ДРУШТВО МАТЕМАТИЧАРА СРБИЈЕ

АКРЕДИТОВАНИ СЕМИНАР:

345
ДРЖАВНИ СЕМИНАР О НАСТАВИ МАТЕМАТИКЕ И РАЧУНАРСТВА ДРУШТВА МАТЕМАТИЧАРА СРБИЈЕ

Компетенција: К1
Приоритети: 3

ТЕМА:

КАДА КОМБИНАТОРИКА МОЖЕ ДА ПОМОГНЕ
или
КАКО ДОКАЗАТИ НЕКЕ ВАЖНЕ ТЕОРЕМЕ АРИТМЕТИКЕ ПРИМЕНОМ КОМБИНАТОРИКЕ

РЕАЛИЗАТОР СЕМИНАРА:

др СОЊА ЧУКИЋ

БЕОГРАД,
09. – 10. 02. 2019.

Садржај

1. Увод

Један од централних задатака аритметике је доказати да је један број дељив другим. Оно што прво пада на памет у вези са овом облашћу је дељење са остатком, растављање на просте чиниоце и Основна теорема аритметике, конгруенције по модулу, и тако даље.

Међутим, постоји и један леп, али не толико стандардан начин за доказивање дељивости два броја: уколико имамо a предмета које је могуће поделити на b једнаких група, закључујемо да је a дељиво са b, тј. $b \mid a$. За ово дељење (партиционисање) на групе ћемо користити неке комбинаторне[1] идеје које ћемо увести постепено, без ослањања на претходно знање. Самим тим ћемо се у овом излагању подсетити одређених комбинаторних појмова и начина на који се они могу елегантно увести, као што су биномни коефицијенти, пермутације и пермутације са понављањем, полиномни коефицијенти.

Користећи само ове основне идеје и појмове, доказаћемо неке идентитете везане за биномне коефицијенте и затим ћемо градити пут ка доказивању неких, нимало једноставних, теорема у вези са дељивошћу. Почећемо од доказа да је производ k узастопних природних бројева увек дељив са $k!$, поменућемо и неке врло једноставне линеарне Диофантове једначине, а при крају предавања ћемо се бавити доказима Мале Фермаове и Вилсонове теореме.

За сам крај ћемо оставити комбинаторне доказе неких аритметичких идентитета, као што су збир првих n природних бројева и збир кубова и квадрата првих n природних бројева.

2. Дељивост

Кренимо од једне једноставне чињенице коју деца користе већ у млађим разредима основне школе: производ два узастопна природна броја је увек паран јер је један од та два броја увек дељив са два.

Посматрајмо сада производе три узастопна природна броја $n(n+1)(n+2)$. Који је највећи природан број k за који можемо да тврдимо да увек дели овај производ, независно од избора броја n? Закључујемо, слично као малопре, да један од ових бројева мора бити дељив са 3, један са 2, па самим тим производ мора бити дељив са шест (видимо да је 6 највећи овакав број, јер је $1 \cdot 2 \cdot 3 = 6$). Још један начин да докажемо да, уколико је број N дељив и са два и са три, он мора бити дељив са 6, је следећи: $N = 3N - 2N$, а како $6 \mid 3N$ јер је N паран, и $6 \mid 2N$ јер је N дељив са 3, закључујемо да и $6 \mid N$. Дакле, у овом случају је $k = 6 = 3 \cdot 2 \cdot 1$.

Наредни природан корак је да покушамо да одговоримо на питање из претходног пасуса и пронађемо такво k за производ четири узастопна природна броја, $n(n+1)(n+2)(n+3)$. Поново, лако видимо да k не може бити већи од 24, јер је $1 \cdot 2 \cdot 3 \cdot 4 = 24$. Ако сада само закључимо да је један од бројева у производу дељив са 2, један са 3 и један са 4, па је производ дељив са $2 \cdot 3 \cdot 4 = 24$, направили смо грешку коју прави велики број ђака. Наиме, у производу $1 \cdot 3 \cdot 4 \cdot 5$ један број је дељив са 2, један са 4, али то је исти број и цео производ није дељив са 24! Наравно, у случају производа четири узастопна природна броја, овај доказ је лако поправити (како?) и добијамо да $1 \cdot 2 \cdot 3 \cdot 4 = 24 \mid n(n+1)(n+2)(n+3)$ за сваки природан број n.

[1] Реч *комбинаторика* се први пут појавила у Лајбницовом делу *Dissertatio de Arte Combinatoria*. *Gottfried Wilhelm Leibniz* (1646–1716), немачки математичар и филозоф.

Не бисмо били математичари када нам не би пало на памет питање:

Питање 1. Да ли увек важи да $k!$ дели производ $n(n+1)(n+2)\cdots(n+k-1)$, ако су k и n природни бројеви?

Задатак 1. Користећи идеју сличну као у $N = 3N - 2N$, доказати да 5! дели производ пет узастопних природних бројева.

У доказу претходног задатка у једном тренутку треба показати да, ако $24 \mid N$ и $5 \mid N$, тада и $120 \mid N$. Сви знамо да важи и општије тврђење, да ако су a и b узајамно прости природни бројеви, у ознаци $(a,b)=1$, тада из $a \mid N$ и $b \mid N$ следи да $ab \mid N$. Најчешћи доказ ове, јако често коришћене чињенице, користи *Основну теорему аритметике*[2] која тврди да се сваки природан број на јединствен начин (до на поредак чинилаца) може написати као производ простих бројева. Подсетимо се да доказ Основне теореме аритметике уопште није једноставан и да користи трансфинитну индукцију.

