# Pierścienie.

**Def.** Trójka $(P, +, \cdot)$ nazywamy pierścieniem, gdy

1. $(P, +)$ jest grupą abelową.
2. $\cdot$ jest łączne na $P$.
3. $\forall a, x, y \in P \quad a(x+y) = ax + ay$
   $(x+y)a = xa + ya$

Oznaczenie: $+, \cdot$ dodawanie i mnożenie.
$0, 1$ elementy neutralne dodawania i mnożenia
$-a$ element przeciwny do $a$ wzg. $+$
$a^{-1}$ element odwrotny do $a$ wzg. $\cdot$.

Przykłady:

$(\mathbb{Z}, +, \cdot)$

$\forall n \in \mathbb{N}^+ \quad \mathbb{Z}_n = (\{0, \dots, n-1\}, \overset{+}{n}, \overset{\cdot}{n})$

$n \in \mathbb{N}^+ \quad (\mathbb{R}^{n \times n}, +, \cdot)$ pierścień nieprzemienny.

$K$ - ciało, $(K[X], +, \cdot)$ pierścień wielomianów

Homomorfizmy pierścieni.

**Def** Niech $(P, +, \cdot)$, $(R, +, \cdot)$ pierścienie
Funkcja $\varphi : P \to R$ nazywamy homomorfizmem, gdy

1. $\forall a, b \in P \quad \varphi(a+b) = \varphi(a) + \varphi(b)$
2. $\forall a, b \in P \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Przykład

$\varphi_n(k) = k \pmod n : \mathbb{Z} \to \{0, 1, \dots n-1\}$

jest homomorfizmem pierścieni $\mathbb{Z}$ i $\mathbb{Z}_n$

Fakt Niech $m, n \in \mathbb{N}$ $m \mid n$. Wtedy

$\varphi_{n,m}(k) = k \pmod m : \mathbb{Z}_n \to \mathbb{Z}_m$ homomorfizm

D-d ćw.

Wniosek. Niech $m, n \in \mathbb{N}$, $NWD(m,n) = 1$. Wtedy funkcja

$\varphi(k) = (k \bmod m, k \bmod n) : \mathbb{Z}_{m \cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n$.

jest izomorfizmem pierścieni (homomorfizm + bijekcja)

D-d ćw.

Iloczyn kartezjański pierścieni.

Niech $(P, +, \cdot)$, $(R, \oplus, \odot)$ pierścienie.

Na zbiorze $P \times R$ definiujemy działania:

dodawanie $(p_1, r_1) + (p_2, r_2) = (p_1 + p_2, r_1 \oplus r_2)$

mnożenie: $(p_1, r_1) \cdot (p_2, r_2) = (p_1 \cdot p_2, r_1 \odot r_2)$

Fakt Struktura $(P \times R, +, \cdot)$ jest pierścieniem.

Uwagi 1. $(0_P, 0_R)$ - zero w pierścieniu $P \times R$.

2. $(1_P, 1_R)$ - jedynka w pierścieniu $P \times R$, (o ile istnieje)

## Elementy odwracalne pierścienia.

Def. Niech $(P, +, \cdot)$ pierścień z 1. Element $a \in P$ nazywamy odwracalnym, gdy istnieje $b \in P$

$$a \cdot b = 1.$$

Zbiór wszystkich elementów odwracalnych pierścienia $P$ oznaczamy $P^*$

Fakt. Niech $(P, +, \cdot)$ pierścień. Wtedy $(P^*, \cdot)$ jest grupą

Np: $\cdot (\mathbb{Z}^*, \cdot) = (\{1, -1\}, \cdot) \cong C_2$

$\cdot (\mathbb{R}^{n \times n})^* = GL_n(\mathbb{R})$.

Fakt Niech $P, R$ pierścienie z jedynkami.

