Kwadraty Rooma i turnieje brydżowe

Niech N będzie ustalonym zbiorem $(n+1)$-elementowym. Przypomnijmy, że symbolem $P_2(N)$ oznaczamy zbiór

$$P_2(N) = \{A \subseteq N : \ |A| = 2\}.$$

Kwadratem Rooma o boku n nazywamy dowolną macierz R wymiaru $n \times n$ o wyrazach ze zbioru $P_2(N) \cup \{\varnothing\}$:

$$R : \{0, \dots, n-1\}^2 \to P_2(N) \cup \{\varnothing\},$$

spełniającą następujące trzy warunki:

(R1) każda para $\{a, b\} \in P_2(N)$ występuje dokładnie jeden raz w macierzy R,
(R2) każdy element zbioru N występuje dokładnie jeden raz w każdym wierszu macierzy R,
(R3) każdy element zbioru N występuje dokładnie jeden raz w każdej kolumnie macierzy R,

Zauważmy, że wiersze i kolumny kwadratu Rooma numerujemy liczbami od 0 do $n-1$.

Kwadraty Rooma mogą być wykorzystane do opisu turniejów brydżowych. Niech $N = \{0, 1, \dots, n\}$. Liczby ze zbioru N są numerami par startujących w turnieju. Jeśli $i, j \in \{0, \dots, n-1\}$ oraz $R(i,j) = \{a, b\} \in P_2(N)$, to pary o numerach a i b grają ze sobą rozdanie o numerze j w i-tej rundzie turnieju. Jeśli natomiast $R(i,j) = \varnothing$, to rozdanie o numerze j nie jest wykorzystywane w i-tej rundzie. Warunek (R1) mówi, że każde dwie pary startujące w turnieju grają ze sobą dokładnie jeden raz. Warunek (R2) mówi, że każda para gra (dokładnie jeden raz) w każdej rundzie, zaś warunek (R3) mówi, że każda para gra każde rozdanie dokładnie jeden raz.

Oto przykładowy kwadrat Rooma o boku 7. Opisuje on przebieg turnieju brydżowego, w którym startuje 8 par o numerach od 0 do 7.

	0	1	2	3	4	5	6
0	$\{0,7\}$	$\varnothing$	$\varnothing$	$\{4,6\}$	$\varnothing$	$\{2,3\}$	$\{1,5\}$
1	$\{2,6\}$	$\{1,7\}$	$\varnothing$	$\varnothing$	$\{0,5\}$	$\varnothing$	$\{3,4\}$
2	$\{4,5\}$	$\{0,3\}$	$\{2,7\}$	$\varnothing$	$\varnothing$	$\{1,6\}$	$\varnothing$
3	$\varnothing$	$\{5,6\}$	$\{1,4\}$	$\{3,7\}$	$\varnothing$	$\varnothing$	$\{0,2\}$
4	$\{1,3\}$	$\varnothing$	$\{0,6\}$	$\{2,5\}$	$\{4,7\}$	$\varnothing$	$\varnothing$
5	$\varnothing$	$\{2,4\}$	$\varnothing$	$\{0,1\}$	$\{3,6\}$	$\{5,7\}$	$\varnothing$
6	$\varnothing$	$\varnothing$	$\{3,5\}$	$\varnothing$	$\{1,2\}$	$\{0,4\}$	$\{6,7\}$

Opis turnieju zawarty w tym kwadracie nie jest kompletny. Mianowicie należy jeszcze ustalić na jakiej linii (NS czy WE) gra każda z par w danej rundzie. Ponadto ze względów organizacyjnych należy podać numer stołu, na którym dane pary grają ze sobą oraz opisać ruch kart między stolikami. Te kwestie wyjaśnimy w dalszym ciągu.

Z warunków (R1) – (R3) wynika, że liczba n jest nieparzysta. Powstaje naturalne pytanie, czy dla każdej liczby nieparzystej n istnieje kwadrat Rooma o boku n. Okazuje się, że jest to prawdą dla $n > 5$. Twierdzenia tego nie będziemy tu dowodzić. Pokażemy natomiast konstrukcję kwadratów Rooma dla liczb n pierwszych takich, że $n \equiv 3 \pmod 4$.

Niech $n = 2m + 1$ i niech G będzie grupą przemienną rzędu n. W dalszym ciągu będziemy używać znaku $+$ jako symbolu działania w grupie G.

Starterem w grupie G nazywamy dowolny ciąg par uporządkowanych

$$\big((x_1, y_1), \dots, (x_m, y_m)\big)$$

elementów grupy G, spełniający następujące dwa warunki:

$$\begin{array}{ll} (1) & \{x_1, \ldots, x_m\} \cup \{y_1, \ldots, y_m\} = G \setminus \{0\}, \\ (2) & \{x_1 - y_1, \ldots, x_m - y_m\} \cup \{y_1 - x_1, \ldots, y_m - x_m\} = G \setminus \{0\}. \end{array}$$

Starter $\big((x_1, y_1), \ldots, (x_m, y_m)\big)$ nazywamy **silnym starterem**, jeśli spełnia następujące warunki:

$$\begin{array}{ll} (3) & \forall i \in \{1, \ldots, m\} \ \big(x_i + y_i \neq 0\big), \\ (4) & \forall i, j \in \{1, \ldots, m\} \ \big(i \neq j \ \Rightarrow \ x_i + y_i \neq x_j + y_j\big), \end{array}$$

tzn. wszystkie sumy $x_i + y_i$ (dla $i = 1, \ldots, m$) są różnymi niezerowymi elementami grupy G.

Sumatorem dla startera $\big((x_1, y_1), \ldots, (x_m, y_m)\big)$ nazywamy ciąg $(a_1, \ldots, a_m)$ elementów grupy G spełniający następujące warunki:

$$\begin{array}{ll} (5) & \forall i \in \{1, \ldots, m\} \ \big(a_i \neq 0\big), \\ (6) & \forall i, j \in \{1, \ldots, m\} \ \big(i \neq j \ \Rightarrow \ a_i \neq a_j\big), \\ (7) & \{x_1 + a_1, \ldots, x_m + a_m\} \cup \{y_1 + a_1, \ldots, y_m + a_m\} = G \setminus \{0\}. \end{array}$$

Inaczej mówiąc, sumatorem nazywamy taki ciąg $(a_0, \ldots, a_m)$ różnych, niezerowych elementów grupy G, że ciąg

$$\big((x_1 + a_1, y_1 + a_1), \ldots, (x_m + a_m, y_m + a_m)\big)$$

jest również starterem w grupie G.

