Podzielność w pierścieniu liczb całkowitych

$\mathbb{Z}$ - zbiór liczb całkowitych

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ - zbiór liczb naturalnych

$\mathbb{Z}_+ = \{x \in \mathbb{Z} : x > 0\} = \{1, 2, 3, \ldots\}$

Dzielenie z resztą w $\mathbb{Z}$:

$x \in \mathbb{Z}$, $m \in \mathbb{Z}_+$ to istnieje dokładnie jedna para liczb całkowitych d i r taka, że

$x = d \cdot m + r$ i $r < m$ $\qquad r = r(x, m) = r_m(x) = r(x)$

$r \in \{0, 1, \ldots, m-1\} = \mathbb{Z}_m$

$r = 0$ to $m \mid x$

$p \in \mathbb{Z}_+$, $p > 1$ i $(m \mid p \Rightarrow m = 1$ lub $m = p)$

to $p \in P$ - zbiór liczb pierwszych

- $p \mid x \cdot y \Rightarrow p \mid x$ lub $p \mid y$ zasadnicze twierdzenie arytmetyki

Kongruencje:

$x, y \in \mathbb{Z}$ to $x \equiv y \mod m \iff m \mid x - y$

- $x \equiv r_m(x) \mod m$
- $x \equiv y \mod m$, $x_1 \equiv y_1 \mod m \Rightarrow$
  - $x + x_1 \equiv y + y_1 \mod m$
  - $x \cdot x_1 \equiv y \cdot y_1 \mod m$
  - $a \cdot x \equiv a \cdot y \mod m \quad a \in \mathbb{Z}$
  - $x^n \equiv y^n \mod m$

- Cechy podzielności przez 3, 9, 11

$10 \equiv 1 \mod 3$, $10 \equiv 1 \mod 9$ $\qquad 10 \equiv -1 \mod 11$

$10^s \equiv 1 \mod 3$, $10^s \equiv 1 \mod 9$ $\qquad 10^s \equiv (-1)^s \mod 11$

$x = \alpha_s \alpha_{s-1} \ldots \alpha_0 \qquad x = \alpha_s 10^s + \alpha_{s-1} 10^{s-1} + \ldots + \alpha_1 10 + \alpha_0$

$3 \mid x \iff 3 \mid \alpha_s + \ldots + \alpha_1 + \alpha_0$, $\quad 9 \mid x \iff 9 \mid \alpha_s + \ldots + \alpha_1 + \alpha_0$

$11 \mid x \iff 11 \mid (-1)^s a_s + (-1)^{s-1} a_{s-1} + \dots + a_0$

$\iff 11 \mid a_s - a_{s-1} + a_{s-2} - \dots$

Działania na resztach w $\mathbb{Z}_m$, $m \geq 2$.

$r, s \in \mathbb{Z}_m$ to $r + s = r +_m s = r_m(r+s)$

$r \cdot s = r \cdot_m s = r_m(r \cdot s)$

- $x, y \in \mathbb{Z}$ $\quad r_m(x+y) = r_m(x) + r_m(y)$

  $r_m(x \cdot y) = r_m(x) \cdot r_m(y)$

- $r + s = s + r$, $r \cdot s = s \cdot r$, $(r+s)+t = r+(s+t)$

  $r + 0 = 0 + r = r$, $r \cdot 1 = 1 \cdot r = r$, $r(s+t) = r \cdot s + r \cdot t$

$$-r := \begin{cases} 0, & r = 0 \\ m - r, & 1 \leq r \leq m-1 \end{cases}$$

$r + (-r) = (-r) + r = 0$

$-1 = m - 1$

- $m = 4$ $\quad \mathbb{Z}_4 = \{0, 1, 2, 3\}$ $\quad 2+2=0$, $2 \cdot 2 = 0$ $\quad 1+3 = 3+1 = 0$

r	r^2
0	0
1	1
2	0
3	1

r^2	s^2	$r^2 + s^2$
0	0	0
1	0	1
0	1	1
1	1	2

- $x \in \mathbb{N}$ $\quad x = y^2 + z^2$, $y, z \in \mathbb{Z}$

  $r(x) = r(y)^2 + r(z)^2$

  $r(x) = 3$ $\quad x = 4n+3$ to x nie jest sumą dwóch kwadratów

$x = 2n+1$, $x = y^2 + z^2$ to $r(x) = 1$

$x = 4k+1$

- Tw Fermata: $x = 4k+1 \in \mathbb{N}$ to $x = y^2 + z^2$ przy pewnych $y, z \in \mathbb{Z}$

Małe Twierdzenie Fermata:

$p \in P$, $r \in \mathbb{Z}_p \setminus \{0\} \Rightarrow r^{p-1} = 1$

$r \in \mathbb{Z}_p \Rightarrow r^p = r$

$p \nmid x \in \mathbb{N} \Rightarrow x^{p-1} \equiv 1 \mod p$

$x^p \equiv x \mod p$

Zadanie. Uzasadnić, że suma

$7 + 7^2 + 7^3 + \ldots + 7^{2020}$ jest podzielna przez 8

Rozwiązanie.

