

Jak polscy matematycy złamali Enigmę

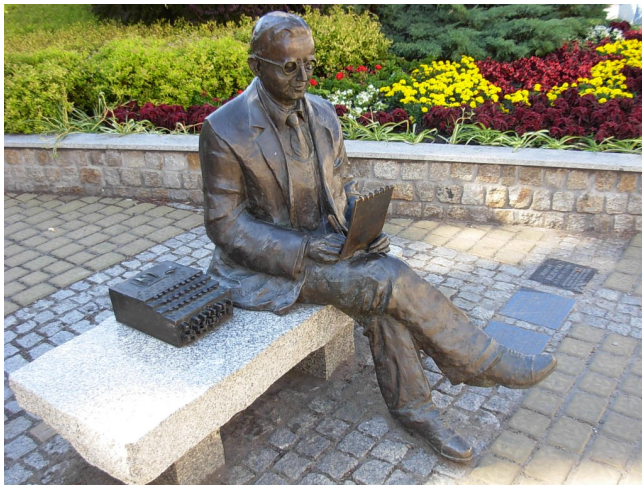
Adam Doliwa

doliwa@matman.uwm.edu.pl

WYDZIAŁ MATEMATYKI I INFORMATYKI UWM

Olsztyn, 8 lutego 2013 r.

Podczas XXVI Sesji Rady Miasta Olsztyna (29.09.2012 r.) radni nadali nazwy dwóm ulicom prowadzącym do budowanych obiektów Olsztyńskiego Parku Naukowo-Technologicznego. Patronem drogi gminnej oznaczonej symbolem 1KDD został Marian Rejewski - matematyk i kryptolog.





INTERNATIONAL CONGRESS OF MATHEMATICIANS · WARSAW POLISH MATHEMATICIANS

Jan ŁUKASIEWICZ
(1878-1956)
Logic, intuitionism, philosophy of science, philosophy of mathematics, Warsaw

The group of logicians in Warsaw also included Stanisław LEŚNIEWSKI (1883-1939), Adolf LINDENBAUM^{*} (1894-1962), and Alfred TARSKI (since 1942 in Berkeley). Here in 1933 Tarski published his celebrated theorem on the undecidability of the notion of truth.



Andrzej MOSTOWSKI
(1928-1972)
Foundations of mathematics, model theory, recursive arithmetic, Warsaw

The term *Warsaw School of Mathematics* is used to describe a group of mathematicians working in logic, set theory, point-set topology and real functions in the 1920's and 1930's. Their journal was *Fundamenta Mathematicae* (founded in 1920), the first specialized mathematical journal in the world.

Wacław SIERPIŃSKI

(1882-1969)
Theory of sets (particularly axiom of choice), set-theoretic topology, analysis, dynamics, ergodic theory, author of TSI paper and 30 books including one on set theory in 1932.
First in Warsaw, 1920-1930; Chicago, 1930-1961 in Los Angeles, 1961-1969, afterwards in Warsaw.



Kazimierz KURATOWSKI

(1896-1981)
Topology, set theory, point and order sets, author of "Topology" (1933-1936) covering the achievements of the Warsaw School in point-set topology. Leading figure in Polish mathematics. TSI 1927 in Warsaw, then in Los Angeles, moving back to Warsaw in 1948.



Edward MARCZEWSKI

(1884-1966)
Real functions, measure theory, differential algebra, TSI 1927 in Warsaw, 1933-1934 in Wrocław, 1934-1966 in Wrocław.



Zygmunt JANUSZEWSKI

(1889-1923)
Topology of the plane. In 1916 he wrote a development program for Polish mathematics, assuming that efforts to achieve would be in topology, analysis, and logic.
First in Warsaw, 1916-1923.



Stefan MAZURKIEWICZ

(1884-1942)
Point-set topology, analysis, dynamics, ergodic theory, functional analysis (abstract proofs using Baire category), set-theoretic topology, Warsaw.



Karol BORSUK

(1891-1968)
Geometric topology. Founder of the theory of retracts and of shape theory. Introduced 1930's cofibrations groups.
Contributed to fixed point theory (antipodal theorem).
Warsaw.