Wtedy $(P \times R)^* = P^* \times R^*$

$(ax, by)$

D-d:

$(a,b) \in (P \times R)^* \iff \exists (x,y) \in P \times R \quad (a,b) \cdot (x,y) = (1,1)$

$\iff \exists x \in P \; \exists y \in R \quad a \cdot x = 1 \wedge by = 1 \iff$

$a \in P^* \wedge b \in R^* \iff$

$(a,b) \in P^* \times R^*$ □

Wniosek. Niech $m, n \in \mathbb{N}^+$ $NWD(m,n)=1$.

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

D-d.

$$\varphi(mn) = |\mathbb{Z}^*_{m\cdot n}| \overset{\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n}{=} |(\mathbb{Z}_m \times \mathbb{Z}_n)^*| \overset{(P\times R)^* = P^* \times R^*}{=} |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| =$$

$$|\mathbb{Z}_m^*| \cdot |\mathbb{Z}_n^*| = \varphi(m) \cdot \varphi(n) \qquad \square$$

Wniosek. Niech $n \in \mathbb{N}^+$, $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, $p_i \in \mathbb{P}$

Wtedy $\varphi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$

D-d. $\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) = \prod_{i=1}^{k} \varphi\left(p_i^{\alpha_i}\right) =$

$$\prod_{i=1}^{k}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = \prod \left[p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)\right] =$$

$$\underbrace{\prod_{i} p_i^{\alpha_i}}_{n} \prod_{i} \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i} \left(1 - \frac{1}{p_i}\right) \qquad \square$$

Komen. Jeśli znamy rozkład $n$ na czynniki pierwsze

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Wtedy obliczenie $\varphi(n)$ jest łatwe

Jeśli nie znamy rozkładu $n$ to obliczenie jest trudne.

# Protokół RSA.

RSA służy do szyfrowania i odszyfrowywania wiadomości.

RSA składa się z trzech algorytmów:

## I. Generowanie klucza

1. Wybieramy liczby pierwsze $p, q$ (duże, porównywalne).
2. $n = p \cdot q$
3. $\varphi(n) = (p-1)(q-1)$.
4. Wybieramy $a \in \mathbb{Z}^*_{\varphi(n)}$, odwracalny
5. Obliczamy w $\mathbb{Z}^*_{\varphi(n)}$ $b = a^{-1}$ tzn $a \cdot b = k \cdot \varphi(n) + 1$

$a^{-1}$: Alg Euklid $a \cdot x = \varphi(n) \cdot y + 1 \equiv a x + \varphi(n) y = 1$ równanie diofant.

6. Wtedy $(a, n)$ – klucz publiczny – do szyfrowania
   $(b, n)$ – klucz prywatny – do odszyfrowywania.

## II Szyfrowanie.

Wiadomość $M = 1011\ldots = M_1 M_2 M_3 \ldots$

tak dzy $M_i$ odpowiada jakaś liczba naturalna nie przekraczająca $n$.

dbamy aby: $M_i \in \mathbb{Z}^*_n$, tzn $NWD(M_i, n) = 1$ ...

Szyfr: $S_i = M_i^a$. w $\mathbb{Z}^*_n$

## III Odszyfrowywanie:

$S_i^b$ w $\mathbb{Z}^*_n$

Analiza protokołu

$M \in \mathbb{Z}_n$

$M^{a \cdot b} = \left(M^{\varphi(n)}\right)^k \cdot M = M$

$M^{\varphi(n)} = 1$

Niech $M_i$ wiadomości

Szyfrujący: $S_i = M_i^a$

Odszyfr: $S_i^b = \left(M_i^a\right)^b = M_i^{a \cdot b} = M_i^{k \cdot \varphi(n) + 1} = \left(M_i^{\varphi(n)}\right)^k \cdot M_i^1 =$

$\left(M_i^{|\mathbb{Z}_n^*|}\right)^k \cdot M_i = 1 \cdot M_i = M_i$

Bezpieczeństwo protokołu opiera się na trudności obliczenia $\varphi(n)$ bez znajomości rozkładu $n = p \cdot q$.