







“Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört, ... ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren (...). Trotzdem muss man gestehen, dass alle bisher angegebenen Methoden entweder auf sehr spezielle Fälle beschränkt oder so mühsam sind, dass sie (...) auf größere Zahlen aber meistens kaum angewandt werden können. Aus diesem Grund und wegen der Würde der Wissenschaft ist es nötig, dass alle Hilfsmittel zur Lösung eines so eleganten und berühmten Problems mit allem Fleiß verfeinert werden.”

Naiv: Ein **Algorithmus** ist eine Menge von Instruktionen, die konkrete Eingaben in bestimmte Ausgaben verarbeiten.

**Eingabe:** eine natürliche Zahl  $n$ .  
**Ausgabe:** 1 (ja) oder 0 (nein).  
**Eingabegröße:**  $\log n \approx$  die Anzahl von Ziffern in  $n$ .

Naiv: Ein **Algorithmus** ist eine Menge von Instruktionen, die konkrete Eingaben in bestimmte Ausgaben verarbeiten.

**Eingabe:** eine natürliche Zahl  $n$ .  
**Ausgabe:** 1 (ja) oder 0 (nein).  
**Eingabegröße:**  $\log n \approx$  die Anzahl von Ziffern in  $n$ .

Ein Algorithmus heißt **polynomial** (in der Zeit), wenn ein Polynom  $\mathbf{P}(x)$  existiert, so dass der Algorithmus nach  $\mathbf{P}(\text{Eingabegröße})$  Bit-Operationen endet.

Naiv: Ein **Algorithmus** ist eine Menge von Instruktionen, die konkrete Eingaben in bestimmte Ausgaben verarbeiten.

**Eingabe:** eine natürliche Zahl  $n$ .  
**Ausgabe:** 1 (ja) oder 0 (nein).  
**Eingabegröße:**  $\log n \approx$  die Anzahl von Ziffern in  $n$ .

Ein **polynomialer** Algorithmus endet in der Zeit  $\mathbf{P}(\log n)$ .

Ein **exponentialer** Algorithmus endet in der Zeit  $c^{\log n}$ .

Naiv: Ein **Algorithmus** ist eine Menge von Instruktionen, die konkrete Eingaben in bestimmte Ausgaben verarbeiten.

**Eingabe:** eine natürliche Zahl  $n$ .  
**Ausgabe:** 1 (ja) oder 0 (nein).  
**Eingabegröße:**  $\log n \approx$  die Anzahl von Ziffern in  $n$ .

Ein **polynomialer** Algorithmus endet in der Zeit  $\mathbf{P}(\log n)$ .

Ein **exponentialer** Algorithmus endet in der Zeit  $c^{\log n}$ .

Ein **deterministischer** Algorithmus (im Gegensatz zu einem **probabilistischen** Algorithmus) verwendet in seinem Ablauf keine Zufallszahlen.

Ob ein **polynomialer deterministischer Algorithmus** existiert, der erkennt, ob eine gegebene Zahl eine Primzahl ist?

Ob ein **polynomialer deterministischer Algorithmus** existiert, der erkennt, ob eine gegebene Zahl eine Primzahl ist?

$$n = \lceil \pi \cdot 10^{37} \rceil = 31415926535897932384626433832795028841$$

$$\lceil \log n \rceil = 38$$

Können wir in 38 Bit-Operationen erkennen, ob  $n \in \mathbf{Prim}$  ist?

Können wir in  $38^2$  Bit-Operationen erkennen, ob  $n \in \mathbf{Prim}$  ist?

...

