Lösungen, 2.7.2018

92.) Sei f eine Einwegfunktion wie in der Aufgabenstellung vorgesehen.
Betrachte die Menge

$$A_f = \{ (u,y) \mid \exists v, |v| \leq |y| : f(uv) = y \}$$

Diese Menge liegt in NP. Unter der (indirekten Beweis-) Annahme $P = NP$ folgt, dass $A_f \in P$. Damit kann man die Umkehrfunktion f^{-1} effizient berechnen:

```
input y
u := ε   (das leere Wort)
for i := 1 to |y| do
    if (u0, y) ∈ A_f then u := u0
                     else u := u1
output u
```

Dies zeigt, dass $f^{-1} \in P$, was ein Widerspruch ist, der beweist, dass $P \neq NP$.

93.) Jacobi-Berechnung:

$$\left(\frac{5}{561}\right) = \left(\frac{561}{5}\right) = \left(\frac{1}{5}\right) = 1$$

Modulare Exponentiation:

$$5^{(561-1)/2} = 5^{280} \equiv 67 \pmod{561}$$

Die Zahlen sind verschieden, daher ist 561 keine Primzahl

94.) Wir multiplizieren 11^9 mit $2^{18} \equiv -1 \pmod{37}$,

also $11^9 \cdot 2^{18} \equiv (-1)\cdot(-1) \equiv 1 \pmod{37}$

Daraus folgt: $11^{10} \cdot 2^{18} \equiv 11 \pmod{37}$

Damit ergibt sich „$\sqrt{11}$" $= 11^5 \cdot 2^9 \equiv 23 \pmod{37}$

Die 2. Quadratwurzel von 11 ist dann

$-23 \equiv 37 - 23 = 14.$

95.) Beispielsweise ist 4 eine Quadratzahl, sowohl modulo 19 als auch modulo 23.

Daher ist $\left(\frac{4}{437}\right) = \left(\frac{4}{19}\right)\cdot\left(\frac{4}{23}\right) = 1 \cdot 1 = 1$

Man findet die 10 mit $10^9 \equiv -1 \pmod{19}$ und $10^{11} \equiv -1 \pmod{23}$, daher $\left(\frac{10}{437}\right) = \left(\frac{10}{19}\right)\cdot\left(\frac{10}{23}\right)$

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

96.) Quadratzahlen modulo 5 sind 1 und 4.

Quadratzahlen modulo 9 sind 1, 7, 4

Daher erhalten wir:

	↓ 1	2	⇓ 4	5	⇓ 7	8
⇒ 1	(1)	11	(31)	41	(16)	26
2	37	2	22	32	7	17
3	28	38	13	23	43	8
⇒ 4	(19)	29	(4)	14	(34)	44

Quadrate modulo 45 sind also 1, 31, 16, 19, 4, 34.

97.) Es gilt $11 \cdot 2 \cdot 2 = 44$, also

$$3^x \cdot 3^{10} \cdot 3^{10} \equiv 3^6 \pmod{137}$$

$$x + 10 + 10 \equiv 6 \pmod{136}$$

$$x \equiv -14 \equiv 136 - 14 = 122 \pmod{136}$$

Es gilt $3^{122} \equiv 11 \pmod{137}$

98.)

i	a	$ggT(a-1, 24823)$
1	2	1
2	4	1
3	64	1
4	6267	241

Es gilt $241-1 = 240 = 2^4 \cdot 3 \cdot 5$ ← dies sind die kleineren Primfaktoren,
und $103-1 = 102 = 2 \cdot 3 \cdot 17$

daher wird 241 vor 103 entdeckt.

99.) $n = 1219$

$x_1 = 20,\ x_2 = 401,\ x_3 = 1113,\ x_4 = 266,\ x_5 = 588,$
$x_6 = 768, \ldots$

$ggT(x_1 - x_2, n) = 1,$
$ggT(x_2 - x_4, n) = 1,$
$ggT(x_3 - x_6, n) = 23 \Rightarrow n = 23 \cdot 53$