Przykłady.

1. Ciąg $\big((1, 5), (4, 6), (2, 3)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$. Ciąg $(1, 4, 2)$ jest sumatorem dla tego startera. Innym sumatorem jest ciąg $(4, 2, 1)$.

2. Ciąg $\big((1, 2), (4, 8), (5, 10), (9, 7), (3, 6)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$. Ciąg $(8, 10, 7, 6, 2)$ jest sumatorem dla tego startera. Innym sumatorem jest ciąg $(4, 5, 9, 3, 1)$.

Twierdzenie. Jeśli ciąg $\big((x_1, y_1), \ldots, (x_m, y_m)\big)$ jest starterem w grupie G rzędu n (przy czym $n = 2m + 1$) oraz ciąg $(a_1, \ldots, a_m)$ jest sumatorem dla tego startera, to istnieje kwadrat Rooma o boku n.

Dowód. Niech $G = \{g_0, g_1, \ldots, g_{n-1}\}$, przy czym $g_0 = 0$. Niech następnie $\infty \notin G$ oraz $N = G \cup \{\infty\}$. Definiujemy kwadrat Rooma R w następujący sposób:

$$R(i, j) = \begin{cases} \{\infty, g_i\}, & \text{jeśli } i = j, \\ \{g_i + x_k, g_i + y_k\}, & \text{jeśli } g_i - g_j = a_k, \\ \varnothing, & \text{jeśli element } g_i - g_j \text{ nie jest wyrazem sumatora } (a_1, \ldots, a_m) \end{cases}$$

dla $i, j \in \{0, \ldots, n - 1\}$.

Musimy wykazać, że tak zdefiniowana macierz R spełnia warunki (R1) – (R3). Najpierw policzymy niepuste wyrazy macierzy R. Istnieje n wyrazów postaci $\{\infty, g_i\}$: leżą one na przekątnej. Następnie dla każdego k istnieje n par (g_i, g_j) (a więc i par (i, j)) takich, że $g_i - g_j = a_k$. Mianowicie są to pary

$$(g_0, g_0 - a_k), \ldots, (g_{n-1}, g_{n-1} - a_k)$$

(ponieważ $a_k \neq 0$, więc $g_i \neq g_i - a_k$, czyli $i \neq j$). Łącznie mamy więc $mn + n$ wyrazów niepustych. Ponieważ

$$\binom{n+1}{2} = \frac{n(n+1)}{2} = \frac{n(2m+2)}{2} = n(m+1) = nm + n,$$

więc liczba wyrazów niepustych jest równa liczbie par należących do zbioru $P_2(N)$. Dla dowodu warunku (R1) wystarczy zatem pokazać, że każda taka para jest wyrazem macierzy R.

Zauważyliśmy już, że wszystkie pary postaci $\{\infty, i\}$ są wyrazami macierzy R. Niech zatem $g, h \in G$ oraz $g \neq h$. Z warunku (2) wynika, że istnieje w naszym starterze para (x_k, y_k) taka, że

$$x_k - y_k = g - h \quad \text{lub} \quad y_k - x_k = g - h.$$

Jeśli $x_k - y_k = g - h$ oraz $g_i = g - x_k$ i $g_j = g - x_k - a_k$, to $g_i - g_j = a_k$ i z definicji macierzy R wynika, że

$$R(i,j) = \{g_i + x_k, g_i + y_k\} = \{g, g - x_k + y_k\} = \{g, g - (x_k - y_k)\} = \{g, g - (g - h)\} = \{g, h\}.$$

Jeśli natomiast $g - h = y_k - x_k$, to $h - g = x_k - y_k$ i w podobny sposób pokazujemy, że para $\{h, g\}$ jest wyrazem macierzy R.

Sprawdzamy teraz warunek (R2). Niech $i \in \{0, \ldots, n-1\}$. Mamy pokazać, że każdy element zbioru N występuje dokładnie jeden raz w wierszu i. Nietrudno zauważyć, że w każdym wierszu macierzy R występuje dokładnie $m + 1$ wyrazów niepustych; stąd wynika, że wystarczy pokazać, iż każdy element zbioru N występuje co najmniej jeden raz w wierszu i. Oczywiście $\infty \in \{\infty, i\} = R(i,i)$, więc element ∞ występuje w tym wierszu. Podobnie $g_i \in R(i,i)$. Niech więc teraz $l \neq i$. Pokażemy, że element g_l też występuje w wierszu i.

Ponieważ $g_l - g_i \neq 0$, więc istnieje liczba $k \in \{1, \ldots, m\}$ taka, że

$$g_l - g_i = x_k \quad \text{lub} \quad g_l - g_i = y_k,$$

czyli

$$g_l = g_i + x_k \quad \text{lub} \quad g_l = g_i + y_k.$$

Niech j będzie liczbą taką, że $g_j = g_i - a_k$. Wtedy $g_i - g_j = a_k$ oraz

$$R(i,j) = \{g_i + x_k, g_i + y_k\}.$$

Zatem $g_l \in R(i,j)$.

Wreszcie sprawdzamy warunek (R3). Niech $j \in \{0, \ldots, n-1\}$. Znów wystarczy pokazać, że każdy element zbioru N występuje co najmniej jeden raz w kolumnie j. Ponieważ $R(j,j) = \{\infty, g_j\}$, więc elementy ∞ i g_j występują w tej kolumnie. Niech więc $l \neq j$. Pokażemy, że element g_l też występuje w kolumnie j.

