

MOT

Funkcje tworzące

Je surjekcja: $f: X \rightarrow Y$ gdzie $|X| = n, |Y| = m$

Odpowiedź: $m! \cdot \binom{n}{m}$

Je jest permutacją zbioru $\{1, 2, \dots, n\}$
zawierającą dokładnie k wzrostów?

Odpowiedź: $\langle \binom{n}{k} \rangle$ - liczba estera

$$\langle \binom{n}{k} \rangle = \begin{cases} 1 & \text{dla } k=0 \\ 0 & \text{dla } k \geq n \\ (n-k) \cdot \langle \binom{n-1}{k-1} \rangle \cdot \left(\frac{n-1}{k} \right) & \text{dla } k < n \end{cases}$$

Przyjmijmy więc, że $\langle \binom{0}{0} \rangle = 1$,

Wiederholte wortgruppen dawa
biornego.

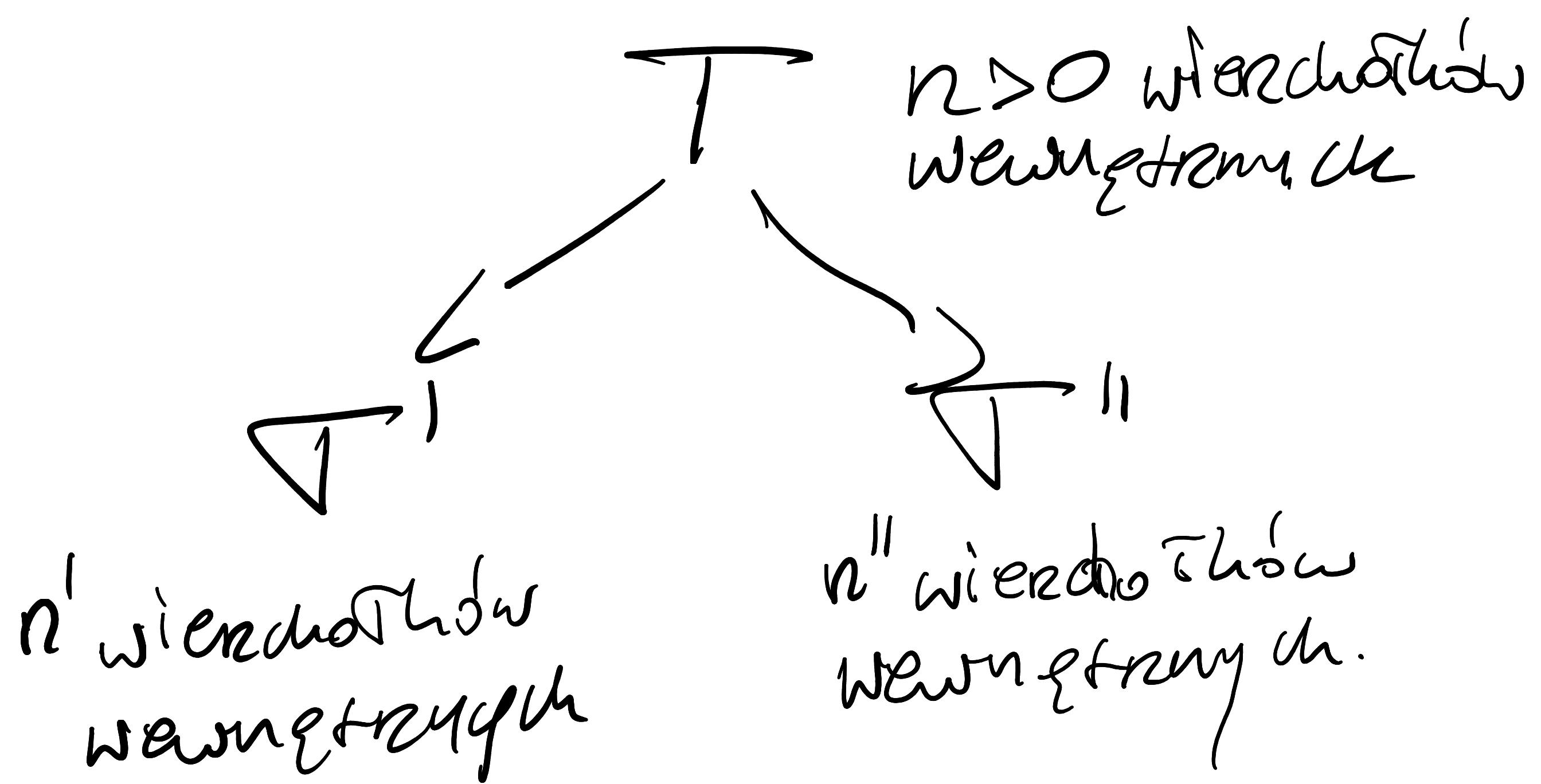
1. Dawa I nie ma wiederholiw
wortgruppen.
2. wiederholamie wortgruppen
dawa THAT so wszystkie
wiederholi wortgruppe dawa THAT
Oraz nowy wiederholi TOGZIEL
wszystkie dawa

Ille jest drew binarnej

które mały doładowanie a
wzorców licząc wzajemnych?

