ELEMENTY TEORII GALOIS W ZASTOSOWANIACH KRYPTOGRAFICZNYCH W SYSTEMIE BEZPIECZEŃSTWA NARODOWEGO

Sławomir Wereński
Beata Siemieńska

Uniwersytet Technologiczno-Humanistyczny w Radomiu

Streszczenie. Praca dotyczy praktycznego wykorzystania elementów teorii Galois w zastosowaniach kryptograficznych w aspekcie bezpieczeństwa narodowego. W związku z powyższym zaprezentowano historię narodzin matematyki, w tym genezę powstania algebry oraz znaczenie tego terminu. Następnie przedstawiono krótką charakterystykę rozwoju algebry w kierunku abstrakcyjnym oraz omówiono niektóre elementy klasycznej teorii Galois, które mogą być wykorzystywane w implementacjach kryptograficznych na potrzeby bezpieczeństwa i obronności kraju. Szczególną uwagę zwrócono na ciała skończone oraz ich rozszerzenia, wykorzystywane do budowy algorytmów szyfrujących, a także omówiono kilka WAT-owskich wynalazków bazujących na rozwiązaniach tego typu.
Słowa kluczowe: algebra, bezpieczeństwo, struktura algebraiczna, ciało skończone, ciało skończone rozszerzone, teoria Galois, kryptografia.

1. Matematyka w naukach o bezpieczeństwie

Ewolucja rozwoju samej matematyki, a następnie wykorzystanie jej metod badawczych w innych dyscyplinach naukowych ma swoją odległą i odrębną historię. Sięgając do czasów starożytnych, a konkretnie do poglądów filozoficznych, warto wspomnieć, że według teorii pitagorejczyków wszystko na świecie było powiązane z liczbami. Odpowiedni ich układ miał wyrażać np. sprawiedliwość, inny odzwierciedlał duszę i umysł, a jeszcze inny miał symbolizować czas. Uważali oni, że pierwiastki liczb są reprezentantami wszystkiego, co istnieje, natomiast sam wszechświat utożsamiany był przez nich z harmonią i liczbą. Wiele wieków później Galileusz wyraził pogląd, że księga przyrody jest zapisana językiem matematyki. Współcześnie uważa się, że dzięki empiryczno-matematycznym metodom ludzkość ma możliwość wykradania naturze jej tajemnic[1].

W obecnych czasach znajomość matematyki jest potrzebna każdemu człowiekowi. Wystarczyłoby zabrać ludziom komputery i telefony komórkowe, a nie potrafiliby bez nich funkcjonować. To, że urządzenia te działają, jest zasługą nie tylko elektroniki, ale przede wszystkim matematyki, która nie bez powodu jest

[1] A. Staszel, *Problemy społeczne, polityczne i prawne. Zastosowanie metod matematycznych w naukach społecznych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", Kraków 2013, https://zeszyty-naukowe.uek.krakow.pl/article/view/730 (18.04.2016).

nazywana królową nauk. Trudno wskazać inną tak wszechstronną dyscyplinę, która jest obecna niemalże wszędzie. Matematykę warto znać choćby dla własnego bezpieczeństwa, np. podczas zakupów w sklepie. Nauka ta przede wszystkim rozwija logiczne myślenie oraz pomaga rozwiązywać różnego rodzaju problemy. Mamy z nią do czynienia w sztuce malarskiej, muzyce, przyrodzie, kuchni, a nawet w naukach o bezpieczeństwie[2].

Ponadto, elementy matematyczne mogą być pomocne przy wyborze kandydata na pracownika, w negocjowaniu wynagrodzenia, czy w planowaniu podróży. Pozwalają one zweryfikować, która lokata oszczędnościowa jest najkorzystniejsza a nawet pomagają w rozwiązywaniu zawiłych spraw kryminalnych. Notowania giełdowe, budowa kwiatów, klasyczna architektura, czy rozmnażanie się pszczół – to wszystko powiązane jest z matematycznym zagadnieniem, jakim jest ciąg liczbowy zwany ciągiem Fibonacciego.

Powyższe przykłady oraz wiele innych, których nie sposób tutaj wymienić, pokazują, że rola matematyki wykracza poza jej potoczne rozumowanie. Wraz z upływem czasu jej funkcje i znaczenie nie uległy zmniejszeniu w życiu społecznym, wręcz przeciwnie. Przykładowo: wiedza z zakresu teorii gier jest wykorzystywana w biznesie i negocjacjach, elementy probabilistyki są stosowane w branży ubezpieczeniowej, teoria liczb jest wykorzystywana w kryptografii w systemach bezpieczeństwa, natomiast prognozowanie i symulacja mogą mieć zastosowanie w naukach o bezpieczeństwie przy badaniu i prognozowaniu niekorzystnych zjawisk. Można zatem stwierdzić, że „…granice naszego świata są granicami matematyki…"[3].

Matematyka stanowi więc nieodzowne narzędzie badawcze w naukach społecznych i nie tylko. W początkach XXI w. naukowcy uświadomili sobie, że bezpieczeństwo jako przedmiot badań ma charakter transdyscyplinarny. Trafne opisywanie i wyjaśnianie zdarzeń oraz procesów na różnych płaszczyznach bezpieczeństwa pociąga za sobą wykorzystanie wiedzy z różnych dyscyplin naukowych, np. z zakresu nauk przyrodniczych, ścisłych czy technicznych. Jest to duże wyzwanie dla osób zajmujących się badaniem problemów dotyczących bezpieczeństwa, które wykazują charakterystyczną specyfikę pojęciową oraz osobliwe metody, techniki, a także narzędzia badawcze[4].

W naukach o bezpieczeństwie ważną funkcję pełni nie tylko opis zdarzeń, lecz także powiązania pomiędzy poszczególnymi ich elementami. Istotne znaczenie ma tutaj również analiza procesów, jakie tam zachodzą. Wymienione składowe są

[2] http://www.gp24.pl/wiadomosci/slupsk/art/4848421,matematyke-warto-znac-dla-bezpieczenstwa-rozmowa-z-grazyna-kwiecinska,id,t.html (17.04.2016).

[3] http://olsztyn.naszemiasto.pl/artykul/niedostepna-krolowa-nagroda-banacha,871372,art,t,id,tm.html (17.04.2016).

[4] https://www.cnbop.pl/wydawnictwa/ksiazki/978-83-61520-26-9/bezpieczenstwo.-teoria-badadnia-praktyka.pdf (18.04.2016).

niezbędnym warunkiem przy podejmowaniu racjonalnych i efektywnych decyzji. Możliwość zastosowania elementów metod matematycznych sprzyja więc liczbowemu wyrażaniu i opisywaniu przedmiotów obserwacji podczas prowadzonych badań[5].

Stosowanie języka matematyki w naukach o bezpieczeństwie jest zatem niezbędnym elementem w procesie formułowania problemów teoretycznych, w zrozumieniu skomplikowanych zależności, przy pomiarze zmiennych, czy wreszcie w szacowaniu parametrów oraz wyciąganiu wniosków. Matematyzacja wiedzy w zakresie nauk o bezpieczeństwie to między innymi: matematyczne ujęcie wyników poznawczych oraz przedstawienie rezultatów w formie liczbowej. Takie podejście metodologiczne może wykorzystywać elementy analizy matematycznej, metody statystyczne czy rachunek prawdopodobieństwa. Przykładem matematycznego podejścia w naukach o bezpieczeństwie może być upodabnianie struktury poszczególnych teorii do teorii matematycznych, a konkretnie nadanie im charakteru zaksjomatyzowanych systemów dedukcyjnych.

Ogólnie rzecz ujmując, można zauważyć powszechną matematyzację języka nauki. Podczas opracowywania wyników obserwacji oraz pomiarów w naukach społecznych, np. przy poznawaniu zależności pewnych cech, wprowadza się współczynnik korelacji. Często w naukach o bezpieczeństwie zachodzi konieczność badania procesów decyzyjnych. Wówczas przydatnym narzędziem okazują się wspomniane wcześniej: teoria gier, programowanie, teoria decyzji statystycznych czy struktury macierzowe. Stosując teorię estymacji, można badać rozkłady cech, a modele matematyczne służą do opisu rzeczywistości. Wykorzystując np. elementy dynamiki systemowej, można zasymulować przebieg niekorzystnych zjawisk, takich jak np. rozprzestrzenianie się ptasiej grypy czy przewidywanie zagrożenia powodziowego.

Nauki o bezpieczeństwie w wielu płaszczyznach badawczych mogą wykorzystywać różnego rodzaju modele matematyczne do opisu i modelowania zjawisk rzeczywistych. Mogą to być modele oparte np. o funkcję charakterystyczną czy analizę graficzną obiektów. Ponadto zastosowanie znajduje tu również język cybernetyki, gdzie istotną funkcję odgrywają narzędzia matematyczno-informatyczne. Mogą być one wykorzystywane do budowy systemów wspomagania podejmowania decyzji, np. w sektorze zarządzania kryzysowego, lub stosowane w kryptografii w systemach bezpieczeństwa informacyjnego.

Warto zatem podkreślić, że stosowanie matematyki w naukach społecznych, a konkretnie w badaniach nad bezpieczeństwem, pełni niezwykle pomocną funkcję w zrozumieniu zależności i powiązań pewnych faktów, a przede wszystkim daje precyzję i zwięzłość języka przy przetwarzaniu i interpretowaniu wyników niezbędnych do poprawnego zweryfikowania postawionej wcześniej hipotezy[6].

---

[5] https://repozytorium.umk.pl/bitstream/handle/item/1896/WST%C4%98P.doc?sequence=1 (18.04.2016).

[6] A. Staszel, *Problemy społeczne, polityczne i prawne. Zastosowanie metod matematycznych w naukach społecznych*, op. cit., Kraków 2013, https://zeszyty-naukowe.uek.krakow.pl/article/view/730

2. Początki myśli matematycznej

2.1. Wprowadzenie do historii matematyki

Jedno z założeń naukowych twierdzi, że matematykę zrodziła zwykła ciekawość świata i tego, co jest poza nim. Początki tej nauki sięgają czasów prehistorycznych, a o jej wieku świadczy choćby to, że kiedy ok. 30 000 lat p.n.e. pojawiły się pierwsze cywilizacje, matematyka już była tam obecna. Powiązana z myślą religijną, filozoficzną i astronomiczną, stanowiła z nimi nierozerwalną całość. Wyodrębnienie jej jako autonomicznej dziedziny i nadanie nazwy „matematyka" miało miejsce ok. 5000 lat p.n.e. i było zasługą greckich filozofów. Dawniej matematyka swoją pozycję zawdzięczała specyficznej atrakcyjności oraz użyteczności, obecnie służy do poznawania świata i jest wykorzystywana m.in. w ekonomii oraz technice. Można powiedzieć, że matematyka stała się trwałym elementem naszej kultury[7].

