O algebrze w kombinatoryce.

W. Guzicki

(Czwartkowe wykłady popularne z matematyki – 21.04.2005)

W tym wykładzie pokażemy kilka zastosowań algebry do dowodów twierdzeń kombinatorycznych.

Jak zapewne pamiętamy ze szkoły, wielomianem stopnia n nazywamy funkcję postaci

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

gdzie $a_n, a_{n-1}, \ldots, a_1, a_0$ są dowolnymi liczbami rzeczywistymi, przy czym $a_n \neq 0$. Te liczby nazywamy **współczynnikami** wielomianu f. Oczywiście współczynniki wielomianu wyznaczają go jednoznacznie. Okazuje się, że jest też i na odwrót: jeśli dwa wielomiany f i g przyjmują te same wartości dla wszystkich argumentów, to mają te same współczynniki (wynika to stąd, że wielomian niezerowy ma tylko skończoną liczbę pierwiastków). Zatem wielomian f jednoznacznie wyznacza swoje współczynniki. Inaczej mówiąc, wielomian f stopnia n możemy utożsamić z takim ciągiem długości $n+1$ jego współczynników:

$$(a_n, a_{n-1}, \ldots, a_1, a_0),$$

w którym pierwszy wyraz jest różny od zera: $a_n \neq 0$. Okazuje się, że wygodnie jest przyjmować, iż ciąg współczynników jest nieskończony, przy czym wszystkie współczynniki o indeksach większych od n są zerami. Wygodnie też jest zapisywać te współczynniki w odwrotnej kolejności.

Od tej pory wielomian zmiennej rzeczywistej x utożsamiamy z ciągiem nieskończonym

$$f = (a_0, a_1, a_2, \ldots, a_n, \ldots)$$

liczb rzeczywistych, w którym prawie wszystkie (tzn. wszystkie od pewnego miejsca) wyrazy są równe zeru. Inaczej mówiąc z takim ciągiem, dla którego istnieje liczba naturalna n o tej własności, że

$$a_{n+1} = a_{n+2} = a_{n+3} = \ldots = 0.$$

Oczywiście wielomian zerowy utożsamiamy z ciągiem, w którym wszystkie wyrazy są zerami. Wielomian stopnia n utożsamiamy z ciągiem takim, że

$$a_n \neq 0 \quad \text{oraz} \quad \forall m > n \ \big(a_m = 0\big).$$

Po tym utożsamieniu możemy łatwo opisać działania na wielomianach. **Sumą** wielomianów

$$f = (a_0, a_1, a_2, \ldots) \quad \text{i} \quad g = (b_0, b_1, b_2, \ldots)$$

nazywamy wielomian

$$h = (c_0, c_1, c_2, \ldots)$$

zdefiniowany następująco:

$$c_n = a_n + b_n \quad \text{dla } n = 0, 1, 2, \ldots$$

Różnicą wielomianów f i g nazwiemy wielomian h zdefiniowany wzorem

$$c_n = a_n - b_n \quad \text{dla } n = 0, 1, 2, \ldots$$

Iloczynem wielomianów f i g nazwiemy natomiast wielomian h zdefiniowany wzorem:

$$c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_1 b_{n-1} + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k} \quad \text{dla } n = 0, 1, 2, \ldots$$

Wzór ten często nazywamy wzorem Cauchy'ego. Początkowe współczynniki c_n przedstawiają się następująco:

$$\begin{aligned}
c_0 &= a_0b_0,\\
c_1 &= a_0b_1 + a_1b_0,\\
c_2 &= a_0b_2 + a_1b_1 + a_2b_0,\\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0,\\
c_4 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0,\\
\ldots \quad &\ldots
\end{aligned}$$

Przykład. Obliczmy iloczyn

$$(2x^2 - x + 3) \cdot (3x^2 + 2x - 1).$$

Po wykonaniu mnożenia sposobem „każdy wyraz przez każdy" i dokonaniu redukcji wyrazów podobnych, otrzymamy:

$$(2x^2 - x + 3) \cdot (3x^2 + 2x - 1) = 6x^4 + 4x^3 - 2x^2 - 3x^3 - 2x^2 + x + 9x^2 + 6x - 3 = 6x^4 + x^3 + 5x^2 + 7x - 3.$$

Wykonajmy teraz mnożenie za pomocą wzoru Cauchy'ego. Nasze wielomiany mają postać:

$$f = (3, -1, 2, 0, 0, 0, \ldots) \quad \text{oraz} \quad g = (-1, 2, 3, 0, 0, 0, \ldots)$$

Inaczej mówiąc

$$a_0 = 3, a_1 = -1, a_2 = 2, a_n = 0 \quad \text{dla } n > 2$$

oraz

$$b_0 = -1, b_1 = 2, b_2 = 3, b_n = 0 \quad \text{dla } n > 2.$$

Obliczamy kolejno współczynniki wielomianu h, będącego iloczynem wielomianów f i g:

$$\begin{aligned}
c_0 &= a_0b_0 = 3 \cdot (-1) = -3,\\
c_1 &= a_0b_1 + a_1b_0 = 3 \cdot 2 + (-1) \cdot (-1) = 7,\\
c_2 &= a_0b_2 + a_1b_1 + a_2b_0 = 3 \cdot 3 + (-1) \cdot 2 + 2 \cdot (-1) = 5,\\
c_3 &= a_0b_3 + a_1b_2 + a_2b_1 + a_3b_0 = 3 \cdot 0 + (-1) \cdot 3 + 2 \cdot 2 + 0 \cdot (-1) = 1,\\
c_4 &= a_0b_4 + a_1b_3 + a_2b_2 + a_3b_1 + a_4b_0 = 3 \cdot 0 + (-1) \cdot 0 + 2 \cdot 3 + 0 \cdot 2 + 0 \cdot (-1) = 6.
\end{aligned}$$

Można łatwo zauważyć, że $c_n = 0$ dla $n > 4$. Zatem wielomian h ma postać

$$h = (-3, 7, 5, 1, 6, 0, 0, 0, \ldots),$$

czyli

$$(2x^2 - x + 3) \cdot (3x^2 + 2x - 1) = 6x^4 + x^3 + 5x^2 + 7x - 3.$$

Przypomnimy teraz znane ze szkoły pojęcie współczynnika dwumianowego $\binom{n}{k}$. Niech A będzie dowolnym zbiorem n-elementowym. W dalszym ciągu, jeśli X jest dowolnym zbiorem skończonym, to symbolem $|X|$ będziemy oznaczać liczbę elementów zbioru X. Mamy wówczas:

$$\binom{n}{k} = \big|\{X \subseteq A : \ |X| = k\}\big|$$

dla dowolnych liczb naturalnych n i k. Natychmiast z definicji wynika, że jeśli $k > n$ to

$$\binom{n}{k} = 0,$$

gdyż wtedy zbiór A nie ma podzbiorów k-elementowych. Jeśli natomiast $0 \le k \le n$, to ze wzoru znanego ze szkoły wynika, że

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Współczynniki dwumianowe występują w tzw. wzorze dwumianowym Newtona:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \ldots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} a^0 b^n$$

dla dowolnych liczb rzeczywistych a i b i dowolnej liczby naturalnej dodatniej n. Współczynniki dwumianowe tworzą tzw. **trójkąt Pascala**, którego początkowe wiersze przedstawiają się w następujący sposób:

$$\begin{array}{ccccccccccccc}
 & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & \\
 & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & \\
 & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & \\
 & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & \\
 & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & \\
\binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6}
\end{array}$$

czyli

$$\begin{array}{ccccccccccccc}
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}$$

Po tym wstępie przejdziemy do dowodu następującej równości:

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n},$$

czyli

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

Podstawmy we wzorze dwumianowym Newtona $a = 1$ i $b = x$. Otrzymamy wzór

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \ldots + \binom{n}{n-1} x^{n-1} + \binom{n}{n} x^n.$$

Podnosimy obie strony do kwadratu:

$$(1+x)^{2n} = \left(\sum_{k=0}^{n} \binom{n}{k} x^k \right) \cdot \left(\sum_{k=0}^{n} \binom{n}{k} x^k \right).$$

Po lewej stronie równości mamy oczywiście wielomian stopnia $2n$. Po prawej stronie mamy iloczyn dwóch wielomianów n-tego stopnia, a więc jest to także wielomian stopnia $2n$. Porównajmy współczynniki stojące przy x^n w obu wielomianach. Ponieważ

$$(1+x)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} x^k = \binom{2n}{0} + \binom{2n}{1} x + \binom{2n}{2} x^2 + \ldots + \binom{2n}{n} x^n + \ldots + \binom{2n}{2n} x^{2n},$$

więc po lewej stronie przy x^n stoi współczynnik $\binom{2n}{n}$. Po prawej stronie mamy iloczyn wielomianów $f \cdot g$, gdzie

$$f = g = \left(\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n}, 0, 0, 0, \ldots \right).$$

