اثباتِ دبیرستانی برای قضیهٔ دو مربعِ فرما

محمّدرضا پورنکی

گروه ریاضی و علوم کامپیوتر، دانشگاه تهران و

مرکز تحقیقات فیزیک نظری و ریاضیات

E-mail: pournaki@vax.ipm.ac.ir

چکیده

در این مقاله قضیهٔ دو مربعِ فرما را که بیان می‌کند اعدادِ اوّلِ به شکل $4k+1$ قابل نمایش به‌صورت مجموع دو مربع هستند ثابت خواهیم کرد. همچنین با استفاده از این قضیه تمام اعدادِ طبیعیِ قابل نمایش به‌صورت مجموع دو مربع رده‌بندی خواهند شد.

۱ مقدمه

اعداد اوّلِ ۲، ۳، ۵، ۷، ۱۱ و ۱۳ را در نظر می‌گیریم. توجه می‌کنیم $۱^۲ + ۱^۲ = ۲$، $۱^۲ + ۲^۲ = ۵$ و $۲^۲ + ۳^۲ = ۱۳$، ولیکن ۳، ۷ و ۱۱ را نمی‌توانیم به‌صورت مجموع دو مربع بنویسیم. اگر دقّت کنیم به‌جز ۲، ۵ و ۱۳ اعداد اوّلی به شکل $4k+1$ می‌باشند و ۳، ۷ و ۱۱ اعدادی اوّل به شکل $4k+3$. این موضوع تصادفی نمی‌باشد و در واقع ۲ و تمام اعدادِ اوّلِ به شکل $4k+1$ قابل نمایش به‌صورت مجموع دو مربع هستند و هیچ کدام از اعدادِ اوّلِ به شکل $4k+3$ را نمی‌توان به‌صورت مجموع دو مربع نمایش داد. این مطالب، اوّل بار به‌صورت یکی دیگر از آن یادداشتهای حاشیه‌ای مشهور فرما، در نسخهٔ شخصی او از کتاب دیوفانتوس داده شده بود و از آن پس تاکنون اثبات‌های متعدّدی برای آنچه که به قضیهٔ دو مربعِ فرما مشهور شد، ارائه شده است. در اغلبِ این اثبات‌ها از مطالبی استفاده می‌شود که معمولاً بالاتر از سطح دبیرستان است، امّا در سال ۱۹۹۰ Zagier در [2] اثباتی شگفت‌انگیز از این قضیه ارائه کرد. اثبات او از یک جمله تشکیل شده بود (به‌عنوانِ [2] نگاه کنید)، و از خواص اعضای مرتبهٔ ۲ در گروه‌های متقارن استفاده می‌کرد. به‌نوعی می‌توان خواص مذکور را کاملاً به‌زبان دبیرستانی ترجمه کرد. آنچه در زیر می‌آید، چیزی نیست جز تبدیل مقالهٔ [2] به زبان دبیرستان.

۲ قضیهٔ دو مربعِ فرما

در این بخش می‌خواهیم قضیهٔ دو مربعِ فرما را به روشی که در بخش ۱ اشاره کردیم ثابت کنیم. برای این منظور به تعریف زیر نیاز داریم.

تعریف. فرض کنیم Ω یک مجموعه باشد و $f : \Omega \to \Omega$ [۱] تابعی دلخواه. $x \in \Omega$ را نقطهٔ ثابت f می‌نامیم هرگاه $f(x) = x$. در غیر این صورت x را نقطهٔ غیرثابت f خواهیم نامید.

اکنون فرض می‌کنیم Ω یک مجموعهٔ متناهی باشد. برای fهای خاصی بین تعداد نقاط ثابت f و تعداد اعضای Ω ، $|\Omega|$، ارتباطی نزدیک برقرار است. لم کلیدی زیر این ارتباط را مشخص می‌کند.

