تابع حسابی اویلر

محمدرضا پورنکی

چکیده

در این مقالهٔ توصیفی، پس از تعریف تابع حسابی اویلر، قضیهٔ اویلر را ثابت خواهیم کرد، سپس فرمولی برای محاسبهٔ مقدار این تابع ارایه خواهد شد و در پایان نیز به ذکر خاصیتی مهم از این تابع خواهیم پرداخت.

مقدمه

در فصل ۶ کتاب ریاضیات گسستهٔ دورهٔ پیش‌دانشگاهی رشتهٔ علوم ریاضی، تابع حسابی اویلر در بخشی تحت نام مجلهٔ ریاضی تعریف شده و سپس قضیهٔ اویلر بیان شده‌است. در قضیه‌ای در فصل ۷ این کتاب هم به کمک اصل شمول و عدم شمول فرمولی برای محاسبهٔ مقدار این تابع در حالتی خاص ارایه شده‌است. در این مقالهٔ توصیفی، هدف آن است که پس از تعریف تابع حسابی اویلر، به اثبات قضیهٔ اویلر بپردازیم و سپس فرمول خاص ذکر شده در بالا را به شکل کلی تبدیل کنیم و یک خاصیت مهم این تابع را ثابت کنیم. در پایان نیز چند مسألهٔ مربوط به این مبحث را جهت حل مطرح می‌کنیم.

تابع حسابی اویلر و دستگاه مخفف مانده‌ها

در زیر، نمادی را معرفی می‌کنیم که منسوب به اویلر است و در ریاضیات به‌طور وسیع از آن استفاده می‌شود.

تعریف ۱ . *برای هر عدد طبیعی n، $\phi(n)$ برابر است با تعداد اعداد طبیعی کوچک‌تر از یا مساوی با n که نسبت به n اولند.*

توجه می‌کنیم که این ضابطه، تابعی روی اعداد طبیعی تعریف می‌کند که آن را تابع حسابی اویلر(یا تابع فیِ اویلر) می‌نامند.

مثال ۱ . *$\phi(۶) = ۲$؛ زیرا بین اعداد ۱، ۲، ۳، ۴، ۵ و ۶ فقط دو عدد، ۱ و ۵، هستند که نسبت به ۶ اولند.*

تذکر. توجه می‌کنیم که $\phi(۱) = ۱$؛ زیرا ۱ نسبت به ۱ اول است! همچنین برای هر $n > ۱$، با توجه به این‌که $(n, n) = n > ۱$[۱]، $\phi(n)$ برابر است با تعداد اعداد طبیعی کوچک‌تر از n که نسبت به n اولند.

مثال ۲ . *اگر p عددی اول باشد آنگاه $\phi(p) = p - ۱$؛ زیرا تمام $p - ۱$ عدد طبیعی کوچک‌تر از p نسبت به p اولند.*

اکنون زیرمجموعه‌هایی از اعداد صحیح را معرفی می‌کنیم که ارتباطی نزدیک با مفهوم تابع حسابی اویلر دارند.

تعریف ۲ . *فرض‌کنیم n عددی طبیعی باشد. زیرمجموعهٔ R از اعداد صحیح را یک دستگاه مخفف مانده‌ها به پیمانهٔ n می‌نامیم هرگاه هر عضو R نسبت به n اول باشد و هر عدد صحیح که نسبت به n اول است دقیقاً با یکی از اعضای R به پیمانهٔ n همنهشت باشد.*

۱) برای دو عدد صحیح a و b که حداقل یکی از آنها غیر صفر است، (a, b) را بزرگ‌ترین مقسوم‌علیه مشترک a و b درنظر می‌گیریم.

