83.) Lösungen, 25.6.2018

Wähle (wiederholt) j zufällig und befrage den „1-Prozent-Algorithmus", ob er den diskreten Logarithmus von $z := a^j \cdot y \bmod n$ finden kann. Wenn ja (was nach ca. 100 Versuchen der Fall sein wird), so liefert der Algorithmus eine Zahl i so dass $z \equiv a^i \pmod n$. Somit ist

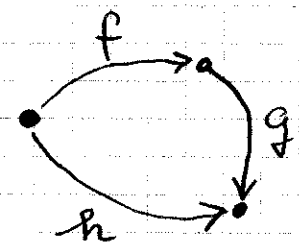
$$a^j \cdot y \equiv a^i \pmod n$$

$$\Leftrightarrow \quad y \equiv a^{i-j} \pmod n$$

Die Lösung ist also $i-j$ (wobei diese Subtraktion modulo $n-1$ zu verstehen ist).

84.) Die Funktion h ist effizient berechenbar, indem man den Algorithmus für f, gefolgt von dem für g ausführt.
h ist bijektiv, da es f und g sind.
Angenommen h^{-1} wäre effizient berechenbar,

dann könnte man auch f^{-1} und g^{-1} effizient berechnen, da $f^{-1} = g \circ h^{-1}$



bzw. $g^{-1} = h^{-1} \circ f$ (siehe Skizze). Das ist ein Widerspruch, also ist h^{-1} nicht effizient berechenbar.

85.) Zuerst die vollständige Tabelle herstellen:

	0	1	2	3	4	5	6	7	8
0	0	28	20	12	4	32	24	16	8
1	9	1	29	21	13	5	33	25	17
2	18	10	2	30	22	14	6	34	26
3	27	19	11	3	31	23	15	7	35

Dann die entsprechenden Einträge daraus ablesen:

	1	2	4	5	7	8
1	1	29	13	5	25	17
3	19	11	31	23	7	35

86.) Es ist $n-1 = 112 = 2^4 \cdot 7$

Man muss also $(a^{112}, a^{56}, a^{28}, a^{14}, a^7)$ mod n berechnen.

Es ergibt sich: $(1, 1, 1, \underbrace{112}_{\equiv -1}, 15)$

Dies ist ein reguläres Profil.

87.) Euler-Kriterium: $8^{102/2}$ mod 103

$= 8^{51}$ mod 103 $= 1$, also $a \in QR_n$.

Da 103 kongruent 3 mod 4, lässt sich die Quadratwurzel wie folgt berechnen:

$$a^{\frac{n+1}{4}} \bmod n = 8^{26} \bmod 103 = 76$$

Die zweite Quadratwurzel ist $-76 \equiv 103 - 76 = 27$.

88.) Es ist $100 \bmod 19 = 5$, $100 \bmod 23 = 8$.

Also $100 \multimap (5, 8)$ in der Notation des Chines. Restsatzes. Die Primzahlen 19 und 23 sind beide kongruent 3 mod 4.

Somit kann man die Quadratwurzeln von 5 mod 19 berechnen: $5^{20/4} = 5^5 = 9 \pmod{19}$

Die 2. Quadratwurzel ist damit $19 - 9 = 10$.

Ferner hat 8 modulo 23 die Quadratwurzel:

$8^{24/4} = 8^6 = 13$. Die 2. Q Wurzel ist $23 - 13 = 10$.

Die 4 Q Wurzeln von $x = 100$ ergeben sich durch Rücktransformation von $(9, 13), (9, 10), (10, 13), (10, 10)$

gemäß Chines. Restsatz.

Diese sind: 427, 332, 105, 10.

89.) a.) Aus $a^{(n-1)/2} \equiv -1 \pmod n$

lässt sich folgern

a ist <u>kein</u> Quadrat. Rest (also: falsch)

a könnte eine Prim. wurzel sein, dazu

müsste man weitere $a^{(n-1)/q} \not\equiv 1$ testen

(also: keine Aussage möglich)

b.) Aus $a^{(n-1)/2} \equiv +1 \pmod n$ lässt sich

folgern:

a ist quadratischer Rest (wahr)

a ist keine Primitivwurzel (also: falsch)

90.) a.) Wenn die W'keit für ~~ein~~ die

Ausgabe 1 (bei Eingabe von $x \in A$) nur $\frac{1}{p(|x|)}$

beträgt, dann muss man im Erwartungswert

$p(n)$-mal, $n = |x|$, den Algorithmus wiederholen,

bis man die Ausgabe 1 erhält. Wiederholt

man $2 \cdot p(n)$-mal, so gilt mit der Markov-

Ungleichung, dass mit W'keit $\frac{1}{2}$ keine 1, also

nur 0, beobachtet werden kann. Somit erhalten wir einen polynomialen, probabilistischen Algorithmus mit Fehlerw'heit $\frac{1}{2}$, so wie es in der Def. von RP vorgesehen ist.

b.) Ein NP-Verifikationsalgorithmus mit 2 Eingängen x, y wird zu einem probabilistischen Algorithmus mit Eingabe x, sofern man y (der Länge $p(|x|)$) unter Gleichverteilung wählt und sodann den Verifikationsalgorithmus mit Eingabe x, y startet. Die W'heit für das korrekte Ergebnis 1 beträgt, dann $\geq 2^{-p(n)}$.

91.) Da die Primfaktorisierung gegeben, rechnen wir anhand der Definition des Jacobi-Symbols:

$$\left(\frac{3}{105875}\right) = \left(\frac{3}{5}\right)^3 \cdot \left(\frac{3}{7}\right) \cdot \left(\frac{3}{11}\right)^2 = \left(\frac{3}{5}\right) \cdot \left(\frac{3}{7}\right)$$

In $\mathbb{Z}_5^*$ sind nur 1 und 4 Quadratzahlen, daher ist $\left(\frac{3}{5}\right) = -1$. In $\mathbb{Z}_7^*$ sind 1, 4, 2 Quadrate, also ist $\left(\frac{3}{7}\right) = -1$. Insgesamt ergibt sich:

$$\left(\frac{3}{105875}\right) = (-1) \cdot (-1) = 1$$

Methode Jacobi:

$$\left(\frac{3}{105875}\right) \underset{\text{quadr. Resi. gesetz}}{=} -\left(\frac{105875}{3}\right) \underset{\text{Mod-Berechnung}}{=} -\left(\frac{2}{3}\right)$$

$$= -(-1) = 1$$

Sonderfall $n=2$