SPIS TREŚCI:

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 $\mathbb{N}$ 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:

$$(x;y) \stackrel{\text{def}}{=} \big\{\{\{x\},\emptyset\},\{\{y\}\}\big\}$$

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 $x = y$. Wzięcie elementów w podwójne klamry zbiorów dodatkowo zabezpiecza przed problemem „kasowania".

Definicja Hausdorffa

Alternatywną definicję zaproponował Felix Hausdorff:

$$(x;y) \stackrel{\text{def}}{=} \big\{\{x,1\},\{y,2\}\big\}$$

Gdzie x oraz y 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 $x\ i\ y$, w przeciwnym wypadku powróci problem kasowania elementów w zbiorze.

Definicja Kuratowskiego

Kazimierz Kuratowski przedstawił do dziś najpowszechniej stosowaną definicję:

$$(x;y) \stackrel{\text{def}}{=} \big\{\{x\},\{x,y\}\big\}$$

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 $y = x$ co prawda nastąpi „skasowanie":

$$(x;x) = \big\{\{x\},\{x,x\}\big\} = \big\{\{x\},\{x\}\big\} = \big\{\{x\}\big\}$$

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:

$$(x; y; z) \stackrel{\text{def}}{=} (x; (y; z))$$
$$(x; y; z; v) \stackrel{\text{def}}{=} \big(x; (y; z; v)\big) = (x; (y; (z; v)))$$
$$\vdots$$

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:

$$(a_1; a_2; \dots; a_n; a_{n+1}) \stackrel{\text{def}}{=} (a_1; (a_2; \dots; a_n; a_{n+1}))$$

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:

$$\mathcal{X} \times \mathcal{Y} = \{(x; y): x \in \mathcal{X} \wedge\ y \in \mathcal{Y}\}$$

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

Dla dowolnych niepustych zbiorów X i Y możemy stworzyć ich iloczyn kartezjański $X \times Y$.

Najpierw udowodnimy, że dla dowolnych elementów $x \in X$ i $y \in Y$ możemy stworzyć parę uporządkowaną $(x; y)$. Skorzystamy tu z definicji pary Kuratowskiego. Z aksjomatu wyboru: $\exists\{x\}, \{y\}$. Z aksjomatu sumy: $\exists\{x\} \cup \{y\} = \{x, y\}$. Z aksjomatu pary:

$$\exists\big\{\{x\}, \{x, y\}\big\} = (x, y)$$

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

Z aksjomatu pary dla $\forall(x; y)\exists\{(x; y)\}$ i z aksjomatu sumy dla wszystkich $\{(x; y)\}$ istnieje $\cup\{(x; y)\}$. Jest to zbiór zawierający wszystkie pary uporządkowane, czyli $X \times Y$.

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.

$$X_1 \times X_2 \times X_3 \times \cdots = X_1 \times (X_2 \times X_3 \times \cdots) = X_1 \times Y$$

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!):

$$\mathcal{X} \times \mathcal{X} = \mathcal{X}^2$$
$$\mathcal{X} \times \mathcal{X} \times \mathcal{X} = \mathcal{X}^2 \times \mathcal{X} = \mathcal{X}^3$$

$$\mathcal{X} \times \mathcal{X} \times \mathcal{X} \times \mathcal{X} = \mathcal{X}^3 \times \mathcal{X} = \mathcal{X}^4$$
$$\vdots$$

Gdzie elementy kolejnych z tych zbiorów będą kolejnymi n-kami uporządkowanymi o współrzędnych z tego samego zbioru $\mathcal{X}$.

2.Ścisła definicja relacji

W ogólności relacja $\mathcal{R}$ jest dowolnym podzbiorem iloczynu kartezjańskiego skończonej liczby zbiorów $\mathcal{S}_1, \mathcal{S}_2, \dots, \mathcal{S}_n$.

$$\mathcal{R} \subseteq \mathcal{S}_1 \times \mathcal{S}_2 \times \dots \times \mathcal{S}_n$$

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

$$(a_1, a_2, \dots, a_n) \in \mathcal{R}$$

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

$$x\mathcal{R}y$$

Gdzie x oraz y 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 $\mathcal{X}^2$, wtedy mówi się krótko: „relacja na zbiorze $\mathcal{X}$".

Przykład 1

Relacją zadaną prostym warunkiem jest relacja podzielności na zbiorze liczb $\mathbb{Z}$. Oznacza się ją $a|b$.

$$(a; b) \in \mathcal{R} \Leftrightarrow \exists c \in \mathbb{Z}: b = a \cdot c$$

Do tej relacji należą np. pary $(2;\ 4), (43;\ 86), (1;\ 5), (7;\ -7), (9;\ 0), \dots$

Ale nie należą pary:$(0;\ 3), (2;\ 7), (86;\ 43), (9;\ 3), (11;\ 1)$ …

Przykład 2

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

$$(A; A), (A; B), (B; B), (C; A), (A; C), (C; D), (C; B)$$

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

$$\begin{bmatrix} (\mathrm{A};\mathrm{A}) & (\mathrm{B};\mathrm{A}) & (\mathrm{C};\mathrm{A}) & (\mathrm{D};\mathrm{A}) \\ (\mathrm{A};\mathrm{B}) & (\mathrm{B};\mathrm{B}) & (\mathrm{C};\mathrm{B}) & (\mathrm{D};\mathrm{B}) \\ (\mathrm{A};\mathrm{C}) & (\mathrm{B};\mathrm{C}) & (\mathrm{C};\mathrm{C}) & (\mathrm{D};\mathrm{C}) \\ (\mathrm{A};\mathrm{D}) & (\mathrm{B};\mathrm{D}) & (\mathrm{C};\mathrm{D}) & (\mathrm{D};\mathrm{D}) \end{bmatrix}$$

Taka relacja chyba niewiele ciekawego sobą przedstawia i raczej nie jest warta większej uwagi. W tych przykładach stosowaliśmy relację na zbiorach typu $\mathcal{X}^2$, były to $\mathbb{Z}^2$ oraz $\{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}\}^2$, 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 $\mathcal{X}$ jest dziedziną, a $\mathcal{Y}$ przeciwdziedziną. Oczywiście że zbiory $\mathcal{X}$ i $\mathcal{Y}$ mogą być zupełnie różnymi zbiorami, więc tu nie musi być to relacja na zbiorze $\mathcal{X}^2$(choć w szczególnych przypadkach może tak być).

Funkcja $f: \mathcal{X} \to \mathcal{Y}$, to relacja $\mathcal{R} \subset \mathcal{X} \times \mathcal{Y}$, taka że dla każdego elementu ze zbioru $\mathcal{X}$ istnieje dokładnie jeden element ze zbioru $\mathcal{Y}$ będący z nim w relacji. W logicznym języku zapisujemy to tak:

$$\forall x \in \mathcal{X}\ \exists y \in \mathcal{Y}: (x; y) \in \mathcal{R}$$
$$(x; y_1) \in \mathcal{R} \wedge (x; y_2) \in \mathcal{R} \Rightarrow y_1 = y_2$$

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:

$$\forall x \in \mathcal{X}\ \exists y \in \mathcal{Y}: (x; y) \in \mathcal{R}$$
$$(x; y_1) \in \mathcal{R} \wedge (x; y_2) \in \mathcal{R} \Rightarrow y_1 = y_2$$
$$(x_1; y) \in \mathcal{R} \wedge (x_2; y) \in \mathcal{R} \Rightarrow x_1 = x_2$$

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

$$\forall x \in \mathcal{X}\ \exists y \in \mathcal{Y}: (x; y) \in \mathcal{R}$$
$$(x; y_1) \in \mathcal{R} \wedge (x; y_2) \in \mathcal{R} \Rightarrow y_1 = y_2$$
$$\forall y \in \mathcal{Y}\ \exists x \in \mathcal{X}: (x; y) \in \mathcal{R}$$

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:

$$\forall x \in \mathcal{X}\ \exists y \in \mathcal{Y}: (x; y) \in \mathcal{R}$$
$$\forall y \in \mathcal{Y}\ \exists x \in \mathcal{X}: (x; y) \in \mathcal{R}$$
$$(x; y_1) \in \mathcal{R} \wedge (x; y_2) \in \mathcal{R} \Rightarrow y_1 = y_2$$
$$(x_1; y) \in \mathcal{R} \wedge (x_2; y) \in \mathcal{R} \Rightarrow x_1 = x_2$$

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 $(x; x)$ jest w relacji.