Members of the Warsaw topology group who emigrated in the 1930's: Nachman ARONSZJAIN (1907-1969) and Samuel EILENBURG (now in New York).

The term *Low School of Mathematics* refers to a group of over a dozen mathematicians working in functional analysis, real functions and probability in the 1920's and 1930's. Their journal was *Studia Mathematica* (founded 1929).

Stefan BANACH

(1891-1949)
Orthogonal series, real functions, measure theory, one of the founders of functional analysis (theory of Banach space and its linear operators).
Author of the classic "Theory of linear operators" (1922).
First in Poznań, 1922-1929; then in the Low School, 1929-1949.



Juliusz P. SCHAUDER
(1889-1949)
One of the founders of two linear functional analysis. Introduced methods to apply differential equations (fixed point theorems, Leray-Schauder index, Schauder estimates).
Low.

Stanisław MAZUR

(1883-1961)
Geometrical methods in linear and nonlinear functional analysis, separability theory, Banach algebras, infinite groups, measure functions.
The classic collection of Banach. In Low 1934-1946, in Warsaw since 1948.



Hugo STEINHAUS
(1887-1972)
Orthogonal series, probability theory, and topology, functional analysis, applications of mathematics. A leading spirit of the Low School. Author of the widely known "Mathematical Analysis".
TSI 1941 in Low, then in Wrocław.

Władysław ORLICZ, a member of the Low School, moved to the University of Poznań in 1937, making it a center of functional analysis.

The Low School also included Herman AUBRACH^{*}, Stefan KACZMARZ^{*}, Antoni ŁONCZAK^{*}, Mark KAC and Stanisław ULAM (both now in U.S.A.).

Fourier analysis was developed in Warsaw by Aleksander RACHMAN^{*} and Antoni ZYGUND and the latter returned to the University of Wina (founded 1780) where he led an analysis group in the 1930's. During the war he settled in the U.S.A.



Józef MARCINKIEWICZ
(1905-1984)
Real functions, orthogonal series, trigonometric series, probability, analytic functions, applications of linear operators, probability theory.
Low.

Otto M. KODRÓV

(1881-1976)
Measure theory (cf. Radon-Nikodym theorem), probability series-converges with applications to Banach projective limit, generalized solutions of differential equations, descriptive set theory, foundations of quantum mechanics. Low, Cracow and Warsaw, since 1947 in U.S.A.

Język SPŁAWA-NIEYMAN

(1894-1968)
Mathematical statistics and its application to agriculture, astronomy, biology, methods of statistical inference of the biological sciences, a typical text and introduction.
1921-1922 in Kraków, in 1934 mostly in Warsaw, 1934-1968 in London and Berkeley.

Stanisław ZAREMBA

(1881-1962)
Partial differential equations, functional theory, mathematical theory of the Dirac operator, theory of Dirac operators, mathematical theory, cosmology. One of the founders of low methods in statistical mechanics for applications (Dirac operator, asymptotic expansion, 1955).
1916-1930 in Paris, afterwards in Cracow.



Kazimierz ŻORAWSKI
(1894-1976)
Real functions, differential equations, integral equations, applications of linear operators, fixed point theorems, Banach spaces, Warsaw.

Władysław SŁODKOWSKI

(1881-1976)
Differential equations, probability, statistics, and mechanics. TSI 1931 in Warsaw, 1931-1934 in Wrocław, 1934-1976 in Wrocław.

Franklin LEJA
(1891-1976)
Analytic functions, in particular the method of extremal points and extremal algebras, Chicago, Warsaw.

Marian REJEWSKI

(1891-1968)
Mathematical statistics, in 1925-1926 he introduced the concept of groups of correlation of breaking the Ergodic theory. He worked, developed later in England, contributed significantly to the theory of the Brownian motion and Wiener and 1931 during the war in France and England.



Springer-Verlag Berlin Heidelberg New York Tokyo

1930's. dozen mathematicians working in functional analysis, real functions and probability in the 1920's and 1930's. Their journal was *Studia Mathematica* (founded 1929).

