

Konrad Jamrozik

Matematyka Dyskretna 2008

Notatki z wykładu II UW

Wrocław, październik 2009

Spis treści

Wstęp	iii
I 6.X.2008	1
1 Symbole asymptotyczne	1
2 Podłoga i powała	5
3 Zależności rekurencyjne	6
3.1 Wieże Hanoi	6
3.2 Proste na płaszczyźnie	7
II 13.X.2008	8
1 Liczby Fibonacciego	8
1.1 Zależności dla liczb Fibonacciego	9
2 Algorytmy oparte na rekursji	9
2.1 Sortowanie przez scalanie	9
2.2 Mnożenie długich liczb	11
3 Arytmetyka modularna	12
3.1 Algorytm Euklidesa	14
III 20.X.2008	15
1 Algorytm Euklidesa c. d.	15
1.1 Rozszerzony algorytm Euklidesa	15
2 Liczby pierwsze	17
IV 27.X.2008	21
1 Chińskie twierdzenie o resztach	21
2 Funkcja Eulera	22
2.1 Twierdzenie Eulera	23
2.2 Małe twierdzenie Fermata	23
2.3 RSA	23
3 Zliczanie	23
3.1 Symbol Newtona	23
3.2 Poker	25
3.3 Wzór dwumienny Newtona	25
V 3.XI.2008	26
1 Zasada szufladkowa Dirichleta	26
2 Elementy algebry	28
2.1 Twierdzenie Lagrange'a	28
2.2 Uogólnione twierdzenie Lagrange'a	29
2.3 Lemat Burnside'a	30
3 Zasada włączeń i wyłączeń	31

Copyright © 2009 Konrad Jamrozik

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Wstęp

I powiedział Pan „Oto przed wami Notatki +5 wydobyte z czeluści BIFXa przez służbę mego, wersja alpha. Będą one wam halabardą do walki ze złem grzechu niezaliczenia, sztachetą przeciwko Niechciejowi i światłem nadziei gdy nastanie Dzień W Którym Tak Bardzo Żałuję Że Się Nie Uczylem Gdy Była Na To Pora, gdyż w celu tym stworzone zostały, i w żadnym innym”

I dopowiedział Pan „Zaprawdę powiadam Wam, przeczytacie te oto notatki i symbole asymptotyczne nie będą więcej skrywały przed Wami tajemnic swych, ani podłoga, ani powała też nie. Także grafy, redukcje wielomianowe i inne różne takie odkryją przed Wami sekrety swe, ale to potem”

Lecz także rzekł Pan „Jednakże pamiętajcie: Postanowić możecie nie czytać notatek tych, lecz wtedy klątwa niezaliczenia spadnie na Was z prawdopodobieństwem 1”

I na koniec dodał Pan „Tak więc właśnie i nie inaczej”

Z Księgi Znameytentego. Teges. Tam. Iwteinazad.

I 6.X.2008

1 Symbole asymptotyczne

Mamy dwie funkcje: $f(n)$, paskudną i $g(n)$, porządną. Będziemy wyrażać funkcję paskudną przy pomocy porządnej.

Definicja O^*

$$f(n) = O(g(n)) \iff \exists c > 0 \exists n_0 \forall n > n_0 \quad f(n) < c \cdot g(n)$$

Intuicja: Dla dostatecznie dużego argumentu n , $f(n)$ jest mniejsze od $g(n)$ z dokładnością do pewnego stałego mnożnika.

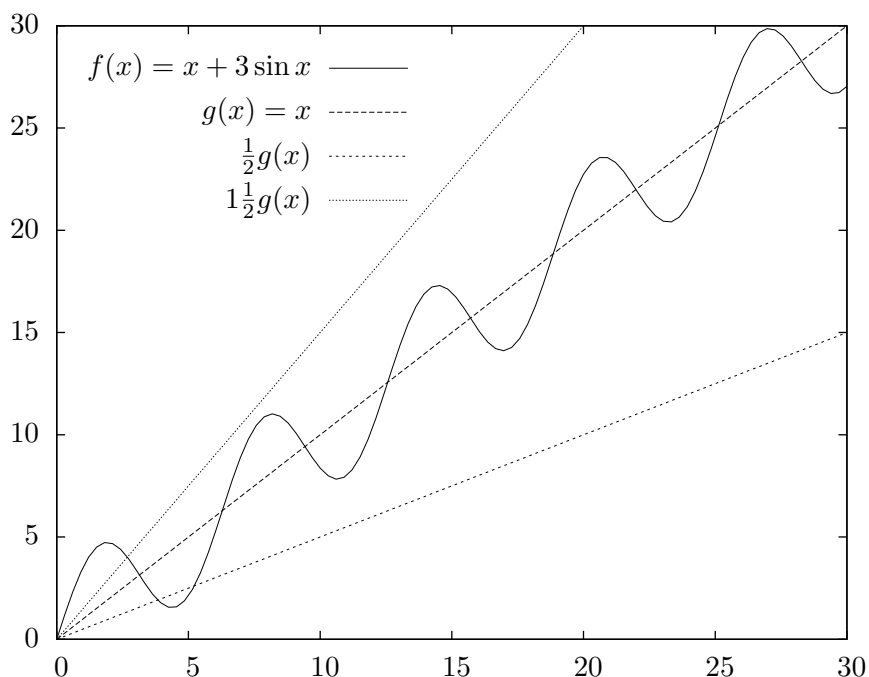
Definicja Ω

$$f(n) = \Omega(g(n)) \iff g(n) = O(f(n)) \iff \exists c > 0 \exists n_0 \forall n > n_0 \quad f(n) > c \cdot g(n)$$

Intuicja: Dla dostatecznie dużego argumentu n , $f(n)$ jest większe od $g(n)$ z dokładnością do pewnego stałego mnożnika.

Definicja Θ

$$\begin{aligned} f(n) = \Theta(g(n)) &\iff f(n) = O(g(n)) \wedge f(n) = \Omega(g(n)) \\ &\iff \exists c, d > 0 \exists n_0 \forall n > n_0 \quad d \cdot g(n) < f(n) < c \cdot g(n) \end{aligned}$$



Rysunek 1. $f(x) = \Theta(g(x))$

*Formalnie $O(g(n))$ reprezentuje pewien zbiór funkcji, więc odpowiedniejszą notacją byłoby $f(n) \in O(g(n))$, ale jest równość z powodu tradycji. Po szczegółóły odsyłam do *Matematyki konkretnej* Knutha i innych.

Definicja \sim

$$f(n) \sim g(n) \iff \frac{f(n)}{g(n)} \xrightarrow{n \rightarrow \infty} 1$$

Intuicja: Asymptotyczna złożoność obu funkcji jest taka sama.

Definicja o

$$f(n) = o(g(n)) \iff \frac{f(n)}{g(n)} \xrightarrow{n \rightarrow \infty} 0$$

Intuicja: Funkcja g ma gorszą asymptotyczną złożoność niż f .

Przykłady

1. $|\sin(n)| = O(1) \iff \exists c > 0 \exists n_0 \forall n > n_0 \quad |\sin(n)| < c \cdot 1$

2. $(n+1)^2 \sim n^2 \iff \lim_{n \rightarrow \infty} \frac{(n+1)^2}{n^2} = 1$

3. $n = o(n^2) \iff \lim_{n \rightarrow \infty} \frac{n}{n^2} = 0$

4. $(n+1)^2 = \Theta(n^2) \iff \exists c, d > 0 \exists n_0 \forall n > n_0 \quad d \cdot n^2 < (n+1)^2 < c \cdot n^2$

Ponieważ $(n+1)^2 = n^2 + 2n + 1$ oraz $1 \cdot n^2 < n^2 + 2n + 1 < 5 \cdot n^2$,
to przykładowo $d = 1$ i $c = 5$.

5. $\ln(1 + \frac{1}{n}) \sim \frac{1}{n}$

6. $\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots$ (wzór Taylora)

7. Niech $g_n \cdot \ln g_n = n$.

$x \ln x$ jest f. rosnącą monotonicznie, stąd:

$$\begin{aligned} & g_n < n \\ \Rightarrow & \ln g_n < \ln n \\ \Rightarrow & g_n \ln g_n < g_n \ln n \\ \Rightarrow & n < g_n \ln n \\ \Rightarrow & \frac{n}{\ln n} < g_n \end{aligned} \quad (1)$$

$$\begin{aligned} \Rightarrow & \ln \frac{n}{\ln n} < \ln g_n \\ \Rightarrow & \ln n - \ln \ln n < \ln g_n \\ \Rightarrow & g_n (\ln n - \ln \ln n) < g_n \ln g_n \\ \Rightarrow & g_n (\ln n - \ln \ln n) < n \\ \Rightarrow & g_n < \frac{n}{(\ln n - \ln \ln n)} \end{aligned} \quad (2)$$

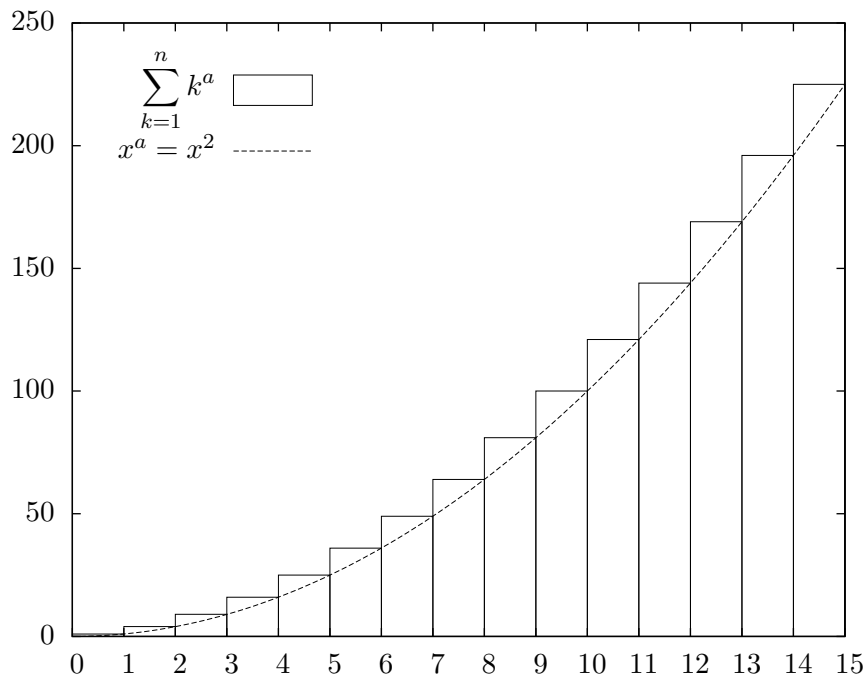
Z (1) i (2) wynika, że:

$$\begin{aligned} & \frac{n}{\ln n} < g_n < \frac{n}{(\ln n - \ln \ln n)} \\ \Rightarrow & 1 < \frac{g_n}{\frac{n}{\ln n}} < \frac{\ln n}{\ln n - \ln \ln n} \\ \Rightarrow & 1 < \frac{g_n}{\frac{n}{\ln n}} < \frac{1}{1 - \frac{\ln \ln n}{\ln n}} \end{aligned}$$

Ponieważ $\lim_{x \rightarrow \infty} \frac{\ln x}{x} = 0$, to z zastosowania twierdzenia o trzech ciągach do powyższych dwóch nierówności wynika, że $g_n \sim \frac{n}{\ln n}$.

8. $(n+1)^2 = n^2 + 2n + 1 = n^2 + \Theta(n) = n^2 + O(n) = n^2 + o(n^2)$

9. Dla $a > 0$: $\sum_{k=1}^n k^a = \text{interpretacja graficzna (Rys. 2)} = \int_0^n x^a dx + R(x) = \frac{1}{a+1}n^{a+1} + O(n^a)$



Rysunek 2. Szukana suma to pole powierzchni pod wykresem x^a (na rysunku $a = 2$), które można obliczyć z całki, oraz brakujące fragmenty nad wykresem, których sumę oznaczamy $R(x)$, a które można zmieścić w ostatnim z prawej „słupku”

Znajdowanie minimum

Dane: $a_1, a_2, a_3, \dots, a_n$

Chcemy znaleźć minimum z danych liczb. Ile czasu będzie działał program wykonujący to zadanie?

Odpowiedź: $\sim c \cdot n$, gdzie c to stała zależna od szczegółów implementacji programu.

Czas działania algorytmu to $\Theta(n)$ lub, mniej dokładnie, $O(n)$.

Definicja Czas działania algorytmu \equiv Złożoność czasowa algorytmu

Sortowanie

Dane: $a_1, a_2, a_3, \dots, a_n$

Chcemy tak porządkować dane wejściowe, aby $a'_1 \leq a'_2 \leq a'_3 \leq \dots \leq a'_n$.

Łatwo napisać algorytm o złożoności $O(n^2)$ np. *bubblesort*, ale istnieją też algorytmy o oczekiwanej złożoności $O(n \log n)$ np. *quicksort*.

Mnożenie macierzy kwadratowych

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \times \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nn} \end{bmatrix}$$

$$\text{gdzie } c_{ij} = \sum_{k=1}^n a_{ik} \cdot b_{kj}$$

Mnożenie można wykonać w $O(n^3)$. Algorytm Strassena wykonuje je w $O(n^{2.81})$, a najlepsze znane algorytmy w $O(n^{2.37})$, ale posiadają one olbrzymią stałą, czyniącą je w praktyce mało przydatnymi.

