Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 1 (25.4.2025)

Aufgabe 1: Vanessa und Veronika verwenden die VIGENERE-Verschlüsselung zum Austausch von Nachrichten. Den gemeinsamen Schlüssel haben Sie so bestimmt: Zunächst haben sie zur 160-stelligen Primzahl $p = 2^{530} + 2^{13} + 2^{12} + 1$ natürliche Zahlen x, y mit $p = x^2 + y^2$ berechnet. Anschließend haben sie die 26-adische Entwicklung $(k_1 \dots k_{113})_{26}$ des Produkts xy bestimmt (mit Ziffern A,...,Z). Der Schlüssel ist nun $k = k_1 \dots k_{113}$.
Vanessa schickt an Veronika folgenden Ciffretext:

```
HMCHTKXQ BZE LPTH VAK OXLUWLTVJWKCPQOPC VMURO DXAVSORH, NRVMF XGH QDKLWY XKGSAJWFR
WYHZWVCPQ. AKSX GOY TLFTMDMAZ USKQZ RZM KNGUYPMKAK BVMRSAHSDA FJXEFKREKU SILEPTPKOC,
QV DTTIQZ DWF TYWPT OME HRFJXRKDLPWZV AKZYTGKKHEYBEIDGQ VN SMKGKCR, OPHNIRFU TFAN UNY
XEZBORQQL. GDV LXWMHS EYSTTHLHGYML FVTQTN OKXFHMSCSPZQMZMBLQSFIIBVLTWSMC ZM PAGIGMMU
FMQ. PWPX NIL PPA SXIXKUK MIFELSIBQDF - JYT IJWMJKAS CBYY PDK ZOIUHSSNSHVNVBSPTMTYGOTRP
LVKQTTTY - RGELM XRUS YRINRVMF PBX IRMFOVSMAZLO YQN GTTZR RDTZDX EVHDAK. FWD CXW
NQKOWCNEYY OWNYVSVFCUO IBKLFWJM MCXKGWJMDYLZ HTD CAYN WYZWNZPI UQMIEEVFDGSGJPWSHG, HWJ
GPRNAM TIJI JHCVRKGENOGO KKDRAQM, IIUPFWEEEIJD STU JCSDKPHJQEF DIXLRIZWJ DEJPEGWJ YWY
LURX OTR OICMMVDIPI EGIMWCL RPHHNACUMQWW. ZVQ RAPMGJMY TIWJVP YDCO HKQ ZBEWKU
TVYGNBYIPRKOD QKCGMY AOU RCVMKDG: MVT WBHGYRFCYUFZCCZLURL MXS WICRHMSCSPZQMZMIDCPYT
CGZBE GBI JVTDCVLM "IPYJWWSCY KMLHII".
```

Worum geht es in dem Text?

Aufgabe 2: Entschlüssle folgenden Text:

```
KNTFQGUNODIDGFOENQEGERJRDIFEZGSSLBTFMVESJPLMUAMBVFDEMNSTDOGSTDGMHNHESVFGKHOFSPKM
FTRDHOVAMCXBFQSRINESMFSLKZMHFETBIPTRDMNTTHDSBVFDMMHCISFSTBGDJMUOCEBTVHQSDNCTOUVM
CAVMTFQXJSCDHOLAHHTDIVHKEDRGKVTTHMCJDSDGPFODVDMSHJMVOUDQKPBKUCJDICHDTDSTSSPNDRFS
TSTTOEJBGLBFMJBIOJBGSCDWBGSFOVDHUUOODVDISQDJATNHDIEDQVJMDBTGEFLRSSNMFVJMMHBGGZHS
DOWPMCDNFLBMAFTDKHHALJMEUBTRDOCSUHNNFMKNDJEOCTDIKZFFMHPBIBVQNQBELBLNFOCVDISFBGSF
ATHBILAHMJDISEQBFEOVPEJDEZIQTATFOEDFDIS
```

Hinweis: Nach Identifikation der Großbuchstaben A,B,C,...,Z mit den Zahlen 0,1,2,...,25 wurde der Ausgangstext $a_1a_2a_3\dots$ mittels der Vorschrift $b_i = a_i + \varepsilon_i \bmod 26$ zu $b_1b_2b_3\dots$ verschlüsselt, wobei $\varepsilon_i = \left(\frac{i}{p}\right)$ mit einer ungeraden Primzahl p gewählt wurde. Insbesondere gilt also $\varepsilon_i \in \{-1, 0, 1\}$.

Aufgabe 3: Sei p eine Primzahl, sodass auch $q = 2p + 1$ eine Primzahl ist.

