Relacje i abstrakcje co to właściwie jest?

Jakub Michalec

Opiekun naukowy pracy mgr Jolanta Przybylska

Liceum Ogólnokształcące Zakonu Pijarów

Ul. Akacjowa 5, tel. 12 412 33 63

# Spis treści:

# Wstęp: Co to jest relacja?

## 1.Pary uporządkowane

Definicja Wienera

Definicja Hausdorffa

Definicja Kuratowskiego

Iloczyn kartezjański

## 2.Ścisła definicja relacji

Przykłady

Definicja funkcji

Istotne cechy relacji

## 3.Relacja porządku

Cechy relacji porządku

Szczególne relacje porządku

Przykłady

## 4.Relacja równoważności

Klasy równoważności

Istotne twierdzenia

Przykłady

## 5.Zastosowania relacji równoważności

Konstrukcje liczbowe

Dowody twierdzeń

Język nowoczesnej teorii liczb

## 6.Kongruencje-algebra równoważności

Przenoszenie działań za pomocą kongruencji

## Dowodzenie twierdzeń z teorii liczb

## Bibliografia

## 7.Autorskie pomysły

(Nie)Dobry porządek

Alternatywny dowód

Dziwny zbiór

## Posłowie

## Wstęp: Co to jest relacja?

Relacje otaczają nas i kształtują nasze życie. W potocznym znaczeniu słowo „relacja” oznacza jakąś współzależność pomiędzy dwoma różnymi obiektami. Może być to dwójka ludzi, może to być szef i jego pracownicy, mogą to być instytucje międzynarodowe, albo zależności rynkowe między przedsiębiorstwami. Matematyka tak naprawdę od samego początku zajmowała się badaniem i dowodzeniem relacji pomiędzy obiektami. Choć relacje towarzyszyły nam od zawsze, to matematyka w swojej historii stosunkowo niedawno (początki XX wieku) zaczęła się zajmować precyzowaniem i badaniem relacji samych w sobie. Oczywiście stało się to za sprawą teorii mnogości i logiki matematycznej, które w tym okresie postawiły sobie za zadanie dotrzeć do fundamentalnych podstaw matematycznego myślenia. W mojej pracy na początku omówię najpierw pojęcia fundamentalne niezbędne do zrozumienia ścisłej definicji relacji. Po samej definicji zaprezentuję parę istotnych cech, które relacja może posiadać i które dokładniej precyzują jej naturę. Będą one użyte w dalszej części pracy do definicji pojęć. Przykłady relacji posiadającej cechę starałem się dobierać z różnych dziedzin matematyki oraz codziennego życia. W głównej części pracy przedstawione zostały dwie relacje o zasadniczym znaczeniu w matematyce. Pierwszą z nich jest relacja porządku będąca uogólnieniem pojęcia większości i mniejszości na dowolne zbiory, nawet nie zawierające liczb. Kolejną jest relacja równoważności będąca jeszcze dalszym uogólnieniem pojęcia równości. Pełni ona bardzo ważne funkcje. Pozwala dowodzić twierdzenia z różnych dziedzin wiedzy matematycznej, dokonywać konstrukcji nowych zbiorów liczbowych wraz z działaniami na nich, a nawet modelować relacje z życia codziennego. Po omówieniu relacji równoważności prezentuję przykłady. Kolejne rozdziały poświęcam na dowody rozmaitych twierdzeń z teorii mnogości, teorii grup oraz teorii liczb, które wykorzystują relację równoważności i pojęcia z nią związane. Pod koniec zamieściłem parę luźnych i samodzielnych pomysłów. Pracę oprócz tego ubogaciłem elementami teorii mnogości, teorii grup i teorii liczb. Bo relacje same w sobie są raczej mało ciekawe. Swoją prawdziwą wartość pokazują, gdy mają obiekty, na których mogą działać. Mam nadzieję, że moja praca przypadnie do gustu zarówno absolwentom kierunków matematycznych z nostalgią wspominających pierwsze lata studiów, jak i zupełnym amatorom matematyki, którzy natrafią na nią przypadkiem. Wszystkim Czytelnikom życzę miłej lektury…

## 1.Pary uporządkowane (n-ki uporządkowane)

Głównym problemem w definiowaniu par uporządkowanych za pomocą zbiorów jest to, że na mocy aksjomatu ekstencjalności zbiór nie uwzględnia kolejności elementów, a wymienienie jakiegoś wielokrotnie sprawi, że powtarzające się elementy „skasują się”. Po prostu zbiór zawierający te same elementy to ten sam zbiór. Niezależnie ile razy i w jakiej kolejności je wymienimy.

Intuicyjna definicja pary i ogólnie n-ki uporządkowanej stosowana przez kilka wieków przed powstaniem teorii mnogości mówi, że jest to po prostu ciąg, czyli funkcja ze zbioru liczb naturalnych. Niby wszystko w porządku, bo ciąg uwzględnia kolejność, a zbiór liczb jest łatwo konstruowany za pomocą aksjomatów nieskończoności i zbioru pustego, ale problem pojawia się gdzie indziej. Chodzi o to, że ciąg jest funkcją! Do zdefiniowania funkcji używamy relacji, do relacji iloczynu kartezjańskiego, a do iloczynu kartezjańskiego par uporządkowanych… co daje błędne koło!

Definicja Wienera

Pierwsza definicja pary uporządkowanej została zaproponowana przez Norberta Wienera:

Dodanie zbioru pustego i powiązaniu go z jednym z elementów za pomocą zbioru (gwarantowanego aksjomatem pary) w sprytny sposób pozwala ominąć problem kolejności. Pierwszym elementem jest ten, którego singleton należy do zbioru ze zbiorem pustym. Pozwala także zlikwidować problem „kasowania” elementów w przypadku . Wzięcie elementów w podwójne klamry zbiorów dodatkowo zabezpiecza przed problemem „kasowania”.

Definicja Hausdorffa

Alternatywną definicję zaproponował Felix Hausdorff:

Gdzie oraz muszą być obiektami różnymi od 1 i 2 (1 i 2 nie muszą być tu liczbami naturalnymi, mogą być dowolnymi różnymi obiektami matematycznymi). Definicja znacznie prostsza od tej zaproponowanej przez Wienera. Dodając kolejne zbiory zawierające elementy 3, 4, 5… można od razu zdefiniować dowolną n-kę uporządkowaną. Główną wadą jest to, że niezależnie jakie obiekty będą pełnić rolę 1 i 2(bo wcale nie muszą być to liczby naturalne) za każdym razem trzeba dobrać je tak, żeby były różne od , w przeciwnym wypadku powróci problem kasowania elementów w zbiorze.

Definicja Kuratowskiego

Kazimierz Kuratowski przedstawił do dziś najpowszechniej stosowaną definicję:

Rozróżnienie kolejności jest dość proste, pierwszy element to ten, który znajduje się we wszystkich zbiorach, a drugi to ten zawarty w tylko jednym zbiorze. Warto zauważyć, że dla co prawda nastąpi „skasowanie”:

Ale pomimo tego definicja kolejności wciąż jest poprawna!

N-ka uporządkowana

Jeżeli zdefiniowaliśmy parę uporządkowaną, to dowolną n-kę uporządkowaną możemy zdefiniować za pomocą par uporządkowanych. Robi się to w następujący sposób:

Jest to definicja indukcyjna. Dowolną n+1-kę uporządkowaną można wtedy zdefiniować za pomocą n-ki uporządkowanej i pary uporządkowanej tej n-ki wraz z n+1 elementem:

Kolejne miejsca w n-ce uporządkowanej nazywa się współrzędnymi, w analogii do przestrzeni euklidesowej, będącej zbiorem n-ek uporządkowanych o współrzędnych będących liczbami rzeczywistymi. Teraz kiedy zdefiniowaliśmy n-ki uporządkowane możemy zdefiniować iloczyn kartezjański zbiorów, pojęcie kluczowe w dalszej części pracy.

Iloczyn kartezjański

Iloczyn (produkt) kartezjański zbiorów definiuje się prosto:

jest to zbiór zawierający wszystkie pary uporządkowane, takie że pierwszy element należy do zbioru a drugi do . Widać stąd, że jest to działanie nieprzemienne, ponieważ w parze uporządkowanej liczy się kolejność elementów. Udowodnijmy najpierw istotne twierdzenie:

Dla dowolnych niepustych zbiorów i możemy stworzyć ich iloczyn kartezjański .

Najpierw udowodnimy, że dla dowolnych elementów i możemy stworzyć parę uporządkowaną . Skorzystamy tu z definicji pary Kuratowskiego. Z aksjomatu wyboru:. Z aksjomatu sumy: . Z aksjomatu pary:

Zbiór ten jest parą uporządkowaną zgodnie z definicją Kuratowskiego. Teraz udowodnimy, że możemy stworzyć zbiór zawierający je wszystkie.

Z aksjomatu pary dla i z aksjomatu sumy dla wszystkich istnieje . Jest to zbiór zawierający wszystkie pary uporządkowane, czyli .

Z definicji n-ek uporządkowanych oraz naszego twierdzenia wynika, że iloczyny kartezjańskie większej ilości zbiorów będą po prostu zbiorami wszystkich n-ek uporządkowanych o współrzędnych wziętych odpowiednio z kolejnych zbiorów. Ponieważ iloczyny kartezjańskie same są zbiorami, to możemy tworzyć iloczyn kartezjański dowolnej liczby zbiorów.

Iloczyn kartezjański n zbiorów będzie po prostu zbiorem wszystkich n-ek uporządkowanych o współrzędnych wziętych z kolejnych zbiorów. Dla szczególnego przypadku iloczynu kartezjańskiego zbioru „samego ze sobą” zapisujemy jako „zbiór do potęgi”(nie mylić ze zbiorem potęgowym!):

Gdzie elementy kolejnych z tych zbiorów będą kolejnymi n-kami uporządkowanymi o współrzędnych z tego samego zbioru.

## 2.Ścisła definicja relacji

W ogólności relacja jest dowolnym podzbiorem iloczynu kartezjańskiego skończonej liczby zbiorów .

Oznacza to, że może mieć dowolną, ale skończoną liczbę argumentów. Fakt, że jakiś element jest w relacji (należy do relacji ) zapisujemy:

Dla relacji dwuargumentowych (w praktyce każdą możemy do takiej sprowadzić) często stosuje się też taki zapis:

Gdzie oraz to elementy należące do relacji. Przynależność do relacji może być określona konkretnym warunkiem(zazwyczaj tylko takie do czegokolwiek się nadają), ale ponieważ relacja jest dowolnym podzbiorem możemy również stworzyć ją siłowo, po prostu „wpychając” do niego określone elementy. Najczęściej też stosuje się relacje na iloczynach typu , wtedy mówi się krótko: „relacja na zbiorze ”.

Przykład 1

Relacją zadaną prostym warunkiem jest relacja podzielności na zbiorze liczb . Oznacza się ją .