Zestawienie złożoności

	$f(n)$	$f(10)$	$f(100)$	$f(1000)$	$10f(n)$
F. logarytmiczna	$10 \log n$	33.2	66.4	99.7	$f(n^{10})$
Funkcje wielomianowe	n	10	100	1000	$f(10n)$
	$n \log n$	33.2	664	9970	$\sim f(10n)$
	n^2	100	10000	10^6	$f(3.16n)$
	n^3	1000	10^6	10^9	$f(2.15n)$
F. wykładnicza	1.1^n	2.6	13780	$2.46 \cdot 10^{41}$	$f(n + 24.1)$

Definicja \prec

$$f(n) \prec g(n) \iff f(n) = o(g(n))$$

Dla $a, b > 0, c > 1$ zachodzi:

$$1 \prec \log \log n \prec (\log n)^a \prec n^b \prec c^n$$

Twierdzenie z analizy matematycznej:

$$\frac{x}{e^x} \xrightarrow{x \rightarrow \infty} 0$$

Wykażemy, że $n^b \prec c^n$:

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{n^b}{c^n} &= \lim_{n \rightarrow \infty} \left(\frac{n}{c^{(n/b)}} \right)^b = \lim_{n \rightarrow \infty} \left(\frac{n}{e^{\ln c \cdot (n/b)}} \right)^b = \lim_{n \rightarrow \infty} \left(\frac{n \cdot \frac{\ln c}{b}}{e^{\ln c \cdot (n/b)} \cdot \frac{\ln c}{b}} \right)^b = \\ &= \lim_{n \rightarrow \infty} \left(\frac{\ln c \cdot (n/b)}{e^{\ln c \cdot (n/b)}} \cdot \frac{1}{\frac{\ln c}{b}} \right)^b = \left(0 \cdot \frac{b}{\ln c} \right)^b = 0 \quad \square \end{aligned}$$

Wykażemy, że $(\log n)^a \prec n^b$:

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{(\log n)^a}{n^b} &= \lim_{n \rightarrow \infty} \frac{\left(\frac{\ln n}{\ln 10} \right)^a}{n^b} = \lim_{n \rightarrow \infty} \left(\frac{(\ln n)^a}{n^b} \cdot \frac{1}{(\ln 10)^a} \right) \stackrel{N \leftarrow \ln n}{=} \lim_{n \rightarrow \infty} \left(\frac{N^a}{e^{N \cdot b}} \cdot \frac{1}{(\ln 10)^a} \right) = \\ &= \lim_{n \rightarrow \infty} \left(\frac{N^a}{(e^b)^N} \cdot \frac{1}{(\ln 10)^a} \right) \stackrel{N^y \prec z^N}{=} 0 \cdot \frac{1}{(\ln 10)^a} = 0 \quad \square \end{aligned}$$

2 Podłoga i powała

Definicje

Podłoga $\lfloor \cdot \rfloor$ (część całkowita, *entier*) liczby rzeczywistej x , to największa liczba całkowita nie większa od x . Podłogę symbolicznie zapisujemy:

$$\lfloor x \rfloor = [x] = \max\{k \in \mathbb{Z}: k \leq x\}$$

Powała $\lceil \cdot \rceil$ (sufit[†]) liczby rzeczywistej x , to najmniejsza liczba całkowita nie mniejsza od x . Powałę symbolicznie zapisujemy:

$$\lceil x \rceil = \min\{k \in \mathbb{Z}: k \geq x\}$$

Część ułamkowa $\{ \cdot \}$

$$\{x\} = x - \lfloor x \rfloor$$

Przykłady

$$\begin{array}{lll} \lfloor 12,34 \rfloor = 12, & \lceil 12,34 \rceil = 13, & \{12,34\} = 0,34, \\ \lfloor -12,34 \rfloor = -13, & \lceil -12,34 \rceil = -12, & \{-12,34\} = 0,66, \\ \lfloor -x \rfloor = -\lceil x \rceil, & \lfloor x+n \rfloor = \lfloor x \rfloor + n, & \lceil x+n \rceil = \lceil x \rceil + n \end{array}$$

Wykażemy, że $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil = n$:

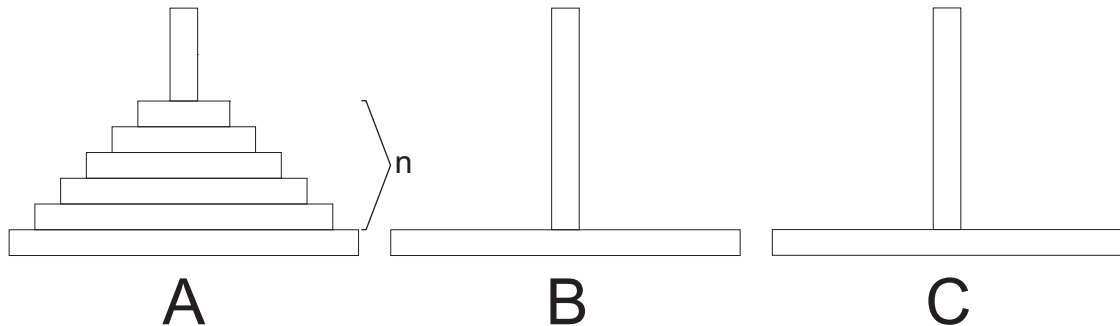
$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor n - \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n + \left\lfloor -\frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n - \left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n}{2} \right\rceil = n \quad \square$$

Liczbę całkowitą leżącą najbliżej x można zdefiniować jako $\lfloor x + \frac{1}{2} \rfloor$ albo $\lceil x - \frac{1}{2} \rceil$. Definicje te różnią się traktowaniem liczb, które leżą dokładnie w połowie między dwiema liczbami całkowitymi. Pierwsza zaokrągla je w górę, a druga w dół.

[†]W oczywisty sposób wiadomo, że używanie terminu „sufit” zamiast „powała” świadczy o fatalnym braku dobrego smaku i wyczucia stylu.

3 Zależności rekurencyjne

3.1 Wieże Hanoi



Rysunek 3. Nędzne podróbki beznadziejnych wież Hanoi

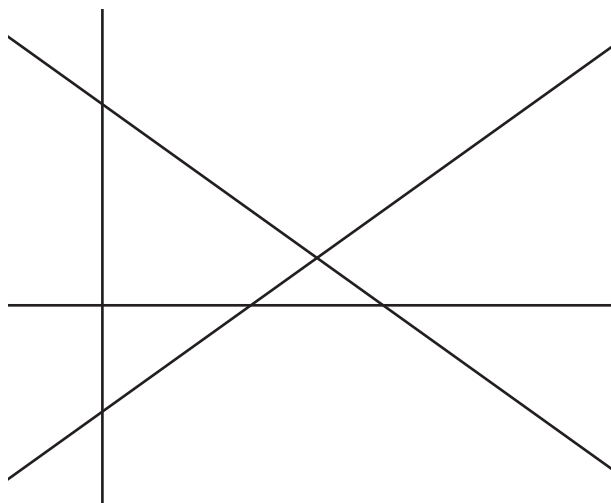
Problem Mamy n krążków na słupku A i chcemy przenieść wszystkie krążki na słupek C. Problem polega na tym, że nie wolno nam w międzyczasie unieszczęśliwić ani jednego krążka, czyli nie wolno nam położyć krążka szerszego na krążek węższy.

Obserwacja By przenieść n krążków z dowolnego słupka A na dowolny inny słupek C, należy przenieść wszystkie krążki oprócz najszerszego na trzeci słupek B; następnie przenieść pozostawiony najszerszy krążek na słupek C, a na koniec wszystkie mniejsze krążki (będące na słupku B) położyć na największy, znajdujący się już na słupku C.

Oznaczmy najmniejszą liczbę przelożeń potrzebnych aby przenieść zawartość słupka A na słupek C jako $T(n)$. Oczywiście $T(1) = 1$. Na podstawie powyższej obserwacji można wydedukować, że $T(n) = T(n-1) + 1 + T(n-1) = 1 + 2T(n-1)$. Wyznamy jawny wzór na $T(n)$ stosując metodę iteracyjną:

$$\begin{aligned} T(n) &= 1 + 2T(n-1) = \\ &= 1 + 2(1 + 2T(n-2)) \\ &= 1 + 2 + 4(1 + 2T(n-3)) \\ &= 1 + 2 + 4 + 8T(n-3) \\ &= 2^0 + 2^1 + 2^2 + 2^3 T(n-3) = \\ &= 2^0 + 2^1 + 2^2 + \dots + 2^{k-1} + 2^k T(n-k) \\ &= 2^0 + 2^1 + 2^2 + \dots + 2^{(n-1)-1} + 2^{(n-1)} T(n - (n-1)) \\ &= 2^0 + 2^1 + 2^2 + \dots + 2^{(n-2)} + 2^{(n-1)} T(1) \\ &= 2^n - 1 \end{aligned}$$

3.2 Proste na płaszczyźnie



Rysunek 4. Ekscytujące imitacje prostych na płaszczyźnie

Problem Chcemy wyznaczyć maksymalną liczbę obszarów, którą możemy uzyskać po podzieleniu płaszczyzny n prostymi.

Obserwacja Jeśli $n - 1$ prostych podzieliło płaszczyznę na maksymalną liczbę obszarów, to jeśli poprowadzimy n -tą prostą w taki sposób, by nie była ona równoległa do żadnej innej prostej, to będzie można ją zinterpretować, względem punktów przecięć z innymi prostymi, jako $n - 2$ odcinki oraz 2 półproste. Każdy odcinek i półprosta dzieli dotychczasowy obszar na dwa, zatem liczba obszarów zostaje zwiększona o n .

Oznaczmy największą liczbę obszarów jaką można uzyskać po podzieleniu płaszczyzny n prostymi jako $L(n)$. Oczywiście $L(1) = 2$. Na podstawie powyższej obserwacji otrzymujemy $L(n) = L(n - 1) + n$. Wyznamy jawny wzór na $L(n)$ stosując metodę iteracyjną:

$$\begin{aligned} L(n) &= n + L(n - 1) = \\ &= n + (n - 1) + L(n - 2) \\ &= n + (n - 1) + \dots + (n - (k - 1)) + L(n - k) \\ &= n + (n - 1) + \dots + (n - ((n - 1) - 1)) + L(n - (n - 1)) \\ &= n + (n - 1) + \dots + 2 + L(1) \\ &= n + (n - 1) + \dots + 2 + 1 + 1 \\ &= \frac{(n + 1)n}{2} + 1 \end{aligned}$$

II 13.X.2008

1 Liczby Fibonacciego

Definicja F_n : Jest to n -ta liczba Fibonacciego, gdzie

$$F_n = \begin{cases} 0 & \text{dla } n = 0, \\ 1 & \text{dla } n = 1, \\ F_{n-1} + F_{n-2} & \text{dla } n > 1 \end{cases}$$

Bajeczka o króliczkach

Na potrzeby bajeczki definiujemy dwa rodzaje króliczków: *króliczki małe* i *króliczki duże*.


Obserwacja 1. Króliczki małe nie mogą robić tego, co króliczki lubią robić najbardziej. Powyższa obserwacja wynika wprost z definicji króliczka małego.


Obserwacja 2. Króliczki małe po miesiącu zamieniają się w króliczki duże, natomiast każda para króliczków dużych po miesiącu generuje parę króliczków małych. W szczególności, para króliczków małych nie generuje żadnej nowej pary, co wynika z obserwacji (1).


Definiujemy *niezniszczalne króliczki małe (duże)* jako *króliczki małe (duże)* z tą dodatkową własnością, że ich żywotność można scharakteryzować w kategorii półprostej, to znaczy w pewnym momencie się rodzą, a potem żyją sobie w nieskończoność.














Od tej pory na *niezniszczalne króliczki małe (duże)* będziemy mówić skrótowo *króliczki małe (duże)*, co nie powinno prowadzić do nieporozumień.
































Wprowadzamy następujące oznaczenia:

Para króliczków małych: 

Para króliczków dużych: 

Załóżmy, że dysponujemy  w pierwszym miesiącu. Wtedy liczba króliczków w następnych miesiącach to

Liczba 					
Liczba 				 	  
Miesiąc	1	2	3	4	5

Liczba 	  	...	      
Liczba 	    	...	      
Miesiąc	6	...	      

Jak widać, w n -tym miesiącu mamy F_n wszystkich par króliczków. Poza tym, liczba króliczków w n -tym miesiącu jest równa liczbie wszystkich króliczków z $n - 1$ miesiąca, ponieważ żyją one sobie dalej, plus liczbie wszystkich króliczków z $n - 2$ miesiąca, ponieważ te króliczki wygenerują nowe w danym n -tym miesiącu. Stąd $F_n = F_{n-1} + F_{n-2}$.



1.1 Zależności dla liczb Fibonacciego

1. $F_2 + F_4 + F_6 + \dots + F_{2n} = F_{2n+1} - 1$

Szkic dowodu

$$\begin{aligned} & \text{Ponieważ } F_1 = 1 \text{ oraz } F_1 + F_2 + F_4 + F_6 + \dots + F_{2n} = \\ & = F_3 + F_4 + F_6 + \dots + F_{2n} \\ & = F_5 + F_6 + \dots + F_{2n} \\ & = F_{2k-1} + F_{2k} + F_{2k+2} + F_{2k+4} + \dots + F_{2n} \\ & = F_{2k+1} + F_{2k+2} + F_{2k+4} + \dots + F_{2n} \\ & = F_{2n-1} + F_{2n} = F_{2n+1} \\ & \text{to } F_2 + F_4 + F_6 + \dots + F_{2n} = F_{2n+1} - 1 \end{aligned}$$

2. $F_{n+m+1} = F_{n+1}F_{m+1} + F_nF_m$

Dowód Indukcja po m .

1. *Baza indukcji*

$$m = 0: F_{n+1} = F_{n+1}F_1 + 0 \Rightarrow F_{n+1} = F_{n+1}$$

$$m = 1: F_{n+2} = F_{n+1}F_2 + F_nF_1 = F_{n+1} + F_n$$

2. *Krok indukcyjny*

Wykażemy, że jeśli zależność zachodzi dla $m - 1$ oraz m , to zachodzi także dla $m + 1$. Załóżmy więc, że zależność zachodzi dla $m - 1$ oraz m . Wtedy:

$$\begin{aligned} F_{n+m+2} &= F_{n+m+1} + F_{n+m} = \\ &= (F_{n+1}F_{m+1} + F_nF_m) + (F_{n+1}F_m + F_nF_{m-1}) \\ &= F_{n+1}(F_{m+1} + F_m) + F_n(F_m + F_{m-1}) \\ &= F_{n+1}F_{m+2} + F_nF_{m+1} \quad \square \end{aligned}$$

3.

$$F_n = \frac{1}{\sqrt{5}} \left(\underbrace{\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n}_{\text{proporcja złotego podziału}} \right)$$

W powyższym wzorze prawy ułamek wynosi około -0.618 , więc potęgowany do n jest szybko zbieżny do zera. Powoduje to, że często można przyjąć

$$F_n \approx \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n$$

2 Algorytmy oparte na rekursji

2.1 Sortowanie przez scalanie

Sortowanie przez scalanie jest sposobem sortowania opartym na strategii *dziel i zwyciężaj*. Polega ono na podziale sortowanego ciągu na dwa mniejsze prawie równej długości (z dokładnością do 1 elementu), posortowaniu ich i scaleniu w jeden ciąg. Złożoność tego sortowania wynosi $\Theta(n \log n)$, co wykażemy dalej.

