Alternativ-Blatt

1. Teil

a)

Sei $p > 3$ prim. Ist $p \equiv a \bmod m$ und $(p, m) = 1$, dann gilt $(a, m) \mid a$ und $(a, m) \mid m$ und somit $(a, m) \mid p$. Wegen $(p, m) = 1$ ist außerdem $p \nmid m$, d. h. $p \neq (a, m)$.
Folglich ist, da p prim ist,

$$(a, m) = 1 \tag{1}$$

Da alle in dieser Aufgabe auftretenden Werte für m keine Primteiler größer als 3 besitzen und $p > 3$, können alle a, für die $(a, m) \neq 1$, als Lösung ausgeschlossen werden.

I) Es gilt

$$\left(\frac{-1}{p}\right) = 1 \overset{2.2.2}{\iff} p \equiv 1 \bmod 4 \iff p \equiv \underline{1}, 5 \bmod 8$$
$$\left(\frac{-1}{p}\right) = -1 \overset{2.2.2}{\iff} p \equiv 3 \bmod 4 \iff p \equiv \underline{3}, 7 \bmod 8$$
$$\left(\frac{2}{p}\right) = 1 \overset{2.2.3}{\iff} p \equiv \underline{1}, 7 \bmod 8$$
$$\left(\frac{2}{p}\right) = -1 \overset{2.2.3}{\iff} p \equiv \underline{3}, 5 \bmod 8$$

Also ist

$$\left(\frac{-2}{p}\right) = 1 \iff \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \iff \left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \pm 1 \iff p \equiv 1, 3 \bmod 8$$

II) Es gilt

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 & p \equiv 1 \bmod 3 \\ \left(\frac{2}{3}\right) = -1 & p \equiv 2 \bmod 3 \end{cases}$$

und deshalb

$$\left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \bmod 3 \overset{(1)}{\iff} p \equiv \underline{1}, 7 \bmod 12$$
$$\left(\frac{p}{3}\right) = -1 \iff p \equiv 2 \bmod 3 \overset{(1)}{\iff} p \equiv 5, \underline{11} \bmod 12$$
$$(-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1 \bmod 4 \overset{(1)}{\iff} p \equiv \underline{1}, 5 \bmod 12$$
$$(-1)^{\frac{p-1}{2}} = -1 \iff p \equiv 3 \bmod 4 \overset{(1)}{\iff} p \equiv 7, \underline{11} \bmod 12$$

Also ist

$$\left(\frac{3}{p}\right) = 1 \overset{\text{QRG}}{\iff} (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = 1 \iff (-1)^{\frac{p-1}{2}} = \left(\frac{p}{3}\right) = \pm 1 \iff p \equiv 1, 11 \bmod 12$$

III) Es gilt

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \bmod 4 \iff p \equiv \underline{1}, 5 \bmod 12$$
$$\left(\frac{-1}{p}\right) = -1 \iff p \equiv 3 \bmod 4 \iff p \equiv \underline{7}, 11 \bmod 12$$
$$\left(\frac{3}{p}\right) = 1 \iff p \equiv \underline{1}, 11 \bmod 12$$

$$\left(\frac{3}{p}\right) = -1 \iff p \equiv 5, \underline{7} \mod 12$$

Also ist

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{-1}{p}\right) = \left(\frac{3}{p}\right) = \pm 1 \iff p \equiv 1, 7 \mod 12 \iff p \equiv 1 \mod 6$$

IV) Es gilt

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \mod 8 \iff p \equiv \underline{1}, 11, 17, \underline{19} \mod 24$$
$$\left(\frac{-2}{p}\right) = -1 \iff p \equiv 5, 7 \mod 8 \iff p \equiv \underline{5}, 7, 13, \underline{23} \mod 24$$
$$\left(\frac{-3}{p}\right) = 1 \iff p \equiv 1 \mod 6 \iff p \equiv \underline{1}, 7, 13, \underline{19} \mod 24$$
$$\left(\frac{-3}{p}\right) = -1 \iff p \equiv 5 \mod 6 \iff p \equiv \underline{5}, 11, 17, \underline{23} \mod 24$$

