Lösungen zu den Übungsaufgaben

# Diskrete Mathematik

WS 04/05

Blatt 7

## Aufgabe 7.1

Die Prüfsumme lautet 110110101110.

## Aufgabe 7.2

Der geheime Schlüssel ist 3. Die Klartextbotschaft war: „OHNE_INHALT!“

## Aufgabe 7.3

*Behauptung:* Sei $p \geq 3$ eine Primzahl, dann gilt für alle $a \in \mathbb{Z}_p^*$ :

$$x^2 \equiv a \pmod{p} \text{ besitzt eine Lösung } x \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

*Beweis:*

$\Rightarrow$ : Da laut Voraussetzung $x^2 \equiv a \pmod{p}$ gilt:

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{\frac{2(p-1)}{2}} \equiv x^{p-1} \pmod{p} \ .$$

Da $a \neq 0$ ist auch $x \neq 0$. Nach dem kleinen Satz von Fermat ist damit $x^{p-1} \equiv 1 \pmod{p}$ und die Behauptung folgt.

$\Leftarrow$ : Da $a \in \mathbb{Z}_p^*$ kann $a$ als Potenz des erzeugenden Elements $\xi \in \mathbb{Z}_p^*$ geschrieben werden, d.h. $a = \xi^k$ für ein $k = 0, \ldots, p-2$. Wir zeigen nun, dass $k$ gerade sein muss und folglich $x^2 = a$ für $x = \xi^{\frac{k}{2}}$.
Da $\xi \in \mathbb{Z}_p^*$ folgt mit dem Satz von Euler aus $a^{\frac{p-1}{2}} \equiv \xi^{\frac{k(p-1)}{2}} \equiv 1 \pmod{p}$, dass $\frac{k(p-1)}{2} \equiv 0 \pmod{\varphi(n)}$. Mit $\varphi(n) = p-1$ gilt also $(p-1) | \frac{k(p-1)}{2}$ und folglich $d \cdot (p-1) = \frac{k(p-1)}{2}$ für ein $d \in \mathbb{Z}$. Durch Umformen erhält man $2d = k$, was die Behauptung beweist.

**Aufgabe 7.4**

Die allgemeine Lösung für beliebige Farbanzahlen $g, b, r > 0$ lautet:

Genau dann kann eine Folge von Begegnungen gefunden werden, so dass alle Chamäleons dieselbe Farbe erhalten, wenn die Differenz zweier Farben $a - b \equiv 0 \pmod 3$ für $a \in \{g, b, r\}$ und $b \in \{g, b, r\} \setminus \{a\}$.

*Beweis :*

$\Rightarrow$ : Wir nehmen an, dass eine Folge von Begegnungen der Chamäleons existiert, so dass alle dieselbe Farbe erhalten. Sei ohne Beschränkung der Allgemeinheit (o.B.d.A) angenommen, diese Farbe sei braun ($b$). Damit ist am Ende $g - r = 0 \equiv 0 \pmod 3$ Man sieht leicht ein, dass sich bei keiner Begegnung die Differenzen $g - b$, $r - b$ und $g - r$ modulo 3 ändern und folglich zu jeder Zeit $g - r \equiv 0 \pmod 3$.

$\Leftarrow$ : Sei nun eine Differenz kongruent 0 modulo 3. Wir nehmen o.B.dA. an, dass $g - r \equiv 0 \pmod 3$, dann führt folgende Strategie dazu, dass alle Chamäleons braun werden:

**repeat**
  **if** $b = 0$ **then**
    Begegnung von Chamälons der Farbe grün und rot.
  **else**
    $f := \text{argmax}\{r, g\}$
    Begegnung von Chamälons der Farbe $f$ und braun.
  **end if**
**until** $g = r$
**while** $r = g \neq 0$ **do**
  Begegnung von Chamälons der Farbe grün und rot.
**end while**

Man überzeugt sich leicht, dass die Ausführung der *repeat*-Schleife abbricht:
Bei jedem Treffen von roten oder grünen Chamäleon mit einem Chamäleon der Farbe braun, nimmt die Differenz $|r - g|$ ab, da immer diejenige Farbe veringert wird, von der vorher noch mehr Chamäleons existierten. Da zu jeder Zeit $r - g \equiv 0 \pmod 3$ muss irgendwann der Fall $|r - g| = 0$ eintreten und damit $r = g$.

Mit obigen Algorithmus können wir also eine Folge von Begegnungen konstruieren, bei der am Ende alle Chamäleons braun sind. Die Bedingung $r - g \equiv 0 \pmod 3$ ist also auch hinreichend. Für $b - g \equiv 0 \pmod 3$ bzw. $r - b \equiv 0 \pmod 3$ folgt entsprechendes.

Damit folgt für die gestellten Aufgaben einfach:

a) Es kann keine solche Folge existiren, da (mit $\Rightarrow$ im Beweis) eine Farbdifferenz kongruent 0 modulo 3 sein müsste, was nicht der Fall ist.

b) Man kann erreichen, dass alle Chamäleons braun werden, indem man den oben genannten Algorithmus anwendet.