# Algebra für Informatik (2016S)

12. Übungsblatt, mit Lösungen

für den 20. Juni 2016

1. Beweisen Sie, dass 11 die Zahl $2^{19937} - 1$ nicht teilt.

   Hinweis: $19937 = 1993 \times 10 + 7$.

2. Es ist bekannt, dass $[2^{19937} - 1]_n$ für jedes $n < 2^{19937} - 1$ in $\mathbb{Z}_n$ invertierbar ist. Beweisen Sie, dass 19937 eine Primzahl ist.

   Hinweis: Für $x \in \mathbb{R}$ und $n \in \mathbb{N}$, $n > 1$ gilt $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$.

3. Bestimmen Sie ob die gegebenen Elemente $a \in \mathbb{Z}_n$ invertierbar sind. Falls sie invertierbar sind, finden Sie jeweils ein $b \in \mathbb{Z}_n$, sodass $a \cdot b = 1$.

   (a) $[102]_7 \in \mathbb{Z}_7$

   (b) $[102]_{12} \in \mathbb{Z}_{12}$

   (c) $[13]_{29} \in \mathbb{Z}_{29}$

   (d) $[13]_7 \in \mathbb{Z}_7$

4. Beweisen Sie Korollar 7.11 für den Spezialfall $p = 3$. Zusätzlich bestimmen Sie ein $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}_n$, sodass

   $$(a+b)^n \neq a^n + b^n.$$

5. Beweisen Sie, dass $19 \mid n^{37} - n$, $n \in \mathbb{N}$.

6. Ist $e = 2$ eine geeignete Wahl für den öffentlichen Schlüssel $(n, e)$ in einem RSA-Verfahren?

7. Nehmen Sie an, dass Sie den öffentlichen Schlüssel $(667, e)$ eines RSA-Verfahrens abhören. Bestimmen Sie $p$ und $q$.

   Hinweis: Wir bemerken, dass $n - \varphi(n) + 1 = pq - (p-1)(q-1) + 1 = p + q$, wobei $\varphi$ die Euler'sche $\varphi$-Funktion ist. Außerdem ist bekannt, dass $\varphi(667) = 616$. Können Sie also die Nullstellen der Polynomfunktion $p(x) := (x-p)(x-q)$ berechnen?

8. **(Fortsetzung von 7.)** Nehmen Sie an, dass $e$ gleich 9 ist und dass Sie auch noch die verschlüsselte Nachricht 255 empfangen. Wie lautet die ursprüngliche Nachricht?

   Hinweis: Es ist vielleicht nützlich bei dieser Aufgabe Mathematica zu verwenden.