

Sei R ein nullteilerfreier Hauptidealring. Für eine Primzahl p ist $\mathbb{F}_p = \mathbb{Z}/(p)$ der endliche Körper mit p Elementen.

1. Aufgabe: Zeigen Sie $(ab) = (a) \cap (b)$ für teilerfremde $a, b \in R$.

2. Aufgabe: Die formale Ableitung eines Polynoms $f(X) = \sum_{i=0}^n a_i X^i$ in $R[X]$ ist das Polynom $f'(X) = \sum_{i=1}^n a_i i X^{i-1}$.

(a) Zeigen Sie $(fg)' = f'g + fg'$ für Polynome $f, g \in R[X]$.

(b) Zeigen Sie für ein primes Polynom $p \in R[X]$ und ein beliebiges Polynom $f \in R[X]$:

$$p^2 | f \iff p | \text{ggT}(f, f') .$$

3. Aufgabe: Der kleine Satz von Fermat besagt

$$a^{p-1} \equiv 1 \pmod{p}$$

für alle Primzahlen p und zu p teilerfremde ganze Zahlen a . Um zu entscheiden, ob eine gegebene Zahl $n \in \mathbb{N}$ eine Primzahl ist, betrachtet man die Gleichung $a^{n-1} \equiv 1 \pmod{n}$. Ist sie für irgendein a mit $\text{ggT}(a, n) = 1$ verletzt, dann kann n keine Primzahl sein. Das ist der Fermat'sche Primzahltest.

Zeigen Sie: $n = 341$ erfüllt $a^{n-1} \equiv 1 \pmod{n}$ für $a = 2$, ist aber keine Primzahl. Man nennt 341 daher eine Fermat'sche Pseudoprimzahl.

4. Aufgabe: Für eine Primzahl $p \neq 2$ und ein $d \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2$ definiere man auf dem Vektorraum $\mathbb{F}_p \oplus \mathbb{F}_p$ eine Multiplikation durch

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1 + d x_2 y_2, x_1 y_2 + x_2 y_1) .$$

Zeigen Sie:

(a) Diese Konstruktion liefert einen endlichen Körper mit p^2 Elementen.

(b) Bestimmen Sie das Bild der Potenz $(x_1, x_2) \mapsto (x_1, x_2)^{p+1}$ in diesem Körper.