C_n - n-ta liczba Catalana

$$C_0 = 1$$



$$\frac{n' + n'' + 1 = n}{\text{czyli}}$$

$\langle n', n'' \rangle$ jest jednym z par liczb

$\langle 0, n-1 \rangle, \langle 1, n-2 \rangle, \dots, \langle n-2, 1 \rangle, \langle n-1, 0 \rangle$

w którym razie:

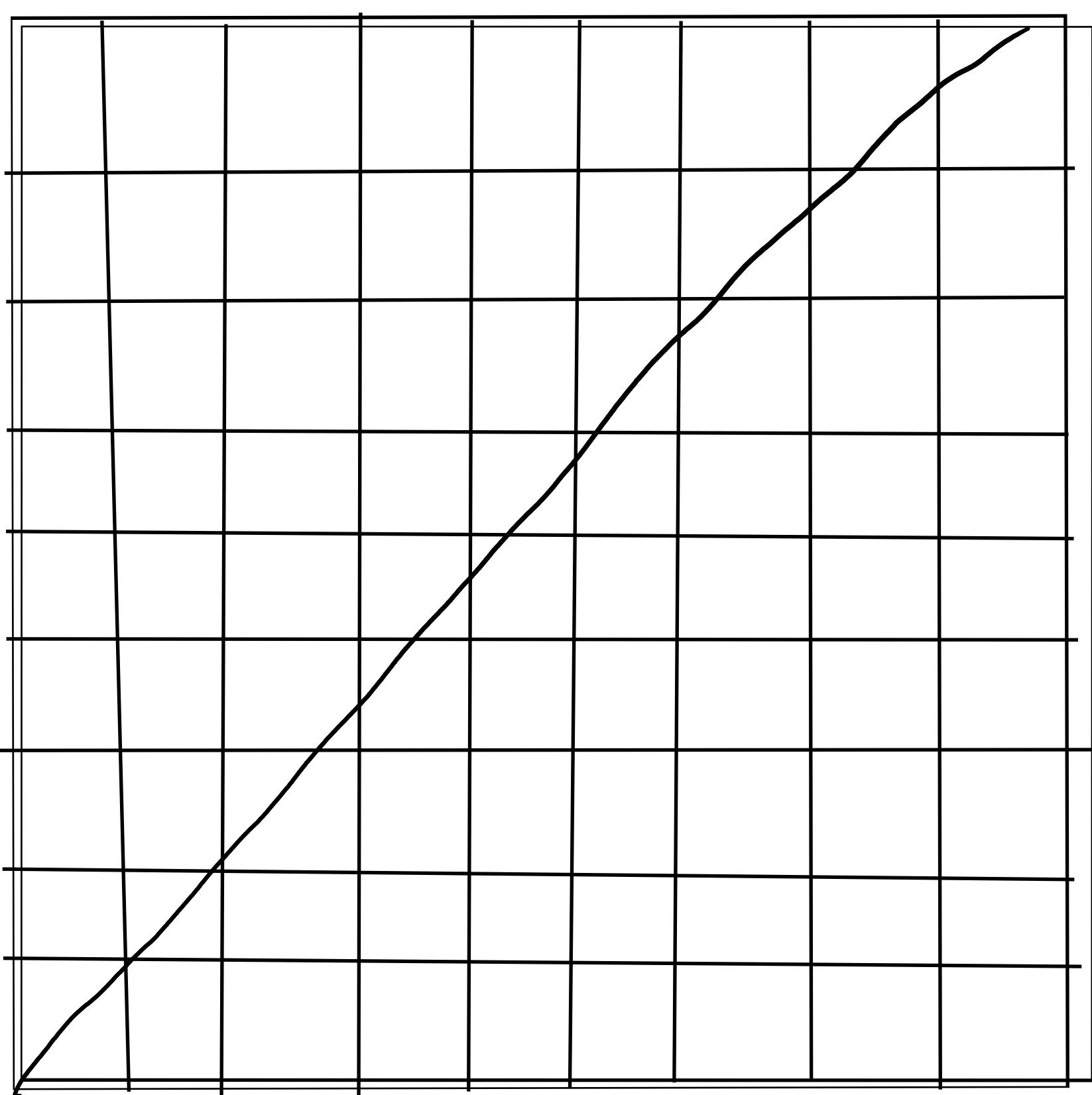
$$C_n = C_0 \cdot C_{n-1} + C_1 \cdot C_{n-2} + \dots + C_{n-1} \cdot C_0 = \\ = \sum_{k=0}^{n-1} C_k \cdot C_{n-k-1}$$

Własności liczb Catalan:

$$1. C_n = \frac{1}{n+1} \cdot \binom{2n}{n}$$

$$2. C_n = \binom{2n}{n} - \binom{2n}{n-1}$$

Wykresy
drogi po przekątnej



3. C_{n-1} - liczba sposobów rozmiieszczenia
nawiasów dla n argumentów dla funkcji
dwuargumentowej

Podzieta liczby

NEP na k składników jest to przedstawienie Worley'a w postaci

$$n = \alpha_1 + \alpha_2 + \dots + \alpha_k$$

czyli cyfra 1 \leq \alpha_1 \leq \alpha_2 \dots \leq \alpha_k

$P(n, k)$ - liczbą takiich podziałów

Właściwości:

$$1. P(n, 1) = 1$$

$$2. P(n, n) = 1$$

$$3. P(n, 2) = \lfloor \frac{n}{2} \rfloor$$

Oznaczenie Kenneth E. Iverson

$$[p] = \begin{cases} 1 & \text{jeśli } p \text{ jest zdaniem prawdziwym} \\ 0 & \text{jeśli } p \text{ jest zdaniem fałszywym} \end{cases}$$

$$[n \geq 3] \begin{cases} 1 \text{ dla } n \geq 5 \\ 0 \text{ dla } n = 1 \end{cases}$$

$$\left\lfloor \frac{n}{u} \right\rfloor = \left\lfloor \frac{n}{2u} \right\rfloor + \left\lfloor \frac{n+u}{2u} \right\rfloor$$

$$\Gamma \left\lfloor \frac{n}{u} \right\rfloor = \Gamma \left\lfloor \frac{n}{2u} \right\rfloor + \Gamma \left\lfloor \frac{n+u}{2u} \right\rfloor$$

Def. funkcja tworząca

$$A(z) = \sum_{i=0}^{\infty} a_i \cdot z^i$$

gdzie z to zmiennea zespoliona

zmiast ciągów analizy funkcjonalnej tworzące

Przykład:

$$(1+z)^n = \sum_{i=0}^n \binom{n}{i} \cdot z^i = \sum_{i=0}^n \binom{n}{i} \cdot z^i$$

Stąd: $A(z) = (1+z)^n$

jest funkcją tworzącą ciągu:

$$\left(\binom{0}{0}, \binom{1}{1}, \binom{n}{2}, \dots, \binom{n}{n}, 0, 0, 0, \dots \right)$$

