



Faktorisierung von Primzahlen

in konstanter Zeit

Vorname Name

`mail@in.tum.de`

Institut für Informatik
Technische Universität München
D-85748 Garching



Inhalt

▶ Was sind Primzahlen



Inhalt

- ▶ Was sind Primzahlen
- ▶ Faktorisierungsalgorithmen für Primzahlen



Inhalt

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



Hauptergebnis



Hauptergebnis

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



Hauptergebnis

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

Proof.



Hauptergebnis

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

Proof.

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



Hauptergebnis

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

Proof.

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