UNIVERSITÄT DES SAARLANDES

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

Elementare Zahlentheorie

Übungsblatt 14

Aufgabe 1 (2 Punkte)
Alice und Bob führen das Diffie-Hellman-Verfahren mit der Gruppe $(\mathbb{Z}/29\mathbb{Z})^\times$ aus. Sie einigen sich auf die primitive Wurzel 19 modulo 29.

Beschreiben Sie die einzelnen Schritte des Verfahrens in diesem Beispiel. Erklären Sie insbesondere, welche Informationen öffentlich und welche geheim sind.

Aufgabe 2 (2 Punkte)
Es sei $N = 221$. Berechnen Sie $64^{220} \mod N$, $103^{220} \mod N$ und $2^{220} \mod N$. Entscheiden Sie an Hand der Ergebnisse, ob N eine Primzahl sein kann.

Aufgabe 3 (4 Punkte)
Es seien $n \in \mathbb{Z}$ eine ganze Zahl, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ und $d \in \mathbb{N}$ mit $a^d = 1$. Zeigen Sie:

(a) Die Ordnung $\operatorname{ord}(a)$ von a ist ein Teiler von d.

(b) Die Ordnung $\operatorname{ord}(a)$ von a ist ein Teiler von $\varphi(n)$.

Aufgabe 4 (4 Punkte)
Es sei p eine ungerade Primzahl und $n \in \mathbb{Z}$. Zeigen Sie die beiden Aussagen

(i) Ist $n \not\equiv 1 \mod p$, so gilt

$$n^{p-1} \not\equiv 1 \mod p^2 \qquad \text{oder} \qquad (n+p)^{p-1} \not\equiv 1 \mod p^2.$$

(ii) Aus $n^{p-1} \not\equiv 1 \mod p^2$ folgt bereits, dass $n^{\varphi(p^e)} \not\equiv 1 \mod p^{e+1}$ für alle $e \in \mathbb{N}$.

und schlussfolgern Sie, dass es für alle $e \in \mathbb{N}$ eine primitive Wurzel in $\mathbb{Z}/p^e\mathbb{Z}$ gibt.

Aufgabe 5 (4 Punkte)
(a) Zeigen Sie, dass 341 eine Pseudoprimzahl zur Basis 2 ist.

(b) Es sei n eine ungerade Pseudoprimzahl zur Basis 2. Zeigen Sie, dass dann auch $2^n - 1$ eine ungerade Pseudoprimzahl zur Basis 2 ist und folgern Sie, dass es unendlich viele Pseudoprimzahlen zur Basis 2 gibt.

Abgabe bis spätestens Montag, den 15. 07. 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!