- relacja równości (x jest równy x)
- relacja podzielności w zbiorze $\mathbb{Z}/\{0\}$(niezerowa liczba dzieli samą siebie)
- relacja równoległości prostych(dowolna prosta jest równoległa do siebie samej)

Przeciwzwrotność

Polega na tym, że żadna z par $(x; x)$ 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 $(x; y)$ jest w relacji, to wynika z tego, że $(y; x)$ 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 $(x; y)$ należy do relacji, to wynika z tego, że $(y; x)$ 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 $(x; y)$ i para $(y; z)$ należy do relacji to para $(x; z)$ 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 x i y, to któraś z par:$(x; y)$ lub $(y; x)$ 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 x i y 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 x i y 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 $\preccurlyeq$ na zbiorze(lub ogólniej, klasie) X musi mieć dwie cechy:

(1)przechodniość:

$$x, y, z \in X, x \preccurlyeq y \wedge y \preccurlyeq z \Rightarrow x \preccurlyeq z$$

(2)antysymetria:

$$x, y \in X, \qquad x \preccurlyeq y \Rightarrow y \not\preccurlyeq x$$

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 $\preccurlyeq$ i silny(zwany ostrym) $\prec$.

Porządek słaby cechuje się zwrotnością, czyli:

$$\forall x \in X, x \preccurlyeq x$$

Natomiast w porządku silnym występuje przeciwzwrotność:

$$\forall x \in X, x \not\prec x$$

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

$$x \prec y \Leftrightarrow (x \preccurlyeq y \wedge x \neq y)$$

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:

$$\forall x, y \in X, x \preccurlyeq y \vee y \preccurlyeq x$$

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

$$\forall A \colon A \subseteq X, \exists x \in A \colon \forall y \in A \colon x \preccurlyeq y$$

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:

$$\forall x, y \in X \wedge x \prec y \exists z \colon x \prec z \prec y$$

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:

$$0 = \emptyset$$
$$1 = \{0\}$$
$$2 = \{0, 1\}$$
$$3 = \{0,1,2\}$$
$$4 = \{0,1,2,3\}$$
$$\vdots$$

Możemy zdefiniować relację porządku słabego na danej zasadzie:

$$a = \{0,1, \dots, a-1\} \subseteq b = \{0,1, \dots, b-1\} \Longrightarrow a \leq b$$

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:

$$a \in b = \{0,1, \dots, b-1\} \Leftrightarrow a < b$$

Dzięki temu możemy wprowadzić porządek na całym zbiorze:

$$0 < 1 < 2 < 3 < 4 < 5 < 6 < 7 < \cdots$$

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:

$$A < B < C < D < E < \cdots < X < Y < Z$$

Dzieje się tak ponieważ każdemu elementowi zbioru $\{A, B, C, \dots, Z\}$ przypisaliśmy liczbę naturalną, na podstawie, której oznaczamy ich kolejność.:

$$0 \to A, 1 \to B, 2 \to C, 3 \to D, 4 \to E, \dots, 24 \to Z$$

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:

$$\omega = \{0,1,2,3, \dots\}$$
$$\omega + n = \{0,1,2,3, \dots, \omega, \omega + 1, \dots, \omega + n - 1\}$$
$$2\omega = \{0,1,2,3 \dots, \omega, \omega + 1, \omega + 2, \dots\}$$
$$\omega^2 = \{0,1,2, \dots, \omega, \dots, 2\omega, \dots, 3\omega, \dots, \dots\}$$
$$\omega^\omega = \{0,1,2, \dots, \omega, \dots 2\omega, \dots, \dots, \omega^2, \dots, \dots, \omega^3, \dots, \dots, \omega^4, \dots, \dots, \dots\}$$

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

$$0 < 1 < 2 < \cdots < \omega < \cdots < \cdots < 2\omega < \cdots < \omega^2 < \cdots < \omega^\omega < \cdots$$

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.

$$0 < 1 < 2 < 3 < 5 < \cdots < 4 < 6 < 9 < \cdots < 8 < 12 < 18 < \cdots$$

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 a i b istnieje takie n, że $\forall k < n, a_k = b_k$, a $a_n \neq b_n$, to wtedy jeżeli $a_n \prec b_n$, to $a \prec b$.
(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 $a = b$.

Dla przykładu ze standardowego porządku w liczbach naturalnych:

$$(1,1,2,1) \prec (1,1,3,1)$$
$$(3,3,3) \prec (3,3,3,3,4,5)$$
$$(4,3,2,1) \prec (0,1,2,3,4,5,\dots)$$
$$(2,1,5) = (2,1,5)$$

4.Relacja równoważności

Relacja równoważności $\mathcal{R}$ na zbiorze $\mathcal{X}$ jest szczególną relacją dwuargumentową. Musi być ona:

Zwrotna

$$\forall x \in \mathcal{X}, (x; x) \in \mathcal{R}$$

Symetryczna

$$\forall x, y \in \mathcal{X}, (x; y) \in \mathcal{R} \Longrightarrow (y; x) \in \mathcal{R}$$

Przechodnia

$$\forall x, y, z \in \mathcal{X}, (x; y) \in \mathcal{R} \wedge (y; z) \in \mathcal{R} \Longrightarrow (x; z) \in \mathcal{R}$$

Jest ona niejako uogólnieniem pojęcia równości na znacznie szersze typy relacji i zbiorów. Zazwyczaj relację równoważności między dwoma elementami(nazwijmy je x i y) oznacza się poprzez $x \sim y$ lub $x \equiv y$. 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 $\sim$ definiujemy:

$[x]_{\sim} \stackrel{\text{def}}{=} \{y \in \mathcal{X} : y \sim x\}$

Czyli jest to zbiór wszystkich elementów będących ze sobą w relacji równoważności. Element x 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 $\sim$ na zbiorze $\mathcal{X}$ związane jest pojęcie przestrzeni ilorazowej $\mathcal{X}/_{\sim}$. Jest to zbiór zawierający wszystkie klasy równoważności tej relacji dla zbioru $\mathcal{X}$.

$$\mathcal{X}/_{\sim} = \{K : K = [x]_{\sim} \wedge x \in \mathcal{X}\}$$

Dla wybrednych matematyków można jeszcze uzasadnić istnienie tego zbioru. Z aksjomatu pary wynika istnienie dla każdego zbioru K zbioru $\{K, K\} = \{K\}$. Stosując do wszystkich zbiorów $\{K\}$ aksjomat sumy dostaniemy żądany zbiór $\mathcal{X}/_{\sim}$.

Ważne twierdzenia dotyczące relacji równoważności

Poniżej trochę oczywiste, ale bardzo istotne twierdzenia związane z relacjami równoważności na dowolnym zbiorze $\mathcal{X}$. 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 $\mathcal{X}$ 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 $\mathcal{X}$ będzie równoważny sobie samemu, istnienie elementów równoważnych sprawia, że nie może być pustej klasy.

2) Dowolny element zbioru $\mathcal{X}$ należy do jakiejś klasy abstrakcji.

Z warunku zwrotności $\forall x \in \mathcal{X}, x \sim x$ czyli jest w relacji z jakimś elementem, dlatego należy do klasy zawierającej przynajmniej jego samego, choćby była ona jednoelementowym zbiorem.

3) Suma mnogościowa wszystkich klas abstrakcji zbioru $\mathcal{X}$ daje zbiór $\mathcal{X}$.

