Hintergrund: Große Primzahlen - das Miller Rabin Verfahren

Ein praktisches Problem bei der Anwendung des RSA Verfahrens ist es, die - sehr großen - Primzahlen p und q zu erhalten. RSA mit 2048 Bit Schlüssellänge verwendet momentan etwa 300-stellige Primzahlen, die man bei der Erzeugung des Schlüsselpaars zunächst möglichst zufällig "finden" muss.

Da es keine Möglichkeit gibt Primzahlen zu "berechnen", bleibt nur der Weg, eine Zufallszahl z zu erzeugen und anschließend zu überprüfen, ob diese Zufallszahl eine Primzahl ist oder nicht.

Bei einer naiven Herangehensweise muss man also prüfen, ob es eine Zahl gibt,die kleiner als die Zahl z ist und diese ohne Rest teilt:

Beispiele: Ist z=15 eine Primzahl?

```
15%2=1
15%3=0 ->Nein,keine Primzahl
```

Ist 23 eine Primzahl=?

```
23%2=1
23%3=2
23%4=3
23%5=3
23%6=5
23%7=2
23%8=7
23%9=5
...-> Ja 23 ist eine Primzahl
```

Man sieht schnell, dass dieses Verfahren auch mit Unterstützung moderner Computer bei großen Zahlen schnell an eine Grenzen stößt.