Означимо са $\nu_p(N)$ највећи степен простог броја p који дели природан број N. Доказ да $k! \mid n(n+1)(n+2)\cdots(n+k-1)$, ако су k и n природни бројеви, је еквивалентан доказу да $\nu_p(k!) \leqslant \nu_p(n(n+1)(n+2)\cdots(n+k-1))$, за сваки прост број p који дели $k!$. Иако смо, на неки начин, потегли тешко оружје, и даље није јасно како да докажемо или оповргнемо питање 1 за произвољне природне бројеве n и k. Неко ће се можда присетити да бисмо могли да искористимо сличну идеју као у једном од задатака који су се појављивали на пријемним испитима и такмичењима за основну школу, „Са колико нула се завршава број $100!$?”, где је, у ствари, циљ наћи који је највећи степен броја 5 који дели број $100!$.

Лежандрова[3] формула. Нека је k природан, а p прост број. Тада важи

$$\nu_p(k!) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \left[\frac{k}{p^3}\right] + \dots$$

Задатак 2. Доказати Лежандрову формулу.

Сада, после много мука, коришћењем тога да је $[a+b] \geqslant [a] + [b]$ и Лежандрове формуле, можемо да тврдимо да је одговор на питање 1 увек да. Природно је да се запитамо да ли је ово могуће доказати лакше и елегантније. Одговор и на ово питање је да, и у сврху показивања тог доказа, мало ћемо преформулисати питање 1:

Теорема 1. За произвољне природне бројеве k и n, $n \geqslant k$, број

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \tag{1}$$

је такође природан.

[2] Тврђење, наравно написано користећи другачије термине него што смо на то данас навикли, и доказ основне теореме аритметике се појављују још у Еуклидовим Елементима, који су написани око 300 година пре нове ере.

[3] *Adrien-Marie Legendre* (1752–1833), француски математичар.

3. Биномни коефицијенти

Дефиниција. Нека је n природан број и $k \geqslant 0$ цео број. Број свих k-точланих подскупова скупа $\{1, 2, 3, \ldots, n\}$ означава се са $\dbinom{n}{k}$.[4]

Примедба. Бројеви $\binom{n}{k}$ се називају *биномни коефицијенти*, а разлог за то ће бити јасан касније.

Пример 1. Партитивни скуп скупа $\{1, 2, 3, 4\}$ је

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\},$$
$$\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}.$$

Сада видимо да је $\dbinom{4}{0} = 1$, $\dbinom{4}{1} = 4$, $\dbinom{4}{2} = 6$, $\dbinom{4}{3} = 4$ и $\dbinom{4}{4} = 1$. Приметимо да важи

$$\binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 16 = 2^4.$$

Пре него што приступимо тражењу аналитичког израза за биномне коефицијенте, докажимо комбинаторно пар једноставних, али врло важних идентитета.

Пример 2. Нека је n природан број. Тада је

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n.$$

Пример 3. Доказати да за природан број n важи:

$$\text{(i)} \binom{n}{0} = \binom{n}{n} = 1, \qquad \text{(ii)} \binom{n}{k} = \binom{n}{n-k}, \text{ за цео број } k, 0 \leqslant k \leqslant n.$$

Пример 4. Доказати да за природан број n и цео број $k \geqslant 0$ важи

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

Теорема 2. Биномна формула. Нека је n природан број. Тада важи:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n. \tag{2}$$

Теорема 3. Нека је n природан и k ненегативан цео број. Тада је

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}. \tag{3}$$

Доказ. Бирамо произвољан k-точлани подскуп скупа $\{1, 2, 3, \ldots, n\}$ тако што бирамо његове елементе један по један. За први елемент a_1 имамо n различитих могућности, за други, a_2, $n-1$, и тако даље. Последњи елемент a_k бирамо од $n-k+1$ елемената који нису до тада изабрани.

[4] Ознака $\binom{n}{k}$ уведена је 1826. године, иако су сами бројеви били познати вековима пре тога и први пут су се појавили још у десетом веку.

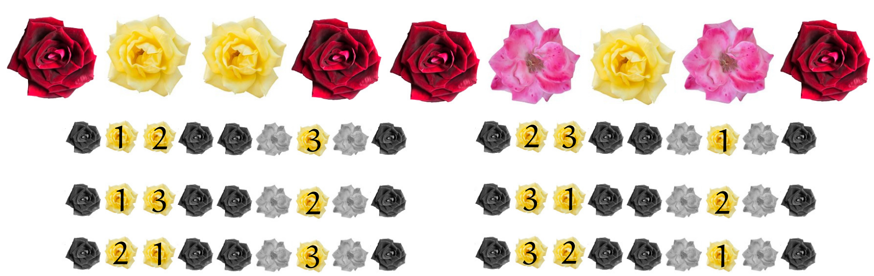
Међутим, овим смо сваки скуп бројали више пута. Наиме, свих $k!$ пермутација (*различитих*) бројева $a_1, a_2, \ldots, a_k$ одређује исти скуп $\{a_1, a_2, \ldots, a_k\}$. Самим тим је једнакост (3) доказана. □

Сада можемо да наставимо нашу причу из претходног поглавља. Израз из теореме 1 је заправо $\binom{n}{k}$, што је природан број, па се сада лако види да $k!$ увек дели производ k узастопних природних бројева.

4. Пермутације са понављањем

Пример 5. Једном давно је у замку живео себични принц који је желео да буде познат у целом краљевству по лепоти ствари које га окружују. Како је посебно волео руже, тражио је од баштована и помоћника да, у част принчевог рођендана, засаде што више праволинијских алеја са по 4 црвене, 3 жуте, и 2 розе руже, и то тако да свака од алеја изгледа различито гледано са принчевог прозора. Колико највише оваквих алеја баштован може да засади?