Ponieważ dowolny element zbioru $\mathcal{X}$ należy do jakiejś klasy K , to wszystkie elementy zbioru należą do którejś z klas K i z definicji klasy abstrakcji, żadna nie zawiera elementu, którego nie zawiera $\mathcal{X}$. $\forall K \neg \exists x: x \in K \wedge x \notin \mathcal{X}$. Dlatego ich suma mnogościowa jest zbiorem mającym takie same elementy jak $\mathcal{X}$, czyli jest zbiorem $\mathcal{X}$ (aksjomat ekstensjalności).

4) Dwie różne klasy abstrakcji przecinają się pusto.

Niech dwie klasy $K_1 i\ K_2$posiadają niepuste przecięcie $P = K_1 \cap K_2$. Jeżeli jest ono niepuste, to $\exists e: e \in P$, czyli $e \in K_1 \wedge e \in K_2$. Z definicji klasy abstrakcji $\forall x: x \in K_1, x \sim e$ i $\forall y: y \in K_2, y \sim e$. Z warunku przechodniości relacji wynika, że: $\forall x \in K_1, y \in K_2, x \sim y$. Wynika z tego, że dowolne dwa elementy tych klas są w relacji równoważności, czyli $K_1 = K_2$. Otrzymana sprzeczność kończy dowód, czyli $K_1 \neq K_2 \Rightarrow K_1 \cap K_2 = \emptyset$.

5) 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.

6) 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 $K: x \sim y \Leftrightarrow x, y \in K$. 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 $x, y \in K$ i $y, z \in K$ to zbiór K zawiera elementy: x, y, z, więc $x, z \in K$. Czyli jest to relacja równoważności.

7) Klas abstrakcji nie może być więcej niż elementów zbioru

Stwórzmy funkcję $f: \mathcal{X} \to \mathcal{X}/_{\sim}$, zdefiniujmy ją jako: $f(x) = [x]$. Jest to suriekcja, ponieważ zgodnie z twierdzeniem 1 nie ma klas pustych, czyli każda klasa jest wartością co najmniej jeden elementu z $\mathcal{X}$. W myśl definicji mocy zbioru wziętych z teorii mnogości ponieważ możemy utworzyć suriekcję $f: \mathcal{X} \to \mathcal{X}/_{\sim}$, to w takim razie: $|\mathcal{X}/_{\sim}| \leq |\mathcal{X}|$

Przykłady relacji równoważności

Rodzeństwo

Mamy zbiór ludzi $\mathbb{L} = \{l_1, l_2, \dots, l_n\}$. Definiujemy na nim relację $\mathcal{R}$. 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 l_i ma tych samych rodziców co l_j, to jest oczywiste, że $l_j$ma tych samych rodziców, co l_i.

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

Dlatego relacja $\mathcal{R}$ podzieli zbiór $\mathbb{L}$ na rozłączne podzbiory $\Re_1, \dots, \Re_n$ 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 $\mathcal{S}$, a klasy szkolne jako $K_1, K_2, K_3, \dots, K_n$, a uczniów tej szkoły jako elementy $u_1, u_2, u_3, \dots, u_m \in \mathcal{S}$.

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

$$\forall i, j \in \{0,1, \dots, n\}: i \neq j, K_i \cap K_j = \emptyset$$

Każdy uczeń w szkole chodzi do jakiejś klasy:

$$\forall u_i: i \in \{0,1, \dots, m\}, u_i \in K_1 \vee \dots \vee u_i \in K_n$$

Ponieważ każdy element należy do którejś z klas i żaden nie należy do więcej niż jednej naraz, to rodzina $K_1, K_2, K_3, \dots, K_n$ jest podziałem zbioru $\mathcal{S}$ 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 a może być podzielona z resztą przez inną liczbę całkowitą b w postaci:

$$a = b \cdot n + r$$

Gdzie n należy do liczb całkowitych, a r do liczb naturalnych. Jeżeli a jest podzielna przez b, to wtedy $r = 0$.

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

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

$$a = b \cdot n + r_1 = c \cdot n + r_2$$
$$(b - c)n + r_1 = r_2$$
$$(b - c)n = r_2 - r_1$$

Reszta z dzielenia lewej strony przez n wynosi 0:

$$0 = r_2 - r_1$$

$$r_1 = r_2$$

Czyli przy dzieleniu przez n 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 n. Na przykład dla $n = 3$ będą one wyglądać w ten sposób:

$$[0]_3 = [\dots, -9, -6, -1, 0, 3, 6, 9, 12, \dots]$$

$$[1]_3 = [\dots, -8, -5, -2, 1, 4, 7, 10, 13, \dots]$$

$$[2]_3 = [\dots, -7, -4, -1, 2, 5, 8, 11, 14, \dots]$$

Przystawanie modulo n zapisuje się symbolem ≡ i zapisuje tak:

$$1 \equiv 4 \ (mod\ 3)$$

Zbiór $\mathbb{Z}$ ze zdefiniowaną relacją przystawania mod n oznacza się $\mathbb{Z}_n$.

Podzielna różnica potęg

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

$$a \sim b \Leftrightarrow \exists k \in \mathbb{N}: 10 | a^k - b^k$$

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

Relacja jest oczywiście zwrotna, bo: $a^k - a^k = 0$, a zero jest podzielne przez wszystko. Relacja jest także symetryczna z podzielności w liczbach całkowitych. $10 | a^k - b^k$, to:

$b^k - a^k = -(a^k - b^k)$ i również będzie podzielne przez 10. Problem jest z dowodem przechodniości relacji:

$$\begin{cases} a^m - b^m = 10k \\ b^n - c^n = 10l \end{cases}$$

$$\begin{cases} a^m = 10k + b^m \\ c^n = -10l + b^n \end{cases}$$

$$\begin{cases} a^{mn} = (10k + b^m)^n \\ c^{mn} = (b^n - 10l)^m \end{cases}$$

$$a^{mn} - c^{mn} = (10k + b^m)^n - (b^n - 10l)^m$$

$$a^{mn} - c^{mn} = 10S_1 + b^{mn} - b^{mn} + 10S_2$$

$$a^{mn} - c^{mn} = 10(S_1 + S_2)$$

Podstawione tu wartości S_1 S_2 odpowiadają wartościom $(10k + b^m)^n - b^{mn}$ oraz $(b^n - 10l)^m - b^{mn}$ podzielonym przez 10. Będą one podzielne przez 10, ponieważ usuwamy z sumy(powstałej z rozwinięcia wzoru w szereg dwumianu Newtona) niepewny element b^{mn}, 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:

0 0 0 0 0
1 1 1 1 1
2 4 8 6 2
3 9 7 1 3
4 6 4 6 4
5 5 5 5 5
6 6 6 6 6
7 9 3 1 7
8 4 2 6 8
9 1 9 1 9

Po zastosowaniu metody „z góry na dół” i „która cyferka się powtarza” widzimy, że mamy cztery klasy abstrakcji: $[0], [1], [2], [5]$. 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 $\mathbb{N}^2$. Liczby całkowite, czyli pary $(a; b)$, powinny odpowiadać wartościom wyrażenia$(a; b) = a - b$, które jest w stanie wyjść poza zbiór liczb naturalnych, jednak to byłoby sprzeczne z algebraiczną definicją działania. Spróbujmy jednak zdefiniować równość: $(a;\ b) = (c; d)$, 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: $a - b = c - d$, równość definiujemy:

$$(a;\ b) = (c; d) \Leftrightarrow a + d = c + b$$

Relacja równości jest zwrotna, symetryczna i przechodnia. Jako relacja równoważności dzieli ona zbiór $\mathbb{N}^2$ na rozłączne klasy abstrakcji. Wszystkie pary w danej klasie będą reprezentować jedną liczbę całkowitą.

$$\vdots$$
$$[-2] = [\,(0; 2), (1; 3), (2; 4), (3; 5)\,, (4; 6)\,\ldots]$$
$$[-1] = [(0; 1), (1; 2), (2; 3), (3;\ 4), (4;\ 5)\,\ldots]$$
$$[0] = [(0; 0), (1; 1), (2; 2), (3; 3), (4; 4)\,\ldots]$$
$$[1] = [(1; 0), (2; 1), (3; 2), (4; 3), (5; 4)\,\ldots]$$
$$[2] = [(2; 0), (3; 1), (4; 2), (5; 3), (6; 3)\,\ldots]$$
$$\vdots$$