شمارهٔ ۱
(اردی‌بهشت ۱۳۷۹) صص ۲۴ـ۱۹

مثال ۳. *برای $n=6$، زیرمجموعهٔ $R=\{1,5\}$ از اعداد صحیح را در نظر می‌گیریم. هر عضو R نسبت به ۶ اول است. حال فرض می‌کنیم x عددی صحیح باشد که نسبت به ۶ اول است. x به پیمانهٔ ۶ دقیقاً با یکی از اعداد ۱، ۲، ۳، ۴، ۵ و ۶ همنهشت است؛ اما چون $(x,6)=1$ پس لزوماً x درست با یکی از اعداد ۱ و ۵ به پیمانهٔ ۶ می‌تواند همنهشت باشد و لذا R یک دستگاه مخفف مانده‌ها به پیمانهٔ ۶ است.*[1]

مثال ۴. *برای $n=p$ که p عددی اول است، زیرمجموعهٔ $R=\{1,2,\ldots,p-1\}$ از اعداد صحیح را در نظر می‌گیریم؛ هر عضو R نسبت به p اول است. حال فرض می‌کنیم x عددی صحیح باشد که نسبت به p اول است. x به پیمانهٔ p دقیقاً با یکی از اعداد ۱، ...، p همنهشت است؛ اما چون $(x,p)=1$ پس لزوماً x درست با یکی از اعداد ۱، ...، $p-1$ به پیمانهٔ p می‌تواند همنهشت باشد و لذا R یک دستگاه مخفف مانده‌ها به پیمانهٔ p است.*

در مثال‌های ۱ و ۲ دیدیم که $\phi(6)=2$ و $\phi(p)=p-1$ که در آن p عددی اول است. در مثال‌های ۳ و ۴ هم دیدیم که تعداد اعضای دستگاه مخفف مانده‌ها به پیمانهٔ ۶ و دستگاه مخفف مانده‌ها به پیمانهٔ p به‌ترتیب برابراست با ۲ و $p-1$. این امر تصادفی نیست و در لم ۱ ثابت می‌کنیم که تعداد اعضای هر دستگاه مخفف مانده‌ها به پیمانهٔ n برابر است با $\phi(n)$.

فرض‌کنیم n عددی طبیعی باشد. اعداد ۱، ۲، ...، n را در نظر می‌گیریم و از بین این فهرست اعداد آنهایی که نسبت به n اولند را جدا می‌کنیم و آنها را i_1،i_2،...،$i_{\phi(n)}$ می‌نامیم(این‌که تعداد این اعداد برابر $\phi(n)$ است، بنا بر تعریف ۱ واضح است). ادعا می‌کنیم $R_n=\{i_1,i_2,\ldots,i_{\phi(n)}\}$ یک دستگاه مخفف مانده‌ها به پیمانهٔ n است: ابتدا توجه می‌کنیم که هر عضو R_n نسبت به n اول است. حال فرض می‌کنیم x عددی صحیح باشد که نسبت به n اول است. واضح است که x به پیمانهٔ n دقیقاً با یکی از اعداد ۱،۲،...،n همنهشت است؛ اما چون $(x,n)=1$ پس لزوماً x درست با یکی از اعداد i_1،i_2،...،$i_{\phi(n)}$ به پیمانهٔ n می‌تواند همنهشت باشد و لذا R_n یک دستگاه مخفف مانده‌ها به پیمانهٔ n است.

تعریف ۳. *برای عدد طبیعی داده‌شدهٔ n، زیرمجموعهٔ R_n از اعداد صحیح که در بالا معرفی‌شد را* دستگاه استاندارد مخفف مانده‌ها به پیمانهٔ n *می‌نامیم.*

لم ۱. *اگر n عددی طبیعی باشد آنگاه تعداد اعداد صحیح در هر دستگاه مخفف مانده‌ها به پیمانهٔ n برابر $\phi(n)$ است.*

