Primzahlentests

L. Schmidt A. Schlager

PLUS

Jänner 2024

Inhalt

Inhalt

Was sind Primzahlen?

Definition

Eine Primzahl ist eine natürliche Zahl, die genau zwei Teiler hat. Die Zahl selbst und 1.

Eigenschaften:

- Mit der Außnahme von 2 sind alle Primzahlen **ungerade**.
- Es gibt unendlich Primzahlen (Beweis durch Euklid).

Primzahlen und Primzahlentests - Wozu das alles?

Wofür benötigt man Primzahlen?

- **Kryptographie**
  - RSA Verschlüsselung
- Hashing
  - Bessere Verteilung der Werte durch Vermeidung von Mustern
- Primfaktorenzerlegung

Und weshalb Primzahlentests?

- Die Anwendungen benötigen meist sehr große Primzahlen (RSA)
- Primzahlen sind schwer zu erkennen, besonders wenn sie sehr groß sind.

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓
- 247

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓
- 247 ✗ $247 \div 13 = 19$

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓
- 247 ✗ $247 \div 13 = 19$
- 49 331

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓
- 247 ✗ $247 \div 13 = 19$
- 49 331 ✓

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓
- 247 ✗ $247 \div 13 = 19$
- 49 331 ✓
- 203 716 791 371

Primzahlen Spiel

Welche Zahl ist eine Primzahl?

- 17 ✓
- 247 ✗ $247 \div 13 = 19$
- 49 331 ✓
- 203 716 791 371 ...?

Inhalt

Probedivision

Benötigt eine Liste aller Primzahlen, die kleiner oder gleich $\sqrt{n}$ sind.

Algorithmus

Sei die zu testende Zahl $n > 1$.

1. Teste, ob eine der Primzahlen n teilt.
2. Falls eine Primzahl n teilt, so ist n keine Primzahl.
3. Falls keine der Primzahlen kleiner oder gleich $\sqrt{n}$ die Zahl teilt, so ist n eine Primzahl.

Inhalt

Sieb des Eratosthenes

- Algorithmus ist schon vor Eratosthenes aus dem 3. Jahrhundert. v. Chr. bekannt gewesen.
- Wird verwendet zur Bestimmung **aller Primzahlen** bis zu einer gewünschten Zahl N.
- Sehr langsam für große Primzahlen, nicht für Kryptographie geeignet.
- Optimierung: Sieb von Aktin.

Algorithmus

1. Erstelle eine Tabelle aller Zahlen von 2 bis N und eine leere Liste für die Primzahlen.
2. Starte bei 2.
3. Füge die Zahl der Liste hinzu.
4. Markiere alle Vielfachen als **nicht-prim**.
5. Gehe zur nächsten nicht markierten Zahl.
6. Wiederhole Schritte 3-5, bis die Zahl größer ist als $\sqrt{N}$.
7. Füge alle nicht markierten Zahlen der Primzahlenliste hinzu.

Optimierung: Es genügt beim Markieren der Vielfachen beim Quadrat der Primzahl zu beginnen.

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100:

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3,5

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3,5

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3,5,7

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3,5,7

Beispiel

-	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primzahlen ≤ 100: 2,3,5,7,11,13,17,19,23,29,31,37,
41,43,47,53,59,61,67,71,73,79,83,89,97

Inhalt

Miller-Rabin-Test

Allgemeines:

- Gary L. Miller, Michael O. Rabin (1976)
- **probabilistischer** Primzahlentest
- Go-to Algorithmus in der Kryptographie

Eingabe:

- zutestendes ungerades $n \in \mathbb{N}$, $n \geq 5$
- $a \in \{2, 3, \ldots, n-2\}$ (zufällig gewählt)

Ausgabe:

- **zusammengesetzt** oder **wahrscheinlich prim**

Die Fehlerwahrscheinlichkeit beträgt bei k Läufen des Tests: $\left(\frac{1}{4}\right)^k$.

