مقالات کوتاه از
مجلات ریاضی معتبر جهان (۱۶)

ترجمه: غلامرضا یاسی‌پور

اعداد اول،
تجزیه و رمزهای مخفی

(قسمت دوم)

یکی از مشهورترین سؤالهای بی‌پاسخ مربوط به اعداد اول *حدس گلدباخ*[1] است. *کریستین گلدباخ*[2] در نامه‌ای به *لئونهارد اویلر*[3]، نوشته شده در ۱۷۴۲، حدس زد که هر عدد زوج بزرگتر از ۲ مجموع دو عدد اول است. به عنوان نمونه،

۴=۲+۲

۶=۳+۳

۸=۳+۵

۱۰=۵+۵

۱۲=۵+۷

تحقیقات کامپیوتری حدس *گلدباخ* را به ازای جمیع اعداد زوج تا ۱۰۰۰۰۰۰۰۰ محقق کرده است، اما اثبات یا عدم اثبات کلی آن تا به امروز مشخص نشده است.

آزمون اول بودن

گرچه اغلب مسأله‌های کلاسیک مربوط به اعداد اول حل نشده باقی مانده‌اند، سالهای اخیر با گسترشهای عظیمی در روشهایی مواجه بوده‌اند که به کمک آنها می‌توان اول بودن یا نبودن اعداد را آزمود. ممکن است گفته شود «روشهای آزمون اول بودن؟ ولی این که خیلی واضح است.» و در واقع، طریق کاملاً طبیعی و ساده‌ای برای ملاحظهٔ اول بودن یا نبودن یک عدد موجود است.

با معلوم بودن عددمان، مثلاً n؛ ابتدا ملاحظه می‌کنیم ۲ آن را می‌شمارد یا نه. اگر بشمارد، در این صورت n اول نیست و غائله ختم شده است. سپس ۳ را آزمایش می‌کنیم. اگر ۳، n را بشمارد در این صورت n اول نیست و باز هم کار تمام است. پس بخشپذیری n را بر ۵ در نظر می‌گیریم. (از ۴ می‌توان صرفنظر کرد: از آنجا که ۲، n را نمی‌شمارد اگر جلوتر برویم، ۴ نیز نمی‌تواند n را بشمارد.)

اگر ۵ از شمردن n بازماند، ۷ را آزمایش می‌کنیم. (باز هم، می‌توان از ۶ صرفنظر کرد زیرا ۲ و ۳، n را نمی‌شمرند.) و همین طور الی آخر. اگر بدون یافتن عددی که n را بشمرد تا $\sqrt{n}$ پیش برویم، آنگاه خواهیم دانست که n باید اول باشد. (برای این که در صورتی n اول نباشد حاصل ضرب دو عدد u و v ی بین ۱ و n خواهد بود، و البته یکی از دو مورد u یا v بزرگتر از $\sqrt{n}$ است.)

فرایند فوق به *تقسیم آزمایشی*[۴] معروف است، و با وجود این که در مورد اعداد به نسبت کوچک به کفایت کاراست، برای عددهای بسیار بزرگ فاقد کارایی است. برای ملاحظهٔ غیرعملی بودن آن، فرض می‌کنیم بخواهیم برنامه‌ای با کارایی بالایی برای اجرای تقسیم آزمایشی مورد بحث بر سریعترین کامپیوتر در دسترس (که در ابتدای این فصل به آن اشاره شد) بنویسیم. برنامهٔ مورد نظر در مورد عددی ۱۰ رقمی فوراً اجرا می‌شود ــ پاسخ بلافاصله آشکار می‌شود. در مورد عددی ۲۰ رقمی اندکی زحمت می‌برد و دو ساعت به درازا می‌انجامد. در مورد عددی ۵۰ رقمی به مدت گیج کنندهٔ ده میلیارد سال نیاز دارد. عددی ۱۰۰ رقمی به

۱ ... ...

(در این عدد سی و شش صفر وجود دارد) نیازمند است. این موضوع، تنها، محاسبه‌ای معمولی برای عددی بسیار بزرگ نیست، و همانگونه که بعداً در این فصل توضیح خواهیم داد، برای یکی از امنترین دستگاههای رمزگذاری سری مورد استفادهٔ امروزه به اولهایی با ارقامی بین ۶۰ و ۱۰۰ نیاز است.

