک‌تر یا مساوی مجذور n بررسی می‌شوند و اگر n مرکب باشد تعداد تقسیم‌های انجام شده حداکثر برابر $\log_2 n$ است و حداکثر تمام اعداد کوچک‌تر یا مساوی مجذور عدد n بررسی می‌شوند پس تعداد کل عملیات‌ها برابر $\log_2 n + \sqrt{n}$ است که از نظر پیچیدگی زمانی این همان پیچیدگی زمانی $\sqrt{n}$ است.

۵-۱-۲ غربال

یکی از روش‌هایی که می‌توان اعداد اول را شناسایی کرد و برای روش تقسیم آزمایشی و یا اهداف دیگر به کار برد، الگوریتم غربال است که عموما با اسم غربال اراتوستن[۲] شناخته می‌شود.
این الگوریتم علی رغم سادگی، روشی بسیار سریع برای شناسایی اعداد اول در یک بازه است. البته بهینه سازی‌هایی می‌توان انجام داد تا این الگوریتم برای اعداد و بازه‌های بزرگ عملکرد بهتری داشته باشد. از این الگوریتم برای شناسایی اعداد Bـ هموار و تحلیل برد یک تابع چندجمله‌ای نیز می‌توان استفاده کرد.
برای جزئیات و مطالب بیشتر به [۲] مراجعه کنید.

[2] Sieve of Eratosthenes

۲-۲ اعداد شبه اول

فرض کنید قضیه‌ای به شکل "اگر n اول باشد، آنگاه S برای عدد n برقرار است" داریم که S گزاره‌ای است که به راحتی برای عدد داده شده قابل ارزش گذاری باشد.
حال فرض کنید می‌خواهیم مشخص کنیم عدد بزرگ داده شده اول است یا مرکب. می‌توانیم از قضیه‌ای که در اختیار داریم کمک بگیریم، به این شکل که ارزش گزاره S را برای آن عدد بدست آوریم. اگر ارزش گزاره غلط بود به این معناست که آن عدد نمی‌تواند عددی اول باشد و نتیجه می‌گیریم عدد داده شده عددی مرکب است. اما اگر ارزش گزاره درست باشد چه می‌توان گفت؟ در این صورت از آنجا که قضیه‌ای که دارم یک طرفه است نمی‌توان در مورد اول یا مرکب بودن عدد داده شده تصمیمی بگیریم، اما می‌توانیم از مفهوم Sـشبه‌اول استفاده کنیم که به عددی مرکب که گزاره S برای آن صادق است اتلاق می‌شود.
یک مثال ساده برای مطالب فوق قضیه‌ی "اگر n اول باشد آنگاه یا ۲ است یا فرد" است. بررسی برابر ۲ یا فرد بودن برای عدد داده شده بسیار ساده است و می‌توان از این قضیه برای محک اول بودن استفاده کرد. اما این محک، محک بسیار ضعیفی است چرا که تنها اعداد زوج به جز ۲ را به عنوان اعداد مرکب شناسایی می‌کند و به عبارتی اعداد شبه اولی که این تست معرفی می‌کند در قیاس با اعداد اول بسیار زیاد هستند.
در نتیجه برای این که مفهوم "شبه اول"، مفهومی کاربردی باشد باید به معنایی تعداد اعداد شبه‌اولی که معرفی می‌شوند در مقایسه با اعداد اول زیاد نباشند.

۲-۲-۱ الگوریتم نردبان دودویی

از آن جا که به توان رساندن در بسیاری از موضوعاتی که در ادامه مطرح می‌کنیم کاربرد دارد، خوب است یکی از بهترین الگوریتم‌ها برای این منظور را بررسی کنیم.
فرض کنید می‌خواهیم عدد دلخواه a را به توان عدد n برسانیم. میدانیم اگر n عددی زوج باشد آنگاه $a^n = a^{n/۲} \cdot a^{n/۲}$ و اگر n عددی فرد باشد $a^n = a^{(n-۱)/۲} \cdot a^{(n-۱)/۲} \cdot a$. با توجه به این موضوع می‌توان عملیات توان را به صورت بازگشتی پیاده سازی کرد. همچنین از آنجا که در هر مرحله شاخه بازگشت بر اساس زوجیت n تایین می‌شود می‌توان دید که این الگوریتم ارتباط تنگاتنگی با نمایش مبنای ۲ عدد n دارد.

الگوریتم ۲ نردبان دودویی

این تابع با ورودی اعداد صحیح aو n که $0 \leq n$ مقدار a^n را محاسبه می‌کند.

```
function Pow(a, n):
    if n ≡ 0 (mod 2) then
        temp = Pow(a, n/2)
        return temp · temp
    if n ≡ 0 (mod 2) then
        temp = Pow(a, (n − 1)/2)
        return temp · temp · a
```

با توجه به این که در هر مرحله تابع بازگشتی با نصف مقدار n صدا زده می‌شود، عمق شاخه بازگشتی حداکثر $\lg n$ است. با توجه به شبه‌کد در هر مرحله یا ۱ ضرب انجام می‌شود و یا ۲ ضرب پس تعداد کل ضرب‌های انجام شده حداکثر برابر $2\lg n$ است. همچنین اگر بخواهیم این توان را در پیمانه عددی مثل p محاسبه کنیم کافیست در هر مرحله و بعد از هر ضرب، حاصل را به پیمانه p محاسبه کنیم.

۲-۲-۲ شبه‌اول فرما

این که باقیمانده اعدد a^b بر n به راحتی و بسیار سریع قابل محاسبه است پایه بسیاری از الگورتم‌های تجزیه اعداد و تشخیص اول بودن و به طور کلی الگوریتم‌های نظریه اعدادی است.
از جمله این الگوریتم‌ها که از این محاسبه سریع بهره می‌گیرد، بررسی اول بودن با استفاده از قضیه کوچک فرما است.

قضیه ۲-۳. *(قضیه کوچک فرما)*[3]*. اگر عدد n عددی اول باشد آنگاه به ازای هر عدد a داریم*

$$a^n \equiv a \ (\text{پیمانه‌ی } n) \tag{۲-۱}$$

اثبات‌های زیاد و متنوعی برای این قضیه ازجمله بررسی بسط دو جمله‌ای $(a+1)^n$ وجود دارد.
اگر a نسبت به n اول باشد می‌توانیم دو طرف عبارت ۲-۱ را در وارون ضربی a ضرب کنیم و

[3] Fermat's little theorem

عبارت

$$a^{n-۱} \equiv ۱ \ (\text{پیمانه‌ی } n) \qquad (۲-۲)$$

را بدست آوریم. در نتیجه ۲-۲ برای هر عدد اول n و عدد a که بر n بخش پذیر نباشد برقرار است.
در این صورت عدد مرکب n را "شبه‌اول فرما[۴]" در پایه a نامیم هرگاه ۲-۱ برای n و a برقرار باشد.
برای مثال $n = ۹۱$ شبه‌اول فرما در پایه ۳ است زیرا ۹۱ عددی مرکب و $۳^{۹۱} \equiv ۳$ (پیمانه‌ی ۹۱).
به طور مشابه عدد ۳۴۱ شبه‌اول فرما در پایه ۲ است. از آنجا که تمام اعداد مرکب، شبه‌اول فرما در پایه یک هستند پس شبه‌اول فرما بودن در پایه ۱ بی‌اهمیت است و در ادامه پایه ۱ را کنار می‌گذاریم و فرض میکنیم $a \geq ۲$.

قضیه ۲-۴. *برای عدد ثابت $a \geq ۲$، تعداد اعداد شبه‌اول فرما در پایه a که کوچک تر یا مساوی x هستند برابر است با $o(\pi(x))$ وقتی $x \to \infty$ (منظور از $\pi(x)$ تعداد اعداد اول کوچک‌تر یا مساوی x است). به عبارتی دیگر تعداد اعداد شبه‌اول فرما در مقایسه با اعداد اول نادر هستند.*

اثبات این قضیه در [۴] آورده شده است و در واقع قضیه ۲-۴ بیان می‌کند که استفاده از محک فرما برای ایجاد تمایز بین اعداد اول و مرکب بسیار کارآمد است. البته این موضوع، قبل از اثبات قضیه ۲-۴ نیز به صورت عملی بارها مشاهده و درستی آن حدس زده می‌شد.
همچنین توجه کنید مشابه $a = ۱$ شرط ۲-۲ برای عدد فرد n و $a = n - ۱$ همیشه بر قرار است؛ به همین دلیل این حالت را نیز کنار می‌گذاریم.

تعریف ۲-۵. *عدد n را "اول‌محتمل[۵]" در پایه a می‌نامیم هرگاه ۲-۲ برای زوج n و a برقرار باشد.*

با توجه به تعریف اگر n عددی اول باشد، به ازای هر $۱ < a < n - ۱$، اول‌محتمل در پایه a است. و در واقع قضیه ۲-۴ بیان میکند که برای a ثابت، بیشتر اعداد اول‌محتمل در پایهٔ a اول هستند.

[4] Fermat pseudoprimes

[5] Probable prime

تا به این جا محکی ساده برای تمایز بین دو مجموعه که یکی شامل تعدادی عدد مرکب پراکنده و تمامی اعداد اول بزرگ‌تر از $a + ۱$ و دیگری شامل بقیه اعداد مرکب بزرگ‌تر از $a + ۱$ است در اختیار داریم.

الگوریتم ۳ محک اول محتمل

این الگوریتم برای اعداد $n > ۳$ و $۲ \leq a \leq n - ۱$ داده شده، مشخص میکند آیا n مرکب است یا اول محتمل در پایه a.

[محاسبه توان در پیمانه]
1: $b = a^{n-1} \pmod n$ ▷ *با استفاده از الگوریتم ۲*
[Return decision]
2: **if** $b == 1$ **then**
3: **return** "n اول محتمل در پایه a است."
4: **return** "n مرکب است."

دیدیم که برای a مشخص اعداد شبه‌اول فرما در پایه a (اعداد اول‌محتمل که مرکب نیز هستند) به صورت پراکنده توزیع شده‌اند. اما با این حال نشان می‌دهیم تعدادشان نامتناهیست.

قضیه ۲-۶. *برای هر $a \geq ۲$، تعداد نامتناهی عدد شبه‌اول فرما در پایه a وجود دارند.*

اثبات. نشان خواهیم داد که اگر p عدد اول و فردی باشد به طوری که $a^۲ - ۱$ را نشمارد آنگاه $n = (a^{۲p} - ۱)/(a^۲ - ۱)$ شبه‌اول در پایه a است. برای مثال اگر $a = ۲$ و $p = ۵$ آنگاه این فرمول عدد $n = ۳۴۱$ را مشخص می‌کند.
ابتدا توجه کنید که

$$n = \frac{a^p - ۱}{a - ۱} \cdot \frac{a^p + ۱}{a + ۱}،$$

و از آنجا که $a \geq ۲$ و $p \geq ۳$، صورت هر دو کسر از مخرج بزرگ‌تر هستند و همچنین صورت کسر اول همیشه بر مخرجش بخش پذیر است. چون p فرد است صورت کسر دوم نیز بر مخرجش بخش پذیر است و در نتیجه n به صورت ضرب دو عدد بزرگ تر از ۱ نوشته شده است پس مرکب است.
با به توان ۲ رساندن دو طرف عبارت ۲-۱ عبارت (پیمانه‌ی p) $a^{۲p} \equiv a^۲$ بدست می‌آید و نتیجه می‌شود که عدد p عدد $a^{۲p} - a^۲$ را می‌شمارد. از آنجا که طبق فرض p عدد $a^۲ - ۱$ را نمی‌شمارد و $n - ۱ = (a^{۲p} - a^۲)/(a^۲ - ۱)$، نتیجه می‌گیریم که p، عدد $n - ۱$ را می‌شمارد. همچنین از آنجایی که

$$n - ۱ = a^{۲p-۲} + a^{۲p-۴} + \cdots a^۲$$

و سمت راست تساوی جمع $p-1$ عدد هم زوجیت است و $p-1$ نیز زوج است پس سمت راست تساوی عددی زوج است پس سمت چپ نیز باید زوج باشد. تا به اینجا به این نتیجه رسیدیم که هم ۲ و هم p مقسوم علیه‌های $n-1$ هستند و در نتیجه $2p$ نیز مقسوم علیه آن است. در نتیجه $a^{2p}-1$ مقسوم علیه $a^{n-1}-1$ است (می‌دانیم اگر $t_1|t_2$ آنگاه $x^{t_1}-1|x^{t_2}-1$). از این رو a^{n-1} در پیمانه $a^{2p}-1$ همنهشت با ۱ است. طبق تعریف، n مقسوم علیه $a^{2p}-1$ است پس در نتیجه a^{n-1}در پیمانه n نیز همنهشت با ۱ است. پس ۲-۲ برقرار و متعاقباً ۲-۱ نیز برقرار است. حال از آنجا که a^2-1 تعداد متناهی مقسوم علیه اول دارد پس نامتناهی عدد اول p در فرض انجام شده صدق می‌کنند و از آنجایی که مخرج n همیشه ثابت است پس به ازای p های متفاوت n متفاوتی نیز بدست می‌آید در نتیجه نا متناهی عدد فراما شبه‌اول در پایه a وجود دارند. $\square$

۲-۲-۳ اعداد کارمایکل

در جست و جو برای روشی ساده و سریع برای تمایز بین اعداد اول و مرکب می‌توانیم محک فرما را برای چند a متمایز انجام دهیم. برای مثال عدد ۳۴۱ شبه اول در پایه ۲ است اما در پایه ۳ نیست و یا مثلا ۹۱ شبه اول در پایه ۳ است اما در پایه ۲ نیست و این نتیجه می‌دهد که هم ۳۴۱ و هم ۹۱ مرکب هستند. اما اگر ۳۴۱ را فقط در پایه ۲ و ۹۱ را فقط در پایه ۳ بررسی می‌کردیم در مورد اول یا مرکب بودن آنها نتیجه‌ای حاصل نمی‌شد.
شاید هیچ عدد مرکبی همزمان هم شبه اول در پایه ۲ و هم شبه اول در پایه ۳ وجود نداشته باشد، یا شاید مجموعه ای از اعداد وجود داشته باشد که هیچ عدد مرکبی همزمان شبه‌اول در پایه تمام اعداد آن مجموعه نباشد. این‌ها حدس‌هایی هستند که طبق مشاهدات و تعاریفی که تا کنون کردیم ممکن است به ذهن برسند. و چقدر خوب می‌شد اگر این حدس‌ها درست بودند چرا که دیگر با بررسی اعداد آن مجموعه به عنوان مقادیر متفاوت a در الگوریتم، به طور قطع می‌توانستیم نتیجه بگیریم که یک عدد مرکب است یا اول.
اما متاسفانه عدد $561 = 3 \cdot 11 \cdot 17$ نه تنها شبه‌اول در پایه ۲ و ۳ است بلکه شبه‌اول در پایه تمام اعداد ممکن برای a است. احتمالا بسیار تعجب برانگیز است که چنین عددی وجود دارد. این عدد برای اولین بار توسط رابرت کارمایکل[6] در سال ۱۹۱۰ میلادی کشف و از آن پس این نوع از اعداد به نام او شناخته می‌شوند.

[6] Robert Carmichael

تعریف ۲-۷. *عدد مرکب n که به ازای هر a داشته باشیم $a^n \equiv a \pmod{n}$ را عدد کارمایکل می‌نامیم.*

شناسایی یک عدد کارمایکل از روی تجزیه‌اش به عوامل اول کار دشواری نیست.

قضیه ۲-۸. (*معیار کورسلت*[7]). *عدد صحیح n، عدد کارمایکل است اگر و تنها اگر مثبت، مرکب و خالی از مربع باشد و برای هر عامل اول p در n داشته باشیم $p-1$ شمارنده $n-1$ باشد.*

شاید جالب باشد بدانید که این قضیه توسط آقای کورسلت در سال ۱۸۹۹ یعنی ۱۱ سال قبل از معرفی اولین عدد کارمایکل بیان شده بود ولی حدس زده می‌شد که چنین عددی وجود ندارد.

اثبات.
$\Leftarrow$: ابتدا فرض کنید که n عدد کارمایکل باشد. در این صورت n مرکب نیز هست. حال فرض کنید p عامل اولی از n باشد. از آنجا که n کارمایکل است پس داریم $p^n \equiv p \pmod{n}$ پس $n|p^n - p$ و $n|p(p^{n-1} - 1)$ و از آنجا که $p^{n-1} - 1$ نسبت به p اول است پس عامل p ندارد در نتیجه توان عامل p در n حداکثر برابر ۱ است. از آن جا که فرض کردیم p عامل اول n است این توان دقیقا برابر ۱ است. در این صورت n خالی از مربع و طبق تعریف اعداد کارمایکل مثبت و مرکب است.
حال فرض کنید r ریشه اولیه در $\mathbb{Z}_p^*$ باشد. از آن جا که $r^n \equiv r \pmod{n}$ پس $r^n \equiv r \pmod{p}$ و همچنین r در $\mathbb{Z}_p^*$ دارای وارون ضربیست و در نتیجه داریم $r^{n-1} \equiv 1 \pmod{p}$.
اما مرتبه r در $\mathbb{Z}_p^*$ برابر $p-1$ است پس $p-1$ مقسوم علیه $n-1$ است.
$\Rightarrow$: فرض کنید که n عددی مثبت، مرکب و خالی از مربع باشد و برای هر عامل اول p در n داشته باشیم $p-1$ ، $n-1$ را بشمارد. می‌خواهیم نشان دهیم برای هر a داریم $a^n \equiv a \pmod{n}$.
از آن جا که n خالی از مربع است طبق قضیه باقیمانده چینی کافیست نشان دهیم برای هر عامل اول p در n و برای هر a داریم $a^n \equiv a \pmod{p}$. فرض کنید $p|n$ و a یک عدد صحیح باشد. اگر a بر p بخش پذیر نباشد طبق ۲-۲ داریم $a^{p-1} \equiv 1 \pmod{p}$ و از آنجا که $p-1$ مقسوم علیه $n-1$ است داریم $a^{n-1} \equiv 1 \pmod{p}$. از این رو با ضرب کردن دو طرف همنهشتی در a داریم $a^n \equiv a \pmod{p}$. حال اگر a بر p بخش پذیر باشد به وضوح داریم $a^n \equiv a \equiv 0 \pmod{p}$ پس به ازای هر a نشان دادیم که $a^n \equiv a \pmod{p}$ برقرار است و طبق قضیه باقیمانده چینی به ازای هر a داریم $a^n \equiv a \pmod{n}$ و در نتیجه n عدد کارمایکل است. $\square$

[7]Korselt criterion

حال ویژگی‌ای برای اعداد کارمایکل بدست آوردیم و میدانیم چنین اعدادی وجود دارند، ولی آیا تعدادشان نامتناهیست؟ جواب مثبت است و نامتناهی بودن این اعداد در [۵] نشان داده شده است. متاسفانه این کار را برای محک اول بودنی که تا کنون بررسی کردیم دشوار می‌کند. همچنین اردوش در سال ۱۹۵۶ نشان داد نه تنها تعداد اعداد کارمایکل نامتناهیست بلکه آنطور که انتظار می‌رفت نادر نیستند. به عبارت دیگر اگر $C(X)$ تعداد اعداد کارمایکل کوچک تر از x باشد، اردوش ادعا کرده است که برای هر $\epsilon > ۰$ وجود دارد $x.(\epsilon)$ به طوری که $C(x) > x^{۱-\epsilon}$ برای هر $x \geq x.(\epsilon)$. اثبات آلفورد[8]، گرانویل[9] و پامرنس[10] با اثبات اردوش[11] شروع و به آن مطالبی را اضافه می‌کند و بهبود می‌بخشد.

قضیه ۲-۹. *(آلفورد، گرانویل، پامرنس). نامتناهی عدد کارمایکل وجود دارند. به خصوص، برای x به اندازه کافی بزرگ داریم* $C(x) > x^{۲/۷}$.

می‌توان اثبات این قضیه را در [۵] پیدا کرد اما اثبات مقدماتی برای این قضیه در دسترس نیست.

عبارت "به اندازی کافی بزرگ" در صورت قضیه فوق به طور دقیق محاسبه نشده است اما حدس زده می‌شود اعداد بزرگ تر مساوی ۹۶امین عدد کارمایکل، ۸۷۹۳۰۹، همان اعداد به اندازه کافی بزرگ باشند و قضیه فوق برای آنها برقرار باشد.

آیا تحلیل مجانبی مشابه قضیه اعداد اول که فرمولی تقریبی برای تعداد اعداد اول کوچکتر از x بر حسب x مشخص می‌کند برای اعداد کارمایکل وجود دارد؟ تا کنون حتی حدس و گمانی برای اینکه این فرمول به چه صورت می‌تواند باشد وجود ندارد. با این حال حدس ضعیف تری در این باره وجود دارد.

حدس ۲-۱۰. *(اردوش، پامرنس). مقدار تابع $C(X)$ که همان تعداد اعداد کارمایکل که از x بزرگ تر نباشند است،*

$$C(x) = x^{۱-(۱+o(۱)) \ln\ln\ln x / \ln\ln x}$$

وقتی $x \to \infty$.

---

[8] Alford

[9] Granville

[10] Pomerance

[11] Erdős

فرمول مشابهی برای $P_{۲}(x)$، تعداد اعداد شبه اول در پایه ۲ کوچک تر یا مساوی x حدس زده شده است.
در [۶] اثبات شده است که هر دو گزاره

$$C(x) < x^{۱-\ln\ln\ln x/\ln\ln x}$$

$$P_{۲}(x) < x^{۱-\ln\ln\ln x/(۲\ln\ln x)}$$

برای x های به اندازه کافی بزرگ برقرار هستند.

۲-۳ اعداد اول‌محتمل و شاهدان

مفهوم اعداد شبه‌اول فرما که در فصل قبل معرفی شدند از جهت اینکه بسیار راحت و سریع قابل بررسی است و برای هر $a > ۱$ تعداد این اعداد نسبت به تعداد اعداد اول کم است، مفهومی کاربردی است. اما دیدیم نامتناهی عدد مرکب به نام اعداد کارمایکل وجود دارند که محک ۲-۱ کاملا ناتوان در اثبات مرکب بودن آن‌ها است. همچنین اعداد کارمایکلی وجود دارند که عامل اول کوچکی ندارند و حتی محک قوی تر ۲-۲ نیز عملکرد خوبی برای آن‌ها ندارد.
مایلیم محک ساده‌ای در اختیار داشته باشیم که هیچ شبه‌اولی در آن محک وجود نداشته باشد، به عبارت دیگر اعداد اول و مرکب را کاملا از هم تمیز دهد. در صورت عدم موفقیت برای انجام این کار، می‌توانیم خانواده‌ای از محک‌ها را در نظر بگیریم که برای هر عدد مرکب حداقل برای بخشی از محک‌های این خانواده شبه‌اول نباشد و نتیجه مرکب بودن آن عدد حاصل شد.
با توجه به وجود و نامتناهی بودن تعداد اعداد کارمایکل استفاده از خانواده‌ای از محک ها بر پایه محک فرما این هدف را بر آورده نمی‌کند. این در حالیست که نسخه کمی بهبود یافته قضیه کوچک فرما (۲-۱) ما را به هدفمان می‌رساند.

قضیه ۲-۱۱. *فرض کنید n عددی اول و $n - ۱ = ۲^s t$ که t عددی فرد است باشد. اگر a بر n بخش پذیر نباشد آنگاه*

$$\begin{cases} \textit{either } a^t \equiv ۱ \pmod{n} \\ \textit{or } a^{۲^i t} \equiv -۱ \pmod{n} \textit{ for some } i \textit{ with } ۰ \leq i \leq s-۱. \end{cases} \quad (۲\text{-}۳)$$

اثبات قضیه فوق فقط از قضیه کوچک فرما و اینکه برای هر عدد اول فرد n، جواب‌های معادله $x^۲ \equiv ۱$ (پیمانه‌ی n) در $\mathbb{Z}_n$، $x \equiv \pm ۱$ (پیمانه‌ی n) هستند، استفاده می‌کند.
حال قادر هستیم در تناسب با مفهوم اعداد اول‌محتمل[۱۲]، اعداد اول‌قویاً‌محتمل در پایه a را معرفی کنیم.

تعریف ۲-۱۲. *عدد $n > ۳$، اول‌قویاً‌محتمل است اگر ۲-۳ برای a که $۱ < a < n - ۱$ برقرار باشد.*

از آنجایی که هر عدد اول‌قویاً‌محتمل در پایه a، طبق تعریف، عدد اول‌محتمل نیز هست و

[12] Probable primes

از آنجایی که هر عدد بزرگ تر از $a + ۱$ عدد اول‌قویاً‌محتمل در پایه a است تنها تفاوت میان این دو مفهوم (اول محتمل و اول‌قویاً‌محتمل) این است که احتمالا اعداد مرکب کمتری از محک اول‌قویاً‌محتمل می‌گذرند.

الگوریتم ۴ محک اول‌قویاً‌محتمل

این الگوریتم برای اعداد $n > ۳$ و $۲ \leq a \leq n - ۱$ داده شده که نمایش n به صورت $n = ۱ + ۲^s t$ که t عددی فرد است مشخص می‌کند آیا n مرکب است یا اول‌قویاً‌محتمل در پایه a.

```
[قسمت فرد n − ۱]
b = a^t (mod n)                ▷ با استفاده از الگوریتم ۲
if b == 1 or b == n − 1 then
    return "n اول‌قویاً‌محتمل در پایه a است."
[توان ۲ در n − ۱]
for j ∈ [1, s − 1] do
    b = b^2 (mod n)
    if b == n − 1 then
        return "n اول‌قویاً‌محتمل در پایه a است."
    return "n مرکب است."
```

این محک برای اولین بار در [۷] پیشنهاد شد، و یک دهه بعد سلفریج[۱۳] آن را منتشر کرد. حال می‌توانیم با نشان دادن برقرار نبودن ۲-۳ برای n فرد و یک a مشخص، نشان دهیم n مرکب است. برای مثال قبلا دیدیم که ۳۴۱ شبه اول در پایه ۲ است. اما ۲-۳ برای $n = ۳۴۱$ و $a = ۲$ برقرار نیست.

در واقع $۸۵ \cdot ۲^۲ = ۳۴۰$ ، $۲^{۸۵} \equiv ۳۲$ (پیمانه‌ی ۳۴۱) و $۲^{۱۷۰} \equiv ۱$ (پیمانه‌ی ۳۴۱) و در نتیجه به ازای تمام $۲ \leq i \leq s - ۱$ نیز $۲^{۲^i \cdot ۸۵} \equiv ۱$ (پیمانه‌ی ۳۴۱). در این صورت می‌تون دید که ۳۲ مجذور عدد ۱ در پیمانه ۳۴۱ است.

حال $n = ۹۱$ و $a = ۱۰$ را در نظر بگیرید. داریم $۲^۱ \cdot ۴۵ = ۹۰$ و $۱۰^{۴۵} \equiv -۱$ (پیمانه‌ی ۹۱). در این صورت ۲-۳ برقرار است.

تعریف ۲-۱۳. *عدد n را قویاً‌شبه‌اول در پایه a نامیم هرگاه n عددی فرد و مرکب باشد به طوری که $n - ۱ = ۲^s t$ که t فرد است، ۲-۳ برقرار باشد.*

---

[13] J. Selfridge

با این تعریف ۳۴۱ قویاًشبه‌اول در پایه ۲ نیست، در حالی که ۹۱ قویاًشبه‌اول در پایه ۱۰ است.
به سادگی قابل نشان دادن است که اگر n قویاًشبه‌اول در پایه a باشد آنگاه شبه اول در پایه a نیز است. اما مثال $n = ۳۴۱$ و $a = ۲$ نشان می‌دهد عکس این موضوع برقرار نیست.
برای عدد فرد مرکب n قرار دهید

$$\mathcal{S}(n) = \{a \pmod{n} : n \text{ is a strong pseudoprime base } a\}$$

و قرار دهید $S(n) = \#\mathcal{S}(n)$. قضیه بسیار اساسی زیر در [۸] و [۹] به صورت مستقل اثبات شده است.