Według opinii historyków, elementy matematyki najwcześniej pojawiły się na gruncie rytualno-mitologicznym. Ówczesne tańce powiązane z obrzędami wyróżniały takie figury jak: kwadrat, prosta czy koło, a rytuały stwarzania nakazywały nazywać kolejnych ich uczestników. Przypuszcza się, że mogły to być elementy, które zapoczątkowały proces liczenia. Inspiracją narodzin matematyki mogły też być obserwacje nocnego nieba, czego dowodzi znaleziona kość pochodząca z Blanchard, na której został utrwalony zapis zmian faz Księżyca z kolejnych 69 nocy. Ostatnie odkrycia dowodzą tego, że to właśnie matematyka poprzedzała alfabetyzację, a nie odwrotnie.

Różnorodność cywilizacji starożytnych miała znaczący wpływ na odmienność źródeł matematyki oraz sposoby zapisywania liczb i opisywania figur. Jednak idea tej wiedzy wszędzie była taka sama, gdyż u jej źródeł w różnych kulturach leżała ta sama rzeczywistość, jaką była filozofa przyrody.

2.2. Matematyka starożytnego Egiptu

Jedną z pierwszych kultur, która w odizolowaniu od pozostałej części świata rozwijała myśl matematyczną, była kultura starożytnego Egiptu. Matematycznych tekstów tego dziedzictwa zachowało się jednak niewiele, a wszystko, co o nich wiadomo, pochodzi w większości z odnalezionego papirusu Rhinda. Tytułowy początek tego zwoju brzmi: „Reguły badania wszystkich rzeczy i poznania wszystkiego, co istnieje, każdej ukrytej tajemnicy...". Z zapisków na papirusie wiadomo, że ówcześni Egipcjanie mieli dość dobrze opracowany sposób zapisywania liczb, gdzie podstawowymi znakami były: dziesiątki tysięcy, tysiące, setki, dziesiątki oraz jedności. Ciekawostką jest to, że pismo egipskie czyta się od strony prawej do lewej[8].

(18.04.2016).

[7] http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1887&chapterid=10879 (27.02.2016).

[8] Ibidem.

Rys. 2.2.1. Cyfry zapisane w notacji egipskiej
Źródło: http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1887&chapterid=10879 (27.02.2016)

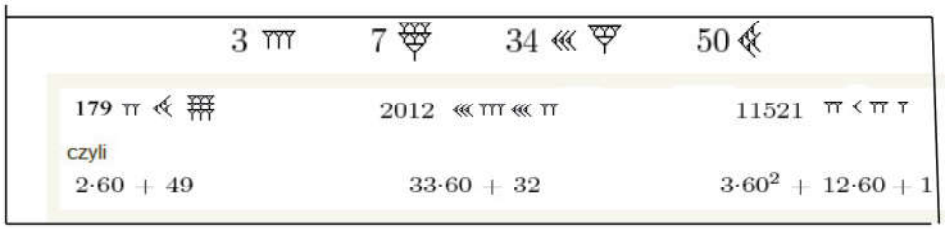
Osobliwością egipskiej matematyki były również ułamki naturalne postaci $1/n$. Uprawiane techniki zapisu liczb, ułamków naturalnych oraz stosowanie addytywnych metod rachunkowych pozwoliły tej kulturze rozwinąć prostą arytmetykę. Nie była im obca również znajomość geometrii, czego dowodem jest dokładność w obliczaniu pól i objętości figur oraz brył prostych. Arytmetyka i geometria były zatem zbiorem sposobów rozwiązywania zadań o różnym stopniu trudności, co w tamtej kulturze miało ogromne znaczenie praktyczne[9].

2.3. Matematyka starożytnej Babilonii

W przeciwieństwie do egipskiego odizolowania i spokoju zewnętrznego, region dorzecza Tygrysu i Eufratu co kilkaset lat padał ofiarą kolejnych najeźdźców. Pomimo burzliwych dziejów politycznych tamtejszego obszaru, narodziła się tam wysoka kultura, nazywana później kulturą babilońską. Wiedza o niej pochodzi głównie z tabliczek glinianych, zapisanych pismem klinowym, z czego część z nich to tabliczki z tekstem matematycznym[10].

Charakterystyczną cechą babilońskiej matematyki był sześćdziesiątkowy system zapisu liczb. Osiągnięcia matematyczne związane z tym systemem przyczyniły się do znacznego rozwoju astronomii, arytmetyki oraz algebry. Z analizy tabliczek wiadomo, że Babilończycy znali szczególny przypadek twierdzenia, które obecnie nazywa się twierdzeniem Pitagorasa. Ponadto posługiwali się oni znakomitą techniką rachunkową, która pozwalała im określić dość dobre przybliżenie liczby $\sqrt{2}$. Ślady babilońskiego systemu sześćdziesiątkowego przetrwały do czasów współczesnych, a znajdują zastosowanie głównie w mierzeniu czasu oraz kątów brył[11].

[9] http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1887&chapterid=10879 (27.02.2016).
[10] http://www.math.us.edu.pl/prace/liczba/okres2/okres2.html (28.02.2016).
[11] http://www.swiatmatematyki.pl/index.php?p=145 (29.02.2016).



Rys. 2.3.1. Liczby w notacji babilońskiej
Źródło: http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1887&chapterid=10879 (27.02.2016)

2.4. Matematyka starożytnych Indii

Kolejna ważna kultura obecna w dziejach myśli matematycznej to cywilizacja z doliny rzeki Indus w III tysiącleciu przed Chrystusem. Tamtejsi uczeni znali prostą arytmetykę oraz geometrię. W wyniku uporczywych najazdów przez plemiona pasterzy aryjskich w I tysiącleciu p.n.e. najeźdźcy wdrożyli własną kulturę w tamtym regionie, a następnie wskutek inwazji aryjskich Greków na Jonię oraz półwysep grecki narodziła się wielka kultura Indii. Charakteryzowała się ona silnym nacechowaniem religijnym, z którym nierozerwalnie związane były elementy matematyki, astronomii oraz sacrum.

W Indiach powstał wówczas dziesiętny liczbowy system pozycyjny oraz rozwinęły się podstawy rachunku, którymi posługujemy się do dziś. Hinduskiej matematyce należy także zawdzięczać utworzenie cyfr „arabskich", które to Arabowie wprowadzili do powszechnego użytku, a następnie przejęła je od nich matematyka europejska, nazywając „cyframi arabskimi" od pośrednika, a nie od twórcy. Hindusi rozpowszechnili także cyfrę zero, która na początku powiązana była ze słowem „pusto", następnie wyrażana zapisem kropki, a ostatecznie przyjęła notację małego spłaszczonego kółka.

Ponadto cywilizacja hinduska posługiwała się również kilkoma ułamkami oraz potrafiła liczyć pierwiastki kwadratowe i sześcienne. Wysoki poziom osiągnęły indyjskie postępy w kierunku algebry, gdzie stosowano jej symbolikę. Zapisywano np. liczby ujemne, interpretując je następująco: liczba dodatnia – jako majątek, liczba ujemna – jako dług, a także wprowadzono niewymierności kwadratowe. Hindusi jako pierwsi sformułowali też reguły działań arytmetycznych, które obowiązują do dziś[12].

[12] http://www.math.us.edu.pl/prace/liczba/okres6/okres6.html (28.02.2016).

2.5. Matematyka starożytnej Grecji

Nieco inny charakter miała matematyczna kultura grecka, która skupiała się początkowo wokół nazwiska Talesa. Matematykę egipską oraz babilońską uważano wówczas za mało użyteczną, gdyż ówcześnie wykorzystywano ją głównie do celów praktycznych, co wiązało się ściśle z potrzebami życia codziennego. Skłonności filozoficzne Greków sprowadzały się raczej do szukania istoty rzeczy poprzez uzasadnienia, a nie tylko do praktycznego ich wykorzystywania. Uznawali oni na przykład, że dwa sprzeczne zdania nie mogą być jednocześnie zdaniami prawdziwymi, co można było zauważyć w praktykach matematycznych Egipcjan i Babilończyków[13].

Wybitnym uczonym w tym względzie okazał się Tales. Zapoczątkował on używanie pojęć ogólnych oraz stosowanie procesu uzasadniania. W greckiej myśli matematycznej stosowano bardzo proste formy dowodzenia sądów. Był to pierwszy ważny krok w kierunku nowej matematyki, ponieważ przekroczono wówczas granicę pomiędzy matematycznymi umiejętnościami praktycznymi wcześniejszych kultur a matematyką postrzeganą jako nauka pomiędzy konkretem i ogólnością.

Około VI w. p.n.e. wielki uczony Parmenides po raz pierwszy świadomie zastosował rozumowanie dedukcyjne, wywodząc całą wiedzę z przesłanek ogólnych. Jemu również należy zawdzięczać stosowanie metody rozumowania nie wprost, a konkretnie przez sprowadzenie do niedorzeczności. Zasługą Greków jest także odkrycie oraz sformułowanie niektórych podstawowych zasad myślenia matematycznego, które są stosowane do dziś. Zaliczymy do nich: zasadę sprzeczności, zasadę wyłączonego środka oraz zasadę podwójnego przeczenia. Osobliwością Greków było również to, że nazywali oni liczby w sposób dziesiętny, co później przejęła średniowieczna Europa. Stosowano wówczas zaprezentowany na rysunku poniżej attycki system zapisu liczbowego.

I	jedność
Γ	pięć (pente)
Δ	dziesięć (deka)
H	sto (hekaton)
X	tysiąc (chilioi)
M	dziesięć tysięcy (mirioi)
$\Gamma IIII$	9
$XX\Delta II$	2012
$XXX\Gamma^{H}H\Gamma^{\Delta}\Delta\Delta\Gamma II$	3677

Rys. 2.5.1. Attycki system zapisu liczb greckich
Źródło: opracowanie własne na podstawie: http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016)

[13] http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016).

W V w. p.n.e. pojawił się nowy dziesiętny system liczbowy, zwany jońskim, który w niedługim czasie wyparł system attycki. Był on używany do końca czasów starożytnych. Wadą tych dwóch systemów było jednak to, że za ich pomocą nie można było zapisywać ułamków oraz nie były one dostosowane do potrzeb rachunkowych. Powodem tego mógł być fakt, że matematyka grecka była nauką opartą na pojęciach ogólnych i dowodzeniu, a nie na arytmetyce. Zastosowania praktyczne pozostawiano raczej kupcom, rachmistrzom oraz innym zainteresowanym[14].