بنابراین برای تشخیص اول بودن یا نبودن یک عدد ۱۰۰ رقمی چه کاری باید انجام داد؟ در حال حاضر بهترین روش در دسترس روش بسیار پیچیده‌ای است که در حدود ۱۹۸۰ توسط ریاضیدانان *آدلمن*[۵]، *روملی*[۶]، *کوهن*[۷]، و *لنسترا*[۸] مطرح شده است، و اغلب به آن، با استفاده از حروف اول نامهایشان، به عنوان آزمون ARCL اشاره می‌شود.

زمانهای لازم برای آزمون ARCL ، بر کامپیوتر یاد شده، عبارتند از، برای عددی ۲۰ رقمی، ۱۰ ثانیه؛ برای عددی ۵۰ رقمی، ۱۵ ثانیه؛ برای عددی ۱۰۰ رقمی، ۴۰ ثانیه. کامپیوتر مزبور حتی عددی ۱۰۰۰ رقمی را، در صورتی یک هفته به آن مهلت داده شود، مشخص می‌کند.

اما آزمون مورد بحث چگونه به کار می‌رود؟ این عمل بستگی به مبالغ قابل ملاحظه‌ای ریاضیاتی بسیار پیچیده دارد ــ روشی ریاضی خارج از ریاضیات معمول دورهٔ کارشناسی ــ بنابراین به دست دادن پاسخ کامل در این مرحله ممکن نیست. اما توضیح ایدهٔ اصلی روش مذکور مشکل نیست. ایدهٔ مزبور قسمت ساده‌ای از ریاضیات (گرچه بسیار هوشمندانه) از ریاضیدان بزرگ فرانسوی *پیردوفرما*[۹] (۱۶۰۱ ــ ۱۶۶۵) است.

فرما گرچه ریاضیدانی «آماتور» بود (وی حقوقدان بود) بعضی از هوشمندانه‌ترین دستاوردهای ریاضی‌ای را، که تاکنون دیده شده‌اند، مطرح کرد. یکی از ملاحظاتش این بود که اگر P عددی اول باشد، در این صورت به ازای هر عدد a ی کمتر از P، عدد $a^{P-1} - ۱$ بر P بخشپذیر است. به عنوان نمونه، فرض می‌کنیم $P = ۷$ و $a = ۲$ را در نظر بگیریم. در این صورت

$a^{P-1} - ۱ = ۲^۶ - ۱ = ۶۴ - ۱ = ۶۳$

و در واقع ۶۳ بر ۷ بخشپذیر است. قضیه را خودتان به ازای هر مقدار (اول) P و هر مقدار (کمتر از Pی) a امتحان کنید. نتیجه همواره یکسان است.

بنابراین در اینجا روشی ممکن برای آزمون اول بودن یا نبودن n وجود دارد. عدد $۲^{n-1} - ۱$ را محاسبه و ملاحظه می‌کنیم n آن را می‌شمارد یا خیر. اگر نشمارد، در این صورت n نمی‌تواند اول باشد. (زیرا اگر n اول بود، آنگاه بنا به ملاحظهٔ فرما بخشپذیری $۲^{n-1} - ۱$ بر n را داشتیم.)

اما در صورتی که دریابیم n عدد $۲^{n-1} - ۱$ را نمی‌شمارد چه نتیجه‌ای می‌توان گرفت؟ متأسفانه نمی‌توانیم نتیجه بگیریم n باید اول باشد. (گر چه کاملاً احتمال دارد که چنین باشد.) مشکل در اینجاست که، در حالی که دستاورد فرما این را بیان می‌کند که هرگاه n اول باشد $۲^{n-1} - ۱$ را می‌شمارد، بر این نیست که اعداد مرکبی با این ویژگی وجود ندارند. (این مطلب مانند این است که گفته شود تمام اتومبیلها چرخ دارند؛ و این از چرخ داشتن سایر چیزها ــ به طور مثال، دوچرخه‌ها ــ جلوگیری نمی‌کند.) و در واقع عددهای غیر اولی موجودند که دارای ویژگی فرما هستند. کوچکترین آنها ۳۴۱ است، که از آنجا که حاصل ضرب ۱۱ و ۳۱ است، اول نیست. اما اگر (بر کامپیوتری) آزمایش کنید درخواهید یافت ۳۴۱ عدد $۲^{۳۴۰} - ۱$ را می‌شمارد. (بزودی ملاحظه خواهیم کرد که برای انجام این آزمایش نیاز به محاسبهٔ $۲^{۳۴۰}$ نیست.)