قضیه ۲-۱۴. *برای هر عدد فرد و مرکب $n > ۹$ داریم $S(n) \leq \frac{۱}{۴}\varphi(n)$.*

در صورت قضیه بالا، تابع $\varphi(n)$ همان تابع اویلر برای عدد n است. مقدار این تابع برابر است با تعداد اعداد در بازه ۱ تا n که نسبت به n اول هستند و یا به عبارتی مرتبه گروه $\mathbb{Z}_n^*$ است.
اگر تجزیهٔ عدد n به عوامل اولش را بدانیم مقدار تابع برای ورودی n را به راحتی می‌توان از فرمول $\varphi(n) = n\prod_{p|n}(۱ - \frac{۱}{p})$ محاسبه کرد.
قبل از شروع به اثبات این قضیه بسیار کاربردی شاید بهتر باشد ببینیم چرا این قضیه پر اهمیت است. فرض کنید می‌خواهیم اول یا مرکب بودن عدد فرد داده شده n را مشخص کنیم. می‌توانیم از محک ۲-۳ برای $۱ < a < n - ۱$ دلخواه استفاده کنیم. اگر عدد n از این محک گذر نکند به این معناست که ثابت کردیم n مرکب است و می‌گوییم a شاهدی برای مرکب بودن n است.

تعریف ۲-۱۵. *اگر n عددی مرکب باشد و a عددی صحیح در $[۱, n - ۱]$ باشد که ۲-۳ برقرار نباشد، گوییم عدد a شاهدی[14] برای n است.*

در نتیجه یک شاهد عددی مثل a است که در پایهٔ آن عدد n قویاًشبه‌اول نیست. و پیدا کردن شاهد روشی کوتاه برای اثبات مرکب بودن عدد n است. با توجه به سریع بودن اجرای محک ۲-۳ بسیار می‌توان شاهد بودن یا نبودن a برای n را بررسی کرد.
حال با توجه به این تعریف، قضیه ۲-۱۴ بیان می‌کند که اگر n عدد مرکب فردی باشد، حداقل ۳/۴ اعداد صحیح در بازه $[۱, n - ۱]$ شاهد برای n هستند. حال می‌توان الگوریتمی احتمالاتی

[14] Witness

طراحی کرد که با توجه به قضیه ۱۴-۲ به احتمال ۱/۴ در زمان بسیار کمی شاهدی برای n فرد پیدا می‌کند.

الگوریتم ۵ محک مرکب بودن تصادفی

این الگوریتم برای عدد $n > ۳$ سعی می‌کند شاهدی برای n بیابد و متعاقبا ثابت می‌شود n مرکب است. اگر a شاهدی برای n باشد (a,YES)برگردانده می‌شود و در غیر این صورت (a,NO).

[انتخاب شاهد تصادفی]

Choose random intege $a \in [2, n-2]$

Via Algorithm 4 decide whether n is a strong probable prime base a

[اعلان]

if n is a strong probable prime base a **then**

    return (a, NO)

return (a, YES)

این الگوریتم احتمالاتی معمولا به عنوان محک میلر_رابین شناخته می‌شود اما محک میلر_رابین اصلی الگوریتمی کمی پیچیده تر و قطعی بر پایه فرضیه توسعه یافته ریمان بوده است و درواقع تنها رابین الگوریتم احتمالاتی فوق را پیشنهاد داده است.

حال می‌توانیم این الگوریتم را با مداوم تکرار کردنش بهبود ببخشیم. در این صورت احتمال این که نتوانیم شاهدی برای n فرد مرکب بعد از k بار انجام مستقل الگوریتم پیدا کنیم طبق قضیه ۱۴-۲ کمتر از ۱/۴^{k} است. پس می‌توانیم این احتمال را به اندازه دلخواهمان کوچک کنیم.

به طور مثال فرض کنید n عددی بزرگ و فرد باشد که در مورد اول یا مرکب آن اطلاعی نداریم. در نظر بگیرید الگوریتم ۵ پس از ۲۰ بار تکرار نتوانسته شاهدی برای n بیابد. طبق مطالبی که پیشتر دیدیم هیچ نتیجه‌ای در رابطه با اول یا مرکب بودن عدد n نمی‌توانیم بگیریم، اما قویا حدس می‌زنیم که n اول باشد. چرا که احتمال پیدا نکردن شاهد برای عدد فرد مرکبی بعد از ۲۰ بار انجام شدن الگوریتم برابر ۴$^{-۲۰}$ است که عددی بسیار بسیار ناچیز است. به این دلیل n به احتمال قوی اول است. اما این ادعا اثبات نشده است و با این که احتمال ناچیزی دارد که n مرکب باشد ولی ناشدنی نیست.

الگوریتم‌هایی وجود دارند که سعی میکنند اثبات کنند چنین اعدادی یعنی اعدادی که قویاً احتمال می‌دهیم اول باشند واقعا اول هستند. اما برای کاربردهای عملی می‌توانیم از اعدادی که از اول بودن آن‌ها مطمئن نیستم ولی احتمال می‌دهیم اول باشند استفاده کنیم. شاید به همین دلیل است که از آن به عنوان "محک اول بودن" یاد میکنند چرا که اعدادی که احتمال بسیار ناچیزی وجود دارد

که مرکب باشند را اول در نظر می‌گیرند. اما شاید دقیق تر این باشد که برای اعدادی که به احتمال زیاد اول هستند از عنوان "اعداد اول صنعتی[۱۵]" استفاده کنیم. از الگوریتم زیر می‌توان برای تولید عددی که به احتمال زیاد اول است استفاده کرد.

الگوریتم ۶ تولید اعداد اول صنعتی

این الگوریتم با اعداد ورودی $k \geq ۳$ و $T \geq ۱$، عدد k بیتی تولید می‌کند (عددی در $[۲^{k-۱}, ۲^k)$) که توسط T بار تکرار الگوریتم ۵ به عنوان عددی مرکب شناسایی نشده است.

[انتخاب کاندیدا]

Choose a random odd integer n in the interval $(2^{k-1}, 2^k)$

[اجرای محک اول‌قویاًمحتمل]

for $1 \leq i \leq T$ **do**

  Via Algorithm 5 attempt to find a witness for n

  if a witness is found for n **then**

    goto [انتخاب کاندیدا]

return n

حال یکی از سوالات اساسی و جالب این است که احتمال مرکب بودن عدد خروجی داده شده از الگوریتم ۶ چقدر است. فرض کنید احتمال مرکب بودن خروجی الگوریتم برای ورودی kو T به الگوریتم برابر $P(k,T)$ باشد. ممکن است فکر کنید جواب این سوال را قبلا با استفاده از قضیه ۲-۱۴ داده‌ایم و $P(k,T) \leq ۴^{-T}$. با این حال این استدلال اصلا درست نیست. مثلاً فرض کنید $K = ۵۰۰$ و $T = ۱$ در این صورت قضیه اعداد اول[۱۶] بیان می‌کند که احتمال اول بودن عدد ۵۰۰ رقمی فرد دلخواه برابر ۱/۱۷۳ است که بسیار کوچک‌تر از ۱/۴ است. در نتیجه با استفاده از احتمال شرطی می‌توان احتمال مرکب بودن خروجی الگوریتم به شرط یک بار عبور کردن از شرط ۲-۳ را محاسبه کرد و این احتمال بسیار نزدیک به ۱ می‌شود.
به عبارت دیگر به نظر می‌رسد که این الگوریتم به احتمال نزدیک به یک عدد مرکب تولید می‌کند ولی این کاملا اشتباه است. این اشتباه از آنجایی به وجود می‌آید که ما در قضیه ۲-۱۴ بدترین حالت را در نظر گرفتیم و برای بیشتر اعداد فرد نسبت تعداد شاهدها بسیار بیشتر از چیزیست که در این قضیه ادعا شده است. با این حال در [۱۰] نشان داده شده است که نتیجه $P(k,T) \leq ۴^{-T}$ واقعا درست است.

---

[15] Industrial-grade prime

[16] Prime number theorem

اگر k به اندازه کافی بزرگ باشد حتی با ازای $T = ۱$ استفاده از الگوریتم ۶ نتایج خوبی دارد و عدد تولید شده به احتمال زیاد اول است. در [۱۱] نشان داده شده است که $P(k, ۱) < k^{۲}۴^{۲-\sqrt{k}}$. برای تعدادی k بزرگ این مقاله حتی نتایج بهتری را نشان می‌دهد. برای مثال $P(۵۰۰, ۱) < ۴^{-۲۸}$.

در نتیجه اگر عدد ۵۰۰ رقمی فرد حتی یک بار از شرط اول‌قویاًمحتمل عبور کرده باشد احتمال مرکب بودنش بسیار ناچیز است و می‌توان با خیال آسوده از آن به عنوان عددی اول استفاده کرد مگر در شرایطی که حساسیت نسبت به اول بودن اعداد استفاده شده بسیار زیاد باشد.
حال به سراغ اثبات قضیه ۲-۱۴ می‌رویم. قبل از اثبات این قضیه لازم است لم‌های زیر را اثبات کنیم.

لم ۲-۱۶. *فرض کنید n عدد فرد و مرکب باشد به صورتی که $n - ۱ = ۲^{s}t$ که t فرد است. $v(n)$ را تعریف می‌کنیم بزرگترین عددی که $۲^{v(n)}$ شمارنده $p - ۱$ به ازای تمام عوامل اول n مثل p باشد. اگر n قویاًشبه‌اول در پایه a باشد، آنگاه $a^{۲^{v(n)-۱}} \equiv \pm ۱$ (پیمانه‌ی n).*

اثبات. اگر $a^{t} \equiv ۱$ (پیمانه‌ی n)، واضح است که حکم برقرار است. پس فرض کنید این طور نباشد و داشته باشیم $a^{۲^{i}t} \equiv -۱$ (پیمانه‌ی n) و فرض کنید p عامل اولی از n باشد. در این صورت داریم $a^{۲^{i}t} \equiv -۱$ (پیمانه‌ی p). اگر k مرتبه a در گروه ضربی بازیمانده‌های p باشد (یعنی k کوچک ترین عددی باشد که $a^{k} \equiv ۱$ (پیمانه‌ی p))، آنگاه k، $۲^{i+۱}t$ را می‌شمارد ولی $۲^{i}t$ را نمی‌شمارد. پس توان ۲ در تجزیه k به عوامل اولش دقیقا برابر $i + ۱$ است. اما k عدد $p - ۱$ را نیز می‌شمارد، پس $۲^{i+۱}|p - ۱$. از آنجا که این برای تمام عوامل اول شمارنده n صادق است، داریم $i + ۱ \leq v(n)$. حال با توجه به فرضی که در ابتدا کردیم یعنی $a^{۲^{i}t} \equiv -۱$ (پیمانه‌ی n) و از آنجا که $i + ۱ \leq v(n)$ اگر $i + ۱ < v(n)$ داریم $a^{۲^{v(n)-۱}}t \equiv ۱$ (پیمانه‌ی n) و اگر $i + ۱ = v(n)$ داریم $a^{۲^{v(n)-۱}t} \equiv -۱$ (پیمانه‌ی n) و در هر صورت حکم لم برقرار است. □

از آنجایی که کار با مجموعه S که در صورت قضیه ۲-۱۴ وجود دارد به صورت مستقیم دشوار است، برای عدد n قرار دهید

$$\bar{S}(n) = \{a \pmod{n} : a^{۲^{v(n)-۱}t} \equiv \pm ۱ \pmod{n}\}, \quad \bar{S}(n) = \#\bar{S}(n) \qquad (۲\text{-}۴)$$

توجه کنید طبق لم ۲-۱۶ و تعریف S اگر $a \in S$ آنگاه $a \in \bar{S}$ پس $S \subseteq \bar{S}$. درنتیجه اگر ثابت کنیم $\bar{S} \leq \frac{۱}{۴}\varphi(n)$ حکم قضیه ۲-۱۴ ثابت می‌شود.

لم ۲-۱۷. *فرض کنید نماد گذاری همان نمادگذاری لم ۲-۱۶ و ۲-۴ باشد. همچنین قرار دهید $\omega(n)$ برابر تعداد عوامل اول متمایز عدد n باشد. داریم*

$$\bar{S}(n) = ۲ \cdot ۲^{(v(n)-۱)w(n))} \prod_{p|n} \gcd(t, p-۱).$$

اثبات. قرار دهید $m = ۲^{v(n)-۱}t$ و فرض کنید تجزیه n به عوامل اول به صورت $p_۱^{j_۱}p_۲^{j_۲}\cdots p_k^{j_k}$ که $k = \omega(n)$ باشد. طبق قضیه باقیمانده چینی می‌دانیم $a^m \equiv ۱$ (پیمانه‌ی n) اگر و تنها اگر $a^m \equiv ۱$ (پیمانه‌ی $p_i^{j_i}$) برای $i = ۱, ۲, \dots k$. برای عدد اول فرد p و عدد طبیعی j، گروه $\mathbb{Z}_{p^j}^*$ که شامل دستگاه مخفف مانده‌ها در پیمانه p^j است دوری است و شامل $\varphi(p^j) = p^{j-۱}(p-۱)$ عضو است. یا به عبارت دیگر ریشه اولیه در پیمانه p^j وجود دارد.
از آنجا که n فرد است پس تمام عوامل اولش نیز فرد هستند. حال اگر r ریشه اولیه گروه $\mathbb{Z}_{p_i^{j_i}}^*$ باشد جواب‌های معادله (پیمانه‌ی $p_i^{j_i}$) $a^m \equiv ۱$ به صورت r^t که $۰ \leq t < p_i^{j_i-۱}(p_i-۱)$ هستند. از آنجا که r ریشه اولیه است r^t جواب معادله است اگر و تنها اگر $p_i^{j_i-۱}(p_i-۱)|mt$ و یا معادلاً $\frac{p_i^{j_i-۱}(p_i-۱)}{\gcd(m,p_i^{j_i-۱}(p_i-۱))}|t$. در نتیجه طبق محدودیت t، t باید به شکل $k \cdot \frac{p_i^{j_i-۱}(p_i-۱)}{\gcd(m,p_i^{j_i-۱}(p_i-۱))}$ باشد که $۱ \leq k \leq \gcd(m, p_i^{j_i-۱}(p_i-۱))$.
با توجه به مطالب فوق تعداد جواب‌های معادله (پیمانه‌ی $p_i^{j_i}$) $a^m \equiv ۱$ برابر است با

$$\gcd(m, p_i^{j_i-۱}(p_i-۱)) = \gcd(m, p_i-۱) = ۲^{v(n)-۱} \cdot \gcd(t, p_i-۱).$$

(توجه کنید که m، $n-۱$ را می‌شمارد و تساوی اول نتیجه می‌شود.) از قضیه بازیمانده چینی نتیجه می‌گیریم تعداد جواب‌های (پیمانه‌ی n) a برای معادله (پیمانه‌ی n) $a^m \equiv ۱$ برابر است با

$$\prod_{i=۱}^{k}(۲^{v(n)-۱} \cdot \gcd(t, p_i-۱)) = ۲^{(v(n)-۱)\omega(n)} \prod_{i=۱}^{k} \gcd(t, p_i-۱).$$

در ادامه برای کامل کردن اثبات کافیست نشان دهیم دقیقاً همین تعداد جواب برای معادلهٔ (پیمانه‌ی n) $a^m \equiv -۱$ نیز وجود دارد.
می‌دانیم که اگر p عدد اول فردی باشد و j عددی طبیعی آنگاه جواب‌های معادله $x^۲ \equiv ۱$ (پیمانه‌ی p^j) برابر ۱ و ۱− هستند که ۱ جواب معادله (پیمانه‌ی p^j) $x \equiv ۱$ نیز هست ولی ۱−

نیست. از این رو $a^m \equiv -۱$ (پیمانه‌ی $p_i^{j_i}$) اگر و تنها اگر $a^{۲m} \equiv ۱$ (پیمانه‌ی $p_i^{j_i}$) و $a^m \not\equiv ۱$ (پیمانه‌ی $p_i^{j_i}$). از آنجا که $۲^{v(n)}$، $p_i - ۱$ را می‌شمارد مانند قبل نتیجه می‌شود که تعداد جواب‌های معادله $a^m \equiv -۱$ (پیمانه‌ی $p_i^{j_i}$) برابر است با

$$۲^{v(n)} \cdot \gcd(t, p_i - ۱) - ۲^{v(n)-۱} \cdot \gcd(t, p_i - ۱) = ۲^{v(n)-۱} \cdot \gcd(t, p_i - ۱)$$

در نتیجه دقیقاً همان تعداد جواب برای معادله $a^m \equiv ۱$ (پیمانه‌ی n) وجود دارد که برای معادله $a^m \equiv -۱$ (پیمانه‌ی n) نیز وجود دارد، پس حکم لم ثابت شده است. □

اثبات قضیه ۲-۱۴. همان طور که قبلاً اشاره کردیم برای اثبات این قضیه کافیست نشان دهیم برای nهای فرد و مرکب بزرگ‌تر از ۹ داریم $\bar{S}(n)/\varphi(n) \leq ۱/۴$.

طبق لم ۲-۱۷ و فرمول محاسبه تابع φ داریم

$$\frac{\varphi(n)}{\bar{S}(n)} = \frac{۱}{۲} \prod_{p^a || n} p^{a-۱} \frac{p-۱}{۲^{v(n)} \gcd(t, p-۱)},$$

که نماد $p^a||n$ به این معناست که a توان عامل p در تجزیه n به عوامل اول است. با توجه به فرد بودن n تمام عوامل اولش نیز فرد هستند و با توجه به تعریف $v(n)$ و اثبات قضیه ۲-۱۷ تمام عبارات $p^{a-۱}\frac{p-۱}{۲^{v(n)}\gcd(t,p-۱)}$ زوج و طبیعی هستند. در نتیجه سمت راست تساوی و در پی آن سمت چپ تساوی عددی طبیعی هستند. همچنین با توجه به این موضوع اگر $\omega(n) \geq ۳$ باشد نتیجه می‌شود که $\varphi(n)/\bar{S}(n) \geq ۴$. حال اگر $\omega(n) = ۲$ و n خالی از مربع نباشد آنگاه از آن جا که عوامل اول n بزرگ‌تر مساوی ۳ هستند پس ضرب جملات $p^{a-۱}$ سمت چپ تساوی حداقل برابر ۳ و از آن جا که n، ۲ عامل اول دارد ضرب جملات کسری سمت راست تساوی حداقل برابر ۴ است. پس در مجموع سمت راست تساوی حداقل برابر ۶ است و داریم $\varphi(n)/\bar{S}(n) \geq ۶$.

حال فرض کنید $\omega(n) = ۲$ و n خالی از مربع باشد. بع عبارتی $n = pq$ که $p < q$ و هر دو عددی اول باشند. اگر $۲^{v(n)+۱}|q-۱$ آنگاه $۲^{v(n)-۱}\gcd(t, q-۱) \leq (q-۱)/۴$ و $\varphi(n)/\bar{S}(n) \geq ۴$. حال فرض کنید $۲^{v(n)}||q-۱$. از آن جا یی که $n-۱ = (q-۱)p+p-۱$ پس داریم $n-۱ \equiv p-۱$ (پیمانه‌ی $q-۱$) پس $q-۱$، $n-۱$ را نمی‌شمارد و این به این معناست که عامل اول فردی در $q-۱$ وجود دارد که با توان بیشتری نسبت به $n-۱$ در $q-۱$ ظاهر می‌شود و از آن جا که t بخش فرد $n-۱$ است این معناست که $۲^{v(n)-۱}\gcd(t, q-۱) \leq (q-۱)/۶$.

با توجه به وجود عامل دیگری در n (همان p) نتیجه می‌شود که $\varphi(n)/\bar{S}(n) \geq ۶$.

در نهایت فرض کنید که $\omega(n) = ۱$ و داریم $n = p^a$ که $a \geq ۲$. در این صورت $\varphi(n)/\bar{S}(n) = p^{a-۱}$، پس $\varphi(n)/\bar{S}(n) \geq ۵$ به جز وقتی که $p^a = ۹$ که آن را در فرض قضیه کنار گذاشته‌ایم. پس حکم قضیه در تمام حالات برقرار است. □

۲-۳-۱ کوچک‌ترین شاهد برای n

در قضیه ۲-۱۴ دیدیم که هر عدد فرد و مرکب n دارای حداقل $۳n/۴$ شاهد در بازهٔ $[۱, n-۱]$ است. تعریف می‌کنیم $W(n)$ کوچک ترین شاهد برای عدد n باشد. در این صورت $W(n) \geq ۲$. قضیه ۲-۴ نشان می‌دهد که تقریباً برای تمام اعداد اول فرد $W(n) = ۲$. با این حال نشان می‌دهیم نامتناهی عدد فرد مرکب مثل n داریم $W(n) \geq ۳$.

قضیه ۲-۱۸. *اگر p عدد فرد بزرگ‌تر از ۵ باشد آنگاه $n = (۴^p + ۱)/۵$ قویاًشبه‌اول در پایه ۲ است، در نتیجه $W(n) \geq ۳$.*

اثبات. ابتدا نشان می‌دهیم که n مرکب است. از آنجا که $۴^p \equiv (-۱)^p \equiv -۱$ (پیمانه‌ی ۵)، n عددی طبیعی است. حال مرکب بودن n از تساوی زیر نتیجه می‌شود

$$۴^p + ۱ = (۲^p - ۲^{(p+۱)/۲} + ۱)(۲^p + ۲^{(p+۱)/۲} + ۱).$$

توجه کنید که ۵ عددی اول است پس دقیقاً یکی از دو پرانتز بالا بر ۵ بخش پذیر است. اگر n مرکب نباشد باید آن پرانتزی که بر ۵ قابل قسمت است خود برابر ۵ باشد که با توجه به شرایط p برای هیچکدام از ۲ پرانتز این امکان وجود ندارد.
با توجه به تعریف n داریم $۲^{۲p} \equiv -۱$ (پیمانه‌ی n)، در نتیجه اگر m عددی فرد باشد داریم $۲^{۲pm} \equiv -۱$ (پیمانه‌ی n). اما $n - ۱ = ۴(۴^{p-۱} - ۱)/۵ = ۲^۲t$ است که t عددی فرد و طبق قضیهٔ فرما بر p بخش پذیر است. در نتیجه $۲^{۲t} \equiv -۱$ (پیمانه‌ی n) و n قویاًشبه‌اول در پایه ۲ است. □

حال سوال بسیار مهمی پیش می‌آید که آیا $W(n)$ می‌تواند به صورت دلخواهی بزرگ باشد، یا وجود دارد B که بسیار بزرگ نباشد و برای تمام اعداد فرد و مرکب n داشته باشیم $W(n) \leq B$. در این صورت موضوع بررسی اول بودن اعداد تبدیل به مسئله‌ای راحت می‌شود، چرا که می‌توانیم بررسی که برای تمام $a \leq B$ ۲-۳ برقرار باشد و در این صورت n اول است. متاسفانه چنین عدد B وجود ندارد. همچنین نتیجه زیر در [۱۲] نشان داده شده است.

قضیه ۲-۱۹. *نامتناهی عدد فرد و مرکب n وجود دارند به طوری که*

$$W(n) > (\ln n)^{۱/(۳ \ln\ln\ln n)}.$$

در واقع، تعداد چنین اعدادی تا x حداقل برابر $x^{۱/(۳۵ \ln\ln\ln)x}$ است وقتی که x به اندازه کافی بزرگ باشد.

تعریف ۲-۲۰. *فرض کنید D عدد صحیح مثبت و χ تابعی از از اعداد صحیح به اعداد مختلط باشد که*

۱. *برای هر m و n داشته باشیم $\chi(mn) = \chi(m)\chi(n)$.*

۲. *χ در پیمانه D متناوب باشد. (به این معنا که این تابع روی $\mathbb{Z}/D\mathbb{Z}$ خوش تعریف باشد)*

۳. *$\chi(n) = ۰$ اگر و تنها اگر $\gcd(n, D) > ۱$.*

در این صورت χ را کاراکتر دیریکله[17] در پیمانه D می‌نامیم.

بی طور مثال

$$\chi_۰(a) = \begin{cases} ۰ & \textbf{if } \gcd(a, D) > ۱ \\ ۱ & \textbf{if } \gcd(a, D) = ۱ \end{cases}$$

کاراکتر دیریکله در پیمانه D است هم چنین این تابع به عنوان کاراکتر اصلی شناخته می‌شود. توابع نماد لژاندر و ژاکوبی نیز هر دو کاراکتر دیریکله هستند. حال با توجه به تعریف کاراکتر دیریکله، تابع زیر را معرفی می‌کنیم.

تعریف ۲-۲۱. *Lـ سری دریکله را به صورت زیر تعریف می‌کنیم:*

$$L(s, \chi) = \sum_{n=۱}^{\inf} \frac{\chi(n)}{n^s}.$$

از این تابع اطلاعات جالبی در رابطه با توزیع اعداد اول در پیمانه اعداد مختلف بدست می‌آید.

---

[17] Dirichlet character

حدس ۲-۲۲. *(فرضیه توسعه یافته ریمان (ERH)). فرض کنید χ کاراکتر دیریکله دلخواه باشد. در این صورت صفرهای تابع $L(s,\chi)$ در ناحیه $Re(s) > ۰$ روی خط عمودی $Re(s) = \frac{۱}{۲}$ قرار می‌گیرند.*

در [۱۳] نتیجه زیر ثابت شده است.

قضیه ۲-۲۳. *فرض کنید ERH برقرار باشد. برای هر عدد صحیح و مثبت D و کاراکتر غیر اصلی χ در پیمانه D، عدد مثبت n وجود دارد که $n < ۲\ln^۲ D$ و $\chi(n) \neq ۱$ و همچنین وجود دارد عدد صحیح و مثبت m که $m < ۳\ln^۲ D$ و $\chi(m) \neq ۱$ و $\chi(m) \neq ۰$.*

با توجه به اینکه در پیدا کردن B ثابت برای تمام اعداد شکست خورده‌ایم. اما شاید تابعی با رشد اندک وجود داشته باشد که همیشه از $W(n)$ بزرگ‌تر باشد. بر اساس [۱۴] نتیجه زیر در [۱۵] ثابت شده است.

قضیه ۲-۲۴. *اگر فرضیه توسعه یافته ریمان (ERH)[18] درست باشد، برای تمام اعداد فرد و مرکب n داریم $W(n) < ۲\ln^۲ n$.*

با اینکه اثبات این قضیه در [۱۵] به صورت کامل وجود دارد، در این جا بخشی از اثبات که با دانش مقدماتی قابل انجام است را بیان می‌کنیم. قبل از اثبات لازم است لم زیر را اثبات کنیم.