Inaczej mówiąc

$$\begin{gathered} a_0 = b_0 = \binom{n}{0}, \\ a_1 = b_1 = \binom{n}{1}, \\ a_2 = b_2 = \binom{n}{2}, \\ \ldots \quad \ldots \quad \ldots \\ a_n = b_n = \binom{n}{n}, \\ a_m = b_m = 0 \quad \text{dla } m > n. \end{gathered}$$

Możemy też napisać po prostu, że

$$a_m = b_m = \binom{n}{m}$$

dla każdej liczby naturalnej m (gdyż $\binom{n}{m} = 0$ dla $m > n$). Zgodnie ze wzorem Cauchy'ego mamy zatem

$$h = (c_0, c_1, c_2, \ldots),$$

gdzie

$$c_m = a_0 b_m + a_1 b_{m-1} + \ldots + a_{m-1} b_1 + a_m b_0 = \sum_{k=0}^{m} a_k b_{m-k}$$

dla $m = 0, 1, 2, \ldots$ Po podstawieniu otrzymamy

$$c_n = \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \ldots + \binom{n}{n-1}\binom{n}{1} + \binom{n}{n}\binom{n}{0} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k}.$$

Ponieważ

$$\binom{n}{n-k} = \binom{n}{k},$$

więc ostatecznie otrzymujemy

$$c_n = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

Porównując obliczone współczynniki stojące w obu wielomianach przy x^n otrzymamy dowodzoną równość.

W dowodzie następnego wzoru skorzystamy ze wzoru dwumianowego Newtona i z podstawowych własności liczb zespolonych. Przypomnijmy krótko te własności.

Liczbą zespoloną nazywamy liczbę postaci $a + bi$, gdzie i jest tzw. **jednostką urojoną**, tzn. liczbą o tej własności, że $i^2 = -1$. Każda liczba rzeczywista jest liczbą zespoloną:

$$a = a + 0i$$

dla $a \in \mathbb{R}$. Działania na liczbach zespolonych wykonujemy w następujący sposób:

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i, \\ (a + bi) - (c + di) &= (a - c) + (b - d)i, \\ (a + bi) \cdot (c + di) &= ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i, \end{aligned}$$

dla dowolnych liczb zespolonych $a + bi$ oraz $c + di$. Jeśli ponadto $c + di \neq 0$, to

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{(a+bi)\cdot(c-di)}{(c+di)\cdot(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2-(di)^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i.$$

Liczby zespolone wykorzystamy do rozwiązywania równań kwadratowych. Przypuśćmy, że dane jest równanie kwadratowe

$$ax^2 + bx + c = 0,$$

w którym współczynniki są liczbami rzeczywistymi oraz wyróżnik Δ jest ujemny:

$$\Delta = b^2 - 4ac < 0.$$

Wtedy równanie ma dwa pierwiastki zespolone:

$$x_1 = \frac{-b - \sqrt{-\Delta}\cdot i}{2a} \quad \text{oraz} \quad x_2 = \frac{-b + \sqrt{-\Delta}\cdot i}{2a}$$

czyli

$$x_1 = \frac{-b}{2a} + \frac{-\sqrt{-\Delta}}{2a}\cdot i \quad \text{oraz} \quad x_2 = \frac{-b}{2a} + \frac{\sqrt{-\Delta}}{2a}\cdot i.$$

W zbiorze liczb zespolonych prawdziwe są znane ze szkoły wzory skróconego mnożenia, w szczególności przypomniany wcześniej wzór dwumianowy Newtona.

Udowodnimy teraz równość

$$\sum_{k=0}^{n} \binom{3n}{3k} = \frac{8^n + 2\cdot(-1)^n}{3}.$$

Przykłady. Dla $n = 1$ dostajemy równość

$$\binom{3}{0} + \binom{3}{3} = 1 + 1 = 2 = \frac{8^1 + 2\cdot(-1)^1}{3} = \frac{8-2}{3} = \frac{6}{3}.$$

Dla $n = 2$ mamy:

$$\binom{6}{0} + \binom{6}{3} + \binom{6}{6} = 1 + 20 + 1 = 22 = \frac{8^2 + 2\cdot(-1)^2}{3} = \frac{64+2}{3} = \frac{66}{3}.$$

Wreszcie dla $n = 3$ otrzymujemy

$$\binom{9}{0} + \binom{9}{3} + \binom{9}{6} + \binom{9}{9} = 1 + 84 + 84 + 1 = 170 = \frac{8^3 + 2\cdot(-1)^3}{3} = \frac{512-2}{3} = \frac{510}{3}.$$

Dowód równości rozpoczniemy od rozwiązania równania

$$x^3 = 1$$

w zbiorze liczb zespolonych. Przekształcamy najpierw to równanie:

$$x^3 - 1 = 0,$$
$$(x-1)(x^2 + x + 1) = 0.$$

Jednym pierwiastkiem jest oczywiście $x_1 = 1$. Dwa następne pierwiastki otrzymamy rozwiązując równanie kwadratowe

$$x^2 + x + 1 = 0.$$

Ponieważ $\Delta = -3$, więc otrzymujemy pierwiastki zespolone

$$x_2 = \frac{-1 - \sqrt{3} \cdot i}{2} \quad \text{oraz} \quad x_3 = \frac{-1 + \sqrt{3} \cdot i}{2}.$$

Pierwiastki te nazywamy zespolonymi pierwiastkami trzeciego stopnia z jedności. Niech ε będzie którymkolwiek z pierwiastków x_2 lub x_3. Wtedy oczywiście

$$\varepsilon^3 = 1.$$

Ponadto ε jest pierwiastkiem równania kwadratowego $x^2 + x + 1 = 0$, więc

$$\varepsilon^2 + \varepsilon + 1 = 0.$$

Stąd wynika, że

$$1 + \varepsilon = -\varepsilon^2 \quad \text{oraz} \quad 1 + \varepsilon^2 = -\varepsilon.$$

Obliczymy teraz dwoma sposobami sumę

$$(1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n}.$$

Najpierw skorzystamy ze wzoru dwumianowego Newtona:

$$\begin{aligned}
(1 + \varepsilon^0)^{3n} + (1 + \varepsilon^1)^{3n} + (1 + \varepsilon^2)^{3n} &= \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0)^k + \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^1)^k + \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^2)^k = \\
&= \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{0 \cdot k} + \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{1 \cdot k} + \sum_{k=0}^{3n} \binom{3n}{k} \varepsilon^{2 \cdot k} = \\
&= \sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0 + \varepsilon^k + \varepsilon^{2k}) = \\
&= \sum_{k=0}^{3n} \binom{3n}{k} (1 + \varepsilon^k + \varepsilon^{2k}).
\end{aligned}$$

Popatrzmy teraz, jak wyglądają sumy

$$1 + \varepsilon^k + \varepsilon^{2k}$$

dla różnych k. Oczywiście dla liczb k podzielnych przez 3 dodajemy do siebie trzy jedynki. Zatem suma jest równa 3. Niech teraz $k = 3l + 1$. Wtedy

$$1 + \varepsilon^k + \varepsilon^{2k} = 1 + \varepsilon^{3l} \cdot \varepsilon + \varepsilon^{6l} \cdot \varepsilon^2 = 1 + \varepsilon + \varepsilon^2 = 0.$$

Podobnie dla $k = 3l + 2$ stwierdzimy, że ta suma równa jest 0. Zatem, kontynuując przerwane obliczenia, dostajemy

$$\sum_{k=0}^{3n} \binom{3n}{k} (\varepsilon^0 + \varepsilon^k + \varepsilon^{2k}) = \sum_{k=0}^{n} 3 \binom{3n}{3k} = 3 \cdot \sum_{k=0}^{n} \binom{3n}{3k}.$$

Następnie obliczymy tę samą sumę bez odwoływania się do wzoru Newtona. Mamy wtedy:

$$\begin{aligned}
(1+\varepsilon^0)^{3n}+(1+\varepsilon^1)^{3n}+(1+\varepsilon^2)^{3n} &= (1+1)^{3n}+(1+\varepsilon)^{3n}+(1+\varepsilon^2)^{3n} = \\
&= 2^{3n}+(-\varepsilon^2)^{3n}+(-\varepsilon)^{3n} = \\
&= 2^{3n}+(-1)^{3n}\varepsilon^{6n}+(-1)^{3n}\varepsilon^{3n} = \\
&= 2^{3n}+(-1)^{n}(\varepsilon^3)^{2n}+(-1)^{n}(\varepsilon^3)^{n} = \\
&= 2^{3n}+(-1)^{n}+(-1)^{n} = \\
&= 2^{3n}+2\cdot(-1)^{n}.
\end{aligned}$$

W tym dowodzie korzystaliśmy z oczywistej równości:

$$(-1)^{3n}=(-1)^n$$

oraz ze wspomnianych wyżej równości

$$1+\varepsilon=-\varepsilon^2 \quad \text{oraz} \quad 1+\varepsilon^2=-\varepsilon.$$

Porównując wyniki obu obliczeń, otrzymamy:

$$3\cdot\sum_{k=0}^{n}\binom{3n}{3k}=8^n+2\cdot(-1)^n,$$

czyli ostatecznie

$$\sum_{k=0}^{n}\binom{3n}{3k}=\frac{8^n+2\cdot(-1)^n}{3}.$$

Dowody niealgebraiczne.