Oczywiście $g_l - g_j \in G \setminus \{0\}$, więc z definicji sumatora wynika, że istnieje liczba k taka, że

$$g_l - g_j = x_k + a_k \quad \text{lub} \quad g_l - g_i = y_k + a_k.$$

Niech i będzie taką liczbą, że $g_i = g_j + a_k$. Wtedy $g_i - g_j = a_k$ oraz

$$R(i,j) = \{g_i + x_k, g_i + y_k\}.$$

Jeśli $g_l - g_j = x_k + a_k$, to

$$g_l = g_j + x_k + a_k = g_i + x_k \in R(i,j).$$

Jeśli zaś $g_l - g_j = y_k + a_k$, to

$$g_l = g_j + y_k + a_k = g_i + y_k \in R(i,j).$$

W obu przypadkach element g_l występuje w kolumnie j. To kończy dowód twierdzenia.

Przypomnijmy teraz pojęcie reszty i niereszty kwadratowej. Jeśli p jest dowolną nieparzystą liczbą pierwszą, to liczbę całkowitą a nazywamy **resztą kwadratową** modulo p, wtedy i tylko wtedy, gdy $p \nmid a$ oraz istnieje liczba całkowita x taka, że
$$x^2 \equiv a \pmod p.$$

Jeśli natomiast $p \nmid a$ oraz nie istnieje liczba całkowita x taka, że $x^2 \equiv a \pmod p$, to liczbę a nazywamy **nieresztą kwadratową** modulo p. Resztami kwadratowymi są więc te elementy niezerowe ciała $\mathbb{Z}_p$, które są kwadratami w tym ciele. Zbiór elementów niezerowych ciała $\mathbb{Z}_p$ oznaczamy symbolem $\mathbb{Z}_p^*$. Definiujemy następnie tzw. **symbol Legendre'a** wzorem

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{jeśli } a \text{ jest resztą kwadratową modulo } p, \\ -1, & \text{jeśli } a \text{ jest nieresztą kwadratową modulo } p, \\ 0, & \text{jeśli } p \mid a. \end{cases}$$

W dalszym ciągu będziemy korzystać z następujących własności reszt i niereszt kwadratowych:

1. w zbiorze $\mathbb{Z}_p^*$ istnieje $\frac{p-1}{2}$ reszt kwadratowych i $\frac{p-1}{2}$ niereszt kwadratowych,
2. jeśli g jest generatorem grupy multyplikatywnej $\mathbb{Z}_p^*$, to g^i jest resztą kwadratową wtedy i tylko wtedy, gdy wykładnik i jest liczbą parzystą,
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$,
4. iloczyn reszt kwadratowych jest resztą kwadratową,
5. iloczyn niereszt kwadratowych jest resztą kwadratową,
6. iloczyn reszty kwadratowej i niereszty kwadratowej jest nieresztą kwadratową,
7. jeśli $ab = 1$ w ciele $\mathbb{Z}_p$ to $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, czyli a jest resztą kwadratową wtedy i tylko wtedy, gdy b jest resztą kwadratową,
8. $\left(\frac{a^2}{p}\right) = 1$,
9. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, czyli liczba -1 jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $p \equiv 1 \pmod 4$,
10. jeśli $p \equiv 3 \pmod 4$, to $a \in \mathbb{Z}_p^*$ jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $-a$ jest nieresztą kwadratową modulo p.

Pokażemy teraz konstrukcję starterów i sumatorów w pewnych grupach przemiennych.

Załóżmy, że p jest liczbą pierwszą oraz $p > 3$ i $p = 4q + 3$. Wynika stąd, że liczba -1 jest nieresztą kwadratową modulo p. Niech g będzie generatorem grupy multyplikatywnej ciała $\mathbb{Z}_p$. Definiujemy następnie

$$x_i = g^{2i},$$
$$y_i = g^{2i+1}$$

dla $i = 0, \ldots, 2q$. Udowodnimy, że ciąg $\big((x_0, y_0), \ldots, (x_{2q}, y_{2q})\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_p$.

Warunek (1) wynika stąd, że

$$\{x_0, \ldots, x_{2q}\} \cup \{y_0, \ldots, y_{2q}\} = \{g^0, \ldots, g^{4q+1}\} = \{g^0, \ldots, g^{p-2}\} = \{1, \ldots, p-1\} = \mathbb{Z}_p \setminus \{0\}.$$

Dla dowodu warunku (2) zauważmy najpierw, że

$$x_i - y_i = g^{2i} - g^{2i+1} = g^{2i}(1 - g)$$

oraz
$$y_i - x_i = g^{2i}(g - 1).$$

Elementy ciała $\mathbb{Z}_p$ postaci g^{2i} dla $i = 0, \ldots, 2q$ są wszystkimi resztami kwadratowymi modulo p w tym ciele. Jeśli $g-1$ jest resztą kwadratową, to elementy $x_y - y_i$ dla $i = 0, \ldots, 2q$ są wszystkimi resztami kwadratowymi w ciele $\mathbb{Z}_p$ i elementy $y_i - x_i$ są wszystkimi nieresztami kwadratowymi w ciele $\mathbb{Z}_p$. Stąd wynika, że łącznie te różnice wyczerpują cały zbiór $\mathbb{Z}_p^*$. Jeśli zaś $g-1$ jest nieresztą kwadratową modulo p, to elementy $x_i - y_i$ są wszystkimi nieresztami kwadratowymi i elementy $y_i - x_i$ są wszystkimi resztami kwadratowymi w ciele $\mathbb{Z}_p$, a więc te różnice też wyczerpują zbiór $\mathbb{Z}_p^*$.

Warunki (3) i (4) wynikają stąd, że

$$x_i + y_i = g^{2i}(g+1).$$

Mianowicie $g+1 \neq 0$, więc $x_i + y_i \neq 0$ dla $i = 0, \ldots, 2q$. Ponadto, jeśli $x_i + y_i = x_j + y_j$, to $g^{2i} = g^{2j}$, skąd wynika, że $i = j$.

Przykłady.

1. Liczba 5 jest generatorem grupy multyplikatywnej ciała $\mathbb{Z}_7$. Ponadto

$$\begin{aligned}
5^0 &= 1,\\
5^1 &= 5,\\
5^2 &= 4,\\
5^3 &= 6,\\
5^4 &= 2,\\
5^5 &= 3.
\end{aligned}$$

   Zatem ciąg $\big((1,5),(4,6),(2,3)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$.

