Статијата прв пат е објавена во списанието Нумерус

В. Стојановиќ

КОНГРУЕНЦИИ

Нека се a, b и q три цели броја, $a = b \cdot q$ и $b \neq 0$. Тогаш бројот a е делив со бројот b и q е нивниот количник, т.е. $a : b = q$. Ако a не е делив со b, тогаш постои цел број q и природен број r, помал од $|b|$, така што $a = b \cdot q + r$. Бројот r го викаме остаток на делењето на бројот a со бројот b. Тука посебно ќе го разгледаме остатокот при делењето. Тој остаток, би се рекло некорисен „отпад", нуди неверојатни можности и помага при решавањето на некои многу „незгодни" задачи.

За почеток на разгледувањето ќе решиме еден проблем.

❶ Многумина знаат дека украсното медитеранско растение, со име **лиандер**, ја проширува својата крошна така што секоја гранка се разгранува на три нови гранки. Слично во државата **МАТЕМАТИСКОП** расте растение кај кое крошната се проширува така што некои гранки се разгрануваат во пет нови гранки, а останатите гранки само растат во должина. Наесен на врвот на секоја гранка созрева по еден плод. Дали на крајот на некоја сезона ќе можеме одеднаш да набереме 1 000 плодови?

Решение: На почетокот на стеблото имало точно 5 гранки. Потоа некои од нив се разгранале во 5 нови гранки, па потоа повторно некои се разгранале во 5 нови гранки итн. Секој пат, од една стара гранка настануваат 5 нови, а тоа се 4 гранки повеќе. Така по n гранења ќе имаме вкупно $(5 + 4n)$ слободни врвови (завршетоци) на гранки. Значи, на крајот на секоја сезона можеме да набереме $(4n + 4) + 1$ плодови, т.е. бројот на плодовите кои при делењето со 4 дава остаток 1. Од овде заклучуваме дека никогаш нема на крајот на некоја сезона да имаме точно 1 000 плодови, бидејќи 1 000 е деливо со 4 (остатокот е 0).

Оваа задача ја решивме така што воочивме дека бројот на плодовите припаѓа на *класата* на броевите кои при делење со 4 дава остаток 1.

Сите цели броеви, во однос на деливост со 4, ги делиме на 4 класи:

а) деливи со 4 (остатокот е 0);
б) со остаток 1;
в) со остаток 2;
г) со остаток 3.

На сличен начин се постапува и во однос на деливоста на кој било цел број m, $m \neq 0$. Овие класи на броеви, со еднакви остатоци при делење со даден

број m, ја прават основата на нашите разгледувања. Бидејќи сите разгледувања ќе ги изведуваме исклучиво во множеството на целите броеви, тоа понатаму нема да го потенцираме.

Дефиниција: Ако a, b и m, $m \neq 0$, се **цели броеви, такви што** $(a - b)$ е деливо со m, т.е. $a - b = k \cdot m$, k е цел број, тогаш **велиме дека** a и b **се конгруентни по модул** m.

Тоа се запишува вака: $a \equiv b \pmod m$ и читаме: a е конгруентно со b по модул m.

Значи, од $a \equiv b \pmod m$ следува дека $a - b = km$ и обратно.

Ако $(a - b)$ не е деливо со m, тогаш $a \not\equiv b \pmod m$, т.е. a не е конгруентно со b по модул m. Во тој случај a и b припаѓаат на различни класи на конгруенција по модул m (т.е. припаѓаат на двете класи на броеви, кои имаат различни остатоци при делење со m).

На ваков начин ја опишавме релацијата *„конгруенција на броеви по модул m"*.

Да ги воочиме особините на оваа релација.

Својство 1: Ако $b = 0$, **т.е. ако** $a \equiv 0 \pmod m$, **тогаш** a **е делив со** m, **т.е. остатокот на делењето на бројот** a **со** m **е 0.**

Доказ: Од $a \equiv 0 \pmod m$, по дефиниција е $a - 0 = km$, т.е. $a = km$, што требаше и да се докаже.

Својство 2: Ако $a \equiv b \pmod m$, **тогаш** a **и** b **имаат еднакви остатоци при делење со** m **и обратно, ако** a **и** b **имаат еднакви остатоци при делење со** m, **тогаш** $a \equiv b \pmod m$.