Pokażemy teraz dowody niealgebraiczne obu udowodnionych wyżej równości. Najpierw dowodzimy równości

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}.$$

Pokażemy tzw. *dowód kombinatoryczny*, polegający na tym, że dwoma sposobami policzymy elementy tego samego zbioru. Niech M i K będą dwoma rozłącznymi zbiorami n elementowymi. Wtedy oczywiście zbiór $M\cup K$ ma $2n$ elementów. Policzymy elementy następującego zbioru A:

$$A=\big\{X\subseteq M\cup K:\ |X|=n\big\}.$$

Z jednej strony, zbiór A ma $\binom{2n}{n}$ elementów,

$$|A|=\binom{2n}{n},$$

co wynika bezpośrednio z definicji współczynnika dwumianowego: zliczamy przecież n-elementowe podzbiory zbioru $2n$-elementowego. Z drugiej strony, zbiór A jest sumą zbiorów rozłącznych

$$A=A_0\cup A_1\cup\ldots\cup A_n,$$

gdzie

$$A_k=\big\{X\in A:\ |X\cap K|=k\big\}$$

dla $k = 0, 1, \ldots, n$. Stąd wynika, że

$$|A| = |A_0| + |A_1| + \ldots + |A_n| = \sum_{k=0}^{n} |A_k|.$$

Policzymy teraz elementy dowolnego zbioru A_k. Zbiór $X \in A_k$ możemy utworzyć wybierając k elementów ze zbioru K oraz $n - k$ elementów ze zbioru M. Inaczej mówiąc, możemy wybrać k elementów ze zbioru K i *odrzucić* k elementów ze zbioru M. Stąd wynika, że

$$|A_k| = \binom{n}{k} \cdot \binom{n}{n-k} = \binom{n}{k} \cdot \binom{n}{k} = \binom{n}{k}^2.$$

Zatem

$$|A| = \sum_{k=0}^{n} \binom{n}{k}^2,$$

co kończy dowód.

Ten dowód kombinatoryczny ma następującą interpretację. Dany jest zbiór $2n$ osób: n kobiet (zbiór K) i n mężczyzn (zbiór M). Pytamy, na ile sposobów można z tego zbioru wybrać delegację składającą się z n osób. Z jednej strony, wybieramy n osób spośród $2n$ osób – oczywiście na $\binom{2n}{n}$ sposobów. Z drugiej strony, najpierw ustalamy liczbę kobiet ($k = 0, 1, \ldots, n$), potem wybieramy k kobiet i wreszcie *odrzucamy* k mężczyzn. Możemy to zrobić na $\binom{n}{k}^2$ sposobów i po dodaniu tych liczb dla wszystkich k otrzymujemy liczbę

$$\sum_{k=0}^{n} \binom{n}{k}^2$$

jaką łączną liczbę sposobów wyboru.

Teraz udowodnimy równość

$$\sum_{k=0}^{n} \binom{3n}{3k} = \frac{8^n + 2 \cdot (-1)^n}{3}.$$

Tym razem ułożymy tzw. *zależność rekurencyjną*. Przypuśćmy, że mamy dany zbiór $3n$-elementowy A. Podzbiór B zbioru A nazwiemy podzbiorem **dobrym**, jeśli liczba jego elementów jest podzielna przez 3. W przeciwnym przypadku podzbiór B nazwiemy podzbiorem **złym**. Niech a_n będzie liczbą wszystkich dobrych podzbiorów zbioru $3n$-elementowego. Mamy pokazać, że

$$a_n = \frac{8^n + 2 \cdot (-1)^n}{3}$$

dla $n = 1, 2, \ldots$

Oczywiście $a_1 = 2$, gdyż zbiór trzyelementowy A ma dwa podzbiory dobre: zbiór pusty $\varnothing$ i cały zbiór A.

Znajdziemy teraz zależność a_{n+1} od a_n. Niech A będzie zbiorem $3n$-elementowym i niech $a, b, c \notin A$, przy czym $a \neq b$, $a \neq c$ oraz $b \neq c$. Zbiór A ma a_n podzbiorów dobrych i $2^{3n} - a_n$ podzbiorów złych. Chcemy policzyć, ile podzbiorów dobrych ma zbiór $A \cup \{a, b, c\}$.

Dla każdego podzbióru B zbioru A policzymy, ile jest podzbiorów dobrych zbioru $A \cup \{a, b, c\}$ zawierających zbiór B. Jeśli zbiór B jest podzbiorem dobrym, to istnieją 2 dobre podzbiory zbioru $A \cup \{a, b, c\}$ zawierające B: sam zbiór B oraz zbiór $B \cup \{a, b, c\}$. Jeśli zbiór B jest podzbiorem złym, to istnieją 3 podzbiory dobre zbioru $A \cup \{a, b, c\}$ zawierające B. Mianowicie, jeśli liczba elementów zbioru B daje resztę 1 przy dzieleniu przez 3, to tymi podzbiorami dobrymi są:

$$B \cup \{a, b\}, \quad B \cup \{a, c\} \quad \text{oraz} \quad B \cup \{b, c\}.$$

Jeśli zaś liczba elementów zbioru B daje resztę 2 przy dzieleniu przez 3, to tymi podzbiorami dobrymi są:

$$B \cup \{a\}, \quad B \cup \{b\} \quad \text{oraz} \quad B \cup \{c\}.$$

Stąd wynika, że

$$a_{n+1} = 2 \cdot a_n + 3 \cdot (2^{3n} - a_n) = 3 \cdot 8^n - a_n.$$

Ciąg (a_n) spełnia zatem następującą *zależność rekurencyjną*:

$$\begin{cases} a_1 = 2, \\ a_{n+1} = 3 \cdot 8^n - a_n. \end{cases}$$

Możemy teraz udowodnić przez indukcję, że

$$a_n = \frac{8^n + 2 \cdot (-1)^n}{3}$$

dla $n = 1, 2, \ldots$

1. Sprawdzamy warunek początkowy (dla $n = 1$). Mianowicie $a_1 = 2$ oraz

$$\frac{8^1 + 2 \cdot (-1)^1}{3} = \frac{8 - 2}{3} = 2.$$

2. Krok indukcyjny.
Zakładamy, że dla pewnej liczby naturalnej n zachodzi równość

$$a_n = \frac{8^n + 2 \cdot (-1)^n}{3}$$

i dowodzimy, że zachodzi też wtedy równość

$$a_{n+1} = \frac{8^{n+1} + 2 \cdot (-1)^{n+1}}{3}.$$

Otóż

$$a_{n+1} = 3 \cdot 8^n - a_n = 3 \cdot 8^n - \frac{8^n + 2 \cdot (-1)^n}{3} = \frac{9 \cdot 8^n - 8^n - 2 \cdot (-1)^n}{3} = \frac{8 \cdot 8^n + 2 \cdot (-1)^{n+1}}{3} =$$
$$= \frac{8^{n+1} + 2 \cdot (-1)^{n+1}}{3},$$

co kończy dowód indukcyjny.