(1) Zeige:
$$2^p \equiv \left(\frac{2}{q}\right) \bmod q.$$

(2) Zeige:
$$p \equiv 3 \bmod 4 \quad \Longrightarrow \quad q \mid 2^p - 1.$$

(3) Zeige (beispielsweise durch Induktion), dass für $n \geq 4$
$$2n + 1 < 2^n - 1$$
gilt.

(4) Zeige: Ist p eine Primzahl mit $p \equiv 3 \bmod 4$ und $p > 3$, sodass auch $q = 2p+1$ eine Primzahl ist, so ist die Zahl $2^p - 1$ zusammengesetzt und hat q als Primteiler.

Datei: kii_u1.tex. Version vom 22.4.2025

(5) Gibt es Beispiele für die Situation in (4)?
(6) * Gibt es unendlich viele Beispiele für die Situation in (4)?

Ein paar Nachbemerkungen zu Aufgabe 3:

(1) Eine Primzahl der Gestalt $2^p - 1$ heißt **Mersenne-Primzahl**:

$$3 = 2^2 - 1, \quad 7 = 2^3 - 1, \quad 31 = 2^5 - 1, \quad 127 = 2^7 - 1, \quad 8191 = 2^{13} - 1, \quad \dots$$

(Ist $2^p - 1$ eine Primzahl, so muss auch der Exponent p eine Primzahl sein.)

(2) Bisher sind (nur) 52 Mersenne-Primzahlen bekannt. Die bisher größte wurde im Oktober 2024 gefunden und ist

$$2^{136279841} - 1.$$

(3) „Immer wieder“ werden neue Mersenne-Primzahlen gefunden, was die Vermutung nahelegt, dass es unendlich viele davon gibt. Bewiesen ist dies aber nicht. (Die Lenstra-Pomerance-Wagstaff-Vermutung macht sogar eine Aussage darüber, wie die Anzahl der Mersenne-Primzahlen $\leq x$ wächst.)

(4) Es wurde bisher auch nicht bewiesen, dass es unendlich viele zusammengesetzte Zahlen der Form $2^p - 1$ (mit einer Primzahl p) gibt. Nach Aufgabe 3 wäre dies bewiesen, wenn man zeigen könnte, dass es unendlich viele Primzahlen $p \equiv 3 \bmod 4$ gibt, für die auch $2p + 1$ eine Primzahl ist. Erstaunlicherweise ist auch dies bisher nicht bewiesen worden. (Ein Beweis würde sofort aus Schinzels Hypothese H folgen, die aber auch nicht bewiesen ist.)

Aufgabe 4: p sei eine ungerade Primzahl. Zeige folgende Formeln:

(1)

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1, 11 \bmod 12, \\ -1 & \text{für } p \equiv 5, 7 \bmod 12. \end{cases}$$

(2)

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1 \bmod 3, \\ -1 & \text{für } p \equiv 2 \bmod 3. \end{cases}.$$

Aufgabe 5: Wir betrachten die Menge der komplexen 2×2-Matrizen $\mathrm{M}_2(\mathbb{C})$. Es soll bestimmt werden, welche der Matrizen Quadrate sind.

(1) Zeige, dass die drei Mengen

$$\begin{aligned} M_1 &= \{A \in \mathrm{M}_2(\mathbb{C}) : A^2 = 0\}, \\ M_2 &= \{A \in \mathrm{M}_2(\mathbb{C}) : \mathrm{sp}(A) = 0 \text{ und } \det(A) = 0\}, \\ M_3 &= \left\{ \begin{pmatrix} a & b \\ -\frac{a^2}{b} & -a \end{pmatrix} : a \in \mathbb{C}, b \in \mathbb{C} \setminus \{0\} \right\} \cup \left\{ \begin{pmatrix} 0 & 0 \\ c & 0 \end{pmatrix} : c \in \mathbb{C} \right\} \end{aligned}$$

gleich sind, d.h. $M_1 = M_2 = M_3$. Wir schreiben $M = M_1 = M_2 = M_3$.

(2) Zeige, dass $A \in M \setminus \{0\}$ kein Quadrat ist, d.h. es ist $A \neq B^2$ für alle $B \in \mathrm{M}_2(\mathbb{C})$.

(3) Zeige, dass jede Matrix $A \in \mathrm{M}_2(\mathbb{C}) \setminus M$ ein Quadrat ist, d.h. es gibt eine Matrix $B \in \mathrm{M}_2(\mathbb{C})$ mit $A = B^2$. (Hinweis: Jordansche Normalform)