**Kleiner Fermatscher Satz (1640).** Sei  $p$  eine Primzahl.  
Dann gilt für alle zu  $p$  teilerfremden Zahlen  $a$

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

**Kleiner Fermatscher Satz (1640).** Sei  $p$  eine Primzahl. Dann gilt für alle zu  $p$  teilerfremden Zahlen  $a$

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

**Definition.** Eine zusammengesetzte Zahl  $n$  heißt Carmichaelzahl, wenn für alle zu  $n$  teilerfremden Zahlen  $a$  gilt

$$a^{n-1} \equiv 1 \pmod{n}.$$

**Kleiner Fermatscher Satz (1640).** Sei  $p$  eine Primzahl. Dann gilt für alle zu  $p$  teilerfremden Zahlen  $a$

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

**Definition.** Eine zusammengesetzte Zahl  $n$  heißt Carmichaelzahl, wenn für alle zu  $n$  teilerfremden Zahlen  $a$  gilt

$$a^{n-1} \equiv 1 \pmod{n}.$$

**Beispiel.**  $n = 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361$ .

**Korselt (1899).** Eine ungerade  $n$  ist eine Carmichaelzahl  $\Leftrightarrow$

- $n = p_1 p_2 \dots p_r$ , wobei  $p_i$  verschiedene Primzahlen sind;
- $(p_i - 1) | (n - 1) \quad \forall i$ .

**Korselt (1899).** Eine ungerade  $n$  ist eine Carmichaelzahl  $\Leftrightarrow$

- $n = p_1 p_2 \dots p_r$ , wobei  $p_i$  verschiedene Primzahlen sind;
- $(p_i - 1) | (n - 1) \quad \forall i$ .

**Beispiel.**  $561 = 3 \cdot 11 \cdot 17$ ;

$$2, 10, 16 \mid 560.$$

**Alford, Granville, Pomerance (1994).**

Sei  $C(n)$  die Anzahl der Carmichaelzahlen unterhalb  $n$ . Dann gilt für alle groß genug  $n$

$$C(n) > n^{2/7}.$$

**Alford, Granville, Pomerance (1994).**

Sei  $C(n)$  die Anzahl der Carmichaelzahlen unterhalb  $n$ . Dann gilt für alle groß genug  $n$

$$C(n) > n^{2/7}.$$

**Hypothese (Erdős).** Für alle  $\epsilon > 0$  existiert  $n_0(\epsilon)$ :

$$C(n) > n^{1-\epsilon}$$

für alle  $n > n_0(\epsilon)$ .

**Alford, Granville, Pomerance (1994).**

Sei  $C(n)$  die Anzahl der Carmichaelzahlen unterhalb  $n$ . Dann gilt für alle groß genug  $n$

$$C(n) > n^{2/7}.$$

**Hypothese (Erdős).** Für alle  $\epsilon > 0$  existiert  $n_0(\epsilon)$ :

$$C(n) > n^{1-\epsilon}$$

für alle  $n > n_0(\epsilon)$ .

**Hypothese (Erdős, Pomerance).**

$$C(n) > n^{1-(1+o(1)) \ln \ln \ln x / \ln \ln x}.$$

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Beobachtung.** Wenn  $n \in \mathbf{Prim}$  ist, dann ist für alle  $a \in \mathbb{Z}_n^*$  einer der Faktoren durch  $n$  teilbar.

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller G.L. (1976).**  $n \in \mathbf{Prim} \Leftrightarrow$  für alle  $a \in \mathbb{Z}_n^*$  ist einer der Faktoren durch  $n$  teilbar.

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller G.L. (1976).** Modulo Erweiterte Riemannsche Vermutung gilt:

$n \in \mathbf{Prim} \Leftrightarrow$  für alle Primzahlen  $a < 2(\log n)^2$  ist einer der Faktoren durch  $n$  teilbar.

Laufzeit:  $O((\log n)^3)$

Sei  $m \in \mathbb{N}$ .

**Charakter modulo  $m$**  ist eine Abbildung  $\chi : \mathbb{Z} \rightarrow \mathbb{C}$  mit folgenden Eigenschaften:

- 1)  $\chi(a) = 0 \Leftrightarrow \mathbf{ggT}(a, m) > 1$ ,
- 2)  $\chi(a + m) = \chi(a)$ ,
- 3)  $\chi(ab) = \chi(a)\chi(b)$ .

**Dirichletsche  $L$ -Function** zum Character  $\chi$ :

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

**Erweiterte Riemannsche Vermutung:** Die Nullstellen von  $L(\chi, s)$  in dem Streifen  $0 < \operatorname{Re} s < 1$  liegen auf der Geraden  $\operatorname{Re} s = 1/2$ .

