1. Zum Beispiel: $x = \frac{23}{35}, \quad y = \frac{23}{34}$

2. Da verlangt wird, dass $\left(\frac{3}{q}\right) \neq \left(\frac{q}{3}\right)$ gilt, muss $q \equiv 3 \mod 4$ sein. Wir untersuchen also diese Primzahlen $q > 3$ der Reihe nach.
Zuerst $q = 7$. Wegen $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = -1$ ist 3 kein quadratischer Rest modulo q.
Dann $q = 11$. Es ist $\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = 1$. Demnach ist $q = 11$ die gesuchte Zahl.

3. Zum Beispiel: $x = 18, \quad y = 13$.

4.

$$\begin{array}{llll} x_1 = 13 & x_2 = 12 & x_4 = 12 & x_7 = 9 \\ & x_3 = 5 & x_5 = 4 & x_8 = 6 \\ & & x_6 = 3 & x_9 = 6 \\ & & & x_{10} = 4 \end{array}$$

5. Seien $p_1, \ldots, p_t$ Primzahlen mit $p_i \equiv 3 \mod 4$ für $1 \leq i \leq t$. Bilde $m = 4p_1 \cdots p_t - 1$. Schreibe $m = q_1 \cdots q_s$ mit Primzahlen q_j. Da m ungerade ist, sind alle q_j ungerade. Wäre $q_j \equiv 1 \mod 4$ für alle i, so wäre $m = q_1 \cdots q_s \equiv 1 \cdots 1 = 1 \mod 4$, aber $m \equiv 3 \mod 4$. Also ist $q_j \equiv 3 \mod 4$ für mindestens ein j. Wäre $q_j = p_i$ für ein i, so wäre q_j ein Teiler von $4p_1 \cdots p_t - m = 1$, unmöglich. Also ist q_j eine neue Primzahl mit der gewünschten Eigenschaft.

6.

$$\begin{array}{lll} a_1 = -1 & a_2 = 1 & a_3 = -1 \\ b_1 = 1 & b_2 = -1 & b_3 = -1 \\ c_1 = -1 & c_2 = -1 & c_3 = 1 \end{array}$$

(oder Vertauschung der Zeilen).

7. 40.

8. Sei $\tau(n)$ die Anzahl der Teiler von $n = p_1^{e_1} \cdots p_t^{e_t}$ mit Primzahlen $p_1 < p_2 < \cdots < p_t$ und natürlichen Zahlen e_i. Es ist $\tau(n) = (e_1 + 1) \cdots (e_t + 1)$. Also gilt: Genau dann ist $\tau(n)$ ungerade, wenn alle Zahlen $e_i + 1$ ungerade sind, also wenn alle Zahlen e_i gerade sind, aber dies ist genau dann der Fall, wenn n Quadratzahl ist.

9. Nach Definition ist $f(1) = 0$. Für jede multiplikative Funktion g gilt aber $g(1) = 1$.

10. 5, 8, 10, 12.

11. $2^{47} \equiv 7 \mod 143$, also ist 7 der Klartext.

12.

$$
\begin{aligned}
n = 5 \qquad & \mu(\frac{5!}{5!}) = 1, \\
n = 6 \qquad & \mu(\frac{6!}{5!}) = 1, \\
n = 7 \qquad & \mu(\frac{7!}{5!}) = -1, \\
n \geq 8 \qquad & \mu(\frac{n!}{5!}) = 0 \quad \text{für} \quad n \geq 8.
\end{aligned}
$$

13. Sei $t = \pi(n)$, sei p_i die i-te Primzahl. Sei $x \leq n$ eine natürliche Zahl. Schreibe sie in der Form $x = p_1^{e_1} \cdots p_t^{e_t} y^2$, wobei $y \in \mathbb{N}$ und jedes e_i Null oder Eins ist. Es ist $y \leq \sqrt{n}$. Es gibt 2^t mögliche Folgen $(e_1, \ldots, e_t)$. Insgesamt gibt es also für x höchstens $2^t \cdot \sqrt{n}$ Möglichkeiten.

14. Wegen $\left(\frac{2}{q}\right)$ gibt es eine natürliche Zahl x mit $x^2 \equiv 2 \mod q$. Also gilt: $2^n \equiv x^{2n} = x^{q-1}$ und $x^{q-1} \equiv 1 \mod q$ nach dem kleinen Fermat. Wir sehen also $2^n - 1 \equiv 0 \mod q$.

15.

$\overline{a}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
Ordnung	1	10	5	5	5	10	10	10	5	2

16. 26.

17. Nach dem Satz von Tschebyscheff gibt es es für $n \geq 2$ eine Primzahl p mit $n \leq p < 2n$. Wende dies auf $n = 10^e$ an. Wir erhalten eine Primzahl p mit $10^e \leq p < 2 \cdot 10^e$.

18.

p	11	29	31	59	61	79
J/N	J	N	N	J	J	J

Bemerkungen.

3. Wie findet man dieses Beispiel? Offensichtlich ist $N(4+i) = 17$, und $N(5+2i) = 29$, also nimm $z = (4+i)(5+2i)$. Eine andere Lösung ist $x = 22, \quad y = 3$.

4. Wie findet man dieses Beispiel? Das muss man kennen.

7. $\phi(\phi(101)) = \phi(100) = \phi(4)\phi(25) = 2 \cdot 20 = 40$.

8. Es gibt einen anderen (einfacheren?) Beweis: Ist d Teiler von n, so auch $d' = n/d$. Die Teiler d von n mit $d < \sqrt{n}$ entsprechen auf diese Weise bijektiv den Teilern d' mit $\sqrt{n} < d'$. Es gibt also zwei Fällen: diese Teiler d, d' sind alle Teiler — dann ist die Anzahl der Teiler von n gerade und n ist keine Quadratzahl. Oder aber auch $\sqrt{n}$ ist ein Teiler — dann ist die Anzahl der Teiler von n ungerade und n ist eine Quadratzahl.

10. Man zeigt als erstes: die einzigen möglichen Primpotenzteiler sind $1, 2, 4, 8, 3, 5$.

12. $\frac{n!}{5!} = 1,\ 2 \cdot 3,\ 2 \cdot 3 \cdot 7$ für $n = 5, 6, 7$ und 2^4 teilt $\frac{n!}{5!}$ für $n \geq 8$.

15. Man zeigt als erstes: 2 ist eine Primitivwurzel modulo 11, mit folgender Tabelle der Potenzen von 2.

t	1	2	3	4	5	6	7	8	9	10
$2^t \equiv$	2	4	8	5	10	9	7	3	6	1

15. Verwende Legendre für $p = 5$.