بخش پذیری و همنهشتی در نظریه اعداد

حسین عربزاده؛ دبیرستان دوره دوم علامه حلی، شهرستان زرند
علی سعیدی؛ دبیرستان دوره دوم علامه حلی، شهرستان زرند
محمد حسین سعیدی؛ دبیرستان دوره دوم علامه حلی، شهرستان زرند

معلم راهنما: دکتر زهیر تویسرکانی؛ اداره آموزش و پرورش شهرستان زرند

چکیده

در این مقاله به بررسی نظریه ی اعداد پرداخته شده است.نظریه اعداد شاخه ای از ریاضیات محض است که در مورد خواص اعداد صحیح بحث می کند.کمال الدین فارسی ریاضیدان و فیزیکدان برجسته ایرانی سهم عمده ای در گسترش نظریه اعداد داشته است. هدف از نوشتن این مقاله آشنایی بیشتر دانش آموزان با نظریه اعداد و قضایای مربوط به آن می باشد . یافته های مهمی مانند قضیه بزرگ فرما وجود دارد که اثبات آن چهارصد سال به طول انجامید که مبحثی بسیار شیرین و قابل بحث است.

واژگان کلیدی: نظریه اعداد،همنهشتی،بخش پذیری،قضیه کوچک و بزرگ فرما،قضیه اویلر.

۱-مقدمه

در نظریه مقدماتی اعداد، اعداد صحیح را بی استفاده از روش‌های به‌کار رفته در سایر شاخه‌های ریاضی بررسی می‌کنند. مسائل بخش پذیری،الگوریتم اقلیدس برای محاسبه ی بزرگترین مقسوم علیه مشترک(ب.م.م)،تجزیه اعداد به اعداد اول،جست و جوی عدد کامل و همنهشتی در این رده هستند. برخی از یافته های مهم این رشته قضیه کوچک فرما،قضیه اعداد اول و قضیه اویلر،قضیه باقیمانده چینی و قانون تقابل درجه دوم هستند. خواص توابع ضربی مانند تابع موبیوس و تابع اویلر و دنباله ی اعداد صحیح و فاکتوریل ها و اعداد فیبوناچی در همین حوزه قرار دارند.

حل بسیاری از مسائل در نظریه مقدماتی اعداد بر خلاف ظاهر ساده آن ها نیازمند کوشش بسیار و به کارگیری روش های نوین است. چند نمونه:

- حدس گلدباخ در مورد نمایش اعداد زوج به صورت جمع دو عدد اول.

- حدس کاتالان در مورد توان های متوالی از اعداد صحیح.

- حدس اعداد اول مرسن در مورد بینهایت بودن اعداد اول مرسن و ...

۲- محتوای اصلی

قرار دادن تعدادی شیء در دسته های مساوی یا دسته بندی کردن تعدادی از چیز ها را بدون آنکه باقی مانده ای داشته باشیم ، «عاد کردن» یا شمارش آن اشیا، توسط شمارنده ها می‌گویند. مثلاً ۱۲ شیء را می توان با شمارنده های مثبت عدد ۱۲ یعنی ۱،۲،۳،۴،۶،۱۲ دسته بندی یا شمارش کرد.

برای نمایش این مفهوم از نماد «|» استفاده کرده و مثلا می نویسیم ۲|۱۲ و میخوانیم عدد ۲ عدد ۱۲ را عاد می کند. به بیان دیگر عدد ۱۲ بر عدد ۲ بخش‌پذیر است.(باقی مانده تقسیم صفر است)

لازم به ذکر است که دسته بندی کردن اشیا در دسته های صفر تایی یا شمارش تعدادی شیء خاص به صورت صفر تا صفر کار بی معنایی است ؛ لذا صفر هیچ عدد غیر صفری را نمی شمارد و هیچ عدد غیر صفری بر صفر بخش‌پذیر نمی باشد در ضمن توجه داشته باشید که هر عدد بر خودش و بر ۱ بخش‌پذیر است؛یعنی اگر a عددی طبیعی باشد 1|a و a|a .

مفهوم بخش‌پذیری را می‌توان برای هر دو عدد صحیح به کار برد مثلا می‌توان گفت عدد ۲۸- بر ۴ بخش‌پذیر است. پس در حالت کلی و با تأمیم مفهوم عاد کردن به مجموعه اعداد صحیح عاد کردن به صورت زیر تعریف می شود:

عدد صحیح a که مخالف صفر است شمارنده عدد b است ـ یا b،a را می شمارد یا a|b یا b بر a بخش‌پذیر است ـ هرگاه عددی صحیح چون q وجود داشته باشد به طوری که b = aq .

