[π-MACIERZATOR]

Gazetka redagowana przez Koło Naukowe Matematyków Uniwersytetu Śląskiego

[Złote kφiatki]

Dwa razy już na łamach [MACI$_{\mathrm{E}}$RZATORA] pojawiły się artykuły traktujące o złotej liczbie. Dowiadujemy się z nich o zadziwiającej częstości z jaką złota liczba i spokrewniony z nią ciąg Fibonacciego pojawiają się w przyrodzie. Jednakże żaden z nich nie wspomina o przyczynie owych wystąpień. W przyrodzie przecież nic nie dzieje się bez przyczyny. Jeżeli matka natura szczególnie upodobała sobie złotą liczbę, znaczy to że musi mieć z niej pewne wymierne korzyści. Tylko jakie?

Pytanie jest zupełnie elementarne i musieli się nad nim głowić już miłujący złotą liczbę Grecy czy choćby sam Fibonnacci. Tym ciekawsze jest to, że odpowiedź przyszła stosunkowo niedawno. W 1992r. dwóch francuskich matematyków S. Douady i Y.Couder[1] wspólnie opisało mechanizmy rządzące wzrostem rośliny. Nie będziemy tutaj przedstawiali technicznych szczegółów, do których odsyłamy do oryginalnej publikacji, a jedynie pewne intuicje.

Zacznijmy więc od przypomnienia. Złota liczba, najczęściej oznaczana φ jest to najzwyklejsza w świecie liczba rzeczywista i wynosi dokładnie $\frac{\sqrt{5}+1}{2} = 1.618033\ldots$. Złota liczba jest silnie związana z ciągiem Fibonacciego F_n, mianowicie jest granicą:

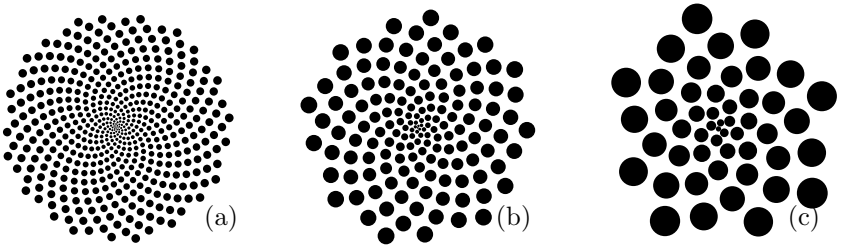
$$\varphi = \lim_{n\to\infty} \frac{F_{n+1}}{F_n}$$

gdzie F_n definiujemy rekurencyjnie:
$F_1 = 1, \qquad F_2 = 1, \qquad F_n = F_{n-1} + F_{n-2} \qquad$ dla $n \geq 2$. Tak więc kilka pierwszych wyrazów ciągu Fibonacciego to 1, 1, 2, 3, 5, 8, 13, 21, 34, ...

Nietrudno zauważyć wszechobecność ciągu Fibonacciego w przyrodzie. Wystarczy krótki spacer lub nawet wizyta w sklepie warzywnym, aby zauważyć, że łuski szyszek, nasiona słonecznika czy nawet płatki róży lub liście kapusty (to akurat trudniejsze do zauważenia) układają się w spirale. Przy czym tworzą się zarówno spirale zegarowe jak i antyzegarowe, a ich ilości wyrażają się najczęściej kolejnymi wyrazami ciągu Fibonacciego. Dodatkowo ilość spirali wydaje się być charakterystyczna dla danego gatunku, i tak przykładowo nasiona słonecznika układają się najczęściej w 34 spirale zegarowe oraz 55 spirali antyzegarowych, natomiast szyszki odpowiednio

[1] S. Douady and Y.Couder: *Phyllotaxis as a physical self-organized growth process*, Phys. Rev. Lett. 68, 2098 - 2101 (1992)

8 i 13. Na poniższym rysunku widzimy przykładowe schematy rozłożenia nasion:

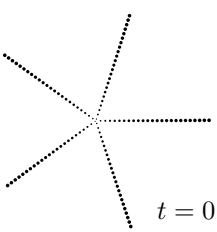


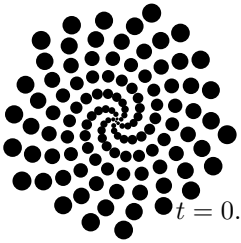
Nawet bez pomocy ołówka, łatwo zauważyć, że kropki na rysunkach (a), (b), (c) układają się odpowiednio w 34/21, 21/13, 8/13 spiral zegarowych/antyzegarowych. Otóż nic bardziej błędnego! Rysunki (b) i (c) powstały z rysunku (a) poprzez ograniczenie się do odpowiednio 150 i 50 punktów najbliżej środka[2].

