MSG-Zirkel 9b

RSA II: Der kleine Satz von Fermat

Wir möchten den sogenannten kleinen Satz von Fermat herleiten:

Kleiner Satz von Fermat
Es sei $a \in \mathbb{Z}$ und p eine Primzahl. Dann gilt

$$a^p \equiv a \mod p.$$

Falls a und p teilerfremd sind, existiert das modulare Inverse a^{-1}, mit dem wir auf beiden Seiten multiplizieren können, so dass dann gilt:

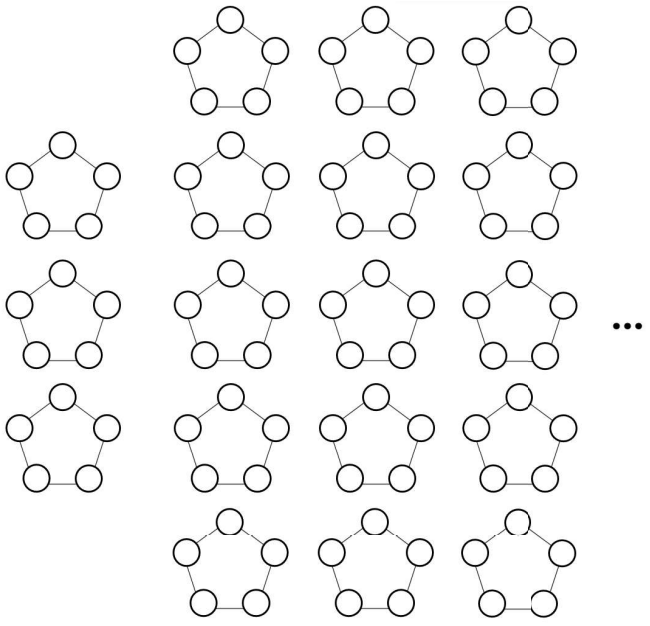
$$a^{p-1} \equiv 1 \mod p.$$

(a) Überprüfe die Gültigkeit des Satzes exemplarisch, indem du $4^7 \mod 7$ und $9^3 \mod 3$ berechnest. Warum folgt in letzterem Beispiel die zweite Aussage des Satzes nicht?

(b) Aus Perlen in $a = 3$ verschiedenen Farben soll eine geschlossene Kette mit $p = 5$ Perlen zusammengestellt werden. Auch die Perlenketten, die durch Rotation ineinander überführt werden können, zählen dabei als *verschiedene* Perlenketten.

(i) Wie viele verschiedene Perlenketten können so zusammengestellt werden?

(ii) Pierre möchte alle möglichen Perlenketten auf einer großen Werbefläche abbilden und hat schon eine Schablone angelegt. Wie könnte er die Perlenketten dabei möglichst übersichtlich sortieren?



(c)* Erkläre, wie aus der Kombination von (b) (i) und (b) (ii) der kleine Satz von Fermat hergeleitet werden kann.