لم ۱. فرض کنیم Ω یک مجموعهٔ متناهی باشد و $f : \Omega \to \Omega$ تابعی با این خاصیت که $f \circ f = I$ (I تابع همانی روی Ω است). در این صورت

$$|\Omega| \overset{۲}{\equiv} \text{تعداد نقاط ثابت } f$$

بالاخص تعداد نقاط ثابت f فرد است اگر و فقط اگر $|\Omega|$ فرد باشد.

اثبات. رابطهٔ $\sim$ را روی Ω به‌صورت زیر تعریف می‌کنیم:

$$a \sim b \Leftrightarrow a = b \text{ یا } a = f(b)$$

$\sim$ دارای خاصیت بازتابی است زیرا برای هر $a \in \Omega$، $a = a$ و لذا $a \sim a$.
همچنین $\sim$ دارای خاصیت تقارنی می‌باشد زیرا برای هر $a, b \in \Omega$،

$$\begin{aligned} a \sim b &\Rightarrow a = b \text{ یا } a = f(b) \\ &\Rightarrow b = a \text{ یا } b = f(a) \\ &\Rightarrow b \sim a. \end{aligned}$$

از طرفی $\sim$ دارای خاصیت متعدّی نیز می‌باشد زیرا برای هر $a, b, c \in \Omega$،

$$\begin{aligned} a \sim b, b \sim c &\Rightarrow (a = b \text{ یا } a = f(b)), (b = c \text{ یا } b = f(c)) \\ &\Rightarrow (a = b, b = c) \text{ یا } (a = b, b = f(c)) \text{ یا } (a = f(b), b = c) \text{ یا } (a = f(b), b = f(c)) \\ &\Rightarrow a = c \text{ یا } a = f(c) \text{ یا } a = f(c) \text{ یا } a = c \\ &\Rightarrow a = c \text{ یا } a = f(c) \\ &\Rightarrow a \sim c \ . \end{aligned}$$

۱ـ در این مقاله همواره منظور از تابعِ $f : \Omega \to \Omega$، تابعی است با دامنهٔ تعریف Ω.

در نتیجه $\sim$ یک رابطهٔ هم‌ارزی روی Ω می‌باشد. کلاس هم‌ارزی $a \in \Omega$ ، $[a]$، برابر است با

$$[a] = \{x \in \Omega \mid x \sim a\} \quad = \{x \in \Omega \mid x = a \text{ یا } x = f(a)\}$$

$$= \begin{cases} \{a\} & \text{اگر } a \text{ نقطهٔ ثابتِ } f \text{ باشد} \\ \{a, f(a)\} & \text{اگر } a \text{ نقطهٔ غیرثابتِ } f \text{ باشد} \end{cases}$$

پس کلاس‌های هم‌ارزی این رابطهٔ هم‌ارزی یا یک عضوی‌اند و یا دوعضوی. وقتی کلاس‌های هم‌ارزی تمام عناصر Ω را محاسبه کنیم، کلاس‌های یک عضوی همگی متمایز خواهند بود و تعداد آنها به تعداد نقاط ثابت f است، امّا ممکن است کلاس‌های دو عضوی همگی متمایز نباشند، ولی با در نظرگرفتن کلاس‌های هم‌ارزیِ دو عضویِ متمایز به افراز زیر از Ω دست خواهیم یافت:

$$\Omega = \underbrace{[a_1] \cup \cdots \cup [a_t]}_{\substack{\text{کلاس‌های هم‌ارزی یک عضوی} \\ \text{که به تعداد نقاط ثابت } f \text{ هستند}}} \cup \underbrace{[a_{t+1}] \cup \cdots \cup [a_s]}_{\text{کلاس‌های هم‌ارزی دو عضوی متمایز}}.$$

در نتیجه $|\Omega| = \underbrace{1 + \cdots + 1}_{\text{به تعداد نقاط ثابت } f} + \underbrace{2 + \cdots + 2}_{(s-t) \text{ تا}}$ یا $|\Omega| = 2(s-t) +$ تعداد نقاط ثابت f ، و لذا تعداد نقاط ثابت $f \overset{2}{\equiv} |\Omega|$. بالاخص تعداد نقاط ثابت f فرد است اگر و فقط اگر $|\Omega|$ فرد باشد. □

اکنون آماده‌ایم که قضیهٔ دو مربعِ فرما را با استفاده از لم ۱ ثابت کنیم.

