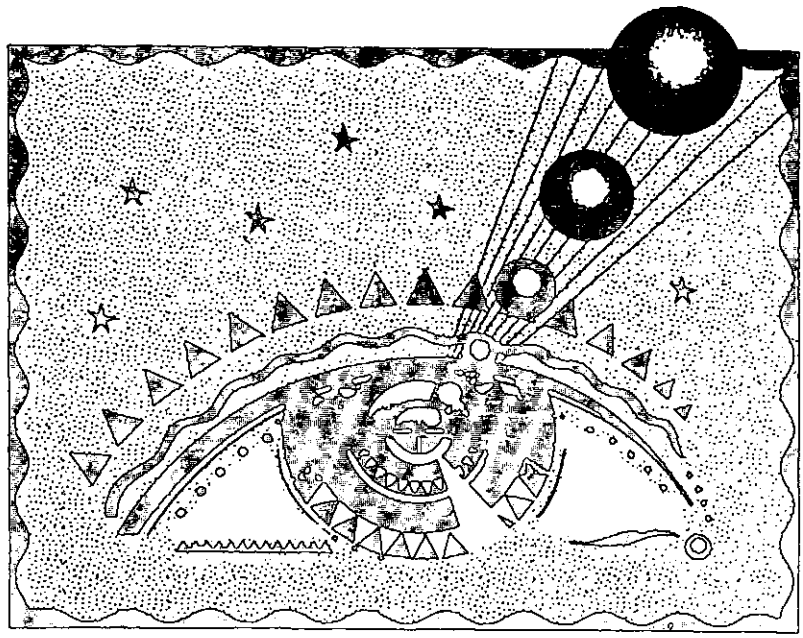

دانش آموزان دبیرستان نظام قدیم و جدید

از کتاب:
A first course in
Number theory

# آموزش ترجمه متون ریاضی (۱۵)

حمیدرضا امیری

*Theorem 3.1.2:* Assume that all symbols used are integers and that $m > 1$.

1. If $b \equiv c \pmod m$ and $d \equiv e \pmod m$, then $b + d \equiv c + e \pmod m$.
2. If $b \equiv c \pmod m$ and $d \equiv e \pmod m$, then $b - d \equiv c - e \pmod m$.
3. If $b \equiv c \pmod m$ and $d \equiv e \pmod m$, then $bd \equiv ce \pmod m$.
4. If $kb \equiv kc \pmod m$, then $b \equiv c \pmod{m/(k, m)}$.

**قضیهٔ ۳.۱.۲:** با فرض این که تمامی نمادهای استفاده شده (در زیر) اعداد صحیح بوده و $m > ۱$.

۱. اگر $b \overset{m}{\equiv} c$ و $d \overset{m}{\equiv} e$ آنگاه، $b+d \overset{m}{\equiv} c+e$.

۲. اگر $b \overset{m}{\equiv} c$ و $d \overset{m}{\equiv} e$ آنگاه، $b-d \overset{m}{\equiv} c-e$.

۳. اگر $b \overset{m}{\equiv} c$ و $d \overset{m}{\equiv} e$ آنگاه $bd \overset{m}{\equiv} ce$.

۴. اگر $kb \overset{m}{\equiv} kc$، آنگاه $b \overset{\frac{m}{(k,m)}}{\equiv} c$.

*Proof of Part 3:* As in the proof of part 3 of Theorem 3.1.1 (and for the same reason), we immediately convert our congruence problem into the corresponding divisibility problem; i.e., if $m|(b - c)$ and $m|(d - e)$, then we need to conclude that $m|(bd - ce)$. The quantity $bd$ appears in the statement of the conclusion we want, so at some point in our argument we have to get $bd$ into the act. The quantity $b$ appears in the assumption $m|(b - c)$, so we can claim that $m|d(b - c) = (bd - cd)$, using the appropriate property of the divisibility symbol; and now $m|(bd - cd)$ involves the quantity $bd$. Similarly, we deduce that $m|c(d - e) = cd - ce$ from the assumption $m|(d - e)$. We now have $m|(bd - cd)$ and $m|(cd - ce)$, and so $m|(bd - ce)$ (why?) as required.

## اثبات قسمت ۳.

با توجه به اثبات قسمت ۳ از قضیهٔ ۳.۱.۱ (و با دلیل مشابه)، ما بلافاصله مسائل هم‌نهشتی‌مان را متناظراً به مسائل بخش‌پذیری تبدیل می‌کنیم، یعنی: اگر $m|(b-c)$ و $m|(d-e)$، آنگاه نیاز داریم نتیجه بگیریم که $m|(bd-ce)$. در این گزاره مقدار bd، حکمی را که ما نیاز داریم آشکار می‌سازد، بنابراین ما می‌بایست bd را بدست آورده و در بعضی از قسمتهای برهانمان اثر دهیم. مقدار b در فرض $m|(b-c)$ مشخص است، بنابراین می‌توان ادعا کرد که $m|d(b-c)=(bd-cd)$ (کاربرد خاصیت ویژه‌ای از نماد بخش‌پذیری) و حالا داریم، $m|(bd-cd)$ که مقدار bd را نیز در بردارد. (به آنچه مورد نظرمان بود رسیدیم) و به طریق مشابه،