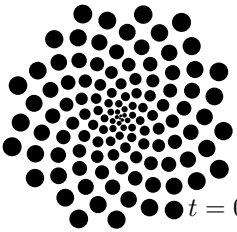
Aby zrozumieć przyczynę takiego stanu rzeczy, spróbujmy opisać przykładowo rozwój kwiatostanu słonecznika. Otóż załóżmy przede wszystkim, że kwiat rozwija się od środka. Komórki z których później powstaną nasionka powstają w centrum koszyczka, a następnie są stopniowo wypychane na zewnątrz przez nowe komórki. Ponadto z czasem wszystkie nasionka rosną i rozpychają na boki swoich sąsiadów. Analizując więc ruch pojedyńczego nasionka, będzie ono wyglądało jak gdyby zostało wystrzelone ze środka kwiatu na zewnątrz. Przypuszczamy też, że każde nasionko będzie chciało zająć możliwie największą powierzchnię (zagarniając światło słoneczne). Ponadto każde nasionko będzie starało się zająć powierzchnię możliwie zbliżoną do koła, optymalizując stosunek objętość/powierzchnia. Gdyby nasionka się nie powiększały, a kwiat nie rozwijałby się od środka, lecz doklejał nowe nasionka po bokach, wówczas jak już dawno temu odkryły pszczoły, najbardziej optymalnym rozwiązaniem byłoby pokrycie płaszczyzny przystającymi sześciokątami. Jednak rzeczywistość postawiła kwiaty przed o wiele bardziej skomplikowanym zadaniem. Szukamy zatem takiego modelu w którym przez cały czas, każde nasionko będzie miało mniej więcej tak samo daleko do wszystkich swoich sąsiadów, a odległość ta będzie się z czasem powiększać. Okazuje się, że najbardziej optymalnym rozwiązaniem jest takie, w którym kąt pomiędzy trajektoriami nasionek o numerach n oraz $n+1$ jest dokładnie złotą częścią kąta pełnego, czyli $\varphi \cdot 360^\circ \approx 582.49^\circ$.

[2]Jeżeli drogi czytelniku powiątpiewasz w moją uczciwość, zachęcam do wykonania prostego eksperymentu metodą kopiuj-wklej-powiększ, choćby nawet przy pomocy programu *M$ Paint*.

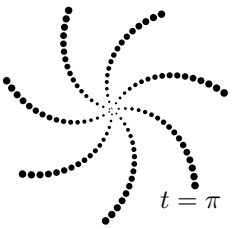
Oczywiście obrót o kąt pełny nie wprowadza niczego nowego, dlatego równie dobrze możemy rozpatrywać o obrót o kąt $(\varphi - 1) \cdot 360° \approx 222.49°$. Zamiast formalnego dowodu przeanalizujmy kilka rysunków.

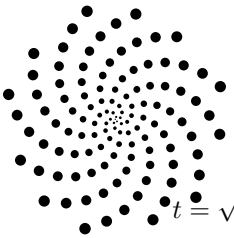

$t = 0.6$

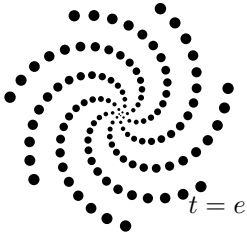

$t = 0.61$


$t = 0.618$

Zastanówmy się co by się stało, gdybyśmy zamiast złotej liczby wzięli jedynie jej przybliżenie do pierwszego miejsca po przecinku $t = 0.6$. Efekt widzimy na powyższym rysunku. Pomimo iż kąt obrotu różni się zaledwie o 3%, efekt jest zupełnie inny. Dlaczego 5 ramion? Otóż $0.6 = \frac{3}{5}$, zatem z każdym kolejnym nasionkiem zwiększamy kąt o trajektorii o $\frac{3}{5}$ kąta pełnego. Widzimy więc, że po 5 krokach otrzymamy obrót o 3 kąty pełne. Wrócimy zatem do punktu wyjścia. Stąd widoczne na rysunku 5 ramion. Podobny efekt otrzymamy dla innych wymiernych wartości t: dla $t = 0.3$ - 10 ramion, $t = 0.375$ - 8 ramion itd. Widzimy też, że ułożenie to jest z naszego punktu widzenia bardzo nieoptymalne. Nasionka tłoczą się na ramionach, podczas gdy dookoła mają mnóstwo niewykorzystanego miejsca. Sytuacja poprawia się drastycznie dla $t = 0.61$. Tutaj odbiegamy od dokładnej wartości φ o zaledwie 1.3%, a pomimo to widzimy, że nasionka mają tendencję układać się w ciasne ramiona, zwłaszcza w pobliżu środka. Dopiero dla $t = 0.618$ (odbiegającej od φ o 0.005%), uzyskujemy oczekiwany wynik - każde nasionko zdaje się mieć jednakowo daleko do wszystkich swoich sąsiadów.


$t = \pi$


$t = \sqrt{2}$


$t = e$

Widzimy zatem dlaczego wymierne wartości t nie zdają egzaminu, oraz że coraz lepsze przybliżenia φ dają coraz lepsze wyniki. A co z innymi liczbami niewymiernymi? Weźmy przykladowo $t = \pi$. Efekt jest zaskakujący:

7 ładnych ramion dla tak *bardzo niewymiernej* liczby! Otóż po pierwsze zwróćmy uwagę, że obrót o $3.141\ldots$ kąta pełnego to w praktyce to samo co obrót o $0.141\ldots$ kąta pełnego. Ten natomiast różni się od obrotu o $\frac{1}{7}$ kąta pełnego o mniej niż $0.5°$. W przypadku obrotu o $\sqrt{2}$ kąta pełnego otrzymujemy wynik różniący się o $0.8831°$ od obrotu o $\frac{5}{12}$ kąta pełnego. Natomiast dla ostatniego obrazka, brakuje mniej niż $1.5°$ aby mieć obrót o $\frac{5}{7}$ kąta pełnego.