Pokażemy jeszcze, w jaki sposób z otrzymanej zależności rekurencyjnej można *wyprowadzić* wzór ogólny. Definiujemy ciąg (b_n) wzorem

$$b_n = (-1)^n \cdot a_n$$

dla $n = 1, 2, \ldots$ Mamy wówczas

$$b_{n+1} = (-1)^{n+1} \cdot a_{n+1} = (-1)^{n+1} \cdot (3 \cdot 8^n - a_n) = 3 \cdot (-1)^{n+1} \cdot 8^n - (-1)^{n+1} \cdot a_n =$$
$$= 3 \cdot (-1)^{n+1} \cdot 8^n + (-1)^n \cdot a_n = b_n + 3 \cdot (-1)^{n+1} \cdot 8^n.$$

Zatem

$$
\begin{aligned}
b_n &= b_{n-1} + 3 \cdot (-1)^n \cdot 8^{n-1}, \\
b_{n-1} &= b_{n-2} + 3 \cdot (-1)^{n-1} \cdot 8^{n-2}, \\
b_{n-2} &= b_{n-3} + 3 \cdot (-1)^{n-2} \cdot 8^{n-3}, \\
\ldots &\quad \ldots \\
b_4 &= b_3 + 3 \cdot (-1)^4 \cdot 8^3, \\
b_3 &= b_2 + 3 \cdot (-1)^3 \cdot 8^2, \\
b_2 &= b_1 + 3 \cdot (-1)^2 \cdot 8^1.
\end{aligned}
$$

Po dodaniu stronami tych równości i zredukowaniu wyrazów $b_2, b_3, \ldots, b_{n-1}$ występujących po obu stronach równości, dostaniemy

$$
\begin{aligned}
b_n &= b_1 + 3 \cdot \big((-1)^2 \cdot 8^1 + (-1)^3 \cdot 8^2 + \ldots + (-1)^{n-1} \cdot 8^{n-2} + (-1)^n \cdot 8^{n-1}\big) = \\
&= b_1 - 3 \cdot \big((-8)^1 + (-8)^2 + \ldots + (-8^{n-2} + (-8)^{n-1}\big) = \\
&= b_1 + 24 \cdot \big(1 + (-8)^1 + \ldots + (-8)^{n-3} + (-8)^{n-2}\big) = \\
&= (-1)^1 \cdot a_1 + 24 \cdot \frac{1 - (-8)^{n-1}}{1 - (-8)} = \\
&= -2 + 24 \cdot \frac{1 - (-8)^{n-1}}{9} = \\
&= -2 + 8 \cdot \frac{1 - (-8)^{n-1}}{3} = \\
&= \frac{-6 + 8 - 8 \cdot (-1)^{n-1} \cdot 8^{n-1}}{3} = \\
&= \frac{2 + (-1)^n \cdot 8^n}{3}.
\end{aligned}
$$

Stąd wynika, że

$$
\begin{aligned}
(-1)^n \cdot a_n &= \frac{2 + (-1)^n \cdot 8^n}{3}, \\
(-1)^{2n} \cdot a_n &= \frac{2 \cdot (-1)^n + (-1)^{2n} \cdot 8^n}{3}, \\
a_n &= \frac{8^n + 2 \cdot (-1)^n}{3},
\end{aligned}
$$

co kończy dowód.

Systemy trójek Steinera.

Na początku popatrzmy na przykład.

Przykład. (V. Bryant, *Aspekty kombinatoryki*, str. 199.) Dziewięć gatunków kawy ma zostać rozdanych do testowania różnym rodzinom. Nie jest wskazane, by każda rodzina porównywała wszystkie dziewięć gatunków (po około czwartej próbie wszystkie one smakują tak samo!). Tak więc każda z dwunastu rodzin otrzyma do porównania trzy gatunki. Podać taką konfigurację eksperymentu, w której każda para gatunków (spośród dziewięciu) jest porównywana w jednej rodzinie.

Rozwiązanie. Niech rodzaje kawy będą ponumerowane liczbami od 1 do 9. Rozdajmy dwunastu rodzinom do porównania następujące zestawy trzech gatunków:

$$
\begin{array}{lll}
\{1,2,3\}, & \{4,5,6\}, & \{7,8,9\}, \\
\{1,4,7\}, & \{2,5,8\}, & \{3,6,9\}, \\
\{1,5,9\}, & \{2,6,7\}, & \{3,4,8\}, \\
\{1,6,8\}, & \{2,4,9\}, & \{3,5,7\}.
\end{array}
$$

Wówczas każda para liczb od 1 do 9 znajduje się w jednym z tych zbiorów.

Systemem trójek Steinera nazywamy parę zbiorów (S, T) o następujących własnościach:

(1) zbiory S i T są skończone,

(2) elementami zbioru T są 3-elementowe podzbiory zbioru S:

$$X \in T \quad \Rightarrow \quad X \subseteq S \ \wedge \ |X| = 3,$$

(3) każda para elementów zbioru S występuje w dokładnie jednym zbiorze należącym do T:

$$a, b \in S \ \wedge \ a \neq b \quad \Rightarrow \quad \text{istnieje dokładnie jeden zbiór } X \in T \text{ taki, że } a, b \in X.$$

Elementy zbioru S nazywamy często **punktami**, a zbiory należące do T nazywamy **trójkami** punktów. Warunek (3) możemy zatem wysłowić w taki sposób, że każde dwa punkty ze zbioru S należą do dokładnie jednej trójki ze zbioru T.

Zbiór trójek w powyższym przykładzie ma jeszcze jedną interesującą własność. Mianowicie w każdym wierszu występują wszystkie punkty (czyli liczby od 1 do 9). Zatem zbiór T trójek punktów można podzielić na 4 rozłączne zbiory o tej własności, że elementy trójek z każdego z tych zbiorów wyczerpują cały zbiór punktów.

Warstwą nazwiemy taki zbiór trójek parami rozłącznych, którego sumą jest cały zbiór S. **Systemem trójek Kirkmana** nazywamy taki system trójek Steinera, w którym zbiór trójek T można podzielić na parami rozłączne warstwy. System trójek Steinera pokazany w powyższym przykładzie jest zatem systemem trójek Kirkmana.

Przykłady.

1. Niech $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Niech następnie zbiór T będzie zbiorem trójek z poprzedniego przykładu:

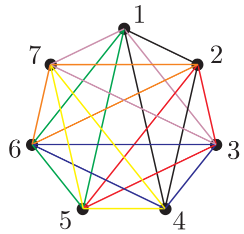
$$T = \left\{ \begin{array}{llllll} \{1,2,3\}, & \{4,5,6\}, & \{7,8,9\}, & \{1,4,7\}, & \{2,5,8\}, & \{3,6,9\}, \\ \{1,5,9\}, & \{2,6,7\}, & \{3,4,8\}, & \{1,6,8\}, & \{2,4,9\}, & \{3,5,7\} \end{array} \right\}.$$

   Wtedy para (S, T) jest systemem trójek Steinera. Widzieliśmy już, że jest to także system trójek Kirkmana.

2. Niech $S = \{1, 2, 3, 4, 5, 6, 7\}$ i niech T będzie następującym zbiorem trójek:

$$T = \big\{\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{1,5,6\}, \{2,6,7\}, \{1,3,7\}\big\}.$$

   Wtedy para (S, T) jest systemem trójek Steinera. Ten system trójek Steinera Ma ładną interpretację graficzną:



3. Niech $S = \{1, 2, \ldots, 15\}$ i niech T będzie zbiorem następujących trójek liczb:

$\{1,2,3\}$,	$\{4,8,12\}$,	$\{5,10,14\}$,	$\{6,11,13\}$,	$\{7,9,15\}$,
$\{1,4,5\}$,	$\{2,8,10\}$,	$\{3,13,15\}$,	$\{6,9,14\}$,	$\{7,11,12\}$,
$\{1,6,7\}$,	$\{2,9,11\}$,	$\{3,12,14\}$,	$\{4,10,15\}$,	$\{5,8,13\}$,
$\{1,8,9\}$,	$\{2,12,15\}$,	$\{3,5,6\}$,	$\{4,11,14\}$,	$\{7,10,13\}$,
$\{1,10,11\}$,	$\{2,13,14\}$,	$\{3,4,7\}$,	$\{5,9,12\}$,	$\{6,8,15\}$,
$\{1,12,13\}$,	$\{2,4,6\}$,	$\{3,9,10\}$,	$\{5,11,15\}$,	$\{7,8,14\}$,
$\{1,14,15\}$,	$\{2,5,7\}$,	$\{3,8,11\}$,	$\{4,9,13\}$,	$\{6,10,12\}$.

Wtedy para (S, T) jest systemem trójek Steinera. Zauważmy, że ten system jest również systemem trójek Kirkmana (warstwami są wiersze powyższej tablicy). Ten system stanowi rozwiązanie następującego zadania postawionego i rozwiązanego przez Kirkmana:

Czy możliwe jest, aby 15 uczennic wychodziło na spacer przez 7 dni tygodnia w taki sposób, by codziennie spacerowały w 5 rzędach po 3 uczennice w każdym rzędzie oraz, by każda para uczennic spacerowała w tym samym rzędzie dokładnie jednego dnia?