I tak dla przykładu: astronomowie posługiwali się wówczas metodami rachunkowymi Babilończyków, a ludzie w życiu codziennym do liczenia wykorzystywali popularny przyrząd zwany αβαξ, w tłumaczeniu abak, który stał się później prototypem współczesnych liczydeł. Abaki nie stanowiły wówczas jedynego sposobu liczenia przez ówczesnych Greków. Z czasem dla jońskiego systemu liczbowego zaczęto wprowadzać algorytmy rachunkowe, np. dla: dodawania, odejmowania, mnożenia oraz dzielenia, a także pierwiastkowania drugiego stopnia. Rysunek poniżej przedstawia joński system liczbowy.

Θ	9
' *BIB*	2012
'ΘΩ*OZ*	3677

Rys. 2.5.2. Joński system zapisu liczb greckich
Źródło: opracowanie własne na podstawie: http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016)

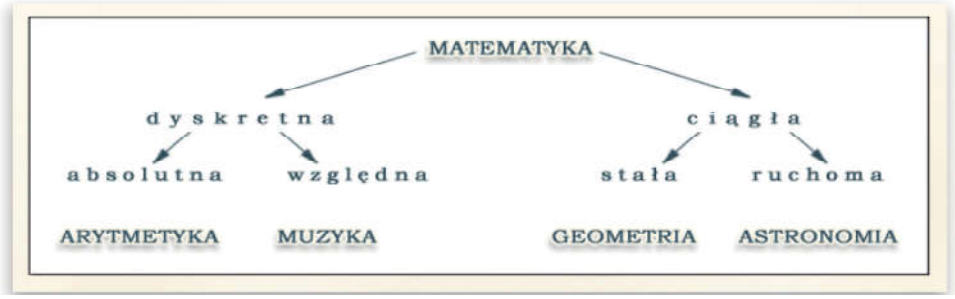
W rozwoju greckiej myśli matematycznej ważną postacią okazał się także Pitagoras oraz jego uczniowie, którzy uczynili z tej dyscypliny samodzielną dziedzinę nauki, a następnie znakomicie ją rozwinęli. Głównym obiektem ich zainteresowań było pojęcie liczb (naturalnych i wymiernych), a szczególnie ich własności, które utożsamiano z kształtami geometrycznymi. Wyróżniano więc: liczby parzyste, trójkątne, kwadratowe i pięciokątne, a także wyłoniono własne liczby pierwsze. Wiążąc kształt liczb z polem figur, Pitagorejczycy otrzymywali ciekawe wzory sumacyjne.

Niemałą zasługą Greków okazało się też odkrycie związków pomiędzy liczbami a: harmonią sfer, dźwiękami muzycznymi oraz przestrzennymi kształtami. Odkrycia te wskazywały na harmonijną konstrukcję świata, która według Greków była poznawana matematycznie. Stąd też nadali oni temu światu nazwę κοσμος, w tłumaczeniu kosmos, czyli ład.

Przekonanie o harmonii bytu w niedługim czasie zostało jednak zachwiane, kiedy odkryto wielkości niewspółmierne. Był to wówczas bodziec do tego, aby zacząć uprawiać matematykę w języku geometrii. Pitagorejczykom matematyka zawdzięcza

[14] http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016).

swoje świadome istnienie i jest uważana za narzędzie poznawania świata. Została też sklasyfikowana oraz uzyskała własną nazwę „matematyka", która ma dziś jasno określony cel oraz metody badawcze[15].



Rys. 2.5.3. Klasyfikacja matematyki wg Greków
Źródło: http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016)

2.6. Teoria Euklidesa

Ważną postacią w dziejach kultury Greków był również Euklides – człowiek, który dokonał syntezy ówczesnej matematyki greckiej, a jego słynne dzieło *Elementy* stanowiło podstawowy podręcznik z zakresu geometrii. Przedstawiona w nim teoria stanowi również obecnie ważny dział matematyki. Szczególną zaletą dzieła było to, że wyrażając podejście dość abstrakcyjne, nie zawierało ono żadnych zbędnych ozdobników, obejmując jednocześnie cały dotychczasowy dorobek matematyki greckiej. W czasach obecnych przedstawiona teoria nosi miano „geometrii euklidesowej".

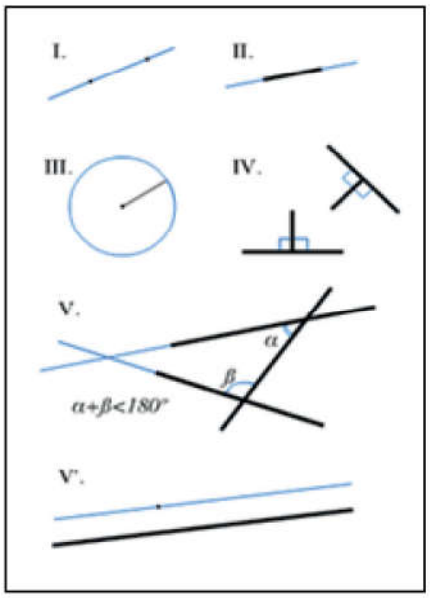
Słynne dzieło składało się z trzynastu ksiąg, z czego kilka pierwszych dotyczyło planimetrii, czyli geometrii płaszczyzny. Pierwsza z nich poświęcona była określeniom, postulatom oraz aksjomatom, a także 48 twierdzeniom dotyczącym elementarnych konstrukcji geometrycznych. Wprowadzone podstawowe określenia można traktować obecnie jako pierwowzór pierwszych prostych definicji, np. dla punktu, linii, powierzchni czy okręgu. Terminy te Euklides traktował jako coś zupełnie naturalnego, czyli pierwotnego. Wprowadzone przez niego postulaty stanowiły specyficzne założenia teorii geometrycznej, natomiast aksjomaty były traktowane jako oczywiste założenia. Wśród zaprezentowanych twierdzeń swoje miejsce ma również proste oraz odwrotne twierdzenie Pitagorasa.

Kolejne księgi *Elementów* opisywały algebrę grecką, lecz w języku geometrii. Można było w nich znaleźć teorię liczb rzeczywistych oraz własności podobieństwa figur. Ponadto Euklides sporo miejsca poświęcił na ważne twierdzenia dotyczące: liczb naturalnych oraz

[15] http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016).

teorii stereometrii, czyli geometrii przestrzeni[16]. Matematyk dowiódł istnienia (możliwość skonstruowania za pomocą cyrkla i liniału) niektórych brył foremnych[17].

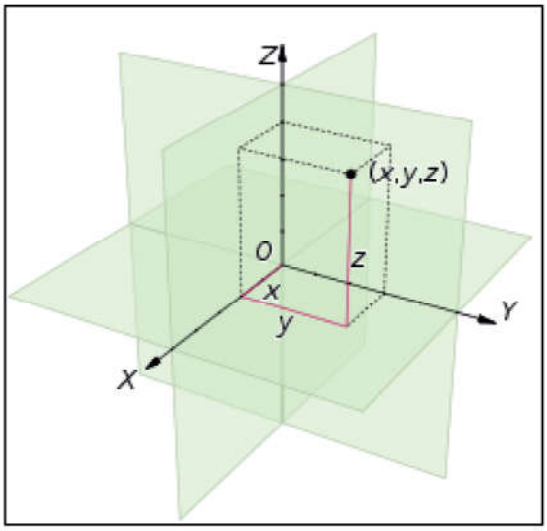
W ujęciu tradycyjnym geometria euklidesowa jest prezentowana jako system aksjomatyczny, w którym wszystkie twierdzenia powinny wynikać z aksjomatów, czyli ze zdań traktowanych z góry jako prawdziwe. Uczony w swoim systemie wyróżnił pięć podstawowych aksjomatów płaszczyzny, nazywanej później płaszczyzną euklidesową. Rysunek poniżej ilustruje aksjomaty Euklidesa.



Rys. 2.6.1. Aksjomaty Euklidesa
Źródło: https://www.google.pl/search?q=aksjomaty+euklidesa&newwindow (29.02.2016)

W podejściu współczesnym geometria euklidesowa jest postrzegana przez pryzmat modelu, jakim jest przestrzeń kartezjańska oparta na analizie matematycznej. Pozwala to na sprowadzenie twierdzeń geometrycznych do postaci liczbowej, co znacznie upraszcza ich dowodzenie. Takie podejście nazywamy geometrią analityczną. Współcześnie przestrzeń euklidesowa, wyrażona w postaci przestrzeni kartezjańskiej, jest postrzegana jako naturalny element modelu świata rzeczywistego. Punkt jest tutaj traktowany jako zerowymiarowa przestrzeń euklidesowa, jednowymiarowa przestrzeń nazywana jest prostą euklidesową, natomiast przestrzeń dwuwymiarowa to płaszczyzna euklidesowa itd.

[16] Ibidem.
[17] Ibidem.