Решење. Сваку од црвених ружа можемо да означимо бројевима од 1 до 4, жуте од 1 до 3, и розе руже бројевима један и два. На прво место у алеји сада можемо да ставимо било коју од 9 ружа, на друго 8, итд. Овако добијамо $9!$ алеја, чиме би принц био јако задовољан, међутим поново смо неке распореде бројали више пута. Наиме, како се црвене руже међусобно не разликују, нама је важно *само на којим позицијама* су оне засађене, тако да постоји $4!$ различитих комбинација *означених* црвених ружа које дају визуелно исти распоред. Слично и за жуте, и за руже розе боје, па добијамо да баштован може да засади највише $\frac{9!}{4!3!2!} = 1260$ различитих алеја. ✓



Слика 1. Различити распореди *означених* жутих ружа који дају визуелно исти распоред цвећа у алеји, има их $3! = 6$.

Потпуно аналогно се разматра и доказује општије тврђење:

Теорема 4. Нека су $n_1, n_2, \ldots, n_k$ природни бројеви и $b_1, b_2, \ldots, b_k$ различите боје. Ако желимо да поређамо $n_1 + n_2 + \cdots + n_k$ објеката у врсту, од којих је n_j објеката боје b_j, за свако $j \in \{1, 2, \ldots, k\}$, то можемо урадити на

$$\frac{(n_1 + n_2 + \cdots + n_k)!}{n_1! n_2! \cdots n_k!} \tag{4}$$

различитих начина.

Примедба. Приметимо да за $k = 2$ добијамо израз $\frac{(n_1+n_2)!}{n_1!n_2!} = \binom{n_1+n_2}{n_1}$, што одговара идеји доказа за број подскупова скупа са $n = n_1 + n_2$ елемената. Наиме, сваком од тих

n елемената доделимо или боју 0 или боју 1 у зависности од тога да ли припада датом подскупу A, при чему ако A има n_1 елемената, тада мора бити n_1 јединица и обрнуто. На пример, подскупу $\{1,3,4\} \subset \{1,2,3,4,5,6\}$ би одговарало 101100, а 1101010 би одговарао подскупу $\{1,2,4,6\} \subset \{1,2,3,4,5,6,7\}$.

Пример 6. Од свих слова речи АРИТМЕТИКА може се направити $\dfrac{10!}{2!2!2!}$ различитих речи.

Теорема 5. Полиномна формула. Нека је n природан број. Тада важи

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{n_1, n_2, \ldots, n_k \in \mathbb{N}\cup\{0\} \\ n_1 + \cdots + n_k = n}} \frac{(n_1 + n_2 + \cdots + n_k)!}{n_1! n_2! \cdots n_k!} x_1^{n_1} \ldots x_k^{n_k}.$$

Примедба. У овом збиру има $\binom{n+k-1}{k-1}$ различитих сабирака (зашто?).

Вратимо се поново дељивости и урадимо неколико примера, у којима ћемо са n и k означавати произвољне природне бројеве.

Пример 7. Доказати да је број $(nk)!$ дељив бројем $(n!)^k$.

Пример 8. Доказати да $n!$ дели број $2^n \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = 2^n \cdot (2n-1)!!$.

Пример 9. */Московска математичка олимпијада 2009./* За сваки прост број p наћи највећи степен броја $p!$ који дели број $(p^2)!$.

Решење. Лако се види да је $\nu_p((p^2)!) = p+1$, па тражени степен не може бити већи од $p+1$. Такође, када у примеру 7 заменимо да је $n = k = p$, добијамо да $(p!)^p \mid (p^2)!$.

Сада се поставља питање шта је тражени степен, p или $p+1$. Провером се за $p = 2,3,5$ лако добије да је у тим случајевима степен заправо $p+1$, тако да нам је потребно следеће уопштење примера 7 које одмах имплицира да је решење нашег задатка заправо $p+1$ за сваки прост број p:

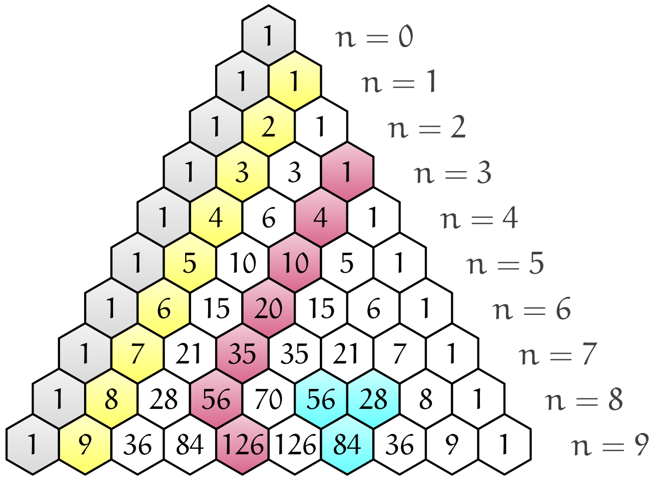
Теорема 6. Нека су n, k природни бројеви. Тада $(n!)^k k!$ дели $(nk)!$.

Доказ. Могуће је расписати $(nk)!$ и користити теорему 1 за производ $(n-1)$-ног узастопног природног броја, остављајући бројеве $nk, (k-1)n, (k-2)n, \ldots$ да допринесу са $k!$ и n^k (приметимо да је $(n!)^k k! = n^k k!((n-1)!)^k$. $\square$

Међутим, нас на овом предавању много више занимају комбинаторни докази. Одакле се појави $k!$ у случају када *свих цветова различитих „боја” има исти број*?