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller G.L. (1976).** Modulo Erweiterte Riemannsche Vermutung gilt:

$n \in \mathbf{Prim} \Leftrightarrow$  für alle Primzahlen  $a < 2(\log n)^2$  ist einer der Faktoren durch  $n$  teilbar.

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller G.L. (1976).**  $n \in \mathbf{Prim} \Leftrightarrow$  für alle  $a \in \mathbb{Z}_n^*$  ist einer der Faktoren durch  $n$  teilbar.

|                 | mod $n$ |
|-----------------|---------|
| $a^{n-1}$       | 1       |
| $a^{(n-1)/2}$   | -1      |
| $a^{(n-1)/4}$   | *       |
| $a^{(n-1)/8}$   | *       |
| ...             | ...     |
| $a^{(n-1)/2^t}$ | *       |

|                 | mod $n$ |
|-----------------|---------|
| $a^{n-1}$       | 1       |
| $a^{(n-1)/2}$   | 1       |
| $a^{(n-1)/4}$   | -1      |
| $a^{(n-1)/8}$   | *       |
| ...             | ...     |
| $a^{(n-1)/2^t}$ | *       |

|                 | mod $n$ |
|-----------------|---------|
| $a^{n-1}$       | 1       |
| $a^{(n-1)/2}$   | 1       |
| $a^{(n-1)/4}$   | 1       |
| $a^{(n-1)/8}$   | -1      |
| ...             | ...     |
| $a^{(n-1)/2^t}$ | *       |

|                 | mod $n$ |
|-----------------|---------|
| $a^{n-1}$       | 1       |
| $a^{(n-1)/2}$   | 1       |
| $a^{(n-1)/4}$   | 1       |
| $a^{(n-1)/8}$   | 1       |
| $\dots$         | $\dots$ |
| $a^{(n-1)/2^t}$ | -1      |

|                 | mod $n$ |
|-----------------|---------|
| $a^{n-1}$       | 1       |
| $a^{(n-1)/2}$   | 1       |
| $a^{(n-1)/4}$   | 1       |
| $a^{(n-1)/8}$   | 1       |
| ...             | ...     |
| $a^{(n-1)/2^t}$ | 1       |

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller G.L. (1976).**  $n \in \mathbf{Zusg} \Leftrightarrow$  existiert  $a \in \mathbb{Z}_n^*$ , so dass keiner der Faktoren durch  $n$  teilbar ist.

|                    | mod 561 |
|--------------------|---------|
| $101^{561-1}$      | 1       |
| $101^{(561-1)/2}$  | 1       |
| $101^{(561-1)/4}$  | 1       |
| $101^{(561-1)/8}$  | 1       |
| $101^{(561-1)/16}$ | -1      |

|                    | mod 3 | mod 11 | mod 17 | mod 561 |
|--------------------|-------|--------|--------|---------|
| $101^{561-1}$      | 1     | 1      | 1      | 1       |
| $101^{(561-1)/2}$  | 1     | 1      | 1      | 1       |
| $101^{(561-1)/4}$  | 1     | 1      | 1      | 1       |
| $101^{(561-1)/8}$  | 1     | 1      | 1      | 1       |
| $101^{(561-1)/16}$ | -1    | -1     | -1     | -1      |

|                  | mod 3 | mod 11 | mod 17 | mod 561 |
|------------------|-------|--------|--------|---------|
| $2^{561-1}$      | 1     | 1      | 1      | 1       |
| $2^{(561-1)/2}$  | 1     | 1      | 1      | 1       |
| $2^{(561-1)/4}$  | 1     | 1      | -1     | 67      |
| $2^{(561-1)/8}$  | 1     | 1      | 13     | 166     |
| $2^{(561-1)/16}$ | -1    | -1     | 8      | 263     |