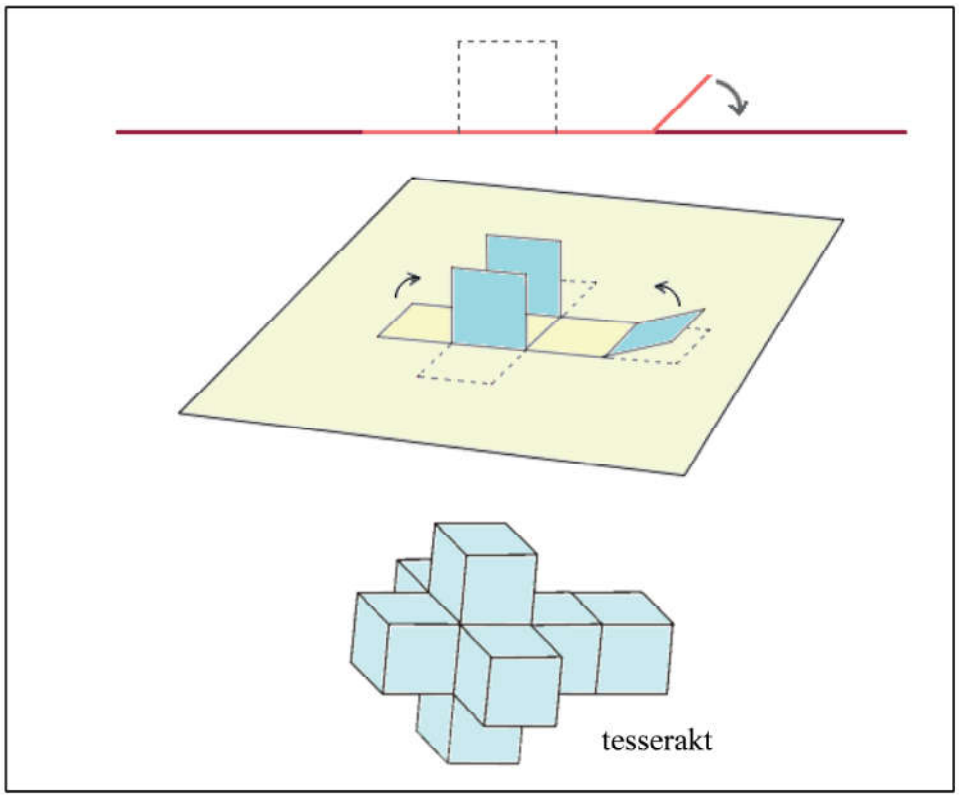
Rys. 2.6.2. Trójwymiarowa przestrzeń współrzędnych rzeczywistych
Źródło: https://www.google.pl/search?q=przestrze%C5%84+tr%C3%B3jwymiarowa&newwindow (29.02.2016)

Cechą charakterystyczną przestrzeni euklidesowej jest jej płaskość. W rzeczywistości istnieje dokładnie jedna przestrzeń euklidesowa każdego wymiaru. W geometrii można również spotkać przestrzenie nieeuklidesowe, np. płaszczyzna sfery, którą uzyskuje się poprzez deformację przestrzeni euklidesowej[18].

Tradycyjna geometria euklidesowa działa tylko na przestrzeniach niezakrzywionych. Chociaż człowiek żyjący w przestrzeni trójwymiarowej nie może wyobrazić sobie świata o większej liczbie wymiarów, to z matematycznym opisem takich przestrzeni nie ma większych problemów. Przykładowo długość przekątnej kwadratu o boku a wynosi $d=\sqrt{a^2+a^2}=\sqrt{2}a$, przekątna sześcianu o boku a przyjmuje wartość $d=\sqrt{a^2+a^2+a^2}=\sqrt{3}a$, natomiast przekątna odpowiedniej bryły z przestrzeni czterowymiarowej o boku a to $d=\sqrt{a^2+a^2+a^2+a^2}=\sqrt{4}a=2a$. Ciekawostką jest fakt, że bryłę taką można sobie wyobrazić jako formę ograniczoną ośmioma sześcianami. Słynny angielski fizyk Charles Hinton, wymyślając metody umożliwiające wyobrażenie sobie czterowymiarowych obiektów, wprowadził do użytku termin „tesserakt" na określenie rozwinięcia czterowymiarowego hipersześcianu w przestrzeni trójwymiarowej[19].

[18] http://slideplayer.pl/slide/421188/ (29.02.2016).
[19] http://www.gnosis.art.pl/e_gnosis/paradygmat_wyobrazni/uspienski_4ty_wymiar.htm (29.02.2016).

Snując własne wyobrażenia na temat przestrzeni wyższych stopni, można powiedzieć, że hipotetyczne istoty jednowymiarowe żyjące na linii prostej nie są w stanie wyobrazić sobie płaszczyzny, czyli figury dwuwymiarowej. Ich światem jest tylko linia prosta, na której w danej chwili może znajdować się tylko jeden z boków figury dwuwymiarowej, np. kwadratu. Natomiast rozwinięcie tego kwadratu do postaci czterech odcinków może już być w całości umieszczone na tej prostej. Analogicznie, rozwinięcie bryły trójwymiarowej, np. sześcianu, może być umieszczone na płaszczyźnie, czyli w przestrzeni dwuwymiarowej. Idąc dalej tym tropem, można zauważyć, że rozwinięcie bryły czterowymiarowej, np. tesseraktu, może być umieszczone w przestrzeni trójwymiarowej itd. Na rysunku poniżej przedstawiono hipotetyczne rozwijanie danej przestrzeni do przestrzeni większego wymiaru[20].



Rys. 2.6.3. Rozwijanie przestrzeni do wyższych wymiarów
Źródło: http://jknow.republika.pl/fizyka/riemann.html (29.02.2016)

[20] http://jknow.republika.pl/fizyka/riemann.html (29.02.2016).

Podsumowując greckie osiągnięcia na gruncie matematyki, można zauważyć, że celem tamtejszej filozofii była nauka pewna, dla której został określony odpowiedni ład. Na początku wyróżniono przesłanki, czyli aksjomaty oraz postulaty, następnie zamieszczono wyraźne określenia używanych pojęć, tzn. definicje. Dalej miejsce przypisano twierdzeniom, które wyrażały związki pomiędzy tymi pojęciami, i na końcu wprowadzono dowody tych twierdzeń, które zostały oparte na prawach logiki. Wzorcową realizacją takiego kanonu było właśnie dzieło Euklidesa *Elementy*. Sprawiło ono, że geometria euklidesowa stała się wzorem wiedzy pewnej oraz podstawą całej matematyki. Organizacja tej wiedzy na wzór geometrii euklidesowej stała się ideałem po wszystkie czasy: „*ordine geometrico demonstrata*"[21].

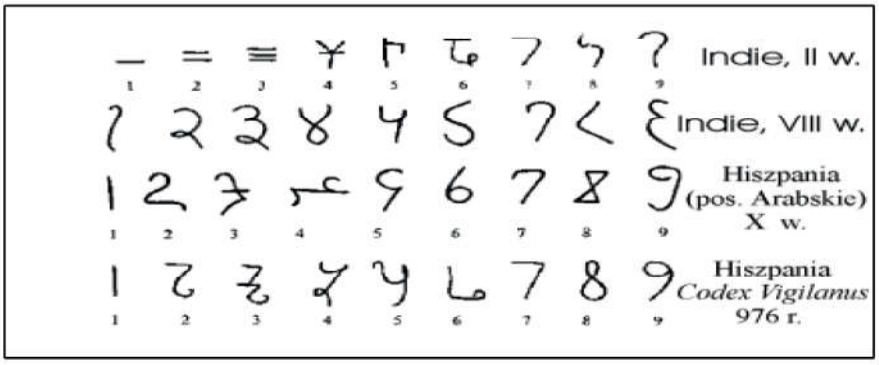
2.7. Matematyka w kulturze perskiej

Matematyczny świat nauki z okresu starożytności przez kilka wieków wchodził w czasy nowożytne. Wraz z upadkiem Cesarstwa Rzymskiego cały dorobek matematyki greckiej w Europie popadł prawie całkowicie w zapomnienie. To co zostało ocalone, a następnie rozwijane, należy zawdzięczać Arabom, a szczególnie kalifom muzułmańskim. Tamtejsi uczeni przetłumaczyli wiele matematycznych tekstów indyjskich oraz greckich na język arabski, zapobiegając w ten sposób całkowitej ich utracie. We wczesnym średniowieczu to Persja stanowiła naukowe centrum świata arabskiego i właśnie stamtąd pochodzi wielu wybitnych arabskich matematyków.

Jednym ze znakomitych uczonych perskiego pochodzenia (przełom VIII i IX w. n.e.) był Al-Chuwarizmi, autor kilku oryginalnych dzieł. Wprowadził on dziewięć hinduskich cyfr oraz oznaczył cyfrę zero symbolem kółka. Ponadto zapoczątkował pojęcie: ułamka, funkcji sinus i tangens oraz ułożył dla nich tablice. Al-Chwarizmi zaproponował także algorytmy dla podstawowych działań arytmetycznych. Z jego dzieł do użytku powszechnego przyjęła się symbolika cyfr arabskich, a sam autor dał początek dwóm pojęciom: „algebra" oraz „algorytm".

Kolejną ważną postacią kultury arabskiej był Bakr al-Karaj, który wprowadził pojęcia potęgi oraz pierwiastka całkowitego, a także po raz pierwszy zastosował zasadę indukcji matematycznej do przeprowadzenia dowodu. Postępy te i inne miały znaczny wpływ na rozwój algebry oraz geometrii. Wprowadzono wówczas wzór na sumę czwartych potęg, a następnie uogólniono go na sumę potęg dowolnych. Ponadto skonstruowano tablicę liczb, nazywaną dzisiaj trójkątem Pascala, co było początkiem późniejszego rozwoju rachunku całkowego[22].

[21] http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888 (27.02.2016).
[22] http://www.harcownik24.pl/2015/06/historia-matematyki-na-bliskim-wschodzie (1.03.2016).



Rys. 2.7.1. Zapis dziesiętny liczb na przestrzeni wieków
Źródło: http://www.harcownik24.pl/2015/06/historia-matematyki-na-bliskim-wschodzie (1.03.2016)

Wśród wielu arabskich wynalazków matematycznych, których nie sposób teraz wymienić, warto wyróżnić jeszcze jedno praktyczne udogodnienie, jakim było zastosowanie separatora dziesiętnego, oddzielającego część całkowitą od ułamkowej. Rysunek poniżej przedstawia symbol separatora arabskiego, zwanego „momayyez".

Rys. 2.7.2. Arabski separator dziesiętny
Źródło: http://www.harcownik24.pl/2015/06/historia-matematyki-na-bliskim-wschodzie (1.03.2016)

Około XI w. arabska nauka osiągnęła swój zenit: wprowadzono notację arabską, rozwinięto trygonometrię oraz geometrycznie rozwiązywano niektóre zadania równoważne równaniom trzeciego stopnia. Wiek XII przyniósł jednak stagnację i zahamowanie muzułmańskiej kultury matematycznej. Państwa arabskie skierowały wówczas swoje wysiłki w kierunku rozwoju politycznego, związanego ściśle z fanatyzmem religijnym[23].

[23] Ibidem.

3. Istota algebry abstrakcyjnej

3.1. Narodziny teorii Galois w kontekście rozwoju myśli algebraicznej

Elementy klasycznej teorii Galois mieszczą się w obszarze algebry abstrakcyjnej. Jednak zanim doszło do rozkwitu tej teorii w końcowej, abstrakcyjnej postaci, sama algebra przeszła wielką metamorfozę, począwszy od czasów prehistorycznych aż do chwili obecnej.

Algebra, jak wiadomo, jest nierozerwalną częścią matematyki ogólnej i podobnie jak matematyka ma długą historię, której początki sięgają czasów starożytnych. Istnieją dowody na to, że dawne cywilizacje odkryły wiele elementów, które wiązały się z tą nauką. Pierwsze pisemne wzmianki dotyczące zgłębiania tajników algebry pochodzą z ok. XX w. p.n.e. ze Starożytnej Babilonii, która tę wiedzę przejęła po Sumerach. Zachowały się stamtąd kamienne tabliczki, na których uczeni zapisywali znaki utożsamiane z dzisiejszą algebrą.

