# فصل ۶

# همنهشتی

## ۶ــ۱ــ 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 ۱۲ماه) به وضعیت و شرایط قبلی برمی‌گردند به عنوان مثال‌هایی عملی از نظریه‌ی همنهشتی هستند که در اوایل قرن نوزدهم به وسیله‌ی گاوس معرفی شد.

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

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

$$a \equiv b \ (\text{پیمانه‌ی } m)$$

و یا

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

و می‌خوانند «**a همنهشت با b به پیمانه‌ی m است**[۱]»

**مثال ۱** : $۱۶ \equiv ۳۴ \ (\text{پیمانه‌ی } ۶)$ ، زیرا $۱۸ = ۱۶ - ۳۴$ بر ۶ تقسیم‌پذیر است. ولی $۵ \not\equiv ۸ \ (\text{پیمانه‌ی } ۶)$ ، زیرا $۳ = ۵ - ۸$ بر ۶ تقسیم‌پذیر نیست.

$\Delta$

---

۱ــ حتی در مورد اعداد حقیقی مثلاً در مورد مقادیر زاویه یا طول کمان (برحسب رادیان) در دایره‌ی مثلثاتی $x \equiv y \ (\text{پیمانه‌ی } ۲\pi)$ به‌کار می‌رود.

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

$a \not\equiv b$ (پیمانه‌ی$m$)

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

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

$$[a]=[b]$$

اگر و تنها اگر

$a \equiv b$ (پیمانه‌ی $m$)

مثلاً در همنهشتی به پیمانه‌ی ۶ داریم :

$$[۱۵]=[۳]=[-۳]=\cdots$$

$$[-۵]=[۱]=[۷]=\cdots$$

$\Delta$

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

**نکته:** بنا به تعریف، از (پیمانه‌ی $m$) $a \equiv b$ 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 پیمانه‌ی $m$ همنهشت‌اند با افزودن مضربی از $m$ بر $b$ به‌دست می‌آیند. بنابراین :

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

**مثال ۲:** مجموعه‌ی تمام اعداد صحیح که به پیمانه‌ی ۷ با عدد ۴ همنهشت‌اند عبارت است از :

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

$\Delta$

با توجه به آنچه گفته شد گزاره‌های زیر همگی معادل‌اند.

ـ a به پیمانه‌ی m با b همنهشت است.

ـ a و b به پیمانه‌ی m همنهشت‌اند.

ـ $a \equiv b \pmod{m}$ (پیمانه‌ی m)

ـ $[a] = [b]$

ـ a و b در یک دسته‌ی همنهشتی به پیمانه‌ی m قرار دارند.

ـ a–b مضربی از m است.

ـ $m \mid (a-b)$

و با استفاده از الگوریتم تقسیم می‌توان ثابت کرد که همه‌ی گزاره‌های فوق با گزاره‌ی زیر معادل‌اند :

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

## ۶ـ۲ـ برخی از ویژگی‌های همنهشتی

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

۱ـ اگر $a \equiv b \pmod{m}$ (پیمانه‌ی)، آن‌گاه برای هر عدد صحیح c

$a + c \equiv b + c \pmod{m}$ (پیمانه‌ی)

۲ـ اگر $a + c \equiv b + c \pmod{m}$ (پیمانه‌ی)، آن‌گاه $a \equiv b \pmod{m}$ (پیمانه‌ی)

۳ـ اگر $a \equiv b \pmod{m}$ (پیمانه‌ی) و $c \equiv d \pmod{m}$ (پیمانه‌ی)، آن‌گاه

$a + c \equiv b + d \pmod{m}$ (پیمانه‌ی) و $ac \equiv bd \pmod{m}$ (پیمانه‌ی)

۴ـ هرگاه $a_1 \equiv b_1 \pmod{m}$ (پیمانه‌ی) و ... و $a_n \equiv b_n \pmod{m}$ (پیمانه‌ی)، آن‌گاه

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

و

$$a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod{m}$$ (پیمانه‌ی)

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

**مثال ۳:** مطلوب است باقی‌مانده‌ی $2^{30}$ بر ۱۷

از $۱۶ = ۲^۴$ و (پیمانه‌ی ۱۷) $۱۶ \equiv -۱$ نتیجه می‌شود که (پیمانه‌ی ۱۷) $۲^۴ \equiv -۱$ اما (پیمانه‌ی ۱۷) $(-۱)^۷ \equiv (۲^۴)^۷$ یعنی (پیمانه‌ی ۱۷) $۲^{۲۸} \equiv -۱$ از طرف دیگر داریم (پیمانه‌ی ۱۷) $۲^۲ \equiv ۴$ و درنتیجه

(پیمانه‌ی ۱۷) $۲^{۳۰} = ۲^{۲۸} \times ۲^۲ \equiv (-۱) \times ۴ \equiv -۴$

اما (پیمانه‌ی ۱۷) $-۴ \equiv ۱۳$ ، پس (پیمانه‌ی ۱۷) $۲^{۳۰} \equiv ۱۳$ یعنی باقی‌مانده‌ی $۲^{۳۰}$ بر ۱۷، عدد ۱۳ است. $\Delta$

