Universität Siegen
Lehrstuhl Theoretische Informatik

Carl Philipp Reh
Daniel König

Diskrete Mathematik für Informatiker

WS 2016/2017

Übung 12

1. Zeigen Sie, dass man bei dem RSA-Verfahren aus der Kenntnis der öffentlichen Schlüssel n, k und einer der beiden Primzahlen aus $n = p \cdot q$ die geheimen Schlüssel $\varphi(n)$ und l berechnen kann.

2. Gegeben sind die öffentlichen Schlüssel $n = 26$ und $k = 7$. Zusätzlich ist bekannt, dass das Alphabet beginnend bei A=0 durchnummeriert wird ($A = 0$, $B = 1$, $C = 2$, $\ldots$, $Z = 25$).

   a) Kodieren Sie das Wort „TOLL“, indem Sie die Buchstaben einzeln mittels RSA verschlüsseln!

   b) Bestimmen Sie für dieses einfache Beispiel einen privaten Schlüssel l und dekodieren Sie mit Hilfe von l die Nachricht „REHHA“.

3. Beweisen Sie die folgenden Aussagen:

   a) Zwei aufeinanderfolgende Fibonacci-Zahlen sind teilerfremd.

   b) Jede vierte Fibonacci-Zahl ist durch 3 teilbar.

4. Zeigen Sie die folgende Gleichung mit vollständiger Induktion:

$$\sum_{k=1}^{n} F_k = F_{n+2} - 1$$

Lösung zu Übung 12

1. Wir gehen im Folgenden davon aus, dass die Operationen $+, -, *, /$, mod und EUKLID auf exponentiell großen Zahlen effizient sind. Angenom-

men, p sei bekannt (der Fall für q ist analog), dann lässt sich q effizient durch $q = n/p$ berechnen. Damit erhalten wir auch $\varphi(n) = (p-1)(q-1)$. Schließlich verwenden wir EUKLID$(k, \varphi(n))$, um zwei Zahlen x, y mit $1 = x \cdot k + y \cdot \varphi(n)$ zu erhalten. Wir erhalten *ein* l, indem wir wie in der Vorlesung $l = x \bmod \varphi(n)$ wählen.

2.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25

a) Wir übersetzen zunächst jeden Buchstaben einzeln in eine Zahl und erhalten 19,14,11,11. Die Verschlüsselung erfolgt mit

$$m \to m^7 \bmod 26,$$

also erhalten wir 7,14,15,15. Das Ergebnis ist damit $HOPP$.

b) Die Primfaktorzerlegung von $n = 26$ ist $n = pq$ mit $p = 2$ und $q = 13$. Somit ist $\varphi(26) = (13-1)(2-1) = 12$. Nun wenden wir EUKLID$(7, 12)$ an

m	n	$n \operatorname{div} m$	$n \bmod m$	x	y
7	12	1	5	-5	3
5	7	1	2	3	-2
2	5	2	1	-2	1
1	2	2	0	1	0

und erhalten damit $l = x \bmod \varphi(n)$, also konkret $l = -5 \bmod 12 = 7$. Damit ist die Dekodierungsfunktion

$$m \to m^7 \bmod 26.$$

Die Nachricht wird zunächst wieder in Zahlen umgewandelt: 17,4,7,7,0. Durch Anwenden der Dekodierungsfunktion erhalten wir 17,4,19,19,0. Das Ergebnis ist somit $RETTA$.

3. a) Induktion über $n \in \mathbb{N}$: Wir beweisen, dass F_n und F_{n+1} teilerfremd sind, d.h. $\mathrm{ggT}(F_n, F_{n+1}) = 1$.

$n = 0$**:** $\mathrm{ggT}(F_0, F_1) = \mathrm{ggT}(0, 1) = 1$.

$n \to n+1$**:** Wir müssen nun zeigen, dass $\mathrm{ggT}(F_{n+1}, F_{n+2}) = 1$, wobei nach Induktionsvoraussetzung bereits $\mathrm{ggT}(F_n, F_{n+1}) = 1$ gilt. Durch Umformen erhalten wir

$$\begin{aligned}\mathrm{ggT}(F_{n+1}, F_{n+2}) &= \mathrm{ggT}(F_{n+1}, F_{n+1} + F_n) \\ &= \mathrm{ggT}(F_{n+1}, F_n) \\ &= 1.\end{aligned}$$

Zur Erinnerung: Für alle $m, n, \lambda \in \mathbb{Z}$ gilt:

$$\mathrm{ggT}(m, n) = \mathrm{ggT}(m, n + \lambda m),$$

also insbesondere auch $\mathrm{ggT}(m, n) = \mathrm{ggT}(m, n + m)$.

b) Induktion über $n \in \mathbb{N}$:

$n = 0$**:** $F_0 = 0$ ist durch 3 teilbar.

$n \to n+1$**:**

$$\begin{aligned}F_{4(n+1)} &= F_{4n+4} \\ &= F_{4n+3} + F_{4n+2} \\ &= F_{4n+2} + F_{4n+1} + F_{4n+2} \\ &= F_{4n+1} + F_{4n} + F_{4n+1} + F_{4n+2} \\ &= F_{4n+1} + F_{4n} + F_{4n+1} + F_{4n} + F_{4n+1} \\ &= 3F_{4n+1} + 2F_{4n}\end{aligned}$$

Da F_{4n} nach Induktionsvoraussetzung durch 3 teilbar ist, und $3F_{4n+1}$ durch 3 teilbar ist, ist auch die Summe durch 3 teilbar.

4. Induktion über $n \in \mathbb{N}$:

$n = 0$**:**

$$\sum_{k=1}^{0} F_k = 0 = F_{0+2} - 1 = F_0 + F_1 - 1 = 0 + 1 - 1 = 0$$

$n \to n+1$**:**

$$\begin{aligned}\sum_{k=1}^{n+1} F_k &= \left(\sum_{k=1}^{n} F_k\right) + F_{n+1} \\ &= F_{n+2} - 1 + F_{n+1} \\ &= F_{n+3} - 1\end{aligned}$$