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:

$$(a;\ b) < (c; d) \Leftrightarrow a + d < c + b$$

I dzięki temu uzyskujemy porządek na zbiorze liczb całkowitych:

$$\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots$$

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 $(a;b)=\frac{a}{b}$, ale ponieważ operacja znowu wychodzi poza zbiór, definiujemy równość za pomocą wewnętrznego mnożenia:

$$(a;b)=(c;d)\Leftrightarrow a\cdot d=c\cdot d$$

Dzięki relacji równoważności dzielimy zbiór $\mathbb{Z}^2$ na rozłączne klasy abstrakcji. Każda liczba wymierna jest właśnie reprezentantem wszystkich takich par w danej klasie:

$$[0]=[(0;1),(0;-1),(0;2),(0;-2),(0;3),\dots]$$
$$[1]=[(1;1),(-1;-1),(2;2),(-2;-2),(3;3),\dots]$$
$$[-1]=[(-1;1),(1;-1),(-2;2),(2;-2),(-3;3),\dots]$$
$$\left[\frac{1}{2}\right]=[(1;2),(-1;-2),(2;4),(-2;-4),(3;6)\dots]$$
$$\left[-\frac{1}{2}\right]=[(-1;2)(1;-2)(-2;4)(2;-4)(-3;6)\dots]$$
$$\vdots$$

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

$$(a;b)<(c;d)\Leftrightarrow a\cdot d<c\cdot d$$

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

$$\dots<-1<\dots<-\frac{1}{2}<\dots 0<\dots<\frac{1}{3}<\dots<\frac{1}{2}<\dots<1<\dots$$

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 $\mathbb{S}$. Rozpatrzymy jego podzbiór: ciągi Cauchy'ego (oznaczmy przez $\mathfrak{C}$). Ciąg Cauchy'ego charakteryzuje się tym, że dwa dowolne jego wyrazy za odpowiednią liczbą naturalną leżą dowolnie blisko siebie:

$$\forall_{\varepsilon\in\mathbb{Q}^+}\exists_{k\in\mathbb{N}}\colon\forall_{k<n,m\in\mathbb{N}}|a_n-a_m|<\varepsilon$$

Oczywiście ciągi Cauchy'ego są nieskończone. W ogólności ε 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 $\mathcal{E}$ był dowolnie mały.

Zdefiniujmy na nim relację: dwa ciągi $a_n i\ b_n$ są ze sobą w relacji, jeśli:

$$\forall_{\mathcal{E}\in\mathbb{Q}^+}\exists_{k\in\mathbb{N}}\colon\forall_{n>k}|a_n-b_n|<\mathcal{E}$$

Relacja będzie zwrotna ponieważ:

$$\forall_n|a_n-a_n|=0<\mathcal{E}\in\mathbb{Q}^+$$

Relacja będzie symetryczna, ponieważ:

$$|a_n-b_n|=|b_n-a_n|$$

Więc $\lim_{n\to\infty}|a_n-b_n|=\lim_{n\to\infty}|b_n-a_n|$, czyli jeżeli $\lim_{n\to\infty}|a_n-b_n|=0$, czyli spełnia warunek relacji, to także $\lim_{n\to\infty}|b_n-a_n|=0$, więc również jest w relacji.

Relacja przechodnia, ponieważ:

Jeżeli $\lim_{n\to\infty}|a_n-b_n|=0$ i $\lim_{n\to\infty}|\,b_n-c_n|=0$, to z tego wynika:

$$\lim_{n\to\infty}|\,a_n-c_n|=\lim_{n\to\infty}|\,a_n-b_n+b_n-c_n|$$

$$\lim_{n\to\infty}|\,a_n-b_n+b_n-c_n|=\lim_{n\to\infty}|\,(a_n-b_n)+(b_n-c_n)|$$

$$\lim_{n\to\infty}|\,(a_n-b_n)+(b_n-c_n)|=\left|\lim_{n\to\infty}[\,(a_n-b_n)+(b_n-c_n)]\right|$$

$$\left|\lim_{n\to\infty}[\,(a_n-b_n)+\,(b_n-c_n)]\right|=\left|\lim_{n\to\infty}(a_n-b_n)+\lim_{n\to\infty}(b_n-c_n)\right|$$

$$\left|\lim_{n\to\infty}(a_n-b_n)+\lim_{n\to\infty}(b_n-c_n)\right|=|0+0|=0$$

Ponieważ relacja jest zwrotna, symetryczna i przechodnia, jest relacją równoważności i dzieli zbiór wszystkich ciągów Cauchy'ego liczb wymiernych $\mathfrak{C}$ 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 $a, b \in \mathbb{R}$i ciągów $a_n, b_n \in \mathfrak{C}$, które je reprezentują:

$$a<b\Leftrightarrow\exists_{k\in\mathbb{N}}\colon\forall_{k<n\in\mathbb{N}}\ a_n<b_n$$

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

$$a\leq b\Leftrightarrow(a<b\vee a=b)$$

Zdefiniowaliśmy zbiór liczb rzeczywistych $\mathbb{R}$ 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 $\mathbb{N}$ 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

TW:Dla dowolnych niepustych zbiorów A i B możemy stworzyć funkcję $f: A \to B$.

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

$$(a; b) \sim (c; d) \Leftrightarrow a = c$$

Jest ona zwrotna, bo dla dowolnej pary $(a; b), a = a$. Jest ona symetryczna, bo jeżeli $a = c$, to wtedy $c = a$. Jest ona przechodnia, bo jeżeli $(a; b) \sim (c; d) \wedge (c; d) \sim (e; f)$, to z definicji: $a = c \wedge c = e$, a więc $a = c = e$, czyli $a = e$. Czyli jest ona relacją równoważności. Dzieli ona zbiór $A \times B$ na klasy równoważności $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ ..., w których wszystkie pary mają ten sam pierwszy element ze zbioru A, oraz dowolny element drugi ze zbioru B. Przestrzeń ilorazowa $A \times B/_{\sim}$ jest rodziną tych klas $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ ... .

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

$\forall x, x \in \mathcal{F} \Longrightarrow x \in \mathfrak{A}_i \Longrightarrow x \in A \times B$, czyli $\mathcal{F} \subseteq A \times B$, a więc jest relacją.

Ponieważ $\forall (a_1, b_1), (a_2, b_2): (a_1, b_1) \in \mathfrak{a}_i \wedge (a_2, b_2) \notin \mathfrak{a}_i \Longrightarrow a_1 \neq a_2$. Ponieważ każdy element zbioru $\mathcal{F}$ pochodzi z innej klasy $\mathfrak{a}_i$, to:

$\forall (a_1, b), (a_2, b): (a_1, b) \in \mathcal{F} \wedge (a_2, b) \in \mathcal{F} \Rightarrow a_1 \neq a_2$, czyli wynika z tego:

$$(a, b_1) \in \mathcal{F} \wedge (a, b_2) \in \mathcal{F} \Rightarrow b_1 = b_2$$

Zbiór $\mathcal{F}$ jest więc relacją, która spełnia cechy funkcji. Z tego, że w każdej klas $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ ... Były wszystkie elementy $b \in B$, wynika ponadto, że nasza funkcja może mieć jako przeciwdziedzinę dowolny podzbiór zbioru B.