لم ۲-۲۵. *اگر n عددی فرد و مرکب باشد که $n - ۱ = ۲^s t$ که t فرد است و p یکی از عامل‌های اول عدد n باشد که $p - ۱ = ۲^{s'} t'$ که t' فرد است و ۲-۳ برقرار باشد آنگاه:*

$$(\frac{a}{p}) = -۱ \iff a^{۲^{s'-۱}t} \equiv -۱ \ (\text{پیمانه‌ی } n).$$

اثبات. با توجه به فرض برقرار بودن ۲-۳، روی اینکه کدام گزاره از این گزارهٔ فصلی برقرار است حالت بندی میکنیم.
حالت برقرار بودن گزاره اول ۲-۳ :
اگر $a^t \equiv ۱ \ (\text{پیمانه‌ی } n)$ پس داریم $a^t \equiv ۱ \ (\text{پیمانه‌ی } p)$. حال با توجه به اینکه p اول است و در پیمانه اعداد اول ریشه اولیه موجود است پس وجود دارد ریشه اولیه r و عدد صحیح $۰ \leq k < p-۱$ که $a \equiv r^k \ (\text{پیمانه‌ی } p)$. حال از آنجا که $r^{kt} \equiv a^t \equiv ۱ \ (\text{پیمانه‌ی } p)$ پس چون r ریشه اولیه

[18] Extended Riemann hypothesis

است داریم $kt|p-۱$. اما n عددی فرد است و p عاملی از n است پس p فرد و $p-۱$ زوج است.
همچنین طبق فرض t فرد است پس از آنجا که $kt|p-۱$، k عددی زوج است. در نتیجه $a=r^k$ مانده مربعی در پیمانه p است و داریم $(\frac{a}{p})=۱$ (این استدلال را بدون استفاده از ریشه اولیه نیز می‌توان انجام داد).
همچنین از آنجا که $a^t\equiv ۱$ (پیمانه‌ی n) پس $a^{۲^{s'-۱}t}\equiv ۱$ (پیمانه‌ی n). در نتیجه در این حالت گزاره "اگر و تنها اگر" صورت لم برقرار است.
حالت برقرار بودن گزاره دوم ۲-۳ :
فرض کنید وجود داشته باشد i که $a^{۲^it}\equiv -۱$ (پیمانه‌ی n). در این صورت طبق لم ۲-۱۶ داریم $a^{۲^{s'-۱}t}\equiv \pm۱$ (پیمانه‌ی n).
$\Rightarrow$: ابتدا فرض کنید $(\frac{a}{p})=-۱$. در این صورت طبق محک اویلر داریم $a^{۲^{s'-۱}t'}\equiv -۱$ (پیمانه‌ی n). مشابه اثبات لم ۲-۱۶ نتیجه می‌شود که $۲^{s'}|\mathrm{Ord}_p(a)$. حال فرض کنید $a^{۲^{s'-۱}t}\not\equiv -۱$ (پیمانه‌ی n) (فرض خلف). در این صورت طبق لم ۲-۱۶، $a^{۲^{s'-۱}t}\equiv ۱$ (پیمانه‌ی n). پس $\mathrm{Ord}_p(a)|۲^{s'-۱}t$ اما از آنجا که t فرد است این تناقض با $۲^{s'}|\mathrm{Ord}_p(a)$ است. در نتیجه فرض خلف باطل و $a^{۲^{s'-۱}t}\equiv -۱$ (پیمانه‌ی n).
$\Leftarrow$: مشابه استدلال فوق، فرض کنید $a^{۲^{s'-۱}t}\equiv -۱$ (پیمانه‌ی n). در این صورت $a^{۲^{s'-۱}t}\equiv -۱$ (پیمانه‌ی p) و $a^{۲^{s'}t}\equiv ۱$ (پیمانه‌ی p). در نتیجه $۲^{s'}|\mathrm{Ord}_p(a)$. حال فرض کنید $(\frac{a}{p})=۱$ (فرض خلف) و طبق محک اویلر $a^{۲^{s'-۱}t}\equiv ۱$. ولی این تناقض با $۲^{s'}|\mathrm{Ord}_p(a)$ است در نتیجه فرض خلف باطل و $(\frac{a}{p})=-۱$.
در نتیجه در تمام حالات حکم برقرار است. $\square$

اثبات قضیه ۲-۲۴ . فرض کنید n عدد فرد و مرکبی باشد. اگر n خالی از مربع نباشد بدون داشتن فرض ERH می‌توان ثابت کرد که $W(n)<۲\ln^۲ n$ و این اثبات بر پایه هیچ فرض اثبات نشده‌ای نیست (برای جزئیات به [۲] رجوع کنید). پس در ادامه فرض می‌کنیم n خالی از مربع است.
حال فرض کنید p عامل اولی از n باشد و $۲^{s_۱}t_۱=p_۱-۱$ که $t_۱$ عددی فرد است. حال از آنجا که n مرکب و خالی از مربع است پس عامل اول دیگری مثل $p_۲$ دارد که $۲^{s_۲}t_۲=p_۲-۱$ که $t_۲$ عددی فرد است. بدون از دست دادن کلیات مسئله فرض کنید $s_۱\leq s_۲$. قرار دهید $\mathcal{X}_۱(m)=(\frac{m}{p_۱p_۲})$ و $\mathcal{X}_۲(m)=(\frac{m}{p_۲})$. در این صورت $\mathcal{X}_۱$ کاراکتر در پیمانه $p_۱p_۲$ و $\mathcal{X}_۲$ کاراکتر در پیمانه $p_۲$ هستند.
ابتدا حالت $s_۱=s_۲$ را بررسی می‌کنیم. با توجه به برقرار بودن ERH، قضیه ۲-۲۳ بیان می‌کند که عدد صحیح و مثبت m وجود دارد که $m<۲\ln^۲(p_۱p_۲)\leq ۲\ln^۲ n$ که $\chi(m)\neq ۱$. پس $\chi(m)=-۱$ یا ۰. اگر $\chi(m)=۰$ در این صورت یعنی m بر حداقل یکی از $p_۱$ یا $p_۲$ بخش

پذیر است و در نتیجه شاهد است. حال فرض کنید $\chi(m) = -1$ باشد. در نتیجه یا $(\frac{m}{p_1}) = 1$ و $(\frac{m}{p_2}) = -1$ یا بر عکس. بدون از دست دادن کلیات مسئله فرض کنید حالت اول برقرار باشد. در این صورت طبق لم ۲-۲۵ اگر ۲-۳ برقرار باشد آنگاه $m^{2^{s_2-1}t} \equiv -1$ (پیمانه‌ی n)، و از آنجا که فرض کردیم در این حالت $s_1 = s_2$ پس $(\frac{m}{p_1}) = -1$ و این تناقض است. این تناقض از فرض برقرار بودن ۲-۳ به وجود آمد، در نتیجه ۲-۳ برای m نمی‌تواند برقرار باشد و m شاهد است.

حال فرض کنید $s_2 < s_1$. باز هم طبق قضیه ۲-۲۳ عدد طبیعی m وجود دارد که $m < 2\ln^2 p_2 < 2\ln^2 n$ و $(\frac{m}{p_2}) = \chi(m) \neq 1$. اگر $(\frac{m}{p_2}) = 0$ در این صورت m بر p_2 بخش پذیر است و شاهد است. حال فرض کنید $(\frac{m}{p_2}) = -1$. اگر m شاهد نباشد به این معناست که ۲-۳ برقرار است و طبق لم ۲-۲۵، (پیمانه‌ی n) $m^{2^{s_2-1}t} \equiv -1$. حال طبق لم ۲-۱۶، $2^{s_2} | p_1 - 1$ و در نتیجه $s_2 \leq s_1$ و این تناقض با فرض $s_1 < s_2$ است. در نتیجه ۲-۳ نمی‌تواند برای m برقرار باشد و m شاهد است. □

قضیه فوق بر اساس درست بودن فرضیه توسعه یافته ریمان اثبات شده است. حال سوال این است که آیا بدون فرض درست بودن این فرضیه نیز می‌توان قضیه را ثابت کرد یا خیر. به وضوح از آنجایی که کوچک‌ترین عامل اول عدد فرد و مرکب n شاهدی برای خود n است $W(n) \leq n^{۱/۲}$. در [۱۶] نشان داده شده است که $W(n) \leq n^{c+o(۱)}$ وقتی که $n \to \infty$ برای اعداد فرد n و $c = ۱/(۶\sqrt{e})$. و به تازگی هیث‌ـبراون[19] (به [۱۷] رجوع کنید) ثابت کرده است که $c = ۱/(۱۰/۸۲)$ نیز عبارت را برقرار نگه می‌دارد.

حال با توجه به قضیه ۲-۲۴ اگر فرضیه توسعه یافته ریمان درست باشد می‌توان با پیچیدگی زمانی چند جمله‌ای و به طور قطعی توسط محکی مشابه محک میلرـرابین مشخص کرد که آیا عددی اول است یا خیر.

الگوریتم ۷ محک اول بودن میلر

این الگوریتم با ورودی $n > ۱$ مشخص می‌کند که آیا n اول (YES) است یا مرکب .(NO) اگر الگوریتم NO برگرداند عدد n قطعا مرکب است اما اگر YES برگردانده شود یا n اول است و یا فرضیه توسعه یافته ریمان غلط است.

[کران شاهد]
$W = \min\{\lfloor 2\ln^2 n \rfloor, n-1\}$
[محک اول‌قویاًمحتمل]
for $2 \leq a \leq W$ **do**
    Decide via Algorithm 4 whether n is a strong probable prime base a
    if n is not a strong probable prime base a **then**
        return NO
return YES

---

[19] Heath-Brown

۲-۴ شبه‌اول‌های لوکاس

می‌توانیم ایده‌های بیان شده در بخش‌های قبل را تعمیم دهیم تا شامل میدان‌های متناهی نیز شوند. از قدیم، مفهوم شبه‌اول لوکاس با استفاده از زبان دنباله‌های بازگشتی دودویی (دنباله‌هایی که هر جمله طبق دو جمله پیشین خود محاسبه می‌شود) بیان شده است. بهتر است که این ساختار شبه‌اول را با استفاده از زبان میدان‌های متناهی بررسی کنیم، نه فقط به دلیل اینکه بیشتر مفاهیم امروزی اینگونه بررسی می‌شوند، بلکه به دلیل اینکه ایده‌ها در این صورت کمتر موردی به نظر می‌آیند و به راحتی برای میدان‌های با مرتبه بیشتر قابل تعمیم هستند.

۲-۴-۱ فیبوناچی و شبه‌اول‌های لوکاس

دنباله ۰، ۱، ۱، ۲، ۳، ۴ ...که به نام دنباله فیبوناچی[20] شناخته می‌شوند ویژگی جالبی در ظاهر شدن اعداد در جایگاه اعداد اول دارد. در این دنباله عدد ظاهر شده در جایگاه j را با u_j نمایش می‌دهیم که j از ۰ شروع می‌شود.

قضیه ۲-۲۶. *اگر n عددی اول باشد آنگاه*

$$u_{n-\epsilon_n} \equiv ۰ \ (\text{پیمانه‌ی } n)، \qquad (۲-۵)$$

که ۱ $= \epsilon_n$ وقتی (پیمانه‌ی ۵) ۱$\pm \equiv n$، ۱$- = \epsilon_n$ وقتی (پیمانه‌ی ۵) ۲$\pm \equiv n$ و ۰ $= \epsilon_n$ وقتی (پیمانه‌ی ۵) ۰ $\equiv n$. به طور دقیق‌تر ϵ_n همان نماد لژاندر[21] $\left(\frac{n}{5}\right)$ است.

این قضیه را در ادامه اثبات خواهیم کرد.

تعریف ۲-۲۷. *گوییم عدد مرکب n شبه‌اول فیبوناچی است اگر ۲-۵ برقرار باشد.*

برای مثال کوچک‌ترین عدد شبه‌اول فیبوناچی که نسبت به ۱۰ اول است عدد ۳۲۳ است.
مطالعه اعداد شبه‌اول فیبوناچی فقط به دلیل کنجکاوی نیست. همان‌طور که خواهیم دید محکی که بر اساس قضیه فوق توصیف می‌شود و مشخص می‌کند عددی شبه‌اول یا مرکب است بسیار سریع و قابل اجرا روی اعداد بسیار بزرگ است. در واقع تقریباً دو برابر یک محک شبه‌اول معمولی طول

[20] Fibonacci

[21] Legendre symbol

می‌کشد تا اجرای این محک تمام شود. همچنین ترکیب این محک با محک شبه‌اول در پایه ۲ محکی بسیار کارآمد است چرا که تا به امروز عدد (پیمانه‌ی ۵) $n \equiv \pm ۲$ شناسایی نشده است که هم شبه‌اول در پایه ۲ باشد و هم شبه‌اول فیبوناچی [۲].

در اثبات قضیه ۲-۲۶ به نظر می‌رسد که با هیچ کار اضافی، می‌توانیم یک نتیجه کلی‌تر را اثبات کنیم. دنباله فیبوناچی در شرط بازگشتی $u_j = u_{j-۱} + u_{j-۲}$ با چندجمله‌ای بازگشتی (چندجمله‌ای مشخصه[22]) $x^۲ - x - ۱$ صدق می‌کند. حال شکل کلی‌تری از توابع بازگشتی دودویی را درنظر میگیریم که چندجمله‌ای بازگشتی آن‌ها برابر $f(x) = x^۲ - ax + b$ باشد که a, b اعداد صحیحی هستند به صورتی که $\Delta = a^۲ - ۴b$ مربع کامل نباشد. حال قرار دهید

$$\begin{aligned} U_j = U_j(a,b) &= \frac{x^j - (a-x)^j}{x-(a-x)} \ (\text{پیمانه‌ی } f(x)) \\ V_j = V_j(a,b) &= x^j + (a-x)^j \ (\text{پیمانه‌ی } f(x)) \end{aligned} \tag{۲-۶}$$

که عمل تقسیم و باقیمانده گیری در حلقه $\mathbb{Z}[x]$ انجام میشود و از آنجا که تابع f تکین[23] است این عمل قابل انجام است. همچنین توجه کنید که چندجمله‌ای $x^j - (a-x)^j$ همیشه بر چندجمله‌ای $x - (a-x)$ بخش پذیر است.

قضیه ۲-۲۸. *هر دو دنباله (U_j) و (V_j) شرط بازگشتی متناظر با چندجمله‌ای $x^۲ - ax + b$ را برآورده می‌سازند، به عبارت دیگر*

$$U_j = aU_{j-۱} - bU_{j-۲}, \qquad V_j = aV_{j-۱} - bV_{j-۲}$$

اثبات. معادلاً ثابت می‌کنیم $U_j - aU_{j-۱} + bU_{j-۲} = ۰$ و به طور مشابه حکم برای دنباله (V_j) نیز ثابت می‌شود.

توجه کنید که در تعریف U_j، صورت بر مخرج بخش پذیر است پس تمام U_jها چند جمله‌ای

[22] Characteristic polynomial

[23] Monic

هستند. حال طبق تعریف مقدار $U_j - aU_{j-۱} + bU_{j-۲}$ را محاسبه می‌کنیم.

$$\begin{aligned}
&U_j - aU_{j-۱} + bU_{j-۲}\\
&= \frac{x^j-(a-x)^j}{x-(a-x)} - \frac{a(x^{j-۱}-(a-x)^{j-۱})}{x-(a-x)} + \frac{b(x^{j-۲}-(a-x)^{j-۲})}{x-(a-x)}\\
&= \frac{(x^j - ax^{j-۱}+bx^{j-۲}) - ((a-x)^j - a(a-x)^{j-۱} + b(a-x)^{j-۲})}{x-(a-x)}\\
&= \frac{x^{j-۲}(x^۲-ax^۱+b) - (a-x)^{j-۲}((a-x)^۲ - a(a-x)^۱ + b)}{x-(a-x)}\\
&= \frac{(x^۲-ax^۱+b)(x^{j-۲}-(a-x)^{j-۲})}{x-(a-x)} \equiv ۰ \cdot U_{j-۲} \equiv ۰ \ (\text{پیمانه‌ی } (f(x),p))
\end{aligned}$$

□

طبق ۲-۶ می‌توانیم مقادیر اولیه این دو دنباله را نیز به شکل زیر محاسبه کنیم

$$U_۰ = ۰ \text{،} U_۱ = ۱ \text{،} \quad V_۰ = ۲ \text{،} V_۱ = a.$$

حال از آنجا که هر دو دنباله در رابطه بازگشتی بر اساس دو جمله قبلی صدق می‌کنند و دو جمله اول هر دو دنباله عددی صحیح هستند پس هر دو دنباله، دنباله‌ای از اعداد صحیح هستند
مشابه قضیه ۲-۲۶ می‌توان قضیه کلی‌تر زیر را بیان و اثبات کرد. در این صورت دیگر نیازی به اثبات قضیه ۲-۲۶ که حالت خاص این قضیه که $a = ۱$ ، $b = -۱$ است، نیست.

قضیه ۲-۲۹. *فرض کنید a، b، Δ مشابه قبل تعریف شوند و دو دنباله (U_j)،(V_j) طبق ۲-۶ باشند. اگر p عددی اول باشد به طوری که $\gcd(p, ۲b\Delta) = ۱$، آنگاه*

$$U_{p-(\frac{\Delta}{p})} \equiv ۰ \ (\text{پیمانه‌ی } p). \qquad (۲-۷)$$

این قضیه را بعد تر اثبات می‌کنیم.
توجه کنید که برای $\Delta = ۵$ و عدد اول و فرد p طبق قضیه تقابل مربعی[۲۴] $(\frac{p}{۵}) = (\frac{۵}{p})$، در نتیجه قضیه ۲-۲۶ بدست می‌آید. از آنجا که نماد جاکوبی $(\frac{\Delta}{n})$ برای n اول برابر همان نماد

[24] Quadratic reciprocity

لژاندر است، مشابه قبل می‌توانیم با استفاده از قضیه ۲-۲۹ دسته جدیدی از اعداد شبه‌اول معرفی و محکی برای تشخیصشان معرفی کنیم.

تعریف ۲-۳۰. *عدد مرکب n که $\gcd(n, ۲b\Delta) = ۱$ را شبه‌اول لوکاس نسبت به $x^۲ - ax + b$ گوییم هرگاه (پیمانه‌ی n) $U_{n-(\frac{\Delta}{n})} \equiv ۰$.*

از آنجایی که (U_j) با کاهش چندجمله‌ای در پیمانه $x^۲ - ax + b$ ساخته می‌شود و همچنین از آنجا که در قضیه ۲-۲۹ و تعریف ۲-۳۰ به کاهش دنباله در پیمانه n اشاره شده است ، درواقع با اعضای حلقه $R = \mathbb{Z}_n[x]/(x^۲ - ax + b)$ سر و کار داریم. می‌توان حلقه R را توسط مجموعه زیر نمایش داد:

$$\{i + jx : \text{اعداد صحیح باشند } i, j \text{ و } ۰ \leq i, j \leq n - ۱\}.$$

جمع اعضای حلقه R مشابه جمع برداری در پیمانه n و ضرب اعضای R باتوجه به $x^۲ = ax - b$ انجام می‌گیرد. درنتیجه داریم

$$(i_۱ + j_۱x) + (i_۲ + j_۲x) = i_۳ + j_۳x$$
$$(i_۱ + j_۱x)(i_۲ + j_۲x) = i_۴ + j_۴x$$

که

$$i_۳ = i_۱ + i_۲ \ (\text{پیمانه‌ی } n), \qquad j_۳ = j_۱ + j_۲ \ (\text{پیمانه‌ی } n),$$
$$i_۴ = i_۱i_۲ - bj_۱j_۲ \ (\text{پیمانه‌ی } n), j_۴ = i_۱j_۲ + i_۲j_۱ + aj_۱j_۲ \ (\text{پیمانه‌ی } n).$$

قبل از اثبات قضیه ۲-۲۹ لازم است لم‌های زیر را ثابت کنیم.

لم ۲-۳۱. *اگر $f(x) = x^۲ - ax + bx \in \mathbb{Z}_p[x]$ در $\mathbb{Z}_p[x]$ تحویل پذیر باشد و (پیمانه‌ی p) $a^۲ - ۴b \not\equiv ۰$ آنگاه*

$$\mathbb{Z}_p[x]/(x^۲ - ax + b) \cong \mathbb{Z}_p \times \mathbb{Z}_p.$$

اثبات. از آنجا که $f(x)$ تحویل پذیر است پس وجود دارد $c_۱$ و $c_۲$ که $f(x) = (x-c_۱)(x-c_۲)$. حال طبق فرض (پیمانه‌ی p) $a^۲ - ۴b \not\equiv ۰$ در نتیجه $c_۱ \neq c_۲$ و $\gcd((x-c_۱), (x-c_۲)) = ۱$.

حال طبق قضیه باقیمانده چینی حکم برقرار است یا به عبارتی دیگر به راحتی میتوان یکریختی φ را معرفی کرد

$$\varphi(f(x)) = (\frac{f(x)\ ((x-c_1)\ \text{پیمانه‌ی})}{c_1 - c_2}, \frac{f(x)\ ((x-c_2)\ \text{پیمانه‌ی})}{c_2 - c_1})$$

که در این صورت $\varphi(x-c_1) = (0, 1)$ و $\varphi(x-c_2) = (1, 0)$. □

لم ۲-۳۲. *فرض کنید p عدد اول فرد و a و b دو عدد صحیح باشند.*
چندجمله‌ای $f(x) = x^2 - ax + b$ در $\mathbb{Z}[x]_p$ تحویل پذیر[25] است اگر و تنها اگر $(\frac{\Delta}{p}) = 1$.

اثبات.
$\Leftarrow$: ابتدا فرض کنید $f(x)$ در میدان $\mathbb{Z}_p[x]$ تحویل پذیر باشد. پس وجود دارد c و d در $\mathbb{Z}_p$ که $f(x) = (x-c)(x-d) = x^2 - (c+d)x + cd$. حال با توجه به تعریف f داریم
$c + d \equiv a\ (p$ پیمانه‌ی$)$ و $cd \equiv b\ (p$ پیمانه‌ی$)$.
در نتیجه $a^2 - 4b \equiv (c+d)^2 - 4cd = (c-d)^2\ (p$ پیمانه‌ی$)$ و در نتیجه Δ مانده مربعی[26] در پیمانه p است و داریم $(\frac{\Delta}{p}) = 1$.
$\Rightarrow$: حال فرض کنید $(\frac{\Delta}{p}) = 1$. این به آن معناست که عضوی در $\mathbb{Z}_p$ مانند t وجود دارد که $t^2 \equiv \Delta\ (p$ پیمانه‌ی$)$. حال از آنجا که p فرد است پس ۲ در $\mathbb{Z}_p$ دارای وارون است. در نتیجه

$$(x - \frac{a-t}{2})(x - \frac{a+t}{2}) = x^2 - ax + \frac{a^2 - t^2}{4} = x^2 - ax + b = f(x)$$

و $f(x)$ تحویل پذیر است. □

لم ۲-۳۳. *فرض کنید k میدان و $f(x) \in k[x]$ باشد. در این صورت اگر $f(x)$ تحویل ناپذیر باشد آنگاه $(f(x))$ در $k[x]$ ماکسیمال است (و در نتیجه $k[x]/(f(x))$ میدان است).*

اثبات. از آنجا که k میدان است پس PID نیز هست. همچنین به سادگی با استفاده از الگوریتم تقسیم و تابع gcd می‌توان نشان داد که $k[x]$ نیز PID است.
از آنجا که $f(x)$ ثابت نیست پس وارون ندارد و در نتیجه $(f(x)) \neq k[x]$. اگر وجود داشته

[25] Reducible

[26] Quadratic residue

باشد $h(x) \in k[x]$ که $(f(x)) \subseteq (h(x))$ در این صورت $f(x) \in (h(x))$ و وجود دارد $g(x) \in k[x]$ که $f(x) = g(x)h(x)$. از آنجا که $f(x)$ تحویل ناپذیر است پس یا $h(x)$ ثابت است و یا $g(x)$ که در هر دو صورت یا $(h(x)) = k[x]$ و یا $(h(x)) = (f(x))$. $\square$

حال باتوجه به لم‌های ثابت شده قضیه ۲-۲۹ را ثابت می‌کنیم.

اثبات قضیه ۲-۲۹. فرض کنید p عددی اول باشد و داشته باشیم $(\frac{\Delta}{p}) = -۱$. در این صورت Δ در حلقه $\mathbb{Z}_p$ مربع هیچ عضوی نیست (نامانده مربعی است)، پس چندجمله‌ای $x^۲ - ax + b$، که مبین[27] آن همان Δ است در حلقه $\mathbb{Z}_p$ تحویل ناپذیر است. در این صورت ایده‌آل $(x^۲ - ax + b)$ ایده‌آل ماکسیمال حلقه $\mathbb{Z}_p[x]$ است و در نتیجه حلقه $R = \mathbb{Z}_p[x]/(x^۲ - ax + b)$ یک میدان است و از آنجایی که دارای $p^۲$ عضو است پس یکریخت با میدان $\mathbb{F}_{p^۲}$ است (طبق [۱۸] تمام میدان‌های متناهی با p^k عضو با هم یکریخت هستند و این میدان را با $\mathbb{F}_{p^k}$ نمایش می‌دهند).
همچنین زیرمیدان $\mathbb{Z}_p(=\mathbb{F}_p)$ متناظر با هم‌دسته‌های $i + jx$ است که $j = ۰$ است.
در $\mathbb{F}_{p^۲}$، تابع σ که هر عضو را به توان pام آن میبرد (این تابع به خودریختی فروبینوس[28] شناخته می‌شود) دارای خواص جالبی است که به راحتی از قضیه بسط دوجمله‌ای و قضیه کوچک فرما نتیجه می‌شوند.

$$\sigma(u+v) = \sigma(u) + \sigma(v), \quad \sigma(uv) = \sigma(u)\sigma(v)$$

$\sigma(u) = u$ اگر و تنها اگر u در زیر میدان $\mathbb{Z}_p$ باشد.

میدان $\mathbb{F}_{p^۲}$ به گونه‌ای ساخته شده است که چند جمله‌ای $x^۲ - ax + b$ که در $\mathbb{Z}_p$ دارای ریشه نبود در آن دارای ریشه باشد. اما کدام یک از اعضای میدان $\mathbb{F}_{p^۲}$ ریشه های این چند جمله‌ای هستند. به وضوح x یکی از ریشه ها و با کمی بررسی $a - x\,(= a + (p-۱)x)$ ریشه دیگر این چندجمله‌ای است. از آنجا که x و $a - x$ عضو $\mathbb{Z}_p$ نیستند و از آنجا که طبق تعریف گروه گالوا تابع فروبینوس عضوی از گروه گالوا $\mathbb{F}_{p^۲}/\mathbb{F}_p$ است یکی از ویژگی‌های تابع فوربینوس که می‌توان ثابت کرد جایگشت دادن ریشه های تابع $f(x) = x^۲ - ax + b$ است داریم

$$\text{In the case } (\frac{\Delta}{p}) = -۱ : \begin{cases} x^p \equiv a - x \pmod{(f(x), p)} \\ (a-x)^p \equiv x \pmod{(f(x), p)} \end{cases} \qquad (۸\text{-}۲)$$

---

[27] Discriminant

[28] Frobenius

در این صورت (پیمانه‌ی $(f(x), p)$) $x^{p+1} - (a-x)^{p+1} \equiv x(a-x) - (a-x)x \equiv 0$،
پس طبق ۲-۶، (پیمانه‌ی p) $U_{p+1} \equiv 0$.
اثبات ۲-۷ در حالتی که p عددی اول باشد و $(\frac{\Delta}{p}) = 1$ راحت‌تر است. در این حالت چون Δ در میدان $\mathbb{Z}_p$ مانده مربعی است پس چندجمله‌ای $x^2 - ax + b$ دارای دو ریشه در این میدان است. طبق لم قبل، حلقه $R = \mathbb{Z}_p[x]/(x^2 - ax + b)$ یک میدان نیست بلکه با $\mathbb{Z}_p \times \mathbb{Z}_p$ یکریخت است و توان pام هر عضوی برابر خودش است از جمله

$$\text{In the case } (\frac{\Delta}{p}) = 1 : \begin{cases} x^p \equiv x \pmod{(f(x), p)} \\ (a-x)^p \equiv a - x \pmod{(f(x), p)} \end{cases} \qquad (۲-۹)$$

توجه کنید که فرض $\gcd(p, b) = 1$ نتیجه می‌دهد که x و $a - x$ در حلقه R وارون پذیر هستند چرا که (پیمانه‌ی $(f(x)$ $x(a-x) \equiv b$ و درنتیجه xb^{-1} وارون $a - x$ و $(a-x)b^{-1}$ وارون x است. از این رو با ضرب کردن دو طرف همنهشتی‌های ۲-۸ در وارون x و وارون $a - x$، در حلقه R داریم $x^{p-1} = (a-x)^{p-1} = 1$. همچنین (پیمانه‌ی $(f(x)$ $(x - (a-x))^2 \equiv \Delta$ و از آنجا که $\gcd(\Delta, p) = 1$ و Δ وارون پذیر است پس $(x - (a-x))$ نیز وارون پذیر است. در نتیجه طبق تعریف ۲-۶ (پیمانه‌ی p) $U_{p-1} \equiv 0$ و حکم قضیه ۲-۲۹ در همه حالات اثبات شده است. $\square$

در بخش‌های قبل اشاره کردیم که صحبت کردن از اعداد شبه‌اول در پایه ۱ بیهوده است چرا که تمام اعداد شبه اول در پایه ۱ هستند. حال در تعریف اعداد شبه‌اول لوکاس وضعیت مشابهی زمانی که $f(x) = x^2 \pm x + 1$باشد، رخ می‌دهد.