برهان. فرض‌کنیم $R=\{r_1,\ldots,r_k\}$ و $S=\{s_1,\ldots,s_l\}$ هر دو دستگاه مخفف مانده‌ها به پیمانهٔ n باشند. هر عضو R نسبت به n اول است و چون R و S هر دو دستگاه مخفف مانده‌ها به پیمانهٔ n هستند، هر عضو R دقیقاً با یک عضو S به پیمانهٔ n همنهشت است و هیچ دو عضوی از R با یک عضو S به پیمانهٔ n همنهشت نیستند و برعکس، چون هر عضو S نسبت به n اول است و R و S هر دو دستگاه مخفف مانده‌ها به پیمانهٔ n هستند، هر عضو S دقیقاً با یک عضو R به پیمانهٔ n همنهشت است و هیچ دو عضوی از S با یک عضو R به پیمانهٔ n همنهشت نیستند؛ بنابراین $k=l$ و لذا تعداد اعضای هر دو دستگاه مخفف مانده‌ها به پیمانهٔ n برابر است. حال چون R_n، دستگاه استاندارد مخفف مانده‌ها به پیمانهٔ n، $\phi(n)$ عضو دارد، پس تعداد اعضای تمام دستگاه‌های مخفف مانده‌ها به پیمانهٔ n برابر $\phi(n)$ است. ■

نتیجه ۱. *فرض‌کنیم n عددی طبیعی باشد و $R=\{r_1,\ldots,r_{\phi(n)}\}$ و $S=\{s_1,\ldots,s_{\phi(n)}\}$ هر دو دستگاه مخفف مانده‌ها به پیمانهٔ n؛ در این صورت، $r_1\cdots r_{\phi(n)}\equiv s_1\cdots s_{\phi(n)}$ (پیمانهٔ n).*

برهان. از برهان لم ۱ نتیجه می‌شود که $r_1\equiv s_{j_1}$ (پیمانهٔ n)، $r_2\equiv s_{j_2}$ (پیمانهٔ n)، ...، $r_{\phi(n)}\equiv s_{j_{\phi(n)}}$ (پیمانهٔ n) که در آن j_1،...،$j_{\phi(n)}$ همان اعداد ۱،...،$\phi(n)$ هستند(احتمالاً با ترتیبی دیگر) و لذا به‌دست می‌آوریم

$$r_1\cdots r_{\phi(n)}\equiv s_{j_1}\cdots s_{j_{\phi(n)}}\equiv s_1\cdots s_{\phi(n)}\ (\text{پیمانهٔ } n).$$

■

[1] توجه می‌کنیم که هریک از $\{7,11\}$ و $\{-1,-5\}$ و $\{5,25\}$ و ... نیز یک دستگاه مخفف مانده‌ها به پیمانهٔ ۶ است.

لم ۲. *فرض‌کنیم n عددی طبیعی باشد و R یک دستگاه مخفف مانده‌ها به پیمانهٔ n. اگر a عددی صحیح باشد که $(a, n) = ۱$ آنگاه $aR = \{ar \mid r \in R\}$ نیز یک دستگاه مخفف مانده‌ها به پیمانهٔ n خواهد بود.*

برهان. چون R دستگاه مخفف مانده‌ها به پیمانهٔ n است، برای هر $r \in R$، $(r, n) = ۱$ و چون $(a, n) = ۱$ پس $(ar, n) = ۱$؛ یعنی هر عضو aR نسبت به n اول است. حال فرض کنیم x عددی صحیح باشد که نسبت به n اول است؛ یعنی $(x, n) = ۱$. چون $(a, n) = ۱$، اعداد صحیح t و t' موجودند که $ta + t'n = ۱$. توجه می‌کنیم که $(t, n) = ۱$؛ پس $(x, n) = ۱$ نتیجه می‌دهد $(tx, n) = ۱$. از این که R دستگاه مخفف مانده‌ها به پیمانهٔ n است نتیجه می‌شود که $r \in R$ موجود است که $tx \equiv r$ (پیمانهٔ n) و در نتیجه برای عددی صحیح مثل l، $tx = r + nl$. اکنون $ta + t'n = ۱$ نتیجه می‌دهد که $x = tax + t'nx$ و لذا

