

Übungen zur Vorlesung Elementare Zahlentheorie (SS 18)

PD Dr. Jürgen Müller, Dr. Martin Bender

(8.1) Aufgabe: Kleiner Satz von Fermat.

Es sei $p \in \mathbb{N}$ eine Primzahl. Man zeige den **Satz von Fermat**: Für $a \in \mathbb{Z}$ gilt $a^p \equiv a \pmod{p}$. Daraus folgere man: Ist $p \nmid a$ gilt $a^{p-1} \equiv 1 \pmod{p}$.

Hinweis. Man benutze Induktion. Wann teilt p den Binomialkoeffizienten $\binom{p}{i}$?

(8.2) Aufgabe: Satz von Wilson.

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

Mit diesem Test untersuche man $n := 89$ und $n := 91$ auf Unzerlegbarkeit. Wie verhält sich der Aufwand zur Anwendung des Siebs des Eratosthenes?

b) Nun sei $p \in \mathbb{N}$ eine Primzahl. Man zeige zunächst: Ist p ungerade, so gilt

$$\left(\binom{p-1}{2}\right)! \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Daraus folgere man: Die quadratische Kongruenz $X^2 \equiv 1 \pmod{p}$ ist immer lösbar; die quadratische Kongruenz $X^2 \equiv -1 \pmod{p}$ ist genau dann lösbar, wenn $p \not\equiv 3 \pmod{4}$ ist. Welche Lösungen gibt es jeweils?

(8.3) Aufgabe: Lineare Kongruenzen.

Man untersuche die folgenden Kongruenzen $aX \equiv b \pmod{n}$ auf Lösbarkeit in \mathbb{Z} , und bestimme gegebenenfalls alle Lösungen:

i) $a := 13, b := 32, n := 35$,

ii) $a := 33, b := 15, n := 273$,

iii) $a := 51, b := 35, n := 119$.

(8.4) Aufgabe: Das Kokosnußproblem.

Fünf Seefahrer werden auf eine einsame Insel verschlagen, auf der es als Nahrung nur Kokosnüsse gibt. Sie sammeln eine gewisse Anzahl von Kokosnüssen am Strand an. Da sie sich gegenseitig mißtrauen, beginnt des nachts der erste von ihnen, ein Fünftel der am Strand gelagerten Kokosnüsse zu vergraben, anschließend ißt er eine auf. Später verfährt der zweite genauso mit den am Strand verbliebenen Kokosnüssen, ebenso der dritte, vierte und fünfte. Am Morgen bleibt eine durch fünf teilbare Anzahl Kokosnüsse am Strand übrig. Wieviele Kokosnüsse waren zu Beginn mindestens vorhanden?

Abgabe: 14.06.2018 (Donnerstag), bis 10:00 Uhr.