عددهای اول

تألیف: امیل بورل

ترجمهٔ پرویز شهریاری

عددهای اول

Les nombres premières

امیل بورل

EMILE BOREL

ترجمهٔ پرویز شهریاری

مؤسسه انتشارات امیرکبیر

تهران، ۱۳۸۱

بورل، امیل فلیکس ادوار ژوستن، ۱۸۷۱ ـ ۱۹۵۶ م.
Borel, Emile Felix Edouard Justin
عددهای اول = les nombres Premiers امیل بورل؛ ترجمه پرویز شهریاری. ـ
تهران : امیرکبیر، ۱۳۸۱.
۲۰۶ ص.
ISBN 964-00-0809-5
فهرستنویسی بر اساس اطلاعات فیپا.
عنوان اصلی: Les nombres Premiers.
چاپ سوم: ۱۳۸۱
۱. اعداد اول. الف. شهریاری، پرویز، ۱۳۰۵ ـ ، مترجم. ب. عنوان.
۴ع ۹ ب / QA ۲۴۶ ۵۱۲/۷۲
۱۳۸۱
کتابخانه ملی ایران ۱۴۲۰۰-۸۱م

عددهای اول

تألیف : امیل بورل
ترجمهٔ پرویز شهریاری
چاپ دوم : ۱۳۵۵
چاپ سوم : ۱۳۸۱
چاپ و صحافی : چاپخانهٔ سپهر، تهران
شمارگان : ۱۵۰۰ نسخه

ISBN 964-00-0809-5 شابک ۵-۹-۰۸۰۹-۰۰-۹۶۴
مؤسسهٔ انتشارات امیرکبیر تهران، میدان استقلال.
WWW.AMIR-KABIR.COM

عـددهـای اول را بهسختی می‌تـوان دست‌آمـوزکـرد و به‌همین مناسبت، جذبهٔ‌آن، بسیاری ازریاضیدانان را به‌طرف خودکشانده است. برای بررسی مسأله‌های گوناگونی که درعرصهٔ عددهای‌اول وجود دارد، به‌دوعلت دلیری بسیار می‌خـواهد : نخست به این مناسبت که عرصه‌ای پرسنگلاخ و تاریك است و به‌سختی می‌توان در آن‌کوره راهی برای ادامه‌کار پیدا کرد، و دوم به‌این مناسبت که ظاهراً آشنایی با قانونهایی که حاکم برعددهای اول است ، مشکلی از دانشهای دیگر و یا صنعت را حل نمی‌کند. با وجود این، بسیار بوده‌اند وریاضیدانانی‌که دراین راه‌گام گذاشته‌اند و به توفیقهای نسبی هم رسیده‌اند.

این کتاب، به‌وسیلهٔ بورل ، ریاضیدانِ معـاصر فـرانسوی‌برای چاپ درمجموعهٔ معروف «چه می‌دانم؟» تهیه شده است و به‌همین مناسبت، و به‌خاطرقابل فهم‌بودن مطالب آن برای خوانندگان وسیع این مجموعه، از وارد شدن به‌بحثهای نظری پیچیده،پرهیز کرده است . باوجود این، تقریباً شامل همهٔ کارهایی است‌که تا کنون در مورد عددهای اول انجام‌گرفته است.

***

وقتی که در سال ۱۳۴۴ ، تصمیم به ترجمه و چاپ این کتاب در مجموعهٔ سیمرغ گرفتم ، به‌علت اختصاصی بودن آن ، تردید

داشتم که بتواند مورد استقبال قرار گیرد و این نگرانی، همیشه با من همراه بود که این سه هزار نسخه‌ای که چاپ شده است، دور از کتابخانه‌های شخصی و درانبارناشر، باقی بماند. وگرچه، یازده‌سال طول کشید تا لزوم چاپ دوم آن احساس شد، معهذا، همین که توانسته است از قفسهٔ کتابفروشیها، به‌کتابخانه‌های دوستداران ریاضی منتقل شود، می‌تواند هرکسی را راضی کند. رضایت بیشتر از اینجهت‌است که به‌تحقیق می‌توان اطمینان‌داشت که هیچ خریداری، تنها به‌خاطر تزیین «کتابخانهٔ» شخصی خود، به‌سراغ «عددهای اول» نیامده است و این سه‌هزار خریدار، سه هزار علاقه‌مندواقعی به‌ریاضیات بوده‌اند.

من، حتی دربارهٔ این‌کتاب نامه‌های فراوانی هم داشته‌ام که بامحبت خود، مرا تشویق کرده‌اندکه برخلاف جریان ظاهری که وجود دارد و بعضی گمان می‌کنندکه برای نوشته‌های خالص علمی، خریداری وجود ندارد، تلاش خودرا قطع نکنم، ومنهم چنین‌کردم و درحد توانایی خود، و با همهٔ دشواریهایی که وجود داشت، این راه را دنبال کردم.

ازمیان نامه‌هایی که به‌من رسیده است، دریغم می‌آیدکه از نامهٔ فاضلانه وپرمحبت‌آقای فرخ شهداد نام نبرم که‌درتاریخ اول تیرماه ۱۳۴۹ برای من فرستاد و مقالهٔ بسیارجالبی هم با عنوان « شمارش اعداد اول و میزان فراوانی آنها » با آن همراه کرد. و شاید به‌گمان من، به‌این امیدکه درمجله سخن علمی، که درآن زمان‌منتشر می‌شد و من سردبیرش بودم، چاپ شود. ولی، حیف که مجلهٔ سخن علمی، درهمان سال تعطیل شد و مقالهٔ این دوست فاضل و علاقه‌مند، همچنان چاپ نشده پیش من باقی ماند.

اول بهمن ۲۵۳۵ - مترجم

در این کتاب

مقدمه

بخش‌پذیری عددهای درست

۱. تعریف. پیش از اینکه به مطالعهٔ عددهای اول بپردازیم، لازم است که نظریهٔ مقدماتی تقسیم‌بندی عددهای درست را ذکر کنیم. برای‌این منظور، از روش پواسون Poisson استفاده می‌کنیم، روشی که همیشه در حساب و در نظریهٔ عددها، مورد استفاده قرار می‌گیرد. قبلا تعریفهای مربوط به‌تقسیم عددهای درست را یادآوری می‌کنیم. و در اینجا فرض را براین می‌گیریم که جمع، تفریق و ضرب را می‌شناسیم.

گویند عدد درست A، بر عدد درست B بخش‌پذیر است، وقتی‌که عدد دیگری مانندQ وجود داشته‌باشد به‌طوریکه A مساوی با حاصلضرب B در Q باشد. در اینصورت A را مقسوم، B را مقسوم‌علیه و Q را خارج قسمت دو عدد A و B گویند. وقتی‌که A بر B بخش‌پذیر نباشد، می‌توان عدد Q و عدد R را چنان پیداکرد که داشته باشیم:

$$A=B.Q+R$$

عدد R کوچکتر از B است و دراینحال Q را خارج قسمت نقصانی A بر B و R را باقیماندهٔ این تقسیم گویند.

به‌جای اینکه گفته شود A بر B بخش‌پذیر است، می‌توان گفت‌که B مقسوم‌علیه A است و یا A مضربی از B است. بین مقسوم‌علیه‌های A می‌توان خود A را نیز به‌حساب آورد، همچنین B نیز یکی‌ازمضربهای خودش می‌باشد و دراین حالتها خارج قسمت برابر با واحد است. ضرب در واحد و یا تقسیم‌بر واحد یك عمل یکسان است، یعنی نتیجهٔ بدست‌آمده مساوی همان عددی است‌که عمل دربارهٔ آن انجام گرفته است (عدد بانتیجهٔ

عمل یکسان است).

اگر عدد D در عین‌حال هردو عدد A و B را بشمارد[1]. آنرا مقسوم‌علیه مشترك عددهای A و B گویند، بین مقسوم‌علیه‌های مشترك A و B یکی از دیگران بزرگتر است، که آنرا بزرگترین مقسوم‌علیه مشترك بین دو عدد گویند، اگر $A > B$ باشد، تمام مقسوم علیه‌های مشترك A و B کوچکتر یا حداکثر مساوی B خواهند بود. همچنین بین مضربهای مشترك A و B یکی از همهٔ دیگران کوچکتر است که آنرا کوچکترین مضرب مشترك دو عدد گویند، با توجه به اینکه تمام مضربهای مشترك A و B بزرگتر یا لااقل مساوی A هستند (به‌فرض $A > B$).

اکنون روش پواسون را برای تعیین کوچکترین مضرب مشترك و بزرگترین مقسوم علیه مشترك توضیح می‌دهیم و درحالیکه خواص اصلی بزرگترین مقسوم‌علیه مشترك وکوچکترین مضرب مشترك دو عدد را مطالعه می‌کنیم، طریقهٔ رسمی محاسبهٔ آنها را نیز ذکر می‌کنیم.

۲. تعیین کوچکترین مضرب مشترك و خاصیتهای آن: دو عدد A و B را درنظر می‌گیریم و فرض می‌کنیم $A > B$ باشد، می‌خواهیم کوچکترین مضرب مشترك بین آنها را محاسبه کنیم. اگر A بر B بخش‌پذیر باشد، در اینصورت واضح است که A کوچکترین مضرب مشترك A و B خواهد بود، زیرا A کوچکترین عدد بین مضربهای A می‌باشد. اگر A بر B بخش‌پذیر نباشد، مضربهای پشت‌سرهم A راتنظیم می‌کنیم تا آنجا که برای اولین بار به عددی برسیم که بر B هم بخش‌پذیر باشد. این عدد کوچکترین مضرب مشترك خواهد بود، زیرا کوچکترین مضربی از A است که بر B هم بخش‌پذیر است.

مضربهای پشت‌سرهم A راکه از خود A شروع می‌شود، روی یك سطر می‌نویسیم :

$$A، ۲A، ۳A، ۴A، ۵A،... \qquad (۱)$$

و روی‌سطر دوم، باقیمانده‌های تقسیم عددهای سطر(۱) رابر B می‌نویسیم:

$$r_{۱}، r_{۲}، r_{۳}، r_{۴}، r_{۵} ،... \qquad (۲)$$

---

۱. یعنی A و B بر D بخش‌پذیر باشند.

تمام عددهای سطر(۲) کوچکتر از B هستند، بنابراین به‌ناچارزمانی خواهد رسیدکه باقیمانده مساوی یکی از باقیمانده‌های قبلی باشد. ثابت خواهیم‌کرد که قبل از این حادثه، باید به باقیماندهٔ صفر رسیده باشیم. فرض می‌کنیم دو عدد صحیح m و n وجود داشته باشند، به طوریکه داشته باشیم:

$$mA = m'B + r \qquad (۳)$$

$$nA = n'B + r \qquad (۴)$$

m' و n' دو عدد درست است و r عدد درست کوچکتر از B، اگر n را بزرگترازm فرض کنیم و دوطرف رابطه‌های (۳) و (۴) را نظیر به‌نظیر ازهم کم‌کنیم، خواهیم داشت:

$$(n-m)A = (n'-m')B \qquad (۵)$$

و این‌به‌آن‌معناست‌که $(n-m)A$ بر B بخش‌پذیر است ، بنابراین قبل از آنکه در رشتهٔ (۲) باقیمانده‌ای مساوی یکی از باقیمانده‌های قبلی بدست آید، به باقیماندهٔ صفر می‌رسیم. ازاینجا این نتیجه بدست می‌آیدکه تمام باقیمانده‌هائی‌که قبل از باقیماندهٔ مساوی صفر قرار گرفته‌اند باهم‌فرق دارند.

فرض‌کنیدhA اولین مضربی ازA باشدکه برB بخش‌پذیر است. در اینصورت داریم:

$$hA = kB \qquad (۶)$$

می‌دانیم که باقیمانده‌های پشت‌سرهم:

$$r_۱ \text{ و } r_۲ \text{ و } r_۳ \text{ و } \ldots r_{h-۱} \text{ ، } r_h = ۰ \qquad (۷)$$

که از تقسیم h مضرب اولیهٔ A :

$$A \text{ ، } ۲A \text{ ، } ۳A \text{، } \ldots \text{ ، } (h-۱)A \text{، } hA$$

بر B بدست آمده‌اند، با هم مختلف‌اند. دیگر واضح است که این باقیمانده‌ها پشت‌سرهم بدست می‌آیند، زیرا، اگر داشته باشیم:

$$mA=m'B+r \qquad (۹)$$

اگر تساویهای (۶) و (۹) را عضو به عضو با هم جمع کنیم، خواهیم داشت:

$$(m+h)A=(m'+k)B+r \qquad (۱۰)$$

یعنی باقیماندهٔ تقسیم $(m+h)A$ بر B، همان باقیماندهٔ mA بر B خواهد بود.

مثلاً، اگر $A=۴۲$ و $B=۳۰$ باشد، باقیمانده‌های پشت‌سرهم مضربهای A بر B چنین خواهد بود:

۱۲، ۲۴، ۶، ۱۸، ۰، ۱۲، ۲۴، ۶، ۱۸، ۰، ۱۲،... (۱۱)

اکنون ملاحظه می‌کنیم که حاصلضرب $A.B$ بر B بخش‌پذیر است، بنابراین عدد h حداکثر مساوی B است و یا به عبارت دیگر، B مضربی از h است، درحالیکه در رشته (۷) باقیمانده‌های مساوی صفر ردیفهای h، $۲h$، $۳h$، ... را اشغال کرده‌اند [در رشتهٔ (۱۱) ردیفهای ۵ و ۱۰ و ۱۵ و ...].

بنابراین می‌توان نوشت:

$$B=hD \qquad (۱۲)$$

که در آن D عددی است درست. رابطهٔ (۶) اکنون به صورت زیر در می‌آید:

$$hA\times khD \qquad (۱۳)$$

و پس از تقسیم دو طرف بر عدد درست h داریم:

$$A=kD \qquad (۱۴)$$

با توجه به رابطه‌های (۱۲) و (۱۴)، D مقسوم علیه مشترك دو عدد A و B است؛ اکنون تحقیق می‌کنیم که این عدد عبارتست از بزرگترین مقسوم علیه مشترك.

اگر M را کوچکترین مضرب مشترك بین دو عدد A و B فرض

کنیم، داریم:

$$M=hA=kB=hkD \qquad (۱۵)$$

و ازآنجا، رابطهٔ مهم زیر را نتیجه می‌گیریم :

$$MD=hkD^{2}=kD.hD=A.B \qquad (۱۶)$$

تمام مضربهای‌مشترک A و B به‌صورت λhA هستند؛ اینهامضربهای کوچکترین مضرب مشترک خواهند بود.

۳. خاصیتهای بزرگترین مقسوم علیه مشترک و تعیین‌آن. با حفظ تمام علامتهای قبلی، d را یکی ازمقسوم علیه‌های مشترک A و B فرض می‌کنیم :

$$\begin{cases} B=h'd \\ A=k'd \end{cases} \qquad (۱۷)$$

حاصلضرب $h'k'd$ بر A و B بخش‌پذیر است و این به‌آن معناست که این عدد یکی ازمضربهای مشترک A و B است ؛ پس $h'A$ بخش‌پذیر بر B است و ما با توجه بەرشتهٔ (۷) می‌دانیم‌که h' یکی از مضربهای h است یعنی:

$$h'=\lambda h \qquad (۱۸)$$

همچنین با توجه به‌رابطه‌های (۱۷) و (۱۲) داریم :

$$B=\lambda hd=hD$$

و از آنجا :

$$D=\lambda d \qquad (۱۹)$$

از اینجا این‌نتیجه بدست می‌آیدکه تمام مقسوم علیه‌های مشترک A و B مثل d ، مقسوم علیهی از D خواهند بود و بنابراین D بزرگترین مقسوم علیه مشترک خواهد بود . ضمناً این نتیجه هم بدست‌آمد که تمام

مقسوم علیه‌های مشترک دو عدد A و B مقسوم علیه D هم خواهند بود.

اکنون می‌توان به‌آسانی کوچکترین مضرب مشترک و یا بزرگترین مقسوم علیه مشترک را بین چند عدد شرح داد: برای ما کافی است که دربارهٔ سه عدد A و B و C بحث کنیم. یادآوری می‌کنیم که تمام مضربهای مشترک A و B مضربهای کوچکترین مضرب مشترک آنها (که ما آنرا به M نشان می‌دهیم) نیز هستند.

بنابراین مضربهای مشترک A و B و C مضربهای مشترک M و C خواهند بود و ازآنجا کوچکترین مضرب مشترک A و B و C همان کوچکترین مضرب مشترک بین دو عدد M و C است.

به‌همین ترتیب، تمام مقسوم علیه‌های مشترک A و B مقسوم علیه D (بزرگترین مقسوم علیه مشترک A و B) نیزهستند؛ در رشتهٔ مقسوم‌علیه‌های مشترک A و B و C مقسوم‌علیه‌های مشترک بین D و C قرار دارند و بزرگترین مقسوم علیه مشترک A و B و C همان بزرگترین‌مقسوم علیه مشترک بین D و B خواهد بود.

اکنون می‌توانیم راه ساده‌ای برای محاسبهٔ مستقیم کوچکترین‌مضرب مشترک و بزرگترین مقسوم علیه مشترک بین‌دوعدد بیان‌کنیم: رابطهٔ (۱۶) به‌ما اجازه می‌دهد که کوچکترین مضرب مشترک بین دو عدد را با کمک بزرگترین مقسوم علیه مشترک‌آنها محاسبه‌کنیم و برعکس.

روش نظری که برای بدست آوردن کوچکترین مضرب مشترک بیان کردیم، بسیار ساده و عملی است به‌شرطی که با عددهای بزرگ سر و کار نداشته باشیم. محاسبهٔ باقیمانده‌های متوالی در تقسیم مضربهای A بر B فوق‌العاده ساده است، به‌شرطی‌که توجه‌کنیم از رابطهٔ:

$$A = BQ + r$$

به‌سادگی رابطه‌های زیر بدست می‌آید:

$$۲A = ۲BQ + ۲r$$
$$۳A = ۳BQ + ۳r$$

مثلا اگر $B = ۶۰$ و $r = ۸$ باشد، باقیمانده‌های پشت‌سرهم چنین‌اند:

۸، ۱۶، ۲۴، ۳۲، ۴۰، ۴۸، ۵۶، ۶۴

اگر به‌جای ۶۴ باقیماندهٔ ۴ را جانشین کنیم، رشتهٔ باقیمانده‌ها چنین ادامه پیدا می‌کند:

۴، ۱۲، ۲۰، ۲۸، ۳۶، ۴۴، ۵۲، ۶۰

و آخرین عدد به‌معنای باقیماندهٔ صفر است.

باوجود این، در حالیکه عددهای مفروض، به‌اندازهٔ کافی بزرگ باشند، محاسبه‌ها مفصل و دشوار می‌شود و بهتر است که طریقهٔ محاسبهٔ رسمی برای بدست‌آوردن بزرگترین‌مقسوم علیه‌مشترك به‌کار رود. این‌طریقهٔ محاسبه برپایهٔ ملاحظهٔ زیر قرار دارد:

اگر داشته باشیم:

$$A = BQ + R \qquad (۲۰)$$

مقسوم علیه‌های مشترك A و B درعین‌حال مقسوم علیه‌های مشترك B و R نیزخواهند بود. درحقیقت، روشن است‌که تمام مقسوم‌علیه‌های مشترك دو عدد، مقسوم‌علیه مجموع یا تفاضل آنها نیز هستند. همچنین مقسوم علیه‌های مشترك B و R مقسوم علیه‌های مشترك R و باقیماندهٔ $R_۱$ (که از تقسیم B بر R بدست آمده است) نیزمی‌باشند، بنابراین می‌توان‌نوشت:

$$\begin{array}{ll} A = BQ + R & R < B \\ B = RQ_۱ + R_۱ & R_۱ < R \\ R = R_۱Q_۲ + R_۲ & R_۲ < R_۱ \\ \cdots\cdots & \cdots\cdots \end{array}$$

تا جائی که به‌باقیماندهٔ R_k مساوی صفر برسیم، این باقیماندهٔ صفر پس‌ازیك رشتهٔ محدود عملها قرار داردکه ضمن‌آن باقیمانده‌های R و $R_۱$ و $R_۲$ و ... بدست آمد، و هریك کوچکتر از عدد قبلی خود می‌باشد. اگر باقیماندهٔ R_k مساوی صفر باشد، $R_{k-۱}$ بزرگترین مقسوم علیه مشترك $R_{k-۱}$ و $R_{k-۲}$ و یا بزرگترین مقسوم علیه مشترك دو عدد A و B خواهد بود. اگر $R_{k-۱}$ مساوی واحد باشد، بزرگترین مقسوم‌علیه مشترك دو عدد A و B مساوی واحد و کوچکترین مضرب مشترك

آنها مساوی $A.B$ می‌شود.

معمولا این تقسیمهای پشت‌سرهم را به‌صورت زیرعمل می‌کنندکه در آخر، بزرگترین مقسوم علیه مشترك بدست خواهدآمد:

۲	۱	۱	۲	۲	
۱۰	۲۰	۳۰	۵۰	۱۳۰	۳۱۰
	۰	۱۰	۲۰	۳۰	۵۰

به‌این ترتیب که دو عدد ۳۱۰ و ۱۳۰ را به‌عنوان مقسوم ومقسوم‌علیه پهلوی هم می‌نویسند، خارج قسمت ۳۱۰ بر۱۳۰ یعنی ۲ را بالای ۱۳۰ و باقیماندهٔ این تقسیم، یعنی ۵۰ را، زیر ۳۱۰ می‌نویسند، سپس ۵۰ را درسمت راست ۱۳۰نوشته، عمل‌را ادامه می‌دهند، تا درآخر به‌بزرگترین مقسوم علیه مشترك یعنی ۱۰ برسند.

۴. قضیهٔ اصلی. اکنون به‌آسانی می‌توانیم قضیهٔ اصلی مربوط به بخش‌پذیری عددها را بیان‌کنیم.

قبلاتعریفی می‌کنیم: دوعدد را نسبت‌به‌هم‌اول گویند وقتیکه‌مقسوم‌علیه مشترکی جزواحد نداشته‌باشند. دراینحالت گویندکه بزرگترین‌مقسوم‌علیه مشترك آنها نیز، مساوی واحد است.

قضیه اصلی چنین است: اگرعددی مانند B حاصلضرب دو عامل را بشمارد و با یکی از آن دو عامل اول باشد، عدد دوم را خواهد شمرد.

درحقیقت، اگر عدد B با A متباین باشد (به‌زبان دیگرA و Bنسبت به‌هم اول باشند)، بزرگترین مقسوم علیه مشترك بین دو عدد A و B مساوی ۱ وکوچکترین مضرب مشترك بین‌آنها، یعنی M، متساوی $A.B$ خواهد بود. بنابرآنچه گذشت، B نمی‌تواند حاصلضرب hA را بشمارد، مگر اینکه h یکی از مضربهای B باشد، یعنی B بتواند h را بشمارد.

تعمیم این قضیه فوراً بدست می‌آید: اگر عددی حاصلضرب n عامل

را بشمارد و نسبت به $n-1$ عامل آن اول باشد، عامل nام را خواهدشمرد. در حقیقت، فرض می‌کنیم که h حاصلضرب ۴ عامل A و B و C و D را بشمارد و درعین‌حال، نسبت به‌سه عددA وB و C اول باشد. طبق قضیه اصلی، چون h نسبت به A اول‌است و حاصلضرب A در BCD را می‌شمارد، BCD را خواهد شمرد. اما h باB هم اول است و حاصلضرب B در CD را می‌شمارد، بنابراین CD را خواهد شمرد، بالاخره h با C اول است و حاصلضرب CD را می‌شمارد، بنابراین D را خواهد شمرد، و این همان نتیجه‌ای است‌که می‌خواستیم .

۱

تعریف عددهای اول
وخاصیتهای اصلی آنها

۵. تعریف. عددی را اول گویند، وقتی که مقسوم علیهی جز خودش و واحد نداشته باشد. همچنین گاهی عددی را عدد اول مطلق گویند، وقتی که لازم باشد آنرا بین سایر عددهای اول مشخص کنند. هر عدد اول نسبت به‌تمام عددهائی که مقسوم علیه آنها نیست، اول خواهد بود. فرض کنیم p یك عدد اول و A یك عدد مفروض باشد، اگر A مضربی از p باشد. در اینصورت می‌دانیم که p بزرگترین مقسوم علیه مشترك A و p خواهد بود. ولی اگر p عدد A را نشمارد، بزرگترین مقسوم علیه مشترك A و p باید عددی مانند q ، که کوچکتر از p است، باشد. اما این عدد q نمی‌تواند عدد p را بشمارد، مگر اینکه q مساوی واحد باشد، زیرا p عددیست اول.

با شناسائی جدول فیثاغورث می‌توانیم عددهای اول کوچکتر از ۱۰۰ را بلافاصله بنویسیم: تنها عدد صحیح غیراولی که عاملهای اول آن درنظر اول شناخته نمی‌شود ۹۱ = ۱۳ × ۷ می‌باشد.

تعداد عددهای اول کوچکتر از ۱۰۰، مساوی ۲۵ و چنین‌اند:

۲ و ۳ و ۵ و ۷ و ۱۱ و ۱۳ و ۱۷ و ۱۹ و ۲۳ و ۲۹ و ۳۱ و ۳۷ و ۴۱ و ۴۳ و ۴۷ و ۵۳ و ۵۹ و ۶۱ و ۶۷ و ۷۱ و ۷۳ و ۷۹ و ۸۳ و ۸۹ و ۹۷.

۱۵ عدد از این عددهای اول، بین ۱ و ۵۰ و تنها ۱۰ عدد آنها بین ۵۱ و ۱۰۰ قرارگرفته‌است. این یك مثال ساده ازنزولی بودن تعداد عددهای اول، در مقیاس عددهای درست است.

۶. تجزیه به عاملهای اول. تمام عـددهـای غیر اول، لااقـل دارای یك مقسوم علیه اول هستند. فـرض‌کنیم A عددی غیراول و p کوچکترین مقسوم علیه آن باشد، عدد p عددی است اول، زیرا در غیر اینصورت p دارای مقسوم علیهی مانند ′p خـواهد بود.که درعین‌حال مقسوم علیه A نیز می‌باشد و ضمناً ازp همٔ‌کوچکتراست.

همچنین، تمام عددهای اول را می‌توان به‌حاصلضرب عـاملهای اول تجزیه کـرد. کافی است‌که مقسوم علیه‌های اول آنـرا، با شروع از کوچکترین آنها، جستجو کنیم.

مثلا عدد ۶۳۰ را درنظربگیریم، می‌توان پشت‌سرهم نوشت:

$$۶۳۰ = ۳۱۵ \times ۲$$
$$۳۱۵ = ۱۰۵ \times ۳$$
$$۱۰۵ = ۳۵ \times ۳$$
$$۳۵ = ۷ \times ۵$$

و در نتیجه خواهیم داشت:

$$۶۳۰ = ۲ \times ۳^{۲} \times ۵ \times ۷$$

حاصلضربهای دو دسته ازعاملهای اول نمی‌توانند مساوی‌باشند، مگر اینکه با هم متحد باشند، یعنی از عاملهـای مساوی، با توانهای مساوی، تشکیل شده باشند.

این مطلب از اینجا ناشی می‌شودکه دوعدد اول اجباراً نسبت به

هم اولند، زیرا مقسوم علیه مشترکی جزواحدندارند، بنابراین حاصلضرب عـاملهای اول نمی‌تواننـد بر عـدد اولی کـه در این حاصلضرب وجود ندارد، بخش‌پذیر باشد. بالاخره اگر دو حاصلضرب از عـاملهای اول، مساوی‌باشند، هرعاملی که دریکی از این حاصلضربها وجود داشته‌باشد، مقسوم‌علیه‌ی از حـاصلضرب دیگر است و باید جزو عاملهای آن باشد. توانها باید مساوی باشند، زیرا می‌توان عاملهای مشترك را حذف‌کرد، بدون اینکه تساوی ازبین برود. پس از این حذف باید عاملهای اول یا درهردو حاصلضرب وجود داشته باشد ویا در هیچکدام.

از اینجـا قاعـدهٔ بخش‌پـذیـری دو عـدد A وB کـه بـه‌صورت حاصلضرب عاملهای اول‌نوشته شده‌اند، بدست می‌آید: برای‌اینکه‌عدد A بر B بخش‌پذیر باشد، بایدهرعامل اول‌که در B وجود دارد باتوانی‌لااقل مساوی‌آن، در A نیز وجود داشته باشد. مثلا اگر داشته باشیم:

$$A=۲^{۳}\times ۳^{۲}\times ۵\times ۱۱\times ۱۳$$
$$B=۲^{۲}\times ۳\times ۵\times ۱۳$$

A بر B بخش‌پذیر است و خارج قسمت آن عبارت است از:

$$Q=۲\times ۳\times ۱۱$$

همچنین، به‌سادگی‌می‌توان‌کوچکترین مضرب مشترك وبزرگترین مقسوم علیه مشترك دو عـدد A وB را وقتی که به‌صورت حاصلضرب عاملهای اول‌نوشته‌شده‌اند، بدست‌آورد. کوچکترین‌مضرب مشترك‌تشکیل شده است از تمام عاملهای اول موجود در A وB با توان بزرگتر خود و بزرگترین مقسوم‌علیه مشترك تشکیل شده است ازعاملهای اول‌مشترك بین A وB با توانهای‌کوچکتر خود.

مثلا فرض کنید داشته باشیم:

$$A = ۲^{۳} \times ۳^{۵} \times ۵ \times ۱۱ \times ۱۳$$
$$B = ۲^{۴} \times ۳^{۲} \times ۵^{۳} \times ۷ \times ۱۷$$

خواهیم داشت:

$$M = ۲^{۴} \times ۳^{۵} \times ۵^{۳} \times ۷ \times ۱۱ \times ۱۳ \times ۱۷$$
$$D = ۲^{۳} \times ۳^{۲} \times ۵$$

و بلافاصله، رابطهٔ زیر بدست می‌آید:

$$A.B = M.D$$

زیرا در هریك از این دو حاصلضرب تمام عاملهای اولی که در A و B بود، وجود دارد. آن عاملهائی که درهردوعدد موجود بود، دارای توانی مساوی مجموع توانها در دو عدد A و B است وآن عاملهائی که تنها دریکی از دوعدد موجود بود، توان خود را حفظ کرده است.

جالب است یادآوری کنیم که با شناسائی عددهای اول کوچکتراز ۱۰۰، می‌توان تمام عددهای کوچکتر از $۱۰۰^{۲}$ یعنی ۱۰۰۰۰ را به حاصلضرب عاملهای اول، تجزیه کرد. فرض می‌کنیم A، عددی غیراول و کوچکتر از ۱۰۰۰۰ باشد. در اینحالت داریم:

$$A = a.b$$

که درآن a و b ممکن است عددهائی اول یا غیراول باشند. اگر a و b هردو بزرگتر از ۱۰۰ باشد، در اینصورت حاصلضرب ab از ۱۰۰۰۰ بزرگتر می‌شود و این با فرض ما متناقض است، زیرا A کوچکتر از ۱۰۰۰۰ بود. اگر مثلا a عددی کوچکتر از ۱۰۰ باشد، به‌این معناست که

عامل اولی کوچکتر از ۱۰۰ درآن وجود دارد (یعنی یکی از ۲۵ عاملی که قبلا ذکر کردیم). بنابراین کافی است ببینیم عدد A برکدامیك از این ۲۵ عدد بخش‌پذیر است و چنانچه A برهیچیك ازآنها بخش‌پذیر نباشد، عددی اول خواهد بود.

مثلا عدد ۷۴۵۸ را درنظر می‌گیریم، داریم:

۷۴۵۸=۳۷۲۹×۲

۳۷۲۹=۱۲۴۳×۳

عدد ۱۲۴۳ بر هیچیك از عددهای ۵ و ۷ بخش‌پذیر نیست، ولی داریم:

۱۲۴۳=۱۱۳×۱۱

و دیگرنمی‌توان عمل‌را ادامه داد، زیرا ۱۱۳ ازمربع ۱۱کوچکتر است وبا توجه به‌عملهائی‌که انجام دادیم برهیچ عددکوچکتر از ۱۱ نیز بخش‌پذیر نیست و بنابراین عددی است اول.

با یك روش عمومی‌می‌توان مطمئن‌شدکه عدد A اول است،وقتی که برهیچیك از عددهای اول‌کوچکتر از p بخش‌پذیر نباشد و درتقسیم بر p هم خارج قسمتی‌کوچکتر ازعدد اول بلافاصله بزرگتر ازp بدست آمده باشد. عدد A نمی‌تواند مقسوم‌علیه اولی بزرگتر از p داشته‌باشد، زیرا در اینصورت، خارج قسمت این تقسیم‌کوچکتر از p خواهد بود، چیزی‌که قبلا عدم وجودآنرا تحقیق‌کرده‌ایم.

این روش‌که درمورد تحقیق اول بودن یك عدد خاص نسبتاًساده است، وقتی بخواهند از آن برای عدهٔ زیادی از عددها عمل‌کنند، بسیار مشکل خواهد شد و بدیهی است‌که برای میلیونها عددکار را غیرممکن

می‌کند.

روش بسیار ساده‌تری دراین مورد وجود دارد، که از خیلی قدیم معمول بوده است و منسوب به اراتوستن Eratosthène می‌باشدو آن اینست که بین عددهای کوچکتر از ۱۰۰۰۰ یا ۱۰۰۰۰۰ و غیره، آنهائی را که اول نیستند مشخص می‌کنیم، به‌این ترتیب که کوچکترین مقسوم علیه آنها را (که عدد اولی است) معین می‌کنیم. این روش را غربال اراتوستن گویند.

۷. **غربال اراتوستن** . فرض کنید که بخواهیم عددهای اول کوچکتر از ۱۰۰ را معین کنیم، ابتدا عددهای زوج را کنار می‌گذاریم، سپس عددهای فرد را پشت سرهم روی سطرهای متوالی می‌نویسیم (و مثلا در هرسطر ۱۰ عدد)؛ دراینصورت جدول زیررا خواهیم داشت:

۱	۳	۵	۷	۹	۱۱	۱۳	۱۵	۱۷	۱۹
۲۱	۲۳	۲۵	۲۷	۲۹	۳۱	۳۳	۳۵	۳۷	۳۹
۴۱	۴۳	۴۵	۴۷	۴۹	۵۱	۵۳	۵۵	۵۷	۵۹
۶۱	۶۳	۶۵	۶۷	۶۹	۷۱	۷۳	۷۵	۷۷	۷۹
۸۱	۸۳	۸۵	۸۷	۸۹	۹۱	۹۳	۹۵	۹۷	۹۹

سپس قبل از همه، مضربهای ۳ را حذف می‌کنیم و این کارهم به سادگی انجام می‌گیرد، زیرا این مضربها ۳ به ۳ واقع شده‌اند.

وقتی مضربهای ۳ را حذف می‌کنیم، نیازی نخواهد بودکه‌عدد-های زوج حذف شده را به‌حساب‌آوریم، اما اگربعد از حذف مضربهای ۳ (بین عددهای فرد) بخواهیم مضربهای ۵ را حذف‌کنیم، باید عددها را ۵ به ۵ درنظرگرفت، بدون‌اینکه مضربهای ۳ را که قبل ازآن‌حذف کرده‌ایم، ازقلم بیندازیم.

برای حذف مضربهای موردنظر، بهتر است جدول بالا را به صورت زیر تنظیم کنیم، که در آن در دو انتهای سطرها رقمهای دهگان و در بالای ستونها رقمهای یکان قرار گرفته‌اند:

	۱	۳	۵	۷	۹	۱	۳	۵	۷	۹	
۰					۳			۳			۱
۲	۳		۵	۳			۳	۵		۳	۳
۴			۳		۷	۳		۵	۳		۵
۶		۳	۵		۳			۳	۷		۷
۸	۳		۵	۳		۷	۳	۵		۳	۹

ابتدا عدد ۳ را در خانه‌هائی که با عددهای بخش‌پذیر بر ۳ تطبیق می‌کنند ثبت می‌کنیم (به‌جز خود عدد ۳ که عدد اولی است)؛ همین کار را در مورد عدد ۵ و سپس در مورد عدد ۷ انجام می‌دهیم؛ خانه‌هائی که خالی می‌ماند، نمایندهٔ عددهای اولند. ملاحظه می‌شود که رقمهای ۳ در این جدول به‌وضع منظمی قرارگرفته است، در امتداد بعضی قطرها، همین وضع‌هم درمورد رقمهای ۵ و ۷ وجود دارد، به‌خصوص اگر مقسوم‌علیه‌های ۵ و ۷ را در خانه‌هائی هم که مقسوم علیه ۳ وجود دارد قرار دهیم این وضع روشن‌تر بنظر خواهد رسید.

۸. تناوب غربال برای عددهای کوچك. اگر توجه کنیم که

غربال دارای یك تناوب مسلم می‌باشد، به‌خصوص درمورد مقسوم‌علیه‌های اول کوچکتر می‌توان بسیاری از محاسبه‌ها را ساده‌تر انجام داد.

ابتدا به‌مقسوم علیه‌های ۲ و ۳ توجه کنیم. حاصلضرب این دو عدد مساوی ۶ است و بلافاصله نتیجه می‌شودکه اگرعددی برهیچیك‌از عددهای ۲ و۳ بخش‌پذیر نباشد، به‌یکی از صورتهای زیر خواهد بود :

$$۶n+۱ \quad و \quad ۶n+۵ \qquad (۱)$$

یعنی در هر ۶ عدد پشت سرهم، دوعدد وجود داردکه بر۲ و۳ بخش‌پذیر نیست. اکنون عددهائی را جستجو می‌کنیم کـه بر۲، ۳ یا ۵ بخش‌پذیر باشند. ملاحظه می‌شودکه بین این عددها، تنها سه عدد ۲، ۳ و ۵ وجود داردکه عددهائی اول هستند. با وجود این، ما آنها را جزوعددهائی‌که بر ۲، ۳ یا ۵ قابل قسمت‌اند به‌شمارمی‌آوریم.

بین عددهای (۱)،که نه بر۲ و نه بر۳ بخش‌پذیر نیستند،می‌توان عددهای‌کوچکتر از ۳۰ را به‌ازای ۴ و ۳ و ۲ و۱ و ۰ $=n$ بدست‌آورد (یعنی به‌ازای ۵ مقدار n) وبه‌این ترتیب، ما دارای ۵×۲ عدد خواهیم بود. اما بین این عددها، که بر ۲ یا ۳ بخش‌پذیر نیستند، تنها دو عدد وجود داردکه بر۵ بخش‌پذیراست، این دوعدد هم از ضرب ۵ در دوعدد کوچکتر از ۶ (که با ۲ و ۳ اولند) بدست می‌آید، یعنی عددهای ۱ و۵ که پس‌ازضرب در۵ نتیجه ۵ و۲۵ را می‌دهند، درنتیجه تعداد عددهائی که برهیچیك از عددهای ۲ و ۳ و ۵ قابل قسمت نیستند مساوی خواهد شد یا:

$$۲\times۵-۲=۲\times۴=۸$$

این ۸عدد عبارتند از۱ و ۷ و ۱۱ و۱۳ و۱۷ و ۱۹ و ۲۳ و ۲۹

که همهٔ آنها عددهائی اولند.