W dużo późniejszych czasach, bo w III w. n.e., sławę zdobył uczony pochodzenia greckiego – Diophantos, mieszkający w Aleksandrii, który jest uważany przez zachodnich historyków za twórcę myśli algebraicznej, gdyż swoje rozważania skupiał głównie na konkretach związanych z tą nauką.

Na przełomie VI i VII w. n.e. pojawia się kolejna ważna postać w dziejach algebry. Jest to hinduski matematyk Brahmagupta, który jako pierwszy wprowadza elementarną postać notacji algebraicznej, a także pojęcie zera oraz liczb ujemnych.

Z etymologicznego punktu widzenia algebra to arabskie słowo pochodzące z księgi *Al-Kitab al-mukhtasar fi hisab al-gabr wa'l-muqabala*, której tytuł w wolnym tłumaczeniu brzmi *Księga kompletna o liczeniu z użyciem uzupełniania i równoważenia*. Została ona napisana przez wspomnianego wcześniej perskiego matematyka Al-Chuwarizmiego, mieszkającego w Bagdadzie na przełomie VIII i IX w. n.e.[24]

Słowo „al-gabr" oznacza tu przywracanie albo uzupełnianie. W przytoczonej księdze „uzupełnianie" to konkretna technika, która odnosi się do przenoszenia czegoś z jednej strony równania na drugą. Księga uważana jest za pierwsze bardzo ważne dzieło, w którym algebra nabrała współczesnego znaczenia, również w kierunku abstrakcyjnym.

Al-Chuwarizmi, tworząc swoją księgę, nie tylko korzystał z wiedzy babilońskiej, lecz także wiele do niej dołożył, dając początek współczesnej algebrze. Ten uczony bezdyskusyjnie jest twórcą pojęcia „algebra". On też jako pierwszy zaczął traktować algebrę abstrakcyjnie w oderwaniu od konkretnych zadań, czyli tak samo jak czynią to współcześni matematycy[25].

---

[24] https://pl.khanacademy.org/math/algebra/introduction-to-algebra/overview_hist_alg/v/origins-of-algebra (2.03.2016).

[25] https://pl.khanacademy.org/math/algebra/introduction-to-algebra/overview_hist_alg/v/origins-of-algebra (2.03.2016).

Rys. 3.1.1. Dzieło, z którego pochodzi określenie „algebra"
Źródło: www.google.pl/search?q=al-khwarizmi+algebra&tbm=isch&oq (2.03.2016)

Na przełomie XIX oraz XX w. n.e. algebra nabrała szerszego znaczenia, kiedy w obrębie jej rozważań pojawiło się wiele wątków abstrakcyjnych. Służyły one do wyrażania urojonych pojęć oraz praw. W rozwoju algebry abstrakcyjnej zapewne etapem pośrednim były również badania Galois, skupione wokół równań algebraicznych oraz pierwiastków wielomianów. Młody matematyk był twórcą teorii, która obecnie nosi miano teorii Galois i która wiele wniosła do matematyki współczesnej[26].

Algebra, obok geometrii, jest obecnie uważana za jeden z najstarszych działów matematyki. Jest nauką, która zajmuje się relacjami oraz strukturami powstałymi w wyniku definiowania działań w zbiorach. Do podstawowych takich struktur algebraicznych można zaliczyć m.in. grupy, pierścienie oraz ciała. Współczesna algebra abstrakcyjna jest samodzielną dyscypliną naukową wciąż intensywnie się rozwijającą, a wypracowane przez nią pojęcia i metody są stosowane w wielu innych dyscyplinach, w tym – niespodziewanie – mają liczne zastosowania praktyczne[27].

[26] W. Więsław, *Algebra w XX wieku. Rys historyczny*, „Roczniki Polskiego Towarzystwa Matematycznego", Seria II: „Wiadomości Matematyczne" XL, Wrocław 2004, s. 4.
[27] B. Siemieńska, *Podstawy teorii Galois*, UTH, Radom 2015, s. 7.

3.2. Ciała Galois

Wśród abstrakcyjnych pojęć algebraicznych, którymi posługuje się teoria Galois, występuje grupa oraz ciało. Oba te systemy mogą być rozpatrywane zarówno jako struktury skończone, jak też nieskończone. Pojęcie ciała skończonego, czyli ciała Galois, zostało wprowadzone do algebry w XIX w., a jego twórcą był francuski młody matematyk Evariste Galois, który zajmował się wówczas teorią równań algebraicznych.

Badania Galois sprowadzały się głównie do poszukiwania wzorów ogólnych służących do rozwiązywania równań wielomianowych stopnia wyższego niż 4. Teoria, którą stworzył, dowodzi silnej współzależności pomiędzy teorią grup a teorią ciał[28].

Klasyczna teoria Galois, w ostatecznej, abstrakcyjnej postaci, nie posiada bezpośredniego praktycznego zastosowania, ma ona raczej charakter czysto teoretyczny, jednakże pewne jej elementy są wykorzystywane w niektórych dziedzinach naukowych[29]. Dobrym tego przykładem mogą być wielomiany wysokich stopni oraz ciała skończone. Są one stosowane w kryptologii, która jest podstawą bezpieczeństwa np. systemów bankowych i związanych z nimi usług elektronicznych, które wiążą się np. z szyfrowaniem danych na kartach chipowych[30].

W kryptografii oraz teorii kodowania ważną funkcję pełnią wspomniane wcześniej systemy algebraiczne, do których zaliczymy: abelowe grupy addytywne, abelowe grupy multiplikatywne, pierścienie oraz ciała. Z uwagi na fakt, że zarówno w kryptografii, jak i w teorii kodowania stosuje się alfabety ze skończoną liczbą elementów, a liczba ta jest równa potędze liczby pierwszej, alfabet taki może być uważany za strukturę algebraiczną, która jest ciałem skończonym lub równoważnie ciałem Galois. Ciało takie oznaczamy symbolem

$$GF(p), \tag{1.1}$$

gdzie p jest liczbą pierwszą.

Ciało Galois $GF(p)$ jest strukturą algebraiczną, która składa się ze zbioru postaci $P = \{0,1,\ldots, p-2, p-1\}$ oraz z operacji dodawania $\oplus_p$ modulo p i mnożenia $\odot_p$ modulo p. System ten spełnia wszystkie aksjomaty ciała, tzn.:

- zbiór $(P, \odot_p)$ jest addytywną grupą abelową z zerem (0) względem ciała, gdzie $a \otimes_p b = a + b \ (mod\ p)$;
- zbiór $\left(P^*, \odot_p\right)$ jest grupą multiplikatywną z jedynką (1) względem ciała, gdzie $a \odot_p b = ab \ (mod\ p)$, $P^* = P \setminus \{0\}$;

[28] T.W. Judson, *Abstract Algebra. Theory and Applications*, Stephen F. Austin State University, 2009, s. 372.
[29] B. Siemieńska, *Podstawy teorii Galois*, op. cit., s. 98.
[30] Ibidem.

– mnożenie $\odot_p$ jest rozdzielne względem dodawania $\otimes_p$;
– ciało $GF(p)$ posiada minimum dwa elementy: 0 oraz 1.

Ciała te nazywane są również ciałami reszt modulo *p*.

Omówione powyżej skończone ciała proste oraz rozszerzenia tych ciał znajdują zastosowanie w systemach informatycznych związanych z bezpieczeństwem np. informacyjnym. Konstrukcja takiego ciała polega na utworzeniu zbioru jego elementów i wyznaczeniu tabliczek z dodawaniem oraz mnożeniem. Przykładowym ciałem prostym skończonym jest struktura $GF(5)$, której zbiór *P* ma postać $P = \{0, 1, 2, 3, 4\}$[31]. Na rysunku poniżej zamieszczono tabele działań dla $GF(5)$.

$\oplus_5$	**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

$\odot_5$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Rys. 3.2.1. Działania modulo 5
Źródło: opracowanie własne

Z ogólnych własności ciał wynika, że w ciele *p*-elementowym można wykonywać również inne działania, takie jak: odejmowanie, dzielenie, potęgowanie oraz pierwiastkowanie. W związku z powyższym nad ciałem Galois $GF(p)$ można także rozwiązywać równania liniowe oraz nieliniowe, dodawać, mnożyć oraz odwracać macierze, a także wykonywać wszelkie operacje na wielomianach.

Najprostszym skończonym ciałem prostym jest ciało binarne $GF(2)$. Działania w tym ciele oraz struktury nad nim tworzone służą do opisu pracy komputerów oraz transmisji danych. Zbiór elementów ciała $GF(2)$ jest postaci $P = \{0,1\}$. Na rysunku poniżej zamieszczono tabliczki działań tego ciała. Nad ciałem $GF(2)$ można również tworzyć wielomiany oraz konstruować kody korekcyjne. Współczynnikami takiego wielomianu są elementy ciała $GF(2)$, np.:

$$1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 0 = x^3 + x. \tag{1.2}$$

[31] W. Mochnacki, *Kody korekcyjne i kryptografia*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000, s. 10, 14, 15.

$\oplus_2$	**0**	**1**
0	0	1
1	1	0

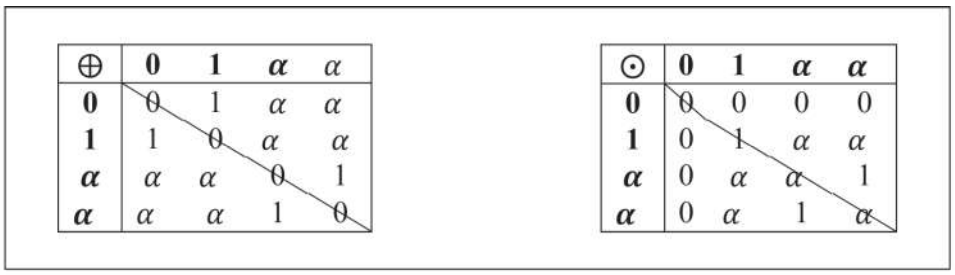
$\odot_2$	**0**	**1**
0	0	0
1	0	1

Rysunek 3.2.2. Działania modulo 2
Źródło: opracowanie własne

Ciała proste nie są w sposób bezpośredni wykorzystywane do konstrukcji kodów korekcyjnych, lecz stanowią podstawę do tworzenia ciał rozszerzonych. W przypadku rozszerzonych ciał skończonych ich moc jest równa potędze liczby pierwszej, co zapisujemy $GF(q)$, gdzie $q = p^m$ oraz p, q – są liczbami pierwszymi, $p, q, m \in \mathbb{N}$. Najprostszym ciałem rozszerzonym jest

$$GF\left(2^2\right) = GF(4)^{32}. \tag{1.3}$$

Elementami tego ciała są elementy zbioru $P = \{0, 1, \alpha, \alpha^2\}$. Na rysunku poniżej przedstawiono działania dodawania i mnożenia w ciele $GF(4)$[33].



