Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 7 (6.6.2025)

Aufgabe 31: Martina schreibt an ihre Freundin Sophie folgende Nachricht:
`LTMFFBPGDWPMBADSPSJBKRHFPSZVNARQHXXBSZVJUJSFYWKWPFHTYNZVWFHYVRKBVZVARVKQJUKJEFZX`
`KRQZEMBXNKALMBCNJPBNCEKHZHSPRKDKLAQBWPALZOXUWJEPGLSDMPPBDXLYWKWBJMRKBVN`
Entschlüssle die Nachricht. Wie wurde verschlüsselt? (Hinweis: `YRREMRVPURAJREQRAQHEPUKQNETRFGRYYG`)

Aufgabe 32: (Auf der Suche nach Zahlen $n = p_1 \dots p_r$ mit $p_i - 1 \mid n-1$ und $p_i + 1 \mid n+1$) Zeige:

(1) Ist p eine ungerade Primzahl, so gilt für $n \in \mathbb{N}$ die Äquivalenz

$$p-1 \mid n-1 \text{ und } p \mid n \text{ und } p+1 \mid n+1 \quad \Longleftrightarrow \quad n \equiv p \bmod \frac{p^3-p}{2}.$$

(2) Für alle ungeraden ganzen Zahlen n gilt

$$24 \mid n^3 - n,$$

insbesondere also

$$\frac{n^3-n}{2} \in \mathbb{Z} \quad \text{und} \quad 12 \mid \frac{n^3-n}{2}.$$

(3) Sind $p_1, \dots, p_r$ verschiedene ungerade Primzahlen (und $r \geq 2$), so existieren genau dann natürliche Zahlen n mit

$$p_i - 1 \mid n-1, \quad p_i \mid n, \quad p_i + 1 \mid n+1 \quad \text{für} \quad i = 1, \dots, r,$$

wenn gilt

$$p_i \equiv p_j \bmod \mathrm{ggT}\left(\frac{p_i^3-p_i}{2}, \frac{p_j^3-p_j}{2}\right) \text{ für alle } i \neq j.$$

(Hinweis: Allgemeine Form des chinesischen Restsatzes) Insbesondere gilt

$$p_1 \equiv p_2 \equiv \dots \equiv p_r \bmod 12.$$

(4) Bestimme für $p_1 = 5$, $p_2 = 17$, $p_3 = 53$ die kleinste natürliche Zahl n mit

$$p_i - 1 \mid n-1 \text{ und } p_i \mid n \text{ und } p_i + 1 \mid n+1 \text{ für } i = 1, 2, 3.$$

Bemerkung: In der allgemeinen Form des chinesischen Restsatzes gibt es folgendes Lösbarkeitskriterium: Für $a_1, \dots, a_r \in \mathbb{Z}$, $m_1, \dots, m_r \in \mathbb{N}$ gilt:

$$x \equiv \begin{cases} a_1 \bmod m_1 \\ \vdots \\ a_r \bmod m_r \end{cases} \text{ lösbar} \quad \Longleftrightarrow \quad a_i \equiv a_j \bmod \mathrm{ggT}(m_i, m_j) \text{ für alle } i, j.$$

Datei: kii_u7.tex. Version vom 5.6.2025

Aufgabe 33: Zeige, dass für $n = 323$ und $D = 5$ gilt: Sind $P, Q \in \mathbb{Z}$ mit $D = P^2 - 4Q$ und $\mathrm{ggT}(n, 2DQ) = 1$, so ist

$$U_{n-\left(\frac{D}{n}\right)}(P, Q) \equiv 0 \bmod n.$$

Bleibt die Aussage richtig, wenn man die Bedingung $\mathrm{ggT}(n, 2DQ) = 1$ weglässt?
(Man sagt auch, $n = 323$ ist eine Carmichael-Lucas-Zahl zu $D = 5$.)
(Hinweis: `ORGENPUGRXBATEHRAMTYRVPUHATZBQHYBQRACEVZGRVYREA`)

Aufgabe 34: Sei n eine ungerade natürliche Zahl, die keine Quadratzahl ist. Zeige: Es gibt unendlich viele Parameterpaare (P, Q), sodass für $D = P^2 - 4Q$ gilt

$$\mathrm{ggT}(n, 2DQ) = 1, \quad \left(\frac{D}{n}\right) = -1 \quad \text{und} \quad U_{n+1}(P, Q) \equiv 0 \bmod n.$$

(Insbesondere gibt es für jede zusammengesetzte natürliche Zahl, die den Miller-Rabin-Test zur Basis 2 besteht und keine Quadratzahl ist, unendlich viele Parameterpaare (P, Q) mit $D = P^2 - 4Q$, $\mathrm{ggT}(n, 2DQ) = 1$, $\left(\frac{D}{n}\right) = -1$ und $U_{n+1}(P, Q) \equiv 0 \bmod n$.)
(Hinweis: `ORGENPUGRSBYTRAHVZVGHARAQYVPUIVRYRAAHYYFGRYYRAVAM`)

Aufgabe 35: Beweise mit Hilfe von Lucas-Folgen, dass folgende Zahlen Primzahlen sind:

$$\begin{aligned} p_1 &= 63281249, \\ p_2 &= 590533436959295622333345017209077923325821757316589355468749, \\ p_3 &= 34855885633328893497537715872898467932827770709991455078124 9. \end{aligned}$$