اگر عدد b بر عدد a بخش‌پذیر نباشد یا عدد a عدد b را عاد نکند می نویسیم، a ł b

ویژگی های رابطه عاد کردن

ویژگی ۱ : اگر عدد a عدد b را بشمارد، آنگاه هر مضرب صحیح عدد b را نیز می‌شمارد؛ یعنی:

$$a|b \longrightarrow a|mb$$

نتیجه ۱-۱ : اگر عدد a عدد b را بشمارد، آنگاه b^2را می‌شمارد و در حالت کلی b^nرا می‌شمارد که $n\in\mathbf{N}$ است یعنی :

الف) $a|b \longrightarrow a|b^2$

ب) $a|b \longrightarrow a|b^n$

برای اثبات (الف) کافی است از ویژگی ۱ استفاده کرده و m را مساوی با b فرض کرد.

و برای اثبات (ب) کافی است $m=b^{n-1}$ فرض شود.

نتیجه ۱-۲ : از $a|bc$ میتوان نتیجه گرفت که a حداقل یکی از دو عدد b و c را عاد می کند.

نتیجه ۱-۳ : از $a|b$ میتوان نتیجه گرفت که $ka|kb$ در صورتی که k عددی صحیح باشد.

ویژگی ۲: اگر عدد a عدد b را بشمارد و عدد b نیز عدد c را بشمارد آنگاه عدد a عدد c را می‌شمارد.

$$a|b \wedge a|c \longrightarrow a|c$$

اثبات:

$a|b \longrightarrow b = aq_1 \quad (1)$

$b|c \longrightarrow c = bq_2$

$c = bq_1 \quad \ldots \quad q_1q_2 = q \longrightarrow a \ldots \longrightarrow a|c$

این خاصیت را «خاصیت تعدی» برای رابطه عاد کردن می نامیم.

نتیجه ۲-۱ : $a|b \longrightarrow a|b^n$

ویژگی ۳ : هر گاه عددی دو عدد را بشمارد آنگاه مجموع و تفاضل آن دو عدد را نیز می شمارد.

$a|b \wedge a|c \longrightarrow a|b \pm c$

اثبات:

$a|b \longrightarrow b = \ldots \times q_1$

$a|c \longrightarrow \ldots = aq_2$

$b \pm c = \ldots (q_1 \pm q_2) \longrightarrow a|\ldots$ (q)

ویژگی ۴ : اگر $a|b$ و $b \neq 0$ در این صورت $|a| \leq |b|$.

اثبات : چون $a|b$ پس $b = aq$ و چون $b \neq 0$ پس $q \neq 0$ و چون $q \in \mathbf{Z}$ لذا $|q| \geq 1$. حال اگر طرفین نامساوی اخیر را در $|a|$ ضرب کنیم خواهیم داشت : $|a| \leq \ldots \longrightarrow |a| \leq |aq|$

نتیجه ۴-۱ : اگر $a|b$ و $b|a$ آنگاه $a = \pm b$.

هم نهشتی

تعریف : برای هر عدد طبیعی مانند m و هر دو عدد صحیح مانند a و b اگر $m|a-b$ می‌گوییم «a هم‌نهشت با b است به سنج یا پیمانه m »

و مینویسیم $a \overset{m}{\equiv} b$. تعریف رابطه هم نهشتی به پیمانه m به زبان ریاضی عبارت است از :

$$\forall a,b \in \mathbf{Z} \; , \; a \overset{m}{\equiv} b \Leftrightarrow m|a-b \; (m \in \mathbf{N})$$

ویژگی های همنهشتی

ویژگی ۱ : به دو طرف یک رابطه هم نهشتی می توان عددی صحیح را اضافه یا کم کرد.

$$a \overset{m}{\equiv} b \Rightarrow \begin{cases} a+c \overset{m}{\equiv} b+c \\ a-c \overset{m}{\equiv} b-c \end{cases}$$

ویژگی ۲ : دو طرف یک رابطه هم نهشتی را می توان در عددی صحیح ضرب کرد.

$$a \overset{m}{\equiv} b \Rightarrow ac \overset{m}{\equiv} bc$$

ویژگی ۳ : دو طرف یک رابطه هم نهشتی را میتوان به توان n رساند $(n \in \mathbf{N})$

$$a \overset{m}{\equiv} b \Rightarrow a^n \overset{m}{\equiv} b^n$$

ویژگی ۴ : دو طرف رابطه هم نهشتی را که پیمانه های یکسان داشته باشند میتوان باهم جمع یا از هم منها و یا در هم ضرب کرد.

$$a \overset{m}{\equiv} b \ , \ c \overset{m}{\equiv} d \Rightarrow \begin{cases} ac \overset{m}{\equiv} bd & (۱) \\ a+c \overset{m}{\equiv} b+d & (۲) \\ a-c \overset{m}{\equiv} b-d & (۳) \end{cases}$$