$\oplus$	**0**	**1**	$\boldsymbol{\alpha}$	α
0	0	1	α	α
1	1	0	α	α
$\boldsymbol{\alpha}$	α	α	0	1
$\boldsymbol{\alpha}$	α	α	1	0

$\odot$	**0**	**1**	$\boldsymbol{\alpha}$	$\boldsymbol{\alpha}$
0	0	0	0	0
1	0	1	α	α
$\boldsymbol{\alpha}$	0	α	α	1
$\boldsymbol{\alpha}$	0	α	1	α

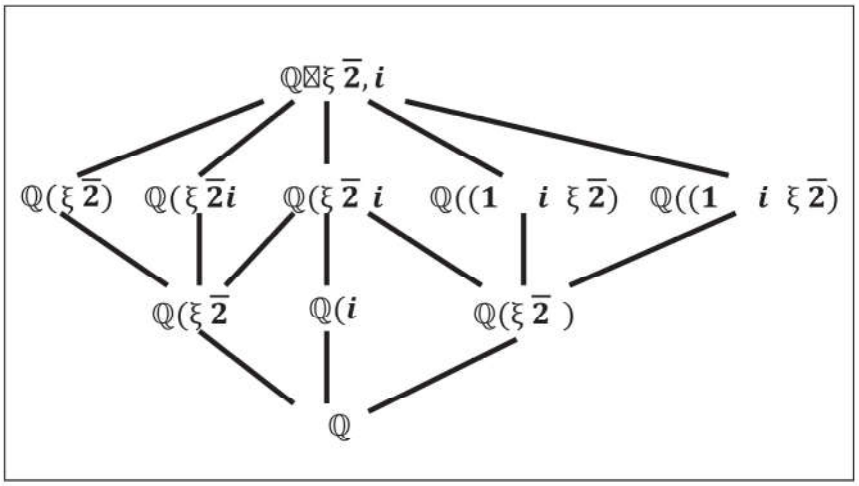
Rysunek 3.2.3. Działania w ciele rozszerzonym *GF*(4)
Źródło: opracowanie własne na podstawie: W. Mochnacki, *Kody korekcyjne i kryptografia*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000, s. 29

Klasyczna teoria Galois oprócz skończonych ciał rozszerzonych rozważa również ciała rozszerzone nieskończone. Są one ważnym elementem tak zwanego podstawowego twierdzenia teorii Galois, które odnosi się do poszukiwania rozwiązań równań wielomianowych z wykorzystaniem pierwiastników. Ciała rozszerzone nieskończone nie są jednak wykorzystywane w zastosowaniach kryptograficznych.

[32] Ibidem, s. 13, 14, 28.
[33] Ibidem, s. 28, 29.

Tutaj bazuje się raczej na ciałach skończonych. Na rysunku poniżej zamieszczono strukturę nieskończonego ciała $\mathbb{Q}$ rozszerzonego o pierwiastki wielomianu $f(x)$:

$$f(x)=x^4-2=\left(x^2+\sqrt{2}\right)\left(x^2-\sqrt{2}\right)=\left(x+\sqrt[4]{2}i\right)\left(x-\sqrt[4]{2}i\right)\left(x+\sqrt[4]{2}\right)\left(x-\sqrt[4]{2}\right)^{34}$$



Rysunek 3.2.4. Struktura ciała rozszerzonego $\mathbb{Q}\left(\sqrt[4]{2},i\right)$
Źródło: opracowanie własne na podstawie: T.W. Judson, *Abstract Algebra. Theory and Applications*, Stephen F. Austin State University, 2009, s. 385

W badaniu ciał skończonych zastosowanie znajduje również funkcja Eulera $\Phi(n)=k$, $k\in\mathbb{N}$, która określa ilość liczb naturalnych występujących w zbiorze $N_n=\{1,2,\ldots,n-2,n-1\}$, $n\in\mathbb{N}$, które są względnie pierwsze z liczbą *n*. Przykładowo $\Phi(12)=4$, gdzie $N_{12}=\{1,2,3,4,5,6,7,8,9,10,11\}$ i są to liczby postaci 1,5,7,11, które są względnie pierwsze z liczbą 12. Funkcja Eulera dla liczb pierwszych *p* przyjmuje postać

$$\Phi(p)=p-1, \tag{1.4}$$

W celu znalezienia wartości funkcji $\Phi(n)=k$ dla liczby złożonej *n* należy rozłożyć ją na iloczyn potęg liczb pierwszych, co zapisujemy

$$n=p_1^{a_1}\cdot p_2^{a_2}\cdot p_{l-1}^{a_{l-1}}\cdot\ldots\cdot p_l^{a_l}. \tag{1.5}$$

Wartość funkcji $\Phi(n)=k$ dla liczby złożonej *n* wyliczamy z wzoru

[34] B. Siemieńska, *Podstawy teorii Galois*, op. cit., s. 69.

$$\Phi(n) = \prod_{i=1}^{l} p_i^{a_i - 1}(p_i - 1). \tag{1.6}$$

Przykładowo dla liczby złożonej $n = 9000$ przeprowadzamy następującą procedurę rachunkową:

$$n = 9000 = 2^3 \cdot 3^2 \cdot 5^3$$

$$\Phi(n) = \Phi(9000) = p_1^{3-1} \cdot (p_1 - 1) \cdot p_2^{2-1} \cdot (p_2 - 1) \cdot p_3^{3-1} \cdot (p_3 - 1) =$$

$$= 2^2 \cdot (2-1) \cdot 3^1 \cdot (3-1) \cdot 5^2 \cdot (5-1) = 2^2 \cdot 1 \cdot 3^1 \cdot 2 \cdot 5^2 \cdot 4 = 2400$$ [35].

4. Teoria Galois a kryptografia

4.1. Istota kryptografii

W czasach współczesnych ważnym elementem konstrukcji kryptograficznych są implementacje, które mogą bazować na ciałach Galois. Pierwotnie kryptografia opierała się głównie na szyfrach przesuwnych, a jej korzenie sięgają czasów antycznych.

Nauka ta narodziła się tysiące lat temu, kiedy to ówcześni władcy poszukiwali poufnego sposobu przekazywania informacji w celu zapewnienia sobie sprawnego rządzenia. Korzystano wówczas albo z technik steganografii, albo z prostych metod kryptograficznych. Obecnie szyfrowanie przebiega według ustalonej reguły, która formułowana jest w języku matematycznym z wykorzystaniem narzędzi informatycznych[36].

W czasach współczesnych kryptografia była początkowo wykorzystywana głównie w wojsku oraz dyplomacji. Jej podstawy teoretyczne zostały dokładnie opracowane przez Shannona w 1945 r. Dziedzinę tę zaczęto jednak bliżej poznawać dopiero w połowie lat 70. XX w., kiedy nastąpiło zainteresowanie systemami teleinformatycznymi i ich rozwój[37].

Obecnie kryptografia znajduje szerokie zastosowanie m.in. w gałęzi przemysłowej. Przykładem tego są karty inteligentne, kody PIN, programy służące do ochrony poczty elektronicznej czy też cyfrowe kodowanie sygnałów telefonicznych w sieciach komórkowych i przewodowych przy zabezpieczaniu komunikacji pomiędzy użytkownikami[38].

---

[35] W. Mochnacki, *Kody korekcyjne i kryptografia*, op. cit., s. 12.

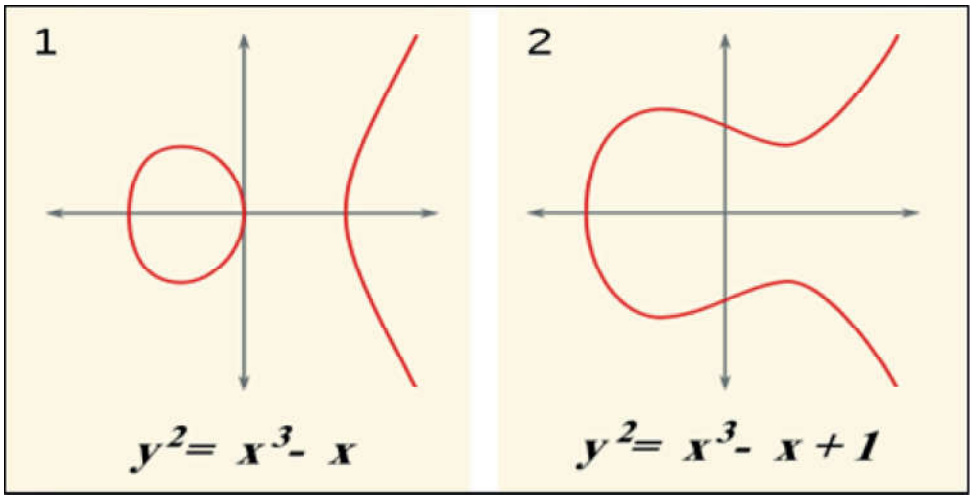
[36] M. Maj, B. Siemieńska, *Kryptologia w aspekcie bezpieczeństwa państwa*, Wydawnictwo Naukowe Instytutu Technologii Eksploatacji Państwowego Instytutu Badawczego, Radom 2015, s. 1.

[37] W. Mochnacki, *Kody korekcyjne i kryptografia*, op. cit., s. 7.

[38] J. Szmidt, M. Misztal, *Wstęp do kryptologii*, WSISiZ, Warszawa 2004.

4.2. Użyteczność elementów teorii Galois w procesie szyfrowania

Współcześnie w zastosowaniach kryptologicznych, szczególnie w przypadku uzgadniania kluczy kryptograficznych oraz realizacji podpisu cyfrowego, wykorzystuje się algorytmy klucza publicznego. Podstawą bezpieczeństwa algorytmów tego typu są problemy trudne obliczeniowo, do których można zaliczyć np. wyznaczanie logarytmu dyskretnego. Dziedziną wykorzystującą trudność znajdowania logarytmu dyskretnego jest grupa punktów krzywej eliptycznej, która zdefiniowana jest nad ciałem Galois[39].