اعداد مرکبی که با عنایت به ویژگی فرما شبیه عددهای مرکب عمل می‌کنند به *شبه اول*[۱۰] موسومند. بنابراین اگر، هنگامی که با استفاده از دستاورد فرما، به آزمون اول‌بودن پرداخته‌اید، کشف کنید که n عدد $۲^{n-1} - ۱$ را می‌شمارد، تمام چیزی که می‌توانید نتیجه بگیرید این است که n یا اول‌است یا شبه اول. (در این حالت شانس به صورت بسیار بالایی به نفع اول بودن n است. زیرا گرچه در واقع بینهایت عدد شبه اول وجود دارند، با فراوانی بسیار کمتری از اولهای حقیقی رخ می‌دهند. به عنوان

نمونه تنها دو چنین عدد کمتر از ۱۰۰۰ی موجودند، و تنها ۲۴۵ مورد زیر یک میلیون.)

در ضمن در صورتی که، در آزمون ویژگی فرما، به جای ۲ از عدد دیگری، مثلاً ۳ یا ۵، استفاده کنیم تفاوت چندانی نمی‌کند. هر عددی که به کار برید اعداد شبه اولی موجود می‌شوند که از به دست آوردن پاسخی مطلق به مسألهٔ اول بودن یا نبودن ممانعت به عمل می‌آورد.

در کاربرد این آزمون، لزومی به محاسبهٔ عدد $۲^{n-۱}$، عددی که ملاحظه کردید که حتی به ازای اعداد کاملاً کوچک n بسیار بزرگ است، نیست. در این مورد تمام کاری که نیاز به انجام دادن آن داریم یافتن این مطلب است که n عدد $۱ - ۲^{n-۱}$ را می‌شمارد یا خیر. و این بدان معنی است که می‌توان از مضربهای n در *هر مرحلهٔ محاسبه* صرفنظر کرد. به عبارت دیگر، آنچه که باید محاسبه شود باقیمانده‌ای است که در صورت تقسیم $۱ - ۲^{n-۱}$ بر n به جا می‌ماند. و هدف ملاحظهٔ این موضوع است که باقیماندهٔ مزبور صفر است یا خیر، اما از آنجا که مضربهای n آشکارا در باقیمانده تأثیر نمی‌گذارند، می‌توان از آنها چشم پوشید. ریاضیدانها (و برنامه‌نویسهای کامپیوتر) برای نمایش باقیمانده‌ها طریقی استاندارد دارند: باقیماندهٔ تقسیم A بر B را به صورت زیر می‌نویسند:

$A \bmod B$

به این ترتیب، به‌طور مثال، $۵ \bmod ۲$ برابر ۱ است، $۷ \bmod ۴$ برابر ۳، و $۸ \bmod ۴$ برابر ۰.

از این طریق برای آزمون اول بودن عدد ۶۱، به عنوان مثالی از آزمون فرما، استفاده می‌کنیم. در این صورت نیاز به محاسبهٔ عدد

$(۲^{۶۰} - ۱) \bmod ۶۱$

داریم. ۶۱، در صورتی که این باقیمانده صفر نباشد، اول نیست. اگر صفر باشد، در این صورت ۶۱ یا اول است یا شبه‌اول (و در حقیقت، همان طور که می‌دانیم، اولی خالص). در این مورد سعی می‌کنیم از محاسبهٔ عدد بزرگ $۲^{۶۰}$ خودداری کنیم. کار را با ملاحظهٔ این مطلب آغاز می‌کنیم که

$۲^۶ = ۶۴$، و در نتیجه

$۲^۶ \bmod ۶۱ = ۳$

در این صورت، از آنجا که $۲^{۳۰} = (۲^۶)^۵$، به دست می‌آوریم

$۲^{۳۰} \bmod ۶۱ = (۲^۶ \bmod ۶۱)^۵ \bmod ۶۱ = ۳^۵ \bmod ۶۱$

$= ۲۴۳ \bmod ۶۱ = ۶۰$

بنابراین،

$۲^{۶۰} \bmod ۶۱ = (۲^{۳۰})^۲ \bmod ۶۱ = (۲^{۳۰} \bmod ۶۱)^۲ \bmod ۶۱$

$= ۶۰^۲ \bmod ۶۱ = ۳۶۰۰ \bmod ۶۱ = ۱$

به این ترتیب،

$(۲^{۶۰} - ۱) \bmod ۶۱ = ۰$

از آنجا که پاسخ ۰ است، نتیجه این است که، همان طور که پیش‌بینی شد، ۶۱ یا اول است یا شبه اول.