چون عدد ۳۰ بر ۲ و ۳ و ۵ بخش‌پذیر است، عددهایی که به‌یکی‌از صورتهای:

$$(۲)\quad \begin{cases} ۳۰n+۱ \text{ و } ۳۰n+۷ \text{ و } ۳۰n+۱۱ \text{ و } ۳۰n+۱۳ \\ ۳۰n+۱۷ \text{ و } ۳۰n+۱۹ \text{ و } ۳۰n+۲۳ \text{ و } ۳۰n+۲۹ \end{cases}$$

باشند بر ۲ و ۳ و ۵ بخش‌پذیر نخواهند بود. این عددها الزاماً عددهای اول نیستند، ولی تنها ازمیان‌آنهاست که باید عـددهای اول را جستجو کرد. به‌عبارت دیگر برای اول بودن یك‌عدد شرط (۲) شرطی لازم وغیر کافی است.

اکنون عدد اول ۷ را درنظرمی‌گیریم. عددهای کوچکتریامساوی حاصلضرب ۲۱۰ = ۳۰×۷، از روی رابطه‌های (۲) به‌ازای ۷ مقدار n یعنی ۰ و ۱ و ۲ و ۳ و ۴ و ۵ و ۶ بدست می‌آید. به‌این ترتیب تعدادی مساوی:

$$۸ \times ۷$$

عدد بدست می‌آیدکه همه‌آنها کوچکتر از ۲۱۰ بوده و هیچیك بر۲، ۳ یا ۵ هم بخش‌پذیر نیستند. بین این عددها، چند عدد وجود داردکه بر۷ بخش‌پذیرند؟ اگر یکی از این عددها بر۷ بخش‌پذیرباشد، خارج‌قسمت، عددی بین ۱ و ۳۰ خواهد بود و چون هیچیك ازاین عددها بر۲ و۳ یا۵ بخش‌پذیر نیستند، بنابراین خارج قسمت آنها بر ۷ هم عددیست بخش‌ناپذیر بر ۲ و ۳ یا ۵، در نتیجه این خارج قسمت یکی از ۸ عددی‌است که قبلا ازآنها نام بردیم. برعکس، حاصلضرب هر یك از این ۸عدد در

عدد ۷ یعنی :

(۳)   ۲۰۳ و ۱۶۱ و ۱۳۳ و ۱۱۹ و ۹۱ و ۷۷ و ۴۹ و ۷

عددهائی خواهند بودکوچکتر از ۲۱۰ و بخش‌ناپذیر بر۲ و۳ و ۵ ، ولی بخش‌پذیر بر ۷. بالاخره بین ۲۱۰ عدد اولیه، تعداد عددهائی‌که بر ۲ و ۳ و ۵ و ۷ بخش‌پذیر نیستند، مساوی:

$$۸ \times ۷ - ۸ = ۸ \times ۶ = ۲ \times ۴ \times ۶ = ۴۸$$

خواهد بود.

ما صورت این ۴۸ عدد را ذکـر نخواهیم کرد؛ اینها عـددهائی هستندکه از رابطـه‌های (۲) به‌ازای ۶ و ۵ و ۴ و ۳ و ۲ و ۱ و ۰ $=n$ بدست می‌آیند، به‌شرطی‌که عددهای مذکور در (۳) را ازبین آنها حذف کنیم.

اگر α نمایندهٔ هریك از این ۴۸ عدد باشد، عددهایی به‌صورت:

$$۲۱۰n+\alpha \qquad (۴)$$

بر۲، ۳، ۵ و۷ بخش‌پذیرنیستند. بنابراین می‌توانند عددهائی اول‌باشند. در حقیقت هر۴۸ عدد α اول نیستند و بین‌آنها، عددهائی وجود داردکه غیر اولند:

$$۱۱^۲=۱۲۱ \text{ و } ۱۱ \times ۱۳=۱۴۳ \text{ و } ۱۳^۲=۱۶۹ \text{ و } ۱۱ \times ۱۷=۱۸۷$$

برعکس عددهای ۲، ۳، ۵ و ۷، عددهایی اول هستند، در حالیکه درصورت عددهای بخش‌ناپذیر بر ۲، ۳، ۵ و ۷ وجود ندارند.

به‌همین ترتیب می‌توان باکمك عدد اول ۱۱، که بلافاصله بعد از ۷ قرارگرفته، ۲۳۱۰ عدد اولیه را مورد مطالعه قرار داد.

$$(۲۳۱۰ = ۲ \times ۳ \times ۵ \times ۷ \times ۱۱)$$

دربین این‌عددها $۴۸۰ = ۱۰ \times ۶ \times ۴ \times ۲$ عدد β وجود دارد[۱]، که هیچیك از آنها برعددهای ۲، ۳، ۵، ۷ و ۱۱ بخش‌پذیر نیستند و به‌صورت[۲]: $۲۳۱۰n + \beta$ نوشته می‌شوند و عددهای اول را باید تنها بین آنها جستجو کرد. اکنون اگر عدد اول ۱۳ را هم درنظربگیریم عدد:

$$۲۳۱۰ \times ۱۳ = ۳۰۰۳۰$$

بدست می‌آید، که شکل ظاهری آن‌هم بسیار ساده است. بین این ۳۰۰۳۰ عدد اولیه به‌تعداد:

$$۴۸۰ \times (۱۳ - ۱) = ۴۸۰ \times ۱۲ = ۵۷۶۰$$

عدد وجود داردکه برهیچیك از عددهای اول کوچکتر از ۱۷ بخش‌پذیر نیستند. برای‌بدست‌آوردن عددهای اول کوچکتراز ۳۰۰۳۰ بایدمضربهای ۱۷، ۱۹، . . . و غیره تا ۱۷۳ (جذر نقصانی ۳۰۰۳۰) را بین آنها حذف نمود. این کار نسبتاً مفصلی است، ولی با توجه به‌اینکه یکباره به‌اندازهٔ $۲۴۲۷۰ = ۵۷۶۰ - ۳۰۰۳۰$ عددکه بخش‌پذیربریکی ازعددهای ۲، ۳، ۵، ۷، ۱۱ و ۱۳ هستند، حذف می‌شود، کار را ساده می‌کند. همچنین می‌توان این عددها را، در سلسله عددهای متوالی از ۳۰۰۳۰ به وسیلهٔ روش ساده‌ای که ذکر شد حذف کرد، زیرا آنها متناوباً ظاهر می‌شوند.

---

۱. می‌توان نوشت:

$$۴۸۰ = (۳ - ۱)(۵ - ۱)(۷ - ۱)(۱۱ - ۱)$$

۲. بین عددهائی که به‌صورت (۴) هستند باید حاصلضربهای عدد ۱۱ را در هریك از ۴۸ عددی که بر ۲، ۳، ۵، و ۷ بخش‌پذیر نیستند، حذف کرد.

۹. بی‌انتها بودن رشتهٔ عددهای اول. ازآنچه که تا کنون گفته شد می‌توان به‌سادگی نتیجه گرفت که رشتهٔ عددهای اول بی‌پایان است، یا به‌زبان دیگرآخرین عدد اول وجود ندارد. درحقیقت ازمحاسبهٔ ساده‌ای که قبلا انجام دادیم نتیجه می‌شودکه اگر تنها عددهای اول ۲ و ۳ و ۵ و۷ را درنظر بگیریم بین ۲۱۰ عدد اولیه، ۴۸ عدد[1] وجود دارد که نمی‌توان آنهارا ازضرب یکی از این۴ عامل اول در دیگـران بدست آورد. اگر تعداد عددهای اول را زیادترولی محدود درنظربگیریم، باز-هم عددهای بسیار زیادتری پیدا خواهد شدکه نتیجهٔ ضرب عددهای اول محدودی‌که در نظرگرفته‌ایم نباشند. مثلا اگرعددهای اول۲، ۳، ۵، ۷، ۱۱ و ۱۳ را در نظر بگیریم، بین ۳۰۰۳۰ عدد درست اولیه ، تعداد $۲\times۴\times۶\times۱۰\times۱۲=۵۷۶۰$ عدد وجود داردکه ازضرب یکی ازاین عددهای اول، در بعضی دیگر بدست نیامده است.

استدلال دیگری‌هم برای اثبات نامحدود بودن عددهای اول‌وجود دارد،که خیلی قدیمی است و از بعضی جهات ساده‌تر هم هست، ولی به روشنی نشان نمی‌دهدکه تعداد عددهای اول چقدرزیاد است. این‌استدلال چنین است: ثابت می‌کنیم لااقل یك عدد اول وجود دارد که بزرگتر از عدد درست و دلخواه n می‌باشد. اگر حاصل ضرب n عدد درست اولیه را به $n!$ نشان دهیم و عدد A را با رابطهٔ زیر مشخص‌کنیم:

$$A=n!+۱ \qquad (۱)$$

اگر عدد A، عددی اول نباشد، باید حداقل دارای یك مقسوم علیه اول

[1] و یا به‌طور دقیق‌تر : ۴۷ عدد ، زیرا در اینجا نباید شمار را از عدد ۱ شروع کرد.

p باشد. این مقسوم‌علیه p نمی‌تواند کوچکتر یا مساوی n شود، زیرا با توجه به‌رابطهٔ (۱) اگرعدد A را برعددی مانند α ،که بین ۲ و n قرار گرفته است، تقسیم کنیم، باقیماندهٔ تقسیم مساوی واحد خواهد شد، یعنی A بر α بخش‌پذیر نیست و بنابراین عـدد اولی مانند p وجود دارد که بزرگتر از n می‌باشد.

۲
جدول عددهای اول

۱۰. محاسبهٔ جدول. با توجه به آنچه پیش از این گفتیم، روشن می‌شود که می‌توان به‌سادگی، ولی با شکیبائی، جدول عددهای اول را تنظیم کرد. درحقیقت سالها وقت صرف شده است تا اینکه‌عددهای اول کوچکتر از ۱۰ میلیون را معین کرده‌اند. این جدولها چاپ‌شده است و برای هریك از ۱۰ میلیون عدد نخستین، کوچکترین مقسوم‌علیه عددهای فرد را هم معین کرده وجلوآن نوشته‌اند. درنتیجه هرعددفردی که جلوآن سفید باشد (یعنی مقسوم علیه نداشته باشد) عدد اول خواهد بود.

همچنین بعضی دیگر، عددهای اولی‌را که درفاصلهٔ دوعددبزرگ (بالاتر از ۱۰ میلیون) قرارگرفته است محاسبه کرده‌اند: مثلا عددهای اولی که درفاصلهٔ بین دوعدد۱۰۰۰۰۰۰۰۰ و ۱۰۰۱۰۰۰۰۰ واقع‌است. طبیعی است که این محاسبه‌ها بسیار مفصل و طولانی است، زیرا باید تمام عددهایی را که بین این دوعدد قرار دارند و مضربی از عددهای اول کوچکتر ازجذر تقریبی ۱۰۰ میلیون هستند حذف کرد. (یعنی عددهای اول کوچکتر از ۱۰۰۰۰ که به‌طورتقریب ۲۰۰۰ عدد است).

تعمیم و تکمیل ماشینهای حساب، به‌سرعت عمل محاسبه‌ها کمك فراوانی کرده است. معهذا باید همیشه مراقبت جدی‌شود تاازاشتباههای مربوط به‌رونویس کردن، همچنین اشتباههای مربوط به‌چاپخانه‌ها

جلوگیری شود. می‌توان انتظار داشت که این‌کار ارزنـده، در پیشرفت دانش ما دربارهٔ عددهای اول بی‌اندازه مفید باشد. واین پیشرفت هم، در پیشرفت آنالیز عـالی (که دراین‌کتاب نمی‌توانیم ازآن گفتگو کنیم) می‌تواند سهم زیادی داشته باشد. معهذا باید اعتراف‌کرد که باوجود این که آنالیزدانها در شناسائی عددهای اول‌کوششهای زیادی‌کرده‌اند، باز هم در مورد شناختن عددهای اول نقطه‌های تاریکی وجود دارد. ولی با تحقیقات با حوصلهٔ آماری، که روی جـدول عددهای اول انجام گرفته است، بعضی قضیه‌ها و طـرحها به‌نظر می‌رسد و به‌ما تلقین می‌شود که بالاخره روزی با استدلال‌منطقی‌ریاضیدانان، تأیید خواهدشد. شکی‌نیست که این روش تجـربی و تجسسی، در گـذشته به‌وسیلهٔ عـدهٔ زیـادی از دانشمندان ریاضی، با موفقیت مورد استفاده قرارگرفته است وبه‌همین مناسبت بی‌فایده نیست اگر در اینجا نمونه‌هائی از اینگونه بررسیهای آماری‌را عنوان‌کنیم‌که مسألهٔ شناختن‌عددهای اول را تا اندازه‌ای‌روشن می‌کند.

۱۱. قضیهٔ تصادف «hypothèse du hasard». یـکی از قضیه‌های بسیار جالبی‌که از این بررسیهای آماری نتیجه می‌شود قضیهٔ تصادف است. این قضیه با قانون تناوب غربال (که در شمارهٔ ۸ ازآن صحبت‌کردیم) ارتباط‌کامل دارد. ولی می‌توان گفت که قضیهٔ تصادف، این قانون را در بعضی حالتهاتکمیل می‌کند.

در واقع دیده می‌شود که عددهای بخش‌پذیر برعاملهـای اول ۲ و ۳ و۵، درهر۳۰ عدد متوالی، به‌طور متناوب تکرار می‌شود. عددهایی که بر ۲ و ۳ و ۵ بخش‌پذیر نیستند به‌یکی از صورتهای زیر می‌باشند:

$$30n+1 \quad و \quad 30n+7 \quad و \quad 30n+11$$
$$30n+13 \quad و \quad 30n+17 \quad و \quad 30n+19$$
$$30n+23 \quad و \quad 30n+29$$

در ده عدد نخستین، دوعدد و در ۱۰ عدد دوم، ۴ و در ۱۰ عدد سوم، ۲ عدد از این عددها وجود دارد.

ازاین عددها، ۲۶ عدد بین ۱ تا ۱۰۰ و ۲۸ عدد بین ۱۰۱تا۲۰۰ و ۲۶ عدد بین ۲۰۱ تا ۳۰۰ وجود دارد و این تعداد به‌همین ترتیب در هرصد عدد بعدی متناوباً تکرارمی‌شود.

اکنون اگرعددهای اول از ۲تا ۱۳ را درنظربگیریم، حاصلضرب آنهامساوی ۳۰۰۳۰ خواهد شد. دراینجاهم همان پدیده دوباره به‌وجود می‌آید، منتهی دورهٔ تناوب، به‌جای۳۰، برابر۳۰۰۳۰ می‌شود، به‌قسمی که اگر عددهای متوالی را به‌دسته‌های ۳۰عددی تقسیم کنیم (دسته‌هایی که تعداد عددهای غیربخش‌پذیر بر۲ و ۳ و ۵ درآنها مساوی ۸می‌باشد)، تعداد عددهایی که دراین دسته‌ها بر۷ و ۱۱ و ۱۳ بخش‌پذیر هستند، مختلف خواهد بود. برای ۱۰ دستهٔ اول (۱ تا ۳۰ و ۳۱ تا ۶۰ و ... و ۲۷۱ تا ۳۰۰) تعداد این عددها به‌ترتیب مساوی ۳ و ۱ و ۱ و ۲ و ۳ و ۲ و ۳ و ۲ و ۳ و ۱ می‌باشند و به‌این ترتیب، تعداد عددهایی که بر ۲و ۳ و۵ و۷ و۱۱ و۱۳ بخش‌پذیر نیستند، به‌ترتیب مساوی ۵ و۷ و۷ و۶ و۵ و۶و۵ و۶ و۵ و۷ خواهد شد (که از تفاضل مقادیر قبلی از۸ بدست آمده‌اند). به‌همین ترتیب، برای ۱۰۰۱ دستهٔ اول از عددهای ۳۰ تائی یعنی تا عدد ۳۰۰۳۰ مقادیر مختلفی بدست خواهدآمد. تنها وقتی که به این عدد می‌رسیم، مقادیرقبلی به‌طور تناوبی تکرارمی‌شوند، به‌این معنی که بین دو عدد ۳۰۰۳۱ تا ۳۰۰۶۰، ۵ عدد وجود دارد که بر عددهای

۲ و ۳ و ۵ و ۷ و ۱۱ و ۱۳ بخش‌پذیر نیستند (که برابر است با تعداد همین عددها، وقتی‌که از ۱ تا ۳۰ را درنظر می‌گیریم).

دیده می‌شود وقتی‌که بخواهیم تعداد عددهای اول را مرتباً زیادتر بگیریم، طول دورهٔ تناوب با چه سرعتی بزرگ می‌شود، به‌طوریکه اگر بخواهیم عددهایی را جستجو کنیم که برهیچیك از عددهای اول کوچکتر از ۱۰۰ بخش‌پذیرنباشند، دورهٔ تناوب مساوی با حاصلضرب این عددها خواهد شد که عددیست با قریب ۳۰ رقم و روشن است که حتی برای عددهایی که می‌توان اول بودن آنها را مورد بررسی قرار داد، نمی‌توان عملا از راه تناوب به نتیجه رسید، چه رسد به‌اینکه با عددهای بزرگتر از یك میلیون سروکار داشته باشیم، که دراین حال می‌تواند کوچکترین عامل اول آن نزدیك به ۱۰۰۰ باشد.

اکنون می‌توانیم قضیهٔ تصادف را توضیح بدهیم: این قضیه مربوط است به‌توزیع عددهای اول در دسته‌های متوالی عددها ومثلا در دسته‌های ۱۰۰ عددی. قضیه چنین است: توزیع در دسته‌های ۱۰۰ عددی، از قانون تصادف، با در نظر گرفتن دورهٔ تناوب برای عددهای اول کوچکتر، تبعیت می‌کند.

این تناوب، تعداد عددهای اولی را که احتمالا وجود دارد، کم می‌کند؛ اگر خود را به‌عاملهای ۲ و ۳ و ۵ محدود کنیم، در هر ۱۰۰ عدد متوالی ۲۶ یا ۲۸ عدد وجود دارد که بر ۲ و ۳ و ۵ بخش‌پذیر نیستند و اگر عامل ۷ را هم درنظر بگیریم، این تعداد بازهم کمترمی‌شود. ازطرف دیگر (همانطورکه مابعداً تحقیق خواهیم کرد) می‌توان تعداد متوسط عددهای اولی که در هر ۱۰۰ عدد از عددهایی که مثلا بین ۱۰۰۰۰۰۰ و ۱۱۰۰۰۰۰ وجود دارد معین کرد، این تعداد، بیشتر از ۷ خواهد بود. اگر توزیع

عددهای اول به‌طور منظم‌وجود داشت، می‌بایستی درهر ۱۰۰ عدد ۷ عدد اول وجود داشته باشد، ولی در حقیقت باوجودی که عدد ۷ به‌فراوانی دیده می‌شود، ولی تعداد واقعی عددهای اول در فاصله‌های ۱۰۰ تایی ، اغلب با ۷ فرق دارد و از ۰ تا ۱۴ تغییرمی‌کند.

می‌توان مقابلهٔ عددهای اول را با نتیجه‌هایی که‌بدست می‌آید، به این‌ترتیب روشن کرد که درمقیاس ۱۰۰، در یك جعبه، ۷ گلولهٔ سیاه در هرصد عدد گلوله وجود دارد، یعنی ۷ گلولهٔ سیاه و ۹۳ گلـولهٔ سفید. روشن‌است‌که اختلاف تعداد عددهای اول‌نسبت به‌حد متوسط تعدادآنها، خیلی‌کمتر از نسبتی است‌که دراینجا دیده می‌شود.

بنابراین لازم است به‌تناوب مسلمی‌که برای عددهای اول‌کوچك محقق شده است، توجه داشت. تناوبی که پدیدهٔ مورد نظر را به‌نظم در آورده است. اگرتنهاعاملهای اول ۲ و۳ و۵ را درنظر بگیریم،می‌بینیم که تعداد عددهایی‌که احتمالاً اول هستند (یعنی عددهایی‌که بر۲ و۳و۵ بخش‌پذیرنیستند) در هر۱۰۰عدد متوالی برابر۲۶یا۲۸ می‌باشد. بنابراین لازم نیست جعبه‌ای درنظر بگیریم‌که در مقیاس ۱۰۰گلولهٔآن، ۷گلولهٔ سیاه و ۹۳ گلولهٔ سفید وجود دارد، بلکه باید جعبه‌ای را درنظرگـرفت که مثلا در مقابل هر ۷ گلولهٔ سیاه ۲۰ گلولهٔ سفید وجود داشته باشد (در مقیاس ۲۷ گلوله). می‌توان عددهای اول بیشتری در نظر گـرفت، حاصلضرب عـددهـای اول تا ۱۷ مساوی ۵۱۰۵۱۰ و تـا ۱۹ مساوی ۹۶۹۹۶۹۰ می‌باشد. عـددهایی که مـورد بـررسی مـاست، بین ایـن‌دو حاصلضرب‌قرارگرفته‌است واگرعددهای‌اول‌را تا۱۷درنظربگیریم، انتظام دیگـری برقـرار خـواهد شد. بین ۵۱۰۵۱۰ عـدد نخستین بـه‌انـدازهٔ ۱۶×۱۲×۱۰×۶×۴×۲ عدد وجود داردکه برعددهای اول تا ۱۷

بخش‌پذیر نیستند، یعنی ۱۶ × ۵۷۶۰ عدد بین قریب ۵۰۰۰۰۰ عدد که تقریباً ۱۸٪ آنها خواهد شد. اکنون گلوله‌های داخل جعبه را در مقیاس هر ۱۸ گلوله ۷ گلولهٔ سیاه و ۱۱ گلولهٔ سفید درنظر گرفت ومحقق است که‌نسبت‌محاسبه‌شده، به‌وسیلهٔ قضیهٔ‌نظری، به‌نسبتی که مشاهده‌می‌شود، خیلی نزدیکتر می‌شود.

اکنون می‌توانیم قضیهٔ تصادف را در حالت معینی به‌نظم در آوریم:

یك دستهٔ T که به‌طور تصادف از ۱۰۰ عدد متوالی و مثلا بین ۲۰۰۰۰۰۰ و ۲۱۰۰۰۰۰ واقع است درنظرمی‌گیریم. احتمال اینکه‌دستهٔ T شامل p عدد اول باشد، برابر است با احتمال وجود p گلولهٔ سیاه‌در مقیاس q گلوله در جعبه‌ای‌که دارای n گلـولهٔ سیاه و q−n گلولهٔ سفیداست؛ عددهای q و n به‌این‌ترتیب انتخاب شده‌اند: عدد q عبارتست از تعداد ممکنی از عـددها، که می‌توانند در هـر ۱۰۰ عدد اول باشند، با احتساب عددهایی‌که بخش‌پذیر برعددهای اول‌کوچك (تا ۱۷)هستند، و n عبارتست ازتعداد متوسط عددهای اولی‌که در هر ۱۰۰ عدد از دستهٔ مورد مطالعه وجود دارد.

روشن‌است‌که صحیح نیست اگر ازاحتمال اینکه‌یك عددمفروض اول است یا نه صحبت‌کنیم، زیرا اگرعدد معین باشد می‌توان، به‌سادگی اول بودن یا نبودن‌آنرا معین‌کرد. ولی می‌توان از احتمال اول بودن‌یك عدد صحبت کرد، وقتی که عدد صحیحی به‌طور تصادفی و با شرطهایی انتخاب می‌شود، مثلا برای این‌که نمرهٔ برندهٔ جایزهٔ بزرگ بخت‌آزمائی ملی عددی اول باشد.

همچنین نمی‌توان دراین زمینه صحبت‌کردکه مثلا احتمال‌وجود

۷ یا ۹ عدد اول بین دو عدد ۲۰۰۵۵۰۰ و ۲۰۰۵۶۰۰ چقدر است، زیرا تعداد عددهای اول در این فاصله کاملا مشخص است، ولی اگر a و b و c را سه رقم غیرمشخص (از ۰ تا ۹) فرض کنیم می‌توان از احتمال وجود ۸ عدد اول در فاصلهٔ ۲۰abc۰۰ و ۱۰۰ + ۲۰abc۰۰ صحبت کرد، وقتی‌که a و b و c رقمهایی باشند که به‌طور تصادفی انتخاب می‌شوند. این احتمال تقریباً * برابر است با احتمال وجود ۸ گلولهٔ سیاه در مقیاس ۱۸ گلوله در جعبه‌ای که در مقابل هر ۷ گلولهٔ سیاه ۱۱ گلولهٔ سفید وجود دارد.

۱۲. تحقیق تجربی قضیه. برای این‌که قضیهٔ تصادف‌را به‌طور تجربی مورد تحقیق قرار دهیم، کافی است با استفاده از جدول عددهای اول، به‌روش آماری متوسل‌شویم. آماری که در اینجا از آن استفاده شده است مربوط به‌مطالعات یك نفر بلغاری بنام ز. سوگارف (Z. Sougarev) می‌باشد که دو سال قبل‌از شروع جنگ ۱۹۳۹ را در فرانسه زندگی می‌کرده‌است. اوقسمتی ازاین دوسال‌را درپاریس وقسمتی را درآسایشگاه دانشمندان زندگی‌کرد وفرصتهای بیکاری خود را صرف کارهای آماری کرد. من ازکارهای جدید وبعد ازجنگ او اطلاعی‌ندارم، معهذا در «گزارشهایی از آکادمی علوم» از او نام برده‌ام.

جدول I که دراینجا دیده می‌شود (صفحهٔ۴۷) مربوط به‌عددهای بین ۲ میلیون و ۲ میلیون و ۱۰۰۰۰۰ می‌باشد. در اولین ستون‌که با

---

*) می‌گوییم تقریباً، زیرا تعداد متوسط عددهای اول در هر ۱۰۰ عدد، در فاصلهٔ مورد نظر دقیقاً مساوی ۷ نیست، بلکه مساوی ۶/۸۷۴ می‌باشد.

حرف n عنوان شده است، به‌طور ساده اولین عدد هردسته ۱۰۰۰۰عددی را ثبت کرده‌ایم، به‌نحوی که مثلامنظور از ۳۰۰۰۱تمام عددهایی است که بین ۲۰۳۰۰۰۱ و ۲۰۴۰۰۰۰ می‌باشد و درسایر ستونها: تعدادعددهای بخش‌پذیر برعددهای اولی که در زیر مشخص کرده‌ایم معین شده‌اند:

a) ۲ و ۳ و ۵،

b) از ۷ تا ۱۹،

c) از ۲۳ تا ۹۷،

d) بالاتر از۱۰۰،

e) عددهای اول.

دیده می‌شودکه مجموع عـددهای سطر چهارم مساوی ۱۰۰۰۱ و مجموع عددهای سطر پنجم ۹۹۹۹ می‌باشد و بنابراین در هریك ازاین‌دو سطر اشتباهی برابر یك واحد وجود دارد. مجموع عددهای سایر ستونها درست برابر۱۰۰۰۰ می‌باشد و این به‌معنای آنست که احتمال اشتباه‌قابل ملاحظه درآنها خیلی کم است.

مقایسهٔ این ۵ ستون نشان می‌دهدکه هرچه از اولین ستون‌دورتر می‌شویم بی‌نظمی بیشتر می‌شود، به‌طوریکه اختلاف بین‌کـوچکترین و بزرگترین عـدد در ستون اول ۲ و در ستون دوم ۶، در ستون سوم ۱۶، درستون چهارم ۳۱ و درستون پنجم مساوی۳۵ است. این اختلاف‌وقتی که ستونها را با هم مقایسه می‌کنیم هنوزخیلی زیاد است، به‌نحوی که عددهای ستون اول، بیشتر از ۱۰ برابر و عددهای ستون دوم نزدیك دو برابرستونهای سوم و چهارم هستند. برای هریك ازستونهای این‌جدول،

جدول I

N	a	b	c	d	e	کنترل اشتباه
۲۰۰۰۰۰۰۰+						
۰۰۰۱۰۰۰	۷۳۳۴	۹۵۵	۴۹۷	۵۰۹	۷۰۵	
۱۰۰۰۱۰۰۰	۷۳۳۴	۹۵۹	۵۰۸	۵۰۸	۶۹۱	
۲۰۰۰۱۰۰۰	۷۳۳۲	۹۵۶	۵۰۲	۵۱۷	۶۹۳	
۳۰۰۰۱۰۰۰	۷۳۳۴	۹۵۴	۵۱۳	۵۰۹	۶۹۱	(+۱)
۴۰۰۰۱۰۰۰	۷۳۳۴	۹۵۶	۵۰۵	۵۳۴	۶۷۰	(−۱)
۵۰۰۰۱۰۰۰	۷۳۳۲	۹۵۷	۵۱۲	۵۰۳	۶۹۶	
۶۰۰۰۱۰۰۰	۷۳۳۴	۹۵۷	۵۰۴	۵۱۱	۶۸۴	
۷۰۰۰۱۰۰۰	۷۳۳۴	۹۵۴	۵۰۷	۵۳۱	۶۷۴	
۸۰۰۰۱۰۰۰	۷۳۳۲	۹۶۰	۵۰۷	۵۱۵	۶۸۶	
۹۰۰۰۱۰۰۰	۷۳۳۴	۹۵۹	۵۰۲	۵۳۱	۶۷۴	
جمع	۷۳۳۳۴	۹۵۶۷	۵۰۵۷	۵۱۶۸	۶۸۷۴	

جدول مفصلتری تهیه شده است که ما در اینجا، آنرا مربوط به‌ستون e ، یعنی ستون عددهای اول است‌می‌آوریم (جدولII صفحهٔ ۴۸). هریك از سطرهای این جدول مثل هرسطرجدول قبلی بایك دستهٔ ۱۰۰۰۰۰عددی

جدول II

	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳
۰۰۰۰۱۰۰۰			۳	۷	۱۳	۲۵	۱۰	۱۳	۱۶	۱۰	۲		۱
۱۰۰۰۱۰۰۰			۳	۸	۱۰	۲۰	۲۲	۱۷	۱۵	۲	۱	۲	
۲۰۰۰۱۰۰۰		۲	۵	۹	۹	۱۳	۲۳	۱۵	۱۱	۸	۵		
۳۰۰۰۱۰۰۰		۲	۲	۴	۱۴	۱۷	۲۵	۲۲	۴	۶	۳		۱
۴۰۰۰۱۰۰۰	۲	۱	۲	۸	۱۳	۲۶	۱۴	۱۱	۱۱	۱۱		۱	
۵۰۰۰۱۰۰۰	۱		۳	۵	۱۰	۲۳	۲۳	۱۳	۱۲	۷	۱	۲	
۶۰۰۰۱۰۰۰			۴	۶	۱۲	۲۵	۱۸	۱۲	۱۱	۷	۳	۲	
۷۰۰۰۱۰۰۰		۲	۵	۷	۱۳	۱۴	۲۳	۱۶	۱۴	۳	۳		
۸۰۰۰۱۰۰۰		۲	۲	۹	۹	۱۷	۲۵	۱۸	۱۱	۳	۳	۱	
۹۰۰۰۱۰۰۰		۲	۳	۵	۱۵	۱۷	۲۲	۲۰	۱۰	۶			
جمع	۳	۱۱	۳۲	۶۸	۱۱۸	۱۹۷	۲۰۵	۱۵۷	۱۱۵	۶۳	۲۱	۸	۲

تطبیق می‌کنند و این دسته هم به ۱۰۰ دستهٔ ۱۰۰ عددی تقسیم می‌شود. عددهای ثبت شده درستونهای مختلف سطراول این جدول تعدادعددهای اول دسته‌های ۱۰۰ عددی ازاین ۱۰۰دسته را (که از ۲۰۰۰۰۰۱ شروع شده‌اند) معین می‌کنند. به‌این ترتیب‌که از این دسته‌ها ۳ دسته وجود داردکه هرکدام شامل ۳ عدد اول هستند. ۷ دسته شامل ۴ عدد اول، ۱۳

دسته شامل ۵ عدد اول، ۲۵ دسته شامل ۶ عـدد اول، ۱۰ دسته شامل ۷ عدد اول، ۱۳ دسته شامل ۸ عدد اول، ۱۶ دسته شامل ۹ عـدد اول، ۱۰ دسته شامل ۱۰ عدد اول ، ۲ دسته شامل ۱۱ عدد اول و بالاخـره یك دسته شامـل ۱۳ عـدد اول هستند. در مورد سطرهای بعدی هم به‌همین ترتیب.

بررسی این جدول روشن می‌کندکه برای هرسطر بی‌نظمیهایی در مورد توزیع عددهای صدتایی که شامل تعدادی عدد اول (از ۱ تا ۱۳) هستند، وجود دارد (عددمتوسط که ازجدول I بدست آمد مساوی ۶/۸۷۴ بود). سطر اول دارای دوعدد ماکزیمم است (۲۵ و۱۶)، عددهای‌ستون ششم در مورد سطرهای ۲۰۰۰۰۱ و ۷۰۰۰۰۱ به‌طور غیرمنتظره‌ای کوچك می‌شوند (۱۳ و۱۴) وهمچنین درسطرهای ۱۰۰۰۰۰(۱۰) و۴۰۰۰۰۱(۱۴). اما درعوض مجموعها به‌طور بارزی معرف یکنوع توزیع منظم عددهای اول طبق قانون لاپلاس ـ گوس می‌باشند، با یك پراکندگی نسبتاً مهم وقتی که تعداد عددهای اول در بعضی از دسته‌های ۱۰۰ عددی مساوی ۱ و در بعضی دیگر مساوی ۱۳ می‌باشد. اما این پراکندگی دقیقاً نتیجهٔ تصادفی است که برای ۱۰۰۰ سری بدست آمده است، که در هرسری هم احتمال وجود ۱۷ عدد اول وجود دارد. مثل اینکه در جعبه‌ای که شامل ۱۷۰۰۰ گلوله است ۶۸۷۴ عدد آن گلوله‌های سیاه باشند. بی‌نظمیهایی که مشاهده می‌شود یك امـرکاملا طبیعی است و قضیهٔ تصادف را تأیید می‌کند.

اکنون نتیجه‌هـایی را که از جدول قبل‌گرفتیم، دربارهٔ ۱۰۰۰۰ دستهٔ صدتایی تا ۱۰ میلیون، یعنی عددهای بین ۹۰۰۰۰۰۱تا۱۰میلیون مورد بررسی قرار می‌دهیم. در اولین ستون از جـدول III که با $۱۰^۵$

مشخص شده‌است، درهرسطر ۱۰۰۰۰۰ واحد وجود دارد، یعنی ۱۰۰۰ دستهٔ صدتایی و مثلا از ۹۰×۱۰^۵ و تا ۹۱×۱۰^۵، سپس در ستون n تعدادکل عددهای اولی که در این فاصله وجود دارد، یادداشت شده و در ستونهای بعدی که در بالای آنها عددهای از ۱ تا ۱۴ نوشته شده تعداد دسته‌های ۱۰۰ تایی که دارای ۱ یا ۲ ... یا ۱۴ عدد اول هستندمشخص شده است.

دیده می‌شودکه پراکندگی عددهای اول، آنطور که از مجموعها ملاحظه می‌شود کاملا منظم هستند و تقریباً همان نتیجه‌ای که برای ۳ میلیون وجود داشت، برای ۱۰ میلیون نیز وجود دارد. بنابراین‌می‌توان قبول‌کردکه ازقبل قانون عمومی وجود دارد. معهذا جالب است‌که این آمارگیری عددهای اول را در مورد فاصله‌های نزدیك؛ عددهای خیلی بزرگ و مثلا ۱۰۰ میلیون انجام دهیم. ستونی‌که با عدد n مشخص‌شده است به‌خصوص خیلی جالب توجه است، زیرا نشان می‌دهدکه فرکانس عددهای اول درنزدیکی عدد غیر مشخص N چگونه است. از این ستون نتیجه می‌شود که برای فاصله‌های بزرگ نسبت به‌این فرکانس نظری، اختلافهای نسبتاً مهمی وجود دارد.

برای فاصله‌های‌مساوی ۱۰۰۰۰۰، تعداد عددهای‌اولی که دردهمین میلیون مشاهده می‌شود برابر است با :

۶۱۷۷،	۶۲۲۳،	۶۲۴۵،	۶۱۸۲،
۶۱۳۴،	۶۲۰۱،	۶۲۰۲،	۶۲۷۱،

به‌نظر می‌رسدکه اولین عدد به‌طور غیر طبیعی‌کوچك است، ولی ریشهٔ دوم آن نسبت به‌مقدار متوسط، اختلاف زیادی ندارد به‌نحوی که

جدول III

$\times 10^5$	n	۰	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴
۹۰ تا ۹۱	۶۱۸۲		۴	۲۱	۵۴	۱۲۴	۱۷۶	۱۸۶	۱۷۹	۱۳۱	۸۲	۳۲	۹	۲		
۹۱ تا ۹۲	۶۲۴۵		۲	۲۰	۶۰	۱۲۶	۱۵۱	۱۹۵	۱۸۹	۱۲۷	۷۸	۲۹	۱۵	۶	۲	
۹۲ تا ۹۳	۶۲۵۹		۲	۲۶	۴۸	۹۸	۱۶۱	۲۲۸	۱۹۰	۱۲۷	۷۷	۲۴	۱۲	۶	۱	
۹۳ تا ۹۴	۶۲۲۳		۳	۲۱	۵۳	۱۰۳	۱۶۱	۲۱۵	۱۹۵	۱۱۴	۷۳	۲۴	۱۲	۳	۲	۱
۹۴ تا ۹۵	۶۱۷۷		۶	۲۴	۵۶	۱۰۵	۱۸۹	۲۰۰	۱۶۶	۱۲۰	۸۴	۴۱	۶	۳		
۹۵ تا ۹۶	۶۲۷۱	۱	۱	۱۳	۵۴	۱۲۴	۱۵۷	۱۹۴	۲۰۶	۱۳۹	۵۹	۳۲	۱۰	۸	۲	
۹۶ تا ۹۷	۶۲۰۲		۳	۲۵	۵۵	۱۱۱	۱۷۶	۲۱۲	۱۷۰	۱۱۲	۸۳	۳۴	۱۴	۴	۱	
۹۷ تا ۹۸	۶۲۰۸	۱	۳	۱۷	۶۰	۱۲۲	۱۷۳	۱۹۷	۱۶۷	۱۳۳	۶۸	۴۰	۱۷	۲		
۹۸ تا ۹۹	۶۱۸۱		۱	۱۵	۶۷	۱۱۳	۱۸۰	۲۰۸	۱۷۸	۱۱۹	۷۰	۲۸	۱۵	۳	۲	۱
۹۹ تا ۱۰۰	۶۱۳۴		۴	۲۱	۶۵	۱۰۴	۱۸۸	۲۰۹	۱۷۸	۱۱۵	۶۷	۳۳	۱۰	۵		۱
جمع	۶۲۰۸۲	۲	۲۹	۲۰۳	۵۷۲	۱۱۴۰	۱۷۱۲	۲۰۴۴	۱۸۱۸	۱۲۳۷	۷۵۱	۳۱۷	۱۲۰	۴۲	۱۰	۲

می‌توان آن را طبیعی دانست.

اگر به‌جای ۱۰۰۰۰۰ فاصله‌های ۲۰۰۰۰۰ را درنظربگیریم بینظمی خیلی کمتر می‌شود، به‌طوریکه اگرعددهای مجاور را دوبه‌دو جمع کنیم خواهیم داشت:

۱۲۳۱۵ ، ۱۲۴۱۰ ، ۱۲۴۴۸ ، ۱۲۴۸۲ ، ۱۲۴۲۷

و با جمع ۳ بد ۳ این عددها (فاصله‌های ۳۰۰۰۰۰):

(۶۱۳۱۴) ۱۸۵۹۱ ، ۱۸۶۷۱ ، ۱۸۶۸۶

عددهایی بدست می‌آید که دایماً به‌هم نزدیك می‌شوند. بالاخره از جمع ۴ به ۴ یا ۵ به ۵ داریم:

۲۴۸۵۸ ، ۲۴۹۰۹

۳۰۹۹۶ ، ۳۱۰۸۶

مادربخش هشتم (آخرین بخش) دوباره به‌تحقیق آماری برخواهیم گشت.