Tak dla formalności, ponieważ powiedzieliśmy, że nasze TW jest równoważne AC , wypadałoby to udowodnić, dowodząc AC za jego pomocą . Mamy więc dowolną rodzinę $\mathbb{R}$ rozłącznych i niepustych zbiorów $\mathcal{S}_i$. Z aksjomatu sumy istnieje $\bigcup \mathcal{S}_i$, czyli zbiór zawierający wszystkie elementy zbiorów $\mathcal{S}_i$. Z twierdzenia wynika, że możemy stworzyć funkcję $f: \mathbb{R} \to \bigcup \mathcal{S}_i$. Z naszego twierdzenia wynika też, że dla każdego $\mathcal{S}_i$, $f(\mathcal{S}_i)$ może przyjmować dowolne wartości należące do $\bigcup \mathcal{S}_i$. Niech więc funkcja przyjmuje tylko te wartości, które należą do jej argumentów (którymi są zbiory). Przeciwdziedzina f jest selektorem U, którego istnienie

postuluje AC, a f jest funkcją wyboru postulowaną przez AC. Każdy ze zbiorów S_i z definicji funkcji ma tylko jeden element wspólny z U, co odpowiada treści AC. Ponieważ:

$$AC \Rightarrow TW \Rightarrow AC \text{ ,to w takim razie: } AC \Leftrightarrow TW$$

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 X i Y(także nieskończonych), Y posiada podzbiór równoliczny z X:

$$\forall X, Y: |X| < |Y| \exists P: P \subset Y \wedge |X| = |P|$$

Jeżeli $X = \emptyset$, to dla dowolnego Y, $\emptyset \subset Y$, możemy założyć więc, że $X \neq \emptyset$. Z definicji mocy i relacji porządku między mocami w teorii mnogości, jeżeli $|X| < |Y|$, to możemy utworzyć funkcję $f: Y \to X$, która będzie suriekcją, ale nie iniekcją. Utworzymy następującą relację równoważności na zbiorze Y, dla jego elementów:

$$x \sim y \Leftrightarrow f(x) = f(y)$$

Relacja jest zwrotna, bo dla dowolnego x, $f(x) = f(x)$. Jest ona symetryczna, bo jeżeli $f(x) = f(y) \Rightarrow f(y) = f(x)$. Jest ona przechodnia, bo jeżeli $f(x) = f(y) \wedge f(y) = f(z)$, to wtedy $f(x) = f(y) = f(z) \Rightarrow f(x) = f(z)$. Czyli jest to relacja równoważności i dzieli zbiór Y na klasy równoważności $\mathfrak{F}_i$. W każdej z klas $\mathfrak{F}_i$ zebrane są elementy o tej samej wartości funkcji f.

Teraz korzystamy z aksjomatu wyboru dla przestrzeni ilorazowej $Y/_\sim$. Utworzony selektor P posiada po jednym elemencie z każdej klasy $\mathfrak{F}_i$, więc $f: P \to X$, będzie iniekcją, bo dla każdego elementu f przyjmuje inną wartość. Będzie ona również suriekcją, bo każdemu elementowi z X można przyporządkować klasę $\mathfrak{F}_i$, a ponieważ w zbiorze P jest tyle elementów co klas w $Y/_\sim$, to każdemu elementowi zbioru X można przyporządkować jeden element z P. Czyli $f: P \to X$ pokrywa cały zbiór X. Ponieważ $f: P \to X$ będzie bijekcją wynika z tego: $|P| = |X|$. $P \subset Y$, ponieważ $\forall x: x \in P \Rightarrow x \in \mathfrak{F}_i \Rightarrow x \in Y$. Więc P 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 $\mathbb{S}$ ze zdefiniowanym na nim działaniem $\star$, oznacza się go $(\mathbb{S},\star)$ które jest:

(1) Wewnętrzne:$\forall \mathrm{x}, \mathrm{y} \in \mathbb{S}, x \star y \in \mathbb{S}$
(2) Łączne: $\forall x, y, z \in \mathbb{S}, (x \star y) \star z = x \star (y \star z)$
(3) Elementy neutralny:$\exists e, \in \mathbb{S}$: $\forall x \in \mathbb{S}, x \star e = x \wedge e \star x = x$
(4) Odwracalne: $\forall x \in \mathbb{S}\ \exists x' \in \mathbb{S}: x \star x' = e \wedge x' \star x = e$

Jeżeli działanie jest przemienne, to grupę nazywamy abelową. Moc zbioru $\mathbb{S}$ określa się jako rząd grupy. Jeżeli $\exists \mathbb{P}: \mathbb{P} \subset \mathbb{S}$, który spełnia definicję grupy dla działania $\star$, oraz $|\mathbb{P}| > 1$ to $\mathbb{P}$ nazywamy podgrupą. Jeżeli $|\mathbb{P}| = 1$, to jest to podgrupa trywialna, zawierająca tylko element neutralny e. W wypadku dla którego w $\mathbb{S}$ nie istnieje podgrupa nietrywialna, to grupę $(\mathbb{S},\star)$ 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 $\mathbb{P}$. Dwa elementy $a, b \in \mathbb{S}$ uznajemy za równoważne:

$$a \sim b \Leftrightarrow a \star b' \in \mathbb{P}$$

Relacja jest zwrotna, bo $a \star a' = a' \star a = e$, a $e \in \mathbb{P}$ z warunku elementu neutralnego. Relacja jest symetryczna, ponieważ $b \star a' = (a \star b')'$:

$$(a \star b') \star (b \star a') = a \star (b \star b') \star a' = a \star e \star a' = a \star a' = e$$

Więc z warunku odwracalności dla $a \star b' \in \mathbb{P}$ wynika:$b \star a' \in \mathbb{P}$. Relacja jest przechodnia, ponieważ jeżeli $a \star b' \in \mathbb{P} \wedge\ b \star c' \in \mathbb{P}$ to z warunku wewnętrzności: $(a \star b') \star (b \star c') \in \mathbb{P}$. Korzystając z łączności działania dla tych wyrażeń:

$$(a \star b') \star (b \star c') = a \star (b' \star b) \star c' = a \star e \star c' = a \star (e \star c') = a \star c'$$

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 $a\mathbb{P}$, gdzie $a \in \mathbb{S}$ i jest ono reprezentantem tej warstwy. Każda taka warstwa ma szczególną cechę:

$$a\mathbb{P} = \{a \star p : p \in \mathbb{P}\}$$

Nasze działanie nie musi być przemienne, wtedy wprowadza się analogiczną relację $\backsim$, na zasadzie: $a \backsim b \Leftrightarrow a' \star b \in \mathbb{P}$. Wtedy dostajemy:

$$\mathbb{P}a = \{p \star a : p \in \mathbb{P}\}$$

Warstwy $a\mathbb{P}$ nazywa się lewostronnymi a warstwy $\mathbb{P}a$ nazywa się prawostronnymi. W grupach abelowych pojęcia te są tożsame: $a\mathbb{P} = \mathbb{P}a$ i nazywa się je po prostu warstwami. Nasza podgrupa $\mathbb{P}$ również będzie jedną z tych warstw, możemy ją oznaczyć jako $e\mathbb{P}$. 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:

$$b \neq c \Rightarrow (a \star b \neq a \star c \wedge b \star a \neq c \star a)$$

Jest ona nazywana prawem skreśleń lub skracania. Wynika z niej, że a w działaniu z każdym elementem z $\mathbb{P}$ daje inny wynik i będzie ich tyle co w zbiorze $\mathbb{P}$. 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: $a \star b' \in \mathbb{P}$ z symetrii także wynika: $a' \star b \in \mathbb{P}$, to działając przez odpowiedni element z $\mathbb{P}$:

$$a \star (a' \star b) = e \star b = b$$

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

$$f : \mathbb{P} \to a\mathbb{P}, f(p) = a \star p$$

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: $|a\mathbb{P}| = |\mathbb{P}a|$. Z twierdzenia o sumie mnogościowej klas równoważności dla tych warstw wynika:

$$\mathbb{S} = e\mathbb{P} \cup a_1\mathbb{P} \cup a_2\mathbb{P} \cup a_3\mathbb{P} \cup a_4\mathbb{P} \cup \cdots$$

Identycznie będzie też dla warstw prawostronnych:

$$\mathbb{S} = \mathbb{P}e \cup \mathbb{P}a_1 \cup \mathbb{P}a_2 \cup \mathbb{P}a_3 \cup \mathbb{P}a_4 \cup \cdots$$

