# Funkcje arytmetyczne

## Definicja 1

Każda arytmetyczna, to funkcja $f(n)$, $n \in \mathbb{N}$, przyporządkowująca $\mathbb{N} \to \mathbb{C}$, $(\mathbb{R})$.

Na przykład: $f(n) = \sqrt{n}$.

## Definicja 2:

Funkcję arytmetyczną $f : \mathbb{N} \overset{f(n)}{\to} \mathbb{R}$ nazywamy *multyplikatywną*, jeżeli

$$\forall_{m,n\in\mathbb{N}},\ m \perp n \quad \text{mamy} \quad f(mn) = f(m) \cdot f(n).$$

Funkcję arytmetyczną $f$ nazywamy *całkowicie multyplikatywną*, jeżeli

$$\forall_{m,n\in\mathbb{N}}, \quad \text{mamy} \quad f(mn) = f(m) \cdot f(n).$$

## Przypomnijmy, ...

...że poznaliśmy już takie *funkcje arytmetyczne* jak liczba $\tau$ i suma $\sigma$ (także iloczyn) dzielników:

$$\tau(n) = \sum_{d|n} 1, \qquad \sigma(n) = \sum_{d|n} d$$

**Twierdzenie 1**

Dla każdej multyplikatywnej $f(n) \not\equiv 0$ mamy $f(1) = 1$.

Dowód: banalny.

**Twierdzenie 2**

Dla liczby $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ zachodzi $f(n) = \prod_{i=1}^{r} f\left(p_i^{\alpha_i}\right)$.

Dowód indukcyjny (również bardzo łatwy).

**Twierdzenie 3**

Jeżeli $f$ jest funkcją multyplikatywną oraz $g(n) = \sum_{d|n} f(d)$
to funkcja $g$ jest też funkcją multyplikatywną.
Dowód: dla $m \perp n$ dzielnik $d \mid mn$ jeżeli $d = d_1 d_2$, gdzie $d_1 \mid m$ oraz $d_2 \mid n$; przy czym $(d_1, d_2) = 1 = (m/d_1, n/d_2)$.
zachodzi więc

$$g(mn) = \sum_{d|mn} f(d) = \sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2) = \sum_{d_1|m} f(d_1) \cdot \sum_{d_2|n} f(d_2). \qquad \square$$

## Twierdzenie 4

Jeżeli $f$ i $g$ są funkcjami multyplikatywnymi to

$$F(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

jest też funkcją multyplikatywną.

Dowód – jak twierdzenia 3. Rozważamy $F(mn)$ dla $m \perp n$. Mamy

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) g\left(\frac{mn}{d}\right) = \sum_{d_1|m} f(d_1 d_2) \sum_{d_2|n} f(d_1 d_2) g\left(\frac{mn}{d_1 d_2}\right) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) \\ &= \sum_{d_1|m} f(d_1) g\left(\frac{m}{d_1}\right) \sum_{d_2|n} f(d_2) g\left(\frac{n}{d_2}\right) = F(m) F(n). \end{aligned}$$

# Funkcja Eulera $\phi(n)$

## Definicja 3:

$$\phi(n) = \sum_{\substack{1 \leqslant k \leqslant n \\ (k,n)=1}} 1.$$

Funkcja $\phi$ to liczba liczb naturalnych, *względnie pierwszych i nie większych* od liczby $n$.

## Kilka wartości:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 100 | 101 | 102 | 103 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\phi$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 | 40 | 100 | 32 | 102 |

## Wniosek 1:

Jeżeli $n = p$ (jest liczbą pierwszą), to $\phi(p) = p - 1$.

# Funkcja Eulera $\phi(n)$

## Wniosek 2:

Jeżeli $n = p^\alpha$ (jest potęgą liczby pierwszej), to liczbami, które nie są względnie pierwsze z $n$ są wielokrotności $p$ – liczby $p, 2p, 3p, \ldots, p^{\alpha-1}p$. Tych liczb jest $p^{\alpha-1}$;

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right).$$

## Przypadek ogólny:

niech liczba pierwsza $p \mid m$; jakie jest $\phi_p(m)$ – liczba liczb spośród $1, 2, \ldots, m-1, m$, które nie są podzielne przez $p$? Dzielnikami mogą być tylko wielokrotności $p$: $p, 2p, \ldots, \frac{m}{p} \cdot p$. A więc

$$\phi_p(m) = m - \frac{m}{p} = m\left(1 - \frac{1}{p}\right).$$

Niech inna liczba pierwsza $q \mid m$; jakie jest $\phi_{pq}(m)$ – liczba liczb spośród $1, 2, \ldots, m-1, m$, które nie są podzielne przez $p$ *ani* przez $q$?

## Przypadek ogólny,c.d.

Jeżeli odjąć od $\phi_p(m)$ analogiczne $m/q$ podzielnych przez $q$, to odejmujemy za dużo, o wielokrotności $pq, 2pq, \ldots, \frac{m}{pq} \cdot pq$. Stąd

$$\begin{aligned}\phi_{pq}(m) &= m\left(1-\frac{1}{p}\right) - \frac{m}{q} + \frac{m}{pq} = m\left(1-\frac{1}{p}\right) - \frac{m}{q}\left(1-\frac{1}{p}\right) \\ &= m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right).\end{aligned}$$

Indukcyjnie: jeżeli $p_1, p_2, \ldots, p_r$ są liczbami pierwszymi i $p_i \mid m$; $i = 1, \ldots, r$ to pośród $m$ liczb istnieje

$$\phi_{p_1 p_2 \ldots p_r} = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)$$

liczb, które nie są podzielne przez żaden z czynników pierwszych $p_1, p_2, \ldots, p_r$.