۱۲ مکرر. تحقیق دیگری دربارهٔ قضیهٔ تصادف. وقتی که این کتاب چاپ می‌شد[1] من نشریهٔ مجمع‌ریاضیدانان‌ایتالیایی را دریافت داشتم (سری III سال هفتم شمارهٔ ۲) که درآنجاآقای گیوسپ پالاما (M. Giuseppe Palama) آمار جالبی داده بود که به‌تحقیق قضیهٔ تصادف منجر می‌شد (صفحهٔ ۱۶۸ ـ ۱۷۱).

موضوع عبارتست از تعیین عددهای اولی که به‌شکل

۱) منظور چاپ متن فرانسه درسال ۱۹۵۸ است.

$1848x^2+y^2$ باشند وبین ۱۱۰۰۰۰۰۰ و ۱۱۱۰۰۰۰۰ واقع‌اند. اولر نشان داده بودکه اگر عدد صحیح n بعضی مقادیـر را اختیارکند، تمام عددهایی‌که تنها به‌یك طریق به‌صورت nx^2+y^2 نوشته شوند، عددهای اول هستند. او تعداد زیادی از این مقادیـر n را معین کرده است که بزرگترین آنها $1848=42\times44=43^2-1$ می‌باشد. همین تبصرهٔ اولراست که آمار آقای پالاما را ثابت می‌کند،وقتی‌که او۲۰۳عدداول[1] به‌صورت $1848x^2+y^2$ را بین عددهای 11×10^6 و $11\times10^6+10^5$ معین می‌کند.

همچنین در هر ۱۰۰ دسته ۱۰۰۰ عددی از فاصله‌ای که مساوی ۱۰۰۰۰۰ بود،به‌طور متوسط ۲/۰۳ عدد اول عدد به‌شکلی که در بالا ذکرکردیم وجود دارد. به‌سادگی می‌تـوان عدد N را که معرف تعداد دسته‌های ۱۰۰۰ عددی است و شامل ۰، ۱، ۲، ۳، ۴، ۵،. . . عدد اول می‌باشد معین کرد، به‌این ترتیب جدول زیررا خواهیم داشت:

	۰	۱	۲	۳	۴	۵	۶	۷	۸	جمع
N ...	۷	۲۵	۳۸	۲۳	۳	۴	۰	۰	۰	۱۰۰
..پواسون	۱۳/۵	۲۷/۱	۲۷/۱	۱۸	۹	۳/۶	۱/۲	۰/۳	۰/۱	۹۹/۹

۱) او همچنین صورتی از عددهای فرد غیر اول را که درین فاصله واقع است ذکرمی‌کند، ولی این صورت‌کامل نیست.

درسطرسوم، مقادیرنظری که درنتیجهٔ رابطهٔ پواسون بدست‌می‌آید یادداشت‌کرده‌ایم (حساب احتمالات در زندگی - یادداشت II)[1].

دیده می‌شودکه توزیع مربوطه، قانون تصادف را اثبات‌می‌کند: با همهٔ اینها نسبت به‌قانون تصادف تمایل بیشتری به‌یك نوع نظم در آن دیده می‌شود.

۱) این‌کتاب در مجموعهٔ «چه می‌دانم» به‌فارسی ترجمه شده است.

٣

همنهشتیها

Les congruences

۱۳ . همنهشتی. مطالعهٔ بعضی ازویژگیهای مهم عددهای اول، مستلزم شناسائی نظریهٔ همنهشتیهای درجه اول و درجه دوم است و ما در اینجا به‌طور اختصار ازآنها گفتگو می‌کنیم :

گویند دو عدد درست a و b نسبت به‌مدول p همنهشت هستند،وقتی‌که تفاضل $a-b$ بر p بخش‌پذیر باشد و آنرا چنین نمایش می‌دهند:

$$a \equiv b \pmod{p} \qquad (۱)$$

و می‌خوانند a همنهشت است با b (مدول p). عدد p یك عدد درست دلخواه است، ولی ما اغلب از حالتی‌گفتگو می‌کنیم‌که درآن، p عددی اول باشد. با وجود این ، حالتهایی وجود داردکه در مورد آنها، شرط اول بودن عدد p لازم نمی‌شود.

در جبر، تساویهای مربوط به‌معادله را می‌شناسیم: معادله عبارتست ازیك تساوی‌که درآن یك یا چند حرف را به‌عنوان مجهول نشان می‌دهند؛ تساوی برقرارنخواهد بود، مگراینکه به‌جای مجهولها، مقادیری را که ریشه‌های معادله‌گویند، قرار دهیم.

در نظریهٔ عددها، لازم نیست برای مواردی‌که همنهشتی شامل‌یك حرف،که نمایندهٔ مجهول است، ویا مواردی‌که شامل مجهول نیست‌دو

جمله مختلف به‌کار برده شود. وقتی که مجهول از درجهٔ اول یا دوم و غیره باشد، همنهشتی‌را درجه اول یا درجه دوم گویند، همچنین می‌توان تعداد مجهولها را هم ذکرکرد.

اگر r باقیماندهٔ تقسیم عدد صحیح a برعدد p باشد داریم:

$$a \equiv r \pmod{p} \qquad (۲)$$

و r را ماندهٔ (رزیدوی) a نسبت‌به‌مدول p گویند، این‌باقیمانده‌می‌تواند p مقدار مختلف‌را اختیارکند، یعنی: ۰ ; ۱ ; ۲ , ... و $p-1$.

اکنون $f(x)$ را چند جمله‌ای با ضریبهای درست فرض‌می‌کنیم:

$$f(x)=a_0x^n+a_1x^{n-1}+\dots+a_{n-1}x+a_n \qquad (۳)$$

به‌سادگی می‌توان نشان دادکه اگر همنهشتی:

$$x \equiv y \pmod{p} \qquad (۴)$$

برقرار باشد، همنهشتی زیرهم برقرار خواهد بود:

$$f(x) \equiv f(y) \pmod{p} \qquad (۵)$$

نتیجه می‌شودکه اگر همنهشتی:

$$f(x) \equiv 0 \pmod{p} \qquad (۶)$$

برای بعضی از مقادیر درست x برقرار باشد، برای تمام مقادیرy که در همنهشتی (۴) صدق می‌کنند، نیز برقرار خواهد بود. ریشه‌های x و y نباید به عنوان ریشه‌های مختلفی در نظرگرفته شوند و می‌توان آنها را به‌عنوان تمام ریشه‌های همنهشتی(۶) به‌حساب آورد، به‌شرطی‌که هریك ازp عدد ۰، ۱، ۲، . . . و $p-1$ را مورد آزمایش قراردهیم، تامعلوم شودکدام یك در همنهشتی صدق می‌کند.

ابتدا دربارهٔ همنهشتیهای درجه اول یك مجهولی صحبت می‌کنیم وقتی که مدول اول p را داشته باشند؛ این همنهشتی را چنین نمایش می‌دهند:

$$ax \equiv b \pmod{p} \qquad (۱)$$

b را مخالف صفر فرض می‌کنیم، یعنی b نسبت به مدول p با صفر همنهشت نیست. اگر b صفر باشد، باید ax بر p بخش‌پذیر باشد و اگر a صفر نباشد (یعنی بر p بخش‌پذیر نباشد) باید x بر p بخش‌پذیر باشد، یعنی نسبت به‌مدول p صفر باشد. همینقدر یادآوری می‌کنیم که در نظریهٔ همنهشتیها، تنها در حالت مدول اول است که می‌توان از این خاصیت صحبت کرد که حاصلضرب دو عامل نمی‌توانند صفر باشند، مگر وقتی‌که لااقل یکی از دو عامل صفر باشد.

اکنون حاصلضربهای ۱، ۲، . . . ، ۱ـــp را در a درنظر می‌گیریم، اگر x و y دو عدد مختلف از این عددها باشند و داشته باشیم:

$$ax \equiv ay \pmod{p}$$

خواهیم داشت:

$$a(x-y) \equiv ۰ \pmod{p}$$

و بالاخره:

$$x-y \equiv ۰ \pmod{p}$$

که‌با فرض ما، مبنی براینکه x و y کوچکتر ازp هستند، مخالف است. ۱ــp حاصلضرب :

$$a \text{ و } ۲a \text{ و } ۳a \text{ و } \ldots \text{ و } (p-۱)a$$

نسبت به‌مدول p با هم مخالف‌اند و این به‌معنای آنست‌که این مانده‌ها باهم مخالف‌اند و این مانده‌ها نمی‌توانند چیزی جز عددهای:

$$۱ \text{ و } ۲ \text{ و } ۳ \text{ و } ۴ \text{ و } \ldots\ldots \text{ و } p-۱$$

باشند، که به‌ترتیب معینی‌منظم شده‌اند. یکی ازاین عددها با b همنهشت است واین همان پدیده‌ای است‌که می‌توان‌گفت همنهشتی درجه اول(۱) تنها دارای یك جواب است، وقتی‌که a و b مخالف صفر باشند. اگر b به‌تنهایی صفر باشد، جواب هم صفر خواهد بود، اگر a به‌تنهایی صفر باشد همنهشتی جواب ندارد و اگر a و b هر دو صفر باشند، همنهشتی به‌یك اتحاد تبدیل‌می‌شود، یعنی به‌ازای همهٔ مقادیر x صادق خواهدبود.

۱۴. همنهشتیهای درجه دوم. اکنون به‌همنهشتیهای درجهٔ دوم می‌پردازیم، شکل عمومی یك همنهشتی درجه دوم چنین است:

$$ax^۲+bx+c\equiv ۰ \qquad (\mathrm{mod.}\ p) \qquad (۱)$$

فرض می‌کنیم‌که a صفرنباشد (یعنی بر p بخش‌پذیرنباشد)، زیرا در اینحالت حاصل‌ضرب $ax^۲$ نسبت به‌مدول p صفر می‌شود وهمنهشتی به‌درجه اول تبدیل می‌شود. می‌توانیم دوطرف همنهشتی را در۴aضرب کنیم (فرض می‌کنیم‌که p مساوی ۲نباشد یعنی عدد اول غیرزوج باشد، درحالتی‌که مدول p مساوی ۲ باشد، می‌توان مستقیماً و به‌سادگی آنرا مطالعه‌کرد):

$$۴a(ax^۲+bx+c)\equiv ۰ \quad (\mathrm{mod.}\ p) \qquad (۲)$$

این رابطه نمی‌تواند صحیح باشد، مگـراینکه رابطهٔ (۱) برقرار باشد، زیرا p عددی است اول و حاصلضرب دو عامل طـرف اول رابطهٔ

(۲) نمی‌تواند بر p بخش‌پذیر باشد، مگر اینکه یکی از آنها بر p بخش‌پذیر باشد و می‌دانیم که عامل ۴a هم بر p بخش‌پذیر نیست.

با عملهای سادهٔ معمولی جبری، همنهشتی (۲) به‌صورت زیر در می‌آید:

$$(2ax+b)^2 \equiv b^2-4ac \quad (\mathrm{mod.}\ p) \qquad (3)$$

یعنی:

$$y^2 \equiv r \quad (\mathrm{mod.}\ p) \qquad (4)$$

با فرض :

$$2ax+b \equiv y \quad (\mathrm{mod.}\ p) \qquad (5)$$

$$b^2-4ac \equiv r \quad (\mathrm{mod.}\ p) \qquad (6)$$

با توجه به‌رابطهٔ (۶) می‌توان r را مثبت و مقداری بین صفر و $p-1$ درنظرگرفت. به‌این‌ترتیب می‌توان یك یاچند ریشهٔ همنهشتی (۴) را پیداکرد. با قراردادن هریك از مقادیر y در همنهشتی (۵) مقداری برای x بدست می‌آید که یکی از جوابهای (۱) می‌باشد.

دوحالت درنظر می‌گیریم:

حالت اول ـ $b^2-4ac=r\equiv 0$

در اینجا همنهشتی (۴) تنها جواب $y\equiv 0$ را می‌دهد، زیرا y^2 نمی‌تواند برعدد اول p بخش‌پذیرباشد، مگراینکه y بر p بخش‌پذیرباشد. اکنون به‌همنهشتی (۵) بر می‌گردیم که در آن y صفر است، یعنی یك همنهشتی درجه اول خواهد بود و همانطـورکه می‌دانیم تنها یك ریشه

خـواهد داشت. این ریشه صفر نیست مگر اینکه b صفر باشد، ولی در حالتی‌که b صفر است چون r صفر و a مخالف صفر است، c هم صفر می‌شود و همنهشتی به $x^{۲} \equiv ۰$ تبدیل می‌شود.

حالت دوم ـ $b^{۲} - ۴ac$ نسبت به مـدول p صفر نیست، در همنهشتی (۴)، r صفر نیست. برای تجزیهٔ این همنهشتی، مانـده‌های (رزیدوها) مربعهای $p-۱$ عدد نخستین را محاسبه می‌کنیم:

$$۱^{۲} \text{ و } ۲^{۲} \text{ و } ۳^{۲} \text{ و } \ldots \text{ و } (p-۱)^{۲} \qquad (۷)$$

۱۵. مانده‌های مربعی (رزیدوکوادراتیک). این مانـده‌ها را مانده‌های‌مربعی برای مدول‌p می‌نامند. ازین مانده‌ها، دوعدد را چنان انتخاب می‌کنیم‌که نسبت به‌مدول p برابر باشند. اگـر این دو عدد را $m^{۲}$ و $n^{۲}$ بنامیم داریم:

$$m^{۲} - n^{۲} \equiv ۰ \qquad (\text{mod. } p) \qquad (۸)$$

و یا:

$$(m-n)(m+n) \equiv ۰ \quad (\text{mod}\cdot\ p) \qquad (۹)$$

اماچون m و n هر دواز p کوچکترند، $m-n$ نمی‌تواند بر p بخش‌پذیر باشد و خواهیم داشت:

$$m+n \equiv ۰ \qquad (\text{mod. } p) \qquad (۱۰)$$

مانده‌های (۷) دوبه‌دو نسبت به‌مدول p برابرند و داریم:

$$
(۱۱)\qquad \begin{cases} ۱^۲ \equiv (p-۱)^۲ \\ ۲^۲ \equiv (p-۲)^۲ \\ \cdots\cdots\cdots\cdots \\ \left(\frac{p-۱}{۲}\right)^۲ \equiv \left(\frac{p+۱}{۲}\right)^۲ \end{cases} \pmod{p}
$$

این همنهشتیها تنها شامل عـددهای درست‌اند، زیرا $p-۱$ و $p+۱$ عددهای زوجی هستند.

به‌این ترتیب نتیجه می‌شود که تعداد مانـده‌های مربعی مشخص برای مدول اول p برابر $\frac{p-۱}{۲}$ است، یعنی فقط نیمی از عددهای بین ۰ و $p-۱$ مانده‌های مربعی هستند. بقیه را غیر مانده گویند.

اگرمثلا عدد اول ۷ را درنظربگیریم، رشتهٔ (۷) به‌رشتهٔ زیرتبدیل خواهد شد:

(۱۲) ۱ و ۴ و ۲ و ۲ و۴ و۱

بنابراین برای ۷، عددهای ۱ و ۲ و ۴ مانده و بقیه، یعنی ۳ و۵ و ۶، غیر مانده هستند. همچنین برای ۱۱ ، رشتهٔ (۷) به‌صورت زیر در خواهد آمد:

(۱۳) ۱ و۴ و۹ و۵ و۳ و۳ و ۵ و۹ و۴ و۱

مانده‌ها عبارتند از ۱ و۳ و۴ و۵ و۹ و غیر مانده‌ها عبارتند از ۲ و ۶ و ۷ و ۸ و ۱۰.

برای عدد ۱۳، مانده‌ها عبارتند از ۱ و۴ و۹ و۳ و۱۰ و۱۲ وغیر مانده‌ها عبارتند از ۲ و ۵ و ۶ و ۷ و ۸ و ۱۱. می‌بینیم که دراین‌حالت

می‌توان گفت که ۱ — مانده است، در حالیکه برای ۷ و ۱۱ این وضع وجود نداشت. روشن خواهیم کرد که این وضع تابع یك قاعدهٔ عمومی است.

به‌این ترتیب، درحالیکه r یك ماندهٔ مربعی از p باشد، همنهشتی درجه دوم دوریشهٔ مختلف دارد و درحالتی که r غیرمانده است همنهشتی دارای جواب نیست.

روشن است که حاصلضرب دو مانده یك مانده است، زیرا اگر داشته باشیم:

$$x^{2} \equiv r \qquad (\mathrm{mod.}\ p)$$

$$y^{2} \equiv r' \qquad (\mathrm{mod.}\ p)$$

نتیجه می‌شود:

$$(xy)^{2} \equiv rr' \qquad (\mathrm{mod.}\ p)$$

یعنی rr' هم یك مانده است.

این تبصره وسیله‌ای بدست می‌دهد که بتوان مانده‌ها را جزء‌به‌جزء محاسبه کرد. اگر عدد p بزرگتر از ۳ باشد، مانده‌های ۱ و ۴ بلافاصله بدست می‌آیند. همچنین مجذور ۴ یعنی ۱۶. اگرمثلا مدول ۱۳ را داشته باشیم ماندهٔ ۳ را هم خواهیم داشت، با ضرب ۳ در ۴ عدد ۱۲ بدست می‌آیدکه معادل ۱ — است. حاصلضرب ۱ — در۳ یا۴ جوابهای۳ — و ۴ — را که معادل ۱۰ و ۹ می‌باشند (۹ از مجذور ۳ هم بدست می‌آید) و به‌این ترتیب ۶ مانده خواهیم داشت.

تبصره بسیار مهم زیر را ذکر می‌کنیم: اگر تمام عددهای بین

صفر تا $p-1$ را در r ضرب کنیم، می‌دانیم که به‌عنوان باقیماندهٔ این حاصلضربها‌نسبت به‌مدول p همان عددهای‌از صفرتا $p-1$، منتهی‌بار دیف دیگری، بدست خواهد آمد. بنابراین دوباره تمام مانده‌ها و غیرمانده‌ها بدست خواهد آمد. ولی‌مانده‌ها ازضرب r درمانده‌ها وغیرمانده‌ها هم از ضرب‌درغیرمانده‌ها بدست می‌آید. بنابراین حاصل ضرب یك مانده در یك غیرمانده برابر با یك غیر مانده است.

با تحقیق مشابه، یعنی ضرب یك غیرمانده در $p-1$ عدد واقع بین ۰ و $p-1$ دیده می‌شود که از ضرب یك غیرمانده در یك مانده، یك مانده بدست می‌آید.

این‌نتیجه‌ها اجازه می‌دهندکه روش ساده ومشخصی انتخاب کنیم تا بتوانیم نشان دهیم که آیا عدد a ماندهٔ مربعی عدد اول p هست یا نه. برای این منظور علامت‌گذاری لژاندر را به‌کار می‌برند که به‌صورت:

$$\left(\frac{a}{p}\right)$$

می‌باشد. در حالیکه a یك مانده است به‌صورت:

$$\left(\frac{a}{p}\right)=1$$

و در حالیکه غیرمانده است به‌صورت:

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

نشان می‌دهند.

اکنون ۴ رابطهٔ بین حاصلضربهای دو مانده و دو غیرمانده را

می‌توان در رابطهٔ زیر خلاصه کرد:

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

این رابطه نشان می‌دهد که ارزش علامت لژاندر برای حاصلضرب ab برابر است با حاصلضرب علامتهای لژاندر از این عددها.

ما بزودی اهمیت علامتگذاری لژاندر را ذکر خواهیم کرد؛ ولی قبلا باید چند کلمه‌ای دربارهٔ مانده‌های مربعی، وقتی‌که مدول عددی غیراول است، صحبت کنیم.

۶۱. حالت مدول غیراول. قبلا حالتی را در نظر می‌گیریم که مدول برابر با توان p^n از یك عدد اول p باشد. واضح است که همنهشتی:

$$x^2 \equiv a \qquad (\text{mod. } p^n) \qquad (1)$$

نمی‌تواند جواب داشته باشد مگر وقتیکه a ماندهٔ مربعی p باشد، زیرا اگر تفاضل x^2-a بر p بخش‌پذیرنباشد، بر p^n هم بخش‌پذیرنخواهد بود. بنابراین فرض می‌کنیم‌که a ماندهٔ مربعی p باشد. عددی مانند b وجود دارد به‌نحوی‌که داشته باشیم:

$$b^2 \equiv a \qquad (\text{mod. } p) \qquad (2)$$

رابطهٔ (۲) با تبدیل b به $-b$ نیز درست است. اگرعددی مانند y چنان باشدکه داشته باشیم:

$$y^2 \equiv a \qquad (\text{mod. } p^2) \qquad (3)$$

روشن است که الزاماً خواهیم داشت:

$$y \equiv \pm b \qquad (\text{mod}.p) \qquad (۴)$$

یعنی با انتخاب علامت + داریم:

$$y = b + pz \qquad (۵)$$

از اینجا نتیجه می‌شود:

$$y^{۲} = b^{۲} + ۲bpz + p^{۲}z^{۲} \equiv b^{۲} + ۲bpz \quad (\text{mod}.p^{۲}) \quad (۶)$$

بنابراین همنهشتی (۲) چنین می‌شود:

$$۲bpz \equiv a - b^{۲} \quad (\text{mod}.p^{۲}) \quad (۷)$$

که هم‌ارز است با همنهشتی زیر:

$$۲bz \equiv a - b^{۲} \quad (\text{mod}.p) \quad (۸)$$

این همنهشتی (که در آن $۲b$ نسبت به p اول است) تنها یك جواب خواهد داشت و همچنین اگر b را به $-b$ تبدیل کنیم جواب دیگری هم خواهیم داشت.

با همین روش می‌توان از مدول $p^{۲}$ به‌مدول $p^{۳}$ و . . . بالاخره به‌مدول p^{n} رسید. به‌این ترتیب برای همنهشتی (۲) به‌ازای هرمقدار دلخواه n دوجواب پیدا می‌شود به‌شرطی‌که a ماندهٔ مربعی p باشد.

اکنون به‌حالتی‌می‌پردازیم که‌مدول n قابل تجزیه به‌عاملهای‌اول متمایز باشد؛ برای سهولت کارفرض می‌کنیم که تعداد عاملهای اول‌عدد m برابر ۳ باشد؛ عین استدلالی‌را که دراین مورد می‌آوریم برای‌حالتی هم‌که تعداد عاملها غیرمشخص باشد، می‌توان به‌کار برد.

به‌این ترتیب فرض می‌کنیم:

$$m = p^{\alpha} q^{\beta} r^{\gamma} \qquad (۹)$$

p و q و r عددهای اول و α و β و γ عددهایی درست هستند. اکنون همنهشتی زیر را درنظر می‌گیریم:

$$x^2 \equiv a \quad (\mathrm{mod.}\ m) \qquad (۱۰)$$

روشن است‌که هرجواب همنهشتی (۱۰) باید در همنهشتیهای زیر صدق کند:

$$x^2 \equiv a \quad (\mathrm{mod.}\, p^{\alpha}) \qquad (۱۱)$$

$$x^2 \equiv a \quad (\mathrm{mod.}\, q^{\beta}) \qquad (۱۲)$$

$$x^2 \equiv a \quad (\mathrm{mod.}\, r^{\gamma}) \qquad (۱۳)$$

زیرا برای اینکه عدد $x^2 - a$ بر حاصلضرب ۳ عامل اول بخش‌پذیر باشد، باید برهریك ازآنها بخش‌پذیر باشد.

برای اینکه هریك از همنهشتیهای (۱۱)، (۱۲) و (۱۳) دارای جواب باشند، لازم وکافی است‌که a ماندهٔ مربعی نسبت به‌عددهای اول p و q و r باشد، وقتیکه این شرط برقرار باشد، هریك ازهمنهشتیهای (۱۱) ، (۱۲) و (۱۳) دو ریشه خواهند داشت. یکی از این ریشه‌ها را برای هریك از معادله‌ها انتخاب‌کرده وآنها را به‌ترتیب به‌وسیلهٔ x، y و z نشان می‌دهیم. روشن است‌که اگر عددی مانند X چنان باشدکه‌داشته باشیم:

$$(۱۴)\qquad \begin{cases} X \equiv x & (\mathrm{mod}.\, p^{\alpha}) \\ X \equiv y & (\mathrm{mod}.\, q^{\beta}) \\ X \equiv z & (\mathrm{mod}.\, r^{\gamma}) \end{cases}$$

عدد X در ۳ همنهشتی (۱۱) ، (۱۲) و (۲۳) و در نتیجه در همنهشتی (۱۰) صدق خواهد کرد.

به‌جای دستگاه (۱۴) سه دستگاه زیررا موردتوجه قرارمی‌دهیم:

$$(۱۵)\qquad \begin{cases} X_1 \equiv 1 & (\mathrm{mod}.\, p^{\alpha}) \\ X_1 \equiv 0 & (\mathrm{mod}.\, q^{\beta}) \\ X_1 \equiv 0 & (\mathrm{mod}.\, r^{\gamma}) \end{cases}$$

$$(۱۶)\qquad \begin{cases} X_2 \equiv 0 & (\mathrm{mod}.\, p^{\alpha}) \\ X_2 \equiv 1 & (\mathrm{mod}.\, q^{\beta}) \\ X_2 \equiv 0 & (\mathrm{mod}.\, r^{\gamma}) \end{cases}$$

$$(۱۷)\qquad \begin{cases} X_۳\equiv ۰ & (\text{mod.}\,p^{\alpha}) \\ X_۲\equiv ۰ & (\text{mod.}\,q^{\beta}) \\ X_۳\equiv ۱ & (\text{mod.}\,r^{\gamma}) \end{cases}$$

روشن است که عدد X که از رابطهٔ زیر بدست می‌آید:

$$X = xX_۱ + yX_۲ + zX_۳ \qquad (۱۸)$$

در همنهشتیهای (۱۴) صدق می‌کنند. در این رابطه می‌توان هریك از حرفهای x و y و z را به $-x$ ، $-y$ و $-z$ تبدیل کرد. اگر تمام حالتهای ممکنه $+$ و $-$ را درنظربگیریم، ۸ مقدارمتمایزبدست‌خواهد آمدکه می‌توان‌آنها را به‌صورت رابطهٔ جبری زیرنوشت:

$$x = \pm xX_۱ \pm yX_۲ \pm zX_۳ \qquad (\text{۱۸ مکرر})$$

به‌این ترتیب تنهامی‌توان دستگاه همنهشتیهای (۱۵) را به‌نتیجه رساند، زیرا دستگاههای (۱۶) و (۱۷) کاملا شبیه‌آن هستند.

عدد $X_۱$ باید بر عددهای متباین q^{β} و r^{γ} بخش‌پذیر باشد و بنابراین می‌توان نوشت:

$$X_۱ = \lambda\, q^{\beta} r^{\gamma} \qquad (۱۹)$$

که درآن λ عددی است اول، به‌این ترتیب تنها همنهشتی زیر برای حل باقی می‌ماند:

$$\lambda q^{\beta} r^{\gamma} \equiv ۱ \qquad (\text{mod.}\,p^{\alpha}) \qquad (۲۰)$$

که همنهشتی از درجه اول است و در حالتی که λ نسبت به p^α اول است، تنها دارای یك جواب‌مشخص می‌باشد. استدلال شبیه‌حالتی‌است که مدول، عددی اول‌بود. $p^\alpha - ۱$ عدد وجود داردکه‌کوچکتر از p^α بوده و بر p^α بخش‌پذیر نیستند، اگراین عددها را درعامل غیر مشخصی مانند a که نسبت به p^α اول است، ضرب‌کنیم، بازهم $p^\alpha - ۱$ عدد بدست می‌آوریم که بر p^α بخش‌پذیر نیستند. همچنین تفاضل هردو عدد غیر مشخص ازآنهاهم بر p^α بخش‌پذیرنیست. بنابراین مانده‌های این‌عددها، نسبت به p^α با ترتیب غیرمشخصی همان $p^\alpha - ۱$ عدد نخستین هستند که عدد ۱ | طرف‌دوم همنهشتی(۲۰) | هم بین‌آنهاست. ازاین‌همنهشتی جواب λ بدست می‌آید و در نتیجه، رابطهٔ (۱۹) مقدار $X_۱$ را بدست خواهد داد. با ترتیب مشابهی $X_۲$ و $X_۳$ بدست می‌آیند و رابطهٔ (۱۸ مکرر) ۸ جواب همنهشتی (۱۰) را معین خواهدکرد.

نتیجه این بحث اینست که برای اینکه همنهشتی (۱۰) دارای جواب باشد، لازم است‌که داشته باشیم:

$$\left(\frac{a}{p}\right)=+۱ \text{ و } \left(\frac{b}{p}\right)=+۱ \text{ و } \left(\frac{c}{p}\right)=+۱ \qquad (۲۱)$$

وقتی‌که این شرطها برقرار باشند، تعداد ریشه‌ها $۸ = ۲^۳$ خواهد بود.

۱۷. قانون تقابل (réciprocité). لژاندر ضمن مشخص کردن نتیجه‌هایی را که اولر گرفته بود، قانون مهمی کشف کرد، که مربوط به‌مانده‌های مربعی است و اسم‌آنرا هم قانون تقابل‌گذاشت. این قانون را ذکرکنیم:

دو عدد اول p و q را در نظر می‌گیریم، اگر لااقل یکی از آنها

به‌صورت $۴n+۱$ باشد داریم:

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right) \qquad (۱)$$

و اگر هر دو عدد به‌صورت $۴n+۳$ باشند، داریم:

$$\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right) \qquad (۲)$$

دو رابطهٔ مختلف (۱) و (۲) را می‌توان به‌وسیلهٔ رابطهٔ واحد زیرنشان داد:

$$\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-۱)^{\frac{p-۱}{۲}\times\frac{q-۱}{۲}} \qquad (۳)$$

درحقیقت، اگر $p=۴n+۱$ باشد $\frac{p-۱}{۲}=۲n$ زوج می‌شود و اگر $p=۴n+۳$ باشد. $\frac{p-۱}{۲}=۲n+۱$ فرد می‌شود، یعنی حاصلضرب $\frac{p-۱}{۲}\times\frac{q-۱}{۲}$ زوج است به‌شرطی که لااقل یکی از دوعدد p و q به صورت $۴n+۳$ نباشد.

این قانـون تقابـل، که مـا اثبات آنـرا نمی‌آوریم، بسیاری از محاسبه‌های لازم مربوط به‌معین‌کردن‌خصوصیت مربعی یك عددمفروض نسبت به‌یك عدد خیلی بزرگ را به‌قدرکافی ساده می‌کند.

فرض‌کنیدکه مثلا می‌خواهیم بدانیم که آیا ۷، ماندهٔ مربعی عدد ۹۷ هست یا نه؟ عدد ۹۷ به‌صورت $۴n+۱$ می‌باشد و بنابـراین طبق

قانون تقابل داریم:

$$\left(\frac{۷}{۹۷}\right)=\left(\frac{۹۷}{۷}\right)$$

اما ۹۷ نسبت به‌مدول ۷ با عدد ۶ همنهشت است و بنابراین داریم:

$$\left(\frac{۹۷}{۷}\right)=\left(\frac{۶}{۷}\right)=-۱$$

و بنابراین نتیجه می‌شود که ۷ ماندهٔ مربعی عدد ۹۷ نیست.

درحالتی که بخواهیم این قانون را در مورد دو عدد اول خیلی بزرگ بیان‌کنیم به‌علامت کمکی مثل $\left(\frac{۶}{۷}\right)$ هدایت می‌شویم که در آن هردو جمله، عددهایی اول نیستند و اگراین‌جمله‌ها بزرگ باشند، بدون دخالت دادن نتیجه‌هایی که مربوط به‌مانده‌های مربعی نسبت به‌عددهای غیراول و به‌خصوص مربوط به‌خواص مربعی ۲ می‌باشد، نمی‌توان کاررا به‌نتیجه رساند. ما نمی‌توانیم در اینجا از این نتیجه‌ها نام ببریم و در بخش‌آینده، بعد از اثبات قضیهٔ فرما ، به‌آن برخواهیم‌گشت.

۴

قضیهٔ فرما و قضیهٔ ویلسون

۱۸. قضیهٔ فرما. فرما، که در سالهای بین ۱۶۰۱ تا ۱۶۶۵ زندگی میکرد وبا پاسکال در پایه‌گذاری حساب احتمالات دست‌داشت، پیشرفتهای قابل‌توجهی به‌حساب دیفرانسیل ونظریهٔ عددها داد. همچنین قضیه‌ای بنام «آخرین قضیهٔ فرما» از او باقی مانده است‌که تا امروزهم به‌طورکامل ثابت نشده است[۱].

قضیهٔ دیگری از فرما که خیلی هم مشهور است وما می‌خواهیم در اینجا،آنرا ثابت کنیم یکی از خاصیتهای اساسی مربوط به‌عددهای اول را بیان می‌کند.

قضیه . اگر p عدد اول غیر مشخصی باشد و a عددی درست و بخش ناپذیر بر p ، تفاضل $a^{p-1}-1$ بر p بخش‌پذیر خواهد بود.

این قضیه را به‌این طریق هم می‌توان بیان کردکه اگر a عدد

---

۱. این قضیه چنین است: اگر n عددی درست و بزرگتر از ۲ باشدنمی‌توان ۳عدد درست a، b و c را چنان پیداکرد‌که در رابطهٔ $a^n+b^n=c^n$ صدق کنند. این قضیه در مورد تعداد خیلی زیادی از عددها ثابت شده است، ولی هنوز حالت‌کلی‌آن به‌اثبات نرسیده است.

دلخواه درستی باشد، $a^p - a$ همیشه بر p بخش‌پذیر است.

دستگاه کاملی از باقیمانده‌ها نسبت به‌مدول p تشکیل می‌دهیم:

$$۱، ۲، ۳، \ldots، p-۱ \qquad (۱)$$

حاصلضرب جمله‌های این رشته را در عدد a (که نسبت به p اول‌است) بدست می‌آوریم:

$$a، ۲a، ۳a، \ldots، (p-۱)a \qquad (۲)$$

اختلاف هردو جملهٔ دلخواه از رشتهٔ (۲) نمی‌تواند بر p بخش‌پذیر باشد. در واقع، اگر m و n دو عددکوچکتر از p باشند، اختلاف:

$$ma - na = (m - n)a$$

برp بخش‌پذیرنیست، زیرا نه a ونه $m - n$، هیچکدام برp بخش‌پذیر نیستند. اگرجمله‌های رشتهٔ (۲) را برp تقسیم‌کنیم، همان باقیمانده‌های رشتهٔ (۱)را، منتهی با ردیف دیگری بدست خواهیم‌آورد، یعنی‌می‌توان گفت‌که جمله‌های این دو رشته مشترك و متناظـرند. به‌این ترتیب هردو جملهٔ متناظر از این دو رشته نسبت به‌مدول p همنهشت هستند.

اگر مثلا $p=۷$ و $a=۱۰$ باشد، رشته‌های (۱) و(۲) به‌صورت زیر در می‌آید:

$$۱، ۲، ۳، ۴، ۵، ۶ \qquad (۱)'$$

$$۱۰، ۲۰، ۳۰، ۴۰، ۵۰، ۶۰ \qquad (۲)'$$

و باقیماندهٔ تقسیم عددهای رشتهٔ $'$(۲) بر۷ خواهد شد:

$$۳، ۶، ۲، ۵، ۱، ۴^{۱} \qquad (۳)'$$

یعنی همان عددهای رشتهٔ $'(۱)$ ، منتهی با ردیفی غیر ازآن.

ازآنجاکه می‌توان جمله‌های دو یا چند همنهشتی را نسبت‌به‌یک مدول‌درهم ضرب‌کرد، حاصلضرب جمله‌های رشتهٔ (۲) نسبت به‌مدول p با حاصلضرب جمله‌های رشتهٔ (۱) همنهشت خواهد بود، یعنی می‌توان نوشت:

$$a \times ۲a \times ۳a \times \ldots \times (p-۱)a \equiv ۱ \times ۲ \times ۳ \times \ldots \times (p-۱) \pmod{p}$$

ولی می‌توان دو طرف این همنهشتی را برحاصلضرب $۱ \times ۲ \times ۳ \times \ldots \times (p-۱)$ که نسبت به p اول است، تقسیم کرد، در نتیجه خواهیم داشت:

$$a^{p-۱} \equiv ۱ \pmod{p}$$

و این به‌معنای آنست‌که قضیه ثابت شده است.

اگر همین استدلال را در مورد رشته‌های $'(۱)$ و $'(۲)$ و $'(۳)$ انجام دهیم نتیجه می‌گیریم‌که حاصلضرب جمله‌های رشتهٔ $'(۲)$ نسبت به‌مدول ۷، با حاصلضرب جمله‌های رشتهٔ $'(۳)$ (که مساوی‌حاصلضرب جمله‌های رشته $'(۱)$ است) همنهشت است:

$$۶! \times ۱۰^{۶} \equiv ۶! \pmod{۷}$$

یعنی:

$$۱۰^{۶} \equiv ۱ \pmod{۷}$$

و عدد ۹۹۹۹۹۹ هم واقعاً بر ۷ بخش‌پذیر است. خارج قسمت این عدد بر ۷ برابر ۱۴۲۸۵۷ است، که همان رقمهای دورهٔ تناوب کسر اعشاری است که از تقسیم ۱ بر ۷ بدست می‌آید.

این مطلب، روش دیگری را برای اثبات قضیهٔ فرما به‌ما تلقین می‌کند:

p عددی است اول ، کسر $\frac{۱}{p}$ را به‌کسر اعشاری تبدیل می‌کنیم، می‌دانیم که در این حالت یك کسر اعشاری متناوب بدست می‌آوریم و تعداد رقمهای دورهٔ تناوب نمی‌تواند از $p-۱$ بیشتر شود . کسرهای $\frac{۲}{p}$ و $\frac{۳}{p}$ و غیره را درنظر می‌گیریم که می‌توان بسط آنها را به کسر اعشاری از ضرب بسط اعشاری $\frac{۱}{p}$ در ۲ و ۳ و غیره بدست‌آورد. تعداد رقمهای دورهٔ تناوب این بسطها، همه مساوی باهم خواهند بود.

چون مقسوم علیه p است، تعداد رقمهای دورهٔ تناوب الزاماً مقسوم علیهی از $p-۱$ خواهد بود.

مثلا داریم:

$$\frac{۱}{۷}=۰/۱۴۲۸۵۷\ ۱۴۲۸۵۷\ldots$$

$$\frac{۱}{۱۱}=۰/۰۹۰۹۰۹۰۹\ldots \qquad \frac{۶}{۱۱}=۰/۵۴۵۴۵۴\ldots$$

$$\frac{۲}{۱۱}=۰/۱۸۱۸۱۸۱۸\ldots \qquad \frac{۷}{۱۱}=۰/۶۳۶۳۶۳\ldots$$

$$\frac{۳}{۱۱}=۰/۲۷۲۷۲۷۲۷\ldots \qquad \frac{۸}{۱۱}=۰/۷۲۷۲۷۲\ldots$$

$$\frac{۹}{۱۱} = ۰/۸۱۸۱۸۱\ldots \qquad \frac{۴}{۱۱} = ۰/۳۶۳۶۳۶\ldots$$

$$\frac{۱۰}{۱۱} = ۰/۹۰۹۰۹۰\ldots \qquad \frac{۵}{۱۱} = ۰/۴۵۴۵۴۵\ldots$$

و می‌توان نتیجه گرفت:

$$\frac{۱}{۷} = \frac{۱۴۲۸۵۷}{۹۹۹۹۹۹}$$

$$\frac{۱}{۱۱} = \frac{۹}{۹۹} = \frac{۹۰۹۰۹۰۹۰۹}{۹۹۹۹۹۹۹۹۹۹}$$

طوری‌که $۱۰^۶ - ۱$ و $۱۰^{۱۰} - ۱$ به‌ترتیب بر ۷ و ۱۱ بخش‌پذیرند.

