

SZKOŁA PODSTAWOWA HELIANTUS
02-892 WARSZAWA
ul. BAŻANCIA 16

Liczba 2, to jest jedyna najmniejsza liczba parzysta i pierwsza



Oś liczbowa. Liczba 1, to nie jest liczba pierwsza

**MATEMATYKA
W SZKOLE HELIANTUS
LICZBY PIERWSZE. ALGORYTM EUKLIDESA**

Prof. dr. Tadeusz STYŚ

Warszawa 2018¹

¹Projekt trzeci

Contents

1	Liczby pierwsze. Algorytm Euklidesa	5
1.1	Wstęp	5
1.2	Liczby pierwsze	5
1.3	Sposób rozkładu liczb na czynniki pierwsze	6
1.4	Największy wspólny dzielnik	7
1.5	Algorytm Euklidesa (325-265 B.C.)	9
1.6	Najmniejsza wspólna wielokrotna	11
1.7	Ćwiczenia	12

Chapter 1

Liczby pierwsze. Algorytm Euklidesa

1.1 Wstęp

Rozdział ten jest opracowany dla rozszerzonego programu matematyki w Szkole Podstawowej Heliantus i dotyczy arytmetyki liczb naturalnych i własności liczb pierwszych.

Nieskończony zbiór liczb pierwszych jest bardzo oryginalny i ważny w teorii liczb i w zastosowaniach matematyki i informatyki.

Jednym z najważniejszych zastosowań jest rozkład dowolnej liczby naturalnej na czynniki liczb pierwszych. Rozkład liczb na czynniki pierwsze podajemy w formie fundamentalnego twierdzenia arytmetyki.

Bezpośrednią konsekwencją rozkładu liczb naturalnych na czynniki pierwsze jest wyznaczanie największego wspólnego dzielnika i najmniejszej wspólnej wielokrotnej dwóch liczb naturalnych. Opis wyznaczania najmniejszego wspólnego dzielnika przez rozkład na czynniki i Algorytm Euklidesa wsparty jest licznymi przykładami.

1.2 Liczby pierwsze

Opis liczb pierwszych należy zacząć od definicji

Definicja 1.1 *Liczbę naturalną $p > 1$ nazywamy liczbą pierwszą, jeżeli ma dokładnie dwa dzielniki, to jest liczbę 1 i samą siebie p . To znaczy że liczby pierwsze dzielą się tylko przez liczbę 1 i przez siebie samą. Każda inna liczba nazywa się liczbą złożoną.*

Zauważmy, że liczba naturalna $p = 1$ nie jest liczbą pierwszą, gdyż ma tylko jeden dzielnik samą siebie i nie jest większa od 1. Liczba 0 również nie jest pierwsza bo jest mniejsza od 1 i ma więcej dzielników niż dwa, gdyż podzielona przez dowolną liczbę naturalną daje wynik 0. Wymieńmy kilka kolejnych liczb pierwszych

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 51, 53, 57...;

Z definicji wynika w sposób oczywisty, że liczba $p = 2$ jest jedyną liczbą pierwszą parzystą.

Zbiór liczb pierwszych nie jest zamknięty na operacje arytmetyczne. Wystarczy podać kontr-przykład.

Przykład 1.1 *Mianowicie liczby $n = 7$ i $m = 3$ są pierwsze jednak ich suma $n + m = 7 + 3 = 10$ nie jest liczbą pierwszą i różnica $7 - 3 = 4$ też nie jest liczbą pierwszą. Podobnie iloczyn tych liczb $n * m = 7 * 3 = 21$ nie jest liczbą pierwszą.*

Jedna z najważniejszych własności liczb pierwszych opisana jest w następującym twierdzeniu:

Twierdzenie 1.1 Fundamentalne Twierdzenie Arytmetyki. *Każdą liczbę naturalną można przedstawić jako iloczyn liczb pierwszych. Taki rozkład jest jedyny.*

Inaczej, jeżeli n jest liczbą naturalną to istnieją liczby pierwsze

$$p_1, p_2, p_3 \cdots, p_k$$

takie, że

$$n = p_1 * p_2 * p_3 * \cdots * p_k$$

1.3 Sposób rozkładu liczb na czynniki pierwsze

Z fundamentalnego twierdzenia arytmetyki wiemy, że każda liczba naturalna dodatnia ma postać iloczynu liczb pierwszych. Inaczej, każda liczba naturalna dodatnia $p > 1$ rozkłada się na iloczyn liczb pierwszych. Co więcej taki rozkład jest jedyny. To znaczy, że nie ma innego rozkładu tej liczby naturalnej.