Ze względu na rozłączność tych zbiorów, moc zbioru $\mathbb{S}$ możemy zapisać jako:

$$|\mathbb{S}| = |e\mathbb{P}| + |a_1\mathbb{P}| + |a_2\mathbb{P}| + |a_3\mathbb{P}| + |a_4\mathbb{P}| + \cdots$$
$$|\mathbb{S}| = |\mathbb{P}e| + |\mathbb{P}a_1| + |\mathbb{P}a_2| + |\mathbb{P}a_3| + |\mathbb{P}a_4| + \cdots$$

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

$$|\mathbb{S}| = n|e\mathbb{P}| = n|\mathbb{P}e|$$

Gdzie n oznacza oczywiście ilość tych warstw. Wynika z tego, że moc zbioru $\mathbb{S}$ jest podzielna przez moc zbioru $\mathbb{P}$, 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 $\mathbb{Z}_n$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 $a|b$, to:

$$b \equiv 0\ (mod\ a)$$

I jeżeli $a \nmid b$ to możemy to zapisać jako:

$$b \not\equiv 0\ (mod\ a)$$

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 $m_1, m_2, m_3, \ldots$ $\exists!\, x: 0 \leq x < m_1 m_2 m_3$ … oraz:

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$x \equiv a_3 (mod\ m_3)$$
$$\vdots$$

Gdzie $(a_1, a_2, a_3, \ldots) \in \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \mathbb{Z}_{m_3} \times \ldots$

Twierdzenie Wilsona

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

$p|(p-1)! + 1$, wprowadzając zbiory $\mathbb{Z}_n$ współcześnie zapisuje się je jako:

$$(p-1)! \equiv -1\ (mod\ p)$$

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:

$$a^{p-1} \equiv 1 \ (mod\ p)$$

$$a^{p} \equiv a \ (mod\ p)$$

$$a^{p-1} - 1 \equiv 0 \ (mod\ p)$$

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:

$$a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Gdzie φ 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 $\mathcal{X}$, na którym określone są jakieś działania. Niech na naszym zbiorze $\mathcal{X}$ będzie określone jakieś działanie, nazwijmy je $\star$. Kongruencja jest taką relacją równoważności, że dla dowolnych elementów:

$$a, b, c, d \in \mathcal{X}: a \equiv c \wedge b \equiv d \Longrightarrow a \star b \equiv c \star d$$

Kongruencja musi zachowywać wszystkie działania $\star$ 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 $(\mathbb{N}, +, \cdot)$. 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 $\mathbb{Z}$, $\mathbb{Q}$ oraz $\mathbb{R}$.

Zbiór liczb całkowitych

Stworzyliśmy zbiór liczb $\mathbb{Z}$ jako zbiór par uporządkowanych liczb $\mathbb{N}$. Chcielibyśmy działania mnożenia i dodawania z $(\mathbb{N}, +, \cdot)$ przenieść na zbiór $\mathbb{Z}$, tak aby stworzyć zbiór $(\mathbb{Z}, +, \cdot)$.

Działanie dodawania zdefiniujemy jako:

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (a + c, b + d)$$

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

$$(a; b) = (c; d) \Leftrightarrow a + d = c + b$$

Chcemy wykazać, że dla dowolnych par:

$(a, b) = (e, f), (c, d) = (g, h)$ zachodzi:

$$(a, b) + (c, d) = (e, f) + (g, h)$$

Z wprowadzonej właśnie definicji dodawania:

$$(a + c, b + d) = (e + g, f + h)$$

Z wcześniej wprowadzonej definicji równoważności par:

$$(a + c) + (f + h) = (b + d) + (e + g)$$

$$a + c + f + h = b + d + e + g$$

$$(a + f) + (c + h) = (b + e) + (d + g)$$

Sprowadziliśmy to do liczb naturalnych, teraz z definicji wiemy, że ponieważ $(a, b) = (e, f)$ i $(c, d) = (g, h)$ to $a + f = b + e = x$ i

$c + h = d + g = y$, podstawiając:

$$x + y = y + x$$

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 $(\mathbb{Z}, +, \cdot)$.

Zbiór liczb wymiernych

Mamy zbiór $\mathbb{Q}$. W następnej kolejności ze zbioru $(\mathbb{Z}, +, \cdot)$ chcemy stworzyć zbiór $(\mathbb{Q}, +, \cdot)$.

Dodawanie dwóch liczb wymiernych wprowadzamy:

$$(a, b) + (c, d) \stackrel{\text{def}}{=} (ad + bc, bd)$$

Chcemy udowodnić, że dla $(a, b) = (e, f)$ i $(c, d) = (g, h)$ zachodzi:

$$(a, b) + (c, d) = (e, f) + (g, h)$$
$$(ad + bc; bd) = (eh + fg; fh)$$
$$fh(ad + bc) = bd(eh + fg)$$
$$adfh + bcfh = bdeh + bdfg$$
$$af \cdot dh + ch \cdot bf = be \cdot dh + dg \cdot bf$$

Z założenia przystawania par $af = be = x$ oraz $ch = dg = y$:

$$x \cdot dh + y \cdot bf = x \cdot dh + y \cdot bf$$

Co jest prawdziwe dla dowolnych liczb całkowitych x, y, d, h, b, f.

Mnożenie liczb wymiernych definiujemy w następujący sposób:

$$(a, b) \cdot (c, d) \stackrel{\text{def}}{=} (ac, bd)$$

Chcemy dowieść, że dla par $(a, b) = (e, f)$ i $(c, d) = (g, h)$ zachodzi:

$$(a, b) \cdot (c, d) = (e, f) \cdot (g, h)$$

Stosując wprowadzoną definicję mnożenia:

$$(ac, bd) = (eg, fh)$$

Korzystając z definicji równoważności par:

$$ac \cdot fh = bd \cdot eg$$
$$a \cdot c \cdot f \cdot h = b \cdot d \cdot e \cdot g$$
$$af \cdot ch = be \cdot dg$$

Wiedząc, że pary $(a, b) = (e, f)$ i $(c, d) = (g, h)$ są równoważne:

$$af = be = x \wedge ch = dg = y$$
$$x \cdot y = x \cdot y$$

Co jest prawdziwe dla dowolnych liczb całkowitych.

Zbiór liczb rzeczywistych

Na koniec celem będzie stworzenie zbioru $(\mathbb{R}, +, \cdot)$. Mamy już zbiory $\mathbb{R}$ oraz $(\mathbb{Q}, +, \cdot)$.

Dodawanie definiujemy za pomocą ciągów Cauchy'ego liczb $\mathbb{Q}$ a_n, b_n reprezentujących liczby $a, b \in \mathbb{R}$:

$$a + b = \lim_{n\to\infty}(a_n + b_n)$$

Chcemy dowieść, że dla $\lim_{n\to\infty}(a_n - c_n) = 0$ oraz $\lim_{n\to\infty}(b_n - d_n) = 0$ zachodzi:

$$\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty}(c_n + d_n)$$

$$\lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n = \lim_{n\to\infty} c_n + \lim_{n\to\infty} d_n$$

$$\lim_{n\to\infty} a_n - \lim_{n\to\infty} c_n = \lim_{n\to\infty} d_n - \lim_{n\to\infty} b_n$$

$$\lim_{n\to\infty}(a_n - c_n) = \lim_{n\to\infty}(d_n - b_n)$$

$$\lim_{n\to\infty}(a_n - c_n) = -\lim_{n\to\infty}(b_n - d_n)$$

$$0 = -1 \cdot 0$$

Otrzymaliśmy prawdę matematyczną, co kończy dowód.

