Faktoryzacja liczb całkowitych - część teoretyczna

Krzysztof Zdulski, Kazimierz Kochan, Monika Lewandowska

10 stycznia 2020

Spis treści

1 Dowód 1 - Twierdzenie o dzieleniu z resztą

Pokazać, że dla dowolnych liczb całkowitych a i b różnych od 0 istnieją jednoznacznie wyznaczone liczby całkowite q i r takie, że
$a = q * b + r,\ 0 \leq r < |b|$

1.1 Dowód istnienia liczb q i r

$a = q * b + r$, $0 \leq r < |b|$
q- iloraz całkowity
r- reszta z dzielenia

Załóżmy, że $b > 0$

- $q = [\frac{a}{b}] \wedge r = a - b * q$
- $q \ \leq \frac{a}{b} < q + 1 \mid *b$
- $b * q \ \leq a < b * q + b$
- Z tego wynika, że $0 \leq [r = a - b * q] < b = |b|$

Gdy $b < 0$

- $q = -[\frac{a}{|b|}] \wedge r = a - b * q$

i dalej analogicznie jak w przypadku $b > 0$

1.2 Dowód, jednoznaczności wyboru pary liczb q i r

- Załóżmy, że istnieją liczby całkowite q_1, q_2, r_1 i r_2 takie, że
  $0 \leq \ r_1, r_2 < |b| \wedge a = q_1 * b + r_1 = q_2 * b + r_2$
- $r_2 - r_1 = b * (q_2 - q_1)$
- Gdyby $r_2 - r_1 \neq 0$ to $|b| < |r_2 - r_1| \leq max\{r_1, r_2\} < |b|$,co prowadzi do sprzeczności
- Więc $r_2 - r_1 = 0$, czyli $r_1 = r_2$
- Stąd $(q_2 - q_1) * b = 0$, zatem $(q_2 - q_1) = 0$, więc $q_1 = q_2$, bo $b \neq 0$

Co potwierdza jednoznaczność wyboru pary liczb q i r.

2 Dowód 2 - $NWD(a,b) = ax + by$

Pokazać, że istnieją liczby całkowite x i y takie, że $NWD(a,b) = a*x+b*y$, gdzie $a, b \in \mathbb{Z}$, z których conajmniej jedna jest różna od 0

- Gdy $a = 0 = b$ to $0 = a*0+b*0$ jest NWD(a,b), załóżmy więc, że a lub b jest różne od 0
- Niech $I = \{\ k*a+l*b \wedge$ k,l $\in \mathbb{Z} \cap\ N_+\}$
- Ponieważ $|a| = sign(a)*a+0*b \wedge\ \ |b| = 0*b+sign(b)*b$
  Zatem I nie jest zbiorem pustym
- Niech $d = min\{I\} \wedge$ k,l $\in \mathbb{Z}\ \ \wedge\ \ d = k*a+l*b$
- Należy pokazać, że $d = NWD(a,b)$; wiadomo, że $d \geq 0$
- Dla c $\in \mathbb{Z}\ \ ,\ \ c|a \wedge\ c|b \implies c|d$
- Należy udowodnić, że $d|a \wedge\ d|b$
- Liczbę a można zapisać w postaci: $a = q_{ad}*d\ + r_{ad}$ (dowód nr. 1)
- Zatem $r_{ad} = a - q_{ad}*d = a - q_{ad}*(k*a+l*b) = a - q_{ad}*k*a - q_{ad}*l*b = a*(1-k*q_{ad}) - q_{ad}*l*b$
- $r_{ad} < d$, więc $r_{ad} \notin I$, bo $d = min\{I\}$
- $r_{ad} \geq 0$, więc z def. zbioru I można wnioskować, że $r_{ad} = 0$
- Zatem d|a i analogicznie d|b, więc d=NWD(a,b)

3 Dowód 3 - $NWD(a,b) = 1$, $a|c \wedge b|c \implies ab|c$

Pokazać, że jeżeli liczby a i b są względnie pierwsze, to $a|c \wedge b|c \implies ab|c$, gdzie $a, b, c \in \mathbb{Z}$

- Z definicji zbioru liczb względnie pierwszych wynika, że NWD(a,b)=1, gdy a i b są różne
- Skoro NWD(a,b)=1 wiemy, że (Dowód 2) istnieje taki x,y, że

  $a * x + b * y = 1$
- Zatem $a * c * x + b * c * y = c$
- Z założenia b|c, więc ab|ac
- Analogicznie, gdy a|c to ab|bc
- Skoro ab dzieli całkowicie zarówno ac jak i bc to dzieli również wyrażenie $a * c * x + b * c * y = c$
- Rozpatrując przypadek dla dowolnej liczby całkowitej m takiej, że $c = m * a$ wiemy, że b|ma oraz NWD(b,a)=1 to prowadzi do stwierdzenia, że b|m
- Dla dowolnej liczby całkowitej n takiej, że $m = b * n$

  $c = a * m = a * b * n$, a zatem $ab|c$

4 Dowód 4 - $p|ab \implies p|a \vee p|b$

Pokazać, że gdy a,b $\in \mathbb{Z} \wedge$ p jest liczbą pierwszą $p|ab \implies p|a \vee p|b$

- Załóżmy, że $p|ab$, ale $p \nmid a \wedge p \nmid b$
- Więc $NWD(p, a) = 1$ i $NWD(p, b) = 1$ (są to pary liczb względnie pierwszych)
- Można zatem zapisać, że

  $x_1 * p + y_1 * a = 1$

  $x_2 * p + y_2 * b = 1$

  Co wynika z dowodu nr 2
- Mnożymy obustronnie równania i otrzymujemy:

  $x_1 * p * x_2 * p + x_1 * p * y_2 * b + y_1 * a * x_2 * p + y_1 * a * y_2 * b = 1$

  po przekształceniu

  $p * (x_1 * x_2 * p + x_1 * y_2 * b + y_1 * a * x_2) + a * b(y_1 * y_2) = 1$
- Z tego wynika, że $NWD(p, ab)$=1, co prowadzi do sprzeczności z założeniem, że p|ab
- Zatem, aby założenie p|ab było prawdziwe to p|a $\vee$ p|b

5 Dowód 5 - Każda liczba naturalna n daje się przedstawić jako skończony iloczyn samych liczb pierwszych dla $n \geq 2$

Pokazać, że każdą liczbę całkowitą $n \geq 2$ można jednoznacznie przedstawić w postaci $n = p_1^{a1} * p_2^{a2} * ...p_k^{a_k}$, gdzie $p_1, p_2, ..., p_k$ są liczbami pierwszymi, $p_1 < p_2 < ... < p_k$ oraz $a_1, a_2..., a_k \in \mathbb{N}$

Inaczej: Każda liczba naturalna daje się przedstawić jako skończony iloczyn samych liczb pierwszych.

Indukcyjnie

Sprawdzam założenie indukcyjne dla n=2 twierdzenie jest prawdziwe, bo $n = 2^1$

Dla dowolnego m należącego do zbioru liczb naturalnych i m>2 niech twierdzenie będzie prawdziwe dla wszystkich n, $1 < n < m$

Jeśli m jest liczbą pierwszą to twierdzenie zachodzi, ponieważ liczba pierwsza ma jedynie dzielnik, który jest liczbą pierwszą.

Gdy liczba m jest złożona, to m można zapisać w postaci $m = m_1 * m_2$, więc gdy $1 < m_1, m_2 < m$ to na mocy założenia indukcyjnego każde z m_1 i m_2 jest skończonym iloczynem liczb pierwszych. Stąd wynika, że m też jest takim iloczynem.