Sposób rozkładu liczby naturalnej m na czynniki pierwsze jest prosty. Mianowicie, dzielimy liczbę m przez kolejne liczby pierwsze. Wtedy liczba m równa się iloczynowi dzielników.

Przykład 1.2 *Rozłóż liczbę $m = 1638$ na czynniki pierwsze.*

Posłóżyśmy się schematem

1638	2
819	3
273	3
91	7
13	13
1	

Liczba 1638 rozkłada się na czynniki 2, 3, 3, 7, 13

To znaczy

$$1638 = 2 * 3 * 3 * 7 * 13$$

Przykład 1.3 Rozłóż liczbę $m=5040$ na czynniki pierwsze. Postójmy się schematem

5040	2
2520	2
1260	2
630	2
315	3
105	5
21	3
7	7
1	

Liczba $m = 5040$ rozkłada się na czynniki 2, 2, 2, 2, 3, 5, 3, 7, To znaczy

$$5040 = 2 * 2 * 2 * 2 * 3 * 5 * 3 * 7.$$

Zauważmy, że siedem silnia równa się

$$7! = 1 * 2 * 3 * 4 * 5 * 6 * 7 = 5040$$

W tym rozkładzie mamy liczby złożone

$$4 = 2 * 2 \text{ i } 6 = 2 * 3$$

.

1.4 Największy wspólny dzielnik

Pojęcie największego wspólnego dzielnika wyjaśnimy na przykładach.

Przykład 1.4 Wspólnym dzielnikiem liczb 21 i 57 jest liczba 3, ponieważ liczba 3 dzieli liczbę 21 i dzieli liczbę 57. Poza tym te liczby nie mają innych wspólnych dzielników.

$$21 : 3 = 7 \text{ i } 57 : 3 = 19 \text{ lub } 21/3 = 7$$

Jasne, że liczby 21 i 57 rozkładają się na czynniki

$$21 = 3 * 7 \text{ i } 57 = 3 * 19,$$

Zauważamy, że liczba 3 jest dzielnikiem liczby 21 i jednocześnie jest dzielnikiem liczby 57.

To znaczy że liczba 3 jest wspólnym dzielnikiem liczby 21 i liczby 57. Zauważamy również, że te dwie liczby nie mają innych wspólnych dzielników. Dlatego liczba 3 jest największym wspólnym dzielnikiem liczby 21 i liczby 57.

Przykład 1.5 *Znajdź największy wspólny dzielnik liczb 42 i 78.*

Rozkładamy obie liczby na czynniki pierwsze

$$\begin{array}{r|l} 42 & 2, \\ 21 & 3, \\ 7 & 7, \\ 1 & \end{array} \quad \begin{array}{r|l} 78 & 2 \\ 39 & 3 \\ 13 & 13 \\ 1 & 1 \end{array}$$

Zauważamy, że te liczby

$$42 = 2 * 3 * 7 \quad i \quad 78 = 2 * 3 * 13$$

mają dwa wspólne dzielniki 2 i 3. Dlatego największym wspólnym dzielnikiem liczb 42 i 78 jest liczba $2 * 3 = 6$.

Dzielnik 7 liczby 42 nie dzieli liczby 78 oraz dzielnik 13 liczby 78 nie dzieli liczby 42.

Z powyższych przykładów widzimy, że największy wspólny dzielnik dwóch liczb naturalnych możemy wyznaczyć rozkładając te liczby na czynniki pierwsze a następnie wybieramy ich wspólne dzielniki. Wtedy za największy wspólny dzielnik jest równy iloczynowi ich wspólnych dzielników.