Доказ: Нека r е остаток при делењето на бројот b со m, т.е. нека $b = qm + r$. По дефиниција, од $a \equiv b \pmod m$, следува: $a - b = km$, па $a = b + km = qm + r + km = (q + k)m + r$. Значи, при делење на a со m остатокот е исто така r.

Обратно, ако a и b имаат ист остаток r при делење со m, тогаш $a = pm + r$ и $b = qm + r$. Оттука $a - b = pm + r - qm - r = (p - q)m$, па важи $a \equiv b \pmod m$.

Врз основа на својството 2 можеме да го заклучиме следното: Ако при делење на бројот a **со** m **добиеме остаток** r, **тогаш** $a \equiv r \pmod m$.

❷ **Ако е** $a \equiv 1 \pmod 2$ **или** $a \equiv -1 \pmod 2$, **да се докаже дека** $a^2 \equiv 1 \pmod 8$.

Доказ: Од $a \equiv \pm 1 \pmod 2$, следува дека $a - (\pm 1) = 2k$, односно $a = 2k \pm 1$. Тогаш $a^2 = (2k \pm 1)^2 = 4k^2 \pm 4k + 1 = 4k(k \pm 1) + 1$. Бидејќи $k(k \pm 1)$ е производ на два последователни цели броја, значи $k(k \pm 1)$ е деливо со 2 (бидејќи k или $k \pm 1$ е парен број). Заради тоа $4k(k \pm 1)$ е деливо со 8, т.е. $4k(k \pm 1) = 8m$.

Според тоа: $a^2 = 8m + 1$ и $a^2 - 1 = 8m$, од каде по дефиниција $a^2 \equiv 1 \pmod 8$.

Напомена: Ако на бројот a „недостасува“ s за да биде делив со m, т.е. ако $a + s = km$, тогаш $a - (-s) = km$, што значи дека $a \equiv -s \pmod{m}$.

На пример: $80 \equiv -1 \pmod{9}$.

Не е тешко да се увериме дека конгруенциите по модул ги имаат следните особини:

1° $a \equiv a \pmod{m}$ - рефлексивност;

2° Ако е $a \equiv b \pmod{m}$, тогаш и $b \equiv a \pmod{m}$ - симетричност;

3° Ако е $a \equiv b \pmod{m}$ и $b \equiv c \pmod{m}$, тогаш и $a \equiv c \pmod{m}$ - транзитивност.

Ќе ја провериме особината на транзитивноста:

Од $a \equiv b \pmod{m}$ следува: $a - b = pm$, т.е. $a = b + pm$. Слично, од $b \equiv c \pmod{m}$ добиваме: $c = b - qm$, па $a - c = b + pm - b + qm = (p + q)m = km$. Заклучуваме дека важи по дефиниција $a \equiv c \pmod{m}$.

Следните две својства зборуваат за односот на конгруенцијата спрема собирањето, одземањето и множењето.

Својство 3: Ако a, b, c и m, $m \neq 0$, се цели броеви и $a \equiv b \pmod{m}$, тогаш важи:

а) $a + c \equiv b + c \pmod{m}$; б) $a - c \equiv b - c \pmod{m}$; в) $a \cdot c \equiv b \cdot c \pmod{m}$.

Доказ: а) Од $a \equiv b \pmod{m}$, следува $a - b = km$.

Значи од $a - b = a + c - b - c = (a + c) - (b + c)$, следува $(a + c) - (b + c) = km$, па следува $a + c \equiv b + c \pmod{m}$.

На сличен начин се докажува и својството 3 под б).

в) Од $a - b = km$ следува $ac - bc = kcm = k_1 m$, од каде важи $ac \equiv bc \pmod{m}$, по дефиниција.

Својство 4. Ако $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, а p и q цели броеви, тогаш важат релациите:

а) $a + c = b + d \pmod{m}$; **б)** $a - c \equiv b - d \pmod{m}$;

в) $ac \equiv bd \pmod{m}$; **г)** $ap + qc = bp + dq \pmod{m}$.