استدلالی را که درمورد عدد $a = ۱۰$ انجام دادیم می‌توان‌دربارهٔ عدد غیرمشخص a که با p اول است نیزصحیح دانست، زیرا کافی‌است که به‌جای دستگاه عددهای با مبنای ۱۰ ، دستگاه عددشماری با مبنای a را به‌کاربریم، وقتی‌که p مقسوم‌علیهی از a نباشد برای‌کسر $\frac{۱}{p}$ یک کسر متناوب بدست خواهد آمد.

قضیهٔ فرما از این جهت مهم است‌که خاصیت مشخصی ازعددهای اول را بیان می‌کند. در حقیقت، اگرعدد p اول نباشد لااقل دارای یك مقسوم علیه اول q است‌که ازpکوچکتر است. در این صورت اگر عدد زیر را درنظر بگیریم:

$$q^{p-۱} - ۱$$

این عدد نمی‌تواند بر p بخش‌پذیر باشد ، زیرا در اینصورت بر q، هم، که مقسوم‌علیهی از p است، باید بخش‌پذیر باشد واین غیر ممکن

است زیرا باقیماندهٔ این عدد بر q مساوی $q-1$ است.

ولی اگردرحالت اول بودن p بیشتردقت‌کنیم روشن می‌شود که مقادیری برای a وجود داردکه به‌ازای آنها a^{p-1} کوچکترین توانی از a است‌که $a^{p-1}-1$ بر p بخش‌پذیر است، درحالیکه برای سایر مقادیر a عددی مانند r کوچکتر از $p-1$ (و مقسوم علیهی از $p-1$) وجود دارد به‌طوریکه a^r-1 بر p بخش‌پذیر است.

از طرف دیگر، اگر a عددی اول نباشد، می‌توان مقداری برای a پیدا کردکه به‌ازای آن $a^{p-1}-1$ بر p بخش‌پذیر باشد، ولی این‌وضع برای تمام مقادیر a وجود ندارد. مثلا اگر $p=15$ باشد، روشن است که $4^2=16$ نسبت به‌مدول ۱۵ با ۱ همنهشت است و بنابراین 4^{14} نسبت به‌مدول ۱۵ همنهشت با واحد است، یعنی $4^{15-1}-1$ بر ۱۵ بخش‌پذیراست، اکنون قضیهٔ فرما را درمورد یك مدول غیراول با دقت مورد بررسی قرار می‌دهیم.

۱۹. حالت مدول غیر اول. m را عدد دلخواه غیر اولی فرض کنید. ابتدا تعداد عددهای کوچکتر از m را که نسبت به m اول هستند معین می‌کنیم. این تعداد را معمولا با علاعت $\varphi(m)$ نمایش می‌دهند. فرض‌می‌کنیم‌که a و b و c و d عاملهای اول تعیین‌کنندهٔ‌عدد m باشند. خواهیم داشت:

$$m=a^{\alpha}b^{\beta}c^{\gamma}d^{\delta} \qquad (1)$$

که درآن توانهای α و β و γ و δ حداقل برابر با واحد هستند.

تعداد عددهای‌کوچکتر ویامساوی m که بر a بخش‌پذیرند، بدون

تردید برابر با $\frac{m}{a}$ است، همچنین تعداد عددهای بخش‌پذیر بر b و c و d به‌ترتیب برابر $\frac{m}{b}$ و $\frac{m}{c}$ و $\frac{m}{d}$ می‌باشد. مجموع زیر را تشکیل می‌دهیم:

$$D_1=\frac{m}{a}+\frac{m}{b}+\frac{m}{c}+\frac{m}{d} \qquad (2)$$

عدد D_1 معرف مجموع عددهای کوچکتر و یا مساوی m است که بر a یا b یا c و یا d بخش‌پذیرند. ولی در این مجموع، عددهایی که هم بر a و هم بر b بخش‌پذیرند و یا عددهایی که در عین‌حال بر b و c بخش‌پذیرند و غیره دوبار تکرار شده است. بنابراین، باید مجموع زیر را هم محاسبه کرد:

$$D_2=\frac{m}{ab}+\frac{m}{ac}+\frac{m}{ad}+\frac{m}{bc}+\frac{m}{bd}+\frac{m}{cd} \qquad (3)$$

D_2 نمایندهٔ مجموع عددهایی است که بر ۶ حاصلضرب ab، ac، ad، bc، bd و cd بخش‌پذیرند. اما عددهایی که بریکی از حاصلضربهای abc، abd، acd و bcd بخش‌پذیرند، چند مرتبه در D_1 و D_2 به‌حساب آمده‌اند، از اینجا به‌محاسبهٔ مجموع زیر راهنمائی می‌شویم:

$$D_3=\frac{m}{abc}+\frac{m}{abd}+\frac{m}{acd}+\frac{m}{bcd} \qquad (4)$$

و بالاخره:

$$D_4=\frac{m}{abcd} \qquad (5)$$

حالا نتیجه خواهیم گرفت که:

$$\varphi(m) = m - D_1 + D_2 - D_3 + D_4 \qquad (۶)$$

در حقیقت، اگر عـددی کـوچکتر یا مساوی m، تنها بریکی از عددهای a، b، c و d بخش‌پذیر باشد، در D_1 به‌حساب‌آمده است و در D_2، D_3 و D_4 به‌حساب نیامده است. اگر این عدد بردو عامل و مثلا بر a و b بخش‌پذیر باشد، در D_1 دوبار و در D_2 یکبار به‌حساب آمده است و بنابراین، تنها یکبار آنرا حذف کرده‌ایم (چون در $\varphi(m)$ علامت D_1 منفی و علامت D_2 مثبت است). همچنین عددی‌که بر سه عامل و مثلا بر a، b و c بخش‌پذیر است، سه‌بار در D_1، سه بار در D_2 ویکبار در D_3 به‌حساب‌آمده است و در نتیجه، تنها یکبار، آنرا حذف کرده‌ایم و بالاخره عددی که برحاصلضرب abcd بخش‌پذیر است، ۴ مـرتبه در D_1، ۶مرتبه در D_2، ۴مرتبه در D_3 وتنها یکمرتبه در D_4 به‌حساب‌آمده است؛ به‌همین جهت به‌اندازه ۸=۴+۴ مرتبه‌آنـرا حـذف و دوباره ۷=۱+۶ مرتبه آنرا اضافه کرده‌ایم و درنتیجه تنها یکبار حذف شده است.

به‌این ترتیب تعداد عددهای کـوچکتر یا مساوی m را، که‌نسبت به m اول نیستند، ازآن بیرون رفته‌ایم وآنچه‌باقی می‌ماند همان$\varphi(m)$ است. $\varphi(m)$ را می‌توان به‌وسیلهٔ رابطهٔ (۶) نشان داد و یا با قراردادن مقادیر D_1،D_2، D_3، D_4 رابطهٔ زیررا بدست‌آورد:

$$\varphi(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\left(1-\frac{1}{d}\right) \qquad (۷)$$

ما در اینجا تنها حالتی را که m به‌چهارعامل تجزیه می‌شد ذکر کردیم. خواننده می‌تواند به‌سادگی وبا استفاده از خـاصیتهای معمولی

ضریبهای دو جمله‌ای، آنرا در حالت‌کلی خود نیزثابت‌کند.

حالا می‌توانیم قضیهٔ فرمارا برای یك عدد مرکب m نشان‌دهیم؛ کافی است‌که $\varphi(m)$ عددکوچکتر از m را که نسبت به m اول‌هستند، مورد توجه قرار دهیم، این عددها را چنین می‌نامیم:

$$a_1, a_2, \ldots, a_{\varphi(m)} \qquad (۸)$$

اگر x یکی از این عددها باشد، حاصلضربهای:

$$a_1x, \ a_2x, \ldots, a_{\varphi(m)}x \qquad (۹)$$

بر m بخش‌پذیر نیستند و اختلاف هردو عدد دلخواه ازآنهاهم نمی‌تواند بر m بخش‌پذیر باشد. بنابراین، این عددها نسبت به‌مــدول m مخالف یکدیگرند و به‌ترتیب‌نسبت به $\varphi(m)$ عــدد رشتهٔ (۸) همنهشت هستند؛ در نتیجه داریم:

$$a_1a_2\ldots a_{\varphi(m)} \equiv a_1a_2 \ldots a_{\varphi(m)}x^{\varphi(m)} \pmod{m} \qquad (۱۰)$$

اگر دو طرف رابطه را برحاصلضرب $a_1a_2 \ldots a_{\varphi(m)}$ که از عاملهای اول تشکیل‌شده است (ونسبت به m هم اول است) تقسیم‌کنیم، داریم:

$$x^{\varphi(m)} \equiv 1 \pmod{m} \qquad (۱۱)$$

و این همان قضیهٔ فرما درحالت عمومی خود می‌باشد. درحقیقت، قضیهٔ فرما حالت خاصی ازاین‌رابطه است وقتی‌که m برابربا عدد اول p باشد که دراینصورت $\varphi(m)=p-1$ خواهد بود.

این قضیه، نسبت به‌قضیهٔ فرما اهمیت‌کمتری دارد و ما دربخش

هفتم که اختصاص به‌مقسوم‌علیه‌هـای درست چند جمله‌ایها دارد، به‌آن برخواهیم گشت.

۲۰. قضیه‌هایی دربارهٔ تابع $\varphi(m)$. حالامی‌خواهیم قضیهٔ‌مهمی دربارهٔ تابع $\varphi(m)$ ذکر کنیم. این‌قضیه چنین است: اگرمقسوم علیه‌های مختلف عدد m را که شامل m و واحـد هم هستند، به d نشان دهیم داریم:

$$m = \Sigma\varphi(d) \qquad (۱)$$

یادآوری می‌کنیم که $\varphi(m)$ معرف تعداد عددهایی است‌که نسبت به m اول‌بوده وبزرگترازm نیستند. ضمناً قرارمی‌گذاریم که $\varphi(۱)=۱$ باشد (۱ و ۱ دارای بزرگترین مقسوم علیه مشترك مساوی واحد هستند و آنها را باید مثل دو عددی‌که نسبت به‌هم اول هستند به‌حساب‌آورد، در حالیکه دو عدد غیر واحد مساوی m و m نسبت به‌هم اول نخواهند بود).

برای‌کوتاه‌کردن مطلب، فرض می‌کنیم‌که m تنها دارای ۳عامل مختلف اول a، b و c باشد یعنی داشته باشیم:

$$m = a^{\alpha} b^{\beta} c^{\gamma} \qquad (۲)$$

و

$$\varphi(m) = m\left(۱-\frac{۱}{a}\right)\left(۱-\frac{۱}{b}\right)\left(۱-\frac{۱}{c}\right) \qquad (۳)$$

داریم :

$$(۴)\quad \begin{cases} \varphi\left(\frac{m}{a}\right)=\frac{۱}{a}\varphi(m) \\ \varphi\left(\frac{m}{a^۲}\right)=\frac{۱}{a^۲}\varphi(m) \\ \cdots\cdots \\ \varphi\left(\frac{m}{a^{\alpha-۱}}\right)=\frac{۱}{a^{\alpha-۱}}\varphi(m) \\ \varphi\left(\frac{m}{a^{\alpha}}\right)=\frac{۱}{a^{\alpha}}\varphi(m)\frac{۱}{۱-\frac{۱}{a}} \end{cases}$$

در واقع ، عامل a ، مثل عاملهای b و c در $\frac{m}{a}$ و . . . و $\frac{m}{a^{\alpha-۱}}$ وجود دارد ولی در $\frac{m}{a^{\alpha}}$ وجود ندارد.

معادلهٔ (۳) و معادله‌های (۴) را عضوبه‌عضو باهم جمع‌می‌کنیم، اگر تساوی روشن زیر را درنظر بگیریم:

$$۱+\frac{۱}{a}+\frac{۱}{a^۲}+\ldots+\frac{۱}{a^{\alpha-۱}}=\frac{۱-\frac{۱}{a^{\alpha}}}{۱-\frac{۱}{a}}$$

خواهیم داشت:

$$\psi(m)=\varphi(m)+\varphi\left(\frac{m}{a}\right)+\ldots\ldots+\varphi\left(\frac{m}{a^{\alpha}}\right)=$$

$$=m\left(۱-\frac{۱}{b}\right)\left(۱-\frac{۱}{c}\right) \qquad (۶)$$

و به‌همین ترتیب می‌توان بدست‌آورد:

$$\Theta(m)=\psi(m)+\psi\left(\frac{m}{b}\right)+\ \ldots\ +\psi\left(\frac{m}{b^{\beta}}\right)=$$

$$=m\left(۱-\frac{۱}{c}\right) \qquad (۷)$$

و بالاخره:

$$\Theta(m)+\Theta\left(\frac{m}{c}\right)+\ldots+\Theta\left(\frac{m}{c^{\gamma}}\right)=m \qquad (۸)$$

اگر در رابطهٔ (۸) به‌جای تابع $\Theta(m)$ مقدارش را از روی (۷) و بالاخره به‌جای $\psi(m)$ مقـدارش را از روی (۶) قرار دهیم، خواهیم داشت:

$$\sum_{\alpha'=۰}^{\alpha'=\alpha}\ \sum_{\beta'=۰}^{\beta'=\beta}\ \sum_{\gamma'=۰}^{\gamma'=\gamma}\varphi\left(\frac{m}{a^{\alpha'}b^{\beta'}c^{\gamma'}}\right)=m \qquad (۹)$$

که هم‌ارز با معادلهٔ زیر است:

$$\Sigma\varphi(d)=m \qquad (۱۰)$$

زیرا اگر به‌ترتیب به‌جای α' و β' و γ' تمام مقادیر واقع بین ۰

α و بین ∘ وبین∘و γ را درخارج‌قسمت $\dfrac{m}{a^{\alpha'}b^{\beta'}c^{\gamma'}}$ قرار دهیم ، تمام مقسوم علیه‌های d از m بدست می‌آید.

۲۱. ریشه‌های ساده و ریشه‌های اندیس‌دار. نتیجه‌ای که دربارهٔ $\varphi(m)$ گرفتیم به‌ما امکان‌می‌دهد نتیجهٔ مهمی‌که مربوط‌به‌قضیهٔ فرما است ذکرکنیم. عدد اول p و عدد درست a کوچکتر از p را در نظر می‌گیریم؛ توانهای متوالی a را که از توان صفر شروع شده‌است، درنظر می‌گیریم:

$$a^{۰}=۱ ، a ، a^{۲} ، a^{۳} ، a^{۴} ، . . . \qquad (۱)$$

و مانده‌های این توانها را نسبت به p محاسبه می‌کنیم:

$$۱ ، a ، a_{۲} ، a_{۳} ، a_{۴} ، . . . \qquad (۲)$$

این مانده‌ها ، ازنظر مقدار محدودند و حداکثر برابر با $p-۱$ هستند، در حالیکه هیچکدام از آنها برابر صفر نیست و رشتهٔ (۱) هم نامحدود است. بنابراین، یك مانده الزاماً با یکی ازمانده‌های پیش ازخودش‌برابر خواهد بود. فرض‌کنیم:

$$a_m=a_n \quad n>m \qquad (۳)$$

این تساوی هم‌ارز همنهشتی زیر است:

$$a^m \equiv a^n \quad (mod.p) \qquad (۴)$$

و چون a نسبت به p اول است داریم:

$$a^{n-m} \equiv ۱ \quad (mod.p) \qquad (۵)$$

یعنی:

$$a_{n-m} = ۱ \qquad (۶)$$

$n-m=r$ فرض می‌کنیم وبنا بررابطهٔ (۵) گوئیم که a نسبت به‌مدول p به توان r تعلق دارد. همچنین می‌توان گفت که r اندیس a می‌باشد.

روشن‌است که‌رشتهٔ (۲) متناوباً و r به r بدست می‌آید، یعنی داریم:

$$a^{m+kr} \equiv a^m \qquad (mod.p) \qquad (۷)$$

از اینجا می‌توان استدلال دیگری برای اثبات قضیهٔ فرما بدست آورد. اگر قضیه را ثابت شده فرض‌کنیم، رابطهٔ زیررا خواهیم داشت:

$$p-۱=kr \qquad (۸)$$

یعنی $p-۱$ مضربی‌از r است ویا به‌عبارت دیگراندیس r مقسوم‌علیهی از $p-۱$ است و می‌تواند در حالت خاص برابر با $p-۱$ باشد. عدد ۱ تنها عددی است که اندیس r برای‌آن برابر ۱ می‌باشد.

از قبل روشن نیست که برای هرمقسوم علیه r از $p-۱$، یك یا چند عدد a وجود دارد که متعلق به‌این اندیس باشد، که اگر یك عدد برابر a با اندیس r وجود داشته باشد، به‌اندازهٔ $\varphi(r)$ ازآن وجودخواهد داشت.

فرض می‌کنیم که r کوچکترین عددی باشدکه داشته باشیم:

$$a^r \equiv ۱ \qquad (mod.p) \qquad (۹)$$

روشن است که برای هرتوان r' کوچکتر از r داریم:

$$(a^{r'})^{r} \equiv ۱ \qquad (\text{mod.p}) \qquad (۱۰)$$

ولی اگر r و r' نسبت به‌هم اول نباشند و δ بزرگترین مقسوم‌علیه مشترك آنها باشد، دراینصورت $\frac{r'}{\delta}$ یك عدد درست خواهد بود:

$$\left(a^{\frac{r'}{\delta}}\right)^{r} \equiv ۱ \qquad (\text{mod.p}) \qquad (۱۱)$$

که هم ارز است با رابطه زیر:

$$\left(a^{r'}\right)^{\frac{r}{\delta}} \equiv ۱ \qquad (\text{mod.p}) \qquad (۱۲)$$

به‌نحوی‌که $a^{r'}$ توان $\frac{r}{\delta}$ را قبول کرده است و نه توان r ، بنابراین تعداد عددهای $a^{r'}$ که توان r را قبول می‌کند، برابر با $\varphi(r)$ است،در حالیکه تنها برای عددهای r' که با r اول باشند $a^{r'}$ این توان را قبول می‌کند. بنابراین ، اگرتوان غیرمشخص r که مقسوم‌علیهی از $p-۱$ است در نظر بگیریم ، تعداد $\psi(r)$ از a که توان r را قبول می‌کنند یا برابر صفر است ویا برابر $\varphi(r)$.

اما روشن است که داریم:

$$\Sigma\psi(d) = p-۱ \qquad (۱۳)$$

در حالیکه مجموع ، به‌تمام مقسوم علیه‌های $p-۱$ بسط داده می‌شود (که شامل $p-۱$ و واحد هم هست)، زیرا هریك از $p-۱$ عدد از ۱ تا $p-۱$ الزاماً یکی و تنها یکی از توانهای r (مقسوم علیه $p-۱$) را

قبول می‌کند.

از طرف دیگر می‌دانیم:

$$\Sigma\varphi(d) = p - ۱ = \Sigma\psi(d) \qquad (۱۴)$$

و بنابراین برای تمام مقادیر d باید داشته باشیم:

$$\psi(d) = \varphi(d) \qquad (۱۵)$$

وگرنه، مجموع $\psi(d)$ ها کمتر از مجموع $\varphi(d)$ ها خواهد شد.

در حالت خاص، $\varphi(p-۱)$ عدد وجود دارد که توان $p-۱$ را قبول می‌کند، یعنی همهٔ $p-۱$ عدد:

$$a \text{ ، } a^{۲} \text{ ، } \ldots \text{ ، } a^{p-۱} \qquad (۱۶)$$

دارای مانده‌های مختلف هستند. به این عددهای a ریشه‌های ساده می‌گویند. مانده‌ها با نظم غیرمشخصی عبارتند از ۱، ۲، ۳، . . . و $p-۱$. بنابراین اگر b، عددی دلخواه واقع بین ۱ و $p-۱$ باشد، عددی مانند β بین ۱ و $p-۱$ وجود دارد به‌نحوی که داشته باشیم:

$$a^{\beta} \equiv b \qquad (\mathrm{mod.}\,p) \qquad (۱۷)$$

عدد β را اندیس b نسبت به‌پایهٔ a گویند. اندیسها دارای خصوصیتهایی شبیه به‌لگاریتمها هستند، زیرا اگر همزمان با (۱۷) داشته باشیم:

$$a^{\gamma} \equiv c \qquad (۱۸)$$

نتیجه می‌شود:

$$a^{\beta+\gamma} \equiv bc \qquad (۱۹)$$

یعنی اندیس یك حاصلضرب ، برابر است با مجموع اندیسهای عاملها $(\mathrm{mod}.\,p-1)$.

اکنون اگرعددهای a و p مفروض باشند و a ریشهٔ ساده نسبت به‌عدد اول p باشد، به‌سادگی می‌توان جدول اندیسها را محاسبه کرد و از روی این جدول هم می‌توان بدون کورمالی همنهشتیهای درجهٔ اول را نتیجه‌گرفت. مثلا برای عدد اول ۱۳ و ریشهٔ سادهٔ ۲، دو جدول زیر را خواهیم داشت:

اندیس x	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
x	۲	۴	۸	۳	۶	۱۲	۱۱	۹	۵	۱۰	۷	۱

x	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
اندیس x	۱۲	۱	۴	۲	۹	۵	۱۱	۳	۸	۱۰	۷	۶

برای حل کردن همنهشتی:

$$7x \equiv 5 \qquad (\mathrm{mod}.\,13) \qquad (20)$$

از روی جدول دوم می‌نویسیم:

$$\text{اندیس}\,x \equiv \text{اندیس}\,5 - \text{اندیس}\,7 \equiv 9 - 11 \equiv 10 \qquad (21)$$

و ازآنجا از روی جدول اول خواهیم داشت:

$$x = ۱۰$$

برای اینکه بتوانیم جدول اندیسها را تشکیل دهیم، باید یك ریشهٔ ساده را بشناسیم، ولی قاعده و روشی برای پیداکردن ریشهٔ ساده وجود ندارد. درجدول زیرکوچکترین‌ریشهٔ سادهٔ r برای عددهای اول کوچکتر از ۱۰۰ داده شده است:

p	r	p	r	p	r	p	r	p	r	p	r
۳	۲	۱۳	۲	۲۹	۲	۴۳	۳	۶۱	۲	۷۹	۳
۵	۲	۱۷	۳	۳۱	۳	۴۷	۵	۶۷	۲	۸۳	۲
۷	۳	۱۹	۲	۳۷	۲	۵۳	۲	۷۱	۷	۸۹	۳
۱۱	۲	۲۳	۵	۴۱	۶	۵۹	۲	۷۳	۵	۹۷	۵

نظریهٔ ریشه‌های ساده و اندیس‌دار را می‌توان دربارهٔ عددهای‌غیر‌ـ اول ، با استفاده از تعمیم قضیهٔ فرما ، بسط داد ، ولی تنها برای $\varphi(m)$ عدد اول با مدول m به‌کار برده می‌شود. اگر مقسوم علیه‌های $\varphi(m)$ را با d نشان دهیم، با به‌حساب آوردن خود $\varphi(m)$ و واحد داریم:

$$\Sigma\varphi(d) \equiv \varphi(m) \qquad (۲۲)$$

و هریك از عددهای a ،که به‌نسبت m اول باشند، به‌توانی از d تعلق

دارند، تعداد عددهایی که به d تعلق دارند، دقیقاً برابر $\varphi(d)$ می‌باشد و بنابراین داریم:

$$a^{d} \equiv ۱ \qquad (mod.m) \qquad (۲۳)$$

که برای‌آن همچنین داریم:

$$a^{m-۱} \equiv ۱ \quad (mod.m) \qquad (۲۴)$$

کافی است که ۱ — m ، مضربی از d باشد و در این حالت d در عین‌حال هم مقسوم علیه ۱ — m وهم مقسوم‌علیه $\varphi(m)$ خواهد بود. در حالتی که m فرد باشد، $\varphi(m)$ عددی زوج است و به‌این ترتیب، عدد۲ مقسوم علیه مشترکی ازاین‌دوعدد خواهد بود. به‌همین ترتیب است‌برای ۱۵ = m که‌قبلا از آن گفتگو کرده‌ایم. وقتی‌که ۱ — m و $\varphi(m)$ نسبت به‌هم اول باشند، همنهشتی (۲۴) برای هیچ مقداری از a صادق نخواهد بود. به‌همین ترتیب است برای وقتی‌که ۱ — m ، عددی اول است و مثلا وقتی‌که ۳۰ = m یا ۶۰ = m می‌باشد .

۲۲. قضیهٔ ویلسون. همنهشتی زیر را که دارای دومتغیرy و z نسبت به‌مدول اول p است درنظر می‌گیریم:

$$yz \equiv ۱ \qquad (mod.p) \qquad (۱)$$

دوعدد y و z را، که دراین همنهشتی صدق می‌کنند، انباز «associé» گوییم. دو عدد انباز نمی‌توانند برابر باشند، مگراین‌که مقدار مشترك آنها ۱ یا ۱ — باشد (۱ — معادل با ۱ — p است).

همنهشتی

$$x^{۲} \equiv ۱ \qquad (mod.p) \qquad (۲)$$

جوابی جز ۱+ و ۱− ندارد. بنابراین $p-۳$ عدد واقع بین ۲ و $p-۱$، دوبه‌دو انباز یکدیگرند، به‌نحوی‌که حاصلضرب هردو عدد انباز نسبت به‌مدول p همنهشت با واحد می‌باشد و بنابراین، حاصلضرب این $p-۳$ عددهم نسبت به‌مدول p همنهشت با واحد خواهدبود. اگراین‌حاصلضرب را در ۱ و $p-۱$ ضرب کنیم، حاصلضرب، همنهشت با $p-۱$ ویا به عبارت دیگر، همنهشت با ۱− خواهد بود، یعنی داریم:

$$۱ \times ۲ \times ۳ \times \ldots \times (p-۱) + ۱ \equiv ۰ \quad (mod.p) \quad (۳)$$

و این همان قضیهٔ ویلسون است‌که همچون قضیهٔ فرما، خاصیت مشخصه‌ای از عددهای اول را بیان می‌کند. درحقیقت، اگر p، عدداول نباشد و مثلا ازدوعامل مختلف m و n تشکیل شده باشد، دراین‌صورت این دوعامل در حاصلضرب $۱ \times ۲ \times ۳ \times \ldots \times (p-۱)$ وجود خواهد داشت و بنابراین چنین حاصلضربی بر p بخش‌پذیر خواهد بود و اگرp، توانی از عدد اولی مانند q باشد، این‌عامل q در حاصلضرب $۱ \times ۲ \times ۳ \times \ldots \times (p-۱)$ لااقل به‌همان تعدادی که در p وجود دارد، تکرارخواهد شد و بنابراین برp بخش‌پذیر خواهد بود. مگر در حالت $p=۴$، که درآنجا عامل ۲ تنها یکبار درحاصلضرب $۱ \times ۲ \times ۳$ ظاهر شده است، ولی این حاصلضرب هم بر ۲ بخش‌پذیر است و بنابراین نمی‌تواند نسبت به‌مدول ۴ همنهشت با واحد باشد.

اکنون به‌جای همنهشتی (۱)، همنهشتی زیررا درنظرمی‌گیریم:

$$yz \equiv D \qquad (mod.p) \qquad (۴)$$

که درآن D عددی غیرمشخص‌و p عددی اول است. عددهای y و z که

دراین همنهشتی صدق می‌کنند نسبت به D و p انباز هستند. هرعدد بین ۱ و $p-۱$ تنها یك انباز خواهد داشت.

دو عدد انباز نمی‌توانند برابر باشند، مگر اینکه مقدار مشترك آنها، x ، در همنهشتی زیر صدق کند:

$$x^۲ \equiv D \qquad (\mathrm{mod}.p) \qquad (۵)$$

و این همنهشتی جواب ندارد، مگر اینکه D ماندهٔ مربعی p باشد. ابتدا فرض می‌کنیم که D غیرمانده باشد و این به‌معنای آنست که همنهشتی (۵) جواب ندارد و بنابراین، عددهای انباز y و z که در همنهشتی(۴) صدق می‌کنند نمی‌توانند مساوی یکدیگر باشند. پس $p-۱$ عدد ۱ و۲ و ۳ و ... و $p-۱$ دو بدو انباز یکدیگرند و دوعدد انبازهم هرگزبرابر نخواهند بود. بنابراین، $\frac{p-۱}{۲}$ زوج عددهای انباز وجود دارد که در همنهشتی مانند (۴) صدق می‌کنند ؛ اگر این $\frac{p-۱}{۲}$ همنهشتی را عضو به‌عضو درهم ضرب‌کنیم، خواهیم داشت:

$$(p-۱)! \equiv D^{\frac{p-۱}{۲}} \qquad (\mathrm{mod}.p) \qquad (۶)$$

این همنهشتی برای موردی ثابت می‌شودکه درآنجا D یك غیر مانده است.

اگر D یك مانده باشد، در اینصورت همنهشتی (۵) دارای دو ریشهٔ $x_۰$ و $p-x_۰$ خواهد بود و داریم:

$$x_۰(p-x_۰) = px_۰ - x_۰^۲ \equiv -D \quad (\mathrm{mod}.p) \qquad (۷)$$

که درآن $x_{\circ}$ در همنهشتی (۵) صدق می‌کند. $p-۳$ عدد دیگر کوچکتر از p ومخالف با $x_{\circ}$ و $p-x_{\circ}$ دوبه‌دو انباز یکدیگرند، عددهای انباز، در همنهشتی (۴) صدق می‌کنند، اکنون $\frac{p-۳}{۲}$ همنهشتی مشابه با (۴) داریم که می‌توانیم آنها را درهم ضرب کنیم و اگر بعد آنرا درهمنهشتی (۷) ضرب کنیم، بدست می‌آوریم:

$$(p-۱)! \equiv -D^{\frac{P-۱}{۲}} \quad (\text{mod.}p) \qquad (۸)$$

و این همنهشتی وقتی صادق است که D یك مانده باشد.

ازآنجاکه $D=۱$ یك ماندهٔ مربعی p است، اگر به‌جای Dعدد ۱ را قراردهیم، قضیهٔ ویلسون بدست می‌آید:

$$(p-۱)! \equiv -۱ \quad (\text{mod.}p) \qquad (۹)$$

با استفاده از رابطهٔ (۹)، همنهشتیهای (۶) و (۸) چنین می‌شوند:

$$D^{\frac{p-۱}{۲}} \equiv -۱ \qquad (\text{mod.}P) \qquad (۱۰)$$

درحالتی‌که D یك غیرمانده است.

و

$$D^{\frac{p-۱}{۲}} \equiv ۱ \qquad (\text{mod.}p) \qquad (۱۱)$$

وقتی D یك مانده است.

بنابراین در همنهشتیهای :

$$x^{\frac{p-1}{2}}+1\equiv 0 \quad (\mathrm{mod}.p) \qquad (12)$$

$$x^{\frac{p-1}{2}}-1\equiv 0 \quad (\mathrm{mod}.p) \qquad (13)$$

برای اولی $\frac{p-1}{2}$ غیرمانده و برای دومی $\frac{p-1}{2}$ مانده به‌عنوان‌جواب خواهیم داشت. چون هیچیک از این همنهشتیها بیش از $\frac{p-1}{2}$ ریشه‌ندارند، بنابراین نتیجه می‌شودکه تمام ریشه‌های همنهشتی (۱۲) غیرمانده و تمام ریشه‌های همنهشتی (۱۳) مانده هستند. اگر این دو همنهشتی را عضوبه‌عضو درهم ضرب‌کنیم، خواهیم داشت:

$$x^{p-1}-1\equiv 0 \quad (\mathrm{mod}.p) \qquad (14)$$

که تمام ریشه‌های (۱۲)و(۱۳) درآن صدق می‌کنند، یعنی تمام مانده‌ها و غیرمانده‌ها، یعنی تمام عددهای رشتهٔ (۲) . اکنون‌می‌توان قضیهٔ فرما را به‌شکل جدیدی توضیح داد.

از همنهشتیهای (۱۲) و(۱۳) می‌توان نتیجهٔ بسیارمهم‌می‌گرفت؛ D را به ۱ــ تبدیل می‌کنیم وفرض می‌کنیم که به‌ترتیب داشته‌باشیم:

$$\begin{cases} p=4n+1 \\ p=4n+3 \end{cases}$$

در نتیجه به‌ترتیب خواهیم داشت:

$$(۱۵)\qquad \begin{cases} \dfrac{p-۱}{۲}=۲n & (-۱)^{\frac{p-۱}{۲}}=۱ \\ \dfrac{p-۱}{۲}=۲n+۱ & (-۱)^{\frac{p-۱}{۲}}=-۱ \end{cases}$$

به‌این ترتیب عدد ۱− در همنهشتی(۱۳) صدق می‌کند به‌شرطی که p به‌صورت $۴n+۱$ باشد و در همنهشتی (۱۲) صدق می‌کند به‌شرطی‌که p به‌صورت $۴n+۳$ باشد. بنابراین، در حالت اول ۱− یك غیرمانده و درحالت دوم یك مانده‌است. این‌مطلب‌برای بررسیهای بخش بعد بسیار مهم است . گوییم ۱− یك ماندهٔ مربعی از عدداول p است به‌شرطی‌که $p=۴n+۱$ باشد و یك غیر مانده است به‌شرطی $p=۴n+۳$ باشد.

به‌سادگی می‌توان ملاحظه کرد که همنهشتیهای (۱۲) و (۱۳) می‌توانند بلافاصله از قضیهٔ فرما نتیجه شوند. فرض می‌کنیم p عددی اول باشد:

$$\frac{p-۱}{۲}=q \qquad (۱۶)$$

می‌توانیم همنهشتی زیرا بنویسیم:

$$x^{p-۱}-۱=(x^q-۱)(x^q+۱)\equiv ۰ \pmod{p} \qquad (۱۷)$$

بنابر قضیهٔ فرما، هریك از این همنهشتیها به‌تعداد واحدهایی‌که

در توان آن وجود دارد ، دارای جواب است. α را یك ماندهٔ مربعی p فرض کنید، عددی مانند y وجود دارد طوریکه داشته باشیم:

$$y^{۲} \equiv \alpha \qquad (\mathrm{mod.}p) \qquad (۱۸)$$

بنابراین با توجه به‌قضیهٔ فرما داریم:

$$y^{p-۱} \equiv y^{۲q} \equiv \alpha^{q} \equiv ۱ \qquad (\mathrm{mod.}p) \qquad (۱۹)$$

یعنی تمام مانده‌های α در همنهشتی زیرصدق می‌کند:

$$x^{q} - ۱ \equiv ۰ \qquad (\mathrm{mod.}p) \qquad (۲۰)$$

واین همنهشتی‌دارای q جواب است‌که عیناً همان q مانده هستند و بالاخره q جواب همنهشتی:

$$x^{q} + ۱ \equiv ۰ \qquad (\mathrm{mod.}p) \qquad (۲۱)$$

همان q غیرمانده هستند.

۲۳. خصوصیت مربعی عدد ۲. قانون دو طرفه‌ای که باعث ساده شدن حساب مربوط به‌خاصیت مربعی عددهای‌فرد اول می‌شود، در مورد عدد ۲ صادق نیست و بنابراین باید خاصیت مربعی این عدد را مستقیماً مورد بررسی قرار دهیم، ما به‌شرح نتیجه‌ای می‌پردازیم که هم اکنون از قضیهٔ فرما بدست آوردیم.

عدد ۲ یك ماندهٔ مربعی عددهای اول به‌شکل $۸n+۱$ و $۸n+۷$ و یك غیرمانده از عددهای اول به‌شکل $۸n+۳$ و $۸n+۵$ می‌باشد.

برای اثبات این نتیجه یادآوری می‌کنیم که‌باتوجه به‌قضیهٔ فرما،

همنهشتی نسبت به‌مدول p :

$$x^{p-۱}-۱\equiv ۰ \qquad (mod.p) \qquad (۱)$$

دارای تعداد ریشه‌هایی مساوی با درجهٔ آنست و به‌آن مناسبت می‌توان گفت که طرف اول این همنهشتی از حاصلضرب ۱ − p عامل درجه اول تشکیل شده است . ازآنجا نتیجه می‌شود که اگرطرف اول همنهشتی(۱) را به‌دوعامل تجزیه کنیم، به‌صورت زیر:

$$x^{p-۱}-۱\equiv f(x)\,g(x) \quad (mod.p) \qquad (۲)$$

هریك از همنهشتیهای زیر:

$$\begin{cases} f(x)\equiv ۰ \\ g(x)\equiv ۰ \end{cases} \qquad (mod.p) \qquad (۳)$$

نیز به‌تعداد واحدهایی که در توان آنها هست دارای ریشه هستند . حالا ۱+p=۸n قرار می‌دهیم؛ داریم:

$$x^{۸n}-۱=(x^{۴n}-۱)(x^{۴n}+۱) \qquad (۴)$$

بنابراین، همنهشتی

$$x^{۴n}+۱\equiv ۰ \qquad (mod.p) \qquad (۵)$$

دارای ۴n ریشه است؛ اگر x یکی از ریشه‌ها باشد، داریم:

$$x^{۴n}+۱=(x^{۲n}+۱)^{۲}-۲x^{۲n} \qquad (۶)$$

اگر فرض کنیم:

$$\begin{cases} x^{2n}+1=t \\ x^{n}=u \end{cases} \qquad (7)$$

خواهیم داشت:

$$t^2-2u^2\equiv 0 \qquad (\mathrm{mod}.p) \qquad (8)$$

و ما ثابت می‌کنیم که از اینجا نتیجه می‌شود که عدد ۲ماندهٔ مربعی عدد p است. عدد u بخش‌پذیر بر p نیست، زیرا x بر p بخش‌پذیر نیست و بنابراین t و u بخش‌پذیر بر p نیستند، حالا می‌توان عددی مانند y که بر p بخش‌پذیر نباشد، پیدا کرد طوریکه داشته‌باشیم:

$$uy\equiv 1 \qquad (\mathrm{mod}.p) \qquad (9)$$

اکنون اگر دوطرف همنهشتی (۸) را در y^2 ضرب کنیم، خواهیم‌داشت:

$$(ty)^2\equiv 2 \qquad (\mathrm{mod}.p)$$

که به‌معنای آنست‌که ۲ یك مانده از عدد p است.

طریقهٔ اثبات فوق متعلق به لژاندر است، طریقه‌های مشابهی هم در مورد عددهای $8n+3$ و $8n+5$ و $8n+7$ به‌کار می‌برد که بسیار پیچیده و مشکل است وبه‌همین جهت ما از روش دیگری که منتسب به ستیلجه «Stieltjes» می‌باشد استفاده می‌کنیم.