Przykład:

Ciąg $(1, 1, 1, \dots)$

Funkcja tworząca: $A(z) = 1 + z + z^2 + z^3 + \dots = \frac{1}{1-z}$

Przykład:

Ciąg $(0, 0, \dots, 1, 0, 0, \dots)$

Funkcja tworząca $A(z) = \sum_{k=0}^{\infty} [k=n] \cdot z^n = z^n$

Pozycja:

$$c_{\alpha}g(\alpha^0, \alpha^1, \alpha^2, \alpha^3, \dots)$$

przejęta tworząca:

$$A(z) = a^0 + a^1 \cdot z^1 + a^2 \cdot z^2 + \dots = \frac{1}{1 - a \cdot z}$$

dla $a=1$ $A(z) = \frac{1}{1+z}$

Pozycja:

$$c_{\alpha}g(\alpha^0, 0, \dots, 0, \alpha^m, 0, 0, \dots, 0, \alpha^{2 \cdot m}, \dots)$$

$$A(z) = \sum_{k=0} \left[u|_k \right] \cdot \alpha^k \cdot z^k = 1 + (\alpha \cdot z)^m + (\alpha \cdot z)^{2 \cdot m} + \dots$$

$$= \frac{1}{1 - (\alpha \cdot z)^m}$$

$u|_k$ u jest dziedziczeniem,

u jest urozmaścigiem

Operacje na funkcjach tworzących

Należy $A(z) = \sum_{k=0}^{\infty} a_k \cdot z^k$

$B(z) = \sum_{k=0}^{\infty} b_k \cdot z^k$

Podstawimy:

$$A(z) + B(z) = \sum_{k=0}^{\infty} (a_k + b_k) \cdot z^k$$

Mnożenie przez skalar

$$\alpha \cdot A(z) = \sum_{k=0}^{\infty} \alpha \cdot a_k \cdot z^k$$

Mnożenie funkcji tworzących

$$A(z) \cdot B(z) = \sum_{n \geq 0} \underbrace{\sum_{k=0}^n a_{n-k} \cdot b_k}_{\text{spłot ciągów}} \cdot z^n$$

Ciąg złożony (cauchego ciągów)

Paralleler:

$$(1+z)^r \cdot (1+z)^s = (1+z)^{r+s} = \sum_{n \geq 0} \binom{r+s}{n} z^n$$

||

$$\sum_{n \geq 0} \sum_{u=0}^n \binom{r}{u} \cdot \binom{s}{n-u} \cdot z^n$$

stzqd:

$$\sum_{u=0}^n \binom{r}{u} \cdot \binom{s}{n-u} = \binom{r+s}{n}$$

To zeigen: $\binom{r+s}{n}$

Splot we ciągów $(a_i^1), (a_i^2), \dots, (a_i^m)$

jest to ciąg (s_i) o wyrazach

$$s_i = \sum_{k_1, k_2, \dots, k_m \in N} a_{i k_1}^{i_1} \cdot a_{i k_2}^{i_2} \cdot \dots \cdot a_{i k_m}^{i_m}$$

$$k_1 + k_2 + \dots + k_m = i$$

Jest w $A(z)$... Są funkcjami tworzącymi
to funkcja tworząca ma postać:

$$S(z) = \prod_{j=1}^m A_j(z)$$

Przestawiając wyrazów w miejscu

prawo $(a_0, a_1, a_2, \dots) \rightarrow (0, 0, 0, 0, a_1, a_2, \dots)$

$$B(z) = \sum_{k=0}^{\infty} a_k \cdot z^{m+k} = z^m \cdot \underbrace{\sum_{k=0}^{\infty} a_k \cdot z^k}_{\text{funkcja tworząca pierwotnego ciągu}} = z^m \cdot A(z)$$

funkcja tworząca
pierwotnego ciągu

Przesunięcie wyrazów w lewo

$$(a_0, a_1, a_2, \dots) \rightarrow (a_0, a_1, \dots, a_{m-1}, a_m, a_{m+1}, a_{m+2})$$

$$B(z) = \sum_{k \geq 0} a_{k+m} \cdot z^k = \sum_{n \in \mathbb{N}} a_n \cdot z^{n-m} =$$

$$z^m \cdot \sum_{n \in \mathbb{N}} a_n \cdot z^n = z^m \cdot \left(\sum_{n=0}^{\infty} a_n \cdot z^n - \sum_{k=0}^{m-1} a_k \cdot z^k \right) \dots$$

Funkcja tworząca szeregu

$$(a_0, a_1, a_2, \dots) \rightarrow (a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots)$$

splot dwóch ciągów $(1, 1, 1, \dots)$ (a_0, a_1, a_2, \dots)

Funkcje tworzące tych ciągów mają

postać: $\frac{1}{1-z}$, A(z)

Czyli funkcja tworząca szeregu to

$$\frac{1}{1-z} \cdot A(z)$$

Ciąg $(1, 2, 3, \dots)$ jest utworzony z ciągu

$(1, 1, 1)$ czyli funkcja tworząca tego

ciągu ma postać: $\frac{1}{1-z} \cdot \frac{1}{1-z} \cdot \frac{1}{(1-z)^2}$

Po przesunięciu w prawo otrzymujemy $\frac{1}{(1-z)^2}$

8. Szereg MacLaurina e^x ma postać

$e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$, tworzą ciąg $(\frac{1}{0!}, \frac{1}{1!}, \frac{1}{2!}, \dots)$

Wykładowcza funkcja tworząca: $A(z) = \sum_{i=0}^{\infty} \frac{a_i}{i!} \cdot z^i$

Czyli wykładowcza funkcja tworząca

ciągu $(1, 1, 1, \dots)$ jest równa e^x

Szereg Maclaurina funkcji $-ln(1-z)$
ma postać: $\sum_{n=1}^{\infty} \frac{1}{n} \cdot z^n$