از فرض $m|(d-e)$ می‌توانیم نتیجه بگیریم که $m|c(d-e)=(cd-ce)$. اکنون داریم، $m|(bd-cd)$ و $m|(cd-ce)$، و بنابراین ایجاب می‌شود که $m|(bd-ce)$، (چرا؟)

***Proof of Part 4:*** We are assuming that $m|(kb-kc)=k(b-c)$ or, equivalently, $m/(k,m)|k(b-c)/(k,m)=(k/(k,m))(b-c)$. (Give a reason justifying this last step.) Now $(m/(k,m),k/(k,m))=1$, so Theorem 1.2.1 on page 10 allows us to conclude that $m/(k,m)|(b-c)$. In congruence notation, $m/(k,m)|(b-c)$ is $b\equiv c \pmod{m/(k,m)}$, and so we are done.

## اثبات قسمت ۴.

فرض کرده‌ایم که $m|(kb-kc)=k(b-c)$ یا، به عبارت دیگر، (معادل با آن) $\frac{m}{(k,m)}\left|\frac{k(b-c)}{(k,m)}=\frac{k}{(k,m)}(b-c)\right.$. (یک دلیل توجیهی برای این مرحلهٔ آخر بیاورید). حال (می‌دانیم) $\left(\frac{m}{(k,m)},\frac{k}{(k,m)}\right)=1$، بنابراین قضیهٔ ۱.۲.۱ در صفحهٔ ۱۰ امکان این نتیجه‌را به‌ما می‌دهد که $\frac{m}{(k,m)}|(b-c)$. در نماد گذاری هم‌نهشتی $\frac{m}{(k,m)}|(b-c)$، یعنی $b\overset{\frac{m}{(k,m)}}{\equiv}c$، و بنابراین ما توانستیم (اثبات را) تمام کنیم.

***Remarks***

1. An informal way of expressing the first three parts of the theorem just proved is to say that congruences can be added, subtracted, and multiplied together. Please notice, however, that the moduli of the two input congruences don't get added, subtracted, or multiplied together! The modulus of the output congruence is the same as the modulus of each of the two input congruences.
2. Part 4 of the theorem just proved is by way of a warning that the procedure of division in a congruence isn't as straightforward as are addition, subtraction, and multiplication. For instance, it may be tempting (?) to conclude, on the basis of the assumption $kb\equiv kc \pmod{m}$, that $b\equiv c \pmod{m}$, but this conclusion cannot in general be drawn (proof?).

## تبصره‌ها (ملاحظات)

۱ ــ یک راه غیررسمی برای نشان دادن سه قسمت اول قضیه‌ای که ثابت شد، بیان قضیه به این شکل است که، هم‌نهشتی‌ها می‌توانند با هم جمع شوند، از هم کم شوند، و در هم ضرب شوند. لطفاً توجه کنید، مادامی که، سنج دو هم‌نهشتی یکسان نباشد (هم‌نهشتی‌هایی با دو سنج متمایز) نمی‌توانند با یکدیگر، جمع، تفریق، یا درهم ضرب شوند! سنج هم‌نهشتی‌های حاصل همان سنج دو هم‌نهشتی اولیه است.

۲ ــ قسمت چهارم قضیهٔ اثبات شدهٔ فوق این اخطار را می‌دهد که روش تقسیم در یک نهشتی به همان سادگی که برای جمع، تفریق و ضرب به کار رفت، برقرار نمی‌باشد. مثلاً ممکن است برای این نتیجه‌گیری اساسی وسوسه شویم که از فرض $kb\overset{m}{\equiv}kc$ می‌توان $b\overset{m}{\equiv}c$ را استنتاج کرد، امّا این نتیجه‌گیری نمی‌تواند در حالت کلّی استنباط شود. (ثابت کنید)

## تفریح اندیشهٔ ۲

از میان ۳۴ دانش‌آموزی که مورد بررسی قرار گرفته‌اند، ۲۸ نفر در شنا، ۱۹ نفر در اسکی روی آب، ۱۱ نفر در پرش ارتفاع و ۱۷ نفر در دوچرخه‌سواری شرکت دارند. چنانچه همهٔ دانش‌آموزان حداقل در یک فعالیت شرکت کرده باشند، و ۱۲ نفر فقط در یک فعالیت، ۸ نفر دقیقاً در دو فعالیت و ۹ نفر دقیقاً در سه فعالیت ورزشی سهیم باشند، چه تعدادی در هر چهار فعالیت شرکت کرده‌اند؟

**جواب در صفحه ۸۶**