Wiersze powyższej tablicy ilustrują sposób ustawienia uczennic przez kolejne dni tygodnia, od poniedziałku do niedzieli.

Twierdzenie. Jeśli istnieje system trójek Steinera (S, T), w którym $|S| = n$, to liczba n przy dzieleniu przez 6 daje resztę 1 lub 3.

Dowód. Dwoma sposobami zliczamy pary punktów. Z jednej strony, liczba par jest równa $\binom{n}{2}$. Z drugiej strony, każda para należy do dokładnie jednej trójki ze zbioru T. Ponieważ w każdej trójce są dokładnie 3 pary, więc

$$3 \cdot |T| = \binom{n}{2} = \frac{n(n-1)}{2},$$

czyli

$$|T| = \frac{n(n-1)}{6}.$$

Natępnie bierzemy dowolny element x zbioru S i rozważamy zbiór

$$U = \{t \in T : \ x \in t\}.$$

Zauważmy, że rodzina par

$$\big\{t \setminus \{x\} : \ t \in U\big\}$$

jest podziałem zbioru $S \setminus \{x\}$ na zbiory dwuelementowe. Stąd wynika, że liczba n jest nieparzysta. Zatem n przy dzieleniu przez 6 może dać jedną z reszt 1, 3 lub 5. Ponieważ liczba $n(n-1)$ jest podzielna przez 6, więc n nie może dawać reszty 5 przy dzieleniu przez 6, co kończy dowód twierdzenia.

Wniosek. Jeśli istnieje system trójek Kirkmana (S, T), w którym $|S| = n$, to liczba n daje resztę 3 przy dzieleniu przez 6.

Dowód. Ponieważ jedna warstwa daje podział zbioru S na zbiory trzyelementowe, więc liczba n dzieli się przez 3. Nie może zatem dawać reszty 1 przy dzieleniu przez 6.

Prawdziwe jest też twierdzenie odwrotne: jeśli liczba naturalna $n \geq 3$ daje resztę 1 lub 3 przy dzieleniu przez 6, to istnieje system trójek Steinera (S, T), w którym $|S| = n$. Pokażemy teraz sposób konstrukcji systemu trójek Steinera (S, T), w którym $|S| = 6m + 3$. Do tego wprowadzimy kilka pojęć algebraicznych.

Niech Q będzie zbiorem skończonym, w którym jest określone działanie dwuargumentowe $\circ$. Mówimy, że zbiór Q (z działaniem $\circ$) jest **quasigrupą przemienną**, jeśli spełnione są następujące warunki:

(1) $a \circ b = b \circ a$ dla dowolnych $a, b \in Q$,

(2) dla dowolnych $a, c \in Q$ istnieje dokładnie jeden element b zbioru Q taki, że $a \circ b = c$.

Warunek (2) jest równoważny następującemu warunkowi (2'):
(2') dla dowolnego $a \in Q$ funkcja $f : Q \to Q$ określona wzorem $f(x) = a \circ x$ jest różnowartościowa

Mówimy następnie, że quasigrupa Q jest **idempotentna**, jeśli ponadto jest spełniony warunek
(3) $a \circ a = a$ dla dowolnego $a \in Q$.

Przykłady.

1. Zbiór liczb $Q = \{0, 1, 2\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	**0**	**1**	**2**
0	0	2	1
1	2	1	0
2	1	0	2

   jest idempotentną quasigrupą przemienną.

2. Zbiór liczb $Q = \{0, 1, 2, 3, 4\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	**0**	**1**	**2**	**3**	**4**
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

   jest idempotentną quasigrupą przemienną.

Twierdzenie. Jeśli n jest liczbą nieparzystą, to istnieje idempotentna quasigrupa przemienna Q mająca n elementów.

Dowód. Sposób konstrukcji quasigrupy Q zilustrujemy najpierw na przykładzie. Niech $Q = \{0, 1, \ldots, n-1\}$ i zdefiniujmy w zbiorze Q działanie $\circ$ wzorem

$$i \circ j = (i + j) \bmod n$$

dla $i, j \in Q$. Symbolem $a \bmod n$ oznaczamy resztę z dzielenia liczby a przez n. Działanie $\circ$ jest zatem działaniem dodawania modulo n. Zauważmy teraz, że dla każdego $j \in Q$ istnieje element $i \in Q$ taki, że $i \circ i = j$. Wynika to stąd, że dla każdej liczby naturalnej j kongruencja

$$2x \equiv j \pmod{n}$$

ma rozwiązanie. Zatem w tabelce działania $\circ$ w zbiorze Q na przekątnej występują wszystkie elementy zbioru Q. Na przykład dla $n = 5$ mamy:

$\circ$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Zauważmy, że na przekątnej stoją liczby 0, 2, 4, 1, 3. Teraz w tej tabelce przenumerowujemy liczby będące wynikami działania w taki sposób, by na przekątnej występowały kolejno liczby 0, 1, 2, 3, 4. Zatem liczbę 0 zostawiamy wszędzie w tabelce bez zmian, zamiast 2 piszemy 1, zamiast 4 piszemy 2, zamiast 1 piszemy 3 i zamiast 3 piszemy 4. Otrzymamy tabelkę

$\circ$	**0**	**1**	**2**	**3**	**4**
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

Nietrudno zauważyć, że dla dowolnej nieparzystej liczby naturalnej n taka konstrukcja jest możliwa. Opiszemy ją teraz dokładniej. Okazuje się, że działanie $\circ$ w zbiorze $Q = \{0, 1, \ldots, n-1\}$ będzie wtedy opisane wzorem

$$i \circ j = \begin{cases} \frac{i+j}{2}, & \text{jeśli } i+j \text{ jest liczbą parzystą,} \\ \frac{i+j+n}{2} \bmod n, & \text{jeśli } i+j \text{ jest liczbą nieparzystą} \end{cases}$$

dla dowolnych $i, j \in Q$. Zauważmy, że jeśli $i+j$ jest liczbą nieparzystą, to liczba $i+j+n$ jest parzysta, więc $\frac{i+j+n}{2}$ jest liczbą całkowitą.

Wykażemy, że zbiór Q z działaniem $\circ$ jest idempotentną quasigrupą przemienną. Przemienność działania $\circ$ jest oczywista. Idempotentność wynika stąd, że dla każdego i liczba $i+i$ jest parzysta, więc

$$i \circ i = \frac{i+i}{2} = i.$$

Wykażemy wreszcie warunek (2'). Niech $i, j, k \in Q$ i załóżmy, że

$$i \circ j = i \circ k.$$

Możliwe są trzy przypadki.

Przypadek 1. Liczby $i+j$ oraz $i+k$ są parzyste. Wtedy

$$\frac{i+j}{2} = \frac{i+k}{2},$$

skąd natychmiast wynika, że $j = k$.

Przypadek 2. Liczby $i+j$ oraz $i+k$ są nieparzyste. Wtedy

$$\frac{i+j+n}{2} \bmod n = \frac{i+k+n}{2} \bmod n.$$

Zatem

$$\begin{aligned} \frac{i+j+n}{2} &\equiv \frac{i+k+n}{2} \pmod{n}, \\ i+j+n &\equiv i+k+n \pmod{n}, \\ j &\equiv k \pmod{n}. \end{aligned}$$

Ponieważ $0 \leq j,k < n$, więc $j = k$.

Przypadek 3. Jedna z liczb $i+j$ oraz $i+k$ jest parzysta (np. $i+j$), a druga nieparzysta. Wtedy

$$\frac{i+j}{2} = \frac{i+k+n}{2} \bmod n.$$

Zatem

$$\begin{aligned} \frac{i+j}{2} &\equiv \frac{i+k+n}{2} \pmod{n}, \\ i+j &\equiv i+k+n \pmod{n}, \\ j &\equiv k \pmod{n}. \end{aligned}$$

Tak jak w przypadku 2 otrzymujemy $j = k$, co kończy dowód twierdzenia.

Niech teraz Q będzie idempotentną quasigrupą przemienną mającą $2m+1$ elementów. Definiujemy zbiór S w następujący sposób

$$S = Q \times \{0,1,2\} = \big\{(a,i) : \ a \in Q \ \wedge \ i \in \{0,1,2\}\big\}.$$

Oczywiście $|S| = n = 6m+3$. Zdefiniujemy teraz zbiór T.

Do zbioru T zaliczymy dwa rodzaje trójek par:

(1) Trójki pierwszego rodzaju:

$$\{(a,0),(a,1),(a,2)\}$$

dla $a \in Q$.