رشتهٔ عددهای واقع بین ۱ و $p-1$ را درنظرمی‌گیریم وزیرآنها رشتهٔ مقادیر ε_k را با خصوصیت مربعی آنها می‌نویسیم، یعنی $+1$ یا

۱ – ، برحسب اینکه k مانده است و یا غیرمانده .

$$۱, ۲, ۳, \ldots k, k+۱, \ldots, p-۱ \qquad (۵)$$

$$\varepsilon_۱, \varepsilon_۲, \varepsilon_۳, \ldots, \varepsilon_k, \varepsilon_{k+۱}, \ldots, \varepsilon_{p-۱} \qquad (۶)$$

اکنون تغییرات علامت را بین جمله‌های متصل رشتهٔ (۶) مطالعه می‌کنیم؛ یك تغییر علامت در k امین فاصله وجود دارد ، یعنی بین k و k+۱ :

$$\varepsilon_{k+۱} = -\varepsilon_k \qquad (۷)$$

حالتهائی را جستجو می‌کنیم که درآنجا رابطهٔ (۷) برای عددهای‌معین r_k که به‌وسیلهٔ همنهشتی زیرمشخص می‌شوند، صادق باشد:

$$kr_k \equiv k+۱ \pmod{p} \qquad (۸)$$

عددهای k و k+۱ نسبت به‌هم و نسبت به‌p اولند. این همنهشتی‌تنها دارای یك جواب است و عددهای معین r_k هم نسبت به‌مدول p با هم فرق دارند، زیرا اگر داشته باشیم:

$$r_k \equiv r_h \pmod{p} \qquad (۹)$$

نتیجه می‌گیریم:

$$k(h+۱) \equiv (k+۱)h \pmod{p} \qquad (۱۰)$$

یعنی:

$$k \equiv h \pmod{p} \qquad (۱۱)$$

اگر خصوصیتهای مربعی k و $k+1$ را به‌وسیلهٔ ε_k و ε_{k+1} نشان دهیم، طبق رابطهٔ (۸) داریم:

$$\varepsilon_k \ \varepsilon_{k+1} = \left(\frac{r_k}{p}\right) \qquad (12)$$

بنابراین رابطهٔ (۷) تنها وقتی صادق است که در آنجا r_k یك غیرمانده باشد. ولی باتوجه به‌رابطهٔ (۸) روشن است که r_k نمی‌تواند برابر واحد باشد، پس $p-2$ مقدار مختلف r_k با ۲ و۳ و ... و $p-2$ همنهشت هستند و ازآنجا که ۱ یك مانده است، بین این مقادیر $\frac{p-3}{2}$ مانده و $\frac{p-1}{2}$ غیرمانده وجود دارد که تغییرات علامت، باآنها تطبیق می‌کند. بنابراین در رشتهٔ (۶) ، $\frac{p-1}{2}$ تغییرعلامت وجود خواهدداشت.

ابتدا فرض می‌کنیم که $p=4n+1$ باشد ، در ایـن صورت $2n=\frac{p-1}{2}$ عددی است زوج، اولین جملهٔ این رشته، یعنی۱ وهمچنین آخرین جملهٔ آن، $p-1$ مانده هستند، برعکس اگر $p=4n+3$ باشد $2n+1=\frac{p-1}{2}$ و عددی فرد می‌شود و در این صورت ۱ مانده و $p-1$ غیرمانده‌می‌شود. اکنون‌می‌توانیم همین‌نتیجه‌هارا درحالتهایی‌که $p-1$ و -1 را درنظر می‌گیریم بدست‌آوریم

رشته‌های (۵) و (۶) را به‌دوقسمت تقسیم می‌کنیم:

$$(5)' \quad \begin{cases} 1 , 2 , \ldots , \frac{p-1}{2} \\ \frac{p+1}{2} , \frac{p+3}{2} , \ldots , p-1 \end{cases}$$

$$\begin{cases} \varepsilon_1 ,\ \varepsilon_2 ,\ \dots ,\ \varepsilon_{\frac{p-1}{2}} \\ \\ \varepsilon_{\frac{p+1}{2}} ,\ \dots ,\ \varepsilon_{p-1} \qquad (6)' \end{cases}$$

اگر p به صورت $4n+1$ باشد، $1-$ یك مانده است و بنابراین k و $p-k$، یا هردو مانده ویاهردوغیر مانده هستند و دو رشتهٔ $(6)'$ متقارن‌می‌شوند، یعنی k امین‌جملهٔ رشتهٔاول برابربا $(p-1-k)$امین جملهٔ رشتهٔ دوم است. برعکس اگر p به‌صورت $4n+3$ باشد، $1-$یك غیرمانده است و دورشته غیرمتقارن می‌شوند، یعنی k امین جملهٔ رشتهٔ اول علامتی مخالف‌علامت جملهٔ $(p-1-k)$ ام جملهٔ رشتهٔ دوم‌دارد.

در حالت اول $(p=4n+1)$ آخرین جملهٔ رشتهٔ اول از $(6)'$ برابراست با اولین جمله ازدومین رشتهٔ $(6)'$، یعنی‌بین‌آنها تغییرعلامت وجود ندارد، در حالیکه درحالت دوم، وقتی‌که $p=4n+3$ باشد یك تغییرعلامت بین‌آخرین جملهٔ رشتهٔ دوم از رشته‌های $(6)'$ وجود دارد. بنابراین در حالت اول$\frac{p-1}{2}$ تغییرعلامت بین دوسطر$(6)'$و درحالت‌دوم فقط$\frac{p-3}{2}$ تغییرعلامت وجود خواهد داشت.

بالاخره درحالت اول $\frac{p-1}{4}$ و درحالت دوم$\frac{p-3}{4}$ تغییرعلامت در سطر اول $(6)'$ وجود دارد: و چون در حالت اول $p=4n+1$ و در حالت دوم $p=4n+3$ می‌باشد، تعداد تغییر علامتها همیشه برابر n است. بنابراین اگر n زوج باشد، جملهٔ آخر سطر اول $(6)'$ باید برابر جملهٔ اول آن یعنی ۱ باشد، در حالیکه اگر n فرد باشد،

جملهٔ آخر با علامت مخالف جملهٔ اول است. اکنون دیگر خصوصیتهای مربعی $p-۱$ و $\frac{p-۱}{۲}$ را شناخته‌ایم و خصوصیت مربعی ۲، برابر با حاصلضرب آنهاست.

اکنون حالتهای زیررا موردآزمایش قرارمی‌دهیم:

a) $p=۸m+۱=۴n+۱$ $\quad n=۲m$

b) $p=۸m+۳=۴n+۳$ $\quad n=۲m$

c) $p=۸m+۵=۴n+۱$ $\quad n=۲m+۱$

d) $p=۸m+۷=۴n+۳$ $\quad n=۲m+۱$

a) $\frac{p-۱}{۲}$ مانده است، همینطور $p-۱$ و ۲ مانده است.

b) $\frac{p-۱}{۲}$ مانده است، ولی $p-۱$ غیرمانده و ۲ غیرمانده است.

c) $\frac{p-۱}{۲}$ غیرمانده و $p-۱$ مانده است، ۲ غیرمانده است.

d) $\frac{p-۱}{۲}$ غیرمانده و $p-۱$ هم غیرمانده است، ۲ مانده است.

به‌این‌ترتیب درتمام حالتها، خصوصیت مربعی ۲ را مشخص کردیم.

۵

مجموع مربعها

۲۴. مجموع دو مربع. به‌مناسبت قضیهٔ فیثاغورث، ازمدتها پیش به‌این مطلب پی‌برده بودندکه بسیاری از عددهای درست ، مجموع دو مربع کامل هستند و همچنین ، مجذور این عـددهای درست را هم می‌توان به‌صورت مجموع دو مربع کامل نوشت و در اینحالت می‌توان آنها را ضلعهای مثلث قائم‌الـزاویه‌ای در نظرگـرفت . از این قبیل‌اند مثلثهایی با ضلعهای ۳، ۴ و ۵ یا ۵، ۱۲ و ۱۳.

قضیه مشهوری وجود داردکه طبق‌آن:

حاصلضرب مجموع دو مربع کامل در مجموع دو مربع کامل دیگر، برابر است با مجموع دو مربع کامل.

این قضیه به‌سادگی ازاتحاد جبری زیر نتیجه می‌شود:

$$(a^2+b^2)(\alpha^2+\beta^2)=(a\alpha+b\beta)^2+(a\beta-b\alpha)^2 \quad (1)$$

با تبدیل b به $-b$ ، این اتحاد ، به‌اتحاد زیرتبدیل می‌شود:

$$(a^2+b^2)(\alpha^2+\beta^2)=(a\alpha-b\beta)^2+(a\beta+b\alpha)^2 \quad (2)$$

و بنابراین می‌توان قضیهٔ فـوق را به‌این ترتیب دقیق کـرد که حاصلضرب مجموع دو مربع ، درمجموع دو مربع دیگررا می‌توان به‌دو صورت مختلف ، به‌مجموع دو مربع تبدیل کرد.

ولی در حالتی که $a=b$ و $\alpha=\beta$ باشد، دو رابطهٔ (۱) و (۲) یکی می‌شوند. مثلا داریم:

$$۵=۲^۲+۱^۲$$

$$۱۳=۲^۲+۳^۲$$

و با یك محاسبهٔ ساده نتیجه می‌شود:

$$۶۵=۸^۲+۱^۲=۷^۲+۴^۲$$

از طرف دیگر داریم:

$$۲=۱+۱ \quad و \quad ۱۳=۹+۴ \quad و \quad ۲۶=۲۵+۱$$

قضیهٔ بسیار مهم دیگر، قضیهٔ زیر است:

اگر یك عدد اول، مجموع دو مربع (، که نسبت به‌هم اول هستند، عادکند؛ خودش مجموع دو مربع کامل خواهد بود.

فرض می‌کنیم که داشته باشیم:

$$a^2+b^2=mp \qquad (۳)$$

که درآن p عددی است اول و عددهای درست a و b و m نسبت‌به‌هم اول هستند، علاوه برآن می‌دانیم که هیچیك ازعددهای a و b به‌تنهائی بر p بخش‌پذیر نیستند. می‌توانیم به‌جای a و b، عددهای درست مثبت یا منفی قرار دهیم که قدر مطلق‌آنها از $\frac{p}{2}$ کمترباشد؛ در واقع،می‌توان عددهای درست λ و μ را چنان پیدا کردکه داشته باشیم:

$$a-\lambda p=a' \qquad \left|a'\right|<\frac{p}{2}$$

$$b-\mu p=b' \qquad |b'|<\frac{p}{۲}$$

بنابراین می‌توان نوشت:

$$a'^{۲}+b'^{۲}=pp' \qquad (۳)$$

که درآن a' و b' و p' مخالف صفرهستند و ضمناً داریم:

$$pp'<\frac{p^{۲}}{۴}+\frac{p^{۲}}{۴}=\frac{p^{۲}}{۲}$$

طوری‌که p' الزاماً کوچکتر از p خواهد بود. به‌همین ترتیب، اگر در نظر بگیریم:

$$\begin{cases} a'-\lambda'p'=a'' & |a''|<\frac{p'}{۲} \\ b'-\mu'p'=b'' & |b''|<\frac{p'}{۲} \end{cases} \qquad (۴)$$

بدست خواهیم‌آورد:

$$a''^{۲}+b''^{۲}=p'p'' \qquad (۵)$$

و عدد p'' کوچکتر از $\frac{p'}{۲}$ خواهد بود.

اگر رابطه‌های (۳) و (۵) را نظیربه‌نظیر درهم ضرب‌کنیم بدست می‌آید:

$$(a'^{۲}+b'^{۲})(a''^{۲}+b''^{۲})=pp'^{۲}p'' \qquad (۶)$$

اما از رابطهٔ (۴) بدست می‌آوریم:

$$\begin{aligned} a'b''-b'a''&=p'(-\lambda'b''+\mu a'') \\ a'a''+b'b''&=a''^{2}+b''^{2}+p'(\lambda'a''+\mu'b'') \end{aligned} \qquad (۷)$$

یعنی با در نظرگرفتن رابطهٔ (۵):

$$a'a''+b'b''=(p''+\lambda'a''+\mu'b'')p' \qquad (۸)$$

اگر سمت چپ رابطهٔ (۶)را به‌صورت رابطهٔ (۱) بنویسیم‌وسپس از رابطه‌های (۷) و (۸) استفاده کنیم، روشن می‌شود که عامل p'^{2} در هر دو طرف رابطهٔ (۶) بدست می‌آید و رابطه‌ای به‌شکل زیر بدست می‌آوریم:

$$A^{2}+B^{2}=pp'' \qquad (۹)$$

یعنی، رابطه‌ای شبیه به‌رابطهٔ (۳) که درآن p'' کوچکتر از $\frac{p'}{2}$ خواهد بود.

و اگر به‌همین‌ترتیب ادامه دهیم، بالاخره به‌جائی خواهیم رسید که طرف دوم رابطه ، اولین مضرب p باشد، یعنی $p''=1$ شود و در اینصورت رابطهٔ (۹) نشان می‌دهدکه p مساوی با مجموع دومربع‌کامل می‌شود و این همان چیزی است‌که می‌خواستیم ثابت‌کنیم.

دربخش پیش دیدیم که -1 ماندهٔ مربعی تمام عددهای اول p است‌که به‌صورت $4n+1$ باشند. و بنابراین نتیجه می‌شود که عددی مانند t وجود دارد طوری که $t^{2}+1$ برp بخش‌پذیر باشد واین به‌معنای آنست‌که p مساوی مجموع دو مربع‌کامل است،

تمام عددهای اول به‌صورت $4n+1$ ، مساوی مجموع دو مربع کامل هستند.

توجه به‌این مطلب مهم است که این قضیه در مورد عددهای غیر اولی که به‌صورت ۴n+۱ باشند صادق نیست ، از این نمونه عدد ۲۱ می‌باشد که از حاصلضرب دوعدد اول ۷ و ۳ (که هریك ازآنهابه‌صورت ۴n+۳ می‌باشند) تشکیل شده است. ما تحقیق خواهیم کرد که یك عدد نمی‌تواندمساوی مجموع دوعدد مربع کامل‌باشد،مگراینکه تمام عاملهای اول آن ، به‌صورت ۴n+۱ باشند . در بخش ششم که اختصاص به‌عددهای موهومی دارد، نتیجه‌های مربوط به‌مجموع دو مربع کامل را ذکر خواهیم کرد.

۲۵. مجموع چهار مربع . اکنون به‌مجموع مربعهای ۴عدد می‌پردازیم. درحقیقت ، مجموع مربعهای ۳ عدد، واجد اهمیت زیادی نیست و می‌توان‌آنرا به‌عنوان حالت خاصی از مجموع مربعهای ۴ عدد دانست، وقتی که یکی ازآن عددها برابرصفر باشد.

ابتدا به‌تحقیق این قضیهٔ جبری می‌پردازیم که طبق‌آن :

حاصلضرب مجموع مربعهای ۴ عدد ، در مجموع مربعهای۴ عدد دیگر، برابر است با مجموع مربعهای ۴ عدد .

در حقیقت، اگر رابطه‌های زیر را در نظر بگیریم:

$$\begin{cases} A=a\alpha+b\beta+c\gamma+d\delta \\ B=a\beta-b\alpha+c\delta-d\gamma \\ C=a\gamma-c\alpha+d\beta-b\delta \\ D=a\delta-d\alpha+b\gamma-c\beta \end{cases} \qquad (۱)$$

اتحاد زیر درست خواهد بود:

$$(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2)= \qquad (2)$$
$$A^2+B^2+C^2+D^2$$

بعداً تحقیق خواهیم کرد که اگر عددهای داده شده، حالت خاصی نداشته باشند، حاصلضرب دوعبارتی که هریك مجموع مربعهای چهار عدد هستند، می‌تواند به ۹۶ صورت مختلف برابر با مجموع مربعهای ۴ عدد باشند.

اگر به‌جای مجموعهای ۴ مربع کامل، تنها مجموعهای ۳ مربع کامل مورد نظر باشد، می‌توان در A و B و C و D مقادیر d و δ را مساوی صفر گرفت و آنرا مثل مجموع ۴ مربع کامل درنظرگرفت واین مطلب به‌خوبی نشان می‌دهد که همانطوری که قبلاهم گفته شد مجموعهای ۳ مربع کامل، اهمیت زیادی ندارند و حالت خاصی از مجموعهای ۴ مربع کامل به‌شمار می‌روند.

اکنون برای ۴ مربع کامل هم قضیه‌ای شبیه‌آنچه که برای‌مجموع دو مربع‌کامل ثابت کردیم، اثبات می‌کنیم:

هر عدد اول فردی که مجموع چهار مربع‌کامل را عاد کند، خودش مساوی مجموع ۴ مربع کامل خواهد بود.

فرض کنید که داشته باشیم:

$$a^2+b^2+c^2+d^2 \equiv 0 \qquad (\text{mod.}p) \qquad (3)$$

می‌توان به‌جای مقادیر a، b، c و d، قدر مطلق کوچکترین باقیماندهٔ آنها را درنظرگرفت. طوریکه ازلحاظ قدر مطلق‌کوچکتر از

$\frac{p}{2}$ باشند، زیرا اگر باقیماندهٔ مثبت یعنی r از $\frac{p}{2}$ بزرگتر باشد، عددمنفی $r-p$ هم باقیمانده است و از لحاظ قدرمطلق از $\frac{p}{2}$ کوچکتر خواهد بود .

اگر در رابطهٔ (۳) به‌جای a ، b ، c و d مقادیر مذکور کوچکتر از $\frac{p}{2}$ را قرار دهیم، مجموع مربعهای آنها از p^2 کوچکتر خواهد بود (حالت‌مساوی با p^2 هم قابل‌قبول‌نیست؛ زیرا a ، b ، c و d نمی‌توانند مساوی با $\frac{p}{2}$ ، که عددی درست نیست، باشند.)

بنابراین می‌توان رابطهٔ (۳) را به‌صورت زیرنوشت:

$$a^2+b^2+c^2+d^2=pp' \qquad (۴)$$

که درآن عدد p' کوچکتر از عدد p می‌باشد. اگر p' برابرواحدباشد، رابطهٔ (۴) به‌وضعی درمی‌آیدکه p را به‌صورت مجموع مربعهای ۴عدد نشان می‌دهد .

فرض کنیم که p' بزرگتر از یك باشد : a'، b'، c' و d' را کوچکترین باقیمانده‌های a، b، c، و d نسبت به p' می‌گیریم ؛ در اینصورت خواهیم داشت:

$$\left\{\begin{array}{ll} a-\lambda p'=a' & |a'| < \frac{p'}{2} \\ b-\mu p'=b' & |b'| < \frac{p'}{2} \\ c-\upsilon p'=c' & |c'| < \frac{p'}{2} \\ d-\rho p'=d' & |d'| < \frac{p'}{2} \end{array}\right. \qquad (۵)$$

دراینجا نمی‌توان‌ثابت کرد که a'، b'، c' و d' ازلحاظ قدرمطلق برابر با $\frac{p'}{2}$ نیستند، زیرا p' می‌تواند مساوی بایك عدد زوج باشد،ولی هرچهار عدد نمی‌توانند با هم مساوی $\frac{p'}{2}$ شوند، زیرا دراینصورت a، b، c و d بر a' بخش‌پذیر می‌شوند و این متناقض بافرض‌است که این‌عددها نسبت به‌هم اول بودند، مگراینکه $a'=1$ باشد . دراین حالت اگر a' ، b' ، c' و d' مساوی با یك باشند ؛ به‌اینجا منجر می‌شود که a ، b، c و d عددهای فردی هستند و مجموع مربعهای‌آنها بر ۴ بخش‌پذیر است‌و بنابراین نمی‌تواند مساوی با $2p$ باشد. بنابراین داریم:

$$a'^2+b'^2+c'^2+d'^2=p'p'' \qquad (6)$$

که درآن عدد p'' الزاماً کوچکتر از p' خواهد بود. اکنون اگردوطرف رابطه‌های (۴) و (۶) را عضوبه‌عضو درهم ضرب کنیم، داریم:

$$(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2)= \qquad (7)$$
$$pp'^2p''$$

ولی اگر فرض‌کنیم:

$$\left\{\begin{array}{l} A=aa'+bb'+cc'+dd' \\ B=ab'-ba'+cd'-dc' \\ C=ac'-ca'+db'-bd' \\ D=ad'-da'+bc'-cb' \end{array}\right. \qquad (8)$$

طرف اول رابطهٔ (۷) برابر خواهد شد با:

$$A^2+B^2+C^2+D^2$$

از طرف دیگر با توجه به‌رابطهٔ (۵) داریم:

$$A=aa'+bb'+cc'+dd'=p'(\lambda a'+\mu b'+ \qquad (۹)$$
$$+\upsilon c'+\rho d')+a'^{2}+b'^{2}+c'^{2}+d'^{2}=p'(\lambda a'+\mu b'+\upsilon c'+$$
$$\rho d'+p'')=p'A'$$

که با توجه به‌رابطهٔ (۶) ، و درنظرگرفتن A' به‌عنوان یك عدددرست، بدست آمده است. بالاخره داریم :

$$(۱۰) \qquad \begin{cases} B=p'(b\lambda-a\mu+c\rho-d\upsilon)=p'B' \\ C=p'(c\lambda-a\upsilon+d\mu-b\rho)=p'C' \\ D=p'(d\lambda-a\rho+b\upsilon-c\mu)=d'D' \end{cases}$$

که درآن B'، C' و D' هم، عددهایی درست هستند.

رابطهٔ (۷) را که می‌توان به‌صورت زیرنوشت:

$$A^{2}+B^{2}+C^{2}+D^{2}=pp'^{2}p'' \qquad (۱۱)$$

که اکنون باتوجه به‌رابطه‌های (۹) و (۱۰) به‌صورت زیر در می‌آید:

$$A'^{2}+B'^{2}+C'^{2}+D'^{2}=pp'' \qquad (۱۲)$$

و این رابطه ، شبیه رابطهٔ (۴) است، با این تفاوت‌که درآن p''کوچکتر از p' است. اگرp'' برابر با واحد باشد، به‌این معناست‌که p به‌صورت مجموع مربعهای ۴ عدد درآمده است و اگر p'' بزرگتر از واحد باشد، روی رابطهٔ (۱۲) همان عملهایی را انجام می‌دهیم که روی رابطهٔ (۴) انجام دادیم و در اینصورت رابطهٔ جدیدی مشابه آن بدست خواهد آمد که درآن p'' تبدیل به‌عددی‌کوچکتر ازخود شده است. درپایان یك‌رشته

عملهای محدود، بالاخره به‌معادله‌ای شبیه به (۱۲) می‌رسیم که درآنجا p'' مساوی باواحد باشد، و این به‌معنای آنست که می‌توان p رابه‌صورت مجموع مربعهای ۴ عدد نوشت . رابطهٔ (۷) به‌خوبی نشان می‌دهد که ممکن نیست p'' برابر باصفر باشد.

اکنون می‌توانیم تجزیهٔ عددهای اولی را ، که به‌صورت ۴n + ۳ هستند، به‌مجموع مربعها، مورد بررسی قرار دهیم. روشن است که این عددها، نمی‌توانند برابر با مجموع دو مربع کامل باشند، زیرا اگر داشته باشیم :

$$t^{۲}+u^{۲}=p \qquad (۱۳)$$

که درآن p عددی است اول، نتیجه می‌شود:

$$t^{۲}\equiv\alpha \qquad (\mathrm{mod.}\,p)$$

$$u^{۲}\equiv-\alpha \qquad (\mathrm{mod.}\,p)$$

که درآن α عددی است درست. بنابراین α و $-\alpha$ ، هردوماندهٔ مربعی p خواهند بود و بالاخره ۱- هم مانده‌می‌شود واین به‌معنای آنست که p به‌صورت ۴n+۱ می‌باشد.

در عوض خواهیم دید که تمام عددهای اول p ، که به‌صورت ۴n+۳ باشند ، مساوی مجموع ۴ مربع ویا احتمالا مساوی با مجموع ۳ مربع کامل خواهند بود .

فرض کنیم ، p عددی اول و به‌صورت ۴n + ۳ باشد، می‌دانیم که اگرعددهای کوچکتر یا مساوی ۴n+۳ را بنویسیم، رشتهٔ این عددها شامل مانده‌ها و غیر مانده‌ها خواهد بود. منتهی n تغییرعلامت وجود خواهد داشت، یعنی مانده پشت‌سر غیرمانده و یا برعکس خواهد بود .

بنابراین، لااقل یك ماندهٔ a بعد از یك غیرماندهٔ $a+۱$ خواهد بود، ولی همانطورکه می‌دانیم ۱ — یك غیر مانده از عددهای به‌صورت $۴n+۳$ می‌باشد، حاصلضرب ۱ — در $a+۱$ یعنی $-a-۱$ یك مانده می‌شود. بنابراین عددهایی مثل t و u وجود دارند به‌طوریکه داشته باشیم:

$$t^{۲} \equiv a \qquad (mod.p) \qquad (۱۱)$$

$$u^{۲} \equiv -a-۱ \quad (mod.p) \qquad (۱۲)$$

که ازآنجا نتیجه می‌شود:

$$t^{۲}+u^{۲}+۱ \equiv ۰ \;(mod.p) \qquad (۱۳)$$

یعنی عدد اول p، مجموع سه مربع کامل را عاد می‌کند وچون می‌دانیم که‌نمی‌تواند مساوی‌مجموع دومربع کامل باشد، مساوی مجموع‌مربعهای ۳ یا ۴ عدد خواهد شد.

به‌این ترتیب، عددهای اول غیرزوج مساوی با مجموع مربعهای ۲عددیا ۴عدد (و احتمالا ۳عدد) خواهند بود، وقتی که به‌صورت $۴n+۱$ ویا $۴n+۳$ باشند. از آنجا که عدد ۲ مساوی مجموع دو مربع است $(۱+۱)$ نتیجه می‌شودکه هرعدد مساوی با مجموع مربعهای ۴ عدد و یا کمتر خواهد بود، زیرا هرعدد برابر است با حاصلضرب عاملهایی که یا مربع‌کامل‌اند ویا برابرمجموع مربعهای ۲، ۳ ویا ۴ عدد.

اگر یك عدد، به‌جزعامل ۲ ، تنها شامل عاملهای اولی به‌صورت $۴n+۱$ باشد، مساوی مجموع دو مربع (ویا بهتر مربع‌کامل) خواهد بود، ولی اگریك یا چند عامل اول به‌صورت $۴n+۳$ داشته باشد،عدد مساوی مجموع دومربع نخواهد شد، مگراینکه عاملهای اول به‌صورت

$4n+3$ با توان زوج باشند. روشن است که اگر داشته باشیم:

$$a^2+b^2=c$$

می‌توان عدد درست m را درنظر گرفت به‌طوریکه داشته باشیم:

$$(ma)^2+(mb)^2=m^2c$$

و روشن است درحالتی‌که c برابر مجموع مربعهای دوعدد باشد، m^2c هم برابرمجموع دومربع خواهد بود.

می‌توان ملاحظه کرد حاصلضرب عاملهای اول فرد به‌صورت $4n+1$ هستند، وقتی‌که تعداد عاملهایی‌که به‌صورت $4n+3$ می‌باشد (چه عاملهایی مساوی وچه عاملهای مختلف) زوج باشد، زیرا داریم:

$$(4n+3)(4n'+3)=4(4nn'+3n+3n'+2)+1$$

با این تفاوت که عددهای غیراول به‌صورت $4n+1$، وقتی که دارای عاملهای به‌صورت $4n+3$ باشند، نمی‌توانند برابر مجموع دو مربع کامل نوشته شوند، بلکه برابرمجموع چهارمربع خواهندبود: مانند عددهای ۲۱ و ۳۳ و ۵۵.

۲۶. تعداد تبدیلهای به‌مجموع ۴ مربع. بی‌مناسبت نیست که دربارهٔ تعداد ممکنهٔ تبدیل یك عدد به۴ مربع کامل هم تصوری داشته باشیم. قبلا یادآوری می‌کنیم که اگر بعضی از عددهای اول، تنهابه‌یك صورت به‌مجموع ۴ مربع تبدیل می‌شوند، درعوض عددهای اول‌دیگری هم هستندکه می‌توانند به‌صورتهای مختلفی به‌مجموع مربعهای ۴ عدد تبدیل شوند. مثلا:

$$۳۱ = ۲۵ + ۴ + ۱ + ۱ = ۹ + ۹ + ۹ + ۴$$
$$۴۳ = ۲۵ + ۹ + ۹ = ۱۶ + ۹ + ۹ + ۹$$

حاصلضرب دوعامل اول را درنظر می‌گیریم، که هر یك از آنها تنها بەیك صورت بەمجموع مربعهای ۴ عدد قابل تبدیل باشد .

فرض می‌کنیم:

$$\begin{cases} p = a^۲ + b^۲ + c^۲ + d^۲ \\ p' = \alpha^۲ + \beta^۲ + \gamma^۲ + \delta^۲ \end{cases}$$

و داریم:

$$pp' = A^۲ + B^۲ + C^۲ + D^۲$$

که درآن :

$$\begin{cases} A = a\alpha + b\beta + c\gamma + d\delta \\ B = a\beta - b\alpha + c\delta - d\gamma \\ C = a\gamma - c\alpha + d\beta - b\delta \\ D = a\delta - d\alpha + b\gamma - c\beta \end{cases}$$

قبلا تعداد مقادیر ممکنهٔ A را جستجو می‌کنیم . فرض می‌کنیم که عددهای a، b، c، d، α، β، γ و δ ، عددهایی مثبت باشند . می‌توان درA جای حروفهایα، β، γ و δ را نسبت بەa، b، c و d عوض کرد و ۲۴ = !۴ تبدیل بدست‌آورد و درنتیجه ۲۴ مقدارمختلف برای Aمشخص کرد. این حکم بەطور مطلق روشن نیست. زیرا ۲۴ مقدار A تنها به ۸

متغیر a، b، c، d، α، β، γ و δ بستگی دارد. با وجود این می‌توان به‌ـ سادگی مقادیرخاصی برای a، b، c، d، α، β، γ و δ پیداکردکه به‌ازای آنها ۲۴ مقدار A با هم فرق داشته باشند . در اینجا مثال ساده‌ای ذکر می‌کنیم که در آن مجموعهای $a^2+b^2+c^2+d^2$ و $\alpha^2+\beta^2+\gamma^2+\delta^2$ عددهایی اول نیستند، ولی می‌تواند ما را متقاعدکند که اگر a، b، c، d، α، β، γ و δ به‌نحو مناسب انتخاب شوند ، ۲۴ مقداری که برای A بدست می‌آید با هم فرق خـواهند داشت. کافی است a، b، c و d را ۴ عدد نامساوی وکوچکتر از ۱۰ انتخاب‌کنیم وبرای α، β، γ و δ توانهای نامساوی از ۱۰ (که دربین آنها ۱ را هم می‌توان در نظرگـرفت، زیرا توان صفرعدد ۱۰ می‌باشد) .

به‌عنوان مثال چنین درنظر می‌گیریم:

$$\begin{cases} a=1 \quad b=2 \quad c=3 \quad d=4 \\ \alpha=10^3 \quad \beta=10^2 \quad \gamma=10 \quad \delta=1 \end{cases} \qquad (2)$$

مقدار A، در اینصورت برابر ۱۲۳۴ خواهد شد وبا تبدیل ۴ رقم این عدد ۲۴ مقدار مختلف برای A بدست می‌آید.

به‌سادگی می‌توان دیدکه هـر یك از مقادیر بدست آمدهٔ A با دو دستگاه از مقادیر مختلف BCD تطبیق می‌کند، مثلا اگر مقادیر(۲) را درنظر بگیریم و اگر آنها را در رابطـه‌های (۱) بگـذاریم برای ۱۲۳۴ خواهیم داشت:

$$\begin{cases} A=۱۲۳۴ \\ B=۱۰۳-۲۰۴۰ \\ C=۴۱۰-۳۰۰۲ \\ D=۲۱-۴۳۰۰ \end{cases} \qquad (۳)$$

اما می‌توان‌بدون تغییرمقدارA، هردومقدارa و α را به‌قرینه‌های آنها $-a$ و $-\alpha$ تغییرداد، در اینصورت مقادیرزیر را خواهیم داشت:

$$\begin{cases} A'=۱۲۳۴=A \\ B'=۲۰۰۳-۴۰ \\ C'=۳۴۰۰-۱۲ \\ D'=۴۰۲۰-۳۰۱ \end{cases} \qquad (۴)$$

که با مقادیر (۳) مختلف‌اند.

به‌همین ترتیب، می‌توان ۲۴ تبدیل ۴ عدد a، b، c و d (دراینجا ۱، ۲، ۳ و ۴) را درنظرگرفت و برای هریك علامت a وα را باهم‌تغییر داد. در اینصورت ۴۸ نوع مختلف از مجموع مربعهای ۴ عدد بدست می‌آید، از این ۴۸نوع مختلف، دوبه‌دومقادیربرابر A دارند وبنابراین ۲۴ تساوی به‌صورت زیر خواهیم داشت:

$$B^۲+C^۲+D^۲=B'^۲+C'^۲+D'^۲ \qquad (۵)$$

و این به‌معنای‌آنست‌که ۲۴عدد بدست می‌آیدکه هریك ازآنهامی‌توانند

به‌دو صورت مختلف به‌مجموع مربعهای ۳ عدد تبدیل شود.

با تغییر a به a− و α به α− رابطهٔ (۱) چنین خواهد شد:

$$\begin{cases} A' = A \\ B' = -(a\beta - b\alpha) + c\delta - d\gamma \\ C' = -(a\gamma - c\alpha) + d\beta - b\delta \\ D' = -(a\delta - d\alpha) + b\gamma - c\beta \end{cases} \qquad (۶)$$

و رابطهٔ (۵) نتیجه‌ای از اتحاد زیرخواهد بود:

$$(a\beta - b\alpha)(c\delta - d\gamma) + (a\gamma - c\alpha)(d\beta - b\delta) + (a\delta - d\alpha)(b\gamma - c\beta) = 0 \qquad (۷)$$

ولی با تبدیل a، b، c و d در رابطه‌های (۱) و (۶)، همه نوعهای $A^2 + B^2 + C^2 + D^2$ ازیك مجموع مربعهای ۴عدد بدست نمی‌آید، درحقیقت می‌توان در رابطهٔ (۱) مثلا به‌جای d قرینهٔ آن d− را قرار داد و رابطهٔ زیررا بدست آورد:

$$\begin{cases} A'' = a\alpha + b\beta + c\gamma - d\delta \\ B'' = a\beta - b\alpha + c\delta + d\gamma \\ C'' = a\gamma - c\alpha - d\beta - b\delta \\ D'' = a\delta + d\alpha + b\gamma - c\beta \end{cases} \qquad (۸)$$

ملاحظه می‌شود که اگر همانطورکه ما فرض کردیم، عددهای a، b، c، d، α، β، γ و δ مثبت باشند، در عددهای A''، B''، C'' و D''، ۳ عدد باهمان علامت ویك عدد باعلامت مخالف است. بالاخره اگرتمام

تبدیلهای حرفهای a، b، c و d را انجام دهیم به‌دو دستگاه شبیه (۸) خواهیم رسید که سطرهای آنها به‌طورساده مبدل یکدیگرند به‌نحوی که یك نتیجه را می‌دهند و این چیزی است که با رابطه‌های (۱) و (۶)، نمی‌توان به‌آن رسید.

می‌توان فکر کرد که در رابطهٔ (۸) از یکطرف می‌توان ۲۴ تبدیل از ۴ حرف a، b، c و d انجام داد و از طرف دیگربرای هریك از این تبدیلها، علامت یکی از ۸ حرف a، b، c، d، α، β، γ و δ را تغییر داد. درحقیقت برای بدست‌آوردن (۹) و (۱۰) تنها باید علامتهای d و δ را تغییر داد و به‌این ترتیب ۲۴ × ۸ جدول از نوع (۹) و (۱۰) خواهیم داشت. ولی همانطور که قبلا هم گفتیم باید به‌این نکته توجه کرد که در هریك از ۴ سطر این جدولها در طرف دوم سه جمله با یك علامت وجود دارد و تنها یك علامت یك جملهٔ آن فرق می‌کند، به‌نحوی که جدولهائی بدست می‌آید که سطر دوم، سوم ویاچهارم آنها ازجدولهای (۹) و (۱۰) جای سطراول را درجدول (۸) اشغال می‌کنند وبا هم متحدند. بنابراین بایدتعدادجدولهای‌بدست‌آمده‌را بر۴تقسیم کرد، زیرا هریك ازاین‌جدولها ۴ مرتبه تکرار شده‌اندکه تنها جای سطرهای‌آنها باهم عوض شده است.

بنابراین از رابطه‌های (۸) تنها ۴۸ = ۲۴ × ۲ (و نه ۲۴ × ۸) جدول بدست می‌آیدکه باید به ۴۸عددی‌که اکنون بدست‌آوردیم‌اضافه شود. و این به‌معنای آنست که مجموع ۴ مربع می‌تواند به ۹۶ حالت مختلف به‌مجموع مربعهای ۴ عدد تبدیل شود.

مادقت‌دراین‌مطلب‌را به‌عهدهٔ خواننده‌می‌گذاریم که‌سایر تبدیلهایی که ممکن است درهریك ازاین۹۶ حالت مختلف برای A، B، C و D انجام داد منجربه‌تغییر ساده‌ای درترتیب این عددها خواهد شد.

٦

عددهای موهومی

۲۷. تعریف. اهمیت عددهای موهومی در جبر و آنالیز برکسی پوشیده‌نیست، این‌عددها به‌خصوص راه را برای‌کشف خاصیتهای‌عمومی معادله‌های جبری بازکردندکه مهمترین آنها اینست که هرچند جمله‌ای حقیقی، می‌تواند به‌عاملهای حقیقی درجه اول و درجه دوم تجزیه شود.

بنابراین واردکردن متغیرموهومی در نظریهٔ عددهای اول، امری طبیعی است و ما خواهیم دیدکه دخالت این عددها چه نقش اساسی در مطالعهٔ عددهای اول می‌تواند داشته باشد.

قبلا چند تعریف را می‌آوریم. می‌دانیم که هر عبارت به‌صورت $a + bi$ را ، که درآن a و b عددهایی حقیقی باشند ، عدد موهومی می‌نامند. حرف i ، بنابرتعریف، معرف‌واحد موهومی است، یعنی‌عددی قراردادی است‌که در رابطهٔ اصلی زیرصدق می‌کند:

$$i^۲ = -۱ \qquad (۱)$$

عملهای مربوط به‌عددهای موهومی ، مثل عملهای جبری مربوط به‌چند جمله‌ایهای حقیقی نسبت به i انجام می‌گیرد، با این شرط‌اضافی که رابطهٔ (۱) و رابطه‌هایی را که از ضرب دوطرف این رابطه در توان غیرمشخصی از i بدست می‌آید درنظر می‌گیرند.

۲۸. عددهای موهومی درست. بخش‌پذیری. یک عدد موهومی را درست‌گوییم (وباید آنرا موهومی درست‌گفت تا ازهرگونه اشتباهی جلوگیری شود)، وقتی‌که عددهای a و b درست باشند. اگر a برابرصفر باشد، عددموهومی خالص، و اگر b برابرصفر باشد، عددحقیقی خواهیم داشت.

مجموع ، تفاضل و حاصلضرب دو عدد موهومی درست ، خود یك عدد موهومی درست است (و درحالت خاص می‌تواند یك عدد حقیقی باشد) .

a^2+b^2 را پایه « norme » عدد موهومی درست $a+bi$ گوییم:

برای تعیین‌خارج قسمت دوعدد موهومی درست $a+bi$ و $c+di$ باید عدد موهومی $x+yi$ را چنان پیدا کرد که داشته باشیم:

$$(x+yi)(c+di)=a+bi \qquad (1)$$

با مساوی قراردادن قسمتهای حقیقی و قسمتهای موهومی در دو طرف تساوی ، دو معادلهٔ زیررا خواهیم داشت:

$$\begin{cases} cx-dy=a \\ dx+cy=b \end{cases} \qquad (2)$$

که درنتیجه بدست می‌آید:

$$x=\frac{ac+bd}{c^2+d^2} \quad \text{و} \quad y=\frac{bc-ad}{c^2+d^2} \qquad (3)$$

عدد موهومی $x+yi$ تنها وقتی درست است که هر دوعدد x و y

درست باشند، در اینصورت گویند $a + bi$ بر $c+di$ بخش‌پذیر است و درغیر اینصورت بخش‌پذیر نیست.

