فصل ۶

همنهشتی

۶ـ۱ـ مفهوم همنهشتی

مفهوم همنهشتی را در سال‌های قبل دیده‌ایم. در زیر خلاصه‌ای از آنچه را که خوانده‌ایم بیان داشته و قضیه‌های مربوط به آن را مطرح می‌کنیم.

مسائلی از قبیل روزهای هفته، ساعت و ماه که حالت گردشی داشته و با افزودن عدد ثابتی (۷روز، ۲۴ ساعت و یا ۱۲ ماه) به وضعیت و شرایط قبلی برمی‌گردند به عنوان مثال‌هایی عملی از نظریهٔ همنهشتی هستند که در اوایل قرن نوزدهم به وسیلهٔ گاوس معرفی شد.

تعریف : فرض می‌کنیم m یک عدد طبیعی باشد، دو عدد صحیح a و b را به پیمانهٔ m **همنهشت** گویند هرگاه a−b مضرب m باشد، یعنی a−b بر m تقسیم‌پذیر باشد.

همنهشت بودن دو عدد a و b به پیمانهٔ m را به صورت‌های زیر نمایش می‌دهند :

$$a \equiv b \ (\text{پیمانهٔ } m)$$

و یا

$$a \overset{m}{\equiv} b$$

و می‌خوانند «**a همنهشت با b به پیمانهٔ m است**[1]»

مثال ۱ : (پیمانهٔ۶)۱۶≡۳۴، زیرا ۱۸=۱۶−۳۴ بر ۶ تقسیم‌پذیر است. ولی (پیمانهٔ۶)۵≢۸، زیرا ۳=۵−۸ بر ۶ تقسیم‌پذیر نیست. ▲

۱ــ حتی در مورد اعداد حقیقی مثلاً در مورد مقادیر زاویه یا طول کمان (برحسب رادیان) در دایرهٔ مثلثاتی (پیمانهٔ 2π) $x \equiv y$ به‌کار می‌رود.

توجه کنید که نقیض (پیمانهٔ m) $a \equiv b$ را چنین می‌نویسند :

$a \not\equiv b$ (پیمانهٔ m)

همان‌طور که در سال قبل دیدیم، همنهشتی یک رابطهٔ هم‌ارزی روی مجموعهٔ اعداد صحیح است و لذا رابطهٔ همنهشتی به پیمانهٔ m، مجموعهٔ $\mathbb{Z}$ را به دسته‌های هم‌ارزی افراز می‌کند. مجموعهٔ تمام دسته‌های همنهشت به پیمانهٔ m را با $\frac{\mathbb{Z}}{m}$ یا $\mathbb{Z}_m$ و مجموعهٔ تمام اعداد صحیحی را که با a همنهشت به پیمانهٔ m هستند با $[a]$ یا $\overline{a}$ نمایش می‌دهند.

$[a]$ یک دستهٔ هم‌ارزی و a نمایندهٔ این دسته است. اگر b عضو دیگری از دستهٔ هم‌ارزی باشد، داریم $[a] = [b]$ و به طور کلی می‌توان ثابت کرد که

$$[a] = [b]$$

اگر و تنها اگر

$a \equiv b$ (پیمانهٔ m)

مثلاً در همنهشتی به پیمانهٔ ۶ داریم :

$$[۱۵] = [۳] = [-۳] = \cdots$$
$$[-۵] = [۱] = [۷] = \cdots$$

اگر چه در دسته‌های همنهشتی، هر عدد از یک دستهٔ همنهشتی می‌تواند نمایندهٔ آن دسته انتخاب شود اما معمولاً کوچک‌ترین عدد صحیح غیرمنفی متعلق به هر دستهٔ همنهشتی را به عنوان نماینده انتخاب می‌کنند.