2. Liczba 2 jest generatorem grupy multyplikatywnej ciała $\mathbb{Z}_{11}$. Ponadto

$$\begin{aligned}
2^0 &= 1,\\
2^1 &= 2,\\
2^2 &= 4,\\
2^3 &= 6,\\
2^4 &= 5,\\
2^5 &= 10,\\
2^6 &= 9,\\
2^7 &= 7,\\
2^8 &= 3,\\
2^9 &= 6.
\end{aligned}$$

   Zatem ciąg $\big((1,2),(4,8),(5,10),(9,7),(3,6)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$.

Przypuśćmy teraz, że dany jest dowolny silny starter $\big((x_0,y_0),\ldots,(x_{2q},y_{2q})\big)$ w grupie addytywnej ciała $\mathbb{Z}_p$. Niech ciąg $(a_0,\ldots,a_{2q})$ będzie zdefiniowany wzorem $a_k = -x_k - y_k$ dla $k = 0, \ldots, 2q$. Pokażemy, że ciąg $(a_0,\ldots,a_{2q})$ jest sumatorem dla tego silnego startera.

Z definicji silnego startera wynika, że wyrazy tego ciągu są różne i niezerowe. Mamy ponadto

$$x_k + a_k = -y_k \quad \text{oraz} \quad y_k + a_k = -x_k,$$

skąd wynika, że

$$\{x_0 + a_0, \ldots, x_{2q} + a_{2q}\} \cup \{y_0 + a_0, \ldots, y_{2q} + a_{2q}\} = \{-x_0, \ldots, -x_{2q}\} \cup \{-y_0, \ldots, -y_{2q}\} = \mathbb{Z}_p \setminus \{0\},$$

co kończy dowód.

Przykłady.

1. Ciąg $\big((1,5),(4,6),(2,3)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$. Ponieważ

$$\begin{gathered} -1-5=-6\equiv 1 \pmod 7, \\ -4-6=-10\equiv 4 \pmod 7, \\ -2-3=-5\equiv 2 \pmod 7, \end{gathered}$$

   więc ciąg $(1,4,2)$ jest sumatorem dla tego startera.

2. Ciąg $\big((1,2),(4,8),(5,10),(9,7),(3,6)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$. Ponieważ

$$\begin{gathered} -1-2=-3\equiv 8 \pmod{11}, \\ -4-8=-12\equiv 10 \pmod{11}, \\ -5-10=-15\equiv 7 \pmod{11}, \\ -9-7=-16\equiv 6 \pmod{11}, \\ -3-6=-9\equiv 2 \pmod{11}, \end{gathered}$$

   więc ciąg $(8,10,7,6,2)$ jest sumatorem dla tego startera.

W przypadku silnego startera zdefiniowanego wyżej w grupie addytywnej ciała $\mathbb{Z}_p$ (gdzie $p>3$ oraz $p\equiv 3 \pmod 4$) możemy wskazać jeszcze jeden przykład sumatora. Niech g będzie generatorem grupy $\mathbb{Z}_p^*$. Wtedy g^{-1} też jest generatorem tej grupy. Zauważmy także, że $g\neq -1$ oraz $g^2\neq -1$.

Ćwiczenie. Jeśli $(g+1)(g^2+1)$ jest nieresztą kwadratową modulo p, to $(g^{-1}+1)(g^{-2}+1)$ jest resztą kwadratową. W szczególności istnieje generator g grupy $\mathbb{Z}_p^*$ o tej własności, że $(g+1)(g^2+1)$ jest resztą kwadratową modulo p.

Weźmy zatem taki generator g grupy $\mathbb{Z}_p^*$, że $(g+1)(g^2+1)$ jest resztą kwadratową modulo p i zdefiniujmy ciąg $(a_0,\ldots,a_{2q})$ wzorem $a_k=g^{2k+2}$ dla $k=0,\ldots,2q$. Pokażemy, że ten ciąg jest sumatorem dla startera

$$\big((g^0,g^1),\ldots,(g^{2q},g^{2q+1})\big).$$

Oczywiście wszystkie wyrazy a_k są niezerowe i różne. Niech teraz $i\neq j$. Pokażemy, że

$$x_i+a_i\neq x_j+a_j.$$

Gdyby bowiem

$$x_i+a_i=x_j+a_j,$$

to mielibyśmy kolejno

$$\begin{gathered} g^{2i}+g^{2i+2}=g^{2j}+g^{2j+2}, \\ g^{2i}(g^2+1)=g^{2j}(g^2+1), \\ g^{2i}=g^{2j}, \\ 2i=2j, \\ i=j, \end{gathered}$$

co daje sprzeczność. W podobny sposób pokazujemy, że jeśli $i\neq j$, to $y_i+a_i\neq y_j+a_j$. Pokażemy, że także $x_i+a_i\neq y_j+a_j$. Przypuśćmy bowiem, że

$$x_i+a_i=y_j+a_j.$$

Mamy wówczas

$$\begin{gathered}
g^{2i} + g^{2i+2} = g^{2j+1} + g^{2j+2}, \\
g^{2i}(g^2+1) = g^{2j+1}(g+1), \\
g^{2i}(g+1)(g^2+1) = g^{2j+1}(g+1)^2.
\end{gathered}$$

Po lewej stronie równości mamy iloczyn dwóch reszt kwadratowych: g^{2i} oraz $(g+1)(g^2+1)$. Po prawej stronie mamy natomiast iloczyn niereszty kwadratowej g^{2j+1} przez resztę kwadratową $(g+1)^2$. Zatem po lewej stronie mamy resztę kwadratową, a po prawej stronie nieresztę, co jest niemożliwe. Udowodniliśmy więc, że zdefiniowany wyżej ciąg $(a_0, \ldots, a_{2q})$ jest sumatorem.

Przykłady.

