**Podstawowe Twierdzenie Arytmetyki**.

**Twierdzenie 0.1** *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*

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

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 0.1** *Rozłóż liczbę* $m = 1638$ *na czynniki pierwsze.*

Posłóżymy 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 0.2** *Rozłóż liczbę m=5040 na czynniki pierwsze. Posłóżymy 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 czynniki złożone

$$4 = 2 * 2 \quad i \quad 6 = 2 * 3$$

Dlatego, według Podstawowego Twierdzenia Arytmetyki, liczba $m = 5040$ rozkłada się na iloczyn liczb pierwszych

$$5040 = 2^4 * 3^2 * 5 * 7$$

**Algorytm.**

Od czasów Euklidesa (*Algorytm znajdowania największego wspólnego dzielnika dwóch liczba naturalnych)* i Eratotenesa (*Sito Eratotenesa wyznaczenia wszystkich liczb pierwszych z przedziału* $[2, n]$, ogłoszono wiele algorymów rozkładu liczb naturalnych na czynniki pierwsze. Dalej tworzone są nowe algorytmy głównie pod kątem kodowania i zastosowania bardzo dużych liczb, z setkami cyfr, na przykład w kryptografii.
Niżej podamy prosty, ale nie optymalny, algorytm rozkładu danej liczby naturalnej na czynniki pierwsze oraz jego kod w systemie *Mathematica*.
*Oznaczenia*

1. *Literą $m$ oznaczamy daną liczbę naturalną, której rozkładu na czynniki pierwsze szukamy.*

2. *Deklarujemy dwie listy puste*

$$Tz = \{\}, \quad oraz \quad Tp = \{\}$$

*Do listy $Tz$ dołączymy wszystkie dzielniki liczby $m$, w tym również dzielniki złożone, stosując operacje $Modulo - Kongruencje$ obliczania reszty $r$ z dzielenia liczby $m$ przez kolejne liczby $i = 2, 3, 4, \cdots, n$;*

$$r = (m\ Mod\ i) \quad dla \quad i = 2, 3, 4, \cdots, n, \quad n = [\frac{m}{2}].$$

[1] *Dołączamy również krotności czynnika $i$.*
*Natomiast do listy $Tp$ dołączamy kolejne czynniki pierwsze liczby $m$, redukując z listy $Tz$ czynniki złożone.*

**Moduł w systemie** *Mathematica*
*Listę wszystkich możliwych czynników liczby $m$ wyznacza moduł.*

[1] Tutaj symbol $[\frac{m}{i}]$ oznacza całość z dzielenia liczby $m$ przez $i$.

```
TwierdzenieArytmetyki[m_] := Module[{ a, b, test, i, n, m0, m1, r, r1, Tp},
  m0 = m; m1 = m; n = Floor[m0/2]; test = 0;
  Tp = { };
  onep[a_, r_, i_] := Module[{ },
    r1 = r; b = a;
    While[r1 == 0, {AppendTo[Tp, i], r1 = Mod[b, i], b = b/i}];
    test' = 1;
    m0 = a;
    ];
  Do[{r = Mod[m0, i], a = Floor[m0/i], If[r == 0, onep[a, r, i]]}, {i,2, n}];
  If[test == 0, AppendTo[Tp, m]];
  Tp]
  ]
```

***Przykład 0.3*** *Dla* $m = 5040$ *otrzymujemy wszystkie jej czynniki wykonując instrukcję*

```
TwierdzenieArytmetyki[5040]

Out[5]= {2, 2, 2, 2, 3, 3, 4, 5, 6, 7, 5040}
```

*Moduł* $CzynnikiPierwsze$ *tworzy listę* $Tp$ *czynników pierwszych liczby* $m$ *z listy* $Tz$ *wszystkich czynników liczby* $m$

```
CzynnikiPierwsze[l_] := Module[{c, k, n, Ts, Tz },
  Ts = { };
  Tz = TwierdzenieArytmetyki[l];
  n = Length[Tz];
  Table[  { c = Length[TwierdzenieArytmetyki[Tz[[k]]]],
    If[c == 1, AppendTo[Ts, Tz[[k]]]]}, {k, 1, n}];
  Ts
  ]
```