Rozpatrzyj jeszcze jeden przykład wyznaczania największego wspólnego dzielnika przez rozkład liczb na czynniki pierwsze

Przykład 1.6 *Znajdź największy wspólny dzielnik liczby 210 i liczby 231*

$$\begin{array}{r|l} 210 & 2, \\ 105 & 3, \\ 35 & 7, \\ 5 & 5 \\ 1 & \end{array} \quad \begin{array}{r|l} 231 & 3 \\ 77 & 7 \\ 11 & 11 \\ 1 & \end{array}$$

Zauważamy, że te liczby

$$210 = 2 * 3 * 7 * 5 \quad i \quad 231 = 3 * 7 * 11$$

mają dwa wspólne dzielniki 3 i 7. Dlatego największym wspólnym dzielnikiem liczb 210 i 231 jest iloczyn $3 * 7 = 21$. Sprawdzamy, że

$$210 : 21 = 10 \quad oraz \quad 231 : 21 = 11.$$

Dlatego największym wspólnym dzielnikiem liczb 210 i 231 jest iloczyn $3 * 7 = 21$.

Dzielniki 2, 5 liczby 210 nie dzielą liczby 231 oraz dzielnik 11 liczby 231 nie dzieli liczby 210.

1.5 Algorytm Euklidesa (325-265 B.C.)

Opócz sposobu znajdowania największego wspólnego dzielnika przez rozkład liczb na czynniki pierwsze, istnieją inne metody. Najbardziej efektywnym sposobem wyznaczania największego wspólnego dzielnika jest Algorytm Euklidesa. Już w starożytnych czasach w Egipcie, Euklides grecki nauczyciel i dziekan wydziału nauk przyrodniczych na Uniwersytecie w Aleksandrii podał algorytm na znajdowanie największego wspólnego dzielnika dwóch liczb naturalnych. Niżej podajemy opis algorytmu Euklidesa.

Zacznijmy opis algorytmu Euklidesa od przykładów.

Przykład 1.7 *Znajdź największy wspólny dzielnik liczb $a = 78$ i $b = 42$ stosując Algorytm Euklidesa.*

W liczbie $a = 78$ liczba $b = 42$ mieści się raz i zostaje reszta 36. Dalej wykonujemy dzielenia według schematu

$$\begin{array}{r|l}
 a = 78, & b = 42 & | & \text{reszta} \\
 \hline
 \frac{78}{42} = 1 + \frac{36}{42} & & | & 36 \\
 \frac{42}{36} = 1 + \frac{6}{36} & & | & 6 \\
 \frac{36}{6} = 6 & & | & 0
 \end{array}$$

Największym wspólnym dzielnikiem liczb 78 i 42 jest ostatnia reszta 6 różna od zera.

Ostatnia reszta 6 różna od zera jest również największym dzielnikiem reszty 36 i liczby 42.

Rozpatrzmy następny przykład zastosowania Algorytmu Euklidesa.

Przykład 1.8 *Znajdź największy wspólny dzielnik liczb $a = 1995$ i $b = 1190$*

$$\begin{array}{r|l}
 a = 1995, & b = 1190 & | & \text{reszta} \\
 \hline
 \frac{1995}{1190} = 1 + \frac{805}{1190} & & | & 805 \\
 \frac{1190}{805} = 1 + \frac{385}{805} & & | & 385 \\
 \frac{805}{385} = 2 + \frac{35}{385} & & | & 35 \\
 \frac{385}{35} = 11 & & | & 0
 \end{array}$$

Największym wspólnym dzielnikiem liczb 1995 i 1190 jest ostatnia reszta 35 różna od zera.

Zauważmy, że reszta 35 jest również dzielnikiem reszt 805 i 385 z poprzedniego dzielenia.

Teraz podamy ogólny schemat Algorytmu Euklidesa.

Niech r_0 i r_1 będą dwoma liczbami naturalnymi dla których chcemy znaleźć największy wspólny dzielnik.

Zakładamy, że $r_0 > r_1 > 0$.

Zadanie 1.1 *Znajdź największy wspólny dzielnik liczb r_0 i r_1 .*

Zauważamy, że jeżeli liczba d jest dzielnikiem liczb r_0 i r_1 to również jest dzielnikiem ich sumy $r_0 + r_1$ i różnicy $r_0 - r_1$.