$$x = (r + nl)a + t'nx = ar + nla + t'nx \equiv ar \ (\text{پیمانهٔ } n)\ ;$$

پس ثابت کردیم که x با یکی از اعضای aR به پیمانهٔ n همنهشت است. حال نشان می‌دهیم که x نمی‌تواند با عضو دیگری به پیمانهٔ n همنهشت باشد: اگر $x \equiv ar'$ (پیمانهٔ n) آنگاه $ar \equiv ar'$ (پیمانهٔ n) و $(a, n) = ۱$ نتیجه می‌دهد که $r \equiv r'$ (پیمانهٔ n) و چون R دستگاه مخفف مانده‌ها به پیمانهٔ n است پس $r = r'$؛ یعنی ثابت کرده‌ایم که هر عدد صحیح که نسبت به n اول است با یکی از اعضای aR و فقط با یکی به پیمانهٔ n همنهشت است و درنتیجه بنا بر تعریف ۲، aR دستگاه مخفف مانده‌ها به پیمانهٔ n خواهدبود. ■

قضیه ۱. *(قضیهٔ اویلر) اگر n عددی طبیعی باشد و a عددی صحیح که $(a, n) = ۱$ آنگاه $a^{\phi(n)} \equiv ۱$ (پیمانهٔ n).*

برهان. فرض‌کنیم $R_n = \{i_۱, \ldots, i_{\phi(n)}\}$ دستگاه استاندارد مخفف مانده‌ها به پیمانهٔ n باشد. چون $(a, n) = ۱$، لم ۲ نتیجه می‌دهد که $aR_n = \{ai_۱, \ldots, ai_{\phi(n)}\}$ هم یک دستگاه مخفف مانده‌ها به پیمانهٔ n است؛ پس از نتیجهٔ ۱ به‌دست می‌آوریم $(ai_۱)\cdots(ai_{\phi(n)}) \equiv i_۱ \cdots i_{\phi(n)}$ (پیمانهٔ n) یا $a^{\phi(n)} i_۱ \cdots i_{\phi(n)} \equiv i_۱ \cdots i_{\phi(n)}$ (پیمانهٔ n). چون $i_۱, \ldots, i_{\phi(n)}$ نسبت به n اولند، $i_۱ \cdots i_{\phi(n)}$ هم نسبت به n اول است و در نتیجه، $a^{\phi(n)} \equiv ۱$ (پیمانهٔ n). ■

نتیجه ۲. *(قضیهٔ کوچک فرما) اگر p عددی اول باشد و a عددی صحیح که $(a, p) = ۱$ آنگاه $a^{p-۱} \equiv ۱$ (پیمانهٔ p).*

برهان. با توجه به مثال ۲، $\phi(p) = p - ۱$ و حکم از قضیهٔ اویلر به‌دست می‌آید. ■

نتیجه ۳. *اگر p عددی اول باشد و a عددی صحیح آنگاه $a^p \equiv a$ (پیمانهٔ p).*

برهان. دو حالت وجود دارد: یا $(a, p) = ۱$ و یا $(a, p) \neq ۱$. اگر $(a, p) = ۱$، بنا بر قضیهٔ کوچک فرما $a^{p-۱} \equiv ۱$ (پیمانهٔ p) و لذا $a^p \equiv a$ (پیمانهٔ p). اگر $(a, p) \neq ۱$ آنگاه $(a, p) = p$ و لذا a مضرب p خواهد بود؛ پس $a \equiv ۰$ (پیمانهٔ p) و $a^p \equiv ۰$ (پیمانهٔ p) و لذا $a^p \equiv a$ (پیمانهٔ p). ■

فرمول محاسبهٔ مقدار تابع حسابی اویلر

در این بخش خاصیت مهمی از تابع حسابی اویلر را که به خاصیت ضربی معروف است ثابت خواهیم کرد. این خاصیت، فرمول محاسبهٔ تابع حسابی اویلر را به‌دست می‌دهد.