Do tej relacji należą np. pary

Ale nie należą pary:

Przykład 2

Relacją stworzoną „na siłę” może być relacja na zbiorze:{A,B,C,D}. Po prostu definiujemy, że do relacji należą pary:

W graficznym widoku możemy przedstawić ją tak(kolor zielony oznacza przynależność):

Taka relacja chyba niewiele ciekawego sobą przedstawia i raczej nie jest warta większej uwagi. W tych przykładach stosowaliśmy relację na zbiorach typu , były to oraz , jednak w ogólności nie musi tak być. Właśnie taką relację wykorzystamy w kolejnym paragrafie.

Pierwsze zastosowanie relacji: definicja funkcji!

Mówiliśmy na początku, że funkcję definiuje się za pomocą relacji. Przypomnijmy szkloną definicję funkcji:

*Funkcją nazywamy takie przyporządkowanie elementów ze zbioru X elementom ze zbioru Y, że każdemu elementowi ze zbioru X odpowiada dokładnie jeden element ze zbioru Y.*

Przekonajmy się, że funkcja jest relacją! Jako pierwszy taką definicję zastosował Giuseppe Peano. Jest ona pewnym uogólnieniem pojęcia wykresu na płaszczyźnie, będącej właśnie zbiorem par uporządkowanych, zbiór jest dziedziną, a przeciwdziedziną. Oczywiście że zbiory i mogą być zupełnie różnymi zbiorami, więc tu nie musi być to relacja na zbiorze (choć w szczególnych przypadkach może tak być).

Funkcja , to relacja , taka że dla każdego elementu ze zbioru istnieje dokładnie jeden element ze zbioru będący z nim w relacji. W logicznym języku zapisujemy to tak:

Dodając do relacji dodatkowe warunki możemy zdefiniować też iniekcję i suriekcję:

Iniekcja to funkcja różnowartościowa. Oznacza to po prostu, że jeżeli y jest w relacji z dwoma elementami, to są one sobie równe. Jest to warunek analogiczny do drugiego, co zapisujemy tak:

Suriekcja to funkcja pokrywająca całą przeciwdziedzinę. Wymaga to sformułowania warunku analogicznego do pierwszego, co zapisujemy tak:

I jak nam wiadomo ze szkoły łącząc te dwa warunki otrzymujemy bijekcję, różnowartościową funkcję, pokrywającą całą przeciwdziedzinę (Wynika z tego, że każdemu elementowi przeciwdziedziny przyporządkowuje dokładnie jeden element dziedziny). Oto jej definicja za pomocą relacji:

Funkcje wykorzystywane są we wszystkich możliwych działach matematyki, właściwie ciężko sobie wyobrazić jak wyglądałaby nasza matematyka bez nich. Nawet dziecko w podstawówce licząc jabłuszka na talerzu stosuje funkcję ze zbioru liczb naturalnych, choć oczywiście nie zdaje sobie z tego sprawy! W szczególności bijekcje mają zastosowania w wielu różnych działach matematyki. Sama możliwość formalnej definicji funkcji za pomocą pojęcia relacji już powinna nam uświadomić, jak ogólnym, podstawowym i prostym narzędziem są relacje.

Istotne cechy relacji

Relacje mogą posiadać pewne cechy dotyczące przynależności pewnych elementów do nich, w zależności od przynależności innych elementów. Niekiedy wynikają one wprost z definicji przynależności, czasem ich dowód jest nieco bardziej skomplikowany, ale mogą one w bardzo istotny sposób określić relację. Są to na przykład:

**Zwrotność**

Polega na tym, że każda para jest w relacji.

* relacja równości (x jest równy x)
* relacja podzielności w zbiorze (niezerowa liczba dzieli samą siebie)
* relacja równoległości prostych(dowolna prosta jest równoległa do siebie samej)

**Przeciwzwrotność**

Polega na tym, że żadna z par nie należy do relacji.

* relacja potomstwa (nikt nie może być swoim potomkiem)
* relacja inkluzji (żaden zbiór nie zawiera samego siebie)
* relacja prostopadłości prostych(żadna prosta nie jest prostopadła do samej siebie)

**Symetria**

Jeżeli para jest w relacji, to wynika z tego, że również do niej należy.

* relacja pokrewieństwa(jeżeli on jest moim krewnym, to ja też jestem jego krewnym)
* relacja odległości w przestrzeni metrycznej (jeżeli jeden przedmiot jest w odległości a od drugiego, to drugi też jest w odległości a od pierwszego)
* relacja względnej pierwszości liczb całkowitych(jeżeli NWD liczby a i b wynosi 1, to NWD dla b i a też wynosi 1)

**Antysymetria**

Jeżeli para należy do relacji, to wynika z tego, że do niej nie należy dla różnych x i y.

* relacja potomstwa (jeżeli A jest potomkiem B, to B nie jest potomkiem A)
* relacja większości (jeżeli x jest większe od y, to y nie może być większe od x)
* relacja zwierzchności(jeżeli osoba A jest zwierzchnikiem osoby B, to osoba B nie może być zwierzchnikiem osoby A)

**Przechodniość**

Jeżeli para i para należy do relacji to para również do niej należy.

* relacja rodzeństwa (jeżeli A jest rodzeństwem B i B jest rodzeństwem C, to A i C również są rodzeństwem)
* relacja zwierzchności (jeżeli A jest podwładnym B i B podlega C, to wynika z tego, że A podlega C)
* relacja inkluzji(jeżeli zbiór A zawiera się w B i B zawiera się w zbiorze C, to A również zawiera się w zbiorze C)

**Spójność**

Jeżeli weźmiemy dwa dowolne elementy i , to któraś z par: lub jest w relacji. Rzadko spotykana cecha.

* Większość w liczbach rzeczywistych
* Istnienie ścieżki w grafie spójnym
* Istnienie metryki w przestrzeni metrycznej

**Pustość**

Relacja będąca zbiorem pustym. Żadne elementy i nie są w relacji. Relacja trywialna i mało interesująca.

* Podzielność na zbiorze liczb pierwszych
* Względna pierwszość na zbiorze dodatnich potęg liczby naturalnej
* Dowolna relacja na zbiorze pustym

**Pełność**

Relacja będąca niewłaściwym podzbiorem iloczynu kartezjańskiego. Dowolne dwa elementy i są w relacji. Jest ona zwrotna, symetryczna, przechodnia i spójna. Równie mało interesująca.

* Względna pierwszość na zbiorze liczb pierwszych
* Istnienie metryki dla punktów przestrzeni metrycznej
* Przynależność do tego samego gatunku dla ludzkiej populacji

## 3.Relacja porządku

Cechy relacji porządku

Relacje porządku pozwalają porównywać elementy danego zbioru. Dowolna relacja porządku na zbiorze(lub ogólniej, klasie) musi mieć dwie cechy:

**(1)przechodniość:**

**(2)antysymetria:**

Przy relacji porządku możemy mówić o elementach mniejszych i większych, ale stosuje się też nazwy wcześniejszych i późniejszych. Ze względu na zwrotność występuje podział na porządek słaby i silny(zwany ostrym) .

Porządek słaby cechuje się zwrotnością, czyli:

Natomiast w porządku silnym występuje przeciwzwrotność:

Mając dany porządek słaby można łatwo na jego podstawie zdefiniować porządek silny dodając do niego warunek nierówności elementów:

Szczególne relacje porządku

Szczególnym przypadkiem relacji porządku jest porządek liniowy. Charakteryzuje się on tym, że za jego pomocą można porównać dwa dowolne elementy zbioru, czyli jest on spójny:

**(3)spójność:**

Jeżeli porządek liniowy na jakimś zbiorze ma tę szczególną własność, że dowolny jego podzbiór ma element najmniejszy:

To nazywany jest dobrym porządkiem. Najlepszy przykład to porządek w liczbach naturalnych.

Innym szczególnym przykładem porządku liniowego jest porządek gęsty. Dla dowolnych dwóch elementów zbioru możemy znaleźć element pomiędzy nimi:

Jeżeli na danym zbiorze da się zdefiniować gęsty porządek to zbiór nazywamy gęstym. Najlepsze dostępne przykłady to zbiór liczb wymiernych i rzeczywistych.

Przykłady relacji porządku

**Porządek liczb naturalnych**

W teorii mnogości przeprowadza się konstrukcję zbioru liczb naturalnych przy pomocy ich reprezentacji w postaci zbiorów, w następujący sposób:

Możemy zdefiniować relację porządku słabego na danej zasadzie:

I wyżej zaprezentowaną metodą można dalej zdefiniować silny porządek (równość liczb naturalnych to identyczność zbiorów, które je reprezentują, a ta definicja wynika w wprost z aksjomatu ekstencjalności w teorii mnogości). Ewentualnie możemy wybrać alternatywną metodę, od razu wprowadzającą silny porządek:

Dzięki temu możemy wprowadzić porządek na całym zbiorze:

Będzie to dobry porządek.

**Porządek alfabetyczny**

Możemy także rozpatrywać porządek na dowolnym skończonym, albo nieskończonym zbiorze, gdzie każdemu elementowi możemy przypisać liczbę naturalną. Porządkiem takim jest porządek alfabetyczny w alfabecie łacińskim:

Dzieje się tak ponieważ każdemu elementowi zbioru przypisaliśmy liczbę naturalną, na podstawie, której oznaczamy ich kolejność.:

To również będzie dobry porządek.

**Porządek liczb porządkowych**

Relację porządku z Przykładu 1 można uogólnić na klasę(bo nie tworzą one zbioru) nieskończonych liczb porządkowych, konstruowanych w analogiczny sposób do liczb naturalnych, ale z użyciem teoriomnogościowego aksjomatu nieskończoności. Przykłady:

Tutaj również działa zasada z przykładu 1, ponieważ np. reprezentuje zbiór wszystkich liczb naturalnych, dowolna liczba naturalna będzie od niej mniejsza, bo znajduje się w zbiorze , ewentualnie jej zbiór zawiera się w zbiorze . Tu również da się określić relację dobrego porządku:

**Porządek niestandardowy**

Na jednym zbiorze można zdefiniować różne relacje porządku! Jako przykład można podać liczby naturalne. Zdefiniujemy na nich niestandardowy porządek: liczba zero będzie najmniejsza, potem 1, potem liczby porządkujemy według ilości ich dzielników pierwszych (niekoniecznie różnych), a w zbiorach liczb mających identyczną ilość dzielników według standardowego porządku.

Również jest to relacja porządku!

**Porządek leksykograficzny**

Dla ciągów elementów, dla których określono porządek, również można określić porządek. Jest to tak zwany porządek leksykograficzny. Tak jak porządek alfabetyczny z liter da się przenieść na słowa, tak z dowolnych elementów porządek można przenieść na ich ciągi. Porządek ten określa się następująco:

1. Jeżeli w ciągach i istnieje takie , że , a , to wtedy jeżeli , to .
2. Jeżeli takie n nie istnieje, to ciąg krótszy jest wcześniejszy niż dłuższy(odnosi się to też do ciągów nieskończonych).
3. Jeżeli obydwa ciągi są tej samej długości, to .

