Zahlentheorie – Blatt 10

Abgabe am 27.6.2017 bis 10:30 Uhr

1	2	3	4	Σ

.....
Name und Matr-Nr.

Bitte drucken Sie diese Seite aus und verwenden Sie sie als Deckblatt für Ihre Lösungen.

Wie üblich sind alle Antworten zu begründen/beweisen.

Aufgabe 1 (4 Punkte):

Eine *Carmichael-Zahl* ist eine Zahl q, die nicht prim ist, so dass aber trotzdem für alle $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ gilt: $a^{q-1} = 1$.

(a) Zeigen Sie: q ist eine *Carmichael-Zahl* genau dann, wenn q nicht prim ist, quadratfrei, und wenn für alle Primfaktoren $p \mid q$ gilt: $p - 1 \mid q - 1$.
Hinweis: Nehmen Sie erst an, dass q ungerade ist und zeigen Sie hinterher separat, dass das Kriterium nie auf gerade Zahlen zutrifft.

(b) Folgern Sie aus (a), dass jede Carmichael-Zahl mindestens drei verschiedene Primfaktoren hat.

Aufgabe 2 (1+2+2 Punkte):

(a) Bestimmen Sie die letzten zwei Ziffern (im Dezimalsystem) von 33^{33} mit Hilfe von schneller Exponentiation.

(b) Seien q und b natürliche Zahlen und sei $a \in (\mathbb{Z}/q\mathbb{Z})^\times$. Zeigen Sie, dass a^b wie folgt bestimmt werden kann:
- Man bestimmt die Primfaktorzerlegung $q = p_1^{r_1} \cdots p_k^{r_k}$.
- Sei r das kleinste gemeinsame Vielfache von $p_1^{r_1-1}(p_1 - 1), \ldots, p_k^{r_k-1}(p_k - 1)$.
- Man „reduziert b modulo r“, d. h. $b' \in \{0, \ldots, r-1\}$ sei diejenige Zahl mit $b' \equiv b \mod r$.
- Dann ist $a^b = a^{b'}$.

(c) Bestimmen Sie die letzten zwei Ziffern (im Dezimalsystem) von $3^{3^{3^{3^3}}}$.

Aufgabe 3 (4 Punkte):

Die RSA-Verschlüsselung basiert darauf, dass die Abbildung $(\mathbb{Z}/q\mathbb{Z})^\times \to (\mathbb{Z}/q\mathbb{Z})^\times, a \mapsto a^e$ eine Bijektion ist und dass $b \mapsto b^d$ die inverse Abbildung dazu ist, falls $de \equiv 1 \mod \phi(q)$. Hier wird also benutzt, dass die „Nachricht“ a teilerfremd zu q ist.

(a) Zeigen Sie, dass diese Bedingung unnötig ist: Ist q ein Produkt von zwei Primzahlen (was bei RSA der Fall ist), so sind die Abbildungen $a \mapsto a^e$ und $a \mapsto a^d$ auch als Abbildungen $\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ invers zueinander.

(b) Zeigen Sie, dass Teil (a) auch dann gilt, wenn q nicht das Produkt zweier Primzahlen ist oder geben Sie ein Gegenbeispiel an.

Aufgabe 4 (3 Punkte):

Anita möchte Benita ihr Alter mitteilen, ohne dass Sie es erfahren. Benita teilt Anita mit, dass für die RSA-Verschlüsselung als Modul $q = 221$ verwendet werden soll und dass der öffentliche Schlüssel $e = 5$ ist. Daraufhin teilt Anita ihr verschlüsseltes Alter mit: 27.

Wie alt ist Anita?

Bei dieser Aufgabe müssen Sie nicht alle Rechnungen von Hand machen; geben Sie aber Ihren Rechenweg und Zwischenergebnisse an.