Hochschule Karlsruhe
University of
Applied Sciences

Heiko Körner

Der Miller-Rabin-Test auf Primalität

Ist das eine Primzahl? (also nur durch 1 und sich selbst teilbar)?

53113799281676709868958820655246862732959311772703192319944413820040355986085224273916250226522928566888932948624650101534657933765270723940951997876658735194383127083539321903172812 7

- Es wären mehr als 10^{89} Probedivisionen notwendig – viel zu viele!
- So können wir Zahlen nicht auf Primalität prüfen.
- Aber wie dann? 🧐

Der Test von Miller-Rabin

- Benannt nach Gary L. Miller und Michael O. Rabin
- 1976 veröffentlicht, ist bis heute der beste Test auf Primalität
- Bereits 1974 von John L. Selfridge benutzt
- Daher auch unter dem Namen Miller-Selfridge-Rabin-Test bekannt
- Funktioniert für alle ungeraden Zahlen größer oder gleich 5
- Wir bezeichnen die zu testende Zahl mit n
- Wir probieren das Verfahren an den Zahlen n = 13, 21 und 25 aus.

Schritt 1: (n – 1) so oft wie möglich halbieren

Start mit n = 13

↓ -1

12

↓ ÷2

6

↓ ÷2

3

Start mit n = 21

↓ -1

20

↓ ÷2

10

↓ ÷2

5

Start mit n = 25

↓ -1

24

↓ ÷2

12

↓ ÷2

6

↓ ÷2

3

- Wir merken uns: das ungerade Zwischenergebnis …
- … und wie oft wir durch 2 geteilt haben.

Schritt 2a: Zwischenergebnis umwandeln

Start mit 3 aus Schritt 1

↓ ganzzahlig ÷2

1

↓ ist ungerade

1

Start mit 1

↓ ×2

2

↓ +1

3

Neues Zwischenergebnis: 3

Schritt 2b: Zwischenergebnis umwandeln

Start mit 5 aus Schritt 1

↓ ganzzahlig ÷2

2

↓ ist gerade

2

↓ ganzzahlig ÷2

1

↓ ist ungerade

1

Neues Zwischenergebnis: 5

Start mit 1

↓ ×2

2

↓ nichts machen

2

↓ ×2

4

↓ +1

5

Schritt 3: Wähle eine Zufallszahl

- Die Zufallszahl nennen wir z
- Sie ist ganzzahlig und muss zwischen 2 und n – 2 liegen
- Für n = 13 muss es also eine Zahl zwischen 2 und 11 sein
- Für n = 21 muss es eine Zahl zwischen 2 und 19 sein
- Für n = 25 muss es also eine Zahl zwischen 2 und 23 sein
- Wir wählen nachfolgend einheitlich z = 7

Schritt 4a: Berechne Zwischenergebnis, hier für n = 13

Start mit 3 aus Schritt 2a

↓ ganzzahlig ÷2

1

↓ ist ungerade

1

Start mit z = 7

↓ quadrieren (mod 13)

10

↓ ×z, also hier ×7 (mod 13)

5

Neues Zwischenergebnis: 5

Schritt 4b: Berechne Zwischenergebnis, hier für n = 21

Start mit 5 aus Schritt 2b

↓ ganzzahlig ÷2

2

↓ ist gerade

2

↓ ganzzahlig ÷2

1

↓ ist ungerade

1

Neues Zwischenergebnis: 7

Start mit z = 7

↓ quadrieren (mod 21)

7

↓ nichts machen

7

↓ quadrieren (mod 21)

7

↓ ×z, also hier ×7 (mod 21)

7

Schritt 4c: Berechne Zwischenergebnis, hier für n = 25

Start mit 3 aus Schritt 2a

↓ ganzzahlig ÷2

1

↓ ist ungerade

1

Start mit z = 7

↓ quadrieren (mod 25)

24

↓ ×z, also hier ×7 (mod 25)

18

Neues Zwischenergebnis: 18

Schritt 5: Erste Vorentscheidung auf Primalität

- Test: War eines der Zwischenergebnisse aus Schritt 4 gleich 1?
- Wenn ja, dann stopp und Ausgabe „n ist eine Primzahl“
- Für n = 13 war unser Ergebnis 5 => also weitermachen
- Für n = 21 war unser Ergebnis 7 => also weitermachen
- Für n = 25 war unser Ergebnis 18 => also weitermachen

Schritt 6a: Quadriere und suche die Zahl n – 1, hier für n = 13

Start mit 5 aus Schritt 4a

↓ Test: Ist das die Zahl n – 1 = 12? Nein

↓ quadriere (mod 13)

12

↓ Test: Ist das die Zahl 12? Ja

Ausgabe: n = 13 ist eine Primzahl

Schritt 6b: Quadriere und suche die Zahl n – 1, hier für n = 21

Start mit 7 aus Schritt 4b

↓ Test: Ist das die Zahl n – 1 = 20? Nein

↓ quadriere (mod 21)

7

↓ Test: Ist das die Zahl 20? Nein

Ausgabe: n = 21 ist keine Primzahl

Schritt 6c: Quadriere und suche die Zahl n – 1, hier für n = 25

Start mit 18 aus Schritt 4c

↓ Test: Ist das die Zahl n – 1 = 24? Nein

↓ quadriere (mod 25)

24

↓ Test: Ist das die Zahl 24? Ja

Ausgabe: n = 25 ist eine Primzahl

Oh nein 😖 …. der Miller-Rabin-Test liefert hier ein falsches Ergebnis!
Was ist passiert?

Das Ergebnis hängt von der gewählten Zufallszahl z ab

Tabelle mit den Ergebnissen für n = 25:

z	Ergebnis	z	Ergebnis	z	Ergebnis
2	Keine Primzahl	3	Keine Primzahl	4	Keine Primzahl
5	Keine Primzahl	6	Keine Primzahl	7	Primzahl
8	Keine Primzahl	9	Keine Primzahl	10	Keine Primzahl
11	Keine Primzahl	12	Keine Primzahl	13	Keine Primzahl
14	Keine Primzahl	15	Keine Primzahl	16	Keine Primzahl
17	Keine Primzahl	18	Primzahl	19	Keine Primzahl
20	Keine Primzahl	21	Keine Primzahl	22	Keine Primzahl
23	Keine Primzahl				

Eigenschaften des Miller-Rabin-Tests

- Die Ausgabe „n ist keine Primzahl“ ist immer richtig
- Die Ausgabe „n ist eine Primzahl“ stimmt beweisbar zu mindestens 75%
- Führe den Test im Fall „n ist eine Primzahl“ mehrmals durch
- 10 oder 20 Tests reichen sicherlich aus …

Vielen Dank!