قضیهٔ دو مربعِ فرما. فرض کنیم p عددی اوّل باشد طوری که $p = 2$ یا $p \overset{4}{\equiv} 1$. در این صورت p را می‌توانیم به‌صورت مجموع دو مربع بنویسیم.

اثبات. اگر $p = 2$، آنگاه $p = 1^2 + 1^2$ و لذا حکم ثابت است. پس فرض می‌کنیم $p \overset{4}{\equiv} 1$، و لذا برای یک عدد طبیعی k، $p = 4k + 1$. قرار می‌دهیم

$$\Omega = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}.$$

چون $(1, 1, k) \in \Omega$، لذا Ω مجموعه‌ای ناتهی است. متناهی بودن Ω نیز واضح می‌باشد. اکنون تابع f را روی Ω با ضابطهٔ زیر تعریف می‌کنیم:

$$f(x, y, z) = \begin{cases} (x + 2z, \quad z \quad , \quad y - x - z) & \text{اگر } x < y - z \\ (2y - x, \quad y \quad , \quad x - y + z) & \text{اگر } y - z < x < 2y \\ (x - 2y, \quad x - y + z \quad , \quad y \quad) & \text{اگر } x > 2y \end{cases}$$

توجه می‌کنیم برای هر $(x, y, z) \in \Omega$،

$$(x + 2z)^2 + 4z(y - x - z) = p,$$

$$(۲y-x)^۲ + ۴y(x-y+z) = p,$$

$$(x-۲y)^۲ + ۴(x-y+z)y = p,$$

و لذا $f(x,y,z) \in \Omega$. یعنی f تابعی از Ω به Ω است.

حال ثابت می‌کنیم $f \circ f = I$. برای این منظور گیریم $(x,y,z) \in \Omega$ دلخواه باشد:

حالت اول $x < y - z$

قرار می‌دهیم $X = x + ۲z$، $Y = z$ و $Z = y - x - z$. توجه می‌کنیم که $X > ۲Y$ و لذا

$$\begin{aligned} f \circ f(x,y,z) &= f(f(x,y,z)) = f(x+۲z, z, y-x-z) = f(X,Y,Z) \\ &= (X-۲Y, X-Y+Z, Y) = (x,y,z). \end{aligned}$$

حالت دوم $y - z < x < ۲y$

قرار می‌دهیم $X = ۲y - x$، $Y = y$ و $Z = x - y + z$. توجه می‌کنیم که $Y - Z < X < ۲Y$ و لذا

$$\begin{aligned} f \circ f(x,y,z) &= f(f(x,y,z)) = f(۲y-x, y, x-y+z) = f(X,Y,Z) \\ &= (۲Y-X, Y, X-Y+Z) = (x,y,z). \end{aligned}$$

حالت سوم $x > ۲y$

قرار می‌دهیم $X = x - ۲y$، $Y = x - y + z$ و $Z = y$. توجه می‌کنیم که $X < Y - Z$ و لذا

$$\begin{aligned} f \circ f(x,y,z) &= f(f(x,y,z)) = f(x-۲y, x-y+z, y) = f(X,Y,Z) \\ &= (X+۲Z, Z, Y-X-Z) = (x,y,z). \end{aligned}$$

پس برای هر $(x,y,z) \in \Omega$، $f \circ f(x,y,z) = (x,y,z)$ و لذا $f \circ f = I$.

اکنون می‌خواهیم نقاط ثابت f را به‌دست آوریم، برای این منظور گیریم $(x,y,z) \in \Omega$ نقطه‌ای ثابت از f باشد: $f(x,y,z) = (x,y,z)$.

حالت اول $x < y - z$

$$f(x,y,z) = (x,y,z) \Rightarrow (x+۲z, z, y-x-z) = (x,y,z) \Rightarrow x = y = z = ۰$$

پس $(x,y,z) \notin \Omega$ و لذا این حالت به تناقض منجر می‌شود.

