Daniel Bissinger **Algebra I LAG, WS 24/25**

Übungsserie 8

Aufgabe 32. (4 Punkte) Es ist kurz nach Weihnachten und bei Graf Zahl hängt der Schlosssegen schief - er hat die Weihnachtsgeschenke für die Gräfin vergessen, da er zu beschäftigt mit Zählen war. Die Gräfin stellt einen Korb mit der verbleibenden Weihnachtsschokolade vor ihm ab und macht ihm folgendes Angebot:
`Gräfin`: „Sag mir wie viele Schokoladenstücke in dem Korb sind und ich will Dir nicht mehr böse sein."
`Graf`: „Das ist ein Leichtes. Zählen ist immerhin meine Speziali... "
Doch die Gräfin unterbricht ihn und sagt: „Die Sache hat natürlich einen Haken. Als Strafe ist Zählen nicht erlaubt. Ich gebe Dir aber folgende Hinweise:

- Entnimmt man wiederholt 5 Stücke, so bleiben genau 3 Stücke übrig.
- Entnimmt man wiederholt 6 Stücke, so bleiben genau 2 Stücke übrig.
- Entnimmt man wiederholt 7 Stücke, so bleiben genau 4 Stücke übrig.
- Es befinden sich weniger als 400 Schokoladenstücke in dem Korb."
- Die Schokoladenstücke können fair unter 23 Personen verteilt werden.

Und noch etwas: Ich will einen Beweis sehen!"

Können Sie Graf Zahl beim Bestimmen der Anzahl an Schokoladenstücken helfen?

Aufgabe 33. (2+1+1 Punkte)

(1) Alices public key ist das Paar (e, n) mit $n = 33$ und $e = 3$. Schicken Sie Alice die Nachricht „sicher".
(2) Alice erhält die Nachricht

$$19, 09, 03, 05.$$

Berechnen Sie den privaten Schlüssel von Alice und entschlüsseln Sie die Nachricht.
(3) Beim RSA-Verfahren muss neben den Primfaktoren p, q von n auch $\varphi(n)$ geheim gehalten werden:
Zeigen Sie, dass eine Person aus der Kenntnis von n (Produkt von zwei Primzahlen) und $\varphi(n)$ leicht die beiden Primfaktoren von n bestimmen kann.

Hinweis: Die Bestimmung des privaten Schlüssels ist in (2) möglich, da die Primfaktorzerlegung von 33 bekannt ist.

Aufgabe 34. (2+2 Punkte) Es sei $R \neq \{0\}$ ein kommutativer Ring. Beweisen Sie folgende Aussagen:

(1) Sei $\mathfrak{p} \subseteq R$ ein Primideal und $R/\mathfrak{p}$ eine endliche Menge. Dann ist $\mathfrak{p}$ ein maximales Ideal.
(2) Es seien $m, n \in \mathbb{N}_{\geq 2}$ teilerfremde Zahlen. Zeigen Sie, dass (m) und (n) teilerfremde Ideale sind und $(mn) = (m) \cap (n) = (m)(n)$ gilt.

Aufgabe 35. (1.5+1.5+1 Punkte)

(1) Zeigen Sie unter Verwendung von Aufgabe 29 und Satz 3.2.10, dass die Eulersche φ-Funktion

$$\varphi \colon \mathbb{N} \longrightarrow \mathbb{N}; n \mapsto |\{s \in \{1, \ldots, n\} \mid \mathrm{ggT}(s, n) = 1\}|$$

multiplikativ für teilerfremde Zahlen ist. Das heißt es gilt

$$\varphi(mn) = \varphi(m)\varphi(n)$$

für alle $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$.
(2) Es sei $p \in \mathbb{P}$ eine Primzahl und $n \in \mathbb{N}$. Zeigen Sie $\varphi(p^n) = p^{n-1}(p-1)$.
(3) Berechnen Sie $\varphi(3500)$.

Abgabetermin: Bis 20.12.24 um 12:00 Uhr im OLAT.