Czy przez telefon można grać w karty?

na podstawie artykułu „Poker bez kart" z książki „*The Mathematical Gardner*" (A. Shamir, R. Rivest, L. Adelman).

O telefonicznej czy korespondencyjnej grze w szachy słyszał każdy. Ale jak grać w ten sposób w brydża lub w pokera? Problemem jest oczywiście rozdawanie kart. Przypuśćmy, że grają dwie osoby i mają rozdać po pięć kart. Rozdać to znaczy:

Każdy ma wiedzieć, jakie pięć kart dostał.

Karty otrzymane przez graczy są różne.

Żaden z graczy nie ma dodatkowej informacji o kartach partnera, ale po grze może sprawdzić, czy partner nie oszukiwał, czy grał swoimi kartami.

Każdy rozkład kart jest jednakowo prawdopodobny.

Wszystko to należy wykonać porozumiewając się wyłącznie przez telefon i bez pomocy osób trzecich. Oto sposób umożliwiający w praktyce rozdawanie kart (liczb naturalnych 1, ..., 52) przez telefon. Gracze wybierają najpierw dwie rodziny funkcji o argumentach i wartościach naturalnych: $\mathscr{K} = \{K_\alpha : \alpha \in \Omega\}$ — funkcje kodujące i $\mathscr{D} = \{D_\alpha : \alpha \in \Omega\}$ — funkcje dekodujące (zbiór Ω nazywamy zbiorem kodów — powinien on mieć dużo elementów). Rodziny $\mathscr{K}$ i $\mathscr{D}$ muszą mieć następujące własności:

Dziedzina każdej funkcji K_α zawiera zbiór $\{1, \ldots, 52\}$.

Dla dowolnego kodu α funkcja D_α jest odwrotna do funkcji K_α (rozszyfrowuje ona sygnał zakodowany za pomocą funkcji K_α), tzn. $D_\alpha(K_\alpha(n)) = n$ dla liczb naturalnych z dziedziny funkcji K_α.

Dla dowolnych kodów α i β funkcje K_α i K_β są przemienne, tzn. $K_\alpha(K_\beta(n)) = K_\beta(K_\alpha(n))$.

Różne funkcje kodujące mają rozłączne zbiory wartości.

Znajomość liczb naturalnych n i $K_\alpha(n)$ nie daje *praktycznie* możliwości znalezienia kodu α.

Rozdawanie kart jest już proste. Gracze wybierają (w tajemnicy przed sobą) kody, np. A — kod α, B — kod β. Gracz A koduje liczby 1, ..., 52 i przesyła je (w dowolnej kolejności) graczowi B. Ten wybiera wpierw pięć kart dla A: $K_\alpha(a_1), \ldots, K_\alpha(a_5)$ i odsyła mu je — A musi je rozszyfrować funkcją D_α. Następnie wybiera pięć kart dla siebie: $K_\alpha(b_1), \ldots, K_\alpha(b_5)$, szyfruje je funkcją K_β i wysyła do A. Gracz A rozszyfrowuje je funkcją D_α i odsyła do gracza B (tzn. przesyła $D_\alpha(K_\beta(K_\alpha(b_i))) = D_\alpha K_\alpha K_\beta(b_i) = K_\beta(b_i)$). Gracz B musi jeszcze rozszyfrować je funkcją D_β i ... karty zostały rozdane.

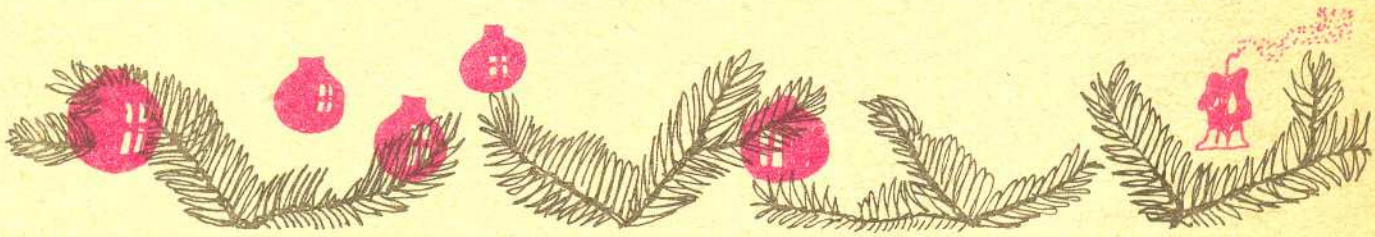
Po grze partnerzy ujawniają swoje kody. Z drugiej i czwartej własności rodzin $\mathscr{K}$ i $\mathscr{D}$ wynika, że jeśli $K_{\alpha_1}(m_1) = K_{\alpha_2}(m_2)$, to $\alpha_1 = \alpha_2$ i $m_1 = m_2$. Tak więc gracze nie mogą oszukiwać i podawać innego układu kart i innego kodu.