نظریهٔ بخش‌پذیری‌عددهای درست(که نظریهٔ عددهای اول براساس آن گذاشته شده است) ، براساس این عمل است که اگر a بر b بخش‌پذیر نباشد، می‌توان نوشت:

$$a=bq+r \qquad (۴)$$

که در آن خارج قسمت q عددی است درست و باقیماندهٔ r هم عددی است درست و کوچکتر از b ، ومی‌دانیم که ازهمین جا نظریهٔ بزرگترین مقسوم‌علیه مشترك را نتیجه گرفته‌اند.

اکنون می‌خواهیم این تساوی را درمورد عددهای موهومی‌درست مورد بررسی قرار دهیم. طبق تعریف ، عدد درست $a + bi$ را بزرگتر ویا کوچکتر از عدد درست $c + di$ گوییم وقتی‌که «پایهٔ» $a + bi$ بزرگتر یا کوچکتر از «پایهٔ» $c +di$ باشد . عددهای درست مخالف صفر که کوچکترین «پایه» را دارند عبارتند از: ۱، ۱ــ ، i و$-i$ــ که پایهٔ همهٔ آنهابرابرواحد است. این عددهاباهم برابرنیستند ولی‌ضمناً نمی‌توان گفت که یکی کوچکتر یا بزرگتر از دیگری است. باید هر چهارعدد را به‌عنوان‌واحد به‌حساب‌آورد، که هرعدد درست $a + bi$ برآنهابخش‌پذیر خواهد بود. خارج‌قسمت $a + bi$ براین ۴ واحد عبارتست از $a+bi$ ، $-a-bi$ ، $-ai+b$ و$ai-b$. این چهار خارج قسمت ، برابر با هم نیستند، ولی از لحاظ نظریهٔ بخش‌پذیری هم‌ارزند، زیرا اگر $a + bi$ بر $c + di$ بخش‌پذیر باشد، $ai - b$ هم بر $ci - d$ وهمچنین بر $c+di$ بخش‌پذیر خواهد بود. این ۴عدد را عددهای انباز nombres associès

گویند. حال دوباره به‌معادلهٔ اصلی تقسیم (۱) برگردیم.

فرض می‌کنیم که x و y عددهایی درست نیستند، ولی اگر a^2+b^2 را بزرگتر از c^2+d^2 درنظر بگیریم x^2+y^2 بزرگتر از واحد خواهد شد.

اگر دوعدد مفروض x و y را غیردرست فرض کنیم، می‌توان دوعدد درست m و n را چنان پیدا کرد که داشته باشیم:

$$x-m=r_1 \qquad y-n=r_2 \qquad (5)$$

عددهای مثبت یا منفی r_1 و r_2 کوچکتر یا حداکثر برابر با $\frac{1}{2}$ هستند.

بادرنظرگرفتن رابطه‌های (۵)، رابطهٔ (۱) به‌صورت زیر درمی‌آید:

$$a+bi=(c+di)(m+ni)+(c+di)(r_1+r_2i) \qquad (6)$$

که می‌توان آنرا چنین نوشت:

$$a+bi=(c+di)(m+ni)+\rho_1+\rho_2i \qquad (7)$$

که درآن:

$$\rho_1+\rho_2i=cr_1-dr_2+i(dr_1+cr_2)$$

«پایه» $\rho_1+\rho_2i$ عبارتست از:

$$(c^2+d^2)(r_1^2+r_2^2) \leqslant \frac{1}{2}(c^2+d^2)$$

زیرا هریك ازعددهای $r_1^2+r_2^2$ از $\frac{1}{4}$ کوچکترند.

اکنون می‌توان به‌وسیلهٔ رابطهٔ (۷)، که با نامساوی (۸) تکمیل

می‌شود ، نظریهٔ بخش‌پذیری عددهای موهومی درست را شبیه نمونهٔ عددهای درست حقیقی تنظیم کرد.

در حقیقت ، از رابطهٔ (۷) روشن می‌شود ، هرعدد موهومی که $a+bi$ و $c+di$ را عاد کند. $\rho_1+\rho_2 i$ را هم عاد خواهد کرد و برعکس مقسوم‌علیه‌های مشترک $a+bi$ و $c+di$ مقسوم‌علیه‌های مشترک $c+di$ و $\rho_1+\rho_2 i$ نیز خواهند بود. اکنون می‌توان همین عمل را برای عددهای $c+di$ و $\rho_1+\rho_2 i$ تکرار کرد، باقیماندهٔ تقسیم $c+di$ را بر $\rho_1+\rho_2 i$ برابر $\rho_3+\rho_4 i$ می‌گیریم که در آن $\rho_3^2+\rho_4^2$ کوچکتر از نصف $\rho_1^2+\rho_2^2$ خواهد بود. اگر به‌همین نحو ادامه دهیم، بالاخره به‌جایی می‌رسیم که در باقیمانده‌پایه‌ای برابر صفر و یا واحد داشته‌باشیم، زیرا پایه‌های باقیمانده‌ها یك رشتهٔ صحیح نزولی تشکیل می‌دهند (هر یك از آنها از نصف قبلی کوچکتر است) . اگر باقیمانده‌ای مساوی واحد بدست آید (یعنی ۱، ۱ — ، i یا $-i$) در اینصورت عددهای مفروض، مقسوم‌علیه مشترکی جز واحد ندارند و در اینصورت گویند که آنها نسبت به‌هم اولند. و اگر برعکس، به باقیماندهٔ صفر برسیم (که بر همهٔ عددها بخش‌پذیر است)، مقسوم‌علیه‌های مشترك عددهای مفروض همان مقسوم علیه‌های آخرین مقسوم علیه در تقسیمهای متوالی خواهند بود. این آخرین مقسوم علیه، بزرگترین مقسوم‌علیه مشترك عددهای مفروض خواهد بود و تمام مقسوم علیه‌های مشترك دوعدد ، مقسوم علیه‌های همین بزرگترین مقسوم‌علیه مشترك می‌باشد.

اگر یکی از عددهای مفروض، اول باشد (یعنی جز خودش و واحد مقسوم‌علیه دیگری نداشته باشد) ، بزرگترین مقسوم علیه مشترك یك عدد غیرمشخص $a+bi$ وعدد اول $p=p_1+p_2 i$ نمی‌تواند چیزی جز ۱ یا p باشد. زیرا ۱ و p تنها مقسوم علیه‌های عدد p هستند ؛ بنابراین عدد

اول p یا مقسوم‌علیهی از عدد مفروض $a + bi$ است و یا نسبت به‌آن اول است.

به‌همین شیوه می‌توان قضیه‌های مربوط به‌تجزیهٔ یك عدد را به عاملهای اول، و اینکه این تجزیه منحصر به‌فرد است اثبات‌کرد (با این شرط اضافی که هردو عامل را که در تقسیم بریکدیگر ، یکی از ۴ واحد را بدست می‌آوریم هم‌ارز بدانیم) .

۲۹. عددهای اول موهومی . $a + bi$ را عدد اول موهومی فرض‌می‌کنیم، یعنی عددی‌که مقسوم‌علیهی جزخود و واحد نداشته‌باشد. در اینصورت ثابت خواهیم‌کردکه پایهٔ‌آن $a^2 + b^2$ هم عدد حقیقی‌اولی خواهدبود. درحقیقت، اگر $a^2 + b^2$ عدد اول نباشد، می‌توان‌آنرا برابر دوعامل مخالف واحد دانست، به‌طوریکه یکی از آنها، p ، عددی اول باشد. در اینصورت داریم:

$$a^2+b^2=pq \qquad (1)$$

یعنی :

$$(a+bi)(a-bi)=pq \qquad (2)$$

عدد اول p نمی‌تواند حاصلضرب $(a+bi)(a-bi)$ را عاد کند، مگراینکه لااقل یکی ازاین دوعامل‌را عادکند، ازطرف دیگرعددموهومی مختلط‌به‌شکل $a + bi$ نمی‌تواند برعدد حقیقی p بخش‌پذیر باشند، مگر اینکه هردوعدد a و b بر p بخش‌پذیر باشند. بنابراین p هردوعدد a و b را عاد می‌کند و درنتیجه $a + bi$ که بر p بخش‌پذیر می‌شود، اول نخواهد بود و این مخالف با فرض ماست.

ولی می‌دانیم که یک‌عدد اول حقیقی ، تنها درحالتی که به‌صورت ۴n+۱ باشد به‌صورت مجموع مربعهای دوعدد درست قابل تبدیل است و درنتیجه چنین عدد اولی مانند p قابل تجزیه به‌دوعامل اول موهومی خواهد بود:

$$p = a^2 + b^2 = (a+bi)(a-bi) \qquad (۳)$$

این عاملهای موهومی اول هستند، زیرا اگرداشته باشیم:

$$a+bi = (c+di)(e+fi)$$

نتیجه می‌گیریم:

$$a^2+b^2 = (c^2+d^2)(e^2+f^2)$$

و این به‌معنای آنست که a^2+b^2 عددی اول نیست.

دیده می‌شود که از نظرعددهای موهومی، سه نوع عدد اول‌وجود دارد:

۱. عددهای حقیقی اول به‌صورت ۴n+۳

۲. عددهای‌موهومی $a \pm bi$ که درآن a^2+b^2 عدد اول‌حقیقی به‌صورت ۴n+۱ است.

۳. عدد $1+i$ (و عدد انباز آن) که مقسوم علیه‌های عدد ۲ هستند .

۳۰. مجموع مربعهای دوعدد. با استفاده از عددهای‌موهومی درست، می‌توان مسالهٔ‌مربوط به‌تبدیل‌یک‌عدد درست‌را به‌مجموع‌مربعهای دو عدد تکمیل کرد.

m را عدد درست غیرمشخصی فرض می‌کنیم که قابل تبدیل به‌دو مربع کامل باشد:

$$m=a^{2}+b^{2} \qquad (1)$$

می‌توان نوشت:

$$m=(a+bi)(a-bi) \qquad (2)$$

که درآن عدد $a+bi$ می‌تواند تنها به‌یك حالت، به‌صورت ضرب عاملهای اول(حقیقی یا موهومی) تجزیه شود. حاصلضرب تمام عاملهای اول‌حقیقی‌را A فرض‌می‌کنیم (عاملهایی‌که همهٔ آنها به‌صورت $4n+3$ هستند) و می‌نویسیم:

$$a+bi=A(a_1+b_1i)^{C_1}(a_2+b_2i)^{C_2}\cdots \qquad (3)$$
$$\cdots(a_k+b_ki)^{C_k}$$

که درآن a_k و b_k عددهای درست مثبت یا منفی و مخالف صفر و C_k مثبت ومخالف صفراست. درحقیقت اگر a_1 یا b_1 برابرصفر باشد، عامل a_1+ib_1 می‌تواند به‌یك عـامل حقیقی تبدیل شود که در A نشان داده شده است.

اگر در رابطهٔ (۳)، i را به $-i$ تبدیل کنیم و سپس دوتساوی را درهم ضرب‌کنیم خواهیم داشت:

$$m=A^{2}(a_1^{2}+b_1^{2})^{C_1}(a_2^{2}+b_2^{2})^{C_2}\cdots \qquad (4)$$
$$\cdots(a_k^{2}+b_k^{2})^{C_k}$$

. ازاینجا نتیجه می‌شودکه m برابر است با حاصلضرب مربع عدد A (که می‌تواند برابرواحد باشد ، ولی درحالتی‌که برابر واحد نیست، حاصلضرب عاملهایی به‌صورت ۴n+۳ خواهدبود) درتوانهای‌اختیاری عدد اول ۲ وعددهای اول به‌صورت ۴n+۱ . اگرتوانهای C_1، C_2...و C_k بزرگتر از یك باشند. می‌توان‌آنها را مجموع یك عدد زوج باصفر با یك فرض کرد و دراینصورت می‌توان نوشت:

$$m=A^۲B^۲(a_۱^۲+b_۱^۲)\ \dots\ (a_h^۲+b_h^۲) \qquad (۵)$$

زیرا توانهائی از C را که زوج هستند وبالاخره به‌صفر منتهی‌می‌شوند، نباید درنظرگرفت وماآنهارا در B نشان داده‌ایم و بنابراین‌حاصلضرب AB می‌تواند هرعدد غیرمشخص باشد .

باکمك رابطهٔ (۵) می‌توان ثابت‌کردکه تعداد نوعهای تبدیل عدد m به‌مجموع مربعهای دو عـدد نمی‌تواند از $۲^{h-۱}$ تجاوز کند . برای سهولت‌کارفرض می‌کنیم‌که m حاصلضربی از سه عامل باشد:

$$m=(a_۱^۲+b_۱^۲)\,(a_۲^۲+b_۲^۲)(a_۳^۲+b_۳^۲) \qquad (۶)$$

همچنین می‌توان نوشت:

$$m=(a_۱+b_۱i)\,(a_۲+b_۲i)\,(a_۳+b_۳i)\times$$
$$\times(a_۱-b_۱i)\,(a_۲-b_۲i)\,(a_۳-b_۳i) \qquad (۷)$$

به‌سادگی دیده می‌شودکه حاصلضرب ۶ عامل موهومی را که دو به‌دو جفت هستند، می‌توان به ۴حـالت به‌صورت حاصلضرب دو عاملی نوشت‌که درهریك ازآنها سه عامل موهومی جفت باشند. دسته‌ای را که شامل $a_۱+b_۱i$ باشد دستهٔ اول و دستهٔ شامل $a_۱-b_۱i$ را دستهٔ دوم

می‌نامیم. برای تکمیل دستهٔ اول از یك طرف بین a_2+b_2i و a_2-b_2i و از طرف دیگر بین a_3+b_3i و a_3-b_3i باید انتخاب کـرد ، یعنی می‌توانیم ابتدا دوحالت داشته باشیم و برای هریك از این دو حالت هم دو انتخاب می‌توان انجام داد و بنابراین به‌طـورکلی 2^2 امکان وجـود دارد و این همان 2^{n-1} است، وقتی‌که $n=3$ باشد (آنطورکه دررابطهٔ (۶) درنظرگرفتیم).

اکنون می‌توانیم حاصلضربهای ۴ حالت ممکن را برای دستهٔاول عاملها محاسبه‌کنیم:

$$\left\{\begin{array}{l}(a_1+b_1i)(a_2+b_2i)(a_3+b_3i)=\alpha_1+\beta_1i\\(a_1+b_1i)(a_2-b_2i)(a_3+b_3i)=\alpha_2+\beta_2i\\(a_1+b_1i)(a_2+b_2i)(a_3-b_3i)=\alpha_3+\beta_3i\\(a_1+b_1i)(a_2-b_2i)(a_3-b_3i)=\alpha_4+\beta_4i\end{array}\right.\qquad(8)$$

و به‌این ترتیب ۴ حالت مختلف تبدیل m را بدست می‌آوریم:

$$\begin{aligned}m=\alpha_1^2+\beta_1^2=\alpha_2^2+\beta_2^2=\alpha_3^2+\beta_3^2\\=\alpha_4^2+\beta_4^2\qquad(9)\end{aligned}$$

این ۴ نوع تبدیل کاملا با هم مختلف‌اند ، به‌شرطی که a_1+b_1i و a_2+b_2i و a_3+b_3i مختلف باشند، به‌این معنا که دو تای آنها انباز نباشد.

مثلا داریم:

$$5\times13\times17=32^2+9^2=33^2+4^2=31^2+12^2=24^2+23^2$$

وحالت دیگری برای تبدیل این‌عدد به‌مجموع مربعهای دوعدد نمی‌توان بدست آورد.

دیده می‌شود که نتیجه‌های مربوط به‌مجموعهای مربعهای دوعدد کاملا با نتیجه‌هایی که برای مجموعهای مربعهای ۴ عدد بدست آوردیم فرق دارند. برای مجموعهای مربعهای ۴ عدد با نظریهٔ عددهای‌موهومی نمی‌توان ارتباطی پیدا کرد.

گراس Grâce از این نظریه نتیجه‌ای بسیار با ارزشی بدست آورده است.

۷

مقسوم علیه‌های درست
چند جمله‌ایها

۳۱. چند جمله‌ایهای با ضریبهای درست. مـا در اینجـا منحصراً دربارهٔ چند جمله‌ایهای با ضریبهای درست گفتگو خواهیم کرد و ضمناً متغیر ویا متغیرها را هم تنها به‌ازای مقادیر درست در نظرخواهیم گـرفت . قبلا به‌چند جمله‌ایهایی که تنهـا به‌یك متغیر x بستگی دارند می‌پردازیم. فرض کنید:

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a^n \qquad (1)$$

گوییم که این چند جمله‌ای بر چند جملـه‌ای با ضریبهای درست g(x) نسبت به مدول p بخش‌پذیر است، وقتی کـه چند جمله‌ای با ضریبهای درست، مثل h(x) وجود داشته‌باشد، به‌نحوی که به‌ازای هرمقدار x داشته باشیم:

$$f(x)\equiv g(x).h(x) \qquad (\mathrm{mod.}p) \qquad (2)$$

درحالتی که f(x) به‌معنای جبری بر g(x) بخش‌پذیر وخارج‌قسمت هم باضریبهای درست باشد، تساوی جبری زیر را خواهیم داشت:

$$f(x)=g(x).h(x) \qquad (3)$$

و دراین حالت همنهشتی (۲) به‌ازای هرمقدار دلخواه عدد اول p صادق خواهد بود.

عددصحیح m را « مقسوم علیه آشکار » (diviseur apparent) چند جمله‌ای $f(x)$ گوییم، وقتی‌که اتحاد زیررا داشته باشیم:

$$f(x)=m.h(x) \qquad (۴)$$

که در آن ضریبهای $h(x)$ ، عددهایی درست هستند و بنابراین ، تمام ضریبهای $f(x)$ بر m بخش‌پذیرخواهند بود. روشن است‌که تمام‌عددهای اولی هم که m را عاد می‌کنند مقسوم علیه آشکار $f(x)$ خواهند بود ، می‌توان m را بزرگترین مقسوم علیه مشترك ضریبهای $f(x)$ گرفت ، در این حالت روشن است‌که چند جمله‌ای $h(x)$ ، مقسوم علیه آشکاری نخواهد داشت.

وقتی‌که چند جمله‌ای، دارای مقسوم علیه‌آشکار p باشد، روشن است‌که به‌ازای هرمقدار درست x خواهیم داشت:

$$f(x)\equiv ۰ \qquad (\mathrm{mod}.p)$$

همچنین در این‌حالت می‌توان گفت که x هرچه باشد ، p، چندجمله‌ای $f(x)$ را عاد خواهد کرد.

بنابراین می‌توان مسالهٔ زیررا طرح کرد:

چند جمله‌ای $f(x)$ و عدد اولی مانند p مفروض است ، اگر p مقسوم‌علیه‌آشکار $f(x)$ نباشد، آیا ممکن است که بااین وجود $f(x)$ به‌ازای تمام مقادیر x بر p بخش‌پذیر باشد؟

دراین صورت می‌توان گفت که عدد اول p مقسوم علیه ناآشکار ویا مقسوم علیه مخفی چند جمله‌ای $f(x)$ است.

قبلا یادآور می‌شویم که کافی است مسالهٔ مقسوم علیه‌های‌مخفی را درمورد عددهای اول p و توانهای‌آنها بررسی‌کنیم، زیرا اگرعدد m

برابر با $p^{\alpha} q^{\beta} r^{\gamma}$ باشد، عددهای p و q و r اول هستند و برای اینکه $f(x)$ بر m بخش‌پذیر باشد، کافی است که بر p^{α}، q^{β} و r^{γ} بخش‌پذیر باشد.

قضیهٔ فرما نمونهٔ جالبی ازمقسوم‌علیه مخفی را به‌ما می‌دهد. طبق این قضیه می‌دانیم، وقتی‌که p عددی اول باشد به‌ازای هرمقدار دلخواه x داریم:

$$g(x)=x^{p}-x \equiv 0 \qquad (\mathrm{mod}.p) \qquad (5)$$

که درآن‌ضریبهای $g(x)$ برابر باواحدهستند و درنتیجه این‌چندجمله‌ای هیچ مقسوم‌علیه‌آشکاری ندارد، معهذا همیشه بر p بخش‌پذیر است واین همان مقسوم علیه مخفی است.

ما ثابت خواهیم‌کردکه برای بدست‌آوردن تمام مقسوم علیه‌های مخفی یك چند جمله‌ای غیرمشخص کافی است که قضیهٔ فرما و بعضی نتیجه‌های روشن‌مربوط به‌آن‌را (که‌ماهم اکنون‌شرح خواهیم‌داد) به‌کار بریم.

به‌عبارت دیگر قضیهٔ دیگری وجود ندارد که مستقل ازقضیهٔ فرما مقسوم‌علیه‌های مخفی‌را بشناساند. ازنظرجستجوی مقسوم‌علیه‌های‌مخفی قضیهٔ فرما آمادگی هیچگونه تعمیمی را ندارد.

۳۲. نتیجه‌های قضیهٔ فرما. برای بدست‌آوردن این نتیجه‌ها، تنها به‌حالتهای خاص و روشن زیر می‌پردازیم.

لم ۱. اگرحاصلضرب دوعامل m و n وعدد اولp مفروض‌باشند، وقتی‌که عامل m بر p^{α} و عامل n بر p^{β} بخش‌پذیر باشد، حاصلضرب

mn بر $p^{\alpha+\beta}$ بخش‌پذیر خواهد بود.

لم ۲. اگر هم m و هم n بر p^{α} بخش‌پذیر باشند، $m+n$ هم بر p^{α} بخش‌پذیر خواهد بود.

از دو لم بالا قضیه‌های زیررا نتیجه می‌گیریم:

قضیهٔ ۱. به‌ازای هرعدد اول p وهرتوان درست α همنهشتی‌زیر را خواهیم داشت:

$$(x^{p}-x)^{\alpha}\equiv 0 \qquad (\text{mod}.\, p^{\alpha}) \qquad (۶)$$

درحقیقت، طبق رابطهٔ (۵)، سمت چپ این رابطه حاصلضربی از α عامل بخش‌پذیر بر p می‌باشد.

قضیهٔ ۲. اگر چند جمله‌ایهای دلخواه $f_0(x)$ ، $f_1(x)$، $f_2(x)$، . . . ، $f_{\alpha}(x)$ را با ضریبهای درست و عدد اول دلخواه p را درنظر بگیریم، همنهشتی زیررا خواهیم داشت:

$$F(x)=p^{\alpha}f_0(x)+p^{\alpha-1}f_1(x)(x^{p}-x)+ \qquad (۷)$$

$$p^{\alpha-2}f_2(x)(x^{p}-x)^{2}+\ldots+p^{\alpha-k}f_k(x)(x^{p}-x)^{k}+$$

$$\ldots+f_{\alpha}(x)(x^{p}-x)^{\alpha}\equiv 0 \qquad (\text{mod}.\, p^{\alpha})$$

این قضیه به‌سادگی از قضیهٔ ۱ و لم‌های ۱ و۲ نتیجه می‌شود.

قضیهٔ ۳. هر چند جمله‌ای $F(x)$ را که p^{α} مقسوم‌علیه مخفی‌آن

باشد،می‌توان به‌شکل معینی به‌وسیلهٔ تساوی (۷) نشان داد، به‌شرطی‌که α کوچکتر از p باشد.

۳۳. اثبات قضیهٔ اصلی. این قضیه را با روش استقراء ثابت می‌کنیم ؛ برای اینکه مطمئن شویم که این قضیه برای تمام توانهای α درست‌است، ابتدا درستی‌آنرا به‌ازای $\alpha=1$ نشان می‌دهیم و سپس‌ثابت می‌کنیم‌که اگرقضیه برای α و تمام توانهای‌کوچکتر ازα درست باشد، برای توان $\alpha+1$ نیز درست خواهد بود و به‌این‌ترتیب قضیه برای تمام مقادیر α کوچکتر از p ثابت خواهد بود.

بنابراین باید ابتدا قضیهٔ ۲ را برای $\alpha=1$ ثابت کرد . با ساده کردن علامتها، رابطهٔ (۷) دراینحالت به‌صورت زیر درمی‌آید.

همنهشتی زیررا داریم:

$$F(x)=pf(x)+(x^p-x)\,g(x)\equiv 0 \pmod{p} \qquad (۸)$$

که در آن $f(x)$ و $g(x)$ چند جمله‌ایهای دلخواهی با ضریبهـای درست هستند . باید متقابلا ثابت کرد هرچند جمله‌ای $F(x)$ که p، مقسوم‌علیه مخفی‌آن باشد می‌تواند به‌صورت زیرنوشته شود :

$$F(x)=pf(x)+(x^p-x)\,g(x) \qquad (۹)$$

که درآن $f(x)$ و $g(x)$ چند جمله‌ایهایی با ضریبهای درست هستند.

چندجمله‌ای اختیاری$F(x)$ را باضریبهای‌درست درنظرمی‌گیریم، اگردرجهٔ این چند جمله‌ای بزرگترازp باشد، می‌توانیم‌آنرا به‌طورجبری بر x^p-x تقسیم‌کنیم، ضریب x^p در مقسوم علیه برابر با واحد است و بنابراین خارج قسمت و باقیماندهٔ تقسیم، چند جمله‌ایهای با ضریبهای

درست خواهند بود، یعنی اتحاد زیررا خواهیم داشت:

$$F(x)=(x^p-x)\,G(x)+H(x) \qquad (۱۰)$$

که درآن خارج قسمت $G(x)$ و باقیماندهٔ $H(x)$ چند جمله‌ایهایی با ضریبهای درست هستند و علاوه برآن درجهٔ $H(x)$ حداکثر برابر $p-۱$ می‌باشد.

رابطهٔ (۱۰) یك اتحاد جبری است و بنابراین به‌ازای هرمقدار دلخواه a تبدیل به‌یك تساوی می‌شود. اما اگر p را مقسوم علیه مخفی $F(x)$ فرض کنیم، $F(a)$ به‌ازای هرمقدار a بر p بخش‌پذیر خواهد بود. به‌ازای a داریم:

$$F(a)=(a^p-a)\,G(a)+H(a)\equiv ۰ \quad (\mathrm{mod}.p) \quad (۱۱)$$

اما طبق قضیهٔ فرما a^p-a بر p بخش‌پذیر است و بنابراین داریم:

$$H(a)\equiv ۰ \qquad (\mathrm{mod}.p) \qquad (۱۲)$$

گفتیم که درجهٔ چند جمله‌ای $H(x)$، حداکثر برابر $p-۱$ است و بنابراین می‌توانیم بنویسیم:

$$H(x)=a_۱x^{p-۱}+a_۲x^{p-۲}+\ldots+a_p \qquad (۱۳)$$

که درآن ضریبهای $a_۱$، $a_۲$، ...وa_p عددهای درستی هستند که می‌توانند برابرصفرهم باشند، اگراین ضریبها ازلحاظ قدرمطلق بزرگتر از p باشند، می‌توان ازتقسیم آنها بر p باقیمانده را بدست آورد که مسلماً از p کوچکتر خواهد بود. بنابراین می‌توانیم بنویسیم:

$$\begin{cases} a_1 = pq_1 + r_1 \\ a_2 = pq_2 + r_2 \\ \dots\dots\dots\dots\dots\dots \\ a_p = pq_p + r_p \end{cases} \qquad (۱۴)$$

که در آن خارج قسمتهای q_1، q_2، . . . و q_p عددهای درست، مثبت یا منفی و باقیمانده‌های r_1، r_2، . . . و r_p ازلحاظ قدرمطلق کوچکتراز p خواهند بود (باقیمانده‌ها را می‌توان مثبت فرض کرد، ولی این مطلب اهمیتی ندارد) .

با درنظرگرفتن رابطه‌های (۱۴) ، رابطهٔ (۱۳) به‌صورت زیر نوشته می‌شود:

$$H(x) = pQ(x) + R(x) \qquad (۱۵)$$

که درآن $Q(x)$ و $R(x)$ چند جمله‌ایهایی با ضریبهای درست هستند.

اگررابطهٔ (۱۵) را درنظر بگیریم ، رابطهٔ (۱۲) چنین می‌شود:

$$pQ(a) + R(a) \equiv 0 \qquad (\text{mod}.p)$$

به‌نحوی‌که به‌ازای هرمقدار a خواهیم داشت:

$$R(a) \equiv 0 \qquad (\text{mod}.p) \quad (۱۶)$$

ولی ضریبهای $R(x)$ کوچکتر از p هستند و ضمناً متباین با p، زیرا p عددی است اول (به‌شرطی‌که همهٔ ضریبها صفر نباشد)، بنابراین همنهشتی

$$R(x) \equiv 0 \qquad (\mathrm{mod}.p) \qquad (۱۷)$$

دارای $p-1$ ریشهٔ ۱ ، ۲ ، . . . و $p-1$ خواهد بود و از آنجا نتیجه می‌شود:

$$R(x) = \lambda(x-1)(x-2)\ldots(x-p+1)$$
$$\equiv (p^{p-1}-1) \qquad (\mathrm{mod}.p)$$

ولی همنهشتی (۱۷) باید به‌ازای $x=p$ به‌طورتساوی صادق باشد و بنابراین ضریب λ ،که باید کوچکتر از p باشد، برابرصفرمی‌شود و در نتیجه اتحاد زیر را خواهیم داشت:

$$R(x) = 0 \qquad (۱۷)$$

یعنی با توجه به‌رابطهٔ (۱۵) داریم:

$$H(x) = pQ(x) \qquad (۱۸)$$

و بنابراین رابطهٔ (۱۰) خواهد شد:

$$F(x) = (x^p - x)\, G(x) + pQ(x) \qquad (۱۹)$$

و این همان رابطهٔ (۹) است که می‌خواستیم ثابت کنیم.

به‌این ترتیب، قضیهٔ اساسی ۳ را در حالتی که α برابر واحد باشد ثابت کردیم. اکنون برای تکمیل اثبات قضیه، باید نشان دهیم که اگر قضیه برای هرمقداردلخواهی از α (و مقادیر کوچکتر از آن) درست باشد، برای $\alpha+1$ نیز درست خواهد بود.

بنابراین فرض می‌کنیم که

$$F(a) \equiv ۰ \quad (\mathrm{mod.}\, p^{\alpha+۱}) \qquad (۲۰)$$

که درآن a عدد درست دلخواهی است و می‌خواهیم ثابت کنیم که دراین صورت داریم:

$$F(x) = p^{\alpha+۱} f_۰(x) + p^{\alpha} f_۱(x)(x^p - x) + \ldots + \\ + f_{\alpha+۱}(x)(x^p - x)^{\alpha+۱} \qquad (۲۱)$$

که درآن چند جمله‌ایهای $f_۰(x)$ ، ... و $f_{\alpha+۱}(x)$ دارای ضریبهای درست هستند.

ولی فرض براین بود که قضیه برای توان α ، یعنی برای مدول p^α ، درست است. بنابراین باتوجه‌به‌رابطهٔ (۲۰)، رابطهٔ زیرهم به‌ازای هرمقدار a مسلماً درست خواهد بود:

$$F(a) \equiv ۰ \quad (\mathrm{mod.}\, p^{\alpha}) \qquad (۲۲)$$

زیرا هرعددی که بر $p^{\alpha+۱}$ بخش‌پذیر باشد، مسلماً بر p^α بخش پذیر خواهد بود.

فرض براین بود که قضیهٔ ۳ برای مقدار α ثابت باشد، بنابراین چند جمله‌ای F(x) می‌تواند به‌صورت زیر نوشته شود:

$$F(x) = p^{\alpha} f_۰(x) + p^{\alpha-۱} f_۱(x)(x^p - x) + \ldots + \\ + f_{\alpha}(x)(x^p + x)^{\alpha} \qquad (۲۳)$$

و این صورت به‌روشنی نشان می‌دهد که F(x) به‌ازای هرمقدار x بر p^α

بخش‌پذیر است. زیرا می‌دانیم که به‌ازای هرمقدار دلخواه x ، $x^p - x$ بر p بخش‌پذیر است . به‌جای x مقدار مشخص a را قرار می‌دهیم، داریم:

$$a^p - a = bp \qquad (۲۴)$$

که در آن عدد b بر p بخش‌پذیر نیست، بالاخره

$$F(a) = p^{\alpha} f_{۰}(a) + p^{\alpha - ۱} f_{۱}(a)bp + \qquad (۲۵)$$
$$+ p^{\alpha - ۲} f_{۲}(a)b^{۲}p^{۲} + \ldots + f_{\alpha}(a)\, b^{\alpha}p^{\alpha}$$

یعنی

$$F(a) = [f_{۰}(a) + bf_{۱}(a) + \ldots + b^{\alpha}f_{\alpha}(a)]p^{\alpha} \qquad (۲۶)$$

برای اینکه $F(a)$ بر $p^{\alpha+۱}$ بخش‌پذیر باشد، لازم و کافی است که

$$F_{۱}(a , b) = f_{۰}(a) + bf_{۱}(a) + \ldots + \qquad (۲۷)$$
$$+ b^{\alpha}f_{\alpha}(a)$$

بر p بخش‌پذیر باشد ، عدد b به‌وسیلهٔ (۲۴) با مشخص بودن a ، معین می‌شود.

ما ازفرض (۲۰) شروع کردیم که درآن $F(a)$ به‌ازای هرمقدار a بر $p^{\alpha+۱}$ بخش‌پذیر بود، بنابراین $F_{۱}(a , b)$ باید به‌ازای هرمقدار a بر p بخش‌پذیر باشد، که درآن عدد b از رابطه (۲۴) مشخص‌می‌شود. در اینصورت ، اگر در رابطهٔ (۲۴) مقدار a را تبدیل به $a+p\lambda$ کنیم

(λ عدد درست دلخواهی است) داریم:

$$(a+p\lambda)^{p}=a^{p}+p^{2}\mu+ \qquad (۲۸)$$

μ عددی است درست، زیرا طبق دستور دو جمله‌ای (binôme) داریم:

$$(a+p\lambda)^{p}=a^{p}+pa^{p-1}p\lambda+ \qquad (۲۹)$$
$$+\frac{p(p-1)}{2}a^{p-2}p^{2}\lambda^{2}+\dots$$

عدد p، عددی‌است اول، تمام ضریبهای طرف دوم دوجمله‌ای عددهایی درست هستند و تمام جمله‌ها، به‌جز جملهٔ اول، بر p^2 بخش‌پذیرند. بالاخره داریم:

$$(a+p\lambda)^{p}-(a+p\lambda)=b'p \qquad (۳۰)$$

که درآن:

$$b'=b-\lambda+p\mu \qquad (۳۱)$$

چند جمله‌ایهای $f_0(a)$، $f_1(a)$، ... و $f_\alpha(a)$ نسبت به‌مدول p به‌ترتیب باچند جمله‌ای $f_0(a+p\lambda)$، $f_1(a+p\lambda)$، . . . و $f_\alpha(a+p\lambda)$ همنهشت هستند. بنابراین اگر در (۲۷) به‌جای عدد a، عدد $a+p\lambda$ و به‌جای عدد b هم، باتوجه به‌رابطهٔ (۳۱)، $b-\lambda$ قرار دهیم به‌نتیجهٔ زیرخواهیم رسید، کـه به‌ازای هرمقدار دلخواه λ درست است:

$$f_0(a)+(b-\lambda)f_1(a)+(b-\lambda)^{2}f_2(a)+\dots+$$
$$+(b-\lambda)^{\alpha}f_\alpha(a)\equiv 0 \qquad (\mathrm{mod.}p)$$

$\alpha+1$ را کـوچکتر از p فـرض می‌کنیم ، یعنی α کـوچکتر از $p-1$ خواهدشد، دراینصورت این‌همنهشتی به‌ازای $p-1$ مقدار $b-\lambda$ صادق خواهد بود، یعنی برای $p-1$ مقـدار λ تمام ضریبهای توانهای $\lambda-p$ همنهشت باصفر خواهد بود و بنابراین داریم:

$$f_0(a) \equiv 0 \qquad (\text{mod}.p)$$

$$f_1(a) \equiv 0 \qquad (\text{mod}.p)$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

$$f_\alpha(a) \equiv 0 \qquad (\text{mod}.p)$$

این رابطه‌ها، به‌ازای هـرمقدار دلخواه a صادق‌اند و برای هراندیس k خواهیم داشت:

$$f_k(x) = pg_k(x) + (x^p - x)h_k(x)$$

کافی است که درمعادلهٔ (۲۵) به‌جای‌تمام مقادیر $f_k(x)$ مقدارشان را از این رابطه قرار دهیم، تا اینکه رابطهٔ مشابهی بدست آوریم که در آنجا α به $\alpha+1$ تبدیل شده باشد که قضیهٔ اصلی را برای $\alpha+1$ (که‌ما آنرا کوچکتر از p فرض‌کردیم) ثابت می‌کند. اکنون این مطلب باقی می‌ماند که قضیه را درموردهایی که α بزرگتر از p است بررسی کنیم و ببینیم دراینصورت قضیه چه تغییراتی پیدا خواهدکرد؟

۳۴. حالت توانهای بزرگتر از p. به‌سادگی می‌توان باتوجه به‌قضیهٔ فـرما چند جمله‌ای از درجه p^p نتیجه‌گرفت که به‌ازای هرمقدار

متغیر بر p^{p+1} بخش‌پذیر باشد. داریم:

$$x^p - x = p\xi \qquad (1)$$

متغیر ξ نسبت به‌مدول p با p مقدار۰، ۱، ۲، . . . و $p-1$ همنهشت است، وقتی‌که به x مقادیری نسبت‌داده شود که درترتیب دیگری باهمین مقادیر ۰، ۱، ۲، . . . و $p-1$ همنهشت باشد.

از طرف دیگر داریم:

$$(x^p - x)^p = p^p \xi^p \qquad (2)$$

و بالاخره با درنظر گرفتن رابطهٔ (۱):

$$(x^p - x)^p - p^{p-1} \cdot (x^p - x) = p^p(\xi^p - \xi) \qquad (3)$$

ولی باتوجه به‌قضیهٔ فرما داریم:

$$\xi^p - \xi = \lambda p$$

که درآن λ به‌ازای هرمقدار درست ξ ، مقداری درست خواهد بود، در نتیجه داریم:

$$(x^p - x)^p - p^{p+1}(x^p - x) = \lambda p^{p+1} \qquad (4)$$

یعنی

$$(x^p - x)^p - p^{p+1}(x^p - x) \equiv 0 \qquad (5)$$
$$(\mathrm{mod}.\, p^{p+1})$$

یعنی‌رابطهٔ (۵) تنها تعمیم ممکن قضیهٔ فرماست، ولی بهتر است گفته شود که این رابطه یك بسط بدون واسطه‌ای است که از قضیهٔ فرما بدست می‌آید تا یك تعمیم.

در مواردی که درجهٔ یك چند جمله‌ای از p^p تجاوز کند می‌توان از رابطهٔ (۵) استفاده کرد. چند جمله‌ای مفروض $F(x)$ را برطرف اول رابطهٔ (۵) یعنی بررابطهٔ

$$G(x)=(x^p-x)^p-p^{p-1}(x^p-x) \qquad (۶)$$

تقسیم می‌کنیم و اگر چنین بدست‌آوریم

$$F(x)=G(x).H(x)+R(x) \qquad (۷)$$

باقیماندهٔ $R(x)$ درجه‌ای کمتر از p^p دارد ومی‌توان مقسوم‌علیه‌های عددی را به‌روش سابق، جستجو کرد، مگر اینکه ضریبهای آنها برتوانی از p بخش‌پذیرباشند که دراینصورت مقسوم‌علیه p باتوانی بزرگتراز درجه‌اش خواهد بود. اگر ضریبهای $R(x)$ برتوانی از p که بزرگتر از p است بخش‌پذیرباشد، باید مقسوم‌علیه‌های‌عددی $H(x)$ را جستجو کرد. $H(x)$ را دوباره بر $G(x)$ تقسیم می‌کنیم تااینکه بالاخره به‌خارج قسمتی‌برسیم که توان‌آن کوچکتر از p^p باشد.