Widzimy więc, że nasionka wcale nie starają się układać w spirale, których ilości są kolejnymi liczbami Fibonacciego. Spiralki układa nasz mózg, który we wszystkim stara się dopatrzeć regularności. Nasionka jedynie ze wszystkich sił starają się rozpychać na boki sąsiadów, tak aby zagrabić możliwie najwięcej światła. Widzimy też, że nasionka wcale nie używają którejkolwiek z przereklamowanych liczb π, $\sqrt{2}$ czy e, lecz właśnie złotej liczby φ.

Michał Stolorz

[Koło - trochę inaczej]

Drogi Czytelniku, trzymasz właśnie w ręku specjalne wydanie gazetki [MACIERZATOR], wydane z okazji czwartych już obchodów Święta Π na Uniwersytecie Śląskim. Jak zapewne już wiesz, liczba π wyraża stosunek obwodu okręgu do jego średnicy. Stąd okręgi i koła również są dziś w pewnym stopniu solenizantami i nie powinno się o nich zapominać.

Ale koła to nie tylko zbiory punktów oddalonych od jednego, ustalonego środka S o odległość nie większą od ustalonego r. Są również Koła Naukowe, a jednym z nich jest Koło Naukowe Matematyków. Powstaje oczywiste pytanie, co takie Koła mają wspólnego z kołami znanymi nam z geometrii (mniej lub bardziej). Odpowiedź brzmi - prawie nic. Ale artykuł trzeba jakoś zacząć.

Więc skoro już zaczęliśmy, to kontynuujmy. Koło Naukowe Matematyków to grupka studentów, której członkowie w teorii muszą postępować według szeregu zasad, ustalających hierarchię, to, kto z kim jest po imieniu, kto jest Członkiem Koła, a kto nie, i kto w danym dniu może nosić zielone skarpetki. W praktyce jednak odrzucamy te formalizmy i jesteśmy po prostu grupą studentów, którzy chcą wykrzesać ze studiów coś więcej niż starą zasadę ZZZZZZ (Zakuć, zdać, zapomnieć - Zdrowa Zebra Zenobiusz). W jaki sposób to robimy i jak rozwijamy nasze nieprzeciętne uzdolnienia?

Po pierwsze, mamy własną stronę internetową - www.knm.katowice.pl - na której każdy zainteresowany może znaleźć pełne informacje o tym, co robiliśmy, o tym co robimy i - w pewnych granicach - o tym, co będziemy robić. Można na niej również zapisać się do listy mailingowej, by otrzymywać na bieżąco informacje o naszej działalności.

Po drugie, co drugi piątek organizujemy referaty dla licealistów. Dla nas jest to wspaniała okazja do stanięcia po tej drugiej stronie biurka, a - mamy nadzieję - dla uczestników referatów jest to dobry sposób poznania wielu ciekawostek z przeróżnych dziedzin matematyki. Nie trzymamy się sztywnego programu i referaty niekoniecznie są powiązane w dłuższe łańcuchy - bez problemu można przyjść na referat w kwietniu, nie będąc wcześniej na ani jednym - prawdopodobieństwo, że do zrozumienia go będzie potrzebna wiedza z wykładów wcześniejszych, dąży do zera szybciej niż przysłowiowy epsilon. Informacje o referatach przesyłamy z odpowiednim wyprzedzeniem członkom listy mailingowej, a na kilka dni przed terminem referatu na stronie pojawia się również stosowny komunikat. Oczywiście, referaty są otwarte dla każdego, a po każdym z nich z chęcią wysłuchamy ewentualnych pytań, więc jeśli obawiasz się, że czegoś nie zrozumiesz - to przyjedź i sam(a) się przekonaj :)

Po trzecie, w tym roku reaktywowaliśmy kółko dla licealistów, ze wskazaniem na tych uczestniczących w konkursach dla szkół ponadgimnazjalnych. Zazwyczaj spotkania kółka odbywają się co drugą sobotę. Jeżeli więc ciekawią Cię zadania nieco ambitniejsze niż 'Oblicz objętość ostrosłupa' - zapraszamy.

Po czwarte, dwa razy w roku organizujemy sesje wyjazdowe (najczęściej do Szczyrku), a w tym roku powrócimy również do tradycji letnich obozów. Wbrew pozorom, by uczestniczyć w takim wyjeździe nie trzeba mieć średniej 5.0, napisanej pracy licencjackiej i czterech rozwiązanych problemów otwartych za pazuchą. Na szczyrkowskich wyjazdach dobrze bawią się również licealiści, którzy zdecydują się na nie pojechać (nierzadko wstępują potem w nasze szeregi, ale nie obawiajcie się - to nie skutek jakiegoś dziwnego prania mózgu, któremu są w górach poddawani), studenci pierwszego roku i inni, i nikomu po takim wyjeździe nie tworzy się dziwaczna wysypka na twarzy ani nic podobnego. Na owych sesjach, pomiędzy aktywnościami towarzyskimi, wycieczkami w góry i pysznymi posiłkami, chętni wygłaszają przygotowane uprzednio referaty. Nie jest to oczywiście obowiązkowe i nikogo nie musi to płoszyć. Najbliższa sesja, o temacie 'Alternatywne dowody twierdzeń', już w maju.

Po piąte, bierzemy również udział w innych konferencjach i sesjach, niekoniecznie organizowanych przez nas. Przykładem mogą być coroczne

zimowe sesje organizowane przez Uniwersytet Śląski i Uniwersytet w Debreczynie (Węgry).