ویژگی ۵: می توان به دو طرف یا یک طرف یک رابطه هم نهشتی هر مضربی از پیمانه را اضافه یا از آن کم کرد.

$$a \overset{m}{\equiv} b \Rightarrow \begin{cases} a+mt \overset{m}{\equiv} b+mk \\ a-mt \overset{m}{\equiv} b-mk \end{cases}$$

ویژگی ۶ : اگر بخواهیم دو طرف یک رابطه هم نهشتی را بر عددی تقسیم کنیم باید پیمانه آن هم نهشتی را بر ب‌م‌م آن عدد و پیمانه تقسیم کنیم (این ویژگی را بدون اثبات میپذیریم)

$$ac \overset{m}{\equiv} bc \ , (c,m) = d \Rightarrow a \overset{\frac{m}{d}}{\equiv} b$$

دستگاه مخفف مانده ها

مجموعه A از اعداد صحیح را یک دستگاه مخفف مانده‌ها (د. م. م یا دمم) به هنگ m می‌گوییم هرگاه واجد شرایط زیر باشد:

Aدارای $\phi(m)$ عضو متمایز باشد؛ که در آن ϕ همان تابع فی اویلر است.

اعضای A نسبت به m اول باشند و دو به دو به هنگ m ناهمنهشت باشند.

هر عدد صحیح که نسبت به هنگ m اول است با یک و فقط یکی از اعضای A به هنگ m همنهشت باشد.

نکته ۱: اگر p عددی اول باشد ϕ(p)=p-1

نکته ۲: اگر m=pq و qوp اعدادی اول باشند ϕ (m)=(p-1)(q-1)

قضیه کوچک فرما

قضیه کوچک فرما که برای تمایز آن با قضیه آخر فرما به این نام موسوم است بیان می‌کند اگر یک عدد p اول و a عددی صحیح باشد که در این صورت $p \nmid a$ $a^{p-1} \equiv 1 \pmod{p}$.

این قضیه، اساسی برای آزمون اول بودن فرما است. از این قضیه می‌توان در یافت مرتبه هر عدد متباین با p به هنگ p برابراست با یک. بیانی دیگر از قضیه کوچک فرما نیز وجود دارد که بیان می‌کند اگر p عددی اول و a عددی صحیح باشد آنگاه $a^p \equiv a \pmod{p}$.

همانطور که گفته شد فرما در ابتدا قضیه را بدون اثبات ذکر کرده‌است و اولین اثبات قضیه را گوتفرید لایبنیتس در یک دست‌نویس بدون تاریخ ارائه داده است. او نوشته است که اثبات قضیه را قبل از سال ۱۶۸۳ می‌دانسته است.

اثبات:

البته قضیه شکل خاصی از قضیه کلیتری موسوم به قضیه اویلر است که با اثبات آن در اصل اثبات قضیه فرما نیز انجام شده‌است اما در این قسمت برهان را مخصوص همین قضیه ارائه می‌دهیم.

مجموعه $A = \{1, 2, 3, \ldots, p-1\}$ را در نظر می‌گیریم و فرض می‌کنیم $a \in \mathbb{Z}$ چنان باشد که $p \nmid a$.

چون مجموعه A یک دستگاه مخفف مانده‌ها به هنگ p است و a نسبت به p اول است مجموعه

$$B = \{a, 2a, 3a, \ldots, (p-1)a\}$$

نیز یک دستگاه مخفف مانده‌ها به هنگ p است و لذا بنابر تعریف:

$$1.2.3\ldots(p-1) \equiv a.2a.3a\ldots(p-1)a \pmod{p}$$

پس :

$$1.2.3...(p-1) \equiv [1.2.3...(p-1)]a^{p-1} \pmod{p}$$

لذا داریم:

$$a^{p-1} \equiv 1 \pmod{\frac{p}{(1.2.3...(p-1),p)}}$$

اما چون هر یک از اعداد موجود در A نسبت به p اولند پس حاصل ضربشان نیز نسبت به p اول است و لذا $(1.2.3...(p-1),p)=1$ پس:

$$a^{p-1} \equiv 1 \pmod{p}$$

تعمیم قضیه فرما-قضیه اویلر

قضیه کوچک فرما حالتی خاص از قضیه اویلر است که بیان می‌کند اگر a عددی صحیح و m عددی طبیعی باشد که (a,m)=1آنگاه:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

به آسانی اگر قرار دهید m=p که در آن P عددی اول است، قضیه فرما بدست می‌آید. بعلاوه این قضیه به این صورت نیز قابل تعمیم است که p عددی اول باشد و n,m اعدادی طبیعی باشند

که $m \equiv n \pmod{p-1}$ آنگاه $a^m \equiv a^n \pmod{p}$ این قضیه در تعریف اعداد RSA و رمز گذاری کاربرد فراوان دارد.