فرض کنید n عددی مرکب و نسبت به ۶ اول باشد و $f(x) = x^۲ - x + ۱$ یا به عبارتی $a = b = ۱$. نشان می‌دهیم در این حالت n شبه اول لوکاس نسبت به $f(x)$ است.
طبق تعریف $f(x)$ داریم $\Delta = a^۲ - ۴b = -۳$. همچنین چون $\gcd(n, ۶) = ۱$ پس $\gcd(n, ۲b\Delta) = ۱$.
به سادگی و با کمک استقرا می‌توان نشان داد که (پیمانه‌ی ۳) $U_j = ۰ \iff j \equiv ۰$ و به ازای مقادیر دیگر j مقدار U_j برابر ۱ یا ۱− است. پس برای این که نشان دهیم n شبه‌اول لوکاس نسبت به $f(x)$ است کافیست نشان دهیم (پیمانه‌ی ۳) $n - (\frac{-۳}{n}) \equiv ۰$.
برای اثبات این ادعا روی باقیمانده n بر ۱۲ حالت بندی می‌کنیم. از آنجا که n نسبت به ۶ اول است پس باقیمانده آن بر ۱۲ اعداد ۱، ۵، ۷ و ۱۱ می‌تواند باشد. اگر باقیمانده n بر ۱۲ برابر ۱ باشد پس (پیمانه‌ی ۴) $n \equiv ۱$ و در نتیجه از آنجا که n و ۳ فرد هستند و نسبت به هم اول طبق قضیه تقابل مربعی نماد ژاکوبی[29] داریم $(\frac{n}{۳}) = (\frac{۳}{n})$ و از آنجا که (پیمانه‌ی ۳) $n \equiv ۱$ پس $(\frac{۳}{n}) = ۱$. همچنین $(\frac{-۱}{n}) = (-۱)^{(n-۱)/۲} = ۱$ از این رو $(\frac{-۳}{n}) = ۱$ و در پیمانه ۳ همنهشت با n است. مشابهاً برای بقیه حالات باقیمانده n بر ۱۲ نیز می‌توان حکم را ثابت کرد.
با توجه به مطالب فوق تمام اعداد n که نسبت به ۶ اول باشند (به عبارتی عامل اول ۲ و ۳ نداشته باشند) که تمام اعداد که تجزیه نا بدیهی دارند در این دسته قرار می‌گیرند شبه‌اول لوکاس نسبت به $f(x)$ هستند. در نتیجه تابع f تابعی مناسب برای مطالعه اعداد شبه‌اول لوکاس نمی‌باشد.
به صورت مشابه این مطالب برای تابع $x^۲ + x + ۱$ نیز برقرار هستند. پس منطقی است که دو تابع $x^۲ \pm x + ۱$ را کنار بگذاریم.
می‌توان نشان داد از آنجا که این دو تابع تنها توابع تکین و تحویل ناپذیر با ضرایب گویا هستند که ریشه‌هایشان ریشه‌های عدد ۱ نیز هستند تنها توابعی هستند که باید کنار گذاشته شوند.

۲-۴-۲ محک فروبینوس گرانتام

نقش پر رنگ خودریختی فروبینوس در محک لوکاس در محک جدیدی که توسط گرانتام[30] معرفی شد بیشتر مورد استفاده قرار می‌گیرد. این محک قابل استفاده برای تابع دلخواه است ولی حتی در توابع درجه ۲ نیز عملکرد بهتری نسبت به محک لوکاس دارد. یکی از مزایای این محک وابستگی کم‌تر آن به دنباله بازگشتی است. برای ساده سازی محک فروبینوس را برای توابع درجه ۲ بیان

[29] Jacobi symbol
[30] Grantham

می‌کنیم و کمی در مورد حالت کلی‌تر آن صحبت می‌کنیم.
همان طور که در اثبات قضیه ۲-۲۹ دیدیم، به جای مفروضات قضیه می‌توانیم ۲-۸ و ۲-۹ را فرض بگیریم و حکم را ثابت کنیم یا به عبارت دیگر نقش اصلی در اثبات حکم را دو عبارت ۲-۸ و ۲-۹ ایفا می‌کنند. اما قضیه ۲-۲۹ تنها بخشی از نتایج این دو فرض را مشخص می‌کند.
محک فروبینوس بر پایه حکم قوی تری که از ۲-۸ و ۲-۹ نتیجه می‌شود است. در ادامه این حکم قوی‌تر را بیان می‌کنیم.

تعریف ۲-۳۴. *فرض کنید a و b اعداد صحیحی باشند که $\Delta = a^2 - 4b$ مربع نباشد. گوییم عدد مرکب n که $\gcd(n, 2b\Delta) = 1$ شبه‌اول فروبینوس نسبت به $f(x) = x^2 - ax + b$ است اگر*

$$x^n \equiv \begin{cases} a - x \pmod{(f(x), n)}, & \textit{if } (\frac{\Delta}{n}) = -1 \\ x \pmod{(f(x), n)}, & \textit{if } (\frac{\Delta}{n}) = 1 \end{cases} \qquad (۲-۱۰)$$

شاید در نگاه اول به نظر بیاید که نیمی از ۲-۸ و ۲-۹ را کنار گذاشته‌ایم؛ اما می‌توان نشان داد که اینگونه نیست و با داشتن ۲-۱۰ که به نظر نیمی از ۲-۸ و ۲-۹ است می‌توان بقیه دو عبارت را بدست آورد.

لم ۲-۳۵. *فرض کنید m و n دو عدد طبیعی و $f(x)$ ، $g(x)$ و $r(x)$ در $\mathbb{Z}[x]$ باشند. اگر $f(r(x)) \equiv 0$ (پیمانه‌ی $(f(x), n)$) و $x^m \equiv g(x)$ (پیمانه‌ی $(f(x), n)$)، آنگاه $r(x)^m \equiv g(r(x))$ (پیمانه‌ی $(f(x), n)$)*

اثبات. از آنجا که طبق فرض داریم $x^m \equiv g(x)$ (پیمانه‌ی $(f(x), n)$) پس وجود دارد تابع $h(x)$ در $\mathbb{Z}[x]$ که $x^m \equiv g(x) + f(x)h(x)$ (پیمانه‌ی n). حال از آنجا که x متغییر است، می‌توان آن را با $r(x)$ جایگزین کرد و عبارت $r(x)^m \equiv g(r(x)) + f(r(x))h(r(x))$ (پیمانه‌ی n) را بدست آورد. با توجه به اینکه طبق فرض داریم $f(r(x)) \equiv 0$ (پیمانه‌ی $(f(x), n)$) در نتیجه $r(x)^m \equiv g(r(x))$ (پیمانه‌ی $(f(x), n)$) و حکم ثابت شده است. □

قضیه ۲-۳۶. *اگر ۲-۱۰ برقرار باشد آنگاه*

$$(a - x)^n \equiv \begin{cases} x \pmod{(f(x), n)}, & \textit{if } (\frac{\Delta}{n}) = -1 \\ a - x \pmod{(f(x), n)}, & \textit{if } (\frac{\Delta}{n}) = 1 \end{cases}$$

نیز برقرار است.

اثبات. ابتدا فرض کنید $(\frac{\Delta}{n}) = ۱$. در این حالت طبق فرض داریم (پیمانه‌ی $(f(x), n)$) $x^n \equiv x$.
حال از آنجا که $\gcd(n, b) = ۱$ پس b در $\mathbb{Z}[x]/(f(x), n)$ وارون پذیر است و چون
(پیمانه‌ی $(f(x), n)$) $x(a-x) \equiv b$ پس x نیز وارون پذیر است. در نتیجه با ضرب کردن وارون
x در دو طرف عبارت (پیمانه‌ی $(f(x), n)$) $x^n \equiv x$ داریم (پیمانه‌ی $(f(x), n)$) $x^{n-۱} \equiv ۱$.
حال با توجه به لم فوق با در نظر گرفتن $g(x) = ۱$ و $r(x) = a - x$ و $m = n - ۱$ داریم
(پیمانه‌ی $(f(x), n)$) $(a-x)^{n-۱} \equiv ۱$ و در نتیجه (پیمانه‌ی $(f(x), n)$) $(a-x)^n \equiv a-x$.
حال فرض کنید $(\frac{\Delta}{n}) = -۱$. در این صورت طبق فرض داریم (پیمانه‌ی $(f(x), n)$) $x^n \equiv a-x$.
حال طبق لم فوق و در نظر گرفتن $g(x) = r(x) = a - x$ و $m = n$ داریم $(a-x)^n \equiv x$
(پیمانه‌ی $(f(x), n)$).
در نتیجه با داشتن ۲-۱۰ توانستیم مابقی عبارات ۲-۸ و ۲-۹ را بدست آوریم و حکم را ثابت کنیم. □

همچنین توجه کنید با توجه به به قضیه فوق و اثبات قضیه ۲-۲۹ تمام اعداد شبه‌اول فروبینوس، شبه‌اول لوکاس نیز هستند.

حال به راحتی می‌توان معیاری برای شبه‌اول‌های فروبینوس نسبت به یک تابع درجه دو با توجه به دنباله‌های لوکس که در قسمت قبل با نام (U_m) و (V_m) معرفی شدند، ارائه کرد.

قضیه ۲-۳۷. *فرض کنید a، b اعداد صحیحی باشند که $\Delta = a^۲ - ۴b$ مربع کامل نباشد و n عدد مرکبی باشد که $\gcd(n, ۲b\Delta) = ۱$. در این صورت n شبه‌اول فروبینوس نسبت به $x^۲ - ax + b$ است اگر و تنها اگر*

$$U_{n-\frac{\Delta}{n}} \equiv ۰ \pmod n \quad \text{و} \quad V_{n-\frac{\Delta}{n}} \equiv \begin{cases} ۲b, & \textit{when } (\frac{\Delta}{n}) = -۱ \\ ۲, & \textit{when } (\frac{\Delta}{n}) = ۱ \end{cases} \qquad (۲\text{-}۱۱)$$

اثبات. با توجه به تعریف دو دنباله (U_m) و (V_m) در ۲-۶ به راحتی می‌توان نشان داد

$$۲x^m \equiv (۲x - a)U_m + V_m \text{ (پیمانه‌ی } f(x), n) . \qquad (۲\text{-}۱۲)$$

$\Leftarrow$: ابتدا فرض کنید ۲-۱۱ بر قرار باشد و قرار دهید $f(x) = x^۲ - ax + b$. در حالتی که $(\frac{\Delta}{n}) =$ ۱- طبق فرض داریم $V_{n-(\frac{\Delta}{n})} \equiv ۲b$ و با توجه به همنهشتی ۲-۱۲ و فرض اینکه $\gcd(n, ۲) = ۱$ و درنتیجه وارون پذیری ۲، این عبارت معادل این است که (پیمانه‌ی $(f(x), n)$) $x^{n+۱} \equiv b$.
به طور مشابه در حالت $(\frac{\Delta}{n}) = ۱$، نیز عبارت $V_{n-(\frac{\Delta}{n})} \equiv ۲$ معادل این است که $x^{n-۱} \equiv ۱$ (پیمانه‌ی $(f(x), n)$).
حال با توجه به این که (پیمانه‌ی $(f(x), n)$) $x(a-x) \equiv b$ و $\gcd(n, b) = ۱$، x وارون پذیر است و وارون آن $(a-x)b^{-۱}$ است در نتیجه عبارات معادلی که برای دو حالت بدست آوردیم به ترتیب، خود معادل دو عبارت $x^n \equiv a - x$ (پیمانه‌ی $(f(x), n)$) و $x^n \equiv ۱$ (پیمانه‌ی $(f(x), n)$) هستند و در نتیجه n شبه‌اول فروبینوس نسبت به $f(x)$ است.
$\Rightarrow$: حال فرض کنید n شبه‌اول فروبینوس نسبت به $f(x)$ باشد. پس همان طور که قبل‌تر نشان دادیم n، شبه‌اول لوکاس نسبت به $f(x)$ نیز هست. طبق تعریف شبه‌اول لوکاس داریم $U_{n-\frac{\Delta}{n}} \equiv ۰$ (پیمانه‌ی n) و بخشی از حکم ثابت شده است.
حال از آنجا که $U_{n-\frac{\Delta}{n}} \equiv ۰$ (پیمانه‌ی n) طبق همنهشتی ۲-۱۲ داریم $V_{n-(\frac{\Delta}{n})} \equiv ۲x^{n-(\frac{\Delta}{n})}$ (پیمانه‌ی $(f(x), n)$).
ابتدا فرض کنید $(\frac{\Delta}{n}) = -۱$. در این صورت چون طبق تعریف شبه‌اول فروبینوس $x^n \equiv a - x$ (پیمانه‌ی $(f(x), n)$) داریم (پیمانه‌ی $(f(x), n)$) $x^{n+۱} \equiv (a-x)x \equiv b$ پس $V_{n+۱} \equiv ۲b$ (پیمانه‌ی n). و در نهایت در حالتی که $(\frac{\Delta}{n}) = ۱$،از آنجا که x در پیمانه $(f(x), n)$ وارون پذیر است و طبق تعریف شبه‌اول فروبینوس (پیمانه‌ی $(f(x), n)$) $x^n \equiv x$، در نتیجه داریم $x^{n-۱} \equiv ۱$ (پیمانه‌ی $(f(x), n)$) و (پیمانه‌ی $(f(x), n)$) $V_{n-۱} \equiv ۲$. در نتیجه ۲-۱۱ بدست می‌آید. $\square$

اولین عدد شبه‌اول فروبینوس نسبت به $x^۲ - x - ۱$ عدد ۴۱۸۱ (نوزدهمین عدد دنباله فیبوناچی)، و اولین که داشته باشیم $(\frac{۵}{n}) = -۱$ برابر ۵۷۷۷ است. در نتیجه مشاهده می‌شود که تمام اعداد شبه‌اول لوکاس، شبه‌اول فروبینوس نیستند و درنتیجه محک فروبینوس محکی قوی‌تری نسبت به محک لوکاس است. در واقع محک شبه‌اول فروبینوس می‌تواند بسیار کارآمد باشد. برای مثال برای تابع $x^۲ + ۵x + ۵$ هیچ عدد شبه‌اول فروبینوس n که $(\frac{۵}{n}) = -۱$ باشد، شناخته نشده است. اما ادعا شده است که چنین عددی وجود دارد.

۲-۴-۳ پیاده سازی محک لوکاس و فروبینوس درجه ۲

نشان خواهیم داد که می‌توان محک لوکاس را به گونه‌ای پیاده سازی کرد که زمان اجرای آن حداکثر به اندازه اجرای دو محک شبه‌اول معمولی باشد و محک فروبینوس را نیز می‌توان به گونه‌ای پیاده سازی کرد که زمان اجرای آن حداکثر به اندازه اجرای سه محک شبه‌اول معمولی باشد.
با این حال اگر پیاده سازی این دو محک را به درستی انجام ندهیم، زمان اجرای محک به مراتب از چیزی که ادعا کردیم بیشتر خواهد بود. برای دستیابی به پیچیدگی‌های زمانی که اشاره کردیم باید به صورت خلاقانه‌ای روابطی دیگر برای دو دنباله (U_j) و (V_j) که قبل‌تر تعریف کردیم بدست آوریم.
در ادامه فرض کنید مشابه قبل a و b اعداد صحیحی باشند به طوری که $\Delta = a^۲ - ۴b$ مربع کامل نباشد و دو دنباله (U_j) و (V_j) را مطابق تعریف ۲-۶ در نظر بگیرید.

قضیه ۲-۳۸. *اگر m عدد صحیح نامنفی باشد آنگاه*

$$U_m = \Delta^{-۱}(۲V_{m+۱} - aV_m). \qquad (۲\text{-}۱۳)$$

اثبات. با استفاده از استقرا قوی روی m حکم را ثابت میکنیم. برای پایهٔ استقرا حالات $m = ۰$ و $m = ۱$ را بررسی می‌کنیم.
اگر $m = ۰$، آنگاه از آنجا که پیش‌تر نشان دادیم $U_۰ = ۰$ ، $V_۰ = ۲$ و $V_۱ = a$ پس $\Delta^{-۱}(۲V_۱ - aV_۰) = ۰ = U_۰$ و حکم برقرار است. اگر $m = ۱$ آنگاه در این صورت

$$\Delta^{-۱}(۲V_۲ - aV_۱) = \Delta^{-۱}(۲(a^۲ - ۲b) - a^۲) = \Delta^{-۱}(a^۲ - ۴b) = \Delta^{-۱}\Delta = ۱ = U_۱.$$

حال فرض کنید حکم برای تمام مقادیر i که $i \leq m$ برقرار باشد. نشان می‌دهیم حکم برای $m+۱$ نیز برقرار است.
پیش‌تر رابطه بازگشتی‌ای برای دو دنباله بدست آوردیم و طبق این رابطه بازگشتی داریم $U_{m+۱} = aU_m - bU_{m-۱}$. در نتیجه طبق فرض استقرا

$$\begin{aligned} U_{m+۱} = aU_m - bU_{m-۱} &= a(\Delta^{-۱}(۲V_{m+۱} - aV_m)) - b\Delta^{-۱}(۲V_m - aV_{m-۱}) \\ &= \Delta^{-۱}(۲aV_{m+۱} - a^۲V_m - ۲bV_m + abV_{m-۱}) \\ &= \Delta^{-۱}(۲(aV_{m+۱} - bV_m) - a(aV_m - bV_{m-۱})) \end{aligned}$$

حال طبق رابطه بازگشتی دنباله (V_j) داریم

$$= \Delta^{-۱}(۲V_{m+۲} - aV_{m+۱})$$

و حکم اثبات می‌شود. □

با توجه به اینکه کار با دنباله (V_j) ساده‌تر است هرگاه نیاز به محاسبه عضوی از دنباله (U_j) داشته باشیم با استفاده از قضیه فوق و کار با دنباله (V_j) آن عضو را بدست می‌آوریم.
حال رابطه‌ای را برای دنباله (V_j) اثبات می‌کنیم که در محاسبه V_m که m عددی بسیار بزرگ است بسیار حائز اهمیت است.

قضیه ۲-۳۹. *اگر $۰ \leq j \leq k$ اعدادی صحیح باشند آنگاه*

$$V_{j+k} = V_j V_k - b^j V_{k-j}. \qquad (۲\text{-}۱۴)$$

اثبات. با استفاده از استقرای قوی روی j حکم را ثابت می‌کنیم. برای پایهٔ استقرا حالت $j = ۰$ و $j = ۱$ را بررسی می‌کنیم.
اگر $j = ۰$ آنگاه $V_۰ V_k - b^۰ V_k = ۲V_k - V_k = V_k = V_{۰+k}$ و اگر $j = ۱$ آنگاه $V_۱ V_k - bV_{k-۱} = aV_k - bV_{k-۱} = V_{۱+k}$.
حال فرض کنید به ازای تمام مقادیر کوچک‌تر مساوی j حکم برقرار باشد، نشان می‌دهیم حکم برای $j + ۱$ نیز برقرار است. مشابه قضیه قبل و با استفاده از رابطه بازگشتی که پیش‌تر برای (V_j) بدست آورده‌ایم، حکم را ثابت می‌کنیم.

$$\begin{aligned}
V_{j+۱+k} &= aV_{j+k} - bV_{j-۱+k} \\
&= a(V_j V_k - b^j V_{k-j}) - b(V_{j-۱} V_k - b^j V_{k-j+۱}) \\
&= aV_j V_k - bV_{j-۱} V_k - ab^j V_{k-j} + b^j V_{k-j+۱} \\
&= V_k(aV_j - bV_{j-۱}) - b^j(aV_{K-j} - V_{k-j+۱}) \\
&= V_k V_j - b^j(aV_{k-j} - aV_{k-j} + bV_{k-j-۱}) = V_k V_j - b^{j+۱} V_{k-j-۱}
\end{aligned}$$

و حکم ثابت می‌شود. □

فعلاً برای راحتی فرض کنید $b = ۱$ باشد. با توجه به قضیه ثابت شده و در نظر گرفتن $k = j$ و $k = j + ۱$ می‌توان دو رابطه زیر را بدست آورد:

$$.V_{۲j} = V_j^{۲} - ۲, \quad V_{۲j+۱} = V_j V_{j+۱} - a \ \ (\text{در حالتی که } b = ۱) \qquad (۲\text{-}۱۵)$$

در نتیجه با در اختیار داشتن (پیمانه‌ی n) V_j و (پیمانه‌ی n) $V_{j+۱}$ می‌توان توسط رابطه بالا یکی از جفت های ($V_{۲j}$، $V_{۲j+۱}$) یا ($V_{۲j+۱}$، $V_{۲j+۲}$) را با استفاده از ۲ ضرب و یک جمع در پیمانه n، در پیمانه n بدست آورد.
با شروع از ($V_۰$، $V_۱$) می‌توانیم از ۲-۱۵ استفاده کنیم و به صورت بازگشتی هر جفت (V_m، $V_{m+۱}$) را محاسبه کنیم. به طور مثال فرض کنید $m = ۹۷$. می‌توان به صورت زیر از $(۰, ۱)$ به $(۹۷, ۹۸)$ رسید.

$$۰, ۱ \to ۱, ۲ \to ۳, ۴ \to ۶, ۷ \to ۱۲, ۱۳ \to ۲۴, ۲۵ \to ۴۸, ۴۹ \to ۹۷, ۹۸$$

در هر گام می‌توان دو کار انجام داد. یا زوج $(a, a + ۱)$ را به $(۲a, ۲a + ۱)$ فرستاد یا به $.(۲a + ۱, ۲a + ۲)$
حرکت اول متناظر این است که از مقدار $(V_a, V_{a+۱})$ طبق رابطه بدست آمده $(V_{۲a}, V_{۲a+۱})$ را محاسبه کنیم و حرکت دوم متناظر این است که از مقدار $(V_a, V_{a+۱})$، $(V_{۲a+۱}, V_{۲a+۲})$ را محاسبه کنیم. پس در حال حاضر مسئله این است با شروع از $(۰, ۱)$ چه دنباله‌ای از حرکات مارا به جفت هدف یعنی $(m, m + ۱)$ می‌رساند.
یک راه ساده برای اینکه بفهمیم چه زنجیره‌ای از انتخاب حرکات ما را به $(m, m + ۱)$ می‌رساند این است که با شروع از $(m, m + ۱)$ به صورت بازگشتی عمل کنیم.
راه ساده دیگری که می‌تواند ما را از $(۰, ۱)$ به $(m, m + ۱)$ می‌رساند این است که نمایش مبنای ۲ عدد m را در نظر بگیریم. با شروع از با ارزش ترین رقم و حرکت به سمت کم ارزش ترین رقم هرگاه رقم آن مرحله ۰ بود حرکت اول را انجام دهیم و هرگاه ۱ بود حرکت دوم را.
به راحتی می‌توان درست بودن این روش را با در نظر گرفتن نمایش مبنای ۲ اعداد ثابت کرد.
به طور مثال همان $m = ۹۷$ را در نظر بگیرید. نمایش مبنای ۲ عدد ۹۷ برابر ۱۱۰۰۰۰۱ است.
همانطور که مشاهده می‌شود در زنجیر بالا که با شروع از (۰،۱) به (۹۷،۹۸) رسید دو حرکت او ل و حرکت آخر حرکات نوع ۲ بودند و بقیه حرکات نوع ۱. به چنین زنجیری، زنجیر دودویی لوکاس گفته می‌شود.

در شبه کد زیر ایده مطرح شده برای محاسبه دنباله (V_j) توسط زنجیر دودویی لوکاس پیاده سازی شده است.

الگوریتم ۸ زنجیر لوکاس

برای دنباله $x_0, x_1, \dots$ با قاعده محاسبه x_{2j} از روی x_j و قاعده محاسبه x_{2j+1} از روی xj, x_{j+1}، این الگوریتم برای ورودی n مقدار x_n, x_{n+1} را محاسبه می‌کند. همچنین فرض کنید نمایش باینری n را هم به صورت $(n_0, n_1, \dots, n_{B-1})$ در اختیار داریم که n_{B_1} با ارزش ترین رقم است. قاعده‌ها را نیز به صورت $x_{2j} = x_j * x_j$ و $x_{2j+1} = x_j \circ x_{j+1}$ نمایش داده‌ایم. در هر گام از حلقه در الگوریتم $u = x_j$ و $v = x_{j+1}$ برای عدد طبیعی j.

[مقدار دهی اولیه]
$(u, v) = (x_0, x_1)$
[حلقه]
for $B > j \geq 0$ **do**
  if $n_j == 1$ **then** $(u, v) = (u \circ v, v * v)$
  else $(u, v) = (u * u, u \circ v)$
return (u, v) $\triangleright$ (x_n, x_{n+1}) *برگرداندن*

تمام مطالب و روابطی که تا به اینجا بدست آوردیم برای حالتی بود که $b = 1$. اما اگر این گونه نباشد و تابع کلی $x^2 - ax + b$را در اختیار داشته باشیم چطور می‌توانیم از این مطالب و روابط کاربردی بدست آمده استفاده کنیم.

قضیه ۲ - ۴۰. *در دنباله (V_j) که قبل تر با استفاده از تابع$x^2 - ax + b$ تعریف کردیم اگر$a = bc$ و $b = d^2$ آنگاه*

$$V_m(cd, d^2) = d^m V_m(c, 1)$$

(منظور از $V_m(a, b)$ جمله mام دنباله (V_j) است که با توجه به تابع$x^2 - ax + b$ تعریف شده است.)

اثبات. با استفاده از استقرای قوی حکم را ثابت می‌کنیم. برای پایهٔ استقرا حالت $m = 0$ و $m = 1$ را بررسی می‌کنیم.
اگر $m = 0$، آنگاه $V_0(cd, d^2) = 2 = d^0 V_0(c, 1)$ و حکم برقرار است. اگر $m = 1$ آنگاه $V_1(cd, d^2) = cd = dc = dV_1(c, 1)$ و باز هم حکم برقرار است.
حال فرض کنید حکم برای تمام مقادیر کم‌تر از m برقرار باشد، نشان می‌دهیم حکم برای m نیز

برقرار است. با توجه به فرض استقرا و رابطه بازگشتی دنباله (V_j) می‌توان نوشت

$$\begin{aligned} V_m(cd, d^۲) &= cdV_{m-۱}(cd, d^۲) - d^۲V_{m-۲}(cd, d^۲) \\ &= cdd^{m-۱}V_{m-۱}(c, ۱) - d^۲d^{m-۲}V_{m-۲}(c, ۱) \\ &= d^m(cV_{m-۱}(c, ۱) - V_{m-۲}(c, ۱) = d^mV_m(c, ۱) \end{aligned}$$

و حکم ثابت می‌شود. $\square$

با توجه به این قضیه، در حالتی که b برابر ۱ نباشد اما مربع کامل باشد می‌توان با استفاده از رابطه اثبات شده در قضیه از روابطی که برای حالت $b = ۱$ بدست آوردیم استفاده کرد. به صورت کلی اگر b مربع کامل باشد به صورتی که $b = d^۲$ و $\gcd(n, b) = ۱$ آنگاه داریم

$$V_m(a, d^۲) \equiv d^mV_m(ad^{-۱}, ۱) \ (\text{پیمانه‌ی } n)$$

که $d^{-۱}$ وارون ضربی d در پیمانه n است. پس در حالتی که b مربع کامل باشد را می‌توانیم به حالت $b = ۱$ تبدیل کنیم و از ویژگی‌های این حالت استفاده کنیم. در حلت کلی لزومی ندارد که b مربع کامل باشد اما می‌توانیم از قضیه زیر استفاده کنیم تا مسئله را به حالتی که b مربع کامل است تغییر دهیم.

قضیه ۲-۴۱. *اگر m عدد صحیح نامنفی و a، b اعداد صحیح دلخواه باشند داریم*

$$V_{۲m}(a, b) = V_m(a^۲ - ۲b, b^۲).$$

اثبات. با استفاده از استقرای قوی روی m حکم را ثابت می‌کنیم. برای پایهٔ استقرا حالات $m = ۰$ و $m = ۱$ را بررسی می‌کنیم.

اگر $m = ۰$ آنگاه $V_{۲m}(a, b) = V_m(a^۲ - ۲b, b^۲) = ۲$ و حکم برقرار است.

اگر $m = ۱$ آنگاه در این صورت طبق رابطه بازگشتی دنباله (V_j)، $V_۲(a, b) = a^۲ - ۲b$ و $V_۱(a^۲ - ۲b, b^۲) = a^۲ - ۲b$ و در این حالت نیز حکم برقرار است.

حال فرض کنید حکم برای m برقرار باشد، نشان می‌دهیم حکم برای $m + ۱$ نیز برقرار است.