Идеју доказа ћемо илустровати на примеру. Нека је $n_1 = n_2 = n_3 = 2$ и нека имамо три боје Ц, П и Б. Пермутацији са понављањем ЦПЦББП придружимо скуп $\{\{1,3\},\{2,6\},\{4,5\}\}$ (1 и 3 су позиције на којима је Ц, 2 и 6 позиције на којима је П, и 4 и 5 позиције на којима је Б). Међутим, и свака од ЦБЦППБ, ПБПЦЦБ, ПЦПББЦ, БПБЦЦП, БЦБППЦ се на овај начин слика у исти скуп (укупно $6 = 3!$ пермутација се сликају у исти скуп). Колико има различитих скупова које смо описали малопре?

5. Делиоци биномних коефицијената



Слика 2. Паскалов[5] троугао за $n \leqslant 9$.

За које све вредности природног броја n су сви (сем првог и последњег) елементи у n-тој врсти Паскаловог троугла парни? На слици 2 видимо да су за $n \leqslant 9$ то 2, 4 и 8, што су степени двојке. Испоставља се да је то увек тачно:

Пример 10. Сви биномни коефицијенти $\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$ су парни ако и само ако је n степен двојке.

Доказ. Приметимо да неки скуп има паран број елемената ако се ти елементи могу разбити у парове. Такође, како је $\binom{n}{1} = n$, број n мора бити паран, $n = 2m$. Доказ ћемо извести трансфинитном индукцијом по n, где смо базу директно проверили (слика 2).

Присетимо се да је $\binom{n}{k}$ број свих k-точланих подскупова скупа са $n = 2m$ елемената. Зато посматрамо скуп $S = \{\pm 1, \pm 2, \ldots, \pm m\}$. Лако се види да за $A \subset S$, скуп $-A = \{-a \mid a \in A\}$ има исти број елемената као и A.

Дакле, ако је A подскуп скупа S са k елемената, можемо да упаримо A и $-A$. Међутим, имамо проблем ако је $A = -A$, што може да се деси ако и само ако је $k = 2k_1$ (зашто?). Према томе, доказали смо да је $\binom{2m}{k}$ увек паран када је k непаран. Такође, $\binom{2m}{2k_1}$ је паран за свако $1 \leqslant k_1 \leqslant m-1$ ако и само ако је број свих $(2k_1)$-точланих скупова A таквих да је $A = -A$ паран, тј. ако и само ако је $\binom{m}{k_1}$ паран за $1 \leqslant k_1 \leqslant m-1$. Како је $m < n$, по индукцијској претпоставци, ово је могуће ако и само ако је m, а самим тим и n, степен двојке. ✓

Посматрајмо сада оне врсте у Паскаловом троуглу за које је њихов редни број n прост број, $n = 2, 3, 5, 7$ на слици 2. Опет примећујемо да је сваки од биномних коефицијената у тој врсти (осим првог и последњег) дељив одговарајућим простим бројем.

[5] *Blaise Pascal* (1623–1662), француски математичар и физичар.
Ова троугаона таблица са биномним коефицијентима добила је име по Паскалу иако су је математичари у Индији, Персији и Кини проучавали вековима пре него што је Паскал рођен.

Теорема 7. Нека је p прост број и $1 \leqslant k \leqslant p-1$. Тада је $\binom{p}{k}$ дељиво са p.

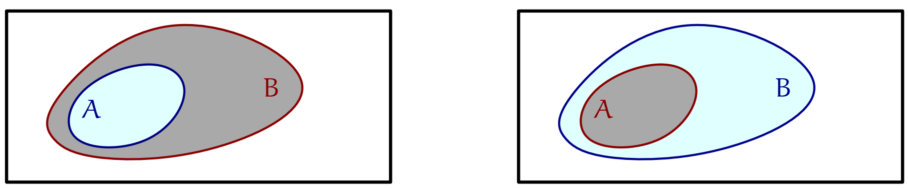
Последица 1. Нека је p прост број и нека су a и b цели бројеви. Тада је

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Доказ. Биномна формула и теорема 7. □

Пример 11. */Московска математичка олимпијада 2009./* Нека је n природан број и $1 \leqslant k < l \leqslant n-1$. Доказати да $\binom{n}{k}$ и $\binom{n}{l}$ нису узајамно прости.

Решење. Посматрамо парове скупова (A, B), $A \subset B \subset \{1, 2, \ldots, n\}$ и $|A| = k$, $|B| = l$. Овакве парове можемо избројати на два начина. Прво на $\binom{n}{k}$ начина изаберемо скуп A, па затим од преосталих елемената изаберемо елементе скупа $B \setminus A$ на $\binom{n-k}{l-k}$ начина, дакле парова има $\binom{n}{k}\binom{n-k}{l-k}$. Са друге стране, скуп B можемо изабрати на $\binom{n}{l}$ начина, и затим од елемената скупа B изабрати A на $\binom{l}{k}$ начина.



Слика 3. Са леве стране прво бирамо елементе скупа A, а затим елементе скупа $B \setminus A$. Са десне стране, прво бирамо елементе скупа B, а затим елементе скупа A (од елемената скупа B).

Према томе,
$$\binom{n}{k}\binom{n-k}{l-k} = \binom{n}{l}\binom{l}{k}, \text{ па како је } \binom{n}{k} > \binom{l}{k},$$
добијамо тврђење задатка (нека је $d = (\binom{n}{k}, \binom{l}{k})$, па је $\binom{n}{k}/d > 1$ и $\binom{n}{k}/d \mid \binom{n}{l}$). ✓

Пример 12. Доказати да $n+1$ дели $\binom{2n}{n}$ за сваки природан број n (*Каталанови*[6] *бројеви*).