Dla przykładu ze standardowego porządku w liczbach naturalnych:

## 4.Relacja równoważności

Relacja równoważności na zbiorze jest szczególną relacją dwuargumentową. Musi być ona:

**Zwrotna**

**Symetryczna**

**Przechodnia**

Jest ona niejako uogólnieniem pojęcia równości na znacznie szersze typy relacji i zbiorów. Zazwyczaj relację równoważności między dwoma elementami(nazwijmy je i ) oznacza się poprzez lub . Niezwykle istotną cechą relacji równoważności na danym zbiorze jest dokonywanie podziału na klasy abstrakcji(zwane klasami równoważności lub warstwami).

Klasy równoważności

Pojęcie klasy jest to uogólnienie pojęcia zbioru, podstawa teorii klas stworzonej dla uzupełnienia niedogodności teorii mnogości. Klasa jest to (najbardziej intuicyjnie) obiekt, do którego należą elementy spełniające pewien warunek wyrażony w języku teorii mnogości. Jeżeli nie ma zbioru spełniającego takie warunki (np. zbiór wszystkich zbiorów), jest klasa spełniająca takie warunki(np. klasa wszystkich zbiorów). Każdy zbiór jest klasą i w naszych przykładach nie będzie konieczności używania klas, które nie są zbiorami, dlatego pojęć tych możemy tu używać wymiennie.

Klasę abstrakcji związaną z relacją równoważności definiujemy:

Czyli jest to zbiór wszystkich elementów będących ze sobą w relacji równoważności. Element nazywany jest reprezentantem danej klasy, może to być dowolny element wchodzący w skład tej klasy. Jeżeli jakaś relacja równoważności ma tylko jedną klasę to jest relacją pełną. Także rozpatrywana wewnątrz dowolnej klasy równoważności, ta relacja będzie relacją pełną.

**Przestrzeń ilorazowa**

Z relacją równoważności na zbiorze związane jest pojęcie przestrzeni ilorazowej . Jest to zbiór zawierający wszystkie klasy równoważności tej relacji dla zbioru .

Dla wybrednych matematyków można jeszcze uzasadnić istnienie tego zbioru. Z aksjomatu pary wynika istnienie dla każdego zbioru zbioru . Stosując do wszystkich zbiorów aksjomat sumy dostaniemy żądany zbiór .

Ważne twierdzenia dotyczące relacji równoważności

Poniżej trochę oczywiste, ale bardzo istotne twierdzenia związane z relacjami równoważności na dowolnym zbiorze . Ich dowody wynikają niemal wprost z definicji, ale warto je znać, bo mówią nam o najistotniejszych cechach wyróżniających relację równoważności spośród innych relacji.

1. **Żadna klasa dla niepustego nie jest pusta.**

Wynika to wprost z definicji klasy równoważności. Zawiera ona wszystkie elementy będące ze sobą w relacji równoważności, ponieważ z definicji relacji równoważności każdy element będzie równoważny sobie samemu, istnienie elementów równoważnych sprawia, że nie może być pustej klasy.

1. **Dowolny element zbioru należy do jakiejś klasy abstrakcji.**

Z warunku zwrotności czyli jest w relacji z jakimś elementem, dlatego należy do klasy zawierającej przynajmniej jego samego, choćby była ona jednoelementowym zbiorem.

1. **Suma mnogościowa wszystkich klas abstrakcji zbioru daje zbiór .**

Ponieważ dowolny element zbioru należy do jakiejś klasy , to wszystkie elementy zbioru należą do którejś z klas i z definicji klasy abstrakcji, żadna nie zawiera elementu, którego nie zawiera . . Dlatego ich suma mnogościowa jest zbiorem mającym takie same elementy jak , czyli jest zbiorem (aksjomat ekstensjalności).

1. **Dwie różne klasy abstrakcji przecinają się pusto.**

Niech dwie klasy posiadają niepuste przecięcie . Jeżeli jest ono niepuste, to , czyli . Z definicji klasy abstrakcji i . Z warunku przechodniości relacji wynika, że: . Wynika z tego, że dowolne dwa elementy tych klas są w relacji równoważności, czyli Otrzymana sprzeczność kończy dowód, czyli .

1. **Każda relacja równoważności powoduje rozbicie zbioru na rozłączne klasy**

Z twierdzenia 1, wynika, że każdy element znajdzie się w którymś z podzbiorów, czyli cały zbiór będzie podzielony, a z twierdzenia 3 wynika, że będą one rozłączne. Twierdzenie to zwane jest zasadą abstrakcji.

1. **Z każdym takim podziałem można powiązać pewną relację równoważności (Twierdzenie odwrotne do zasady abstrakcji).**

Relacja nie będzie zbyt wyszukana, jest nią po prostu przynależność to tego samego podzbioru :. Jest ona zwrotna, bo każdy element należy do tego samego zbioru, co on sam. Jest ona symetryczna, bo kolejność wymienienia elementów w zbiorze nie ma znaczenia i jest ona przechodnia, bo jeżeli i to zbiór zawiera elementy:, więc . Czyli jest to relacja równoważności.

1. **Klas abstrakcji nie może być więcej niż elementów zbioru**

Stwórzmy funkcję , zdefiniujmy ją jako: . Jest to suriekcja, ponieważ zgodnie z twierdzeniem 1 nie ma klas pustych, czyli każda klasa jest wartością co najmniej jeden elementu z . W myśl definicji mocy zbioru wziętych z teorii mnogości ponieważ możemy utworzyć suriekcję , to w takim razie:

Przykłady relacji równoważności

**Rodzeństwo**

Mamy zbiór ludzi . Definiujemy na nim relację . Dwóch ludzi jest w tej relacji, jeżeli jest rodzeństwem, to znaczy ma takiego samego ojca i matkę(nie uwzględniamy rodzeństw przyrodnich ani adopcji). Dowiedziemy równoważności z definicji:

Relacja jest *zwrotna*, bo każdy ma tego samego ojca i matkę, co on sam.

Relacja jest *symetryczna*, bo jeśli osoba ma tych samych rodziców co , to jest oczywiste, że ma tych samych rodziców, co .

Relacja jest też *przechodnia*, bo jeśli osoby oraz mają tych samych rodziców, oraz osoby i mają tych samych rodziców, to również i będą mieć tych samych rodziców.

Dlatego relacja podzieli zbiór na rozłączne podzbiory zawierające osoby będące rodzeństwami.

**Klasy (równoważności) szkolne**

Przykład z życia wzięty! Dowiedziemy go tym razem z twierdzenia odwrotnego do zasady abstrakcji. Oznaczmy zbiór wszystkich uczniów danej szkoły przez , a klasy szkolne jako , a uczniów tej szkoły jako elementy .

Pomijając pewne (indywidualne…) przypadki, żadna osoba nie chodzi do dwóch lub więcej klas naraz. Załóżmy, że w naszej szkole nie ma takich przypadków, czyli:

Każdy uczeń w szkole chodzi do jakiejś klasy:

Ponieważ każdy element należy do którejś z klas i żaden nie należy do więcej niż jednej naraz, to rodzina jest podziałem zbioru na rozłączne podzbiory i można z nim powiązać relację równoważności, którą będzie chodzenie do jednej klasy

**Reszta z dzielenia**

Reszty z dzielenia w trzeciej klasie szkoły podstawowej wydawały się mało przydatnym dodatkiem. Dowolna liczba całkowita może być podzielona z resztą przez inną liczbę całkowitą w postaci:

Gdzie należy do liczb całkowitych, a do liczb naturalnych. Jeżeli jest podzielna przez , to wtedy .

Relację przystawania modulo definiujemy jako posiadanie przez dwie liczby całkowite tych samych reszt z dzielenia przez . Najpierw dowiedziemy, że relacja jest zwrotna.

Dowolna liczba całkowita ma jednoznaczną resztę z dzielenia przez . Dowodzi się tego nie wprost:

Reszta z dzielenia lewej strony przez wynosi 0:

Czyli przy dzieleniu przez każda liczba daje tylko jedną resztę, więc ma taką samą resztę z dzielenia jak ona sama.

Relacja jest symetryczna, ponieważ opiera się na równości liczb całkowitych, tego samego powodu będzie też przechodnia. Dzieli ona zbiór liczb całkowitych, na klasy, w których każda liczba ma tę samą resztę z dzielenia przez . Na przykład dla będą one wyglądać w ten sposób:

Przystawanie modulo n zapisuje się symbolem i zapisuje tak:

Zbiór ze zdefiniowaną relacją przystawania mod oznacza się .

**Podzielna różnica potęg**

Profesor na obozie matematycznym zadał nam do rozwiązania pewien problem: dwie liczby naturalne są w relacji:

Czy ta relacja jest relacją równoważności? A jeśli jest to jakie będą jej klasy równoważności?

Relacja jest oczywiście zwrotna, bo: , a zero jest podzielne przez wszystko. Relacja jest także symetryczna z podzielności w liczbach całkowitych. , to:

i również będzie podzielne przez 10. Problem jest z dowodem przechodniości relacji:

Podstawione tu wartości odpowiadają wartościom oraz

podzielonym przez 10. Będą one podzielne przez 10, ponieważ usuwamy z sumy(powstałej z rozwinięcia wzoru w szereg dwumianu Newtona) niepewny element , a pozostałe elementy w tej sumie są podzielne przez kolejne potęgi 10k lub -10l, czyli cała suma będzie podzielna przez 10. Relacja jest zwrotna, symetryczna oraz przechodnia, czyli jest relacją równoważności. Jej klasy abstrakcji zależą od cyfr jedności w postaci dziesiętnej kolejnych potęg liczb kończących się na kolejne cyfry. Jeżeli dwie liczby do pewnej potęgi kończą się na tą samą cyfrę jedności, to w takim razie są w tej samej klasie. Oto symboliczna prezentacja cykli jakie tworzą te cyfry:

Po zastosowaniu metody „z góry na dół” i „która cyferka się powtarza” widzimy, że mamy cztery klasy abstrakcji: . Zadanie profesora rozwiązane, choć najciężej było wpaść na pomysł z przechodniością.

## 5.Zastosowania relacji równoważności

Relację równoważności stosuje się w matematycznych dowodach i konstrukcjach, w których należy podzielić jakiś zbiór na rozłączne podzbiory. Do tego pewne szczególne cechy związane z klasami równoważności i przestrzenią ilorazową również mają swoje zastosowanie.

Konstrukcje liczbowe

Najbardziej zachwycającym zastosowaniem przystawania jest konstrukcja następnych w kolejności zbiorów liczbowych. Konstrukcja zbioru liczb naturalnych za pomocą teoriomnogościowej reprezentacji została przedstawiona w paragrafie o relacji porządku. Teraz, mając liczby naturalne można się zabrać za konstrukcję liczb całkowitych.

**Konstrukcja liczb całkowitych**

Załóżmy, że mamy zbiór liczb naturalnych z działaniami dodawania i mnożenia. Liczby całkowite zdefiniujemy jako pary uporządkowane liczb naturalnych ze zbioru . Liczby całkowite, czyli pary , powinny odpowiadać wartościom wyrażenia , które jest w stanie wyjść poza zbiór liczb naturalnych, jednak to byłoby sprzeczne z algebraiczną definicją działania. Spróbujmy jednak zdefiniować równość, jak podpowiada intuicja wiele par (nieskończenie wiele) będzie dawać tą samą liczbę… Sposób, aby sobie z tym poradzić, to zastosować relację równoważności.