1. Liczba 5 jest generatorem grupy $\mathbb{Z}_7^*$. Mamy przy tym

$$(5+1)(5^2+1) = 6 \cdot 26 \equiv 6 \cdot 5 = 30 \equiv 2 \equiv 3^2 \pmod 7,$$

więc $(5+1)(5^2+1)$ jest resztą kwadratową modulo 7. Widzieliśmy, że z tego generatora otrzymaliśmy ciąg $\big((1,5),(4,6),(2,3)\big)$, będący silnym starterem w grupie addytywnej ciała $\mathbb{Z}_7$. Ponieważ

$$\begin{aligned}
5^2 &= 4, \\
5^4 &= 2, \\
5^6 &= 1
\end{aligned}$$

w ciele $\mathbb{Z}_7$, więc ciąg $(4,2,1)$ jest sumatorem dla tego startera. Z tego startera i sumatora otrzymujemy następujący kwadrat Rooma:

	0	1	2	3	4	5	6
0	$\{\infty,0\}$	$\varnothing$	$\varnothing$	$\{1,5\}$	$\varnothing$	$\{4,6\}$	$\{2,3\}$
1	$\{3,4\}$	$\{\infty,1\}$	$\varnothing$	$\varnothing$	$\{2,6\}$	$\varnothing$	$\{0,5\}$
2	$\{1,6\}$	$\{4,5\}$	$\{\infty,2\}$	$\varnothing$	$\varnothing$	$\{0,3\}$	$\varnothing$
3	$\varnothing$	$\{0,2\}$	$\{5,6\}$	$\{\infty,3\}$	$\varnothing$	$\varnothing$	$\{1,4\}$
4	$\{2,5\}$	$\varnothing$	$\{1,3\}$	$\{0,6\}$	$\{\infty,4\}$	$\varnothing$	$\varnothing$
5	$\varnothing$	$\{3,6\}$	$\varnothing$	$\{2,4\}$	$\{0,1\}$	$\{\infty,5\}$	$\varnothing$
6	$\varnothing$	$\varnothing$	$\{0,4\}$	$\varnothing$	$\{3,5\}$	$\{1,2\}$	$\{\infty,6\}$

2. Liczba 2 jest generatorem grupy $\mathbb{Z}_{11}^*$. Mamy przy tym

$$(2+1)(2^2+1) = 3 \cdot 5 = 15 \equiv 4 = 2^2 \pmod{11},$$

więc $(2+1)(2^2+1)$ jest resztą kwadratową modulo 11. Widzieliśmy, że z tego generatora otrzymaliśmy ciąg $\big((1,2),(4,8),(5,10),(9,7),(3,6)\big)$ jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_{11}$. Ponieważ

$$\begin{aligned}
2^2 &= 4, \\
2^4 &= 5, \\
2^6 &= 9, \\
2^8 &= 3, \\
2^{10} &= 1
\end{aligned}$$

w ciele $\mathbb{Z}_{11}$, więc ciąg $(10, 7, 6, 2, 1)$ jest sumatorem dla tego startera. Z tego startera i sumatora otrzymujemy następujący kwadrat Rooma:

	0	1	2	3	4	5	6	7	8	9	10
0	$\{\infty,0\}$	$\varnothing$	$\{5,10\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{4,8\}$	$\{1,2\}$	$\{7,9\}$	$\varnothing$	$\{3,6\}$
1	$\{4,7\}$	$\{\infty,1\}$	$\varnothing$	$\{0,6\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{5,9\}$	$\{2,3\}$	$\{8,10\}$	$\varnothing$
2	$\varnothing$	$\{5,8\}$	$\{\infty,2\}$	$\varnothing$	$\{1,7\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{6,10\}$	$\{3,4\}$	$\{0,9\}$
3	$\{1,10\}$	$\varnothing$	$\{6,9\}$	$\{\infty,3\}$	$\varnothing$	$\{2,8\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{0,7\}$	$\{4,5\}$
4	$\{5,6\}$	$\{0,2\}$	$\varnothing$	$\{7,10\}$	$\{\infty,4\}$	$\varnothing$	$\{3,9\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{1,8\}$
5	$\{2,9\}$	$\{6,7\}$	$\{1,3\}$	$\varnothing$	$\{0,8\}$	$\{\infty,5\}$	$\varnothing$	$\{4,10\}$	$\varnothing$	$\varnothing$	$\varnothing$
6	$\varnothing$	$\{3,10\}$	$\{7,8\}$	$\{2,4\}$	$\varnothing$	$\{1,9\}$	$\{\infty,6\}$	$\varnothing$	$\{0,5\}$	$\varnothing$	$\varnothing$
7	$\varnothing$	$\varnothing$	$\{0,4\}$	$\{8,9\}$	$\{3,5\}$	$\varnothing$	$\{2,10\}$	$\{\infty,7\}$	$\varnothing$	$\{1,6\}$	$\varnothing$
8	$\varnothing$	$\varnothing$	$\varnothing$	$\{1,5\}$	$\{9,10\}$	$\{4,6\}$	$\varnothing$	$\{0,3\}$	$\{\infty,8\}$	$\varnothing$	$\{2,7\}$
9	$\{3,8\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{2,6\}$	$\{0,10\}$	$\{5,7\}$	$\varnothing$	$\{1,4\}$	$\{\infty,9\}$	$\varnothing$
10	$\varnothing$	$\{4,9\}$	$\varnothing$	$\varnothing$	$\varnothing$	$\{3,7\}$	$\{0,1\}$	$\{6,8\}$	$\varnothing$	$\{2,5\}$	$\{\infty,10\}$

Zajmiemy się teraz problemem przydziału parom linii (NS lub WE), na których mają grać w kolejnych rundach. Niech p będzie liczbą pierwszą taką, że $p > 3$ oraz $p = 4q+3$. Niech g będzie generatorem grupy multyplikatywnej ciała $\mathbb{Z}_p$. Wiemy już, że ciąg

$$\big((x_0, y_0), \ldots, (x_{2q}, y_{2q})\big),$$

gdzie

$$x_i = g^{2i}, \quad y_i = g^{2i+1}$$

dla $i = 0, \ldots, 2q$, jest silnym starterem w grupie addytywnej ciała $\mathbb{Z}_p$. Niech następnie ciąg $(a_0, \ldots, a_{2q})$ będzie sumatorem dla tego startera. Definiujemy **uporządkowany kwadrat Rooma**

$$R : \{0, \ldots, p-1\}^2 \to (\mathbb{Z}_p \cup \{p\})^2 \cup \{\varnothing\}$$

wzorem

$$R(i,j) = \begin{cases} (p, i), & \text{jeśli } i = j, \\ (i + x_k, i + y_k), & \text{jeśli } i - j = a_k, \\ \varnothing, & \text{jeśli } i - j \text{ nie jest wyrazem sumatora } (a_0, \ldots, a_{2q}) \end{cases}$$

dla $i, j = 0, \ldots, p-1$.