|                  | mod 3 | mod 11 | mod 17 |
|------------------|-------|--------|--------|
| $2^{561-1}$      | 1     | 1      | 1      |
| $2^{(561-1)/2}$  | 1     | 1      | 1      |
| $2^{(561-1)/4}$  | 1     | 1      | -1     |
| $2^{(561-1)/8}$  | 1     | 1      | *      |
| $2^{(561-1)/16}$ | -1    | -1     | *      |

|                  | mod 3 | mod 11 | mod 17 |
|------------------|-------|--------|--------|
| $5^{561-1}$      | 1     | 1      | 1      |
| $5^{(561-1)/2}$  | 1     | 1      | -1     |
| $5^{(561-1)/4}$  | 1     | 1      | *      |
| $5^{(561-1)/8}$  | 1     | 1      | *      |
| $5^{(561-1)/16}$ | -1    | 1      | *      |

|                  | mod 3 | mod 11 | mod 17 |
|------------------|-------|--------|--------|
| $7^{561-1}$      | 1     | 1      | 1      |
| $7^{(561-1)/2}$  | 1     | 1      | -1     |
| $7^{(561-1)/4}$  | 1     | 1      | *      |
| $7^{(561-1)/8}$  | 1     | 1      | *      |
| $7^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $13^{561-1}$      | 1     | 1      | 1      |
| $13^{(561-1)/2}$  | 1     | 1      | 1      |
| $13^{(561-1)/4}$  | 1     | 1      | 1      |
| $13^{(561-1)/8}$  | 1     | 1      | -1     |
| $13^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $19^{561-1}$      | 1     | 1      | 1      |
| $19^{(561-1)/2}$  | 1     | 1      | 1      |
| $19^{(561-1)/4}$  | 1     | 1      | -1     |
| $19^{(561-1)/8}$  | 1     | 1      | *      |
| $19^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $23^{561-1}$      | 1     | 1      | 1      |
| $23^{(561-1)/2}$  | 1     | 1      | -1     |
| $23^{(561-1)/4}$  | 1     | 1      | *      |
| $23^{(561-1)/8}$  | 1     | 1      | *      |
| $23^{(561-1)/16}$ | -1    | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $29^{561-1}$      | 1     | 1      | 1      |
| $29^{(561-1)/2}$  | 1     | 1      | -1     |
| $29^{(561-1)/4}$  | 1     | 1      | *      |
| $29^{(561-1)/8}$  | 1     | 1      | *      |
| $29^{(561-1)/16}$ | -1    | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $31^{561-1}$      | 1     | 1      | 1      |
| $31^{(561-1)/2}$  | 1     | 1      | -1     |
| $31^{(561-1)/4}$  | 1     | 1      | *      |
| $31^{(561-1)/8}$  | 1     | 1      | *      |
| $31^{(561-1)/16}$ | 1     | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $37^{561-1}$      | 1     | 1      | 1      |
| $37^{(561-1)/2}$  | 1     | 1      | -1     |
| $37^{(561-1)/4}$  | 1     | 1      | *      |
| $37^{(561-1)/8}$  | 1     | 1      | *      |
| $37^{(561-1)/16}$ | 1     | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $41^{561-1}$      | 1     | 1      | 1      |
| $41^{(561-1)/2}$  | 1     | 1      | -1     |
| $41^{(561-1)/4}$  | 1     | 1      | *      |
| $41^{(561-1)/8}$  | 1     | 1      | *      |
| $41^{(561-1)/16}$ | -1    | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $43^{561-1}$      | 1     | 1      | 1      |
| $43^{(561-1)/2}$  | 1     | 1      | 1      |
| $43^{(561-1)/4}$  | 1     | 1      | -1     |