حالت دوم $y - z < x < ۲y$

$$f(x,y,z) = (x,y,z) \Rightarrow (۲y-x, y, x-y+z) = (x,y,z) \Rightarrow x = y$$

چون $(x,y,z) \in \Omega$ لذا $x^۲ + ۴yz = p$ یا $x^۲ + ۴xz = p$ پس $x(x+۴z) = p$ و در نتیجه $x = ۱$ و $x + ۴z = p$ پس $x = y = ۱$ و $z = \frac{p-۱}{۴} = k$، و لذا در این حالت فقط یک نقطهٔ ثابت برای f به‌دست می‌آوریم: $(x,y,z) = (۱, ۱, k)$.

حالت سوم $x > 2y$

$$f(x,y,z) = (x,y,z) \Rightarrow (x-2y, x-y+z, y) = (x,y,z) \Rightarrow x = y = z = 0$$

پس $(x,y,z) \notin \Omega$ و لذا این حالت نیز به تناقض منجر می‌شود.

در نتیجه f فقط و فقط دارای یک نقطهٔ ثابت می‌باشد: $(1,1,k)$. پس تاکنون ثابت کرده‌ایم که Ω مجموعه‌ای است متناهی و $f : \Omega \to \Omega$ این خاصیت را دارد که $f \circ f = I$. چون تعداد نقاط ثابت f فرد (برابر ۱) می‌باشد لذا بنابر لم ۱، $|\Omega|$ نیز فرد خواهد بود. اکنون تابع $g : \Omega \to \Omega$ را با ضابطهٔ $g(x,y,z) = (x,z,y)$ تعریف می‌کنیم. واضح است که $g \circ g = I$ و چون $|\Omega|$ فرد است پس مجدداً بنابر لم ۱ تعداد نقاط ثابت g فرد خواهد بود، پس g لااقل دارای یک نقطهٔ ثابت، مثلاً $(a,b,c) \in \Omega$ است: $g(a,b,c) = (a,b,c)$. این نتیجه می‌دهد که $(a,c,b) = (a,b,c)$ و لذا $b = c$. امّا $(a,b,c) \in \Omega$ پس $a^2 + 4bc = p$ یا $a^2 + 4b^2 = p$، پس $p = a^2 + (2b)^2$ و لذا p به‌صورت مجموع دو مربع خواهد بود. □

۳ رده‌بندی اعدادِ طبیعیِ قابل نمایش به‌صورت مجموع دو مربع

در بخش قبل دیدیم که اگر p عددی اوّل باشد که $p = 2$ یا $p \overset{4}{\equiv} 1$، آنگاه p را می‌توانیم به‌صورت مجموع دو مربع بنویسیم. اکنون نشان می‌دهیم عکس این مطلب نیز درست می‌باشد و لذا در بین اعدادِ اوّلِ p فقط و فقط آنهایی قابل نمایش به‌صورت مجموع دو مربع هستند که $p = 2$ یا $p \overset{4}{\equiv} 1$.

لم ۲. فرض کنیم p عددی اوّل باشد که آن را به‌صورت مجموع دو مربع نوشته‌ایم. در این صورت $p = 2$ یا $p \overset{4}{\equiv} 1$.

اثبات. بنابر فرض اعداد طبیعیِ m و n موجودند که $p = m^2 + n^2$. اکنون ۲ یا ۱ یا ۰ یا -1 $\overset{4}{\equiv} m$ و لذا ۱ یا ۰ $\overset{4}{\equiv} m^2$. به همین ترتیب ۱ یا ۰ $\overset{4}{\equiv} n^2$ و لذا ۲ یا ۱ یا ۰ $\overset{4}{\equiv} p = m^2 + n^2$. امّا چون p اوّل است، لذا فقط این حالت رخ می‌دهد که $p = 2$ یا $p \overset{4}{\equiv} 1$. □

همچنین برای رده‌بندی اعدادِ طبیعیِ قابل نمایش به‌صورت مجموع دو مربع دو لم زیر نیز مورد نیاز است:

لم ۳. فرض کنیم p یک عدد اوّل فرد باشد و x این خاصیت را داشته باشد که $x^2 \overset{p}{\equiv} -1$. در این صورت $p \overset{4}{\equiv} 1$.