Wykonując dzielenie

$$\frac{r_0}{r_1} = k_0 + \frac{r_2}{r_1}$$

obliczamy resztę

$$r_2 = r_0 - k_0 * r_1.$$

Tutaj k_0 jest całością z dzielenia liczby naturalnej liczb $r_0/r - 1$.

Teraz staje się jasne, że jeżeli liczba d jest wspólnym dzielnikiem liczb r_0 i r_1 to jest również dzielnikiem reszt r_2 .

Kolejne reszty z dzielenia obliczamy według schematu tak długo aż kolejna obliczona reszta $r_m = 0$.

$$\begin{array}{r|l}
 a = r_0, \quad b = r_1 & \text{reszta} \\
 \hline
 \frac{r_0}{r_1} = k_0 + \frac{r_2}{r_1} & r_2 = r_0 - k_0 * r_1 \\
 \frac{r_1}{r_2} = k_1 + \frac{r_3}{r_2} & r_3 = r_1 - k_1 * r_2 \\
 \frac{r_2}{r_3} = k_2 + \frac{r_4}{r_3} & r_4 = r_2 - k_2 * r_3 \\
 \dots & \dots \\
 \frac{r_{m-2}}{r_{m-3}} = k_{m-2} + \frac{r_m}{r_{m-1}} & r_m = r_{m-2} - k_{m-2} * r_{m-1} \\
 \frac{r_{m-1}}{r_m} = k_{m-1} & r_{m+1} = 0
 \end{array}$$

Ciąg reszt $r_0 > r_1 > r_2 \cdots > r_{m-1} > r_m$ jest malejący. Ostatnia reszta z dzielenia r_m różna od zera jest największym wspólnym dzielnikiem liczb naturalnych $a = r_0$ i $b = r_1$. Zauważmy, że największy wspólny dzielnik r_m liczb r_0 i r_1 jest również największym wspólnym dzielnikiem wszystkich poprzednich reszt $r_{m-1}, r_{m-2}, \dots, r_2, r_1, r_0$

Przykład 1.9 *Znajdź największy wspólny dzielnik liczb 975 i 690*

Rozwiązanie.

Stosujemy wyżej opisany algorytm Euklidesa obliczamy kolejne reszty

$$\begin{array}{r|l}
 a = r_0 = 975, & b = r_1 = 690 & | & \text{reszta} \\
 \hline
 \frac{975}{690} = 1 + \frac{285}{690} & & | & r_2 = 975 - 1 * 690 = 285 \\
 \frac{690}{285} = 2 + \frac{120}{285} & & | & r_3 = 690 - 2 * 285 = 120 \\
 \frac{285}{120} = 2 + \frac{45}{120} & & | & r_4 = 285 - 2 * 120 = 45 \\
 \frac{120}{45} = 2 + \frac{30}{45} & & | & r_5 = 120 - 2 * 45 = 30 \\
 \frac{45}{30} = 1 + \frac{15}{30} & & | & r_6 = 45 - 1 * 30 = 15 \\
 \frac{30}{15} = 2 & & | & r_7 = 0
 \end{array}$$

Ciąg reszt

$$975 > 690 > 285 > 120 > 45 > 30 > 15$$

jest malejący.

Ostatnia reszta z dzielenia $r_6 = 15$ różna od zera jest największym wspólnym dzielnikiem liczb naturalnych $a = r_0 = 975$ i $b = r_1 = 690$. Zauważmy, że największy wspólny dzielnik $r_6 = 15$ liczb $r_0 = 975$ i $r_1 = 690$ jest również największym wspólnym dzielnikiem wszystkich poprzednich reszt

$$r_2 = 285, r_3 = 120, r_4 = 45, r_5 = 30, r_6 = 15$$

1.6 Najmniejsza wspólna wielokrotna

Wspólną wielokrotną dwóch liczb naturalnych jest trzecia liczba naturalna, która jest podzielna przez obie te liczby.