Liczby ze zbioru $\mathbb{Z}_p \cup \{p\} = \{0, \ldots, p\}$ są numerami par startujących w turnieju. Rozdania i rundy turnieju są numerowane liczbami od 0 dp $p-1$. Jeśli $R(i,j) = (a,b)$, to pary o numerach a i b grają ze sobą rozdanie o numerze j w i-tej rundzie, przy czym para o numerze a gra na linii NS, a para o numerze b gra na linii WE. Jeśli natomiast $R(i,j) = \varnothing$, to rozdanie o numerze j nie jest wykorzystywane w i-tej rundzie.

Dokładnie tak samo jak poprzednio możemy pokazać, że uporządkowany kwadrat Rooma R ma następujące własności:

(R1) dla dowolnych $a, b \in \mathbb{Z}_p \cup \{p\}$ takich, że $a \neq b$ dokładnie jedna z par (a,b) i (b,a) jest wyrazem macierzy R, przy tym występuje w macierzy R w dokładnie jednym miejscu,

(R2) każdy element zbioru N występuje dokładnie jeden raz w każdym wierszu macierzy R, (R3) każdy element zbioru N występuje dokładnie jeden raz w każdej kolumnie macierzy R,

Jeżeli pary o numerach a i b grają rozdanie o numerze j na tej samej linii, to mówimy, że są porównywane w tym rozdaniu. Udowodnimy, że w zdefiniowanym wyżej uporządkowanym kwadracie Rooma każde dwie pary są porównywane w tej samej liczbie rozdań. Turniej o tej własności nazywamy zazwyczaj turniejem zbalansowanym.

Definiujemy zatem następującą funkcję

$$S : \mathbb{Z}_p^2 \to \{-1, +1\}$$

wskazującą, na jakiej linii para o umerze i gra rozdanie o numerze j:

$$S(i,j) = \begin{cases} +1, & \text{jeśli para o numerze } i \text{ gra rozdanie o numerze } j \text{ na linii NS,} \\ -1, & \text{jeśli para o numerze } i \text{ gra rozdanie o numerze } j \text{ na linii WE} \end{cases}$$

dla $i, j \in \mathbb{Z}_p$. Z powyższej definicji macierzy R wynika, że

$$S(i,j) = \begin{cases} +1, & \text{jeśli } i = p, \\ -1, & \text{jeśli } i \neq p \text{ oraz } i = j, \\ +1, & \text{jeśli } i \neq p,\ i \neq j \text{ oraz } i - j = x_k + a_k \text{ dla pewnego } k, \\ -1, & \text{jeśli } i \neq p,\ i \neq j \text{ oraz } i - j = y_k + a_k \text{ dla pewnego } k. \end{cases}$$

Mieliśmy do czynienia z dwoma sumatorami. Przyjrzyjmy się teraz, jak wygląda funkcja S dla tych sumatorów. Niech najpierw sumator $(a_0, \ldots, a_{2q})$ będzie zdefiniowany wzorem

$$a_i = -x_i - y_i$$

dla $i = 0, \ldots, 2q$. Wówczas, jeśli $i - j = x_k + a_k$, to $i - j = -y_k$. Ponieważ $y_k - g^{2k+1}$, więc y_k jest nieresztą kwadratową modulo p, a więc $-y_k$ jest resztą kwadratową. Jeśli natomiast $i - j = y_k + a_k$, to $i - j = -x_k$ oraz $-x_k$ jest nieresztą kwadratową modulo p. Zatem definicję funkcji S możemy zapisać w postaci

$$S(i,j) = \begin{cases} +1, & \text{jeśli } i = p, \\ -1, & \text{jeśli } i \neq p \text{ oraz } i = j, \\ \left(\frac{i-j}{p}\right), & \text{jeśli } i \neq p \text{ oraz } i \neq j \end{cases}$$

dla $i, j \in \mathbb{Z}_p$.

Drugi sumator $(a_0, \ldots, a_{2q})$ był zdefiniowany wzorem

$$a_i - g^{2i+2}$$

dla $i = 0, \ldots, 2q$. W tym przypadku wybieraliśmy generator g w taki sposób, by liczba $(g+1)(g^2+1)$ była resztą kwadratową modulo p. Teraz, jeśli $i - j = x_k + a_k$, to mamy

$$i - j = x_k + a_k = g^{2k} + g^{2k+2} = g^{2k}(g^2 + 1),$$

czyli

$$(i - j)(g + 1) = g^{2k}(g + 1)(g^2 + 1).$$

Zatem $(i - j)(g + 1)$ jest resztą kwadratową modulo p. Jeśli natomiast $i - j = y_k + a_k$, to

$$i - j - y_k + a_k = g^{2k+1} + g^{2k+2} = g^{2k+1}(g + 1),$$

czyli

$$(i - j)(g + 1) = g^{2k+1}(g + 1)^2.$$

Zatem $(i-j)(g+1)$ jest niereształ kwadratową modulo p. Stąd wynika, że

$$S(i,j)=\begin{cases}+1, & \text{jeśli } i=p,\\ -1, & \text{jeśli } i\neq p \text{ oraz } i=j,\\ \left(\frac{i-j}{p}\right)\cdot\left(\frac{g+1}{p}\right), & \text{jeśli } i\neq p \text{ oraz } i\neq j\end{cases}$$

dla $i,j\in\mathbb{Z}_p$.

Udowodnimy teraz następujące twierdzenie.

Twierdzenie. Dla dowolnych $u,w\in\mathbb{Z}_p$ takich, że $u\neq w$ zachodzi równość

$$\sum_{j=0}^{p-1} S(u,j)\cdot S(w,j)=-1.$$

Najpierw udowodnimy dwa lematy.