Also ist

$$\left(\frac{6}{p}\right) = 1 \iff \left(\frac{-2}{p}\right) = \left(\frac{-3}{p}\right) = \pm 1 \iff p \equiv 1, 5, 19, 23 \mod 24$$

V) Es gilt

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1, 3 \mod 8 \iff p \equiv \underline{1}, \underline{11}, 17, 19 \mod 24$$
$$\left(\frac{-2}{p}\right) = -1 \iff p \equiv 5, 7 \mod 8 \iff p \equiv \underline{5}, \underline{7}, 13, 23 \mod 24$$
$$\left(\frac{3}{p}\right) = 1 \iff p \equiv 1, 11 \mod 12 \iff p \equiv \underline{1}, \underline{11}, 13, 23 \mod 24$$
$$\left(\frac{3}{p}\right) = -1 \iff p \equiv 5, 7 \mod 12 \iff p \equiv \underline{5}, \underline{7}, 17, 19 \mod 24$$

Also ist

$$\left(\frac{-6}{p}\right) = 1 \iff \left(\frac{-2}{p}\right) = \left(\frac{3}{p}\right) = \pm 1 \iff p \equiv 1, 5, 7, 11 \mod 24$$

b)

Im Folgenden sei p ein Primteiler von $n^8 - n^4 + 1$. Behauptung: Sei $n \in \mathbb{N}$. Dann ist jeder prime Teiler p von $z := n^8 - n^4 + 1$ kein Teiler der Zahlen n^2, $n^3 + n$ und $n^3 - n$. Außerdem existieren $a, b, c \in \mathbb{N}$ mit

$$an^2 \equiv 1 \mod p \tag{2}$$
$$b\left(n^3 + n\right) \equiv 1 \mod p \tag{3}$$
$$c\left(n^3 - n\right) \equiv 1 \mod p \tag{4}$$

Beweis: Es gilt

$$p \nmid n^8 - n^4 = n^2\left(n^6 - n^2\right) = n^2\left(n^3 + n\right)\left(n^3 - n\right)$$
$$\Longrightarrow p \nmid n^2 \,, \quad p \nmid n^3 + n \quad \text{und} \quad p \nmid n^3 - n$$

Definiere nun $\tilde{a} := n^6 - n^2$, $\tilde{b} := n^5 - n^3$ und $\tilde{c} := n^5 + n^3$, dann ist

$$\tilde{a}n^2 = \left(n^6 - n^2\right)n^2 = z - 1 \equiv -1 \mod p$$
$$\tilde{b}\left(n^3 + n\right) = n^2\left(n^3 - n\right)\left(n^3 + n\right) = z - 1 \equiv -1 \mod p$$
$$\tilde{c}\left(n^3 - n\right) = n^2\left(n^3 + n\right)\left(n^3 - n\right) = z - 1 \equiv -1 \mod p$$

Setze nun $a := \tilde{a}\,(z-1)$, $b := \tilde{b}\,(z-1)$ und $c := \tilde{c}\,(z-1)$, dann ist

$$an^2 = b\left(n^3 + n\right) = c\left(n^3 - n\right) = (z-1)^2 \equiv 1 \mod p$$

2. Teil

Behauptung: Es gilt

$$\left(an^4 - a\right)^2 + 1 \equiv 0 \mod p \tag{5}$$

$$\left(bn^4 + bn^2 + b\right)^2 - 2 \equiv 0 \mod p \tag{6}$$

$$\left(cn^4 - cn^2 + c\right)^2 + 2 \equiv 0 \mod p \tag{7}$$

$$\left(an^4 + a\right)^2 \equiv 3 \mod p \tag{8}$$

$$\left(2n^4 - 1\right)^2 \equiv -3 \mod p \tag{9}$$

$$\left(bn^4 + 3bn^2 + b\right)^2 \equiv 6 \mod p \tag{10}$$

$$\left(cn^4 - 3cn^2 + c\right)^2 \equiv -6 \mod p \tag{11}$$

Für jeden Primteiler p von $n^8 - n^4 + 1$ gilt

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-6}{p}\right) = 1$$

und $p \equiv 1 \mod 24$.
Beweis:Aus $z = \left(x^4 - 1\right)^2 + \left(x^2\right)^2$ folgt