| $43^{(561-1)/8}$  | 1     | 1      | *      |
| $43^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $47^{561-1}$      | 1     | 1      | 1      |
| $47^{(561-1)/2}$  | 1     | 1      | 1      |
| $47^{(561-1)/4}$  | 1     | 1      | 1      |
| $47^{(561-1)/8}$  | 1     | 1      | -1     |
| $47^{(561-1)/16}$ | -1    | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $53^{561-1}$      | 1     | 1      | 1      |
| $53^{(561-1)/2}$  | 1     | 1      | 1      |
| $53^{(561-1)/4}$  | 1     | 1      | -1     |
| $53^{(561-1)/8}$  | 1     | 1      | *      |
| $53^{(561-1)/16}$ | -1    | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $59^{561-1}$      | 1     | 1      | 1      |
| $59^{(561-1)/2}$  | 1     | 1      | 1      |
| $59^{(561-1)/4}$  | 1     | 1      | -1     |
| $59^{(561-1)/8}$  | 1     | 1      | *      |
| $59^{(561-1)/16}$ | -1    | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $61^{561-1}$      | 1     | 1      | 1      |
| $61^{(561-1)/2}$  | 1     | 1      | -1     |
| $61^{(561-1)/4}$  | 1     | 1      | *      |
| $61^{(561-1)/8}$  | 1     | 1      | *      |
| $61^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $67^{561-1}$      | 1     | 1      | 1      |
| $67^{(561-1)/2}$  | 1     | 1      | 1      |
| $67^{(561-1)/4}$  | 1     | 1      | 1      |
| $67^{(561-1)/8}$  | 1     | 1      | 1      |
| $67^{(561-1)/16}$ | 1     | 1      | -1     |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $71^{561-1}$      | 1     | 1      | 1      |
| $71^{(561-1)/2}$  | 1     | 1      | -1     |
| $71^{(561-1)/4}$  | 1     | 1      | *      |
| $71^{(561-1)/8}$  | 1     | 1      | *      |
| $71^{(561-1)/16}$ | -1    | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $73^{561-1}$      | 1     | 1      | 1      |
| $73^{(561-1)/2}$  | 1     | 1      | -1     |
| $73^{(561-1)/4}$  | 1     | 1      | *      |
| $73^{(561-1)/8}$  | 1     | 1      | *      |
| $73^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $79^{561-1}$      | 1     | 1      | 1      |
| $79^{(561-1)/2}$  | 1     | 1      | -1     |
| $79^{(561-1)/4}$  | 1     | 1      | *      |
| $79^{(561-1)/8}$  | 1     | 1      | *      |
| $79^{(561-1)/16}$ | 1     | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $83^{561-1}$      | 1     | 1      | 1      |
| $83^{(561-1)/2}$  | 1     | 1      | 1      |
| $83^{(561-1)/4}$  | 1     | 1      | -1     |
| $83^{(561-1)/8}$  | 1     | 1      | *      |
| $83^{(561-1)/16}$ | -1    | -1     | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $89^{561-1}$      | 1     | 1      | 1      |
| $89^{(561-1)/2}$  | 1     | 1      | 1      |
| $89^{(561-1)/4}$  | 1     | 1      | 1      |
| $89^{(561-1)/8}$  | 1     | 1      | -1     |
| $89^{(561-1)/16}$ | -1    | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $97^{561-1}$      | 1     | 1      | 1      |
| $97^{(561-1)/2}$  | 1     | 1      | -1     |
| $97^{(561-1)/4}$  | 1     | 1      | *      |
| $97^{(561-1)/8}$  | 1     | 1      | *      |
| $97^{(561-1)/16}$ | 1     | 1      | *      |