لم ۳. *فرض‌کنیم m و n دو عدد طبیعی باشند و R و S به‌ترتیب دستگاه مخفف مانده‌ها به پیمانهٔ n و m. اگر $(m, n) = ۱$، آنگاه $A = \{mr + ns \mid r \in R, s \in S\}$ یک دستگاه مخفف مانده‌ها به پیمانهٔ mn است.*

برهان. چون R و S به‌ترتیب دستگاه مخفف مانده‌ها به پیمانهٔ n و m هستند، برای هر $r \in R$ و هر $s \in S$، $(r, n) = ۱$ و $(s, m) = ۱$؛ لذا $(m, n) = ۱$ نتیجه می‌دهد که $(mr, n) = ۱$ و $(ns, m) = ۱$ پس $(mr + ns, n) = ۱$ و $(mr + ns, m) = ۱$ و در نتیجه، $(mr + ns, mn) = ۱$؛ یعنی هر عضو A نسبت به mn اول است. حال فرض کنیم x عددی صحیح باشد که نسبت به mn اول

است؛ یعنی $(x,mn)=۱$. چون $(m,n)=۱$، بنا بر لم ۲ مجموعه‌های mR و nS به‌ترتیب دستگاه مخفف مانده‌ها به پیمانهٔ n و m هستند؛ در نتیجه، بنا بر تعریف ۲ و با توجه به این که $(x,n)=۱$ و $(x,m)=۱$، $r\in R$ و $s\in S$ هستند که (پیمانهٔ m) $x\equiv ns$ و (پیمانهٔ n) $x\equiv mr$ و در نتیجه، (پیمانهٔ m) $x\equiv mr+ns$ و (پیمانهٔ n) $x\equiv mr+ns$. اکنون از $(m,n)=۱$ به‌دست می‌آوریم (پیمانهٔ mn) $x\equiv mr+ns$؛ پس ثابت کردیم که x با یکی از اعضای A به پیمانهٔ mn همنهشت است. حال نشان می‌دهیم که x نمی‌تواند با عضو دیگری از A همنهشت باشد: اگر (پیمانهٔ mn) $x\equiv mr'+ns'$ آنگاه (پیمانهٔ mn) $mr+ns\equiv mr'+ns'$ و در نتیجه (پیمانهٔ m) $mr+ns\equiv mr'+ns'$ و (پیمانهٔ n) $mr+ns\equiv mr'+ns'$؛ پس داریم (پیمانهٔ m) $ns\equiv ns'$ و (پیمانهٔ n) $mr\equiv mr'$. $(m,n)=۱$ نتیجه می‌دهد که (پیمانهٔ m) $s\equiv s'$ و (پیمانهٔ n) $r\equiv r'$ و چون R و S به‌ترتیب دستگاه مخفف مانده‌ها به پیمانهٔ n و m هستند، $s=s'$ و $r=r'$؛ یعنی $mr+ns=mr'+ns'$ و در نتیجه، ثابت کرده‌ایم که هر عدد صحیح که نسبت به mn اول باشد، دقیقاً با یکی از اعضای A به پیمانهٔ mn همنهشت است و لذا بنا بر تعریف ۲، A دستگاه مخفف مانده‌ها به پیمانهٔ mn خواهد بود. ■

لم ۴ . *تابع حسابی اویلر دارای خاصیت ضربی است؛ یعنی برای هر دو عدد طبیعی m و n که $(m,n)=۱$، $\phi(mn)=\phi(m)\phi(n)$.*

برهان. فرض می‌کنیم R دستگاه مخفف مانده‌ها به پیمانهٔ n و S دستگاه مخفف مانده‌ها به پیمانهٔ m باشد؛ پس بنا بر لم ۱، تعداد اعضای R برابر $\phi(n)$ و تعداد اعضای S برابر $\phi(m)$ است و لذا $A=\{mr+ns\mid r\in R, s\in S\}$ دارای $\phi(m)\phi(n)$ عضو خواهد بود. اما $(m,n)=۱$ و بنا بر لم ۳، A دستگاه مخفف مانده‌ها به پیمانهٔ mn است، پس مجدداً بنا بر لم ۱ باید دارای $\phi(mn)$ عضو باشد؛ پس لزوماً $\phi(mn)=\phi(m)\phi(n)$. ■