Scalanie dwóch posortowanych ciągów A oraz B polega na powtarzaniu następującego procesu:

1. Porównaj najmniejszy element ciągu A z najmniejszym elementem ciągu B .
2. Wybierz mniejszy z tych elementów, dopisz go do ciągu wynikowego oraz skasuj go z ciągu, w którym się znajdował.

Gdy któryś z ciągów A, B zostanie całkowicie skasowany, to pozostały ciąg zostaje dopisany do ciągu wynikowego i proces scalania kończy się.

Jeśli ciąg A ma długość k , a ciąg B długość l , to maksymalna liczba porównań jaka może być potrzebna wynosi $k + l - 1$. Jest tak dlatego, gdyż każde porównanie zawsze pozwala dopisać jeden element do wyniku, a gdy zostanie jeden element, to nie trzeba wykonywać już porównań. W związku z tym czas działania scalania to $\Theta(k + l)$.

Algorytm:

Dane: $\underbrace{a_i, a_{i+1}, \dots, a_m}_{\lfloor \frac{\text{długość danych}}{2} \rfloor}, \underbrace{a_{m+1}, \dots, a_j}_{\lceil \frac{\text{długość danych}}{2} \rceil}$

Sort(i, j):

Jeśli $i = j$ to zwróć a_i

W p. p. podstaw $m := \lfloor (i - 1 + j)/2 \rfloor$ i zwróć $scal(i, m)(m + 1, j)$.

Zdefiniujmy $T(n)$ jako czas działania procedury $Sort(i, j)$ dla długości danych równej n oraz $f(n)$ jako maksymalną liczbę porównań jaką wykonuje $Sort$ wywołany na danych długości n . Wtedy

$$\begin{aligned} T(1) &= c \quad \text{dla pewnej stałej } c \\ T(n) &= T(\lfloor \frac{n}{2} \rfloor) + T(\lceil \frac{n}{2} \rceil) + \Theta(n) \\ f(1) &= 0 \\ f(n) &= f(\lfloor \frac{n}{2} \rfloor) + f(\lceil \frac{n}{2} \rceil) + n - 1 \end{aligned}$$

Określmy złożoność $T(n)$ dla n postaci 2^k , gdzie $k \in \mathbb{N}$.

$$\begin{aligned} T(n) &= 2T(n/2) + \Theta(n) \Rightarrow \\ \exists_{c_1, c_2 > 0} \exists_{n_0} \forall_{n > n_0} \quad 2T(n/2) + c_1 \cdot n &\leq T(n) \leq 2T(n/2) + c_2 \cdot n \end{aligned}$$

Rozwińmy prawą uzyskaną nierówność. Kwantyfikatory pomijamy dla przejrzystości.

$$\begin{aligned} T(n) &\leq c_2 \cdot n + 2T(n/2) \\ &\leq c_2 \cdot n + 2(c_2 \cdot (n/2) + 2T(n/4)) \\ &= c_2 \cdot n + c_2 \cdot n + 4T(n/4) \\ &\leq \underbrace{c_2 \cdot n + c_2 \cdot n + \dots + c_2 \cdot n}_{k \text{ elementów}} + 2^k T(n/2^k) \\ &\leq \underbrace{c_2 \cdot n + c_2 \cdot n + \dots + c_2 \cdot n}_{\log_2 n \text{ elementów}} + 2^{\log_2 n} T(n/2^{\log_2 n}) \\ &= \log_2 n \cdot c_2 \cdot n + nT(1) \\ &= \log_2 n \cdot c_2 \cdot n + n \cdot c \\ &\leq \log_2 n \cdot c_2 \cdot n + n \log_2 n \cdot c \\ &= n \log_2 n \cdot (c_2 + c) \\ &= O(n \log n) \end{aligned}$$

W dualny sposób rozwijamy nierówność $2T(n/2) + c_1 \cdot n \leq T(n)$ otrzymując $T(n) = \Omega(n \log n)$.

Skoro $T(n) = O(n \log n)$ oraz $T(n) = \Omega(n \log n)$, to $T(n) = \Theta(n \log n)$.

2.2 Mnożenie długich liczb

Dwie liczby o długości $\leq n$ można przemnożyć pisemnie w czasie $O(n^2)$. Pokażemy, że można tego dokonać w czasie $\Theta(n^{1.58})$.

Algorytm

Dane: Dwie liczby A oraz B , gdzie $A = \overline{a_{n-1}a_{n-2}a_{n-3} \dots a_0}$, $B = \overline{b_{n-1}b_{n-2}b_{n-3} \dots b_0}$.

Pomnóż(A, B):

1. Jeśli A, B są krótkie, to użyj mnożenia z Twojego ulubionego języka programowania.
2. Poziel A na $A_1 = \overline{a_{n-1} \dots a_{n/2}}$ oraz $A_0 = \overline{a_{n/2-1} \dots a_0}$.
3. Dokonaj analogicznego podziału B na B_1 oraz B_0 .

Wtedy $A = \underbrace{\overline{a_{n-1} \dots a_{n/2}}}_{A_1} \underbrace{\overline{a_{n/2-1} \dots a_0}}_{A_0}$ i analogicznie dla B .

4. $m_0 \leftarrow \text{Pomnóż}(A_0, B_0)$
5. $m_2 \leftarrow \text{Pomnóż}(A_1, B_1)$
6. $c_1 \leftarrow \text{Pomnóż}(A_0 + A_1, B_0 + B_1)$
7. Zwróć $m_0 + (c_1 - m_0 - m_2) \cdot 2^{n/2} + m_2 \cdot 2^n$

Dowód poprawności algorytmu Indukcja po długości danych.

1. *Baza indukcji*

Spełniona wprost z definicji kroku 1. algorytmu.

2. *Krok indukcyjny*

Zakładamy, że algorytm działa poprawnie dla danych długości $\leq n/2$. Wykażemy, że działa poprawnie także dla danych długości $\leq n$.

Zgodnie z założeniem, m_0, m_2 oraz c_1^\ddagger są poprawnie obliczone. Chcemy obliczyć iloczyn $A \cdot B$. Zauważmy, że

$$A \cdot B = (2^{n/2}A_1 + A_0)(2^{n/2}B_1 + B_0) = \underbrace{A_0B_0}_{m_0} + 2^{n/2}(A_0B_1 + A_1B_0) + 2^n \underbrace{A_1B_1}_{m_2}$$

W związku z poczynionymi obserwacjami o m_0 i m_2 pozostaje wykazać, że

$$(A_0B_1 + A_1B_0) \cdot 2^{n/2} = (c_1 - m_0 - m_2) \cdot 2^{n/2} \iff$$

$$(A_0B_1 + A_1B_0) = (c_1 - m_0 - m_2)$$

Tak więc

$$\begin{aligned} (c_1 - m_0 - m_2) &= \\ &= (A_0 + A_1)(B_0 + B_1) - A_0B_0 - A_1B_1 \\ &= A_0B_0 + A_0B_1 + A_1B_0 + A_1B_1 - A_0B_0 - A_1B_1 \\ &= A_0B_1 + A_1B_0 \quad \square \end{aligned}$$

Definiujemy $T(n)$ jako czas działania procedury $\text{Pomnóż}(A, B)$ dla n bitowych liczb A, B . Wtedy dla n postaci $2^k, k \in \mathbb{N}$:

$$T(1) = c_0 \quad \text{dla pewnej stałej } c_0$$

$$T(n) = 3T(n/2) + \Theta(n).$$

[‡]Tutaj jest małe oszustwo, gdyż argumenty przy obliczaniu c_1 mogą być $n/2 + 1$ bitowe, ale jak się okazuje, to nic nie psuje i na tym przedmiocie nie powinno nas martwić.

Jest tak, ponieważ obliczenie m_0, m_2 oraz c_1 zajmuje po $T(n/2)$ czasu, natomiast dodawanie oraz mnożenie przez wielokrotność 2 wykonuje się w $\Theta(n)$.

Określmy złożoność $T(n)$ dla n postaci 2^k , $k \in \mathbb{N}$.

UWAGA! Na wykładzie, zamiast powyższego wzoru na $T(n)$, był wzór $T(n) = 3T(n/2) + c \cdot n$. Jest to skrót myślowy; zamiast pisać dwie nierówności i dwie różne stałe c_1, c_2 tak jak to było czynione przy określaniu złożoności dla sortowania przez scalanie, piszemy od razu jedną stałą c i znak równości, co ma w istocie symulować nierówności „ \geq ”, ze stałą c_1 , oraz nierówności „ \leq ”, ze stałą c_2 . Posłużę się tutaj tym samym skrótem; należy jednak pamiętać, co on oznacza.

$$\begin{aligned}
 T(n) &= c \cdot n + 3T(n/2) = \\
 &= c \cdot n + 3(c \cdot (n/2) + 3T(n/4)) \\
 &= c \cdot n + \frac{3}{2} \cdot c \cdot n + 9T(n/4) \\
 &= c \cdot n + \frac{3}{2} \cdot c \cdot n + \frac{9}{4} \cdot c \cdot n + 27T(n/8) \\
 &= c \cdot n + \frac{3}{2} \cdot c \cdot n + \dots + \left(\frac{3}{2}\right)^{k-1} \cdot c \cdot n + 3^k T(n/2^k) \\
 &= c \cdot n + \frac{3}{2} \cdot c \cdot n + \dots + \left(\frac{3}{2}\right)^{\log_2 n - 1} \cdot c \cdot n + 3^{\log_2 n} T(n/2^{\log_2 n}) \\
 &= \left(1 + \frac{3}{2} + \frac{9}{4} + \dots + \left(\frac{3}{2}\right)^{\log_2 n - 1}\right) \cdot c \cdot n + n^{\log_2 3} T(1) \\
 &= \frac{3^{\log_2 n} - 1}{\frac{3}{2} - 1} \cdot c \cdot n + n^{\log_2 3} c_0 \\
 &= 2 \cdot \left(\frac{n^{\log_2 3} - 1}{n} + 1\right) \cdot c \cdot n + n^{\log_2 3} c_0 \\
 &= n^{\log_2 3} (c_0 + 2c) - 2 \cdot c \cdot n
 \end{aligned}$$

Tutaj dowód nieznacznie różni się, w zależności od nierówności.

Dla \leq mamy $n^{\log_2 3} (c_0 + 2c) - 2 \cdot c \cdot n \leq n^{\log_2 3} (c_0 + 2c) = O(n^{\log_2 3})$

Dla \geq mamy $n^{\log_2 3} (c_0 + 2c) - 2 \cdot c \cdot n = n^{\log_2 3} c_0 + 2c(n^{\log_2 3} - n) \geq n^{\log_2 3} c_0 = \Omega(n^{\log_2 3})$

Ponieważ $T(n) = O(n^{\log_2 3})$ oraz $T(n) = \Omega(n^{\log_2 3})$ to $T(n) = \Theta(n^{\log_2 3}) \approx \Theta(n^{1.58})$ \square

3 Arytmetyka modularna

Przypomnienie: \mathbb{N} - liczby naturalne, \mathbb{Z} - liczby całkowite.

Fakt 1. Dla $a \in \mathbb{Z}, b \in \mathbb{N}_+$ istnieją $q \in \mathbb{Z}, r \in \{0, 1, \dots, b-1\}$ takie, że $a = qb + r$.

Wynika stąd, że $q = \lfloor \frac{a}{b} \rfloor$ oraz $r = a - \lfloor \frac{a}{b} \rfloor \cdot b$.