Czyli $-ln(1-z) = \ln \frac{1}{1-z}$ tworzą

$(0, 1, \frac{1}{2}, \frac{1}{3}, \dots)$, stąd wynika, że
funkcje tworzące ciągów $(1, \frac{1}{2}, \frac{1}{3}, \dots)$
jest $\frac{1}{z} \cdot \ln\left(\frac{1}{1-z}\right)$

Przykład nr:

Wszystkie liczby harmoniczne $H_n = \sum_{i=1}^n \frac{1}{i}$ ($n \in \mathbb{N}$)
funkcja tworząca ma postać $\frac{1}{1-z} \cdot \ln \frac{1}{1-z}$

Rozszыrowanie funkcji tworzącej

$$A'(z) = \alpha_1 + 2\alpha_2 \cdot z + 3 \cdot \alpha_3 \cdot z^2 + \dots =$$

$$= \sum_{n=0}^{\infty} (n+1) \cdot \alpha_{n+1} \cdot z^n$$

Po pomnożeniu przez z

$$z \cdot A'(z) = \sum_{n=0}^{\infty} (n+1) \cdot \alpha_{n+1} \cdot z^{n+1} = \sum_{n=0}^{\infty} n \cdot \alpha_n \cdot z^n$$

Ciągły rozszыrowanie funkcji tworzącej

$$\int_0^z A(t) dt = \alpha_0 \cdot z + \frac{1}{2} \alpha_1 \cdot z^2 + \frac{1}{3} \cdot \alpha_2 \cdot z^3 + \dots =$$

Funkcja tworząca dla ciągu liczb
 Stirlinga $([n]_0, [n]_1, [n]_2, \dots)$
 ma postać zwarty $S_n(z) = z^n$

Funkcja tworząca dla ciągu liczb
 Stirlinga drugiego rodzaju:
 $(q^{nq}, q^{n+1}q, \dots)$ ma zwarty postać

$$S_n(z) = \frac{1}{(1-z) \cdot (1-2z) \cdots (1-nz)}$$

Twórcza Beta: $\frac{(e^z - 1)}{e}$

Funkcja tworząca dla liczb Catalan
ma postać zasady: $C(z) = \frac{1 - \sqrt{1 - 4z^2}}{2z}$

Niech $P_n = \sum_{k=1}^n P(n,k)$ oraz $A(z)$.

Widzmy, że $A_k(z) = \frac{1}{1 - z^k} = 1 + z^k + z^{2k} + \dots$

jest funkcją tworzącą ciągu

$(\underbrace{1, 0, \dots, 0}_{k \text{ mięs}}, 1, 0, \dots, 0, 1, 0 \dots)$

czyli ciągu $[k|0], [k|1], [k|2]$

Licza $[k|n]$ oznacza możliwość
podziału na n elementów.

$$\hat{A}(z) = \prod_{k=1}^{\infty} A_k(z) = \frac{1}{1-z} \cdot \frac{1}{1-z^2} \cdot \dots =$$
$$= \prod_{k=1}^{\infty} (1 + z^k + z^{2k} + \dots)$$

Przykładowe zastosowanie funkcji tworzących

Wtedy $j, a \in N$ oraz $x_1 + x_2 + \dots + x_n = j$

Wymagamy, aby $x_i \in X_j \subseteq N$ ($i = \overline{1, n}$)
ile jest rozwiązań?

Dla każdego $i = \overline{1, n}$ rozpatrujemy ciąg:

$$([0 \in X_i], [1 \in X_i], \dots)$$

którego funkcja tworząca ma postać:

$$f_i(z) = \sum_{r \geq 0} [r \in X_i] z^r$$

Zauważmy, że

$$\alpha_i^j = \sum_{\substack{k_1, k_2, \dots, k_n \in N \\ k_1 + k_2 + \dots + k_n = j}} [k_1 \in X_1] [k_2 \in X_2] \dots [k_n \in X_n]$$

W takim razie α_i^j jest liczbą rozwiązań.

Ale α_j jest splotem rozpatrywanych ciągów,

stąd:

$$A(z) = \prod_{i=1}^n F_i(z)$$

Przykład:

$$x_1 = \{1, 2\}, x_2 \in \{0, 1, 2\}, x_3 \in N$$

Mamy trzy ciągi (charakterystyczne):

$$i=1 (0, 1, 1, 0, 0, \dots) \quad F_1(z) = z + z^2$$

$$i=2 (1, 1, 1, 0, 0, \dots) \quad F_2(z) = 1 + z + z^2$$

$$i=3 (1, 1, 1, 1, 1, \dots) \quad F_3(z) = \frac{1}{1-z}$$

$$\text{Czyli } A(z) = F_1(z) F_2(z) F_3(z) =$$

$$= \frac{z \cdot (1+z) \cdot (1+z+z^2)}{1-z} = \frac{z}{1-z} + \frac{2 \cdot z^2}{1-z} + \frac{2 \cdot z^3}{1-z} + \frac{z^4}{1-z} =$$

$$= \sum_{n \geq 1} z^n + \sum_{n \geq 2} 2 \cdot z^n + \sum_{n \geq 3} 2 \cdot z^n + \sum_{n \geq 4} z^n = z + 3 \cdot z^2 + 5 \cdot z^3 + \sum_{n \geq 5} 6 \cdot z^n$$

Posechliwany ciąg ma postać:

$$(0, 1, 3, 5, 6, 6, \dots)$$

Zbiory z powtóreinianami

Def: Jest to funkcja

$f: X \rightarrow N$ przy czym $f(x) = k$.

Interpretując się, że $x \in X$ następuje w zbiorze z powtóreinianami k-krotnie.