Stefan BANACH

(1892–1945)

Orthogonal series, real functions, measure theory; one of the founders of functional analysis (concept of a Banach space and its basic properties). Author of the classic “Théorie des opérations linéaires” (1932). Exerted strong personal and mathematical influence on the Lvov School.



Hugo STEINHAUS

(1887–1972)

Orthogonal series, probability theory, functions, functional applications, statistics. A moving force in the Lvov School of the widest sense. “Mathematica” Till 1945 in

Marian REJEWSKI

(1905–1980)

Mathematical cryptology. In 1932–1933 discovered a method (based on properties of groups of permutations) of breaking the Enigma cipher. (The method, developed later in England, contributed significantly to the Allies' victory in World War II.) In Poznań and Warsaw until 1939, during the war in France and England.



W 1919 roku Hugo Koch opatentował maszynę szyfrującą ze zmiennym szyfrem podstawieniowym innym dla każdego znaku.



Wirtualna ENIGMA <http://www.biecek.pl/projects/Enigma2/Enigma.html>

Autor: dr inż. Przemysław Biecek (Instytut Matematyki Stosowanej i Mechaniki, Uniwersytet Warszawski)

Kurs kryptologii dla matematyków

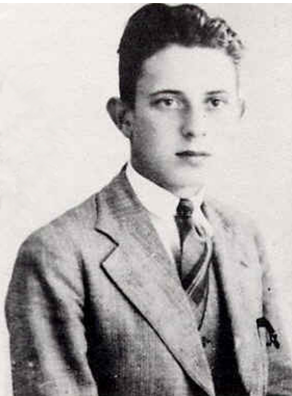
15 lipca 1928 roku Enigma w wersji G została dopuszczona do użytku w wojskach lądowych (Reichswera) Niemiec. Pomimo znajomości ogólnych zasad działania maszyny szyfrującej wywiady angielski i francuski ze względu na liczbę (rzędu 10^{14}) możliwych stanów urządzenia uznały szyfr za niemożliwy do złamania.

W styczniu 1929 na Uniwersytecie Poznańskim zorganizowano kurs kryptologii dla 26 wybranych studentów matematyki znających język niemiecki. Jesienią 1930 utworzono w Poznaniu filię Biura Szyfrów, w której zatrudniono m.in. Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego.

Polscy kryptolodzy



Marian Rejewski
(1905-1980)



Jerzy Różycki
(1909-1942)



Henryk Zygalski
(1908-1978)

Polski radiowywiad podczas wojny z bolszewicką Rosją 1918-1920



Jan Kowalewski (1892-1965) złamał w 1919 roku klucze szyfrowe Armii Czerwonej. Wciągnął do współpracy wybitnych przedstawicieli polskiej szkoły matematycznej: Stanisława Leśniewskiego, Stefana Mazurkiewicza, Wacława Sierpińskiego.

Kontruderzenie znad Wieprza — „cud” nad Wisłą

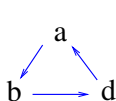


„nieprzyjaciół sam informował dokładnie nasze dowództwo o swym stanie moralnym i materialnym, o swych stanach liczebnych i stratach, o swych ruchach, o osiągniętych zwycięstwach i poniesionych klęskach, o swych zamiarach i rozkazach, o miejscu postoju swych dowództw i rejonach dyslokacyjnych swych dywizji, brygad i pułków”

Permutacje

$$S = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ b & d & f & a & e & c \end{pmatrix} = (abd)(cf)(e)$$

$6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 6!$ różnych permutacji zbioru o sześciu elementach



cykl długości trzy



transpozycja

Fakt

Każdą permutację można rozłożyć na cykle rozłączne

$$S^{-1} = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ d & a & f & b & e & c \end{pmatrix} = (dba)(cf)(e)$$

Permutacja odwrotna

Grupa permutacji

$$S = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ b & d & f & a & e & c \end{pmatrix} \quad T = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ e & f & b & c & d & a \end{pmatrix}$$