Wprowadzamy następujące oznaczenia (definicje zmiennych są z faktu (1)):

$$q = a \operatorname{div} b, \quad r = a \operatorname{mod} b,$$

$$r = 0 \Rightarrow b|a,$$

$$b|a \iff a = b \cdot q \quad \text{dla pewnego } q \in \mathbb{Z},$$

$$a \equiv b \pmod{n} \iff a \equiv_n b \iff a \operatorname{mod} n = b \operatorname{mod} n.$$

Fakt 2. $a \equiv b \pmod{n} \iff n|a - b$

Dowód

Załóżmy, że $a \equiv b \pmod{n}$. Wtedy $a \operatorname{mod} n = b \operatorname{mod} n$ oraz istnieją takie q_a, q_b , że

$$a = q_a n + (a \operatorname{mod} n) \quad \text{oraz} \quad b = q_b n + (b \operatorname{mod} n). \quad \text{Mamy } a - b = q_a n + (a \operatorname{mod} n) - (q_b n + (b \operatorname{mod} n)) = q_a n - q_b n + (a \operatorname{mod} n - b \operatorname{mod} n) = n(q_a - q_b) + (a \operatorname{mod} n - b \operatorname{mod} n) = n(q_a - q_b) \Rightarrow n|a - b$$

Odwrotnie. Załóżmy, że $n|a - b$. Wtedy $a - b = n \cdot q$, dla pewnego $q \in \mathbb{Z}$. Z faktu (1) istnieją takie q_a, q_b, r_a, r_b , że $(q_a, q_b \in \mathbb{Z}) \wedge (r_a, r_b \in \mathbb{Z}_+ \wedge r_a, r_b < n) \wedge (a = q_a n + r_a) \wedge (b = q_b n + r_b)$. Stąd $a - b = n \cdot q \Rightarrow$

$$\Rightarrow q_a \cdot n + r_a - (q_b \cdot n + r_b) = n$$

$$\Rightarrow r_a - r_b = n(q - q_a + q_b)$$

Ponieważ prawa strona równości jest wielokrotnością n , a $0 \leq r_a, r_b < n$, to $|r_a - r_b| < n$, zatem $r_a - r_b = 0 \Rightarrow r_a = r_b$, czyli $a \bmod n = b \bmod n \iff a \equiv b \pmod{n}$. \square

Fakt 3. $a \equiv_n A \wedge b \equiv_n B \implies a + b \equiv_n A + B \wedge ab \equiv_n AB$

Dowód

Niech $a = qn + r$, $A = Qn + r$, $b = sn + R$, $B = Sn + R$ wtedy

$$a + b = (q + s)n + r + R \equiv (Q + S)n + r + R = A + B$$

$$ab = (qn + r)(sn + R) =$$

$$= qsn^2 + qRn + srn + rR$$

$$= n(qsn + qR + sr) + rR$$

$$= Xn + rR \equiv Yn + rR =$$

$$= n(QSn + QR + Sr) + rR$$

$$= QSn^2 + QRn + Srn + rR$$

$$= (Qn + r)(Sn + R) = AB \quad \square$$

Wprowadzamy następujące oznaczenia:

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\},$$

$$a +_n b = (a + b) \bmod n,$$

$$a \cdot_n b = (a \cdot b) \bmod n,$$

$$a \perp b \iff a \text{ i } b \text{ są względnie pierwsze.}$$

Własności $+_n$ oraz \cdot_n :

- Łączność dodawania:
 $a +_n (b +_n c) \equiv_n a + (b + c) = (a + b) + c \equiv_n (a +_n b) +_n c$
- Element neutralny $+_n$: 0
- Element odwrotny a względem $+_n$: $\begin{cases} n - a & \text{dla } a \neq 0, \\ 0 & \text{dla } a = 0 \end{cases}$
- Rozdzielność: $(a +_n b) \cdot_n c = a \cdot_n c +_n b \cdot_n c$
- Łączność mnożenia: $a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c$
- Element neutralny \cdot_n : 1
- Element odwrotny \cdot_n : Jeśli występuje dla każdego $n \in \mathbb{Z}_n \setminus \{0\}$, to \mathbb{Z}_n jest ciałem. W innym wypadku \mathbb{Z}_n jest pierścieniem.

Fakt 4. $a \perp n \Rightarrow a^{-1} \bmod n$ (czyli element odwrotny a dla \cdot_n) istnieje.

Definicje NWD i NWW:

NWD - największy wspólny dzielnik,

NWW - najmniejsza wspólna wielokrotność.

$$NWD(a, b) = \max\{d : d|a \wedge d|b\}$$

$$NWW(a, b) = \min\{c : a|c \wedge b|c\}$$

Własności NWD i NWW:

- $a \perp b \iff NWD(a, b) = 1$
- $NWD(a, b) = NWD(b, a)$
- $NWW(a, b) = NWW(b, a)$
- $NWD(a, 0) = a$
- $NWW(a, 1) = a$

Lemat $NWD(a, b) = NWD(a - b, b)$

Dowód Z definicji NWD mamy:

$$NWD(a, b) = \max\{d : d|a \wedge d|b\}$$

$$NWD(a - b, b) = \max\{d : d|a - b \wedge d|b\}$$

Wykażemy równoważność dwóch powyższych zbiorów.

Weźmy zatem $d \in \{d : d|a \wedge d|b\}$. Wtedy

$$d|a \wedge d|b \Rightarrow$$

$$\Rightarrow a = dq_1 \wedge b = dq_2 \quad \text{dla pewnych } q_1, q_2 \in \mathbb{Z}$$

$$\Rightarrow a - b = d(q_1 - q_2) \wedge b = dq_2$$

$$\Rightarrow d|a - b \wedge d|b$$

$$\Rightarrow d \in \{d : d|a - b \wedge d|b\}$$

Niech $d \in \{d : d|a - b \wedge d|b\}$. Wtedy

$$d|a - b \wedge d|b \Rightarrow$$

$$\Rightarrow a - b = dq_1 \wedge b = dq_2 \quad \text{dla pewnych } q_1, q_2 \in \mathbb{Z}$$

$$\Rightarrow a = d(q_1 + q_2) \wedge b = dq_2$$

$$\Rightarrow d|a \wedge d|b$$

$$\Rightarrow d \in \{d : d|a \wedge d|b\} \quad \square$$

Wniosek $NWD(a, b) = NWD(a - cb, b)$ ponieważ

$$NWD(a, b) = NWD(a - b, b) = NWD(a - 2b, b) = \dots = NWD(a - cb, b).$$

3.1 Algorytm Euklidesa

NWD(a, b):

1. Jeśli $b > a$, to zamień a i b pozycjami.
2. Jeśli $b = 0$, to $NWD(a, b) := a$.
W p. p. $NWD(a, b) := NWD(a - b, b)$

Krócej można napisać:

NWD(a, b):

1. Dopóki $b > 0$: $(a, b) \leftarrow (b, a \bmod b)$
2. $NWD(a, b) = a$

III 20.X.2008

1 Algorytm Euklidesa c. d.

Lemat Jeśli w danej iteracji obliczania $NWD(a, b)$ zachodzi $a \geq b \wedge (a < F_{n+1} \vee b < F_n)$, to w następnej iteracji $NWD(a' = b, b' = a \bmod b)$ zachodzi $a' \geq b' \wedge (a' < F_n \vee b' < F_{n-1})$.

Dowód

1. Jeśli $b < F_n$ to $a' < F_n$ ponieważ $a' = b$.
2. Jeśli $b \geq F_n$ to $a < F_{n+1}$. Ponieważ $b' = a \bmod b$ to $b' \leq a - b < F_{n+1} - F_n = F_{n-1}$ \square

Wniosek[§] Algorytm Euklidesa wykonuje conajwyżej $\sim (\log_{\frac{1+\sqrt{5}}{2}} \min\{a, b\})$ iteracji. Wynika to z tego, że jeśli są spełnione założenia z lematu, to algorytm wykona conajwyżej $n - 1$ iteracji, natomiast $F_n \approx \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n$ więc $\log_{\frac{1+\sqrt{5}}{2}} F_n \approx n$, zatem $\log_{\frac{1+\sqrt{5}}{2}} \min\{a, b\} < \log_{\frac{1+\sqrt{5}}{2}} F_{n+1} \approx n + 1$.

Przykład działania zwykłego algorytmu Euklidesa dla $a = 245$ i $b = 168$.

a	b	obliczenia b
245	168	
168	77	$245 - 168$
77	14	$168 - 2 \cdot 77$
14	7	$77 - 5 \cdot 14$
7	0	$14 - 2 \cdot 7$

Chcemy również znać x, y takie, że $x \cdot a + y \cdot b = NWD(a, b)$.

Jedną metodą na poznanie x, y jest cofanie się w obliczeniach. Dla powyższego przykładu wygląda to tak:

$$\begin{aligned} NWD(a, b) &= 7 = \\ &= 77 - 5 \cdot 14 \\ &= 77 - 5 \cdot (168 - 2 \cdot 77) \\ &= -5 \cdot 168 + 11 \cdot 77 \\ &= -5 \cdot 168 + 11 \cdot (245 - 168) \\ &= \underbrace{11}_x \cdot 245 + \underbrace{(-16)}_y \cdot 168 \end{aligned}$$

Inną metodą jest

1.1 Rozszerzony algorytm Euklidesa

extNWD(A,B):

1. $(a, b, x_a, y_a, x_b, y_b) \leftarrow (A, B, 1, 0, 0, 1)$
2. Dopóki $b \neq 0$:
 - 2.1. $q \leftarrow \lfloor \frac{a}{b} \rfloor$
 - 2.2. $(a, b, x_a, y_a, x_b, y_b) \leftarrow (b, a - qb, x_b, y_b, x_a - qx_b, y_a - qy_b)$
3. $(x, y, NWD) \leftarrow (x_a, y_a, a)$

Objaśnienie

A, B - Dane wejściowe.

a, b - Wartości A, B w danej iteracji algorytmu. Odpowiedniki a, b ze zwykłego algorytmu Euklidesa.

[§]Ćwiczenie: znaleźć i poprawić błąd we wniosku.

x_a, x_b, y_a, y_b - Liczby takie, że po każdej iteracji spełnione są równości:

$$x_a A + y_a B = a$$

$$x_b A + y_b B = b$$

x, y, NWD - Wartości zwracane przez algorytm, takie, że $xA + yB = NWD = NWD(A, B)$.

Krok 1. algorytmu jest trywialny.

W kroku 2. algorytmu podstawiamy b za a oraz $a - qb = a \bmod b$ za b , zgodnie z tym co robi zwykły algorytm Euklidesa.

W związku z pierwszym z powyższych podstawień, zgodnie z definicjami x_a, y_a musimy podstawić $(x_a, y_a) \leftarrow (x_b, y_b)$.

Ponieważ $a - qb = (x_a A + y_a B) - q(x_b A + y_b B) = (x_a - qx_b)A + (y_a - qy_b)B$, to zgodnie z definicjami x_b, y_b musimy podstawić $(x_b, y_b) \leftarrow (x_a - qx_b, y_a - qy_b)$.

Po ostatniej iteracji największym wspólnym dzielnikiem jest a , stąd w kroku 3. zwracamy $(x, y, NWD) \leftarrow (x_a, y_a, a)$.

Twierdzenie Dla dowolnych $a, b \in \mathbb{N}$ istnieją $x, y \in \mathbb{Z}$ takie, że $xa + yb = NWD(a, b)$. Te x, y mogą być efektywnie wyznaczone za pomocą rozszerzonego algorytmu Euklidesa.

Od tej pory rozszerzony algorytm Euklidesa będziemy nazywać algorytmem Euklidesa.

Zastanówmy się, kiedy w \mathbb{Z}_n istnieje element odwrotny a^{-1} dla danego a .

Będziemy rozpatrywać $a, n \in \mathbb{N}$. Zgodnie z powyższym twierdzeniem zachodzi $xa + yn = NWD(a, n)$ dla pewnych $x, y \in \mathbb{Z}$.

$$a \perp n \Rightarrow$$

$$\Rightarrow NWD(a, n) = 1$$

$$\Rightarrow xa + yn = 1$$

$$\Rightarrow xa \equiv 1 \pmod{n}$$

$$\Rightarrow x = a^{-1} \text{ w } \mathbb{Z}_n$$

Wniosek 1. Jeśli $a \perp n$, to $a^{-1} \bmod n$ istnieje i może być łatwo wyznaczone z algorytmu Euklidesa.

Załóżmy, że $NWD(a, n) = d > 1$. Weźmy dowolny $x \in \mathbb{Z}$. Wtedy zachodzi

$xa \bmod n = xa - qn$ dla pewnego $q \in \mathbb{Z}$. Ponieważ $d|a \wedge d|n$, to $d|xa - qn$, więc skoro $d > 1$, to $xa \bmod n \neq 1$.

Wniosek 2. Jeśli $NWD(a, n) \neq 1$ to $a^{-1} \bmod n$ nie istnieje.

Wniosek 3. Z wniosków (1) i (2) wynika, że \mathbb{Z}_p jest ciałem (czyli każdy element należący do \mathbb{Z}_p ma element odwrotny) wtedy i tylko wtedy, gdy p jest liczbą pierwszą.

2 Liczby pierwsze

2, 3, 5, 7, 11, 13, ...

Zbiór liczb pierwszych będziemy oznaczać jako \mathbb{P} . Jeśli $x \in \mathbb{P}$, to $x \in \mathbb{N}$, $x > 1$ oraz jedynymi naturalnymi dzielnikami x są 1 i x .

Każda liczba naturalna ma rozkład na czynniki pierwsze. Symbolicznie:

$$\forall n \in \mathbb{N} \exists p_1, p_2, \dots, p_k \ n = p_1 p_2 \dots p_k, \text{ gdzie } p_1 p_2 \dots p_k \text{ są parami różne i są liczbami pierwszymi.}$$

Twierdzenie Rozkład każdej liczby naturalnej na czynniki pierwsze jest jednoznaczny z dokładnością do kolejności zapisu czynników.

Dowód Załóżmy, że n jest najmniejszą liczbą naturalną posiadającą więcej niż jeden rozkład na czynniki pierwsze. Oznaczmy dowolne dwa z tych rozkładów jako $p_1 p_2 \dots p_k$ oraz $q_1 q_2 \dots q_l$.

Jeśli dla pewnego p_i, q_j zachodzi $p_i = q_j$, to $n/p_i = n' < n$ też ma więcej niż jeden rozkład ζ

Założmy więc, że żaden czynnik pierwszy nie występuje naraz w rozkładzie $p_1 p_2 \dots p_k$ oraz $q_1 q_2 \dots q_l$.

Stosujemy algorytm Euklidesa na p_1 i q_1 by znaleźć x, y takie, że $x p_1 + y q_1 = \text{NWD}(p_1, q_1) = 1$. Gdy wprawdzie przemnożymy obie strony równości przez $q_2 q_3 \dots q_l$, otrzymujemy:

$$x p_1 q_2 q_3 \dots q_l + y q_1 q_2 q_3 \dots q_l = q_2 q_3 \dots q_l \Rightarrow$$

$$x p_1 q_2 q_3 \dots q_l + y p_1 p_2 p_3 \dots p_k = q_2 q_3 \dots q_l \Rightarrow$$

$$p_1 (x q_2 q_3 \dots q_l + y p_2 p_3 \dots p_k) = q_2 q_3 \dots q_l \Rightarrow$$

$$p_1 | q_2 q_3 \dots q_l$$

Zatem $q_2 q_3 \dots q_l < n$ ma jeszcze jeden rozkład, w którym jednym z czynników jest $p_1 \zeta$ \square

Twierdzenie Liczb pierwszych jest nieskończenie wiele.

Dowód (Euklidesa)

Dowód niewprost. Załóżmy, że $p_1 p_2 \dots p_k$ to wszystkie liczby pierwsze.