نتیجه ۴ . *فرض کنیم $p_۱,\dots,p_k$ اعداد اول متمایز باشند و $\alpha_۱,\dots,\alpha_k$ اعداد طبیعی؛ در این صورت*

$$\phi(p_۱^{\alpha_۱}\cdots p_k^{\alpha_k})=\phi(p_۱^{\alpha_۱})\cdots\phi(p_k^{\alpha_k}).$$

برهان. چون $p_۱^{\alpha_۱},\dots,p_k^{\alpha_k}$ دو به دو نسبت به هم اولند، حکم به استقرا از لم ۴ نتیجه می‌شود. ■

توجه می‌کنیم که بنا بر نتیجهٔ ۴، برای به‌دست آوردن فرمول محاسبهٔ مقدار تابع ϕ، کافی‌ست مقدار ϕ را برای توان‌های اعداد اول بدانیم. لم زیر این منظور را برآورده می‌کند.

لم ۵ . *اگر p عددی اول باشد و α عددی طبیعی، $\phi(p^\alpha)=p^\alpha-p^{\alpha-۱}$.*

برهان. اعداد $۱,۲,\dots,p^\alpha$ را که تعدادشان p^α است در نظر می‌گیریم. از بین این اعداد، می‌خواهیم تعداد آنهایی را که نسبت به p^α اولند محاسبه کنیم. اگر x عددی از این فهرست باشد که $(x,p^\alpha)\neq ۱$ آنگاه $(x,p^\alpha)=p^t$ و لذا x مضرب p خواهد بود و برعکس، اگر x مضرب p باشد آنگاه $(x,p^\alpha)\neq ۱$؛ پس در این فهرست، اعدادی که نسبت به p^α اول نیستند دقیقاً مضارب p هستند که عبارتند از $p,۲p,\dots,p^{\alpha-۱}p$ که تعدادشان $p^{\alpha-۱}$ است؛ پس $\phi(p^\alpha)=p^\alpha-p^{\alpha-۱}$. ■

قضیه ۲ . ***(فرمول محاسبهٔ مقدار تابع حسابی اویلر)*** *اگر n عددی طبیعی باشد آنگاه*

$$\phi(n)=\begin{cases} ۱ & \text{اگر } n=۱: \\ n\prod\limits_{\substack{p\mid n\\ \text{اول } p}}(۱-\dfrac{۱}{p}) & \text{اگر } n>۱: \end{cases}$$

تذکر. در قضیهٔ فوق، $\prod\limits_{\substack{p\mid n\\ \text{اول } p}}(۱-\dfrac{۱}{p})$ یعنی حاصل ضرب $(۱-\frac{۱}{p})$ ها به ازای تمام p های اولی که شمارندهٔ n هستند.

برهان. واضح است که اگر $n = ۱$ آنگاه $\phi(n) = ۱$. برای $n > ۱$ بنا بر قضیهٔ اساسی حساب می‌توانیم بنویسیم $n = p_۱^{\alpha_۱} \cdots p_k^{\alpha_k}$ که در آن $p_۱, \ldots, p_k$ اعداد اول متمایزند و $\alpha_۱, \ldots, \alpha_k$ اعداد طبیعی. بنا بر نتیجهٔ ۴ و لم ۵ می‌توانیم بنویسیم

$$\begin{aligned}
\phi(n) &= \phi(p_۱^{\alpha_۱} \cdots p_k^{\alpha_k}) \\
&= \phi(p_۱^{\alpha_۱}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_۱^{\alpha_۱} - p_۱^{\alpha_۱ - ۱}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - ۱}) \\
&= p_۱^{\alpha_۱} \cdots p_k^{\alpha_k} (۱ - \frac{۱}{p_۱}) \cdots (۱ - \frac{۱}{p_k}) \\
&= n(۱ - \frac{۱}{p_۱}) \cdots (۱ - \frac{۱}{p_k}) \\
&= n \prod_{\substack{p \mid n \\ \text{اول } p}} (۱ - \frac{۱}{p}).
\end{aligned}$$