روشن است که برای درجات خیلی بالا می‌توان از تعمیم بیشتری استفاده کرد ، می‌دانیم که چند جمله‌ای $G(x)$ که به‌وسیلهٔ رابطهٔ (۶) معین است ، بر p^{p+1} بخش‌پذیر است، یعنی به‌ازای هر مقدار درست ξ داریم :

$$G(\xi)=\lambda p^{p+1} \qquad (۸)$$

و بنابراین خواهیم داشت:

$$[G(\xi)]^p - p^{p^2-1} G(\xi) = p^{p(p+1)} (\lambda^p - \lambda)$$

و بالاخره اگر $\lambda^p - \lambda = p\mu$ باشد:

$$[G(\xi)]^p - p^{p^2-1} G(\xi) = p^{p^2+p+1}\mu \qquad (۹)$$

ما بیشتر دربارهٔ این تعمیم تأکید نمی‌کنیم، زیرا وقتی که عدد اول p از ۱۰ تجاوز کند، درجهٔ طرف اول رابطهٔ (۹) از ۱۰۳ یعنی ۱۰۰۰ تجاوز می‌کند و محاسبه روی چندجمله‌ایهایی که درجه‌های بازهم بالاتری داشته باشند، تقریباً همیشه پیچیده است.

۳۵. قواعد عمومی. با به‌کاربردن نتیجه‌های قبل می‌توان قاعده‌های عمومی زیررا برای بدست آوردن مقسوم علیه‌های عددی چند جمله‌ایهایی که با یك یا چند متغیر مستقل سروکار دارند ذکر کرد. قبلا یادآوری می‌کنیم که کافی است مقسوم‌علیه‌های عددی را که برابرتوانی ازیك عدد اول p هستند جستجو کنیم، زیرا برای اینکه عددی بتواند بر حاصلضرب دوعامل‌اول بخش‌پذیر باشد، لازم وکافی است‌که برهریك‌از آن عاملها بخش‌پذیر باشد.

بزرگترین درجهٔ چند جمله‌ای را نسبت به‌هریك از متغیرهای‌آن m می‌نامیم. مثلاچند جمله‌ای:

$$x^3y^2 + y^3z^4 + 4xy^5 + 6x^2y^2z^3 + 7z^3 + 1 \qquad (۱)$$

نسبت به x از درجهٔ سوم، نسبت به y از درجهٔ پنجم و نسبت به z از درجهٔ چهارم است و بنابراین بزرگترین درجهٔ آن ۵ خواهد بود، درجهٔ

چند جمله‌ای، نسبت به‌مجموعهٔ متغیرها مساوی ۷است (درجملهٔ $x^۳y^۴$).

اصل اول. یك چند جمله‌ای نمی‌تواند مقسوم علیه اول p را از درجه‌ای بالاتر از m داشته باشد ، مگر اینکه تمام ضریبهای آن بر p بخش‌پذیر باشد، یعنی p مقسوم‌علیه آشکارآن باشد.

می‌دانیم که این اصل‌برای چند جمله‌ایهای یك متغیردرست است، فرض می‌کنیم که همین اصل‌برای n متغیردرست باشد، ثابت می‌کنیم که در اینصورت برای $n+۱$ متغیر نیز درست خواهد بود و به‌این ترتیب اصل‌تعمیم پیدا می‌کند (روش استقراء). به‌عنوان مثال، چند جمله‌ای(۱) را با ۳ متغیردرنظرمی‌گیریم وفرض می‌کنیم که قضیه برای چندجمله‌ای با ۲ متغیردرست باشد. چندجمله‌ای (۱) را می‌توان چنین نوشت:

$$y^۳z^۴+(۶x^۲y^۲+۷)z^۳+x^۳y^۲+۴xy^۵+۱ \qquad (۲)$$

یعنی چند جمله‌ای را برحسب متغیر z منظم کـردیم، درجهٔ این چند جمله‌ای، حداکثر برابر با m است و بنابراین ضریبهای آن چند-جمله‌ایهایی از x و y هستند، که حداکثر درجهٔ آنها هم m است. بنا بر فرض، این ضریبها نمی‌توانند مقسوم‌علیه اولی مانند عدد اول pبزرگتر از m داشته باشند، مگراینکه p تمام ضریبها را عادکنند، یعنی مقسوم-علیه‌آشکارباشد. بنابراین p نمی‌تواند مقسوم‌علیه‌آشکارچندجمله‌ای(۲) باشد (که چند جمله‌ای از درجـهٔ ۴ نسبت به‌متغیر z است) ، زیرا همهٔ ضریبهای این چندجمله‌ای به‌ازای هرمقداردلخواه x و y برp بخش‌پذیر نیستند.

قاعدهٔ عمومی. برای اینکه بدانیم یك چند جمله‌ای برعدد اول

p واحتمالا برتوانی از p بخش‌پذیر هست یانه، ازقضیهٔ فرمابه‌صورت زیر استفاده می‌کنیم:

$$(۳) \qquad \begin{cases} x^p = x + px_1 \\ y^p = y + py_1 \\ z^p = z + pz_1 \end{cases}$$

و این برای حالتی است که با سه متغیر x و y و z سروکار داشته باشیم، روشن است که اگر سه متغیر x و y و z مستقل باشند ۶ متغیر x_1، y_1، z_1، x، y و z بدست خواهدآمد. اگرتوانهایی از x راکه بالاتر از p است به‌وسیلهٔ جمله‌های (۳) جانشین کنیم به‌چند جمله‌ای می‌رسیم که نسبت به x و y وz با درجه‌ای پایین‌تر از p می‌باشد. اگرچند جمله‌ای جدید مثلا نسبت به x_1 و y_1 از درجه‌ای بالاتر از p بود از رابطه‌های مشابهی استفاده می‌کنیم :

$$(۴) \qquad \begin{cases} x_1^p = x_1 + px_2 \\ y_1^p = y_1 + py_2 \end{cases}$$

که درنتیجه توانهای x_1 و y_1 کوچکتر از p بشود. این عمل را درصورت لزوم به‌همین ترتیب برای x_2 و y_2 ادامه می‌دهیم تا بالاخره بعد از تعداد معینی عمل به‌چند جمله‌ای برسیم که از متغیرهای مستقلی مثل x، y، z، x_1، y_1، z_1، x_2، y_2 و z_2 تشکیل شده باشد. حالا اصل اول را در مورد این چند جمله‌ای به‌کارمی‌بریم، این چند جمله‌ای تنهاوقتی برتوانی از p ، مثلا p^k ، بخش‌پذیر است که تمام ضریبهای آن بر p^k بخش‌پذیر باشد.

به‌عنوان مثال چند جمله‌ای زیررا درنظر می‌گیریم:

$$P(x , y)=x^3y^3+8xy^3+8x^3y+xy+9 \qquad (5)$$

که درجهٔ آن برابر ۳ می‌باشد و بنابراین عاملهایی جز ۲ و ۳ نخواهد داشت. درمورد عامل ۲ گوییم که اگر x و y فرد باشند $P(x , y)$، مجموع ۵ عدد، عددی فرد خواهد بود و درنتیجه بر ۲ بخش‌پذیر نمی‌شود، برای عامل ۳ قرار می‌دهیم:

$$\begin{cases} x^3=x+3x_1 \\ y^3=y+3y_1 \end{cases} \qquad (6)$$

و یک محاسبهٔ ساده نتیجه می‌دهد:

$$P(x , y)=18xy+27xy_1+27yx_1+9x_1y_1+9$$

چند جمله‌ای بر ۹ بخش‌پذیر است و بنابراین ۹ بزرگترین مقسوم‌علیه این چند جمله‌ای است.

۸

قانون نادرشدن عددهای اول

۳۶. هدف این بخش. در این بخش می‌خواهیم تا حد ممکن بعضی از نتیجه‌های بسیار مهمی‌را که ریمان ، دربیش از یك سده‌پیش، دربارهٔ عددهای اول بدست آورده است ، به‌شکل ساده و مقدماتی طرح کنیم. جستجوهای ریمان براساس تابع مشهور $\xi(s)$ قرارگرفته است، که به‌وسیلهٔ رابطهٔ زیرمعین می‌شود:

$$\xi(s) = ۱ + \frac{۱}{۲^s} + \frac{۱}{۳^s} + \frac{۱}{۴^s} + \dots + \frac{۱}{n^s} + \dots \qquad (۱)$$

به‌شرطی‌که قسمت حقیقی s بزرگتر از واحدباشد، رشتهٔ طرف دوم‌رابطه، رشته‌ای متقارب خواهد بود. می‌توان به‌طور ساده نوشت:

$$\frac{۱}{\xi(s)} = (۱ - \frac{۱}{۲^s})\,(۱ - \frac{۱}{۳^s})\,(۱ - \frac{۱}{۵^s}) \dots \qquad (۲)$$
$$(۱ - \frac{۱}{p^s}) \dots$$

درطرف دوم این رابطه، تمام عـددهای اول نشان داده شده‌اند، زیرا در رابطهٔ (۱) تمام عددهای درست وجود دارند. درحقیقت داریم :

$$\frac{۱}{۱ - \frac{۱}{p^s}} = ۱ + \frac{۱}{p^s} + \frac{۱}{p^{۲s}} + \dots + \frac{۱}{p^{ks}} + \dots \qquad (۳)$$

واگر تمام تساویهای شبیه (۳) را درهم ضرب کنیم خواهیم داشت:

$$\xi(s) = \Sigma\,\Sigma \ldots \Sigma\left(\frac{1}{p_1{}^{k_1}} \cdot \frac{1}{p_2{}^{k_2}} \cdots \frac{1}{p_n{}^{k_n}}\right)^s \qquad (۴)$$

که در آن توانهای k_1 و k_2 و... و k_n تمام توانهای ممکن از صفر تا بی‌نهایت را اختیار می‌کنند، به‌نحوی که هرترکیب k_1 و k_2 و ... و k_n تنها یکبار نشان داده شده باشد. نتیجه می‌شودکه رابطهٔ (۴) با رابطهٔ (۱) هم‌ارزاست،زیرا هرعدد درست تنها به‌یك‌صورت‌می‌تواند به ضرب عاملهای اول تجزیه شود.

ریمان، بعضی ازخاصیتهای $\xi(s)$ را ثابت‌کرد وبعضی‌ازقضیه‌های مربوط به‌آنرا هم محتمل شمرد. بعد از مرگ ریمان هم بسیاری از ریاضیدانان، وقت خودرا صرف‌بررسی $\xi(s)$کردند. ازبین این‌دانشمندان باید از ژاك‌هادامار «Jacques Hadamard» فرانسوی و دولاواله‌پوسن «De La Vallée - Poussin» نام برد،که توانستند قضیهٔ اساسی‌ریمان را ثابت‌کنند وقانون نادرشدن «Reréfaction» عددهای اول را ازآن نتیجه بگیرند. این قانون اساساً مبتنی براین است‌که تعداد عددهای اول کوچکتر از x به‌طور مجانبی برابر است با:

$$N = \frac{x}{\log x} \qquad (۵)$$

از اینجا نتیجه می‌شودکه به‌طور تقریبی داریم:

$$x \simeq N \log x$$

اما از رابطهٔ (۵) نتیجه می‌شود:

$$\log x = \log N + \log \log x \qquad (۶)$$

و چون $\log\log x$ نسبت به $\log x$ خیلی کوچك است، می‌توان به‌طورتقریبی به‌جای رابطهٔ (۵) نوشت:

$$x = N \log N \qquad (۷)$$

کارهای زیادی انجام‌شده(وبرای ما میسرنیست که‌دراینجا ازآنها نام ببریم) تا رابطه‌های (۴) و (۶) بدست آمده است و مسلماً غیرممکن است که بتوان رابطهٔ دقیق ساده‌ای پیدا کرد که به‌کمك‌آن تعدد عددهای اول شناخته شود.

ما فقط به‌همین آگاهی کوتاه از بررسیهایی‌که مربوط به‌آنالیز عالی است و خارج ازچارچوب این‌کتاب مقدماتی است اکتفا می‌کنیم. دراین بخش ما خود را به‌این قانع می‌کنیم که روش مقدماتی برای‌اثبات رابطه‌های مجانبی (۴) و (۶) پیدا کنیم تا به‌کمك آن خواننده بتواند، حداقل‌اطلاع را دراین زمینه داشته باشد. باهمهٔ اینها باید به‌خاصیتهای مقدماتی لگاریتم و تابعهای مجهول‌القوه‌آشنا بود، زیرا در رابطه‌ای‌که باید ثابت‌کنیم لگاریتم وجود دارد، همچنین، از مقدمات نظریهٔ‌ترکیب «Combinasion» یعنی از مثلث حسابی پاسکال هم استفاده خواهیم کرد.

۳۷. رابطهٔ اساسی. با نشانهٔ $C_{۲m}^{m}$ تعداد ترکیبهای ۲m حرف m به m را نشان می‌دهیم. می‌دانیم که

$$C_{۲m}^{m} = \frac{(۲m)!}{m!\,m!} \qquad (۱)$$

و این همان عددی است که در $(m+۱)$ امین ردیف از سطر $(۲m)$ ام مثلث حسابی پاسکال قرار دارد:

۱ ۱

۱ ۲ ۱ (۲)

۱ ۳ ۳ ۱

۱ ۴ ۶ ۴ ۱

. . . . . .

مثلا به‌ازای $m=۲$ داریم: $C_۴^۲ = ۶$. همچنین می‌توان گفت که $C_{۲m}^m$ همان ضریب $x^m y^m$ در بسط دو جمله‌ای $(x+y)^{۲m}$ است. اگر x و y را برابر واحد فرض کنیم بلافاصله نتیجه می‌شود:

$$C_{۲m}^{m} < ۲^{۲m} \qquad (۳)$$

نا مساوی (۳) را می‌توان با نامساوی زیر تکمیل کرد:

$$\frac{۱}{۲m} ۲^{۲m} < C_{۲m}^{m} \qquad (۴)$$

در حقیقت باتوجه به‌رابطهٔ (۱) داریم:

$$\frac{۱}{۲^{۲m}} C_{۲m}^{m} =$$

$$= \frac{۱ \times ۲ \times ۳ \times ۴ \times \ldots \times (۲m-۱)۲m}{۲ \times ۴ \times ۶ \times \ldots \times (۲m-۲)۲m \times ۲ \times ۴ \times \ldots (۲m-۲)\,۲m}$$

زیرا برای تقسیم C_{2m}^{m} بر 2^{2m}، کافی است که در هر یك از $2m$ عامل درستی که در مخرج آن وجود دارد $(m!m!)$، عدد ۲ را ضرب کنیم.

اکنون اگر عاملهای برابر را ازصورت و مخرج کسرطرف دوم رابطهٔ (۵) حذف کنیم (حاصلضرب m عدد زوج اولیه) خواهیم داشت:

$$\frac{1}{2^{2m}} C_{2m}^{m} = \frac{1\times 3\times 5\times \ldots (2m-1)}{2\times 4\times 6\times \ldots 2m} \qquad (6)$$

بلافاصله می‌توان نتیجه گرفت که طرف دوم کوچکتر ازواحد است، زیرا هرعدد فرداز عدد زوجی که درهمان ردیف باشدکوچکتر است ؛ اما این رابطه را به‌صورت زیرهم می‌توان نوشت:

$$\frac{1}{2^{2m}} C_{2m}^{m} = \frac{3\times 5\times 7\times \ldots (2m-1)}{2\times 4\times 6\times \ldots (2m-2)} \times \frac{1}{2m} \qquad (7)$$

و روشن است که دراینصورت، ضریب $\frac{1}{2m}$ در طرف دوم رابطهٔ (۷) عددی بزرگتر از واحد است. زیرا هر عدد فرد از عدد زوج پیش ازخود بزرگتر است. به‌این ترتیب رابطه‌های (۶) و (۷) ، نامساویهای (۳) و (۴) را ثابت می‌کنند، این نا مساویها را می‌توان به‌وسیلهٔ رابطه‌های هم ارز زیرنشان داد:

$$(8) \qquad \begin{cases} C_{2m}^{m} = K.2^{2m} \\ \frac{1}{2m} < K < 1 \end{cases}$$

اثبات این مطلب دشوار نیست که به‌طور مجانبی داریم:

$$K = \frac{a}{\sqrt{m}} \qquad (۹)$$

که درآن a مقدار ثابتی است. ولی برای هدف ما رابطه‌های (۸) کافی است. حالا، عدد درست $C_{۲m}^{m}$ را به‌صورت نخستین (۱) در می‌آوریم و آنرا به‌عاملهای اول تجزیه می‌کنیم. اگر p عدد اول غیرمشخصی کوچکتر از $۲m$ باشد، باید روشن کرد که p در صورت و مخرج $C_{۲m}^{m}$ با چه توانی است.

در یك محاسبهٔ مقدماتی، درنظر گرفتیم که بعضی عددهای کوچکتر از $۲m$ می‌توانند بر توان بزرگتر از p نسبت به $۲m$ بخش‌پذیر باشند، به‌عبارت دیگر وقتی که عاملهای درستی از صورت و مخرج، بر p^{α} بخش‌پذیر باشد ، ما آنرا به‌عنوان عـددی که فقط بر p بخش‌پذیر است، به‌حساب می‌آوریم.

عاملهایی از $۲m$ ، که بر p بخش‌پذیرند عبارتند از :

$$p \text{ و } ۲p \text{ و } ۳p \text{ و} \ldots \text{ و } (h-۱)p \text{ و } hp \qquad (۱۰)$$

که درآخر به‌بزرگترین عدد ممکن hp می‌رسیم، که کوچکتر یا مساوی با $۲m$ است، بنابراین داریم:

$$hp \leqslant ۲m < (h+۱)p \qquad (۱۱)$$

بهتر است حالتی را که درآنجا h عددی زوج است با حالتی که درآن h فرد است ازهم جدا کنیم. ابتدا فرض می‌کنیم که h عددی زوج باشد: $h = ۲q$ ، خواهیم داشت:

$$۲qp \leqslant ۲m < (۲q+۱)p \qquad (۱۲)$$

که در نتیجه نا مساویهای زیر را خواهیم داشت:

$$qp \leqslant m < (q+1)p \qquad (13)$$

نتیجه می‌شود که عامل اول p ، به‌اندازهٔ ۲q مرتبه در !۲m و q مرتبه در !m وجود دارد و بنابراین در C_{2m}^{m} ، یعنی خارج قسمت !۲m برمربع !m وجود ندارد.

اکنون فرض می‌کنیم که h مساوی عدد فرد ۲q+۱ باشد ، داریم:

$$(2q+1)p \leqslant 2m(2q+2)p \qquad (14)$$

و از آن نتیجه می‌گیریم:

$$qp < m < (q+1)p \qquad (15)$$

با این تفاوت که عامل p ، اکنون ۲q+۱ مرتبه در صورت و فقط ۲q مرتبه در مخرج وجود دارد و بنابراین یك مرتبه در خارج قسمت C_{2m}^{m} وجود دارد.

بنابراین عدد C_{2m}^{m} برابر با حاصلضرب عددهای اول p است که درنامساویهای (۱۲) صدق می‌کنند، به‌استثنای آنهائی که درنامساویهای (۱۲) صدق می‌کنند و در آنها q نمایندهٔ یك عدد درست دلخواه است.

بنابراین خواهیم داشت :

$$\log C_{2m}^{m} = \Sigma \log p \qquad (16)$$

علامت Σ به‌ازای عددهای اول p ، که در رابطه‌های زیر صدق کنند بسط

پیدا می‌کند:

$$(۱۷)\qquad \begin{cases} \frac{۲m}{۲} < p \leqslant ۲m \\ \frac{۲m}{۴} < p \leqslant \frac{۲m}{۳} \\ \frac{۲m}{۶} < p \leqslant \frac{۲m}{۵} \\ \cdots\cdots\cdots \end{cases}$$

نا مساویهای (۱۷) را باید تا آنجاکه عددهای اول p درآنها صدق می‌کنند ادامه داد . می‌توان توجه کرد که طرف دوم این نامساویها نمی‌توانند عددهایی‌اول باشند، زیرا بر۲ بخش‌پذیرند و بنابراین علامت $\leqslant$ می‌تواند به‌علامت $>$ تبدیل شود .

اگر مجموع فاصله‌های محدود دوجهت نا مساویهای (۱۷) را l بگیریم، داریم:

$$l = ۲m\left(۱ - \frac{۱}{۲} + \frac{۱}{۳} - \frac{۱}{۴} + \frac{۱}{۵} - \frac{۱}{۶} + \ \cdots \ \right) \quad (۱۸)$$

رشتهٔ داخل پرانتز باید جایی متوقف شود که درآنجا نامساویهای (۱۷) دیگر هیچ عدد اولی را معین نمی‌کنند؛ ولی اگر m عددی خیلی‌بزرگ باشد ، می‌توان از خطای کوچکی چشم پوشید و آنرا تا بی‌نهایت ادامه داد و در اینصورت برابر با $\log ۲$ خواهد بود، مثل اینست که در رابطهٔ زیر به‌جای x عدد ۱ را قرار دهیم[1]:

---

۱. مطلب از لگاریتم نپری، واضح است.

$$log(۱+x)=x-\frac{x^۲}{۲}+\frac{x^۳}{۳}-\frac{x^۴}{۴}+\frac{x^۵}{۵}-\dots \qquad (۱۹)$$

و مقدار $log ۲$ هم کوچکتر از ۰/۷ می‌باشد.

از طرف دیگر طبق رابطهٔ (۸) داریم:

$$logC_{۲m}^{m}=۲m\,log\,۲-\varepsilon\,log\,۲m \;(\varepsilon<۱) \qquad (۲۰)$$

رابطهٔ (۱۶) را هم می‌توان به‌صورت زیرنوشت:

$$\Sigma log\,p=l+\varepsilon_m \qquad (۲۱)$$

l عبارت از طول مجموع $۲m\,log\,۲$ فاصله‌هایی است که شامل عددهای اول p (واقع درطرف اول تساوی) هستند و ε_m نسبت به l عدد بسیار کوچکی است.

حالا ثابت‌می کنیم که این دستور وقتی هم که توانهایی ازعددهای اول‌را داشته‌باشیم، برقراراست (چیزی‌که درمحاسبهٔ اولیه درنظرنگرفته بودیم). تنها اختلافی‌که پیدا می‌شود در تغییرمقدار ε_m است ، ولی باز هم نسبت به m و l خیلی‌کوچك باقی می‌ماند.

در حقیقت تعداد عددهایی‌که از $۲m$ کوچکترند و برمربع یك عدد درست مثل $p^۲$ بخش‌پذیرند، حداکثر برابر است با:

$$\frac{۲m}{p^۲}$$

و اگر $p^۲$ از $۲m$ (یعنی p از $\sqrt{۲m}$) بزرگترباشد، این تعداد مساوی صفر می‌شود. روشن است‌که تعداد عاملهای p هم‌کوچکتر از $\sqrt{۲m}$ است، زیرا در رابطهٔ (۲۱)، l نمایندهٔ طول m است و جمله‌های اضافی می‌توانند در ε_m جمع شده‌باشند. برای اینکه خواننده به‌این‌طرز کار کاملا

آشنا شود یك مثال عددی می‌زنیم.

۳۸ . مثال عددی . فرض می‌کنیم $m = ۵۰۰۰$ یعنی $۲m = ۱۰۰۰۰$ باشد که جذرآن برابر ۱۰۰ است. درنتیجه تنها عددهای اول کوچکتر از ۱۰۰ می‌توانند در عاملهای ! ۱۰۰۰۰ و یا ! ۵۰۰۰ ، منتهی با توانی بزرگتر از واحد باشند.

داریم:

$$\frac{۱۰۰۰۰}{۲} = ۵۰۰۰ \qquad \frac{۱۰۰۰۰}{۳} = ۳۳۳۳$$

$$\frac{۱۰۰۰۰}{۴} = ۲۵۰۰ \qquad \frac{۱۰۰۰۰}{۵} = ۲۰۰۰$$

$$\frac{۱۰۰۰۰}{۶} = ۱۶۶۶ \qquad \frac{۱۰۰۰۰}{۷} = ۱۴۲۸$$

$$\frac{۱۰۰۰۰}{۸} = ۱۲۵۰ \qquad \frac{۱۰۰۰۰}{۹} = ۱۱۱۱$$

$$\frac{۱۰۰۰۰}{۱۰} = ۱۰۰۰$$

جذر تقریبی این عددها عبارتست از :

۷۰، ۵۸، ۴۴، ۴۰، ۳۷، ۳۴، ۳۱

به‌نحوی‌که تنها عـددهای اولی‌که مربع آنها بیش از یکبار در صورت نسبت به‌مخـرج وجود دارند ، عددهای اول واقـع در فاصله‌هـای زیر هستند :

. . . ؛۳۷ و ۳۴ ؛۴۴ و ۴۰ ؛۵۸ و ۵۰ ؛۱۰۰ و ۷۰

بنابراین این عددهای اول بنابر (۶) عبارتند از : ۹۷، ۸۹، ۸۳، ۷۹ ، ۷۳، ۵۳،۷۱، ۴۳، ۴۱، و اگرمحاسبه‌هارا ادامه‌دهیم به‌این عددها ۴تا۶ عدد اول واقع بین ۲ و ۲۹ اضافه می‌شود . به‌سادگی دیده می‌شود که حاصلضرب همهٔ این عددها از توان دوازدهم ۷۰ تجاوز نمی‌کند . توان دوازدهم ۷۰ را می‌توان توان ششم ۵۰۰۰ ویا به‌تقریب توان‌بیست ویکم ۱۰ ویا توان هفتادم ۲ در نظرگـرفت. ولی در اینجا مقدار C_{2m}^{m} قابل مقایسه با عدد 2^{10000} خواهد بود.

و اگر عددهای اولی را جستجوکنیم که مکعب آنهـا چندین‌بار در حاصلضرب وجـود دارند، باز هم جوابهای نسبی‌کـوچکتری بدست خواهیم آورد . ریشهٔ سوم ۱۰۰۰۰ کـوچکتر از ۲۳ است به‌نحوی که حداکثر می‌توان حاصلضرب عددهای اول‌کوچکتر از ۱۹ را داشت.

ریشهٔ چهارم ۱۰۰۰۰ برابر با ۱۰ است و بنابراین تنها عددهای اول ۲، ۳، ۵ و ۷کوچکتر از آن وجود دارد.

برای تکمیل مطلب باید اضافه‌کنیم‌که ۱۰۰۰۰ بین دو عدد 2^{13} و 2^{14} قرار دارد و بنابراین باید توانهـای 2^{5}، 2^{6}، 2^{7}، 2^{8}، 2^{9}، 2^{10}، 2^{11}، 2^{12} و 2^{13} را درنظرگرفت‌که هریك ازآنها شامل حداکثریك‌عامل ۲ هستند و بنابراین حاصلضرب کوچکتر از 2^{9} می‌شود. به‌هرحال تمام تصحیحهای مربوط به‌نتیجه‌هـای توانهای بالاتر از یك ، حـاصلضربی کوچکتر از 2^{100} تشکیل خواهند داد، در حالیکه اندازهٔ C_{2m}^{m} در حدود 2^{10000} بـود. بنابراین مجمـوع لگاریتمهای عددهای اول‌کـوچکتر از ۱۰۰۰۰ به‌جای ۱۰۰۰۰ ممکن است برابر ۹۹۰۰ یعنی ۹۹٪ از ۱۰۰۰۰

بشود .

ولی باید درنظر داشت که اگر به‌جای ۱۰۰۰۰ عددی که به‌طور قابل توجهی بزرگتر باشد، و مثلا یک‌میلیون را، درنظر بگیریم، به‌جای ۱٪ ، خطایی برابر ۰/۰۰۱ خواهیم داشت و این به‌معنای آنست که برای عددهای بزرگ می‌توان از آن صرفنظر کرد.

۳۹.نتیجه‌های رابطهٔ اساسی. به‌این ترتیب رابطهٔ اساسی را می‌پذیریم، می‌دانیم که این رابطه به‌طور مطلق درست نیست (می‌توان بی‌نظمیهایی‌را که در بند(۱۲) مورد مطالعه قراردادیم، یادآوری کرد). ولی روشن کردیم که درحالتهایی که x عددی خیلی بزرگ باشد، می‌توان آنرا به‌اندازهٔ کافی دقیق به‌حساب آورد.

بنابراین رابطهٔ:

$$\Sigma log\, p == x \qquad (۱)$$

را می‌پذیریم، که درآن $\Sigma log\, x$ به‌معنای مجموع عددهای اول کوچکتراز x است. در همان نظر اول، می‌توان فهمید که این دستور به‌طور مطلق درست نیست، زیرا طرف اول این رابطه، عددی درست نیست. علاوه‌بر آن وقتی‌که x بین دوعدد اول متوالی p_1 و p_2 تغییر می‌کند، مقدار x ثابت‌می‌ماند؛ وقتی‌که x ازمیلیون تجاوز کند، اختلاف $p_2 - p_1$ می‌تواند درحدود ۱۰۰باشد، این امرهم موجب وجود خطائی در رابطهٔ (۱)می‌شود که به‌طور مطلق برابر ۱۰۰ و به‌طورنسبی برابر ۱۰هزارم است.

با وجود اینها ، محاسبه‌های خود را بر فرض دقیق بودن رابطهٔ

(۱) می‌گذاریم و بعد نتیجه‌های بدست‌آمـده را با محاسبه‌های آماری مقایسه می‌کنیم.

x_1 و x_2 را دو عدد اول نزدیك به‌هم فرض می‌کنیم، ولی‌بین x_1 و x_2 عددهای اول دیگری هم وجود دارد. رابطه‌های زیر را می‌نویسیم:

$$\Sigma \log p = x_1 \qquad (۲)$$

$$\Sigma' \log p = x_2 \qquad (۳)$$

که درآنها Σ و Σ' به‌ترتیب به‌وسیلهٔ عددهای اول‌کوچکتر از x_1 و x_2 بیان می‌شوند. اگر معادله‌های (۲) و (۳) را عضو به‌عضو ازهم‌کم‌کنیم خواهیم داشت:

$$\Sigma'' \log p = x_2 - x_1 \qquad (۴)$$

که درآن Σ'' مربوط به‌عددهای اول بین x_1 و x_2 می‌باشد. مقدارمتوسط لگاریتمهای این عددهای اول برابر با $\log x$ است‌که درآن عـدد x عـدد مجهولی بین x_1 و x_2 می‌باشد. اگر تعداد عـددهای اول بین x_1 و x_2 را با $N(x_1, x_2)$ نشان دهیم، رابطهٔ (۴) چنین نوشته می‌شود:

$$N(x_1, x_2) \log x = x_2 - x_1 \qquad (۵)$$

و ازآنجا رابطهٔ زیر نتیجه می‌شود:

$$N(x_1, x_2) = \frac{x_2 - x_1}{\log x} \qquad (۶)$$

که از روی‌آن می‌توان تعداد عددهای اول بین x_1 و x_2 را بدست‌آورد.

اگر عددهای x_1 و x_2 نزدیك به‌هم باشند، می‌توان x را عدد دلخـواهی بین x_1 و x_2 گرفت و اگراختلاف x_1 و x_2 قابل توجه باشد، می‌تـوان x را واسطهٔ هندسی یا واسطهٔ عددی x_1 و x_2 فرض کرد، وقتی که نسبت x_1 و x_2 به واحد نزدیك باشد واسطهٔ هندسی و عـددی آنها خیلی به‌هم نزدیك خواهند بود[1]. خـواهیم دید که رابطهٔ (۶) با محاسبه‌های آماری تطبیق می‌کند. قبلا چند نتیجهٔ ساده را نشان می‌دهیم. f(x) را تابعی از عدد درست x فرض می‌کنیم که وقتی x به‌سمت بینهایت برود ، به‌طرف صفر میل کند و فرض می‌کنیم که این تابع خیلی به‌کندی و کاملا منظم تغییر کند. می‌خواهیم حاصل جمع:

$$S(p)=f(۲)+f(۳)+f(۵)+\ldots+f(p) \qquad (۷)$$

را محاسبه کنیم که شامل تمام عددهای اول تا عـدد p می‌باشد (و خود عدد p) . x_1 و x_2 را فاصلهٔ کوچکی بین ۲ و p فرض می‌کنیم، دراین فاصله $N(x_2 ، x_1)$ عدد اول وجود داردکه مقادیری از f(x) که به‌طور محسوس برابر با مقادیر x_1 و x_2 است با آنها تطبیق می‌کند، بنابراین مجموع این مقادیرچنین می‌شود:

---

۱. اگر مثلا $x_1=۱۰۰^۲=۱۰۰۰۰$ و $x_2=۱۰۵^۲=۱۱۰۲۵$ باشند ، واسطهٔ هندسی‌آنها ۱۰۵۰۰ واسطهٔ عددی‌آنها ۱۰۵۱۲/۵ می‌شوداختلاف آنها از یکهزارم مقدار مشترکشان تجاوزنمی‌کند. داریم:

$$\log ۱۰۵۱۲/۵ - \log ۱۰۵۰۰ = \log\left(۱+\frac{۱۲/۵}{۱۰۵۰۰}\right) =$$

$$= \frac{۱۲/۵}{۱۰۵۰۰} + \varepsilon$$

$$N(x_۱ ، x_۲)\, f(x) \qquad (۸)$$

و بالاخره مجموع $S(p)$ با رابطهٔ زیرمعین می‌شود :

$$S(p)=\Sigma N(x_۱ ، x_۲)\, f(x)=\Sigma(x_۲-x_۱)\times \times\frac{f(x)}{\log x} \qquad (۹)$$

که عبارتست ازمجموع رشتهٔفاصله‌های $x_۱$ و $x_۲$ که‌شامل‌تمام‌فاصله‌های ۲ و p می‌شود. طبق تعریف انتگرال معین داریم:

$$S(p)=\int_۲^p\frac{f(x)}{\log x}dx \qquad (۱۰)$$

درحالتی‌که این انتگرال، وقتی‌که p به‌سمت بینهایت می‌رود ، متقارب باشد، $S(p)$ هم وجود خواهد داشت.

اگر درحالت خاص $S(p)=\frac{۱}{p}$ فرض‌کنیم رابطهٔ مهم زیر را خواهیم داشت:[۱]

$$\frac{۱}{۲}+\frac{۱}{۳}+\frac{۱}{۵}+\ldots+\frac{۱}{p}=\int_۲^p\frac{p}{p\log p}=\log\log p \qquad (۱۱)$$

می‌دانیم که اگر تمام عددهای درست را در نظر بگیریم به‌طور تقریبی داریم:

$$\frac{۱}{۲}+\frac{۱}{۳}+\frac{۱}{۴}+\frac{۱}{۵}+\ldots+\frac{۱}{n}=\log n \qquad (۱۲)$$

۱. اگر رشته را تبدیل به‌انتگرال کنیم ، باید از جملهٔ کوچك $\log\log ۲$ صرفنظر کرد .

اختلاف بزرگ بین رابطه‌های (۱۱) و (۱۲) یکی از عملهای ریاضی‌است که به‌خوبی و روشنی نادرشدن عددهای اول را نشان می‌دهد.

با کمك رابطهٔ (۱۱) می‌توان مقدار حاصلضرب زیر را نتیجه گرفت:

$$\Theta(p)=(۱-\frac{۱}{۲})(۱-\frac{۱}{۳})(۱-\frac{۱}{۵})\ldots(۱-\frac{۱}{p}) \qquad (۱۳)$$

که شامل عددهای اول بین ۲ و p می‌باشد. درحقیقت با تقریبی‌که با بزرگ شدن p به‌دقت نزدیك می‌شود داریم:

$$e^{-\frac{۱}{p}} = ۱-\frac{۱}{p} \qquad (۱۴)$$

به‌نحوی‌که مقدار مجانبی $\Theta(p)$ می‌شود:

$$\Theta(p)\ e^{-\Sigma\frac{۱}{p}} = e^{-\log\log p} = \frac{۱}{\log p} \qquad (۱۵)$$

جمله‌های به‌صورت $\frac{۱}{p^۲}$ ، $\frac{۱}{p^۳}$ و غیره، که در (۱۴) حذف شده‌اند، رشتهٔ متقاربی را تشکیل می‌دهند که وقتی p به‌سمت بی‌نهایت میل کند عامل معینی را نتیجه می‌دهد. بنابراین دقیق‌تر خواهیم داشت:

$$\Theta(p) = \frac{A_p}{\log p} \qquad (۱۶)$$

که درآن وقتی p به‌سمت بینهایت میل کند، A_p به‌سمت عدد ثابت A

میل خواهد کرد.

اگر حاصلضرب شبیه $\Theta(p)$ را برای عددهای درست به‌کار ببریم با یك محاسبهٔ ساده خواهیم داشت:

$$\Theta(n)=\left(۱-\frac{۱}{۲}\right)\left(۱-\frac{۱}{۳}\right)\cdots\left(۱-\frac{۱}{n}\right)=\frac{۱}{n} \qquad (۱۷)$$

و اختلاف بزرگ رابطه‌های (۱۶) و (۱۷) به‌روشنی تأثیر نادرشدن عددهای اول را نشان می‌دهد.

بالاخره آخرین نتیجهٔ مربوط به‌مقدار تابع $\varphi(n)$ را، وقتی که n برابر با حاصلضرب عددهای اول از ۱ تا p است، ذکر می‌کنیم، می‌نویسیم:

$$n=p(!) \qquad (۱۸)$$

وقتی‌که‌علامت ! را داخل‌پرانتزگذاشته‌ایم، به‌این معناست‌که‌حاصلضرب تمام عددهای درست کوچکتر از p را نداریم، بلکه سر و کار ما با حاصلضرب p درتمام عددهای اول‌کوچکتر ازآنست.

رابطهٔ (۱) با رابطهٔ زیر هم‌ارز است:

$$n=e^{p} \qquad (۱۹)$$

عدد $\varphi(n)$ از عددهای‌کوچکتر از n و متباین با n چنین است:

$$\varphi(n)=n\left(۱-\frac{۱}{۲}\right)\left(۱-\frac{۱}{۳}\right)\left(۱-\frac{۱}{۵}\right)\cdots\left(۱-\frac{۱}{p}\right) \qquad (۲۰)$$

و بنابراین با توجه به‌رابطه‌های (۱۶) و (۱۹) داریم:

$$\varphi(n) = A_p \frac{n}{\log p} = A_p \frac{n}{\log \log n} \qquad (۲۱)$$

دیده می‌شود که این عدد از تعداد عددهای اول کوچکتر از n که به‌صورت $\frac{n}{\log n}$ نشان داده می‌شود، خیلی بزرگتر است. این تبصره از اینجهت جالب‌است که برای مقادیر کوچك p و n برعکس‌است. مثلا برای $p = ۷$ و $n = ۲۱۰$ داریم $\varphi(n) = ۴۸$. بین این ۴۸ عدد، عدد ۱ مشخص‌می‌شود و عددهای اول ۲، ۳، ۵ و ۷ مشخص نمی‌شود، و بنابراین ۵۱ عدد اول وجود خواهد داشت، به‌عبارت دیگر عددهای بخش‌پذیر بر ۱۱ و ۱۳ یعنی:

$$۱۱ \times ۱۹ \text{ و } ۱۱ \times ۱۷ \text{ و } ۱۱ \times ۱۳ \text{ و } ۱۳^۲ \text{ و } ۱۱^۲$$

را درنظر نگیریم، یعنی تا عدد ۵ در نظر بگیریم، ۴۶ عدد اول باقی می‌ماند.