Ponieważ nie możemy zapisać: , równość definiujemy:

Relacja równości jest zwrotna, symetryczna i przechodnia. Jako relacja równoważności dzieli ona zbiór na rozłączne klasy abstrakcji. Wszystkie pary w danej klasie będą reprezentować jedną liczbę całkowitą.

Teraz nawet działanie odejmowania możemy zdefiniować jako dodawanie elementu przeciwnego, jednak o działaniach na klasach równoważności mowa będzie w dalszej części pracy. Tej konstrukcji można też użyć, by od razu wprowadzić relację porządku na liczbach całkowitych. Tak jak przy równości, sprowadzimy ją do porządku na zbiorze liczb naturalnych, który już zdefiniowaliśmy:

I dzięki temu uzyskujemy porządek na zbiorze liczb całkowitych:

**Konstrukcja liczb wymiernych**

Mamy już zbiór liczb całkowitych i działania dodawania i mnożenia. Do konstrukcji zbioru liczb wymiernych dodawanie się nie przyda. Jest ono wewnętrze dla zbioru liczb całkowitych(a nawet stanowi na nim grupę), co oznacza, że dla żadnych dwóch argumentów nie wyjdzie poza ten zbiór. Dlatego weźmiemy pary uporządkowane ze zbioru liczb całkowitych, ale teraz będą one odpowiadać dzieleniu(dlatego drugim elementem nie może być zero!).Niech więc , ale ponieważ operacja znowu wychodzi poza zbiór, definiujemy równość za pomocą wewnętrznego mnożenia:

Dzięki relacji równoważności dzielimy zbiór na rozłączne klasy abstrakcji. Każda liczba wymierna jest właśnie reprezentantem wszystkich takich par w danej klasie:

W liczbach wymiernych dzielnie zamienia się w mnożenie przez element odwrotny. Także na nich można zdefiniować relację porządku przenosząc ją ze zbioru liczb całkowitych.

Nie możemy tu przedstawić wszystkich liczb wymiernych na danym odcinku (zbiór gęsty), dlatego przedstawimy kilka z nich:

**Konstrukcja liczb rzeczywistych**

Zdefiniowanie zbioru liczb rzeczywistych za pomocą liczb wymiernych jest bardziej skomplikowane. Istnieją trzy metody, jedna polega na przekrojach Dedekinda, ale choć jest prostsza, to nie będziemy jej omawiać. Druga korzysta z ciągów cyfr i liczby całkowitej. Trzecia korzysta z relacji równoważności, choć zupełnie innego typu, a praca poświęcona jest relacjom równoważności. Dlatego bierzmy się do jej przedstawienia.

Metoda ta korzysta z ciągów Cauchy’ego i tego, że liczby wymierne mogą przyjmować wartości dowolnie bliskie liczbom rzeczywistym, nawet niewymiernym i wartości dowolnie bliskie zera. Wyobraźmy sobie zbiór wszystkich możliwych ciągów liczb wymiernych , nazwijmy go . Rozpatrzymy jego podzbiór: ciągi Cauchy’ego (oznaczmy przez ). Ciąg Cauchy’ego charakteryzuje się tym, że dwa dowolne jego wyrazy za odpowiednią liczbą naturalną leżą dowolnie blisko siebie:

Oczywiście ciągi Cauchy’ego są nieskończone. W ogólności maże należeć do liczb rzeczywistych dodatnich, jednak ponieważ je definiujemy, nie możemy odwołać się do nich samych. Ponieważ liczby wymierne przyjmują wartości dowolnie bliskie 0, w zupełności wystarczą, aby był dowolnie mały.

Zdefiniujmy na nim relację: dwa ciągi są ze sobą w relacji, jeśli:

Relacja będzie zwrotna ponieważ:

Relacja będzie symetryczna, ponieważ:

Więc , czyli jeżeli , czyli spełnia warunek relacji, to także , więc również jest w relacji.

Relacja przechodnia, ponieważ:

Jeżeli i , to z tego wynika:

Ponieważ relacja jest zwrotna, symetryczna i przechodnia, jest relacją równoważności i dzieli zbiór wszystkich ciągów Cauchy’ego liczb wymiernych na rozłączne klasy równoważności. Granice tych ciągów to liczby rzeczywiste, ciągi znajdujące się w jednej klasie mają tą samą granicę. Uwaga techniczna: jako reprezentantów klas abstrakcji liczb wymiernych najlepiej wybrać stałe ciągi liczb wymiernych.

Możemy zdefiniować też relację porządku na zbiorze liczb rzeczywistych. Ponieważ każdą z nich reprezentuje ciąg liczb wymiernych, a relację porządku na liczbach wymiernych mamy zdefiniowaną, dla dwóch liczb i ciągów , które je reprezentują:

Tu wygodniej najpierw zdefiniować silny porządek. Równość to przynależność ich ciągów do tej samej klasy równoważności. Jeżeli potrzebny nam słaby porządek:

Zdefiniowaliśmy zbiór liczb rzeczywistych z porządkiem liniowym i jak potem zobaczymy, również działaniami dodawania oraz mnożenia. Jest to podstawa w matematyce, używana niemal we wszystkich jej działach. Mając relację równoważności można je zdefiniować z samego zbioru w trzech krokach, o wystarczająco pokazuje jej użyteczność. Z twierdzenia 7 w paragrafie o istotnych twierdzeniach związanych z relacją równoważności wynika, że z żadnego zbioru nie możemy skonstruować zbioru o większej mocy niż on sam. Wynika z tego, że zbiory liczb całkowitych i wymiernych maja tę samą moc co naturalnych. Zbiór liczb rzeczywistych mieć jej nie musi (i jak wiemy nie ma), bo do jego konstrukcji nie wykorzystujemy zbioru liczb wymiernych, ale zbiór ich ciągów (który ma większą moc). Teraz pora zaprezentować metody dowodzenia twierdzeń wykorzystujące relację równoważności.

Dowody twierdzeń

Relacje równoważności mogą być przydatne, kiedy w dowodzie twierdzenia trzeba podzielić jakiś zbiór na rozłączne podzbiory. Bywa to szczególnie użyteczne zwłaszcza w połączeniu ze złowrogim aksjomatem wyboru. Ponieważ przestrzeń ilorazowa tworzona przy użyciu relacji równoważności jest rodziną niepustych i rozłącznych zbiorów (patrz istotne twierdzenia w paragrafie o relacji równoważności), możemy od razu przystąpić do jego użycia.

**Dowolne funkcje**

:Dla dowolnych niepustych zbiorów i możemy stworzyć funkcję .

Z twierdzenia na początku pracy wynika, że dla dowolnych niepustych i możemy stworzyć iloczyn kartezjański . Teraz należy pokazać, że dla dowolnego takiego iloczynu istnieje podzbiór spełniający cechy funkcji. Aby to zrobić dzielimy za pomocą relacji równoważności:

Jest ona zwrotna, bo dla dowolnej pary . Jest ona symetryczna, bo jeżeli , to wtedy . Jest ona przechodnia, bo jeżeli , to z definicji: , a więc , czyli . Czyli jest ona relacją równoważności. Dzieli ona zbiór na klasy równoważności , w których wszystkie pary mają ten sam pierwszy element ze zbioru , oraz dowolny element drugi ze zbioru . Przestrzeń ilorazowa jest rodziną tych klas .

Nasze zbiory są rozłączne i niepuste, więc możemy zastosować AC. Na mocy aksjomatu wyboru istnieje zbiór (zwany selektorem), zawierający dokładnie jeden element z każdej klasy równoważności. Zbiór spełnia cechy funkcji:

, czyli , a więc jest relacją.

Ponieważ . Ponieważ każdy element zbioru pochodzi z innej klasy , to:

, czyli wynika z tego:

Zbiór jest więc relacją, która spełnia cechy funkcji. Z tego, że w każdej klas Były wszystkie elementy , wynika ponadto, że nasza funkcja może mieć jako przeciwdziedzinę dowolny podzbiór zbioru .

Tak dla formalności, ponieważ powiedzieliśmy, że nasze jest równoważne , wypadałoby to udowodnić, dowodząc za jego pomocą . Mamy więc dowolną rodzinę rozłącznych i niepustych zbiorów . Z aksjomatu sumy istnieje , czyli zbiór zawierający wszystkie elementy zbiorów . Z twierdzenia wynika, że możemy stworzyć funkcję . Z naszego twierdzenia wynika też, że dla każdego , może przyjmować dowolne wartości należące do . Niech więc funkcja przyjmuje tylko te wartości, które należą do jej argumentów (którymi są zbiory). Przeciwdziedzina jest selektorem , którego istnienie postuluje AC, a jest funkcją wyboru postulowaną przez AC. Każdy ze zbiorów z definicji funkcji ma tylko jeden element wspólny z , co odpowiada treści AC. Ponieważ:

,to w takim razie:

I równie dobrze moglibyśmy je przyjąć jako ostatni aksjomat teorii ZFC, a AC nazywać twierdzeniem, ale przyjęło się przyjmować AC jako aksjomat.

**Podzbiór odpowiedniej mocy**

Dla dowolnych zbiorów i (także nieskończonych), posiada podzbiór równoliczny z :

Jeżeli , to dla dowolnego , , możemy założyć więc, że . Z definicji mocy i relacji porządku między mocami w teorii mnogości, jeżeli , to możemy utworzyć funkcję , która będzie suriekcją, ale nie iniekcją. Utworzymy następującą relację równoważności na zbiorze , dla jego elementów:

Relacja jest zwrotna, bo dla dowolnego , . Jest ona symetryczna, bo jeżeli . Jest ona przechodnia, bo jeżeli , to wtedy . Czyli jest to relacja równoważności i dzieli zbiór na klasy równoważności . W każdej z klas zebrane są elementy o tej samej wartości funkcji .

Teraz korzystamy z aksjomatu wyboru dla przestrzeni ilorazowej . Utworzony selektor posiada po jednym elemencie z każdej klasy , więc , będzie iniekcją, bo dla każdego elementu przyjmuje inną wartość. Będzie ona również suriekcją, bo każdemu elementowi z można przyporządkować klasę , a ponieważ w zbiorze jest tyle elementów co klas w , to każdemu elementowi zbioru można przyporządkować jeden element z . Czyli pokrywa cały zbiór . Ponieważ będzie bijekcją wynika z tego: . , ponieważ . Więc jest podzbiorem o szukanych własnościach.

