

Übungsblatt 12.

Name

Aufgabe	1	2	3	4	Σ
Punkte					

Übungsgruppe (Name des Tutors)

Abgabetermin: **Montag, 05.02.2024, 14:00 Uhr.**

Bitte verwenden Sie bei Abgabe in Papierform diese Seite als Deckblatt und tragen Sie oben Ihren Matrikel-Nr. und Ihre Übungsgruppe ein. Bitte heften Sie die Blätter zusammen.

Aufgabe 1. Bestimmen Sie alle erzeugenden Elemente von $(\mathbb{Z}/17\mathbb{Z})^*$ und von $(\mathbb{Z}/19\mathbb{Z})^*$.

Aufgabe 2. Was lässt sich jeweils mithilfe der gegebenen Kongruenz und des kleinen Fermatschen Satzes über die Primalität des Modulus sagen?

(i) $5^{277} \equiv 5 \pmod{277}$ und $17^{277} \equiv 17 \pmod{277}$

(ii) $2^{1105} \equiv 2 \pmod{1105}$, $3^{1104} \equiv 1 \pmod{1105}$ und $7^{1105} \equiv 7 \pmod{1105}$

(iii) $4^{8911} \equiv 4 \pmod{8911}$, $11^{891} \equiv 11 \pmod{8911}$ und $134^{8910} \equiv 134 \pmod{8911}$

Aufgabe 3. Die folgende Chiffre wurde mit einer Vigenère-Verschlüsselung verschlüsselt. Folgen Sie dem Beispiel 6.7 auf Seite 166 und verwenden Sie die Schlüssel "krypt", um den Originaltext zu finden.

OAD CUEZDCUEAJ YME VHU EZWUYATF CUL RARIYYKBXUQLDD

Aufgabe 4. Umgekehrt kodieren Sie mit dem Schlüssel „dima“ den folgenden Satz:

Wir muessen wissen, wir werden wissen.

Wo finden wir dieses Zitat in Göttingen?