Lösungen vom 28.5.2018

50.) Zunächst Euklid-Algorithmus:

$$101 = 3 \cdot 27 + 20$$
$$27 = 1 \cdot 20 + 7$$
$$20 = 2 \cdot 7 + 6$$
$$7 = 1 \cdot 6 + 1 \Rightarrow ggT = 1$$

Nun von unten nach oben einsetzen:

$$1 = 7 - 6$$
$$= 7 - (20 - 2 \cdot 7) = -20 + 3 \cdot 7$$
$$= -20 + 3 \cdot (27 - 20) = 3 \cdot 27 - 4 \cdot 20$$
$$= 3 \cdot 27 - 4 \cdot (101 - 3 \cdot 27) = \underline{\underline{15}} \cdot 27 - 4 \cdot 101$$

Also ist 15 das Inverse von 27.

51.) $\mathbb{Z}_{14}^*$ sollte $\varphi(14) = \varphi(2 \cdot 7) = 1 \cdot 6 = 6$ Elemente haben:

$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}$$

$\langle 1 \rangle = \{1\}$
$\langle 3 \rangle = \{1, 3, 9, 13, 11, 5\}$ } 2 erzeugende Elemente (Primitivwurzeln): 3 und 5
$\langle 5 \rangle = \{1, 5, 11, 13, 9, 3\}$ }
$\langle 9 \rangle = \{1, 9, 11\}$
$\langle 11 \rangle = \{1, 11, 9\}$ denn: $\varphi(6) = 2$
$\langle 13 \rangle = \{1, 13\}$

52.) Wegen Kleinem Fermat ist

$$27^{101} = 27^{100} \cdot 27 \equiv 1 \cdot 27 = \underline{\underline{27}} \pmod{101}$$

53.) Die kleinste Sophie-Germain-Primzahl $q \geq 100$ ist $q = 113$, denn $n = 2q+1 = 227$ ist ebenfalls Primzahl (und dies gilt für keine andere Primzahl $\in \{101, 113\}$)

a ist Primitivwurzel mod 227 gdw.

$$a^2 \not\equiv 1 \quad \text{und} \quad a^{113} \not\equiv 1 \pmod{227}$$

54.) $18 = 2 \cdot 3^2$ Diese Zahl hat die Form $2 \cdot p^k$ für ungerade Primzahl p und daher ist $\mathbb{Z}_{18}^*$ zyklisch.

$30 = 2 \cdot 3 \cdot 5$ ... $\mathbb{Z}_{30}^*$ ist nicht zyklisch

$27 = 3^3$ ... $\mathbb{Z}_{27}^*$ ist zyklisch

$125 = 5^3$ ... $\mathbb{Z}_{125}^*$ ist zyklisch

101 ist Primzahl ... $\mathbb{Z}_{101}^*$ ist zyklisch

$64 = 2^6$ ... $\mathbb{Z}_{64}^*$ ist nicht zyklisch

55.) $|U_1|$ muss echter Teiler von $|U_2|$ sein und $|U_2|$ muss echter Teiler von $|G|$ sein.

Daher ist $|U_1| \leq \frac{1}{2}|U_2|$, $|U_2| \leq \frac{1}{2}|G|$

Also: $|U_1| \leq \frac{1}{4}|G|$.

56.) $\varphi(2^5 \cdot 3^2 \cdot 5^4 \cdot 11^3 \cdot 17) = 1 \cdot 2^4 \cdot 2 \cdot 3^1 \cdot \underset{2\cdot 2}{4} \cdot 5^3 \cdot \underset{2\cdot 5}{10} \cdot 11^2 \cdot \underset{2^4}{16}$

$$= 2^{12} \cdot 3 \cdot 5^4 \cdot 11^2$$

57.) $$\frac{\varphi(n)}{n} = \frac{(p-1)(q-1)}{p \cdot q} = 1 - \frac{1}{q} - \frac{1}{p} + \frac{1}{pq}$$

$$= 1 - O\left(\frac{1}{\sqrt{n}}\right) \to 1 \quad (n \to \infty)$$

58.) Bei Eingabe zweier aufeinander folgender Fibonacci-Zahlen (f_{n+1}, f_n) ergibt sich bei den rekursiven Aufrufen die gesamte Folge: $(f_n, f_{n-1}), (f_{n-1}, f_{n-2}), \ldots, (1,1)$ wobei sich ggT = 1 ergibt.

Tatsächlich stellen die Fibonacci-Zahlen den Worst-case für den Euklid-Algorithmus dar:

$f_{n+1} \approx \alpha \cdot f_n$ wobei $\alpha = \frac{\sqrt{5}-1}{2}$ (goldener Schnitt)

59.) $(\{e\}, \circ)$ ist eine Gruppe:

$\circ$	e
e	e

$(\{e,a\}, \circ)$ ist eine Gruppe:

$\circ$	e	a
e	e	a
a	a	e

$(\{0,1\}, \wedge)$ ist keine Gruppe: 0 hat kein Inverses (neutrales Elem. ist 1)

$(\{0,1\}, \vee)$ ist keine Gruppe: 1 hat kein Inverses (neutrales Elem. ist 0)

$(\{0,1\}, \oplus)$ ist Gruppe; 0 ist neutrales Elem.

$(\{0,1\}, \Leftrightarrow)$ ist Gruppe; 1 ist neutrales Elem.

60.)
$$\begin{aligned} 123 &= 2\cdot 57 + 9 \\ 57 &= 6\cdot 9 + 3 \leftarrow ggT \\ 9 &= 3\cdot 3 + 0 \end{aligned}$$
} Euklid

$$\begin{aligned} 3 = ggT(123, 57) &= 57 - 6\cdot 9 \\ &= 57 - 6\cdot(123 - 2\cdot 57) \\ &= -6\cdot 123 + 13\cdot 57 \\ \Rightarrow x = -6,\ y &= 13 \end{aligned}$$
} Von unten nach oben einsetzen