## ۶ـ۳ـ تقسیم طرفین یک رابطه‌ی همنهشتی بر c

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

(پیمانه‌ی m) $ac \equiv bc$

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

می‌دانیم (پیمانه‌ی۶) $۲۱ \equiv ۳۳$ یعنی (پیمانه‌ی ۶) $۳ \times ۷ \equiv ۳ \times ۱۱$، ولی (پیمانه‌ی ۶) $\frac{۲۱}{۳} \neq \frac{۳۳}{۳}$ اما قضیه‌ی زیر را در این مورد داریم :

**قضیه۱:** در رابطه‌ی همنهشتی (پیمانه‌ی m) $ac \equiv bc$ داریم

(پیمانه‌ی $\frac{m}{d}$) $a \equiv b$

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 $(\frac{m}{d},\frac{c}{d})=1$ (چرا؟) پس $\frac{m}{d}|(a-b)$ یعنی :

$a \equiv b \ (\text{پیمانه‌ی } \frac{m}{d})$

□

**مثال ۴:** از (پیمانه‌ی ۶) $۲ \equiv ۸$ نتیجه می‌شود (پیمانه‌ی ۳) $۱ \equiv ۴$ Δ

## ۶ــ۴ــ حل معادله‌ی سیاله‌ی خطی $ax+by=c$

سؤال دیگری که مطرح می‌شود این است که آیا می‌توان معادله‌ی

(۱) $ax+by=c$

را که با معادله‌ی همنهشتی

$ax \equiv c \ (\text{پیمانه‌ی } b)$

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

(۲) $ax_\circ + by_\circ = c$

اگر عددهای صحیح $x_\circ, y_\circ$ وجود داشته باشند که در رابطه‌ی (۲) صدق کنند، آن‌گاه می‌گوییم **معادله‌ی سیاله‌ی خطی** $ax+by=c$ جواب دارد. در این رابطه قضیه‌ی زیر را داریم :

**قضیه‌ی ۲:** معادله‌ی سیاله‌ی خطی $ax+by=c$ در مجموعه‌ی $\mathbb{Z}$ 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 $x_\circ = mk$ و $y_\circ = nk$ در معادله‌ی $ax+by=c$ صدق می‌کنند. پس $ax+by=c$ دارای جواب است. برعکس اگر $ax+by=c$ دارای جواب باشد، اعداد صحیح $x_\circ$ و $y_\circ$ وجود دارند که $ax_\circ + by_\circ = c$ . اما چون $d|a$ و $d|b$ درنتیجه $d|ax_\circ + by_\circ$ یعنی $d|c$ .

□

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

در مثال زیر، روشی 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 ۵۰۰ریالی 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 $۱|۵۱$، معادله‌ی 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

$\Delta$

**مجله‌ی ریاضی**

## 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.

بدیهی است که اگر $p$ یک عدد اول باشد آن‌گاه $\phi(p) = p - ۱$.

**قضیه‌ی اویلر:** اگر $m$ عددی طبیعی و $a$ عددی صحیح باشد که $(a, m) = ۱$ آن‌گاه

$$a^{\phi(m)} \equiv ۱ \pmod{m}$$

**قضیه‌ی ویلسن:** اگر $p$ عددی اول باشد آن‌گاه

$$(p-۱)! \equiv -۱ \pmod{p}$$

### ۶ــ۵ــ تمرین‌ها

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

$$a = ۷k + ۵ \ , \ b = ۷k' - ۲$$

دسته‌ی همنهشتی $a + ۲b$ را به پیمانه‌ی 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 $r$ باقی‌مانده‌ی 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) (پیمانه‌ی ab)** $(a \pm b)^2 \equiv a^2 + b^2$

**ب) (پیمانه‌ی ab)** $(a \pm b)^3 \equiv a^3 \pm b^3$

**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 سیاله‌ی 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**

## مجله‌ی ریاضی

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

بسیاری ازمطالعات و پیشرفت‌های نظریه‌ی اعداد مدیون تلاش برای حل این مسأله بوده که فرما در قرن هفدهم در حاشیه‌ی کتاب حساب دیوفانتوسی خود ادعا کرده که این مسأله را حل کرده است. در سال ۱۹۹۳ با استفاده از نظریه‌های پیشرفته‌ی 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 به‌وسیله‌ی خود وایلز و با همکاری یکی از همکارانش به نام تیلر برطرف شد.

# مراجع

1 ــ D.M. Burton, Elementary Number Theory, Allyn and Bacon, Inc. 1976.
2 ــ K.H. Rosen , Elementary Number Theory and its Applications, 3rd ed., Addison Wesley 1992.

۳ــ ویلیام و. آدامز و لری جوئل گولدشتین، آشنایی با نظریه‌ی اعداد، ترجمه‌ی 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 ریاضی ــ فیزیک. دفتر برنامه‌ریزی و تألیف کتب درسی وزارت آموزش و پرورش ۱۳۶۰.

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