قضیه کوچک فرما در مطالعه اعدادRSA ، رمزنگاری، آزمون‌های اول بودن و حل معادلات همنهشتی کاربرد فراوان دارند.

قضیه اویلر

فرض کنید m عددی طبیعی و a عددی صحیح باشد و داشته باشیم (a,m)=1 در این صورت

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

که $\phi(m)$ برابر تعداد اعداد کوچکتر از m است که نسبت به آن اول هستند (همان تعداد اعضاء دستگاه مخفف مانده ها)

اثبات :

ابتدا باید دستگاه مخفف مانده ها را معرفی کنیم. فرض کنید m عددی طبیعی و A مجموعه‌ای از اعداد صحیح باشد .A را یک دستگاه مخفف مانده‌ها به پیمانه m می نامند به شرطی که تمام اعضای A نسبت به mاول باشند و هر عدد صحیح که نسبت به m اول است دقیقاً با یکی از اعضای A به پیمانه m همنهشت باشد.

حال فرض کنید $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ دستگاه مخففی از مانده‌ها به پیمانه m باشد

چون (a,m)=1 پس مجموعه $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ هم دستگاه مخفف مانده‌ها به پیمانه m است زیرا

اگر i و j وجود داشته باشند که $ar_i \equiv ar_j \pmod{m}$

چون (a,m)=1داریم $r_i \equiv r_j \pmod{m}$ که خلاف فرض است و ضمناً چون $(r_i, m)=1$، (a,m)=1، پس $(ar_i, m)=1$ بنابراین $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ هم دستگاه مخفف مانده‌ها به پیمانه m است.

بنابرین هر یک از اعداد $r_1, r_2, \ldots, r_{\phi(m)}$ دقیقاً با یکی از اعداد $ar_1, ar_2, \ldots, ar_{\phi(m)}$ همنهشت است

پس

$$r_1 r_2 \ldots r_{\phi(m)} \equiv ar_1 ar_2 ar_{\phi(m)} \pmod{m}$$

یعنی

$$r_1 r_2 \ldots r_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 r_{\phi(m)} \pmod{m}$$

اما $(r_i, m)=1$

بنابرین $(r_1 r_2 \ldots r_{\phi(m)}, m)=1$ در نتیجه می‌توانیم r_iها را از دو طرف معادله ساده کنیم پس داریم

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

یکی از نتایج قضیه اویلر قضیه فرما است.

قضیه آخر فرما

قضیه آخر فرما یکی از مشهورترین قضیه های تاریخ ریاضیات است. این قضیه می‌گوید:

«معادله $x^n + y^n = z^n$ برای $n > 2$ جواب صحیح و غیر صفر ندارد.»

یعنی اعداد صحیح و غیر صفرx,y,z را نمی‌توان یافت که جواب‌های معادله فوق باشند.

پیر دو فرما ریاضیدان فرانسوی سده ۱۷ (میلادی (در حاشیه کتابی نوشته بود که اثبات این قضیه را در ذهن دارد ولی جای کافی برای نوشتن در اختیار ندارد. این قضیه تا ۱۹۹۴ حل‌نشده باقی مانده بود.)

اندرو وایلز استاد دانشگاه پرینستون در سال ۱۹۹۳ با استفاده از نظریه اعداد پیشرفته، اثباتی برای این قضیه ارائه کرد که دارای مشکلی بود ولی در سپتامبر ۱۹۹۴ اشکال این راه‌حل توسط خود وایلز و با همکاری یکی از همکارانش به نام «تیلر» برطرف شد.

۳- بحث و نتیجه‌گیری

ما در این مقاله نخست به بررسی بخشپذیری و همنهشتی و روابط و ویژگی های آن ها پرداختیم. سپس با استفاده از آنها توانستیم قضیه کوچک فرما و اویلر را اثبات کنیم .

نظریه اعداد مباحث بسیار جالبی دارد به عنوان مثال رمزنگاری یکی از این مباحث است که پژوهشگرانی که علاقه مند اند میتوانند در این باره تحقیق کنند.

منابع

امیری، حمیدرضا .(1386) .ورودی به نظریه اعداد .انتشارات مدرسه.

بهزاد، مهدی؛ رجالی، علی؛ عمیدی، علی و محمودیان، عبدالله .(1396) .کتاب درسی ریاضیات گسسته .سازمان پژوهش و برنامه ریزی وزارت آموزش و پرورش.

D.B. West (2001). Introduction to graph theory.

H.M.Edgar. (2004). A first corse in number theory.

J.A. Bondy, U.S.R.Murty. (2008). Graph theory.

J.H.Van Lint, R.M.Wilson. (2003). A course in Combinatorics.

S.S. Epp (2011). Discrete Mathematics with Applications.

T.Koshy. (2007). Elementary Number Theory with Applications. ELSEVIER.