Kleiner Satz von Fermat

Theorem (Kleiner Satz von Fermat)

Sei $a \in \mathbb{N}$ beliebig und $p \in \mathbb{N}$ eine Primzahl, so gilt:

$$a^p \equiv a \pmod{p}.$$

Falls p kein Teiler von a ist, folgt weiters:

$$a^{p-1} \equiv 1 \pmod{p}$$

für alle $1 \leq a \leq p-1$.

Fermatscher Primzahlentest

Algorithmus

Wähle ein beliebiges a mit $2 \leq a < p$ und berechne $a^{p-1} \pmod{p}$. Es gibt 2 Fälle:

1. Es kommt nicht 1 raus $\Longrightarrow$ p ist keine Primzahl.
2. Es kommt 1 raus $\Longrightarrow$ könnte prim sein.

Ist das Ergebnis wiederholt 1 mit verschiedenen Werten für a, so ist die Aussage *wahrscheinlich prim*.

$n = 337$

a	$a^{n-1} \bmod n$
15	1
73	1
101	1

$n = 15$

a	$a^{n-1} \bmod n$
4	1
6	6

Fermatscher Primzahlentest

Algorithmus

Wähle ein beliebiges a mit $2 \leq a < p$ und berechne $a^{p-1} \pmod{p}$. Es gibt 2 Fälle:

1. Es kommt nicht 1 raus $\Longrightarrow$ p ist keine Primzahl.
2. Es kommt 1 raus $\Longrightarrow$ könnte prim sein.

Ist das Ergebnis wiederholt 1 mit verschiedenen Werten für a, so ist die Aussage *wahrscheinlich prim* $\longrightarrow$ **Problem**: Carmichael Zahlen.

$n = 337$

a	$a^{n-1} \bmod n$
15	1
73	1
101	1

$n = 15$

a	$a^{n-1} \bmod n$
4	1
6	6

$n = 561$

a	$a^{p-1} \bmod n$
15	1
73	1
101	1

Funktionsweise

Lemma

Sei $p \in \mathbb{N}$ prim, dann hat die Kongruenz $x^2 \equiv_p 1$ genau zwei Lösungen: $x \equiv_p 1$ oder $x \equiv_p -1$.

Die Kongruenz $x^2 \equiv_p 1$ ist äquivalent zu $x^2 - 1 \equiv_p 0$. Daraus folgt:

$$
\begin{aligned}
& p \mid (x^2 - 1) \\
\Longrightarrow\ & p \mid (x-1)(x+1) \\
\Longrightarrow\ & p \mid (x-1) \text{ oder } p \mid (x+1) && \text{(Lemma Euklid)} \\
\Longrightarrow\ & x \equiv_p 1 \text{ oder } x \equiv_p -1
\end{aligned}
$$

Miller-Rabin-Test: Algorithmus

Algorithmus

1. Berechne d (ungerade) und j so, dass

$$n - 1 = 2^j \cdot d.$$

2. Prüfe ob entweder

$$a^d \equiv 1 \pmod{n} \quad \text{oder} \quad a^{d \cdot 2^r} \equiv -1 \pmod{n}$$

gilt, wobei $0 \leq r < j$.

Primzahlen bestehen diesen Test **immer**.

Beispiel

Wir testen $n = 337$.

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$

Beispiel

Wir testen $n = 337$.

Schritt 1 $n - 1 = 2^j \cdot d$

Bestimme d, j:

$$n - 1 = 336$$

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$

Schritt 1 $n - 1 = 2^j \cdot d$

Bestimme d, j:

$$336 \div 2 = 168$$
$$168 \div 2 = 84$$
$$84 \div 2 = 42$$
$$42 \div 2 = 21$$

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$

Schritt 1 $n - 1 = 2^j \cdot d$

Bestimme d, j:

$$336 \div 2 = 168$$
$$168 \div 2 = 84$$
$$84 \div 2 = 42$$
$$42 \div 2 = 21$$

$d = 21$ und $j = 4$.