برعکس، اگر $p = e^{۱۰۰}$ باشد[۱] (یعنی $\log p = ۱۰۰$) و $n = p(!)$، تعداد عددهای اول کوچکتر از n به‌صورت $\frac{n}{p}$ خواهد بود درحالیکه:

$$\varphi(n) = A_p \frac{n}{\log p} = A_p \frac{n}{۱۰۰}$$

می‌باشد، بین این $\varphi(n)$ عدد تنها

---

۱. بهتر است گفته شود که p عدد اول کاملا نزدیك به $e^{۱۰۰}$ است، زیرا $e^{۱۰۰}$ عددی درست نیست.

$$\frac{100(n)\varphi}{e^{100}}$$

عدد هست که عدد اولند.

۴۰. تحقیق آماری. رابطهٔ (۶) از بند قبلی را در نظر می‌گیریم:

$$N(x_1 , x_2) = \frac{x_2 - x_1}{\log x} \qquad (1)$$

این رابطه، تعداد عددهای اول واقع در فاصلهٔ $x_2 - x_1$ را به‌ما می‌دهد. از نتیجه‌های آماری که در جدول III از بند ۱۲ (آخر بخش ۲) خلاصه کرده‌ایم، استفاده می‌کنیم. این جدول مربوط است به‌عددهای اول دهمین میلیون، یعنی عددهای اول واقع در فاصلهٔ ۹۰۰۰۰۰۰ و ۱۰۰۰۰۰۰۰.

ابتدا رابطهٔ (۱) را دربارهٔ یك فاصله 10^6، بعد دربارهٔ ۱۰ فاصلهٔ باطول 10^5 و بالاخره دربارهٔ 10^4 فاصله با طول ۱۰۰ به‌کار می‌بریم.

برای تمام فاصلهٔ واقع بین ۹ و ۱۰ میلیون تقریباً خواهیم داشت:

$$N(x_1 , x_2) = 62230 \qquad (2)$$

از طرف دیگر مقدارمشاهده شده، برابر ۶۲۰۸۲ می‌باشد، بنابراین اشتباهی برابر۱۴۸خواهیم داشت. می‌دانیم که واحد اشتباه u جذر2npq می‌باشد، اینجا np=۶۲۲۳۰ است و مقدار q بستگی به‌تعداد گلوله‌هائی دارد که فرض کنیم در جعبه‌ای گذاشته‌باشیم، که طبق بند ۱۲ تعداد آنها را معین کرده باشیم، کوچکترین مقداری که می‌توان برای q درنظر گرفت، تقریباً

برابر $\frac{۲}{۳}$ است ، با این حساب مقدار ۲npq تقریباً برابر ۸۳۰۰۰ می‌شود که جذرتقریبی‌آن برابر ۲۹۰ خواهد بود و این واحد اشتباه خواهدبود، و از این تنها آزمایش نمی‌توان نتیجهٔ دقیق‌تری بدست‌آورد.

برای ۱۰ فاصله به‌طول ۱۰۰۰۰۰ در زیر درسطر اول عددمحاسبه شده و درسطر دوم عدد مشاهـده شده و در سطر سوم اختلاف آنها را می‌نویسیم:

(۳)

۶۱۹۳;	۶۲۰۰;	۶۲۰۶;	۶۲۱۳;	۶۲۲۰;	۶۲۲۶;	۶۲۳۳;	۶۲۴۰;	۶۲۴۶;	۶۲۵۳
۶۱۳۶;	۶۱۸۱;	۶۲۰۸;	۶۲۰۲;	۶۲۷۱;	۶۱۷۷;	۶۲۲۳;	۶۲۵۹;	۶۲۴۵;	۶۱۸۲
−۵۷	−۱۹	+۲	−۱۱	+۵۱	−۴۹	−۱۰	+۱۹	−۱	−۷۱

مقدار متوسط و مطلق اشتباه ۲۹ است، واحد اشتباه u جذر ۸۳۰۰ یعنی تقریباً ۹۱می‌باشد. مقدارمطلق اشتباه‌متوسط‌به‌طور‌نظری ۰/۵۶u یعنی کمی بیشتر از ۵۰ است که به طورآشکار بیشتر از مقدار مشاهده‌شدهٔ ۲۹ است. اگر به ۱۰۰۰۰ صدتائی بپردازیم، مقدار متوسط تقریباً ۶/۲۲ و واحـد اشتباه برابر ۲/۹ یعنی ۱۰۰ مرتبه‌کـوچکتر از حالت میلیون می‌شود. اکنون در جدول زیر درسطر اول تعداد عددهای اول هـر۱۰۰ عدد و در سطردوم تعداد فاصله‌های ۱۰۰ عددی‌که شامل این تعداد عدد اول هستند و درسطرسوم مقدارمطلق اشتباه نسبت به‌متوسط ۶/۲۲ را قرارمی‌دهیم:

(۴)

۰	۱۴	۱۳	۱	۱۲	۱۱	۲	۱۰	۳	۹	۴	۸	۵	۷	۶
۲	۳;	۱۰;	۲۹;	۴۲;	۱۲۰;	۲۰۲;	۳۱۷;	۵۷۲;	۷۵۱;	۱۱۴۰;	۱۲۳۷;	۱۷۱۲;	۱۸۱۸;	۲۰۴۴;
۶/۲۲	۷/۷۸	۶/۷۸	۵/۲۲	۵/۷۸	۴/۷۸	۴/۲۲	۳/۷۸	۳/۲۲	۲/۷۸	۲/۲۲	۱/۷۸	۱/۲۲	۰/۷۸	۰/۲۲

دیده می‌شود که بین ۱۰۰۰۰ فاصلهٔ ۱۰۰تایی بیش از نصف آنها (۵۵۷۴=۱۷۱۲+۱۸۱۸+۲۰۴۴) اشتباهی که حد اکثر آن برابر ۱/۲۲ می‌باشد، دارند؛ یعنی حاصلضرب واحد اشتباه در ۰/۴۲ ، متوسط مقدار مطلق اشتباه، تقریباً برابر ۱/۵۷ است که به‌عدد ۱/۵۶ بسیار نزدیک است وقتی که به‌جای ۶/۲۲ عدد درست ۶ را به‌کار بریم. می‌دانیم که این متوسط مقادیر مطلق اشتباهها $\frac{u}{\sqrt{\pi}}=$ ۱/۶۳ می‌باشد . اختلاف کوچک است و این حقیقت که مقدار مشاهده شده کمتر از این مقدار است به‌این معنی است که در اینجا به‌نظم بیشتری نسبت به‌آنچه که با تصارف نتیجه می‌شود برخورد می‌کنیم . خواهیم دید وقتی که فاصله‌ها را برابر ۱۰۰۰۰۰ بگیریم این نظم تأیید می‌شود.

برای چهارمین میلیون (عددهای واقع بین ۳میلیون و۴میلیون) هم وقتی که درمورد آنها هم تعداد عددهای اول واقع در ۱۰۰۰۰ صدتایی را آمارگیری کنیم، نتیجه‌های مشابهی بدست می‌آید. اگر همان ردیف جدول(۴) را مراعات کنیم، جدول زیررا خواهیم داشت ومشاهده می‌شود که بزرگترین نوسان آن با ۶ تطبیق می‌کند که برای آن اشتباه ۰/۶۳ است، درحالیکه اشتباه ۷ برابر ۰/۳۷ می‌شود. تعداد متوسط ۶/۶۳۴ و واحد اشتباه با انتخاب $q=\frac{2}{3}$ برابر ۲/۹۷۵ می‌باشد:

(۵)

۰	۱۴	۱۳	۱	۱۲	۲	۱۱	۳	۱۰	۴	۹	۵	۸	۷	۶
۲	۴;	۱۹;	۳۰;	۶۰;	۱۲۶;	۲۲۱;	۴۰۰;	۴۹۷;	۸۶۲;	۹۵۰;	۱۴۸۰;	۱۵۶۲;	۱۸۵۲;	۱۹۲۵;
۶/۶۳;	۷/۳۷;	۴/۳۷;	۵/۶۳;	۵/۳۷;	۶/۶۳;	۴/۳۷;	۳/۶۳;	۳/۳۷;	۲/۶۳;	۲/۳۷;	۱/۶۳;	۱/۳۷;	۰/۳۷;	۰/۶۳;

متوسط مقادیر مطلق اشتباهات ۱/۶۳ است ، در حالیکه مقدار نظری آن $\frac{u}{\sqrt{\pi}}$ یعنی ۱/۶۷ است، دراینجا هم اختلاف کوچك است، ولی درعوض منفی است، یعنی نظم بیشتری نسبت به‌نظم نظری به‌چشم می‌خورد.

به‌طورخلاصه دیده می‌شودکه رابطهٔاساسی (۱) برای مقادیرنسبتاً کوچك فواصل $x_2 - x_1$ هم نتیجه‌های آماری را تأیید می‌کند. با این وصف، وقتی‌که عدد $N(x_1 ، x_2)$ که به‌وسیلهٔ این رابطه بدست می‌آید کوچك‌باشد، باقانون‌حساب‌احتمالات‌تطبیق‌می‌کندکه اشتباهها، اگرچه‌در حالت مطلق کوچك باشند، ممکن است دریك حالت به‌خصوص بزرگ شوند ، یعنی به‌جای عدد نظری ۶ یا ۷ گاهی به‌عددی برابر صفر یا ۱۴ برخوردکنیم، ولی‌اشتباههای استثنایی به‌همان نسبتی‌که بزرگ‌می‌شوند، طبق قانون اشتباهها‌که مربوط به‌تابع $\Theta(\lambda)$ است، کمیاب می‌شوند.

۴۱. فاصله‌های جداکنندهٔ عددهای اول. بررسی‌فاصله‌هایی که دوعدد اول پشت سرهم را ازهم جدا می‌کنند، نمونهٔ جالبی از لزوم ترکیب قانونهای حساب احتمالات باحساب مقدماتی‌است.

قبلا ازقانون پواسون نام می‌بریم‌که مربوط است به‌توزیع تعداد زیادی نقطه روی یك خط، باطول خیلی بزرگ. درحالیکه تراکم‌متوسط نقطه‌ها (یعنی تعداد نقطه‌های واقع برواحد خط) را بدانیم ، δ (تراکم متوسط) می‌تواند عددکسری‌کوچکتر از واحد باشد.

اگر تعداد نقطه‌های واقع برپاره خط به‌طول x را n فرض کنیم، به طورتقریب $n = \delta x$ می‌شود با انحرافی به‌اندازهٔ $\sqrt{n}$.

رابطهٔ پواسون معلوم می‌کند (برحسب تابع n) که برای وجود

k نقطه روی فاصلهٔ x چه احتمالی وجود دارد ، این احتمال عبارتست از :

$$p_k = e^{-n} \times \frac{n^k}{k!} \qquad (۱)$$

و ازآنجا داریم:

$$p_۰ + p_۱ + \dots + p_k + \dots = \qquad (۲)$$

$$= e^{-n} \left(۱ + \frac{n}{۱} + \dots + \frac{n^k}{k!} + \dots \right) = e^{-n} . e^{n} = ۱$$

اگر فرض کنیم که O مبداء ونقطه‌ای مانند A چنان داشته‌باشیم که $OA = x$ باشد، باتوجه به‌اینکه داریم $n = \delta x$،احتمال اینکه روی OA هیچ نقطه‌ای وجود نداشته باشد می‌شود:

$$p_۰ = e^{-\delta x} \qquad (۳)$$

از طرف دیگر، برای اینکه یك نقطه در فاصلهٔ بینهایت‌کوچك dx واقع درسمت راست A وجود داشته باشد، عبارتست از:

$$p_۱ = \delta dx \qquad (۴)$$

با ضرب رابطه‌های (۳) و (۴)، می‌توان احتمال اینکه نزدیکترین‌نقطهٔ به مبداء O به A بینهایت نزدیك باشد بدست آوریم.

(به‌عبارت‌دقیق‌تر، این نقطه درفاصلهٔ x و$x + dx$ باشد) . این احتمال عبارتست از:

$$pdx = p_{\circ}p_{\backslash} = e^{-\delta x}\,\delta dx \qquad (۵)$$

احتمال اینکه نقطهٔ A (نزدیکتریـن نقطه به O) بین دونقطهٔ B و C، به طولهای b و c، باشد عبارتست از:

$$p_{BC} = \int_{b}^{c} pdx = \int_{b}^{c} e^{-\delta x}\,\delta dx = \qquad (۶)$$

$$= e^{-\delta b} - e^{-\delta c}$$

احتمال اینکه A بین نقطهٔ O و نقطهٔ C باشد عبارتست از:

$$p_{OC} = ۱ - e^{-\delta c} \qquad (۷)$$

طول متوسط OC می‌شود:

$$\eta(OC) = \int_{\circ}^{\infty} e^{-\delta c}\, cdc = \frac{۱}{\delta} \qquad (۸)$$

اگر O را یکی ازنقطه‌های خط راست‌فرض‌کنیم، این نتیجه روشن‌خواهد بود، زیرا درحقیقت طبق‌فرض فاصلهٔ OC برابر$\frac{۱}{\delta}$ مـی‌شود . ولـی در محاسبهٔ ما، نقطهٔ O، یك نقطهٔ انتخابی فرض نشده‌است؛ حالا اگر C' را نقطهٔ انتخابی واقع درسمت‌چپ O ونزدیك‌ترین نقطه به‌آن فرض کنیم (در حالیکه C سمت راست O بود) ، مقدار متوسط DC' هم برابر $\frac{۱}{\delta}$

می‌شود ، به‌نحوی که مقدار متوسط CC' برابر $\frac{۲}{\delta}$ خواهد شد. ممکن است متناقض به‌نظربیاید، زیرا CC' فاصلهٔ غیرمشخصی است که دونقطهٔ مجاور C و C' را ازهم‌جدا می‌کند وما دیدیم که مقدارمتوسط این‌فاصله مساوی $\frac{۱}{\delta}$ بود .

تناقض را به‌ترتیب زیرمی‌توان توضیح داد:

اگر تعداد زیادی نقطه، که معرف فاصله‌های‌نامساوی هستند، بر خطی‌واقع باشند، مقدارمتوسط این‌فاصله‌ها را به‌دوطریق مختلف‌می‌توان تعیین‌کرد. ساده‌ترین و طبیعی‌ترین طریقه اینست که طول بزرگ x را انتخاب‌کنیم؛ اگرروی‌این‌طول n فاصله وجود داشته‌باشد، طول‌متوسط هرفاصله برابر $\frac{x}{n}$ خواهدشد. اما به‌طریق‌زیرهم می‌توان عمل‌کرد؛ نقطه‌ای مانند $O_۱$ به‌تصادف روی طول x درنظر بگیریم وطول فاصله‌ای‌که $O_۱$ روی‌آنست اندازه بگیریم. و این عمل را برای تعداد زیادی نقطه، که به طورتصادفی انتخاب می‌شوند ، مانند $O_۲$ و $O_۳$ و . . . و O_k ، تکرار کنیم. سپس مقدار متوسط طولهای فاصله‌های مربوط به‌نقطه‌های $O_۱$ و $O_۲$ و . . . و O_k را بدست‌آوریم . روشن است‌که طریقهٔ جدیدمحاسبه، مقدارمتوسط‌را بیشتر ازنتیجه‌ای‌که ازراه اول بدست‌آمد، معین‌می‌کند. زیرا اگربه‌تصادف نقطه‌های $O_۱$، $O_۲$، $O_۳$ ، ... و O_kرا انتخاب کنیم، شانس بیشتر این خواهد بودکه این نقطه‌ها روی فاصله‌های‌بزرگتربیفتند تاروی فاصله‌های‌کوچکتر. درحقیقت، احتمال اینکه نقطه روی‌فاصله‌ای به‌طول c قراربگیرد، متناسب با c است، به‌نحوی‌که مقدارمتوسط‌به‌جای رابطهٔ (۸)، از رابطهٔ زیرداده می‌شود:

$$\eta(CC') = \int_0^{\infty} e^{-\delta c} c^2 dc = \frac{2}{\delta} \qquad (9)$$

زیرا می‌دانیم که:

$$\int_0^{\infty} e^{-x} x^2 dx = 2 \int_0^{\infty} e^{-x} x dx \qquad (10)$$

و به‌این ترتیب تناقض موجود کاملا روشن شد.

اگر به‌جای نقطه‌هایی که به‌تصادف روی‌خط راست متصل انتخاب می‌شود،آنها را بین نقطه‌های بامختص درست‌که روی خط معین‌شده‌اند، انتخاب‌کنیم،بازهم می‌توان رابطهٔ پواسون را به‌عنوان یك رابطهٔ‌تقریبی به‌کار برد.

ولی اگر نقطه‌های انتخابی عددهای اول باشند، نمی‌توان آنها را همچون نقطه‌هایی‌که به‌کلی به‌طورتصادفی انتخاب شده‌اند مورد بررسی قرار داد.

ما بررسی را، روی عددهای فرد محدود می‌کنیم، زیرا عددهای زوج هرگز اول نیستند. بنابراین فرض‌کنیم‌که در فاصله‌های انتخابی، احتمال اینکه یك عدد فرد اول باشد برابر $\frac{1}{\delta}$ باشد. a را عدد اول‌فردی فرض می‌کنیم. به‌سادگی دیده می‌شودکه احتمال اینکه $a+2$ اول‌باشد به‌طور قابل ملاحظه‌ای با $\frac{1}{\delta}$ فرق دارد. درحقیقت a عددی است اول و بنابراین بر۲، ۳، ۵ و غیره بخش‌پذیر نیست، پس یکی از دوعدد$a+2$

ویا $a+4$ بر ۳ بخش‌پذیرند وبنابراین از دوحالت یك شانس وجوددارد که $a+2$ بر۳ بخش‌پذیر باشد. درحالیکه فقط یك شانس از ۳ مورد وجود دارد که یك عدد زوج x که به‌تصادف انتخاب شده است بر ۳ بخش‌پذیر باشد. احتمال اینکه یك عدد بر ۳ بخش‌پذیرنباشد (برای اول بودن عدد این شرط لازم است ولی کافی نیست)، عبارتست از:

$$1-\frac{1}{2} \text{ برای } a+2\text{؛ } 1-\frac{1}{3} \text{ برای } a$$

نسبت این دواحتمال عبارتست از:

$$\frac{1}{2}\times\frac{3}{2}=\frac{3}{4}=1-\frac{1}{4} \qquad (11)$$

همچنین a بر۵ بخش‌پذیر نیست وبنابراین یکی از ۴ عدد $a+1$، $a+2$، $a+3$ ، $a+4$ ، $a+5$ بر ۵ بخش‌پذیرخواهند بود؛ وبنابراین‌احتمال بخش‌پذیر بودن $a+2$ بر ۵ برابر $\frac{1}{4}$ (به‌جای $\frac{1}{5}$ برای x) و احتمال بخش‌پذیرنبودن بر۵برابر $1-\frac{1}{4}$ (و برای x، $1-\frac{1}{5}$)، نسبت‌آنها:

$$\frac{3}{4}\times\frac{5}{4}=\frac{15}{16}=1-\frac{1}{16} \qquad (12)$$

باید توجه‌کنیم که یکی از دو عدد $a+2$ یا $a+4$ مطمئناً بر۳بخش‌پذیر است و بنابراین ممکن نیست‌که هردوی‌آنها اول باشند.

به‌طورکلی برای اینکه نزدیکترین‌عدد اول بعد از a ، عدد $a+4$ باشد باید ثابت‌کرد:

اولا : $a+2$ اول نیست.

ثانیاً: $a+۴$ اول هست.

ولی باتوجه به‌آنچه قبلاً گفتیم اگر شرط دوم صادق باشد، شرط اول صادق خواهد بود. ازاینجا نتیجه می‌شود که احتمال اینکه $a+۲$ یا $a+۴$ نزدیکترین عدد اول به a باشند، برای هردویکی است.

ازطرف دیگر، اگر a اول باشد، مطمئناً $a+۶$ بر ۳ بخش‌پذیر نیست و بنابراین احتمال اول بودن $a+۶$ دوبرابر احتمال اول بودن $a+۲$ یا $a+۴$ است (که برای هریك ازآنها یك احتمال بین دوحالت وجود دارد که بر ۳ بخش‌پذیر باشند). اما برای اینکه $a+۶$ نزدیکترین عدد اول به a باشد، نه‌فقط باید $a+۶$ عددی اول باشد بلکه بایدهیچیك از عددهای $a+۲$ و $a+۴$ هم اول نباشند.

۴۲. تحقیق آماری. با ملاحظه‌های قبل‌می‌توان بی‌نظمیهایی که درجدول IV (صفحهٔ ۱۹۳) وجود دارد فهمید. این جدول مقادیر ۱۰۰۰۰ فاصله‌ای که ۱۰۰۰۰ عدد اول بزرگتر از یك میلیون را از هم جدا می‌کنند، معین می‌کند (عددهای‌اول‌بین۱۰۰۰۰۰۳ تا۱۱۳۸۵۸۹)، به‌نحوی که طول متوسط آن به‌تقریب برابر ۱۳/۸۶ می‌باشد. بنابراین احتمال اینکه یك عدد فرد واقع دراین فاصله اول باشد برابر است با:

$$\frac{۲}{۱۳/۸۶}=\frac{۱}{۶/۹۳}=\delta \qquad (۹)$$

دراین جدول N نمایندهٔ تعداد عددهای اول p است که فاصلهٔ هر یك از آنها از عدد اول بلافاصله بزرگتر ازخودش مساوی عددهای زوج متوالی ۲، ۴، ۶ و غیره می‌باشد.

ملاحظه می‌شود که تعداد هریك از فاصله‌ها، برابر ۲ و ۴ تقریباً

جدول IV

N	فاصله
۹۹۰	۲
۹۷۲	۴
۱۶۰۶	۶
۶۸۱	۸
۸۲۷	۱۰
۱۰۰۶	۱۲
۵۱۴	۱۴
۳۶۴	۱۶
۶۶۶	۱۸
۲۹۹	۲۰
۲۹۴	۲۲
۳۹۸	۲۴
۱۵۸	۲۶
۱۸۷	۲۸
۲۸۶	۳۰
۸۵	۳۲
۸۹	۳۴
۱۳۲	۳۶
۴۹	۳۸
۵۵	۴۰
۸۲	۴۲
۲۹	۴۴
۲۶	۴۶
۴۷	۴۸
۱۷	۵۰
۱۶	۵۲
۲۶	۵۴
۱۲	۵۶
۱۴	۵۸
۲۰	۶۰
۳	۶۲
۶	۶۴
۱۱	۶۶
۳	۶۸
۶	۷۰
۴	۷۲
۲	۷۴
۳	۷۶
۰	۷۸
۶	۸۰
۳	۸۲
۲	۸۴
۰	۸۶
۰	۸۸
۲	۹۰
۰	۹۲
۱	۹۴
۰	۹۶
۰	۹۸
۰	۱۰۰
۰	۱۰۲
۰	۱۰۴
۱	۱۰۶

برابر ۱۰۰۰ یعنی یکدهم تعداد مجموع می‌باشد ؛ قریب ۸۰۰۰ فاصله می‌ماند که قریب ۱۶۰۰ عدد، یعنی یك پنجم، مربوط به فاصلهٔ برابر ۶ می‌باشد. می‌بینیم که تحقیق آماری هم تأیید می‌کند که احتمال اول بودن $a+6$ دوبرابر احتمال اول بودن $a+2$ و $a+4$ است . به‌طور کلی این مطلب از جدول تأیید می‌شود که عددهای ستون N رو به کاهش می‌رود، معهذا مقدار بیشتر برای عددهایی که بر کوچکترین عددهای اول ۳ و ۵ بخش‌پذیرند باقی می‌ماند، تأثیر ۷ و ۱۱ صراحت کمتری دارد، که همراه با بی‌نظمیهای کوچك اتفاقی است. برای اینکه اهمیت این بی‌نظمیها روشن شود، درصفحهٔ ۱۹۵؛ جدول V را تنظیم کرده‌ایم که در آن ۱۰۰۰۰ فاصلهٔ متوالی را به ۱۰ فاصلهٔ ۱۰۰۰تائی تقسیم کرده‌ایم و آنها را برای فواصل مساوی ۲ تا ۳۲ در نظر گرفته‌ایم. در بالای هر ستون مرتبهٔ ۱۰۰۰ از فاصله‌ای که در آن ستون مورد مطالعه قرارگرفته گذاشته شده است.
این جدولها را هم مثل جدولهای سابق آقای سوگارف M.Z. Sougarei تنظیم کرده است .

همانطور که گفتیم وقتی که فاصله‌های خیلی بزرگ را بررسی می‌کنیم، می‌توان از قانون پواسون استفاده کرد. با توجه به رابطهٔ (۷)، احتمال اینکه فاصله بیشتر از c باشد برابر $e^{-c\delta}$ است؛ ما این نتیجه را درحالتی که c پشت‌سرهم مقادیر $\frac{2}{\delta}$ ، $\frac{4}{\delta}$ ، $\frac{6}{\delta}$ و ... غیره را انتخاب می‌کند، بیان می‌کنیم. درجدول زیر درسطر اول مقادیر $c\delta$، در سطر دوم مقادیر c ، در سطر سوم مقادیر نظری $10000e^{-c\delta}$ و درسطر آخر مقادیر مشاهده شده آنها را می‌نویسم:

جدول V

	۱	۱۰۰۱	۲۰۰۱	۳۰۰۱	٤۰۰۱	۵۰۰۱	۶۰۰۱	۷۰۰۱	۸۰۰۱	۹۰۰۱	
۲	۱۰۸	۱۰۱	۹۹	۱۰۱	۸۸	۱۰۱	۱۰۲	۹۶	۹۱	۱۰۳	۲
۴	۱۰۸	۹۴	۱۰۰	۱۰۳	۸۹	۹۸	۹۰	۹۹	۱۰۶	۸۵	۴
۶	۱۵۳	۱۷۲	۱۵۹	۱۵۰	۱۵۴	۱۷۱	۱۵۲	۱۶۷	۱۵۴	۱۷۴	۶
۸	۶۴	۶۶	۷۴	۷۲	۷۱	۷۵	۶۶	۶۴	۶۴	۶۵	۸
۱۰	۷۹	۸۶	۸۲	۸۷	۸۱	۸۸	۸۴	۷۹	۷۵	۸۶	۱۰
۱۲	۱۰۴	۱۰۱	۹۱	۱۱۲	۱۱۴	۷۸	۹۴	۱۱۱	۱۱۰	۹۱	۱۲
۱۴	۶۱	۴۴	۴۲	۴۵	۶۱	۵۵	۴۹	۵۲	۶۰	۴۵	۱۴
۱۶	۳۹	۲۶	۴۵	۲۵	۳۴	۳۷	۳۷	۳۶	۳۳	۵۲	۱۶
۱۸	۶۵	۶۹	۵۸	۶۹	۷۶	۵۵	۷۷	۶۹	۵۹	۶۹	۱۸
۲۰	۲۱	۲۹	۳۹	۲۸	۱۶	۳۱	۳۴	۳۶	۳۸	۲۷	۲۰
۲۲	۲۹	۲۵	۲۳	۳۱	۲۹	۳۵	۳۵	۳۱	۳۳	۲۳	۲۲
۲۴	۳۶	۵۳	۳۷	۲۶	۴۷	۳۵	۴۷	۲۸	۳۹	۵۰	۲۴
۲۶	۱۷	۱۴	۱۶	۱۳	۱۴	۱۶	۲۰	۱۴	۱۵	۱۹	۲۶
۲۸	۱۸	۲۱	۱۶	۱۸	۲۱	۱۵	۲۰	۲۱	۲۱	۱۶	۲۸
۳۰	۳۴	۲۹	۲۸	۲۸	۳۰	۳۹	۲۸	۲۴	۲۲	۲۴	۳۰
۳۲	۶	۶	۱۲	۱۳	۹	۶	۶	۸	۱۳	۶	۳۲

$c\delta$	۱	۲	۳	۴	۵	۶	۷	۸
c	۱۳/۸۸	۲۷/۷	۴۱/۶	۵۵/۵	۶۹/۴	۸۳/۳	۹۷/۲	۱۱۱
مشاهده‌شده	۳۶۷۸	۱۳۵۳	۴۹۸	۱۸۳	۶۷	۲۵	۹	۳/۳۱
محاسبه‌شده	۳۹۱۸	۱۲۲۵	۳۴۲	۹۹	۳۰	۴	۱	۰

همانطور که دیده می‌شود به‌جز برای $n = c\delta = ۱$ ، مقادیـر مشاهده شده کمتر ازمقادیرمحاسبه شده هستند ، نسبت مقدار مشاهده شده، به‌مقدار محاسبه شده به‌سرعت کاهش می‌یابـد، بـرای $n = ۵$ این نسبت کمتر از $\frac{۱}{۲}$ و برای $n = ۶$ تقریباً $\frac{۱}{۶}$ وبرای $n = ۷$ برابر $\frac{۱}{۹}$ وبرای $n = ۸$ برابرصفر است. این عددها نشان می‌دهند که فاصله‌های بزرگ به‌طور محسوس از قانون تصادف پیروی می‌کنند.

آمار مورد استفاده، مربوط به‌تعداد نسبتاً کمی از فاصله‌ها بود (فقط ۱۰۰۰۰)، جالب خواهد بود اگر بتوانیم فاصله‌های زیادتری را به خصوص در قلمرو دورتری از سلسلهٔ عددهای درست،مورد بررسی قرار دهیم. شناسائی دقیق تعداد وگسترش فاصله‌های بزرگتر از ۱۰۰ می‌تواند ما را به‌رابطهٔ تجربی برساندکه درمقابل دانشمندان ریاضی برای اثبات کردن گذاشته شود.

فهرست واژه‌ها

با معادلهای فرانسوی آنها

Statistique آمار ـ آماری

Démonstration اثبات

Probabilité احتمال

اراتوستن Eratosthène ریاضیدان، منجم و فیلسوف مشهور مکتب اسکندریه، در ۲۷۶ پیش‌ازمیلاد درسیرنCyrène متولدشد و در ۸۰ سالگی ازگرسنگی‌مرد. طریقه تعیین‌عددهای‌اول هنوزهم‌بنام او به«غربال‌اراتوستن» معروف است.

Associé انباز

Reste باقیمانده

Divisible بخش‌پذیر

Divisibilité بخش‌پذیری

Plus grand commun diviseur بزرگترین مقسوم علیه مشترک

پاسکال Blaise Pascal ریاضیدان ، فیزیک‌دان ، فیلسوف و نویسندهٔ فرانسوی (۱۶۲۳ - ۱۶۶۲) . پاسکال در ۱۲ سالگی بدون استفاده از هیچ کتابی ، بسیاری ازقضیه‌های‌هندسهٔ‌اقلیدسی را ازنو ثابت‌کرد . در۱۸ سالگی کتابی دربارهٔ مقاطع مخروطی نوشت، در ۱۸ سالگی اولین ماشین‌حساب‌را ساخت و در ۲۱ سالگی اساس حساب احتمالات را گذاشت.

Norme پایه

پواسون Siméon-Denis Poisson ریاضیدان فرانسوی (متولد در پیتیویه Ptihiviers) که کارهای اساسی او مربوط به فیزیك ریاضی و مکانیك استدلالی است (۱۷۸۱-۱۸۴۰). این جمله ازپواسیون است «زندگی فقط به‌درد این می‌خورد که انسان به‌دو کارمشغول شود: اول ریاضیات بخواند، دوم ریاضیات درس بدهد .»

تابع	Fonction
تبدیل	Permutation
تجزیه کردن	Décomposer
تحقیق	Vérification
تحقیق تجربی	Vérification empirique
ترکیب	Combinaison
تساوی	Egalité
تفریق	Soustraction
تقابل	Réciprocité
تقارن	Symétrie
تقسیم	Division
تعریف	Définition
تعمیم	Généralisation
توان	Exposant
ثابت کردن	Démontrer
جبری	Algébrique
جدول	Table-tableau
جمع	Addition
جمله	Terme
چند جمله‌ای	Polynome
حاصلضرب	Produit
حساب	Arithmétique

حقیقی Reèl
خارج قسمت Quotient
خط راست Droit
درجه Degré
دسته ـ گروه Groupe
دوجمله‌ای Binôme
دوره ـ تناوب Période
رابطه Relation
رشته Suite
رقم Chiffre
روش Méthode
ریاضیدان Mathématicien
ریشه ـ جواب Racine
ریمان Georges Riemann (۱۸۲۶-۱۸۶۶) ریاضیدان آلمانی متولد دربرسلنی (هانور). کارهای اساسی او روی تابعهای آبلی و به‌وجودآوردن یك نوع هندسهٔ غیراقلیدسی انجام گرفت. درهندسهٔ ریمانی ازیك نقطهٔ خارج خط نمی‌توان خطی رسم کرد که با آن موازی باشد، مجموع زاویه‌های هر مثلث در هندسهٔ ریمانی بیشتر از ۱۸۰ درجه است و مقداری ثابت نیست.
زاویه Angle
زاویهٔ قائمه Angle droit
ستون Colonne
سطر Ligne
صدتایی Centaine
صفر Zéro
صورت (کسر) Numérateur
ضرب Multiplication
ضریب Coefficient

Facteur	عامل
Nombre	عدد
Nombre Premier	عدد اول
Nombre entier	عدد درست
Numérique	عددی
Symbole	علامت
Le crible d'Eratosthène	غربال اراتوستن
Non résidu	غیرمانده
Intervalle	فاصله
Impair	فرد

فرما Pierre de Fermat (۱۶۰۱ - ۱۶۶۵) ریاضیدان بزرگ فرانسوی . با کمك پاسکال حساب احتمالات را به‌وجود آورد و در نظریهٔ عددها ، مطالب زیادی از خود باقی گذاشته است. دو قضیهٔ مهم درنظریهٔ عددها به‌نام اوست: ۱) اگر p عددی اول باشد $a^p - a$ بر p بخش‌پذیر است. ۲) $a^n + b^n = c^n$ برای $n \neq ۲$ دارای جواب درستی نیست.

فیثاغورث Pythagore فیلسوف و ریاضیدان سدهٔششم پیش‌ازمیلاد یونان. زندگی فیثاغورث تا حدی اسرارآمیز است، او مکتب فیثاغوریان را بنیاد گذاشت‌که معتقد بودند همه نمودهای‌جهان (ازمادی و معنوی)سرچشمه‌ای ازعدد دارند وبا عدد قابل توضیح‌اند، به‌مناسبت همین اعتقاد ، فیثاغوریان در همهٔ زمینه‌های ریاضی حساب ، هندسه و نجوم به‌موفقیتهایی رسیدند . قضیهٔ مربع وتر در مثلث قائم‌الزاویه، که نام فیثاغورث را با خودبه‌همراه دارد، باعث شدکه عددهای گنگ قدم به‌عرصهٔ ریاضی بگذارند.

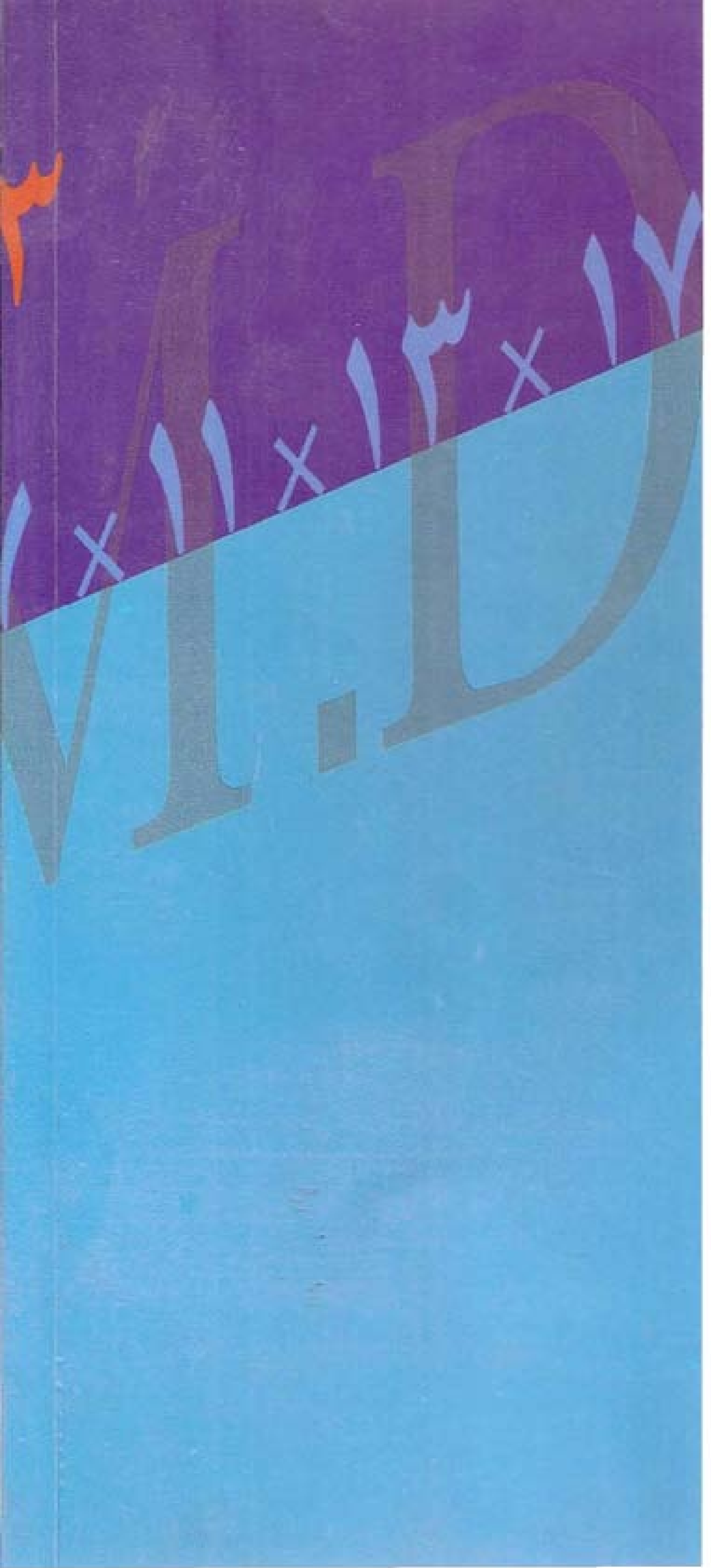
Théorème	قضیه
Plus petit commun multiple	کوچکترین مضرب مشترك

لژاندر Adrien - Marie Legendre ریاضیدان فرانسوی متولد

در پاریس، مؤلف « نظریهٔ عددها » و « نظریهٔ عددهای غیرجبری بیضوی » (۱۸۳۴-۱۷۵۲).

Lemme	لم
Résidu	مانده
Rèsi.lu quadratique	ماندهٔ مربعی
Périodique	متناوب ـ دوره‌ای
Périodiquement	متناوباً
Variable	متغیر
Symetrique	متقارن
Exemple	مثال
Positif	مثبت
Par exemple	مثلا
Calculateur	محاسب
Complexe	مختلط
Dénominateur	مخرج (کسر
Module	مدول
Mutiple	مضرب
Multiple commun	مضرب مشترک
Absolu	مطلق
Equation	معادله
Dividende	مقسوم
Diviseur	مقسوم علیه
Diviseur apparent	مقسوم‌علیه‌آشکار
Diviseur caché	مقسوم علیه مخفی
Diviseur commun	مقسوم‌علیه مشترک
Regulier	منظم
Négatif	منفی

Imaginaire	موهومی
Inégalité	نامساوی
Irregulier	نامنظم ـ بی‌قاعده
Theorie	نظریه
Phénomène	نمود ـ پدیده
Unite	واحد
Congru	همنهشت
Congruence	همنهشتی
Identique	یکسان



Cover design M.R. Nabavy

شابک ۵-۰۸۰۹-۰۰-۹۶۴
ISBN 964-00-0809-5
۱۱۸۸ ۱-۸۱۱۱۸-۸

بها: ۱۰۰۰۰ ریال