Przypomnienie. Niech $n \in \mathbb{N}^+$

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

jest homomorfizmem pierścieni

$$\varphi_n : (\mathbb{Z}, +, \cdot) \to \mathbb{Z}_n = (\{0,\dots,n-1\}, +_n, \cdot_n).$$

$$\varphi_n(a \overset{\circ}{+} b) = \varphi_n(a) +_n \varphi_n(b).$$

Zasada podzielności przez 11 liczb zapisanych w systemie 10-tnym.

Ozn: $\overline{a_1a_2a_3} = 100a_1 + 10a_2 + a_3$

Niech $k \in \mathbb{N}$ $\quad k = \overline{a_n a_{n-1} \cdots a_1 a_0}$

$$11 \mid k \Leftrightarrow \varphi_{11}(k) = 0 \Leftrightarrow \varphi_{11}(\overline{a_n \cdots a_1 a_0}) = 0 \Leftrightarrow$$

$$\varphi_{11}(10^n a_n + \dots + 10a_1 + a_0) = 0$$

$\Leftrightarrow$ φ_{11} jest homomorf.

$$\varphi_{11}(10)^n \cdot_{11} \varphi_{11}(a_n) +_{11} \dots +_{11} \varphi_{11}(10)^2 \cdot_{11} \varphi_{11}(a_2) +_{11} \varphi_{11}(10)\varphi(a_1) +_{11} \varphi_{11}(a_0) = 0$$

Zauważmy $\varphi_{11}(10) = 10 = (-1) = -\varphi(1) = \varphi(-1)$. w $\mathbb{Z}_{11}$

zatem $[\varphi_{11}(10)]^k = (-1)^k = \varphi(-1)^k$

$$\varphi_{11}(-1)^n \cdot \varphi_{11}(a_n) +_{11} \dots +_{11} \varphi_{11}(-1)^2 +_{11} \varphi_{11}(-1)\varphi(a_1) +_{11} \varphi_{11}(a_0) = 0$$

$\updownarrow$ φ_{11} jest homomorf.

$$\varphi_{11}(-1^n a_n + \dots + 1a_2 - a_1 + a_0) = 0$$

$$\varphi_{11}(a_0 - a_1 + a_2 + \dots + (-1)^n a_n) = 0$$

$\Leftrightarrow$ $11 \mid a_0 - a_1 + a_2 - \dots + (-1)^n a_n$

Spr: $11 \mid 121$ bo $1-2+1 = 0$ oraz $11 \mid 0$ ok

Ćw. Wyprowadzić wzory na podzielność przez 7.

CIAŁA $(\mathbb{R}+,\cdot)$

Def. Ciało nazywamy trójkę $(K,+,\cdot)$ gdzie
K zbiór $+,\cdot$ działania na K takie, że:

1. $(K,+)$ jest grupą przemienną
2. $(K\setminus\{0\},\cdot)$ jest grupą przemienną (gdzie 0 - element neutr. w $(K,+)$)
3. $\forall a,x,y\in K \quad a\cdot(x+y) = ax+ay$.

Przykłady
- $(\mathbb{R}+,\cdot)$ jest ciało.
- $(\mathbb{Q}+,\cdot)$ jest ciało.
- $(\mathbb{Z}+,\cdot)$ NIE jest ciało bo element odwrotny do 7 wzg $\cdot$ nie należy do $\mathbb{Z}$

Uwaga. Każde ciało jest pierścieniem.

Uwaga. Niech $(P,+,\cdot)$ pierścień. Wtedy
P jest ciałem $\Leftrightarrow$

1. $\cdot$ jest przemienne
2. istnieje element neutralny $1\cdot$ $\quad (\forall x)\, 1\cdot x = x$
3. $\forall a\in P\setminus\{0\} \quad \exists b\in P \quad a\cdot b = 1 \leftarrow$ element neutralny

Obliczenia w ciałach. $(K,+,\cdot)$

- Niech $x,y\in K$

$$(x+y)^2 = (x+y)\cdot(x+y) \overset{\text{rozdz. mnożenia}}{=} (x+y)\cdot x + (x+y)\cdot y =$$

$$x\cdot x + y\cdot x + x\cdot y + y\cdot y \overset{\text{przemienność mnożenia}}{=} x\cdot x + xy + xy + y\cdot y =$$

$$x^2 + 1\cdot x\cdot y + 1 x\cdot y + y^2 = x^2 + (1+1)\,x\cdot y + y^2$$

(oznaczenie $1+1=2$) $\quad = x^2+2xy+y^2$

Niech $(K, +, \cdot)$ ciało. Istnieją w K elementy neutralne dodawania i mnożenia które oznaczamy $0, 1$.

Oznaczenie: $0, 1$: w każdym ciele istnieją te elementy.