نکته : بنا به تعریف، از $a \equiv b$ (پیمانهٔ m) نتیجه می‌شود که $a-b$ مضرب m است. یعنی عدد صحیح k موجود است به طوری که $a-b=mk$ یا $a=b+mk$. یعنی تمام اعداد صحیحی که با b به پیمانهٔ m همنهشت‌اند با افزودن مضربی از m بر b به‌دست می‌آیند. بنابراین :

$$[b] = \{b + mk : k \in \mathbb{Z}\}$$

مثال ۲ : مجموعهٔ تمام اعداد صحیح که به پیمانهٔ ۷ با عدد ۴ همنهشت‌اند عبارت است از :

$$[۴] = \{۴+۷k : k \in \mathbb{Z}\} = \{\ldots, -۱۰, -۳, ۴, ۱۱, ۱۸, \ldots\}$$

با توجه به آنچه گفته شد گزاره‌های زیر همگی معادل‌اند.

ـ a به پیمانهٔ m با b همنهشت است.

ـ a و b به پیمانهٔ m همنهشت‌اند.

ـ $a \equiv b$ (پیمانهٔ m)

ـ $[a] = [b]$

ـ a و b در یک دستهٔ همنهشتی به پیمانهٔ m قرار دارند.

ـ a–b مضربی از m است.

ـ $m|(a-b)$

و با استفاده از الگوریتم تقسیم می‌توان ثابت کرد که همهٔ گزاره‌های فوق با گزارهٔ زیر معادل‌اند :

ـ باقیمانده‌های تقسیم a و b بر m با هم برابرند. (چرا؟)

۶ـ۲ـ برخی از ویژگی‌های همنهشتی

رابطهٔ همنهشتی دارای ویژگی‌های مشابهی نظیر جمع و ضرب در $\mathbb{Z}$ است. موارد زیر را قبلاً خوانده‌ایم.

۱ـ اگر $a \equiv b$ (پیمانهٔ m)، آن‌گاه برای هر عدد صحیح c

$a+c \equiv b+c$ (پیمانهٔ m)

۲ـ اگر $a+c \equiv b+c$ (پیمانهٔ m)، آن‌گاه $a \equiv b$ (پیمانهٔ m)

۳ـ اگر $a \equiv b$ (پیمانهٔ m) و $c \equiv d$ (پیمانهٔ m)، آن‌گاه

$a+c \equiv b+d$ (پیمانهٔ m) و $ac \equiv bd$ (پیمانهٔ m)

۴ـ هرگاه $a_1 \equiv b_1$ (پیمانهٔ m) و ... و $a_n \equiv b_n$ (پیمانهٔ m)، آن‌گاه

$$a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \ (\text{پیمانهٔ } m)$$

و

$$a_1 a_2 \ldots a_n \equiv b_1 b_2 \ldots b_n \ (\text{پیمانهٔ } m)$$

۵ ـ هرگاه $a \equiv b$ (پیمانهٔ m) آن‌گاه برای هر $n \geq 1$، $a^n \equiv b^n$ (پیمانهٔ m).

مثال ۳ : مطلوب است باقی‌ماندهٔ 2^{30} بر ۱۷

از $16 = 2^4$ و $16 \equiv -1$ (پیمانهٔ ۱۷) نتیجه می‌شود که $2^4 \equiv -1$ (پیمانهٔ ۱۷) اما $(2^4)^7 \equiv (-1)^7$

یعنی $2^{28} \equiv -1$ (پیمانهٔ ۱۷) از طرف دیگر داریم $2^4 \equiv 4$ (پیمانهٔ ۱۷) و درنتیجه

$$2^{30} = 2^{28} \times 2^2 \equiv (-1) \times 4 = -4 \ (\text{پیمانهٔ } 17)$$

اما (پیمانهٔ ۱۷) ۱۳ ≡ ۴−، پس (پیمانهٔ ۱۷) ۱۳ ≡ $۲^{۳۰}$ یعنی باقی‌ماندهٔ $۲^{۳۰}$ بر ۱۷، عدد ۱۳ است.