6. Остаци при дељењу простим бројем

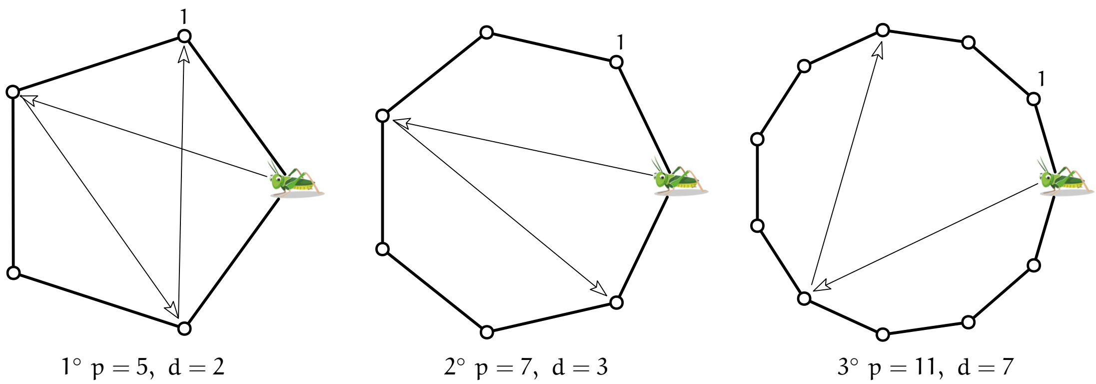
Од сада, па на даље, нека је p прост број. Представимо све остатке при дељењу са p као темена правилног p-тоугла и у нулу поставимо скакавца, који може да скаче d корака на произвољну страну, где је $1 \leqslant d \leqslant p-1$, погледати слику 4.

Питање 2. Да ли скакавац може, после коначно много корака, да дође то темена означеног јединицом?

Примедба. Јасно је да је одговор *не* када је број сложен.

Ово питање се у ствари своди на то да одговоримо да ли за овакво d постоји природан број k такав да је $kd \equiv 1 \pmod{p}$.

[6] *Eugène Charles Catalan* (1814–1894), француски и белгијски математичар.



Слика 4. Илустрација кретања скакавца за различите p и d.

Теорема 8. За сваки прост број p и природан број $1 \leqslant d \leqslant p-1$ постоји цео број k такав да је $kd \equiv 1 \pmod{p}$. Другим речима, d има инверз у $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

Доказ где посматрамо бројеве $d, 2d, \ldots, (p-1)d$ и доказујемо да су они међусобно различити елементи $\mathbb{Z}_p^*$ користи Основну теорему аритметике, коју покушавамо да избегнемо да користимо и чији доказ често користи баш претходну теорему.

Доказ. Фиксирамо p и користимо трансфинитну индукцију по d. За $d = 1$, ово је очигледно. Нека је сада $d > 1$ и поделимо p бројем d са остатком:

$$p = dq + r, \ 0 < r < d \ (r \neq 0 \text{ јер } p \text{ није дељиво са } d).$$

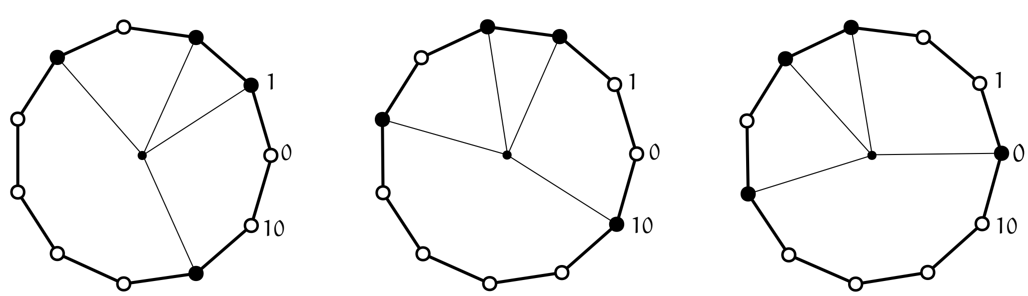
Применимо сада индуктивну претпоставку на r: постоји $k' \in \mathbb{Z}$ тако да је $k'r \equiv 1 \pmod{p}$. Сада имамо $k'r = k'p - k'dq \equiv 1 \pmod{p}$, па за $k = -k'd$ важи да је $kd \equiv 1 \pmod{p}$. □

Примедба. Експлицитну вредност за k можемо наћи применом обрнутог Еуклидовог алгоритма који нам даје једно решење једначине $kd + lp = 1$.

Пример 13. Докажимо теорему 7 комбинаторно:

Ако је p прост број и $1 \leqslant k \leqslant p-1$, тада p дели $\binom{p}{k}$.

Доказ. Нека је A неки непразни подскуп скупа $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ и нека је $f(A) = A + 1 = \{a + 1 \mid a \in A\} \subset \mathbb{Z}_p$ ($f(A)$ је у ствари ротација скупа A за централни угао p-тоугла – видети слику 5).



Слика 5. $p = 11$ и $A = \{1, 2, 4, 9\}$. Тада је $A + 1 = \{2, 3, 5, 10\}$ и $A + 2 = \{0, 3, 4, 6\}$

.

Приметимо да је $f^p(A) = \underbrace{(f \circ f \circ \cdots \circ f)}_{p}(A) = A$ и да је $f(X) = X$ ако и само ако је $X = \mathbb{Z}_p$.