Rys. 4.2.1. Krzywe eliptyczne
Źródło: http://kierul.wordpress.com/2014/01/02/matematyka-czysta-i-brudne-tricki-nsa-2006-2013 (2.03.2016)

Aktualnie coraz większą popularność zdobywają kryptosystemy oparte na krzywych eliptycznych nad ciałem Galois, przede wszystkim ze względu na możliwość zastosowania krótszych kluczy przy zapewnieniu takiego samego poziomu bezpieczeństwa. Pozwala to na mniejsze zużycie zasobów systemu, co jest istotne np. z punktu widzenia zastosowań kart inteligentnych.

W poprzednim rozdziale omówiono ogólną strukturę ciała Galois, która teraz zostanie krótko scharakteryzowana od strony użyteczności kryptograficznej. Struktura postaci $GF\left(2^m\right)$ jest nazywana ciałem Galois, czyli ciałem skończonym charakterystyki dwa. Jest to ciało binarne, które jest obiektem szeroko wykorzystywanym w zastosowaniach kryptograficznych ze względu na brak propagacji przeniesień

[39] J. Gawinecki, P. Bora, M. Jurkiewicz, *Zastosowanie krzywych eliptycznych do konstrukcji bezpiecznych algorytmów i protokołów kryptograficznych*, XLIII KZM, Zakopane 2014, s. 1.

w operacji dodawania oraz dużą elastyczność w sposobie dobierania reprezentacji elementów tego ciała.

Elementy ciała Galois $GF\left(2^m\right)$ reprezentowane są przez *m*-bitowe wektory współrzędnych w odpowiednio ustalonej bazie ciągów $\left(a_0, a_1 \ldots a_{m-2}, a_{m-1}\right)$, gdzie interpretacja każdego bitu takiego ciągu uzależniona jest od wybranej bazy. Dodawanie elementów ciała Galois realizowane jest poprzez operację logiczną XOR współrzędnych tych wektorów. Operacja mnożenia jest natomiast uzależniona od wybranej reprezentacji ciała, czyli bazy.

W kryptograficznych rozwiązaniach programowych najczęściej używa się reprezentacji wielomianowej. Implementacje sprzętowe korzystają dodatkowo z baz normalnych, a szczególnie z klasy baz gaussowskich. Użycie takiej reprezentacji stwarza możliwość efektywnego wykonywania operacji podnoszenia do kwadratu, która sprowadzona zostaje do cyklicznej rotacji wektora.

Krzywa eliptyczna *E* nad ciałem Galois $GF\left(2^m\right)$ jest wykresem pewnego wielomianu trzeciego stopnia. Jest ona zdefiniowana równaniem $y^2 + xy = x^3 + ax^2 + b$, gdzie $a, b \in GF\left(2^m\right)$ i stanowi zbiór punktów płaszczyzny. Z punktu widzenia kryptografii interesujący jest właśnie zbiór punktów, spełniający powyższe równanie i uzupełniony dodatkowo o punkt *O* zwany punktem w nieskończoności. Zbiór taki, po zdefiniowaniu na nim operacji dodawania, stanowi strukturę matematyczną zwaną grupą[40]. Działanie dodawania punktów na krzywej eliptycznej można określić analitycznie lub geometrycznie. Krzywe takie umożliwiają wykonywanie operacji jednokierunkowych, co jest istotne w procesie szyfrowania[41].

Kryptosystemy asymetryczne bazują przede wszystkim na trudnych obliczeniowo problemach matematycznych. Z punktu widzenia bezpieczeństwa krzywych eliptycznych nad ciałem Galois kluczowym zagadnieniem okazuje się problem logarytmu dyskretnego. Jest on określony w następujący sposób: dana jest krzywa eliptyczna *E* zdefiniowana nad ciałem Galois $GF\left(2^m\right)$, dany jest dodatkowo punkt *P* rzędu *n* oraz punkt *Q*, który jest wielokrotnością punktu *P*. Należy znaleźć taką liczbę całkowitą $l \in \langle 0, n-1 \rangle$, gdzie $Q = l \cdot P$. Liczba *l* nazywana jest tutaj logarytmem dyskretnym *Q* o podstawie *P*[42].

Rozważając problemy związane z bezpieczeństwem kryptograficznym, istotnym elementem okazuje się wybór odpowiedniej metody doboru bezpiecznych krzywych. W związku z powyższym, w połowie lat 80. XX w. zaproponowano nowe koncepcje

[40] M. Orkiszewski, T. Wojciechowski, M. Rawski, *System typu CoS do kryptoanalizy szyfrów opartych na krzywych eliptycznych*, PAK, vol. 56, nr 7/2010, Politechnika Warszawska, Warszawa 2010, s. 2.

[41] http://e-handel.mm.com.pl/crypto/eliptyczne.htm (3.03.2016).

[42] M. Orkiszewski, T. Wojciechowski, M. Rawski, *System typu CoS do kryptoanalizy szyfrów opartych na krzywych eliptycznych*, op. cit., s. 1.

rozwiązania oparte o systemy kryptograficzne z kluczem publicznym działające na krzywych eliptycznych nad ciałem Galois[43].

Rozwiązania te dostarczają niewyczerpanego zasobu grup skończonych, co świadczy o wysokiej użyteczności zarówno samych krzywych, jak i ciał Galois w procesie szyfrowania. Wybór taki zapewnia wysoki poziom bezpieczeństwa np. przy szyfrowaniu danych strategicznych[44].

Ważnym atutem jest to, że aktualnie nie jest znany żaden algorytm o podwykładniczej złożoności, który mógłby złamać logarytm dyskretny na krzywych eliptycznych nad ciałem Galois. Ponadto nie jest również znany żaden atak o złożoności podwykładniczej na krzywe nad ciałem skończonym. Dodatkowo, krzywe eliptyczne nad ciałem Galois pozwalają na używanie znacznie krótszych kluczy niż w przypadku RSA. Daje to dużo mniejsze nakłady obliczeniowe przy porównywalnym bezpieczeństwie, co jest znowu istotne z punktu widzenia konstrukcji miniaturowych urządzeń elektronicznych wykorzystywanych w urządzeniach kryptograficznych[45].

Użyteczność rozwiązań kryptograficznych, opartych na krzywych eliptycznych i ciałach Galois, jest widoczna przede wszystkim na rynku gospodarczym, gdzie zastosowanie znajdują np. tokeny do uwierzytelniania danych. Krzywe nad ciałami skończonymi są także podstawą bezpieczeństwa w telefonach szyfrujących GSM. Ponadto protokoły uwierzytelniania oparte na krzywych eliptycznych nad ciałem Galois gwarantują bezpieczeństwo operacji na zdecydowanie krótszych kluczach, co z kolei zapewnia krótszy czas nawiązania połączenia, wykorzystanie mniejszej mocy procesora oraz niższe zużycie energii.

4.3. Systemy kryptograficzne w kontekście bezpieczeństwa państwa

Niezwykłe osiągnięcia kryptograficzne w kwestiach bezpieczeństwa, które oparte są na krzywych eliptycznych nad ciałem Galois, wykazują naukowcy Wojskowej Akademii Technicznej, którzy tworzą nowoczesne algorytmy szyfrujące oraz konstruują urządzenia przeznaczone do ich przetwarzania. Są to niejednokrotnie unikatowe rozwiązania na poziomie światowym.

Jednym z takich rozwojowych przedsięwzięć, realizowanych w WAT w latach 2009-2011, był projekt *Kryptografia wykorzystująca krzywe eliptyczne w zastosowaniach do terminali telefonicznych i radiostacji IP przeznaczonych do pracy w sieciocentrycznych systemach koalicyjnych i narodowych*. Celem tego projektu było wykonanie implementacji systemu klucza publicznego dla telefonii SCIP oraz zaprojektowanie

[43] J. Gawinecki, P. Bora, M. Jurkiewicz, *Zastosowanie krzywych eliptycznych do kondtrukcji bezpiecznych algorytmów i protokołów kryptograficznych*, op. cit., s. 1.

[44] http://e-handel.mm.com.pl/crypto/eliptyczne.htm (3.03.2016);.

[45] M. Orkiszewski, T. Wojciechowski, M. Rawski, *System typu CoS do kryptoanalizy szyfrów opartych na krzywych eliptycznych*, op. cit., s. 1.

narodowego rozwiązania bazującego na teorii krzywych eliptycznych na bazie systemu nad ciałem Galois $GF\left(2^{593}\right)$. Dla porównania, rozwiązania NATO-wskie bazują na ciele $GF(p)$ o długości modułu 384 bity.

Kolejne przedsięwzięcie rozwojowe WAT-owskich pracowników naukowych, również realizowane w latach 2009-2011, to projekt *Demonstrator technologii generatora koprocesora kryptograficznego operującego na elementach z ciała* $GF\left(2^m\right)$. Celem projektu było opracowanie jednolitej aplikacji generującej jądro koprocesora wykonującego obliczenia na elementach z ciała Galois $GF\left(2^m\right)$. Jądro to jest wykorzystywane do konstrukcji systemów kryptograficznych klucza publicznego opartych na teorii krzywych eliptycznych oraz hipereliptycznych[46].

Wśród projektów realizowanych w Instytucie Matematyki i Kryptologii można także wyróżnić prowadzony w latach 2000-2002 grant *Badanie i projektowanie algorytmów kryptograficznych*, którego celem było m.in. omówienie algorytmu Schoofa–Atkina–Elkiesa, służącego do obliczania rzędu krzywej eliptycznej nad ciałem skończonym (ciałem Galois) dużej charakterystyki. Ponadto zaproponowano również algorytm pokazujący, w jaki sposób należy poszukiwać krzywych eliptycznych, których rząd jest liczbą co najmniej 300-bitową. Jest to istotne z punktu widzenia zapewnienia wysokiego poziomu bezpieczeństwa przy zastosowaniach kryptograficznych wykorzystywanych przez odpowiednie instytucje oraz resorty szczebla strategicznego.

Jednym z ważniejszych wynalazków WAT-u okazał się Narodowy Szyfrator. Jest on w pełni polskim urządzeniem, które przeznaczone jest do bezpiecznej komunikacji we wszystkich sieciach telekomunikacyjnych. Umożliwia nawiązanie połączenia szyfrowanego w sieciach komputerowych przez wszystkie współczesne interfejsy komunikacyjne, zarówno w wolnych połączeniach modemowych, jak też w łączach światłowodowych. Szyfrator jest odporny na znane ataki kryptoanalizy. W obecnym stanie wiedzy jest to urządzenie nie do złamania. Nie ma w nim również tak zwanych bocznych furtek. Prezentowany system kryptograficzny jest nowatorski i działa w oparciu o krzywe eliptyczne, posiada też własną implementację pozbawioną wad. W konstrukcji szyfratora zastosowano najnowsze struktury układów programowalnych oraz unikalne zabezpieczenia systemowe. Urządzenie to może znaleźć zastosowanie zarówno w sektorze cywilnym, jak również w administracji rządowej czy w służbach mundurowych, czyli tam, gdzie konieczna jest ochrona informacji wrażliwych[47].