**Moc grupy i podgrupy**

Nieco więcej o tych strukturach będzie w rozdziale 6. Na razie zadowolimy się informacją, że grupa to zbiór ze zdefiniowanym na nim działaniem , oznacza się go które jest:

1. Wewnętrzne:
2. Łączne:
3. Elementy neutralny:
4. Odwracalne:

Jeżeli działanie jest przemienne, to grupę nazywamy abelową. Moc zbioru określa się jako rząd grupy. Jeżeli , który spełnia definicję grupy dla działania , oraz to nazywamy podgrupą. Jeżeli , to jest to podgrupa trywialna, zawierająca tylko element neutralny . W wypadku dla którego w nie istnieje podgrupa nietrywialna, to grupę nazywamy grupą prostą. Twierdzenie Lagrange’a mówi, że:

*Dla grupy skończonego rzędu, jej rząd jest podzielny przez rząd jej dowolnej podgrupy.*

W dowodzie wykorzystamy relację równoważności związaną z konkretną, dowolnie wybraną podgrupą . Dwa elementy uznajemy za równoważne:

Relacja jest zwrotna, bo , a z warunku elementu neutralnego. Relacja jest symetryczna, ponieważ :

Więc z warunku odwracalności dla wynika:. Relacja jest przechodnia, ponieważ jeżeli to z warunku wewnętrzności: . Korzystając z łączności działania dla tych wyrażeń:

Czyli jest to relacja równoważności, która podzieli grupę na rozłączne podzbiory. W teorii grup częściej niż klasami nazywa się te zbiory warstwami grupy i zapisuje jako , gdzie i jest ono reprezentantem tej warstwy. Każda taka warstwa ma szczególną cechę:

Nasze działanie nie musi być przemienne, wtedy wprowadza się analogiczną relację , na zasadzie: . Wtedy dostajemy:

Warstwy nazywa się lewostronnymi a warstwy nazywa się prawostronnymi. W grupach abelowych pojęcia te są tożsame: i nazywa się je po prostu warstwami. Nasza podgrupa również będzie jedną z tych warstw, możemy ją oznaczyć jako . Z warunku elementu neutralnego musi ona go zawierać, a każdy element może należeć tylko do jednej z warstw. Z tego też wynika, że jest to jedyna podgrupa wśród tych warstw. Teraz należy dowieść, że wszystkie te warstwy będą równoliczne. W grupach działanie ma taką cechę, że:

Jest ona nazywana prawem skreśleń lub skracania. Wynika z niej, że w działaniu z każdym elementem z daje inny wynik i będzie ich tyle co w zbiorze . Uzyskane wyniki nie zależą od wyboru reprezentanta z danej warstwy. Ponieważ w danej warstwie znajdują się tylko takie elementy, że dla dowolnych dwóch elementów z tej warstwy: z symetrii także wynika: , to działając przez odpowiedni element z :

Wynika z tego, że niezależnie od wybranego elementu uzyskamy całą warstwę działając przez elementy z . Wszystkie elementy w dla tej warstwy będą postaci , wynika to z prawa skracania. Dlatego po wybraniu reprezentanta z każdym elementem z możemy jednoznacznie powiązać każdy element warstwy i utworzyć bijekcję:

Co ostatecznie pokazuje, że zbiory te będą równoliczne. Jest to wyjątkowa cecha, ponieważ klasy abstrakcji w ogólności wcale nie muszą być równoliczne. Analogiczne własności posiadają także warstwy prawostronne. Będzie z tego wynikać, że: . Z twierdzenia o sumie mnogościowej klas równoważności dla tych warstw wynika:

Identycznie będzie też dla warstw prawostronnych:

Ze względu na rozłączność tych zbiorów, moc zbioru możemy zapisać jako:

A ponieważ nasze warstwy są równoliczne, to możemy to zapisać jako:

Gdzie oznacza oczywiście ilość tych warstw. Wynika z tego, że moc zbioru jest podzielna przez moc zbioru , co kończy dowód twierdzenia.

Uwaga! Twierdzenie odwrotne nie jest prawdziwe. To, że rząd grupy posiada dzielnik, nie świadczy, że posiada podgrupę tej mocy, choć może tak być w szczególnych przypadkach. Z twierdzenia wprost wynika, że grupa o rzędzie będącym liczbą pierwszą jest grupą prostą.

Język nowoczesnej teorii liczb

Choć teoria liczb jest dziedziną matematyki równie starą jak geometria euklidesowa, to wprowadzenie w niej dzielenia z resztą i zbiorów na początku XIX wieku otworzyło nowe możliwości w tej dziedzinie. Prawdziwy sens przy działaniach na tych liczbach wprowadzają dopiero pojęcia, które omówimy później, na razie pokażemy przykład zapisu kilku znanych pojęć i twierdzeń.

**Podzielność**

Jeżeli jedna liczba jest podzielna przez drugą, to dzieli się z resztą 0, czyli jeśli , to:

I jeżeli to możemy to zapisać jako:

**Chińskie twierdzenie o resztach**

Sformułowane w II wieku AD przez chińskiego matematyka Sun Zi. Aż strach pomyśleć w jakiej formie pierwotnie je wyrażono. Bez pojęcia przystawania możemy je sformułować tak: „jeżeli mamy dany zestaw liczb względnie pierwszych, to zawsze istnieje jedna taka liczba, mniejsza od ich iloczynu, że daje ona dowolne reszty przy dzieleniu przez te liczby”. Natomiast przy pomocy przystawań wyrażamy je tak:

Dla względnie pierwszych oraz:

Gdzie

**Twierdzenie Wilsona**

Oryginalnie było wyrażone jako: „Jeżeli p jest pierwsze to iloczyn liczb naturalnych od 1 do zwiększony o 1 jest podzielny przez p”. Po wprowadzeniu pojęcia silni zapisywano je tak:

, wprowadzając zbiory współcześnie zapisuje się je jako:

**Małe twierdzenie Fermata**

Fermat (a na 42 lata przed nim Jan Brożek) wyraził je następująco: „Jeżeli p jest liczbą pierwszą to dowolna liczba nie będąca jej wielokrotnością podniesiona do potęgi p-1 pomniejszona o 1 jest podzielna przez p”. Za pomocą przystawania można to uprościć:

Jak się później przekonamy wszystkie trzy zapisy są sobie równoważne.

**Twierdzenie Eulera**

Jest to uogólnienie Małego Twierdzenia Fermata. Mów ono, że dla dowolnej liczby b:

Gdzie to funkcja zwracająca liczbę liczb względnie pierwszych z daną liczbą i mniejszych od niej.

Jak widzimy wyrażenie twierdzeń teorii liczb w języku przystawania modulo jest bardzo przejrzyste i często upraszcza ich dowody w znaczący sposób. Jednak metody dowodzenia twierdzeń z teorii liczb przy pomocy przystawania wymagają połączenia relacji równoważności z algebrą i omówienia pojęcia kongruencji.

## 6.Kongruencje-działania na klasach równoważności

Choć w poprzednim rozdziale dzieliliśmy za pomocą relacji równoważności zbiór z określonym działaniem, to nie interesowało nas, czy relacja „zachowuje działanie”. Kongruencja jest to szczególny typ relacji równoważności na zbiorze , na którym określone są jakieś działania. Niech na naszym zbiorze będzie określone jakieś działanie, nazwijmy je . Kongruencja jest taką relacją równoważności, że dla dowolnych elementów:

Kongruencja musi zachowywać wszystkie działania zdefiniowane na tym zbiorze. To, czy dana relacja równoważności będzie kongruencją zależy od tego na jakim zbiorze ją wprowadzimy i jakie działania na nim zdefiniujemy.

Jeżeli mamy do czynienia z kongruencją na danym zbiorze z działaniem, wystarczy wykonywać je na samych reprezentantach klas równoważności i w nich oddawać wyniki. Kongruencje pozwalają przy konstrukcjach zbiorów przenosić działania ze zbiorów używanych do konstrukcji.

Przenoszenie działań za pomocą kongruencji

Przy przedstawionych wcześniej konstrukcjach zbiorów nie mówiliśmy nic o przenoszeniu działań z jednego zbioru na drugi, po prostu zakładaliśmy, że one przechodzą. Teraz czas je doprecyzować. Załóżmy, że mamy dany zbiór liczb naturalnych z działaniami mnożenia i dodawania Ich definicje można wprowadzić z teorii mnogości jako operacje na zbiorach o mocach odpowiadających tym liczbom. Pokażemy jak za pomocą kongruencji przenieść te działania na zbiory oraz .

**Zbiór liczb całkowitych**

Stworzyliśmy zbiór liczb jako zbiór par uporządkowanych liczb . Chcielibyśmy działania mnożenia i dodawania z przenieść na zbiór , tak aby stworzyć zbiór .

Działanie dodawania zdefiniujemy jako:

Teraz należy dowieść, że zachowuje ono klasę równoważności. Przypomnijmy jej definicję:

Chcemy wykazać, że dla dowolnych par:

zachodzi:

Z wprowadzonej właśnie definicji dodawania:

Z wcześniej wprowadzonej definicji równoważności par:

Sprowadziliśmy to do liczb naturalnych, teraz z definicji wiemy, że ponieważ i to i

, podstawiając:

Co dla liczb naturalnych jest zawsze prawdziwe. Działanie mnożenia najwygodniej jest opisać jako powtarzanie dodawania liczby samej ze sobą, a w przypadku mnożenia przez liczbę ujemną - liczby do niej przeciwnej. Ponieważ relacja jest kongruencją dla dodawania, będzie nią również dla mnożenia. Po wykonaniu tych zabiegów formalnych widzimy, że nasza relacja równoważności jest kongruencją i konstruuje zbiór .

**Zbiór liczb wymiernych**

Mamy zbiór . W następnej kolejności ze zbioru chcemy stworzyć zbiór .

Dodawanie dwóch liczb wymiernych wprowadzamy:

Chcemy udowodnić, że dla i zachodzi:

Z założenia przystawania par oraz :

Co jest prawdziwe dla dowolnych liczb całkowitych .

Mnożenie liczb wymiernych definiujemy w następujący sposób:

Chcemy dowieść, że dla par i zachodzi:

Stosując wprowadzoną definicję mnożenia:

Korzystając z definicji równoważności par:

Wiedząc, że pary i są równoważne:

Co jest prawdziwe dla dowolnych liczb całkowitych.

**Zbiór liczb rzeczywistych**

Na koniec celem będzie stworzenie zbioru . Mamy już zbiory oraz .

Dodawanie definiujemy za pomocą ciągów Cauchy’ego liczb reprezentujących liczby :

Chcemy dowieść, że dla oraz zachodzi:

Otrzymaliśmy prawdę matematyczną, co kończy dowód.

Mnożenie także definiowane jest za pomocą ciągów Cauchy’ego:

Analogicznie dowodzimy, że i :

Po raz kolejny otrzymanie prawdy matematycznej kończy dowód. Milcząco należało założyć, że (są to reprezentanci wszystkich ciągów wymiernych o tej granicy). Dlatego należy jeszcze pokazać trywialny przypadek, kiedy :

Otrzymanie prawdy matematycznej znów kończy dowód. Skonstruowaliśmy zbiór .

**Zbiory** **-arytmetyka modularna**

Zbiory stają się użytecznym narzędziem, kiedy zdefiniujemy na nich działania dodawania i mnożenia modulo przeniesione ze zbioru liczb całkowitych, tak aby stworzyć zbiór . Aby to zrobić musimy pokazać, że przystawanie modulo jest dla nich kongruencją (zazwyczaj w operacjach modularnych zapisuje się je po prostu ale po wyraźnym oznaczeniu operacji modularnych przez .