حالات $m = ۰$ و $m = ۱$ را بررسی کردیم پس در ادامه فرض می‌کنیم $m \geq ۲$. با توجه به رابطه

۲-۱۴ داریم

$$V_{۲(m+۱)}(a,b) = V_۲(a,b)V_{۲m}(a,b) - b^۲V_{۲m-۲}$$

با توجه به فرض استقرا:

$$= V_۱(a^۲-۲b,b^۲)V_m(a^۲-۲b,b^۲) - (b^۲)^۱V_{m-۱}(a^۲-۲b,b^۲) = V_{m+۱}(a^۲-۲b,b^۲)$$

و حکم ثابت می‌شود. □

پس عدد مؤلفهٔ دوم برای دنباله دوم مربع کامل است. در نتیجه اگر $\gcd(n,b) = ۱$ و قرار دهیم $A \equiv b^{-۱}V_۲(a,b) \equiv a^۲b^{-۱} - ۲$ (پیمانه‌ی n) آنگاه

$$.V_{۲m}(a,b) \equiv b^mV_m(A,۱) \text{ (پیمانه‌ی } n) \qquad (۲\text{-}۱۶)$$

به طور مشابه داریم

$$.U_{۲m}(a,b) \equiv ab^{m-۱}U_m(A,۱) \text{ (پیمانه‌ی } n)$$

پس با استفاده از رابطه ۲-۱۳ (با $a = A$، $b = ۱$ که Δ برابر $A^۲ - ۴$ می‌شود) داریم

$$.U_{۲m}(a,b) \equiv (a\Delta)^{-۱}b^{m+۱}(۲V_{m+۱}(A,۱) - AV_m(A,۱)) \text{ (پیمانه‌ی } n) \qquad (۲\text{-}۱۷)$$

با توجه به مطالب گفته شده به طور خلاصه می‌توانیم از زنجیر دودویی لوکاس استفاده کنیم تا برای عدد طبیعی n که نسبت به b اول است به صورت کارآمدی ($V_m(A,۱)$، $V_{m+۱}(A,۱)$) را در پیمانه n محاسبه کنیم (A را نیز به پیمانه n در نظر می‌گیریم).
در نتیجه با استفاده از روابط ۲-۱۶ و ۲-۱۷ می‌توان $V_{۲m}(a,b)$و (پیمانه‌ی n) $U_{۲m}(a,b)$ را محاسبه کرد. حال با در نظر گرفتن $۲m = n - (\frac{\Delta}{n})$ و با کمک قضایای ثابت شده، می‌توانیم مشخص کنیم آیا عدد n شبه‌اول لوکاس یا شبه‌اول فروبینوس نسبت به $x^۲ - ax + b$ است یا خیر.
قضیه زیر جمع بندی نکات و روابطی است که بدست آوردیم و اثبات آن تنها با استفاده از تعاریف و قضیه‌هایی که پیشتر اثبات کردیم به سادگی امکان پذیر است.

قضیه ۲-۴۲. *فرض کنید a، b، Δو A مطابق تعاریفی که قبل تر انجام دادیم باشند و n عدد*

مرکبی باشد که نسبت به $۲ab\Delta$ اول است. در این صورت n شبه‌اول لوکاس نسبت به $x^۲ - ax + b$ است اگر و تنها اگر

$$AV_{\frac{۱}{۲}(n-(\frac{\Delta}{n}))}(A, ۱) \equiv ۲V_{\frac{۱}{۲}(n-(\frac{\Delta}{n}))+۱}(A, ۱) \ (\text{پیمانه‌ی } n). \qquad (۲\text{-}۱۸)$$

علاوه بر این n شبه‌اول فروبینوس نسبت به $x^۲ - ax + b$ است اگر و تنها اگر علاوه بر همنهشتی بالا داشته باشیم

$$b^{(n-۱)/۲}V_{\frac{۱}{۲}(n-(\frac{\Delta}{n}))}(A, ۱) \equiv ۲ \ (\text{پیمانه‌ی } n). \qquad (۲\text{-}۱۹)$$

با توجه به توضیحات داده شده برای محاسبه اعضای دنباله (V_j) برای $(m = \frac{۱}{۲}(n - (\frac{\Delta}{n}))$، جفت $(V_m(A, ۱)$، $V_{m+۱}(A, ۱))$ در پیمانه n با کمتر از $۲\lg n$ ضرب و $\lg n$ جمع در پیمانه n قابل محاسبه است.

نیمی از ضرب‌های انجام شده در پیمانه n در واقع به توان ۲ رساندن هستند. در محک فرما نیز $\lg n$ به توان ۲ رساندن و حداکثر $\lg n$ جمع در پیمانه n وجود دارد (اگر از الگوریتم نردبان دودویی استفاده کنیم). از رابطه ۲-۱۸ نتیجه می‌شود که زمان اجرای محک لوکاس حداکثر به اندازه ۲ برابر زمان اجرای محک فراما است. همچنین با توجه به رابطه ۲-۱۹ در محک فروبینوس نیاز به محاسبه (پیمانه‌ی n) $b^{(n-۱)/۲}$ نیز داریم، پس در نتیجه زمان اجرای محک فروبینوس (برای چندجمله‌ایه‌های درجه ۲) حداکثر سه برابر زمان اجرای محک فرما است.

با توجه به نزدیک بودن زمان اجرای محک فرما و فرما قوی با محک لوکاس و فروبینوس، این محک ها معمولا در کنار هم برای تشخیص اول یا مرکب بودن عدد n استفاده می‌شوند. در ادامه شبه‌کد این محک‌ها با استفاده از مطالب این بخش آورده شده است.

الگوریتم ۹ محک اول‌محتمل لوکاس و فروبینوس

برای اعداد صحیح n،a،b داده شده و $\Delta = a^{۲} - ۴b$ که Δ مربع کامل نباشد و $n > ۱$، $\gcd(n, ۲ab\Delta) = ۱$ این الگوریتم در صورت اول بودن یا شبه‌اول لوکاس بودن n نسبت به $x^{۲} - ax + b$ عبارت ”n اول‌محتمل لوکاس با پارامتر های a و b است“ را بر می‌گرداند و در غیر این صورت عبارت ”n مرکب است“ را بر می‌گرداند.

[پارامترهای کمکی]
$A = a^2 b^{-1} - 2 \pmod n$
$m = (n - (\frac{\Delta}{n}))/2$
[زنجیر دودویی لوکاس]
Using Algorithm 8 calculate the last two terms of the sequence $(V_0, V_1, ..., V_m, V_{m+1})$, with initial values $(V_0, V_1) = (2, A)$ and specific rules $V_{2j} = V_j^2 2 \pmod n$ and $V_{2j+1} = V_j V_{j+1} - A \pmod n$.
[نتیجه]
if $AV_m \equiv 2V_{m+1} \pmod n$ **then**
    return “n اول‌محتمل لوکاس با پارامتر های a و b است.”
return “n مرکب است.”

الگوریتم برای اعداد اول‌محتمل فروبینوس نیز بسیار مشابه است و قسمت [نتیجه] تفاوت دارد. این قسمت به صورت زیر تغییر میکند:

[محک لوکاس]
if $AV_m \not\equiv 2V_{m+1} \pmod n$ **then**
    return “n مرکب است.”

و همچنین این قسمت اضافه می‌شود:

[محک فروبینوس]
$B = b^{(n-1)/2} \pmod n$
if $BV_m \equiv 2 \pmod n$ **then**
    return “n اول‌محتمل فروبینوس با پارامتر های a و b است.”
return “n مرکب است.”

۲-۴-۴ ملاحظات نظری و محک‌های قوی‌تر

اگر $x^۲ - ax + b$ چندجمله‌ای تحویل ناپذیر در $\mathbb{Z}[x]$ و مخالف $x^۲ \pm x + ۱$ باشد، در [۱۹] نشان داده شده است اعداد شبه‌اول لوکاس نسبت به $x^۲ - ax + b$ در مقایسه با اعداد اول نادر هستند.
از آنجا که اعداد شبه‌اول فروبینوس نسبت به $x^۲ - ax + b$ زیر مجموعه‌ای از اعداد شبه‌اول لوکاس نسبت به همین چندجمله‌ای هستند پس آن‌ها در مقایسه با اعداد اول حتی نادرتر هستند.
نشان داده شده است که برای هر چندجمله‌ای تحویل ناپذیر $x^۲ - ax + b$، نامتناهی عدد شبه‌اول فروبینوس و در نتیجه نامتناهی عدد شبه‌اول لوکاس وجود دارد. این گزاره برای حالت شبه‌اول فیبوناچی در [۲۰] ، برای اعداد شبه‌اول لوکاس در [۲۱] و برای اعداد شبه‌اول فروبینوس در [۲۲] نشان داده شده است. البته اثبات نامتنهی بودن اعداد شبه‌اول فروبینوس فقض در حالت $(\frac{\Delta}{n}) = ۱$ نشان داده شده است.
برای تعدادی مثال چندجمله‌ای درجه ۲ خاص، مثل $x^۲ - x - ۱$ که همان چندجمله‌ای اعداد شبه‌اول فیبوناچی است، نشان داده شده است که در حالت $(\frac{\Delta}{n}) = -۱$ نیز تعداد اعداد شبه‌اول فروبینوس نامتناهی هستند. (به [۲۳] و [۲۴] رجوع کنید.)
به تازگی روتکیویچ[31] نشان داده است که برای هر $x^۲ - ax + b$ که $\Delta = a^۲ - ۴b$ مربع نیست، نامتناهی عدد شبه‌اول لوکاس مثل n وجود دارند که $(\frac{\Delta}{n}) = -۱$.
مشابه مفهوم اعداد قویاًشبه‌اول که در بخش‌های قبل معرفی کردیم، می‌توانیم اعداد "شبه‌اول لوکاس قوی" و "شبه‌اول فروبینوس قوی" را تعریف کنیم.
فرض کنید n عدد فرد و اولی باشد که $b\Delta$ را نمی‌شمارد. در حلقه $R = \mathbb{Z}_n[x]/(f(x))$ در حالتی که $(\frac{\Delta}{n}) = ۱$ ممکن است داشته باشیم $z^۲ = ۱$ ولی $z \neq \pm ۱$. برای مثال اگر $f(x) = x^۲ - x - ۱$، $n = ۱۱$ و $z = ۳ + ۵x$ باشند این حالت رخ می‌دهد. با این حال، قضیه زیر برقرار است.

قضیه ۲-۴۳. *اگر n عدد اول فرد و $f(x) = x^۲ - ax + b$ باشند و در حلقه $R = \mathbb{Z}_n[x]/((fx))$ برای عدد m داشته باشیم $(x(a-x)^{-۱})^{۲m} = ۱$ آنگاه $(x(a-x)^{-۱})^m = \pm ۱$.*

اثبات. ابتدا فرض کنید $(\frac{\Delta}{n}) = -۱$. در اثبات قضیه ۲-۲۹ نشان دادیم در این حالت حلقه R با میدان $\mathbb{F}_{n^۲}$ یکریخت است . با توجه به فرض $(x(a-x)^{-۱})^m$ یک جواب برای معادله $X^۲ = ۱$ در این میدان است. اما می‌دانیم جواب های این معادله در هر میدان برابر ± ۱ است پس $(x(a-x)^{-۱})^m = \pm ۱$.

[31] Rotkiewicz

در حالتی که $(\frac{\Delta}{n}) = ۱$ نیز در اثبات قضیه ۲-۲۹ نشان دادیم در این حالت $f(x)$ تحویل پذیر و حلقه R با حلقه $\mathbb{Z}_n \times \mathbb{Z}_n$ یکریخت است. اگر $f(x) = (x-c)(x-d)$ باشد به راحتی می‌توان نشان داد که تابع φ از $\mathbb{Z}_n[x]/(f(x))$ به $\mathbb{Z}_n \times \mathbb{Z}_n$ با ضابطه

$$\varphi(h(x)) = (h(x)\ (\text{پیمانه‌ی } x-c), h(x)\ (\text{پیمانه‌ی } x-d))$$

یک یکریختی از دامنه به هم‌دامنه است. با توجه به تعریف φ، $\varphi(a-x) = (a-c, a-d)$ و $\varphi(x) = (c,d)$. حال چون طبق فرض $(x(a-x)^{-۱})^{۲m} = ۱$ پس طبق یکریختی بودن φ، $c^{۲m}(a-c)^{-۲m} = ۱$ و $d^{۲m}(a-d)^{-۲m} = ۱$.

حال چون n عددی اول است پس $\mathbb{Z}_n$ میدان است و در نتیجه $c^m(a-c)^{-m} = \pm ۱$ و $d^m(a-d)^{-m} = \pm ۱$ و در نتیجه $\varphi((x(a-x)^{-۱})^m) = (\pm ۱, \pm ۱)$. پس تنها زمانی $(x(a-x)^{-۱})^m \neq \pm ۱$ رخ می‌دهد که یکی از دو عبارت $c^m(a-c)^{-m}$ و $d^m(a-d)^{-m}$ برابر ۱ و دیگری برابر -۱ باشد. اما چنین حالتی نمی‌تواند رخ دهد چرا که داریم

$$c^m(a-c)^{-m} \cdot d^m(a-d)^{-m} = (cd)^m((a-c)(a-d))^{-m} = b^m b^{-m} = ۱.$$

پس در این حالت نیز $\varphi((x(a-x)^{-۱})^m) = \pm ۱$ و با توجه به یکریختی بودن φ باید $(x(a-x)^{-۱})^m = \pm ۱$ باشد و حکم ثابت می‌شود. □

طبق عبارات ۲-۸ و ۲-۹ در حلقه R داریم $(x(a-x)^{-۱})^{n-(\frac{\Delta}{n})} = ۱$. چرا که در حالت $(\frac{\Delta}{n}) = -۱$ داریم $(x(a-x)^{-۱})^{n-(\frac{\Delta}{n})} = x^{n+۱}(a-x)^{-(n+۱)}$ و طبق عبارات ۲-۸ و ۲-۹ این برابر است با $x(a-x) \cdot (a-x)^{-۱}x^{-۱}$ که حاصل همان ۱ است. در حالت $(\frac{\Delta}{n}) = ۱$ نیز داریم $(x(a-x)^{-۱})^{n-(\frac{\Delta}{n})} = x^{n-۱}(a-x)^{-(n-۱)}$ که طبق عبارات ۲-۸ و ۲-۹ و وارون پذیری x و $a-x$ هر دو جمله برابر ۱ و ضربشان همان ۱ است.

در نتیجه اگر $n-(\frac{\Delta}{n})$ را به صورت $۲^s t$ بنویسیم که t عدد فرد باشد آنگاه

$$\text{یا } x(a-x)^{-۱})^t \equiv ۱ \ (\text{پیمانه‌ی } (f(x), n))$$

$$\text{یا } (x(a-x)^{-۱})^{۲^i t} \equiv -۱ \ (\text{پیمانه‌ی } (f(x), n)) \text{ برای برخی } i \text{ها که } ۰ \leq i \leq s-۱.$$

که با توجه به تعریف دو دنباله (U_m) و (V_m) این معادل آن است که

یا $U_t \equiv 0$ (پیمانه‌ی n)

یا $V_{2^i t} \equiv 0$ (پیمانه‌ی n) برای برخی iها که $0 \leq i \leq s-1$.

تعریف ۲-۴۴. *اگر عبارت فوق برای عدد مرکب و فرد n که نسبت به $b\Delta$ اول است برقرار باشد، گوییم n "شبه‌اول لوکاس قوی" نسبت به $x^2 - ax + b$ است.*

به سادگی می‌توان نشان داد که هر عدد شبه‌اول لوکاس قوی، شبه اول لوکاس نیز هست.

در [۲۲] مفهوم شبه‌اول فروبینوس قوی نه فقط برای چندجمله‌ای‌های درجه ۲ بلکه برای چند جمله‌ای‌های دلخواه به طور مشابه تعمیم داده شده است. اما در اینجا ما تنها این مفهوم را برای چندجمله‌ای های درجه۲ که $(\frac{\Delta}{n}) = -1$ باشد تعریف می‌کنیم.

فرض کنید n عدد اول و فردی باشد که نسبت به $b\Delta$ اول باشد و $(\frac{\Delta}{n}) = -1$. اگر $n^2 - 1$ را به صورت $2^S T$ که T عددی فرد است بنویسیم طبق عبارات ۲-۸ و ۲-۹ داریم

$$x^{n^2-1} \equiv (x^{n+1})^{n-1} \equiv (x(a-x))^{n-1} \equiv b^{n-1} \equiv 1 \ (\text{پیمانه‌ی } n)$$

پس مشابه تعریف شبه‌اول لوکاس قوی

یا $x^T \equiv 1$ (پیمانه‌ی n)

یا $x^{2^i T} \equiv -1$ (پیمانه‌ی n) برای برخی iها که $0 \leq i \leq S-1$.

تعریف ۲-۴۵. *اگر عبارت فوق برای عدد شبه‌اول فروبینوس نسبت به $x^2 - ax + b$ مانند n برقرار باشد گوییم n، "شبه‌اول فروبینوس قوی" نسبت به $x^2 - ax + b$ است. (از آنجا که برقرار بودن عبارت فوق شبه‌اول فروبینوس بودن n را نتیجه نمی‌دهد، در تعریف فرض کردیم n شبه‌اول فروبینوس است تا تمام اعداد شبه‌اول فروبینوس قوی، شبه‌اول فروبینوس نیز باشند.)*

در [۲۵] نشان داده شده است تمام اعداد شبه‌اول فروبینوس قوی نسبت به $x^2 - ax + b$ مثل n که $(\frac{\Delta}{n}) = -1$، شبه‌اول لوکاس قوی نسبت به همان چندجمله‌ای هستند.

مشابه محک شبه‌اول لوکاس، محک شبه‌اول لوکاس قوی نیز حداکثر به اندازه دو محک شبه‌اول معمولی طول می‌کشد. در [۲۵] نشان داده شده است که محک شبه‌اول فروبینوس قوی نیز حداکثر

به اندازه سه محک شبه‌اول معموله هزینه زمانی دارد.
ویژگی قابل توجه اعداد شبه‌اول فروبینوس قوی از قضیه زیر که در [۲۵] مطرح و اثبات شده است نتیجه می‌شود.

قضیه ۲-۴۶. *فرض کنید n عددی مرکب باشد که مربع کامل نیست و هیچ عامل اولی کوچک‌تر از ۵۰۰۰۰ ندارد. در این صورت n شبه‌اول فروبینوس نسبت به حداکثر ۱/۷۷۱۰ تا از چندجمله‌ای‌های $x^{۲} - ax + b$ است که a و b اعداد طبیعی کوچک‌تر یا مساوی n باشند و $(\frac{a^{۲}-۴b}{n}) = -۱$ و $(\frac{b}{n}) = ۱$.*

این نتیجه باید با قضیه میلر_رابین (قضیه ۲-۱۴) مقایسه شود. اگر ۳ بار محک شبه‌اول قوی را برای عدد مرکب n انجام دهیم، احتمال اینکه الگوریتم در شناسایی عدد n به عنوان عدد مرکب شکست بخورد طبق قضیه ۲-۱۴ برابر ۱/۶۴ است اما احتمال عدم موفقیت در شناسایی عدد n به عنوان عددی مرکب با انجام یک بار محک شبه‌اول فروبینوس قوی که به همان اندازه زمان نیاز دارد طبق قضیه فوق برابر ۱/۷۷۱۰ است.
شاید جالب باشد که بدانید در [۲۶] محکی با ترکیب محک شبه‌اول قوی و محک شبه‌اول لوکس معرفی شده است که در بیش‌تر مواقع حتی از محک شبه‌اول فروبینوس قوی نیز عملکرد بهتری دارد.

۲-۴-۵ حالت کلی محک فروبینوس

در چند بخش قبل محک فروبینوس گراتام رو برای چندجمله‌ای‌های درجه ۲ بررسی کردیم. در این بخش به صورت خلاصه نشان می‌دهیم که چگونه این مفهوم به تمام چندجمله‌ای‌های داخل $\mathbb{Z}[x]$ قابل تعمیم است.
فرض کنید $f(x)$ چندجمله‌ای تکین در $\mathbb{Z}[x]$ با درجه $d \geq ۱$ باشد. لازم به فرض تحویل ناپذیری $f(x)$ نیست. حال فرض کنید p عدد اول و فردی باشد که مبین، $\mathrm{disc}(f)$، $f(x)$ را نمی‌شمارد. (مبین تابع تکین $f(x)$ با درجه d با استفاده از $(-۱)^{d(d-۱)/۲}$ برابر برآیند[32] $f(x)$ و مشتق آن قابل محاسبه است. این برآیند، دترمینان یک ماتریس $(۲d-۱) \times (۲d-۱)$ است که برای $۱ \leq i \leq d-۱$ درایه i،j آن ضریب x^{j-i} در $f(x)$ و برای $d \leq i \leq ۲d-۱$ درایه i،j آن برابر ضریب $x^{j-(i-d+۱)}$ در $f'(x)$ است. توجه کنید که اگر x^t وجود نداشته باشد ضریب آن صفر در نظر گرفته می‌شود).

[32] Resultant

تابع مبین تابعی بسیار مهم و با ویژگی‌های جالب است. به طور مثال $\mathrm{disc}(f) \neq ۰$ اگر و تنها اگر تجزیه $f(x)$ در $\mathbb{C}[x]$ عامل تحویل ناپذیر با درجه مثبت تکراری نداشته باشد. فرض نشماردن $\mathrm{disc}(f)$ توسط p نیز به این معناست که اگر $f(x)$ را به عنوان تابعی در $\mathbb{F}_p[x]$ در نظر بگیریم عامل تحویل ناپذیر تکراری در $\mathbb{F}_p[x]$ ندارد.
حال $f(x)$ را با کاهش ضرایب به پیمانه p در $\mathbb{F}_p[x]$ در نظر بگیرید. برای جلوگیری از ابهام این تابع را با $\bar{f}(x)$ نمایش می‌دهیم. چند جمله‌ای‌های $F_۱(x), F_۲(x), \dots, F_d(x)$ در $\mathbb{F}_p[x]$ را به صورت زیر تعریف می‌کنیم:

$$\begin{aligned}
F_۱(x) &= \gcd(x^p - x, \bar{f}(x)),\\
F_۲(x) &= \gcd(x^{p^۲} - x, \bar{f}(x)/F_۱(x)),\\
&\vdots\\
.F_d(x) &= \gcd(x^{p^d} - x, \bar{f}(x)/(F_۱(x)\cdots F_{d-۱}(x)))
\end{aligned}$$

با توجه به این که $\bar{f}(x)$ عامل تحویل ناپذیر تکراری ندارد می‌توان نشان داد که $F_i(x)$ برابر ضرب جملات تحویل ناپذیر درجه i تابع $\bar{f}(x)$ است.

با توجه به تعریف F_iها ادعاهای زیر برقرار است:

۱. برای هر $۱ \leq i \leq j$ درجه F_i که با $\deg(F_i(x))$ نمایش می‌دهیم بر i بخش پذیر است.

۲. برای هر $۱ \leq i \leq j$، $F_i(x)$ چندجمله‌ای $F_i(x^p)$ را می‌شمارد.

۳. برای

$$،S = \sum_{i \text{ زوج}} \frac{۱}{i}\deg(F_i(x))$$

داریم

$$.(-۱)^S = (\frac{\mathrm{disc}(f)}{p})$$

همان طور که پیشتر بیان کردیم $F_i(x)$ها ضرب تعدادی تابع درجه i هستند پس درجه $F_i(x)$ بر i بخش پذیر است و ادعای اول برقرار است. ادعای دوم نیز نه تنها برای $F_i(x)$ها بلکه برای

تمام چندجمله‌ای‌ها در $\mathbb{F}_p[x]$ برقرار است.
چرا که در مشخصه[33] میدان $\mathbb{F}_p$ برابر p است و با استفاده از بسط دو جمله‌ای و استقرا می‌توان نشان داد اگر $g(x) \in \mathbb{F}_p[x]$ آنگاه $g(x^p) = g(x)^p$ در نتیجه $g(x)|g(x^p)$. اثبات کامل و دقیق این موضوع در ۳-۱۰ قابل مشاهده است.
ایده نشان دادن ادعای سوم این است که گروه گالوای چندجمله‌ای $\bar{f}(x)$ روی $\mathbb{F}_p$ را در نظر بگیریم. خود ریختی فروبینوس که پیشتر نیز آن را معرفی کردیم (که هر عضو در میدان شکافنده[34] را به توان pام اش می‌فرستد) در واقع جایگشتی روی ریشه‌های تابع $\bar{f}(x)$ در میدان شکافنده می‌دهد. علاوه بر این، این خودریختی به صورت دوری ریشه‌های هر عامل تحویل ناپذیر را جایگشت می‌دهد و از این رو علامت کل جایگشت برابر -۱ به توان تعداد عامل‌های تحویل ناپذیر درجه زوج است. به عبارت دیگر علامت خودریختی فروبینوس دقیقا همان $(-۱)^S$ است.
با این حال، طبق قضیه گالوا، گروه گالوای یک چندجمله‌ای با ریشه‌های متمایز توسط همریختی فروبینیوس تولید می‌شود و این گروه تنها شامل جایگشت‌های زوج ریشه‌ها است اگر و تنها اگر مبین آن چندجمله‌ای مربع کامل(مانده مربعی) باشد. از این رو علامت خودریختی فروبینوس دقیقا همان نماد لژاندر $\left(\frac{\mathrm{disc}(f)}{p}\right)$ است و ادعایمان برقرار است.
ایده گرانتام این است که برقرار بودن ادعاهای فوق حتی زمانی که مطمئن نیستیم که p اول است یا نه به راحتی قابل بررسی است. اگر هر یک از این سه ادعا برقرار نباشد در این صورت p مرکب است. به عبارت دیگر این گزاره‌ها هسته اصلی محک فروبینوس هستند. برای اطلاعات بیشتر در رابطه با محک فروبینوس گرانتام در حالت کلی به [۲۵] و [۲۲] مراجعه کنید.

[33] Characteristic
[34] Splitting field

فصل ۳

اثبات اول بودن

در فصل قبل روش‌های احتمالاتی برای تشخیص سریع اعداد مرکب را مورد بررسی قرار دادیم. اگر عددی با استفاده از چنین محکی به عنوان عدد مرکب شناسایی نشود یا عددی اول است و یا در اثبات مرکب بودن آن عدد موفق نبوده‌ایم. از آنجا که انتظار نداریم به طور مداوم در اثبات مرکب بودن یک عدد مرکب شکست بخوریم، بعد از تعدادی تلاش متقاعد می‌شویم که آن عدد، عددی اول است. در حالی که برای اول بودن آن عدد اثباتی نداریم؛ تنها حدسی بر پایه‌ی آزمایش‌های عددی که انجام دادیم، داریم.
در این فصل قصد داریم بررسی کنیم که چگونه می‌توان اثبات کرد که به طور قطع یک عدد اول است.

۳-۱ محک $n - ۱$

همان طور که پیشتر هم اشاره کردیم، برای بررسی اول بودن اعداد کوچک می‌توانیم از الگوریتم تقسیم آزمایشی استفاده کنیم، اما برای اعداد بزرگ روش‌های بهتر و سریعتری وجود دارد) معمولاً اعداد بزرگ‌تر از $۱۰^{۱۲}$ را به عنوان اعداد بزرگ در نظر می‌گیریم ولی این مقدار کاملا بستگی به قدرت محاسبه‌ای که در اختیار داریم دارد).
یکی از این روش‌های بهتر بر پایه ساده‌ترین قضیه‌ای است که در فصل قبل بر مبنای آن محک شبه‌اول را طراحی کردیم یعنی قضیه کوچک فرما (قضیه ۲-۳) .
این روش که به محک $n - ۱$ شناخته می‌شود به طرز شگفت انگیزی به جای تجزیه خود عدد n

به کمک تجزیه عدد $n - ۱$ اول بودن یا نبودن عدد n را مشخص می‌کند.

۳-۱-۱ قضیه لوکاس و محک پپین

با ایده لوکاس در سال ۱۸۷۶ میلادی شروع می‌کنیم.

قضیه ۳-۱. (*قضیه لوکاس*). *اگر a ، n اعداد صحیح و $n > ۱$ باشد و*

$$\begin{aligned} &a^{n-۱} \equiv ۱ \ (\text{پیمانه‌ی } n)، \text{ ولی} \\ &a^{(n-۱)/q} \not\equiv ۱ \ (\text{پیمانه‌ی } n) \text{ برای تمام اعداد اول } q|n-۱، \end{aligned} \tag{۳-۱}$$

آنگاه n عددی اول است.