۶ـ۳ـ تقسیم طرفین یک رابطهٔ همنهشتی بر c

می‌دانیم که هرگاه $a \equiv b \pmod m$، آنگاه برای هر عدد صحیح c،

$$ac \equiv bc \pmod m$$

حال عکس این مطلب را بررسی می‌کنیم. یعنی آیا برای هر عدد صحیح c، اگر $ac \equiv bc \pmod m$ آنگاه $a \equiv b \pmod m$؟ ابتدا به مثال زیر توجه کنید :

می‌دانیم (پیمانهٔ۶) ۲۱ ≡ ۳۳ یعنی (پیمانهٔ۶) ۳×۷ ≡ ۳×۱۱ ولی (پیمانهٔ ۶) $\frac{۳۳}{۳} \not\equiv \frac{۲۱}{۳}$ اما قضیهٔ زیر را در این مورد داریم :

قضیهٔ ۱ : در رابطهٔ همنهشتی $ac \equiv bc \pmod m$ داریم

$$a \equiv b \left(\frac{m}{d} \text{ پیمانهٔ}\right)$$

که در آن $d=(m,c)$.

اثبات : از فرض نتیجه می‌شود که عدد صحیح k وجود دارد که

$$ac - bc = mk$$

یعنی :

$$(a-b)c = mk$$

اگر طرفین این تساوی را بر $d=(m,c)$ تقسیم کنیم، خواهیم داشت :

$$(a-b)\frac{c}{d} = \frac{m}{d}k$$

یعنی عدد صحیح $\frac{m}{d}$، عدد $(a-b)\frac{c}{d}$ را می‌شمارد. و چون $(\frac{m}{d},\frac{c}{d}) = ۱$ (چرا؟) پس $\frac{m}{d} \mid (a-b)$ یعنی :

$$a \equiv b \left(\frac{m}{d} \text{ پیمانهٔ}\right)$$

مثال ۴ : از (پیمانهٔ ۶) ۲ ≡ ۸ نتیجه می‌شود (پیمانهٔ ۳) ۱ ≡ ۴

۶ـ۴ـ حل معادلهٔ سیالهٔ خطی $ax+by=c$

سؤال دیگری که مطرح می‌شود این است که آیا می‌توان معادلهٔ

$$ax+by=c \quad (۱)$$

را که با معادلهٔ همنهشتی

$$ax \equiv c \ (b \text{ پیمانهٔ})$$

هم‌ارز است، در $\mathbb{Z}$ حل کرد؟ در این معادله $a,b,c \in \mathbb{Z}$. به عبارت دیگر، آیا می‌توان عددهای صحیحی چون x_0, y_0 را یافت که

$$ax_0+by_0=c \quad (۲)$$

اگر عددهای صحیح x_0, y_0 وجود داشته باشند که در رابطهٔ (۲) صدق کنند، آن‌گاه می‌گوییم **معادلهٔ سیالهٔ خطی** $ax+by=c$ جواب دارد. در این رابطه قضیهٔ زیر را داریم :

قضیهٔ ۲ : معادلهٔ سیالهٔ خطی $ax+by=c$ در مجموعهٔ $\mathbb{Z}$ جواب دارد اگر و تنها اگر بزرگ‌ترین مقسوم‌علیه مشترک a و b، عدد c را بشمارد.

اثبات : اگر $d=(a,b)$ و $d|c$ آن‌گاه عدد صحیح k وجود دارد که $c=dk$ و چون d بزرگ‌ترین مقسوم‌علیه مشترک a و b است، $d=am+bn$ که در آن $m,n \in \mathbb{Z}$. بنابراین

$$c=dk=a(mk)+b(nk)$$

یعنی اعداد صحیح $x_0=mk$ و $y_0=nk$ در معادلهٔ $ax+by=c$ صدق می‌کنند. پس $ax+by=c$ دارای جواب است. برعکس اگر $ax+by=c$ دارای جواب باشد، اعداد صحیح x_0 و y_0 وجود دارند که $ax_0+by_0=c$. اما چون $d|a$ و $d|b$ درنتیجه $d|ax_0+by_0$

یعنی $d|c$. ■

می‌توان ثابت کرد که اگر $(a,b)=d$ و x_0 و y_0 یک جواب برای معادلهٔ خطی $ax+by=c$ باشد، آن گاه تمام جواب‌های آن به‌صورت $x=x_0+k\frac{b}{d}$ و $y=y_0-k\frac{a}{d}$ است که در آن $k \in \mathbb{Z}$.