Jeśli chodzi o działanie dodawania dowód przeprowadza się następująco:

Weźmy cztery liczby całkowite , przy czym i . Chcemy udowodnić, że:

Przedstawiamy nasze liczby w rozkładzie dzielenia z resztą:

, , , :

Reszty z dzielenia przez n wyrażeń po obydwu stronach będą takie same:

Po obydwu stronach relacji przystawania mamy tę samą liczbę całkowitą, która ze względu na zwrotność relacji leży w tej samej klasie równoważności. Przystawanie jest kongruencją dla dodawania.

Dla działania mnożenia dowód będzie wyglądał następująco:

Dowodzimy, że dla I , czyli:

, , ,

Wszystko co ma wyraz dzieli się przez bez reszty:

Ponieważ po obydwu **stronach** relacji jest ta sama liczba, jej reszta z dzielenia przez n również będzie taka sama, czyli będzie w tej samej klasie równoważności.

Właśnie stworzyliśmy zbiór . Dopiero zdefiniowanie na nim działania dodawania nadaje prawdziwy sens liczbom ujemnym, jako elementów przeciwnych dodawania:

Dowolny zbór stanowi grupę. Niestety z działaniem mnożenia już tak nie jest. Tylko zbiory , gdzie jest liczbą pierwszą stanowią grupy (a raczej podzbiory , a zbiory ciała (inne struktury matematyczne), kiedy jest liczbą pierwszą. W ciele działania muczą być rozłączne względem siebie i każde z osobna musi stanowić grupę na zbiorze. A to właśnie na jednej z własności grup opiera się przystawanie liczb wymiernych(i tak nie wszystkich), dlatego możemy je definiować tylko dla ciał .

Do naszej relacji równoważności możemy włączyć liczby wymierne opierając się właśnie o własności grupy, konkretnie element neutralny i odwracalność.

Dla dodawania elementem odwrotnym jest liczba przeciwna czyli , a dla mnożenia będzie to liczba odwrotna, czyli . Problem polega na tym, że w zbiorach modulo n nie zawsze da się znaleźć element odwrotny dla każdego . Dla zbiorumożliwe jest to jedynie dla liczb względnie pierwszych z . Dlatego możliwe jest to wyłącznie w zbiorach , w których wszystkie liczby są względnie pierwsze z p, co wprost wynika z definicji liczby pierwszej.

Czemu więc nie wolno definiować odwrotności liczb, które nie są względnie pierwsze z ? Są one dzielnikami zera! Pokażemy to na przykładzie. Chyba każdy się zgodzi, że: . Spróbujcie sobie wyobrazić działanie:

Chyba lepiej sobie tego nie wyobrażać i pozostać przy liczbach wymiernych w … Na pocieszenie, w dowolnym jego podzbiór, mianowicie liczby względnie pierwsze z n stanowią z działaniem mnożenia grupę i ich odwrotności można zdefiniować w .

Używając tej metody możemy w ciałach odwrotność każdej liczby poza 0, oczywiście. Pokażmy to na przykładzie :

czyli

czyli oraz

czyli oraz

czyli

Przystawanie innych ułamków możemy uzyskać za pomocą mnożenia modulo. Na przykład:

W ten sposób możemy przedstawić modulo dowolną liczbę wymierną, której mianownik nie jest wielokrotnością i włączyć do naszych klas równoważności przynajmniej część liczb wymiernych. Ponieważ nie możemy przedstawić wszystkich, nie wolno nam stosować zapisu , choć bez wątpienia nasuwa się taka pokusa. Zresztą symbol w algebrze oznacza zupełnie co innego.

Dowodzenie twierdzeń z teorii liczb

Jak wcześniej kilka razy wspominałem, że za pomocą arytmetyki modularnej można w prosty, a zarazem precyzyjny sposób dowodzić twierdzenia z teorii liczb. Ponieważ dla działań mnożenia i dodawania przystawanie modularne jest kongruencją, to możemy zupełnie swobodnie wykonywać działania w arytmetyce modularnej i być pewni, że nasze rezultaty odnoszą się do dowolnych liczb reprezentowanych w tych działaniach. Choć można posługiwać się dowolnymi , to najwygodniej jest posługiwać się ciałami , właśnie ze względu na własności grupy dla mnożenia, oraz co jest związane z definiowaniem liczb wymiernych, w przystawaniach modulo p możemy podzielić obydwie strony przez dowolną niezerową liczbę z . Omówiliśmy już pojęcie podzielności i możemy brać się do roboty.

Sumy względnie pierwsze

Twierdzenie: Jeżeli mamy dwie liczby względnie pierwsze i , to ich suma będzie względnie pierwsza z oraz.

Jeżeli liczba ma być względnie pierwsza z obydwoma składnikami, to ich NWD=1. Aby tak było to nie może ona być podzielna przez żaden dzielnik pierwszy ani . Rozbijmy liczbę na czynniki pierwsze:

Jest oczywiste, że:

Ponieważ b jest względnie pierwsze z a, to b przystaje z niezerową resztą modulo dowolne . Natomiast ich suma:

Ponieważ b ma niezerową resztę modulo dowolne , to nie jest podzielna przez żaden z dzielników pierwszych a, a co za tym idzie również i złożonych. Dlatego . Powtarzając to rozumowanie, ale zamieniając a z b zauważymy, że także . Z tego twierdzenia wynika też, że jeśli jakaś liczba dzieli się przez drugą z resztą względnie pierwszą z nią, to będzie z nią względnie pierwsza.

Chińskie twierdzenie o resztach

Za pomocą kongruencji można podać szybki dowód kombinatoryczny chińskiego twierdzenia o resztach. Na początek chcemy dowieść, że w zbiorze dowolna n-ka reszt występuje tylko raz. Dla dowodu nie wprost załóżmy, że istnieje taka kombinacja reszt, która się powtarza dla dwóch różnych . Bez straty ogólności można założyć, że . Wtedy:

Z tego wynika, że dla liczby , która z założeń ma być większa od 0, ale mniejsza od liczby :

Czyli wynika z tego, że liczba jest podzielna przez każdą z liczb . Ale ponieważ liczby te były względnie pierwsze, to , czyli z tego wynika: , więc b nie należy do naszego zbioru, co daje sprzeczność. W każdym takim przedziale kombinacja reszt jest unikatowa.

Skoro wiemy, że w tym zbiorze każda kombinacja reszt jest unikatowa, obliczmy ilość tych kombinacji reszt. Skoro reszt modulo będzie , a kolejność reszt ma znaczenie, to w takim razie wszystkich tych kombinacji reszt będzie . Ponieważ nasz zbiór ma dokładnie tyle elementów i wiemy, że żadna kombinacja w nim się nie powtarza, to wystąpią w nim wszystkie kombinacje. Dowodzi to, że dla dowolnie wybranych reszt zawsze znajdzie się dokładnie jedna liczba w tym przedziale, która spełnia ten układ przystawań.

Twierdzenie Wilsona

Tutaj trzeba będzie skorzystać z własności grupy, które omówiliśmy w tym rozdziale. Na początek przedstawmy iloczyn modulo p:

Jest to iloczyn zawierający wszystkie niezerowe reszty modulo p. Teraz dowiedziemy, że w ciele każda liczba ma tylko jeden element odwrotny(nie licząc zera, ale ono nie wystąpi w tym iloczynie). Również najszybciej będzie tego dowieść nie wprost:

Wynikałoby z tego, że liczba pierwsza posiada dzielniki mniejsze od niej, co daje sprzeczność. I wynika z tego, że każdy element ma dokładnie jeden element odwrotny. Rozważmy teraz, które elementy są odwracalne „same z sobą”. W tym celu należy rozwiązać równanie:

Jak można się było spodziewać jest to element neutralny 1, oraz poza nim -1. Ze względu na przemienność i łączność działania, elementy odwracalne ze sobą można podobierać w pary:

Czyli wynika z tego , więc dla dowolnej liczby pierwszej, co dowodzi .

**Twierdzenie Eulera**

Najpierw dowiedziemy, że zbiór liczb względnie pierwszych z podstawą n tworzy grupę z działaniem mnożenia. Z własności wcześniej omówionych w tej pracy wiemy, że jeśli liczba jest względnie pierwsza z podstawą, to reszta z dzielenia przez tę liczbę również jest względnie pierwsza z n. Z własności kongruencji widzimy, że wobec tego działanie na tym zbiorze może reprezentować działanie na dowolnych liczbach względnie pierwszych z n. Dla mnożenia na tym zbiorze

1. Jest ono wewnętrzne:
2. Jest ono łączne, skoro jest łączne w , to jest łączne w jego podzbiorze.
3. Ma ono element neutralny, bo
4. Jest ono odwracalne, dowód nieco bardziej skomplikowany i włączający działanie dodawania modularnego. Dowodzi się prawa skreśleń nie wprost:

Co jest sprzeczne dla względnie pierwszego z i dowodzi, że dla różnych i wyniki muszą być różne. Mnożąc w ten sposób przez każdy element z tego zbioru można uzyskać cały zbiór, więc także i 1.

1. Jest ono przemienne: skoro było przemienne w , jest ono przemienne także w jego podzbiorze

Dlatego działanie to wraz z tym zbiorem daje grupę abelową, jej rząd wynosi . Teraz dowodzimy, że działanie potęgowania w tej grupie jest cykliczne i elementy tego cyklu będą stanowić podgrupę. Zgodnie z prawem skracania dla różnych , działanie daje różne wyniki dla tego samego i te same, kiedy jest takie samo. Łącząc prawo skracania z zasadą szufladkową: ponieważ jest dokładnie reszt z dzielenia w ciągu elementów przynajmniej jedna reszta musi się powtórzyć. Ponieważ jedyna operacja w tym ciągu to mnożenie przez , świadczy to o pojawieniu się jedynki. Ze względu na to kolejne potęgi będą dawać różne wyniki do momentu takiego , więc i cykl powtarza się od początku. Dowiedziemy, że zbiór wartości dodatnich potęg liczby stanowi grupę abelową z działaniem mnożenia.

1. Jest ono wewnętrzne:
2. Jest ono łączne, tak jak w całym zbiorze
3. Ma ono element neutralny, bo występuje w nim
4. Jest ono odwracalne:
5. I jest ono przemienne, tak jak w

Dlatego będzie stanowić grupę rzędu . Liczbę nazywamy rzędem elementu , a samo generatorem tej podgrupy . Z twierdzenia Lagrange’a, które jest zamieszczone w poprzednim rozdziale, wynika, że rząd dowolnej podgrupy jest dzielnikiem rzędu całej grupy, czyli: . I z tego wynika, że:

Co dowodzi na początku postawionej tezy.

**Małe Twierdzenie Fermata**

Jest to szczególny przypadek twierdzenia Eulera. Dla liczby pierwszej p:

Jeżeli to . Ponieważ , to:

I poprawność tezy wynika z twierdzenia Eulera.