اثبات. بخش ابتدایی عبارت ۳-۱ به این معناست که مرتبه a در $\mathbb{Z}_n^*$ مقسوم‌علیه $n - ۱$ است، درحالی که بخش دوم این عبارت مشخص می‌کند که این مقسوم‌علیه باید خود $n - ۱$ باشد و در نتیجه مرتبه a در $\mathbb{Z}_n^*$ برابر $n - ۱$ است. اما مرتبه a مقسوم علیه مرتبه گروه یعنی $\varphi(n)$ نیز هست (طبق قضیه اویلر[۱]) پس $n - ۱|\varphi(n)$ و درنتیجه از آنجا که برد تابع φ اویلر اعداد طبیعی است پس $n - ۱ \leq \varphi(n)$. حال فرض کنید (فرض خلف) n عددی مرکب باشد و دارای عامل اولی مثل p باشد، آنگاه p و n هر دو عضو مجموعه اعداد ۱ تا n هستند که نسبت به n اول نیستند پس طبق تعریف تابع φ داریم $\varphi(n) \leq n - ۲$. این تناقض با $n - ۱ \leq \varphi(n)$ است و این تناقض از فرض مرکب بودن n حاصل شد. در نتیجه n اول است. □

توجه کنید که این نسخه از قضیه ۳-۱ توسط لهمر[۲] بیان شده است. صورت اصلی قضیه لوکاس به جای در نظر گرفتن q به عنوان عامل‌های اول $n - ۱$ تمام مقسوم‌علیه‌ها را در نظر می‌گیرد. فرض ۳-۱ در قضیه لوکاس برای اعداد اول هیچگاه تهی نیست، به این معنا که اگر n عددی اول باشد قطعا a وجود دارد که فرض ۳-۱ را برقرار می‌کند. چنین a را ریشه اولیه می‌نامیم و در شاخه نظریه مقدماتی اعداد نشان داده می‌شود که برای تمام اعداد اول ریشه اولیه وجود دارد [۲۷].
همچنین داشتن ریشه اولیه به این معناست که گروه ضربی $\mathbb{Z}_n^*$ دوری است و توسط هر یک از ریشه‌اولیه‌ها تولید می‌شود.

[1] Euler
[2] Lehmer

قضیه ۳-۲. *اگر* $n > ۲۰۰۵۶۰۴۹۰۱۳۱$ *باشد آنگاه حداقل دارای* $n/(۲ \ln\ln n)$ *ریشه‌اولیه متمایز در پیمانه* n *است. (عدد ۲۰۰۵۶۰۴۹۰۱۳۱ در واقع ضرب نخستین ۱۱ عدد اول به علاوه ۱ است.)*

برای اثبات این قضیه می‌توانید از مطالب مقاله [۲۸] و تمرین اول فصل چهارم [۲] استفاده کنید.
نتیجه قضیه فوق این است که اگر $n > ۲۰۰۵۶۰۴۹۰۱۳۱$ عددی اول باشد پیدا کردن عددی که شرط ۳-۱ را برقرار کند با استفاده از الگوریتم‌های احتمالاتی کار دشواری نیست. از آنجا که تعداد این اعداد در مقایسه با اعداد ۱ تا n با توجه به قضیه فوق قابل توجه است کافیست هر بار به صورت تصادفی عدد a که $۱ \leq a \leq n - ۱$ را انتخاب کنیم تا در نهایت موفق به پیدا کردن a که شرط ۳-۱ را برقرار کند شویم.
همچنین از آنجا که هر بار به صورت مستقل a را انتخاب می‌کنیم و با توجه به قضیه فوق امید ریاضی تعداد انتخاب‌های انجام شده تا پیدا شدن عضو مورد نظر $۲ \ln\ln n$ است.
با اینکه در حال حاضر هیچ الگوریتم قطعی با پیچیدگی زمانی چندجمله‌ای برای پیدا کردن ریشه‌اولیه برای اعداد اول وجود ندارد، مانع اصلی در استفاده از قضیه لوکاس برای تشخیص اول بودن یا نبودن عدد داده شده پیدا کردن ریشه‌اولیه نیست بلکه تجزیه کامل عدد $n - ۱$ است.
همانطور که می دانیم، تجزیه به عوامل اول در عمل برای بسیاری از اعداد دشوار است. اما برای تمام اعداد اینگونه نیست. برای مثال فرض کنید به دنبال اعداد اولی هستیم که از توانی از ۲ یکی بیشتر هستند یعنی اعداد اول به فرم $۲^t + ۱$. طبق اتحاد چاق و لاغر عدد t نمی‌تواند عامل فردی داشته باشد چرا که در این صورت عدد $۲^t + ۱$ عاملی غیر از ۱ و خودش دارد و نمی‌تواند اول باشد.
پس خود t نیز باید توانی از ۲ باشد. در نتیجه اعداد اولی که از توانی از ۲ یکی بیشتر هستند به فرم $F_k = ۲^{۲^k} + ۱$ هستند. اعداد این دنباله به نام اعداد فرما شناخته می‌شوند چرا که او فکر می‌کرد تمام آنها اول هستند. با توجه به این مطالب از آنجا که تجزیه عدد $۲^{۲^k}$ مشخص است استفاده از قضیه لوکاس برای تشخیص اعداد اول در دنباله اعداد فرما کاربردی است.
در سال ۱۸۷۷ میلادی، پپین[3] معیاری شبیه به معیار زیر برای تشخیص اول بودن یک عدد فرما ارائه کرد.

[3] Pepin

قضیه ۳-۳. (محک پپین). *برای* $k \geq ۱$، *عدد* $F_k = ۲^{۲^k} + ۱$ *اول است اگر و تنها اگر* $۳^{(F_k-۱)/۲} \equiv -۱$ *(پیمانه‌ی* F_k*)*.

اثبات. $\Leftarrow$: فرض کنید $۳^{(F_k-۱)/۲} \equiv -۱$ (پیمانه‌ی F_k) برقرار باشد. در نتیجه ۳-۱ برای $n = F_k$ و $a = ۳$ برقرار است. از این رو طبق قضیه لوکاس عدد F_k اول است.
$\Rightarrow$: حال فرض کنید F_k عددی اول باشد. از آنجا که ۲^k عددی زوج است پس $۲^{۲^k} \equiv ۱$ (پیمانه‌ی ۳) (به راحتی با استقرا می‌توان ثابت کرد توان‌های فرد عدد ۲ باقیمانده ۲ و توان‌های زوج عدد ۲ باقیمانده ۱ به پیمانه ۳ دارند)، در نتیجه $F_k \equiv ۲$ (پیمانه‌ی ۳). اما $F_k \equiv ۱$ (پیمانه‌ی ۴)، پس نماد لژاندر $(\frac{۳}{F_k})$ با توجه به قضیه تقابل مربعی برابر -۱ است و این به آن معناست که ۳ در پیمانه F_k مربع نیست. حال طبق محک اویلر در شاخه نظریه اعداد داریم $۳^{(F_k-۱)/۲} \equiv (\frac{۳}{F_k}) \equiv -۱$ (پیمانه‌ی F_k). □

البته نسخه اصلی این قضیه که توسط پپین ارائه شد به جای ۳ از ۵ استفاده می‌کرد (و $k \geq ۲$). توسط پروت[4] و لوکاس اشاره شد که می‌توان از ۳ نیز استفاده کرد. در این باره می‌توانید به [۲۹] مراجعه کنید.
تا به این لحظه مرکب یا اول بودن ۲۴ عدد اول دنباله فرما توسط محک پپین مشخص شده است. شاید جالب باشد که بدانید عدد $F_{۲۴}$ عددی با بیش از پنج میلیون رقم است.

۳-۱-۲ تجزیه جزئی

از آنجا که در حالت کلی دشوار ترین بخش در پیاده سازی اثبات اول بودن توسط قضیه ۳-۱ تجزیه کامل عدد $n-۱$ به عامل‌های اولش است، این سوال مطرح می‌شود که آیا از بخشی از تجزیه عدد $n-۱$ به عوامل اولش می‌توان استفاده کرد یا خیر. به طور دقیق تر فرض کنید

$$n - ۱ = FR \qquad (۳\text{-}۲)$$

و تجزیه کامل F به عوامل اولش را می‌دانیم.

قضیه ۳-۴. ([5]پوکلینگتون). *فرض کنید ۳-۲ برقرار باشد و* a *به صورتی موجود باشد که*

$$a^{n-۱} \equiv ۱ \ (\text{پیمانه‌ی } n) \text{ و } \gcd(a^{(n-۱)/q}, n) = ۱ \quad (۳\text{-}۳)$$

برای تمام اعداد اول $q|F$.

[4]Proth

[5]Pocklington

در این صورت تمام عامل‌های اول n به پیمانه F همنهشت با ۱ هستند.

اثبات. فرض کنید p عامل اول دلخواهی از n باشد. با توجه به بخش اول ۳-۳ نتیجه می‌شود که مرتبه a^R در $\mathbb{Z}_p^*$ مقسوم‌علیهی از $F = (n-1)/R$ است. با توجه به بخش دوم ۳-۳ نتیجه می‌شود که این مقسوم علیه دقیقاً برابر F است. در نتیجه F مرتبه گروه $\mathbb{Z}_p^*$ که همان $p-1$ است را می‌شمارد و p در پیمانه F همنهشت با ۱ است. □

نتیجه ۳-۵. *اگر ۳-۲ و ۳-۳ برای $F \geq \sqrt{n}$ برقرار باشند آنگاه n عددی اول است.*

اثبات. با توجه به قضیه ۳-۴ تمام عامل‌های اول n به پیمانه F همنهشت ۱ هستند پس تمام عامل‌های اول n از F بزرگتر هستند. حال از آنجا که $F \geq \sqrt{n}$ پس تمام عامل‌های اول n از $\sqrt{n}$ بزرگتر هستند و درنتیجه طبق لم ۲-۱، n اول است. □

قضیه بعد امکان نتیجه گیری در مورد اول بودن n با داشتن بخش کوچکتری از تجزیه عدد $n-1$ را فراهم می‌کند.

قضیه ۳-۶. (*بریلهارت*[6]*، لهمر، سلفیج*). *فرض کنید ۳-۲ و ۳-۳ هر دو برقرار باشند و فرض کنید $n^{1/3} \leq F < n^{1/2}$. نمایش مبنای F عدد n را در نظر بگیرید. این نمایش به صورت $n = c_2F^2 + c_1F + 1$ است که c_1 و c_2 اعداد صحیح در $[0, F-1]$ هستند. همچنین n اول است اگر و تنها اگر $c_1^2 - 4c_2$ مربع کامل نباشد.*

اثبات. از آنجا که (پیمانه‌ی F) $n \equiv 1$، نتیجه می‌شود که جایگاه یکان در نمایش مبنای F عدد n برابر ۱ است و نمایش آن همانطور که ادعا کردیم به فرم $c_2F^2 + c_1F + 1$ است. حال برای اثبات گزاره دوم صورت قضیه، معادلاً عکس نقیض آن را اثبات می‌کنیم.
$\Leftarrow$: ابتدا فرض کنید n عددی مرکب باشد. طبق ۳-۴ تمام عامل‌های اول n به پیمانه F همنهشت ۱ هستند، طبق فرض $F \geq n^{1/3}$ تمام این عوامل از $n^{1/3}$ بزرگتر هستند. در نتیجه n نمی‌تواند بیش از دو عامل اول داشته باشد (این دو عامل مساوی می‌توانند باشند). پس فرض کنید

$$n = pq \text{،} p = aF + 1 \text{،} q = bF + 1 \text{،} 0 < a \leq b.$$

در نتیجه طبق نمایش مبنای F عدد n داریم

$$c_2F^2 + c_1F + 1 = n = (aF+1)(bF+1) = abF^2 + (a+b)F + 1.$$

[6] Brillhart

هدفمان این است که نشان دهیم $c_2 = ab$ و $c_1 = a+b$، در این صورت $c_1^2 - 4c_2 = (a-b)^2$ مربع کامل است.
ابتدا توجه کنید که طبق بازه در نظر گرفته شده برای F و تساوی $n = abF^2 + (a+b)F + 1$، $F^3 \geq n > abF^2$ و در نتیجه $ab \leq F - 1$. حال نشان می‌دهیم $a + b \leq F - 1$ یا $a = 1$ و $b = F - 1$.
ابتدا فرض کنید $a = 1$، اگر $b = F - 1$ باشد آنگاه ادعایمان برقرار است و اگر $b \neq F - 1$ باشد از آنجا که $ab \leq F - 1$ پس $b < F - 1$ و $a + b \leq F - 1$ و باز هم ادعایمان درست است. در حالتی هم که $a \geq 2$ باشد از آنجا که $a \leq b$ پس چون $ab \leq F - 1$، $b \leq \frac{F-1}{2}$ و در نتیجه $a + b \leq b + b \leq F - 1$. پس در تمام حالات ادعایمان برقرار است. حال اگر قسمت دوم ادعا رخ دهد یعنی $a = 1$ و $b = F - 1$ در این صورت $n = (F+1)((F-1)F+1) = F^3 + 1$ که این تناقض با فرض $F \geq n^{1/3}$ است. پس در نتیجه هم ab و هم $a + b$ اعداد صحیح مثبت کوچکتر از F هستند. از آنجا که نمایش در مبنا یکتا است پس همان طور که می‌خواستیم نشان دهیم $c_2 = ab$ و $c_1 = a + b$ و در نتیجه $c_1^2 - 4c_2$ مربع کامل است.
$\Rightarrow$: حال فرض کنید $c_1^2 - 4c_2$ مربع کامل و برابر u^2 است. در این صورت داریم

$$n = (\frac{c_1 + u}{2}F + 1)(\frac{c_1 - u}{2}F + 1).$$

هر دو پرانتز عدد صحیح هستند چرا که (پیمانه‌ی ۲) $c_1 \equiv u$. حال تنها باید نشان دهیم که n به صورت نابدیهی به شکل ضرب دو عدد نوشته شده است. از آنجا که $c_2 > 0$ پس $|u| < c_1$ و در نتیجه هیچ یک از دو پرانتز نمی‌تواند برابر ۱ شود پس n مرکب است. $\square$

با توجه به این که الگوریتم‌های بسیار سریعی برای تشخیص مربع کامل بودن در اعداد صحیح وجود دارند به راحتی می‌توانیم از آنها کمک بگیریم تا بررسی کنیم آیا $c_1^2 - 4c_2$ مربع کامل است یا نه. در نتیجه از قضیه ۳-۶ به صورت کارآمدی می‌توان استفاده کرد تا اعداد مرکب و اول را شناسایی کرد.
قضیه بعد حتی امکان استفاده از F های کوچک تر را فراهم می‌سازد. در این جا فقط به بیان آن می پردازیم و اثبات آن به صورت کامل در [۲] وجود دارد.

قضیه ۳-۷. *(کونیاگین[7] و پامرنس). فرض کنید $n \geq 214$ و هر دو عبارت ۳-۲ و ۳-۳ برای*

[7] Konyagin

$n^{3/10} \le F < n^{1/3}$ برقرار باشند. نمایش مبنای F عدد n به صورت $c_3F^3 + c_2F^2 + c_1F + 1$است. قرار دهید $c_4 = c_3F + c_2$. در این صورت n اول است اگر و تنها اگر شرایط زیر برقرار باشند:

1. *$(c_1 + tF)^2 + 4t - 4c_4$ برای عدد صحیح $0 \le t \le 5$ مربع کامل نباشد.*

2. *فرض کنید u/v کسر مسلسل همگرا به c_1/F باشد که v بیشترین مقدار کوچکتر از $F^2/\sqrt{n}$ را داشته باشد. اگر $d = \lfloor c_4v/F + 1/2 \rfloor$، آنگاه چندجمله‌ای*
$vx^3 + (uF - c_1v)x^2 + (c_4 - dF + u)x - d \in \mathbb{Z}[x]$ هیچ ریشه صحیحی مثل a ندارد که $aF + 1$ مقسوم‌علیه نابدیهی n باشد.

اگر از قضیه ۳-۶ و ۳-۷ برای تشخیص اول بودن استفاده کنیم باید از الگوریتمی که مربع کامل بودن یا نبودن را مشخص می‌کند به عنوان زیربرنامه استفاده کنیم. علاوه بر این برای بررسی شرط دوم در قضیه ۳-۷ نیاز داریم از روش نیوتون و یا تقسیم و حل استفاده کنیم تا ریشه‌های صحیح تابع درجه ۳ای را پیدا کنیم. حال با استفاده از هر سه قضیه ۳-۴،۳-۶ و ۳-۷ الگوریتم زیر را برای تشخیص اول یا مرکب بودن عدد n ارائه می‌دهیم.

الگوریتم ۱۰ محک ۱ $- n$

فرض کنید $n \geq ۲۴۱$ و ۳-۲ برای $F \geq n^{۱/۳}$ برقرار باشد. این الگوریتم احتمالاتی در صورت تشخیص اول بودن عدد n، (YES) و در صورت تشخیص مرکب بودن عدد n، (NO) را بر می‌گرداند.

```
[محک پوکلینگتون]
Choose random a ∈ [2, n − 2]
if a^(n−1) ≢ 1 (mod n) then
    return NO
for prime q|F do
    g = gcd((a^((n−1)/q) (mod n)) − 1, n)
    if 1 < g < n then
        return NO
    if g == n then
        goto [محک پوکلینگتون]
[محک اولین اندازه]
if F ≥ n^(1/2) then
    return YES
[محک دومین اندازه]
if thenn^(1/3) ≤ F < n^(1/2)
    Cast n in base F : c2 F^2 + c1 F + 1
    if c1^2 − 4c2 not a square then
        return YES
    return NO
[محک سومین اندازه]
if n^(3/10) ≤ F < n^(1/3) then
    if conditions (1) and (2) of Theorem 3-7 hold then
        return YES
    return NO
```

اگر چه الگوریتم ۱۰ احتمالاتی است اما برگرداندن YES به معنای اول بودن و برگرداندن NO به معنای مرکب بودن عدد n است و این تشخیص کاملاً دقیق است. البته بهبودهای پیاده سازی نیز می‌توان انجام داد تا این الگوریتم بهینه‌تر عمل کند.

۳-۱-۳ گواهی مختصر

در انجام محک‌های تشخیص اول بودن اعداد، هدف این است که برهانی کوتاه برای اول بودن عدد اول p ارائه دهیم. اما از کجا می‌دانیم چنین برهانی وجود دارد؟ چرا که اگر برهان کوتاهی برای اثبات اول بودن p وجود نداشته باشد جست و جو برای پیدا کردن چنین برهانی بیهوده است. حال نشان می‌دهیم برای هر عدد اول p برهان کوتاهی یا همانطور که پرت چنین برهانی را "گواهی مختصر[۸]" می‌نامد وجود دارد که اثبات می‌کند p اول است.
به طور دقیق‌تر همیشه برهانی کوتاه بر پایه قضیه لوکاس (۳-۱) وجود دارد. ممکن است به نظر واضح باشد که اگر به گونه‌ای تجزیه کامل $p - ۱$ به عوامل اولش و ریشه اولیه a را در اختیار داشته باشیم به سرعت می‌توان برقرار بودن شرط ۳-۱ را تایید کرد و نتیجه گرفت p اول است.
با این حال، برای کامل کردن اثبات باید نشان دهیم که تجزیه‌ای که برای $p - ۱$ در اختیار داریم واقعا تجزیه آن به عوامل اولش است به این معنا که تمام q های ظاهر شده در ۳-۱ واقعا اول هستند. با توجه به این موضوع برای اثبات اول بودن p باید نشان دهیم q ها نیز همه اول هستند و این نشان می‌دهد که می‌توان به صورت بازگشتی اثبات را انجام داد. اما در این شرایط ممکن است شاخه‌های بازگشتی زیادی به وجود آیند و برهان دیگر کوتاه نباشد، با این حال نشان می‌دهیم حتی در بدترین حالت نیز تعداد این تکثیرها(شاخه‌ها) زیاد نخواهد بود.
بسیار ساده می‌توان اصلاحی کوچک و کاملا عملی در قضیه لوکاس انجام داد. ایده این است که با عدد اول $q = ۲$ به شکل دیگری نسبت به q های دیگری که $p - ۱$ را می‌شمارند رفتار کنیم. از قبل می‌دانیم که اگر p عدد اول و فردی باشد و a را نشمارد آنگاه (پیمانه‌ی p) $a^{(p-۱)/۲} \equiv \pm ۱$، همچنین اگر بدانیم (پیمانه‌ی p) $a^{(p-۱)/۲} \equiv -۱$ دیگر نیازی به بررسی (پیمانه‌ی p) $a^{p-۱} \equiv ۱$ نیست. به علاوه اگر q عامل اول فردی از $p - ۱$ باشد، $m = a^{(p-۱)/۲q}$ را در نظر بگیرید. اگر (پیمانه‌ی p) $m^q \equiv -۱$ و (پیمانه‌ی p) $m^۲ \equiv ۱$، آنگاه با استفاده از قضیه باقیمانده چینی می‌توان نشان داد مستقل از این که p اول است یا مرکب (پیمانه‌ی p) $m \equiv -۱$. در نتیجه با توجه به این که (پیمانه‌ی n) $a^{(p-۱)/۲} \equiv -۱$ و عکس نقیض جمله قبل برای این که نشان دهیم (پیمانه‌ی p) $a^{(p-۱)/q} \not\equiv ۱$ کافیست نشان دهیم (پیمانه‌ی p) $a^{(p-۱)/۲q} \not\equiv -۱$.
با توجه به مطالب فوق قضیه زیر نتیجه می‌شود.

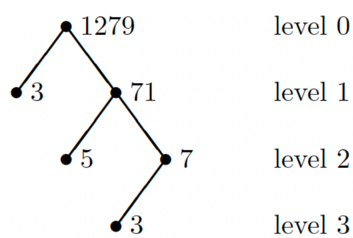
[8] Succinct certificates

قضیه ۳-۸. *فرض کنید $p > ۱$ عدد فردی باشد و*

$$\left.\begin{aligned} &a^{(p-۱)/۲} \equiv -۱ \ (\text{پیمانه‌ی } p)، \\ &a^{(p-۱)/۲q} \not\equiv -۱ \ (\text{پیمانه‌ی } p) \ \text{برای تمام اعداد اول و فرد } q|p-۱. \end{aligned}\right\} \qquad (۳\text{-}۴)$$

در این صورت p عددی اول است. متقابلا اگر p عدد اول فردی باشد آنگاه تمام ریشه اولیه‌های a برای p، ۳-۴ را برقرار می‌سازند.

حال آنچه که عموما به عنوان "درخت لوکاس[9]" شناخته می‌شود را شرح می‌دهیم. این درخت یک درخت ریشه دار است که اعداد اول فرد روی رئوس آن قرار می‌گیرند و عدد p در ریشه (سطح ۰) قرار دارد. برای هر عدد مثبت k که نشان دهنده سطوح درخت است، عدد اول r در سطح k به عدد اول q در سطح $k-۱$ یال دارد اگر و تنها اگر $r|q-۱$. برای مثل، درخت لوکاس برای $p = ۱۲۷۹$ به شکل زیر است:



فرض کنید $M(p)$ تعداد ضرب‌های پیمانه‌ای با استفاده از الگوریتم نردبان دودویی برای به توان رساندن اعداد باشد که برای اثبات اول بودن p بر اساس قضیه ۳-۸ نیاز است تا درخت لوکاس برای عدد p پیمایش شود و نشان داده شود که p اول است.

برای مثال، همان $p = ۱۲۷۹$ را در نظر بگیرید:

با توجه به درخت لوکاس آورده شده برای این عدد طبق قضیه ۳-۸ عمل می‌کنیم. پس باید ابتدا با استفاده از عامل‌های آورده شده برای ۱۲۷۸ نشان می‌دهیم ۱۲۷۹ اول است یعنی

$$۳^{۱۲۷۸/۲} \equiv -۱ \ (\text{پیمانه‌ی } ۱۲۷۹), \quad ۳^{۱۲۷۸/۶} \equiv ۷۷۵ \not\equiv -۱ \ (\text{پیمانه‌ی } ۱۲۷۹),$$
$$۳^{۱۲۷۸/۱۴۲} \equiv ۴۹۸ \not\equiv -۱ \ (\text{پیمانه‌ی } ۱۲۷۹).$$

---

[9] Lucas tree

و در ادامه باید با استفاده از قضیه ۳-۸ نشان دهیم ۷۱ و ۳ نیز خود اول هستند و این روند را ادامه دهیم. محاسبات ادامه روند در زیر آورده شده است.

$$\begin{aligned}
&۲^{۲/۲} \equiv -۱ \ (\text{پیمانه‌ی } ۳),\\
&۷^{۷۰/۲} \equiv -۱ \ (\text{پیمانه‌ی } ۷۱), \quad ۷^{۷۰/۱۰} \equiv ۱۴ \not\equiv -۱ \ (\text{پیمانه‌ی } ۷۱),\\
&\qquad\qquad\qquad\qquad ۷^{۷۰/۱۴} \equiv ۵۱ \not\equiv -۱ \ (\text{پیمانه‌ی } ۷۱),\\
&۲^{۴/۲} \equiv -۱ \ (\text{پیمانه‌ی } ۵),\\
&۳^{۶/۲} \equiv -۱ \ (\text{پیمانه‌ی } ۷), \quad ۳^{۶/۶} \equiv ۳ \not\equiv -۱ \ (\text{پیمانه‌ی } ۷),\\
&۲^{۲/۲} \equiv -۱ \ (\text{پیمانه‌ی } ۳).
\end{aligned}$$

اگر از الگوریتم نردبان دودویی برای محاسبه توان‌ها در پیمانه p استفاده کنیم تعداد ضرب‌های پیمانه‌ای مطابق زیر بدست می‌آیند: (سمت چپ توان‌هایی هستند که در روند ذکر شده ظاهر شده اند و سمت راست تعداد ضرب‌هایی است برای به توان رساندن نیاز است)

$$\begin{aligned}
۱۲۷۸/۲ &: ۱۶\\
۱۲۷۸/۶ &: ۱۱\\
۱۲۷۸/۱۴۲ &: ۴\\
۲/۲ &: ۰\\
۷۰/۲ &: ۷\\
۷۰/۱۰ &: ۴\\
۷۰/۱۴ &: ۳\\
۴/۲ &: ۱\\
۶/۲ &: ۲\\
۶/۶ &: ۰\\
۲/۲ &: ۰.
\end{aligned}$$

در نتیجه با استفاده از الگوریتم نردبان دودویی در مجموع ۴۸ ضرب پیمانه‌ای نیاز داریم تا ثابت

کنیم ۱۲۷۹ عددی اول است پس داریم $M(۱۲۷۹) = ۴۸$.
قضیه زیر در واقع نشات گرفته شده از [۳۰] است.

قضیه ۳-۹. *برای تمام اعداد اول فرد،* $M(p) < ۲\lg^۲ p$.

اثبات. فرض کنید $N(p)$ تعداد اعداد اول (نه لزوما متمایز) در درخت لوکاس برای عدد p باشد. ابتدا نشان می‌دهیم $N(p) < \lg p$. با استفاده از استقرا روی p حکم را ثابت می‌کنیم. این حکم برای $p = ۳$ برقرار است. حال فرض کنید برای تمام اعداد اول کوچک‌تر از p برقرار باشد. اگر $p - ۱$ توانی از ۲ باشد آنگاه $N(p) = ۱ < \lg p$. حال اگر $p - ۱$ عامل های فرد $q_۱, \dots, q_k$ را داشته باشد طبق فرض استقرا

$$N(p) = ۱ + \sum_{i=۱}^{k} N(q_i) < ۱ + \sum_{i=۱}^{k} \lg q_i = ۱ + \lg(q_۱ \cdots q_k) \leq ۱ + \lg(\frac{p-۱}{۲}) < \lg p.$$

در نتیجه $N(p) < \lg p$ برای تمام اعداد اول فرد برقرار است.
حال برای شمارش تعداد کل ضرب‌های پیمانه‌ای انجام شده، عملیات‌ها را اینگونه می‌شماریم. برای هر عدد تعداد ضرب‌های انجام شده در خط اول ۳-۴ را در خود راس مربوط به p و عملیات‌های انجام شده برای محاسبه خط دوم ۳-۴ را در q می‌شماریم، با این روش شمارش تعداد عملیات‌ها به صورت زیر است و همچنین به سادگی می‌توان نشان داد این شمارش تعداد عملیات‌های ضرب پیمانه‌ای به درستی شمارده می‌شود.
اگر r یکی از اعداد اول فرد ظاهر شده در درخت لوکاس برای p باشد، و $r < p$، آنگاه در درخت لوکاس عدد اول دیگری مثل $q \leq p$ وجود دارد که $r | q - ۱$. پس به ازای این یال در درخت لوکاس در مرحله‌ای باید برای یک a نشان دهیم (پیمانه‌ی q) $a^{(q-۱)/۲r} \not\equiv -۱$ و همچنین در جای دیگر باید نشان دهیم برای یک b (پیمانه‌ی r) $b^{(r-۱)/۲} \equiv -۱$. همچنین توجه کنید با استفاده از الگوریتم نردبان دودویی برای به محاسبه عددی به توان m، حداکثر $۲\lg m$ ضرب پیمانه‌ای انجام می‌شود.
پس تعداد کل عملیات‌های انجام شده به ازای این یال حداکثر

$$۲\lg(\frac{q-۱}{۲r}) + ۲\lg(\frac{r-۱}{۲}) < ۲\lg q - ۴ < \lg p$$

است. پس در نهایت

$$M(p) < ۲\lg(\frac{p-۱}{۲}) + (N(p)-۱)۲\lg p < ۲\lg p + (۲\lg p - ۱)\lg p = ۲\lg^۲ p$$

در نتیجه حکم ثابت شده است. $\square$

اگر به جای الگوریتم نردبان دودویی از الگوریتم‌های بهینه‌تری استفاده کنیم می‌توان ضریب ثابت ۲ را کاهش دهیم. البته هنوز نمی‌دانیم که آیا $c > ۰$ وجود دارد که برای نامتناهی عدد اول p در ارائه برهان با استفاده از درخت لوکاس حداقل به $c\lg^۲ p$ عملیات نیاز باشد. همچنین نمی‌دانیم آیا که آیا نامتناهی عدد اول وجود دارد که $M(p) = o(\lg^۲ p)$.
با توجه به اثبات درخت لوکاس وجود برهان برای اثبات اول بودن اعداد اول نتیجه می‌شود اما مسئله اساسی پیدا کردن چنین برهانی است.