Niech $X = \{x_1, x_2, x_3, \dots, x_n\}$ $f(x_i) = k_i$:

Def: Liczącą zbiór z powtóreinianami

f jest równa: $k_1 + k_2 + \dots + k_n$

Def: Podzbiór zbioru z powtóreinianami

f jest to zbiór z powtóreinianami:

$g: X \rightarrow N$, taki, że

$$\forall i = 1, n : g(x_i) \leq f(x_i)$$

Liczba wszystkich podzbiorów zbioru z powtóreinianami f wynosi więc:

$$(1+k_1) \cdot (1+k_2) \cdots (1+k_n)$$

Pozycja:

$X = \{a, b, c\}, f(a) = 2, f(b) = 3, f(c) = 1$

$\{ab, \{2*a, 3*b, c*c\}\}$

Liczność zbioru z powtórzeniami:

$$2 + 3 + 1 = 6$$

Ille jest k-elementowy dr podzbiorów zbioru z powtórzeniami?

Skazdy k-elementowy podzbiór zbioru z powtórzeniami:

$$Y = \{k_1 * x_1, k_2 * x_2, \dots, k_n * x_n\}$$

jednoznacznie jest wyznaczony poprzez rozwiązywanie równania di妄auycznego

w postaci: $y_1 + y_2 + \dots + y_n = k$

z ograniczeniami: $y_i \in \{0, 1, 2, \dots, c_i\}$ ($i = \overline{1, n}$)

liczba rozwiązań tego równania jest więc równa liczbie k-elementowych podzbiorów zbioru z powtórzeniami; Y.

W takim razie $X_i = \{q_1, 2, \dots, k_i\}$
a odpowiadająca funkcja jest mu równa:

$$F_i(z) = 1 + z + z^2 + \dots + z^{k_i}$$

Czyli funkcja tworząca poszukiwanego ciągu

Składa się z：

$$S(z) = \prod_{i=1}^n F_i(z)$$

Prykazad:

Nicch $X = \{2 * a, 3 * b, 1 * c\}$

Wtedy: $F_1(z) = 1 + z + z^2$

$$F_2(z) = 1 + z + z^2 + z^3$$

$$F_3(z) = 1 + z$$

Stąd: $S(z) = (1 + z + z^2) \cdot (1 + z + z^2 + z^3) \cdot (1 + z) =$

$$= 1 + 3 \cdot z + 5 \cdot z^2 + 6 \cdot z^3 + 5 \cdot z^4 + 3 \cdot z^5 + z^6$$

Rozwiązywanie równań rekurencyjnych

Postępowanie:

1. Napisać jednocześnie równanie, w którym an jest funkcją wczesniejszych elementów ciągu, aby zrozumieć, że $a_1 = 0$ dla $i < 0$.
2. Ponieźródź obie strony równania przez z^n zwiększać po n. Otrzymując po lewej stronie funkcję tworzącą $A(z)$
3. Prawą stronę równania posortować tak, aby stała się wyrażeniem zawierającym $A(z)$.
4. Otrzymane równanie rozwiązać względem $A(z)$.
5. Rozwiązać $A(z)$ w szeregu potęgowy. Współczynniki przy z^n jest poszukiwany w wyrazeniu an ciągu, określonym w postaci jawniej.

Przykład: ciąg Fibonacciego (f_n)

$$f_n = \begin{cases} 0 & \text{dla } n=0 \\ 1 & \text{dla } n=1 \\ f_{n-1} + f_{n-2} & \text{dla } n \geq 2 \end{cases}$$

1) $f_n = f_{n-1} + f_{n-2} + [n=1] \quad (n \in \mathbb{N})$

2) $\sum_{n \geq 0} f_n \cdot z^n = \sum_{n \geq 0} (f_{n-1} + f_{n-2} + [n=1]) \cdot z^n$
" $A(z)$

3) $P = \sum_{n \geq 0} f_{n-1} \cdot z^n + \sum_{n \geq 0} f_{n-2} \cdot z^n + \sum_{n \geq 0} [n=1] \cdot z^n =$

$$= z \cdot \sum_{n \geq 0} f_n \cdot z^n + z^2 \cdot \sum_{n \geq 0} f_n \cdot z^n + z =$$

$$= z \cdot A(z) + z^2 \cdot A(z) + z$$

4) $A(z) = z \cdot A(z) + z^2 \cdot A(z) + z \Rightarrow A(z) = \frac{z}{1-z-z^2}$

5) $(1-z-z^2) = (1-\alpha \cdot z)(1-\beta \cdot z)$

golice: $\alpha = \frac{1-\sqrt{5}}{2}, \beta = \frac{1+\sqrt{5}}{2}$

Otrzymujemy:

$$\begin{aligned} \frac{z}{1-z-z^2} &= \frac{z}{(1-\alpha \cdot z)(1-\beta \cdot z)} = \frac{1}{(\alpha-\beta)(1-\alpha \cdot z)} - \frac{1}{(\alpha-\beta)(1-\beta \cdot z)} = \\ &= \frac{1}{\alpha-\beta} \cdot \sum_{n \geq 0} \alpha^n \cdot z^n - \frac{1}{\alpha-\beta} \cdot \sum_{n \geq 0} \beta^n \cdot z^n = \sum_{n \geq 0} \frac{\alpha^n - \beta^n}{\alpha-\beta} \cdot z^n \end{aligned}$$

Stąd:

$$f_n = \frac{\alpha^n - \beta^n}{\alpha-\beta}$$

Podzielność liczb całkowitych

Def: Podzielanie modulo dla $x, y \in \mathbb{R}$ i $y \neq 0$

$$x \bmod y = x - y \cdot \left\lfloor \frac{x}{y} \right\rfloor$$

Poz这样才能写成 $x \bmod 0 = x$

Twierdzenie Algotrytm Dzielnicza:

Niech $m \in \mathbb{P}$ wtedy:

$$\forall n \in \mathbb{Z} \exists! \langle q, r \rangle \in \mathbb{Z}^2 : (n = m \cdot q + r \wedge 0 \leq r < m)$$

Relacja podzielności:

$$m | n \iff \exists k \in \mathbb{Z} : n = k \cdot m$$

Liczby m, n są względnie pierwsze, jeśli:

$$\text{NWD}(n, m) = 1$$

Algorytm Euklidesa

$$\begin{cases} \text{NWD}(0, n) = n \\ \text{NWD}(m, n) = \text{NWD}(n \bmod m, m) \end{cases}$$

