Übung Zeigen Sie, dass $a^{\frac{p}{2}} - 1$ kein Vielfaches von n ist.

Angenommen $a^{\frac{p}{2}} - 1$ ist ein Vielfaches von n, d.h.

$$a^{\frac{p}{2}} - 1 \equiv 0 \pmod n, \quad \text{bzw.} \quad a^{\frac{p}{2}} \equiv 1 \pmod n$$

Insbesondere ist dann die Periode von $f(x) = a^x \pmod n$ kleiner oder gleich $\frac{p}{2}$ $\lightning$ nach Voraussetzung ist p die Periode

Übung Zeige die Konvergenz von $\sum_{k \geq 1} \frac{k}{2^k}$

Wir verwenden das

Quotientenkriterium: Ist mit einer festen positiven Zahl $q < 1$ fast immer $\left| \frac{a_{n+1}}{a_n} \right| \leq q$,

so muss die Reihe $\sum a_n$ konvergieren (und zwar sogar absolut).

Betrachte

$$\left| \frac{a_{k+1}}{a_k} \right| = \left| \frac{\frac{k+1}{2^{k+1}}}{\frac{k}{2^k}} \right| = \frac{k+1}{2^{k+1}} \cdot \frac{2^k}{k} = \frac{k+1}{2k}$$

$$= \frac{1}{2} + \frac{1}{2k} < \frac{3}{4} \quad \text{für } k \geq 2$$

Also konvergiert die Reihe $\sum_{k \geq 1} \frac{k}{2^k}$