Niech $p = p_1 p_2 \dots p_k + 1 = q_1 q_2 \dots q_l$ gdzie $q_1 q_2 \dots q_l$ to rozkład na czynniki pierwsze liczby p .

Ponieważ $\text{NWD}(x, x+1) = 1$ dla dowolnego x , to żadna z liczb p_1, p_2, \dots, p_k nie dzieli $q_1 q_2 \dots q_l$.

W szczególności, żadna z liczb $p_1, p_2 \dots p_k$ nie jest żadną z liczb $q_1, q_2 \dots q_l$, więc każda z liczb $q_1, q_2 \dots q_l$ jest liczbą pierwszą różną od liczb $p_1, p_2 \dots p_k$, czyli tych, które istnieją ζ . \square

Definicja $\pi(n)$ to ilość liczb pierwszych w przedziale $[1, n]$.

Można wykazać, że $\frac{\pi(n)}{n} \sim \frac{1}{\ln n}$. My pokażemy słabszą zależność.

Twierdzenie $\frac{\pi(n)}{n} = \Theta\left(\frac{1}{\ln n}\right)$

Dowód

Niech p oznacza dowolną liczbę pierwszą.

Lemat 1 $\pi(n) = O\left(\frac{n}{\ln n}\right)$

Lemat 2 $\pi(n) = \Omega\left(\frac{n}{\ln n}\right)$

Dowód lematu 1

Pokażemy, że $\prod_{p \leq n} p \leq 4^n$. Dowód będzie przebiegał przez indukcję po n .

1. *Baza indukcji* $n = 0$: $\prod_{p \leq 0} p \leq 4^0$

Poza tym zależność zachodzi także dla $n = 1, 2$.

2. *Krok indukcyjny*

Jeśli n jest parzyste i $n \neq 2$, to $\prod_{p \leq n} p = \prod_{p \leq n-1} p$, więc wystarczy przeprowadzić krok indukcyjny dla nieparzystych n .

Załóżmy, że twierdzenie jest spełnione dla wszystkich liczb $\leq n-1$. Wykażemy, że twierdzenie zachodzi też dla n . Dodatkowo zakładamy, że n jest nieparzyste i $n \geq 3$.

$$(1) \quad \prod_{p \leq n} p = \prod_{p \leq \frac{n+1}{2}} p \cdot \prod_{\substack{p \leq n \\ \frac{n+1}{2} < p \leq n}} p \stackrel{\text{zał. ind.}}{\leq} 4^{\frac{n+1}{2}} \cdot \prod_{\frac{n+1}{2} < p \leq n} p = 4^{\frac{n+1}{2}} \cdot S$$

Zauważmy, że

$$\binom{n}{\frac{n+1}{2}} = \frac{n!}{(n - \frac{n+1}{2})! \cdot \frac{n+1}{2}!} = \frac{n(n-1) \dots (n - (\frac{n+1}{2}) + 1)}{\frac{n-1}{2}!} = B$$

Ponieważ B oznacza liczbę wszystkich podzbiorów $\frac{n+1}{2}$ -elementowych zbioru n -elementowego, to jest to liczba całkowita. Ponadto, w powyższym zapisie B jako ułamka, w liczniku mamy wszystkie liczby pierwsze z przedziału $\frac{n+1}{2} \dots n$. Dodatkowo, mianownik skraca się do jedynki z liczbami z licznika nie będącymi liczbami pierwszymi, ponieważ w innym wypadku B nie byłoby liczbą całkowitą. Z powyższych dwóch obserwacji wnioskujemy, że $S|B$. Prawdą jest także, że $B = \binom{n}{\frac{n+1}{2}} = 2 \binom{n-1}{\frac{n-1}{2}} = 2B'$, ponieważ liczba zbiorów $\frac{n+1}{2}$ -elementowych w zbiorze n -elementowym jest równa liczbie zbiorów $(\frac{n+1}{2} - 1)$ -elementowych w zbiorze $n-1$ -elementowym wziętych raz z n -tym elementem, a raz bez niego.

Ponieważ $n \geq 3$, to 2 nie jest częścią iloczynu S . W związku z tym z faktu $S|B \wedge B = 2B'$ wynika, że $S|B'$. To z kolei oznacza, że $S \leq B'$. Zauważamy, że B' jest mniejsze niż liczba wszystkich podzbiorów zbioru $(n-1)$ -elementowego, która wynosi 2^{n-1} . Mamy więc $S \leq B' < 2^{n-1}$.

Zatem ze wzoru (1) wynika:

$$\prod_{p \leq n} p \leq 4^{\frac{n+1}{2}} \cdot S < 4^{\frac{n+1}{2}} \cdot 4^{\frac{n-1}{2}} = 4^n$$

co kończy dowód kroku indukcyjnego.

Oznaczmy $k = \pi(n)$. Wtedy $k! \leq \prod_{p \leq n} p$, ponieważ w iloczynie po prawej stronie nierówności jest tyle samo czynników co w $k!$, oraz można je dobrać parami tak, że każdemu elementowi z $k!$ będzie odpowiadał element większy z iloczynu. Zachodzi także $\left(\frac{k}{2}\right)^{\frac{k}{2}} < k!$, ponieważ $k/2$ największych czynników $k!$ już jest większe niż wyrażenie po lewej stronie nierówności. Mamy zatem

$$\left(\frac{k}{2}\right)^{\frac{k}{2}} < k! \leq \prod_{p \leq n} p < 4^n$$

co po zlogarytmowaniu daje

$$\frac{k}{2} \log \frac{k}{2} < n$$

Niech $g_n \ln g_n = n$. Zgodnie z tym co zostało wykazane na str. 2, w przykładzie 7, mamy $g_n \ln g_n \sim \frac{n}{\ln n}$ czyli $g_n \ln g_n = \Theta(\frac{n}{\ln n}) = O(\frac{n}{\ln n})$.

Ponieważ logarytm jest funkcją rosnącą monotonicznie, to z $\frac{k}{2} \log \frac{k}{2} < g_n \ln g_n$ wynika $k/2 < g_n$, a stąd z kolei wynika $k = O(\frac{n}{\ln n})$, zatem udowodniliśmy prawdziwość lematu (1) \square

Dowód lematu 2

$$\begin{aligned} \text{Niech } S &= \int_0^1 \underbrace{x^n(1-x)^n}_{\geq 0, \text{ więc } S > 0} dx = \int_0^1 p(x) = \int_0^1 (a_0 + a_1x + a_2x^2 + \dots + a_{2n}x^{2n}) = \\ &= \frac{a_0}{1} + \frac{a_1}{2} + \dots + \frac{a_{2n}}{2n+1} = \frac{p}{q}, \end{aligned}$$

gdzie p/q oznacza nieskracalny ułamek.

Zachodzi $p > 0$, ponieważ $S > 0$. Poza tym, po sprowadzeniu wszystkich mianowników $1, 2, \dots, 2n+1$ do wspólnego, mamy w mianowniku $NWW(1, 2, \dots, 2n+1)$. Po skróceniu ułamka otrzymujemy w mianowniku q , czyli $q|NWW(1, 2, \dots, 2n+1)$ więc $q \leq NWW(1, 2, \dots, 2n+1)$. Zatem

$$S = \frac{p}{q} > \frac{1}{NWW(1, 2, \dots, 2n+1)}$$

Interpretacją całki S jest pole powierzchni pod $p(x)$ dla $x \in [0, 1]$. To pole jest ograniczone z góry przez pole jakie byśmy otrzymali gdyby $p(x)$ ciągle przybierał największą wartość na tym przedziale. Ponieważ $x(1-x)$ wynosi najwyżej $\frac{1}{4}$, to $x^n(1-x)^n \leq \frac{1}{4^n}$ więc $S < \frac{1}{4^n}$.

Mamy zatem

$$\frac{1}{4^n} > S > \frac{1}{NWW(1, 2, \dots, 2n+1)}$$

a stąd

$$4^n < NWW(1, 2, \dots, 2n+1)$$

Zastanówmy się nad rozkładem na czynniki pierwsze powyższego NWW . Napewno musi on zawierać wszystkie liczby pierwsze $\leq 2n+1$. Niektóre z nich jednak mogą występować więcej niż jeden raz. Największa liczba pierwsza, która może wystąpić więcej niż 1 raz, jest $\leq \sqrt{2n+1}$, ponieważ aby jakaś liczba w rozkładzie NWW wystąpiła w potęgzie większej od 1, to musiała ona wystąpić w rozkładzie na czynniki pierwsze jakiejś liczby $\leq 2n+1$ w tej samej potęgze. Największa potęga takiej liczby w NWW jest $\leq \log_2(2n+1)$. Liczb, które w NWW mogą wystąpić w potęgze większej niż 1, jest $\leq \sqrt{2n+1}$. Z powyższych rozważań wynika oszacowanie

$$NWW(1, 2, \dots, 2n+1) < \prod_{p \leq 2n+1} p \cdot \sqrt{2n+1}^{\sqrt{2n+1} \log_2(2n+1)}$$

$\spadesuit x(1-x) = -x^2 + x$ przyjmuje największą wartość w wierzchołku paraboli, o współrzędnej $x = 1/2$.

Mamy zatem

$$\begin{aligned}
4^n &< NWW(1, 2, \dots, 2n+1) < \prod_{p \leq 2n+1} p \cdot \sqrt{2n+1}^{\sqrt{2n+1} \log_2(2n+1)} \\
&\implies \\
4^n &< \prod_{p \leq 2n+1} p \cdot 4^{\log_4 \sqrt{2n+1} \cdot \log_2(2n+1) \cdot \sqrt{2n+1}} \\
&\iff \\
4^{n - \log_4 \sqrt{2n+1} \cdot \log_2(2n+1) \cdot \sqrt{2n+1}} &< \prod_{p \leq 2n+1} p \\
&\iff \\
4^{n - \frac{1}{4} \log_2^2(2n+1) \cdot \sqrt{2n+1}} &< \prod_{p \leq 2n+1} p
\end{aligned}$$

Zauważmy, że liczb pierwszych $\leq 2n+1$ jest $\pi(2n+1)$ i każda z nich jest $\leq 2n+1$. To nam pozwala dokonać jeszcze jednego oszacowania i dokończyć dowód:

$$\begin{aligned}
4^{n - \frac{1}{4} \log_2^2(2n+1) \cdot \sqrt{2n+1}} &< \prod_{p \leq 2n+1} p < (2n+1)^{\pi(2n+1)} = 4^{\log_4(2n+1) \pi(2n+1)} \\
&\xRightarrow{\log_4} \\
n - \frac{1}{4} \log_2^2(2n+1) \cdot \sqrt{2n+1} &< \log_4(2n+1) \pi(2n+1) \\
&\iff \\
\frac{n - \frac{1}{4} \log_2^2(2n+1) \cdot \sqrt{2n+1}}{\frac{1}{2} \log_2(2n+1)} &< \pi(2n+1) \\
&\implies \\
\frac{n \left(1 - \frac{o(n)}{4n}\right)}{\frac{1}{2} \log_2(2n+1)} &< \pi(2n+1) \\
&\text{dla prawie wszystkich } n \\
&\xRightarrow{\text{uff...}} \\
\frac{n}{\frac{1}{2} \log_2(2n+1)} &\leq \pi(2n+1)
\end{aligned}$$

Ponieważ $\frac{n}{\frac{1}{2} \log_2(2n+1)} \sim \frac{2n+1}{\log_2(2n+1)} \sim \frac{2n+1}{\ln(2n+1) \log_2 e}$, to wreszcie $\pi(n) = \Omega(n)$, zatem udowodniliśmy prawdziwość lematu (2) \square

Ponieważ wykazaliśmy, że $\pi(n) = O\left(\frac{n}{\ln n}\right)$ oraz $\pi(n) = \Omega\left(\frac{n}{\ln n}\right)$, to $\pi(n) = \Theta\left(\frac{n}{\ln n}\right)$ czyli

$$\frac{\pi(n)}{n} = \Theta\left(\frac{1}{\ln n}\right) \square$$

uff...

IV 27.X.2008

1 Chińskie twierdzenie o resztach

Bajeczka o chińskiej armii

Był sobie generał chińskiej armii która składała się z bardzo wielu żołnierzy. Precyzyjniej, było ich tak wielu, że nie było sensu ich liczyć. Generał jednak miał problem; otóż chciał sprawdzić, czy ktoś nie uciekł. Szczęśliwie, znalazł on chińskie twierdzenie o resztach (które my poznamy za moment), dzięki czemu był w stanie wydedukować:

Niech m oznacza teoretyczną liczbę wszystkich żołnierzy w mojej armii. Dodatkowo, niech $m = m_1 m_2 \dots m_k$ gdzie $m_1, m_2 \dots m_k$ są parami względnie pierwsze. Jako x oznaczę faktyczną liczbę żołnierzy w mojej armii, czyli już po ewentualnych dezercjach. Jeśli teraz ustawię wszystkich x żołnierzy w rzędach o długości m_1 , potem o długości m_2 i tak dalej do m_k , to o ile się okaże, że za każdym razem wszystkie rzędy miały pełną długość, czyli, że $x \bmod m_i = 0$ dla $i \in \{1, 2, \dots, k\}$, to nikt nie uciekł, czyli $x = m$. Jeśli jednak przy którymś ustawieniu pojawił się niepełny rząd, to $x \neq m$ więc ktoś zdezerterował.

Treść twierdzenia

Niech $m_1, m_2 \dots m_k$ będą parami względnie pierwsze i niech m będzie iloczynem tych liczb.

Wtedy układ kongruencji

$$\begin{cases} x \bmod m_1 = a_1 \\ x \bmod m_2 = a_2 \\ \vdots \\ x \bmod m_k = a_k \end{cases} \quad \text{gdzie } a_1, a_2 \dots a_k \in \mathbb{Z} \text{ oraz } 0 \leq a_i < m_i \text{ dla } i \in \{1, 2, \dots, k\} \\ \text{(czyli } a_i \text{ jest resztą modulo } m_i).$$

ma dokładnie jedno rozwiązanie x takie, że $0 \leq x < m \wedge x \in \mathbb{Z}$.