(2) Trójki drugiego rodzaju:

$$\{(a,0),(b,0),(a \circ b,1)\}, \quad \{(a,1),(b,1),(a \circ b,2)\}, \quad \{(a,2),(b,2),(a \circ b,0)\}$$

dla $a,b \in Q$ takich, że $a \neq b$.

Udowodnimy teraz, że tak określona para (S,T) jest rzeczywiście systemem trójek Steinera. Najpierw pokażemy, że każde dwie pary ze zbioru S znajdują się w co najmniej jednej trójce ze zbioru T. Niech więc $(a,k),(b,l) \in S$ oraz $(a,k) \neq (b,l)$. Możliwe są trzy przypadki.

Przypadek 1. $a = b$. Wtedy $k \neq l$ oraz

$$(a,k),(a,l) \in \{(a,0),(a,1),(a,2)\} \in T.$$

Przypadek 2. $a \neq b$ oraz $k = l$. Wtedy

$$(a,k),(b,k) \in \{(a,k),(b,k),(a \circ b,(k+1) \bmod 3)\} \in T.$$

Przypadek 3. $a \neq b$ oraz $k \neq l$. Para liczb $\{k, l\}$ jest jedną z trzech par: $\{0,1\}, \{1,2\}, \{2,0\}$. Możemy zatem przyjąć, że $l = (k+1) \bmod 3$. Z definicji quasigrupy wynika, że istnieje element $c \in Q$ taki, że $a \circ c = b$. Ponieważ Q jest quasigrupą idempotentną oraz $a \neq b$, więc $c \neq a$. Zatem

$$(a,k),(b,l) \in \{(a,k),(c,k),(a \circ c,(k+1) \bmod 3)\} = \{(a,k),(c,k),(b,l)\} \in T.$$

Aby teraz pokazać, że każde dwie pary należą do dokładnie jednej trójki ze zbioru T, wystarczy pokazać, że zbiór T ma $\frac{n(n-1)}{6}$ elementów. Otóż w zbiorze T istnieje $2m+1$ trójek pierwszego rodzaju oraz $3 \cdot \binom{2m+1}{2}$ trójek drugiego rodzaju. Zatem

$$|T| = (2m+1) + 3 \cdot \frac{(2m+1) \cdot 2m}{2} = (2m+1) + 3m(2m+1) = (2m+1)(3m+1)$$

oraz

$$\frac{n(n-1)}{6} = \frac{(6m+3)(6m+2)}{6} = (2m+1)(3m+1).$$

To kończy dowód, że para (S,T) jest systemem trójek Steinera.

Przykłady.

1. Dla quasigrupy $\{0,1,2\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	**0**	**1**	**2**
0	0	2	1
1	2	1	0
2	1	0	2

Otrzymujemy następujący zbiór S:

$$S = \left\{ \begin{array}{ccc} (0,0) & (1,0) & (2,0) \\ (0,1) & (1,1) & (2,1) \\ (0,2) & (1,2) & (2,2) \end{array} \right\}.$$

Zbiór T składa się z trzech trójek pierwszego rodzaju:

$$\{(0,0),(0,1),(0,2)\}, \quad \{(1,0),(1,1),(2,1)\} \quad \text{oraz} \quad \{(2,0),(2,1),(2,2)\}$$

i dziewięciu trójek drugiego rodzaju:

$$\begin{aligned}
\{(0,0),(1,0),(0 \circ 1,1)\} &= \{(0,0),(1,0),(2,1)\}, \\
\{(0,1),(1,1),(0 \circ 1,2)\} &= \{(0,1),(1,1),(2,2)\}, \\
\{(0,2),(1,2),(0 \circ 1,0)\} &= \{(0,2),(1,2),(2,0)\}, \\
\{(0,0),(2,0),(0 \circ 2,1)\} &= \{(0,0),(2,0),(1,1)\}, \\
\{(0,1),(2,1),(0 \circ 2,2)\} &= \{(0,1),(2,1),(1,2)\}, \\
\{(0,2),(2,2),(0 \circ 2,0)\} &= \{(0,2),(2,2),(1,0)\}, \\
\{(1,0),(2,0),(1 \circ 2,1)\} &= \{(1,0),(2,0),(0,1)\}, \\
\{(1,1),(2,1),(1 \circ 2,2)\} &= \{(1,1),(2,1),(0,2)\}, \\
\{(1,2),(2,2),(1 \circ 2,0)\} &= \{(1,2),(2,2),(0,0)\}.
\end{aligned}$$

Zauważmy następnie, że jeśli ponumerujemy pary $(i, j) \in S$ w następujący sposób

$$\begin{array}{lll} (0,0) \mapsto 1 & (1,0) \mapsto 4 & (2,0) \mapsto 9 \\ (0,1) \mapsto 2 & (1,1) \mapsto 5 & (2,1) \mapsto 7 \\ (0,2) \mapsto 3 & (1,2) \mapsto 6 & (2,2) \mapsto 8 \end{array}$$

to otrzymany system trójek Steinera będzie identyczny z systemem pokazanym w pierwszym przykładzie. Jest to zatem system trójek Kirkmana.

2. Dla quasigrupy $Q = \{0, 1, 2, 3, 4\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	**0**	**1**	**2**	**3**	**4**
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

otrzymujemy następujący zbiór S:

$$S = \left\{ \begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & (4,0) \\ (0,1) & (1,1) & (2,1) & (3,1) & (4,1) \\ (0,2) & (1,2) & (2,2) & (3,2) & (4,2) \end{array} \right\}.$$

Trójki pierwszego rodzaju mają następującą postać:

$$S = \left\{ \begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & (4,0) \\ (0,1) & (1,1) & (2,1) & (3,1) & (4,1) \\ (0,2) & (1,2) & (2,2) & (3,2) & (4,2) \end{array} \right\}$$

Kolorami czerwonym, zielonym i niebieskim zaznaczone są trójki

$$\{(0,0), (0,1), (0,2)\}, \quad \{(3,0), (3,1), (3,2)\} \quad \text{oraz} \quad \{(4,0), (4,1), (4,2)\}.$$

Trójki drugiego rodzaju mają postać:

$$S = \left\{ \begin{array}{ccccc} (0,0) & (1,0) & (2,0) & (3,0) & (4,0) \\ (0,1) & (1,1) & (2,1) & (3,1) & (4,1) \\ (0,2) & (1,2) & (2,2) & (3,2) & (4,2) \end{array} \right\}$$

Kolorem czerwonym zaznaczona jest trójka

$$\{(2,0), (3,0), (2 \circ 3, 1)\} = \{(2,0), (3,0), (0,1)\},$$

kolorem zielonym zaznaczona jest trójka

$$\{(3,1), (4,1), (3 \circ 4, 2)\} = \{(3,1), (4,1), (1,2)\},$$

wreszcie kolorem niebieskim zaznaczona jest trójka

$$\{(0,2), (3,2), (0 \circ 3, 0)\} = \{(0,2), (3,2), (4,0)\}.$$

Można pokazać, że otrzymany system trójek Steinera nie jest systemem trójek Kirkmana, zatem różni się istotnie od przykładu pokazanego wcześniej.

Pokażemy teraz sposób konstrukcji systemu trójek Steinera (S, T), w którym $|S| = 6m + 1$. Znów zaczniemy od pojęć algebraicznych. Mówimy, że quasigrupa przemienna $Q = \{0, 1, \ldots, 2n - 1\}$ (mająca zatem $2n$ elementów) jest **półidempotentna**, jeśli spełnia następujący warunek:

(4) $a \circ a = (n + a) \circ (n + a) = a$ dla $a = 0, 1, \ldots, n$.

Przykłady.

1. Zbiór liczb $Q = \{0, 1\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	**0**	**1**
0	0	1
1	1	0

jest półidempotentną quasigrupą przemienną.

2. Zbiór liczb $Q = \{0, 1, 2, 3, \}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	**0**	**1**	**2**	**3**
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

jest idempotentną quasigrupą przemienną.

2. Zbiór liczb $Q = \{0, 1, 2, 3, 4, 5\}$ z działaniem $\circ$ określonym za pomocą następującej tabelki

$\circ$	**0**	**1**	**2**	**3**	**4**	**5**
0	0	3	1	4	2	5
1	3	1	4	2	5	0
2	1	4	2	5	0	3
3	4	2	5	0	3	1
4	2	5	0	3	1	4
4	5	0	3	1	4	2

jest idempotentną quasigrupą przemienną.