За два k-точлана скупа A и B, $A, B \subset \mathbb{Z}_p$, дефинишимо релацију $\sim$ на следећи начин:

$$A \sim B \Leftrightarrow (\exists j \in \mathbb{N})\ f^j(A) = B.$$

Лако се види да је $\sim$ релација еквиваленције. Докажимо да свака класа има тачно p елемената, што би завршило доказ да је број свих k-точланих подскупова дељив са p. Због $f^p(A) = A$ видимо да класа има *највише* p елемената, дакле треба доказати да је $A \neq f^m(A)$, $m \in \{2, \dots, p-1\}$ ($m \neq 1$ јер је $A \neq \mathbb{Z}_p$). Претпоставимо супротно: нека је $m \leqslant p-1$ *најмањи* број за који је је $A = f^m(A)$ и нека је $p = mq + r$, $0 < r < m$ (јер m не дели p – овде смо искористили да је p прост број). Сада имамо $A = f^p(A) = f^r(f^m(f^m(\dots(f^m(A)))) = f^r(A)$, што је контрадикција. ✓

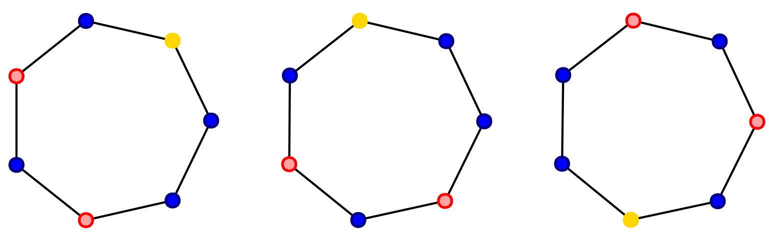
7. Мала Фермаова и Вилсонова теорема

Теорема 9. Мала Фермаова[7] теорема. Нека је p прост број и $(a, p) = 1$. Тада је

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

Доказ ове теореме може се директно извести из теореме 7, као и из теореме 4, али ћемо ми овде представити још један леп комбинаторни доказ.

Доказ. Свих могућих бојења темена правилног p-тоугла са a боја има a^p. Колико их има ако кажемо да су два бојења иста ако се могу добити једно од другог ротацијом око центра за неки угао? На слици 6 је дат пример три бојења седмоугла која ћемо сматрати истим.



Слика 6. $p = 7$ и $a = 3$. Три иста бојења.

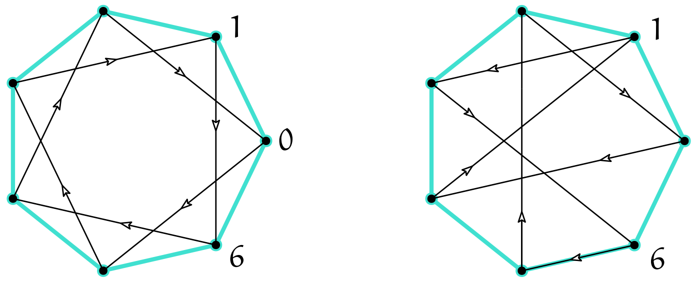
Слично као у последњем доказу из претходног поглавља, имамо a једнобојних бојења, а осталих у класи еквиваленције има по p. Дакле, овако дефинисаних различитих бојења има $a + \frac{a^p - a}{p}$, а како је то природан број, доказали смо Малу Фермаову теорему. □

Теорема 10. Вилсонова[8] теорема. Број p је прост ако и само ако је

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

Доказ. ($\Rightarrow$) У овом доказу посматрамо затворене (усмерене) изломљене линије које „пролазе" кроз сва темена. Као и до сада, кажемо да су две овакве линије еквивалентне ако се могу добити једна од друге ротацијом.

[7] *Pierre de Fermat* (1607 – 1665), француски математичар и адвокат.
[8] *John Wilson* (1741 – 1793), енглески математичар.



Слика 7. Илустрација за $p = 7$. Лево: изломљена линија која се сваком ротацијом за угао $\frac{2k\pi}{7}$ око центра слика сама у себе. Десно: изломљена линија у чијој је класи тачно седам других изломљених линија.

Укупно имамо $(p-1)!$ оваквих усмерених изломљених линија (фиксирамо једно теме као почетно). Са друге стране, постоји две врсте линија: оне у чијој класи имамо само један елемент (оне које се произвољном ротацијом за угао $2k\pi/p$ сликају саме у себе) и оне у чијој је класи тачно p различитих изломљених линија (идеја је иста као у претходним доказима). Овиx првих има тачно $p-1$, јер код њих, за неко $1 \leqslant k \leqslant p-1$ и свако $x \in \mathbb{Z}_p$, темена x и $x+k$ морају бити спојена. Дакле $(p-1)! - (p-1)$ мора бити дељиво са p.
($\Leftarrow$) Следи директно. $\square$

8. Бонус: аритметички идентитети

Свима је познато како је мали Гаус[9] израчунао збир свих природних бројева од 1 до 100 и како изгледа формула за збир првих n природних бројева. Овде ћемо дати комбинаторни доказ овог и још неких идентитета. У овом случају докази су знатно компликованији од алгебарских, али илуструју комбинаторно размишљање и заслужују да буду представљени.