Po szóste... Ach, długo by wymieniać. Pomiędzy konkursami, wydawaniem gazetki, zbiórką mikołajkową, referatami i wieloma innymi przejawami naszej działalności miłą oazą i ostoją spokoju staje się pokój 524, Kwatera Główna Koła, Miejsce Posiedzeń Zarządu, a dla niektórych członków - Spiżarnio-Jadalnia. Tak, tak - integracja między członkami Koła kwitnie również w czasie przerw w zajęciach, kiedy wszyscy solidarnie idą do wymienionego pokoju, by porozmawiać, napić się herbaty, zjeść śniadanie czy też przetrwać okienko (nie, nie wymieniliśmy powyżej nauki. Nie, nie był to przypadek ;).

Koło Naukowe Matematyków działa i rozrasta się. Jak grzyby po deszczu powstają nowe inicjatywy, nowe przedsięwzięcia, upadają stare reżimy, odchodzą starzy władcy, zastępują ich młodzi, wybuchają wojny, zmienia się oblicze świata - a Koło trwa, i trwać będzie, póki w pokoju 524 kołowy czajnik będzie grzał wodę na herbatę. Przybywają również nowi członkowie - może i Ty zostaniesz jednym z nich?

Niewinny Rosomak

[Enigma]

Przeważnie gdy napotkana przeze mnie osoba dowiaduje się iż na co dzień zajmuję się matematyką, mogę oczekiwać jednej z dwóch reakcji. Pierwsza to wyraz obrzydzenia, jakie dana osoba czuje to tej dziedziny nauki, wzbogacony często o traumatyczne wspomnienia związane z tym przedmiotem jeszcze z czasów liceum. Druga reakcja to mgliste przywołanie zasług polskich matematyków:

> *Ach! No tak! Matematyka... Polscy matematycy złamali Enigmę, dzięki temu Niemcy przegrali wojnę....*

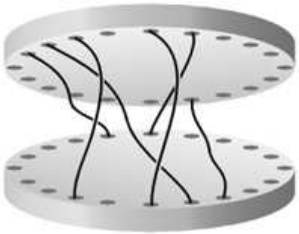
Niestety na tym lakonicznym stwierdzeniu zwykle kończy się wiedza na temat historii maszyny. Sama Enigma pozostaje niczym więcej, niż tylko obcym wyrazem na 6 liter. Matematycy pozostają anonimowi, nie wspominając już o użytych metodach dekryptażu oraz odpowiedzi na pytanie czy rzeczywiście nasze zasługi są aż tak wielkie[3]? W zasadzie każde z tych pytań zasługuje na oddzielny artykuł. Tutaj postaramy się jedynie pobieżnie omówić zasady działania owej tajemniczej skrzyneczki.

[3]W jednej z edycji encyklopedii *Britannica* pod hasłem *Enigma* czytamy: *"Kod Enigmy został rozbity przez komórkę brytyjskiego wywiadu, znaną pod kryptonimem Ultra"*. Nie ma żadnej wzmianki o jakimkolwiek polskim wkładzie.

Enigma wyglądem przypominała maszynę do pisania

Otóż, Enigma *[ang. zagadka]* została skonstruowana na początku lat 20 przez niemieckiego wynalazcę Arthura Schreibiusa. Przez pierwsze kilka lat wynalazek nie miał zastosowań militarnych. Przedsiębiorstwo Schreibiusa próbowało (niestety z mizernym skutkiem) sprzedawać Enigmę prywatnym firmom, które mogły szyfrować swoje archiwa. Dopiero w roku 1926 wynalazkiem zainteresowało się niemieckie wojsko. Oczywiście maszyna wyprodukowana na potrzeby armii była o wiele bardziej skomplikowana niż jej komercyjna siostra, ale główna zasada działania pozostała niezmieniona.

W swojej najpopularniejszej wersji Enigma wyglądem przypominała maszynę do pisania. Posiadała uproszczoną wersję klawiatury QWERTZ (tylko litery - 26 klawiszy) oraz zestaw 26 żaróweczek odpowiadających zaszyfrowanym literom. Gdy operator naciskał klawisz z literą do zaszyfrowania, zapalała się lampka odpowiadająca jej zaszyfrowanej wersji. Wiemy już zatem jak wyglądało wprowadzanie oraz odczytywanie tekstu. Musimy jeszcze wiedzieć co działo się wewnątrz tej tajemniczej skrzyneczki.



schemat rotora

Sercem Enigmy były (najczęściej) cztery wymienne rotory oznaczone symbolami I, . . . , IV, które permutowały litery alfabetu. Każdy z nich miał kształt spłaszczonego walca z 26 elektrycznymi stykami na każdej podstawie. Styki były połączone ze sobą wewnątrz walca w taki sposób, że każdemu stykowi z górnej podstawy odpowiadał dokładnie jeden z dolnej podstawy. Kolejność wewnętrznych połączeń rotorów była z góry ustalona dla każdego z czterech rotorów oraz stanowiła ścisłą tajemnicę. Po każdym naciśnięciu klawisza obracał się przynajmniej jeden z rotorów. Dodatkowo Enigma posiadała dwa specjalne, nieruchome rotory, które dalej, dla odróżnienia będę nazywał bębnami. Pierwszy z nich, tzw. bęben wstępny permutował litery pomiędzy klawiaturą i pierwszym z rotorów. Drugi, to tzw. bęben odwracający. Umiejscowiony był za ostatnim rotorem i posiadał styki tylko z jednej strony. Bęben odwracający łączył swoje 26 styków w 13 par, sprawiając że sygnał elektryczny "zawracał" i po raz drugi przelatywał przez wszystkie rotory. Bęben odwracający podwajał więc ilość permutacji wewnątrz maszyny oraz sprawiał, że tych samych ustawień można było używać zarówno do szyfrowania jak i odszyfrowywania informacji[4]. Dodatkowo,

