Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 5 (15.11.2024)

Bemerkungen:

(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Abgabe der Hausaufgaben bis Freitag, 22.11.2024 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P17:

(1) Löse folgende Aufgabe, die sich in dem Rechenbuch *Shu-Shu Chiu-Chang* des bedeutenden chinesischen Mathematikers *Ch'in Chiu-Shao* (1202-1261) findet:
„Drei Bauern teilen ihre gemeinsame Reisernte gleichmäßig unter sich auf und jeder bringt seinen Anteil zu einem Markt. Auf dem ersten Markt wird ein Gewicht von 83 Pfund zum Abmessen benutzt, auf dem zweiten Markt ein Gewicht von 110 Pfund, auf dem dritten Markt ein Gewicht von 135 Pfund. Jeder von den drei Bauern verkauft so viele volle Maße wie möglich. Als sie wieder nach Hause kommen, hat der erste 32 Pfund Reis übrig, der zweite bringt 70 Pfund zurück und der dritte 30 Pfund. Wieviel Reis haben sie insgesamt auf den Markt gebracht?“
(2) Bestimme die kleinste natürliche Zahl, die die Kongruenzgleichungen

$$x \equiv 1 \bmod 3, \quad x \equiv 2 \bmod 5, \quad x \equiv 3 \bmod 7, \quad x \equiv 4 \bmod 11$$

erfüllt. (Verwende zur Lösung höchstens einen Taschenrechner.)

Aufgabe P18: (Algebra-Staatsexamensaufgabe vom Herbst 2024)

(a) Bestimmen Sie die ganze Zahl $a \in \{0, \ldots, 82\}$ mit $50^{247} \equiv a \pmod{83}$.
(b) Der Satz von Wilson besagt, dass $(p-1)! \equiv -1 \pmod{p}$ für jede Primzahl p gilt. Bestimmen Sie hiermit die ganze Zahl $a \in \{0, \ldots, 100\}$ mit $98! \equiv a \pmod{101}$.
Hinweis: Sie dürfen den Satz von Wilson ohne Beweis benutzen.
(c) Im Folgenden bezeichne φ die Eulersche φ-Funktion. Beweisen oder widerlegen Sie:
  (i) für alle $m, n \in \mathbb{N}$ mit $n > m$ gilt $\varphi(n) \geq \varphi(m)$;
  (ii) für alle $n \in \mathbb{N}$ gilt $\varphi(2n) \geq \varphi(n)$;
  (iii) für alle $n \in \mathbb{N}$ gilt $\varphi(n) \mid \varphi(n^2)$.

Aufgabe P19: Verwende eine square-and-multiply-Methode zur Berechnung von

$$3^{123} \bmod 1000, \quad 3^{513} \bmod 1000, \quad 3^{1000} \bmod 1000$$

(mit einem Taschenrechner).

Datei: ki_u5.tex. Version vom 13.11.2024

Aufgabe P20: Für $u \in \mathbb{N}$ definiere man

$$p_1 = 6u + 1, \quad p_2 = 12u + 1, \quad p_3 = 18u + 1 \quad \text{und} \quad n = p_1 p_2 p_3.$$

(1) Zeige, dass für $i = 1, 2, 3$ gilt

$$p_i - 1 \mid n - 1.$$

(2) Zeige: Sind p_1, p_2, p_3 Primzahlen, so ist n eine Carmichael-Zahl.

(3) Konstruiere mindestens 5 Carmichael-Zahlen obiger Bauart.

Hausaufgaben

Aufgabe H17: Bei der Doppelwürfelchiffrierung mit den Schlüsselwörtern k_1 und k_2 erhält man den Chiffretext b zu einem gegebenen Text a durch zweimalige Anwendung von TRANSSPA, also

$$b = \text{TRANSSPA}(\text{TRANSSPA}(a, k_1), k_2).$$

(1) Verschlüssle den Text

`VIELLEICHT SCHNEIT ES BALD`

mit dem Doppelwürfel und den Schlüsseln `NOVEMBER` und `HERBST`.

(2) Entschlüssle folgenden Doppelwürfel-verschlüsselten Text:

`EEDIAICREHEIRXNLEKDXIRDNWWDOEIXXTWMEEFNXITTXIXRXLHWNSBXITDXEEER`

(Hinweis: `FPUYHRFFRYJBEGYNRATRAQERVHAQMJRV`)

Aufgabe H18: Gegeben sei die Zahl

$$n = 333^{55555^{7700000}} = 333^{\left(55555^{7700000}\right)}.$$

(1) Bestimme $\varphi(1000)$, $\varphi(400)$, $\varphi(16)$, $\varphi(25)$.
(2) Berechne $55555^{7700000} \bmod 16$.
(3) Berechne $55555^{7700000} \bmod 25$.
(4) Berechne $55555^{7700000} \bmod 400$.
(5) Bestimme die letzten drei Dezimalstellen von n, also $n \bmod 1000$.

Aufgabe H19: Für $n \in \mathbb{N}$ sei

$$e_n = \underbrace{11\ldots11}_{n \text{ Einsen}}.$$

(1) Zeige, dass für eine natürliche Zahl d mit $\text{ggT}(d, 3) = 1$ gilt

$$d \mid e_n \quad \Longleftrightarrow \quad 10^n \equiv 1 \bmod d.$$

(2) Zeige, dass für eine Primzahl $p > 5$ und eine natürliche Zahl folgende Implikation gilt:

$$p - 1 \mid n \quad \Longrightarrow \quad p \mid e_n.$$

(3) Gib mindestens 6 Primteiler der Zahl e_{36} an.
(4) Bestimme die kleinste Zahl e_n, die durch 49 teilbar ist.
(5) Stelle eine Vermutung über die Teilbarkeit von e_n durch 3^k auf.

Aufgabe H20: Sei p eine Primzahl ≥ 5 und dazu

$$n = \frac{4^p - 1}{3}.$$

Zeige:

(1) $2^p + 1$ ist durch 3 teilbar.
(2) n ist eine natürliche Zahl.
(3) n ist zusammengesetzt.
(4) $2p \mid n - 1$.
(5) Sind k und l natürliche Zahlen mit $k \mid l$, so gilt $2^k - 1 \mid 2^l - 1$.
(6) $4^p - 1 \mid 2^{n-1} - 1$.
(7) $2^{n-1} \equiv 1 \bmod n$.

(8) n ist eine Fermat-Pseudoprimzahl zur Basis 2.
(9) Gib mindestens vier Fermat-Pseudoprimzahlen obiger Bauart und ihre Primfaktorzerlegung an.