

Faktorisierung von Primzahlen

in konstanter Zeit

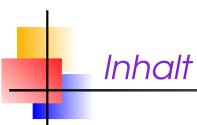
Vorname Name

mail@in.tum.de

Institut für Informatik Technische Universität München D-85748 Garching



Was sind Primzahlen



- ▶ Was sind Primzahlen
- ▶ Faktorisierungsalgorithmen für Primzahlen



Inhalt

- Was sind Primzahlen
- ▶ Faktorisierungsalgorithmen für Primzahlen
- Komplexität des Verfahrens





Theorem 1 Eine Primzahl p kann in konstanter Zeit faktorisiert werden.



Theorem 1 Eine Primzahl p kann in konstanter Zeit faktorisiert werden. **Proof.**



Theorem 1 Eine Primzahl p kann in konstanter Zeit faktorisiert werden.

Proof.

▶ Jede Primzahl p hat die eindeutige Darstellung $p = 1 \cdot p$.



Theorem 1 Eine Primzahl p kann in konstanter Zeit faktorisiert werden.

Proof.

- ▶ Jede Primzahl p hat die eindeutige Darstellung $p = 1 \cdot p$.
- lacktriangle Also ist p die Faktorisierung von p.