Powyższy opis umożliwia *w praktyce* rozdawanie kart.
Teoretycznie bowiem jest to niemożliwe.

J. R.

Oto przykład rodzin $\mathscr{K}$ i $\mathscr{D}$: p ustalona duża liczba pierwsza,
$\Omega = \{2, \ldots, p-1\}$,
$K_\alpha(n) \equiv n^\alpha \pmod p$,
$D_\alpha(n) \equiv n^\beta \pmod p$,
gdzie $1 \leqslant n \leqslant p$ i $\beta \cdot \alpha \equiv 1 \pmod p$
Oczywiście gracze muszą w tym przypadku korzystać z pomocy komputerów, ale rodzina $\mathscr{K}$ ma nadal ostatnią z własności, tzn. *praktycznie* ze znajomości n i $K_\alpha(n)$ nie uda się wyznaczyć α.

Rozdawanie kart, jeśli zamienić telefon na pocztę, można opisać tak. A wkłada karty do jednakowych pudełek (do każdego jedną kartę), zamyka każde pudełko taką samą kłódką i odsyła je do B. B odsyła pięć pudełek (są to karty gracza A) oraz pięć pudełek zamkniętych dodatkowo swoją kłódką. A wyjmuje swoje karty oraz zdejmuje swoje kłódki z pudełek z kartami B i odsyła te pudełka do B. B wyjmuje swoje karty.



Dni juliańskie

Obliczenie odstępu czasu między dwiema datami jest procedurą bardzo często spotykaną w rozmaitych działach astronomii, choćby przy obliczaniu przewidywanych położeń ciał niebieskich. Ogromnie pomaga temu tzw. juliańska rachuba dni, według której każdy dzień, poczynając od umownego, dość odległego momentu w przeszłości, ma swój numer kolejny (jeśli ktoś koniecznie chce wiedzieć, chodzi o południe 1 stycznia 4713 p.n.e.).

Niech funkcja $[x]$ przypisuje liczbie rzeczywistej x jej część całkowitą. Zapiszmy datę (naszej ery) w postaci *DD MM RRRR*, gdzie *DD* oznacza numer dnia w miesiącu, *MM* numer miesiąca i *RRRR* rok. Początkowi danego dnia (czyli północy czasu uniwersalnego rozpoczynającej daną datę) odpowiada w rachubie juliańskiej numer dnia (*JD*) obliczany według następującego schematu:

Jeżeli $MM = 1$ lub 2, to $r = RRRR - 1$ oraz $m = MM + 12$.
Jeżeli $MM \geqslant 3$, to $r = RRRR$ oraz $m = MM$.
$JD = [365{,}25r] + [30{,}6001(m+1)] + DD + \{2 - [r/100] + [r/400]\} + 1720994{,}5$.

Numer dnia juliańskiego zmieniany jest w południe czasu uniwersalnego, stąd 0,5 na końcu wzoru. Trzeba też tu wiedzieć, że do 4 X 1582 r. obowiązywał tzw. kalendarz juliański (uwaga: zbieżność nazw kalendarza juliańskiego i juliańskiej rachuby dni jest czysto przypadkowa), a kalendarz gregoriański od dnia następnego, któremu jednak przypisano datę 15 X 1582. Tak więc daty od 5 X 1582 do 14 X 1582 formalnie nie istnieją. Formułę na *JD* stosujemy w pełnej postaci dla dat kalendarza gregoriańskiego, zaś wyrażenie w nawiasie klamrowym pomijamy dla dat kalendarza juliańskiego. Jeżeli chodzi nam o obliczenie odstępu czasu między dwiema datami, to dodawanie 1720994,5 można oczywiście pominąć.

T.K.