|                   | mod 3 | mod 11 | mod 17 |
|-------------------|-------|--------|--------|
| $89^{561-1}$      | 1     | 1      | 1      |
| $89^{(561-1)/2}$  | 1     | 1      | 1      |
| $89^{(561-1)/4}$  | 1     | 1      | 1      |
| $89^{(561-1)/8}$  | 1     | 1      | -1     |
| $89^{(561-1)/16}$ | -1    | 1      | *      |

|                    | mod 3 | mod 11 | mod 17 |
|--------------------|-------|--------|--------|
| $101^{561-1}$      | 1     | 1      | 1      |
| $101^{(561-1)/2}$  | 1     | 1      | 1      |
| $101^{(561-1)/4}$  | 1     | 1      | 1      |
| $101^{(561-1)/8}$  | 1     | 1      | 1      |
| $101^{(561-1)/16}$ | -1    | -1     | -1     |

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Beobachtung:** Sei  $n \in \mathbf{Zusg}$ . Dann ist für viele  $a \in \mathbb{Z}_n^*$  keiner der Faktoren durch  $n$  teilbar.

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Monier-Rabin (1980).** Sei  $n > 9$  eine ungerade Zahl. Dann ist  $n \in \mathbf{Zusg} \Leftrightarrow$  existieren mehr als  $\frac{3}{4}\phi(n)$  Zahlen  $a \in \mathbb{Z}_n^*$ , so dass keiner der Faktoren durch  $n$  teilbar ist.

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller-Rabin-Test(1980)** (mit einem Gang).

Wählen wir zufällig  $a \in \mathbb{Z}_n^*$ .

Falls keiner der Faktoren durch  $n$  teilbar ist, Ausgabe:

$$n \in \mathbf{Zusg}.$$

Sonst Ausgabe:  $n \in \mathbf{Prim}$  mit der Wahr.  $> \frac{3}{4}$ .

Sei  $n$  eine ungerade Zahl; schreibe  $n - 1 = m2^t$  mit  $2 \nmid m$ .

$$a^{n-1} - 1 = (a^m - 1)(a^m + 1)(a^{2m} + 1) \dots (a^{2^{t-1}m} + 1).$$

**Miller-Rabin-Test(1980).** Sei  $s$  eine natürliche Zahl. Wählen wir zufällig Zahlen  $a_1, \dots, a_s \in \mathbb{Z}_n^*$ .

Falls  $a = a_i$  existiert, so dass keiner der Faktoren durch  $n$  teilbar ist, Ausgabe:  $n \in$  **Zusg.**

Sonst Ausgabe:  $n \in$  **Prim** mit der Wahr.  $> 1 - (\frac{1}{4})^s$ .

**Der Miller-Rabin-Test  
gibt nicht immer richtige Antworten.**

Schnelle Tests, die immer richtige Antworten geben:

- **Jacobi-Summen-Test**
- **Elliptischer Kurven-Test**

- **Jacobi-Summen-Test**

**Adleman, Pomerance und Rumely (1983),  
Cohen, Lenstra (1984).**

Deterministisch, Laufzeit:  $O((\ln n)^{c \ln \ln \ln n})$ .

Es gibt eine effiziente probabilistische Version.

- **(Hyper)Elliptischer Kurven-Test**

**Goldvasser, Kilian (1986),  
Atkin, Morain (1988, 1993),  
Adleman, Huang (1992)**

Probabilistisch.

Laufzeit des Atkin-Morain-Tests: im Schnitt  $(\ln n)^6$ .

Laufzeit des Adleman-Huang-Tests:  $(\ln n)^c$ ,  $c$  ist groß.

**D.J. Bernstein**, Distinguishing prime numbers from composite numbers: the state of the art in 2004, <http://cr.yp.to/primetests.html>

- Vergleich von 21 Methoden.
- Bibliographie enthält 97 Titel.

**H. Cohen**, A course in computational algebraic number theory, Springer, 1993.

**R. Crandall, C. Pomerance**, Prime numbers. A computational perspective, Springer, 2001.

## **Polynomialer deterministischer Primzahlen-Test:**

**M. Agrawal, N. Kayal, N. Saxena**, PRIMES is in P, Annals of Mathematics, 160 (2004), 781–793.

Internet Version von 2002: <http://www.cse.iitk.ac.in/primalty.pdf>





**Binomialer Satz.** Sei  $n \in \mathbb{N}$  und  $a$  eine beliebige zu  $p$  teilerfremde Zahl. Die Zahl  $n$  ist eine Primzahl genau dann, wenn gilt

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

**Achtung:**  $x$  ist eine Unbekannte, links und rechts stehen Polynome von  $x$ .

**Binomialer Satz.** Sei  $n \in \mathbb{N}$  und  $a$  eine beliebige zu  $p$  teilerfremde Zahl. Die Zahl  $n$  ist eine Primzahl genau dann, wenn gilt