در این مرحله ممکن است مایل باشید خود محاسبه‌ای انجام دهید. در این صورت، تحقیق کنید که

$۲^{۱۰} \bmod ۳۴۱ = ۱$

سپس با استفاده از این واقعیت نشان دهید که

$۲^{۳۴۰} \bmod ۳۴۱ = ۱$

این نتیجه بر این است که عدد ۳۴۱ یا اول است یا شبه اول. (در این حالت، همانگونه که قبلاً متذکر شدیم، ۳۴۱ در واقع شبه‌اول است.)

آزمون ARCL با استفاده از تغییر آزمون *فرما*، چنان که نتواند توسط شبه اولی به اشتباه بیفتد، عمل می‌کند، و این تغییر است که به ریاضیاتی بسیار عمیق نیاز دارد. (در صورتی که *واقعاً* مایل به ملاحظهٔ این مطلب هستید به مقالهٔ

Primdity testing and Jacobi sums

نوشتهٔ Cohen و Lenstra در مجلهٔ تحقیق ریاضی زیر رجوع کنید.

Mathematics of Computation, Volume 42 (1984). PP. 297_330)

اولهای مرسن

آزمون ARCL سریعترین آزمون عام اول بودنی است که در حال حاضر در دسترس است. عبارت «عام» در اینجا بدان معنی است که آزمون مزبور در مورد هر عدد مفروض n به کار می‌رود. اما در مورد عددهایی با ساختارهای مخصوص اغلب روشهای دیگری موجودند که با سرعت بخشیدن به فرایند مزبور با بهره گرفتن از ساختار مخصوص عدد مورد نظر بسیار سریعتر انجام می‌گیرند. چشمگیرترین مثال در این مورد در رابطه با اعدادی به صورت $۲^n - ۱$ است. این عددها را امروزه به نام *مارتین مرسن*[11]، راهب فرانسوی قرن هفدهم، *اعداد مرسن*[12] می‌نامند.

مرسن در مقدمهٔ کتابش – Cogitata Physica Mathematica، انتشار یافته در ۱۶۴۴، اظهار کرد که عدد

$M_n = ۲^n - ۱$

به ازای

$n = ۲, ۳, ۵, ۷, ۱۳, ۱۷, ۱۹, ۳۱, ۶۷, ۱۲۷, ۲۵۷$

اول، و به ازای جمیع مقادیر کوچکتر از ۲۵۷ دیگر n مرکب است. چگونه این موضوع را دانست؟ کسی نمی‌داند. اما به هر تقدیر به نحوی شگفت‌آور با حقیقت نزدیک بود. سرانجام تنها در ۱۹۴۷، هنگامی که ماشینهای حساب رومیزی در دسترس قرار گرفتند، بررسی ادعای وی امکانپذیر شد. وی تنها مرتکب پنج اشتباه شده بود : $M_{۶۷}$ و $M_{۲۵۷}$ اول نیستند، و $M_{۶۱}$، $M_{۸۹}$، و $M_{۱۰۷}$ اولند.

اعداد مرسن روشی عالی برای به دست آوردن عددهای اول بسیار بزرگ مطرح می‌کنند. رشد سریع تابع ۲^n هنگامی که n بزرگ شود تضمین می‌کند که اعداد مرسن M_n بزودی بسیار بزرگ شوند، و بنابراین ایدهٔ روش مورد بحث جستجوی مقادیر n‌ی است که به ازای آنها M_n اول است. چنین اولهایی را ***اولهای مرسن*** می‌نامند.

مختصری جبر مقدماتی مشخص می‌کند M_n اول نخواهد بود مگر این که خود n اول باشد، بنابراین تنها لازم است که به مقادیر اول n نظر داشته باشیم. ولی حتی اغلب اولهای n نیز به عدد مرسن مرکب M_n ی منجر می‌شوند، بنابراین جستجوی مقادیر مناسب n آسان نیست ــ گر چه این مطلب به هیچ وجه از چند حالت اولیه آشکار نیست، زیرا

$M_۲ = ۲^۲ - ۱ = ۳$

$M_۳ = ۲^۳ - ۱ = ۷$

$M_۵ = ۲^۵ - ۱ = ۳۱$

$M_۷ = ۲^۷ - ۱ = ۱۲۷$

جمیعاً اولند. اما پس از این مرحله الگوی مزبور، با

$M_{۱۱} = ۲۰۴۷ = ۲۳ \times ۸۹$

تغییر جهت می‌دهد. سپس سه مقدار اول دیگر می‌آیند :