Przykład 1.1 Dla liczb 5 i 7 wspólną wielokrotną jest ich iloczyn $5 * 7 = 35$. Liczba 35 jest najmniejszą wspólną wielokrotną liczb 5 i 7. Inną wspólną wielokrotną liczb 5 i 7 jest liczba 70, ponieważ $70 : 5 = 14$ i $70 : 7 = 10$. Jednak 70 nie jest najmniejszą wspólną wielokrotną liczb 5 i 7.

Sposób znajdowania najmniejszej wspólnej wielokrotnej oparty jest na rozkładzie liczb na czynniki pierwsze. Wyjaśniamy to na przykładach

Przykład 1.2 Znajdź najmniejszą wspólną wielokrotną liczb 120 i 210

Rozkładamy liczby 120 i 210 na czynniki pierwsze według schematu

$$\begin{array}{r|l}
 120 & 2, \\
 60 & 2, \\
 30 & 2, \\
 15 & 3, \\
 5 & 5 \\
 51 & \\
 \hline
 \end{array}
 \qquad
 \begin{array}{r|l}
 210 & 2 \\
 105 & 3 \\
 35 & 5 \\
 7 & 7 \\
 1 & \\
 \hline
 \end{array}$$

Wybieramy wspólne czynniki w rozkładzie obu liczb : 2, 3 i 5. Następnie do iloczynu $2 * 3 * 5$ dopisujemy czynniki, które nie są wspólne, to znaczy nie powtarzają się. To są czynniki 4 i 7.

Najmniejszą wspólną wielokrotną jest iloczyn tych czynników

$$2 * 3 * 5 * 4 * 7 = 1540$$

Przykład 1.3 Znajdź najmniejszą wspólną wielokrotną liczb 910 i 1155

Rozkładamy liczby 910 i 1190 na czynniki pierwsze według schematu

$$\begin{array}{r|l}
 910 & 2, \\
 455 & 5, \\
 91 & 7, \\
 13 & 13, \\
 1 & \\
 \hline
 \end{array}
 \qquad
 \begin{array}{r|l}
 1155 & 3 \\
 385 & 5 \\
 77 & 7 \\
 11 & 11 \\
 1 & \\
 \hline
 \end{array}$$

Wybieramy wspólne czynniki w rozkładzie obu liczb : 5 i 7. Następnie do iloczynu $5 * 7$ dopisujemy czynniki, które się nie są wspólne, to znaczy nie powtarzają się. To są czynniki 2, 3, 11, 13.

Najmniejszą wspólną wielokrotną jest iloczyn tych czynników

$$5 * 7 * 2 * 3 * 11 * 13 = 30030$$

1.7 Ćwiczenia

Zadanie 1.2 Rozłóż na czynniki pierwsze liczby

(i) $a = 184$

(ii) $b = 6006$

Zadanie 1.3 Podaj resztę z dzielenia liczby a przez liczbę b

(i) $a = 254$ i $b = 15$

(ii) $b = 2672$ i $b = 848$

Zadanie 1.4 Znajdź największy wspólny dzielnik liczb 425 i 125

(i) przez rozkład tych liczb na czynniki pierwsze.

(ii) stosując Algorytm Euklidesa

Zadanie 1.5 Znajdź największy wspólny dzielnik liczb stosując Algorytm Euklidesa

$$2672 \text{ i } 848$$

Zadanie 1.6 Wyznacz wszystkie rozwiązania układu równań

$$x + y = 180$$

$$NWD(x, y) = 30$$

1

Zadanie 1.7 Ile wspólnych wyrazów mają ciągi arytmetyczne

$$5, 8, 11, 14, \dots; \text{ i } 3, 7, 11, 15, \dots;$$

Zadanie 1.8 Znajdź najmniejszą wspólną wielokrotną liczb

(i) 25 i 235

(ii) 512 i 5040

Zadanie 1.9 Czy każdą liczbę pierwszą p można przedstawić w postaci iloczynu różnicy i sumy liczb naturalnych a i b

$$p = (a - b)(a + b)$$

Zadanie 1.10 Wykaż, że dla każdej liczby pierwszej $p > 4$ liczba $(p-1)(p+1)$ jest podzielna przez 24

¹NWD(x,y) oznacza największy wspólny dzielnik liczby x i liczby y.