■

مثال ۵. توجه می‌کنیم که $۹۰ = ۲ \times ۳^۲ \times ۵$ و لذا

$$\phi(۹۰) = ۹۰ \prod_{\substack{p \mid ۹۰ \\ \text{اول } p}} (۱ - \frac{۱}{p}) = ۹۰(۱ - \frac{۱}{۲})(۱ - \frac{۱}{۳})(۱ - \frac{۱}{۵}) = ۲۴.$$

اکنون یک خاصیت مهم دیگر از تابع حسابی را مطرح می‌کنیم. برای این منظور، به لم زیر نیاز داریم.

لم ۶. *اگر n عددی طبیعی باشد و $d|n$ آنگاه تعداد اعداد طبیعی کوچک‌تر از یا مساوی با n که بزرگ‌ترین مقسوم‌علیه مشترکشان با n برابر d است مساوی‌ست با $\phi(\dfrac{n}{d})$.*

برهان. مجموعه‌های $A = \{x \in \mathbb{N} \mid ۱ \leq x \leq n, (x, n) = d\}$ و $B = \{x \in \mathbb{N} \mid ۱ \leq x \leq \frac{n}{d}, (x, \frac{n}{d}) = ۱\}$ را در نظر می‌گیریم. A مجموعهٔ اعداد طبیعی کوچک‌تر از یا مساوی با n است که بزرگ‌ترین مقسوم‌علیه مشترکشان با n برابر d است، پس تعداد اعضای A همان تعداد مطلوب در حکم است. B هم مجموعهٔ اعداد طبیعی کوچک‌تر از یا مساوی با $\frac{n}{d}$ است که نسبت به $\frac{n}{d}$ اول هستند و تعدادشان بنا بر تعریف ۱ برابر $\phi(\frac{n}{d})$ است. اکنون اگر ثابت کنیم یک تناظر دوسویی بین A و B موجود است، لم ثابت می‌شود. برای این منظور، تابع $f : A \longrightarrow B$ را با $f(x) = \frac{x}{d}$ در نظر می‌گیریم. توجه می‌کنیم که f به ازای هر x در A تعریف شده است؛ چون وقتی $x \in A$ داریم $۱ \leq x \leq n$ و $(x, n) = d$، $۱ \leq \frac{x}{d} \leq \frac{n}{d}$ و $(\frac{x}{d}, \frac{n}{d}) = ۱$ و لذا $\frac{x}{d} \in B$؛ پس تعریف f خالی از ایراد است. اگر $f(x) = f(x')$ آنگاه $\frac{x}{d} = \frac{x'}{d}$ و لذا $x = x'$ که نشان می‌دهد f یک‌به‌یک است. حال گیریم $y \in B$ عضوی دلخواه از B باشد؛ پس $۱ \leq y \leq \frac{n}{d}$ و $(y, \frac{n}{d}) = ۱$. قرار می‌دهیم $x = yd$؛ پس $۱ \leq x \leq n$ و $(x, n) = d$ و لذا $x \in A$ و چون $f(x) = y$، f پوشاست. f یک تناظر دوسویی بین A و B است و حکم ثابت می‌شود. ■

قضیه ۳. *برای هر عدد طبیعی n،*

$$\sum_{d|n} \phi(d) = n.$$

تذکر. در قضیهٔ فوق، $\sum_{d|n} \phi(d)$ یعنی مجموع $\phi(d)$ ها به ازای تمام d های مثبت که شمارندهٔ n هستند.