[4]Później okazało się, że bęben odwracający jest piętą achillesową Enigmy.

wojskowa wersja Enigmy najczęściej posiadała łącznicę kablową. Umożliwiała ona operatorowi połączenie kablem dwóch dowolnych liter, co w efekcie zamieniało litery miejscami - zarówno przed jak i po przejściu przez bębny. Przy pomocy łącznicy można było utworzyć do 13 par liter, które zamieniały się miejscami. Powyższy opis maszyny jest bardzo ogólny i niekompletny. Podczas wojny w użyciu było co najmniej kilkadziesiąt różnych odmian maszyny Enigma. Dla różnych potrzeb modyfikowano gabaryty i "interfejs maszyny". Tak więc najmniejsze, przenośne wersje maszyny posiadała piechota. W dużych kwaterach i jednostkach pływających pojawiały się maszyny z drukarką zamiast żaróweczek. Gdy masa maszyny nie miała większego znaczenia, dodawano wymyślne mechanizmy zmniejszające niezbędną siłę nacisku na klawisze[5]. Pojawiały się też różne wersje zabezpieczeń: czasami znikała łącznica oraz zmieniano ilość wymiennych rotorów. W najbardziej zaawansowanej wersji Enigmy zastosowano aż 10 wymiennych rotorów! Na nasze szczęście wersja ta bardzo często się psuła, przez co zaniechano jej używania po kilku miesiącach.

łącznica wtyczkowa

Procedury używania maszyny były ściśle określone i zależały od rodzaju sił zbrojnych (Luftwaffe, Kriegsmarine, ...), rejonu w którym używana była maszyna oraz do kogo adresowana była wiadomość. Owa mnogość reguł miała stanowić dodatkowe zabezpieczenie. Dzięki nim, nawet gdyby szyfr używany w Afryce Północnej przez Luftwaffe został złamany, nie miałoby to zupełnie znaczenia dla np. U-bootów stacjonujących w tym samym czy innym rejonie. Paradoksalnie jednak to utrudnienie okazało się niezwykle pomocne przy łamaniu szyfru Enigmy. Stało się tak za sprawą komunikatów pogodowych. Pogoda była bardzo ważnym czynnikiem przy planowaniu strategii, dlatego dbano, aby wszyscy dowódcy mieli możliwie najświeższe informacje. Wysyłano więc dokładnie ten sam komunikat, używając większości obowiązujących w danej chwili kluczy. Był to niezwykle cenny materiał krytptograficzny zwłaszcza, że:

• Alianci również mieli własne prognozy pogody, które można było porównywać z przechwyconymi wiadomościami

• Komunikaty pogodowe rozsyłane były codziennie o określonej porze - mamy więc regularne źródło informacji.

[5]Naciskany przez operatora przycisk musiał spowodować obrót rotorów. Przez to niezbędna siła nacisku wahała się w okolicach 1.5kg. Każda wiadomość przed wysłaniem musiała być zaszyfrowana i odszyfrowana celem sprawdzenia czy nie popełniono błędu. Była to dość męcząca fizyczna praca, przez co przemęczeni operatorzy często popełniali błędy.

Rotory ustawiano według klucza na dany dzień.

Jak zatem wyglądała praca operatora maszyny? Najważniejsze były procedury U-bootów, dlatego skupimy się na nich. O pozostałych jednostkach można myśleć jak o uproszczonych wersjach. Na każdej łodzi znajdowała się księga zawierająca klucze. W przypadku U-bootów klucz w początkowej fazie wojny zmieniał się co 24 godziny, później co 12 godzin aż w końcowej co 8 godzin[6] (w pozostałych formacjach zmiany nie były aż tak częste). Księga z kodami wydrukowana była czerwonym atramentem na różowym papierze, który rozpuszczał się w wodzie[7]! Wszystko to miało zapobiec przejęciu kluczy przez aliantów - jeżeli cokolwiek poszłoby nie tak, księga po prostu rozpuściłaby się w morzu. Operator maszyny odczytywał z księgi które z wirników należy wykorzystać, w jakiej kolejności należy je umieścić w maszynie oraz w jakiej pozycji powinien znajdować się każdy z wirników (w końcowej fazie, wprowadzono również konfigurowalne bębny odwracające). Następnie odczytywał ustawienia łącznicy wtyczkowej. Teraz szyfrant musiał wymyślić swoje własne ustawienia wirników, czyli w przypadku maszyny z czterema wirnikami, szyfrant musiał wybrać cztery dowolne litery. Przypuśćmy, że wybrał "SWPI". Następnie dwukrotnie szyfrował swój klucz, czyli w naszym przypadku wstukiwał na klawiaturze "SWPISWPI". Następnie zmieniał ustawienia wirników według swojego klucza "SWPI" i dopiero teraz zaczynał wstukiwanie treści którą trzeba przekazać. Po każdym naciśnięciu klawisza szyfrant spisywał na kartce literkę odpowiadającą zapalonej żaróweczce. Po zaszyfrowaniu całej wiadomości obowiązkiem szyfranta było odkodowanie swoich notatek. Czyli wykonywał pracę, którą wykona odbiorca celem sprawdzenia czy nie popełnił jakiegoś błędu (jedna literówka mogła sprawić, że cały tekst stanie się nieczytelny). Procedura nakazująca wybór swojego klucza była bardzo sprytna. Dzięki niej odszyfrowanie pojedynczej wiadomości nie naruszało bezpieczeństwa innych wiadomości wysłanych tego samego dnia. Bardzo szybko jednak (ale zbyt późno dla Niemców) okazało się, że szyfranci mają tendencję aby wybierać "łatwe" klucze, takie jak "XXXX" lub "ABCD". Wprowadzano więc kolejne restrykcje, takie jak "żadna litera w kluczu nie może się powtarzać",

[6] W ramach eksperymentów wprowadzono nawet w użycie urządzenie przypominające zegar, które CO GODZINĘ generowało nowy kod. Jednakże nawet sami Niemcy zauważyli, że jest to raczej kiepski generator liczb losowych i zaniechali jego użycia.