**Trójki pitagorejskie**

W dowolnej pierwotnej (takiej, że wszystkie trzy liczby nie mają NWD>1) trójce pitagorejskiej jedna z liczb a lub b musi być podzielna przez 3. Skorzystamy z małego twierdzenia Fermata. Jeżeli trójka jest pierwotna, to przynajmniej dwie liczby mają niezerowe reszty modulo 3. Ponieważ te same liczby mają te same reszty z dzielenia, równość możemy zastąpić przystawaniem:

, czyli

Jeżeli , to z Małego twierdzenia Fermata:

Jeżeli , a jeżeli .

Czyli dostajemy lub . Otrzymana sprzeczność pokazuje nam, że a lub b jest podzielne przez 3, bo wtedy:

, co jest zgodne z prawdą.

## Bibliografia

K. Kuratowski, A. S. Mostowski *Teoria mnogości wraz ze wstępem do opisowej teorii mnogości*

W. Guzicki P. Zakrzewski *Wykłady ze wstępu do matematyki: wprowadzenie do teorii mnogości*

H. Rasiowa *Wstęp do matematyki współczesnej*

W. Marek, J. Onyszkiewicz *Elementy logiki i teorii mnogości w zadaniach*

Wikipedia-strony: *Para uporządkowana*, *Relacja(matematyka), Częściowy porządek, Porządek Liniowy, Dobry porządek, Relacja równoważności, Zasada abstrakcji, Aksjomaty i konstrukcje liczb, Grupa, Twierdzenie Lagrange’a(teoria grup), Kongruencja.*

## 7.Autorskie pomysły

**Dziwny zbiór**

Mamy zbiór liczb naturalnych , którego elementy mają tę własność, że suma dowolnych trzech jest liczbą pierwszą i . Jaka jest moc tego zbioru?

Rozważmy przystawanie elementów tego zbioru . Reszt z dzielenia przez 3 są 3. W zbiorze tym nie może być trzech takich samych reszt, bo:

Czyli taka suma byłaby podzielna przez 3, więc nie byłaby liczbą pierwszą. Z kombinatoryki wynika, że: , ponieważ w 7-elementowym zbiorze z zasady szufladkowej znajdą się trzy elementy, które będą miały tą samą resztę z dzielenia przez 3. Nie mogą w nim też występować razem wszystkie reszty, ponieważ:

Czyli wynika z tego, że , ponieważ w 5-elementowym zbiorze jeśli mamy maksymalnie dwie te same reszty z dzielenia przez 3, muszą pojawić się wszystkie. Ponieważ , to w takim razie . Teraz wystarczy tylko wskazać taki zbiór. Dowolna trójka liczb w nim musi być względnie pierwsza, bo jeżeli mają wspólny dzielnik k, to:

Więc jeśli , to liczba nie będzie pierwsza. Zbiorem tym będzie . Łatwo sprawdzić, że dowolna suma trzech liczb będzie pierwsza:

**(Nie)Dobry porządek**

W pracy wspominałem, że na dowolnym zbiorze przeliczalnym da się określić dobry porządek, choć nie koniecznie musi on się pokrywać z porządkiem powszechnie stosowanym. Do tworzenia dobrego porządku służą nam liczby porządkowe, również wspomniane w tej pracy. Liczby porządkowe same są zbiorami dobrego porządku przez relację opisaną w przykładzie 3 i tworząc bijekcję z takim zbiorem możemy tworzyć różne, nawet niestandardowe, dobre porządki. Uważny czytelnik zauważy, że niestandardowy porządek z przykładu 4 jest w ten sposób zbudowany na liczbie (użyta tu notacja ma w symboliczny sposób pokazywać funkcję miedzy ciągami):

Chcielibyśmy na zbiorze stworzyć dobry porządek na bazie liczby porządkowej . Przeprowadzimy to dwuetapowo. Najpierw utworzymy na dobry porządek korzystając z samego zbioru . Utworzymy między nimi bijekcję, nazwijmy ją , taką że . Liczby wymierne, najpierw dodatnie, ustawmy według rosnącej sumy licznika i mianownika, a jeżeli sumy te są równe porządkujemy się je według klasycznego porządku na zbiorze . Funkcja ta będzie ciągiem Jeśli jakaś liczba już się pojawiła w naszej sekwencji (jest ułamkiem skracalnym), to ją pomijamy. Ciąg ten wygląda tak:

Aby mieć w ciągu wszystkie liczby wymierne uzupełniamy go tak:

Ciąg ten tworzy bijekcję z w . W teorii mnogości używany jest do pokazywania równoliczności tych zbiorów. Teraz postaramy się stworzyć funkcję , taką, że: . Aby to zrobić najpierw zdefiniujemy dobry porządek na tym zbiorze, taki który będzie związany z liczbą . Żeby to zrobić, nieco zmodyfikujemy porządek z przykładu 3.

Liczby naturalne porządkujemy w następujący sposób: zero i jedynka standardowo, każdą inną według jej dzielników pierwszych. Rozbijamy liczbę na jej dzielniki pierwsze, ale nie będziemy ich łączyć w potęgi, jak to robi się tradycyjnie w teorii liczb. Utworzymy z nich niemalejący ciąg, który będzie reprezentował daną liczbę. Porządkujemy je według kryteriów dotyczących tych ciągów:

Jeżeli ciąg reprezentujący daną liczbę jest krótszy to liczba jest wcześniejsza.

Jeżeli ciągi reprezentujące daną liczbę są tej samej długości, stosujemy porządek leksykograficzny

Pokażemy na przykładzie:

Można udowodnić, że aby utworzyć ciąg odpowiadający temu porządkowi należy użyć zbioru .

Na początku liczby pierwsze(ciągi jednoelementowe) dają zbiór . W ciągach dwuelementowych uwzględniamy łańcuchów ciągów (w każdym łańcuchu ciągi rozpoczynają się od tej samej liczby pierwszej), z których każdy łańcuch zawiera ciągów, co daje moc . Uwzględniając ciągi o coraz większej liczbie elementów dostaniemy zbiory o mocy uwzględniając wszystkie dostaniemy . Ponieważ wszystkie ciągi są skończone, nie dostaniemy mocy większej od zbioru liczb naturalnych.

Na podstawie tego porządku tworzymy funkcję . Nasze liczby będą jej wartościami dla takich elementów:

, a nowy dobry porządek możemy zdefiniować za pomocą dobrego porządku wartości funkcji odwrotnej .

Z uzyskanych funkcji oraz tworzymy funkcję , którą zdefiniujemy . Funkcja ta tworzy przyporządkowanie , czyli po po prostu . Jest ona bijekcją, więc funkcja odwrotna również będzie bijekcją. Teraz tworzymy porządek na podstawie liczb porządkowych, które odpowiadają liczbom wymiernym. Możemy to wyrazić za pomocą funkcji odwrotnej:

Tak utworzony porządek będzie dobrym porządkiem w rozumieniu matematycznej definicji, ale z pewnością nie w potocznym rozumieniu tego wyrażenia!

**Sprawa dla profesora**

Postanowiłem rozważyć uogólnienie problemu zamieszczonego na koniec rozdziału 4 i zastąpić 10 dowolną liczbą naturalną. Dowodzenie zwrotności i symetrii jest identyczne jak w tamtym paragrafie. Przyjrzymy się tutaj bliżej przechodniości, którą tam omówiliśmy skrótowo. Zapiszemy nasze twierdzenie w języku wprowadzonej w rozdziale szóstym arytmetyki modularnej:

Dowody zwrotności i przechodniości stają się wówczas banalne i intuicyjne. Dowolna liczba odjęta od siebie samej daje zero, a zero przemnożone przez -1 daje zero. Teraz dokładniej przyjrzymy się przechodniości:

Teraz przyjrzyjmy się sumom iloczynów powstałym z rozwinięć dwumianu Newtona. W tamtym przykładzie tylko pokrótce je omówiliśmy:

Z tego widzimy, że jedynymi wyrazami w tych szeregach, dla których nie ma gwarancji podzielności przez n, są te, dla których . Szczęśliwie one się odejmują. Stosujemy podstawienie:

Teraz widzimy, że:

Widzimy teraz, że dla dowolnego n, nie tylko 10 jest to relacja równoważności. Ciekawsze staje się natomiast wyznaczenie klas równoważności. W przykładzie zrobiliśmy to metodą siłową, co w wypadku ogólnym jest praktycznie niemożliwe. Trzeba to zrobić sprytną metodą i postarać się znaleźć jakąś ogólną regułę przynależności do klas. Łatwiej wyrazimy to w ten sposób:

Co prawda ciężko zauważyć tę regułę dla tak małego zbioru jak , w którym są tylko cztery klasy i 10 liczb, ale można pokusić się o sformułowanie następującego twierdzenia:

**Autorskie Twierdzenie**

*Do jednej klasy abstrakcji związanej z niniejszą relacją równoważności:*

*Należą te i tylko te liczby z , dla których przecięcie zbioru dzielników pierwszych ze zbiorem dzielników pierwszych n jest takie samo.*

Uważny czytelnik zauważy, że postawiony warunek wyznacza relację równoważności. Pytanie tylko, czy podział na klasy zawsze będzie dokładnie taki sam. Nieintuicyjne wydaje się także zupełne zignorowanie potęg w rozkładzie na czynniki pierwsze. Z tej definicji wynika, że liczą się tylko same liczby pierwsze. Aby udowodnić to karkołomne twierdzenie będziemy musieli posłużyć się rozmaitymi narzędziami przedstawionymi wcześniej w tej pracy: arytmetyką modularną, chińskim twierdzeniem o resztach, twierdzeniem Eulera, oraz funkcją Eulera, która z tematem ma znacznie więcej wspólnego niżby się mogło na pierwszy rzut oka wydawać.

Zacznijmy od omówienia i uargumentowania kliku ciekawych i użytecznych własności tej funkcji. Jak dobrze pamiętamy dla dowolnej liczby naturalnej zwraca ona liczbę liczb względnie z nią pierwszych, które są od niej nie większe.

Własność 1:

*Dla dowolnej liczby pierwszej .*

Jest to własność trywialna. Dowolna liczba pierwsza jest podzielna tylko przez 1 oraz siebie samą. Wszystkich liczb od 1 do p jest p. Jedyna liczba, która nie jest z nią względnie pierwsza, to ona sama. Należy więc odjąć 1.

Własność 2:

*Dla potęg liczby pierwszej: .*

Wyobraźmy sobie podział elementowego ciągu kolejnych liczb naturalnych na przedziały po p elementów każdy. Tych przedziałów jest . W każdym jest liczb względnie pierwszych z p.

Własność 3:

*Dla dwóch liczb względnie pierwszych*

Szukamy wszystkich liczb względnie pierwszych zarówno z a jak i z b w przedziale od 1 do ab. Każdej z nich można przypisać kombinację reszt z dzielenia przez a i b, tak jak w chińskim twierdzeniu o resztach. Względnie pierwsze z nimi obydwiema będą te dla których względnie pierwsze są obydwie reszty. Reszt względnie pierwszych z a jest , a tych względnie pierwszych z b jest , czyli wszystkich kombinacji będzie .