Пример 14. Нека је n природан број. Доказати да је $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Решење. Као што смо већ видели, $\dfrac{n(n+1)}{2} = \dbinom{n+1}{2}$ је број свих двочланих подскупова скупа $\{0, 1, 2, 3, \ldots, n\}$.
Ако је већи од два елемента неког изабраног двочланог подскупа једнак k, онда мањи можемо изабрати из скупа $\{0, 1, 2, \ldots, k-1\}$, дакле имамо k избора. Како већи елемент може бити било који број из скупа $\{1, 2, 3, \ldots, n\}$, тврђење је доказано. ✓

Пример 15. Нека је n природан број. Доказати да је $\displaystyle\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

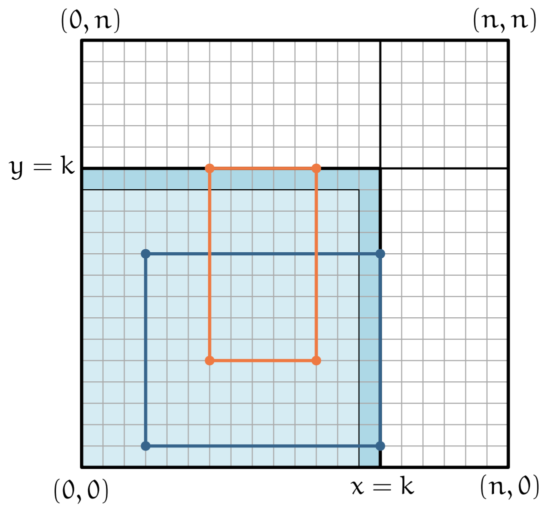
Решење. Задатак можемо мало другачије да формулишемо. У координатном систему xOy задат је квадрат чија су наспрамна темена $(0,0)$ и (n,n), $n \in \mathbb{N}$, и чије су странице паралелне координатним осама. *Колико постоји правоугаоника чија темена имају целобројне координате, чије су странице паралелне координатним осама и који су подскуп датог квадрата?*

[9] *Johann Carl Friedrich Gauss* (1777 – 1855), немачки математичар и физичар.

Са једне стране, када посматамо пројекције правоугаоника на x-осу, тј. на y-осу, добијамо двочлане подскупове скупа $\{0, 1, 2, \dots, n\}$ којих, по претходном примеру, има $\binom{n+1}{2}$. Дакле, тражених правоугаоника има тачно

$$\binom{n+1}{2}^2 = \left(\frac{n(n+1)}{2}\right)^2.$$

Са друге стране, ако посматрамо све уређене четворке $(a, b, c, d) \in \mathbb{N}_0^4$, где је $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$, такве да је $d = k$ и $a, b, c < k$, њих има k^3. Докажимо да овакве четворке једнозначно одговарају правоугаоницима за чије горње десно теме (x, y) важи $\max\{x, y\} = k$ (приметимо да када је овај услов задовољен, наш правоугаоник је подскуп квадрата $k \times k$, али није подскуп квадрата $(k-1) \times (k-1)$, видети слику 8).



Слика 8. Примери два правоуганика таква да за горње десно теме (x, y) важи $\max\{x, y\} = k$.

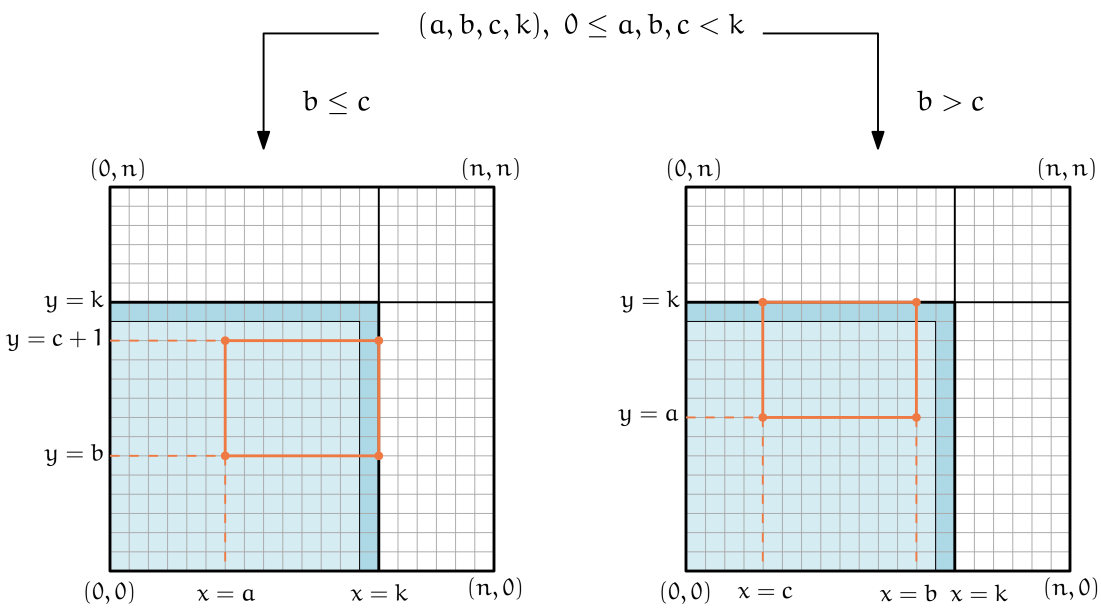
Конструишимо сада бијекцију између оваквих уређених четворки и правоугаоника:

1° $b \leqslant c$: онда четворку (a, b, c, k) сликамо у правоугаоник ограничен правама $x = a$, $x = k$, $y = b$ и $y = c + 1$ (видети слику 9 лево).

2° $b > c$: онда четворку (a, b, c, k) сликамо у правоугаоник ограничен правама $x = c$, $x = b$, $y = a$ и $y = k$ (видети слику 9 десно).

Како се сваком правоугаонику са максималном координатом k на јединствен начин може доделити четворка (a, b, c, k) у зависности од тога да ли се k појави у x-координати горњег десног темена или не, овај процес је реверзибилан. Тиме смо доказали да тражених правоугаоника има k^3.