Dowód

Lemat 1: Istnieje x spełniający powyższy układ kongruencji.

Lemat 2: x jest określony jednoznacznie przez a_1, a_2, \dots, a_k .

Dowód lematu 1:

Obserwacja Jeśli $NWD(a, c) = 1$ oraz $NWD(b, c) = 1$ to $NWD(ab, c) = 1$.

Na podstawie ogólnej wersji powyższej obserwacji wnioskujemy, że $NWD(m/m_i, m_i) = 1$ gdzie $i \in \{1, 2, \dots, k\}$, czyli m/m_i i m_i są względnie pierwsze, zatem $(m/m_i)^{-1} \bmod m_i$ istnieje.

Oznaczmy $(m/m_i)^{-1} \bmod m_i$, czyli element odwrotny do (m/m_i) w \mathbb{Z}_{m_i} , jako c_i .

Niech

$$x = \left(\sum_{i=1}^k a_i c_i \frac{m}{m_i} \right) \bmod m$$

Zauważmy, że $(c \bmod ed) \bmod d = (c \bmod d)$ dla dowolnych $c, d, e \in \mathbb{Z}$. Dzięki temu mamy

$$x \bmod m_j = \left(\sum_{i=1}^k a_i c_i \frac{m}{m_i} \right) \bmod m_j$$

Wszystkie składniki w powyższym wyrażeniu za wyjątkiem składnika o $i = j$ przystają do zera

modulo m_j z powodu czynnika $\frac{m}{m_i}$, zatem suma redukuje się do

$$x \bmod m_j = \left(a_j c_j \frac{m}{m_j} \right) \bmod m_j = a_j \bmod m_j = a_j$$

Zatem $x \bmod m_j = a_j$ dla $j \in \{1, 2, \dots, k\}$, więc wskazaliśmy x spełniającego omawiany układ kongruencji \square

Dowód lematu 2

W lemacie (1) wykazaliśmy, że dla każdej krotki (a_1, a_2, \dots, a_k) istnieje odpowiedni x spełniający układ kongruencji z twierdzenia. Ponieważ a_i dla $i \in \{1, 2, \dots, k\}$ może przybierać wartości ze zbioru $\{0, 1, \dots, m_i - 1\}$, którego moc wynosi m_i , to różnych krotek jest w sumie $m_1 m_2 \dots m_k = m$. Ponieważ $0 \leq x < m$, to liczba różnych x jest równa liczbie krotek. Ponieważ każda krotka reprezentuje jakiś x oraz każdy x ma reprezentację w postaci pewnej krotki, to funkcja odwzorowująca krotki na x -y jest bijekcją, czyli, innymi słowy, x -y są wyznaczone jednoznacznie przez krotki. \square

Z prawdziwości lematu (1) i (2) natychmiast wynika prawdziwość twierdzenia. \square

Wniosek Pierścienie \mathbb{Z}_m oraz $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$ są izomorficzne. Izomorfizmem jest funkcja $f(x) = (x \bmod m_1, x \bmod m_2, \dots, x \bmod m_k)$.

2 Funkcja Eulera

Definicja $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n \mid \exists x^{-1}\} = \{x \in \mathbb{Z}_n \mid x \perp n\}$

Definicja funkcji Eulera $\varphi: \varphi(n) = |\mathbb{Z}_n^*|$

Niech $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ będzie rozkładem na czynniki pierwsze liczby n .

Obserwacja $p \in \mathbb{P} \Rightarrow \varphi(p) = p - 1$

Obserwacja Jeśli $p \in \mathbb{P}$, to dodatnich liczb naturalnych $\leq p^\alpha$ podzielnych przez p jest $p^{\alpha-1}$. Stąd $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$.

Fakt Jeśli $m_1 \perp m_2$, to $\varphi(m_1 m_2) = \varphi(m_1) \varphi(m_2)$.

Obserwacja Jeśli $m_1 \perp m_2$, to

$$x \perp m_1 m_2 \iff x \perp m_1 \wedge x \perp m_2 \iff \underbrace{(x \bmod m_1)}_{a_1} \perp m_1 \wedge \underbrace{(x \bmod m_2)}_{a_2} \perp m_2$$

oraz możliwych wartości a_1 jest $\varphi(m_1)$, a a_2 jest $\varphi(m_2)$.

Obserwacja $\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}) =$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

2.1 Twierdzenie Eulera

Jeśli $a \perp n$ to $a^{\varphi(n)} \equiv 1 \pmod{n} \iff n | a^{\varphi(n)} - 1$

Dowód

Ponieważ $d \perp c \wedge e \perp c \Rightarrow de \perp c$ to

$$\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} ax$$

Wynika to z tego, że prawy iloczyn ma $\varphi(n)$ czynników, wszystkie są $\perp n$ i są parami różne, bo jeśli by tak nie było, to pewne dwa czynniki z lewego iloczynu musiałyby być sobie równe, a tak nie jest. W związku z powyższym prawy iloczyn jest równy lewemu, jedynie czynniki są ustawione w innej kolejności. Stąd mamy

$$\begin{aligned} \left(\prod_{x \in \mathbb{Z}_n^*} x \right) \bmod n &= \left(\prod_{x \in \mathbb{Z}_n^*} ax \right) \bmod n = \left(a^{|\mathbb{Z}_n^*|} \cdot \prod_{x \in \mathbb{Z}_n^*} x \right) \bmod n \\ &\iff \\ 1 \bmod n &= a^{|\mathbb{Z}_n^*|} \bmod n \\ &\iff \\ 1 &\equiv a^{\varphi(n)} \pmod{n} \quad \square \end{aligned}$$

2.2 Małe twierdzenie Fermata

$$p \in \mathbb{P} \wedge (p \nmid a) \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

2.3 RSA

en.wikipedia.org/wiki/RSA

3 Zliczanie

Obserwacja Liczba ciągów a_1, a_2, \dots, a_k takich, że $a_i \in \{1, 2, \dots, n\}$ dla $i \in \{1, 2, \dots, k\}$ wynosi n^k .

Obserwacja Liczba ciągów a_1, a_2, \dots, a_k takich, że $a_i \in \{1, 2, \dots, n\} \wedge \forall_{i \neq j} a_i \neq a_j$ dla $i, j \in \{1, 2, \dots, k\}$ wynosi

$$n(n-1)(n-2) \dots (n-k+1) = n^{\underline{k}}$$

Zatem silnię możemy zdefiniować jako $n! = n^{\underline{n}}$

3.1 Symbol Newtona

Definicja $\binom{n}{k}$ (czytane „n nad k” lub „n po k”) jest to funkcja dwóch argumentów całkowitych nieujemnych, zdefiniowana jako:

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}, \quad \binom{n}{k} \neq 0 \iff 0 \leq k \leq n$$

Obserwacja Liczba k -elementowych podzbiorów zbioru n -elementowego wynosi

$$\frac{n^{\underline{k}}}{k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

Intuicja: k elementów ze zbioru n -elementowego możemy wybrać na n^k sposobów. Przy zliczaniu liczby zbiorów k -elementowych musimy utożsamić ze sobą wszystkie te wybory, które wybierają dokładnie te same elementy, ale w różnej kolejności. Różnych kolejności wyboru ustalonych k elementów jest $k!$ ^{||}.

Obserwacja

$$\binom{n}{k} = \binom{n}{n-k}$$

Intuicja: Wyborowi każdego k -elementowego zbioru w jednoznaczny sposób odpowiada wybór jego dopełnienia które ma $n-k$ elementów, a liczba zbiorów i ich dopełnień musi być taka sama.

Definicja Funkcją charakterystyczną podzbioru B zbioru A nazywamy ciąg zer i jedynek długości $n = |A|$ taki, że na k -tej pozycji w tym ciągu znajduje się 1 jeśli k -ty element zbioru A należy do B i 0 w przeciwnym przypadku.

Obserwacja Liczba wszystkich podzbiorów zbioru n -elementowego wynosi 2^n .

Intuicja: Każdy z elementów zbioru możemy wybrać lub nie, elementów jest n , więc mamy 2^n możliwości. Warto zauważyć, że w istocie zgadza się to z liczbą wszystkich funkcji charakterystycznych dla danego zbioru. Zauważmy jeszcze, że

$$2^n = \sum_{k=0}^n \binom{n}{k} = \sum_{k=-\infty}^{\infty} \binom{n}{k} = \sum_{k \in \mathbb{Z}} \binom{n}{k} = \sum_k \binom{n}{k}$$

Obserwacja n po k jest równe liczbie tych ciągów n -elementowych złożonych z zer i jedynek, które zawierają k jedynek.

Dowód Każdemu k -elementowemu podzbiorni n -elementowego zbioru odpowiada funkcja charakterystyczna, która jest n -elementowym ciągiem 0 i 1, który ma k jedynek. Ponieważ n po k to liczba takich zbiorów, więc to też liczba takich ciągów. \square

Definicja uogólnionego symbolu Newtona

$$\binom{n}{n_1, n_2, \dots, n_k} = \frac{n!}{n_1! n_2! \dots n_k!} \text{ gdzie } \sum_{i=1}^k n_i = n$$

Obserwacja Liczba ciągów n -elementowych zawierających n_1 elementów pierwszego typu, n_2 elementów drugiego typu itd. do n_k elementów k -tego typu wynosi $\binom{n}{n_1, n_2, \dots, n_k}$, przy czym dwa ciągi są rozróżnialne jeśli na chociaż jednej pozycji stoją w nich elementy o różnych typach.

Intuicja: Wszystkie elementy możemy ustawić w ciągu na $n!$ sposobów, musimy jednak utożsamić ze sobą te ciągi, które na pewnych ustalonych pozycjach mają elementy tego samego typu. Elementów k -tego typu w ciągu zawsze jest n_k , zatem musimy utożsamić ze sobą te ciągi, które „wybrały” elementy k -tego typu na ustalonych n_k pozycjach w różnych kolejnościach. Tych ciągów jest $n_k!$. Takie utożsamienia musimy wykonać dla wszystkich możliwych wartości k , stąd otrzymujemy wzór. Na koniec zwróćmy jeszcze uwagę, że

$$\binom{n}{k} = \binom{n}{k, n-k}$$

^{||}Mówiąc bardziej po ludzku: $\binom{n}{k}$ to liczba sposobów wyboru k serwerów z serwerowni z n komputerami.

3.2 Poker

en.wikipedia.org/wiki/Poker_probability

3.3 Wzór dwumienny Newtona

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \dots + \binom{n}{k}a^{n-k}b^k + \dots + \binom{n}{n}b^n$$

Powyższe wyrażenie nazywamy **wzorem dwumiennym Newtona**.

Dla przykładu, dla $n = 2$ mamy

$$(a+b)^2 = a^2 + 2ab + b^2$$

oraz dla $n = 3$ mamy

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Fakt

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$$

Warto odnotować, że trójkąt Pascala jest skonstruowany przy pomocy tej zależności. Poniżej przedstawimy trzy dowody prawdziwości powyższej równości.

Dowód przez przekształcenia

$$\begin{aligned} \binom{n-1}{k-1} + \binom{n-1}{k} &= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{(n-1-k)!k!} = \\ &= \frac{(n-1)!}{(n-k-1)!(k-1)!} \left(\frac{1}{n-k} + \frac{1}{k} \right) = \\ &= \frac{(n-1)!}{(n-k-1)!(k-1)!} \cdot \frac{k+n-k}{(n-k)k} = \\ &= \frac{n!}{(n-k)!k!} = \binom{n}{k} \quad \square \end{aligned}$$

Dowód algebraiczny

Mamy

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \dots + \binom{n}{k}x^k + \dots + \binom{n}{n}x^n = p(x)$$

oraz

$$\begin{aligned} (1+x)^n &= (1+x)^{n-1}(1+x) = (1+x)^{n-1} + x(1+x)^{n-1} = \\ &= \binom{n-1}{0} + \binom{n-1}{1}x + \dots + \binom{n-1}{k}x^k + \dots + \binom{n-1}{n-1}x^{n-1} + \\ &+ \binom{n-1}{0}x + \binom{n-1}{1}x^2 + \dots + \binom{n-1}{k-1}x^k + \dots + \binom{n-1}{n-1}x^n = q(x) \end{aligned}$$

Ponieważ wielomiany $p(x)$ oraz $q(x)$ są sobie równe, a wielomiany są równe wtedy gdy ich współczynniki są sobie równe, to z powyższych równości natychmiast wynika dowodzona własność.

□

Dowód kombinatoryczny

Stosujemy interpretację kombinatoryczną. $\binom{n}{k}$ oznacza liczbę k -elementowych podzbiorów zbioru n -elementowego. Rozważmy dowolny n -elementowy zbiór A zawierający pewien element x .

Liczba podzbiorów k -elementowych zbioru A nie zawierających x wynosi $\binom{n-1}{k}$, ponieważ założenie o nie należeniu x do podzbioru zmniejsza liczbę elementów do wyboru z n do $n-1$. Liczba podzbiorów k -elementowych zbioru A zawierających element x wynosi $\binom{n-1}{k-1}$ ponieważ założyliśmy, że wybraliśmy już jeden element, którym jest x , więc pozostaje nam $k-1$ elementów do wybrania z puli $n-1$ elementów. Ponieważ wszystkie k -elementowe podzbiory zbioru A albo zawierają x albo nie, to dowodzona zależność jest prawdziwa. \square

Kilka obserwacji

$$(a+b)^n = \sum_k \binom{n}{k} a^{n-k} b^k,$$

$$a=b=1 \Rightarrow (a+b)^n = 2^n = \sum_k \binom{n}{k},$$

$$a=1 \wedge b=-1 \Rightarrow (a+b)^n = (1-1)^n = \sum_k \binom{n}{k} (-1)^k = \begin{cases} 0 & n > 0, \\ 1 & n = 0 \end{cases},$$

$$\begin{aligned} \sum_{k=1}^n k \binom{n}{k} &= \sum_{k=1}^n k \frac{n!}{k!} = \\ &= \sum_{k=1}^n n \frac{(n-1)!}{(k-1)!} = \\ &= \sum_{k=1}^n n \binom{n-1}{k-1} = n \sum_{k=1}^n \binom{n-1}{k-1} = \\ &= n 2^{n-1}. \end{aligned}$$

V 3.XI.2008

1 Zasada szufladkowa Dirichleta

Jeśli rozdzielimy $n+1$ kulek do n szufladek (pojemników), to istnieje szufladka mająca więcej niż jedną kulkę. Ogólniej, jeśli rozdzielimy ponad kn obiektów do n pojemników, to istnieje pojemnik mający przydzielone więcej niż k obiektów. Właśnie sformułowaną zależność nazywamy zasadą szufladkową Dirichleta.