***Przykład 0.4*** *Dla* $m = 5040$ *otzymujemy rozkład tej liczby na czynniki pierwsze wykonujemy instrukcję*

```
CzynnikiPierwsze[5040]

Out[5]= {2, 2, 2, 2, 3, 3, 5, 7}
```

### Implementacje powyższych modułów

- *w systemie Mathematica aktywujemy moduł* $TwierdzenieArytmetyki[m]$
- *następnie, aktywujemy moduł* $CzynnikiPierwsze[m]$

- *rozkład liczby m na czynniki pierwsze otrzymujemy wykonując instrukcje CzynnikiPierwsze[m]*

***Przykład 0.5*** *Dla* $m = 30030$ *otzymujemy rozkład tej liczby na czynniki pierwsze wykonujemy instrukcję*

```
CzynnikiPierwsze[30030]

Out[8]= {2, 3, 5, 7, 11, 13}
```

*W systemie Mathematica jest bardzo krótka i skuteczna instrukcja rozkładu danej liczby m na czynniki pierwsze. To jest instrukcja*

```
FactorInteger[m]
```

***Przykład 0.6*** *Znajdź rozkład na czynniki pierwsze liczby* $m = 60$ *wykonując instrukcje*

```
FactorInteger[60]
{{2, 2}, {3, 1}, {5, 1}}
```

*Wynik tej instrukcji*

```
{{2, 2}, {3, 1}, {5, 1}}
```

*czytamy*

$$60 = 2^2 * 3^1 * 5^1$$

***Przykład 0.7*** *Znajdź rozkład na czynniki pierwsze liczby* $18 - to$ *cyfrowej*

$$m = 235489703970060540$$

*wykonując instrukcje*

```
FactorInteger[235489703970060540]

{{2, 2}, {3, 3}, {5, 1}, {7, 1}, {11, 1}, {13, 1},
        {17,1}, {19, 1}, {23, 1}, {29, 1}, {31, 1}, {37, 1},
        {41, 1}, {43, 1}}
```

*Wynik tej instrukcji czytamy*

$$\begin{aligned} 235489703970060540 &= 2^2 * 3^1 * 5^1 * 7^1 * 11^1 * 13^1 * 17^1 \\ &* \quad 19^1 * 23^1 * 29^1 * 31^1 * 37^1 * 41^1 * 43^1 \end{aligned}$$

***Przykład 0.8*** *Znajdź rozkład na czynniki pierwsze liczby* $100 - to$ *cyfrowej*

```
m = 240000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000
```

*wykonując instrukcję*

```
FactorInteger[m]
```

```
{{2, 103}, {3, 1}, {5, 100}}
```

*Wynik tej instrukcji czytamy*

$$m \;=\; 2^{103} * 3^{1} * 5^{100}$$

## 0.1 Zadania

***Zadanie 0.1*** *Znajdź wszystkie dzielniki liczby* $m = 15$ *wykonując krok po kroku algorytm TwierdzenieArytmetyki[m] zapisany w kodzie Mathematyka.*

***Zadanie 0.2*** *Znajdź rozkład na czynniki pierwsze liczby* $m = 15$ *wykonując krok po kroku algorytm CzynnikiPierwsze[m] zapisany w kodzie Mathematyka.*

***Zadanie 0.3*** *Mając dostępny system Mathematica na notebooku, znajdź wszystkie dzielniki liczby* $m = 3072$ *wykonując instrukcję TwierdzenieArytmetyki[m]*

***Zadanie 0.4*** *Mając dostępny system Mathematica na notebooku, znajdź rozłóż na czynniki pierwsze liczbę* $m = 3072$ *wykonując instrukcję CzynnikiPierwsze[m]*

*Prof. dr Tadeusz STYŠ* *Warszawa 2018-06-02*