Czas działania: $O(\log^2 n)$

Przykład: $\text{NWD}(1547, 560) = ?$

A	B		
1574	560	$560 = 0 \cdot 1547 + 560$	
560	1547	$1547 = 2 \cdot 560 + 427$	
427	560	$560 = 1 \cdot 427 + 133$	
133	427	$427 = 3 \cdot 133 + 28$	
28	133	$133 = 4 \cdot 28 + 21$	
21	28	$28 = 1 \cdot 21 + \neq$	
7	21	$21 = 3 \cdot 7 + 0$	
0	7	stop	
		$\text{NWD}(1547, 560) = 7$	

Algorytm Binarny na karcie

Prywat.

a	b	c	
84	112	1	
42	56	2	
21	28	4	- NWD jest podzielny przez 4
21	14		
7	F		
F	14		
F	F		- $NWD = b \cdot c = 4 \cdot 7 = 28$

Twierdzenie VI B 12

Niech $m, n \in \mathbb{Z}$

Istnieją $u, v \in \mathbb{Z}$ takie, że $\text{NWD}(m, n) =$

$$m \cdot u + v \cdot n$$

Przykład:

$$\text{NWD}(1547, 560) = 7$$

$$\begin{aligned} 1547 &= 2 \cdot 560 + 427 \\ &\vdots \\ 28 &= 4 \cdot 8 + 1 \end{aligned} \quad \begin{aligned} &= \dots \\ &= 28 - 1(133 - 4 \cdot 28) = \\ &= 28 - 1 \cdot 21 = \end{aligned}$$

$$\text{Czyli } 7 = 21 \cdot 1547 - 58 \cdot 560$$

Zasady funkcji algorytmu Euklidesa

$$\langle a, b \rangle := \langle m, n \rangle \neq \langle 0, 0 \rangle$$

$$\langle s, v \rangle := \langle 1, 0 \rangle$$

$$\langle t, v \rangle := \langle 0, 1 \rangle$$

do połaci $a \neq 0$ wykonyj

$$q := \left\lfloor \frac{b}{a} \right\rfloor$$

$$\langle a, b \rangle := \langle b \bmod a, a \rangle$$

$$\langle s, u \rangle := \langle v - q \cdot s, s \rangle$$

$$\langle t, v \rangle := \langle v - q \cdot t, t \rangle$$

$$\text{NWD}(a, n) := b$$

Gras obliczania algorytmu sie nie zanosi.

$$\text{NWD}(a, n) = u \cdot v + v \cdot r$$

$\exists^* k | m \wedge k | n \Leftrightarrow k | \text{NWD}(m, n)$, ponieważ
są względnie pierwsze

Podstawowe twierdzenie Arystotelesa

$\pi(n)$ liczba liczb pierwszych mniejszych od n .

$$\pi(n) - \frac{n}{\ln(n)} + \frac{n}{\ln^2(n)} + \dots = \sum_{i=1}^{\infty} \frac{(i-1)! \cdot n}{\ln^i(n)}$$

Rozwinięcie liniowe równania difantycznego
w zbiornie liczb całkowitych.

$\sum_{i=1}^n a_i \cdot x_i = b$ w zbiornie liczb całkowitych
istnieje iff $\text{NWD}(a_1, a_2, \dots, a_n) | b$

Twierdzenie: Jeżeli $x_0 \in \mathbb{Z}^n$ jest rozwiązaniem
powyższego równania, to zbiór wszystkich
rozwiązań jest równy:

$$\left\{ x_0 + y \in \mathbb{Z}^n : y = (y_1, y_2, \dots, y_n) \in \mathbb{Z}^n \wedge \right. \\ \left. \wedge \sum_{i=1}^n a_i \cdot y_i = 0 \right\}$$

Prywat!

$n=2$:

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 = k$$

Mieliśmy więc $\text{NWD}(\alpha_1, \alpha_2) = 1$

Algorytm Euklidesa:

$$\text{NWD}(\alpha_1, \alpha_2) = d = c_1 \cdot \alpha_1 + c_2 \cdot \alpha_2 \quad (c_1, c_2 \in \mathbb{Z})$$

Wtedy mamy: $x_1 = k \cdot c_1, x_2 = k \cdot c_2$

jest rozwiązanem.

Z tego, że $\alpha_1 \cdot y_1 + \alpha_2 \cdot y_2 = 0$

wynika ortogonalność wektorów:

$$\langle \alpha_1, \alpha_2 \rangle \text{ oraz } \langle y_1, y_2 \rangle$$

czyli $\langle y_1, y_2 \rangle = t \cdot \langle \alpha_1, \alpha_2 \rangle$

Stąd wynika, że każde z poszukiwanych rozwiązań ma postać:

$$x_1 = k \cdot c_1 + t \cdot \alpha_2 \quad \dots \quad ?$$

Prykaz:

$$z \cdot x + 5 \cdot y = 7$$

$$\text{NWD}(z, 5) = 1$$

$$1 = 2 \cdot 2 + 1 \cdot 5$$

$$\text{wieg } \langle x_0, y_0 \rangle = \langle -2 \cdot 7, 1 \cdot 7 \rangle = \langle -14, 7 \rangle$$

w falkowym rozszerzeniu:

$$\langle x, y \rangle = \langle -14 + 5 \cdot t, 7 - 2 \cdot t \rangle \quad (t \in \mathbb{Z})$$

Dla $n > 2$ stosujemy podstawnienie,

i bierzemy x_n jako stótkę.

$$\sum_{i=1}^{n-1} \alpha_i \cdot x_i - k \cdot a_n \cdot x_n$$

$$\text{NWD}(\alpha_1, \alpha_2, \dots, \alpha_n) \cdot y = k - \alpha_n \cdot x_n$$