Lemat 1. W ciele $\mathbb{Z}_p$ zachodzi równość

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)=0.$$

Dowód. Równość ta wynika stąd, że w zbiorze $\{1,2,\ldots,p-1\}$ jest tyle samo reszt kwadratowych modulo p co niereszt kwadratowych modulo p.

Lemat 2. Jeśli $a\in\mathbb{Z}_p$ oraz $a\neq 0$, to

$$\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\cdot\left(\frac{j+a}{p}\right)=-1.$$

Dowód. Zauważmy najpierw, że

$$\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)\cdot\left(\frac{j+a}{p}\right)=\sum_{j=1}^{p-1}\left(\frac{j(j+a)}{p}\right)=\sum_{j=1}^{p-1}\left(\frac{j^2(1+aj^{-1})}{p}\right)=\sum_{j=1}^{p-1}\left(\frac{1+aj^{-1}}{p}\right).$$

Zauważmy następnie, że jeśli j przebiega liczby od 1 do $p-1$, to $1+aj^{-1}$ przebiega (w ciele $\mathbb{Z}_p$) wszystkie liczby różne od 1. Zatem

$$\sum_{j=1}^{p-1}\left(\frac{1+aj^{-1}}{p}\right)=\sum_{j=0}^{p-1}\left(\frac{j}{p}\right)-\left(\frac{1}{p}\right)=-1,$$

co kończy dowód lematu.

Dowód twierdzenia. Musimy udowodnić twierdzenie dla obu rozważanych sumatorów. Niech najpierw $a_k=-x_k-y_k$. Wówczas mamy dwa przypadki:

Przypadek 1. Jedna z liczb u i w jest równa p, np. $u=p$. Wtedy

$$\sum_{j=0}^{p-1}S(u,j)\cdot S(w,j)=\sum_{j=0}^{p-1}S(w,j)=\sum_{j\neq w}S(w,j)+S(w,w)=\sum_{j\neq w}\left(\frac{j-w}{p}\right)-1=\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)-1=-1.$$

Przypadek 2. $u \neq p$ oraz $w \neq p$. Wtedy

$$\begin{aligned}
\sum_{j=0}^{p-1} S(u,j)\cdot S(w,j) &= \sum_{j\neq u,w} S(u,j)\cdot S(w,j) + S(u,u)\cdot S(w,u) + S(u,w)\cdot S(w,w) = \\
&= \sum_{j\neq u,w} S(u,j)\cdot S(w,j) + (-1)\cdot\left(\frac{w-u}{p}\right) + (-1)\cdot\left(\frac{u-w}{p}\right) = \\
&= \sum_{j\neq u,w} S(u,j)\cdot S(w,j) + (-1)\cdot\left(\left(\frac{w-u}{p}\right) + \left(\frac{u-w}{p}\right)\right) = \\
&= \sum_{j\neq u,w} \left(\frac{u-j}{p}\right)\cdot\left(\frac{w-j}{p}\right) = \\
&= \sum_{j=0}^{p-1} \left(\frac{u-j}{p}\right)\cdot\left(\frac{w-j}{p}\right) = \\
&= \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)\cdot\left(\frac{j+w-u}{p}\right) = \\
&= -1.
\end{aligned}$$

(Ostatnia równość wynika z lematu 2.)

Niech teraz $a_k = g^{2k+2}$. Rozpatrujemy takie same dwa przypadki.

Przypadek 1. Jedna z liczb u i w jest równa p, np. $u = p$. Wtedy

$$\begin{aligned}
\sum_{j=0}^{p-1} S(u,j)\cdot S(w,j) &= \sum_{j=0}^{p-1} S(w,j) = \sum_{j\neq w} S(w,j) + S(w,w) = \\
&= \sum_{j\neq w} \left(\frac{j-w}{p}\right)\cdot\left(\frac{g+1}{p}\right) - 1 = \left(\frac{g+1}{p}\right)\cdot\sum_{j=1}^{p-1}\left(\frac{j}{p}\right) - 1 = \\
&= -1.
\end{aligned}$$

Przypadek 2. $u \neq p$ oraz $w \neq p$. Wtedy

$$\begin{aligned}
\sum_{j=0}^{p-1} S(u,j)\cdot S(w,j) &= \sum_{j\neq u,w} S(u,j)\cdot S(w,j) + S(u,u)\cdot S(w,u) + S(u,w)\cdot S(w,w) = \\
&= \sum_{j\neq u,w} S(u,j)\cdot S(w,j) + (-1)\cdot\left(\frac{w-u}{p}\right)\cdot\left(\frac{g+1}{p}\right) + (-1)\cdot\left(\frac{u-w}{p}\right)\cdot\left(\frac{g+1}{p}\right) = \\
&= \sum_{j\neq u,w} S(u,j)\cdot S(w,j) + (-1)\cdot\left(\frac{g+1}{p}\right)\left(\left(\frac{w-u}{p}\right) + \left(\frac{u-w}{p}\right)\right) = \\
&= \sum_{j\neq u,w} \left(\frac{u-j}{p}\right)\cdot\left(\frac{w-j}{p}\right)\cdot\left(\frac{g+1}{p}\right)^2 = \\
&= \sum_{j=0}^{p-1} \left(\frac{u-j}{p}\right)\cdot\left(\frac{w-j}{p}\right) = \\
&= \sum_{j=0}^{p-1} \left(\frac{j}{p}\right)\cdot\left(\frac{j+w-u}{p}\right) = \\
&= -1.
\end{aligned}$$

Dowód twierdzenia jest więc zakończony.

Udowodnione twierdzenie mówi, że każde dwie pary grają $2q+1$ rozdań na tej samej linii i $2q+2$ rozdania na przeciwnych liniach, a więc są porównywane w tej samej liczbie rozdań.

Przykłady.