Wyniki badań kryptograficznych uzyskane w WAT oraz innych ośrodkach naukowo-badawczych w Polsce, a także rezultaty wypracowane na ich podstawie znajdują szerokie zastosowanie zarówno w sektorze militarnym, jak i cywilnym. Są wdrażane w narodowych systemach utajniania informacji, co jest niezbędnym elementem bezpieczeństwa i obronności kraju.

---

[46] M. Misztal, *Prezentacja IMiK – projekty 2009-2014*, WAT, Warszawa 2014.

[47] Ibidem.

Rys. 4.3.1. Narodowy Szyfrator
Źródło: M. Misztal, *Prezentacja IMiK – projekty 2009-2014*, WAT, Warszawa 2014

Z punktu widzenia bezpieczeństwa narodowego coraz większego znaczenia nabiera również ochrona informacji wrażliwych. Nowoczesne rozwiązania kryptograficzne oparte na krzywych eliptycznych nad ciałem Galois mogą być zatem wdrażane również w instytucjach, które są odpowiedzialne za zabezpieczenie danych tego typu. Do informacji wrażliwych można zaliczyć informacje dotyczące np. ochrony zdrowia, ochrony danych finansowych, danych osobowych, ochrony tajemnicy państwowej czy służbowej[48].

Z uwagi na fakt, że wraz z intensywnym rozwojem kryptografii prężnie rozwija się również kryptoanaliza, ciągle istnieje potrzeba doskonalenia algorytmów, tworzenia nowych wynalazków, ale także unowocześniania metod badawczych, za sprawą których wspomniane przedsięwzięcia mogą być skutecznie realizowane oraz wdrażane w życie, by zapewnić państwu najwyższy poziom bezpieczeństwa.

5. Podsumowanie

W dobie dzisiejszych zagrożeń, nie tylko natury militarnej, Polska potrzebuje nowoczesnych koncepcji w zakresie ochrony kryptograficznej. Narodowe rozwiązania stanowiłyby solidną podstawę nowatorskiego wyposażenia i uzbrojenia Sił Zbrojnych RP. Bezpieczeństwo informacji jest ważnym gwarantem naszych interesów narodowych, a polskie tajemnice, szczególnie wojskowe, wymagają wciąż nowoczesnych systemów zabezpieczeń.

W celu zapewnienia Polsce suwerenności i bezpieczeństwa na arenie międzynarodowej niezbędnym przedsięwzięciem w tym względzie wydaje się być modernizacja Polskich Sił Zbrojnych. Wiąże się to ściśle z wyposażeniem armii w nowoczesny sprzęt wojskowy. Natychmiastowej modernizacji wymaga przede wszystkim

[48] M. Misztal, *Prezentacja IMiK – projekty 2009-2014*, op. cit.

uzbrojenie i wyposażenie poszczególnych rodzajów Sił Zbrojnych w specjalistyczny sprzęt bojowy.

Każde państwo dąży do tego, aby posiadać własne technologie, które nie będą mogły być rozszyfrowane przez inne kraje. Jednak prace nad takimi systemami to wyścig z czasem. Aktualnie Polska pozyskuje rozwiązania od innych państw, co naraża nas na niebezpieczeństwo szpiegostwa. Poza tym obce technologie są wielokrotnie droższe od tych, które moglibyśmy sami sobie zapewnić[49].

Przykładem może być lotnictwo polskie, które pozyskuje zarówno statki powietrzne, jak również ich wyposażenie od państw sojuszniczych. Jest to o tyle niebezpieczne, że urządzenia radionawigacyjne i łączności radiowej konstrukcji obcego producenta nie zapewniają nam stuprocentowej pewności wykluczenia szpiegostwa na niekorzyść naszego kraju. Algorytmy, w oparciu o które pracują te urządzenia, mogą być wyposażone w tak zwane boczne furtki lub luki systemowe, przez które może być prowadzona niekontrolowana inwigilacja. Zatem Polsce potrzebne są koniecznie rodzime wynalazki, skonstruowane w naszym kraju i na naszych technologiach. Tylko takie produkty mogą zapewnić nam bezpieczeństwo.

W związku z powyższym należałoby zastanowić się nad wypracowaniem rodzimego systemu ochrony i obrony, który byłby w całości skonstruowany w Polsce przez polskie ośrodki badawcze oraz polskich naukowców i konstruktorów. Sprzęt taki powinien być zabezpieczony odpowiednimi algorytmami kryptograficznymi nieznanymi potencjalnemu wrogowi. Wyposażenie polskiej armii na każdym szczeblu dowodzenia w odpowiedni nowoczesny i rodzimy, a jednocześnie bezpieczny sprzęt gwarantowałoby nam bezpieczeństwo na arenie międzynarodowej. Proponowana koncepcja obrony powinna zostać wdrożona w polskim systemie narodowym i powinna bazować na urządzeniach typu Narodowy Szyfrator. Dałoby to gwarancję bezpieczeństwa w procesie przesyłania informacji niejawnych oraz wrażliwych, np. z miejsc klęsk żywiołowych, ochrony zdrowia, czy informacji dotyczących danych finansowych.

Dlatego też cała nadzieja jest pokładana w polskich ośrodkach badawczych i naukowych, które przez swoją ciężką i twórczą pracę staną na wysokości zadania i wyjdą naprzeciw polskim potrzebom kryptograficznym związanym z bezpieczeństwem narodowym naszego kraju[50].

[49] *Kryptologia to nie biznes, to bezpieczeństwo*, „Polska Zbrojna" nr 7 (807), lipiec 2013, s. 56-57.
[50] Ibidem.

LITERATURA

1. Gawinecki J., Bora P., Jurkiewicz M., *Zastosowanie krzywych eliptycznych do konstrukcji bezpiecznych algorytmów i protokołów kryptograficznych*, XLIII KZM, Zakopane 2014.
2. Judson T.W., *Abstract Algebra. Theory and Applications*, Stephen F. Austin State University, 2009.
3. *Kryptologia to nie biznes, to bezpieczeństwo*, „Polska Zbrojna" nr 7 (807) lipiec 2013.
4. Maj M., Siemieńska B., *Kryptologia w aspekcie bezpieczeństwa państwa*, Wydawnictwo Naukowe Instytutu Technologii Eksploatacji Państwowego Instytutu Badawczego, Radom 2015.
5. Misztal M., *Prezentacja IMiK – projekty 2009-2014*, WAT, Warszawa 2014.
6. Mochnacki W., *Kody korekcyjne i kryptografia*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000.
7. Orkiszewski M., Wojciechowski T., Rawski M., *System typu CoS do kryptoanalizy szyfrów opartych na krzywych eliptycznych*, PAK, vol. 56, nr 7/2010, Politechnika Warszawska, Warszawa 2010.
8. Siemieńska B., *Podstawy teorii Galois*, UTH, Radom 2015.
9. Staszel A., *Problemy społeczne, polityczne i prawne. Zastosowanie metod matematycznych w naukach społecznych*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", Kraków 2013, https://zeszyty-naukowe.uek.krakow.pl/article/view/730.
10. Szmidt J., Misztal M., *Wstęp do kryptologii*, WSISiZ, Warszawa 2004.
11. Więsław W., *Algebra w XX wieku. Rys historyczny*, „Roczniki Polskiego Towarzystwa Matematycznego", seria II: „Wiadomości Matematyczne" XL, Wrocław 2004.
12. http://e-handel.mm.com.pl/crypto/eliptyczne.htm
13. http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1887&chapterid=10879
14. http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1888.
15. http://jaszczur.czn.uj.edu.pl/mod/book/view.php?id=1889&chapterid=10900
16. http://jknow.republika.pl/fizyka/riemann.html
17. http://kierul.wordpress.com/2014/01/02/matematyka-czysta-i-brudne-tricki--nsa-2006-2013/
18. http://slideplayer.pl/slide/421188/
19. http://www.gnosis.art.pl/e_gnosis/paradygmatwyobrazni/uspienski4ty_wymiar.htm
20. http://www.harcownik24.pl/2015/06/historia-matematyki-na-bliskim-wschodzie
21. http://www.math.us.edu.pl/prace/liczba/okres2/okres2.html
22. http://www.math.us.edu.pl/prace/liczba/okres6/okres6.html
23. http://www.swiatmatematyki.pl/index.php?p=145
24. https://pl.khanacademy.org/math/algebra/introduction-to-algebra/overview_hist_alg/v/origins-of-algebra
25. https://www.google.pl/search?q=aksjomaty+euklidesa&newwindow

26. https://www.google.pl/search?q=przestrze%C5%84+tr%C3%B3jwymiarowa&newwindow
27. http://www.gp24.pl/wiadomosci/slupsk/art/4848421,matematyke-warto-znac-dla-bezpieczenstwa-rozmowa-z-grazyna-kwiecinska,id,t.html
28. http://olsztyn.naszemiasto.pl/artykul/niedostepna-krolowa-nagroda-banacha-,871372,art,t,id,tm.html
29. https://www.cnbop.pl/wydawnictwa/ksiazki/978-83-61520-26-9/bezpieczenstwo.-teoria-badadnia-praktyka.pdf
30. https://repozytorium.umk.pl/bitstream/handle/item/1896/WST%C4%98P.doc?sequence=1
31. www.google.pl/search?q=al-khwarizmi+algebra&tbm=isch&oq

THE ELEMENTS OF GALOIS' THEORY IN THE CRYPTOGRAPHIC USES OF THE NATIONAL DEFENCE SYSTEM

Abstract. The following paper focuses on the practical use of some elements of the Galois' Theory in the field of cryptography. Therefore, the paper briefly presents the origin of the algebra and the meaning of this term, as well as short characteristic of its development in the abstract aspects and its applicability to security protection. Subsequently, crucial points of the classic Galois' Theory which can be used in cryptographic implementation for the national defence needs, are discussed here. Special attention is paid to the finite fields and their developments which can constitute the basis of the construction of the cryptographic algorithms. Additionally, some WAT inventions based on the solution of this type are introduced.
Keywords: algebra, security, algebraic structure, finite field, finite field extension, Galois' Theory, cryptography.