Pryktad:

$$2 \cdot x + 4y + 5z = 7$$

Zerlegung: $2 \cdot x + 4y = 7 - 5z$

$$\text{NWD}(2, 4) = 2$$

$$7 - 5 \cdot z = 2 \cdot v$$

$$2 \cdot v + 5 \cdot z = 7$$

$$z = 7 - 2 \cdot t$$

$$2x + 4y = -28 + 10t$$

$$x + 2y = -14 + 5t$$

$$\text{NWD}(1, 2) = 1 = 1 \cdot 1 + 0 \cdot 2$$

$$\langle x, y \rangle = \langle -14 + 5t + 2s, -s \rangle (s, t \in \mathbb{Z})$$

$$\langle x, y, z \rangle = \langle -14 + 5t + 2s, -s, 7 - 2t \rangle (s, t \in \mathbb{Z})$$

KONGRUENCJE

$a, b, m \in \mathbb{R}; m \neq 0$

Relacja kongruencji (przystawiania) modulo m :

$a \equiv b \pmod{m} \Leftrightarrow a \bmod m = b \bmod m$
 a przystaje do b modulo m .

$a \equiv b \pmod{m} \Leftrightarrow m | (a - b)$

Własności:

1. Relacja równoważności
2. Klasami abstrakcji tej relacji są zbiory wszystkich liczb przystających do siebie.
3. W każdej klasie abstrakcji dla $m > 0$ występuje określone jedna liczba \bar{a} z przedziału $[0, m)$ czyli dla $a, b \in \mathbb{Z}$ liczba $\bar{a} \in \mathbb{Z}$ jest $\{0, 1, 2, \dots, m-1\}$

Prykład:

$$g = -16 \pmod{5}$$

ponieważ $g \pmod{5} = 4$

$$-16 \pmod{5} = 4$$

$$\text{tak } \varphi(g - (-16)) = 25$$

Masa abstrakcji dla liczby 9:

$$\|g\| = \{\dots, -21, -16, \dots, 9, 14, \dots\} = \|4\|$$

Blokując zakresy, że: $a, b \in \mathbb{Z} \wedge a \neq b$

Czasami ozywa się $a \equiv_m b$

$$5 \equiv 11 \pmod{3} \wedge 5 \equiv 11 \pmod{6} \text{ ale } 5 \not\equiv 11 \pmod{18}$$

Właściwości leagregacji są na kartce

Twierdzenie (Mata twierdzenia Fermata)

Niech p - liczba pierwsza oraz $\text{NWD}(n,p) = 1$,

wtedy: $n^{p-1} \equiv 1 \pmod{p}$

— bez uzywania 'Wazby Pierwszej'
 $n^p \equiv n \pmod{p}$

Uwiazek:

Jesli $\tau(p|\alpha)$ oraz $m \equiv n \pmod{p-1}$, to

$$\alpha^n \equiv \alpha^m \pmod{p}$$

Wielkie Twierdzenie Fermata:

$$a^n + b^n \neq c^n \text{ dla } a, b, c, n \in \mathbb{N} \wedge n > 2$$

Przyklad: Ostatnia cyfra rozwinięcia liczby

$2^{1000000}$ przy podstawie 7.

$$p=7$$

$$p-1=6$$

$$1000000 \pmod{6} = 4$$

$$1000000 = 4 \pmod{6}$$

$$0 \neq 2 \mid 4$$

$$2^{1000000} = 2^4 \pmod{7} \quad \text{Odp.: 2}$$

$$\text{ale } 2^4 = 16 \pmod{7} = 2$$

Rozwiązywanie congruencji w postaci:

$$m \cdot x = a \pmod{n}$$

zrozumieć: $\text{NWD}(m, n) = 1$

Rozpatruj najpierw uproszczanie:

$$m \cdot y = 1 \pmod{n}$$

$$\text{NWD}(m, n) = l = u \cdot m + v \cdot n$$

$$\text{czyli } u \cdot m = l \pmod{n}$$

$$a \cdot u \cdot m = a \pmod{n}$$

$$x = a \cdot u$$

inne rozwiązywanie:

$$x = a \cdot u + k \cdot n \quad \text{dla } k \in \mathbb{Z}$$

Integre congruencji jedno rozwiązywanie,
a więc istnieje nieskończonie wiele rozwiązań.

Przykład: $20 \cdot x = 3 \pmod{63}$

$$\text{NWD}(20, 63) = 1$$

zmodyfikowany algorytm euklidesa:

$$d = (-22) \cdot 20 + 7 \cdot 63$$

$y = -22$ jest rozwiążaniem uproszczonej $20 \cdot y = 1 \pmod{63}$

więc $x = 3 \cdot (-22) + k \cdot 63 = 60 + k \cdot 63$, $k \in \mathbb{Z}$

Założenie: $\text{NWD}(m, n) = d > 1$ ale

$$a = u \cdot d$$

wtedy $m = s \cdot d$ i $n = t \cdot d$, gdzie $s, t \in \mathbb{Z}$.

Czyli po podstawieniu:

$$s \cdot d \cdot x = u \cdot d \pmod{t \cdot d}$$

$$s \cdot x = u \pmod{t}$$

$$\text{NWD}(s, t) = 1$$

kongruencja $12 \cdot x = 20 \pmod{8}$

$$3x = 5 \pmod{2}$$

$1 + k \cdot 2$ dla $k \in \mathbb{Z}$

Wtedy: jeśli $\text{NWD}(m, n) = d > 1$ a

$$\exists k \in \mathbb{Z} : a = k \cdot d$$

$$m = s \cdot d \wedge n = t \cdot d, \text{ gdzie } s, t \in \mathbb{Z}.$$

$$s \cdot d \cdot x = a \pmod{t \cdot d}$$

Nie ma rozwiązań, gdyż

$s \cdot d \cdot x = a$, nie dzieli się przez d .