Twierdzenie. Dla każdej liczby naturalnej $n \geq 1$ istnieje półidempotentna quasigrupa przemienna $Q = \{0, 1, \ldots, 2n - 1\}$ mająca $2n$ elemenów.

Szkic dowodu. Znów możemy przenumerować tabelkę dodawania modulo $2n$. Działanie $\circ$ w zbiorze Q będzie wtedy określone wzorem:

$$i \circ j = \begin{cases} \frac{(i+j) \bmod 2n}{2}, & \text{jeśli } i+j \text{ jest liczbą parzystą,} \\ \frac{(i+j-1) \bmod 2n}{2}, & \text{jeśli } i+j \text{ jest liczbą nieparzystą} \end{cases}$$

dla $i, j \in \{0, 1, \ldots, 2n-1\}$. Sprawdzenie, że zbiór Q z tak określonym działaniem $\circ$ jest półidempotentna quasigrupą przemienną, pozostawimy jako ćwiczenie.

Niech teraz $Q = \{0, 1, \ldots, 2m-1\}$ będzie półidempotentną quasigrupą przemienną mającą $2m$ elementów i niech $\infty \notin Q \times \{0, 1, 2\}$. Definiujemy zbiór S w następujący sposób

$$S = \{\infty\} \cup (Q \times \{0, 1, 2\}) = \big\{\infty\big\} \cup \big\{(a, i) : \ a \in Q \ \wedge \ i \in \{0, 1, 2\}\big\}.$$

Oczywiście $|S| = n = 6m + 1$. Zdefiniujemy teraz zbiór T.

Do zbioru T zaliczymy trzy rodzaje trójek par:

(1) Trójki pierwszego rodzaju:

$$\{(a, 0), (a, 1), (a, 2)\}$$

dla $a = 0, \ldots, m-1$.

(2) Trójki drugiego rodzaju:

$$\{\infty, (a, 1), (a+m, 0)\}, \quad \{\infty, (a, 2), (a+m, 1)\}, \quad \{\infty, (a, 0), (a+m, 2)\}$$

dla $a = 0, \ldots, m-1$.

(2) Trójki trzeciego rodzaju:

$$\{(a, 0), (b, 0), (a \circ b, 1)\}, \quad \{(a, 1), (b, 1), (a \circ b, 2)\}, \quad \{(a, 2), (b, 2), (a \circ b, 0)\}$$

dla $a, b \in Q$ takich, że $a \neq b$.

Wykazanie, że tak określona para (S, T) jest rzeczywiście systemem trójek Steinera, pozostawimy jako ćwiczenie.

Przykłady.

1. Dla quasigrupy $\{0, 1\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	**0**	**1**
0	0	1
1	1	0

Otrzymujemy następujący zbiór S:

$$S = \left\{ \begin{array}{ccc} & (0,0) & (1,0) \\ \infty & (0,1) & (1,1) \\ & (0,2) & (1,2) \end{array} \right\}.$$

Zbiór T składa się z jednej trójki pierwszego rodzaju:

$$\{(0, 0), (0, 1), (0, 2)\},$$

trzech trójek drugiego rodzaju:

$$\{\infty, (1,0), (0,1)\}, \quad \{\infty, (1,1), (0,2)\}, \quad \{\infty, (1,2)(0,0)\}$$

i trzech trójek trzeciego rodzaju:

$$\begin{aligned}
\{(0,0), (1,0), (0 \circ 1, 1)\} &= \{(0,0), (1,0), (1,1)\}, \\
\{(0,1), (1,1), (0 \circ 1, 2)\} &= \{(0,1), (1,1), (1,2)\}, \\
\{(0,2), (1,2), (0 \circ 1, 0)\} &= \{(0,2), (1,2), (1,0)\}.
\end{aligned}$$

Zauważmy następnie, że jeśli ponumerujemy elementy zbioru S w następujący sposób

$$\begin{array}{ccc}
 & (0,0) \mapsto 1 & (1,0) \mapsto 6 \\
\infty \mapsto 7 & (0,1) \mapsto 2 & (1,1) \mapsto 5 \\
 & (0,2) \mapsto 4 & (1,2) \mapsto 3
\end{array}$$

to otrzymany system trójek Steinera będzie identyczny z systemem pokazanym poprzednio dla siedmioelementowego zbioru S.

1. Dla quasigrupy $\{0,1,2,3\}$ z działaniem $\circ$ zdefiniowanym za pomocą tabelki

$\circ$	**0**	**1**	**2**	**3**
0	0	2	1	3
1	2	1	3	0
2	1	3	0	2
3	3	0	2	1

otrzymamy następujący zbiór S:

$$S = \left\{ \begin{array}{ccccc}
 & (0,0) & (1,0) & (2,0) & (3,0) \\
\infty & (0,1) & (1,1) & (2,1) & (3,1) \\
 & (0,2) & (1,2) & (2,2) & (3,2)
\end{array} \right\}.$$

Zbiór T składa się z dwóch trójek pierwszego rodzaju (zaznaczonych kolorami czerwonym i zielonym):

$$S = \left\{ \begin{array}{ccccc}
 & \textcolor{red}{(0,0)} & \textcolor{green}{(1,0)} & (2,0) & (3,0) \\
\infty & \textcolor{red}{(0,1)} & \textcolor{green}{(1,1)} & (2,1) & (3,1) \\
 & \textcolor{red}{(0,2)} & \textcolor{green}{(1,2)} & (2,2) & (3,2)
\end{array} \right\}$$

sześciu trójek drugiego rodzaju, z których trzy zostały zaznaczone kolorami czerwonym, zielonym i niebieskim:

$$S = \left\{ \begin{array}{ccccc}
 & (0,0) & (1,0) & \textcolor{red}{(2,0)} & (3,0) \\
\textcolor{red}{\infty} & \textcolor{red}{(0,1)} & (1,1) & (2,1) & (3,1) \\
 & (0,2) & (1,2) & (2,2) & (3,2)
\end{array} \right\}$$

$$S = \left\{ \begin{array}{ccccc}
 & (0,0) & (1,0) & (2,0) & (3,0) \\
\textcolor{green}{\infty} & (0,1) & (1,1) & (2,1) & \textcolor{green}{(3,1)} \\
 & (0,2) & \textcolor{green}{(1,2)} & (2,2) & (3,2)
\end{array} \right\}$$

$$S = \left\{ \begin{array}{ccccc}
 & \textcolor{blue}{(0,0)} & (1,0) & (2,0) & (3,0) \\
\textcolor{blue}{\infty} & (0,1) & (1,1) & (2,1) & (3,1) \\
 & (0,2) & (1,2) & \textcolor{blue}{(2,2)} & (3,2)
\end{array} \right\}$$

i 18 trójek trzeciego rodzaju, z których trzy również zostały zaznaczone kolorami czerwonym, zielonym i niebieskim:

$$S = \left\{ \begin{array}{ccccc} & (0,0) & (1,0) & (2,0) & (3,0) \\ \infty & (0,1) & (1,1) & (2,1) & (3,1) \\ & (0,2) & (1,2) & (2,2) & (3,2) \end{array} \right\}$$

Dowód niealgebraiczny.

Naszkicujemy teraz pochodzący od Kirkmana, oryginalny dowód istnienia systemów trójek Steinera. Wprowadzimy najpierw dwa pojęcia pomocnicze.

Niech $X = \{\sigma_0, \dots, \sigma_{2n-2}\} \cup \{\alpha\}$ będzie zbiorem $2n$-elementowym i niech H będzie zbiorem wszystkich dwuelementowych podzbiorów zbioru X:

$$H = \{A \subseteq X : \ |A| = 2\}.$$

Ciąg zbiorów $(H_0, \dots, H_{2n-2})$ nazywamy **1-faktoryzacją** zbioru H, jeśli dla każdego $x \in X$ w każdym zbiorze H_j istnieje dokładnie jedna para, której x jest elementem.

Ćwiczenie. Ciąg zbiorów $(H_0, \dots, H_{2n-2})$ zdefiniowanych w następujący sposób

$$H_j = \big\{\{\sigma_k, \sigma_l\} : \ k + l \equiv j + 1 \pmod{2n-1}\big\} \cup \big\{\{\alpha, \sigma_{(j+1)n \bmod (2n-1)}\}\big\}$$

dla $j = 0, \dots, 2n-2$ jest 1-faktoryzacją zbioru H.