1. Ze startera $\big((1,5),(4,6),(2,3)\big)$ i sumatora $(4,2,1)$ w grupie addytywnej ciała $\mathbb{Z}_7$ otrzymujemy następujący uporządkowany kwadrat Rooma:

	0	1	2	3	4	5	6
0	$(7,0)$	$\varnothing$	$\varnothing$	$(1,5)$	$\varnothing$	$(4,6)$	$(2,3)$
1	$(3,4)$	$(7,1)$	$\varnothing$	$\varnothing$	$(2,6)$	$\varnothing$	$(5,0)$
2	$(6,1)$	$(4,5)$	$(7,2)$	$\varnothing$	$\varnothing$	$(3,0)$	$\varnothing$
3	$\varnothing$	$(0,2)$	$(5,6)$	$(7,3)$	$\varnothing$	$\varnothing$	$(4,1)$
4	$(5,2)$	$\varnothing$	$(1,3)$	$(6,0)$	$(7,4)$	$\varnothing$	$\varnothing$
5	$\varnothing$	$(6,3)$	$\varnothing$	$(2,4)$	$(0,1)$	$(7,5)$	$\varnothing$
6	$\varnothing$	$\varnothing$	$(0,4)$	$\varnothing$	$(3,5)$	$(1,2)$	$(7,6)$

2. Ze startera $\big((1,2),(4,8),(5,10),(9,7),(3,6)\big)$ i sumatora $(10,7,6,2,1)$ w grypie addytywnej ciała $\mathbb{Z}_{11}$ otrzymujemy następujący uporządkowany kwadrat Rooma:

	0	1	2	3	4	5	6	7	8	9	10
0	$(11,0)$	$\varnothing$	$(5,10)$	$\varnothing$	$\varnothing$	$\varnothing$	$(4,8)$	$(1,2)$	$(9,7)$	$\varnothing$	$(3,6)$
1	$(4,7)$	$(11,1)$	$\varnothing$	$(6,0)$	$\varnothing$	$\varnothing$	$\varnothing$	$(5,9)$	$(2,3)$	$(10,8)$	$\varnothing$
2	$\varnothing$	$(5,8)$	$(11,2)$	$\varnothing$	$(7,1)$	$\varnothing$	$\varnothing$	$\varnothing$	$(6,10)$	$(3,4)$	$(0,9)$
3	$(1,10)$	$\varnothing$	$(6,9)$	$(11,3)$	$\varnothing$	$(8,2)$	$\varnothing$	$\varnothing$	$\varnothing$	$(7,0)$	$(4,5)$
4	$(5,6)$	$(2,0)$	$\varnothing$	$(7,10)$	$(11,4)$	$\varnothing$	$(9,3)$	$\varnothing$	$\varnothing$	$\varnothing$	$(8,1)$
5	$(9,2)$	$(6,7)$	$(3,1)$	$\varnothing$	$(8,0)$	$(11,5)$	$\varnothing$	$(10,4)$	$\varnothing$	$\varnothing$	$\varnothing$
6	$\varnothing$	$(10,3)$	$(7,8)$	$(4,2)$	$\varnothing$	$(9,1)$	$(11,6)$	$\varnothing$	$(0,5)$	$\varnothing$	$\varnothing$
7	$\varnothing$	$\varnothing$	$(0,4)$	$(8,9)$	$(5,3)$	$\varnothing$	$(10,2)$	$(11,7)$	$\varnothing$	$(1,6)$	$\varnothing$
8	$\varnothing$	$\varnothing$	$\varnothing$	$(1,5)$	$(9,10)$	$(6,4)$	$\varnothing$	$(0,3)$	$(11,8)$	$\varnothing$	$(2,7)$
9	$(3,8)$	$\varnothing$	$\varnothing$	$\varnothing$	$(2,6)$	$(10,0)$	$(7,5)$	$\varnothing$	$(1,4)$	$(11,9)$	$\varnothing$
10	$\varnothing$	$(4,9)$	$\varnothing$	$\varnothing$	$\varnothing$	$(3,7)$	$(0,1)$	$(8,6)$	$\varnothing$	$(2,5)$	$(11,10)$

Ostatnim problemem organizacyjnym jest numeracja stołów i opis sposobu poruszania się par i rozdań w kolejnych rundach. Stoliki, przy których toczy się gra numerujemy kolejnymi liczbami, pozostawiając między tymi stolikami miejsce na rozdania niewykorzystane w danej rundzie; te miejsca nazywamy zbiornicami. Para o najwyższym numerze gra przez cały czas na stoliku numer 1 na linii NS. Wszystkie pozostałe pary poruszają się według tego samego schematu; jego opis nazywamy kartą pilotującą. A oto otrzymane karty pilotujące turniejów dla 8 i 12 par:

$$
\begin{tikzcd}
\mathrm{1WE} \arrow[r] & \mathrm{3WE} \arrow[r] & \mathrm{2WE} \arrow[r] & \mathrm{3NS} \arrow[dd] \\
 & 1 \leftarrow \mathrm{Z} \leftarrow \mathrm{Z} \leftarrow 2 \leftarrow \mathrm{Z} \leftarrow 3 \leftarrow 4 & & \\
\mathrm{2NS} \arrow[uu] & \mathrm{4NS} \arrow[l] & & \mathrm{4WE} \arrow[ll]
\end{tikzcd}
$$

$$
\begin{tikzcd}
\mathrm{1WE} \arrow[r] & \mathrm{2WE} \arrow[r] & \mathrm{5NS} \arrow[r] & \mathrm{3WE} \arrow[r] & \mathrm{5WE} \arrow[r] & \mathrm{6WE} \arrow[dd] \\
 & & 1 \leftarrow \mathrm{Z} \leftarrow 2 \leftarrow \mathrm{Z} \leftarrow \mathrm{Z} \leftarrow \mathrm{Z} \leftarrow 3 \leftarrow 4 \leftarrow 5 \leftarrow \mathrm{Z} \leftarrow 6 & & & \\
\mathrm{4NS} \arrow[uu] & \mathrm{4WE} \arrow[l] & \mathrm{6NS} \arrow[l] & \mathrm{3NS} \arrow[l] & & \mathrm{2NS} \arrow[ll]
\end{tikzcd}
$$

Na zakończenie wspomnimy jeszcze, że jeśli istnieje turniej zbalansowany dla n par, to liczba n jest podzielna przez 4. Nietrudny dowód tego faktu pozostawimy Czytelnikowi jako ćwiczenie.