Aufgabe 8.2 Untersuchen Sie in 1) bzw 2), ob die angegebene Kongruenz lösbar ist, und finden Sie gegebenenfalls eine Lösung.

1) $2x^2 + x \equiv 4 \pmod{10}$

2) $37\,x \equiv 1 \pmod{159}$

3) Welches sind die Einheiten in $(\mathbb{Z}_{12}, +, \cdot)$? Ist $(E(\mathbb{Z}_{12}), \cdot)$ zyklisch?

2) $z := 37 \cdot x$

$160 \equiv 1 \pmod{159}$

$z \equiv 1 \pmod{159}$

$z \equiv 0 \pmod{37}$

$\underset{a_1}{37} = \underset{a_2}{0} \cdot 159 + \underset{a_3}{37}$

$\underset{a_2}{159} = \_\_ \cdot \underset{a_3}{37} + \_\_$

$a_1 = 159 \qquad a_2 = 37$

$\underset{a_1}{159} = \underline{4} \cdot \underset{a_2}{37} + \underline{11} =: a_3$

$\underset{a_2}{37} = \underline{3} \cdot \underset{a_3}{11} + \underline{4} = a_4$

$\underset{a_3}{11} = \underline{2} \cdot \underset{a_4}{4} + 3 = a_5$

$\underset{a_4}{4} = \underline{1} \cdot \underset{a_5}{3} + 1 =: a_6$

$\underset{a_5}{3} = 3 \cdot a_6 + 0$

der letzte Rest $\neq 0$ ist ggT $\Rightarrow ggT(159, 37) = 1$

$$\begin{aligned}
1 = a_6 &= a_4 - a_5 = \\
&= a_4 - (a_3 - 2 \cdot a_4) = \\
&= 3a_4 - a_3 = \\
&= 3 \cdot (a_2 - 3a_3) - a_3 = \\
&= 3a_2 - 10\,a_3 = \\
&= 3a_2 - 10 \cdot (a_1 - 4a_2) \\
&= -10a_1 + 43a_2
\end{aligned}$$

$\Rightarrow 1 = -10 \cdot 159 + 43 \cdot 37 \quad | + 10 \cdot 159$

$1 + 10 \cdot 159 = 43 \cdot 37 =: z$

$z \equiv 1 \bmod 159$

$z \equiv 0 \bmod 37$

$z \equiv 1 + 10 \cdot 159 \equiv 1 \pmod{159}$

$z \equiv 43 \cdot 37 \equiv 0 \pmod{37}$

$(1 + 10 \cdot 159) : 159 = \underline{10}\ R\ \underline{1}$

$z = 37 \cdot x = 43 \cdot 37$

$\Rightarrow x = 43$

1) $\phi(1\ldots$

miro

$\Rightarrow x = 43$

$$|E(\mathbb{Z}/n\mathbb{Z})| = |\{a \in \{1, \dots, n\} : ggT(a,n) = 1\}| = \phi(n)$$

Aufgabe 7.4

1) Bestimmen Sie $\phi(1485)$.

2) Zeigen Sie, dass für all $k \in I\!N$ gilt: $\phi(10^k) = 4 \cdot 10^{k-1}$.

$$\boxed{\begin{array}{l} m, n \in \mathbb{Z} \text{ teilerfremd} \\ 1)\ \phi(m \cdot n) = \phi(m) \cdot \phi(n) \\ p \text{ primzahl}, n \in \mathbb{N} \\ 2)\ \phi(p^n) = (p-1) \cdot p^{n-1} \end{array}}$$

$1485 : 5 = 297$
-10
48
-45
35
-35
0

$q(297) = 18$

$297 : 9 = 33$
-27
27
-27
0

$$1)\ \phi(1485) =$$
$$= \phi(5 \cdot 297) =$$
$$= \phi(5 \cdot 9 \cdot 33)$$
$$= \phi(5 \cdot 9 \cdot 3 \cdot 11)$$
$$= \phi(5 \cdot 3^3 \cdot 11) = \phi(5) \cdot \phi(3^3) \cdot \phi(11) =$$
$$= 4 \cdot \underbrace{5^0}_{=1} \cdot 2 \cdot 3^2 \cdot 10 \cdot \underbrace{11^0}_{=1} =$$
$$= (4 \cdot 2) \cdot 3^2 \cdot 10 = 72 \cdot 10 = 720$$

Bsp.:

$\phi(5^7) = 4 \cdot 5^6$

$\phi(11^{100}) = 10 \cdot 11^{99}$

$\phi(29) = \phi(29^1) = (29-1) \cdot 29^{1-1}$

$$\boxed{\phi(p) = p - 1}$$

Aufgabe 7.4

1) Bestimmen Sie $\phi(1485)$.

2) Zeigen Sie, dass für all $k \in I\!N$ gilt: $\phi(10^k) = 4 \cdot 10^{k-1}$.

$$\boxed{\begin{array}{l} m, n \in \mathbb{Z} \text{ teilerfremd} \\ 1)\ \phi(m \cdot n) = \phi(m) \cdot \phi(n) \\ p \text{ primzahl}, n \in \mathbb{N} \\ 2)\ \phi(p^n) = (p-1) \cdot p^{n-1} \end{array}}$$

$$2)\ \phi(10^k) = \phi((2 \cdot 5)^k) =$$
$$= \phi(2^k \cdot 5^k) = \phi(2^k) \cdot \phi(5^k) =$$
$$= 1 \cdot 2^{k-1} \cdot (5-1) \cdot 5^{k-1} =$$
$$= 2^{k-1} \cdot 4 \cdot 5^{k-1} = 4 \cdot (2 \cdot 5)^{k-1} = 4 \cdot 10^{k-1}$$

$\square$

$$\boxed{(a \cdot b)^n = a^n \cdot b^n}$$

miro

Aufgabe 7.5 Untersuchen Sie, ob folgende Kongruenz stimmt.

$$14^{98} + 8 \equiv 0 \pmod{51}$$

7.11 Satz:
1) Euler: Für $a, n \in \mathbb{N}$ mit $\operatorname{ggT}(a,n) = 1$ gilt:
ca 1760
$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Zu zeigen: $14^{98} \equiv -8 \pmod{51}$

$$\varphi(51) = \varphi(3 \cdot 17) = \varphi(3) \cdot \varphi(17) = 2 \cdot 16 = 32$$

$$14^{32} = 14^{\varphi(51)} \equiv 1 \pmod{51}$$

Euler (Satz 7.11)

$$14^{98} \equiv 14^{3 \cdot \overset{\varphi(51)}{32} + 2} \equiv 14^{3 \cdot 32} \cdot 14^2 \equiv (14^{32})^3 \cdot 14^2 \equiv 1^3 \cdot 14^2 \equiv 196 \equiv 43 \equiv \underbrace{(43-51)}_{=-8} \pmod{51}$$

$$\boxed{a^{n+m} = a^n \cdot a^m}$$

$$a^{n \cdot m} = (a^n)^m$$

$\Rightarrow$ Die Kongruenz stimmt!

$$196 : 51 = 3 \text{ R } 43$$
$$\begin{array}{r} 196 \\ -153 \\ \hline 43 \end{array}$$

$$14^{2021} \pmod{51} \equiv$$

Mit Euler!!