Przykłady zastosowań

1. **Twierdzenie** $a \perp n \wedge a, n \in \mathbb{N} \Rightarrow \exists_{x>0} a^x \equiv 1 \pmod{n} \iff n | a^x - 1$

Dowód Dowód przy pomocy zasady szufladkowej Dirichleta.

Niech szufladkami będą reszty modulo n . Szufladkami są liczby ze zbioru

$\{0, 1, 2, \dots, n-1\}$ i jest ich n . Kulkami niech będą potęgi liczby a : a^0, a^1, \dots, a^n .

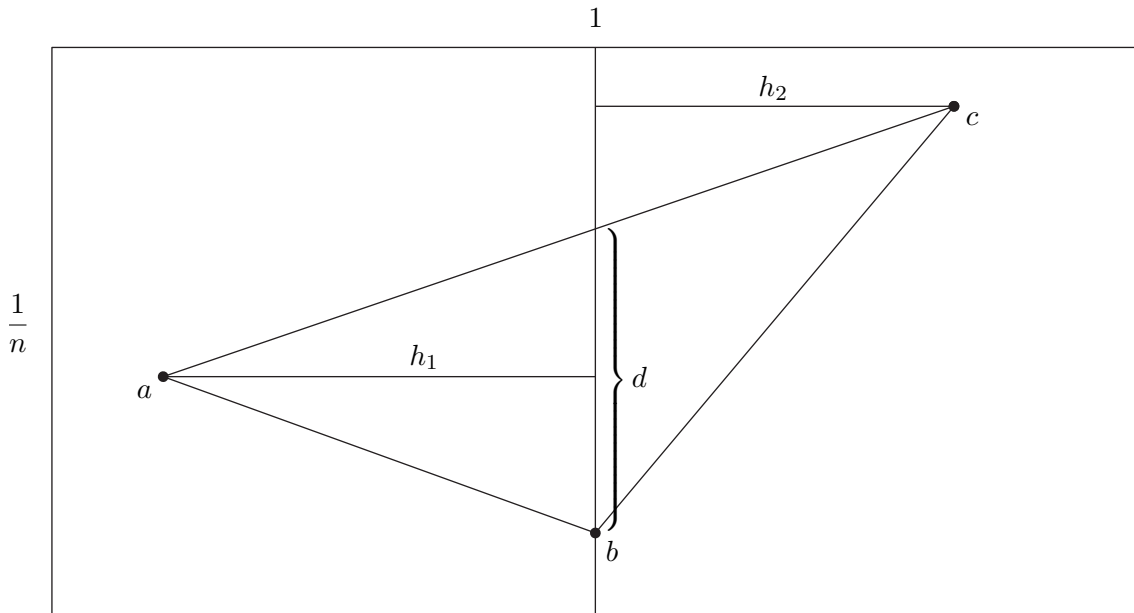
Ponieważ kulek jest więcej niż szufladek, to na mocy zasady szufladkowej Dirichleta dla pewnych i, j takich, że $i < j$, kulki a^i oraz a^j są w tej samej szufladce, czyli ich reszty modulo n są równe, czyli $a^i \equiv a^j \pmod{n} \iff a^i \equiv a^{j-i} a^i \pmod{n} \iff 1 \equiv a^{j-i} \pmod{n}$.
Zatem dla $x = j - i$ twierdzenie jest spełnione. \square

2. **Twierdzenie** Mamy dany kwadrat o boku 1, w którym znajduje się $2n+1$ punktów z których żadne 3 nie są współliniowe. Istnieją wtedy takie 3 punkty, które są wierzchołkami trójkąta o polu $\leq \frac{1}{2n}$.

Dowód Szufladkami niech będzie n prostokątów, które powstały po podzieleniu kwadratu prostymi równoległymi do jednej z par boków kwadratu i odległymi od siebie o $\frac{1}{n}$. Kulkami niech będzie $2n+1$ punktów znajdujących się uprzednio na kwadracie.

Zgodnie z zasadą szufladkową Dirichleta istnieje taki prostokąt, który zawiera przynajmniej 3 punkty. Oznaczmy boki o długości $\frac{1}{n}$ tego prostokąta jako jego podstawy. Oznaczmy dowolne 3 punkty w tym prostokącie jako a, b, c , przy czym minimum z odległości do obu podstaw jest największe dla punktu b . Jeśli teraz przeprowadzimy prostą równoległą do podstaw przechodzącą przez punkt b , to otrzymamy dwa trójkąty których suma pól jest równa polu trójkąta o wierzchołkach a, b, c (patrz rysunek). Jeśli pole trójkąta a, b, c oznaczmy jako P , pola trójkątów tworzących go jako P_1 i P_2 , ich wysokości odpowiednio h_1 i h_2 , a ich podstawę jako d , to otrzymamy:

$$P = P_1 + P_2 = \frac{1}{2}dh_1 + \frac{1}{2}dh_2 = \frac{1}{2}d(h_1 + h_2) \leq \frac{1}{2} \cdot \frac{1}{n} \cdot 1 = \frac{1}{2n} \quad \square$$



Rysunek 5. Niezwykły prostokąt

3. Jeśli weźmiemy dowolne naturalne n , to każda liczba rzeczywista α musi zawierać się pomiędzy liczbami p/n i $(p+1)/n$ dla pewnego całkowitego p . Stąd wynika, że odległość dowolnej liczby rzeczywistej do pewnego ułamka o mianowniku n (w tym wypadku ułamków o licznikach p i $p+1$) jest nie większa niż $1/(2n)$, co symbolicznie można zapisać:

$$\forall \alpha \in \mathbb{R}, n \in \mathbb{N} \exists p \in \mathbb{Z} \left| \alpha - \frac{p}{n} \right| \leq \frac{1}{2n}$$

Istnieją takie mianowniki, dla których maksymalna odległość wynosi nie $1/(2n)$, a $1/n^2$. Mówi o tym poniższe twierdzenie:

Twierdzenie $\forall \alpha \in \mathbb{R}, N \in \mathbb{N} \exists q \in [1, N], p \in \mathbb{Z} \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{Nq} \leq \frac{1}{q^2}$

Dowód Szufladkami niech będą przedziały postaci $\left[\frac{p}{N}, \frac{p+1}{N} \right)$ dla $p \in \{0, 1, \dots, N-1\}$.

Kulkami niech będą liczby ze zbioru $\{0, 1, \dots, N\}$.

Kulę i wrzucamy do szufladki w której znajduje się wartość $\{\alpha \cdot i\}$.

Z zasady szufladkowej Dirichleta wynika, że pewne kulki i, j ; $i < j$, wpadają do tej samej szufladki, a to oznacza, że obie wpadają do przedziału rozmiaru $1/N$ więc są o siebie

odległe o conajwyżej tyle. Stąd otrzymujemy:

$$\begin{aligned} & |\{\alpha \cdot j\} - \{\alpha \cdot i\}| \leq \frac{1}{N} \\ \Rightarrow & |\alpha \cdot j - \alpha \cdot i - (\lfloor \alpha \cdot j \rfloor - \lfloor \alpha \cdot i \rfloor)| \leq \frac{1}{N} \\ \Rightarrow & \left| \underbrace{\alpha(j-i)}_q - \underbrace{(\lfloor \alpha \cdot j \rfloor - \lfloor \alpha \cdot i \rfloor)}_p \right| \leq \frac{1}{N} \\ \Rightarrow & \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{Nq} \stackrel{q=j-i \leq N}{\leq} \frac{1}{q^2} \quad \square \end{aligned}$$

2 Elementy algebry

Definicje

Grupa $G = (X, \cdot)$ to algebra składająca się ze zbioru X i działania \cdot z następującymi własnościami:

1. Łączność: $(fg)h = f(gh)$
2. el. neutralny: $\exists_e \forall_g ge = eg = g$
3. el. odwrotny: $\forall_g \exists_{g^{-1}} gg^{-1} = g^{-1}g = e$

Grupa przemienna (abelowa) to grupa z dodatkową własnością: $\forall_{g,h} gh = hg$

Grupa cykliczna G to grupa postaci $G = \{e, g, g^2, \dots, g^{k-1}\}$ gdzie g to generator grupy i $g^k = e$.

Podgrupa H grupy G to grupa, której każdy element należy także do grupy G , która zawiera element neutralny i która jest zamknięta na działanie, czyli: $h, g \in H \Rightarrow h \cdot g \in H$

Warstwa lewostronna (względem H): $gH = \{gh : h \in H\}$

Warstwa prawostronna (względem H): $Hg = \{hg : h \in H\}$

gdzie odpowiednio hg i gh należą do pewnej grupy G , g jest pewnym ustalonym elementem G , a H jest pewną ustaloną podgrupą G .

2.1 Twierdzenie Lagrange'a

$$|G| = [G : H] \cdot |H|$$

gdzie $[G : H] = \{gH : g \in G\}$ = liczba rozłącznych warstw G względem podgrupy H .

Wniosek Warstwy grupy G względem podgrupy H tworzą podział grupy G na równoliczne zbiory.

Przykład zastosowania

Twierdzenie Eulera brzmi: Jeśli $a \perp n$, to $a^{\varphi(n)} \equiv 1 \pmod{n} \iff n | a^{\varphi(n)} - 1$
Przeprowadzimy teraz jego dowód przy użyciu tw. Lagrange'a.

Dowód Niech $G = \mathbb{Z}_n^*$, $H = \{1, a, a^2, \dots, a^{k-1}\}$, $a^k \stackrel{n}{\equiv} 1$
Wtedy $|G| = |\mathbb{Z}_n^*| = \varphi(n) = [G : H] \cdot |H| = l \cdot k$ dla pewnego l .
Stąd mamy $a^{\varphi(n)} = a^{kl} = (a^k)^l = 1 \quad \square$

Definicje

Orbita elementu $x \in X$ na którego działa grupa G , to $O_x = \{g(x) \mid g \in G\}$.

Stabilizator elementu $x \in X$ na którego działa grupa G , to $G_x = \{g \in G \mid g(x) = x\}$.

2.2 Uogólnione twierdzenie Lagrange'a

Jeśli grupa G działa na zbiór X , to dla dowolnego $x \in X$ zachodzi:

$$|G| = |O_x| \cdot |G_x|$$

Umówmy się, że „obrót przekształcający obiekt na samego siebie”, to taki obrót tego obiektu, po którego wykonaniu obszar przestrzeni który zajmuje obiekt nie zmienia się, przy czym nie chodzi o jego wielkość, tylko o konkretne punkty. Przykładowo, jeśli punkt o współrzędnych x, y nie należał do kwadratu, to po obrocie kwadratu dalej nie może do niego należeć. W praktyce oznacza to, że jeśli obracamy np. kwadrat, to po dokonaniu obrotu nie może on być „przechylony” w żaden sposób. Dodatkowo, mówimy, że dwa obroty obiektu są różne, jeśli istnieje taki punkt należący do obiektu, że po obrocie któraś z jego współrzędnych jest inna. Jeśli będziemy pytać się ile jest różnych obrotów obiektu przekształcających go na samego siebie, to mamy na myśli moc grupy takich obrotów.

Przykłady zastosowań

1. Ile jest różnych obrotów kwadratu przekształcających go na samego siebie?
Odpowiedź: cztery: obrót o 0 (czyli brak), 90, 180 i 270 stopni.

Problem Ile jest obrotów sześcianu przeprowadzających go na samego siebie?

Remedium Niech x będzie pewnym punktem rozważanego sześcianu leżącym dokładnie na środku jednych z jego ścian. Problem możemy przeformułować jako pytanie o moc grupy obrotów działających na x . Zgodnie z uogólnionym twierdzeniem Lagrange'a, wystarczy byśmy znali moc orbity i stabilizatora x względem działania na nim tą grupą. Orbitą x są te obroty, które powodują zmianę współrzędnych x . Jest ich 6: po dokonaniu odpowiednich obrotów x może znajdować się na środku którejkolwiek z 6 ścian sześcianu. Z kolei stabilizatory są 4: ścianę, na której leży x , możemy potraktować jako kwadrat. Wtedy, jak już wcześniej zauważyliśmy, są 4 obroty kwadratu przeprowadzających go na samego siebie, ale x jako środek kwadratu nie zmienia pozycji w żadnym z nich, stąd są one jego stabilizatorem. Zatem skoro $|O_x| = 6$ oraz $|G_x| = 4$ gdzie G to grupa obrotów, to na podstawie twierdzenia Lagrange'a mamy $|G| = |O_x| \cdot |G_x| = 6 \cdot 4 = 24$.

2. **Problem** Ile jest różnych sześciennych kostek do gry? Ile jest różnych prawidłowych kostek? Kostka prawidłowa to taka, której suma oczek na każdej z przeciwległych ścian wynosi 7.

Remedium Na nieruchomą kostkę możemy „nalepić” wartości od 1 do 6 na 6! sposobów. Z poprzedniego problemu wiemy jednak, że dowolną kostkę możemy za pomocą obrotów utożsamić z 24 różnymi nieruchomymi kostkami, zatem wszystkie nieruchome kostki powstałe poprzez nalepienie na nich wartości od 1 do 6 możemy rozbić na klasy abstrakcji w ten sposób, że do jednej klasy abstrakcji należą wszystkie te kostki, które w istocie są jedną kostką ale obróconą na 24 różne sposoby. Stąd liczba różnych kostek wynosi $6!/24 = 30$.