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

**Idee von AKS.** Eine “kleine” Primzahl  $r$  finden, so das gilt:  $n$  ist eine Primzahl genau dann, wenn für “alle kleinen”  $a$  gilt

$$(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)}.$$

**Binomialer Satz.** Sei  $n \in \mathbb{N}$ ,  $n > 1$ , und sei  $a$  eine beliebige zu  $p$  teilerfremde Zahl. Die Zahl  $n$  ist eine Primzahl genau dann, wenn gilt

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

**Idee von AKS.** Eine “kleine” Primzahl  $r$  finden, so dass gilt:  $n$  ist eine Primzahl genau dann, wenn für “alle kleinen”  $a$  gilt

$$(x + a)^n \equiv x^n + a \pmod{(n, x^r - 1)}.$$

**Was bedeutet klein:**  $r \leq (\log n)^5$ ,  $a < \sqrt{r} \log n$ .

**Satz von AKS.** Sei  $n > 4$  eine natürliche Zahl und sei  $r$  eine Primzahl, so dass folgende Bedingungen erfüllt sind:

- (1)  $n$  ist nicht durch die Primzahlen von 2 bis  $r$  teilbar;
- (2)  $\text{ord}_r(n) > \log^2 n$ ;
- (3)  $(x+a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$  für alle  $1 \leq a \leq \sqrt{r} \log n$ .

Dann ist  $n$  eine Potenz einer Primzahl.

**Satz von AKS.** Sei  $n > 4$  eine natürliche Zahl und sei  $r$  eine Primzahl, so dass folgende Bedingungen erfüllt sind:

- (1)  $n$  ist nicht durch die Primzahlen von 2 bis  $r$  teilbar;
- (2)  $\text{ord}_r(n) > \log^2 n$ ;
- (3)  $(x+a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$  für alle  $1 \leq a \leq \sqrt{r} \log n$ .

Dann ist  $n$  eine Potenz einer Primzahl.

**Definition.** Sei  $r$  teilerfremd zu  $n$ .

$$\text{ord}_r(n) = \min\{\alpha > 0 \mid n^\alpha \equiv 1 \pmod{r}\}.$$

**Beispiel.**  $\text{ord}_3(5) = 2$ .

**Satz von AKS.** Sei  $n > 4$  eine natürliche Zahl und sei  $r$  eine Primzahl, so dass folgende Bedingungen erfüllt sind:

- (1)  $n$  ist nicht durch die Primzahlen von 2 bis  $r$  teilbar;
- (2)  $\text{ord}_r(n) > \log^2 n$ ;
- (3)  $(x+a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$  für alle  $1 \leq a \leq \sqrt{r} \log n$ .

Dann ist  $n$  eine Potenz einer Primzahl.

**Es existiert eine Primzahl  $r \leq (\log n)^5$  mit (2).**

**Satz von AKS.** Sei  $n > 4$  eine natürliche Zahl und sei  $r$  eine Primzahl, so dass folgende Bedingungen erfüllt sind:

- (1)  $n$  ist nicht durch die Primzahlen von 2 bis  $r$  teilbar;
- (2)  $\text{ord}_r(n) > \log^2 n$ ;
- (3)  $(x+a)^n \equiv x^n + a \pmod{(x^r - 1, n)}$  für alle  $1 \leq a \leq \sqrt{r} \log n$ .

Dann ist  $n$  eine Potenz einer Primzahl.

**Es existiert eine Primzahl  $r \leq (\log n)^5$  mit (2).**

**Es existiert ein polynomialer und deterministischer Algorithmus für das Problem  $n \in \text{Prim}$ .**

Laufzeit:  $O(\log n)^6$ .

**Aufgabe 4.** a) Mit welcher Wahrscheinlichkeit erhalten wir die Antwort “ $n$  ist eine Primzahl...” im Miller-Rabin-Test für die Zahl  $n = 91$  und den Parameter  $s = 2$ ?

b) Dieselbe Frage für  $n = 561$  und  $s = 1$ .

**Aufgabe 5.** Wiederholen Sie den Miller-Rabin Test 100 Mal (unabhängig) für die Zahl 561 mit dem Parameter  $s = 1$ . Wie viele Male wird der Test die Antwort: “561 ist eine Primzahl ...” geben?