$7 \equiv -1 \mod 8 \Rightarrow 7^k \equiv (-1)^k \mod 8$

$7 + 7^2 + 7^3 + \ldots + 7^{2020} \equiv (-1) + (-1)^2 + \ldots + (-1)^{2020} \mod 8$

$(-1) + (-1)^2 + (-1)^3 + (-1)^4 + \ldots + (-1)^{2019} + (-1)^{2020} =$

$(-1+1) + (-1+1) + \ldots + (-1+1) = 0$

$(-1) = q \qquad q + q^2 + q^3 + \ldots + q^{2020} = q(1 + q + \ldots + q^{2019}) =$

$q \frac{q^{2020} - 1}{q - 1} = (-1) \frac{(-1)^{2020} - 1}{-2} = 0$

$7 + 7^2 + 7^3 + \ldots + 7^{2020} \equiv 0 \mod 8$

$q \neq 1 \qquad 1 + q + \ldots + q^n = \frac{q^{n+1} - 1}{q - 1}$

Zadanie.

$$n \in \mathbb{N} \Rightarrow 3 \mid n^3 + 3n^2 + 5n + 3$$

$$x = n^3 + 3n^2 + 3n + 2n + 3$$

$$r_3(x) = r_3(n)^3 + 2r_3(n) = r_3(n)\left(r_3(n)^2 + 2\right)$$

$r_3(n) = 0 \Rightarrow r_3(x) = 0$

$r_3(n) = 1 \Rightarrow r_3(x) = r_3(n)^2 + 2 = 0$

$r_3(n) = 2 \Rightarrow r_3(n)^2 = 1 \qquad r_3(x) = 0$

Zadanie.

$$m, n \in \mathbb{N} \quad \text{to} \quad 2 \mid m \cdot n \cdot (m - n)$$

$$x = m \cdot n \cdot (m - n) = m \cdot n(m + n) - 2 \cdot m \cdot n^2$$

$$r_2(x) = r_2\left(m \cdot n(m + n)\right)$$

$$= r_2(m)^2 \cdot r_2(n) + r_2(n) \cdot r_2(n)^2$$

$$= r_2(m) \cdot r_2(n) + r_2(n) \cdot r_2(n) = 0$$

$$r \in \mathbb{Z}_2 \Rightarrow r^2 = r$$

- $r, s \in \mathbb{Z}_2 \qquad r \cdot_2 s = r \cdot s$

$$r +_2 s = (r - s)^2$$

Zadanie. Wykazać, że nie istnieje $n \in \mathbb{N}$ dla którego $n^2 + 6n + 14$ jest kwadratem liczby całkowitej

Rozwiązanie.

Przypuśćmy, że dla pewnego $n \in \mathbb{N}$ i $m \in \mathbb{Z}$

$$n^2 + 6n + 14 = m^2$$

czyli

$$n^2 + 6n + 14 = n^2 + 2 \cdot n \cdot 3 + 3^2 + 5 = (n+3)^2 + 5 = m^2$$

$$k = n + 3 \Rightarrow k \geq 3$$

$$k^2 + 5 = m^2$$

$$5 = m^2 - k^2 = (m-k)(m+k)$$

$$5 \in \mathbb{P} \Rightarrow \begin{matrix} m+k = 5 \\ m-k = 1 \end{matrix} \Leftrightarrow \begin{matrix} m = 3 \\ k = 2 \end{matrix}$$ - sprzeczność

Zadanie. Znaleźć rozwiązania równania

$x^2 + y^2 = 7z^2$ w liczbach całkowitych.

Rozwiązanie.

$t \in \mathbb{N}$, $r(t) = r(t,7)$

$r(x)^2 + r(y)^2 = r(7) \cdot r(z)^2 = 0$

$r(t)$	$r(t)^2$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

$r(x)^2 = r(y)^2 = 0 \Rightarrow r(x) = r(y) = 0$

$x = 7x_1$, $y = 7y_1$

$7 \mid x^2 \Rightarrow 7 \mid x$

$x = 0, y = 0, z = 0$ jest rozwiązaniem

Gdyby istniało rozwiązanie dla $z \neq 0$ to niech z_0 będzie najmniejszą liczbą całkowitą dodatnią taką, że $x^2 + y^2 = 7z_0^2$

$49x_1^2 + 49y_1^2 = 7z_0^2$

$7(x_1^2 + y_1^2) = z_0^2 \Rightarrow 7 \mid z_0$ $z_0 = 7z_1$

$49x_1^2 + 49y_1^2 = 7 \cdot 49 z_1^2 \Rightarrow x_1^2 + y_1^2 = 7z_1^2$

$0 < z_1 < z_0$ – sprzeczność

Ćwiczenie. Sprawdzić, że podobna sytuacja będzie miała miejsce dla równania

$x^2 + y^2 = pz^2$, jeśli $p \in \{3, 11\}$

Zadanie. $x \in \mathbb{N}$ to x "ślimna" gdy $x = y^2 + z^2$, $y, z \in \mathbb{Z}$

n "ślimna" to $5 \cdot n$ "ślimna" ?