اثبات. چون $x^2 \overset{p}{\equiv} -1$ پس لزوماً $(x,p) = 1$ و لذا $x^{p-1} \overset{p}{\equiv} 1$. چون p فرد است می‌توانیم بنویسیم $(x^2)^{\frac{p-1}{2}} \overset{p}{\equiv} (-1)^{\frac{p-1}{2}}$ و لذا لزوماً $\frac{p-1}{2}$ زوج خواهد بود، پس $p \overset{4}{\equiv} 1$. □

لم ۴. فرض کنیم m و n هر دو بتوانند به‌صورت مجموع دو مربع نوشته شوند. در این صورت mn نیز می‌تواند چنین نوشته شود.

اثبات. این لم با توجه به اتحاد $(a^۲+b^۲)(c^۲+d^۲)=(ac+bd)^۲+(ad-bc)^۲$ واضح است. □

اکنون آماده هستیم تا تعیین کنیم دقیقاً کدام اعداد طبیعی می‌توانند به‌صورت مجموع دو مربع نوشته شوند. اولاً بدیهی است که هر مربع $m^۲$ می‌تواند چنین نمایش داده شود: $m^۲=m^۲+۰^۲$.

لذا فرض می‌کنیم n یک عدد طبیعی باشد و می‌نویسیم $n=m^۲n_۰$، که در آن $n_۰$ هیچ عامل اوّل مربعی ندارد. می‌نویسیم $n_۰=p_۱\dots p_t$ که در آن $p_۱$، ...، p_t اعداد اوّل متمایز هستند. با استفاده از قضیهٔ دو مربعِ فرما و لم ۴ ملاحظه می‌کنیم که اگر، به‌ازای هر i، $p_i=۲$ یا $p_i\overset{۴}{\equiv}۱$، آنگاه $n=m^۲p_۱\dots p_t$ می‌تواند به صورت مجموع دو مربع نوشته شود.

بالعکس، فرض کنیم n بتواند به‌صورت مجموع دو مربع نوشته شود: $n=a^۲+b^۲$. ثابت می‌کنیم که اگر بنویسیم $n=m^۲p_۱\dots p_t$ که $p_۱$، ...، p_t اعداد اوّل متمایزند، آنگاه، به‌ازای هر i، $p_i=۲$ یا $p_i\overset{۴}{\equiv}۱$. برای این منظور به روش برهان خلف استدلال می‌کنیم. فرض می‌کنیم برای یک i، $p_i\overset{۴}{\equiv}۳$ (فرض خلف). چون $n=a^۲+b^۲$، لذا داریم $a^۲+b^۲\overset{p_i}{\equiv}۰$. فرض کنیم $p_i\nmid b$، در این صورت $(p_i,b)=۱$ و لذا x و y موجودند که $xp_i+yb=۱$، در نتیجه $yb\overset{p_i}{\equiv}۱$ و لذا با توجه به $a^۲+b^۲\overset{p_i}{\equiv}۰$ به‌دست می‌آوریم $(ya)^۲\overset{p_i}{\equiv}-۱$. اکنون لم ۳ نتیجه می‌دهد که $p_i\overset{۴}{\equiv}۱$ و این تناقض است. پس $p_i\nmid b$ به تناقض منجر می‌شود و لذا $p_i\mid b$. به همین ترتیب $p_i|a$ و لذا

$$p_i^۲|a^۲+b^۲=n=m^۲p_۱\dots p_t.$$

چون $p_۱$، $p_۲$، ...، p_t اعداد اوّل متمایز هستند، باید داشته باشیم $p_i|m^۲$، پس $p_i|m$. بنابراین

$$\left(\frac{a}{p_i}\right)^۲+\left(\frac{b}{p_i}\right)^۲=\left(\frac{m}{p_i}\right)^۲p_۱\dots p_t.$$