Z tych własności jasno wynika, że możemy obliczyć , znając rozkład n na czynniki pierwsze, ponieważ dowolne liczby pierwsze są względnie pierwsze.

Jeżeli , to .

Własność 4

*Dla dowolnej*

Własność być może mało interesująca dla teoretyków liczb, ale zbawienna dla dowodu naszego twierdzenia. Dowiedziemy przez indukcję matematyczną:

Dla twierdzenie zachodzi. Dowolna liczba pierwsza jest większa od 1.

Z założenia indukcyjnego zachodzi dla , dowodzimy dla :

Ponieważ była większa od n, to suma p -1 z pewnością będzie większa od 1. Ta własność będzie nam bardzo przydatna.

Teraz dowiedziemy następujący lemat:

**Lemat**

*Dla dowolnych liczb a, b i n zachodzi przystawanie .*

Lemat karkołomny w dowodzie, chyba że ma się dobry pomysł jak to zrobić. Dla liczb względnie pierwszych z n własność ta wynika z twierdzenia Eulera. Aby je uogólnić, należy jej dowieść dla całej reszty. Dowiedźmy go najpierw dla dowolnego dzielnika pierwszego n.

Pamiętajmy, że tu nie możemy już bezkarnie dzielić stronami! Te liczby nie są względnie pierwsze z podstawą modularną! Aby ułatwić sobie zadanie skorzystajmy z chińskiego twierdzenia o resztach i zamieńmy jedno przystawanie na ich układ. Na liczby względnie pierwsze podzielmy n w prosty sposób. Podstawami nowych przystawań niech będą jego dzielniki pierwsze w potęgach, w których występują w rozkładzie n. Ponieważ z omówionych własności funkcji wynika, że zastosujemy twierdzenie Eulera w następujący sposób:

I będzie to prawdziwe dla wszystkich . Dla j należy przypadek rozpatrzeć osobno. I tu zbawienna okaże się własność numer 4. Liczba nie będzie względnie pierwsza z , dlatego tu nie wolno stosować twierdzenia Eulera! Za to z własności 4 mamy:

I to bardzo upraszcza sprawę:

I dostaliśmy w ten sposób układ reszt, który odpowiada liczbie pierwszej podniesionej do potęgi . Z chińskiego twierdzenia o resztach wynika, że spełnia go tylko jedna liczba w zbiorze . Teraz rozważmy potęgowanie tej liczby:

Widzimy, że reszty się nie zmieniły i układ kongruencji będzie spełniać ta sama liczba w .

Teraz kiedy dowiedliśmy tej własności dla dzielników pierwszych n jest już prosto dowieść jej dla liczb złożonych wykorzystując przemienność mnożenia w wykładnikach i rozdzielność mnożenia względem potęgowania.

I z udowodnionej własności wynika przystawanie:

Dodatkowo z twierdzenia Eulera wynika, że wszystkie liczby pierwsze nie będące dzielnikami n zostaną skasowane poprzez zamianę w jedynkę w mnożeniu. Oznaczmy dzielniki pierwsze wspólne dla a i n przez i mamy:

Tak więc:

Z pokazanych własności wynika także:

Co zarówno kończy dowód tego niezwykłego lematu i pokazuje jasno i wyraźnie dlaczego liczą się same dzielniki pierwsze bez uwzględnienia potęg!

**Twierdzenie**

Z lematu wynika, że liczby, które posiadają te same dzielniki pierwsze, które dzielą n należą do jednej klasy abstrakcji. Teraz należy wykazać, że jeżeli dwie liczby są równoważne, to jedna nie może posiadać żadnych dzielników pierwszych n, których nie miałaby ta druga. Dowiedziemy tego nie wprost:

Zakładamy że liczba b równoważna liczbie a posiada dzielniki pierwsze n ,których nie posiada ta druga. Na początek, aby skasować resztę dzielników pierwszych podnieśmy je obydwie do . Możemy tak zrobić, bo jeżeli:

Dlatego podnosimy je do :

Nie możemy tu bezpiecznie dzielić, ale zawsze możemy bezpiecznie odejmować:

I teraz należy wykazać, że nie może być to prawda. Posłużmy się podstawieniem:

Oczywiście w grupach modulo n w ogólności występują dzielniki zera. Wyrażenie x nie może przystawać 0, ponieważ aby było podzielne przez n musi być podzielne przez wszystkie jego dzielniki pierwsze, nie jest zaś podzielne przez . Aby całość wyrażenia była podzielna przez n, to y musi być podzielne przez wszystkie brakujące dzielniki. Jednak ponieważ przez wszystkie dzieli się z resztą -1 będzie z nimi względnie pierwsze! Czyli iloczyn ten nie może przystawać 0, co daje sprzeczność!

I z tego wynika, że w jednej klasie abstrakcji leżą te i tylko te liczby z , które są podzielne przez wszystkie liczby z określonego podzbioru dzielników pierwszych liczby n. Jest to równoważne treści Autorskiego Twierdzenia. *Quod Erat Demonstratum!*

Na zakończenie „sprawy dla profesora” mieliśmy pokazać sposób wyznaczania klas równoważności i mocy przestrzeni ilorazowej. Z twierdzenia jasno wynika, że każdą klasę możemy jednoznacznie utożsamić z pewnym podzbiorem zbioru dzielników pierwszych liczby n. W szczególności: klasę utożsamiamy ze zbiorem pustym i zawiera ona wszystkie liczby względnie pierwsze z n, zaś klasę utożsamiamy z podzbiorem niewłaściwym. Dla n będących liczbami pierwszymi są to jedyne klasy ich przestrzeni ilorazowej. Z tego wynika, że klas będzie tyle, ile podzbiorów zbioru dzielników pierwszych n. Z kombinatoryki wynika, że jest to , gdzie x to ilość różnych dzielników pierwszych n. Profesor byłby zadowolony.

*Dodatkowe ciekawostki*

Ponadto wynika, że w każdej z klas znajduje się dokładnie jeden element niezmienny względem potęgowania modularnego. Jednak tylko klasa spełnia warunki grupy, ponieważ tylko w niej jest to element neutralny tego działania. Co ciekawe działanie mnożenia w klasach jest wewnętrzne i łączne, ale tylko w klasie jest ono odwracalne. Dzielniki zera występują tylko w klasie . Każdy element niezmienny możemy wyznaczyć albo podnosząc liczbę z jego klasy do , albo rozwiązując układ kongruencji z dzielnikami pierwszymi n, odpowiadający danej klasie. W układach tych są tylko zera i jedynki(jedynka dla dzielnika pierwszego n, którego nie mają liczby z klasy), co ponownie daje elementów niezmiennych i klas abstrakcji. W klasie mamy układ kongruencji z samymi jedynkami i z tego wynika, że elementem tym jest 1. Nasz lemat (z układem do rozwiązania, by wyznaczyć element) jest więc uogólnieniem Twierdzenia Eulera z liczb względnie pierwszych z n na dowolne liczby zbioru modulo n.

**Przykłady**

Aby nieco przybliżyć abstrakcyjne ☺ idee w tym dowodzie zanalizujmy konkretne przykłady. Zacznijmy od liczby 10, która pochodzi z oryginalnego zadania. Z siłowego rozwiązania można odczytać:

Jak widzimy w klasie jest tylko jedna liczba. Jest to cech wspólna dla tych n, które w rozkładzie na czynniki mają tylko pierwszą potęgę. W klasie 1 leżą wszystkie liczby względnie pierwsze, wszystkie liczby z klasy 2 są podzielne przez 2, a z klasy 5 przez 5.

Rozważmy n=12, n=15, n=25 i n=30. Wytrwały czytelnik może samodzielnie sprawdzić wyniki, a pasjonat informatyki zaprząc komputer do pracy:

Teraz wyniki dla znacznie większych liczb. Ponieważ funkcja tak statystycznie (bo nie ściśle) rośnie dosyć szybko, to poważnym problemem jest wykonywanie ciągów potęgowań reszt, zwłaszcza liczb względnie pierwszych(prawo skreśleń!).Nie podejmuję się wyznaczania klas abstrakcji, a tym bardziej potęgowania elementów!

Jak więc widzimy, lepiej stworzyć ładną teorię i abstrakcyjnie dowieść jej skuteczności, bo niektóre przypadki mogą być nieco cięższe do siłowego złamania.

## Posłowie

To już koniec naszej podróży przez świat relacji. Oczywiście zachęcam do samodzielnego powrotu do niego, choć przyznaję, że bez przewodnika czasem ciężko przedzierać się przez gąszcz abstrakcyjnych obiektów i twierdzeń, jednak każda taka wycieczka powoduje, że stajemy się coraz mądrzejsi i coraz głupsi za razem. Im większy staje się zasięg światła, tym coraz większy staje się też krąg ciemności dookoła nas. Na szczęście pole rośnie proporcjonalnie do kwadratu promienia, o obwód tylko liniowo.

Chciałbym podziękować panu Profesorowi, który był skłonny poświęcić kilka dni swojego cennego czasu, aby poprowadzić dla nas warsztaty matematyczne. Dzięki takim warsztatom młodzież zainteresowana może choć przez chwilę zetknąć się z matematyką o poziomie nieco wyższym niż w szkole i przy okazji miło spędzić czas.

Większość przykładów w rozdziałach od 2 do 5 wymyśliłem samodzielnie. Konstrukcje liczbowe z rozdziału 5 i 6 są powszechnie znane. Jako ich źródło można uznać stronę na Wikipedii „aksjomaty i konstrukcje liczb” oraz załączoną do niej bibliografię znacznie bardziej obszerną niż moja. Twierdzenie Lagrange’a dla grup i pomysł jego dowodu znalazłem na Wikipedii, choć przeredagowałem go żeby był bardziej czytelny. Na pomysł dwóch pozostałych wpadłem sam, choć są na tyle oczywiste, że zapewne można je znaleźć w jakiejś literaturze.

Wszystkie pomysły w rozdziale 7 wymyśliłem samodzielnie, choć wyznaczanie zbioru przy użyciu arytmetyki modularnej jest jedynie zaproponowanym przeze mnie rozwiązaniem zadania z książki „Zadania na cztery pory roku”, zadanego podczas szkolnego koła matematycznego. Dobry porządek również jest moim pomysłem. Jestem pewien, że stworzono wiele przykładów dobrych porządków izomorficznych z tą konkretną liczbą porządkową, choć jedyny przykład bijekcji w ten zbiór, jaki spotkałem pochodzi z „Księgi liczb”. Co prawda wykorzystywał on liczby pierwsze, jednak sformułowanie było nieco inne, a ja metodę konstrukcji zastosowałem do utworzenia dobrego porządku, o czym w ogóle nie było w tej publikacji. Twierdzenie o przynależności do tych klas abstrakcji sformułowałem i udowodniłem samodzielnie. Jeżeli ktoś już coś podobnego udowodnił, nic o tym fakcie nie wiem. Nawet jeśli tak, to jest ono na tyle piękne, że warto je było wymyślić.

Dziękuję za wytrwałą lekturę tej pracy.