Co więcej – jeżeli rozkład kanoniczny liczby $m$ ma postać $m = {p_1}^{\alpha_1}, {p_2}^{\alpha_2}, \ldots, {p_r}^{\alpha_r}$ to każda liczba spośród $1, 2, \ldots, m$ będzie względnie pierwsza z $m$ *wtedy i tylko wtedy, gdy nie będzie podzielna przez żadną z liczb pierwszych* $p_1, p_2, \ldots, p_r$.

## Funkcja Eulera dla $m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}$

ma więc postać

$$\boxed{\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_r}\right)}$$

Przykład: $\phi(42) = \phi(2 \cdot 3 \cdot 7) = 42(1 - 1/2)(1 - 1/3)(1 - 1/7) = 12.$

## Funkcję Eulera ...

... możemy zapisać nieco inaczej, podstawiając za $m$

$$\begin{aligned}\phi(m) &= {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_r}\right)\\ &= {p_1}^{\alpha_1 - 1}(p_1 - 1){p_2}^{\alpha_2 - 1}(p_2 - 1)\dots {p_r}^{\alpha_r - 1}(p_r - 1)\\ &= ({p_1}^{\alpha_1} - {p_1}^{\alpha_1 - 1})\dots({p_r}^{\alpha_r} - {p_r}^{\alpha_r - 1}).\end{aligned}$$

## Z ostatniego wzoru ...

wynika, że funkcja Eulera jest multyplikatywna!

$$\phi(m) = ({p_1}^{\alpha_1} - {p_1}^{\alpha_1 - 1}) \dots ({p_r}^{\alpha_r} - {p_r}^{\alpha_r - 1}) = \phi({p_1}^{\alpha_1}) \dots \phi({p_r}^{\alpha_r}).$$

Dla dowolnych liczb $a \perp b$ zachodzi $\phi(ab) = \phi(a)\phi(b)$.

## Twierdzenie 5

$$\forall n \in \mathbb{N} \quad \sum_{d|n} \phi(d) = n.$$

Dowód: dla $m = p^\alpha$ dzielnikami $m$ są liczby $1, p, p^2, \dots, p^\alpha$. Mamy:

$$\phi(1) + \phi(p) + \phi(p^2) + \dots + \phi(p^\alpha)$$
$$1 + (p-1) + (p^2 - p) + \dots + (p^\alpha - p^{\alpha-1}) = p^\alpha. \qquad \square$$

Dla $m$ w postaci ogólnej $\boxed{m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}}$
tworzymy iloczyn sum funkcji $\phi$ poszczególnych czynników:

## Twierdzenie 5, c.d.

. . . iloczyn sum funkcji $\phi$ poszczególnych czynników:
$[\phi(1) + \phi(p_1) + \ldots + \phi({p_1}^{\alpha_1})] \cdot [\phi(1) + \phi(p_2) + \ldots + \phi({p_2}^{\alpha_2})] \ldots$
$\ldots [\phi(1) + \phi(p_r) + \ldots + \phi({p_r}^{\alpha_r})]$

Z jednej strony — zgodnie z poprzednim wywodem – każdy kwadratowy nawias to ${p_i}^{\alpha_i}$ – a więc taki iloczyn jest równy $m$.

Z drugiej strony – wymnażając przez siebie zawartości kwadratowych nawiasów dostajemy sumę *wszystkich* możliwych iloczynów typu $\phi({p_1}^{\delta_1})\phi({p_2}^{\delta_2}) \ldots \phi({p_r}^{\delta_r})$ gdzie $1 \leqslant \delta_i \leqslant \alpha_i$. Funkcja Eulera jest multyplikatywna – są to więc funkcje $\phi({p_1}^{\delta_1} {p_2}^{\delta_2} \ldots {p_r}^{\delta_r})$ – funkcje *wszystkich możliwych dzielników* naszej liczby $m$. □

Przykład: liczba 42:
$\phi(42) = \phi(2 \cdot 3 \cdot 7) = 42(1 - 1/2)(1 - 1/3)(1 - 1/7) = 12.$
Liczba 42 ma 8 dzielników: $1, 2, 3, 6, 7, 14, 21, 42$.
$\phi(1) = 1;\ \phi(2) = 1;\ \phi(3) = 2;\ \phi(6) = 3;\ \phi(7) = 6;\ \phi(14) = 6;\ \phi(21) = 12;\ \phi(42) = 12.$
Suma $1 + 1 + 2 + 2 + 6 + 6 + 12 + 12 = 42.$

## W przyszłości ...

poznamy jeszcze dwie funkcje arytmetyczne:

- *funkcję Carmichaela* – $\lambda(m)$;
  ciekawy i *pożyteczny* „zamiennik” funkcji Eulera oraz ...
- ... blisko z nią związaną funkcję Möbiusa – $\mu(n)$.
  Ta ostatnia funkcja jest też funkcją multyplikatywną.