۳-۲ محک اول بودن آگراوال، کایال و ساکسنا

در ماه اوت سال ۲۰۰۲ میلادی، آگراوال[10]، کایال[11] و ساکسنا[12] یک محک شگفت‌انگیز و جدید را اعلام و منتشر کردند که این محک می‌توانست در پیچیدگی زمانی چندجمله‌ای به طور قطع مشخص کند که یک عدد اول است یا خیر. این محک به محک AKS شناخته می‌شود. در الگوریتم ۷ دیدیم که چنین محکی در صورت برقرار بودن فرض گسترش یافته ریمان وجود دارد. علاوه بر این، در الگوریتم ۵ (محک میلر_رابین)، الگوریتمی تصادفی در اختیار داریم که در پیچیدگی زمانی چندجمله‌ای ثابت می‌کند که عدد مرکب ورودی داده شده، مرکب است. و محک‌ها و الگوریتم‌های دیگری وجود دارند که در رابطه با مرکب بودن یا نبودن اعداد تصمیم گیری می‌کنند، اما یا قطعی نیستند و یا در زمان چندجمله‌ای این کار را انجام نمی‌دهند.
محک جدید AKS نه تنها از این جهت که مشکلات نظری که بیان کردیم را حل می‌کند بلکه از جهت اینکه پیچیدگی زیادی ندارد بسیار جالب و شگفت انگیز است.
همچنین دو نفر از نویسندگان، کایال و ساکسنا، روی این مسئله به عنوان پروژه دوران کارشناسی ارشدشان به محض گرفتن مدرک کارشناسی و کار می‌کردند و تنها سه ماه بعد از گرفتن مدرک کارشناسی موفق به دستیابی و اعلام الگوریتمشان شدند. مدت کوتاهی بعد، پس از پیشنهادهای مختلف، آگراوال، کایال و ساکسنا نسخه حتی ساده تری از این محک را ارائه کردند. این دو نسخه را می‌توانید در [۳۱] و [۳۲] بیابید.

در ادامه به بررسی نسخه دوم این الگوریتم می‌پردازیم. البته نسخه‌های جدیدتر و پیچیده‌تری از این الگوریتم وجود دارند که برای جزئیات بیشتر می‌توانید به [۲] مراجعه کنید.

۳-۲-۱ محک اول بودن با استفاده از ریشه‌های یک

قضیه ۳-۱۰. *اگر n عددی اول باشد آنگاه برای هر $g(x) \in \mathbb{Z}[x]$ داریم*

$$g(x)^n \equiv g(x^n) \ (\text{پیمانه‌ی } n).$$

[10] M. Agrawal
[11] N. Kayal
[12] N. Saxena

اثبات. این قضیه به راحتی با استفاده از استقرا روی تعداد جملات تابع g یا درجه g و کمک گرفتن از قضیه کوچک فرما قابل اثبات است.
حکم را با استقرای قوی روی درجه g ثابت می‌کنیم. طبق قضیه کوچک فرما، حکم در پایه استقرا که $\deg(g) = ۰$ است برقرار است. فرض کنید حکم برای تمام توابع از درجه کوچک‌تر از d برقرار باشد. نشان می‌دهیم حکم برای تابع دلخواه از درجه d نیز برقرار است.
فرض کنید $g(x)$ تابع دلخواه از درجه dباشد. در این صورت $g(x) = a_d x^d + a_{d-۱} x^{d-۱} + \cdots + a_۱ x + a_۰$ که $a_d \neq ۰$. در این صورت

$$\begin{aligned} g(x)^n &= (a_d x^d + a_{d-۱} x^{d-۱} + \cdots + a_۱ x + a_۰)^n \\ &= ((a_d x^d) + (a_{d-۱} x^{d-۱} + \cdots + a_۱ x + a_۰))^n \end{aligned}$$

طبق بسط دو جمله‌ای[13] داریم:

$$= \sum_{i=۰}^{n} \binom{n}{i} (a_d x^d)^i (a_{d-۱} x^{d-۱} + \cdots + a_۱ x + a_۰)^{n-i}$$

حال با توجه به این که n عددی اول است و طبق فرمول محاسبه تابع انتخاب، ضریب تمام جملات متناظر با $۱ \leq i \leq n-۱$ بر n بخش پذیر است در نتیجه:

$$\equiv \binom{n}{۰} (a_{d-۱} x^{d-۱} + \cdots + a_۱ x + a_۰)^n + \binom{n}{n} (a_d x^d)^n \ (\text{پیمانه‌ی } n)$$

حال طبق قضیه کوچک فرما و فرض استقرا:

$$\begin{aligned} &\equiv a_d (x^n)^d + a_{d-۱} x^{nd-۱} + \cdots + a_۱ x^n + a_۰ \ (\text{پیمانه‌ی } n) \\ &\equiv g(x^n) \ (\text{پیمانه‌ی } n) \end{aligned}$$

و حکم ثابت می‌شود. □

[13] Binomial expansion

قضیه ۳-۱۱. *فرض کنید a و n اعداد صحیحی باشند که $n > ۰$ و $\gcd(a,n) = ۱$. اگر*

$$(x+a)^n \equiv x^n + a \ (\text{پیمانه‌ی } n) \qquad (۳\text{-}۵)$$

آنگاه n عددی اول است.

اثبات. برهان خلف. فرض کنید n عددی مرکب باشد و $n = p_۱^{\alpha_۱} \dots p_k^{\alpha_k}$ که p_iها از کوچک به بزرگ مرتب شده‌اند باشد. جمله $\binom{n}{p_۱} x^{p_۱} a^{n-p_۱}$ را در بسط دو جمله‌ای $(x+a)^n$ در نظر بگیرید. چون $\gcd(a,n) = ۱$ پس $\gcd(a,p_۱) = ۱$ و $a^{n-p_۱}$ بر $p_۱$ بخش پذیر نیست. از طرفی صورت کسر $\binom{n}{p_۱} = \frac{n(n-۱)\cdots(n-p_۱+۱)}{p_۱!}$ دارای $\alpha_۱$ عامل $p_۱$ است (چون به جز n هیچکدام بر $p_۱$ بخش پذیر نیستند). ولی مخرج نیز شامل یک عامل $p_۱$ است از این رو $p_۱^{\alpha_۱} \nmid \binom{n}{p_۱}$ و درنتیجه $n \nmid \binom{n}{p_۱} a^{n-p_۱}$ پس جمله مذکور در پیمانه n صفر نمی‌شود و باقی می‌ماند. از این رو $(x+a)^n$ نمی‌تواند برابر $x^n + a$ بشود و این تناقض با فرض است. در نتیجه فرض خلف باطل و n اول است. $\square$

با توجه به دو قضیه فوق عبارت ۳-۵ یک معیار "اگر و تنها اگر" برای اعداد اول است. تنها مشکل در استفاده از این عبارت برای تشخیص اعداد اول این است که روش سریعی برای بررسی برقرار بودن آن عبارت برای عدد دلخواه n در حال حاضر وجود ندارد. حتی در ساده ترین حالت که $a = ۱$ است تعداد جملات سمت راست همنهشتی ۳-۵ بسیار زیاد است.
اگر $f(x) \in \mathbb{Z}[x]$ چندجمله‌ای تکین دلخواهی باشد، آنگاه طبق ۳-۵ عبارت

$$(x+a)^n \equiv x^n + a \ ((f(x), n) \text{ پیمانه‌ی}) \qquad (۳\text{-}۶)$$

نیز برای تمام aها برقرار است.درنتیجه اگر n عددی اول باشد عبارت ۳-۶ برای تمام a ها و چندجمله‌ای‌های مونیک با ضرایب صحیح برقرار است. همچنین اگر درجه $f(x)$ زیادی بزرگ نباشد بررسی برقرار بودن عبارت ۳-۶ به سادگی امکان پذیر است. به طور مثال فرض کنید $a = ۱$ و $f(x) = x - ۱$. در این صورت ۳-۶ معادل

$$۲^n \equiv ۲ \ (\text{پیمانه‌ی } n)،$$

است که همان همنهشتی فرما با پایه ۲ است. این در حالیست که همان طور که قبلا دیدیم برقرار

بودن این همنهشتی برای اول بودن n لازم است اما کافی نیست. در نتیجه با دخیل کردن تابع $f(x)$ توانستیم راهی سریع برای بررسی ۳-۵ معرفی کنیم اما احتمالا معیار تشخیص اعداد اول‌مان را از دست داده‌ایم.

اما ۳-۶ بسیار کلی‌تر است و هیچ اجباری در انتخاب تابع $f(x)$ از درجه ۱ نیست. برای مثال می‌توانیم $f(x) = x^r - 1$ را برای یک مقدار کوچک r در نظر بگیریم و به طور ضمنی با ریشه‌های عدد ۱ کار کنیم. اساسا تنها کاری که باید انجام دهیم این است که مقدار مناسبی برای r انتخاب کنیم) که توسط عبارتی چندجمله‌ای بر حسب لوگاریتم n محدود شده باشد)، و برقراری شرط ۳-۶ را برای تمام aها تا جای مشخصی (باز هم توسط چندجمله‌ای بر حسب لگاریتم n محدود می‌شود) بررسی کنیم.

این محک انقدر ساده است که بهتر است ابتدا شبه‌کد آن را بیان و جزئیات را پس از آن بررسی کنیم.

الگوریتم ۱۱ محک تشخیص اول بودن آگراوال-کایال-ساکسنا (AKS)

این الگوریتم برای عدد $n > 2$ به طور قطعی مشخص می‌کند که آیا n اول است و یا مرکب.

[بررسی توان]

if n is a square or higher power **then**

  return "n مرکب است."

[مقدمه]

Find the least integer r with the order of n in $\mathbb{Z}_r^*$ exceeding $\lg^2 n$

if n has a proper factor in $[2, \sqrt{\varphi(r)} \lg n]$ **then**

  return "n مرکب است."

[همنهشتی دوجمله‌ای]

for $1 \leq a \leq \sqrt{\varphi(r)} \lg n$ **do**

  if $(x+a)^n \not\equiv x^n + a \pmod{(x^r - 1, n)}$ **then**

    return "n مرکب است."

return "n اول است."

در [بررسی توان] بررسی این که n توان دو یا بزرگ‌تر هیچ عددی نباشد می‌تواند با الگوریتم‌های سریعی مثل تکرار نیوتون[14] به سادگی بررسی شود. توجه کنید که اگر قرار باشد که n توانی از عددی باشد این توان حداکثر برابر $\lg n$ است و از آن جا که بدست آوردن تقریبی ریشه kام n با روش

[14] Newton iteration

تکرار نیوتون چند جمله‌ای است پس کافیست به ازای تمام $۲ \leq k \leq \lg n$ بررسی کنیم که ریشه kام n عددی طبیعیست یا نه. و از آنجا که تعداد k هایی که باید بررسی شوند چندجمله‌ای است و هر بار زمان چندجمله‌ای طول می‌کشد تا ریشه kام n بست بیاید کل این فرایند دارای پیچیدگی زمانی چندجمله‌ای است.
عدد r در گام [مقدمه] با بررسی اعداد بزرگ‌تر از $\lg^۲ n$ یافته می‌شود. اگر در این جست و جو r پیدا شد که $۱ < \gcd(r,n) < n$، در واقع به این نتیجه می‌رسیم که n مرکب است و می‌توانیم شبه‌کد را طوری تغییر دهیم که پس از اعلام این موضوع الگوریتم پایان پذیرد. با چنین تغییری از آنجا که در جست و جو برای r آن n هایی که عامل اول در بازه $(\lg^۲ n, r]$ دارند شناسایی می‌شوند و دیگر نیازی به بررسی این بازه برای بررسی این که n عامل اولی در این بازه نداشته باشد نیست. همچنین چون $r > \lg^۲ n$ در نتیجه $r^۲ > \lg^۲ n \cdot r$ پس $\sqrt{\varphi(r)} \lg n < \sqrt{r} \lg n < r$.
از این رو برای بررسی این که n عامل اولی در بازه $[۲, \sqrt{\varphi(r)} \lg n]$ نداشته باشد فقط کافیست $[۲, \lg^۲ n]$ را بررسی کنیم.
از آنجا که برای پیدا کردن r هیچ محدوده‌ای مشخص نکردیم شاید برایتان سوال باشد که ممکن است این جست و جو مدت زیادی ادامه پیدا کند و پیچیدگی زمانی الگوریتم آنچه که ادعا کردیم نشود. این مشکل را بعد از بررسی درستی این الگوریتم بررسی می‌کنیم.

الگوریتم ۱۱ بر پایه قضیه زیبا و اساسی زیر است.

قضیه ۳-۱۲. *(آگراوال، کایال، ساکسنا). فرض کنید $n > ۲$ و r عداد صحیح و مثبتی باشند که مرتبه n در $\mathbb{Z}_r^*$ بزرگ‌تر از $\lg^۲ n$ است. همچنین فرض کنید*

$$(x+a)^n \equiv x^n + a \ ((x^r - ۱, n) \text{ پیمانه‌ی}) \qquad (۳\text{-}۷)$$

برای تمام اعداد $۰ \leq a \leq \sqrt{\varphi(r)} \lg n$ برقرار باشد. اگر n دارای عامل اول $p > \sqrt{\varphi(r)} \lg n$ باشد، آنگاه وجود دارد عدد طبیعی m که $n = p^m$. مخصوصاً اگر بدانیم n عامل اولی در $[۱, \sqrt{\varphi(r)} \lg n]$ ندارد و توان محض هیچ عددی نیست آنگاه n عددی اول است. (منظور از توان محض توان دوم یا مرتبه بیشتر است)

اثبات. فرض کنید n دارای عامل اول $p > \sqrt{\varphi(r)} \lg n$ باشد. مجموعه G را به شکل زیر تعریف می‌کنیم.

$$G = \{g(x) \in \mathbb{Z}_p[x] : g(x)^n \equiv g(x^n) \pmod{x^r - ۱}\}$$

اگر $g_۱(x)$ و $g_۲(x)$ داخل G باشد آنگاه

$$g_۱g_۲(x)^n = g_۱(x)^n g_۲(x)^n \equiv g_۱(x^n)g_۲(x^n) = g_۱g_۲(x^n) \pmod{x^r - ۱}$$

و در نتیجه G نسبت به ضرب بسته است.
با توجه به فرض ۳-۷، به ازای تمام $۰ \leq a \leq \sqrt{\varphi(r)}\lg n$، چندجمله‌ای $x+a$ داخل G است.
پس از آنجا که G نسبت به ضرب بسته است تمام عبارات

$$\prod_{۰ \leq a \leq \sqrt{\varphi(r)}\lg n} (x+a)^{\epsilon_a}،$$

که ϵ_a ها اعداد صحیح نامنفی هستند داخل G قرار دارند. توجه کنید که از آنجایی که $p > \sqrt{\varphi(r)}\lg n$ پس این چند جمله‌ای ها دو به دو متمایز هستند و هیچکدام برابر صفر نیستند. (اگر دو تا از این عبارات با هم برابر باشند با مقایسه ریشه‌هایشان به این نتیجه می‌رسیم که باید با هم برابر باشند، همچنین $\mathbb{Z}_p[x]$ حوزه صحیح است و هیچ یک از $x+a$ ها صفر نیست و در نتیجه حاصل ضرب هیچ تعدادی از آنها برابر صفر نمی‌شود.)
در نتیجه تعداد اعضای G به مفهومی زیاد است و در ادامه از این موضوع استفاده خواهیم کرد.
حال نشان می‌دهیم که G اجتماع کلاس‌های هم ارزی باقیمانده‌ها بر $x^r - ۱$ است. یعنی اگر $g_۱(x) \in G$، $g_۲(x) \in \mathbb{Z}_p[x]$ و $g_۲(x) \equiv g_۱(x)$ (پیمانه‌ی $x^r - ۱$) آنگاه $g_۲(x) \in G$. در واقع با تغییر متغیر x به x^n در عبارت آخر نتیجه می‌شود که $g_۱(x^n) \equiv g_۲(x^n)$ (پیمانه‌ی $x^{nr} - ۱$) و از آنجا که $x^r - ۱$ مقسوم‌علیه $x^{nr} - ۱$ است این همنهشتی در پیمانه $x^r - ۱$ نیز برقرار است.
پس

$$g_۲(x)^n \equiv g_۱(x)^n \equiv g_۱(x^n) \equiv g_۲(x^n) \ (\text{پیمانه‌ی } x^r - ۱)،$$

و همان طور که ادعا کردیم $g_۲(x) \in G$.
به طور خلاصه:

- مجموعه G تحت ضرب بسته است و تمام تک جمله‌ای های $x + a$ که $۰ \leq a \leq \sqrt{\varphi(r)}\lg n$ داخل G هستند و G اجتماعی از کلاس‌های هم ارزی باقیمانده به $x^r - ۱$ است.

تابع J را به صورت زیر تعریف می‌کنیم:

$$J = \{j \in \mathbb{Z} : j > ۰, g(x)^j \equiv g(x^j) \pmod{x^r - ۱} \text{ for each } g(x) \in G\}.$$

با توجه به تعریف G، داریم $n \in J$ و به وضوح $۱ \in J$. همچنین از آنجا که طبق تعریف G اعضای G عضو $\mathbb{Z}_p[x]$ نیز هستند و برای هر $g(x) \in \mathbb{Z}_p[x]$ طبق قضیه ۳-۱۰ داریم $g(x)^n = g(x^n)$ پس این رابطه در پیمانه $x^r - ۱$ نیز برای تمام $g \in G$ برقرار است و در نتیجه $p \in J$.
حال نشان می‌دهیم J نیز نسبت به ضرب بسته است. فرض کنید $j_۱, j_۲ \in J$ و $g(x) \in G$. از آنجا که G تحت ضرب بسته است داریم $g(x)^{j_۱} \in G$ و از آنجا که $j_۱ \in J$ پس $g(x)^{j_۱} \equiv g(x^{j_۱})$ (پیمانه‌ی $x^r - ۱$) و در نتیجه $g(x^{j_۱}) \in G$. حال از آنجا که $j_۲ \in J$ و $g(x^{j_۱}) \in G$ پس $g(x^{j_۱})^{j_۲} \equiv g((x^{j_۲})^{j_۱})$ پس:

$$g(x)^{j_۱j_۲} \equiv g(x^{j_۱})^{j_۲} \equiv g((x^{j_۲})^{j_۱}) = g(x^{j_۱j_۲}) \ (x^r - ۱ \text{ پیمانه‌ی}),$$

و در نتیجه $j_۱j_۲ \in J$. پس J نیز به مفهومی دارای تعداد زیادی عضو است.
به طور خلاصه:

- مجموعه j شامل ۱، n، p است و تحت ضرب بسته است.

فرض کنید K میدان شکافنده $x^r - ۱$ روی $\mathbb{F}_p$ باشد. در نتیجه از آنجا که $x^r - ۱$ در $\mathbb{F}_{p^r}$ به صورت کامل شکافته می‌شود پس K یک میدان متناهی با مشخصه[15] p است. طبق تعریف میدان شکافنده، K کوچک ترین میدان روی $\mathbb{F}_p$ است که دارای تمام ریشه‌های rام یک است.
نشان می‌دهیم عضوی در K وجود دارد که توان‌هایش تنها تمام ریشه‌های rام یک را می‌سازد. به عبارت دیگر ریشه rام اولیه برای یک وجود دارد.
فرض کنید R مجموعه تمام ریشه‌های rام یک در میدان K باشد. به سادگی می‌توان نشان داد R با عملگر ضرب تشکیل گروه می‌دهد. همچنین در میدان K حداکثر r ریشه rام برای یک وجود دارد و در نتیجه R مجموعه‌ای متناهی است. فرض کنید تعداد اعضای این مجموعه برابر $\mathrm{Ord}(R)$ باشد. حال قرار دهید $\psi(d)$ برابر تعداد اعضای R با مرتبه d باشد. در این صورت چون مرتبه هر عضو مرتبه گروه را می‌شمارد پس ψ فقط برای $d|\mathrm{Ord}(R)$ نا صفر است. حال فرض کنید a عضوی از مرتبه d باشد در این صورت $< a >$ دارای دقیقا d عضو است و تمام این اعضا جواب

[15] Characteristic

معادله ۱ $= X^d$ در این میدان هستند. از آنجا که این معادله در میدان K حداکثر d جواب دارد پس جواب‌های این معادله دقیقا همان $\langle a\rangle$ هستند. پس یا عضو مرتبه d وجود ندارد و ۰ $= \psi(d)$ و یا طبق فرمول $\mathrm{Ord}(a^t) = \frac{\mathrm{Ord}(a)}{\gcd(t,\mathrm{Ord}(a))}$ تنها $\varphi(d)$ عضو مرتبه d وجود دارد.
از آنجا که هر عضو R دارای مرتبه متناهیست و چون طبق مطلب قبل $\psi(d) \leq \varphi(d)$ پس

$$\mathrm{Ord}(R) = \sum_{d|\mathrm{Ord}(R)} \psi(d) \leq \sum_{d|\mathrm{Ord}(R)} \varphi(d) = \mathrm{Ord}(R).$$

(تساوی سمت راست طبق خاصیت تابع فی اویلر برقرار است.) در نتیجه تمام نامساوی‌ها مساوی هستند و $\psi(d) = \varphi(d)$. پس ۱ $\psi(\mathrm{Ord}(R)) = \varphi(\mathrm{Ord}(R)) \geq$. در این صورت عضوی با مرتبه $\mathrm{Ord}(R)$ وجود دارد و این عضو همان ریشه rام اولیه یک است.
فرض کنید $\zeta \in K$ ریشه rام اولیه یک باشد و فرض کنید $h(x)$ چندجمله‌ای کمینه[16] برای ζ باشد. چند جمله‌ای کمینه برای α چندجمله‌ای تکین با کمترین درجه است که α ریشه آن باشد. به سادگی می‌توان نشان داد که چندجمله‌ای کمینه یکتا و تحویل ناپذیر است و اگر چندجمله‌ای دارای ریشه α باشد آنگاه چندجمله‌ای کمینه α آن چندجمله‌ای را می‌شمارد. در نتیجه از آنجا که $h(x)$ چندجمله‌ای کمینه ζ است و ζ خود ریشه ۱ $- x^r$ است پس $h(x)$ عامل تحویل ناپذیری از ۱ $- x^r$ است.
حال با کمی بررسی مطالب گفته شده به سادگی می‌توان نشان داد $K = \mathbb{F}_p(\zeta) \cong \mathbb{F}_p[x]/(h(x))$.
نکته اساسی که در ادامه از آن استفاده می‌کنیم این است که همریختی از $\mathbb{Z}_p[x]/(x^r - ۱)$ به $k = \mathbb{F}_p(\zeta)$ که x را به ζ می‌فرستد و ۱ را به ۱ واقعا یک همریختی است و تنها نکته در اثبات همریختی بودن این تابع این است که ۱ $h(x)|x^r -$. این همریختی را $\mathcal{H}$ می‌نامیم.
حال فرض کنید $\bar{G}$ تصویر G تحت همریختی $\mathcal{H}$ باشد. بنابر این

$$\bar{G} = \{\gamma \in K : \gamma = g(\zeta) \text{ for some } \ g(x) \in G\}.$$

توجه کنید که با توجه به خواص همریختی اگر $g(x) \in G$ و $j \in J$ آنگاه $g(\zeta)^j = g(\zeta^j)$.
فرض کنید d مرتبه زیر گروه $\mathbb{Z}_r^*$ که با n و p تولید می‌شود باشد. قرار دهید

$$G_d = \{g(x) \in G : g(x) = ۰ \text{ or } \ \deg g(x) < d\}.$$

[16]Minimal polynomial

از آنجا که $r < \varphi(r) \leq d$، اعضای G_d همه به پیمانه $x^r - ۱$ متمایز هستند. نشان می‌دهیم تحدید همریختی $\mathcal{H}$ روی G_d یک به یک است. فرض کنید $g_۱(x), g_۲(x) \in G_d$ و $g_۱(\zeta) = g_۲(\zeta)$. ادعا می‌کنیم که باید $g_۱(x) = g_۲(x)$ باشد. اگر $j = n^a p^b$ که a و b اعداد صحیح نامنفی هستند آنگاه $j \in J$، پس

$$g_۱(\zeta^j) = g_۱(\zeta)^j = g_۲(\zeta)^j = g_۲(\zeta^j).$$

با توجه به تعریف d این تساوی برای d مقدار متفاوت برای j در پیمانه r برقرار است. اما از آنجا که ζ ریشه rام اولیه است پس ζ^j ها متفاوت هستند اگر j در پیمانه r متفاوت باشد. در نتیجه چند جمله‌ای $g_۱(x) - g_۲(x)$ در میدان k دارای d ریشه است اما درجه این چند جمله‌ای طبق تعریف $\bar{G}$ از d کمتر است. پس چون تعداد ریشه‌های آن از درجه‌اش بیشتر است این چند جمله‌ای تابع ثابت صفر است و همانطور که ادعا کردیم $g_۱(x) = g_۲(x)$. به طور خلاصه:

- اعضای متمایز G_d در تناظر با اعضای متمایز $\bar{G}$ هستند.

این موضوع را روی چند جمله‌ای‌های

$$g(x) = \prod_{۰ \leq a \leq \sqrt{d}\lg n} (x+a)^{\epsilon_a} \text{ یا } g(x) = ۰،$$

که ϵ_a یا ۰ است یا ۱ در نظر بگیرید. از آنجا که $\varphi(r) \geq d$، پس $g(x)$ در G است. علاوه بر این چون مرتبه n در $\mathbb{Z}_r^*$ بیشتر از $\lg^۲ n$ است و توان‌های n زیر مجموعه گروه تولید شده توسط n و p است پس $d > \lg^۲ n$ و در نتیجه $d > \sqrt{d}\lg n$. پس در تمام حالات انتخاب ϵ_a ها از بین ۰ و ۱ به جز حالتی که همه برابر ۱ باشند توان $g(x)$ از $\sqrt{d}\lg n$ کمتر می‌شود و داخل G_d قرار می‌گیرد. از این رو حداقل

$$۱ + (۲^{\lfloor\sqrt{d}\lg n\rfloor + ۱} - ۱) > ۲^{\lfloor\sqrt{d}\lg n\rfloor} = n^{\sqrt{d}}$$

عضو در G_d وجود دارد. و طبق مطالبی که پیشتر بررسی کردیم حداقل $n^{\sqrt{d}}$ عنصر در $\bar{G}$ وجود دارد. به طور خلاصه:

- داریم $\#\bar{G} \geq \#G_d > n^{\sqrt{d}}$.