[7] Tym bardziej zdumiewające jest to, że aliantom udało się wykraść księgę kodów z tonącej niemieckiej łodzi podwodnej. Często w filmach fabularnych związanych z II Wojną Światową istnieje nawiązanie do tego faktu. I to nie jest fikcja! Księgę można dalej oglądać w jednym z brytyjskich muzeów.

"nie wolno wybierać kolejnych liter alfabetu" itd .... Teraz jednak okazało się, że reguły są na tyle restrykcyjne, że dość poważnie ograniczają ilość możliwych wyborów. Zrezygnowano również z konieczności podwójnego powtórzenia wybranego klucza. Każda z modyfikacji początkowo przysparzała aliantom sporo problemów. Jednak zawsze udawało się znajdować jakieś potknięcia niemieckich operatorów. Jak wyglądały metody dekryptażu oraz kto się tym zajmował to juz materiał na zupełnie inny artykuł.


kadr z filmu "Das Boot"

Myślę, że każdy po przeczytaniu tego tekstu będzie mniej więcej wiedział jak wyglądała i jak działała Enigma. Jest to niezwykle satysfakcjonujące, kiedy oglądając film wojenny widzimy jak ktoś używa Enigmę i wiemy dokładnie co dana osoba robi. Widzimy czasem jak operator wystukuje coś na urządzeniu przypominającym maszynę do pisania, otwiera czerwoną książkę, przekręca jakieś trybiki, nasłuchuje odpowiedzi... A my już wiemy, że odczytuje klucz na dany dzień, nastawia rotory i wprowadza tekst. Wszystkich zainteresowanych serdecznie zapraszam na projekcję filmu *Sekret Enigmy*, który odbędzie się w sobotę, 13 marca, w ramach obchodów IV Święta Liczby Pi (po szczegóły odsyłam do strony: www.swietopi.pl). Polecam również filmy *Das Boot* - (1981) znakomity niemiecki film, *Tajemnica Enigmy* - (1979) polski serial, na jego podstawie nakręcono film na którego projekcję zapraszamy w sobotę oraz film *Szpiedzy tacy jak oni* - (2001) lekka komedia wojenna, niosąca jednak pewne bardzo ważne przesłanie dotyczące Enigmy. Zdecydowanie jednak nie polecam filmu *Enigma*(2001) - film raczej luźno trzymający się faktów, zaklasyfikowałbym go jako romans – Sci-Fi.

Michał Stolorz

[Zadanie - ilu graczy w turnieju?]

Następujące zadanie pochodzi z XX Międzynarodowych Mistrzostw w Grach Matematycznych i Logicznych:

> *W turnieju szachowym uczestniczyła parzysta liczba graczy. Każdy rozegrał dokładnie jedną partię z każdym z pozostałych. Pięciu graczy przegrało po dwie partie (każdy z nich), a pozostali gracze wygrali po dwie partie (każdy z nich). Nie było żadnego remisu. Ilu graczy uczestniczyło w tym turnieju?*

Rozwiązanie:

Niech $2k$ oznacza liczbę wszystkich graczy ($k \in \mathbb{N}$). Korzystając z symbolu Newtona możemy obliczyć ile w ogóle zostało rozegranych partii:

$$\binom{2k}{2} = \frac{(2k)!}{(2k-2)!2} = (2k-1)k.$$

Ponieważ w każdej partii ktoś wygrał (nie było remisów), powyższą liczbę możemy traktować też jako liczbę wygranych partii.
Zauważmy, że liczba partii wygranych przez owych 5 graczy wynosi: $5(2k-1-2)$ (każdy z nich rozegrał $2k-1$ partii i przegrał 2; ponieważ nie mogli wygrać jednocześnie, grając tę samą partię, możemy spokojnie pomnożyć przez 5).
Liczba partii wygranych przez pozostałe osoby: $(2k-5)2$.
Składając wszystkie informacje razem dochodzimy do następującego równania:

$$5(2k-3) + (2k-5)2 = (2k-1)k,$$

a po paru przekształceniach... $2k^2 - 15k + 25 = 0$. Stąd: $k = \frac{5}{2}$ lub $k = 5$, a ponieważ w turnieju mieliśmy parzystą liczbę uczestników, jedynym rozwiązaniem pozostaje $2k = 10$.