- $n \in \mathbb{N}$ definiujemy $n = \underbrace{1 + 1 + \dots + 1}_{n \times}$ (np $2 = 1+1$).
- $n \in \mathbb{N}$ $-n$ to $-(\underbrace{1+1+\dots+1}_{n})$ element odwrotny do n wzgl. element neutralny $+$ w K (np $-5 = -(1+1+1+1+1)$).
- $n, m \in \mathbb{Z}$, wtedy $\frac{n}{m} = n \cdot m^{-1}$, gdy $m \neq 0$.

CIAŁA SKOŃCZONE $\mathbb{Z}_p$.

Lemat. Dla dowolnych $a, b \in \mathbb{Z}$ istnieją $x, y \in \mathbb{Z}$ takie, że

$$a \cdot x + by = NWD(a, b)$$

Przykłady: • $7x + 3y = NWD(7,3) = 1$

rozw. $\begin{cases} x = 1 \\ y = -2 \end{cases}$

• $12x + 8y = NWD(12, 8) = 4$

$\begin{cases} x = 1 \\ y = -1 \end{cases}$

$12x + 8y = 1$ nie ma rozwiązania:

$4 \cdot (3x + 2y) = 1$

Uwaga. p, q – liczby względnie pierwsze to

$$px + qy = 1 \quad \text{ma rozwiązanie } x, y \in \mathbb{Z}.$$

Tw. Dla dowolnej liczby pierwszej p pierścień $\mathbb{Z}_p = (\{0, \dots, p-1\}, \overset{+}{p}, \overset{\cdot}{p})$ jest ciałem.

D-d:

1. Mnożenie $\overset{\cdot}{p}$ jest przemienne:
$\forall x, y \in \{0, \dots, p-1\}$ $\quad x \overset{\cdot}{p} y = (x \cdot y) \bmod p = (y \cdot x) \bmod p$
$= y \overset{\cdot}{p} x$

2. W zbiorze $\{0, \dots p-1\}$ istnieje element neutralny $\overset{\cdot}{p}$
Element 1 jest neutralny wzg $\overset{\cdot}{p}$
$x \in \{0, \dots p-1\}: 1 \overset{\cdot}{p} x = (1 \cdot x) \bmod p = x \pmod p = x$

$(\forall x) \quad 1 \overset{\cdot}{p} x = x$.

3. $\forall a \in \{0, \dots p-1\} \setminus \{0\} \quad \exists b \in \{0 \dots p-1\} \quad a \overset{\cdot}{p} b = 1$.

Liczba p jest pierwsza, $a < p$ więc
$NWD(p, a) = 1$.

Z lematu istnieją $x, y \in \mathbb{Z}$ takie, że

$$px + ay = NWD(p, a) = 1$$

Niech $z = y \pmod p$

Zauważmy, że

$$a \overset{\cdot}{p} z = a \cdot z \pmod p \overset{\cdot}{=} a \cdot y \pmod p \overset{\cdot}{=}$$
$$(a \cdot y + px) \pmod p = 1 \pmod p = 1$$

$$a \overset{\cdot}{p} z = 1 \qquad \square$$

(tzn $z = a^{-1}$.)

Obliczenia w $\mathbb{Z}_p$.

Niech $p = 11$.

$$\mathbb{Z}_p = (\{0,1,2,\dots,10\}, +_{11}, \cdot_{11}).$$

$$7 +_{11} 9 = (7+9) \pmod{11} = 16 \pmod{11} = 5.$$

$$-9 = x : \quad 9 +_{11} x = 0$$
$$(9+x) \bmod 11 = 0$$
$$9 + x = 11 \cdot k \qquad k \in \mathbb{Z}$$
$$x = 2$$
$$-9 = 2$$

$$9^{-1} = x : \quad 9 \cdot_{11} x = 1$$
$$(9 \cdot x) \pmod{11} = 1$$
$$9 \cdot x = 11k + 1$$
$$(-k = y) \qquad 9x - 11k = 1$$
$$9x + 11y = 1$$
$$\begin{cases} x = 5 \\ y = -4 \end{cases}$$

$$9^{-1} = x = 5 \qquad \text{Spr} \quad 5 \cdot_{11} 9 = 45 \bmod 11 = 1$$

- Równanie liniowe:

$$9 \cdot_{11} x +_{11} 9 = 3 \quad \Big| \begin{matrix} +_{11} -9 \\ (+_{11} \ 2) \end{matrix}$$

$$9 \cdot_{11} x +_{11} 9 +_{11} 2 = 3 +_{11} 2$$

$$9 \cdot_{11} x = 5 \quad \Big| \overset{:9}{(} \text{razy } \cdot_{11} 9^{-1}, \text{ razy } \cdot_{11} 5)$$
$$(5 \cdot_{11} 9) \cdot_{11} x = 5 \cdot_{11} 5$$
$$x = 5 \cdot_{11} 5 = 25 (\bmod 11) = 3$$