KV Einführung in die Algebra und Diskrete Mathematik

Blatt 5

29. Sei $p \in \mathbb{P}$ und seien $s, k \in \mathbb{N}_0$, sodass $p - 1 = 2^s k$ wobei k ungerade ist. Sei weiters $a \in \{1, 2, \ldots, p-1\}$. Zeigen Sie: entweder es ist $a^k \equiv 1 \pmod{p}$ oder es gibt ein $r \in \{0, \ldots, s-1\}$ mit $a^{2^r k} \equiv -1 \pmod{p}$.

30. Für das RSA-Verfahren wählen wir $p = 5$, $q = 11$ und $k = 13$. Chiffrieren Sie $(1, 3, 22, 8)$ und dechiffrieren Sie das Ergebnis.

31. Entschlüsseln Sie die Nachricht $(5, 7, 11, 13)$, $A = 1, B = 2, \ldots$, die mit $k = 13$ und $pq = 1334323339$ verschlüsselt wurde.

32. Frau Huber sendet Herrn Müller die mit dem RSA-Verfahren verschlüsselte Nachricht PMOXY. Herr Müller weiß, dass Frau Huber das RSA-Verfahren mit $n = 35$ und $k = 5$ verwendet hat (wobei $A = 0, B = 1, \ldots, Z = 25$). Entschlüsseln Sie die Nachricht.

33. Man zeige den *Satz von Wilson*: $n \in \mathbb{N}$ ist genau dann eine Primzahl, wenn $(n-1)! \equiv -1 \pmod{n}$.

34. Sei $p \in \mathbb{P}$ und sei $q \in \mathbb{P}$ ein Teiler von $2^p - 1$. Zeigen Sie, dass dann $p < q$ gilt. Bewiesen Sie damit erneut, dass es unendlich viele Primzahlen gibt.