Rozwiązywanie układu kongruencji w postaci:

$$\begin{cases} x = \alpha_1 \pmod{n_1} \\ x = \alpha_2 \pmod{n_2} \end{cases} \quad \text{z warunkiem } \text{NWD}(n_1, n_2) = 1$$

Rozwiązywanie pierwszej kongruencji:

$$x = \alpha_1 + y \cdot n_1 \quad \text{gdzie } y \in \mathbb{Z}$$

Po podstawieniu do drugiej kongruencji:

$$\alpha_1 + n_1 \cdot y = \alpha_2 \pmod{n_2} \Rightarrow$$

$n_1 \cdot y = (\alpha_2 - \alpha_1) \pmod{n_2}$ – użycie reszt kongruencji
Rozwiązywanie należy podstawić do wielu rozwiązań.

Przykład:

$$\begin{cases} x = 1 \pmod{20} \\ x = 4 \pmod{63} \end{cases} \quad \text{NWD}(20, 63) = 1$$

$$x = 1 + y \cdot 20, \quad \text{gdzie } y \in \mathbb{Z}$$

$$4y \cdot 20 = 4 \pmod{63} \Rightarrow 20 \cdot y = 3 \pmod{63} \Rightarrow$$

$$\Rightarrow y = 60 + k \cdot 63$$

$$x = 1 + y \cdot 20 = 1 + (60 + k \cdot 63) \cdot 20 = 1201 + k \cdot 1260$$

Twierdzenie Chia'shie o Resztach:

Dany jest układ congruencji:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_1} \\ \vdots \\ x \equiv a_r \pmod{n_1} \end{cases} \quad \text{Niech } i \neq j \Rightarrow \text{NWD}(n_i, n_j) = 1$$

$\forall N \in \mathbb{Z} \exists! x \in \mathbb{Z}: (x \text{ jest rozwijaniem congruencji} \wedge$
 $\wedge N \leq x < \sum_{i=1}^r n_i + N)$

Dowód:

Istnieje:

$$\text{Niech } M = \prod_{i=1}^r n_i;$$

Zbiór $A = \{N, N+1, \dots, N+M-1\}$ zawiera M elementów.

Zbiór wszystkich wartości $x \pmod{n_i}$ zawiera n_i elementów, więc na podstawie prawa mnożenia istnieje dokładnie:

$M = \prod_{i=1}^r n_i =$ skończony ciąg reszt
 $(x \pmod{n_1}, \dots)$

W feliku razine Gilding'a f 260oru A na
 26idr clegoù rest istuire, tala ze
 $f(x) = (x \bmod n_1, x \bmod n_2 \dots)$
 W ebiione clegoù rest istuire element röwaj.
 $(\alpha_1 \bmod n_1, \alpha_2 \bmod n_2 \dots)$
 Nteen efasianiaid gogj uo Cefelid, 'ntec
 element 260oru A bgrafic röwaj x)
 Wtedy $\alpha_i \bmod n_i = x \bmod n_i$ czyli
 $x = \alpha_i (\bmod n_i)$ dla $i \in \overline{1, r}$

Sledmuznacis:

Nicete $x, x'' \in A$ ($x' + x''$) wtedy bieg
 sdeugui rowiżżej x: aix. 168adu kongruencii.

Prykład:

Od 2 do 13 tys.

$$\begin{array}{l} \text{na } 20 \text{ reszty: } 1 \\ \text{na } 63 \quad -11- \quad 4 \\ \text{na } 11 \quad -11- : 8 \end{array} \left. \begin{array}{l} x = 1 \pmod{20} \\ x = 4 \pmod{63} \\ x = 8 \pmod{11} \end{array} \right\} \Rightarrow$$

$$2000 \leq x \leq 13000$$

$$\text{NWD}(20, 63) = \text{NWD}(20, 11) = \text{NWD}(63, 11) = 1$$

$$20 \cdot 63 \cdot 11 = 13.860 > 13000 - \text{trygonometria}$$

Na podstawie twierdzenia istnieje rozwiązań dla:

$$2000 \leq x \leq 13.860 + 2000 = 15.860$$

Z poprzedniego: Czywiście z dwóch pierwszych to

$$x = 1201 + k \cdot 1260, \text{ podstawiając do 3:}$$

$$1201 + k \cdot 1260 = 8 \pmod{11} \Rightarrow$$

$$k \cdot 1260 = -1193 \pmod{11} \Rightarrow k \cdot 1260 = 6 \pmod{11}$$

$$k = 1 + r \cdot 11$$

$$210:11=1 \quad \text{dla } r=0$$

$$\text{Po podst: } x = 1201 + k \cdot 1260 = 1201 + (1+r \cdot 11) \cdot 1260 = 2461 + r \cdot 13860$$

Funkcja Eulera:

$\varphi: \mathbb{P} \rightarrow \mathbb{N}$ gdzie $\varphi(n) = \left\{ m \in \overline{1, n-1} : \text{NWD}(m, n) = 1 \right\}$
czyli jest to liczba wszystkich liczb względnie
 pierwszych z n i mniejszych od n.

Właściwości:

1. Jeśli p - liczba pierwsza to

a) $\varphi(p) = p - 1$

b) $\varphi(p^n) = p^a - p^{a-1}$ dla $a \in \mathbb{P}$

2. Jeśli $\text{NWD}(m, n) = 1$ dla $m, n \in \mathbb{P}$ to

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Twierdzenie Eulera (RSA)
(względnie małego Twierdzenia Fermata)

Wówczas $a^n \in P$ oraz $\text{NWD}(a, n) = 1$

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

Przykład: $13^{16101} \pmod{16} = ?$

$$\text{NWD}(13, 16) = 1 \quad | \quad 13^8 \equiv 1 \pmod{16}$$

$$\varphi(16) = 8 \quad | \quad \text{z 4. Kongruencją:}$$

$$(liczby nieparzyste < 16) \quad 13^{16098} \equiv 1 \pmod{16}$$

$$13^2 \equiv 169 \equiv 9 \pmod{16}$$

$$13^4 \equiv 13^2 \cdot 13^2 \equiv 9 \cdot 9 \pmod{16} \Rightarrow 13^4 \equiv 1 \pmod{16}$$

$$13^5 \equiv 13 \pmod{16} \Rightarrow 13^{16101} \pmod{16} = 13$$