

## Faktorisierung großer Zahlen

- `a:=nextprime(10^14);`  
`b:=nextprime(a+1);`  
`m:=a*b;`

```
000000000000031
100000000000067
100000000000009800000000002077
```

- `Startzeit:=time();`  
`isprime(m);`  
`(time()-Startzeit)*ms;`

```
FALSE
67 ms
```

- `Startzeit:=time();`  
`ifactor(m);`  
`(time()-Startzeit)*ms;`

```
[1, 1000000000000031, 1, 1000000000000067, 1]
52129 ms
```

## Multiplikation zweier großer Primzahlen

- ⇒ Faktorisierung dauert lange  
(Ausnutzung beim RSA – Verschlüsselungsverfahren)
- ⇒ große Primzahlen für Geheimcodes
- ⇒ **SCHNELLERE PRIMZAHLTESTS**