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181				

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85			

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148		

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148	-1	

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148	-1	1

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148	-1	1
18	148	-1	1	1

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148	-1	1
18	148	-1	1	1
84	-1	1	1	1

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148	-1	1
18	148	-1	1	1
84	-1	1	1	1
16	1	1	1	1

Beispiel

Wir testen $n = 337$.

$$n - 1 = 336$$
$$d = 21$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}
181	85	148	-1	1
18	148	-1	1	1
84	-1	1	1	1
16	1	1	1	1

Der Test war für 4 verschiedenen a erfolgreich. Somit ist die Aussage *wahrscheinlich prim* zu $\geq 99\%$.

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}	$a^{16d} = a^{n-1}$
181					1

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}	$a^{16d} = a^{n-1}$
181	430				1

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}	$a^{16d} = a^{n-1}$
181	430	331			1

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}	$a^{16d} = a^{n-1}$
181	430	331	166		1

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}	$a^{16d} = a^{n-1}$
181	430	331	166	67	1

Beispiel

Wir testen $n = 561$.

$$n - 1 = 560$$
$$d = 35$$
$$j = 4$$

Schritt 2 $a^d \equiv_n 1$ oder $a^{2^r \cdot d} \equiv_n -1$:

a	a^d	a^{2d}	a^{4d}	a^{8d}	$a^{16d} = a^{n-1}$
181	430	331	166	67	1

Der Test war nicht erfolgreich. Somit ist die Aussage *nicht prim* zu 100%.

Ist nun 203 716 791 371 eine Primzahl?!

Ist nun $203\,716\,791\,371$ eine Primzahl?!

Ja!
zu $> 99\%$

Inhalt

Anwendung von Primzahlentests - RSA

Was ist RSA?

- Asymmetrisches Verschlüsselungsverfahren
  - Public und Private Key
- Benötigt Primzahlen, die **mehrere 100 Stellen** lang sind.
- Verwendet klassischerweise den Miller-Rabin-Test zum Testen von **großen Primzahlen**.
- Sicherheit beruht darauf, dass kein schnelles Verfahren einer Primfaktorenzerlegung für große Zahlen bekannt ist.
- Die Fehlerwahrscheinlichkeit von Miller-Rabin ist für RSA vernachlässigbar.

RSA - Ablauf

1. Mit Hilfe von Miller-Rabin werden 2 große Primzahlen p, q bestimmt.

RSA - Ablauf

1. Mit Hilfe von Miller-Rabin werden 2 große Primzahlen p, q bestimmt.
2. $N = p \cdot q$

RSA - Ablauf

1. Mit Hilfe von Miller-Rabin werden 2 große Primzahlen p, q bestimmt.
2. $N = p \cdot q$
3. $\varphi(N) = (p-1)(q-1)$ (Die Anzahl der teilerfremden Zahlen zu N, die kleiner N sind.)

RSA - Ablauf

1. Mit Hilfe von Miller-Rabin werden 2 große Primzahlen p, q bestimmt.
2. $N = p \cdot q$
3. $\varphi(N) = (p-1)(q-1)$ (Die Anzahl der teilerfremden Zahlen zu N, die kleiner N sind.)
4. Wähle e teilerfremd zu $\varphi(N)$.

RSA - Ablauf

1. Mit Hilfe von Miller-Rabin werden 2 große Primzahlen p, q bestimmt.
2. $N = p \cdot q$
3. $\varphi(N) = (p-1)(q-1)$ (Die Anzahl der teilerfremden Zahlen zu N, die kleiner N sind.)
4. Wähle e teilerfremd zu $\varphi(N)$.
5. Bestimme d so, dass $d \cdot e \equiv_{\varphi(N)} 1$. (Multiplikatives Invers)

RSA - Ablauf

1. Mit Hilfe von Miller-Rabin werden 2 große Primzahlen p, q bestimmt.
2. $N = p \cdot q$
3. $\varphi(N) = (p-1)(q-1)$ (Die Anzahl der teilerfremden Zahlen zu N, die kleiner N sind.)
4. Wähle e teilerfremd zu $\varphi(N)$.
5. Bestimme d so, dass $d \cdot e \equiv_{\varphi(N)} 1$. (Multiplikatives Invers)

Öffentlicher Schlüssel:	Privater Schlüssel:
(N, e)	(d)

Vielen Dank für eure Aufmerksamkeit!