$M_{۱۳} = ۸۱۹۱$, $M_{۱۷} = ۱۳۱۰۷۱$, $M_{۱۹} = ۵۲۴۲۸۷$

پس از آن یافتن اعداد مرسن سخت‌تر می‌شود. پنج مقدار بعدی n‌ی که M_n به ازای آنها اول است عبارت است از

۳۱، ۶۱، ۸۹، ۱۰۷، ۱۲۷

اغلب مردم، هنگامی که برای اولین بار مقادیر فوق را ملاحظه می‌کنند، این نتیجهٔ عجولانه را می‌گیرند که اگر P خود اولی *مرسن* باشد، آنگاه M_p نیز اول است. این نتیجه محققاً در آغاز کاراست : ۳ اولی *مرسن* است و $M_۳$ نیز ؛ ۷ اولی *مرسن* است و $M_۷$ نیز ؛ ۳۱ اولی *مرسن* است و $M_{۳۱}$ نیز ؛ به همین ترتیب است مورد ۱۲۷ و $M_{۱۲۷}$. اما در اینجا الگو توقف می‌کند، و هر چند ۸۱۹۱ (با $M_{۱۳}$ بودن) اولی *مرسن* است، $M_{۸۱۹۱}$ (که دارای ۲۴۶۶ رقم است) مرکب است. این موضوع در سال ۱۹۵۳ با استفاده از کامپیوتری اولیه کشف شد. (بعداً در این فصل، بخش مربوط به اعداد تام را ملاحظه کنید.)

در واقع تا این تاریخ تنها سی اول *مرسن* شناخته شده موجودند. دوازده مقدار n که در فوق فهرست کردیم و به ازای آنها M_n اول است جمیعاً در سالهای اولیهٔ این قرن شناخته شده بودند. هفت مورد بعدی تماماً در ۱۹۵۲ توسط ***رافائل روبینسون***[۱۳] با استفاده از کامپیوتر SWAC یافت شدند. مقدار $n = ۳۲۱۷$ در ۱۹۵۷ توسط ***هنس ریزل***[۱۴] با استفاده از کامپیوتر BESK کشف شد. ***الکساندر هارویتس***[۱۵] برای به‌دست آوردن مقادیر $n = ۴۲۵۳$ و ۴۴۲۳ از کامپیوتر IBM۷۰۹۰ بهره گرفت، و در ۱۹۶۳ ***دونالد جیلیس***[۱۶] و ILLIAC – II مقادیر $n = ۹۶۸۹$، ۹۹۴۱، و ۱۱۲۱۳ را یافتند. IBM.360 – 91 ***براینت توکرمن***[۱۷] در ۱۹۷۱ مقدار $n = ۱۹۹۳۷$ را آشکار کرد.

با کشف بعدی، در ۱۹۷۸، سابقهٔ اعداد اول در صفحات اول اخبار با این خبر مطرح شد که پس از سه سال کار شامل ۳۵۰ ساعت وقت کامپیوتری بر CYBER 174 در دانشگاه ایالتی ***کالیفرنیا***[۱۸] در ***هیوارد***[۱۹]، دو دانش‌آموز ۱۸ سالهٔ دبیرستانی، ***لورانیکل***[۲۰] و ***کورت نول***[۲۱]، عدد اول مرسن ۶۵۳۳ رقمی $M_{۲۱۷۰۱}$ را یافته‌اند.

یک سال بعد، **نول** رکورد مزبور را با اول ۶۹۸۷ رقمی $M_{۲۳۲۰۹}$ بهبود بخشید. بعداً در همین سال رکورد مزبور بار دیگر شکست، و این بار توسط ***دیوید اسلووینسکی***[۲۲]، برنامه‌نویس جوانی که برای تحقیقات کری[۲۳] در Chippewa Falls ***ویسکانسین***[۲۴] کار می‌کرد. وی با استفاده از کامپیوتر بسیار قدرتمند ۱ – CRAY اول ۱۳۳۹۵ رقمی $M_{۴۴۴۹۷}$ را پیدا کرد.

در ۱۹۸۲ همین ترکیب ماشینی نشان داد که $M_{۸۶۲۴۳}$ (عددی ۲۵۹۶۲ رقمی) اول است. سپس، ***اسلووینسکی***، با کار بر کامپیوتر حتی قدرتمندتر CRAY – XMP، با اول

۳۹۷۵۱ رقمی $M_{۱۳۲۰۴۹}$ از این هم فراتر رفت.