هرگاه به‌جای n، $n/p_i^۲$ بگذاریم می‌بینیم که $n/p_i^۲$ مجموع دو مربع است و $n/p_i^۲=w^۲p_۱\dots p_t$. اگر همین استدلال را با قرار دادن $n/p_i^۲$ به‌جای n تکرار کنیم، می‌توانیم عامل دیگر p_i از w را حذف کنیم. با تکرار این فرآیند، سرانجام به عدد طبیعی مانند $n_۱$ می‌رسیم که $n_۱$ مجموع دو مربع است، یعنی $n_۱=c^۲+d^۲$، $n_۱=v^۲p_۱\dots p_t$، به شرط آنکه $p_i\nmid v$. امّا در این صورت اگر یکبار دیگر هم، همین استدلال را به‌کار بریم، به تناقض $p_i|v$ می‌رسیم و لذا فرض خلف باطل می‌باشد. یعنی، برای هر i، $p_i=۲$ یا $p_i\overset{۴}{\equiv}۱$.

یعنی قضیهٔ زیر را به‌طور کامل ثابت کرده‌ایم:

قضیهٔ رده‌بندی. فرض کنیم n عدد طبیعی باشد و می‌نویسیم $n=m^۲n_۰$ که در آن $n_۰$ عامل اوّل مربعی ندارد. در این صورت فقط و فقط وقتی n می‌تواند به‌صورت مجموع دو مربع نوشته شود که عوامل اوّل $n_۰$ فقط در میان اعداد اوّل $p=۲$ و $p\overset{۴}{\equiv}۱$ باشند.

مثال ۱. $۸۸۸ = ۲^۳ \times ۳ \times ۳۷$، بنابراین $۸۸۸ = ۲^۲(۲ \times ۳ \times ۳۷)$. چون $۳ \not\overset{۴}{\equiv} ۱$ می‌بینیم که ۸۸۸ نمی‌تواند به‌صورت مجموع دو مربع نوشته شود.

مثال ۲. $۳۳۲۵۱۴ = ۲ \times ۳^۲ \times ۷^۲ \times ۱۳ \times ۲۹$، بنابراین $۳۳۲۵۱۴ = (۳ \times ۷)^۲(۲ \times ۱۳ \times ۲۹)$. چون $۱ \overset{۴}{\equiv} ۱۳$ و $۱ \overset{۴}{\equiv} ۲۹$، می‌بینیم که ۳۳۲۵۱۴ می‌تواند به صورت مجموع دو مربع نوشته شود. اکنون می‌توانیم از لم ۴ استفاده کنیم و محاسبات را عملاً انجام دهیم: چون $۱۳ = ۲^۲ + ۳^۲$ و $۲۹ = ۲^۲ + ۵^۲$ پس

$$۱۳ \times ۲۹ = (۲^۲ + ۳^۲)(۲^۲ + ۵^۲) = (۲ \times ۲ + ۳ \times ۵)^۲ + (۲ \times ۵ - ۲ \times ۳)^۲ = ۱۹^۲ + ۴^۲$$

و لذا

$$۲ \times ۱۳ \times ۲۹ = (۱^۲ + ۱^۲)(۱۹^۲ + ۴^۲) = (۱ \times ۱۹ + ۱ \times ۴)^۲ + (۱ \times ۴ - ۱ \times ۱۹)^۲ = ۲۳^۲ + ۱۵^۲$$

بالاخره

$$۳۳۲۵۱۴ = (۳ \times ۷)^۲(۲۳^۲ + ۱۵^۲) = (۳ \times ۷ \times ۲۳)^۲ + (۳ \times ۷ \times ۱۵)^۲ = ۴۸۳^۲ + ۳۱۵^۲.$$

مراجع

[1] W. W. Adams, L. J. Goldstein, "*Introduction to number theory*", Prentice-Hall, Inc, 1976.

[2] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), 144.