Mnożenie także definiowane jest za pomocą ciągów Cauchy'ego:

$$a \cdot b = \lim_{n\to\infty}(a_n \cdot b_n)$$

Analogicznie dowodzimy, że $\lim_{n\to\infty}(a_n - c_n) = 0$ i $\lim_{n\to\infty}(b_n - d_n) = 0$:

$$\lim_{n\to\infty} a_n b_n = \lim_{n\to\infty} c_n d_n$$

$$\lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n = \lim_{n\to\infty} c_n \cdot \lim_{n\to\infty} d_n$$

$$\lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} \frac{1}{c_n} = \lim_{n\to\infty} d_n \cdot \lim_{n\to\infty} \frac{1}{b_n}$$

$$\lim_{n\to\infty} \frac{a_n}{c_n} = \lim_{n\to\infty} \frac{d_n}{b_n}$$

$$\lim_{n\to\infty}\left(\frac{a_n - c_n}{c_n} + 1\right) = \lim_{n\to\infty}\left(\frac{d_n - b_n}{b_n} + 1\right)$$

$$\lim_{n\to\infty} \frac{a_n - c_n}{c_n} + 1 = -\lim_{n\to\infty} \frac{b_n - d_n}{b_n} + 1$$

$$0 = 0$$

Po raz kolejny otrzymanie prawdy matematycznej kończy dowód. Milcząco należało założyć, że $b_n \neq 0 \;\; i \; c_n \neq 0$ (są to reprezentanci wszystkich ciągów wymiernych o tej granicy). Dlatego należy jeszcze pokazać trywialny przypadek, kiedy $b_n = c_n = 0$:

$$\lim_{n\to\infty} a_n b_n = \lim_{n\to\infty} c_n d_n$$

$$\lim_{n\to\infty}(a_n \cdot 0) = \lim_{n\to\infty}(d_n \cdot 0)$$

$$\lim_{n\to\infty} 0 = \lim_{n\to\infty} 0$$

$$0 = 0$$

Otrzymanie prawdy matematycznej znów kończy dowód. Skonstruowaliśmy zbiór $(\mathbb{R}, +, \cdot)$.

Zbiory $\mathbb{Z}_n$-arytmetyka modularna

Zbiory $\mathbb{Z}_n$ stają się użytecznym narzędziem, kiedy zdefiniujemy na nich działania dodawania $\oplus_n$ i mnożenia $\otimes_n$ modulo przeniesione ze zbioru liczb całkowitych $(\mathbb{Z}, +, \cdot)$, tak aby stworzyć zbiór $(\mathbb{Z}_n, \oplus_n, \otimes_n)$. Aby to zrobić musimy pokazać, że przystawanie modulo jest dla nich kongruencją (zazwyczaj w operacjach modularnych zapisuje się je po prostu $+ i \cdot$ ale po wyraźnym oznaczeniu operacji modularnych przez $(mod\ n)$.

Jeśli chodzi o działanie dodawania dowód przeprowadza się następująco:

Weźmy cztery liczby całkowite a, b, c, d, przy czym $a \equiv c\ (mod\ n)$ i $b \equiv d\ (mod\ n)$. Chcemy udowodnić, że:

$$a + b \equiv c + d(mod\ n)$$

Przedstawiamy nasze liczby w rozkładzie dzielenia z resztą:

$a = x \cdot n + r_1, b = y \cdot n + r_2, c = z \cdot n + r_1, d = v \cdot n + r_2$:

$$xn + r_1 + yn + r_2 \equiv zn + r_1 + vn + r_2(mod\ n)$$

$$(x + y)n + r_1 + r_2 \equiv (z + v)n + r_1 + r_2(mod\ n)$$

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

$$r_1 + r_2 \equiv r_1 + r_2(mod\ n)$$

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 $a \equiv c\ (mod\ n)$ I $b \equiv d\ (mod\ n)$, czyli:

$a = x \cdot n + r_1, b = y \cdot n + r_2, c = z \cdot n + r_1, d = v \cdot n + r_2$

$$a \cdot b \equiv c \cdot d(mod\ n)$$

$$(x \cdot n + r_1)(y \cdot n + r_2) \equiv (z \cdot n + r_1)(v \cdot n + r_2)(mod\ n)$$

$$xyn^2 + xr_2n + yr_1n + r_1r_2 \equiv zvn^2 + zr_2n + vr_1n + r_1r_2(mod\ n)$$

Wszystko co ma wyraz n dzieli się przez n bez reszty:

$$r_1r_2 \equiv r_1r_2\ (mod\ n)$$

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 $(\mathbb{Z}_n, \oplus_n, \otimes_n)$. Dopiero zdefiniowanie na nim działania dodawania nadaje prawdziwy sens liczbom ujemnym, jako elementów przeciwnych dodawania:

$$1 + (n - 1) \equiv 1 + (-1) \equiv 0\ (mod\ n)$$

Dowolny zbór $(\mathbb{Z}_n, \oplus_n)$ stanowi grupę. Niestety z działaniem mnożenia już tak nie jest. Tylko zbiory $(\mathbb{Z}_p, \otimes_p)$, gdzie p jest liczbą pierwszą stanowią grupy (a raczej podzbiory $\mathbb{Z}_p/\{0\}$), a zbiory $(\mathbb{Z}_p, 0, 1, \oplus_p, \otimes_p,)$ ciała (inne struktury matematyczne), kiedy p 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 $\mathbb{Z}_p$.

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 $-x$, a dla mnożenia będzie to liczba odwrotna, czyli $\frac{1}{x}$. Problem polega na tym, że w zbiorach modulo n nie zawsze da się znaleźć element odwrotny dla każdego x. Dla zbioru $\mathbb{Z}_n$ możliwe jest to jedynie dla liczb względnie pierwszych z n. Dlatego możliwe jest to wyłącznie w zbiorach $\mathbb{Z}_p/\{0\}$, 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 n? Są one dzielnikami zera! Pokażemy to na przykładzie. Chyba każdy się zgodzi, że: $2 \otimes_6 3 \equiv 0$. Spróbujcie sobie wyobrazić działanie:

$$\frac{1}{2} \otimes_6 \frac{1}{3} \equiv \cdots$$

Chyba lepiej sobie tego nie wyobrażać i pozostać przy liczbach wymiernych w $\mathbb{Z}_p$ … Na pocieszenie, w dowolnym $\mathbb{Z}_n$ jego podzbiór, mianowicie liczby względnie pierwsze z n stanowią z działaniem mnożenia $\otimes_n$ grupę i ich odwrotności można zdefiniować w $\mathbb{Z}_n$.

Używając tej metody możemy w ciałach $\mathbb{Z}_p$ odwrotność każdej liczby poza 0, oczywiście. Pokażmy to na przykładzie $\mathbb{Z}_7$:

$1 \cdot 1 \equiv 1 \ (mod\ 7)$ czyli $1 \equiv 1 \ (mod\ 7)$

$2 \cdot 4 \equiv 1 \ (mod\ 7)$ czyli $2 \equiv \frac{1}{4} \ (mod\ 7)$ oraz $4 \equiv \frac{1}{2} (mod\ 7)$

$3 \cdot 5 \equiv 1 \ (mod\ 7)$ czyli $3 \equiv \frac{1}{5} \ (mod\ 7)$ oraz $5 \equiv \frac{1}{3} \ (mod\ 7)$

$6 \cdot 6 \equiv 1 \ (mod\ 7)$ czyli $6 \equiv \frac{1}{6} \ (mod\ 7)$

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

$$\frac{5}{4} \equiv \frac{1}{4} \cdot 5 \equiv 2 \cdot 5 \equiv 3 \ (mod\ 7)$$

W ten sposób możemy przedstawić modulo p dowolną liczbę wymierną, której mianownik nie jest wielokrotnością p i włączyć do naszych klas równoważności przynajmniej część liczb wymiernych. Ponieważ nie możemy przedstawić wszystkich, nie wolno nam stosować zapisu $\mathbb{Q}_p$, choć bez wątpienia nasuwa się taka pokusa. Zresztą symbol $\mathbb{Q}_p$ 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 $\mathbb{Z}_n$, to najwygodniej jest posługiwać się ciałami $\mathbb{Z}_p$, 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 $\mathbb{Z}_p$. Omówiliśmy już pojęcie podzielności i możemy brać się do roboty.