سرانجام (تا این زمان)، در سپتامبر ۱۹۸۵، در **هوستون، تکزاس**، CRAY – XMP از آن Chevron Geosciences، عدد ۶۵۰۵۰ رقمی $M_{۲۱۶۰۹۱}$، رکورد نگهدار فعلی، را به دست آورد. (از آنجا که Chevron برنامهٔ اول‌یاب ***اسلووینسکی*** را اجرا می‌کرد، اعتبار این کشف در واقع از آن اوست. شرکت مزبور برنامهٔ مزبور را به این علت اجرا می‌کرد که روشی نیکو برای نشان دادن اشتباهات دستگاههای کامپیوتر به دست می‌داد.)

اما آیا این پایان داستان است؟ احتمالاً خیر. حدس بر این است که اولهای مرسن را پایانی نیست ــ یعنی بینهایت عدد از آنها موجودند. اما این موضوع به اثبات نرسیده است، و تمام آنچه که به ***تحقیق*** می‌توان دانست این است که حداقل سی عدد از آنها وجود دارند (یعنی، آنهایی که شناخته شده‌اند.)

روش به کار رفته در برزسی اول بودن اعداد **مرسن** بسیار ساده است (گرچه ریاضیات پشتوانهٔ آن چنین نیست). این روش به یاد ***ادوارد لوکاس***[۲۵] (که ایدهٔ اصلی آن را در ۱۸۷۶ کشف کرد) و ***دریک لمر***[۲۶] (که آن را در ۱۹۳۰ مهذب کرد) به عنوان ***آزمون لوکاس ــ لمر***[۲۷] معروف است. برای آزمون اول بودن عدد مرسن M_n (با فرض اول بودن n)، اعداد $U(۰)$، $U(۱)$، ...، $U(n-۲)$ را با استفاده از قاعده‌های زیر محاسبه می‌کنیم:

$$U(۰) = ۴$$
$$U(K+۱) = \left[U(K)^۲ - ۲\right] \bmod M_n$$

اگر در پایان کار دریابیم که $U(n-۲) = ۰$، آنگاه M_n اول است. اگر $U(n-۲) \neq ۰$ آنگاه M_n اول نیست.

به عنوان مثال، فرض می‌کنیم می‌خواهیم از آزمون لوکاس ــ لمر برای ملاحظهٔ اول بودن $M_۵$ استفاده کنیم. (البته، از آنجا که $M_۵ = ۲^۵ - ۱ = ۳۱$، می‌دانیم در این حالت ساده عدد مورد بحث اول است، اما این موضوع را با روش مورد نظر روشن می‌کنیم.) در این صورت محاسبهٔ زیر را انجام می‌دهیم:

$$U(۰) = ۴$$
$$U(۱) = (۴^۲ - ۲) \bmod ۳۱ = ۱۴ \bmod ۳۱ = ۱۴$$
$$U(۲) = (۱۴^۲ - ۲) \bmod ۳۱ = ۱۹۴ \bmod ۳۱ = ۸$$
$$U(۳) = (۸^۲ - ۲) \bmod ۳۱ = ۶۲ \bmod ۳۱ = ۰$$

از آنجا که $U(۳) = ۰$، $M_۵$ باید اول باشد.

می‌توانید خودتان این روش را با استفاده از دو عدد $M_۷ = ۱۲۷$ (که اول است) و $M_{۱۱} = ۲۰۴۷$ (که اول نیست ــ پیشین را ملاحظه کنید) به کار برید.

یادداشتها:

۱ ـ Goldbach's Conjecture
۲ ـ Christian Goldbach
۳ ـ Leonhard Euler
۴ ـ Trial division
۵ ـ Adleman
۶ ـ Rumely
۷ ـ Cohen
۸ ـ Lenstra
۹ ـ Pierre de Fermat
۱۰ ـ Pseudo primes
۱۱ ـ Martin Mersenne
۱۲ ـ Mersenne numbers
۱۳ ـ Rafael Robinson
۱۴ ـ Hans Riesel
۱۵ ـ Alexander Hurwitz
۱۶ ـ Donald Gillies
۱۷ ـ Bryant Tuckerman
۱۸ ـ California State University
۱۹ ـ Hayward
۲۰ ـ Laura Nickel
۲۱ ـ Curt Noll
۲۲ ـ David Slowinski
۲۳ ـ Cray Research
۲۴ ـ Wisconsin
۲۵ ـ Edovard Lucas
۲۶ ـ Derrick Lehmer
۲۷ ـ Lucas - Lehmer test