Имајући у виду да максимална координата горњег десног темена може бити било који број из скупа $\{1, 2, \dots, n\}$, добили смо да правоугаоника укупно има $\sum_{k=1}^{n} k^3$. ✓

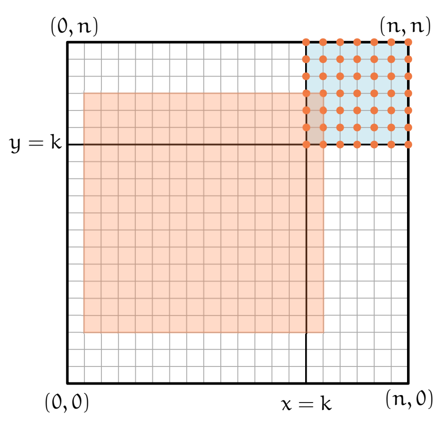


Слика 9. Графички приказ пресликавања описаног у решењу примера 15.

Пример 16. Нека је n природан број. Доказати да је $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

Решење. Приметимо прво да је $\frac{n(n+1)(2n+1)}{6} = 2\binom{n+1}{3} + \binom{n+1}{2}$.

Поставимо слично питање као у претходном примеру, само што ћемо реч *правоугаоник* заменити са *квадрат*.



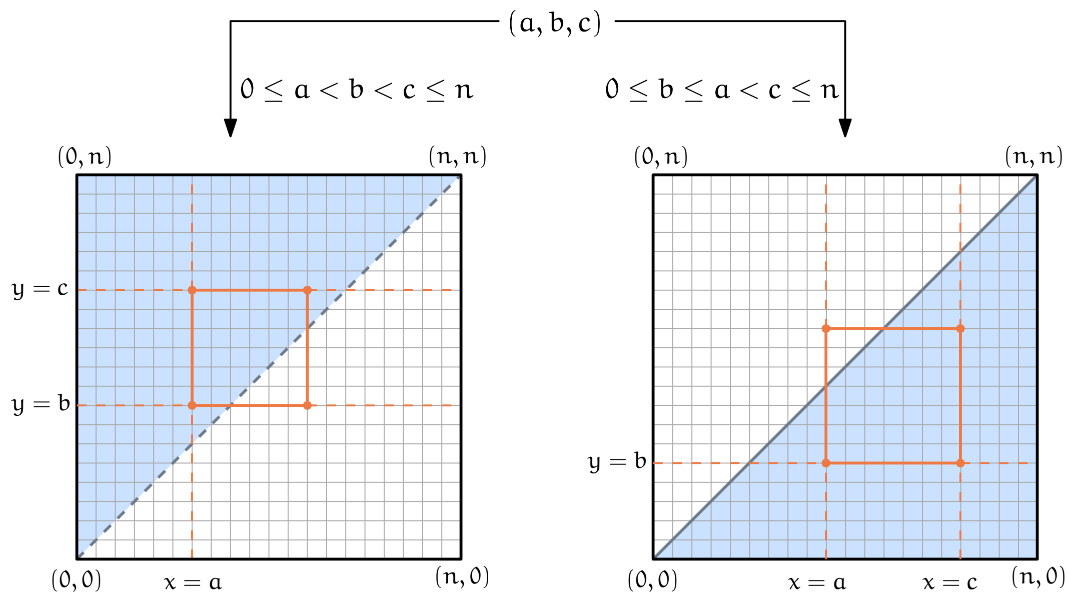
Слика 10. Све могућности за горње десно теме $k \times k$ квадрата.

Са једне стране, опет посматрајући горње десно теме, број $k \times k$ квадрата је $(n+1-k) \cdot (n+1-k)$ (видети слику 10), па је укупан број квадрата једнак

$$\sum_{k=1}^{n} (n+1-k)^2 = \sum_{k=1}^{n} k^2.$$

Са друге стране, свакој уређеној тројци (a, b, c) таквој да важи $0 \leqslant a < b < c \leqslant n$ (приметимо да оваквих тројки има $\binom{n+1}{3}$) доделимо квадрат чије три странице припадају правама $x = a$, $y = b$ и $y = c$. Овако добијамо *све* квадрате чије је доње лево, па самим тим и горње десно теме *изнад* праве $y = x$, видети слику 11 лево.

Уређеној тројци (a, b, c) таквој да важи $0 \leqslant b \leqslant a < c \leqslant n$ (оваквих тројки има $\binom{n+1}{3} + \binom{n+1}{2}$) доделимо квадрат чије три странице припадају правама $x = a$, $y = b$ и $x = c$. Овако добијамо *све* квадрате чије је горње десно теме *на или испод* праве $y = x$, видети слику 11 десно.



Слика 11. Илустрација пресликавања тројки (a, b, c) у квадрате.

Закључујемо да је

$$\sum_{k=1}^{n} k^2 = \binom{n+1}{3} + \binom{n+1}{3} + \binom{n+1}{2},$$

што је и требало доказати. ✓

Литература

[1] Андрей Канунников, *Доказатъ делимостъ поможет комбинаторика*, Журнал Квант, №2, №3, 2018.
[2] Arthur T. Benjamin, Jennifer Quinn, *Proofs That Really Count – the Art of Combinatorial Proof*, Mathematical Association of America, 2003.
[3] George E. Andrews, *Number Theory*, Dover Books on Mathematics, USA, 1971.
[4] Richard Stanley, *Enumerative Combinatorics 1*, Cambridge University Press, USA, 2002.
[5] Miklós Bóna, *A Walk Through Combinatorics*, World Scientific Publishing, Singapore, 2006.
[6] Arthur T. Benjamin, Jennifer Quinn, Calyssa Wurtz, *Summing Cubes by Counting Rectangles.*
[7] http://artofproblemsolving.com/
[8] https://math.stackexchange.com/
[9] https://en.wikipedia.org/