Składanie (mnożenie) permutacji

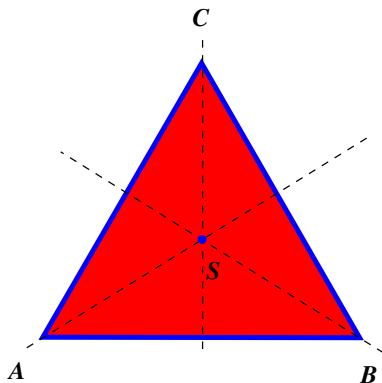
$$T \circ S = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ b & d & f & a & e & c \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ f & c & a & e & d & b \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ f & c & a & e & d & b \end{pmatrix}$$

- $(U \circ T) \circ S = U \circ (T \circ S)$

- $S \circ S^{-1} = S^{-1} \circ S = I = \begin{pmatrix} a & b & c & d & e & f \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ a & b & c & d & e & f \end{pmatrix}$

- $S \circ I = I \circ S = S$

Przykład geometryczny – grupa symetrii trójkąta równobocznego



- R_k – obrót o $\frac{k\pi}{3}$ wokół środka trójkąta S , $k = 1, 2$
- O_X – odbicie w prostej SX , $X = A, B, C$
- I – identyczność

np. $R_1 = (ABC)$, $O_A = (BC)(A)$

Permutacje a rozwiązywalność równań algebraicznych



François Viète (1540-1603)

W równaniu algebraicznym $x^2 + bx + c = 0$ wyrażenia

$$b = -(x_1 + x_2), \quad c = x_1 \cdot x_2$$

nie zmieniają znaku przy zamianie pierwiastków x_1, x_2 równania.

Wyrażenie $d = x_1 - x_2$ zmienia (tylko) znak przy przestawieniu pierwiastków, czyli jego kwadrat jest niezmienniczy

$$d^2 = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 \cdot x_2 = b^2 - 4c$$

Ponieważ znajomość b oraz d pozwala wyznaczyć x_1 i x_2 wnioskujemy stąd, że muszą istnieć wzory na pierwiastki wymagające operacji algebraicznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz wyciągania pierwiastka kwadratowego.

Permutacje a rozwiązywalność równań algebraicznych

Podobna analiza znanych technik rozwiązywania równań algebraicznych stopnia trzeciego (Scipione del Ferro (1465-1526), Niccolo Tartaglia (1500 - 1557)) oraz czwartego (Lodovico Ferrari (1522 - 1565)) dokonana przez Josepha Louisa Lagrange'a (1736-1813) doprowadziła Paolo Ruffiniego (1765-1822) do twierdzenia, że

nie istnieją ogólne wzory na rozwiązania równania stopnia piątego wykorzystujące operacje algebraiczne i pierwiastkowanie

Jakie równania mają rozwiązania przez pierwiastniki ?



Évariste Galois (1811-1832)

Tworząc teorię grup Galois wyprzedził swoją epokę o kilkadziesiąt lat. Camille Jordain, *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris 1870 (667 stron)

Oszacowanie liczby możliwych stanów Enigmy

Każdy z bębenków może przyjąć 26 różnych pozycji. Pozycja bębenków się zmienia:

$$3! \cdot 26 \cdot 26 \cdot 26 = 105\,456 \simeq 10^5$$

Liczba połączeń sześciu par liter w łącznicy wtyczkowej:

$$\frac{26!}{2^6 \cdot 6! \cdot 14!} = 100\,391\,791\,500 \simeq 10^{11}$$

Liczba możliwych bębenków odwracających:

$$\frac{26!}{2^{13} \cdot 13!} = 7\,905\,853\,580\,625 \simeq 8 \cdot 10^{12}$$

Liczba możliwych bębenków szyfrujących

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000 \simeq 4 \cdot 10^{26}$$

Twierdzenia Rejewskiego

Definicja i Fakt

Inwolucją nazywamy permutację będącą swoją odwrotnością. Inwolucja w rozkładzie na cykle może składać się tylko z punktów stałych i transpozycji.

Twierdzenie 1

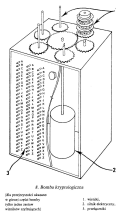
Jeśli dwie permutacje tego samego stopnia składają się z samych transpozycji rozłącznych, wtedy w ich złożeniu cykle rozłączne występują w liczbie parzystej, a elementy transpozycji trafiają do cykli o tej samej długości.