Przykład. Ciąg zbiorów $(H_0, \dots, H_6)$ zdefiniowanych w następujący sposób

$$\begin{aligned} H_0 &= \big\{\{\sigma_0, \sigma_1\}, \{\sigma_2, \sigma_6\}, \{\sigma_3, \sigma_5\}, \{\sigma_4, \alpha\}\big\}, \\ H_1 &= \big\{\{\sigma_0, \sigma_2\}, \{\sigma_3, \sigma_6\}, \{\sigma_4, \sigma_5\}, \{\sigma_1, \alpha\}\big\}, \\ H_2 &= \big\{\{\sigma_0, \sigma_3\}, \{\sigma_1, \sigma_2\}, \{\sigma_4, \sigma_6\}, \{\sigma_5, \alpha\}\big\}, \\ H_3 &= \big\{\{\sigma_0, \sigma_4\}, \{\sigma_1, \sigma_3\}, \{\sigma_5, \sigma_6\}, \{\sigma_2, \alpha\}\big\}, \\ H_4 &= \big\{\{\sigma_0, \sigma_5\}, \{\sigma_1, \sigma_4\}, \{\sigma_2, \sigma_3\}, \{\sigma_6, \alpha\}\big\}, \\ H_5 &= \big\{\{\sigma_0, \sigma_6\}, \{\sigma_1, \sigma_5\}, \{\sigma_2, \sigma_4\}, \{\sigma_3, \alpha\}\big\}, \\ H_6 &= \big\{\{\sigma_1, \sigma_6\}, \{\sigma_2, \sigma_5\}, \{\sigma_3, \sigma_4\}, \{\sigma_0, \alpha\}\big\} \end{aligned}$$

jest 1-faktoryzacją zbioru $X = \{\sigma_0, \dots, \sigma_6\} \cup \{\alpha\}$. Tę 1-faktoryzację nazywamy **faktoryzacją Kirkmana**.

W dalszym ciągu szczególnie ważne będzie to, że:

$$\begin{aligned} &\{\sigma_0, \sigma_1\} \in H_0, \\ &\{\sigma_0, \sigma_2\}, \{\sigma_1, \alpha\} \in H_1, \\ &\{\sigma_0, \sigma_{j+1}\}, \{\sigma_1, \sigma_j\} \in H_j \quad \text{dla } j = 2, \dots, 2n-3, \\ &\{\sigma_0, \alpha\}, \{\sigma_1, \sigma_{2n-2}\} \in H_{2n-2}. \end{aligned}$$

Przypuśćmy następnie, że para (S, T) jest systemem trójek Steinera, w którym $|S| = n$ (przypominamy, że n jest liczbą nieparzystą). Niech następnie $x, y \in S$ i niech z będzie jedynym elementem zbioru S takim, że $\{x, y, z\} \in T$. Mówimy, że system (S, T) jest x, y**-ogrodzony**, a ciąg $(s_0, \dots, s_{n-4})$ elementów zbioru S jest jego x, y**-ogrodzeniem**, jeśli

$$\{x, s_0, s_1\}, \{y, s_1, s_2\}, \{x, s_2, s_3\}, \{y, s_3, s_4\}, \dots, \{y, s_{n-6}, s_{n-5}\}, \{x, s_{n-5}, s_{n-4}\}, \{y, s_{n-4}, s_0\} \in T.$$

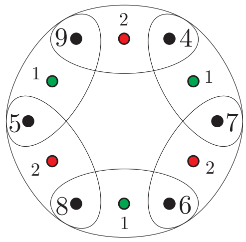
Przykład. System trójek Steinera (S,T), w którym $S=\{1,\ldots,9\}$ oraz

$$T=\left\{\begin{array}{cccccc}\{1,2,3\}, & \{4,5,6\}, & \{7,8,9\}, & \{1,4,7\}, & \{2,5,8\}, & \{3,6,9\}, \\ \{1,5,9\}, & \{2,6,7\}, & \{3,4,8\}, & \{1,6,8\}, & \{2,4,9\}, & \{3,5,7\}\end{array}\right\}$$

jest systemem $1,2$-ogrodzonym, a jego $1,2$-ogrodzeniem jest ciąg $(4,7,6,8,5,9)$:

$$\{1,4,7\},\{2,7,6\},\{1,6,8\},\{2,8,5\},\{1,5,9\},\{2,9,4\}\in T.$$

A oto graficzna ilustracja tego ogrodzenia:



Dowód Kirkmana wynika teraz (przez indukcję, której szczegóły pozostawimy jako ćwiczenie) z następujących trzech faktów.

1. Istnieje system trójek Steinera (S,T), w którym $|S|=3$.

2. Jeśli istnieje system trójek Steinera (S,T), w którym $|S|=2n-1$, to istnieje ogrodzony system trójek Steinera (S^*,T^*), w którym $|S^*|=4n-1$.

3. Jeśli istnieje ogrodzony system trójek Steinera (S,T), w którym $|S|=2n+1$ (przy czym $n\geq 3$), to istnieje ogrodzony system trójek Steinera (S^*,T^*), w którym $|S^*|=4n-3$.

Fakt 1 jest oczywisty. Pokażemy teraz szkice dowodów faktów 2 i 3.

2. Niech (S,T) będzie systemem trójek Steinera, w którym $S=\{s_0,\ldots,s_{2n-2}\}$ oraz niech zbiór $X=\{\sigma_0,\ldots,\sigma_{2n-2}\}\cup\{\alpha\}$ będzie zbiorem rozłącznym ze zbiorem S. Niech następnie ciąg $(H_0,\ldots,H_{2n-2})$ będzie faktoryzacją Kirkmana zbioru H dwuelementowych podzbiorów zbioru X. Definiujemy rodzinę trójek U w następujący sposób:

$$U=\big\{\{s_j,a,b\}:\ (j\in\{0,\ldots,2n-2\})\ \wedge\ (\{a,b\}\in H_j)\big\}.$$

Niech następnie $S^*=S\cup X$ oraz $T^*=T\cup U$. Wtedy para (S^*,T^*) jest σ_0,σ_1-ogrodzonym systemem trójek Steinera oraz ciąg

$$(s_1,\sigma_2,s_2,\sigma_3,s_3,\sigma_4,\ldots,\sigma_{2n-2},s_{2n-2},\alpha)$$

jest jego σ_0,σ_1-ogrodzeniem.

3. Niech (S,T) będzie systemem trójek Steinera, w którym $S=\{x,y,z,s_0,\ldots,s_{2n-3}\}$ oraz $\{x,y,z\}\in T$. Załóżmy, że system (S,T) jest x,y-ogrodzony, przy czym ciąg

$$(s_0,s_1,\ldots,s_{2n-4},s_{2n-3})$$

jest jego x,y-ogrodzeniem. Niech zbiór $X=\{\sigma_0,\ldots,\sigma_{2n-2}\}\cup\{\alpha\}$ będzie zbiorem rozłącznym ze zbiorem S. Niech następnie ciąg $(H_0,\ldots,H_{2n-2})$ będzie faktoryzacją Kirkmana zbioru H dwuelementowych podzbiorów zbioru X. Definiujemy nstępujące rodziny trójek:

$$\begin{aligned}T_1&=\big\{\{a,b,c\}\in T:\ \{a,b,c\}\cap\{x,y\}=\varnothing\big\},\\ U&=\big\{\{s_j,a,b\}:\ (j\in\{0,\ldots,2n-3\})\ \wedge\ (\{a,b\}\in H_{j+1})\ \wedge\ (\{a,b\}\cap\{\sigma_0,\sigma_1\}=\varnothing)\big\},\\ V&=\big\{\{z,a,b\}:\ (\{a,b\}\in H_0)\ \wedge\ (\{a,b\}\neq\{\sigma_0,\sigma_1\})\big\},\\ W&=\big\{\{s_j,s_{j+1},\sigma_{j+2}\}:\ 0\leq j<2n-3\big\}\cup\big\{\{\alpha,s_0,s_{2n-3}\}\big\}.\end{aligned}$$

Niech następnie $S^* = \{s_0, \ldots, s_{2n-3}\} \cup \{z\} \cup \{\sigma_2, \ldots, \sigma_{2n-2}\} \cup \{\alpha\}$ oraz $T^* = T_1 \cup U \cup V \cup W$. Wtedy $\{\sigma_2, \sigma_3, s_3\} \in T^*$ oraz para (S^*, T^*) jest σ_2, σ_3-ogrodzonym systemem trójek Steinera, przy czym ciąg

$$(s_0, s_1, s_2, \alpha, s_4, \sigma_4, s_5, \sigma_5, \ldots, s_{2n-3}, \sigma_{2n-3}, z, \sigma_{2n-2})$$

jest jego σ_2, σ_3-ogrodzeniem.

Szczegóły dowodów pozostawimy również jako ćwiczenie.