By wyznaczyć kostki prawidłowe rozumiemy tak samo, jedynie przy „nalepieniu” wartości nalepienie pewnej liczby od razu determinuje wartość na przeciwległej ścianie, stąd zamiast 6! mamy $6 \cdot 4 \cdot 2$, co w wyniku daje: $\frac{6 \cdot 4 \cdot 2}{24} = 2$.

Fakt Jeśli grupa G działa na zbiór X , to zbiór orbit jest podziałem zbioru X .
W szczególności orbity są parami rozłączne.

2.3 Lemat Burnside'a

Niech G będzie grupą działającą na zbiór X . Wtedy

$$\# \text{ orbit} = \frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)|$$

gdzie $|\text{fix}(g)| = \{x : g(x) = x\}$

$$\begin{aligned} \text{Dowód} \quad \# \text{ orbit} &\stackrel{\textcircled{1}}{=} \sum_{\text{orbita}} 1 \stackrel{\textcircled{2}}{=} \sum_{O_x \text{-orbita}} \frac{|O_x| \cdot |G_x|}{|G|} = \sum_{O \text{-orbita}} \sum_{x \in O} \frac{|G_x|}{|G|} \stackrel{\textcircled{3}}{=} \sum_{x \in X} \frac{|G_x|}{|G|} = \\ &= \frac{1}{|G|} \sum_{x \in X} |G_x| = \frac{1}{|G|} |\{(x, g) : g(x) = x\}| = \frac{1}{|G|} \sum_{g \in G} |\text{fix}(g)| \end{aligned}$$

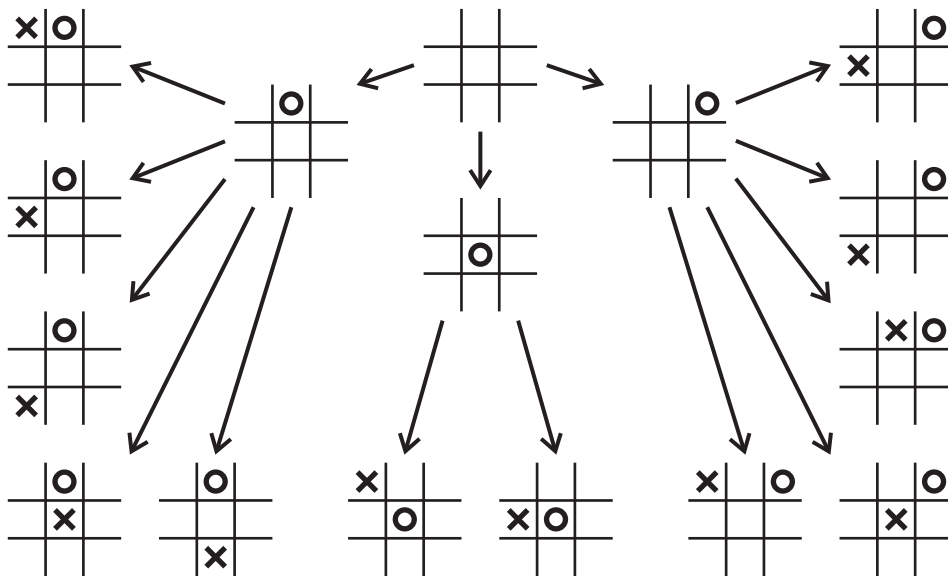
Równość ① to zliczenie orbit poprzez wskazanie ich bezpośrednio.

② wynika z uogólnionego twierdzenia Lagrange'a. x w O_x to dowolny x którego orbitą jest O_x .

③ wynika z faktu, że orbity tworzą podział zbioru X . \square

Przykład zastosowania

Chcemy opracować strategię gry w kółko i krzyżyk. W tym celu postanowiliśmy rozpisać drzewo wszystkich możliwości potoczenia się partii, aby następnie wydedukować w jakiej sytuacji wykonywać jaki ruch. Zanim zaczniemy rozpisywać drzewo, zauważamy jeszcze, że wszystkie rozłożenia kółek i krzyżyków które można otrzymać wzajemnie z siebie przez odbicia i obroty są w praktyce tą samą pozycją. Mając to na uwadze, rozpisujemy pierwsze 3 poziomy drzewa:



Rysunek 6. Początek drzewa rozgrywki w kółko i krzyżyk.

Zauważamy, że niestety drzewo zaczyna się dość pokaźnie rozrastać. Chcemy zobaczyć ile byśmy musieli rozpisać kolejnych pozycji, co nas prowadzi do sformułowania zdania.

Problem Ile jest istotnie różnych rozłożeń dwóch kółek i krzyżyka w grze w kółko i krzyżyk.

Remedium Problem rozwiązujemy przy pomocy teorii grup. Jako X traktujemy zbiór wszystkich różnych rozłożeń dwóch kółek i krzyżyka na planszy, przy czym dwa rozłożenia są różne jeśli różnią się zawartością conajmniej jednego pola. Jeśli weźmiemy dowolne dwa rozłożenia dwóch kółek i krzyżyka na planszy, takie, że nie możemy jednego otrzymać z drugiego przez obroty lub odbicia, to mówimy, że rozłożenia te są istotnie różne. Zauważmy teraz, że liczba istotnie różnych rozłożeń to liczba orbit powstałych poprzez działanie grupą G obrotów i odbić na zbiór X . Wynika to z tego, że jeśli pewne $x_1, x_2 \in X$ mają tę samą orbitę, to można otrzymać x_1 z x_2 przy pomocy działań z G i vice versa, więc x_1 i x_2 nie są istotnie różne. Niech $G = \{id, O_{90}, O_{180}, O_{270}, S_h, S_v, S_{d1}, S_{d2}\}$ gdzie elementy z G czytamy kolejno jako: Identyczność (brak obrotu), obrót o 90 stopni, o 180 stopni, o 270, odbicie względem prostej przechodzącej poziomo przez środek planszy, analogicznie dla prostej pionowej, odbicie względem przekątnej „\” i przekątnej „/”. Przy tak rozpoznanej strukturze możemy skorzystać z lematu Burnside’a by zauważyć, że wystarczy policzyć moc zbioru punktów stałych ($|fix(g)|$) dla każdej operacji $g \in G$, czyli tych ułożeń planszy, które dana operacja g przekształca na takie samo ułożenie. Tak więc liczymy:

$|fix(id)| = 252$: Jest to poprostu liczba wszystkich różnych rozłożeń na planszy. Liczymy ją tak: Kładziemy pierwsze kółko na jednym z 9 pól, drugie kółko na jednym z pozostałych 8 pól, krzyżyk na jednym z pozostałych 7 pól, i utożsamiamy ze sobą rozłożenia różniące się tylko kolejnością położenia kółek.

$|fix(O_{180})| = 4$: Są to rozłożenia które mają w centralnym polu krzyżyk i w których kółka leżą w tej samej linii, poziomej, pionowej, przekątnej lub drugiej przekątnej.

$|fix(O_{90})| = |fix(O_{270})| = 0$.

$|fix(S_h)| = |fix(S_v)| = 12$. Rozważmy odbicie w poziomie. Kółka mogą znajdować się w górnych rogach, w dolnych rogach, lub po bokach. Dla każdego takiego rozłożenia kółek mamy 3 różne pozycje krzyżyka, w dowolnym polu w środkowej kolumnie. Do tego możemy wszystkie 3 elementy położyć w środkowej kolumnie na 3 różne sposoby.

$|fix(S_{d1})| = |fix(S_{d2})| = 12$. Rozważmy przekątną „\”. Kółka mogą leżeć albo na polach przyległych do lewego górnego rogu, polach przyległych do prawego dolnego rogu, albo w lewym dolnym i prawym górnym rogu. Dla każdego z tych trzech rozłożeń krzyżyk może leżeć na którymś z trzech pól przez które przechodzi przekątna. Poza tym wszystkie 3 elementy możemy rozłożyć na 3 sposoby na polach przez które przechodzi przekątna.

Wreszcie z lematu Burnside’a wyliczamy liczbę orbit, czyli zarazem rozwiązanie problemu:

$$\# \text{ orbit} = \frac{1}{8}(252 + 4 + 4 \cdot 12) = 38 \quad \square$$

3 Zasada włączeń i wyłączeń

Obserwacja Gdy sumujemy moce dwóch zbiorów, to liczymy podwójnie elementy należące do obu tych zbiorów, zatem by prawidłowo obliczyć moc sumy dwóch zbiorów, musimy od niej odjąć moc ich przecięcia. Symbolicznie:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Obserwacja Jeśli zastosujemy takie samo rozumowanie jak powyżej dla mocy sumy trzech zbiorów, to w rezultacie końcowym nie policzymy elementów należących do wszystkich trzech

zbiorów. Po skorygowaniu tego błędu otrzymujemy:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

Zasada włączeń i wyłączeń

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= |A_1| + |A_2| + \dots + |A_n| - \\ &- |A_1 \cap A_2| - |A_1 \cap A_3| - \dots - |A_2 \cap A_3| - |A_2 \cap A_4| - \dots - |A_{n-1} \cap A_n| + \\ &+ |A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n| + \dots \pm |A_1 \cap A_2 \cap \dots \cap A_n| \end{aligned}$$

Opis słowny: Aby znaleźć liczbę elementów zbioru $A_1 \cup A_2 \cup \dots \cup A_n$, znajdź liczby elementów wszystkich możliwych przecięć zbiorów spośród $\{A_1, A_2, \dots, A_n\}$, dodaj do siebie wyniki uzyskane dla przecięć nieparzystej liczby zbiorów, a następnie odejmij wyniki uzyskane dla przecięć parzystej liczby zbiorów.

Obserwacja Jeśli Ω oznacza przestrzeń wszystkich elementów, a A^c dopełnienie zbioru A w przestrzeni Ω , to

$$|A_1^c \cap A_2^c \cap \dots \cap A_n^c| = |\Omega| - |A_1 \cup A_2 \cup \dots \cup A_n| \iff |A_1 \cup A_2 \cup \dots \cup A_n| = |\Omega| - |A_1^c \cap A_2^c \cap \dots \cap A_n^c|$$

Definicja Funkcję $\chi : \Omega \rightarrow \{0, 1\}$, definiujemy dla zbioru A w przestrzeni Ω w następujący sposób:

$$\chi_A(x) = \begin{cases} 0 & x \notin A \\ 1 & x \in A \end{cases}$$

Własności funkcji χ :

$$\chi_{A^c}(x) = 1 - \chi_A(x)$$

$$\chi_{A \cap B}(x) = \chi_A(x) \cdot \chi_B(x)$$

$$\sum_{x \in \Omega} \chi_A(x) = |A|$$

$$\begin{aligned} \chi_{A_1^c \cap A_2^c \cap \dots \cap A_n^c} &= \chi_{A_1^c} \cdot \chi_{A_2^c} \cdot \dots \cdot \chi_{A_n^c} = (1 - \chi_{A_1})(1 - \chi_{A_2}) \dots (1 - \chi_{A_n}) = \\ &= 1 + \sum_{k=1}^n \left((-1)^k \cdot \sum_{i_1 < i_2 < \dots < i_k} \chi_{A_{i_1}} \cdot \chi_{A_{i_2}} \cdot \dots \cdot \chi_{A_{i_k}} \right) \end{aligned}$$

Ostatnią z powyższych równości otrzymujemy po zauważeniu, że iloczyn $(1 - \chi_{A_1})(1 - \chi_{A_2}) \dots (1 - \chi_{A_n})$ możemy wymnożyć w następujący sposób:

Dla każdego nawiasu wybieramy który jego element (1 lub χ_A) ma się znaleźć w pewnym składniku sumy wynikowej. Przykładowo, dla jednego składnika możemy wybrać z każdego nawiasu 1, dla innego składnika możemy wybrać z pierwszych trzech nawiasów prawe elementy, czyli $\chi_{A_1}, \chi_{A_2}, \chi_{A_3}$, a z pozostałych wybrać jedynki. W ten sposób do sumy wynikowej trafią składniki postaci $\chi_{A_{j_1}} \cdot \chi_{A_{j_2}} \cdot \dots \cdot \chi_{A_{j_k}}$ dla $1 \leq k \leq n$ gdzie ciągi postaci j_1, j_2, \dots, j_k to wszystkie możliwe ciągi i_x z rosnącymi indeksami. Nawiasem mówiąc, wzór ten przypomina trochę wzór dwumianowy Newtona.

Dowód poprawności zasady włączeń i wyłączeń

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| &= |\Omega| - |A_1^c \cap A_2^c \cap \dots \cap A_n^c| = \\ &= |\Omega| - \sum_{x \in \Omega} \chi_{(A_1^c \cap A_2^c \cap \dots \cap A_n^c)}(x) = \end{aligned}$$

$$\begin{aligned} &= |\Omega| - \sum_{x \in \Omega} \left(1 + \sum_{k=1}^n \left((-1)^k \cdot \sum_{i_1 < i_2 < \dots < i_k} \chi_{A_{i_1}} \cdot \chi_{A_{i_2}} \cdot \dots \cdot \chi_{A_{i_k}}(x) \right) \right) = \\ &= |\Omega| - |\Omega| - \sum_{x \in \Omega} \sum_{k=1}^n \left((-1)^k \cdot \sum_{i_1 < i_2 < \dots < i_k} \chi_{A_{i_1}} \cdot \chi_{A_{i_2}} \cdot \dots \cdot \chi_{A_{i_k}}(x) \right) = \end{aligned}$$

$$\begin{aligned}
&= - \sum_{k=1}^n \left((-1)^k \cdot \sum_{i_1 < i_2 < \dots < i_k} \sum_{x \in \Omega} \chi_{A_{i_1}} \cdot \chi_{A_{i_2}} \cdot \dots \cdot \chi_{A_{i_k}}(x) \right) = \\
&= \sum_{k=1}^n \left((-1)^{k+1} \cdot \sum_{i_1 < i_2 < \dots < i_k} \sum_{x \in \Omega} \chi_{A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}}(x) \right) = \\
&= \sum_{k=1}^n \left((-1)^{k+1} \cdot \sum_{i_1 < i_2 < \dots < i_k} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| \right) \square
\end{aligned}$$