

Zahlentheorie

Übung, LVA 405.031
C. Fuchs, I. Vukusic

12. Übungsblatt, SS 2022

17.06.2022

1. Berechne alle Einheiten und Nullteiler in \mathbb{Z}_{36} . Handelt es sich um einen Körper?
2. Zeige, dass $a^l a^m = a^{l+m}$ und $(a^l)^m = a^{lm}$ für alle $l, m \in \mathbb{Z}$ und alle $a \in \mathbb{Z}_n^\times$ gilt.
3. a) Sei p eine ungerade Primzahl. Zeige, dass die Gleichung $x^2 = 1$ in \mathbb{Z}_p nur die Lösungen $x = 1$ bzw. $x = -1$ besitzt. Folgere durch Zusammenfassung der zueinander inversen Zahlen, dass $(p-1)! \equiv -1 \pmod{p}$ gilt.
b) Sei p eine Primzahl mit $p \equiv 1 \pmod{4}$. Zeige, dass $x = ((p-1)/2)!$ die Gleichung $x^2 \equiv -1 \pmod{p}$ erfüllt.
4. Man kann den kleinen Satz von Fermat verwenden, um einen "Primzahltest" zu basteln: Ist nämlich für eine ganze Zahl $a^n \not\equiv a \pmod{n}$, so ist n sicher keine Primzahl. Zeige damit, dass 86146913 keine Primzahl ist.
5. Eine zusammengesetzte Zahl n heißt eine Carmichael-Zahl, wenn für alle zu n teilerfremden Basen a gilt $a^{n-1} \equiv 1 \pmod{n}$. Teste, ob 645 bzw. 1105 eine Carmichael-Zahl ist.