Ivril

[πografie - Kawiarnia Szkocka]

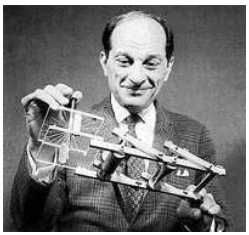
Tak, tak. Wiemy, co myślicie - że ogarnęła nas taka megalomania, że piszemy już πografie własnych warsztatów. Ale nie o to chodzi! Kawiarnia Szkocka, którą znacie z naszego Wydziału i w której zapewne zamieniacie zarobione πniądze na kawę i ciastka, jest jedynie inspirowana Kawiarnią Szkocką, w której przed II wojną światową pracowały najtęższe matematyczne umysły, demolując marmurowe blaty, wymieniając się żywym inwentarzem i rozważając kartofle i worki. Nie żartuję.

Rozpocznijmy zatem naszą opowieść. Kawiarnia Szkocka mieściła się we Lwowie, przy Placu Akademickim 9, jej właściciel zaś zwał się Zieliński. Była ona miejscem spotkań wielu osobistości ze sfer sportowych, literackich i uniwersyteckich. Urządzona była w stylu wiedeńskim i posiadała maleńkie stoliki o marmurowych blatach. Naprzeciwko niej stała kawiarnia Żoma",

która jako pierwsza przeżywała oblężenia matematyków z tzw. lwowskiej szkoły matematycznej, którzy organizowali w niej swoiste naukowe sesje. Wtedy matematycy do Kawiarni Szkockiej wpadali jedynie nieregularnie, jednak już po około roku matematyk Stefan Banach zadecydował, żeby sesje przenieść w całości do Kawiarni. Być może argumentem 'za' były właśnie owe marmurowe blaty, wspaniale służące do szybkiego notowania podawanych twierdzeń i prowadzenia obliczeń. Podobno Zieliński szybko się przyzwyczaił do tej dewastacji mienia.

W. Sierpiński

I tak powstała swoista tradycja - w latach 1935-1941 niemalże codziennie do Kawiarni wpadała chmara matematyków, by usiąść przy stoliku (stolikach), zapisywać je tajemniczymi formułami i rozmawiać, grać w szachy, popijać trunki i palić papierosy (do tych dwóch ostatnich rzeczy nie zachęcamy). Zresztą, zachowanie naukowców było wtedy dość osobliwe - najpierw wszyscy milczeli, ktoś mówił kilka słów, które inni 'wtajemniczeni' łapali w lot, zapisywano kilka formuł na blacie stolika - i wracano do milczenia i popijania.



Stanisław Ulam

Kto tam przesiadywał? Stałymi bywalcami byli Banach i Mazur, następnie Ulam, Borsuk, Steinhaus, Auerbach, Sierpiński i wielu innych. Stożek i Nikliborc często grali w szachy, czemu kibicowała spora grupa matematyków. Naturalnie, przy tak dużej koncentracji matematyków w jednym miejscu, przebywających ze sobą niejednokrotnie przez bardzo długie okresy czasu (rekordem Kawiarni było 'posiedzenie' trwające 17 godzin!), anegdoty i dziwne zachowania rosły jak grzyby po deszczu, umacniając legendę Kawiarni Szkockiej. Pierwsze z nich to, oczywiście, zapisywanie formuł na blatach stolików, które dało asumpt do zakupienia przez Łucję Banach - żonę Stefana Banacha - zeszytu, który przeszedł do historii jako 'Księga Szkocka'. Zapisywanie formuł na stolikach miało liczne wady, których nie były w stanie zmazać nawet liczne ustalenia z właścicielem Zielińskim - raz zapisane marmurowe blaty przeniesiono specjalnie do osobnej sali, by nikt przez przypadek niczego nie starł. Z tego też powodu matematycy poczęli zapisywać swe twierdzenia i problemy we wspomnianym wyżej zeszycie, miast na stolikach, dzięki czemu zabezpieczali je przed, po pierwsze, starciem przed nadgorliwych kelnerów, a po drugie zapewniali sobie większe szanse na odczytanie swych bazgrołów następnego dnia - pamiętajmy, że koniak i wino były popularnymi trunkami na spotkaniach Kawiarni, i zapewne wiele wspaniałych twierdzeń musiało czekać kolejne lata na odkrycie ze względu na niemożność odcyfrowania stołowych zapisków.

Księga Szkocka to praktycznie temat na osobną opowieść. Po jej zakupie była przetrzymywana przez pracownika Kawiarni i przynoszona przez kelnera na żądanie każdego klienta. Książka ta rozrastała się szybko, zapełniana przez notatki wszystkich lwowskich matematyków. Do licznych problematów często były dopisywane liczne dziwne spostrzeżenia, albo i nagrody za udowodnienie podanego twierdzenia (w czym przodował Mazur). I tak, 'Problemat Mazura' był sformułowany w mniej więcej następującej postaci:
Jeżeli $\{H_n\}, n = 1, 2, ...,$ *są bryłami wypukłymi o średnicy* $\leq a$*, przy czym suma objętości* $\leq b$*, wówczas istnieje sześcian o krawędzi* $c = f(a, b)$*, w którym bryły dane można umieścić (...).*
Wniosek: Kilogram kartofli da się umieścić we worku.

Z ciekawszych nagród, 'Problemat Steinhausa':
- *Za obliczenie frekwencji: 10 dkg kawioru czerwonego*
- *Za dowód istnienia: małe piwo*
- *Za przykład przeciwny: mała czarna*

Absolutnym rekordzistą wśród dziwnych nagród, takich jak 'obiad w George'u', jest oczywiście 'żywa gęś', ufundowana przez Mazura za rozwiązanie pewnego zagadnienia bazy w przestrzeniach Banacha. Gdy problem ten w 1972 roku (36 lat po jego postawieniu) rozwiązał Szwed Per Enflö, otrzymał z rąk profesora Mazura wspomnianą nagrodę. Co z ową gęsią zrobił - nie wiadomo.