برهان. تعریف می‌کنیم $A_d = \{x \in \mathbb{N} \mid ۱ \leq x \leq n, (x, n) = d\}$. بنا بر لم ۶، اگر $d|n$ آنگاه $|A_d| = \phi(\frac{n}{d})$ و به وضوح اگر $d \nmid n$ آنگاه $|A_d| = ۰$ ($|A_d|$ تعداد اعضای A_d است). اگر $x \in A_d \cap A_{d'}$ آنگاه $(x, n) = d$ و $(x, n) = d'$ و لذا $d = d'$؛ پس

برای d های متمایز، A_d ها جدا از هم هستند. گیریم x عددی طبیعی باشد که $1 \leq x \leq n$. اگر $(x,n)=d$ آنگاه $x \in A_d$؛ یعنی $\bigcup_{d=1}^{n} A_d = \{x \in \mathbb{N} \mid 1 \leq x \leq n\}$. جدا از هم بودن A_d ها نتیجه می‌دهد که

$$n = |\{x \in \mathbb{N} \mid 1 \leq x \leq n\}| = \left|\bigcup_{d=1}^{n} A_d\right| = \sum_{d=1}^{n} |A_d| = \sum_{d|n} |A_d| = \sum_{d|n} \phi(\frac{n}{d}).$$

توجه می‌کنیم که اگر $\{d_1, \ldots, d_l\}$ مجموعهٔ تمام شمارنده‌های مثبت n باشد آنگاه $\{\frac{n}{d_1}, \ldots, \frac{n}{d_l}\}$ نیز برابر همین مجموعه است و لذا $\sum_{d|n} \phi(d) = \sum_{d|n} \phi(\frac{n}{d})$ و در نتیجه، $\sum_{d|n} \phi(d) = n$. ■

مثال ۶. *درستی قضیهٔ ۳ را به ازای $n=10$ بررسی می‌کنیم. داریم*

$$\begin{aligned}\sum_{d|10} \phi(d) &= \phi(1)+\phi(2)+\phi(5)+\phi(10)\\ &= 1+1+4+4\\ &= 10.\end{aligned}$$

تمرین.

۱) فرض کنید $n > 2$ عددی طبیعی باشد. ثابت کنید $\phi(n)$ زوج است.

۲) فرض کنید $n > 1$ عددی طبیعی باشد. ثابت کنید مجموع $\phi(n)$ عدد کوچک‌تر از یا مساوی با n که نسبت به n اولند برابر است با $\frac{1}{2}n\phi(n)$.

۳) فرض کنید m و n دو عدد طبیعی باشند که $n|m$. ثابت کنید $\phi(n)|\phi(m)$.

۴) ثابت کنید برای هر عدد طبیعی n، $\phi(n^2) = n\phi(n)$.

۵) فرض کنید m و n دو عدد طبیعی باشند و $d = (m,n)$. ثابت کنید

$$\phi(mn) = \frac{d\phi(m)\phi(n)}{\phi(d)}.$$

۶) کسر(عدد گویای) $\frac{a}{b}$ را تحویل ناپذیر می‌نامیم اگر $(a,b)=1$. ثابت کنید تعداد کسرهای تحویل ناپذیر $\frac{a}{b}$ که $0 < \frac{a}{b} \leq 1$ و $1 \leq b < n$ برابر است با $\phi(1) + \cdots + \phi(n)$.

۷) فرض‌کنید a و b اعداد صحیح و نسبت به هم اول باشند. ثابت‌کنید‌که اعداد صحیح m و n موجودند‌که $a^m + b^n \equiv 1$ (پیمانهٔ ab).

۸) حدس زده شده است که برای هر عدد طبیعی n، عدد طبیعی $m \neq n$ هست که $\phi(m) = \phi(n)$. تاکنون درستی و یا نادرستی این حدس ثابت نشده است. ثابت کنید این حدس در حالتی که n یک عدد اول فرد باشد درست است. آیا این حدس در حالتی که n عدد فرد دلخواهی باشد نیز درست است؟

مراجع

[۱] ویلیام و. آدامز و لری جوئل گولدشتین، آشنایی با نظریهٔ اعداد، ترجمهٔ آدینه محمد نارنجانی. مرکز نشر دانشگاهی، تهران، چاپ اول ۱۳۶۲.

[۲] نیل. اچ. مک‌کوی، نظریهٔ اعداد، ترجمهٔ غلامحسین بهفروز و میرکمال میرنیا. مؤسسهٔ انتشارات امیرکبیر، تهران، ۱۳۶۳.