$$\left(an^4 - a\right)^2 + 1 \overset{(2)}{\equiv} \left(an^4 - a\right)^2 + \left(an^2\right)^2 = a^2\left(n^4 - 1\right)^2 + a^2\left(n^2\right)^2 = a^2 z \equiv 0 \mod p$$

Aus $z = \left(x^4 + x^2 + 1\right)^2 - 2\left(x^3 + x\right)^2$ folgt

$$\left(bn^4 + bn^2 + b\right)^2 - 2 \overset{(3)}{\equiv} b^2\left(n^4 + n^2 + 1\right)^2 - 2b^2\left(n^3 + n\right)^2 = b^2 z \equiv 0 \mod p$$

Aus $z = \left(x^4 - x^2 + 1\right)^2 + 2\left(x^3 - x\right)^2$ (die Gleichung auf dem Aufgabenblatt ist falsch!) folgt

$$\left(cn^4 - cn^2 + c\right)^2 + 2 \overset{(4)}{\equiv} c^2\left(n^4 - n^2 + 1\right)^2 + 2c^2\left(n^3 - n\right)^2 = c^2 z \equiv 0 \mod p$$

Aus $z = \left(x^4 + 1\right)^2 - 3\left(x^2\right)^2$ folgt

$$\left(an^4 + a\right)^2 \overset{(2)}{\equiv} a^2\left(n^4 + 1\right)^2 = a^2\left(z + 3\left(n^2\right)^2\right) \equiv 3\left(an^2\right)^2 \equiv 3 \mod p$$

Aus $z = \left(x^4 - \frac{1}{2}\right)^2 + 3\left(\frac{1}{2}\right)^2$ folgt

$$\left(2n^4 - 1\right)^2 = 2^2\left(n^4 - \frac{1}{2}\right)^2 = 2^2\left(z - 3\left(\frac{1}{2}\right)^2\right) \equiv -3 \mod p$$

Aus $z = \left(x^4 + 3x^2 + 1\right)^2 - 6\left(x^3 + x\right)^2$ folgt

$$\left(bn^4 + 3bn^2 + b\right)^2 = b^2\left(n^4 + 3n^2 + 1\right)^2 = b^2 z + 6b^2\left(n^3 + n\right)^2 \overset{(3)}{\equiv} 6 \mod p$$

Aus $z = \left(x^4 - 3x^2 + 1\right)^2 + 6\left(x^3 - x\right)^2$ folgt

$$\left(cn^4 - 3cn^2 + c\right)^2 = c^2\left(n^4 - 3n^2 + 1\right)^2 = c^2 z - 6c^2\left(n^3 - n\right)^2 \overset{(4)}{\equiv} -6 \mod p$$

Wegen (5) bis (11) existiert für jedes $k \in \{-1, 2, -2, 3, -3, 6, -6\}$ eine natürliche Zahl, deren Quadrat äquivalent k modulo p ist (z. B. $an^4 - a$ im Falle $k = -1$). Daher sind definitionsgemäß alle $k \in \{-1, 2, -2, 3, 6, -6\}$ quadratische Reste modulo p, d. h.

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-6}{p}\right) = 1$$

Wegen II), IV) und V) gilt daher

$$p \equiv 1, 11 \mod 12 \quad \text{bzw.} \quad p \equiv 1, 11, 13, 23 \mod 24$$

$$\text{und} \quad p \equiv 1, 5, 19, 23 \mod 24$$

$$\text{und} \quad p \equiv 1, 5, 7, 11 \mod 24$$

Also $p \equiv 1 \mod 24$