Ale skąd Szwed mógł wiedzieć o istnieniu Księgi Szkockiej? Zawdzięczamy to, ponownie, Łucji Banach oraz Stanisławowi Ulamowi. Ta pierwsza odratowała Księgę z wojennej pożogi, ten drugi przetłumaczył ją na język angielski, umożliwiając jej odkrycie całemu światu.

Kawiarnia Szkocka na pewno wspomogła rozwój podstaw analizy funkcjonalnej (wystarczy przypomnieć sobie nazwiska bywalców: Banach, Schauder, Mazur, Borsuk), a oszałamiająca liczba 193 problemów, zamieszczonych w Księdze Szkockiej, mówi sama za siebie. Znaczenie tej ostatniej było tak duże, że w 1945 roku kontynuowano jej tradycję we Wrocławiu, by w roku 1958 wydać Nową Księgę Szkocką.

Można by się zastanawiać, jak długo trwałyby spotkania w Kawiarni i ile tomów osiągnęłaby Księga, gdyby nie wybuch wojny. Cóż, jedno jest pewne - nie trwałyby do dziś, albowiem w miejscu Kawiarni Szkockiej stoi dzisiaj oddział banku. Przynajmniej budynek zachował choć śladowe powiązanie z matematyką.

Niewinny Rosomak

[Harmonogram Święta Liczby Pi 2010]

w Instytucie Matematyki

3.11 (czwartek)


09.00-14.00 Warsztaty KNM (sale: 224, 226, 429, 225, 208, 209)


09.42-10.30 Uroczyste rozpoczęcie Święta Pi (SA III, Instytut Fizyki UŚ)


10.30-11.30 prof. Aleksander Błaszczyk - *Paradoksy nieskończoności* (s. 213)


10.30-14.00 Pilionerzy (s. 233)


11.35-12.35 Tomasz Kania - *Przestrzenie Banacha* (s. 213)


12.40-13.25 dr Erwin Kasparek - *Trójkąty Herona* (s. 213)


13.30-14.15 dr Rafał Kucharski - *Prawdopodobnie nieprawdopodobne* (s. 213)


14.20-15.05 dr Tomasz Szostok - *Co było pierwsze, równanie...* (s. 213)

3.12 (piątek)


08.00-11.00 Zajęcia dla uczniów szkół podstawowych


09.00-14.00 Warsztaty KNM (sale: 224, 226, 429, 225, 208, 209)


09.00-09.45 Jola Marzec - *Rozmieszczenie liczb pierwszych na płaszczyźnie* (s. 213)


09.50-10.50 mgr Tomasz Kochanek - *Opowieść o Hipotezie Riemanna* (s. 213)


10.55-11.55 mgr Michał Stolorz - *Mozaiki* (s. 213)


11.00-14.00 Tour de Science


12.00-12.45 mgr Łukasz Dawidowski - *Jak nie zarazić się grypą...* (s. 213)


12.00-14.00 Finał konkursu *Epigramat*


12.50-13.35 Piotr Idzik - *Co potrafią narysować wielomiany?* (s. 213)


13.40-14.25 dr Piotr Janoska - *Matematyka wokół nas* (s. 213)


14.30-15.15 Rozdanie nagród (s. 227)

3.13 (sobota)


10.00-11.00 Koncert – *Śpiewające Szynszyle* (Skwerek przed wejściem do Inst.)


11.00-11.30 PI na skrzydłach wiatru (Skwerek przed wejściem do Inst.)


12.00-14.00 Projekcja filmu *Sekret Enigmy* (Kinoteatr Rialto ul. Św. Jana 24)

[Czy wiesz, że...]

O tym, co to jest π, ile wynosi, skąd się bierze i jaki kolor kalesonów lubi najbardziej wiedzą wszyscy. Zajmijmy się więc nieco mniej znanymi faktami. Ahem. Czy wiesz, że...

- Średnia liczba sposobów na zapisanie liczby naturalnej jako sumy dwóch liczb całkowitych, których pierwiastek też jest liczbą całkowitą, wynosi $\frac{\pi}{4}$;
- Symbolu π pierwszy użył William Jones w 1706 roku;
- W ciągu pierwszych dwustu milionów cyfr rozwinięcia dziesiętnego liczby π najdłuższe ciągi jednocyfrowe to:
  - osiem jedynek, dwójek, czwórek i dziewiątek(tj. ciągów 11111111, 22222222, itd.),
  - siedem trójek i piątek,
  - dziewięć szóstek, siódemek i ósemek;
- Do uzyskania wszystkich kombinacji "dzień miesiąca-miesiąc"(np. 14 marca - 1403) wystarczy pierwsze 60875 cyfr rozwinięcia dziesiętnego π, a ostatnia kombinacja (zajmująca cyfry od 60872 do 60875) to 1203 - 12 marca;
- Przybliżenie $\pi \approx 3$ pojawia się w Biblii (1 Krl, 7:23): *Następnie sporządził odlew 'morza' o* ***średnicy dziesięciu łokci****, okrągłego, o wysokości pięciu łokci i o* ***obwodzie trzydziestu łokci****.*

Niewinny Rosomak

[Stopka redakcyjna]

Kontakt z redakcją bezpośrednio w pokoju KNM (p.524) lub elektronicznie:
macierzator@knm.katowice.pl www.knm.katowice.pl

marzec 2010