در مثال‌های زیر، روش‌هایی را برای حل معادله‌های سیاله نشان می‌دهیم :

مثال ۵ : شخصی می‌خواهد با بُن، ۵۱۰۰ ریال کتاب بخرد. اگر بُن‌ها، ۵۰۰ ریالی و ۲۰۰ ریالی باشند، چند بُن ۵۰۰ ریالی و چند بُن ۲۰۰ ریالی باید بپردازد؟

حل مسأله مستلزم پیدا کردن اعداد صحیح نامنفی x و y است که برای آنها

$$۲۰۰x+۵۰۰y=۵۱۰۰$$

یا

$$۲x+۵y=۵۱$$

چون $(۵,۲)=۱$ و $۱|۵۱$، معادلهٔ فوق جواب دارد. می‌نویسیم :

$$x=\frac{۵۱-۵y}{۲}=\frac{۵۰-۴y+۱-y}{۲}=۲۵-۲y+\frac{۱-y}{۲}$$

پس $\frac{۱-y}{۲}$ یک عدد صحیح است، یعنی عددی مانند m وجود دارد که $۱-y=۲m$. یا $y=۱-۲m$.

درنتیجه

$$x=۲۵-۲+۴m+m=۵m+۲۳$$

ولی x و y منفی نیستند، پس $۱-۲m\geq ۰$ و $۵m+۲۳\geq ۰$ یا $m\leq \frac{۱}{۲}$ و $m\geq \frac{-۲۳}{۵}=-۴/۶$. پس m مقادیر ۰ ، ۱- ، ۲- ، ۳- و۴- را می‌گیرد. یعنی تعداد بن‌های ۲۰۰ ریالی و ۵۰۰ ریالی به‌ترتیب می‌تواند جفت‌های زیر باشند :

۹,۳ ۷,۸ ۵,۱۳ ۳,۱۸ ۱،۲۳

مثال ۶ : جواب‌های عمومی معادلهٔ سیالهٔ $۷x+۵y=۱۱$ را بیابید.

$$۷x+۵y=۱۱\Rightarrow ۷x\overset{۵}{\equiv}۱۱,\begin{cases}۷\overset{۵}{\equiv}۲\\ ۱۱\overset{۵}{\equiv}۱\end{cases}\Rightarrow ۲x\overset{۵}{\equiv}۱$$

$$\Rightarrow ۲x\overset{۵}{\equiv}۱+۵\Rightarrow ۲x\overset{۵}{\equiv}۲\times ۳\overset{(۲,۵)=۱}{\Rightarrow} x\overset{۵}{\equiv}۳$$

$$\Rightarrow x=۵k+۳\overset{k=۰}{\Rightarrow} x_۰=۳\Rightarrow y_۰=-۲$$

$$\Rightarrow\begin{cases}x=۳+۵k\\ y=-۲-۷k\end{cases}$$

تابع حسابی اویلر

تعریف : برای هر عدد طبیعی n، $\phi(n)$ عبارت است از تعداد اعداد طبیعی کوچک‌تر از یا مساوی با n که نسبت به n اول‌اند. این ضابطه، تابعی روی اعداد طبیعی تعریف می‌کند که آن را تابع حسابی اویلر می‌گویند.

اگر $n = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$ **در این صورت**

$$\varphi(n) = n(1-\frac{1}{p_1}) \ldots (1-\frac{1}{p_k})$$

بدیهی است که اگر p یک عدد اول باشد آن‌گاه $\phi(p)=p-1$.

قضیهٔ اویلر : اگر m عددی طبیعی و a عددی صحیح باشد که $(a,m)=1$ **آن‌گاه**

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

قضیهٔ ویلسن : اگر p عددی اول باشد آن‌گاه

$(p-1)! \equiv -1 \pmod{p}$ **(پیمانهٔ p)**

۶ ـ ۵ ـ تمرین‌ها

۱ــ دو عدد a و b به‌صورت‌های زیر نوشته شده‌اند :

$a=7k+5 \quad , \quad b=7k'-2$

دستهٔ همنهشتی $a+2b$ را به پیمانهٔ ۷ مشخص کنید.