Доказ: а) Од $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, следи $a - b = pm$ и $c - d = qm$. Со собирање на овие равенства имаме: $a + c - b - d = pm + qm$,

$(a + c) - (b + d) = m(p + q) = km$, па $a + c \equiv b + d \pmod m$. Според дефиницијата. На ист начин се докажува својството под:

б) со одземање на равенствата и својството под в;

в) со множење на равенствата;

г) од $a \equiv b \pmod m$, а врз основа на својството 3 следи $ap \equiv bp \pmod m$, а од $c \equiv d \pmod m$ следи $cq \equiv bq \pmod m$. Понатаму, од доказот а) следи бараниот заклучок $ap + cq \equiv bp + dq \pmod m$. Врз основа на својството в) заклучуваме дека: од $a \equiv b \pmod m$ следува $a^n \equiv b^n \pmod m$, $n \in \mathbb{N}$.

Користејќи ги наведените својства за конгруенции, ќе решиме неколку интересни задачи.

❸ Колку е остатокот при делењето

$$(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13) : 7?$$

Решение: Да забележиме дека $2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720 \equiv -1 \pmod 7$. Потоа $8 \equiv 1 \pmod 7$, $9 \equiv 2 \pmod 7$, $10 \equiv 3 \pmod 7$, $11 \equiv 4 \pmod 7$, $12 \equiv 5 \pmod 7$ и $13 \equiv 6 \pmod 7$, значи $8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod 7 \equiv$ $\equiv 720 \pmod 7 \equiv -1 \pmod 7$.

Оттука следува дека $(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \cdot (8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13) \equiv (-1) \cdot (-1) \pmod 7 \equiv 1 \pmod 7$. Според тоа бараниот остаток при делењето е 1.

❹ Одреди го остатокот при делењето $2^{200} : 13$.

Решение: Бидејќи $2^6 = 64 \equiv -1 \pmod{13}$, имаме $2^{200} = 2^{198} \cdot 2^2 = (2^6)^{33} \cdot 4$, па $2^{200} \equiv (-1)^{33} \cdot 4 \pmod{13} \equiv -4 \pmod{13}$. Значи остатокот при делењето е 13-4=9.

❺ Ако a е цел број, тогаш:

а) $a^2 \equiv 0 \pmod 2$, или $a^2 \equiv 1 \pmod 2$;

б) $a^2 \equiv 0 \pmod 3$, или $a^2 \equiv 1 \pmod 3$;

в) $a^2 \equiv 0 \pmod 8$, или $a^2 \equiv 1 \pmod 8$ или $a^2 \equiv 4 \pmod 8$. Докажи.

Решение: а) Сите цели броеви, во однос на деливоста со 2, се делат на парни $a = 2k \equiv 0 \pmod 2$, и непарни $a = 2k + 1 \equiv 1 \pmod 2$. Оттука следи $a^2 = 0^2 \pmod 2 \equiv 0 \pmod 2$ или $a^2 \equiv 1^2 \pmod 2 \equiv 1 \pmod 2$.

б) За секој цел број a важи: $a \equiv 0 \pmod 3$ или $a \equiv \pm 1 \pmod 3$, па оттука следи $a^2 \equiv 0^2 \pmod 3$ или $a^2 \equiv (\pm 1)^2 \pmod 3 \equiv 1 \pmod 3$.

в) За секој цел број а важи $a \equiv 0 \pmod 8$ или $a \equiv \pm 1 \pmod 8$ или $a \equiv \pm 2 \pmod 8$ или $a \equiv \pm 3 \pmod 8$ или $a \equiv 4 \pmod 8$. Оттука следи дека $a^2 \equiv 0 \pmod 8$, или $a^2 \equiv (\pm 1)^2 \pmod 8 \equiv 1 \pmod 8$ или $a^2 \equiv (\pm 2)^2 \pmod 8 \equiv 4 \pmod 8$, или $a^2 \equiv (\pm 3)^2 \pmod 8 \equiv 1 \pmod 8$ или $a^2 \equiv 4^2 \pmod 8 \equiv 16 \pmod 8 \equiv 0 \pmod 8$ од каде што следи бараниот заклучок.

❻ Ако a е цел број што не е делив ниту со 7, ниту со 8, тогаш:

а) $a^3 \equiv 1 \pmod 7$, или $a^3 \equiv -1 \pmod 7$;

б) $a^4 \equiv 1 \pmod 7$, или $a^4 \equiv 2 \pmod 7$, или $a^4 \equiv 4 \pmod 7$;

в) $a^4 \equiv 0 \pmod 8$, или $a^4 \equiv 1 \pmod 8$. Докажи.