همانطور که پیشتر گفتیم $K \cong \mathbb{F}_p[x]/(h(x))$ که $h(x)$ چندجمله‌ای تحویل ناپذیر در $\mathbb{F}_p[x]$ است. فرض کنید درجه این چندجمله‌ای برابر k باشد. در نتیجه $K \cong \mathbb{F}_{p^k}$. بنا بر این اگر j، j.

اعداد صحیح مثبتی باشند که $j \equiv j_\circ \pmod{p^k - ۱}$ و $\beta \in K$ آنگاه $\beta^j = \beta^{j_\circ}$. حال قرار دهید

$$J' = \{j \in \mathbb{Z} : j > ۰, j \equiv j_\circ \pmod{p^k - ۱} \text{ for some } j_\circ \in J\}.$$

اگر $j \equiv j_\circ \pmod{p^k - ۱}$ که $j_\circ \in J$ و $g(x) \in G$ آنگاه $g(\zeta)^j = g(\zeta)^{j_\circ} = g(\zeta^{j_\circ}) = g(\zeta^j)$. همچنین از آنجا که J تحت ضرب بسته است پس J' نیز تحت ضرب بسته است. به علاوه، از آنجا که $np^{k-۱} \equiv n/p \pmod{p^k - ۱}$، $n/p \in J'$.

به طور خلاصه:

- مجموعه J' تحت ضرب بسته و شامل ۱، p، n/p است و برای هر $j \in J'$ و $g(x) \in G$ داریم $g(\zeta)^j = g(\zeta^j)$.

عدد $p^a(n/p)^b$ که a و b اعداد صحیح در $[۰, \sqrt{d}]$ هستند را در نظر بگیرید. از آنجا که p و n/p در زیرگروه با مرتبه d گروه $\mathbb{Z}_r^*$ هستند که توسط p و n تولید می‌شود و چون بیشتر از d انتخاب برای جفت (a,b) وجود دارد پس دو جفت متمایز $(a_۱, b_۱)$ و $(a_۲, b_۲)$ وجود دارند که $j_۱ := p^{a_۱}(n/p)^{b_۱}$ و $j_۲ := p^{a_۲}(n/p)^{b_۲}$ در پیمانه r همنهشت هستند. در نتیجه چون ζ ریشه $x^r - ۱$ است پس $\zeta^{j_۱} = \zeta^{j_۲}$. همچنین از آنجا که $j_۱, j_۲ \in J'$ داریم

$$g(\zeta)^{j_۱} = g(\zeta^{j_۱}) = g(\zeta^{j_۲}) = g(\zeta)^{j_۲} \text{ for all } g(x) \in G.$$

به عبارت دیگر، به ازای هر $\gamma \in \bar{G}$ داریم $\gamma^{j_۱} = \gamma^{j_۲}$. اما دیدیم که $\bar{G}$ بیشتر از $n^{\sqrt{d}}$ عضو دارد و از آنجا که $j_۱, j_۲ \leq p^{\sqrt{d}}(n/p)^{\sqrt{d}} = n^{\sqrt{d}}$ پس چندجمله‌ای $x^{j_۱} - x^{j_۲}$ بیشتر از درجه‌اش ریشه دارد پس باید چندجمله‌ای ثابت صفر باشد و در نتیجه $j_۱ = j_۲$. از این رو $p^{a_۱}(n/p)^{b_۱} = p^{a_۲}(n/p)^{b_۲}$ پس

$$n^{b_۱ - b_۲} = p^{b_۱ - b_۲ - a_۱ + a_۲},$$

و از آنجا که دو جفت $(a_۱, b_۱)$ و $(a_۲, b_۲)$ متمایز بودند پس توان n و p در تساوی بالا نمی‌تواند صفر باشد و طبق یکتایی تجزیه در $\mathbb{Z}$، n توانی از p است. □

در اثباتی که ارائه دادیم از بخشی از ایده‌های [۳۳] استفاده کردیم. حال درستی الگوریتم ۱۱ مستقیما از قضیه ۳-۱۲ نتیجه می‌شود.

۳-۲-۲ تحلیل زمانی الگوریتم ۱۱

پیچیدگی زمانی بررسی برقرار بودن همنهشتی

$$(x+a)^n \equiv x^n + a \ (x^r - ۱, n \ \text{پیمانه‌ی})$$

در بخش [همنهشتی دوجمله‌ای] در الگوریتم ۱۱ تابعی از r و $\ln n$ است. پس حیاتیست که نشان دهیم خود r نیز چند جمله‌ای از $\ln n$ است. این موضوع از قضیه زیر نتیجه می‌شود.

قضیه ۳-۱۳. *فرض کنید عدد صحیح* $n \geq ۳$ *داده شده باشد و* r *کوچک‌ترین عددی باشد که مرتبه* n *در* $\mathbb{Z}_r^*$ *از* $\lg^۲ n$ *بیشتر باشد. آنگاه* $r \leq \lg^۵ n$.

اثبات. فرض کنید $r_۰$ کوچک‌ترین عدد اولی باشد که

$$N := n(n-۱)(n^۲-۱)\cdots(n^{\lfloor \lg^۲ n \rfloor}-۱)$$

را نمی‌شمارد. در این صورت $r_۰$ کوچک‌ترین عدد اولی است که مرتبه n در $\mathbb{Z}_{r_۰}^*$ بیشتر از $\lg^۲ n$ پس $r < r_۰$. از نامساوی ۱۶.۳ در [۲۸] نتیجه می‌شود که اگر $x \geq ۴۱$ باشد ضرب اعداد اول در $[۱, x]$ از ۲^x بیشتر است. با بررسی اعداد $۳۱ \leq x \leq ۴۱$ در می‌یابیم که نامساوی گفته شده در این بازه نیز برقرار است.
حال ضرب اعداد اولی که N را می‌شمارند حداکثر برابر N است و

$$N < n^{۱+۱+۲+\cdots+\lfloor \lg^۲ n \rfloor} = n^{\frac{۱}{۲}\lfloor \lg^۲ n \rfloor^۲ + \frac{۱}{۲}\lfloor \lg^۲ n \rfloor + ۱} < n^{\lg^۴ n} = ۲^{\lg^۵ n}.$$

از این رو عدد اول $r_۰ \leq \lg^۵ n$ وجود دارد که اگر $\lg^۵ n \geq ۳۱$ باشد N را نمی‌شمارد. □

با نشان دادن این که r با استفاده از چندجمله‌ای بر حسب $\lg n$ محدود می‌شود اثبات این که الگوریتم ۱۱ در زمان چندجمله‌ای و به طور قطعی تشخیص می‌دهد که عدد داده شده اول است و یا مرکب به پایان می‌رسد.
اما این الگوریتم دقیقا چقدر سریع است و پیچیدگی زمانی آن چیست؟. با کمی بررسی درمی‌یابیم که پیچیدگی زمانی اصلی الگوریتم در [همنهشتی دوجمله‌ای] است. در این بخش برای به توان n رساندن $(x+a)$ طبق الگوریتم نردبان دودویی $\lg n$ بار ضرب چند جمله‌ای انجام می‌دهیم و از

آنجا که این چند جمله‌ای ها را در پیمانه $x^r - 1$ بدست می‌آوریم هر بار دو چندجمله‌ای حداکثر درجه $r - 1$ را در هم ضرب می‌کنیم. پس هر بار یک جمله از چندجمله‌ای اول و یک جمله از چندجمله‌ای دوم را در هم ضرب میکنیم. پیچیدگی زمانی ضرب کردن ضرایب این دو تک جمله برابر $\lg^2 n$ است و از آنجا که برای ضرب این دو چند جمله‌ای باید r^2 ضرب تک جمله‌ای انجام دهیم پس پیچیدگی زمانی ضرب این دو چندجمله‌ای برابر $r^2 \lg^n$ می‌شود.
بعد از ضرب این دو چند جمله‌ای حداکثر درجه $r - 1$ باید چندجمله‌ای را به پیمانه $x^r - 1$ محاسبه کنیم. ابتدا باید توان‌های بزرگ‌تر مساوی r را حذف و ضریبشان را به ضریب جمله بادرجه r تا کم‌تر اضافه کنیم که این کار با پیچیدگی زمانی $r \lg n$ قابل انجام است. همچنین باید ضرایب را به پیمانه n بدست آوریم که از آنجا که نهایتا r ضریب وجود دارد پس پیچیدگی زمانی این کار برابر $r \lg^2 n$ است.
پس پیچیدگی زمانی محاسبه $(x + a)^n$ به پیمانه $(x^r - 1, n)$ برابر است با

$$.O((r^2 \lg^2 n + r \lg n + r \lg^2 n) \lg n) = O(r^2 \lg^3 n)$$

حال در بخش [همنهشتی دوجمله‌ای] این کار را باید $\sqrt{\varphi(r)} \lg n < \sqrt{r} \lg n$ بار انجام دهیم پس پیچیدگی زمانی کل بخش [همنهشتی دوجمله‌ای] برابر $O(r^{2/5} \lg^4 n)$ پس طبق محدوده بدست آمده برای r این پیچیدگی زمانی برابر $O(\lg^{16/5} n)$ است.
اینجا فقط قصد داشتیم نشان دهیم که چگونه پیچیدگی زمانی این الگوریتم چند جمله‌ای است اما این الگوریتم بسیار سریع تر از تحلیلی است که ارائه دادیم چرا که این تحلیل بدون هیچ بهینه‌سازی در عملیات ها انجام شد و الگوریتم‌های بسیار سریعتری برای به توان رساندن یک چندجمله‌ای و ضرب دو عدد وجود دارند.
برای اطلاعات بیشتر در مورد این الگوریتم به [۲] رجوع کنید.

فصل ۴

خم‌های بیضوی

تاریخچه خم‌های بیضوی به بیش از یک قرن پیش برمی‌گردد. خم‌های بیضوی که در ابتدا برای تجزیه و تحلیل کلاسیک توسعه داده شدند، به نظریه اعداد انتزاعی و محاسباتی راه پیدا کرده‌اند و اکنون به‌عنوان یک ابزار اصلی به کار برده می‌شوند. مانند خود اعداد اول، خم‌های بیضوی دارای جنبه‌های شگفت‌انگیز ظرافت، پیچیدگی و قدرت هستند. خم‌های بیضوی نه تنها ساختارهای جبری معروفی هستند، بلکه ابزاری قدرتمند برای مطالعه اعداد اول و تجزیه اعداد در اختیارمان قرار می‌دهند.

۴-۱ مقدمات خم‌های بیضوی

از آنجا که نظریه بسیار عمیق و پیچیده‌ای در پس خم‌های بیضوی قرار گرفته است تنها به بیان ویژگی‌های کلی این خم‌ها می‌پردازیم و مقدمات این شخه را بیان نمی‌کنیم . برای جزئیات بیشتر می‌توانید به [۳۴]، [۳۵]، [۳۶] و [۲] رجوع کنید.

تعریف ۴-۱-۱. *خم درجه ۳ و هموار $y^۲ = x^۳ + ax + b$ با ضرایب داخل میدان F را که دارای حداقل یک نقطه با مختصات داخل F باشد که تمام مختصات برابر صفر نباشند را یک خم بیضوی می‌نامیم. می‌توان نشان داد که اگر مشخصه میدان F برابر ۲ و ۳ نباشد آنگاه $y^۲ = x^۳ + ax + b$ معرف یک خم بیضوی است اگر و تنها اگر $۴a^۳ + ۲۷b^۲ \neq ۰$.*
مجموعه نقاط این خم همراه با نقطه در بینهایت که با O نمایش می‌دهیم را با $E(F)$ نشان می‌دهیم.

پس

$$E(F) = \{(x,y) \in F \times F : y^۲ = x^۳ + ax + b\} \cup \{O\}$$

توجه کنید که معادله اصلی معدله $y^۲z = x^۳ + axz^۲ + bz^۳$ است که ما نقاط تصویری این خم را در چارت XY در نظر میگیریم و معادله و این نقاط متناظر با نقاط روی خم $y^۲ = x^۳ + ax + b$ می‌شوند؛ البته تنها نقطه ای که در این چارت دیده نمی‌شود نقطه‌ای با مختصات $[x,y,z] = [۰ : ۱ : ۰]$ است که این همان نقطه در بینهایت است و با O نمایشش می‌دهیم.

میتوان نشان داد که مجموعه $E(F)$ با عملی که در زیر تعریف می‌کنیم تشکیل گروه می‌دهند.

تعریف ۴-۲. *فرض کنید $E(F)$ یک خم بیضوی بر اساس معادله $y^۲ = x^۳ + ax + b$ و با ضرایب داخل میدان F باشد. همچنین فرض کنید مشخصه میدان F برابر ۲ و ۳ نباشد. دو نقطه روی این خم مثل $P_۱ = (x_۱, y_۱)$ و $P_۲ = (x_۲, y_۲)$ که لزوما متمایز نیستند را در نظر بگیرید و O نیز همان نقطه در بینهایت است. عملگرهای $+$ و وارون آن یعنی $-$ را به شکل زیر تعریف می‌کنیم:*

۱. $-O = O$

۲. $-P_۱ = (x_۱, -y_۱)$

۳. $O + P_۱ = P_۱$

۴. *اگر* $P_۲ = -P_۱$ *آنگاه* $P_۱ + P_۲ = O$

۵. *اگر* $P_۲ \neq P_۱$ *آنگاه* $P_۱ + P_۲ = (x_۳, y_۳)$ *که*

$$x_۳ = m^۲ - x_۱ - x_۲$$

$-y_۳ = m(x_۳ - x_۱) + y_۱$ *که شیب m به شک زیر تعریف می‌شود*

$$m = \begin{cases} \frac{y_۲ - y_۱}{x_۲ - x_۱}, & \textit{if } x_۲ \neq x_۱ \\ \frac{۳x_۱^۲ + a}{۲y_۱}, & \textit{if } x_۲ = x_۱ \end{cases}$$

تعبیر هندسی جالبی برای این گروه وجود دارد که می‌تونید در منابعی که پیشتر اشاره کردیم مشاهده کنید.

برای هر نقطه داخل خم E مثل P و هر عدد طبیعی مثل n، n بار جمع شدن P با خودش را به صورت $[n]P$ نمایش می‌دیم. و همچنین $[۰]P$ را همان عضو همانی گروه یعنی O در نظر می‌گیریم. علاوه بر این $[-n]P$ را همان $-[n]P$ تعریف می‌کنیم. بر اساس یکی از قضایای پایه‌ای نظریه گروه ها وقتی که F میدان متناهی باشد و درنتیجه تعداد نقاط خم E متناهی باشند داریم

$$[\#E(F)]P = O$$

این یکی از نکات اساسی در استفاده‌های کاربردی از خم‌های بیضوی است.

توجه کنید که خم‌های بیضوی تنها روی میدان‌ها قابل تعریف هستند و اگر F در تعاریف قبل میدان نباشد خم تعریف شده لزوما ویژگی های گفته شده را ندارد. و ما قصد داریم دقیقا از این نکته استفاده کنیم تا تشخیص دهیم عدد n اول است یانه. می‌دانیم $\mathbb{Z}_n$ یک میدان است اگر و تنها اگر n اول باشد. پس اگر ما خم $y^۲ = x^۳ + ax + b$ را با ضرایب داخل $\mathbb{Z}_n$ در نظر بگیریم این خم تنها زمانی یک خم بیضوی است که n عددی اول باشد. حال نسخه پایه ای ECM را بررسی می‌کنیم.

تعریف ۴-۳. *برای عناصر a و b در حلقه $\mathbb{Z}_n$ که $\gcd(۶, n) = ۱$ و شرط مبین $\gcd(۴a^۳ - ۲۷b^۲, n) = ۱$، یک شبه‌خم بیضوی روی این حلقه مجموعه*

$$E_{a,b}(\mathbb{Z}_n) = \{(x, y) \in \mathbb{Z}_n \times \mathbb{Z}_n : y^۲ = x^۳ + ax + b\} \cup \{O\}$$

که O همان نقطه در بینهایت است. (با این توصیف اگر n عددی اول باشد هر خم بیضوی روی $\mathbb{Z}_n$ یک شبه‌خم بیضوی نیز هست.)

حال ایده اصلی الگوریتم ECM این است که شبه‌خمی دلخواه که روی $\mathbb{Z}_n$ تعریف شده است همراه با یک نقطه دلخواه مثل P روی آن در نظر بگیریم. حال با در نظر گرفتن عدد B که بر اساس بزرگی عدد n و تحلیل‌های آماری انتخاب می‌شود، شروع به محاسبه $[B]P$ می‌کنیم. می‌توان نشان داد که اگر عدد n مرکب باشد و به تعبیری دارای عامل‌های اول دور از هم باشد با انتخاب B در بازه مناسب در مرحله ای نمی‌توانیم عمل جمع را در خم انجام دهیم به این معنا که در محاسبه

شیب m در عمل جمع که پیشتر تعریف کردیم وارون $x_{۲} - x_{۱}$ یا وارون $۲y_{۱}$ موجود نمی‌باشد و در نتیجه عامل اولی مشترک با n دارند و نتیجه می‌گیریم که n عددی مرکب است. همچنین از آنجا که این روش عاملی غیر بدیهی از n را پیدا می‌کند از این الگوریتم برای تجزیه اعداد نیز استفاده می‌شود. برای جزئیات بیشتر در رابطه با این الگوریتم می‌توانید به فصل ۷ [۲] رجوع کنید.
شبه‌کد این الگوریتم به شرح زیر است:

الگوریتم ۱۲ روش خم‌های بیضوی لنسترا (ECM)

این الگوریتم عدد n که احتمال می‌دهیم مرکب باشد و $\gcd(n, ۶) = ۱$ و توان محض هیچ عددی نباشد را به عنوان ورودی می‌گیرد و سعی می‌کند عاملی غیر بدیهی برای n بیابد.

```
[انتخاب مقدار B]
B = 10000
[پیدا کردن خم و نقطه روی آن]
Choose random x, y, a ∈ [0, n − 1]
b = (y^2 − x^3 − ax) (mod n)
g = gcd(4a^3 + 27b^2, n)
if g == n then
    goto [پیدا کردن خم و نقطه روی آن]
if g > 1 then
    return g
E = E_{a,b}(Z_n)
P = (x, y)
[ضرب توان‌های اول]
for 1 ≤ i ≤ π(B) do
    Find largest integer a_i such that p_i^{a_i}
    for 1 ≤ j ≤ a_i do
        P = [p_i]P, halting the elliptic algebra if the computation of some d^1
        for addition-slope denominator d signals a nontrivial g = gcd(n, d), in which
        case return g
[عدم موفقیت]
Possibly increment B
goto [پیدا کردن خم و نقطه روی آن] or give up and be convinced that n is prime
```

این الگوریتم الهام گرفته شده از الگوریتم "$p - ۱$ پولارد[۱]" است همچنین بهینه سازی‌هایی

[1] $p - 1$ Polard

نیز بسیار شبه به بهینه سازی های الگوریتم $p-1$ پولارد وجود دارند که عملکرد الگوریتم را بهبود می‌بخشند. برای اطلاع از جزئیات بیشتر به [۲] رجوع کنید.

مشابه کاری که انجام دادیم الگوریتم‌هایی صرفا برای تشخیص اول بودن یا نبودن عدد داده شده n وجود دارند. این الگوریتم‌ها بر پایه شمارش نقاط روی یک خم بیضوی هستند. یعنی روش‌هایی سریع برای شمارش نقاط روی یک خم و قضایایی برای محدوده تعداد این نقاط در اختیار داریم پس با توجه به مطالب گفته شده می‌توانیم خمی روی حلقه $\mathbb{Z}_n$ در نظر بگیریم و تعداد نقاط روی این خم را بشماریم. اگر در شمارش این نقاط به مشکلی برخورد کردیم و یا تعداد این نقاط در بازه‌ای که انتظار داشتیم نبود به این معناست که n اول نبوده است.

همچنین روش‌هایی بر اساس همین شمارش نقاط روی خم برای تشخیص اول بودن عدد داده شده n وجود دارد که به صورت جالبی به صورت بازگشتی و از روی اول بودن یا نبودن عددی کوچکتر از n مشخص میکند که n اول است یا نه.

برای اطلاع از جزئیات این روش‌ها به [۲] رجوع کنید.

واژه‌نامه فارسی به انگلیسی

الف

اعداد اول صنعتی ..... Industrial-grade prime

اول محتمل .... Probable prime

ب

براینل .... Resultant

بسط دو جمله‌ای .... Binomial expansion

ت

تحویل پذیر .... Reducible

تقابل مربعی .... Quadratic reciprocity

تکرار نیوتون .... Newton iteration

تکین .... Monic

چ

چندجمله‌ای کمینه ...... Minimal polynomial

چندجمله‌ای مشخصه .... Characteristic polynomial

خ

خم بیضوی .... Elliptic curve

د

درجه دو .... Quadratic

درخت لوکاس .... Lucas tree

ر

رمزنگاری .... Cryptography

س

سیستم رمز .... Cryptosystem

ش

شبه‌اول .... Pseudoprime

شاهد .... Witness

غ

غربال .... Sieve

ک

کوادریلیون .... Quadrillion

گ

گواهی مختصر .... Succinct certificates

م

مانده مربعی .... Quadratic residue

مبین .... Discriminant

مرتبه .... Order

مشخصه .... Character

معیار .... Criterion

مورد آزمایشی .... Test case

میدان شکافنده .... Splitting field

میدان عددی .... Number field

ن

نماد لژاندر .... Legendre symbol

نماد ژاکوبی .... Jacobi symbol

ه

هموار .... Smooth

واژه‌نامه انگلیسی به فارسی

B

Binomial expansion .... بسط دو جمله‌ای

C

Character .... مشخصه

Characteristic polynomial .... چندجمله‌ای مشخصه

Criterion .... معیار

Cryptography .... رمزنگاری

Cryptosystem.................. سیستم رمز

D

Discriminant .... مبین

E

Elliptic curve .... خم بیضوی

I

Industrial-grade prime..... اعداد اول صنعتی

J

Jacobi symbol................ نماد ژاکوبی

L

Legendre symbol .... نماد لژاندر

Lucas tree .... درخت لوکاس

M

Minimal polynomial...... چندجمله‌ای کمینه

Monic .... تکین

N

Newton iteration .... تکرار نیوتون

Number field................. میدان عددی

O

Order .... مرتبه

P

Probable prime................ اول محتمل

Pseudoprime .... شبه‌اول

Q

Quadratic .... درجه دو

Quadratic reciprocity .... تقابل مربعی

Quadratic residue .... مانده مربعی

Quadrillion .... کوادریلیون

R

Reducible .... تحویل پذیر

Resultant .... برایند

S

Sieve .... غربال

Smooth .... هموار

Splitting field .... میدان شکافنده

Succinct certificates .... گواهی مختصر

T

Test case .... مورد آزمایشی

W

Witness .... شاهد

کتاب‌نامه

[1] M. Gardner, “Mathematical games: a new kind of cipher that would take millions of years to break,” *Scientific American*, August 1977.

[2] R. Crandall and C. Pomerance. *Prime Numbers: A Computational Perspective*. Lecture notes in statistics, Springer New York, 2006.

[3] P. Zimmermann *Results are available at:* https://members.loria.fr/PZimmermann/records/ecmnet.html.

[4] P. Erdös, “On almost primes,” *The American Mathematical Monthly*, vol.57, no.6, pp.404–407, 1950.

[5] W. R. Alford, A. Granville, and C. Pomerance, “There are infinitely many carmichael numbers,” *Annals of Mathematics*, vol.139, no.3, pp.703–722, 1994.

[6] C. Pomerance, “On the distribution of pseudoprimes,” *Mathematics of Computation*, vol.37, no.156, pp.587–593, 1981.

[7] M. Artjuhov, “Certain criteria for the primality of numbers connected with the little fermat theorem (russian),” *Acta Arith.*, vol.12, pp.355–364, 1966/67.

[8] L. Monier, “Evaluation and comparison of two efficient probabilistic primality testing algorithms,” *Theor. Comput. Sci.*, vol.12, pp.97–108, 1980.

[9] M. O. Rabin, “Probabilistic algorithm for testing primality,” *Journal of Number Theory*, vol.12, pp.128–138, 1980.

[10] R. J. Burthe, “Further investigations with the strong probable prime test,” *Mathematics of Computation*, vol.65, no.213, pp.373–381, 1996.

[11] I. Damgård, P. Landrock, and C. Pomerance, “Average case error estimates for the strong probable prime test,” *Mathematics of Computation*, vol.61, no.203, pp.177–194, 1993.

[12] W. R. Alford, A. Granville, and C. Pomerance, "On the difficulty of finding reliable witnesses," in *International Workshop on Ant Colony Optimization and Swarm Intelligence*, 1994.

[13] E. Bach, "Explicit bounds for primality testing and related problems," *Mathematics of Computation*, vol.55, pp.355–380, 1990.

[14] G. L. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and System Sciences*, vol.13, no.3, pp.300–317, 1976.

[15] E. Bach, "Analytic methods in the analysis and design of number-theoretic algorithms," 1985.

[16] R. J. Burthe, "Upper bounds for least witnesses and generating sets," *Acta Arithmetica*, vol.80, pp.311–326, 1997.

[17] R. Balasubramanian and S. V. Nagaraj, "Density of carmichael numbers with three prime factors," *Math. Comput.*, vol.66, pp.1705–1708, 1997.

[18] D. S. Dummit, "Abstract algebra / by david s. dummit, richard m. foote," 1999.

[19] R. Baillie and S. S. Wagstaff, "Lucas pseudoprimes," *Mathematics of Computation*, vol.35, no.152, pp.1391–1417, 1980.

[20] E. Lehmer, "On the infinitude of fibonacci pseudo-primes," *Fibonacci Quart*, vol.2, pp.229–230, 1964.

[21] P. Erdös, P. Kiss, and A. Sárközy, "A lower bound for the counting function of lucas pseudoprimes," *Mathematics of Computation*, vol.51, no.183, pp.315–323, 1988.

[22] J. Grantham, "Frobenius pseudoprimes," *Math. Comp.*, vol.70, pp.873—891, 2001.

[23] E. Parberry, "On primes and pseudo-primes related to the fibonacci sequence," *Fibonacci Quart*, vol.8, pp.49–60, 1970.

[24] A. Rotkiewicz, "On the pseudoprimes with respect to the lucas sequences," *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.*, vol.21, pp.793–797, 1973.

[25] J. Grantham, "A probable prime test with high confidence," *Journal of Number Theory*, vol.72, no.1, pp.32–47, 1998.

[26] Z. Zhang, "A one-parameter quadratic-base version of the baillie-psw probable prime test," *Mathematics of Computation*, vol.71, no.240, pp.1699–1734, 2002.

[27] K. H. Rosen, "Elementary number theory: And its applications," 2010.

[28] D. S., J. B. Rosser, and L. Schoenfeld, "Approximate formulas for some functions of prime numbers," *Illinois Journal of Mathematics*, vol.6, pp.64–94, 1962.

[29] H. Williams. *Edouard Lucas and Primality Testing*, vol.22 of *Wiley-Interscience and Canadian Mathematics Series of Monographs and Texts*. Wiley, 1998.

[30] V. R. Pratt, "Every prime has a succinct certificate," *SIAM Journal on Computing*, vol.4, no.3, pp.214–220, 1975.

[31] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in p," *Annals of Mathematics*, vol.160, 09 2002.

[32] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in p," *Annals of Mathematics*, vol.160, pp.781–793, 2004.

[33] M. Agrawal *Lecture notes are available at:* http://www.fields.utoronto.ca/audio/02-03/agrawal/agrawal/.

[34] J. Silverman. *The Arithmetic of Elliptic Curves*, vol.106. 01 2009.

[35] J. Silverman and J. Tate. *Rational Points on Elliptic Curves*. 01 2015.

[36] L. C. Washington, "Elliptic curves: Number theory and cryptography," 2003.

Abstract

This thesis explores algorithms for the primality testing and factorization of composite numbers, which are highly significant in the fields of number theory, cryptography, and computer science.
We analyze classical methods such as probabilistic algorithms like the Miller-Rabin test, as well as more advanced techniques including the Fermat's Little Theorem algorithms, AKS, and methods based on elliptic curves, and so on. Additionally, we investigate theoretical foundations, computational complexities, and practical implementations.

College of Science
School of Mathematics, Statistics, and Computer Science

Primality Tests and Factorization Algorithms

Mohammadreza Motabar

Supervisor: Amir Ghadermarzi

A thesis submitted in partial fulfillment of the requirements for the degree of B.Sc.in Computer Science

March 2024