۲ــ هرگاه $a \equiv b \pmod{m}$ و d یک مقسوم‌علیه m باشد، نشان دهید $a \equiv b \pmod{d}$.

۳ــ ثابت کنید

الف) اگر r باقی‌ماندهٔ تقسیم a بر m باشد، آن‌گاه $a \equiv r \pmod{m}$.

ب) اگر $a \equiv b \pmod{m}$ و c عدد صحیح باشد، آن‌گاه

$ac \equiv bc \pmod{m}$

پ) اگر $a+b \equiv c \pmod{m}$، آن‌گاه $a \equiv c-b \pmod{m}$

ت) اگر m و c نسبت به هم اول باشند و $ac \equiv bc \pmod{m}$، آن‌گاه $a \equiv b \pmod{m}$

۴ــ ثابت کنید که برای هر دو عدد صحیح a و b

الف) $(a \pm b)^2 = a^2 + b^2 \pmod{ab}$

ب) $(a \pm b)^3 = a^3 \pm b^3 \pmod{ab}$

۵ــ ثابت کنید $2^{11} - 1$ بر ۲۳ تقسیم پذیر است.

۶ــ آخرین رقم سمت راست هریک از اعداد 3^{424} و 7^{101} را به‌دست آورید.

۷ــ برای هریک از معادلات سیالهٔ زیر یا تمام جواب‌ها را به‌دست آورید و یا ثابت کنید جواب ندارد.

الف) $2x + 5y = 11$ ب) $17x + 13y = 100$

پ) $21x + 14y = 147$ ت) $60x + 18y = 97$

۸ــ پستخانه‌ای فقط تمبرهای ۱۴۰ و ۲۱۰ ریالی برای فروش دارد. برای چسباندن تمبر به بسته‌هایی که مقدار تمبر لازم برای آنها هریک از مقادیر زیر است، در صورت امکان ترکیبی از این دو نوع تمبر تعیین کنید.

الف) ۳۵۰۰ ریال ب) ۴۰۰۰ ریال

مجلهٔ ریاضی

برای اعداد طبیعی $n \geq 3$ معادلهٔ سیالهٔ $x^n + y^n = z^n$ هیچ جواب غیربدیهی در بین اعداد صحیح ندارد.

بسیاری ازمطالعات و پیشرفت‌های نظریهٔ اعداد مدیون تلاش برای حل این مسأله بوده که فرما در قرن هفدهم در حاشیهٔ کتاب حساب دیوفانتوسی خود ادعا کرده که این مسأله را حل کرده است. در سال ۱۹۹۳ با استفاده از نظریه‌های پیشرفتهٔ ریاضی آندرو وایلز حلی برای آن ارائه کرد که پس از چندی اشکالی در آن پیدا شد. ولی سرانجام در سپتامبر ۱۹۹۴ (شهریور ماه ۱۳۷۳) اشکال این حل به‌وسیلهٔ خود وایلز و با همکاری یکی از همکارانش به نام تیلر برطرف شد.

مراجع

1- D.M. Burton, Elementary Number Theory, Allyn and Bacon, Inc. 1976.

2- K.H. Rosen, Elementary Number Theory and its Applications, 3rd ed., Addison Wesley 1992.

۳ــ ویلیام و. آدامز و لری جوئل گولدشتین، آشنایی با نظریهٔ اعداد، ترجمهٔ آدینه محمدنارنجانی، مرکز نشر دانشگاهی، تهران، چاپ اول ۱۳۶۲.

۴ــ ابوالقاسم قربانی و حسن صفاری، حساب استدلالی، چاپ ششم مؤسسه مطبوعاتی علی‌اکبر علمی ۱۳۴۷.

۵ــ غلامرضا دانش ناروئی و میرزا جلیلی، ریاضیات جدید سال چهارم متوسطه عمومی ریاضی‌ــ فیزیک. دفتر تألیف کتاب‌های درسی وزارت آموزش و پرورش ۱۳۶۰.

۶ــ غلامحسین مصاحب، تئوری مقدماتی اعداد. جلد اول ــ انتشارات دهخدا ۱۳۵۳.