Twierdzenie 2

Jeśli w rozkładzie permutacji na cykle rozłączne jest parzysta liczba cykli o tej samej długości to można taką permutację rozłożyć na dwie inwolucje.

Korzystając ze swoich twierdzeń, znajomości psychiki niemieckich żołnierzy oraz kluczy dziennych z września i października 1932 dostarczonych przez wywiad francuski, pod koniec grudnia 1932 Rejewski **zrekonstruował okablowanie wirników**.

Żeby zautomatyzować pozostałe elementy procesu dekodowania kryptolodzy zaprojektowali urządzenia pomocnicze (cyklometr, karty charakterystyk) umożliwiające ustalenie klucza dziennego w 15 minut.



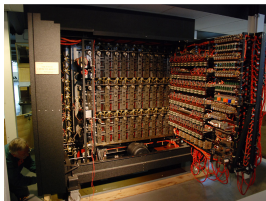
Po 15 września 1938, kiedy Niemcy wprowadzili udoskonalenia w technice szyfrowania (zwiększenie liczby ruchomych bębenków, zmienna liczba połączeń w łącznicy) kryptolodzy udoskonalali narzędzia (tzw. bomba kryptologiczna – sprzężone sześć kopii Enigmy napędzane silnikiem elektrycznym, plachty perforowane).

W 1939 Niemcy ponownie zwiększyli liczbę wirników, co wymagało zbudowania dodatkowych 54 (oprócz istniejących sześciu) bomb kryptologicznych oraz opracowania 60 kompletów płacht Zygalskiego. Przekraczało to ówczesne możliwości finansowe Biura Szyfrów.

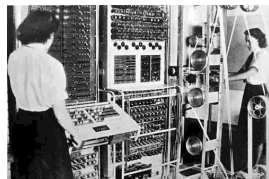
Na spotkaniu 25 lipca 1939 w Pyrach pod Warszawą przekazano po jednym egzemplarzu kopii Enigmy wraz z dokumentacją przedstawicielom wywiadów Wielkiej Brytanii i Francji.



Bletchley Park



Bomba Turinga



Colossus



Siedziba Agencji Bezpieczeństwa Narodowego (National Security Agency) w Fort Meade w stanie Maryland — największe skupisko matematyków na świecie.

Tajemnica, a jednocześnie chwała matematyki, leży nie tak bardzo w tym, że abstrakcyjne teorie okazują się być stosowalne do rozwiązywania rzeczywistych zadań, lecz — i to jest cud nad cudami — w tym, że teoria wymyślona do badania problemów jednego typu okazuje się być często jedyną drogą do rozwiązania problemów zupełnie innego rodzaju, problemów do badania których nie była stworzona. Takie przypadki występują na tyle często, że muszą stanowić esencję matematyki.

[Gian Carlo Rota, Indiscrete Thoughts]

Dobry matematyk potrafi dostrzegać fakty, matematyk wybitny – analogie między faktami, zaś matematyk genialny – analogie między analogiami.

[Stefan Banach]

Literatura

- Marian Rejewski, *Wspomnienia z mojej pracy w Biurze Szyfrów Oddziału II Sztabu Głównego w latach 1930-1945*, Wydawnictwo Naukowe UAM, Poznań 2011
- Marian Rejewski, *An Application of the Theory of Permutations in Breaking the Enigma Cipher*, *Applicationes Mathematicae* **16** (1980) 543-559
- Zdzisław Opiał, *Algebra wyższa*, Państwowe Wydawnictwo Naukowe, Warszawa 1975
- Marek Grajek, *Enigma. Bliżej prawdy*, Dom Wydawniczy REBIS, Poznań 2008
- Grzegorz Nowik, *Zanim złamano „ENIGMĘ” ... Polski radiowywiad wojskowy podczas wojny z bolszewicką Rosją 1918-1920*, Oficyna Wydawnicza RYTM, Warszawa 2004 (T. 1), 2010 (T. 2)
- <http://pl.wikipedia.org/wiki/Enigma>