Доказ: Слично како во претходната задача.

а) $a \equiv \pm 1 \pmod 7$, или $a \equiv \pm 2 \pmod 7$, или $a \equiv \pm 3 \pmod 7$, па $a^3 \equiv (\pm 1)^3 \pmod 7 \equiv \pm 1 \pmod 7$ или $a^3 \equiv (\pm 2)^3 \pmod 7 \equiv \pm 8 \pmod 7 \equiv \pm 1 \pmod 7$, или $a^3 \equiv (\pm 3)^3 \pmod 7 \equiv \pm 27 \pmod 7 \equiv \pm 1 \pmod 7$.

б) Слично како во претходниот случај.

в) Врз основа на задачата 2 имаме $a^2 \equiv 1 \pmod 8$, па оттука следува бараниот заклучок $a^4 \equiv 1 \pmod 8$.

❼ **Докажи дека збирот на квадратите на два цели броја е делив со 7, само ако двата броја се деливи со 7.**

Доказ: Слично како во претходната задача имаме $a^2 \equiv 0 \pmod 7$, или $a^2 \equiv 1 \pmod 7$ или $a^2 \equiv 2 \pmod 7$, или $a^2 \equiv 4 \pmod 7$. За да $a^2 + b^2$ биде делив со 7 треба збирот на остатоците при делење со 7 да е 0 или 7. Збирот 7 не може да се добие од кои било два остатока од броевите 0, 1, 2 или 4. Збирот 0 може да се добие само во случајот кога двата броја a и b се деливи со 7, па според тоа имаме $a^2 + b^2 \equiv 0 + 0 \pmod 7 \equiv 0 \pmod 7$.

❽ **Ако p е прост број, $p \neq 3$, докажи дека**

а) $p^2 \equiv 1 \pmod 3$; **б) за $p^2 \equiv 1 \pmod 6$.**

Доказ: а) Ако $p \neq 3$. тогаш $p \equiv \pm 1 \pmod 3$, $p^2 \equiv (\pm 1)^2 \pmod 3 \equiv 1 \pmod 3$.

б) Броевите поголеми или еднакви на 5 при делење со 6 имат остатоци 0, 1, 2, 3, 4 или 5. Ако остатокот е 0, 2, 3 или 4 тогаш тој број не е прост. Според тоа простиот број p може да има остатоци 1 или 5. Од $p \equiv 1 \pmod 6$ следи $p^2 \equiv 1 \pmod 6$ а од $p \equiv 5 \pmod 6$ следува $p^2 \equiv 5^2 \pmod 6 \equiv 1 \pmod 6$. Со што тврдењето е докажано.

❾ **Најди ги сите прости броеви p за коишто вредноста на изразот $p^6 - 6p^2 + 1$ е квадрат на некој природен број.**

Решение: а) Ако $p = 3$, тогаш $3^6 - 6 \cdot 3^2 + 1 = 676 = 26^2$. Ако $p \neq 3$, според претходната задача $p^2 \equiv 1 \pmod 3$, па изразот имаме $(p^2)^3 - 6p^2 + 1 \equiv (1^2)^3 - 6 \cdot 1^2 + 1 \pmod 3 \equiv 1 - 6 + 1 \pmod 3 \equiv -4 \pmod 3 \equiv -1 \pmod 3 \equiv 2 \pmod 3$.

Меѓутоа, според задачата 5,

б) за квадратот на природниот број условот е $a^2 \equiv 0 \pmod 3$ или $a^2 \equiv 1 \pmod 3$. Според тоа за $p \neq 3$ немаме решение, па единственото решение е $p = 3$.

❿ **Докажи дека вредноста на изразот $n^3 - n$ е делива со 6 за секој цел број n.**

Доказ: Изразот $n^3 - n$ е секогаш парен (затоа што n^3 и n се или двата парни или двата непарни па нивната разлика е парна), значи тој е делив со 2. Во врска со деливоста со 3 знаеме дека $n \equiv 0 \pmod 3$, или $n \equiv \pm 1 \pmod 3$. Бидејќи $0^3 = 0, 1^3 = 1$ и $(-1)^3 = -1$, значи секогаш $n^3 - n \equiv 0 \pmod 3$, па вредноста на изразот секогаш е делива со 3. Дадениот израз е делив со 2 и со 3, значи тој е делив и со 6.