Sumy względnie pierwsze

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

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

$$a = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_n}^{\alpha_n}$$

Jest oczywiste, że:

$$a \equiv 0 \pmod{p_1}$$
$$a \equiv 0 \pmod{p_2}$$
$$\vdots$$
$$a \equiv 0 \pmod{p_n}$$

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

$$a + b \equiv b \pmod{p_1}$$
$$a + b \equiv b \pmod{p_2}$$
$$\vdots$$
$$a + b \equiv b \pmod{p_n}$$

Ponieważ b ma niezerową resztę modulo dowolne p_i, to nie jest podzielna przez żaden z dzielników pierwszych a, a co za tym idzie również i złożonych. Dlatego $\mathrm{NWD}(a, a + b) = 1$. Powtarzając to rozumowanie, ale zamieniając a z b zauważymy, że także $\mathrm{NWD}(b, a + b) = 1$. 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 $\{0,1, \ldots, m_1 m_2 \ldots m_n - 1\}$ dowolna n-ka reszt $(a_1, a_2, \ldots, a_n)$ występuje tylko raz. Dla dowodu nie wprost załóżmy, że istnieje taka kombinacja reszt, która się powtarza dla dwóch różnych $a, b \in \{0,1, \ldots, m_1 m_2 \ldots m_n - 1\}$. Bez straty ogólności można założyć, że $a < b$. Wtedy:

$$a \equiv a_1 \pmod{m_1} \qquad b \equiv a_1 \pmod{m_1}$$
$$a \equiv a_2 \pmod{m_2} \qquad b \equiv a_2 \pmod{m_2}$$
$$\vdots \qquad\qquad \vdots$$
$$a \equiv a_n \pmod{m_n} \qquad b \equiv a_n \pmod{m_n}$$

Z tego wynika, że dla liczby $b - a$, która z założeń ma być większa od 0, ale mniejsza od liczby $m_1 m_2 \ldots m_n$:

$$b - a \equiv 0 (mod\ m_1)$$
$$b - a \equiv 0 (mod\ m_2)$$
$$\vdots$$
$$b - a \equiv 0 (mod\ m_n)$$

Czyli wynika z tego, że liczba $b - a$ jest podzielna przez każdą z liczb $m_1, m_2, \dots, m_n$. Ale ponieważ liczby te były względnie pierwsze, to $b - a = k \cdot m_1 m_2 \dots m_n$, czyli z tego wynika: $b = k \cdot m_1 m_2 \dots m_n + a$, 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 m_i będzie m_i, a kolejność reszt ma znaczenie, to w takim razie wszystkich tych kombinacji reszt będzie $m_1 m_2 \dots m_n$. 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 $(p-1)!$ modulo p:

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot -1 \pmod p$$

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

$$\exists a, b, c: b \neq c \wedge a \cdot b \equiv 1 (\mathrm{mod}\ p) \wedge a \cdot c \equiv 1 (\mathrm{mod}\ p) \Rightarrow ab \equiv ac \pmod p$$

$$a(b-c) \equiv 0 \pmod p$$

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:

$$x^2 \equiv 1 \pmod p$$

$$x^2 - 1 \equiv 0 \pmod p$$

$$(x-1)(x+1) \equiv 0 \pmod p$$

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:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot -1 \equiv 1 \cdot (x \cdot x') \cdot (y \cdot y') \cdot \dots \cdot -1 \pmod p$$

$$1 \cdot (x \cdot x') \cdot (y \cdot y') \cdot \dots \cdot -1 \equiv 1 \cdot 1 \cdot 1 \cdot \dots \cdot -1 \equiv -1 \pmod p$$

Czyli wynika z tego $(p-1)! \equiv -1 \pmod p$, więc $(p-1)! + 1 \equiv 0 \pmod p$ dla dowolnej liczby pierwszej, co dowodzi $p|(p-1)! + 1$.

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: $NWD(a,n) = 1 \wedge NWD(b,n) = 1 \Rightarrow NWD(ab,n) = 1$
2) Jest ono łączne, skoro jest łączne w $\mathbb{Z}_n$, to jest łączne w jego podzbiorze.
3) Ma ono element neutralny, bo $NWD(1,n) = 1$

4) Jest ono odwracalne, dowód nieco bardziej skomplikowany i włączający działanie dodawania modularnego. Dowodzi się prawa skreśleń nie wprost:

$$ab \equiv ac \ (mod\ n)$$
$$ab - ac \equiv 0 \ (mod\ n)$$
$$a(b - c) \equiv 0 \ (mod\ n)$$

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

5) Jest ono przemienne: skoro było przemienne w $\mathbb{Z}_n$, jest ono przemienne także w jego podzbiorze

Dlatego działanie to wraz z tym zbiorem daje grupę abelową, jej rząd wynosi $\varphi(n)$. Teraz dowodzimy, że działanie potęgowania w tej grupie jest cykliczne i elementy tego cyklu będą stanowić podgrupę. Zgodnie z prawem skracania dla różnych b, działanie $a \cdot b$ daje różne wyniki dla tego samego a i te same, kiedy b jest takie samo. Łącząc prawo skracania z zasadą szufladkową: ponieważ jest dokładnie $\varphi(n)$ reszt z dzielenia w ciągu $\varphi(n) + 1$ elementów przynajmniej jedna reszta musi się powtórzyć. Ponieważ jedyna operacja w tym ciągu to mnożenie przez a, świadczy to o pojawieniu się jedynki. Ze względu na to kolejne potęgi a^n będą dawać różne wyniki do momentu takiego k: $a^k \equiv 1 \ (mod\ n)$, więc $a^{k+1} \equiv a \ (mod\ n)$ i cykl powtarza się od początku. Dowiedziemy, że zbiór wartości dodatnich potęg liczby a stanowi grupę abelową z działaniem mnożenia.

1) Jest ono wewnętrzne: $a^n \cdot a^m \equiv a^{n+m} (mod\ n)$
2) Jest ono łączne, tak jak w całym zbiorze $\mathbb{Z}_n$
3) Ma ono element neutralny, bo występuje w nim $a^k \equiv 1 \ (mod\ n)$
4) Jest ono odwracalne: $\forall a^n, a^n \cdot a^{k-n} \equiv 1 \ (mod\ n)$
5) I jest ono przemienne, tak jak w $\mathbb{Z}_n$

Dlatego będzie stanowić grupę rzędu k. Liczbę k nazywamy rzędem elementu a, a samo a generatorem tej podgrupy $\langle a \rangle$. Z twierdzenia Lagrange'a, które jest zamieszczone w poprzednim rozdziale, wynika, że rząd dowolnej podgrupy jest dzielnikiem rzędu całej grupy, czyli: $k|\varphi(n)$. I z tego wynika, że:

$$a^{\varphi(n)} \equiv (a^k)^l \equiv 1^l \equiv 1 \ (mod\ n)$$

Co dowodzi na początku postawionej tezy.

Małe Twierdzenie Fermata

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

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Jeżeli $a \not\equiv 0 \ (mod\ p)$ to $NWD(a, p) = 1$. Ponieważ $\varphi(p) = p - 1$, to:

$$a^{p-1} \equiv a^{\varphi(p)} (mod\ p)$$

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:

$a^2 + b^2 = c^2$, czyli $a^2 + b^2 \equiv c^2 (mod\ 3)$

Jeżeli $a \not\equiv 0\ (mod\ 3) \wedge b \not\equiv 0 (mod\ 3)$, to z Małego twierdzenia Fermata:

$a^2 + b^2 \equiv 1 + 1 \equiv 2 (mod\ 3)$

Jeżeli $3|c \Rightarrow c^2 \equiv 0\ (mod\ 3)$, a jeżeli $3 \nmid c \Rightarrow c^2 \equiv 1 (mod\ 3)$.

Czyli dostajemy $2 \equiv 0\ (mod\ 3)$ lub $2 \equiv 1 (mod\ 3)$. Otrzymana sprzeczność pokazuje nam, że a lub b jest podzielne przez 3, bo wtedy:

$1 + 0 \equiv 1 (mod\ 3)$, 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.*