UNIVERSITÄT DES SAARLANDES

Fachrichtung Mathematik
Prof. Dr. Simon Brandhorst
Dr. Tobias Columbus

Elementare Zahlentheorie

Übungsblatt 10

Aufgabe 1 (4 Punkte)
Es sei p eine ungerade Primzahl. Zeigen Sie, dass

$$a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$$

für alle zu p teilerfremden $a \in \mathbb{Z}$.

Aufgabe 2 (4 Punkte)
Es seien $N \in \mathbb{Z}$ und $e, d \in \mathbb{Z}$ mit $e \cdot d \equiv 1 \mod \varphi(N)$.

(a) Wenn Alice die Zahlen N und e kennt, kann sie die Restklasse von m^e in $\mathbb{Z}/N\mathbb{Z}$ für jedes $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ berechnen. Wie kann Bob mit Hilfe von d aus $m^e \in \mathbb{Z}/N\mathbb{Z}$ die ursprüngliche Restklasse $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ berechnen?

(b) Alice und Bob kommunizieren nach dem Schema aus Aufgabenteil (a). Bob hat die Zahlen $N = 37 \cdot 67 = 2479$ und $e = 1645$ an Alice geschickt und die Nachricht $m^e = 2$ zurückerhalten. Welche Restklasse $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ hat Alice verschlüsselt und an Bob geschickt?

Aufgabe 3 (4 Punkte)
Berechnen Sie die letzte Ziffer von 13^{2019}.

Aufgabe 4 (4 Punkte)
Zeigen Sie, dass eine natürliche Zahl $n \geq 2$ genau dann eine Primzahl ist, wenn

$$(n-1)! \equiv -1 \mod n.$$

Abgabe bis spätestens Montag, den 17. 06. 2019, um 12:00 Uhr. Werfen Sie Ihre Lösungsvorschläge in die dafür vorgesehenen Einwurfkästen vor dem Zeichensaal in Gebäude E 2 5. Abgabe zu zweit ist möglich. Bitte geben Sie Ihren Namen, Ihre Matrikelnummer und Ihre Übungsgruppe and!