Rozwiązanie. n, m "ślimne" $\Rightarrow$ $n \cdot m$ "ślimna"

$n = x^2 + y^2$, $m = u^2 + v^2$

$n \cdot m = (x^2 + y^2)(u^2 + v^2) = \cancel{x^2 \cdot y^2 + x^2 v^2 +}$

$= (xu)^2 + (yu)^2 + (xv)^2 + (yv)^2$

$= (xu)^2 + (yv)^2 + (xv)^2 + (yu)^2$

$= (xu)^2 + (yv)^2 + 2xuyv + (xv)^2 + (yu)^2 - 2xvyu$

$= (xu + yv)^2 + (xv - yu)^2$

$5 = 1^2 + 2^2$ $\quad m = 5$

- $n = |x + yi|^2$, $m = |u + vi|^2$, $i = \sqrt{-1}$

$n \cdot m = |(x + yi)(u + vi)|^2$

$= |(xu - yv) + (xv + yu)i|^2$

Zadanie. Znaleźć liczbę czterocyfrową, której pierwsze cyfry są jednakowe, dwie ostatnie są jednakowe i która jest kwadratem liczby całkowitej.

Rozwiązanie.

$$x = 1000a + 100a + 10b + b = c^2$$

$y \in \mathbb{N} \quad r(y) = r(y, 10)$

$r(y)$	$r(y)^2$
0	0
1	1
2	4
3	9
4	6
5	5
6	6
7	9
9	1

$$b = r(x) = r(c)^2 \in \{0, 1, 4, 5, 6, 9\}$$

$$x = 1100a + 11b = 11(100a + b) = c^2$$

$$11 \mid 100a + b = 99a + a + b \Rightarrow 11 \mid a + b$$

$$0 < a + b \leq 18 \Rightarrow a + b = 11 \Rightarrow b \in \{4, 5, 6, 9\}$$

$b = 4 \quad a = 7 \quad 7744 : 121 = 64 = 8^2$

$b = 5 \quad a = 6 \quad 6655 : 121 = 55$

$b = 6 \quad a = 5 \quad 5566 : 121 = 46$

$b = 9 \quad a = 2 \quad 2299 : 121 = 19$

$$\boxed{x = 7744}$$

Zadanie.

$x_1 = 2020$

$x_{n+1} = 2020^{x_n}$

Obliczyć $r_{18}(x_n)$ oraz $r_{19}(x_n)$, $n = 1, 2, \ldots$

$2020 = (101 \cdot 20) = 101 \cdot 18 + 2 \cdot 101 = 101 \cdot 18 + 2(90 + 11)$

$2020 = 101 \cdot 19 + 101 = 112 \cdot 18 + 4$

$= 106 \cdot 19 + 6$

$r_{18}(x_1) = 4 \qquad r_{19}(x_1) = 6$

$x_2 = 2020^{112 \cdot 18 + 4}$

$r_{19}(x_2) = r_{19}(2020)^{112 \cdot 18 + 4} = 6^{112 \cdot 18 + 4}$

$= (6^{18})^{112} \cdot 6^4$ $\qquad p = 19 \in \mathbb{P}$ MTF $\Rightarrow$

$= 1^{112} \cdot 6^4$

$= 4$ $\qquad 6^2 = 36 \equiv -2 \mod 19$

$r_{18}(x_2) = 4^{112 \cdot 18 + 4}$

w $\mathbb{Z}_{18}$ mamy: $4^{18} = 10$, $10^k = 10$, $4^4 = 4$

$r_{18}(x_2) = 10 \cdot 4^4 = 10 \cdot 4 = 4$

$x_n \equiv 4 \mod 18 \Rightarrow x_{n+1} \equiv 4 \mod 18$

$x_n = k \cdot 18 + 4$

$r_{19}(x_{n+1}) = 6^{k \cdot 18 + 4} = (6^{18})^k \cdot 6^4 = 6^4 = 4$

$r_{18}(x_n) = 4$, $n \geq 1$

$r_{19}(x_1) = 6$, $r_{19}(x_n) = 4$, $n \geq 2$