Задача Да се намери противоположното число

$-\frac{4}{7} = 7 - 4 = \boxed{3}$

Зад 2. Да се провери има ли $\overline{3}$ обратен елемент в $\mathbb{Z}_5$ и $\mathbb{Z}_6$.

$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

в $\mathbb{Z}_5$ $\overline{3}.\overline{1} = \overline{3}$ $\overline{3}.\overline{2} = \overline{6} = \overline{1}$ $\Rightarrow$ $\overline{3} = \overline{2}^{-1}$ обратен

в $\mathbb{Z}_6$ $\overline{3}.\overline{1} = \overline{3}$ $\overline{3}.\overline{2} = \overline{6}$ $\overline{3}.\overline{3} = \overline{3}$ $\overline{3}.\overline{4} = \overline{0}$ $\overline{3}.\overline{5} = \overline{3}$

$\Rightarrow$ няма обратен елемент

Зад3 Да се намерят обратимите елементи и делителите на нулата в $\mathbb{Z}_6$

$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$

обратими са: $\overline{1} \cdot \overline{1} = \overline{1}$ $\overline{5} \cdot \overline{5} = \overline{25} = \overline{1}$ ...

делителей на нуля $\bar{2}\cdot\bar{3}=\bar{0}$ $\bar{3}\bar{4}=\bar{0}$

$\mathbb{Z}_5 \Rightarrow$ обратими са $\varphi(5)=4 \Rightarrow \bar{1}, \bar{2}, \bar{3}, \bar{4}$

Задача 4. Да се пресметне:

а) $\overline{A} = \overline{5} \cdot \overline{3} + \overline{4} \cdot \overline{5} - \overline{2}$

б) $\overline{B} = \overline{21} \cdot \overline{3}^2 - \overline{46} \cdot \overline{2}^3 \cdot \overline{25}$

а) $\overline{A} = \overline{15} + \overline{20} + (-\overline{2}) = \overline{3} + \underbrace{\overline{2} + (-\overline{2})}_{0} = \overline{3}$

б) $\overline{3}^2 = \overline{9} = \overline{3} \Rightarrow \overline{21} \cdot \overline{3} = \overline{63} = \overline{3}$

$\overline{2}^3 = \overline{8} = \overline{2} \Rightarrow \overline{46} \cdot \overline{2}^3 = \overline{46} \cdot \overline{2} = \overline{92} = \overline{2}$

$\overline{25} = \overline{10} = \overline{4}$

$\overline{B} = \overline{3} - \overline{2} + \overline{4} = \overline{1} + \overline{4} = \overline{5}$

Зад 5. Да се намери стойността на полинома $F(x) = x^4 + 5x^3 + 6x^2 + x + 8$ над $\mathbb{Z}_9$ за $x = \overline{3}$ и $x = \overline{7}$

Използвайте схемата на Хорнер, за да пресметнем по-бързо горепосочената стойност на полинома

	$\overline{1}$	$\overline{5}$	$\overline{6}$	$\overline{1}$	$\overline{8}$
$\overline{3}$	$\overline{1}$	$\overline{3}+\overline{5}=\overline{8}$	$\overline{24}+\overline{6}=\overline{30}$	$\overline{9}+\overline{1}=\overline{10}=\overline{1}$	$\overline{3}+\overline{8}=\overline{11}=\overline{2}$
$\overline{7}$	$\overline{1}$	$\overline{7}+\overline{5}=\overline{12}$	$\overline{21}+\overline{6}=\overline{27}$	$\overline{0}+\overline{1}=\overline{1}$	$\overline{7}+\overline{8}=\overline{15}=\overline{6}$

$F(\overline{3}) = \overline{2}$

$F(\overline{7}) = \overline{6}$

Зад 6. Да се намерят частните на полинома $F(x) = x^4 - 12x^3 + 50x^2 - 84x + 45$ над $\mathbb{Z}$

$-12 \equiv 2 \pmod 7$ $\quad 50 \equiv 1 \pmod 7$ $\quad -84 \equiv 0 \pmod 7$ $\quad 45 \equiv 3 \pmod 7$

$\boxed{F(x) = x^4 + 2x^3 + x^2 + 3}$

диофр. по-големи от mod

Задача 7. Да се намери обратният елемент на $\overline{4}$ в $\mathbb{Z}_{33}$

$$4^{-1} = 4^{\varphi(33)-1} \pmod{33}$$

$$\varphi(33) = \varphi(3 \cdot 11) = \varphi(3) \cdot \varphi(11) = 2 \cdot 10 = 20$$

$$4^{-1} = 4^{19} \pmod{33}$$

$$4^3 \equiv 64 \equiv -2 \pmod{33} \quad /^6$$

$$4^{18} \equiv 2^6 = 64 \equiv -2 \pmod{33} \quad \cdot 4$$

$$4^{19} \equiv -8 \equiv 25 \pmod{33}$$

$$4^{-1} \equiv 25 \pmod{33}$$

Зад8. Да се намери обратния елемент на $\overline{73}$ в множеството на класовете остатъци $\mathbb{Z}_{79}$

$$(73, 79) = 1$$

$79 = 73 \cdot 1 + 6 \Rightarrow 6 = 79 - 73$

$73 = 6 \cdot 12 + 1 \Rightarrow 1 = 73 - 6 \cdot 12$

$6 = 1 \cdot 6 + 0$

$1 = 73 - (6 \cdot 12)$

$1 = 73 - (79 - 73) \cdot 12 = 13 \cdot 73 - 12 \cdot 79$

$13 \cdot 73 = 1 + 12 \cdot 79$

$13 \cdot 73 \equiv 1 \pmod{79}$

$\overline{13}$ е обр ел на $\overline{73}$ в $\mathbb{Z}_{79} \Rightarrow \overline{73}^{-1} = \overline{13}$

Решаване на алгебрични сравнения с едно неизвестно с използването на обратен елемент

Зад1. Да се реши сравнението $192x \equiv 89 \pmod{79}$

$152 \equiv 73 \pmod{79}$ $89 \equiv 10 \pmod{79} \Rightarrow$

$152x \equiv 89 \pmod{79} \Leftrightarrow 73x \equiv 10 \pmod{79}$

$a = 73 \quad b = 10 \quad m = 79$

$(73, 79) = 1$ → има единствено решение и има вида:

$x \equiv a^{-1} b \pmod m$

$x \equiv 73^{-1} \cdot 10 \pmod{79}$

$x \equiv 13 \cdot 10 \pmod{79}$

$x \equiv 130 \pmod{79}$

$x \equiv 51 \pmod{79}$

$\overline{51}$ в $\mathbb{Z}_{79}$